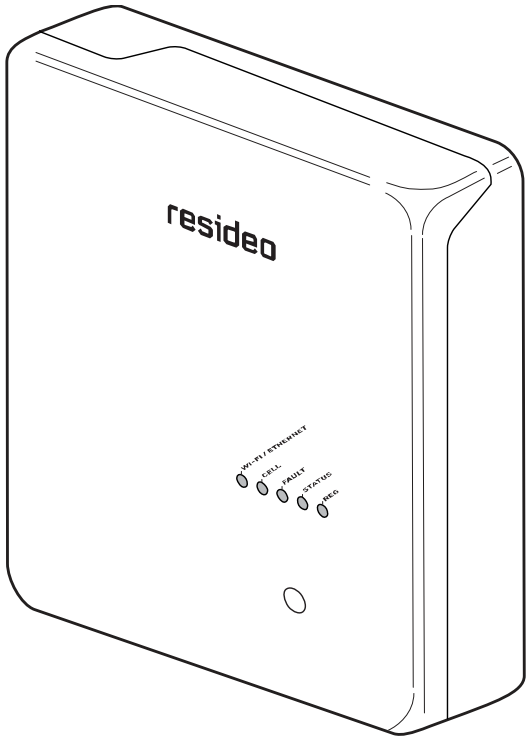
resideo

LTEM-PXV, LTEM-PXA
IP-COM

Internet and Cellular Communicators

Installation and Setup Guide



R800-27327C 12/21 Rev C

Table of Contents

General Information

System Overview

Introduction

The communicators described herein provide Internet communication via Ethernet or Wi-Fi® (Wi-Fi requires optional Wi-Fi module) and easily connect to your security system's control panel, sending alarms and messages to AlarmNet for subsequent transfer to the central monitoring station. Communicators with cell radio backup utilize the latest LTE technology specifically designed for IoT devices to communicate with AlarmNet. The LTE CAT-M1 technology (used in the LTEM-PX series) provides improved power efficiency and signal strength underground and within buildings. LTE CAT-M1 is available everywhere that current LTE networks reach with strong enough reception for consistent connections.

This manual describes the installation and programming for the communicator models listed in the table below. Procedures and information throughout the manual apply to all models unless otherwise noted.

Summary of Communicator Models

Communicator	Models	Description
LTEM-PX Series	LTEM-PXV	Verizon network. Provides Internet communication via Ethernet or optional Wi-Fi with built-in LTE CAT-M1 cell radio backup.
	LTEM-PXA	AT&T® network. Provides Internet communication via Ethernet or optional Wi-Fi with built-in LTE CAT-M1 cell radio backup.
IP-COM	IP-COM	Provides Internet-only communication via Ethernet or optional Wi-Fi.

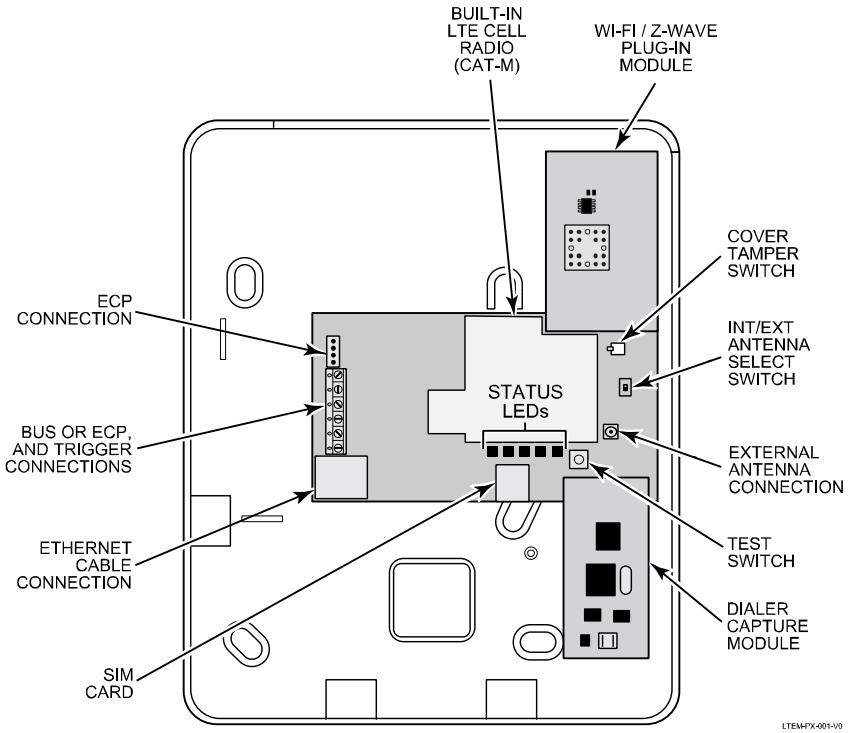
All the listed communicators support the following optional plug-in modules:

- **PROWIFIZW**: Wi-Fi/Z-Wave Module for Wi-Fi® connection to the Internet and/or for control of home automation devices
- **PROWIFI**: Wi-Fi Module for Wi-Fi® connection to the Internet
- **PRODCM**: Dialer Capture Module for connection to non-ECP control panels that send Contact ID signals for alarm reporting via the control panel's Dialer.

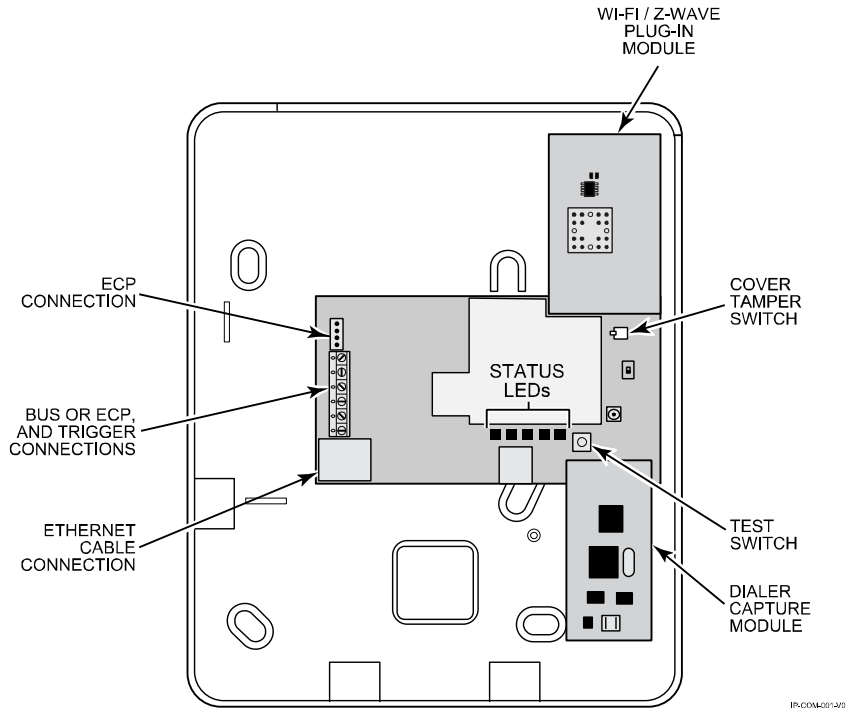
The communicator requires an AlarmNet 360 account. For new installations, please obtain the account information from the central station prior to programming this communicator. For replacement installations, the AlarmNet 360 account is created automatically when the communicator is registered.

Communicator Component Identification

Due to Resideo's continuing effort to improve our products, your device may look slightly different than pictured.



LTEM-PX Series Communicators with Built-In LTE Cell Radio
(shown with optional Wi-Fi and Dialer Capture modules)



IP-COM Internet-Only Communicator
(shown with optional Wi-Fi and Dialer Capture modules)

General Information

The communicators communicate via the Internet (when service is available). The **LTEM-PX** series communicators switch to cell service when the Internet is not available (provided the Communication Path is set to IP & Cell). The **IP-COM** communicates via the Internet only.

Connection to the Internet is made by direct Ethernet cable to the router, or via Wi-Fi® (requires use of the optional PROWIFIZW or PROWIFI module), together referred to as IP. Only one of these methods may be used (Ethernet or Wi-Fi), not both.

In normal operation (with Internet connectivity), these devices communicate from your customer's network connection to the Resideo Network Operations Center (NOC) via the AlarmNet network. The NOC receives data and routes the information to the Central Station of your choice, based on the account number you assign to the communicator. Note that your Central Station needs to give you the account number. The same account number is used for both Internet and cell transmissions. If your current Central Station is capable of receiving signals from the Resideo NOC, they are capable of receiving signals from the communicator.

If, for some reason, Internet connectivity is not available, (for example, your customer's ISP is offline or disconnected) and the Communication Path choice is set to IP & Cell, the **LTEM-PX** series communicators transmit signals via the cellular network to complete these transmissions. These transmissions are sent to the Resideo NOC and then forwarded to your Central Station the same way as if they were received via the Internet. If the Internet AND Cell network are both unavailable, the message will not be sent via these devices.

System Features

Basic features of the communicator include:

- Quick connection to Resideo control panels (e.g., most VISTA controls) and compatible non-Resideo control panels (e.g., DSC, Interlogix)
- Supports both ECP and Bus connections to compatible control panels
- Powered by the control panel's 12VDC auxiliary output
- Supports connection to the Internet via Ethernet cable or Wi-Fi® (Wi-Fi requires installation of PROWIFIZW or PROWIFI module; note that WI-FI supports DHCP [dynamic] IP addressing only, it does not support STATIC IP addressing) – only one method can be used, Ethernet or Wi-Fi, not both
- Ethernet connection supports dynamic (DHCP) or static IP addressing, and installs behind firewalls without compromising network security (provided that the Communication Path includes IP)
- Reports alarms and status messages via the Internet (LTEM-PX series communicators provide cell radio backup reporting)
- Allows uploading and downloading of VISTA control panel data
- Supports Remote Services feature, which allows the end user to access their security system from their computer via a website. Availability of this service is controlled by the dealer via the web-based programming tool on the AlarmNet 360 website
- Multi-function Test switch used to generate test messages, register the communicator with AlarmNet, enter Pairing mode (used during Wi-Fi module installation), reboot the communicator, and to reset the communicator to factory default settings.

Test Switch Functions	
Send Test Message	Short press & release
Register Communicator	Triple-click
Bluetooth Pairing Mode	Press & hold 3 secs
Reboot Communicator	Press & hold 10 secs
Reset to Factory Defaults*	Press & hold 20 secs

*** Setting Factory Defaults:** This function resets all programmed values to original factory settings and removes all Wi-Fi/Bluetooth pairings.

About AlarmNet Internet Application

AlarmNet is a fully encrypted, secure method of delivering alarm messages from a protected premise to an AlarmNet equipped central station. An Internet Communicator transmits status, supervisory, and alarm messages to the AlarmNet Control Center using a broadband Internet connection.

The AlarmNet Control Center identifies, validates, and forwards the messages to the appropriate AlarmNet central station. AlarmNet has an unlimited account capacity.

Supervision Features

The communicator provides the following types of supervision and fault detection:

- **Network communication failure**: In the event the AlarmNet network does not hear a supervisory message from the communicator within a specified time, AlarmNet notifies the central station of a communication failure.
- **Communication path failure** (applies to the **LTEM-PX** series): When the communication path is set to Ethernet & Cell or Wi-Fi & Cell, both the Central Station and the control panel can be notified of a communication path failure. Both failures are considered true faults when the respective fault times have expired ("Cell Fault Time" and "IP Fault Time" for either Wi-Fi or Ethernet options) provided it has been set to a non-zero value. Notification is sent to the central station upon this expiration. Notification to the panel is controlled by the "Notify Panel Of" option (see Programming the Communicator section).

  (**NOTE**: if the "Cell Fault Time" and "IP Fault Time" options are set to zero, faults will not be reported.)
- **Fault Trigger Output**: A fault trigger output (trigger output terminal T1) activates upon the following communicator fault conditions if alarm reporting is enabled for the condition*: tamper, power loss, and loss of network connectivity (communication path loss). The fault trigger output can serve as a fail-safe trigger (if programmed to do so) to ensure the control panel is alerted in the event of a complete communicator power loss. or if the wiring from the communicator to the control panel is cut. Refer to the "Fault Relay Normally On" option in the *Programming the Communicator* section for details.

  *Alarm reporting for the noted condition must be enabled for the condition to trigger the fault output.
- **Cover and wall tamper** condition (“Tamper Report” option).

Remote Services

Resideo offers a series of web-based services that provides consumers with the ability to communicate with their security system remotely in several ways. These web services allow users to:

- Access their security system from a computer via a website (Remote Access feature)
- Receive email and text message notifications of system events (Multi-Mode feature)

Dealers will initially enroll their customers for web services during account programming through the AlarmNet 360 website. The features that can be enabled include Remote Access and Multi-Mode. Once enabled, the specific programming options associated with these features can be programmed into the communications device using the AlarmNet 360 website or mobile app.

Refer to the Compatibility paragraph later in this section for Total Connect 2 features supported when using this communicator with a non-Resideo control panel.

Control Panel Connections

The communicator provides two types of control panel connections so it can be used with various types of control panels, as summarized below.

ECP Connection

- This connection is for Resideo VISTA control panels that support ECP communication with radios (LRR to ECP, herein referred to as ECP).

  Total Connect 2 Compatibility Note: The following VISTA control panel firmware versions support Total Connect 2 Communication (version number is located on the panel's PCB PROM label):

Control Panel	Firmware Version
VISTA-15P / VISTA-20P Family	v9.12 or higher
VISTA-21iP Family	v3.13 or higher
VISTA-128BPT Family	v10.1 or higher
VISTA-250BPT Family	v10.3 or higher

- The communicator connects to the control panel's keypad terminals (Data In, Data Out, Ground, and +12VDC) using the included 4-wire harness connector, and provides 2-way communication with the control panel using ECP messaging
- The control panel treats the communicator as an ECP device, so make sure to program the control panel with the communicator's device address (address 03 recommended)
- Reports are sent in Contact ID format.

Bus Connection

- This connection is for use with compatible control panels that do not support ECP communication
- The communicator typically connects to the control panel via RX/TX/GND/PWR+ terminal block connections; depending on the control panel used, the PRODCM module may also need to be installed
- Reports are sent in Contact ID format.

Optional Accessories

The communicators support the following plug-in modules.

Wi-Fi Module (PROWIFIZW or PROWIFI)

- If a Wi-Fi connection to the router is desired rather than an Ethernet cable connection, install the optional PROWIFIZW Wi-Fi/Z-Wave module or PROWIFI Wi-Fi only module
- The communicator can use only one Internet connection method: Ethernet or Wi-Fi, not both
- PROWIFIZW module also supports the use of Z-Wave devices for home automation.

Dialer Capture Module (PRODCM)

- An optional Dialer Capture module can be used for controls that send Contact ID alarm signals via the control panel's dialer. The alarms are then sent to AlarmNet for routing to the central monitoring station.

External Antennas

The **LTEM-PX** series communicators are equipped with an internal antenna. This feature provides additional security to the installation by making the device tamper resistant. If needed to obtain adequate signal strength, there is a connection for an external antenna. Refer to the *External Antenna* section later in this manual for details on installing the external antenna.

The following antenna kits are compatible with the **LTEM-PX** series communicators:

- CELL-ANTHB
- PROLTE-ANT
- CELLANT3DBPK

NOTE: If an external antenna is used, Adapter Cable ADPT-LTEMPX is also needed. See External Antenna section later in this manual.

Testing the System

After installation the security system should be tested. Refer to the control panel installation instructions for procedures to test the entire system.

WEEKLY TESTING IS REQUIRED TO ENSURE PROPER OPERATION OF THIS SYSTEM

Communications Test

After installation and programming, test the communication path to AlarmNet by performing a Communications Test.

To perform a Communications Test, press and release the Test switch. The communicator then sends a test message to AlarmNet via the primary communication path, which can be viewed via AlarmNet 360 to confirm that the message was successfully received. The Alarm History page shows Contact ID code E601 (manually triggered test) along with the zone number for the communicator. The communication path is also identified ("ethernet" [if Wi-Fi or ethernet is selected] or "cellular" depending on the communication path programmed).

Compatibility (Control Panels, Compass, Total Connect Features)

Control Panels: For a list of control panels that are compatible with various features of this device, go to: www.resideo.com

Compass Version: Compatible with Compass Version v2.2.35.1 (or higher) for VISTA series control panel IP/Cellular Downloading

Total Connect 2 Feature Compatibility with Non-Resideo Control Panels

Features Supported for Non-Resideo Panels	Features Not Supported for Non-Resideo Panels
• Basic security operations (arm stay, arm away, disarm) • Bypass sensors from sensors tab • Panic alarm features • Sensors alarm and alarm clear for supported zone types • Zone types supported include "Fire," "Entry/Exit," "Interior Follower with Auto bypass," and "Instant" • Multiple partitions supported • Multiple users can be created from both Total Connect and the panel (user code must already exist or need to create user code in the panel).	• Bypass clear from Total Connect is not supported • Zone type changes do not automatically sync with Total Connect; need communicator reboot to sync zone related changes with Total Connect • User sync is not supported; need communicator reboot to sync user related changes with Total Connect. • Zone descriptors are not supported (e.g., if zone 01 is assigned zone descriptor "Front Door," Total Connect displays it simply as "Zone 01").

Compliance

These devices have been tested by ETL to meet the following standards:

UL 1610 Central-Station Burglar-Alarm Units

UL 1023 Household Burglar-Alarm System Units

UL 365 Police Station Connected Burglar Alarm Units and Systems

UL 985 Household Fire Warning System Units

ANSI/SIA CP-01 Standard

IP-COM also complies with the following Canadian ULC Standards:
CAN/ULC-S304:2016 ed.3+R1 Control Units, Accessories and Receiving Equipment for Intrusion Alarm Systems
CAN/ULC-S545:2002 Ed.2 Residential Fire Warning System Control Units

Specifications

Mechanical	Dimensions: 7.3" x 9.0" x 1.7" (18.6 cm x 22.8 cm x 4.4 cm) Weight: LTEM-PXV / LTEM-PXA: 16.5 oz. (468g) IP-COM: 16.4 oz. (466g)		
Input Power	12VDC supplied by the control panel		
Current Drain with control panel input voltage	**Model**	**Input Voltage**	**Active Current (mA)**
	LTEM-PXV / -PXA with no modules	12VDC	220
	LTEM-PXV / -PXA with Wi-Fi/ZW module	12VDC	275
	LTEM-PXV / -PXA with PRODCM module	12VDC	230
	LTEM-PXV / -PXA with Wi-Fi/ZW & PRODCM modules	12VDC	310
	IP-COM with no modules	12VDC	190
	IP-COM with Wi-Fi/ZW module	12VDC	240
	IP-COM with PRODCM module	12VDC	200
	IP-COM with Wi-Fi/ZW & PRODCM modules	12VDC	275
Fault Trigger Output	Open collector, 12VDC, 0.25W max		
Ethernet	Network Standard: IEEE 802.3u compliant Data Rate: 10Base-T (10Mbps) / 100Base-T (100Mbps) with auto detect Ethernet Cable: Cat. 5 (min), MDI / MDI-X auto crossover		
Environmental	Operating temperature: 32°F to 120°F (0ºC to +49ºC) Storage temperature: -40°F to 158°F (–40ºC to +70ºC) Humidity: 0 to 95% relative humidity, non-condensing for UL installations: 0% to 85%; for ULC installations 0% to 93% Altitude: to 10,000 ft. (3,048 m) operating, to 40,000 ft. (12,192 m) storage		
Frequency Bands	LTEM-PXV: LTE Bands 4 and 13 LTEM-PXA: LTE Bands 2, 4, and 12		
Output Power	LTEM-PXV / LTEM-PXA: LTE Class 5, 20dBm (conducted)		

Mounting and Wiring

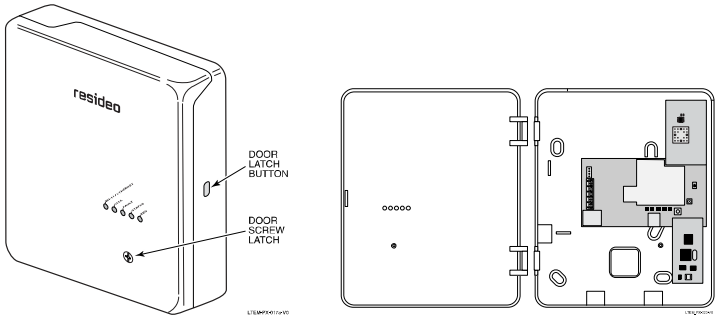
Installation Notes

- The communicator must be installed in accordance with the National Electrical Code, ANSI/NFPA 70.
- The communicator must be mounted indoors within the protected premises.
- Do not install in air-handling spaces.
- Do not mount the communicator on or near metal objects, as this may affect radio communication. It is also good practice to avoid mounting near wiring such as electrical power lines, electrical rooms, telephone, HVAC, computer data cables, etc.
- Unshielded, 22 AWG cable is recommended for the communicator power/data wires.
- Do not connect to a receptacle controlled by a switch.

Removing the Communicator's Door

1. Loosen the door screw latch.
2. Push the door latch button and open the door fully (~180°).
3. Gently push the door open further until the door slides out of the case hinges. Set the door aside.

To reattach the door, position the door hinges against the case hinges and gently push until the hinges engage.



Determining the Signal Strength to Select a Location

Signal strength applies only to the **LTEM-PX** series communicators.
Signal strength does not apply to the **IP-COM** communicator.

When choosing a suitable mounting location, understand that signal strength is very important for proper operation. For most installations using the internal antenna, mounting the unit as high as practical, and avoiding large metal components provides adequate signal strength for proper operation.

You will use the communicator to determine signal strength to find a suitable mounting location.

Initial Power Up: Upon initial power up, the communicator LEDs blink in repeated sequence from right to left indicating network initialization.
Green (REG) → Yellow (STATUS) → Red (FAULT) → Green (CELL) → Green (WI-FI / ETHERNET)
This sequence may take up to 15 minutes. **Do not reset power during this time.**
When initialization is complete, the LEDs may blink (per their respective functions).
After initial network setup, subsequent resets or power ups can take up to 90 seconds.

1. Temporarily connect power from the control panel or a 12VDC battery to the GND and +12VDC terminals on the communicator. When initial power up is complete, position the communicator near a suitable mounting location.
2. Choose the installation site with the best signal quality by observing the Cell LED. If lit, signal strength is acceptable. The best signal strength is usually found at the highest point in the building, near a window.
3. Mark the location for the communicator. Disconnect power.

Mounting the Communicator

There are two mounting options:

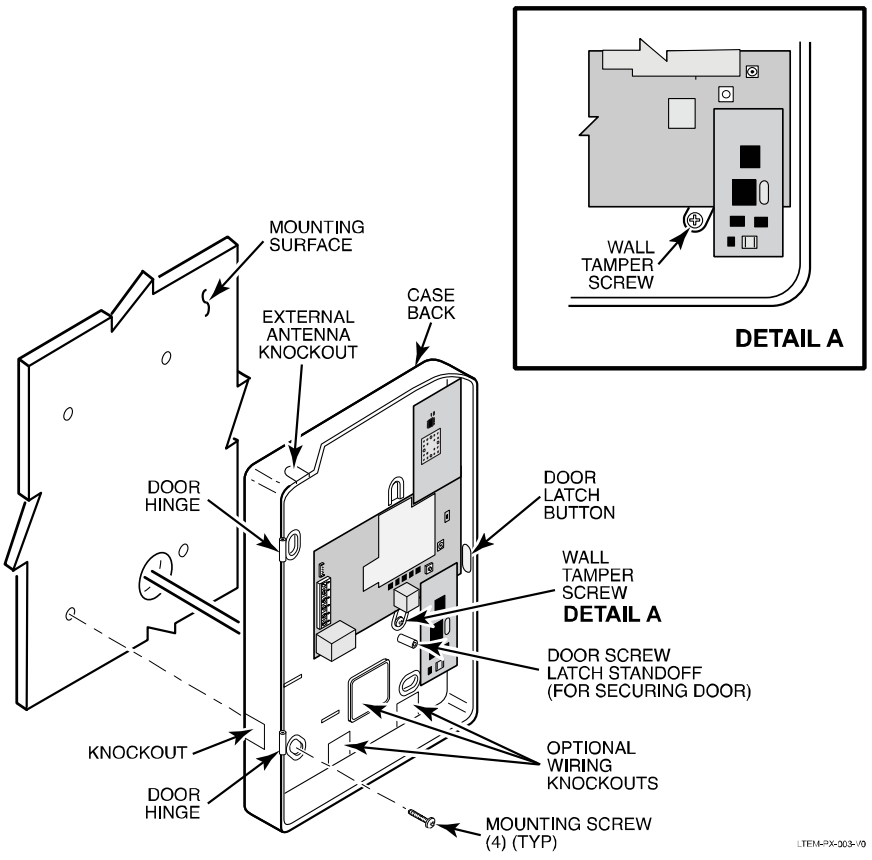
- Mount the Communicator directly to a wall, secured with four screws and a wall tamper screw
- Mount the Communicator to a control panel cabinet, secured to the cabinet via a threaded bushing and locking nut.

Mounting the Communicator on a Wall

1. Ensure power to the control panel (both AC and battery) is off.
2. Locate the back case (back cover) over selected mounting position such that the opening in the back case is aligned with the wire/cable opening on the mounting surface.

   Pass the wires/cable through the large knockout opening in the back case, or route through another removable knockout located on the back case.

   NOTE: Cable tie anchor points are located on the back case around the large center knockout for securing the wiring and providing strain relief.
3. Secure the back case to the mounting surface using four of the five screws provided (2 along the top, 2 along the bottom). After mounting, install the Wall Tamper screw.
4. After all wiring is complete and the unit is powered up, attach and close the front cover door. Secure with the door screw latch. (This is required for UL installations.)



Standard Wall Mounting

Mounting the Communicator on a Control Panel Cabinet

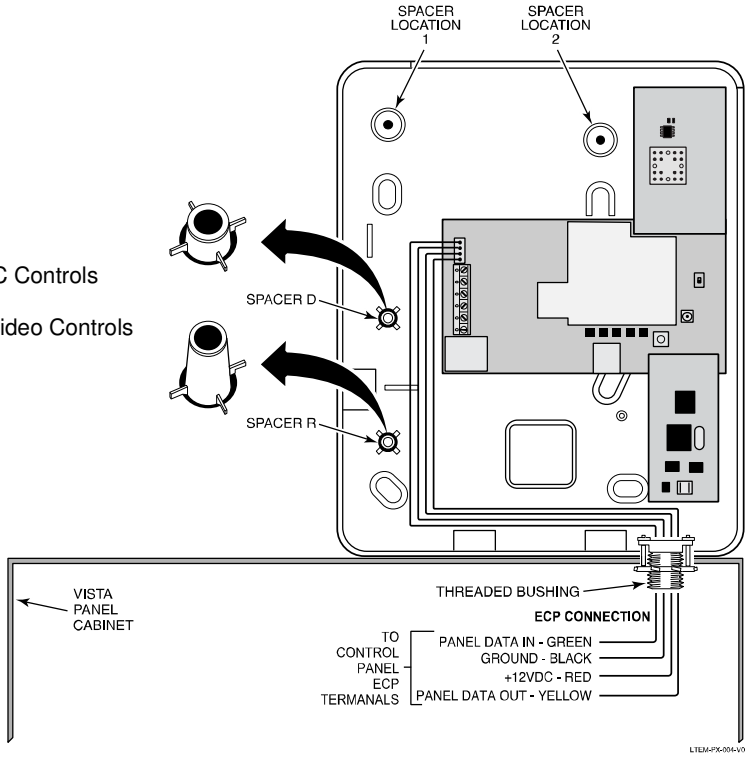
NOTE: Wall tamper not available when mounting the communicator on a control panel cabinet.

1. Ensure power to the control panel (both AC and battery) is off, then remove the desired conduit knockout (left or right) from the top of the control panel cabinet. See diagram for mounting example.
2. Remove the corresponding knockout from the bottom of the communicator for the threaded conduit bushing. Install the threaded bushing into the communicator so it snaps into the plastic retaining tabs.
3. Remove the appropriate spacer from the bottom case of the communicator by snipping the retaining ribs (SPACER R = VISTA control cabinet; SPACER D = DSC control cabinet; Interlogix controls do not require a spacer).
4. On the back of the communicator case, insert the spacer into the recess labeled SPACER LOCATION 1 or SPACER LOCATION 2, depending on which cabinet knockout (left or right) is used. The spacer should be installed in the spacer location that is diagonally opposite the cabinet knockout being used. That is, if using the right-side cabinet knockout, insert the spacer into Spacer Location 1; if using the left-side cabinet knockout, insert the spacer into Spacer Location 2.
5. Mount the communicator assembly onto the cabinet, passing the threaded bushing through the cabinet knockout and fasten with the locking nut. Secure the communicator to the wall using a 2-inch #6 (3.5 mm X 50 mm) Phillips pan head screw (included) through the spacer. See *Installing the Spacer* paragraph on the next page for detailed view.
6. For VISTA controls, connect the 4-wire ECP harness connector to the communicator's ECP connector; for other controls, connect the communicator's terminal block wiring. Thread the wires through the conduit bushing.
7. Refer to the control panel's installation guide and complete the control panel's wiring.
8. Secure the wiring with cable ties as necessary.

   NOTE: Cable tie anchor points are located on the back case around the large center knockout for securing the wiring and providing strain relief.
9. After all wiring is complete and the unit is powered up, attach and close the front cover door. Secure with the door screw latch.

SPACER D: for DSC Controls

SPACER R: for Resideo Controls



Typical Mounting on a VISTA Control Panel Cabinet

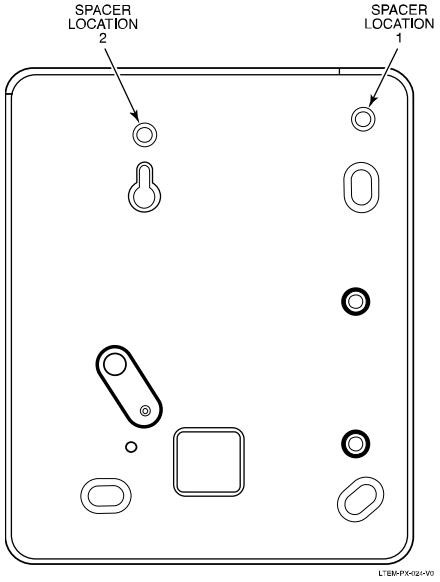
Installing the Spacer

The spacer is used to stabilize and secure the communicator to the wall. Depending on the wall material, an anchor for the screw may be needed.

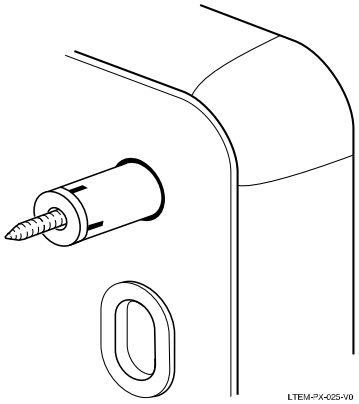
- Use Spacer Location 1 if using the right-side cabinet knockout.
- Use Spacer Location 2 if using the left-side cabinet knockout.

For other control panel cabinet mounting schemes, installer judgement should be used for proper spacer location to stabilize the communicator against the wall.

Use a 2-inch #6 (3.5 mm X 50 mm) Phillips pan head screw (included) through the spacer to secure the communicator to the wall.



Back of Case Spacer Locations



Example of Installed Spacer (Location 1 shown)

Wiring the Communicator

General Connections Information

The communicator can be used with Resideo VISTA control panels that support ECP data communication with radios or can be used with control panels that do not support ECP data communication with radios (e.g., VISTA-40, VISTA-50P, non-Resideo control panels).

Depending on the control panel, connections are made at the communicator's ECP connector or the bus terminals. If required, connections are also made to the communicator's optional Dialer Capture module (PRODCM). Refer to the *Dialer Capture Module* section under *Installing Optional Plug-in Modules* later in this manual for information regarding the use and installation of the Dialer Capture module.

The following table lists the types of connections for various control panels.

Control Panel	Connection to the Communicator
Resideo VISTA control panels that support ECP data communication with radios	Connects to the communicator's 4-wire ECP connector via 4-pin connector harness. Alternatively, can connect to the communicator's bus terminals. See *Wiring for VISTA Series ECP Control Panels* section.
DSC PowerSeries (PC) control panels*	Connects to the communicator's bus terminals. See *Wiring for DSC Control Panels* section.
Interlogix NetworX (NX) Series control panels*	Connects to the communicator's bus terminals and the PRODCM Dialer Capture module terminals. See *Wiring for Interlogix Control Panel Connections* and *Dialer Capture Module* sections later in this manual section.
Other compatible control panels*	Connects to the communicator's ground and +12VDC terminals and the PRODCM Dialer Capture module terminals. See the *Wiring for Other Control Panels* and *Dialer Capture Module* sections later in this manual.

* These controls not evaluated by ETL.

Check the control panel's instructions for wire length/gauge limitations and refer to the *ECP & BUS Connection Maximum Wire Lengths* table in the *Wiring for VISTA Series ECP Control Panels* section. If the tables differ in respective wire lengths, use the shorter length.

After any programming changes are made to DSC or Interlogix control panels, the communicator must be reset/rebooted (press and hold the Test switch for 10 seconds).

If using the communicator's Fault Trigger Output, make sure a common ground connection is made between the communicator's GND (terminal 3) and the control panel's Aux NEG (–) or any common zone ground. See the *Wiring the Fault Trigger Output* section for more information on the Fault Trigger Output.

Supervision Fault (Panel Sync Failure) Indication: If a panel sync failure occurs during the communicator reboot/power up after installation with a non-Resideo control panel, the communicator LEDs will continue to blink from right to left in the boot up marching sequence for up to 10 minutes. During this time, the installer should determine and correct the cause of the sync failure (clear panel alarms, faults, and troubles; disarm the control; clear alarm memory, etc.). If the sync failure is corrected within the 10-minute period, the LEDs enter normal operation mode. However, if the sync failure persists after the 10-minute period, the LEDs enter normal mode, but a supervision fault message is sent.

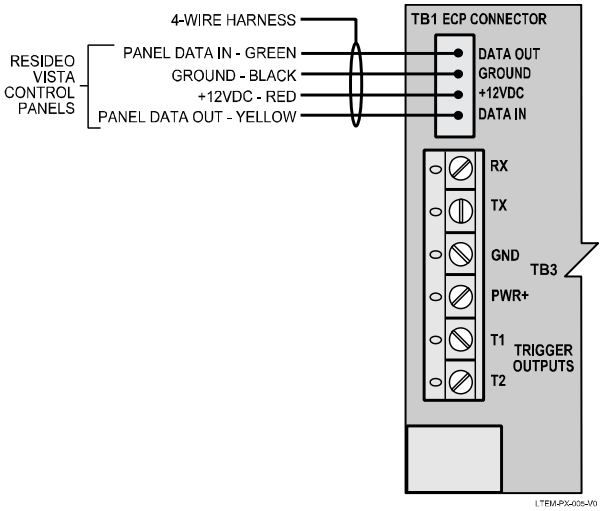
Wiring for VISTA Series ECP Control Panels

Most Resideo VISTA control panels support ECP data communication with communicators, (e.g., VISTA-15P, VISTA-20P, VISTA-128BPT and VISTA-128FBPT). However, there are some panels that do not. Check the *Installation and Setup Guide* for the control panel you are using to see if it supports communication device (LRR) to ECP communication.

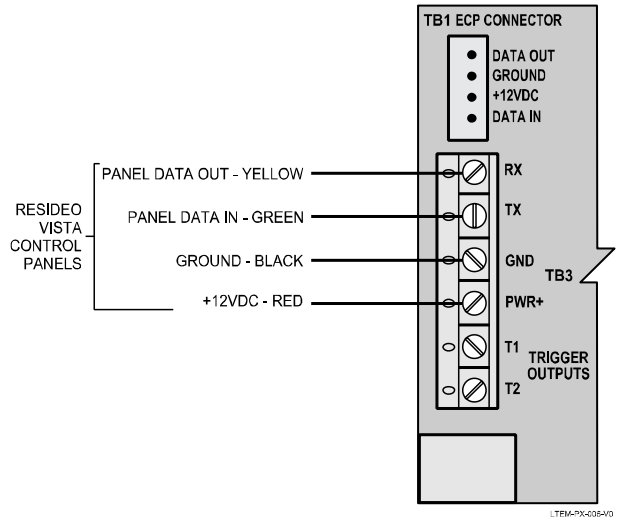
Programming Note: Make sure to program the control panel with the communicator's device address.

1. Ensure power to the control panel (both AC and battery) is off.
2. Connect the VISTA control panel's ECP (keypad) **Data In**, **Data Out**, **Ground,** and **+12VDC** terminals to the communicator's ECP connector using the included 4-wire harness (Resideo part 600-00151). See ECP Option 1 diagram.

   Alternatively, connect the VISTA control panel's ECP (keypad) terminals directly to the communicator's **RX**, **TX**, **GND,** and **+12VDC** terminals as shown in the ECP Option 2 diagram below.
3. Secure the wiring with cable ties as necessary. Cable tie anchor points are provided on the back case around the large center knockout.
4. Refer to the control panel's installation manual for details on powering up and programming the control panel.



ECP Connection Option 1
ECP Connection Using 4-Wire Harness



ECP Connection Option 2
ECP Terminal Block Connections

Wire length/gauge limitations are the same for the communicator as they are for keypads and other peripheral devices connected to the VISTA control panel.

ECP & BUS Connection Maximum Wire Lengths

Minimum Wire Gauge	Distance from Control Panel
#22	75 ft (23m)
#20	120 ft (37m)
#18	170 ft (52m)
#16	270 ft (82m)

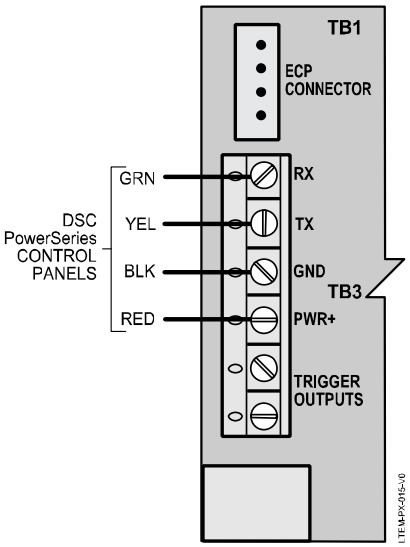
Wiring for DSC Control Panels (not evaluated by ETL)

This section applies to the following DSC PowerSeries™ control panels:

- PC1616
- PC1832
- PC1864

1. Ensure power to the control panel (both AC and battery) is off.
2. Connect the control panel terminals labeled Red (**RED**), Black (**BLK**), Yellow (**YEL**), and Green (**GRN**) to the communicator's **PWR+**, **GND**, **TX**, and **RX** terminals respectively. See diagram.
3. Refer to the control panel's installation manual for details on powering up and programming the control panel.
4. After control panel programming is completed, make sure the control panel is in the "Ready to Arm" state with no alarms or faults present. The following control panel fault/trouble conditions must be cleared in order for the communicator to sync properly with the control panel:
   - General System Trouble
   - General System Tamper
   - General System Supervisory
   - Telephone Line Trouble
   - Comm Fail Trouble
   - Zone Fault

   Refer to the *Clearing DSC Control Panel Trouble Conditions* section that follows for details on how to clear these trouble conditions.



Connections for DSC PowerSeries Control Panels

NOTE: If more than 10 minutes elapses before faults/troubles are corrected, the communicator must be rebooted (press and hold Test switch 10 seconds) after the panel is in the "Ready to Arm" state.

The communicator may take up to 90 seconds to reboot, then take up to an additional five (5) minutes to fully sync with the control panel. During this time, the communicator LEDs blink in repeated sequence from right to left (power-up sequence) while the communicator scans the control panel's partitions and zones. See **Supervision Fault (Panel Sync Failure) Indication** note in the earlier *General Connections Information* section.

After any programming changes are made to DSC control panels, the communicator must be reset/rebooted (press and hold the Test switch for 10 seconds).

After reboot/power up, the communicator can take about 5-7 minutes to complete the scan of the control panel's partitions and zones. The control panel must be in the "Ready" state (no alarms or faults) in order to perform the scan.

Clearing DSC Control Panel Trouble Conditions

Perform the following steps to clear various types of DSC control panel trouble conditions

General System Trouble

This trouble condition may be generated by issues with the PC5204 (power supply module) and/or PC5400 (printer module).

For PC5204, install a 1k resister from terminal O1 to AUX if Output 1 is unused. Also check that the wires are in good condition by measuring resistance.

General System Tamper

This trouble condition may be generated by expander modules and other types of modules. Please check that the tamper switches on expander and other modules are not being triggered.

For zone expander modules, you can install a 1k resistor from the tamper terminal to ground. This condition cannot be cleared through panel programming.

General System Supervisory

Check all module connections to the control panel. Correct any wiring issues.

1. Press [∗] 8 to enter programming mode.
2. Enter the Installer code.
3. Enter 9-0-2.
4. Wait 1 minute.
5. Press [#].
6. Enter 9-0-3.
7. Check that all modules are being supervised.
8. Press [#] [#] to exit programming mode.

Telephone Line Trouble

To clear Telephone Line trouble, disable telephone line trouble reporting.

1. Press [∗] 8 to enter programming mode.
2. Enter the Installer code.
3. Enter 0-1-5.
4. Turn off option 7 (on LED keypad, 7 should be off).
5. Press [#] [#] to exit programming mode.

Comm Fail Trouble

1. Press [∗] 8 to enter programming mode.
2. Enter the Installer code.
3. Enter 3-8-0 (Tel Communicator options).
4. Turn off 1 (Tel Communications Disabled).
5. Press [#] [#] to exit programming mode.

Alternatively, you can also do the following:

1. Press [∗] 6.
2. Press 4 (System test).

Trouble should disappear.

Zone Fault

1. Press [∗] 1 to enter Zone Bypass menu.
2. Enter the 2-digit Zone number showing fault (e.g., 01, 07, 12 etc.)
3. Press [#].
4. Repeat for all faulted zones.

Wiring for Interlogix Control Panels (not evaluated by ETL)

This section applies to the following Interlogix NetworX (NX) Series control panels:

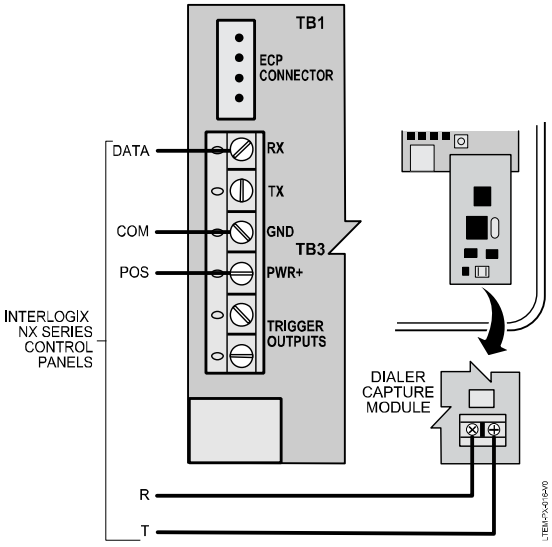
- NX-8E
- NX-4V2
- NX-6V2
- NX-8V2

Connection to an Interlogix control panel requires installation of the PRODCM Dialer Capture Module in the communicator.

1. Ensure power to the control panel (both AC and battery) is off.
2. Connect the control panel's **DATA**, **COM**, and **POS** terminals to the communicator's **RX**, **GND**, and **PWR+** terminals respectively. See diagram.
3. Install the PRODCM Dialer Capture module. See *Dialer Capture Module* section under *Installing Optional Plug-in Modules* later in this manual.
4. Connect the Dialer Capture module's Ring and Tip terminals (module terminals have no Ring/Tip polarity) to the control panel's Telco Ring (**R**) and Tip (**T**) terminals (do not connect to R1/T1).
5. Refer to the control panel's installation manual for details on powering up and programming the control panel.

   Power-Up Note: When using this communicator with an Interlogix control panel, make sure to connect the control's backup battery to the control BEFORE applying AC power to the control.

6. After control panel programming is completed, make sure the control panel is in the "Ready to Arm" state with no alarms or faults present.



Connections for Interlogix NX Series Control Panels

NOTE: If more than 10 minutes elapses before faults/troubles are corrected, the communicator must be rebooted (press and hold Test switch 10 seconds) after the panel is in the "Ready to Arm" state. The communicator may take up to 90 seconds to reboot. See **Supervision Fault (Panel Sync Failure) Indication** note in the earlier *General Connections Information* section.

Programming Notes for Interlogix NX Series Control Panels

- Location 0: Phone number 1 first segment must be 15 for tone dialing.
- Location 2: Report format must be 13 for Ademco Contact ID format.
- Location 23: Segment 3 should be all enabled (or 12345678 to enable all reports), otherwise some alarm reports will be missed via the dialer.

After any programming changes are made to Interlogix control panels, the communicator must be reset/rebooted (press and hold the Test switch for 10 seconds).

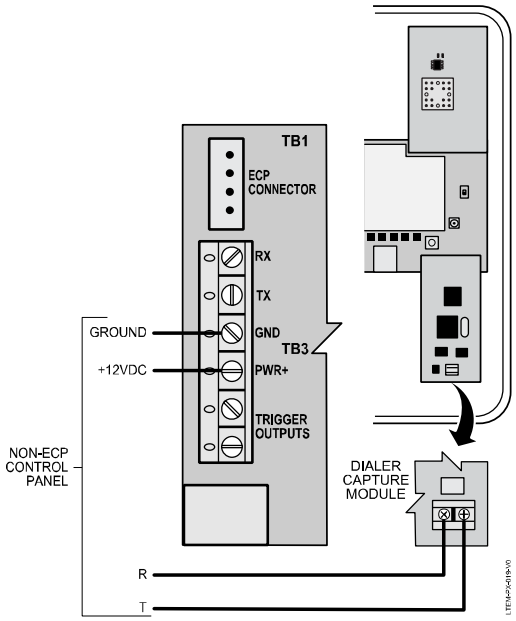
Wiring for Other Control Panels (not evaluated by ETL)

For other non-ECP controls that send Contact ID alarm signals via the control panel's dialer, the optional Dialer Capture module (PRODCM) is used to connect to the control panel. The Dialer Capture module replaces the phone line and simulates the phone service to the control panel. The alarms are then sent to AlarmNet for routing to the central monitoring station.

To install the PRODCM Dialer Capture module, refer to the control panel's instructions, the *PRODCM Dialer Capture Model* instructions (R800-26711), and the *Dialer Capture Module* section later in this manual.

Installation steps are summarized below:

1. Ensure power to the control panel (both AC and battery) is off.
2. Install the PRODCM Dialer Capture module as described in the *Dialer Capture Module* section later in this manual.
3. Connect the control panel's Telco **Ring (R)** and **Tip (T)** terminals individually to the terminals on the Dialer Capture module (module terminals have no Ring/Tip polarity). See diagram.
4. Connect the control panel's **Ground** and **+12VDC** terminals to the communicator's **GND** and **PWR+** terminals respectively. See diagram.
5. Secure the wiring with cable ties as necessary. Cable tie anchor points are provided on the communicator's back case around the large center knockout.
6. Refer to the control panel's installation manual for details on powering up and programming the control panel.



Connections for other Non-ECP Controls

7. After control panel programming is completed, make sure the control panel is in the "Ready to Arm" state with no alarms or faults present.

Do not connect the outside phone line to either the Dialer Capture module or the control panel. There should be no connection to the outside phone line when using the Dialer Capture module.

For replacement installations, make sure to disconnect the outside phone line when using the Dialer Capture module with the communicator.

If using the communicator's Fault Trigger Output, make sure a common ground connection is made between the communicator's GND (terminal 3) and the control panel's Aux NEG (–) or any common zone ground. See the *Wiring the Fault Trigger Output* section for more information on using the Fault Trigger Output.

Wiring the Fault Trigger Output

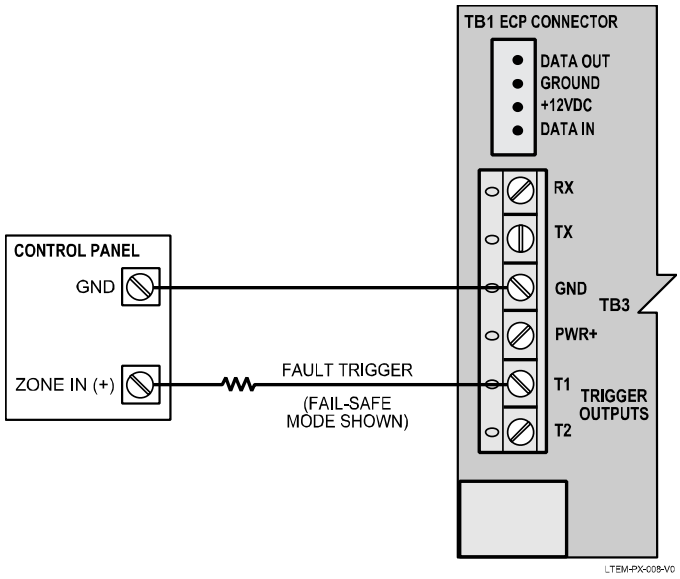
The communicator's fault trigger output (Trigger Output terminal T1) can be wired and programmed for fail-safe mode (see the program option "FAULT RELAY NORMALLY ON").

Use of the Fault Trigger Output requires a common ground* between the communicator and the control panel. Control panels connecting to the communicator's ECP or bus terminals typically include a common ground connection. However, if using a control panel that connects only to the communicator's PRODCM Dialer Capture module (see Dialer Capture Module section later in this manual), a common ground connection must also be made. See step 3.

* PC board ground, not earth ground

To sense a communicator fault at the control panel, do the following and see the diagram below.

1. Connect the communicator's Trigger Output **T1** to a zone "**+**" input at the control panel. (Trigger terminal T2 is not used.)
2. Install the proper end-of-line (EOL) resistor required by the control panel.
3. If the Fault Trigger Output is used with a control panel connected to the PRODCM Dialer Capture module, make sure to also connect the communicator's GND (terminal 3) to the control panel's Aux NEG (–) or any common zone ground.
4. Set the trigger for Fail-Safe mode by selecting the FAULT RELAY NORMALLY ON program option checkbox via AlarmNet 360.



Typical Wiring for the Fault Trigger to a Control Panel Zone for Normally Closed Fault (Fail-Safe mode)

Internet Connection (Ethernet or Wi-Fi®)

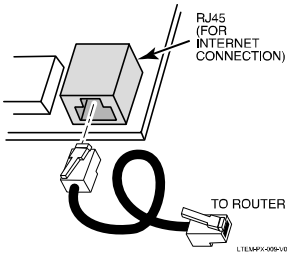
The communicator can connect to the Internet via Ethernet cable direct to a router or via Wi-Fi® using the optional PROWIFIZW Wi-Fi/Z-Wave module or PROWIFI Wi-Fi only module.

The communicator can use only one Internet connection method: Ethernet or Wi-Fi, not both.

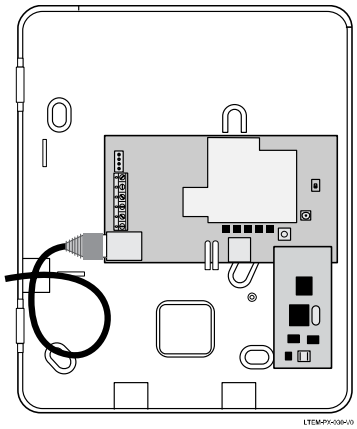
Ethernet Cable Connection

If using an Ethernet cable connection, connect one end of the Ethernet cable (Category 5 or higher) to the communicator's RJ45 connector and the other end to the cable/DSL router as shown in the diagram below. When routing the cable, include a strain relief loop to provide slack on the pcb connection, and use cable ties (included) to secure the cable to the appropriate tie points.

NOTE: When programming the communicator, make sure to program the communication path to the appropriate setting (i.e., **LTEM-PX** = Ethernet & Cell, **IP-COM** = Ethernet).



Ethernet Connection



Example of Ethernet Cable Routing With Strain Relief Loop

Wi-Fi Connection

If using Wi-Fi® to connect to the Internet, the PROWIFIZW or PROWIFI module must be installed. Refer to the *Installing Optional Plug-In Modules* section later in this manual for details on installing the Wi-Fi module.

NOTE: When programming the communicator, make sure to program the communication path to the appropriate setting (i.e., **LTEM-PX** = Wi-Fi & Cell, **IP-COM** = Wi-Fi).

Installing Plug-in Modules

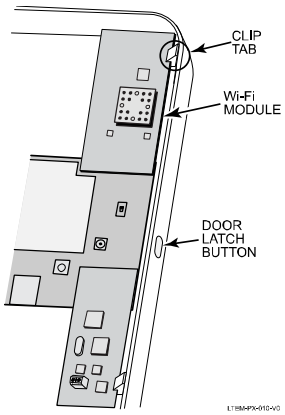
Wi-Fi/Z-Wave Module Installation

If a Wi-Fi® connection to the router is desired rather than an Ethernet cable connection, install the PROWIFIZW Wi-Fi/Z-Wave module or PROWIFI Wi-Fi only module. The PROWIFZW module also provides the ability to control Z-Wave devices for installations that include home automation features.

NOTES:
- The Wi-Fi module requires a router and internet service for Wi-Fi connection. Refer to the instructions included with the module for additional information.
- The current drain for the PROWIFI module is slightly less than that listed in the Specifications section for the PROWIFIZW.
- WI-FI supports DHCP (dynamic) IP addressing only, it does not support STATIC IP addressing.

The communicator can use only one Internet connection method: Ethernet or Wi-Fi, not both.

1. Power down the communicator (remove power to the control panel, both AC and battery).
2. Install the module by mating the module's connector to the edge connector on the upper left side of the communicator's PCB. Make sure the module is fully seated in the connector. Slip the module board under the clip tab to lock it in place as shown below (PROWIFIZW shown).
3. Affix the FCC/IC label provided with the module to the outside of the communicator's back case.
4. After installation, power up the communicator (reconnect AC power and battery to the control panel).



Wi-Fi Module Installation

6. Programming of the module, as well as the inclusion/exclusion of Z-Wave devices (if using PROWIFIZW), is done through the AlarmNet 360™ Programming Tool. On a laptop, PC or Smart Device, go to www.alarmnet360.com.

   NOTE: When programming the communicator, make sure to program the communication path to the appropriate setting.
7. When programming is complete, perform a Communications Test (press and release the Test button).

Z-Wave™ Notice

Your device, when used with the PROWIFIZW Wi-Fi/Z-Wave module, is a Primary Z-Wave Controller which controls a mesh network of wireless Z-Wave™ and Z-Wave Plus™ devices. This system may be used with all devices certified with the Z-Wave certificate and should be compatible with such devices produced by other manufacturers. Z-Wave products are "included" into the Controller, so once they are programed, each device is assigned a unique address which allows them to communicate with each other and cannot be activated by a neighbor's Z-Wave automation system. Z-Wave is a wireless protocol that many manufacturers can add to their products such as in-wall light switches, in-wall outlets/receptacles, plug in lamp/appliance modules, thermostats, door locks, garage door openers, and many more. Z-Wave devices communicate with each other to make sure signals get from the Controller to the destination device. A signal can hop from device to device four times to get to the destination device. Battery operated devices, such as door locks, do not hop signals to other devices. Only constant powered devices can hop signals.

DSK NOTE: The DSK (Device Specific Key) of this Z-Wave device can be viewed on AlarmNet 360's Z-Wave screen.

Wi-Fi® Setup

To set up a Wi-Fi connection to the router, you will need the AlarmNet 360 Mobile App installed on a smartphone or tablet. The app is available for download from the App Store or Google Play.

You will also need the following information:

- Communicator's MAC ID and CRC (both found on a label on the communicator).
  MAC ID:_____ CRC:_____
- SSID and password for the router to which the communicator will be connected.
  SSID:_____ Password:_____

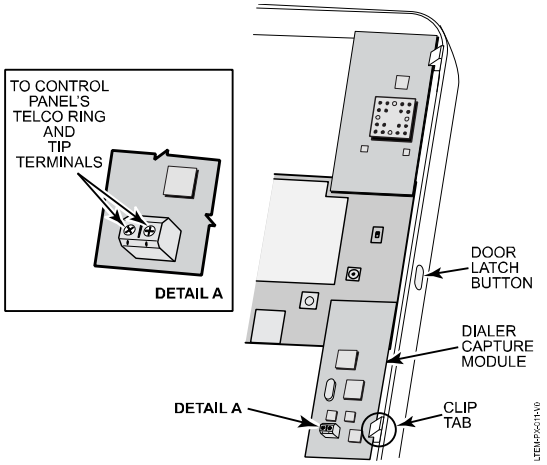
With the Wi-Fi module installed and the communicator powered up, do the following.

1. Connect your smart device to the same Wi-Fi network the communicator will use.
2. Turn on Bluetooth on your smart device.
   Make sure the Bluetooth is not connected to another device.
3. Open the AlarmNet 360 Mobile App and log in.
4. Click the upper left menu icon (3 bars) and select **Connect a Device to the Internet** to display the **Connect Device** page.
5. Review the steps shown on the **Connect Device** page. In summary, the steps as applied to this communicator are as follows:
   Step 1: Power the communicator and activate Bluetooth.
   Step 2: Pair your mobile device with the communicator via Bluetooth.
   Step 3: Configure the Internet connection (choose the Wi-Fi router to which the communicator will be connected).
   Step 4: The communicator searches AlarmNet 360 for an account.
6. When ready, activate Bluetooth Pairing mode on the communicator.
   To activate Bluetooth Pairing mode, press and hold the communicator's Test switch for at least 3 seconds. The **REG** (green), **FAULT** (red), and **WI-FI** (green) LEDs blink in unison indicating the unit is in Pairing mode.
   NOTE: Pairing mode expires after 10 minutes of no screen activity.
7. Click **Get Started**. At the Pair Device screen, wait for the Available Devices to display the communicator's name (e.g., LTEM-PXAxxxx, where xxxx are the last four digits of the MAC ID). Select **Pair**. Click **Pair** at the **Bluetooth Pairing Request** prompt.
8. Enter the communicator's CRC number at the **Enter CRC Number to verify device** prompt.
   A message confirms the Bluetooth connection.
9. At the **Select Wi-Fi Network** prompt, select the desired Wi-Fi router (identified by its SSID).
10. Select **Manual Entry** and at the **Enter Wi-Fi Password** prompt, enter the router's password then click **Submit**. A message confirms successful connection.
    Alternatively, if the user does not want to share the Wi-Fi password, select **Request Entry via Email** instead of **Manual Entry**. Enter the user's email address at the prompt. An email will be sent to the user with a link to a secure website where they can then privately provide their Wi-Fi password.
11. The communicator then searches for its respective AlarmNet 360 account. If the account is found, the "Device connected to account" message appears.
    From there, you can check the communication paths or go to the AlarmNet 360 **Account Overview** page.
12. Exit the AlarmNet 360 app when done.

Dialer Capture Module Installation

An optional Dialer Capture module (PRODCM) can be used for control panels that send Contact ID alarm signals via the control panel's dialer but do not connect via ECP or bus terminals. The Dialer Capture module replaces the phone line and simulates the phone service to the control panel. The alarms are then sent to AlarmNet for routing to the central monitoring station.

1. Power down the communicator (remove power to the control panel, both AC and battery).
2. Install the Dialer Capture module by mating the module's connector to the edge connector on the upper right side of the communicator's PCB. Make sure the module is fully seated in the connector. Slip the module board under the snap tab to lock it in place as shown below.
3. Connect the control panel's Telco Ring (R) and Tip (T) terminals individually to the terminals on the Dialer Capture module (module terminals have no Ring/Tip polarity). See diagram below.
4. If using the communicator's Fault Trigger Output (see *Wiring the Fault Trigger Output* section), make sure a common ground connection is made between the communicator's GND (terminal 3) and the control panel's Aux NEG (–) or any common zone ground.
5. After installation, power up the communicator (reconnect AC power and battery to the control panel).



Dialer Capture Module Connections

NOTE: When the control panel is on hook (not dialing out), Ring (–) and Tip (+) voltage should measure ~27VDC at the PRODCM terminals. When off hook (dial out) voltage drops to ~3VDC.

Do not connect the outside phone line to either the Dialer Capture module or the control panel. There should be no connection to the outside phone line when using the Dialer Capture module.

For replacement installations, make sure to disconnect the outside phone line when using the Dialer Capture module with the communicator.

Control Panel Programming Notes for Dialer Capture

After the Dialer Capture module has been installed, make sure the control panel is programmed for the following:

- Dialer operation is set for DTMF Tone Dialing for each phone number (pulse dialing is not supported and must be disabled in the control panel).
- PABX field is disabled (the Dialer Capture module does not communicate through a PABX).
- Phone numbers and account numbers are programmed (to ensure the maximum number of messages can be transmitted to the central station before a communication failure occurs, ensure the control panel is programmed with a primary and secondary central station number).
- Report format is set to Contact ID for each phone number.
- The maximum number of retry attempts is programmed.
- Desired zone and partition reports are enabled.

Additional Notes When Using the Dialer Capture Module

- The Dialer Capture module supports only one-way communications (from the control panel to the central station). For those control panels that support two-way voice communications, speakerphone, paging, follow-me, etc., these features will no longer be available. The control panel must be programmed for one-way communications only.
- Since Dialer Capture module supports only one-way communications (from the control panel to the central station), the Resideo Compass Downloader cannot be used.
- Total Connect is not supported for controls that communicate with the radio solely via the Dialer Capture module.
- In the event the communicator loses power, the module would not be able to generate a fault trigger to the control panel and set an alarm. In this case, after the panel has exhausted its redial attempts, a communication failure is displayed by the panel (you may have to scroll through the messages).
- The Dialer Capture module cannot sense a fault on the Tip/Ring side. However, during an alarm, if the module cannot forward the alarm, it will trigger a fault and disable the phone line. The phone line will be re-enabled after communication has been re-established.
- If the Dialer Capture module senses a fault, it will send a Trigger signal to the control panel zone (if wired to a zone). At this point the module will also drop the phone line voltage and will not provide a dial tone to the control panel. During this time, the control panel will make retry attempts (8 for residential, and more for commercial) to dial out and send a report. Until the control panel has completed the series of retry attempts it will not be able to detect a Telco fault. To minimize the wait time, for control panels that allow setting the Telco Fault detection time, please set it to the minimum detection time.
- For control panels that may generate erroneous Telco fault conditions based on grounding, turn off "Telco Fault" monitoring at the control panel.
- If the dialer capture module receives a communication path failure from the communicator, the module will drop the voltage and thereby disable the phone line. If Telco Fault is enabled in the panel, the keypad on the system will display the fault. When the dialer capture module receives a fault clear condition, the module will re-enable the phone line. The panel is notified of all other faults if the fault output of the communicator is wired to a zone on the panel.

External Antennas

⚠ Applies only to the **LTEM-PXA** / **LTEM-PXV** communicators.

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

If adequate signal strength cannot be achieved with the internal antenna, an external antenna can be used. An Antenna Kit with an antenna, antenna cable, clamp, and/or bracket will be required. Instructions for mounting the antenna are provided with the kit. In addition, a separate antenna adapter cable is needed (model ADPT-LTEMPX).

The following Antenna Kits are compatible:

- CELL-ANTHB
- PROLTE-ANT
- CELLANT3DBPK

Also Needed:

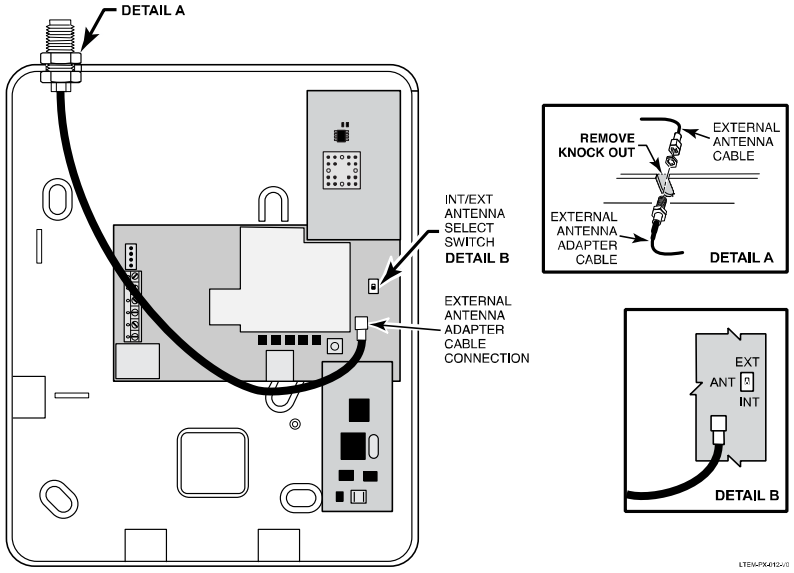
- Adapter Cable: ADPT-LTEMPX

⚠ The Antenna Kits include an adapter cable that is **not suitable** for use with these communicators and should be ignored. Instead, the antenna adapter cable ADPT-LTEMPX must be used (available separately). This cable has an MHF connector on one end and an SMA connector on the other end and is designed specifically for use with these communicators.

To connect an external antenna to the communicator, do the following.

NOTE: Antenna can be installed with the communicator powered up.

1. Remove the antenna port knockout on the top of the communicator case.
2. From inside the case, install the adapter cable's SMA connector in the antenna port knockout and secure with the nut provided. See diagram detail A.
3. Route the adapter cable as shown, then snap the adapter cable's MHF connector onto the communicator's main board external antenna connector. See diagram below.
4. Install the external antenna according to its instructions, using the brackets and hardware provided with the External Antenna kit.
5. Connect the Antenna Kit's antenna cable to the adapter cable's SMA connector previously mounted to the communicator back case.
6. Set the INT/EXT Antenna Select Switch to the EXT (External) position. See diagram Detail B.
7. When complete, perform a communication test (press and release the Test switch).



External Antenna Installation for LTEM-PXA/LTEM-PXV communicators

Programming the Communicator

General Information

The communicator delivers alarms via the Internet to an AlarmNet central station or via the network, using cell technology when the Internet is not available.

NOTE: The communicator requires an AlarmNet 360 account. For new installations, please obtain the account information from the central station prior to programming this communicator. For replacement installations, the AlarmNet 360 account is created automatically when the communicator is registered.

The communicator is programmed using the AlarmNet 360 website or the AlarmNet 360 Mobile App.

After any programming changes are made to DSC or Interlogix control panels, the communicator must be reset/rebooted (press and hold the Test switch for 10 seconds).

Using AlarmNet 360

To program the communicator via the website (if you are already signed up for this service), go to: **www.alarmnet360.com**, or use the AlarmNet 360 Mobile App. Log in and follow the on-screen prompts. Please have the following information available when programming the communicator:

- Primary City ID (two-digit number), obtained from your monitoring station.
- Primary Central Station ID (two-digit number), obtained from your monitoring station.
- Primary Subscriber ID (four-digit number), obtained from your monitoring station.
- Communicator's MAC ID and MAC CRC number (located on the box and inside the communicator).

When AlarmNet 360 programming is complete, use the **Send Data to Device** command to send the programming information to the communicator. After the data has been sent, the **communicator must be registered**. See the ***Registration*** section.

Programming Options

The following is a list of programming options pertinent to this communicator and programmed in the AlarmNet 360 SETTINGS menu.

OVERVIEW FIELDS (Overview fields are programmed when a new account is created in AlarmNet 360)

Communicator MAC xxxxxxxxxxx	The MAC ID is found on a label on the communicator and on its carton.
Alarm Reporting Number xx xx xxxx	Account information is provided by the central station administrator. This field displays account number, consisting of the City ID, Central Station ID, and Subscriber ID numbers. City ID = 01-99; Central Station ID = 01-FE (HEX); Subscriber ID = 0001-9999
Device Type • LTEM-PXA • LTEM-PXV • IP-COM	Device Type displays the various communicator model numbers. Select the appropriate communicator model.

Panel Type • VISTA • VISTA-10P • VISTA-10PSIA • VISTA-15P • VISTA-15PSIA • VISTA-20P • VISTA-20PSIA • VISTA-21iP • Dialer Capture Module • DSC • Interlogix	Panel Type displays various types of control panels. Select the specific control panel model to which the communicator is connected. Select VISTA if the communicator is connected to other VISTA series controls. Select Interlogix or DSC accordingly if the communicator is connected to one of those panels. Select Dialer Capture Module for other control panels connected via the Dialer Capture module.
Supervision • Daily	Supervision time is factory-set to "Daily" (24 hours) and cannot be changed. The AlarmNet network must hear at least one supervisory message from the communicator during this supervision period; otherwise, AlarmNet notifies the central station that a communication failure has occurred.

PATH DETAILS OPTIONS

Communication Path • Ethernet Only • Cellular Only* • Ethernet and Cellular* • Wi-Fi Only • Wi-Fi and Cellular*	Select the desired communication path. If Wi-Fi® is desired, the PROWIFIZW or PROWIFI module must be installed. Refer to the Wi-Fi Module section located in Section 2 earlier in this manual. * Options marked with asterisk are not applicable to the **IP-COM**
LRR ECP Device Address • 1-30	**Applicable only if Panel Type is VISTA or VISTA-20P.** The communicator connects to a VISTA control panel using the ECP bus. Enter the appropriate ECP device address. For VISTA-10P, VISTA-15P, and VISTA-20P series control panels, use address 3. For other control panels, see their Installation and Setup Guide. **NOTES**: 1. When programming the control panel, enable the communicator (or LRR) output. 2. This Device Address must be unique from the "Remote Control Keypad Address" (default address 02) and the “Interactive Event (Multi-Mode) Device Address” (default address 25).
Old Alarm Time • 10 Minutes* • 4 Hours • 15 Minutes • 8 Hours • 30 Minutes • 12 Hours • 1 Hour • 24 Hours • 2 Hours	Sets how long an undeliverable 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. Select the desired time period. * default Old Alarm Time is 10 minutes
IP Fault Time • 00-99	**Applicable only if comm. path includes Ethernet or Wi-Fi.** In the event there is a loss of contact with the network over the Ethernet or Wi-Fi connection, enter the time delay (in minutes) before the communicator notifies the central station. IP failure will always be sent to the central station as Primary Communication Path Failure. Default IP Fault Time is 60 minutes.
Use DHCP • Select • Unselect	**Applicable only if communication path includes Ethernet.** If selected, dynamically allocates the IP addresses for Ethernet (recommended). If unselected, uses fixed IP addresses programmed in the next 4 fields. **NOTE:** Wi-Fi is always set for DHCP.
NIC IP Address xxx.xxx.xxx.xxx	**Applicable only if communication path includes Ethernet.** Enter the 12-digit, 4-part address for this device.
Subnet Mask xxx.xxx.xxx.xxx	**Applicable only if communication path includes Ethernet.** Enter the 12-digit, 4-part address for the 32-bit address mask used to indicate the portion (bits) of the IP address that is being used for the subnet address.

Gateway IP Address xxx.xxx.xxx.xxx	**Applicable only if communication path includes Ethernet.** Enter the 12-digit, 4-part address assigned to the Gateway.
DNS Serv IP Addr xxx.xxx.xxx.xxx	**Applicable only if communication path includes Ethernet.** Enter the 12-digit, 4-part IP address for the DNS (Domain Name System) server.
Cellular Fault Time • 00-99	Option not applicable to the **IP-COM**. In the event the communicator detects a communication path failure, enter the time delay (in minutes) before the communicator notifies the central station. A cell failure will always be sent to the central station as Secondary Communication Path Failure. Default Cellular Fault Time is 60 minutes.
Fault Relay Normally On (Fail-Safe Mode) • Select • Unselect	The Fault Relay Normally On option enables fail-safe mode, which causes the fault trigger open collector output to be normally energized to ground and de-energizes (open circuit) upon a communicator fault condition (if respective alarm reports are enabled). For conditions that trip the fault trigger refer to *Supervision Features* in Section 1. Select this option if Fail-Safe mode is desired. If unselected, the fault trigger output is normally de-energized and energizes when a listed communicator fault condition occurs. Note that if unselected, the control panel will not be alerted if the radio loses complete power or if the wiring from the radio to the control is cut. See *Wiring the Fault Trigger* in Section 2 for information on connecting the trigger output to a control panel.
Notify Panel Of • Neither fault • Both IP and Cellular faults	Option not applicable to the **IP-COM**. **This option appears only if comm. path includes Ethernet & Cell or Wi-Fi & Cell.** If "Both IP (Wi-Fi or Ethernet) and Cellular" is selected, the device will notify the control panel only if both communication paths fail but will always send notification of either failure to the central station. Refer to the control panel's manual for information on enabling local annunciation of communicator faults. **NOTE**: The fault trigger output (if Fault Relay Normally On is selected) is triggered only if "Both IP and Cellular" is selected (If the "Cellular Fault Time" and "IP Fault Time" options are set to zero, faults will not be reported). Select the desired option.
Tamper Report • Select • Unselect	If selected, sends a tamper report when the communicator detects a tamper condition. A tamper restore is automatically sent when the tamper condition clears.

REMOTE SERVICES

Remote Access • Select • Unselect	Select to allow the end user to access their system via Resideo's Total Connect. Availability of this service is controlled by the dealer. To use Remote Access, an account must be created in AlarmNet 360.
Remote Control (AUI) Keypad Addresses • 01-30	Must be programmed if using the Remote Access feature Enter the keypad address intended to be used for remote control. **NOTES:** 1. This address must also be programmed as an alpha keypad in the control panel or an AUI (advanced user interface) type device, if a full enhanced graphic interface to the system is desired and the control panel supports it. DO NOT connect an actual keypad (or any other device) assigned to this address. 2. This address must be unique from the programmed "Device Address." Default address is 02.
Keypad Type • Keypad Only • Full Control	Keypad Only is not applicable for TC2 Total Connect usage. Full Control provides a virtual Total Connect keypad for controlling panel functions and supports User and Panel syncing functions. Used with most Resideo VISTA series control panels.

ADDITIONAL SETTINGS

Email Notification (Multi-Mode Communications) • None • Total Connect 2.0 (Enhanced Rpts)	Select "Total Connect 2.0 (Enhanced Rpts)" if you want system events sent by email to the user. Enhanced Reports enables reporting to Total Connect 2.0 web services. **NOTES**: • To use "Enhanced Reports" ensure the control panel is Total Connect 2.0 Ready. • In order to select email notification (Multi Mode), an account must be created in AlarmNet 360 and "Remote Access" must be selected. ⚠ Multi-Mode (email notification) is intended as a convenience for the user and does not replace Central Station reporting of critical events (alarms, troubles, etc.).
Interactive Event Device Address • 01-30	The Interactive Event Device address must match the address of the RIS Address programmed in the panel. For VISTA-15P and VISTA-20P, the address must be 25. This address is programmable in other VISTA control panels (it is recommended to assign device address 25; where appropriate, select Device Type 12 = RIS). This device address must be unique from the communicator device address and the Keypad Address used for Remote Access.

FIXED SETTINGS (the following options are factory set and not programmable)

Cell Rollover • ON	Option not applicable to the **IP-COM**. Cell Rollover is factory-set to ON and cannot be changed. All messages (including AlarmNet network supervisory messages) are sent over the cell network in the event of an Internet failure.
IP Connection • Auto Detect	IP Connection is factory-set to Auto-Detect and cannot be changed. In Auto Detect mode, the device will always try to use IP* to communicate but it will not generate a Primary Comm Path Failure unless it previously detected the presence of IP. As soon as the presence of IP is detected, a Primary Comm Path Restore message is generated and the value of IP Connectivity programming parameter is changed from "Auto Detect" to "Present". From this point on, the software expects connectivity. The auto detect logic will resume only when the parameter is changed back to "Auto Detect." * Ethernet or Wi-Fi, depending on option selected in Comm Path choice.

ECP Status Codes

When the communicator is configured for ECP usage, it sends status messages to the control panel for power, tamper, and network connectivity failures. Some of the control panels (e.g., VISTA-10P, VISTA-15P and VISTA-20P Series) display these on the keypad as "LngRng Radio" followed by a 4-digit code (listed in the table below). In addition, the Contact ID codes (listed in Appendix B) for these conditions are sent to the central station by the communicator.

Common ECP Keypad Display Status Codes

STATUS CODE	DESCRIPTION
0000	Control panel lost communication with communicator.
0880	Communicator tamper detected (cover removed).
4005	Communicator has lost contact with AlarmNet.
000F	Communicator is not registered; account not activated.
0019	Communicator shutdown.
0400	Communicator power on / reset AND the control panel lost communications with communicator.
0C80	Communicator power on / reset AND tamper detected.
0C8F	Communicator power on / reset AND tamper detected AND not registered.
3000	Primary power loss (will only be displayed in conjunction with another event).

Registration

Registering the Communicator

Once you have programmed the communicator, it must be registered. Registering the communicator activates the account with AlarmNet and enables the security system's control panel to send reports. You can register by using one of the following methods:

- AlarmNet 360 website
- Communicator's Test switch

Before the communicator is registered, the REG (green) LED will be ON. To complete registration, the Cell LED or Wi-Fi/Ethernet LED must be ON.

LED		DESCRIPTION
REG (green)	**ON**	**Module is NOT registered with AlarmNet.**

When the registration successfully completes, the REG (green) LED turns OFF and the communicator enters normal operating mode.

LED		DESCRIPTION
REG (green)	**OFF**	**Module is registered with AlarmNet.**

If registration is not validated by AlarmNet within 90 seconds, the communicator times out, and the REG (green) LED will be ON.

Register using the AlarmNet 360 Website

To register the communicator via the website, go to: www.alarmnet360.com.

Please have the following information available:

- Primary City ID (two-digit number).
- Primary Central Station ID (two-digit hexadecimal number).
- Primary Subscriber ID (four-digit number).
- MAC ID and MAC CRC number (located on the box and inside the communicator).

1. Log in and choose “Programming” page.
2. Search for the account using the Account Information or MAC ID.
3. Under the “Actions” column, use the pulldown menu and select “Register” the account.
4. After successful registration, the REG (green) LED turns off.

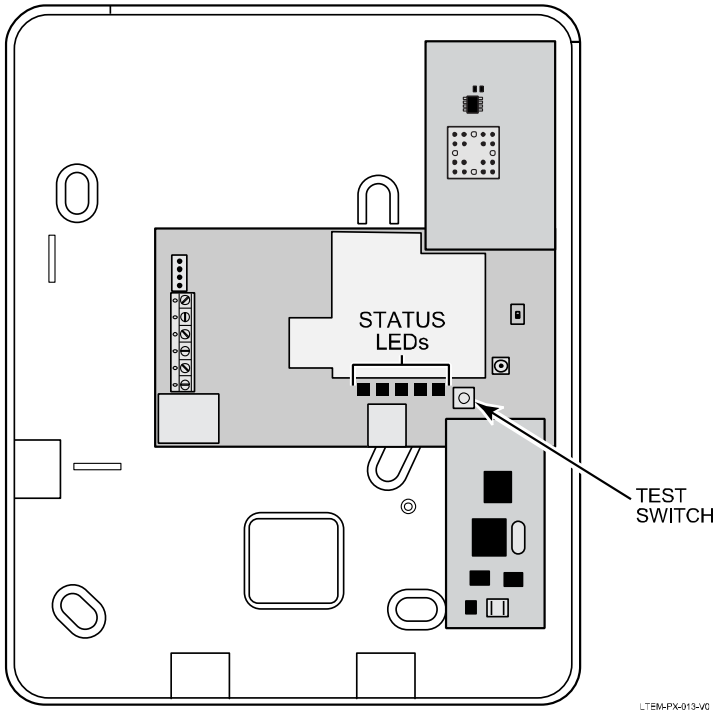
After the communicator is registered, you may log out of the AlarmNet 360 website.

Register using the Test Switch

Initiate the registration sequence by clicking the Test Switch three times.

When registration has been completed successfully, the communicator enters normal operating mode and the REG (green) LED turns off.

If repeated registration attempts time out, check your Internet connection and RSSI level, and verify the communicator account information has been entered correctly.



Triple-Click the Test Switch to Register the Communicator

Appendices

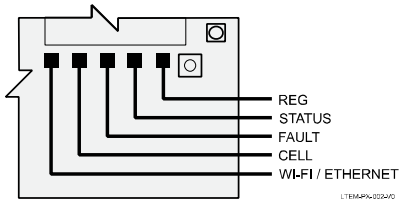
Appendix A: Summary of LED Operation

Initial Power Up: Upon initial power up, the communicator LEDs blink in repeated sequence from right to left indicating network initialization.

Green (REG) → Yellow (STATUS) → Red (FAULT) → Green (CELL) → Green (WI-FI)

LED INDICATIONS

LED		DESCRIPTION
REG (green)	ON	Module is NOT registered with AlarmNet
	OFF	Module is registered with AlarmNet
	FAST BLINK	Download session with Compass in progress
STATUS (yellow)	PERIODIC BLINK	Normal (indicates Power On*)
	FAST BLINK	Cannot deliver alarms
FAULT (red)	ON	No contact with the cell network
	OFF	Normal
	FAST BLINK	No cell network contact AND loss of communication with the panel
	SLOW BLINK	Loss of communication with the panel (ECP fault)
CELL** (green)	ON	Minimum required signal quality is present
	OFF	Cell not enabled
	FAST BLINK	Signal quality is poor
WI-FI / ETHERNET (green)	Wi-Fi CONNECTION (if used)	
	ON	Communicator connected to Internet via Wi-Fi
	OFF	Wi-Fi not enabled
	FAST BLINK	Wi-Fi enabled, no connection to Internet
	ETHERNET CONNECTION (if used)	
	ON	Communicator connected to Internet by Ethernet
	OFF	Ethernet not enabled
	FAST BLINK	Ethernet enabled, no connection to Internet
1st THREE right to left** - REG - STATUS - FAULT	FAST BLINK IN UNISON	Firmware over-the-air (OTA) download in progress
1st FOUR right to left** - REG - STATUS - FAULT - CELL	FAST BLINK IN UNISON	Cell module firmware OTA update in progress
ALL FIVE LEDs - REG - STATUS - FAULT - CELL - WI-FI / ETHERNET	FAST BLINK IN UNISON**	SIM card not present or puk locked
	FAST BLINK IN SEQUENCE	Power-up sequence
LEDs 1, 3, & 5 - REG - FAULT - WI-FI	FAST BLINK IN UNISON	Unit is in Pairing mode (connecting to smart device via Bluetooth)



Status LEDs (Cover Removed)

*** Power On Indication**: If 12VDC is present, Status (yellow) LED blinks periodically.

** Indications marked with double asterisk do not apply to the IP-COM.

Appendix B: Central Station Contact ID Messages

Alarm Condition	Alarm Code	Restore Code
Power On / Reset	E339 C08xx*	
Tamper **(Compromise Indication)**	E341 C08xx*	R341 C08xx*
Power Loss	E337 C08xx*	R337 C08xx*
ECP Supervision **(Compromise Indication)**	E355 C0000	R355 C0000
Primary Comm Path Supervision	E350 C0951	R350 C0951
Secondary Comm Path Supervision	E350 C0952	R350 C0952
Application Code Update	E903 C08xx	R903 C08xx (success)
Application Code Update Failure	E904 C08xx	
Cellular Module Firmware Update	E365 C08xx	R365 C08xx (success)
Cellular Module Firmware Update Failure	E366 C08xx	
Periodic Cell Comm Test Failure	E358 C0803	
Manual Test	E601 00 C803	
Specific to RESIDENTIAL / COMMERCIAL Control Panels (Such as the VISTA-10P, 15P, and 20P series.)		
Communicator Trouble (ECP bus, network) **(Possible Compromise Indication)**	E353 C08xx* ◊	R353 C08xx* ‡
Radio Fault	E353 0 1xx* ‡	R353 0 1xx* ‡
Specific to COMMERCIAL Control Panels (Such as the VISTA-128/250 series.)		
Communicator Trouble (ECP bus, network) **(Possible Compromise Indication)**	E333 C08xx* ‡	R333 C08xx* ‡
Radio Loss of Signal **(Possible Compromise Indication)**	E357 0 8xx* †	R357 0 8xx* ‡ or R380 0 8xx* ‡
Radio Fault (tamper, ECP Bus)	E333 0 8xx* ‡	R333 0 8xx* ‡
AlarmNet Messages		
Communication Failure. **(Possible Compromise Indication)**	E359 0 C950	R 359 0 C950
Authorized New Registration	E360 00 000	
Authorized Radio Substitution	E361 00 000	
Unauthorized Radio Substitution Attempt	E362 00 000	

* xx = Communicator Device Address

† = Message is sent by dialer only.

‡ = Message is sent by dialer and radio.

◊ = Message is sent by dialer only, or dialer and radio, depending on failure.

Appendix C: Glossary

4G LTE	Refers to the fourth generation of cellular wireless standards. It is a successor to 3G and 2G families of standards. 4G provides up to 10 times the data transfer speeds of 3G.
DACT	Digital Automated Communications Terminal
DHCP	Dynamic Host Configuration Protocol, which provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DNS	Domain Name System, which is a distributed hierarchical naming system used to resolve domain names (e.g., www.yahoo.com) into numerical IP addresses (e.g., 204.17.25.1.).
DSL	Digital Subscriber Line.
ECP	Enhanced Console Protocol, which is a proprietary bus used in Resideo control panels to communicate with keypads and peripheral devices. It uses four wires: power, ground, data in, data out.
Gateway IP Address	A gateway (sometimes called a router) is a computer and/or software used to connect two or more networks (including incompatible networks) and translates information from one network to the other. The Gateway IP address is the IP address for the gateway.
IMEI	International Mobile Equipment Identity number.
IP	Internet Protocol.
IP Address	A unique number consisting of four parts separated by periods (for example: 204.17.29.11). An IP Address can be fixed or "static", or "dynamic," where the IP Address is assigned via DHCP at every startup.
ISDN	Integrated Services Digital Network.
ISP	Internet Service Provider.
LAN	Local Area Network.
LRR	Long Range Radio, an older term now referred to as communicator. A broader term communications module or communications device may also be used.
MAC ID	Media Access Code, this is a unique address assigned to every network communications device. For the communicator it is located on the box and inside the communicator.
Subnet Mask	A Subnet is a portion of a network that shares a network address with other portions of the network and is distinguished by a subnet number. The Subnet Mask is a 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.
TCP/IP	Transmission Control Protocol / Internet protocol.

– NOTES –

– NOTES –

Regulatory Notes

REFER TO THE INSTALLATION AND SETUP GUIDE FOR THE CONTROL WITH WHICH THIS DEVICE IS USED FOR LIMITATIONS OF THE ENTIRE SYSTEM.

FEDERAL COMMUNICATIONS COMMISSION & 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, replace it with a quality outdoor antenna.
- Reorient the receiving antenna until interference is reduced or eliminated.
- Move the radio or television receiver away from the receiver/control panel.
- Move the antenna leads away from any wire runs to the receiver/control panel.
- Plug the receiver/control panel 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.

ISED CLASS B STATEMENT

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC / 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 (2) This device must accept any interference received, including interference that may cause undesired operation.

Cet appareil est conforme à la partie 15 des règles de la FCC et exempt de licence RSS d'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: Ademco Inc., a subsidiary of Resideo Technologies, Inc., 2 Corporate Center Drive., Melville, NY 11747, Ph: 516-577-2000
Partie responsable / Émetteur de la déclaration de conformité du fournisseur : Ademco Inc., une filiale de Resideo Technologies, Inc., 2 Corporate Center Drive., Melville, NY 11747, Tél. 516 577-2000

RF Exposure

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

Mise en Garde

Exposition aux Fréquences Radio : La/les antenne(s) utilisée(s) pour cet émetteur doit/doivent être installée(s) à une distance de séparation d'au moins 20 cm (7,8 pouces) de toute personne et ne pas être située(s) ni fonctionner parallèlement à tout autre transmetteur ou antenne, excepté en conformité avec les procédures de produit multi transmetteur FCC et ISED.

IMPORTANT NOTE ABOUT EXTERNAL ANTENNAS

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

TO THE INSTALLER

LTEM-PXV: The external antenna gain shall not exceed 8.9 dBi for 700 MHz (Band 13), 8 dBi for 1700 MHz (Band 4). Under no conditions may an antenna gain be used that would exceed the ERP and EIRP power limits as specified as specified in FCC Parts 22H, 24E and 27.

LTEM-PXA: The external antenna gain shall not exceed 8.6 dBi for 700 MHz (Band 12), 8 dBi for 1700 MHz (Band 4), and 11 dBi for 1800 MHz (Band 2). 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.

TO THE INSTALLER

Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system.

The installer should assume the responsibility of developing and offering a regular maintenance program to the user as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts. Recommendations must be included for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

Summary of Connections

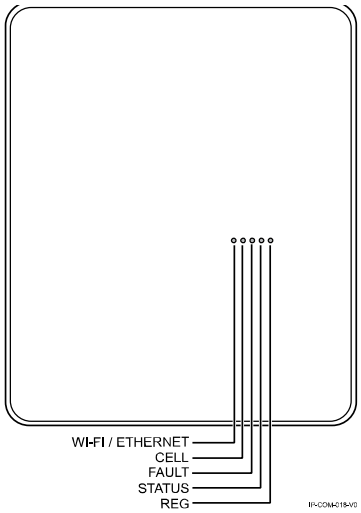
WEEKLY TESTING IS REQUIRED TO ENSURE PROPER OPERATION OF THIS SYSTEM

NOTE: All circuits are supervised, and all circuits are power limited.

IMEI/MAC ID: A label showing the IMEI and MAC ID numbers is located on the PCB shield plate.

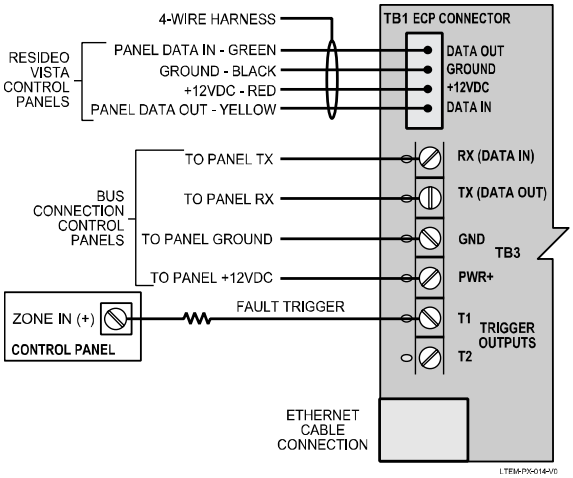
TEST SWITCH FUNCTIONS
Send Test Message: Short press & release
Register Communicator: Triple-click
Bluetooth Pairing Mode: Press & hold 3 secs
Reboot Communicator: Press & hold 10 secs
Reset to Factory Defaults*: Press & hold 20 secs

*** Setting Factory Defaults:** This function resets all programmed values to original factory settings and removes all Wi-Fi/Bluetooth pairings.

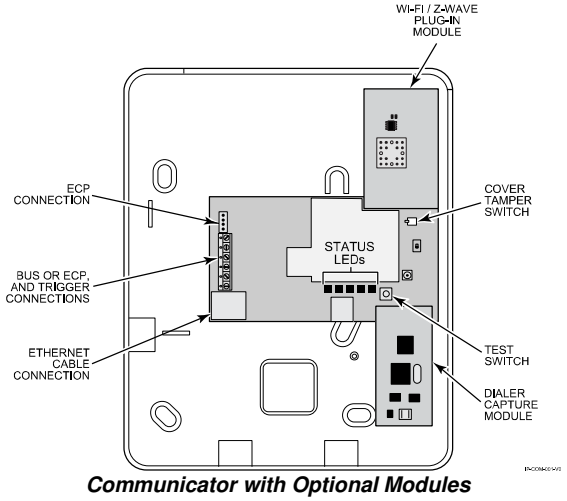


Status LEDs

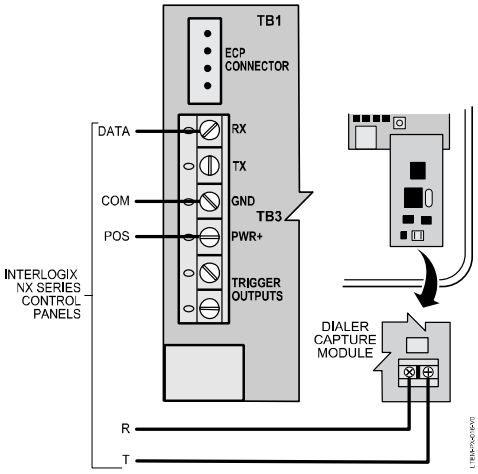
LED STATUS		
REG (green)	ON	NOT registered with AlarmNet
	OFF	Module is registered with AlarmNet
	FAST BLINK	Download session with Compass in progress
STATUS (yellow)	Periodic BLINK	Normal (indicates Power On)
	FAST BLINK	Cannot deliver alarms
FAULT (red)	ON	No contact with the cell network
	OFF	Normal
	FAST BLINK	No cell network & loss of comm with the panel
	SLOW BLINK	Loss of comm with the panel (ECP fault)
CELL (green)	ON	Signal quality is acceptable
	OFF	Cell not enabled
	FAST BLINK	Signal quality is poor
WI-FI / ETHERNET (green)	ON	Connected to Internet via Wi-Fi or Ethernet
	OFF	Wi-Fi/Ethernet option not enabled
	FAST BLINK	Option enabled, no connection to Internet
RIGHT 3	BLINK in UNISON	Firmware OTA download in progress
RIGHT 4	BLINK in UNISON	Cell firmware OTA update in progress
ALL 5	BLINK in UNISON	SIM card not present or puk locked
	BLINK in SEQUENCE	Power up sequence
1 – 3 - 5	BLINK in UNISON	Unit is in Pairing mode



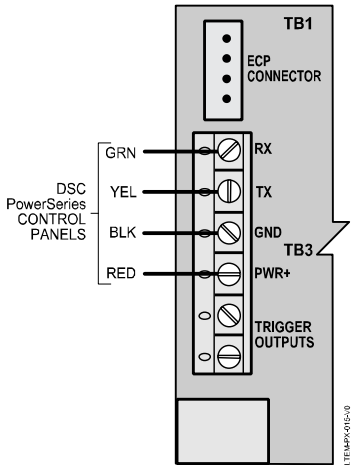
Communicator Wiring Terminals



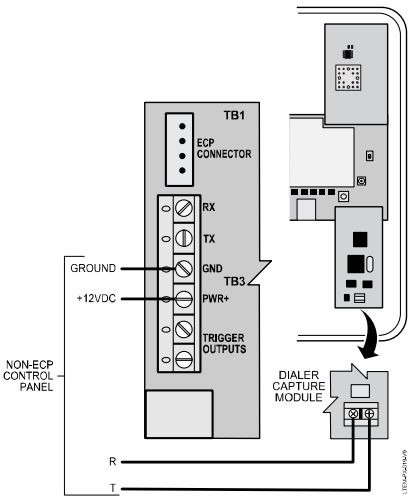
Communicator with Optional Modules



Connections for Interlogix NX Series Control Panels *(not evaluated by ETL)*



Connections for DSC PowerSeries Control Panels *(not evaluated by ETL)*



Connections for other Non-ECP Control Panels *(not evaluated by ETL)*

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.

For Support visit: www.resideo.com
For Warranty information visit: www.resideo.com

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

R800-27327C 12/21 Rev C