

**DIN Rail PostX IP Reporting Module
Installation Manual**

ICT[®]eSecurity.

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2016. All rights reserved.

Publication Date: June 2017

Contents

1	Welcome	6
1.1	Document Conventions	6
1.2	PostX Module Editions	7
2	Installation Requirements	8
3	Mounting	9
3.1	Removal	9
3.2	Wiring Diagram	10
4	DC Power	11
5	Interface Connections	12
5.1	Panel Interface	12
5.2	Telephone Dialler Interface	12
5.3	Ethernet 10/100 Network Interface	13
5.4	GPRS Interface	14
5.5	WiFi Interface	14
6	Interface Configuration	15
6.1	Establishing Ethernet Connection	15
7	Web Interface	16
7.1	User Login	16
7.2	Routing Setup	17
	General Options	18
	Routing Channels	18
	IP Reporting Formats	18
	PSTN Reporting Formats	20
	Polling	20
	Test Report	20
	Communication Failure	20
7.3	Input and Output Control	21
	Zone Inputs	21
	Programmable Outputs	24
7.4	Email Events	27
7.5	Ethernet Configuration	28
7.6	WiFi Configuration	29
7.7	GPRS / SMS Configuration	31
7.8	PSTN Configuration	31

8	Advanced Configuration	32
8.1	General Settings	33
8.2	TCP/IP Serial Port	33
8.3	System Started Message	33
8.4	CSV-IP Settings	34
8.5	PSTN Pass Through	34
9	Duplicate Configuration	35
9.1	Creating a Configuration File	35
9.2	Downloading a Configuration File	35
10	Web User Management	36
10.1	Setup	36
10.2	Access Levels	36
10.3	Default Users	36
11	IP Troubleshooting	37
11.1	Default Static IP Address Mode	37
11.2	DHCP IP Address Mode	37
11.3	Confirm IP Address via Command Line	38
12	Command Line Interface	39
12.1	Command Line Interface Commands	40
13	LED Indicators	42
13.1	Power Indicator	42
13.2	Status Indicator	42
13.3	Fault Indicator	42
13.4	Modem Indicator	43
13.5	Panel Indicator	43
13.6	Ethernet Indicator	43
13.7	Relay 1/Relay 2 Indicators	43
13.8	Zone Status Indicators	44
13.9	WiFi Indicator	44
13.10	GPRS Indicator	45

14	Identification Sticker Details _____	46
15	Warnings _____	47
16	Mechanical Diagram _____	48
17	Mechanical Layout _____	49
18	Technical Specifications _____	50
19	New Zealand and Australia _____	51
20	UL and ULC Installation Requirements _____	52
20.1	UL/ULC Installation Cabinet Options	52
20.2	Central Station Signal Receiver Compatibility List	52
20.3	ULC Compliance Requirements	52
	CAN/ULC-S304-06	52
	CAN/ULC-S319-05	55
	CAN/ULC-S559-04	55
20.4	UL Compliance Requirements	59
	UL1610	59
	UL294	60
21	FCC Compliance Statements _____	62
22	Industry Canada Statement _____	64
23	Ordering Information _____	65
24	Warranty _____	66
25	Contact _____	67

1 Welcome

Thank you for purchasing the PostX DIN Rail IP Reporting Module by Integrated Control Technology. The PostX Module is designed to help transition existing alarm monitoring solutions from traditional PSTN reporting to IP capable devices with minimal effort and at a low cost.

The current features of the PostX module include:

- Full PSTN phone line emulation circuit that will interface with any alarm panel.
- 10/100 Base-T Ethernet
- GPRS support*
- WiFi support*
- Independent modem that supports downstream phones.
- 4 configurable inputs
- 2 programmable outputs.
- Small physical size to fit inside existing installations.
- 12VDC power supply input.
- Emulates a full CID receiver.
- UDP and TCP based IP reporting protocols.
- Configurable 128, 192 or 256 bit AES encryption.
- Fully configurable through an Internet browser.
- Backup reporting options.
- 64 message queue.
- Industry standard DIN Rail mounting
- Online and remote upgradeable firmware

For more information on the PostX DIN Rail IP Reporting Module and other Integrated Control Technology products please visit our website (<http://www.ict.co>).

* Applies to WiFi and/or GPRS editions (see page 7) only.

1.1 Document Conventions

This document uses the following conventions:



Important warnings or cautionary messages to prevent equipment damage, data loss, or other similar conditions



Notes with additional information such as an explanation, a comment, or a clarification about the subject



Tips containing practical information that may help you solve a problem or describing actions that may save you time



Information relating to UL and ULC compliance



Bold text enclosed in brackets is used to show a section number or address of a programmable option or information on programming shortcut sequences

1.2 PostX Module Editions

There are four editions of the PostX module. All editions enable you to program up to 4 communication channels for reporting messages from the connected alarm panel. The communication interface of each channel can be configured independently, allowing you to select from Ethernet, PSTN, WiFi or GPRS, according to the module used.

	Communication Interface			
	Ethernet	PSTN	WiFi	GPRS
CRX-POSTX-DIN PostX DIN Rail IP Reporting Module	✓	✓		
CRX-POST-DIN-WF PostX DIN Rail IP Reporting Module with WiFi	✓	✓	✓	
CRX-POSTX-DIN-GP PostX DIN Rail IP Reporting Module with GPRS	✓	✓		✓
CRX-POSTX-DIN-WFGP PostX DIN Rail IP Reporting Module with WiFi and GPRS	✓	✓	✓	✓

The features specific to modules with a WiFi and/or GPRS interface described in this manual are only relevant if you are using the appropriate edition.

2 Installation Requirements

This equipment is to be installed in accordance with:

- The Product installation instructions
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- The Local Authority Having Jurisdiction (AHJ)

3 Mounting

The PostX Module is designed to mount on standard DIN Rail either in dedicated DIN cabinets or generic DIN Rail mounting strip. A section of this DIN Rail strip has been provided as a mounting option.

When installing the PostX Module ensure that there is adequate clearance around all sides of the device and that air flow to the vents of the unit is not restricted. It is recommended to install the PostX Module in a location that will facilitate easy access for wiring. It is also recommended that the PostX Module is installed in electrical rooms, communication equipment rooms, closets or in an accessible area of the ceiling.

1. Hook the lower tabs under the bottom edge of the DIN Rail.
2. Push the PostX Module against the DIN Rail mount until the upper tab clips over the upper rail.

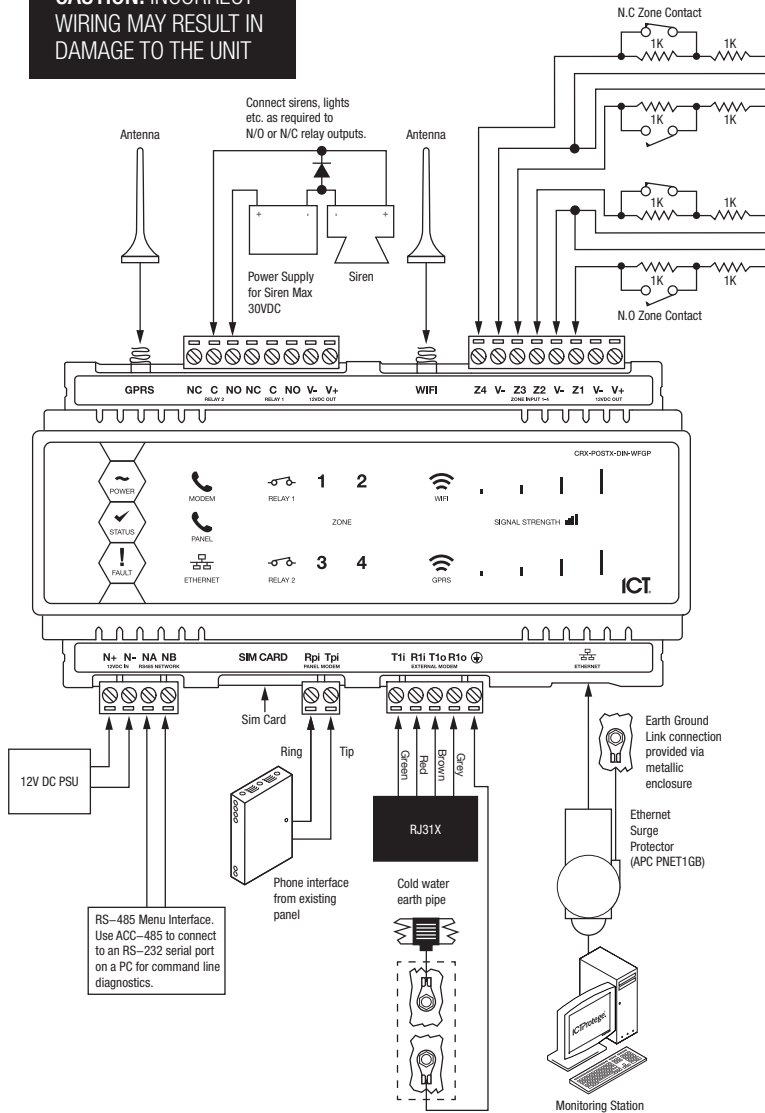
3.1 Removal

The PostX Module can be removed from the DIN Rail mount using the following steps:

1. Insert a flat blade screwdriver into the hole in the tab at the top of the PostX Module.
2. Lever the tab up and rotate the unit off the DIN Rail mount.

3.2 Wiring Diagram

CAUTION: INCORRECT WIRING MAY RESULT IN DAMAGE TO THE UNIT



RS-485 Menu Interface. Use ACC-485 to connect to an RS-232 serial port on a PC for command line diagnostics.

Wiring

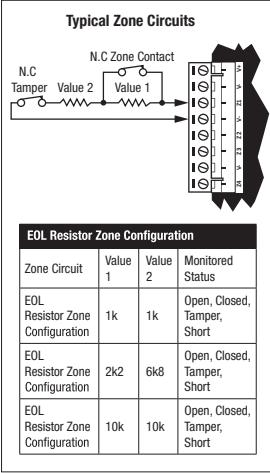
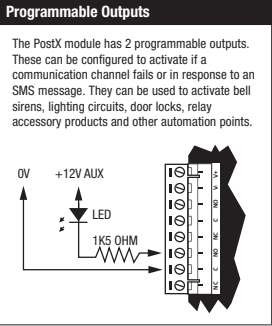
EARTH GND WIRING: Minimum 14AWG solid copper wire.

ZONE WIRING: maximum distance of 300m (1000ft) from the Protege GX DIN Rail PostX Reporting Module when using 22 AWG.

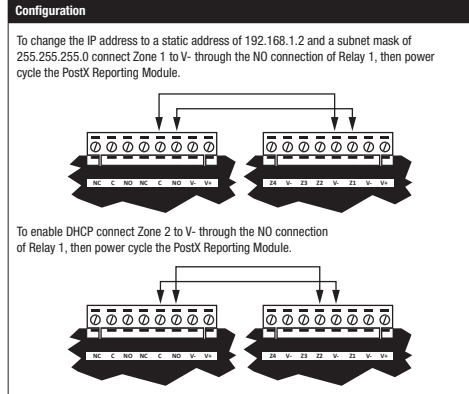
AUX WIRING: Min 22AWG Max 16AWG. (Depends on length and Current consumption). For wire/cable size, a maximum of 5% voltage drop at the terminals of the powered device has to be observed.

ETHERNET WIRING: CAT5e / CAT6 max 100m (330 ft)

MODULE NETWORK WIRING: Recommended Belden 9842 or equivalent. (24AWG twisted pair with characteristic impedance of 120ohm or CAT5e / CAT6 are also supported for Data Transmission when using ground in the same cable. **Do not use extra wires to power devices.**) max 900m (3000ft).

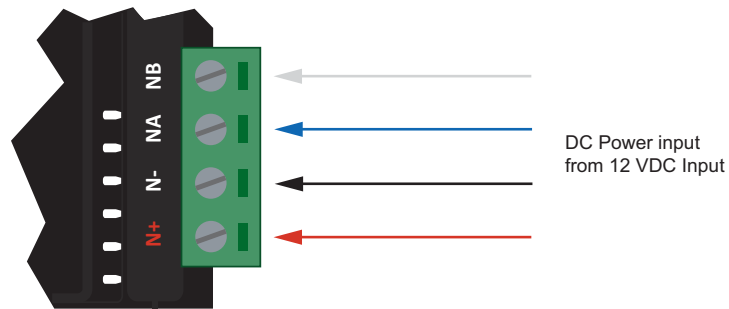


LED	Description	
Power	On	Correct voltage applied.
	Off	Low or no voltage applied.
Status	On	Module starting up.
	Slow flashing	Module operating normally.
Fault	Slow Red flashing	Module is in boot mode awaiting firmware update.
	For further details, please refer to the Error Code Display section in the Installation Manual.	
Modem	On	Onboard modem is off hook.
	Off	Onboard modem is not active.
Panel	On	Subscriber phone is off hook.
	Off	Subscriber phone is not active.
Ethernet	On	Ethernet connection detected.
	Off	No Ethernet connection detected.
Relay 1/2	Fast flash	Active Ethernet data transfer.
	On	Relay is closed.
Input 1-4	Off	Relay is open.
	Red	Input is in the OPEN state.
Wifi	Green	Input is in the CLOSED state.
	Red flashing	Input is in the TAMPERED state.
	Green flashing	Input is in the SHORTED state.
	Wave on	Connection available
	Wave flashing	Communication / data transfer
	Wave on / 1 bar Red	Connection not established
	Wave on / all bars off	Connected RSSI level 0 (lowest signal strength)
	Wave on / 1 bar on	Connected RSSI level 1
	Wave on / 2 bars on	Connected RSSI level 2
	Wave on / 3 bars on	Connected RSSI level 3
	Wave on / 4 bars on	Connected RSSI level 4 (highest signal strength)
	GPRS	Wave on
Wave flashing		Communication / data transfer
Wave on / 1 bar Red		Connection not established
Wave on / all bars off		Connected RSSI level 0 (lowest signal strength)
Wave on / 1 bar on		Connected RSSI level 1
Wave on / 2 bars on		Connected RSSI level 2
Wave on / 3 bars on		Connected RSSI level 3
Wave on / 4 bars on		Connected RSSI level 4 (highest signal strength)



4 DC Power

Module power is supplied by the N+ and N- terminals.



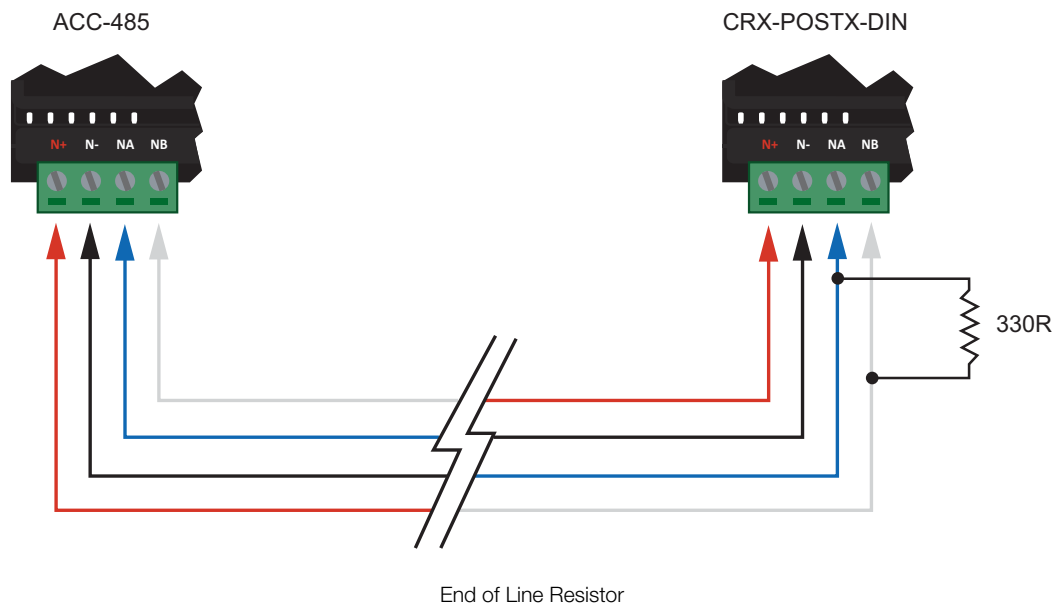
Standard DC Power Connection

Connection of the DC supply should be performed according to the diagram shown above. It is important that the N+ module power be 12VDC supplied from an independent battery backed power supply unit such as the PRT-PSU-DIN capable of supplying the required voltage.



Warning:

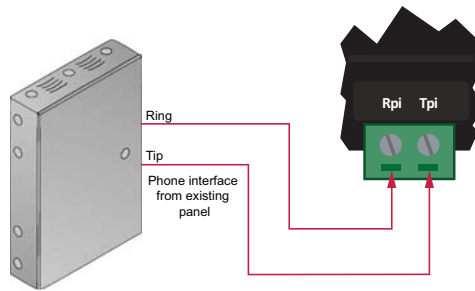
- The 12V N+ and N- DC power input must be supplied from only ONE point. Connections from more than one 12V supply may cause failure or damage to the PostX module.
- The 330 Ohm EOL (End of Line) resistor provided in the accessory bag MUST be inserted between the NA and NB terminals of the ACC-485 module directly connected to the PostX module..



5 Interface Connections

5.1 Panel Interface

The PostX Module has a fully featured PSTN phone line emulation circuit for interfacing to any PSTN device. This interface generates all of the appropriate voltages for powering the connected device. In most applications this device will be an alarm panel modem. The following diagram shows how to connect the existing PSTN device to the PostX Module. Simply connect the Tip and Ring from the device to the terminals marked Tpi (Tip Panel Input) and Rpi (Ring Panel Input).



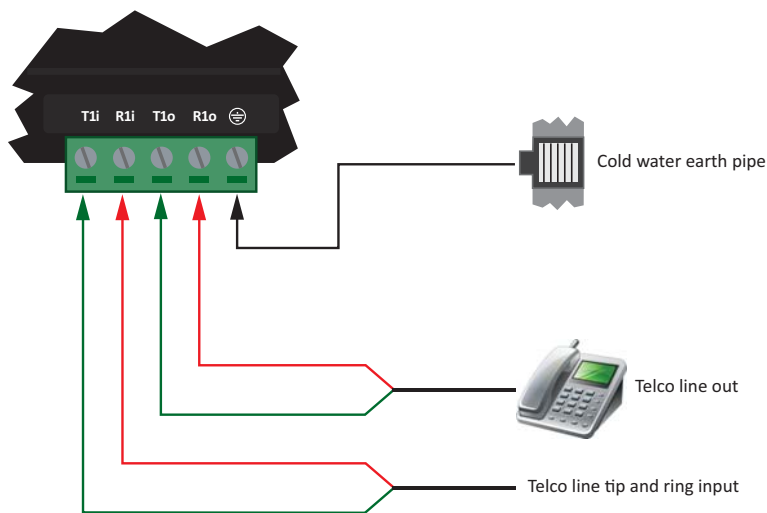
Wiring Interface to Existing Alarm Panel



Warning: NEVER connect the phone line emulator (terminals Rpi and Tpi) to a normal phone line. This will cause permanent damage to the PostX Module.

5.2 Telephone Dialler Interface

The PostX Module also has an outbound modem that can be used for PSTN – PSTN routing or as a backup to the IP Reporting. The telephone lines can be directly connected to the PostX Module using the onboard telephone connection terminals.



Telephone Line Connection



It is recommended that the earth connection for the telephone and main power supply (see page 11) earth be run separately and should be terminated on the cold water pipe or similar grounding point within the installation.

5.3 Ethernet 10/100 Network Interface

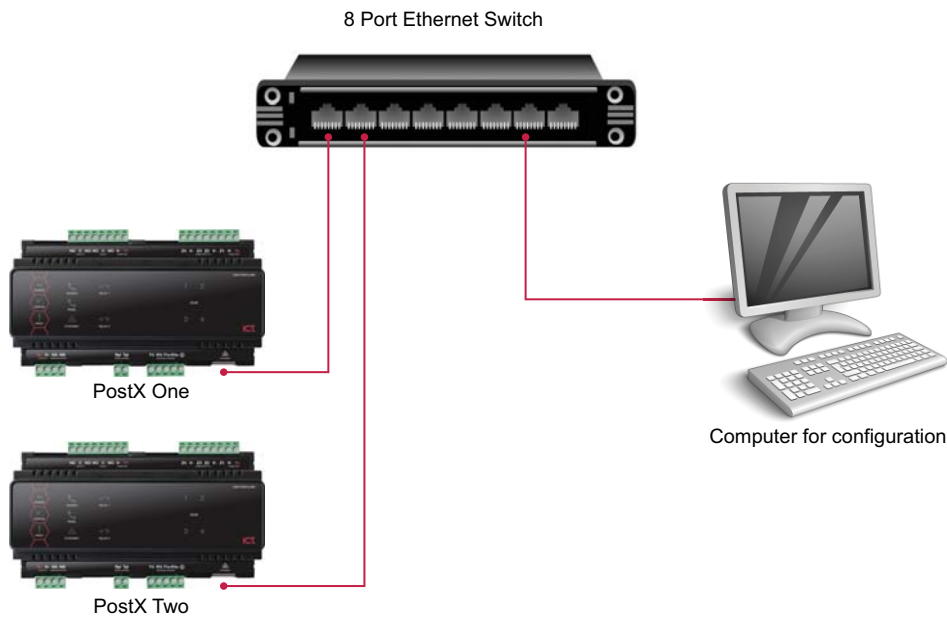
The PostX Module can communicate over a 10/100 Ethernet network using the TCP/IP protocol. This is used for IP Reporting and configuration of the unit using an Internet browser.

The default IP address for the Ethernet interface is set to a static IP address of 192.168.1.2 with a subnet mask of 255.255.255.0. These IP address settings are commonly used for internal networks. There are a number of ways to change the IP address of the PostX Module. Refer to the section Default Static IP Address Mode (see page 37) for details.

When installing an Ethernet connection, the PostX Module should be interfaced using a standard segment (<100M in length) and should be connected to a suitable Ethernet hub or switch.

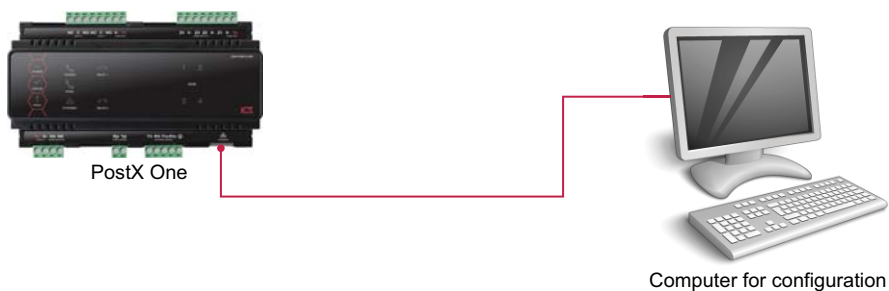


Installing the PostX Module on an active network requires knowledge of the configuration and structure for the network. Always consult the network or system administrator and ask them to provide you with a fixed IP Address that can be assigned to the PostX Module.



Ethernet 10/100 Switch/Hub Connection

Temporary direct connections can be used for onsite configuration by using a standard Ethernet cable.



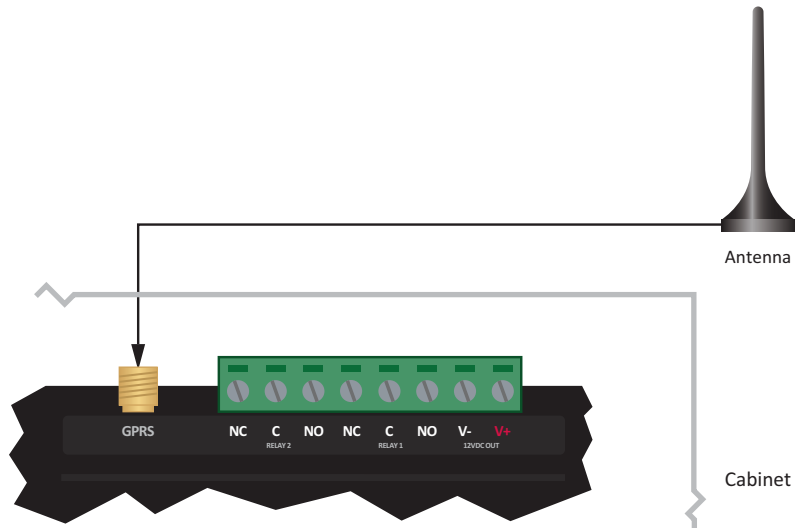
Ethernet 10/100 Direct Connection

5.4 GPRS Interface



This information only applies to the PostX modules that support GPRS and/or WIFI communication.

The antenna must be installed outside the DIN Rail cabinet.



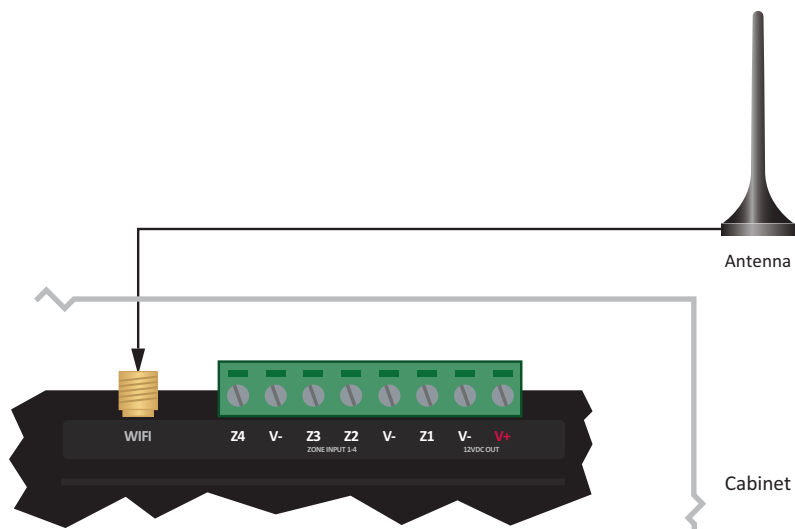
GPRS Antenna connection

5.5 WiFi Interface



This information only applies to the PostX modules that support GPRS and/or WIFI communication.

The antenna must be installed outside the DIN Rail cabinet.



WiFi Antenna connection

6 Interface Configuration

This section details how to establish an Ethernet connection with the PostX Module. When the module comes out of the box it is set to a static IP address of 192.168.1.2 with a subnet mask of 255.255.255.0 for the Ethernet interface. If your computer network is on this subnet, and no other computer on the network uses this address, then you will be able to connect to the PostX Module immediately.



Installing the PostX Module on an active network requires knowledge of the configuration and structure for the network. Always consult the network or system administrator and ask them to provide you with a fixed IP address that can be assigned to the module.

6.1 Establishing Ethernet Connection

DIN Rail PostX IP Reporting Module IP Settings

Before attempting to connect to the PostX Module it is necessary to know the IP address that it is currently set to. The default factory setting for the Ethernet interface IP address of the PostX Module will be:

192.168.1.2

The suggested methods for connecting your PC or laptop to the PostX Module include via either a switch/hub or a direct connection as shown in the section Ethernet 10/100 Network Interface (see page 13).

PC/Laptop IP Settings

You should then configure your PC or laptop's network interface to use the following settings:

IP Address: 192.168.1.4 – 192.168.1.254

Subnet Mask: 255.255.255.0

Please select the IP address for your PC or laptop from the range given above, ensuring it is not currently in use by any other device connected to your network. For information on configuring the network interface for your PC or laptop, please visit the Web Support Centre for your particular operating system. Guides for the following operating systems can be found at:

- **Microsoft® Windows XP**
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/howto_enable_dhcp.mspx?mfr=true
- **Microsoft® Windows Vista**
<http://windows.microsoft.com/en-US/windows-vista/Change-TCP-IP-settings>
- **Microsoft® Windows 7**
<http://windows.microsoft.com/en-US/windows7/Change-TCP-IP-settings>

Should the IP address need to be restored to the default value, please refer to the section on IP Troubleshooting (see page 37) for more details.

7 Web Interface

Configuration for the PostX Module is done through the built in web interface. To access, open an Internet browser (such as Internet Explorer or Mozilla Firefox) and type the IP address of the PostX Module into the address bar. As all of the web pages in the PostX Module are secure, the login screen will appear first. You must have a valid username and password to continue.



To ensure the web interface is displayed correctly, it may be necessary to enable compatibility mode in your web browser. To turn on compatibility view, go to the Tools menu and choose *Compatibility View* settings. Consult your browser help file for additional instructions.

7.1 User Login

By default, the PostX Module comes with two users for the web interface:

Username	Password	Access Level
admin	admin	Administrator
user	user	User

Web Interface Login

Once you enter a valid username and password, the Web Server home page is displayed. From here you can access all of the other pages through the menu on the left.

Please refer to Web User Management (see page 36) for more details about user login.

7.2 Routing Setup

To configure the routing options select the **Routing Setup** link using the web interface. The following shows an example configuration for the PostX Module.

ICT.
Mon Jun 04 11:45:24 2012

Routing Setup

Home

Configuration

Routing Setup

Advanced

IO Control

Network

Email

Ethernet

WiFi

GPRS / SMS

PSTN

Events

Statistics

Users

Logout

Site Name:

Account Code:

Always use this account code (not applicable when using ArmorIP)

Routing Channels

Name	Interface	IP Address/Hostname	Port	Format
CH1	<input type="text" value="Ethernet"/>	<input type="text" value="192.168.10.120"/>	<input type="text" value="9467"/>	<input type="text" value="Armor IP (U)"/>
CH2	<input type="text"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="Armor IP (U)"/>
CH3	<input type="text"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="Armor IP (U)"/>
CH4	<input type="text"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="Armor IP (U)"/>

Polling

Name	Enable	Polling status	Code	Group	Number
CH1	<input checked="" type="checkbox"/>	Primary Polling	<input type="text"/>	<input type="text"/>	<input type="text"/>
CH2	<input type="checkbox"/>	No polling	<input type="text"/>	<input type="text"/>	<input type="text"/>
CH3	<input type="checkbox"/>	No polling	<input type="text"/>	<input type="text"/>	<input type="text"/>
CH4	<input type="checkbox"/>	No polling	<input type="text"/>	<input type="text"/>	<input type="text"/>

Poll Time: (secs)

Test Report

Name	Enable	Code	Group	Number	Time (Hours)
CH1	<input type="checkbox"/>	<input type="text" value="602"/>	<input type="text" value="01"/>	<input type="text" value="000"/>	<input type="text" value="24"/>
CH2	<input type="checkbox"/>	<input type="text" value="602"/>	<input type="text" value="01"/>	<input type="text" value="000"/>	<input type="text" value="24"/>
CH3	<input type="checkbox"/>	<input type="text" value="602"/>	<input type="text" value="01"/>	<input type="text" value="000"/>	<input type="text" value="24"/>
CH4	<input type="checkbox"/>	<input type="text" value="602"/>	<input type="text" value="01"/>	<input type="text" value="000"/>	<input type="text" value="24"/>

Communication Failure

Name	Enable	Code	Group	Number
CH1	<input type="checkbox"/>	<input type="text" value="354"/>	<input type="text" value="00"/>	<input type="text" value="000"/>
CH2	<input type="checkbox"/>	<input type="text" value="354"/>	<input type="text" value="00"/>	<input type="text" value="000"/>
CH3	<input type="checkbox"/>	<input type="text" value="354"/>	<input type="text" value="00"/>	<input type="text" value="000"/>
CH4	<input type="checkbox"/>	<input type="text" value="354"/>	<input type="text" value="00"/>	<input type="text" value="000"/>

General Options

These options apply to all modes of operation.

- **Site Name**
The site name should be set to a useful name as it is included with each ArmorIP reporting message sent to the monitoring station.
- **Account Code**
This is the account code that is sent with each ArmorIP or Contact ID reporting message sent to the monitoring station.
- **Always use this Account Code**
Selecting this option will replace the account code in the received Contact ID message with this account code. **This option is not applicable when using ArmorIP.**

Routing Channels

The PostX Module can be programmed with up to 4 communication channels in order to report any incoming Contact ID messages from the connected alarm panel. Each channel is fully configurable as to what type of communication interface to use (Ethernet, WiFi, GPRS or PSTN). If communication fails on the first programmed channel, the next programmed channel will then try to send the signal. If that channel fails, the next one will be used, and so on. Whether the last signal was sent through the primary or a backup channel, the whole sequence will be repeated on the next incoming event.



Due to memory restrictions with PostX hardware revision 020 and below, the IP Address/Hostname field is limited to a maximum of 32 characters each for Routing Channels 3 and 4, and to a maximum of 256 characters each for Channels 1 and 2.

With PostX hardware revision 030 and above, this field supports a maximum of 256 characters for each channel.

The reporting sequence is on a module base, meaning that an event will be reported once on only one channel, the first that succeeds.

All necessary parameters needed for a channel to report will be entered in that section.

For the IP interfaces (Ethernet, WiFi and GPRS), the IP address or host name, the IP port and the reporting format will be programmed here. Before setting these options you must contact your monitoring station in order to get them.



Most networks will have a firewall between the PostX Module and the Internet. It is necessary to configure the firewall to allow the IP messages through so the PostX Module can communicate with the monitoring station. If the port being used is 10000 and you are using ArmorIP (UDP) the firewall must let UDP packets on 10000 through, both inbound and outbound.

For the PSTN interface, the phone number and reporting format will be programmed here. Again, before setting these options you must contact your monitoring station in order to get them.

IP Reporting Formats

The PostX Module supports eight IP reporting formats and two PSTN reporting formats. For all IP based formats the IP address and port of the monitoring station must be entered.

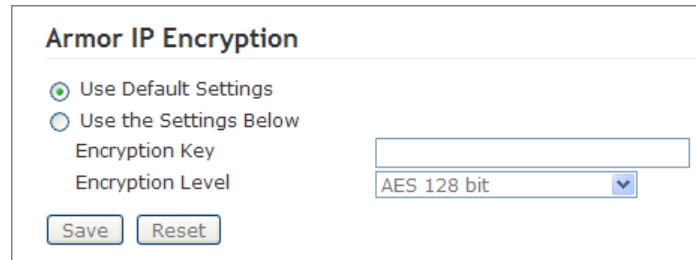
- **ArmorIP (UDP)**
This format communicates with an ArmorIP server using UDP as the transport layer. When using this format the account code must be set to the same account that is saved in the ArmorIP Server the PostX is communicating with. Using UDP to send the messages is faster than TCP as it is a connectionless protocol, the ArmorIP (UDP) protocol includes acknowledge and retry messages to ensure that the message has been received by the server.

- **ArmorIP (TCP)**

This format is identical to ArmorIP (UDP) except it uses TCP as the transport layer.

- **ArmorIP-E (UDP)**

This is the encrypted version of the ArmorIP protocol, using UDP as the transport layer. It uses an AES encryption algorithm that is selectable for 128, 192 or 256 bit encryption. The encryption settings can be found on the *Advanced* page of the PostX Module. If *Use Default Settings* is selected, make sure that this is also selected in the ArmorIP server. When this is selected, no other details need to be entered. If you want to increase the security, use a custom key that must be entered in both the PostX Module and the ArmorIP server.



ArmorIP Encryption



For maximum security it is recommended using an encryption key that contains both letters and numbers and does not form a known word. The encryption key is case sensitive.

- **ArmorIP-E (TCP)**

This format is identical to ArmorIP-E (UDP) except it uses TCP as the transport layer.

- **Contact ID (UDP)**

This format is an ASCII based format that only contains the Contact ID message. In all instances, the message will be 16 characters long with the format detailed below.

The form of the message is: ACCT MT QXYZ GG CCC S, where:

ACCT	4 Digit Account Number
MT	2 Digit Message Type
Q	1 Digit Event Qualifier
XYZ	3 Digit Event Code
GG	2 Digit Group Number
CCC	3 Digit Zone Number
S	1 Digit Checksum

To acknowledge this message the server must send back an identical copy of this message. UDP is used as the transport layer for this protocol.

- **Contact ID (TCP)**

This format is identical to Contact ID (UDP) except it uses TCP as the transport layer.

- **CSV-IP**

This format uses TCP as the transport layer and communicates with central station receivers supporting that format.

- **Patriot LS30**

This TCP format communicates with the LS30 task in Patriot alarm monitoring software.

PSTN Reporting Formats

- **Contact ID**
This is the standard Ademco Contact ID protocol.
- **SIA**
This is the standard SIA 2000 protocol.

Polling

Depending on the interface and format selected for a specified channel, its polling can be enabled. When enabled, the polling will send a poll message to the monitoring station every x seconds (the Poll Time value). It is recommended to use this option to help monitor the Internet link between your PostX Module and the monitoring station.

If the poll message fails, the PostX Module will then try to send it through the next programmed channel that also has its polling feature enabled. If that channel fails, the next one will be used, and so on. Whether the last poll message was sent through the primary or a backup channel, the whole sequence will be repeated on the next poll message.

As with the reporting sequence, the polling sequence is on a module base, meaning that a poll message will be reported once on only one channel, the first that succeeds.

Polling is available only on IP interfaces (Ethernet, WiFi and GPRS) not PSTN.

Furthermore, reporting formats ArmorIP (UDP) and ArmorIP-E (UDP) have dedicated values for the actual poll message and therefore cannot be changed/programmed. All other IP formats can have customized poll messages.

Test Report

A test report is a signal sent to the monitoring station validating the operation of all programmed channels from the Routing Channels (see page 18) section. The interval at which this signal is sent is configurable under Time (Hours) and can range between 1 to 168 hours (1 week).

As opposed to the reporting and polling sequences, the test report sequence is on a channel base, meaning that all channels that have the test report feature enabled, will send their respective programmed codes to their monitoring station via their interface. If the test report fails on a channel, the PostX Module will not try to send it through the next available channel, instead it will disregard this signal and wait for the next test report to occur.

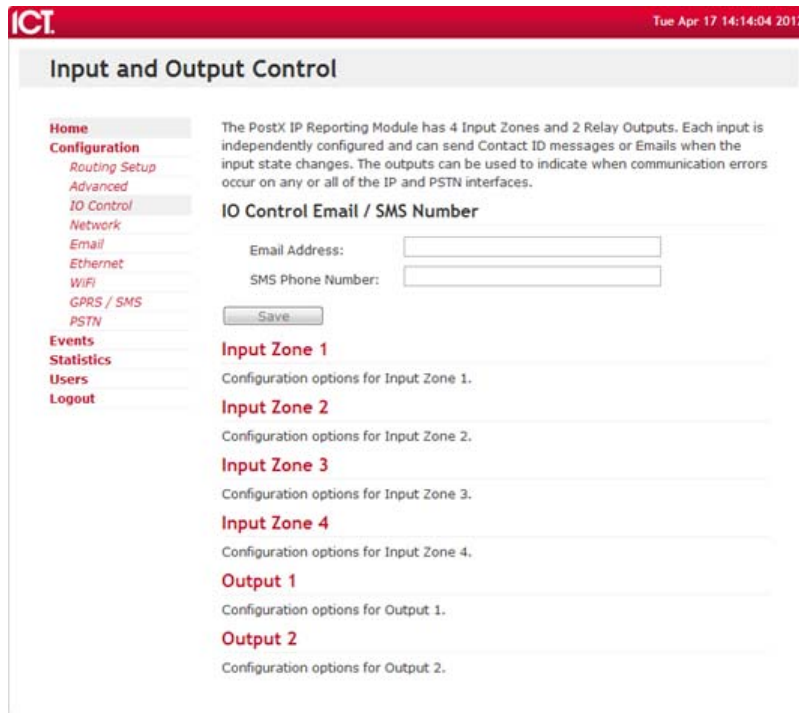
Communication Failure

Communication failure signals are sent to the monitoring station indicating that a channel became unusable for some reason (interface failure, unable to reach the monitoring station etc). If channel one becomes faulty and its communication failure feature is enabled, the next available channel will then send channel one's programmed failure code.

As with the reporting and polling sequences, the communication failure sequence is on a module base, meaning that a communication failure message will be reported once on only one channel, the first that succeeds.

7.3 Input and Output Control

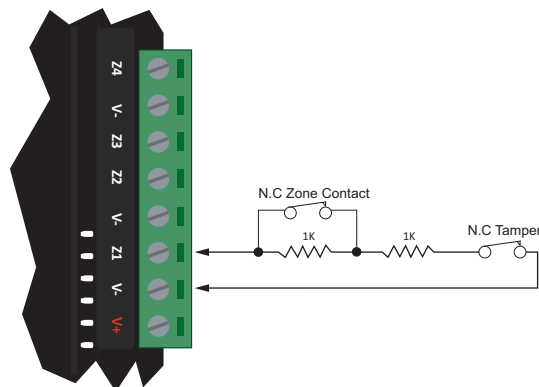
The PostX Module has 4 inputs and 2 outputs. Each input is independently configured and can send Contact ID messages, emails, or SMS messages when the input state changes. The outputs can be used to indicate when communication errors occur.



Zone Inputs

The PostX Module can monitor the state of up to 4 zone inputs using EOL monitored or dry contact devices such as magnetic switches, PIR motion detectors and temperature thermostats. Devices connected to these zones can be installed to a maximum distance of 300m (1000ft) from the PostX Module when using 22 AWG wire. Each zone input may be individually configured for normally opened or normally closed configurations with or without EOL resistors for tamper and short condition monitoring.

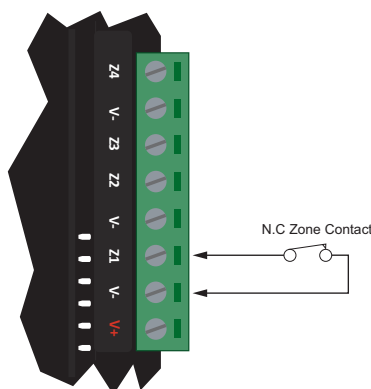
When using a zone with the EOL resistor configuration, the PostX Module generates an alarm condition when the state of a zone changes between open and closed and generates a tamper alarm condition when a wire fault (short circuit) or a cut wire (tampered) in the line occurs.



EOL Resistor Zone Configuration

When using the EOL resistor configuration, the zone input is in the closed state when there is 1k Ohm resistance between the terminal and ground. If the zone contact opens, leaving 2k Ohm resistance between the terminal and ground, the zone moves into the open state.

Each zone input can use a different input configuration. When using the No Resistor configuration (i.e. EOL Resistor option not checked), the PostX Module only monitors the opened and closed state of the connected input device generating the (OPEN) alarm and (CLOSED) sealed conditions.



Normally Closed Zone Configuration No Resistors

Contact ID Messages

Each input can be independently configured to send an Ademco Contact ID message when the zone changes state. These messages will be sent using the settings defined under the Routing Setup (see page 17). In other words, they will be treated the same as messages received from the alarm panel connected to the PostX.

- **Account Code**

This is a 4 digit code that the monitoring station uses to identify where the Contact ID message has come from.

- **Alarm Code**

This is the standard 3 digit Contact ID event code to indicate the type of event that is being reported. The following table shows some example event codes that may be used. It is recommended that you always consult your monitoring station for more details regarding the specific event codes to use.

Alarm Code	Event Type
130	Burglary Alarm
140	General Alarm
146	Silent Burglary
150	24 hour Non-Burglary
300	System Trouble
380	Sensor trouble

- **Tamper Code**

This is the standard 3 digit Contact ID event code to indicate the type of event that is being reported. The following table shows an example event code that may be used. It is recommended that you always consult your monitoring station for more details regarding the specific event codes to use.

Tamper Code	Event Type
137	Input Loop Cut/Shorted

- **Group Number**

The Group Number or Area Number is a 2 digit code to indicate the group or area that the even belongs to. Use 00 to indicate there is no specific group or area information.

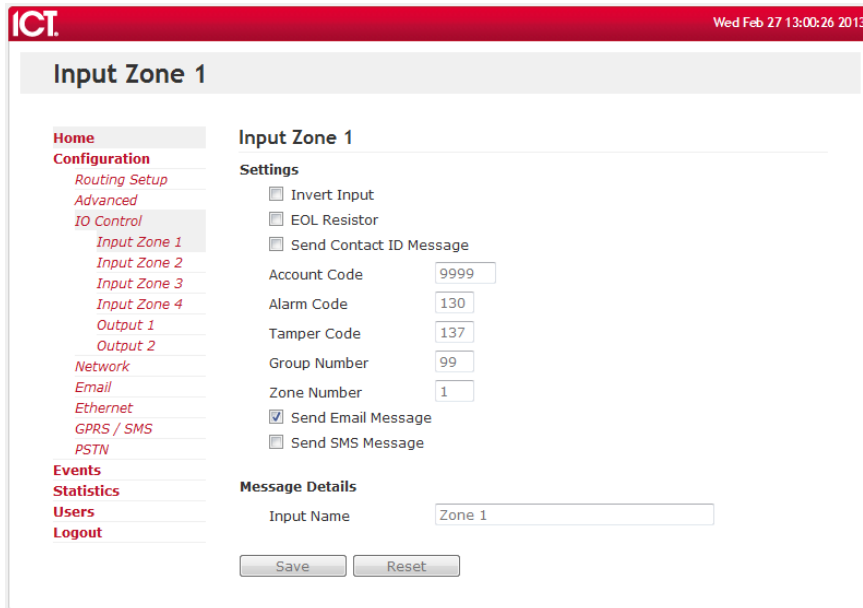
- **Zone Number**

The Zone Number or User Number is the 3 digit code to indicate the specific zone that has had the event. Use 000 to indicate that there is no specific zone or user information.

Email Messages

Each input can also be configured to send an email when the input changes state. This email is sent to the email address defined in the main Input Output Control settings (see page 21).

To have an input send an email, the **Send Email Message** option must be enabled.



For the settings shown above, when the input opens, the following email will be sent by the PostX Module:

Site Name: ICT PostX Module
Zone Message: Zone 1 Opened
Time Stamp: Wed Feb 17 13:00:26 2013

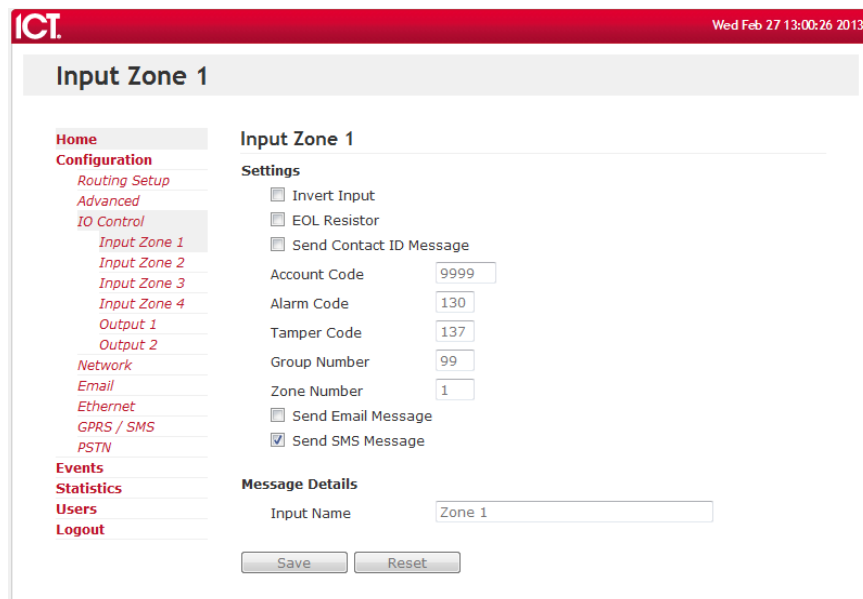
SMS Messages



This information only applies to the PostX modules that support GPRS and/or WIFI communication.

Each input can also be configured to send an SMS when the input changes state. This SMS is sent to the SMS phone number defined in the main Input Output Control settings (see page 21).

To have an input send an SMS, the **Send SMS Message** option must be enabled.



For the settings shown above, when the input opens, the following SMS will be sent by the PostX Module:

Site Name:	ICT PostX Module
Zone Message:	Zone 1 (Zone 1) Opened
Time Stamp:	13:00:26 27/02/2013

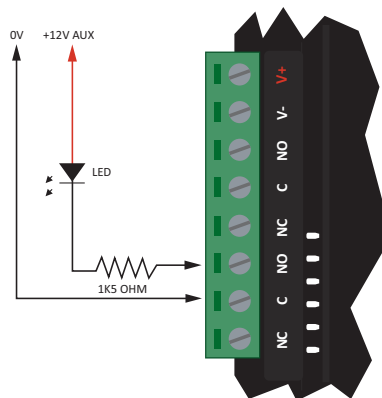
Programmable Outputs

The PostX Module has 2 programmable outputs. These outputs can be configured to be activated when the PostX Module loses a connection. Additionally, the outputs can be used to activate bell sirens, lighting circuits, door locks, relay accessory products and other automation points through SMS messages.



In order to enter any of the IP troubleshooting modes, Relay 1 on the PostX Module will enable briefly on startup. To prevent this from occurring, ensure that at least one of the zone inputs is wired directly to V-.

The 2 Outputs each have a FORM C output relay. The connection example below shows the control of an external LED indicator.



Output Connection (Output 2 Shown)



Warning: Switching inductive loads that can produce high back EMF voltages or large voltage induced spikes can cause the PostX Module to behave unexpectedly and should be avoided. A suitable isolation circuit must be installed between the relay contacts of the PostX Module and the inductive load.

The following shows the various settings that can be applied to these 2 outputs.

The screenshot shows the ICI web interface for configuring Output 1. The interface is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes sections for Home, Configuration (with sub-items like Routing Setup, Advanced, IO Control, Network, Email, Ethernet, WiFi, GPRS / SMS, PSTN), Events, Statistics, Users, and Logout. The main configuration area is titled 'Output 1' and contains several sections: 'Settings' with checkboxes for 'Invert Output', 'Disable when Input in Alarm', and four 'Input Zone' options; 'On Time' and 'Off Time' input fields with 'seconds' labels; 'Activate On' section with checkboxes for various failure events; and 'Receive SMS Activation' section with checkboxes for 'Enable SMS activation' and 'Enable password', and text input fields for 'Output name' (containing 'Garage') and 'Activation password' (containing '123abcd'). At the bottom of the configuration area are 'Save' and 'Reset' buttons.

- **Invert Output**
When enabled, the state of the output will be inverted.
- **On Time**
When the On Time is configured to be non-zero, the output will activate for this number of seconds and then turn off. If the Off Time is also configured to be non-zero, the output will only remain off for the period of time set, before turning on again for the On Time. Configuring both the On and Off Time creates a pulsed output. The On Time can be configured with a value ranging from 0-255 seconds.
- **Off Time**
When the On and Off Time are configured to be non-zero, the output will pulse on and off for the period of time set. The Off Time can be configured with a value ranging from 0-255 seconds.
- **Activate On**
The output can be activated based on the selected failure/s below:
 - Any Channel Failure
 - Channel 1 Failure
 - Channel 2 Failure
 - Channel 3 Failure
 - Channel 4 Failure
 - Primary Ethernet Gateway Failure
 - Secondary Ethernet Gateway Failure

- Primary WiFi Gateway Failure
- Secondary WiFi Gateway Failure

If more than one option is selected, use the OR/AND conditions to determine if at least one of them or all of them have to be met in order to activate.

- **Receive SMS Activation**

The output can also be activated/deactivated via a SMS message. The SMS format to be used is as follows:

<activation password> <output name> <action> <ack>

The PostX module is not case sensitive. The following table describes the control word:

Action	Code
Turn PGM ON	on, On, ON, or 1
Turn PGM OFF	off, Off, OFF, or 0
Acknowledge SMS	ack, Ack, ACK, a, A or 1

For the following examples, PGM 1 has been set with validate by pin, acknowledge by request and the command **garage**. PGM 2 has been set with validate by any, no acknowledge and the command **gate**. This pin code has been set to **house**.

SMS Message	Action
house garage on ack	PGM 1 turned on, and acknowledge SMS sent
house garage off a	PGM 1 turned off, and acknowledge SMS sent
garage on ack	No action taken, pin code (house) not entered
house garage 1 1	PGM 1 turned on, and acknowledge SMS sent
gate on ack	PGM 2 turned on, and acknowledge SMS sent
gate 1	PGM 2 turned on, no acknowledge SMS sent
house garage 1 1 gate 1	PGM 1 turned on, and acknowledge SMS sent, gate is not handled, a separate SMS has to be used

If the Enable password option is set, the SMS control requires the Activation password to be correct for any operation to be performed. The activation password is sent at the start of the message. For example, if the activation password set was **123abcd** you would send **123abcd garage on ack** to open the garage door. If the activation password is wrong, no response is sent to the user even if an acknowledgment is requested.

7.4 Email Events

The PostX Module can send an email to a selected address when any of the four connected inputs change state. If this option is being used the outgoing mail server (SMTP) must be configured.

The screenshot shows the 'Email Setup' configuration page. The left sidebar contains a navigation menu with the following items: Home, Configuration (Routing Setup, Advanced, IO Control, Network, Email, Ethernet, WiFi, GPRS / SMS, PSTN), Events, Statistics, Users, and Logout. The main content area is titled 'Email Setup' and is divided into three sections: 'User Information' with a 'PostX Email Address' text input field; 'Interface' with a dropdown menu currently set to 'Ethernet'; and 'Server Information' with an 'Outgoing Mail Server (SMTP)' field (displaying four '0' characters), a checked checkbox for 'My SMTP server requires authentication', 'Username' and 'Password' text input fields, and a 'Test Account Settings...' link. At the bottom are 'Save' and 'Reset' buttons.

To ensure the emails get through and are not stopped by spam filters, a valid email address must be entered. The PostX Module does not receive any email, so you can use any active email address.

The interface on which the emails will be sent is selectable. Ethernet is available on all variants of the PostX. The others depend on the model. WiFi will be available on the WF variants while the GPRS IP on the GP variant.

The IP address of the SMTP server that is to be used needs to be entered. If the SMTP server is not provided by the ISP (Internet Service Provider) the PostX Module is using, then authentication is required. Enter the username and password for the account into the appropriate fields as shown above.

Once the settings are entered, click **Test Account Settings...** to send a test email. The PostX Module will attempt to send an email to the address specified. If it does not get through in a reasonable amount of time, recheck your settings.

7.5 Ethernet Configuration

If you can connect to the PostX Module the easiest way to change the IP address is using the web interface. Open up an Internet browser (e.g. Internet Explorer or Mozilla Firefox) and type the IP address of the PostX Module into the address bar. The User Login screen will appear for you to enter a valid username and password.



To help ensure your PostX Module cannot be configured by invalid users, change the default passwords for the web interface before commissioning the installation.

The screenshot shows the 'Ethernet' configuration page in the PostX Module web interface. The page has a red header with the 'ICT' logo and the date 'Tue Jun 05 10:56:50 2012'. A left-hand navigation menu includes options like Home, Configuration, Routing Setup, Advanced, IO Control, Network, Email, Ethernet (selected), WiFi, GPRS / SMS, PSTN, Events, Statistics, Users, and Logout. The main content area is titled 'Ethernet' and contains the following sections:

- Home**: A brief introduction to IP settings.
- Configuration**:
 - Physical Address: 00-1b-c2-7e-67-17
 - Obtain an IP address automatically (radio button selected)
 - Use the following IP Address (radio button unselected):
 - IP Address: 192.168.1.2
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - Alternate Gateway: 0.0.0.0
- Domain Name Server**:
 - Preferred DNS Server: 8.8.8.8
 - Alternate DNS Server: 0.0.0.0
- Ethernet Monitoring**:
 - Ethernet monitoring:
 - Ethernet fail Event Code: 350
 - Ethernet fail Group Number: 00
 - Ethernet fail Zone Number: 001
- Restart**: A section with a 'Restart' button and a link to 'Click here' to restart the PostX.

There are two options for configuring the IP address of the PostX Module:

- **IP Configuration via DHCP**
To enable the DHCP service, select the **Obtain an IP address automatically** option.
- **Static IP Configuration**
To assign a static IP, select the **Use the following IP Address** option and enter the new IP address, subnet mask and default gateway you wish to use.

Once all the changes have been made, click **Save** to save the changes. You must restart the PostX Module for the changes to take effect.

7.6 WiFi Configuration



This information only applies to the PostX modules that support GPRS and/or WIFI communication.

When the PostX Module comes out of the box it is set with a static IP address of 192.168.1.3 with a subnet mask of 255.255.255.0 for the WiFi interface. If your computer network is on this subnet, and no other computer on the network uses this IP address, you will be able to connect to the PostX module immediately.

ICI Tue Jun 05 11:13:43 2012

WiFi

Home
Configuration
Routing Setup
Advanced
IP Control
Network
Email
Ethernet
WiFi
GPRS / SMS
PSTN
Events
Statistics
Users
Logout

You can get IP settings assigned automatically if your network supports this capability. Otherwise you need to ask your network administrator for the appropriate IP settings.

Physical Address 00-23-a7-1f-96-36

Obtain an IP address automatically
 Use the following IP Address

IP Address 192 168 1 3
Subnet Mask 255 255 255 0
Default Gateway 192 168 1 1
Alternate Gateway 0 0 0 0

Domain Name Server

Preferred DNS Server 8 8 8 8
Alternate DNS Server 0 0 0 0

Access Point

SSID (case sensitive)
WEP/WPA Password

Apply Above Settings Now

Go to scan mode...

WiFi Monitoring

WiFi monitoring:
WiFi fail Event Code 350
WiFi fail Group Number 00
WiFi fail Zone Number 002

Interface Status

Link Status: ESTABLISHED
IP Address: 192.168.1.3
Module Status: Connected
Duration: 0 day(s) 00:33:39
RSSI Level: LEVEL -54dBm

Restart

To restart the PostX Click [here](#).



Installing the PostX Module on an active network requires knowledge of the configuration and structure for the network. Always consult the network or system administrator and ask them to provide you with a fixed IP Address that can be assigned to the PostX Module.

DIN Rail PostX IP Reporting Module IP Settings

Before attempting to connect to the PostX Module it is necessary to know the IP address that it is currently set to. The default factory setting for the WiFi interface IP address of the PostX Module will be: **192.168.1.3**

The suggested methods for connecting your PC or laptop to the PostX Module include via either a switch/hub or a direct connection as outlined in the section on the Ethernet 10/100 Network Interface (see page 13).

Access Point Information Settings

Before communicating over WIFI, the following must be set:

- **SSID:** WIFI network identification name. Maximum of 32 characters and case sensitive.
- **WEP / WPA / WPA2 Password:** Security password for secured access point. Maximum of 32 characters.
- **Security supported:** WEP / WPA / WPA2

The PostX module's WiFi security mode will adapt to the access point selected in the scanned list under "Scan Mode" or when connecting to the specified SSID.

PC/Laptop IP Settings

You should then configure your PC or laptop's network interface to use the following settings:

IP Address: 192.168.1.4 – 192.168.1.254

Subnet Mask: 255.255.255.0

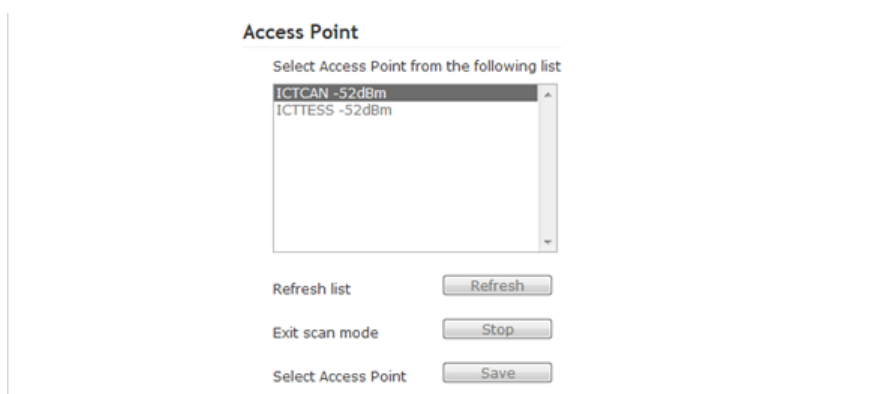
Please select the IP address for your PC or laptop from the range given above, ensuring it is not currently in use by any other device connected to your network. For information on configuring the network interface for your PC or laptop, please visit the Web Support Centre for your particular operating system. Guides for the following operating systems can be found at:

- **Microsoft® Windows XP**
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/howto_enable_dhcp.mspx?mfr=true
- **Microsoft® Windows Vista**
<http://windows.microsoft.com/en-US/windows-vista/Change-TCP-IP-settings>
- **Microsoft® Windows 7**
<http://windows.microsoft.com/en-US/windows7/Change-TCP-IP-settings>

Should the IP address need to be restored to the default value, please refer to the section on IP Troubleshooting (see page 37) for more details.

Scan Mode

You can also select an access point from a list of available networks in your area. Click **Scan...** to display a list of available access points.



- Click **Refresh** to initiate another scan.
- Click **Stop** to exit scanning mode and return to enter parameters manually.
- Click **Save** to save the network you have selected and return to enter parameters manually.

7.7 GPRS / SMS Configuration



This information only applies to the PostX modules that support GPRS and/or WIFI communication.

In order to establish a GPRS connection, the following settings must be entered:

GPRS Settings

Home
Configuration
Routing Setup
Advanced
IO Control
Network
Email
Ethernet
WiFi
GPRS / SMS
PSTN
Events
Statistics
Users
Logout

APN Settings

APN:
User name:
Password:
Save Reset

GPRS Monitoring

GPRS monitoring:
GPRS fail Event Code:
GPRS fail Group Number:
GPRS fail Zone Number:
Save Reset

Interface Status

Link Status: ESTABLISHED
IP Address: 25.48.125.103
Module Status: Connected
Duration: 0 day(s) 00:00:08
RSSI Level: LEVEL 4

- **APN:** Access Point Name. Maximum of 100 characters.
- **User name:** Maximum of 32 characters.
- **Password:** Maximum of 32 characters.

Contact your local network provider for assistance with the information required.

Should anything go wrong while using the GPRS interface, an error code is displayed on the Events page.

7.8 PSTN Configuration

PSTN Settings

Home
Configuration
Routing Setup
Advanced
IO Control
Network
Email
Ethernet
WiFi
GPRS / SMS
PSTN
Events
Statistics
Users
Logout

PABX Settings

PABX Emulation:
PABX Number:
Save

Line Monitoring

Phone line monitoring:
Phone line fail Event Code:
Phone line fail Group Number:
Phone line fail Zone Number:
Save

- **PABX Emulation**
If the alarm panel the PostX Module is connecting to is expecting to dial through a PABX this option needs to be enabled. When the PABX number is dialled the PostX Module starts the dial tone again until the panel starts dialling the external line.
- **PABX Number**
This is the number the panel dials to obtain an external line and must be set if the PABX emulation is enabled.

8 Advanced Configuration

ICT Tue Jul 10 15:00:44 2012

Advanced Configuration

Home
Configuration
Routing Setup
Advanced
IO Control
Network
Email
Ethernet
WiFi
GPRS / SMS
PSTN
Events
Statistics
Users
Logout

General Settings

Modem Dial Attempts:
Modem Dial Time: secs
Max Report Count:
Max IP Attempts:
IP Connection Timeout: secs
Log Poll Events:

TCP/IP Serial Port

Enable TCP/IP Serial Port

TCP Port:
Baud Rate:
Data Bits:
Parity Bits:
Stop Bits:

System Started Message

Send System Started Message on Power Up

System Started Event Code:
System Started Group Number:
System Started Zone Number:

Armor IP Encryption

Use Encryption

Encryption Key:
Encryption Level:

CSV-IP Settings

Account Name:
Account Password:

PSTN Pass Through

Duration (1-255 mins):
Remaining time: deactivated

Restart

To restart the PostX Click [here](#).

Firmware Update

To put the PostX into boot mode and do a firmware update click [here](#). NOTE: We do not recommend doing this remotely.

8.1 General Settings

- **Modem Dial Attempts**

The Modem Dial Attempts is the maximum number of attempts the PostX Module will make to dial a PSTN monitoring station. Once this number of attempts is exceeded the PostX Module will change to use the next phone number or reporting path.
- **Modem Dial Time**

The Modem Dial Time is the length of time in seconds between phone calls.
- **Max Report Count**

The Maximum Report Count is the maximum number of Contact ID messages that will be sent to the monitoring station in one connection. When this is exceeded the PostX Module disconnects from the monitoring station and waits for the period of time set in Modem Dial Time before attempting to call the monitoring station again (if there are more messages to send).
- **Max IP Attempts**

The Max IP Attempts is the maximum number of times the PostX Module will attempt to send a message to a monitoring station for the IP formats.
- **IP Connection Timeout**

The IP Connection Timeout is the number of seconds the PostX Module waits for a response for an IP message.
- **Log Poll Events**

Log the send poll and received ACK poll events. Disabling this option will leave more space for other events in the buffer.

8.2 TCP/IP Serial Port

This feature allows you to use the PostX's on-board serial port remotely via TCP/IP.

- **Enable TCP/IP Serial Port**

When checked, the TCP/IP Serial Port feature is enabled.
- **TCP Port**

Enter here the TCP port number to be used when communicating with the PostX.
- **Baud Rate**

Select the baud rate at which the PostX's serial port will be communicating.
- **Data Bits**

Select the data length for the serial port.
- **Parity Bits**

Select the parity for the serial port.
- **Stop Bits**

Select the number of stop bits for the serial port.

8.3 System Started Message

The system started message option lets you decide if you want the PostX to send a message to the monitoring station upon start up.

- **Send System Started Message On Power Up**

When checked, the PostX will send a message to the monitoring station.
- **System Started Event Code**

This is the standard 3 digit Contact ID event code to indicate the type of event that is being reported.

- **System Started Group Number**

The Group Number or Area Number is a 2 digit code to indicate the group or area that the event belongs to. Use 00 to indicate there is no specific group or area information.

- **System Started Zone Number**

The Zone Number or User Number is the 3 digit code to indicate the specific zone that has had the event. Use 000 to indicate that there is no specific zone or user information.

It is recommended that you always consult your monitoring station for more details regarding the specific event codes to use.

8.4 CSV-IP Settings

This is where you enter the parameters needed if you use the IP reporting format CSV-IP.

- **Account Name**

CSV-IP format account name.

- **Account Password**

CSV-IP format account password.

8.5 PSTN Pass Through

This feature is only available from hardware revision 040 and later of the PostX Module.

PSTN Pass Through gives you the ability to temporarily connect the security control panel directly to the telephone line. This allows you to now call the panel and make any maintenance or programming via that telephone line.

- **Duration (1-255 mins)**

The amount of time the pass through feature will be activated. Valid entries are from 1 to 255 minutes inclusively.

- **Remaining Time**

Displays the time remaining before the pass through relay deactivates.

- **Activate**

Once a valid activation duration is entered, clicking this button will activate the pass through relay for that period of time.

- **Deactivate**

Once activated, the pass through relay can forcibly be deactivated before the duration expires by clicking this button.

- **Refresh**

Clicking this button will update the time remaining display.

Note that the **PSTN Pass Through** feature can also be accessed locally via command line. Refer to the section on Command Line Interface Commands for details.

9 Duplicate Configuration

The PostX Module configuration can be uploaded and downloaded to allow easy duplication of the programming of the device. After the network settings for the PostX Module are defined, including IP address, subnet mask and gateway, all other settings can be downloaded from a configuration file.

9.1 Creating a Configuration File

To create a configuration file, set up a PostX Module with all the required settings. Open the Windows command prompt (Start->All Programs->Accessories->Command Prompt) and type in the following command using the IP address of the PostX Module:

```
tftp -i 192.168.1.2 GET config.bin
```

This will create a file called "config.bin" in the same directory where you typed in the command. This file is the default configuration file you can download to any other PostX Module.

9.2 Downloading a Configuration File

Once a configuration file has been created, it can be downloaded to any other PostX Module. Open the Windows command prompt (Start > All Programs > Accessories > Command Prompt) and change to the directory where the configuration file has been saved. Type in the following command using the IP address of the PostX Module:

```
tftp -i 192.168.1.2 PUT config.bin
```

Restart the PostX Module for the new configuration to take effect.

10 Web User Management

To access any web pages in the PostX Module, the user must be logged in. The PostX Module supports 2 users with 2 different access levels.

10.1 Setup

To edit users in the <PostX Module, navigate to the User Management web page. To do so, you must be logged in as an Administrator user.

To edit an existing user, click on the appropriate checkbox and then click **Edit**. This will open a new page where you can edit the user's settings.

To disable a user, again select the appropriate checkbox and click Edit. This will bring you back to the edit user's settings page. From there simply set the access level to none then click **Save**.

User Name	Password	Access Level
<input type="checkbox"/> admin	admin	Administrator
<input type="checkbox"/> user	user	User



To ensure the security of your PostX Module, please make sure you change the password for this user account from the default.

10.2 Access Levels

The PostX Module supports 2 access levels, Administrator and User. When logged in with an Administrator account, the user can access all pages and change any parameter. In comparison, the User access level only allows access to the home, events and statistics web pages.

10.3 Default Users

The PostX Module comes with the following two default users:

Username	Password	Access Level
admin	admin	Administrator
user	user	User

11 IP Troubleshooting

In the event of the IP address of PostX Module becoming unknown, the following 3 modes will allow you to re-establish Ethernet connection to the PostX Module.

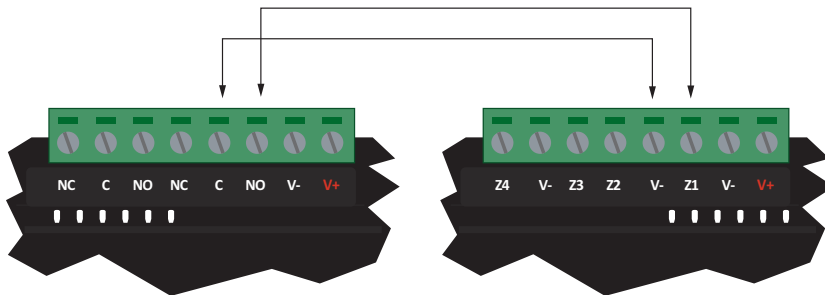


In order to enter any of the IP Troubleshooting modes, Relay 1 on the PostX Module will enable briefly on startup. To prevent this from occurring, ensure that at least one of the zone inputs is wired directly to V-.

11.1 Default Static IP Address Mode

To change the IP address to a static address of 192.168.1.2 and a subnet mask of 255.255.255.0 complete the following steps:

1. Connect the terminals for Zone 1 and NO of Relay 1 together. Repeat the procedure for the V- and C terminals as shown in the diagram below.

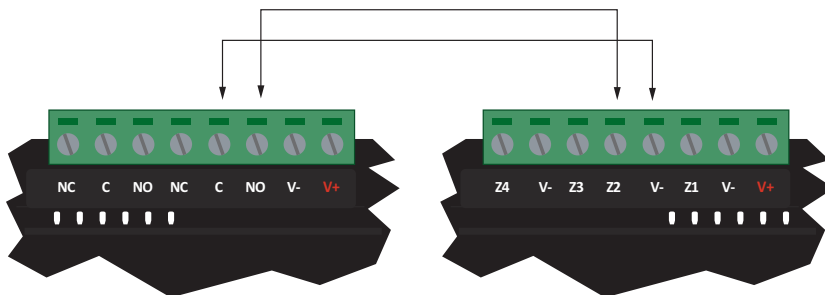


2. Enable DC supply to the PostX Module.

11.2 DHCP IP Address Mode

The PostX Module supports Dynamic IP Address Allocation (DHCP). To use this, there must be a DHCP server on the network you are attempting to connect to. If you cannot select DHCP from the web interface, complete the following steps:

1. Connect the terminals for Zone 2 and NO of Relay 1 together. Repeat the procedure for the V- and C terminals as shown in the diagram below.



2. Enable DC supply to the PostX Module.

11.3 Confirm IP Address via Command Line

Ping is an application that runs in Microsoft Windows and is a very useful tool for helping to diagnose an IP address related issue. It can be used to test a connection with the PostX Module. The following instructions detail how to ping a device:

1. Open a command prompt (Click Start->Run, then type "cmd" into this window and click "OK").
2. Type `ping 192.168.1.2` into the command prompt and press ENTER.
3. Wait for the command prompt to respond. The first of the images below shows a ping attempt where the IP address was not found. The second image shows a successful ping attempt where the IP address was found.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SUPPORT>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\SUPPORT>_
```

Console screenshot of a Ping where the IP address cannot be found

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SUPPORT>ping 192.168.1.2

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

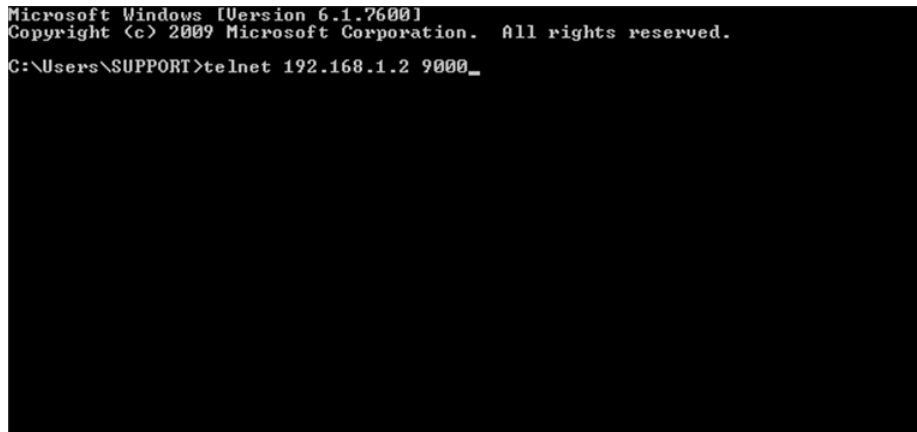
C:\Users\SUPPORT>_
```

Console screenshot of a Successful Ping

12 Command Line Interface

The PostX Module provides a command line interface to help with setup diagnostics. This can be accessed through a Telnet session (Ethernet) or through a serial port connection. The following instructions detail how to establish a Telnet session.

1. Open a command prompt (Click Start | Run, then type "cmd" into this window and click "OK").
2. Type **telnet 192.168.1.2 9000** into the command prompt and press ENTER.
3. Wait for the command prompt to respond. The command prompt "ICTNET>" will come up when a connection has been established. To terminate the telnet session, type "exit" into the command prompt.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SUPPORT>telnet 192.168.1.2 9000_
```

Starting a Telnet Session

If not using Ethernet the command line interface can be accessed through the RS485 interface.

To start using the RS485 interface, apply DC power to the PostX Module and connect the ACC-485 to both the PostX Module and an available RS232 serial port on your computer. Open a terminal program such as HyperTerminal or TeraTerm with the baud rate set to 38400 (38400, 8, n, 1). Press ENTER or ESC to get the command prompt.

12.1 Command Line Interface Commands

Command	Example	Description
arp -a	arp -a	Lists all the entries in the ARP table (IP address and MAC address details)
arp -d	arp -d	Deletes the ARP cache. This is useful if the IP address of a device you are trying to talk to has changed.
boot	boot	Restarts the PostX in boot mode. Note that this will disable the command line interface.
default	default	Defaults the PostX to factory settings
dhcp	dhcp	Displays the DHCP client details
dhcp -d	dhcp -d	Starts the DHCP server discovery process. Note: This does not change the PostX into the DHCP mode. The IP address, subnet mask and default gateway values obtained during the discovery process will become the new settings used in network configuration web interface for static IP configuration when the PostX restarts.
emac	emac	Displays statistics for the Ethernet interface
exit	exit	Disconnects an active telnet session
gprs default	gprs default	Resets GPRS parameters to factory defaults
gprs reset	gprs reset	Restarts the GPRS module
gprs set apn	gprs set apn internet.com	Sets the APN parameter of the GPRS module
gprs set user	gprs set user wapuser1	Sets the user name parameter of the GPRS module
gprs set password	gprs set password wap	Sets the password parameter of the GPRS module
gprs status	gprs status	Displays the GPRS interface status, connected/disconnected, the connection duration time and the signal strength x/5.
ipconfig	ipconfig	Lists the details of the UIP setup, IP address, gateway, subnet mask etc
ipconfig -all	ipconfig -all	Extended IP configuration details
ping	ping 192.168.1.1	Sends a ping command to the selected IP address
pstn on time	pstn on 10	Activates the PSTN pass through relay for 10 minutes
pstn off	pstn off	Deactivates the PSTN pass through relay even if the duration time has not expired
restart	restart	Restarts the PostX
set ip	set ip 192.168.1.56	Sets the IP address. The PostX must be restarted for the change to take effect.
set gateway	set gateway 192.168.1.1	Sets the gateway address. The PostX must be restarted for the change to take effect.
set mask	set mask 255.255.0.0	Sets the subnet mask. The PostX must be restarted for the change to take effect.
set dns1	set dns1 192.168.1.1	Sets the primary DNS server. The PostX must be restarted for the change to take effect

Command	Example	Description
set ntpl	set ntpl 202.156.2.125	Sets the primary SNTP server. The PostX must be restarted for the change to take effect
sntp	sntp 202.156.2.125	Updates the time from the SNTP server at the given IP address. This can be used to confirm the SNTP server is working before you save it in the network configuration.
system	system	Displays the system details including serial number and software version
time	time	Displays the current time stored in the PostX
wifi default	wifi default	Resets the WIFI parameters to factory defaults
wifi reset	wifi reset	Restarts the WIFI module
wifi set ssid	wifi set ssid ICT	Sets the SSID parameter (case sensitive) of the WIFI module
wifi set password	wifi set password 1234ab	Sets the access point password key of the WIFI module
wifi status	wifi status	Displays the WIFI interface status, connected/disconnected, the connection duration time and the signal strength x/4.


13 LED Indicators

The PostX Module includes comprehensive front panel diagnostic indicators that can aid the installer in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.





13.1 Power Indicator

The Power indicator is lit whenever the correct module input voltage is applied across the N+ and N- terminals.

State		Description
	On (green)	Correct module input voltage applied
	Off	Incorrect module input voltage applied


13.2 Status Indicator

The Status indicator displays module status of the PostX Module.

State		Description
	Slow (green) flash	Module operating normally
	On (green)	Module starting up



13.3 Fault Indicator

The Fault indicator is lit any time the module is operating in a non-standard mode.

State		Description
	Slow (red) flash	Module is in boot mode awaiting firmware update



13.4 Modem Indicator

The Modem indicator will show the status of the onboard modem.

State		Description
	On (red)	Onboard modem is off hook
	Off	Onboard modem is not active




13.5 Panel Indicator

The Panel indicator will show the status of the subscriber phone.

State		Description
	On	Subscriber phone is off hook
	Off	Subscriber phone is not active



13.6 Ethernet Indicator

The Ethernet indicator will show the status of the Ethernet connection.

State		Description
	On (green)	"Live" Ethernet connection detected
	Off	No Ethernet connection detected
	Fast (green) flash	Ethernet packet transmitted/received





13.7 Relay 1/Relay 2 Indicators

The Relay 1 and Relay 2 indicators will show the status of the lock output relay.

State		Description
	On (red)	Relay output is ON
	Off	Relay output is OFF

13.8 Zone Status Indicators

Whenever a zone input on the PostX Module changes state, the zone status will be displayed on the front panel indicator (1-4) corresponding to the physical input number (Z1-Z4). This allows you to easily walk test verification of zone inputs.

State	Description	
	Fast flash	Zone is in a SHORT state
	On	Zone is in a CLOSED state
	On	Zone is in an OPEN state
	Fast flash	Zone is in a TAMPER state

13.9 WiFi Indicator



This information only applies to the PostX modules that support GPRS and/or WIFI communication.

The WiFi indicator shows the status of the WiFi connection and signal strength.









State	Description	
	Wave constantly on	Connection available
	Wave flashing	Communication / data transfer
	WiFi constantly on / 1 bar red	Connection not established
	WiFi constantly on / All bars off	Connected RSSI level 0 (lowest signal strength)
	WiFi constantly on / 1 bar on	Connected RSSI level 1
	WiFi constantly on / 2 bars on	Connected RSSI level 2
	WiFi constantly on / 3 bars on	Connected RSSI level 3
	WiFi constantly on / 4 bars on	Connected RSSI level 4 (highest signal strength)

13.10 GPRS Indicator



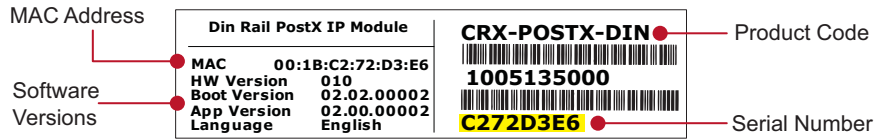
This information only applies to the PostX modules that support GPRS and/or WIFI communication.

The GPRS indicator shows the status of the GPRS connection and signal strength.

State	Description
	Wave constantly on Connection available
	Wave flashing Communication / data transfer
	GPRS constantly on / 1 bar red Connection not established
	GPRS constantly on / All bars off Connected RSSI level 0 (lowest signal strength)
	GPRS constantly on / 1 bar on Connected RSSI level 1
	GPRS constantly on / 2 bars on Connected RSSI level 2
	GPRS constantly on / 3 bars on Connected RSSI level 3
	GPRS constantly on / 4 bars on Connected RSSI level 4 (highest signal strength)

14 Identification Sticker Details

Every PostX Module has a unique identification sticker located on the unit. The identification sticker contains details that may be of use to you, such as the MAC address of the PostX Module. An example of the identification sticker is shown in the diagram below.



15 Warnings

The grant of a telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with the minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

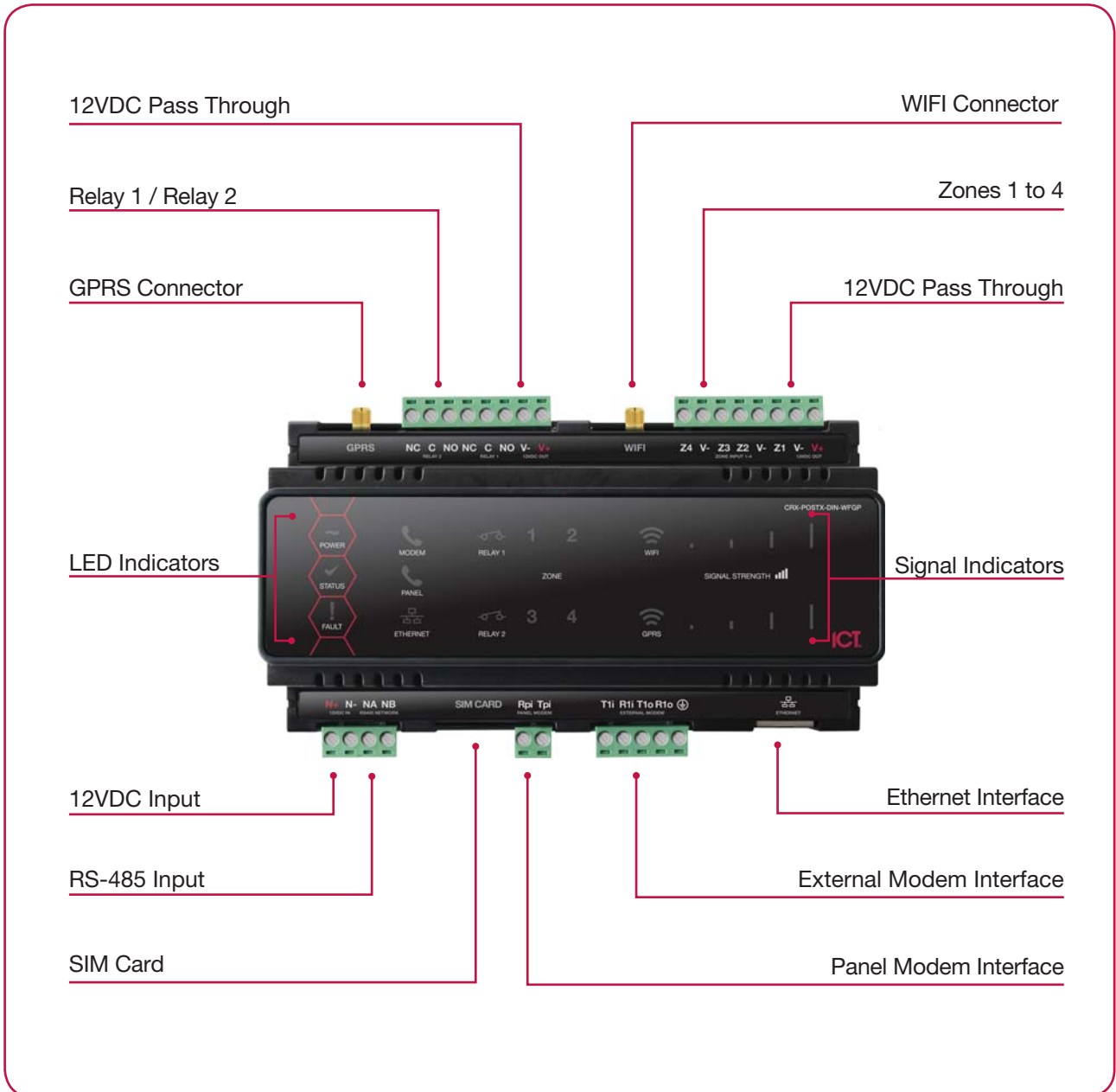
This equipment can be set up to carry out test calls at pre-determined times. Such test calls will interrupt any other calls that may be set up on the line at the same time. The timing set for such test calls should be discussed with the installer.

The timing set for test calls from this equipment may be subject to 'drift'. If this proves to be inconvenient and your calls are interrupted, then the problem of timing should be discussed with the equipment installer. The matter should NOT be reported as a fault to Telecom Faults Service.

In the event of any problem with this device, it is to be disconnected, and a CPE item connected to one of its terminal ports may be connected directly in its place. The user should then arrange for the product to be repaired. Should the matter be reported to Telecom as a wiring fault, and the fault is proven to be due to this product, a call-out charge will be incurred.

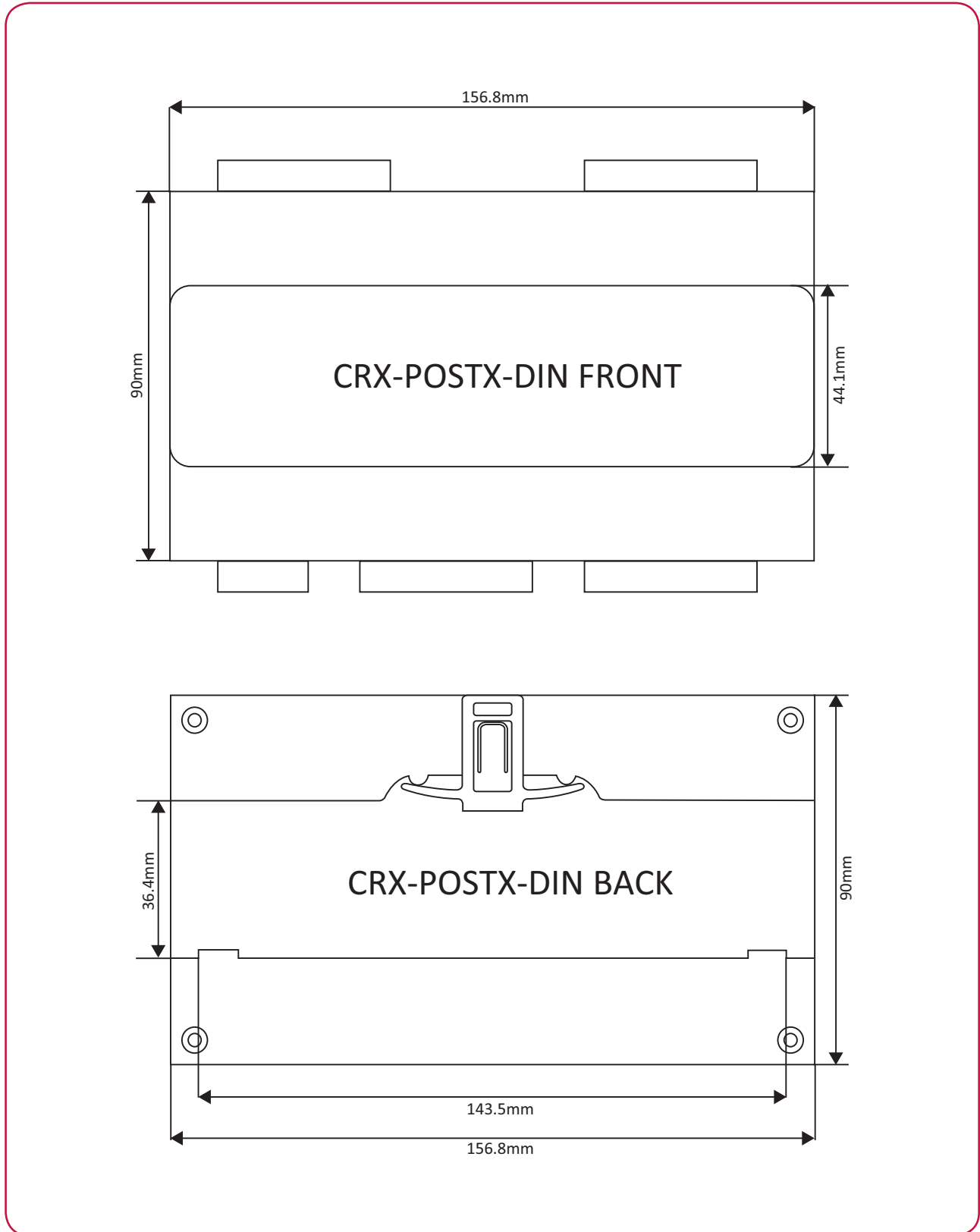
16 Mechanical Diagram

The mechanical diagram shown below outlines the essential details needed to help ensure the correct installation of the PostX Module.



17 Mechanical Layout

The mechanical layout shown below outlines the essential details needed to help ensure the correct installation of the PostX Module.



18 Technical Specifications



The following specifications are important and vital to the correct operation of the PostX Module. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Integrated Control Technology continually strives to increase the performance of its products. As a result, these specifications may change without notice. We recommend consulting the ICT website (<http://www.ict.co>) for the latest documentation and product information.

Power Supply	
DC Input Voltage	12VDC (+/-10%)
Operating Current	110mA (Typical) 220mA (Peak, Panel Off Hook)
Low Voltage Cutout	8.7VDC
Low Voltage Restore	10.5VDC
Communication	
RS-485	RS485 Menu Interface
Ethernet	10/100 Auto Negotiation
Full PSTN Emulation	
Modem Security Reporting	
WiFi	802.11 a/b/g/n
GPRS	2G network 850/900/1800/1900MHz quad band
Outputs	
Programmable Outputs	2 FORM C Relay Outputs, 7A 250V Max
Inputs	
Inputs	4
Dimensions	
Dimensions (L x W x H)	156.8 x 90 x 60mm (6.17 x 3.54 x 2.36")
Weight	453g (15.98oz)
Temperature	
Operating	0°-50°C (32° - 122°F)
Storage	-10° - 85°C (14° - 185°F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)



It is important that the unit is installed in a dry cool location that is not affected by humidity. Do not locate the unit in air conditioning or a boiler room that can exceed the temperature or humidity specifications.

19 New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.



20 UL and ULC Installation Requirements



Only UL / ULC listed compatible products are intended to be connected to a UL / ULC listed control system.

20.1 UL/ULC Installation Cabinet Options

UL/ULC Central Station Fire Monitoring, Central Station Alarm Installations

Cabinet Model	Manufacturer	UL/ULC Installation Listings
EN-DIN-24-ATTACK	ICT	UL1610, UL1635, ULC-S304, ULC-S559

Electronic Access Control System Installations



All cabinet installations of this type must be located **inside the Protected Area**. Not to be mounted on the exterior of a vault, safe or stockroom

Cabinet Model	Manufacturer	UL/ULC Installation Listings
EN-DIN-12	ICT	UL294, CAN/ULC-S319
EN-DIN-31	ICT	UL294, CAN/ULC-S319
EN-DIN-24	ICT	UL294, CAN/ULC-S319
EN-DIN-24-ATTACK	ICT	UL294, CAN/ULC-S319



All cabinet internal covers and lid/doors must be connected to the cabinets main ground point for electrical safety and static discharge protection.

20.2 Central Station Signal Receiver Compatibility List

- IP Receiver via Ethernet Port : Integrated Control Technology ArmorIP Internet Monitoring Receiver. Serial interface to be used with SIMS II version 1.3x central station automation system software and compatible receiving equipment as indicted in the SIMS II Appendix E UL Supplement.
- CID Receiver via Onboard Modem: Any UL and ULC listed receiver that uses the Contact ID protocol.

20.3 ULC Compliance Requirements

CAN/ULC-S304-06

- **Auto Arming**

Control units that support auto arming shall provide an audible signal throughout the protected area not less than 10 min prior to the auto arming taking place. The control unit shall allow authorized users to cancel the auto arming sequence and transmit such cancelation to the signal receiving center with the identification of the authorized user that canceled the action.

The following options must be enabled in the Protege System when using the Auto Arming feature. When the defer warning time is programmed to 10 minutes, the Output group will be activated 10 minutes before the system performs the Auto Arming in the associated Area.

- The **Defer Output or Output Group** must be programmed. Refer to the section Areas | Outputs in the Protege GX Operator Reference Manual (227-1500-000) for programming instructions.
- The **Defer Warning Time** must be programmed to not less than 10 minutes. Refer to the section Areas | Configuration in the Protege GX Operator Reference Manual (227-1500-000).
- The **Defer Automatic Arming** arming option must be enabled. Refer to the section Areas | Options (2) in the Protege GX Operator Reference Manual (227-1500-000).

- **Arming Signal**

A bell or visual indicator used as an arming acknowledgement signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.

- **Double EOL Input Configuration**

Only double EOL Input Configuration shall be used. Refer to the section Inputs of this manual and the section Inputs | Options in the Protege GX Operator Reference Manual (227-1500-000).

- **Multiplex System and Poll Time**

The PRT-CTRL-DIN is compatible with the ICT ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

In the Protege System, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:

- The **Log Polling Message** option must be enabled. Refer to the section Report IP | Options in the Protege GX Operator Reference Manual (227-1500-000).
- The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Protege GX Operator Reference Manual (227-1500-000).

- **Central Station Signal Receiver**

The common equipment of each signal receiving center control unit shall be limited to 1000 alarm systems.

- **Number of attempts**

In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

In the Protege System, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Protege GX Operator Reference Manual (227-1500-000).

- **Check-In Time**

DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**

- The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Protege GX Operator Reference Manual (227-1500-000).
- The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Protege GX Operator Reference Manual (227-1500-000).
- The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Protege GX Operator Reference Manual (227-1500-000).

- **Primary Communication Channel**

The first attempt to send a status change signal shall utilize the primary communication channel.

The Report IP and Contact ID services must be programmed and enabled within the Protege System, and the CID service must be set as the backup service. The following options are required:

- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
Refer to the section Contact ID in the Protege GX Operator Reference Manual (227-1500-000).
- The **Report IP Service** must be enabled as the primary communication channel and the **Service Mode** must be configured to start with the operating system. The **Reporting Protocol** must be set to ArmorIP, and the **Backup Service** must be configured to use the Contact ID Service.

Refer to the section Report IP in the Protege GX Operator Reference Manual (227-1500-000).

- All ULC S304 P3 applications must transmit signals simultaneously over both the Contact ID Reporting Service and the Report ID Service. This will occur automatically with the above programming.

- **Status Change Signal**

An attempt to send a status change signal shall utilize both primary and secondary communication channels.

- **Local Annunciation if Signal Reporting Failure**

Failure of the primary communication channel or secondary communication channel shall result in a trouble signal being transmitted to the signal receiving center within 240 seconds of the detection of the fault.

Failure of either communication channel shall be annunciated locally within 180 seconds of the fault.

The following options must be enabled in the Protege System:

- The **Ethernet Link Failure** Trouble Input must be programmed.
- The **Trouble Input Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Protege GX Operator Reference Manual (227-1500-000).
- The **Log Modem Events to Event Buffer** option must be selected in the Contact ID Reporting Service.

- **Network and Domain Access**

Neither the subscriber control unit nor the signal receiving center receiver shall be susceptible to security breaches in general-purpose operating systems.

Network access policies should be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Ethernet Connections**

All Ethernet network connections shall be installed within the same room as the equipment.

- **Encryption**

For active communications channel security, encryption shall be enabled at all times.

The ArmorIP-E (UDP) protocol must be used and the Encryption Type must be set to AES-256.

The following options must be enabled for the the Report IP service in the Protege System.

- The **Reporting Protocol** must be set to ArmorIP (UDP) Encrypted. The AES key must be set as specified by monitoring station.

Refer to the section Report IP | General in the Protege GX Operator Reference Manual (227-1500-000).

- **Server Configuration**

Where a server is employed for control over network addressing, encryption or re-transmission, such shall be designed to remain in the "on state" at all times.

Communicators are not suitable for active communication channel security and medium or high risk applications unless such can be "on line" at all times, have a minimum 128 bit encryption scheme, have encryption enabled, network and domain security implemented.

Network access policies shall be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Internet Service Provider (ISP)**

The Internet Service Provider (ISP) providing service shall meet the following requirements:

- redundant servers/systems
- back-up power
- routers with firewalls enabled and
- methods to identify and protect against "Denial of Service" attacks (i.e. via "spoofing")

- **Information Technology Equipment, Products or Components of Products**

Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in CAN/CSA-C22.2 No. 60950-1, Information Technology Equipment Safety - Part 1: General Requirements. Where network interfaces, such as the following, are internal to the subscriber control unit or receiver, compliance to CAN/CSA-C22.2 No. 60950-1 is adequate. Such components include, but are not limited to:

- A) Hubs;
- B) Routers;
- C) Network interface devices;

- D) Third party communications service providers;
- E) Digital subscriber line (DSL) modems; and
- F) Cable modems.

- **Backup Power Requirements**

Power for network equipment such as hubs, switchers, routers, servers, modems, etc., shall be backed up or powered by an un-interruptible power supply (UPS), stand-by battery or the control unit, capable of facilitating 24 h standby, compliant with Clauses 16.1.2 and 16.4.1 of CAN/ULC-S304-06.

For communications equipment employed at the protected premises or signal receiving center and intended to facilitate packet switched communications, as defined in CAN/ULC-S304, 24 h back-up power is required.

- **Compromise Attempt Events**

ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

The event is sent with the following details:

- **Account Code** as defined in the Serial Receiver settings
- **Event Code** 0x163
- **Group Code** as defined in the Serial Receiver settings
- **Point Code** as defined in the Serial Receiver settings

Refer to the section [Global Settings | Serial Receiver](#) in the ArmorIP Internet Monitoring Application User's Manual (227-5500-000).

For UL and ULC installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

- **Power Supply Mains Power Connection**

If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

The Power Supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S319-05

- The Models PRT-CTRL-DIN and PRT-RDM2-DIN are intended to be mounted within the enclosure (refer to UL/ULC Installation Cabinet Options (see page 52)), installed inside the protected premise, and are CAN/ULC-S319 Listed for Class I applications only
- Exit devices and wiring must be installed within the protected area.
- For the Models PRT-CTRL-DIN and PRT-RDM2-DIN, all RS485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-S319 listed portal locking device(s) for ULC installations.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The Power Supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S559-04

- **Signal Reporting**

Any fault of an active communication system shall be annunciated and recorded at the signal receiving center within 180 s of the occurrence of the fault.

The Report IP and Contact ID services must be programmed and enabled within the Protege System. The following options are required:

- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.

Refer to the section Contact ID in the Protege GX Operator Reference Manual (227-1500-000).

- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.

Refer to the section Report IP in the Protege GX Operator Reference Manual (227-1500-000).

- The **Trouble Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Protege GX Operator Reference Manual (227-1500-000).

In the ArmorIP Internet Monitoring Software the **Poll Time** must be set to 40 seconds and the **Grace Time** must be set to 20 seconds. Refer to the section Poll/Grace Time in the ArmorIP Internet Monitoring Application User Manual (227-5500-000).

- **Central Station Signal Receiver**

The maximum number of signal transmitting units connected to any transmission channel shall conform to the manufacturer's recommendations. The ArmorIP Receiver supports up to 10000 simultaneous connections.

Refer to the section Internet Connections Requirements in the ArmorIP Receiver Installation Manual (227-5510-000) for further details.

- **Number of attempts**

In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

In the Protege System, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dialing Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Protege GX Operator Reference Manual (227-1500-000).

- **Check-In Time**

DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**

- The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Protege GX Operator Reference Manual (227-1500-000).

- The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Protege GX Operator Reference Manual (227-1500-000).

- The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Protege GX Operator Reference Manual (227-1500-000).

- **Ethernet Connections**

All Ethernet network connections shall be installed within the same room as the equipment.

- **Power Supply Mains Power Connection**

If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

The Power Supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

- **Arming Signal**

A bell or visual indicator used as an arming acknowledgement signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.

- **Keypad Wiring**

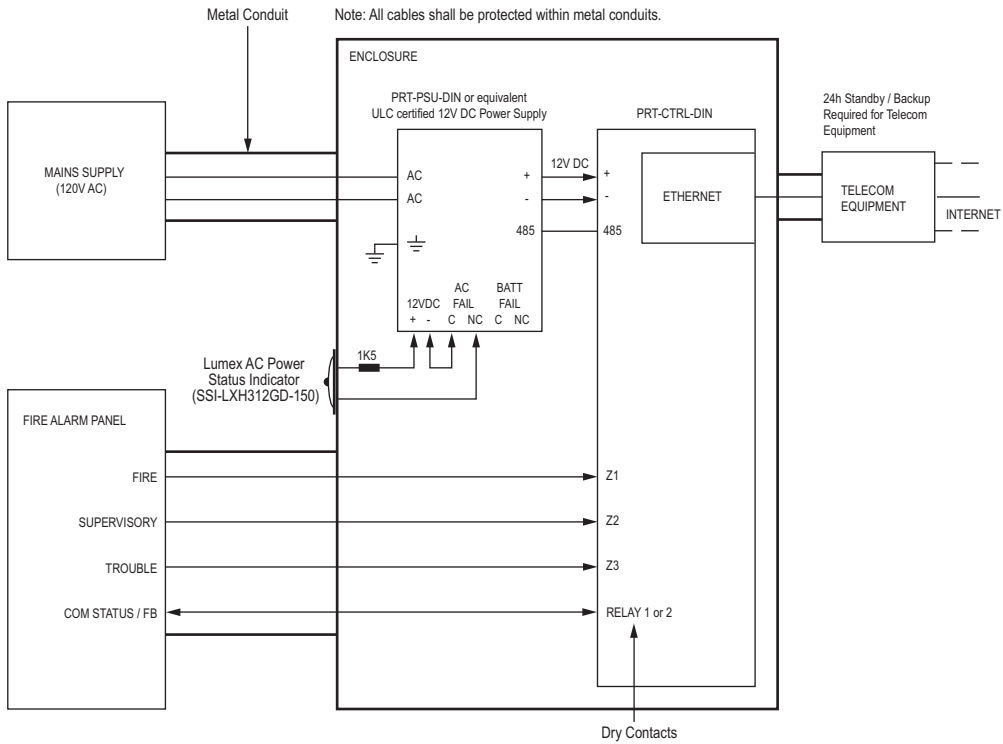
The RS-485 connection to the keypad must be wired such that the shorts and other faults on the RS-485 line connection of the keypad will not cause the controller to malfunction.

- **Fire Zones**

Fire zones shall be separated from burglar zones through area partitioning.

NOTE: Any available dry relay contact on the PRT-CTRL-DIN or PRT-PX8-DIN may be used for the FACP system, provided the selected output is programmed as the Report OK PGM.

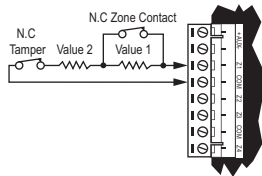
CAN/ULC-S559
PRT-CTRL-DIN
ACTIVE COMMUNICATION



- * The AC FAIL output on the Power Supply **MUST** be programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail
- * Fire zones shall be separated from burglar zones through area partitioning.
- * Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output

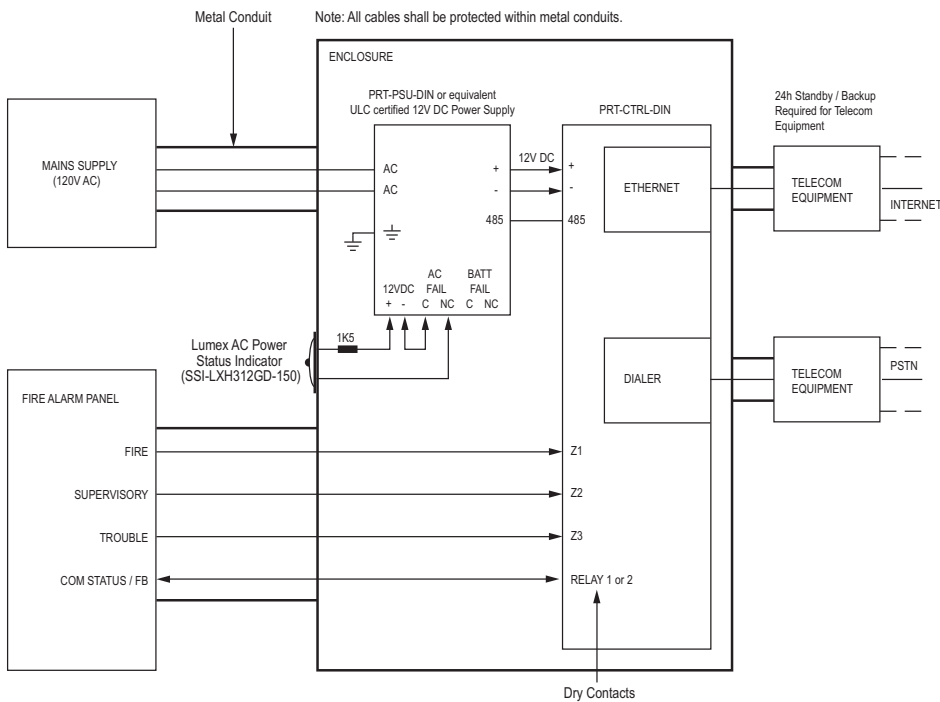
Typical Zone Circuits

EOL Resistor Zone Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



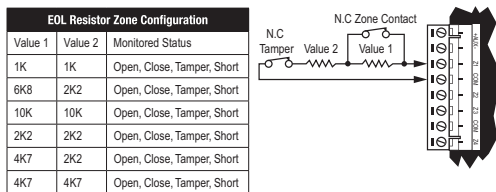
- * EOL resistor must be installed at the Fire Alarm Control Panel Output.

CAN/ULC-S559
PRT-CTRL-DIN
PASSIVE COMMUNICATION



- * The AC FAIL output on the Power Supply **MUST** be programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail
- * Fire zones shall be separated from burglar zones through area partitioning.
- * Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output

Typical Zone Circuits



* EOL resistor must be installed at the Fire Alarm Control Panel output.

• **Fire Zone Inputs and Outputs**

Fire Zone inputs must be programmed as follow:

- FACP Fire Alarm Signal zone type must be programmed as Fire
- Supervisory Trouble Signal zone type must be programmed as 24 Hr Silent
- Trouble Signal zone type must be programmed as 24 Hr Silent

Please refer to the section Inputs | Areas and Input Types in the Protege GX Operator Reference Manual (227-1500-000)

- All fire zone inputs must be placed into an area and this area must be armed. Please refer to the section Inputs | Areas and Input Types in the Protege GX Operator Reference Manual (227-1500-000)
- COM Status

FACP system with a COM STATUS input must have this input connected to one of the dry relay contacts of the Relay1 or Relay2 outputs of the PRT-CTRL-DIN and the selected output must be programmed as the Report OK PGM in the Contact ID Service.

Note: Any available dry relay contact on the PRT-CTRL-DIN or PRT-PX8-DIN may be used for the FACP system, provided the selected output is programmed as the Report OK PGM.

Please refer to section Contact ID | Settings in the Protege GX Operator Reference Manual (227-1500-000)

- Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output.

20.4 UL Compliance Requirements

UL1610

- A local alarm sounding device, alarm housing, and control unit shall comply with the mercantile requirements in the Standard for Police Station Connected Burglar Alarm Units and Systems, UL365.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Exit and entry delay must not exceed 60 seconds. To program the entry and exit delay time, refer to the section [Areas | Configuration](#) in the Protege GX Operator Reference Manual (227-1500-000).
- All Ethernet network connections shall be installed within the same room as the equipment.
- Signals between the premises control unit and the receiving equipment, when not carried by wireless means, shall be protected by the following method:
 - Onboard modem telco connection must be dedicated to the PRT-CTRL-DIN.
 - Ethernet connection to the Internet Service Provider (ISP) with a fixed IP Address must be dedicated to the PRT-CTRL-DIN.
- To comply with the dual signal line transmission system requirement, both transmission lines (onboard modem and IP reporting) must be enabled. Signals shall be sent simultaneously to both, Report IP Service and Contact ID Reporting Service.

The Report IP and Contact ID services must be programmed and enabled within the Protege System. The following options are required:

- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
Refer to the section [Contact ID](#) in the Protege GX Operator Reference Manual (227-1500-000).
- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
Refer to the section [Report IP](#) in the Protege GX Operator Reference Manual (227-1500-000).
- When more than one means of signal transmission is used, loss of communication with the receiving system shall be annunciated at the receiver within 200 seconds. If a fault is detected on any of the signal transmission means, at least one of the signal transmission channels shall send a signal to the central-station to report the fault within 200 seconds.

The Report IP and Contact ID services must be programmed and enabled within the Protege System.

The PRT-CTRL-DIN is compatible with the Integrated Control Technology ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

In the Protege System, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:

- The **Poll Time** must be programmed to 40 seconds. Refer to the [Report IP | General](#) section in the Protege GX Operator Reference Manual (227-1500-000)
- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
Refer to the section [Contact ID](#) in the Protege GX Operator Reference Manual (227-1500-000)
- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
Refer to the section [Report IP](#) in the Protege GX Operator Reference Manual (227-1500-000).
- The **Trouble Input Area** must be armed in 24h mode. Refer to the section [Trouble Inputs | Areas and Input Types](#) in the Protege GX Operator Reference Manual (227-1500-000).

In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

In the Protege System, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The following options are required:

- The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the the Protege GX Operator Reference Manual (227-1500-000).
- DACT communication channel check-in time is not to exceed 24 hrs.
- Trouble Zone Service Test Report
 - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Protege GX Operator Reference Manual (227-1500-000).
 - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Protege GX Operator Reference Manual (227-1500-000).
 - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Protege GX Operator Reference Manual (227-1500-000).
- ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

The event is sent with the following details:

- **Account Code** as defined in the Serial Receiver settings
- **Event Code** 0x163
- **Group Code** as defined in the Serial Receiver settings
- **Point Code** as defined in the Serial Receiver settings

Refer to the section Global Settings | Serial Receiver in the ArmorIP Internet Monitoring Application User's Manual (227-5500-000).

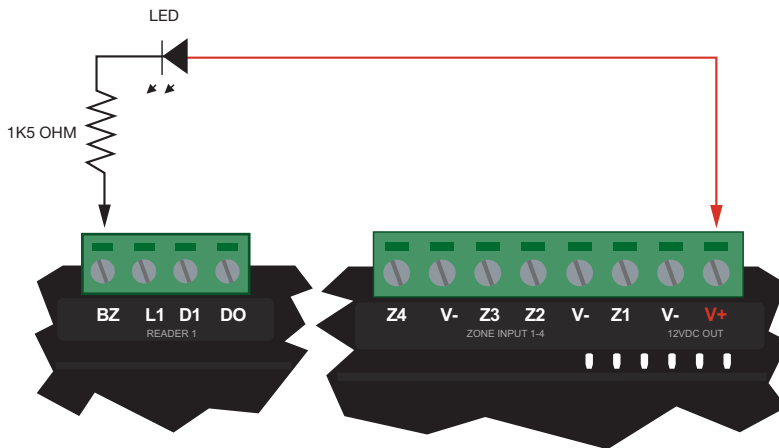
For UL and ULC installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The Power Supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

UL294

- The Models PRT-CTRL-DIN and PRT-RDM2-DIN are intended to be mounted within the enclosure (refer to UL/ULC Installation Cabinet Options (see page 52)), installed inside the protected premise, and are UL 294 Listed for Attack Class I applications only
- Exit devices and wiring must be installed within the protected area.
- For the Models PRT-CTRL-DIN and PRT-RDM2-DIN, all RS485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to UL10B or UL10C.
- Must be installed with UL 1034 listed electronic locks for UL installations.

- AC power on shall be indicated by an external panel mount LED (Lumex SSI-LXH312GD-150) and fitted into a dedicated 4mm hole in the cabinet to provide external visibility. This shall be wired between 12V and a PGM output that is programmed to follow the AC trouble input as shown below:



- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The Power Supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

21 FCC Compliance Statements

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment has been tested and found to comply with the limits for a Class A 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 to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful 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:

- Re-orient 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.
- Changes or modifications not authorized by the party responsible for compliance could void the user's authority to operate this product.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

IMPORTANT INFORMATION

This equipment complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. Inside the cover of this equipment is a label that contains, among other information, a product identifier in the format US: AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

FCC REGISTRATION NUMBER: US: 48DMM00BCRXPOSTXD

RINGER EQUIVALENCE NUMBER: 0.0

USOC Jack: RJ-31X

Telephone Connection Requirements

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See this document for details.

Ringer Equivalence Number (REN)

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Incidence of Harm

If this equipment (PRT-CTRL-DIN Integrated System Controller) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Changes in Telephone Company Equipment or Facilities

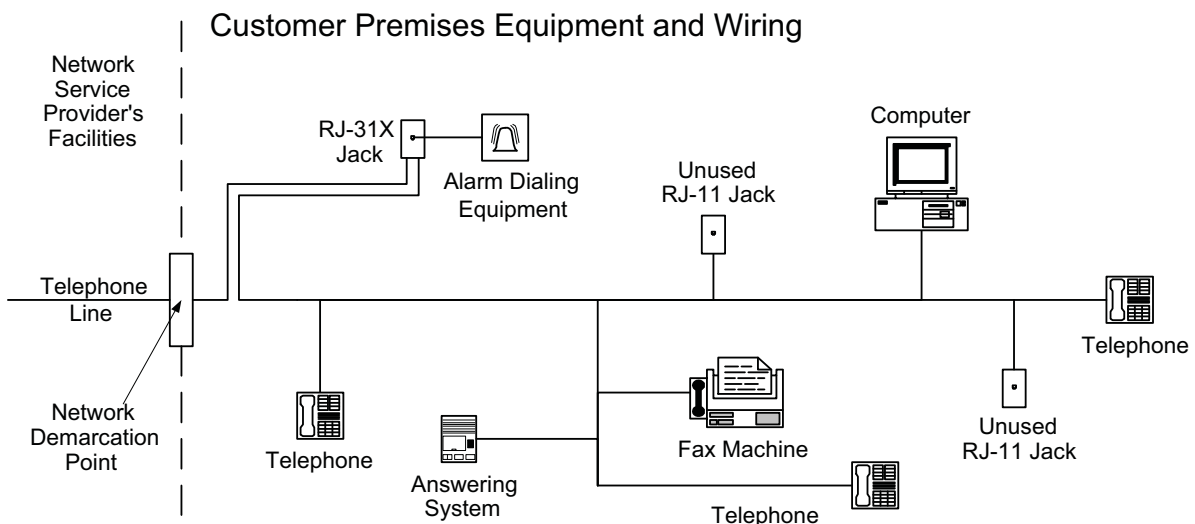
The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

Equipment Maintenance Facility

If trouble is experienced with this equipment (CRX-POSTX-DIN), for repair or warranty information, please contact Integrated Control Technology c/o 150 W 9th Ave, Denver, CO 80204. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. This equipment is of a type that is not intended to be repaired by the end user.

Additional Information

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. Alarm dialing equipment must be able to seize the telephone line and place a call in an emergency situation. It must be able to do this even if other equipment (telephone, answering system, computer modem, etc.) already has the telephone line in use. To do so, alarm dialing equipment must be connected to a properly installed RJ-31X jack that is electrically in series with and ahead of all other equipment attached to the same telephone line. Proper installation is depicted in the figure below. If you have any questions concerning these instructions, you should consult your telephone company or a qualified installer about installing the RJ-31X jack and alarm dialing equipment for you.



22 Industry Canada Statement

This class A digital apparatus complies with Canadian ICES-003.

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

This product meets the applicable Industry Canada technical specifications. The Ringer Equivalence Number (REN) for this terminal equipment is 0.0. The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 0.0. Le présent matériel est conforme aux spécifications techniques applicables d'Industrie Canada. L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

CRX-POSTX-DIN REGISTRATION NUMBER IC: 10012A-CRXPOSTXDIN

CRX-POSTX-DIN NUMÉRO D'ENREGISTREMENT IC: 10012A-CRXPOSTXDIN

23 Ordering Information

Please use the following product codes when placing an order for the DIN Rail PostX IP Reporting Module.

- CRX-POSTX-DIN
- CRX-POSTX-DIN-WF with WIFI interface
- CRX-POSTX-DIN-GP with GPRS interface
- CRX-POSTX-DIN-WFGP with WIFI and GPRS interface

Manuals and additional literature are available on the ICT Website (<http://www.ict.co>).

24 Warranty

Integrated Control Technology (ICT) warrants its products to be free from defects in materials and workmanship under normal use for a period of two years. Except as specifically stated herein, all express or implied warranties whatsoever, statutory or otherwise, including without limitation, any implied warranty of merchantability and fitness for a particular purpose, are expressly excluded. ICT does not install or connect the products and because the products may be used in conjunction with products not manufactured by ICT, ICT cannot guarantee the performance of the security system. ICT's obligation and liability under this warranty is expressly limited to repairing or replacing, at ICT's option, any product not meeting the specifications. In no event shall ICT be liable to the buyer or any other person for any loss or damages whether direct or indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party caused by defective goods or otherwise arising from the improper, incorrect or otherwise faulty installation or use of the merchandise sold.

25 Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (<http://www.ict.co>) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

4 John Glenn Ave
Rosedale
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Toll Free Numbers:

0800 ICT 111 (0800 428 111) - New Zealand

1800 ICT 111 (1800 428 111) - Australia

1855 ICT 9111 (1855 428 9111) - USA/Canada

Email: sales@incontrol.co.nz or support@incontrol.co.nz (<mailto:support@ict.co>)

Web: www.ict.co

APAC

Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@ict.co Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

AMERICAS

Integrated Control Technology (USA) LLC
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@ict.co Toll Free: (855) 428 9111 Phone: 720 442 0767

EMEA

Integrated Control Technology (Europe) Limited
St Mary's Court, The Broadway, Amersham, HP7 0UT, UK
Email: emeasales@ict.co Phone: 44 0 1494 590494

Designers & manufacturers of integrated electronic access control, security and automation products.

Designed & manufactured by Integrated Control Technology Ltd.

Copyright © Integrated Control Technology Limited 2003-2017. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of these products, neither Integrated Control Technology Ltd nor its employees, shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice

227-5135-300

www.ict.co

