

EN50131-1:2006+A1:2009
EN50131-3:2009
EN50131-6:2008
EN50131-5-3:2005+A1:2008



Security Grade 2
Environmental Class II

Software Version > 10



Programming Reference Manual Wireless Alarm System

RINS1707-1

INTERNAL SIREN WARNING
The Enforcer 32-WE control panel
contains a 100 dBA siren,
please be aware of this during
installation



1. Contents page

1. Contents page	2
2. Introduction	3
2.1 Two Way Wireless High Security	3
2.2 Battery Monitoring/Saving	3
2.3 Pyronix Cloud and Home Control+ App	4
3. Writing Texts on the keypad	5
4. The Engineer Menu.....	5
4.1 Navigating in the Engineer and User Menus	5
4.2 Entering The Engineer Menu (Default Engineer Code = 9999)	6
4.3 Exiting The Engineer Menu	6
4.4 Accessing the Engineers Menu on any external wired keypad	6
4.5 Saving The Programming	6
5. Engineer Menu.....	6
5.1 Date and Time?	6
5.2 Learn Wireless Devices?	7
5.3 Program Inputs?.....	11
5.4 Install RIXs?	13
5.5 Program Outputs?.....	13
5.6 Install Keypads and Readers?	16
5.7 Program Timers?	17
5.8 Change Codes?	19
5.9 Volume Control?.....	20
5.10 System Options?.....	21
5.11 Review Logs?	23
5.12 Engineer Tests?	23
5.13 Diagnostics?.....	24
5.14 Engineer Restore Options?	26
5.15 Communications?.....	26
5.16 Alarm Responses?.....	30
5.17 Options Up/Downloading?	32
5.18 PC Connect Menu?	32
5.19 Software Revision?.....	33
5.20 Factory Default?	33
5.21 Exit Engineer Menu?.....	33
6. Adding External Wired Keypad	33
7. Connecting to InSite Software.....	34
8. Options Programmable Only From PC.....	36
8.1 Auto Arm/Disarm Timers	36
8.2 Areas to Arm/Disarm	36
8.3 Programming Logic Gates	37
9. Faults and Troubleshooting.....	38
9.1 Device Fail / Active Faults	38
9.2 System Faults and Troubleshooting	38
10. Event Types	41
11. EN 50131 Terminology	41
12. Access Levels.....	41
13. Factory Defaults.....	42
14. Event Types (SIA and Contact ID codes).....	46
15. Notes.	50

2. Introduction

2.1 Two Way Wireless High Security

The Enforcer 32-WE is a wireless alarm system that has been designed with a customer's security in mind; with quick and easy installation and minimal maintenance, the Enforcer 32-WE protects a property with a multitude of unique features.

Taking full advantage of Pyronix's innovative two way wireless technology, the wireless devices on the Enforcer 32-WE are constantly communicating with each other, using the Pyronix High Security Wireless Encryption Protocol.

The Enforcer 32-WE two way wireless devices are fully operational when the system is armed, making the system more secure, compared to other wireless systems, where devices are disabled for up to five minutes after every activation to save battery, therefore compromising the security.

The Enforcer 32-WE has been engineered by Pyronix as a secure, reliable and easy to use wireless alarm system. It includes the following features below:

2.2 Battery Monitoring/Saving

The Enforcer 32-WE uses advanced technology to preserve the battery life of each wireless device. However, the Enforcer 32-WE indicates when a battery needs replacing a month in advance before the device stops working. This key feature gives enough time to change the battery in the specific device. Other wireless alarm systems may not give a low battery warning signal, meaning that devices could stop working, leaving the environment unprotected.

2.2.1 High Security Encryption

128 bit high security wireless encryption protocol, and intelligent wireless jamming detection.

2.2.2 User Friendly Keyfobs

The fully two way wireless keyfob indicates the status of the control unit via 3 colour LEDs:

System armed: When the system is armed a RED LED will illuminate momentarily

System disarmed: When the system is disarmed a GREEN LED will illuminate momentarily

System fault: When the system is in fault condition an AMBER LED will illuminate momentarily, This will also flash when the keyfob is unable to arm the system.

It is possible to allocate different functions to each keyfob such as arming / disarming different areas, activating outputs to control external devices such as gates, requesting system status, and activating panic alarms. Up to 32 wireless keyfobs can be added to the Enforcer 32-WE. Each wireless keyfob has its own user ID which can be reported to the ARC and user mobile phone which are stored into the event log of the control panel individually.

The keyfob also allows the arming/disarming of every area individually, giving total control of the Enforcer 32-WE.

2.2.3 User Automation Outputs

The Enforcer 32-WE includes user automation outputs that gives the option to operate up to 20 devices such as gates, lights, sprinklers, etc. via the keypad or remotely via a Keyfob, thus extending the use of the Enforcer-32-WE.

2.2.4 SMS Text Notifications and Remote Control

The system will notify via SMS text messages in real time. For example; notification that someone has returned home safely or notification of a leakage of water in a property etc.

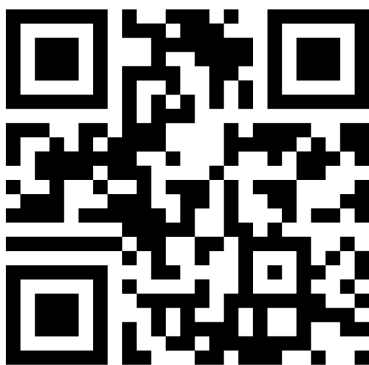
2.3 Pyronix Cloud and Home Control+ App

The Pyronix+ App turns a smartphone into a remote keypad. It can be used to:

- Arm / Disarm the Enforcer 32-WE;
- Activate the automation outputs to remotely turn on / off lights, open gates and so on;
- View real time sensor status and bypass sensors when required;
- View any notifications and event memory log;
- Receive push notifications from a system.

The Pyronix+ App and Pyronix Cloud communication is fully encrypted to the highest standard (AES 256) and no sensitive user data is stored on the Pyronix Cloud.

The Pyronix+ App is available in 2 versions Android from Google Play Store and iOS from Apple store.
www.pyronixcloud.com



3. Writing Texts on the keypad

On the Enforcer 32-WE it is possible to label the following:

- Inputs – 2 labels: Input Number and Location
- Area Names
- Site Name
- Keypad/Reader – 2 labels: Keypad Number and Location
- Input and Output expander location descriptions
- User Names

The Enforcer 32-WE incorporates a predictive text feature (T9 type). For example, enter 'B' and 'Bedroom' will be displayed. If the word that is required doesn't appear, then type the word letter by letter.

To type a word, press the relevant button the appropriate number of times – e.g. for the letter 'k' press **[5]** two times, or for the letter 's' press **[7]** four times. For punctuation marks, press the **[1]** button multiple times until the desired character is shown.

Button meanings:

The following alpha-numerical buttons are used	Other meaning of the buttons
[A] = makes the character into a capital	[A] = Status Area A
[C] = clears letters / adds a space	[B] = Status Area B
[←] = moves cursor left	[C] = Status Area C
[→] = moves cursor right	[D] = Status Area D
	[D] = Press to Enter Master Manager Mode
	[Fire] = Press for 2 sec to generate Fire alarm
	[PA] = Press for 2 sec to generate PA alarm

4. The Engineer Menu

The system is programmed from the Engineer Menu. To enter the Engineer Menu the panel must be in a disarmed state. Whilst in Engineer Mode all tamper alarms (including case tamper), will be disabled.

4.1 Navigating in the Engineer and User Menus

- [X]** = "NO" - Press to move forward when in Engineer or Master Manager mode
- [B]** = "BACK" - Press to move backward when in Engineer or Master Manger mode
- [✓]** = "YES" - Press to enter in a submenu or option when in Engineer or Master Manger mode
- [✓]** = Press to move from one option into another option while in a submenu
- [A]** = Press to quick exit the Engineer Menu from any main menu (written in capital letters)
- [C]** = "CANCEL" - Press to move back from one programmable option to the previous option.

4.1.1 Main Menus and Sub Menus



- A Main Menu item is identified by:
- The maintenance LED is flashing slowly
 - The menu item will be in capital letters



- A Sub-Menu is identified by:
- The maintenance LED is flashing rapidly
 - The menu item will be in small letters with a question mark (?).

In order to navigate in the menu system, one has to answer to the questions in the main and sub menus. For example, if the question is "WIRELESS DEVICE CONTROL?" is displayed, then press **[✓]** or **[X]** depending on the answer.

Pressing **[✓]** will enter a sub-menu called "Control Inputs?" in this example. Pressing **[✓]** will enter the programmable options of this submenu. Pressing **[X]** will exit the individual option, move up from one sub-menu to the next sub-menu or back to the main menu.

4.2 Entering The Engineer Menu (Default Engineer Code = 9999)

Access to the Engineer Menu maybe denied if:

- 1) One or more areas are currently armed.
- 2) The Master User has disabled the function "Allow Engineer Menu" in the Master Manager Menu. If this is the case 'Authorisation required' will be shown on the display.

When in Engineer Menu, the fault (⚠) LED will flash and high pitch tone will be generated regularly.

4.3 Exiting The Engineer Menu

On completion of programming, the system can be returned back to disarmed mode by either scrolling to the 'Exit Engineer Menu' option or press **A** from any main menu option (represented in capital letters).

4.4 Accessing the Engineers Menu on any external wired keypad

It is possible to access the Engineer Menu on any keypad that is part of the system. Whichever keypad that is being used, all other keypads will display 'System Busy'. To access the Engineer menu on one of these keypads press **B**.

4.5 Saving The Programming

Any programming done in the engineer or user mode will not be saved on the system until the Engineer or User menu have been exited.

5. Engineer Menu

Please refer to the Engineer Programming Quick Guide for this chapter. The meaning of every option presented in the quick programming guide is explained here in detail.

5.1 Date and Time?

All log entries and the system display include the date and time so it is vital that the correct date and time is programmed. This may be also programmed in the Master Manager Mode.

NOTE: Please note that powering down the system and removing the battery will reset the time and date information.

5.1.1 Change Year

For the year 2011, enter 11.

5.1.2 Change Month

For March, enter 03.

5.1.3 Change Day

For 31st, enter 31.

5.1.4 Change Hours

Use 24 hour clock format. For 8pm enter 20:00.

5.1.5 Change Minutes

For 7:30, enter 30.

5.1.6 Summer Time Adjust

If activated this option will automatically change 1 hour ahead and backward for the summer and winter time.

5.2 Learn Wireless Devices?

This function learns or deletes all wireless inputs and bells to the Enforcer 32-WE.

NOTE: The keyfobs are learned and programmed from the Master Manager menu.

5.2.1 Learn Inputs?

Learn Devices?

This menu starts the procedure of learning wireless inputs onto the Enforcer 32-WE.

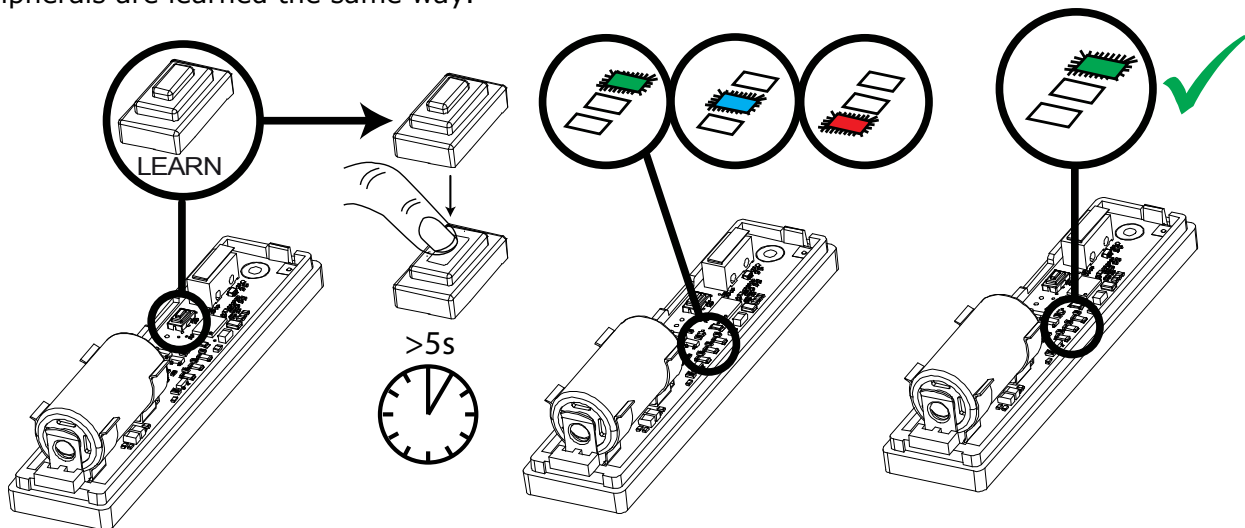
Input

This menu chooses which input on the system is to be learned. 'Learnt' will be displayed if a device is already learnt, or 'Available' will be displayed if it is not.

Input → Learning...

- 1) Open the wireless device.
- 2) Remove the plastic insulation to enable the battery.
- 3) If a Device is not learned = The GREEN and RED LEDs on the Device will flash (alternating).
- 4) Press and hold the 'LEARN' button on the Device = The 3 LEDs start cycling around.
- 5) Release the 'LEARN' button = 'Input Learnt' will be displayed and a confirmation tone will be emitted on the panel.
- 6) If an input has already been learnt, 'Input learnt already' will be displayed.

Example: The image below shows how to learn an MC detector. Please note all other wireless peripherals are learned the same way.



5.2.2 Delete Devices

Already learnt inputs may be deleted from this menu.

Delete All → Enter Code

To delete all wireless input devices enter '2000' (this is the Enforcer Security Code). "Please wait" will be displayed while the Enforcer 32-WE deletes **ALL** the learnt wireless inputs.

Choose Input to Delete

This option deletes only a specific wireless device learnt to an input. Any inputs that display 'learnt' can be deleted. "Please wait" will be displayed while the Enforcer 32-WE deletes the wireless device. Return to this process to delete more devices.

5.2.3 Learn Bells?

Learn Devices?

Entering this menu allows the learning of wireless bells onto the system.

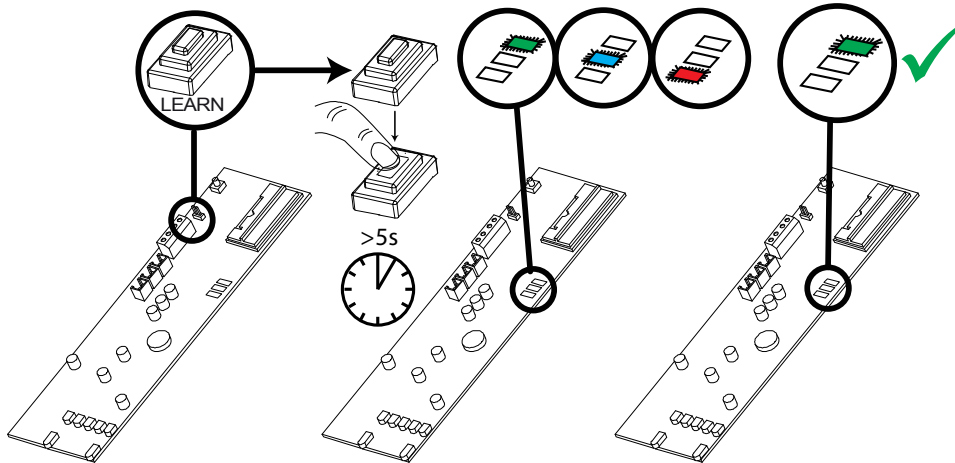
Select Bell

Selects the bell on the system that is to be learnt. 'Learnt' will be displayed if a bell is already learnt, or 'Available' will be displayed if not.

Select Bell → Learning...

- 1) Open the wireless bell.
- 2) Plug the battery connector into the battery terminal.
- 3) If a device is not learnt = The GREEN and RED LEDs on the Device will flash (alternating).
- 4) Press and hold the 'LEARN' button on the Device = The 3 LEDs start cycling around.
- 5) Release the 'LEARN' button = 'Bell Learnt' will be displayed and confirmation tone on the panel will be emitted.

If a bell has already been learnt, 'Bell learnt already' will be displayed.



5.2.4 Delete Devices

Already learnt bells may be deleted by entering this menu.

Delete All → Enter Code

To delete all wireless bells enter '2000' (this is the Enforcer Security Code). "Please wait" will be displayed while the Enforcer 32-WE deletes them.

Choose Bell to Delete

This option deletes only a specific wireless bell that is learnt. Any bells that display 'learnt' can be deleted. "Please wait" will be displayed while the Enforcer 32-WE deletes the wireless bell. Return to this process to delete more devices.

5.2.5 Learn Keyfobs Procedure

The keyfobs are learnt and deleted from the Master Manager menu.

Learn Keyfobs?

- 1) Enter Master Manager Menu (Default Master Code = 1234).
- 2) Scroll to the function 'LEARN USER CODES KEYFOBS & TAGS'.
- 3) Choose a user number to allocate the keyfob to.
- 4) If a keyfob, code or tag are not learnt the space, between the brackets will be empty.
- 5) If a keyfob, code or tag are learnt, the brackets will show [*****].
- 6) Press and hold any of the keyfob buttons for 5sec.
- 7) A confirmation tone will be emitted and keyfob will be shown on the display.

Proceed with the programming of actions to each key.

5.2.6 Delete Keyfobs

- 1) Enter Master Manager Menu (Default Master Code = 1234).
- 2) Scroll to the function 'LEARN USER CODES KEYFOBS & TAGS'.
- 3) Choose the keyfob to delete = Between the brackets will be show [*****].
- 4) Press **[C]** = The brackets will be showing [] to confirm the deletion.

5.2.7 Program Keyfobs

This Menu is used to program the functionality of the buttons on the keyfobs and is available on the EN defaulted panels in the Engineer Menu, otherwise it can be accessed from the Master Manager menu after learning the keyfob.

No	Input Types	Operation
0	Unused	Factory default. Input is disabled.
1	Fire	Active at all times. Audible Response: Differentiated Internal sound. Pulsed external sound. Communicator: 'Fire' signal
2	Gas	Active at all times. Audible Response: Full external + Internal sound. Communicator: 'Gas' signal
3	PA [#]	Active at all times. Audible Response: Differentiated Internal sound. Full external sound. Communicator: 'Personal Attack' and 'Input PA' signals
4	Silent PA [#]	Active at all times. Audible Response: None Communicator: 'Personal Attack' and 'Input PA' signals
5	Tamper	When disarmed: Audible Response: Internal only. Communicator: 'Tamper' signal. When armed: Audible Response: Full external + Internal sound. Communicator: 'Tamper' signal.
6	Instant	Active when armed: Audible Response: Full external + Internal sound. Communicator: 'Burglary' signal
7	Entry Delay1 [#] \$	Active when armed: Initiates 'Entry Timer 1' when door open. If system not disarmed before entry time expires then: Audible Response: Full External + Internal sound. Communicator: 'Burglary' signal. NOTE: See type 43 for Entry Delay2
8	Follow ^{\$}	Active when armed, except during entry time. (Acts as an instant input if an Entry Delay input hasn't been activated beforehand). Audible Response: Full external + Internal sound. Communicator: 'Burglary' signal.
11	Push To Arm	Active during exit time, to complete arming procedure. No audible or communicator response. Panel will communicate a final armed event once the Push to Arm button has been pressed. NOTE: <i>May be used to act as 'doorbell' by use of 'chime' input attribute.</i> Example: Wire the Door Bell button to the input. Enable "Push to Arm" option from "EXIT MODES", add a "Push to Arm" input type to the input and enable the "Chime" attribute for it. Enter user code, the panel starts arming. Exit the building and close the door. Press the Bell button. The system will arm. If pressing the Bell button while the panel is in any other condition the Chime will sound.
12	Switcher	Active at all times in armed and disarmed modes. No audible or communication alarms will be created. When activated it can trigger the associated output for switching external equipment. If the "Special Log" attribute is enabled for this input an SMS message will be sent each time the input is activated. Example: This kind of input type can be used to control CCTV. The concept is that when a switcher input type is activated, there is an output associated with it following that input (the most used solution is the use of output type – 0035). The switcher input is connected to a detector located next to a CCTV camera and the output is connected to video recording / transmitting equipment. If the detector is activated in armed or disarmed mode then the recording or transmission will start.
13	24 Hour	When armed: Audible Response: Full External + Internal sound; Communicator: '24hr Alarm' signal. When disarmed: Audible Response: Full External + Internal sound; Communicator: '24hr Alarm' signal if enabled in "Alarm Responses" menu.
16	Fault	Active when armed or disarmed: Audible Response: internal sounder. Communicator: Fault event. If armed only: Activates 'Global Fault 1' output type. If disarmed or armed: Activates 'Global Fault 2' output type. Note that the 'Technical Fault' output type is triggered every time a fault is active including when the fault input type is active.
17	Arming Control	Active during arming procedure: No audible or communicator response. Prevents system being armed whilst the input is in an active state.
18	Shunt	Active at all times: No audible or communicator response.

		<p>It is possible to associate inputs to the shunt input. It is normally connected to a key-switch (or equivalent) and when On or Off it shunts or un-shunts the inputs assigned to it. Associated outputs are available to follow this input type.</p> <p>Creating a Shunt Group: A shunt group may consist of any number of inputs programmed as Instant, Tamper, 24hr and Follow types. These must all be allocated in the same area.</p> <p>NOTE: <i>These inputs will need to be programmed before allocated to the shunt input.</i> The inputs in the shunt group/list will only activate after 10 seconds of the nominated shunt input.</p> <p>Example: If input 1 is programmed as 'Shunt Input', and inputs 2 and 3 are programmed as "24hr", then once input 1 has been opened, after 10 seconds inputs 2 and 3 become active.</p> <p><u>Action 1:</u> Shunt Input closed <u>Status:</u> Inputs within the shunt list are shunted (Disarmed) <u>Outputs:</u> 'Follow Input' PGM output On</p> <p><u>Action 2:</u> Shunt Input opened <u>Status:</u> After 10 seconds inputs in the shunt list are going to activate, i.e. become Un-shunted (Armed) <u>Outputs:</u> 'Follow Input' PGM output OFF. The 'Shunt Fault' PGM output is on for 10 seconds.</p> <p><u>Action 3:</u> Shunt Input opened with active detector from the shunt list <u>Status:</u> After 10 seconds inputs in the shunt list are going to activate, ie become Un-shunted (Armed) <u>Outputs:</u> 'Follow Input' PGM output OFF. The 'Shunt Fault' (type 36) PGM output pulses until the detector closes.</p>
19	Disarm Only*	Active when armed: Accepts input from keyswitch (or equivalent) to disarm the area(s) assigned to it.
20	Keyswitch Latched*	Accepts input from keyswitch (or equivalent) to arm/disarm the area assigned to it. Arming includes normal exit time, etc. Requires latching switch action. Normal operation is open circuit to arm the system, and close circuit to disarm the system.
21	Entry Shock	Active when system armed: This input type is advised to be used in conjunction with an Entry Delay input. The Entry Delay input is a door contact on the initial entry door, and the Entry Shock input is a non-latching shock sensor fitted to the door frame in the vicinity of the lock. If the door is forced a Burglary alarm will be generated immediately instead.
22	Line Fault	Active when fail. This input type is used to detect external transmission equipment line fail (output). If activated it will give a line fault alarm, and will signal telecom line fault on expiry of line fault timer. It can be used in conjunction with CCTV input (type 39)
23	Keyswitch Pulsed*	Accepts input from keyswitch to arm/disarm the area(s) assigned to it. Requires momentary action switch to toggle arm/disarm state. Note that Grade 1 operation only allows arming from the push button, but requires means to abort arming (not to disarm)
29	Interior	This will work the same as an instant type input, the only difference is that when CID reporting is programmed then any inputs that are programmed as Interior will report CID event 132.
32	Flood	This input type will work as a 24hr input, any inputs that are programmed for Flood will activate the external siren and will report CID event 113.
39	CCTV	Active at all times: No audible alarm or communicator response. The CCTV input should be connected to an external detector located next to a CCTV camera. An output can be programmed to follow this input and the output should be connected to a CCTV recording, transmission or other device. An input programmed as "Line Fault" (input type 22) should also be connected to an output of the CCTV transmission Device. If the CCTV transmission line has been cut or missing the 'Line Fault' input will activate. Following this, at each activation of the CCTV input the panel will signal CID events for 'Silent Burglary' and Line Fault. No audible alarm will be

		created. If the Line Fault is not active it will just log the activations of the CCTV input into the event log.
40	Perimeter	This will work the same as an instant type input, the only difference is that when Contact ID reporting is programmed, then any inputs that are programmed as Perimeter will report Contact ID event 131.
41	Patrol / Keybox	This input type will work similarly to a switcher input, it does not trigger an alarm but will report Contact ID event 250 and is also a useful input type when an output is required to follow the 'Keybox' type input.
42	Medical	This is a 24 Hrs type input it will activate the external sounder and report a Contact ID event 100.
43	Entry Delay 2 [§]	Any input programmed as Entry Delay 2 will act as input type 07, but the associated entry timer will use Entry Timer 2, rather than Entry Timer 1.

Choose User

Select the user keyfob to program.

Chose User → Select Button

The different buttons and button combinations that may be programmed are:

- [1] Lock Button
- [2] Unlock Button
- [3] Button I
- [4] Button II
- [5] Lock + Unlock Buttons
- [6] I + II Buttons
- [7] Lock + I Buttons
- [8] Unlock + II Buttons

Choose User → Select Button → Button Action

Options are 'show status', 'arm area', 'disarm area' and 'operate output'. Two key combinations may also have 'panic attack' assigned to them. 'Arm Area' features a sub option to choose which area to arm. 'Operate Output' features a sub option to choose which output to trigger.

Choose User → Select Button → Button Action → User Controls

If an action is programmed as 'Arm Area' then the areas which the keyfob will control can be selected here.

PLEASE NOTE: ONCE ALL WIRELESS INPUTS (DETECTORS AND DOOR CONTACTS) ARE LEARNT, INPUT TYPE MUST BE ASSIGNED TO THEM, THIS IS PROGRAMMED IN 'PROGRAM INPUTS'.

5.3 Program Inputs?

By default, all inputs are set to 'unused'. Before programming, identify input type required:

#These inputs cannot be bypassed.

*Use of inputs 19, 20 and 23 will make the system unable to comply with EN50131-1 Security Grade 2.

§ Ensure that these inputs are used on an entry/exit route

5.3.1 Choose Input

Choose an input to program.

Input In Area

Enter the areas for input to operate in.

Common Input

In certain situations, a 'common' area may be needed. A common area is an area that only arms if other specific areas are armed.

Example: A reception in a building will only need to be armed if the offices and warehouse are armed. If the office is armed, but the warehouse isn't, then the reception would still need to be inactive so people would be able to leave the premises. One input can be allocated to one or more areas. In this example the inputs located in the reception area will be in the offices and warehouse areas and have the common attribute activated.

Area A: Office - Inputs 1, 2, 3, 4 and 8.

Area B: Warehouse - Inputs 5, 6, 7 and 8.

Input 8: The detector connected to this input is going to be the input located in the Reception and

is common to Area A and Area B.

Input 8 will only be active if the Area A and Area B are both armed. If one of them is disarmed the input 8 will not be active either.

5.3.2 Input Attributes?

No	Attribute	Operation for both wired and wireless inputs
1	Chime	When enabled the system loudspeaker(s) will 'chime' when an input is triggered whilst the alarm panel is disarmed. Chime can be single – sounding once or follow – sounding while the door is left open. NOTE: The chime can be turned On or Off in disarmed mode by pressing [c] when all Entry Delay inputs are closed.
2	Allow Bypass*	Enables the input to be manually bypassed during the arming procedure or from the user menu whilst the panel is disarmed.
3	Double Knock	If enabled, an alarm will be generated if this input is triggered twice within the pre-programmed time window or if the input remains active for that period. The double knock option does not work on 'Follow' input type.
4	Combined Input	Alarm will only be generated if 2 inputs one next to the other with Combined Input attribute have been activated at the same time. This option is very useful for setting up out door perimeter protection.
5	Normally Open [#]	Both wired and wireless inputs are normally set to Normally Closed. This attribute allows to set up the input as a Normally Open.
6	Mask Test	The panel will not arm if the user does not activate each detector with this attribute after starting the arming timer. This is a way to prevent arming the system with masked or faulty detectors.
7	Non Activity Input	This attribute works in conjunction with the NAT (Non Activity) timer. If a detector has not been activated during the NAT time the NAT output if programmed will be activated. An event will be registered in the log too.
8	Special Log (SP)	Forces a log entry when the input is opened or closed, even when an alarm does not result. May be selected to apply when a system is armed, when disarmed, or always.

*Only the bypassing during the arming procedure is EN50131-1 approved

The use of this input attribute will make the system unable to comply to EN50131-1 Security Grade 2

5.3.3 Input Description?

2 text labels can be associated to each input:

Enter Number: This is commonly used to write the Input Number here: Input 1, Input 2 etc. This label will show the event log, following alarms, reported in the SMS alarms as a reference point. There are only 7 characters available for this label.

Enter Name: This is commonly used to write the location of the input. There are 14 characters available for this label. **Example:** Input Number = Input 1; Input Name = Living Room. In case there has been a tamper alarm on the input -on the SMS will be shown: 'Input 2, Living Room, Tamper Alarm'. On the display will be shown: 2-Living Room, Tamper on Input. Meaning: Tamper alarm on input 2 that is the Living Room.

5.3.4 Manually Bypassing Inputs Procedure

Method 1: Whilst the system is arming, press the key to bypass inputs.

Method 2: Enter user menu and from the "Bypass Inputs" option bypass the inputs required.

NOTE: Only Method 1 is EN50131-1 Grade 2 compatible. The input attribute "Allow Bypass" must be enabled on each input that the user has the ability to bypass.

5.3.5 Automatic Bypassing Inputs Procedure

Inputs may be automatically bypassed when the panel auto re-arms if this option is enabled in the system options.

5.4 Install RIXs?

Up to 4 x RIX8i or RIX8+ may be installed on the system. Any Remote Input Expanders (RIXs) installed on the Enforcer 32-WE system must be enabled in the 'Install RIXs' menu. For installation details, please refer to the Installation Reference manual.

5.4.1 RIX Address

Select the address of the RIX to enable (Address 0-3).

5.4.2 RIX Installed

Enable/Disable the RIX installed. 1 = Enabled / 0 = Disabled

5.4.3 RIX Location

The location text is stored for reference on later maintenance visits i.e. "GROUND FLOOR". For information on how to use predictive text, please see page 5.

NOTE: We recommend if adding wired input expander RIX's -to use the version with the PSU integrated on board, because the Enforcer PSU might be insufficient to power multiple additional detectors.

5.5 Program Outputs?

This option enables the programming of the outputs on the Enforcer 32-WE and any devices that are connected.

5.5.1 Endstation PGMs?

These are the outputs on control panel itself. There are 3 outputs on the I/O module of Enforcer – BELL PGM, STB PGM and PGM. All of them are programmable but the BELL and STB are allocated to follow the alarm in any area as bell and strobe.

5.5.2 RIX Module PGMs?

These are the outputs that are located in the RIX8+ input expander module, if used. There are 4 PGMs located on this module.

5.5.3 ROX Module PGMs?

This option enables the addition of a wired ROX module to Enforcer as well as programming of the PGM options for the outputs in the module.

5.5.4 Keypad PGMs?

Allows the programming of the PGM options for the outputs located on the wired keypads.

5.5.5 Reader PGMs?

Allows the programming of the PGM options for the outputs located on the wired readers.

5.5.6 User Outputs?

These outputs are used for creating automation control for Devices. The user can control them remotely from the user menu on the keypad. The automated user outputs can be programmed either latched or pulsed.

Polarity of the PGMs: The polarity of the outputs is normally switched negative i.e. in normal status OFF = 0v and in active status ON = 12v.

NOTE: The PGM Outputs polarity cannot be inverted.

No.	Output Type	Active	Restore
0000	Not Used		
0001	Fire	At fire alarm activation	When a valid code is entered
0002	PA Any	At personal attack activation	When a valid code is entered
0003	Burglary Any	At burglary alarm from any area	At first valid code entry
0004	Final Arm All	When ALL areas are armed	At code entry to disarm
0005	Open After Alarm (Abort)	When system is silenced after 'burglary' alarm has been activated	After 2 minutes
0007	Tamper Any	Tamper alarm in any area	At code entry to silence
0008	Duress Any	At a Duress alarm in any area	When a valid code is entered
0009	PA Device Any	At alarm on a PA input only from any area. (This does not include the keypad PA)	When a valid code is entered
0010	Gas	At gas alarm	When a valid code is entered

0011	Arm Fail	Pre-set time after start of exit time, if exit procedure is not complete	At code entry to rearm
0012	Entry Deviation	When deviation from entry route occurs, during entry time	At code entry to disarm
0013	System Ready Any	When any of the inputs but the Entry Delay and Follow are closed	If fault exists, and after final arm
0014	Bell Any	After alarm in any area	When alarm silenced or when siren timer expires
0016	Strobe Any	After alarm in any area	When disarmed or when strobe timer expires
0017	Bypass Rearm Any	When inputs are bypassed at rearm in any area	When system disarmed
0018	Burglary (Unconfirmed) Any	At Burglary alarm in any area	At code entry to silence
0019	Ready All	When all inputs but the 'Entry Delay' and 'Follow' inputs are closed	If fault exists, and after final arm
0020	Exit Starts All	At start of exit time to arm LAST area	At disarm FIRST area (i.e. no longer fully armed)
0021	Exit Starts Any	When exit time starts to arm FIRST area	At code entry to disarm LAST area
0022	Final Arm Any	When ANY area has been armed	At code entry to disarm LAST area
0023	Strobe if Arm Fail	Works similar to output 016, but also fires if the 'arm fail' timer expires.	
0024	Unable to Arm	This output turns on for 5 seconds when the system is disarmed via a keyswitch input (either pulsed or latched keyswitch)*	
0025	Keyswitch Disarm	Output activates when an arming procedure is completed with inputs bypassed.	
0026	Arm with Bypass	Active when the system is armed with an input bypassed.	
0027	Pulsed Burglary Any	Active when burglary alarm is triggered, but deactivates once the Pulsed Intruder timer has expired (see Program Timers).	
0028	Power Fault	Active during low volts and battery faults. Restores at code entry after fault cleared.	
0031	Entry	Active during any Entry time	
0032	Exit	Active during any Exit time	
0033	Entry / Exit	Active during any entry or exit time	
0034	Lights	When exit or entry timer starts	20 seconds after arm/disarm procedure completed
0035	Follow Input	Active when a specific input number has been activated. It allows the following options to be programmed: <ul style="list-style-type: none"> - Follow Type (Follow, Timed, Latched, Code Reset); - Follow What (Input, Shunt List, Sub-Area, Area); - Follow When (Always, When Armed, When Disarmed); - Input to Follow (between 1 to 64) 	
0036	Shunt Fault	This input activates if someone tries to shunt an input group where some of the inputs allocated to this group are open.	
0037	Restore 1	At code entry to arm. The normal state of this input is 0v and it changes to 12v when activated.	After 3 seconds
0038	Restore 2	Activates whenever an additional area is armed. The normal state of this input is 0v and it changes to 12v when activated.	When disarmed
0039	PIR Latch 1	When armed (and in Walk Test)	At alarm, or when disarmed
0040	PIR Latch 2	This is the inverse polarity to PIR Latch 1	At alarm, or when disarmed
0041	AC Mains Good	Output showing the 230v mains supply is present	

0042	PIR LED Enable	This output activates during walk test	
0043	Follow Test	Output will activate only when tested from the Engineer menu 'Test Outputs' in the 'Engineer Tests'. This output can be used as additional facility for testing the operation of a Bell. An output programmed to one of these configurations (43 & 44) may be used to trigger a relay to break the hold-off connection to the Bell - or even to provide the hold-off directly.	
0044	Off During Test	Output is normally active and will deactivate only when tested from the Engineer menu 'Test Outputs' in the 'Engineer Tests'. Same as 43 but opposite activation.	
0048	Walk Test	This output is active during walk test, and will only deactivate when all detectors have been tested	
0049	Detector Masked	If any detector goes into 'mask' condition the output will activate	When masking fault clears
0050	Follow 24 Hour	If any input programmed as '24 Hour' activates	When input is restored
0051	Line/GPRS Fault	When Telephone or GPRS Line Fault is present.	When fault clears
0052	AC Mains Fail	After pre-set time without mains power	On restoration of mains
0053	Battery Fault	When battery disconnected or load fail detected	At next valid code entry
0054	Low Volts	When less than 11.2v are present	When fault clears
0055	Global Fault 1 (Grade 2)	Activates if any fault occurs only when system is armed	When all faults cleared
0056	Global Fault 2 (Grade 3)	Activates if any fault occurs at any time	When all faults cleared
0057	German Relay	For future development. Do Not Use.	
0058	Guard Code Used	When 'guard' code used on the system	After 60 seconds
0059	Engineer Access	When entering Engineer Mode	When leaving Engineer Mode
0060	Follow Power Up	At power up	Live for 45 seconds
0063	Test UK STU	Activates when a test call is sent	When test completed
0064	Pre RM Service	Activates 1h before the RM Service call	When test completed
0065	Input Fault (Follow NAT)	Activates when there is no activity on an input in the end of the "NAT-Non Activity Timers" in Change Timers.	When there is activity.
0066	ATE Pin Not Used	Makes the ATE pin 5V or 0V depending on whether ATE outputs are inverted	
0067	Follow Chime	Active while a Chime signal is created on the panel	
0170 -- 0199	User Defined 01-30	The user outputs are used for user automation to control external Devices. They can be controlled via the keypad from the user menu and can be programmed as 'latched' or timed (1 to 99 sec).	
0202	PA A (As 0002 for Area A)	0213	System Ready A (As 0013 for Area A)
0203	Burglary A (As 0003 for Area A)	0214	Bell A (As 0014 for Area A)
0204	Final Arm A (As 0004 for Area A)	0216	Strobe A (As 0016 for Area A)
0207	Tamper A (As 0007 for Area A)	0217	Bypass At Rearm A (As 0017 for Area A)
0208	Duress A (As 0008 for Area A)	0218	Burglary (Unconfirmed) A (As 0018 for Area A)
0209	PA Device A (As 0009 for Area A)	0219	Ready A (As 0019 for Area A)
0210	Fire Reset A (As 0010 for Area A)	0220	Exit Starts A (As 0020 for Area A)
0620-0639	Logic Gate 1-20. Logic gate outputs (programmable via the upload/download software)		
Then this pattern repeats for all other areas other areas so that:			
0222-0240 Area B 0242-0260 Area C 0262-0280 Area D			
1001-1066	Active when input opened and close when input is closed		

*The use of pulsed or latched keyswitch will make the system unable to comply with EN50131-1

5.6 Install Keypads and Readers?

Ensure that all keypads and readers are addressed correctly (at the device) before enabling and addressing them in this function. To address at the device please refer to the installation reference manual.

NOTE: At least one keypad/reader should have the ability to disarm any areas programmed.

5.6.1 Device Address

Address [0] is reserved for the Enforcer built in LCD keypad only. In the addresses from [1] to [3] is possible to allocate external wired readers or LCD keypads.

5.6.2 Device Type

The device types that is possible to program are LCD keypads [0] or Readers [1].

Reader Device Type

If a Reader is enabled, it can operate as the following:

Arm/Disarm

This will make the Reader act like a normal keypad (arming/disarming the areas etc.)

Device Arms Areas: This feature programs which area(s) the reader can arm.

Device Disarms: This feature programs which area(s) the reader can disarm.

Device in Area: This feature programs in which area(s) the reader is active.

Door Name: Enter the name of the door such as Front Door.

Door Location: Enter the location of the door such as First Floor.

Arm/Disarm Sub-Area

A reader can be used to create sub-areas controlled independently from the area.

Add Inputs: Each sub-area may consist of any number of inputs, all of which must be allocated to the same area. No input may be allocated to more than one sub-area. Entry Delay input types cannot be allocated to a sub-area and in the sub-area the arming/disarming of the inputs is immediate without delay timers.

The sub-areas can be operated by proximity tag, or by key (or other) switch wired into the first input on the tag reader. Notice that the proximity Tags for sub-area control are programmed through the Manager menu using the 'change codes' options. The reader provides 'Alarm' and 'Ready' outputs dedicated to that sub-area. It also provides relevant indications, including Arm/Disarm status, so should always be located adjacent to the controlling Key switch where this is used.

Sub-Area Arms: If this option is selected as 'If Area Armed' then the sub-area will always arm when the area in which is it located is armed. If selected as 'Never' it will always require manual arming from the tag. The sub-area must ALWAYS be disarmed manually.

An additional option is available in the 'SYSTEM OPTIONS' menu, to permit an 'Open After Alarm' (abort) signal to be generated by silencing an alarm at the Reader after an alarm has been generated in the sub-area. Please see page 21.

Action	Status	Notes
Disarmed	Detectors within sub-areas are inactive	'Disarmed' indication lit
Sub-areas input triggered	No response	
Attempt to arm sub-areas with an open input	-	'Fault' LED flashes and intermittent tone to indicate 'cannot arm'
Arming with no open inputs	Sub-area arms	'Disarmed' LED goes out
Sub-area input triggered	Alarm generated	'Alarm' LED lights, alarm tone generated
Valid code entered at a Keypad whilst alarm in sub-area is active	Alarm silenced by user code	Sub-area remains armed

Sub-Area Control: The sub area can be controlled by Tag or Input. When an input is used to control the sub-area a keyswitch input type should be used and connected to an external key or switch.

Sub-Area Name: Enter the name of the sub-area such as 'Private Office'.

Sub-Area Location: Enter the location of the sub-area such as 'First Floor'.

Assigning Tags to Sub Area Reader: To assign tags to the sub-areas, enter the master manager menu and select 'Change Codes', add a new user code (tag) and when the prompt shows 'Sub Area Access', enter the address of the reader you would like the tag to operate for the sub-areas.

Access Control

Allows the reader to control doors fitted with electrical locks. On the readers there are 2 inputs that also can be outputs. They can be connected to the lock for opening and controlling the door.

Lock Open Time: This is the time the door release is going to be active when a valid tag is presented.

Door Open Time: This is the time the door is allowed to be open before triggering an alarm.

Door Name: Enter the name of the door such as Front Door.

Door Location: Enter the location of the door such as First Floor.

NOTE: Access control falls outside the scope of EN50131-1.

Disarm Only

Allows the reader to be used to disarm the system only.

Device Disarms: This feature programs which area(s) the reader can disarm.

Device in Area: This feature programs in which area(s) the reader is active.

Device Name: Enter the name of the door such as Front Door.

Device Location: Enter the location of the door such as First Floor.

Entry Control

Allows the reader to be used as arm/disarm Device and access control.

Device Arms Areas: This feature programs which area(s) the reader can arm.

Device Disarms: This feature programs which area(s) the reader can disarm.

Device in Area: This feature programs in which area(s) the reader is active.

Lock Open Time: This is the time the door release is going to be active when a valid tag is presented.

Door Open Time: This is the time the door is allowed to be open before triggering an alarm.

Door Name: Enter the name of the door such as Front Door.

Door Location: Enter the location of the door such as First Floor.

Keypad Device Type

Device Arms Areas: This feature programs which area(s) the keypad can arm.

Device Disarms: This feature programs which area(s) the keypad can disarm.

Device in Area: This feature programs in which area(s) the keypad is active.

Door Name: Enter the name of the door such as Front Door.

Door Location: Enter the location of the door such as First Floor.

5.7 Program Timers?

Timers	Description	Options
Entry Time 1 Entry Time 2	Programmes the entry time for each area. If entry time is started at a door programmed in multiple areas, the longest time will apply. Entry time 1 will apply to any inputs programmed as "Entry Delay 1" type, and Entry Time 2 will apply to any inputs programmed as "Entry Delay 2" type. Ensure that timer is no longer than 45 seconds in order to comply with EN50131-1.	0-255 seconds
Exit Time	Programmes the exit time for each area. If the system is being armed at an arm device programmed as 'IN' multiple areas, the longest of those times will apply.	0-255 seconds
Bell Time	Cut off time for external sounder. Separate for each area. Repeat above steps for each of the Enforcer 32-WE areas programmed.	0-15 minutes
Bell Delay	Delay after burglary alarm before bell activation. NOT valid within 3 minutes of final arm, or after entry time started. If 'Silent 1st Alarm' selected in alarm responses, delay commences at confirmed alarm.	0-20 minutes
Strobe Time	The duration of time the strobe output remains live after the bell time ends, '99' means endless.	0-99 minutes
Number Re arms	Number of times system re-arms after bell time ends. Re-arm number applies to each area, and does not affect emergency alarms. '9' = 'always re-arm'.	0-9
AC Fail Delay	Time delay before mains failure or technical alarm signalled. '250' = never alarms. System change-over to battery supply and associated 'alert' indication is always immediate. Mains Fail message on keypad not permitted until valid code entry.	0-250 minutes

Final Door Delay	Time between final door input closing and system arming. When a code is entered to arm the system the exit time will start but the system will not arm until it sees the final exit door open and close and duration of the final door delay.	0-255 seconds
Double Knock	Length of filter period applied to inputs with 'Double Knock' input attribute.	0-75 seconds
Delay Send Entry	Delays 'Burglary' alarm signalling if an alarm is generated by deviation from the entry route. Delay Send Entry must be programmed for a minimum of 30 seconds to comply with EN50131-1.	0-255 seconds
Line Fault Delay	Duration of Telecom (GPRS) Line Fault before 'Line Fault' alarm triggered, '250' endless.	0-250 seconds
Arm Fail Time	If a system has not been armed within the entry delay time, for example if a door was left open -the 'Arm Fail Time' will take over and at the expiry of this time an alarm will be created. This time should be longer than the Entry Delay Time.	0-255 seconds
Guard Code Delay	The minimum time an alarm must have been present before a 'Guard' code will be accepted to disarm.	0-10 minutes
Fire Bell Time	Cut off time for fire alarm. '99' = endless.	1-99 minutes
Arm Fail Warning	The 'Arm Fail Warning' will overwrite the 'Arm Fail Time' feature if the 'Alarm When Arm Fail' in System Options has to be set as 'NO'. Example of how this feature works: Set 'Arm Fail Warning' to a longer time than the 'Entry Delay Time'. For example if the 'Entry Delay Time' is set to 30sec the 'Arm Fail Time' could be set to 1 minute. If the system is not armed after 30sec then the Entry Delay Tones will start and the system will be disarmed at the end of the Arm Fail Warning time. An event called 'Arm Fail Warning Activated' will be logged in the event log too.	0-99 minutes
NAT Day Timer	NAT stands for 'Non-Activity Timer'. This is used in conjunction with the input attribute 'Non Activity Input', and will monitor the chosen input for the selected number of days. At the expiration of the timer, and if the input has not opened within that time, then this will be stored in the panel log as 'Non Activity fault' and there will be an output activated if programmed to it. Send SMS message if "Special Log" is on.	0-14 days
NAT Hours Timer	NAT stands for Non-Activity Timer. This is used in conjunction with the input attribute 'Non Activity Input', and will monitor the chosen input for the selected number of hours. At expiration of timer, and if the input has not opened within that time, then this will be stored in the panel log as Non Activity fault and there will be an output activated if programmed to it. -Sends SMS message if "Special Log" is on.	00-23 hours
Pulsed Burglar Any	This option sets up the duration of the pulse of an output programmed as "Pulsed Burglary Any" which activates after a burglary alarm.	0-255 seconds
WLS Supervision Time	This is the time window before a supervision fault will be signalled. For example: if the time is set for 2 hours, then any device that doesn't communicate with the Enforcer 32-WE within that period will cause a supervision fault. It must be programmed to 2 hours or less for compliance with EN 50131.	0-99 hours
WLS Jamming Time	This is the time window that if a wireless device had its signal 'blocked' a fault would display. For example, if the time is set for 30 seconds, then if a wireless device is 'jammed' for longer than 30 seconds a fault will be displayed. Must be set to 30 seconds or less (but not zero) for compliance with EN 50131.	0-100 seconds
Service Time	This is a timer that can be programmed in days, and will display a message to the user warning that a service is due. An engineer code will clear the message.	367

5.8 Change Codes?

All codes may be 4, 5, or 6 digits long and can also be assigned as proximity tags and keyfobs. 75 user codes are available

NOTES: Only 'Duress/Guard', 'Master Manager' and 'Engineer codes' can be changed by the engineer. User codes can only be changed by the Master Manager from the Master Manager menu. The Master User and Engineer Codes cannot be deleted.

User	Arm and Disarm System. Also for Access Control and Sub Area Control functions	Programmed by Manager only.
Manager Default: 1234	Arm and Disarm System. Also access to Manager menu functions	Programmed by Manager or Engineer.
Engineer	Access to all engineering functions; also arm/disarm system for test purposes.	Programmed by Engineer.
Duress	Disarm system, generating silent 'Duress' signal.	Programmed by Engineer.
Guard	Disarm system, but only after an alarm has been active for a minimum time (programmable). Also arm system. An output type is available to activate whenever this code is used.	Programmed by Engineer.

5.8.1 Change Duress/Guard Codes?

Choose Code Number

If a code or tag is already allocated, the display will show [*****]. Press to clear the code.

Choose Code Number → User Type

The user type can be Duress or Guard.

Duress Code

The Duress code can arm or disarm the system and if used, a Duress communication event will be sent. An output type is available to activate whenever this code is used (Duress type 008 - see page 31 Program Outputs).

User In Area

Choose the area the code is active in - A,B,C,and D.

User In Area → User Arm Options

[0] Disarm/Arm: The code will arm and disarm the areas selected in the previous option.

[1] Disarm Only: The code will only disarm the areas selected in the previous option.

[2] Arm Only: The code will only arm the areas selected in the previous option.

[3] None: No option programmed.

User In Area → User Arm Options → Arm Area Choice

If a user code is allocated to more than one area and the Arm Area Choice option is set to NO, the code will automatically arm all areas it has been allocated to when the code is entered to arm. If the Arm Area Choice has been set to YES then the user will be given the ability to choose which area to arm when the arming procedure has been activated.

User In Area → User Arm Options → Arm Area Choice → User Name

Write the name of the user for this code.

Guard Code

This code can disarm the system, but only after an alarm has been active for a minimum time programmable in the timers. Use of this code will generate a normal user arm/disarm event. An output type is available to signal whenever this code is used.

User In Area

Choose the area the code is active in - A,C,B,and D.

User In Area → User Arm Options

[0] Disarm/Arm: The code will arm and disarm the areas selected in the previous option.

[1] Disarm Only: The code will only disarm the areas selected in the previous option.

[2] Arm Only: The code will only arm the areas selected in the previous option.

[3] None: No option programmed.

User In Area → User Arm Options → Arm Area Choice

If a user code is allocated to more than one area and the Arm Area Choice option is set to NO, the code will automatically arm all areas it has been allocated to when the code is entered to arm. If the Arm Area Choice has been set to YES then the user will be given the ability to choose which area to arm when the arming procedure has been activated.

User In Area → User Arm Options → Arm Area Choice → User Name

Write the name of the user for this code.

NOTE: For both duress and guard codes it is possible to program a tag too. In case a tag is programmed it has to be associated to a reader.

5.8.2 Change Master Manager Code

If a code or tag is already allocated, the display will show [*****]. Press the **C** key to clear the code and use the numeric keys to enter the new code. This option allows the engineer to change the Master Manager code -should this been lost or forgotten.

User In Area

Choose the area the code is active in: A,B,C,and D.

User In Area → User Arm Options

[0] Disarm/Arm: The code will arm and disarm the areas selected in the previous option.

[1] Disarm Only: The code will only disarm the areas selected in the previous option.

[2] Arm Only: The code will only arm the areas selected in the previous option.

[3] None: No option programmed.

User In Area → User Arm Options → Arm Area Choice

If user code is allocated to more than one area and if the 'Arm Area Choice' option is set to 'NO', the code will automatically arm all areas it has been allocated to in the same time. If the Arm Area Choice has been set to YES then the user will be given the ability to choose which area to arm when the arming procedure has been activated.

User In Area → User Arm Options → Arm Area Choice → User Name

Write the name of the user for this code.

5.8.3 Change Engineer Code

If a code or tag is already allocated, the display will show [*****]. Press **C** to clear the code and use the numeric keys to input the new code.

5.9 Volume Control?

The Volume Control function applies to both the buzzer and the internal sounder.

5.9.1 Area A,B,C,D Entry Tone Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.2 Area A,B,C,D Exit Tone Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.3 Alarm Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.4 Fire Alarm Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.5 Technical Alarm Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.6 24 Hour Alarm Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.7 Chime Volume

0=Completely Silent, 1=Silent, but beeps when the system is armed. 2-5 Buzzer 6&7 = Internal Siren

5.9.8 Code Stops Sound

This option is very useful when 2 or more independent areas are used on one system. If programmed as 'Yes', once an alarm has been generated in an area, the user of a different area by

his/her user code on his/her keypad will silence the alarm without disarming the area; and an 'Open After Alarm' (Abort) event will be sent for the silenced area. The area will still be armed until a valid user code that controls that area is entered.

5.9.9 Silent Technical Alert

If enabled, any technical alert sounds (such as mains fail, line fail etc.) will be silent.

5.9.10 Main Sounder All

If enabled, all volumes that are programmed as 2-7 will activate on the main sounder. If disabled, the sounder will only activate on activations programmed on volume 6-7.

5.9.11 Disable Call Fault

If enabled, any call faults will only be displayed in the log and not on the display

5.10 System Options?

This function programs all system options, system displays and exit modes.

5.10.1 Options

Arm With Tamper	If 'Yes', arming will be allowed regardless of the following faults: Case tamper and System tampers.
Arm If Modem Fault	If 'Yes', arming will be allowed regardless of the following conditions: Telecom line fail, Modem failed, ATE line fault, ATE one path fail, Digi dial fail, ATE communication fail.
Arm With Tec/Flt	If 'Yes', arming will be allowed regardless of whether 'mains', 'battery', 'telecom line', or other system fault is present.
Arm Fail = Alarm	If 'Yes' = A graduated alarm will be generated when the 'Arm Fail' timer expires (see Program Timers), if an exit procedure is still incomplete the arm fail output will trigger too. If 'No' = The Exit Time will continue until the Exit door is closed. It will return to disarmed mode at the end of the 'Arm Fail Warning' time if programmed.
Do Battery Load Test	If 'Yes' the system will perform a full load test of the battery at 7.00am each day.
Arm Acknowledge	This function is used to indicate the armed status of the system via the bell. It will activate for 5 seconds. The armed status can be indicated by: Strobe Flash, Bell Squawk; or Both. NOTE: This can create a potential security risk. Since the keyfob can show this status too we recommend using the keyfob instead.
Bypass On Re-Arm	If 'Yes', the input that generates an alarm will be bypassed when the bell time expires. If the input is closed then it will automatically become active again.
Forced Arm	If 'Yes', the Enforcer 32-WE will arm even if an input is open at the time of arming and will be bypassed (bypass attribute must be enabled).
Tag Only Disarm	If 'Yes' the Enforcer 32-WE prevents a user code being entered during the Entry Time, but allows a code to silence the Enforcer 32-WE once in alarm. A tag will disarm and reset the system.
Quick Arm	If 'Yes', the Enforcer 32-WE allows a user to arm the system by pressing the <input checked="" type="checkbox"/> key and then selecting the area: A, B, C or D. NOTE: This option should not be used on EN 50131 Graded systems.
Keypad PA Key	Pressing the dedicated PA button or a combination of <input type="checkbox"/> and <input type="checkbox"/> keys will produce a PA. There are several options for this feature: Disabled=Inactive; Silent+Digi=Silent PA (signalling only); Bells Only=Bells Only (No signalling); Bell+Signal=Signalling and Bells.
Manager Program PA	If 'Yes', a manager will be able to program 'Personal Attack' on a wireless keyfob button action.
Tag Disarm+Door	This is used in conjunction with "Door Control" option in the Reader setting. If 'No', the readers will disarm system but not control doors. If 'Yes', the readers control the arming/disarming and doors as long as the reader has been programmed in the reader options.
Keypad Fire Key	If enabled the fire alarm button on the keypad will be enabled.
Arm with Supervision Fault	If 'Yes' the panel will arm the system if there is a wireless supervision fault. The keypad will flag up a wireless supervision fault but will allow the user to arm the system. If 'No', it will not be possible to arm the system with a supervision fault. The keypad will flag up the fault and the arming procedure will be stopped.

Keyfob on Entry	If 'Yes', it allows use of the wireless keyfob to disarm the system only when the Entry Door has been opened and entry time has started.
6 Digit Codes	All codes can either be 4,5 or 6 digits. If this option is enabled, all codes must be 6 digits.

5.10.2 System Displays

Please see page 5 for the 'Text Programming' section as this function involves programming different text for the Enforcer 32-WE system.

Area Texts	The text can be programmed for each area; Area A for example, you may want to be 'Full House Arm'. A maximum of 16 characters is allowed.
Full Area Text	The text that is displayed when all areas are armed.
Top Display Text	The top display text is shown on the keypad in disarmed mode.
Site Name	The Site Name is used as a "Site Reference" which must match the Site Name entered on the Upload/Download Software. If it does not, connection to the software will not be possible.
Display If Armed	If 'Yes', the keypad display will show 'armed' once the Enforcer 32-WE is armed. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.
Display Alarms	If 'Yes', then the keypad display will show all Alarms without requiring a user to enter their code or present their tag. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.
Ready LED On	If 'Yes', the 'OK' LED will illuminate whilst the panel is disarmed and when all the inputs in the areas (that the keypad controls) are closed. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.
Display PAs	If 'Yes', then the keypad display will show any PA alarms that have occurred without requiring the user to enter their code or tag. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.
Display Silent PAs	If 'Yes', then the keypad display will show any silent PA alarms that have occurred without requiring the user to enter their code or tag. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.
Display Inputs	If 'Yes', then the keypad display will show any inputs that are activated in disarmed mode. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.
Disarm LED ON	If 'Yes', the disarm LED (green) will illuminate continuously whilst the system is in disarmed mode. NOTE: Must be programmed as 'No' to ensure compliance with EN 50131.

5.10.3 Exit Modes

Timed	The system will only arm when the programmed 'Exit Time' has expired providing that all inputs are closed. Any 'Push To Arm' buttons fitted will also be live in this mode. The system allows the programming of 2 different Entry/Exit timers to be used with 'Entry Delay 1' and 'Entry Delay 2' input types.
Final Door	The system will only arm when an input programmed as 'Entry Delay 1' or 'Entry delay 2' opens and closes. This procedure is used to allow arming the system by the action of closing the exit door. It is possible to program a small delay time for the final door delay in 'Change Timers'.
Push To Arm	The system will only arm when a 'Push to Arm' button has been pressed. This function will override the programmed 'Exit Time'. The button can be used as a door bell when the chime input attribute is enabled ('Program Inputs')
Timed Final	This function follows the 'timed' operation, except that the timer will be overridden if an Entry Delay input (door) is opened and closed before the timer expires

NOTE 1: If the arming has not been completed within the programmed 'Entry Delay' time, it is possible to generate an alarm or return in disarmed mode. This option is defined in 'Change Timers' and 'System Options'->Options'.

5.11 Review Logs?

There are two logs available on the system; panel and access control. Each log displays the most recent event first. Use and to move forwards and backwards through the log. To view additional details, press the key. If no other information is available, the display will move to the next log entry. Press to return to the main screen for that log entry.

NOTE: In any disarmed or armed period, the Enforcer 32-WE will only log a maximum of three occurrences of any particular event.

NOTE: It is not permitted under EN50131-1 to delete any logs. The only circumstance in which the logs can be cleared, is part of the "Factory Default" operation - see page 33.

5.11.1 The Panel Log?

Includes Arm, Disarm, Trouble, User, Alarm, Engineer Access, Time & Date changes and etc.

5.11.2 The Access/Control Log?

Includes all Access Control and Guard Tour events.

5.11.3 System Fault Codes

For explanation of all faults that are displayed on the LCD display, please see page: 38.

5.12 Engineer Tests?

The Engineer Tests function allows the engineer to test inputs, outputs (PGMs), batteries and the bell.

5.12.1 Walk Test?

This function allows the engineer to test all programmed inputs on each area. The inputs that haven't been activated will be shown on the display. As each input is triggered, a chime will sound and that input will disappear from the list. Once all the inputs have been walk tested, 'Walk Test Completed' will be displayed. When walk-testing a double-knock detector, it must be triggered twice within the pre-set period. When testing combined detectors the first detector must be activated and then the second detector; next open the second detector and trigger the first detector.

A walk test can also be done on a single input if needed. This can be selected by pressing the key after the areas are displayed.

NOTE: The walk test feature can only be used if inputs are already programmed and saved (i.e. exiting the engineers menu).

5.12.2 Soak Test?

The Soak Test is used when inputs need testing without creating problems for the user. For example testing a perimeter alarm set up when false alarms are likely. If the input in soak test is activated whilst the area(s) in which it is located is armed, it will indicate the activation (at disarm) and enter the details in the system log.

NOTE: If additional inputs are placed on test without removing previously tested ones, they will be returned to soak test.

Test Inputs

The input numbers in test are added through this option. They will be shown on the display in a scrolling list.

Soak Days Left

To start the test for an input or group of inputs the number of days the soak test is required for is programmed in this option. The option also shows how many days are left after the required number of days has been programmed already (99 = 'endless'). For example, if today the engineer sets this option to 10 and checks it after 5 days then he will be shown 05 days left.

NOTE: If a number is not entered, the soak test will not start.

Initial Soak

This option will have to be programmed in the beginning of the test to be the same as the Soak Days Left. In the future when the engineer checks the status of the soak test this option will be used as a reference to know how long the test was set to in the first place. For example, if the test was set to 10 days then this option will show 10 days.

5.12.3 Bell Test?

Any outputs programmed as 'any bell' or 'any strobe' (including the wireless bells) will be activated in this test.

5.12.4 Battery Load Test?

The system performs a check of the battery operation every 10 seconds, by lowering the power supply voltage momentarily, and measuring the system voltage. If the battery voltage measured is below 12.0V, or the battery fuse has failed, a 'BATTERY FAULT 100' warning will be generated. The Enforcer 32-WE may be programmed to perform an automatic battery load test at every power supply at 07:00am each day from 'System Options: Battery Load Test' (See page 21) menu. This will drop the power supply voltage below the battery voltage, whilst monitoring the system diagnostics. The test will NOT take place if: the End Station bell and strobe PGMs are active, the system is in Engineer Mode, any battery fault exists, any mains fault exists, or the system option is not selected. If the test has already started, it will be aborted if any of these conditions apply, other than entry into Engineer Mode. If the test is aborted, it will NOT be performed until the next day.

5.12.5 Test PGMs? (Programmable Outputs)

Before any test begins, the output programming must be saved to the NVM by first exiting the Engineer Menu. The engineer can test all the Programmable Outputs on the End Station, ROXs, keypads and readers.

5.12.6 Send Test Call?

If Contact ID or SIA has been programmed, a test call can be sent. The system will send a test call event once the call is activated. Press the key after you see the prompt "Are you Sure?".

5.12.7 By-pass Fire/PA?

Whilst in the Engineer menu, the Fire and Personal Attack inputs/keypad alarms remain active. This function disables any Fire/PA activations when the Engineer menu is active.

5.13 Diagnostics?

This option enables the engineer to perform full diagnostics on all key wired and wireless components of the system.

5.13.1 Wireless Devices

View Inputs:

This option views the status of all wireless inputs: Open, Close, Tamper, and Fault.

View Inputs / Bells Signal Strength:

This options views the signal strength for any wireless input or bell that is learnt to the Enforcer system. The signal strength is shown on both the individual wireless device and on the Enforcer system in the following ways:

Wireless Device:

- If a Green LED is shown the signal strength is HIGH
- If a Red LED is shown the signal strength is LOW / NONE

Enforcer 32-WE Display:

Once the signal strength menu has been entered, 'Please Wait' will be displayed and a countdown from 300 seconds will begin. This may last up to 5 minutes before all of the wireless devices have been analysed. From this point each device is tested every 15 seconds. On the LCD display it is also possible to view each individual device signal strength in %.

- 3 = Excellent signal – Shows GREEN on the wireless Device / 80 to 100%
- 2 = Good signal – Shows GREEN on the wireless Device / between 30 to 80%
- 1 = Weak signal – Shows RED on the wireless Device / between 10 to 30%
- 0 = Missing – Shows RED on the wireless Device / between 0 to 10%
- '?' = Waiting for device signal strength information

View Inputs / Bells Battery Status?

This option is used to measure the battery levels for wireless inputs and bells. The battery level is shown on the control panel.

Once the battery status menu has been entered, , 'Please Wait' will be displayed and a countdown from 300 seconds will begin. This may last up to 5 minutes before all of the wireless devices have been analysed. From this point each device is tested every 15 seconds.

Testing = Waiting for a Battery result

Good = At least 1 month of battery life remaining

Replace = Battery needs to be replaced immediately

5.13.2 Wired Devices?

View Inputs

This option views the status of all wired inputs: Open, Close, Tamper, and Fault.

Endstation Inputs

The status of the inputs will be shown. C = Closed. O = Open. F = Fault, T = Tamper. The resistance reading can also be shown by pressing for any of the above for statuses.

RIX Inputs: Choose the RIX ID from [0] to [3] to view the inputs status.

View PSUs?

This option allows diagnostics of the power supply information for the PSU on the control panel as well as all the additional peripheral devices such as a RIX or ROX that have a PSU on board.

Endstation PSU

End station voltage readings are displayed = Voltage: 13.7V.

RIX PSUs

Choose the RIX ID from [0] to [3] to read the PSU voltage readings.

ROX PSU

Choose the ROX ID to read the PSU voltage readings.

Keypad Volts

Choose the Keypad ID from [0] to [3] to read the keypad voltage.

Reader Volts

Choose the Reader ID from [0] to [3] to read the reader voltage.

5.13.3 Communications

This function displays the information gathered from the communication device currently fitted.

GPRS Module:

GPRS Signal Strength: The range '0-31' indicates the signal (31 = Excellent. <15 = Poor). '-.-.-' indicates no signal.

App or ARC Status messages: Displays the current connection status of the Pyronix Cloud.

- Initialising – The panel is attempting to connect to the mobile network
- No Network – There is no network available
- Basic Network – The GSM network is available
- Full Network – The panel is logged onto the GPRS network
- Polling Cloud (App only) – The panel is polling the cloud
- Polling ARC (ARC only) – The panel is polling the ARC

Last Polled Cloud: Displays the time period since the last successful poll to the Pyronix Cloud.

Last Polled ARC: Displays the time since the last successful poll to the ARC.

LAN Module:

IP Address: Displays the IP address of the LAN Module (if installed).

Subnet Mask: Displays the Subnet Mask of the LAN Module (if installed).

Gateway: Displays the IP address of the Gateway.

App or ARC Status messages: Displays the current connection status of the Pyronix cloud.

- Initialising – The panel is attempting to connect to the network
- No Network – There is no network available
- Polling Cloud (App only) – The panel is polling the cloud
- Polling ARC (ARC only) – The panel is polling the ARC

Last Polled Cloud: Displays the time period since the last successful poll to the Pyronix Cloud.

Last Polled ARC: Displays the time since the last successful poll to the ARC.

Wi-Fi Module

For future use

5.14 Engineer Restore Options?

Restore Burglary	If 'Yes', then the user code will silence the alarm but the engineer must reset the system with the engineer code before it can be used again. This will not interfere with the generation of PA alarm.
Restore PA	If 'Yes', the Engineer can only reset the Enforcer 32-WE after any PA alarms. This will not interfere with the generation of Gas and Fire alarm.
Restore Tamper	If 'Yes', the Engineer can only reset the Enforcer 32-WE after any tamper alarms.
Restore Soak	If 'Yes', the Engineer can only reset the Enforcer 32-WE after any activated inputs that are under soak test.
Restore Faults	If 'Yes', the Engineer can only reset the Enforcer 32-WE after any of the below faults: ATE telecom fail, Modem fail, ATE single path fail, Telecom line fail, Battery disconnect, Battery charge, Battery load, Excessive charge, Battery critical, Device fail. Mains faults are excluded.
Anti-code Restore	If 'Yes', then the system displays (if one of the above features is enabled) an anti-code number. This code is used by the engineer to generate a reset code via a special software kit, the reset code is then given to the user to reset the system.

5.15 Communications?

The 'Communications' function programs the App, network, ARC, SMS and UDL facilities.

5.15.1 App Set Up

The Pyronix+ App is available in 2 versions: Android from Google Play Store; and iOS from the Apple store. Please refer to the User Manual for set up details.

Enable App: Enables the app functionality.

System ID: Displays the unique Enforcer serial number required to register the Enforcer with the Pyronix Cloud.

Cloud Password: A password is required to allow remote access.

Security

- Standard: Requires only a password for connection.
- High: 3 security options are required:
 - Generate App Password Key: A 24 character Hex-key is generated.
 - View App Password Key: Displays the key that has previously been generated.
 - Send Password Key in an SMS (when a GPRS module is fitted): Once a mobile number is entered, an SMS is sent with the security key.

Poll Server

- Yes: The Enforcer will poll with the App server regularly. The polling will be done often enough so that the Pyronix Cloud is aware of the Enforcer's location.
- No: The Enforcer will not poll with the App server. An SMS being sent to the Enforcer may be required to initiate communication.

The timing of the poll will be adjustable from the Pyronix Cloud. This will be allocated as an option for each panel. It will be adjustable from 1 – 99 seconds (default 8 seconds).

NOTE: If more than 8 seconds is selected a warning will be given that this will use more data and incur higher call costs.

5.15.2 Network Set Up

Three different modules can be connected to the Enforcer to enable different forms of communication. Please refer to the Installation Reference manual for information. The sub-menus will be enabled only for the module installed.

Program GPRS?

GPRS APN: Enter the GPRS APN, for example 'orange internet'.

GPRS User ID: Enter the GPRS user ID if the network requires this.

GPRS Password: Enter the GPRS password if the network requires this.

Program LAN?

Auto Set Up?

- Yes: The Enforcer will obtain the set up data from the router using DHCP.
- No: The following will be required:
 - IP Address: Enter the IP Address where xxx is a number between 1 & 255.
 - Subnet Mask: For most domestic installations the subnet mask will be 255.255.255.0.
 - Gateway: Enter the gateway, which is the routing device that the Enforcer is connected to.
 - 1st DNS IP Address: Enter the DNS Server IP Address.
 - 2nd DNS IP Address: Enter the alternative DNS server IP address if required.

Program Wi-Fi

For future use.

5.15.3 ARC signalling

The Enforcer 32-WE system can communicate with an Alarm Receiving Centre (ARC) using the LAN module or the GPRS modem.

ARC Details: Choose which ARC to program from 1 to 4.

Formats Available:

- Contact ID IP = See **page: 41** for the event table.
- SIA IP = See **page: 41** for the event table.

Valid Areas:

This option permits the set up a different ARC for a different area. Select which area this particular ARC will be reporting. Selecting ABCD means the ARC will be receiving events from all areas.

Area ARC Account → One Area Account

This options permits the engineer to set up individual area account for each area or open common account for all of them. Use the **[A]** key to add hexadecimal values; B to F. Numbers are entered by the number keys.

Redials: If the alarm event has not been received by the monitoring station after the first number has been called the second number will be called. The 2 numbers will be alternated as many times as the redials are set to. If a call has been acknowledged by the monitoring station then the panel will stop calling.

Timeout: This is the time of how long it takes a call to timeout before it is not answered.

Test Calls:

The test call is used to show that the system is still alive when no activations have been made. Setting up a test call asks for start time in hours and minutes and the frequency of call in days, hours & minutes.

Event Types: Please see page: 41 for all event options. If 'Custom' is selected, all event types can be chosen.

Sign Up ARC:

ARC Sign UP IP: The ENIP Address that is supplied by the ARC.

ARC Sign Up Port: The Port of the ENIP Server that is supplied by the ARC.

Security:

- Standard: Requires a password and connection handle (supplied by the ARC),
- High: Send Key by SMS:
 - Yes: The security key will be sent by the ARC software to the Enforcer.
 - No: The security key and connection handle must be entered manually.

Send Sign Up to ARC?

- Sign Up Successful: A message will be displayed indicating that the sign up was successful.
- Sign Up Failed: This may be due to the following reasons:
 - Incorrect Security Key
 - Incorrect Connection Handle
 - ARC Server not available
 - Account already exists

5.15.4 User SMS Signalling

To signal via SMS, a valid mobile number and the desired event types must be programmed.

SMS Details: Up to 10 mobile numbers can be programmed.

User Mobile: The mobile phone where all events will be sent.

Valid Areas:

This option permits the set up a different ARC for a different area. Select which area this particular ARC will be reporting. Selecting ABCD means the ARC will be receiving events from all areas.

Redials: If the alarm event has not been received by the monitoring station after the first number has been called the second number will be called. The 2 numbers will be alternated as many times as the redials is set to. If a call has been acknowledged by the monitoring station then the panel will stop calling.

Timeout: This is the time of how long it takes a call to timeout before it is not answered.

Test Calls:

The test call is used to show that the system is still alive when no activations have been made. Setting up a test call asks for start time in hours and minutes and the frequency of call in days, hours & minutes.

Event Types: Please see page: 41 for all event options. If 'Custom' is selected, all event types can be chosen.

User SMS Common Message:

This message will always be sent as part of the SMS activation text.

SMS Control Enable

The SMS control enables the user to control remotely the panel via SMS commands. This option allows the Engineer to enable and disable with SMS control functions that the end user can access. The options available are Arming, Disarming, and Arming with Inputs Bypassed, Bypassing Inputs, Checking the System Status, Triggering Outputs, Checking Output Status', Editing SMS Telephone Numbers, and Starting the Upload/Download software.

NOTE: Any text message command to the Enforcer will need to start with a valid user code.

NOTE: Text message commands are not case sensitive except when the user outputs have been activated with custom names.

NOTE: If a text message command is not recognised by Enforcer it will send a message back to the user notifying them of the incorrect command.

Arming the Enforcer via SMS text command		
Example SMS command send:	Description:	Example SMS command response:
123456 Arm A	123456 = User Code. Arm A = Will arm the Enforcer in Area A.	Final Arm; Area A
123456 Arm ABCD	123456 = User Code. Arm ABCD = Will arm the Enforcer in Area A, B, C and D.	Final Arm ; Area ABCD
NOTE: If no areas are specified then all areas will arm (default). The default will be Area A.		
Disarming the Enforcer via SMS text command		
Example SMS command send:	Description:	Example SMS command response:
123456 Disarm A	123456 = User Code. Disarm A = Will disarm Area A.	Disarm; Area A
123456 Disarm ABCD	123456 = User Code. Disarm ABCD = Will disarm the Area A, B, C and D.	Disarm ; Area ABCD
NOTE: If no areas are specified then all areas will disarm (default). The default will be Area A.		
Arming with inputs bypassed via SMS text command		

Example SMS command send:	Description:	Example SMS command response:
123456 Arm A Bypass 4	123456 = User Code. Arm A Bypass 4' = Arms Area A and will bypass input number 4.	Input Bypass; Area A Input 04 Forced Arm; Area A
123456 Arm A Bypass Kitchen	123456 = User Code. Arm A Bypass Kitchen= Arms Area A and will bypass the input that is called Kitchen.	Input Bypass; Area A Kitchen 04 Forced Arm; Area A
NOTE: Input numbers need to end with an apostrophe and an Input name needs to be inside quotation marks.		
Bypassing inputs via SMS text command		
Example SMS command send:	Description:	Example SMS command response:
123456 Bypass 6	123456 = User Code. Bypass 6 = Input number 6 will be bypassed on the next arming procedure.	Input Bypass; Area A Input 06
123456 Bypass Garage	123456 = User Code. Bypass Garage = The input called Garage will be bypassed on the next arming procedure.	Input Bypass; Area A Garage 06
NOTE: The name of the output has to be one word and spelled exactly as written in the panel. For example, Garage Door is not acceptable. It has to be written as Garage-Door in the panel and the respective command will be Garage-Door		
Checking the System Status via SMS text command		
Example SMS command send:	Description:	Example SMS command response:
123456 Status	123456 = User Code. Status	Area A Disarmed No Faults Area B Disarmed No Faults Area C Disarmed No Faults Area D Disarmed No Faults

Operating the User Automation Outputs via SMS text commands		
Example SMS command send:	Description:	Example SMS command response:
123456 Output 1 On	123456 = User Code. User Output 1 turns on.	OUTPUT 1 ON
123456 Output Garage-Door On	123456 = User Code output Garage-Door on = Turns output named as Garage-Door on.	OUTPUT Garage-Door ON
123456 Output Garage-Door Off	123456 = User Code output Garage-Door off = Turns output named as Garage-Door off.	OUTPUT Garage-Door OFF
NOTE: The user automation outputs can be also activated via the keypad or the keyfob. NOTE: The name of the output has to be one word and spelled exactly as written in the panel. For example, Garage Door is not acceptable. It has to be written as Garage-Door in the panel and the respective command will be Garage-Door.		
Checking the User Automation Outputs status via SMS text commands		
Example SMS command send:	Description:	Example SMS command response:
1234 Output 1 Status	123456 = User Code. User Output 1 status check.	OUTPUT ON or OUPUT OFF

123456 Output Garage-Door Status	123456 = User Code. Output Garage-Door status check.	OUTPUT Garage-Door ON or OUTPUT Garage-Door OFF
<p><i>NOTE: The name of the output has to be one word and spelled exactly as written in the panel. For example, Garage Door is not acceptable. It has to be written as Garage-Door in the panel and the respective command will be Garage-Door.</i></p>		
Editing an SMS telephone number via SMS text command		
Example SMS command send:	Description:	Example SMS command response:
123456 Change 07777888999 07878888999	123456 = User Code. Change number 07777888999 to number 07878888999	CHANGE 07878888999
Start Uploading/Downloading via SMS text command		
Example SMS command send:	Description:	Example SMS command response:
123456 UDL	123456 = User Code. UDL = The Enforcer will make an outgoing data connection to the programmed PC1 number.	No response as the panel is already connected to the PC1
9999 UDL	9999= Engineer Code UDL = The Enforcer will make an outgoing data connection to the programmed PC1 number.	NO Response as the panel is already connected to the PC1

5.15.5 Advanced Communications

Events can be sent to the PC software which can perform as an ARC -and receive Alarm, Fault, Open/Close and Access Control events.

Send Events UDL:

Events can be sent from the panel to up to 4 remote PCs running UDL software. This option allows the choice of which PC to send the events to.

Modem Telephone Number: Enter the telephone number to which the PC modem is connected.

Press **[A]** button to add any symbols: `,` = 2 second pause, `+` for roaming calls.

Send Alarms: If enabled, the panel will report 'alarm' events to the PC running UDL software.

Send Faults: If enabled, the panel will report any 'fault' events to the PC running UDL software.

Send Open / Close: If enabled, the panel will report 'open/close' (arm/disarm) events to the PC running UDL software.

Send Access Control: If enabled, the Enforcer 32-WE will report any 'access control' events to the PC running UDL software.

5.16 Alarm Responses?

The Alarm Response function controls how the system communicates when certain alarms are active. The different alarm responses are: Keypads, Internal Sounders, Bells Only and Signal Digi (communication to ARC or user). The different alarm responses work on a cycle (starting from 'Keypads' and finishing at 'Digi'). Each alarm response stage will take 15 seconds before moving on to the next response. For example, If the alarm response for Area A starts at 'Internal Sounders' and stops at 'Digi', then once Area A is armed and an alarm has been activated, the internal sounders will first activate, then after 15 seconds the Sirens will activate and then after another 15 seconds the 'Digi Modem' will activate (signal). The Enforcer 32-WE can operate on a combined area basis, for example if both areas 'A' and 'B' are armed; it may be desired to have the process of the alarm responses to change. Therefore the 'If areas armed' section would be used, the desired areas and the alarm responses selected. If A, B, C is entered for example, then A, B & C must be armed for the upgrade to take place. This option is a very useful when an outdoor perimeter area is created. It allows the creation of audible and communication alarms following different rules compared to other areas in the system.

5.16.1 Area A, B, C, D Starts at:

This feature programs where the Alarms for each area A, B, C or D start: Keypads, Internal Sounders, Bells Only or Signal Digi. If programmed as keypads then the alarm will start from

keypad sounders and then depending on where it's programmed to stop at -will progress up to a maximum of communicating the alarm event i.e. 'Digi'. Each alarm response will take 15 seconds before moving on to the next.

5.16.2 Area A, B, C, D Stops at:

Alarms for each area can stop at: Keypads, Internal Sounders, Bells Only and Signal Digi. For example, if programmed to start at keypad and stop at keypad this means the alarm will only be ever displayed on the keypad.

5.16.3 Fire Alarm Starts at:

This feature programs the starting point of alarm responses for fire alarm. The levels are: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.4 Fire Alarm Stops at:

This feature programs the ending point of alarm responses for fire alarm: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.5 Gas Alarm Starts at:

This feature programs the starting point of alarm responses for Gas alarm. The levels are: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.6 Gas Alarm Stops at:

This feature programs the ending point of alarm responses for Gas alarm: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.7 PA Alarm Starts at:

This feature programs the starting point of alarm responses for PA alarm. The levels are: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.8 PA Alarm Stops at:

This feature programs the ending point of alarm responses for PA alarm: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.9 24 Hour Alarm Starts at:

This feature programs the starting point of alarm responses for 24h alarm. The levels are: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.10 24 Hour Alarm Stops at:

This feature programs the ending point of alarm responses for 24h alarm: Keypads, Internal Sounders, Bells Only and Signal Digi.

5.16.11 Any Alarm Starts at:

This feature overrides the settings above. It can be used to create greater flexibility in the use of the alarm responses feature and in this case it's set up for each area if they are in armed status only.

5.16.12 If Areas Armed

Select the areas that the following settings will be applicable to.

5.16.13 Any Alarm Stops at:

For example, if 24 Hour Alarm is set to Start at Keypad and stops at Keypad, this feature allows set up for all Areas if they are armed to make any alarm stopping at Digi.

5.16.14 If Areas Armed

Select the areas that the above setting will be applicable to.

5.17 Options Up/Downloading?

NOTE: THE FUNCTIONS LISTED BELOW APPLY ONLY TO PSTN (DIGI-1200) – SEE SECTION 7 FOR OTHER CONNECTION METHODS

The Uploading/Downloading PC Software allows the servicing and monitor of the system and review of the logs.

Dial Mode Option

This function programs the procedure used for the call between PC and panel:

Auto Answer: When called from a PC the panel will answer the call immediately.

Dial Back: When called from PC the panel will take the line, disconnect and call the PC.

Panel Dials: Does not allow the PC to dial into the panel. A call has to be initiated by the user or engineer from the panel.

Dial In Options

Direct Dial: When the PC dials the panel, it will respond immediately.

AMC Dial (Shared Line): When the PC dials the panel, it will hang up after a designated number of rings, and dial again. The first call primes the panel, which will then answer the second call. The number of rings to prime the panel is entered in "Number of Rings before AMC" menu option.

Number of Rings before AMC: Enter the number of rings needed to prime the panel before answering the next call.

Prefix Telephone Number: The prefix is an extra digit required to reach the panel i.e. dial 9 to get an 'outside' line. This is the phone number of the PC modem where the UDL is installed for performing the automatic remote maintenance service. Press **A** button to add any symbols: `,' = 2 second pause, '+' for roaming calls.

Redials: The number of redials that it will call to the InSite software before it fails.

UDL Password: This password is used to identify the UDL connection. Make sure the password here and on the PC InSite software are the same.

Site Name: If a Site Name is entered, it must be also entered on the UDL software otherwise the connection will fail.

5.18 PC Connect Menu?

NOTE: THE FUNCTIONS LISTED BELOW APPLY ONLY TO PSTN (DIGI-1200)

The PC Connect Menu can be used by the engineer to make the panel dial to a remote PC where the UDL software is installed (rather than the PC dialling the control panel). This menu is also available from the Master Manager menu to enable them to activate a connection from user mode.

5.18.1 Select PC to Dial

Select PC 1 to 4. The telephone number of the PC modem/s (1 to 4) should be pre-programmed in 'Options Up / Downloading' menu.

Select PC to Dial ⇨ Select Operation

If the customer has not been created in UDL software it will take the data automatically from panel and create customer. If the customer has been created in the UDL the panel will connect to this customer database.

Test Call ⇨ Send test call to the ARC.

RM Service – Will force RM Service report for the last 6 months.

Data from PC, Data to PC – Up/Down loading info from/to UDL.

Diagnostics – Forces full panel diagnostic test and sends it to UDL setting new service date.

Commissioning – Just sets a date when the system is going to be used from.

NOTE: There is a shortcut to connect to 'PC number 1' from when the panel is in disarmed mode. To activate such a call from the keypad, press **A** followed by 5555. The display will not change but Enforcer 32-WE will dial the first PC programmed in 'Options Up / Downloading' automatically.

5.19 Software Revision?

This option shows the software version and hub version installed in the panel. Please obtain the software version number prior to contacting customer support so that the correct information can be given upon supporting the product.

5.20 Factory Default?

This option is used to reset the panel to a factory default.

5.20.1 Factory Default Code

Currently the system has 2 default settings. One is EN50131 default and the other default is not compliant to EN50131. The non EN default code is 2000 and the EN default code is 2002.

NOTE: Notice that the panel comes as defaulted to non EN50131 system and if used under the EN 50131 installation requirements MUST be defaulted to EN50131 by using the default code of 2002. Once applied the factory default code the system will be reset to factory defaults.

5.20.2 Clear WLS Data?

This option will give the installer the option not to clear wireless devices if they have been programmed on the system already.

5.20.3 Clear Codes?

This option will give the installer the option not to clear user codes if they have been programmed on the system already.

5.20.4 Clear Logs?

This option will give the installer the option not to clear memory logs if they have been programmed on the system already.

5.21 Exit Engineer Menu?

There are 2 ways to exit from engineer menu. One way is from this option and the other quick way is by pressing **[A]** from any other main menu.

6. Adding External Wired Keypad

The keypads have a small internal menu used mostly for addressing, changing key click volume and brightness of the LCD display.

Entering and Exiting the Keypad Menu

To enter the keypad menu, press and hold the **d** button until 'SECURITY CODE:' is displayed, and then enter '2000'. To exit, press the **[A]** key.

Keypad Menu Options

ADDRESS = Used to assign an address to a keypad [00] is the keypad on the panel

LANGUAGE = Allows you to assign a language –used for the keypad menu only

KEYPAD INPUTS READING = Shows the resistor reading / status on the 2 inputs located on the keypad

KEY-CLICK VOLUME = Sets the volume of the buttons

TAG VOLUME = Sets the volume when tag used

KEYPAD VOLUME = Sets the general volume of the keypad

ID TAG = Used to read the unique ID number of the Tag

RESET KEYPAD = Resets the keypad to factory settings

BACKLIGHT = Sets the backlight intensity of the keypad

DELAY FIRE AND PA BUTTONS = Sets how long the PA and Fire buttons have to be pressed for before an alarm is created

Testing The Keypad

With the system disarmed, press and hold the **[B]** key for 10 seconds at any keypad. This will cause all the LEDs on that keypad to illuminate and the LCD screen to scroll a display testing each pixel. The keypad will revert to normal display approximately 10 seconds after the **[B]** key is released.

7. Connecting to InSite Software

Enforcer 32-WE control panel can be programmed by the LCD menu or the UDL InSite Software provided free of charge. It can be downloaded from <http://www.pyronix.com/pyronix-downloads.php>. The connection between control panel and UDL software can be done in the following ways:

7.1.1 GPRS Connection (DIGI-GPRS)

On the Panel

- 1) Enter the Engineer Menu (code 9999)
- 2) Scroll the menu (button) until on "Options Up/Downloading" – Press
- 3) Choose 'Cloud' (option 6) in the "Download by" options - Press
- 4) Make a note of your System ID (to enter in the Insite Software later) Press
- 5) Select security type – for initial connections we recommend [0] (Standard) - Press
- 6) Create/enter a system password and take note of it - Press
- 7) Now on the 'Poll Server?' screen – select 'Yes' [1] and press
- 8) Now on the 'UDL Password' screen – **DO NOT USE** – leave blank and press
- 9) Now on the 'Site Name' screen – this is optional – if you enter a site name make sure you take a note of it for use later in the Insite software – or leave blank – then Press
- 10) Now on the 'UDL Priority' screen – we recommend setting this to 'High' [0] for initial Connections - Press
- 11) **IMPORTANT:** Make sure that the SIM card in use is enabled for GPRS data and that the correct APN settings have been entered for your network (see Network Setup – page 26).

On InSite UDL software from a PC

First of all once the software has opened, go to the 'configuration' tab and then select 'modem settings'. Look in the table at the top of the window that appears and on the entries has the serial mode listed as 'cloud' click on this line to select it and then click the 'load default string' button at the bottom of the window. Once this has been checked:

- 12) Click on 'UDL/ARC Otions' and select 'Force Dial customer'.
- 13) Select 'Cloud' in the 'Dial Mode' field.
- 14) Enter the 'System ID' of your Panel (See 'Options Up/Downloading' in the Engineer menu on panel) into the field titled 'Serial Number'.
- 15) Enter 'system password' (as entered in 'Options Up/Downloading' on the panel into the field titled 'System password'.
- 16) Leave the UDL security level at 'low' for initial connection test (in 'System UDL Security Level' field)
- 17) Enter the engineer code as used on the panel you are trying to connect.
- 18) Enter 'Site Name' as entered in panel ONLY if it was entered on the panel – otherwise, leave this blank.
- 19) In the 'Enter Customer In Database As' field – simply give the panel you are connecting to an appropriate name.
- 20) Click 'Dial'. If connection is successful, the Cloud Icon will become blue, a dialogue box will appear asking if you would like to create a customer – click 'yes' to continue.
- 21) The Enforcer 32-WE control panel is now successfully connected to the Insite UDL software.

7.1.2 Serial Connection (RS232)

The control panel is set up by the factory with RS232 port enabled as a method of connection to the UDL software.

NOTE: For this connection a special cable that is supplied by Pyronix is required -or it can be created according to the diagram on the right.

NOTE: If the PC does not have serial port, you may require a standard RS-232 to USB converter.

Unscrew and open the Enforcer casing, plug the RS-232 cable into the dedicated connector as shown on the image to the right.

On the Panel

- 1) Enter the Engineer menu (code 9999)
- 2) Scroll the menu (⏏ button) until the "Options Up/Downloading"
- 3) Choose RS-232 in the "Download by" option

On InSite UDL software from a PC

- 1) To setup the COM port associated to "modem" open the software, click on "Configuration", - choose "Modem Settings" and select "RS-232" option
- 2) Make sure that the serial COM used by UDL software is set the same as in Control Panel -> Device Manager -> Ports
- 3) Make sure that the UDL Graphic user interface RS-232 icon has turned green
- 4) Click on "Force Dial Customer"
- 5) Set "Dial Mode" field to "RS-232"
- 6) Enter the Engineer code in the "Engineer Code" field
- 7) Click on "dial"
- 8) If connection is successful, the RS-232 icon will become blue

NOTE: If a Site Name is set up on the panel the UDL Site Name must be the same otherwise the connection will not be possible.

7.1.3 Modem Connection (DIGI 1200, PSTN)

Make sure that the panel and the modem on the PC where UDL is installed are connected to a suitable PSTN line.

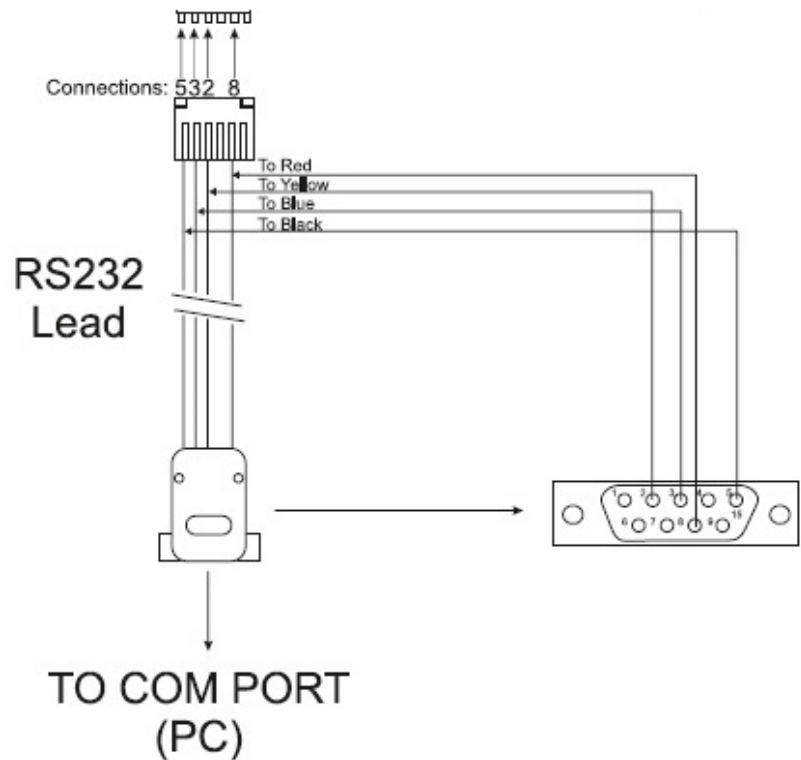
On the Panel

- 1) Enter the Engineer Menu (code 9999)
- 2) Scroll the menu (X button) until the "Options Up/Downloading"
- 3) Choose Modem in the "Download by" option

On InSite UDL software from a PC

- 1) To setup the COM port associated to "modem" open the software, click on "Configuration", choose "Modem Settings" and select "MODEM" option
- 2) Verify that COM port associated to "Modem" in the UDL software is set the same as in Control Panel -> Device Manager -> Ports
- 3) Verify that the modem Icon has turned green in the software Graphic User Interface
- 4) In the "Configurations" menu choose the "Modem Type" from the drop down menu. This is the modem connected to the PC and used to call the panel
- 5) Press "Load Default String" to program the right initialization string for the selected modem
- 6) Click on "Force Dial customer"
- 7) Set "Dial Mode" field to "MODEM"
- 8) Insert the telephone number in "Telephone Number" field
- 9) Enter the Engineer code in the "Engineer Code" field
- 10) Click on "dial"
- 11) If connection is successful, the modem Icon will become blue.

NOTE: If a Site Name is set up on the panel the UDL Site Name must be the same otherwise the



connection will not be possible.

The PSTN modem card (**DIGI-1200**) fits inside the Enforcer 32WE and is used for the following operations:

Send Alarms to the ARC: It is possible to send alarm events to the monitoring station via the Contact ID and SIA Level 1 and Level 3.

Programming the panel remotely via the telephone line: It is possible to program the Enforcer remotely via the telephone line. In order to be able to use this feature it is necessary that the telephone line used is an analogue conventional telephone line.

Receive Automatic Remote Service calls and alarms: It is possible to receive the RM service and alarm calls received by the UDL software installed on a PC and modem.

8. Options Programmable Only From PC

The Enforcer UDL software is available on www.pyronix.com/downloads. The software can be used to upload/download to the control panel and data can be viewed.

Two features that the UDL software incorporates are describe below:

- Auto Arm & Disarm Timer
- Logic Gates

Please refer to the UDL software help guides for help in the initial software set up first.

8.1 Auto Arm/Disarm Timers

This function will allow automatic arming and disarming procedures. This is useful when a premises is left unmanned for a period of time (due to holidays etc.).

Create a new customer, and select 'Enforcer'. The Auto-Arm/Logic Gates will be enabled, click the 'ok' button.

8.1.1 Adding Arm/Disarm actions

1. Select 'Add Action'.
2. Select the Day of the week to be 'Auto Armed'. This will then be displayed in the list.
3. Select the action of this timer (E.g. Arm)
4. Select the time (24 hour: E.g. 14:00) when the action should start.
5. Another action can now be added (E.g. Disarm) and select the time for this action.

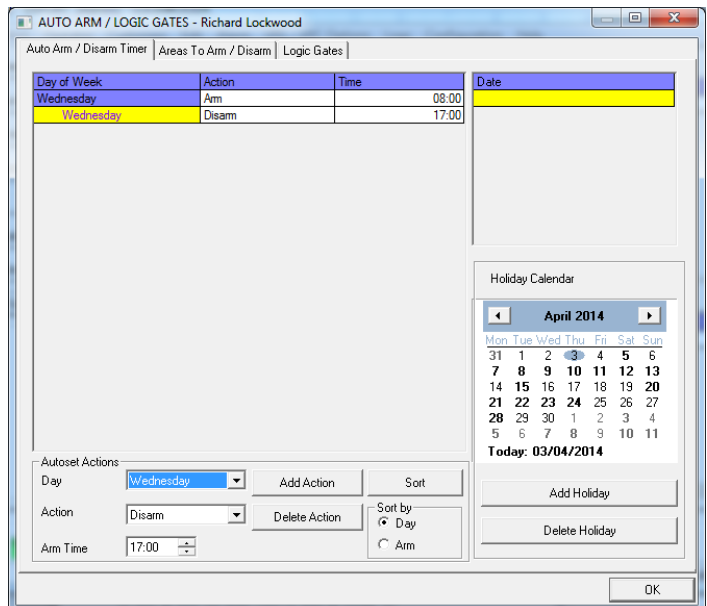
8.1.2 Adding 'Holidays'

A holiday setting will override any auto timers that coincide with the holiday. Once the holiday has passed, it will not repeat the year after or at any other time.

1. Click 'Add Holiday'
2. Select the dates that are required for the holiday period. These will be displayed at the top right of the screen under 'Date.'
3. If any holidays are added by mistake, select that holiday and click 'delete'.

NOTE: Make sure that any action already programmed matches correctly when the holiday period has finished.

E.g. If the dates January 1st, January 2nd, and January 3rd are selected, the panel will stay armed on all dates regardless of the auto timers. However, an auto timer should be set up to disarm the day after the holiday has ended if required.



8.2 Areas to Arm/Disarm

This section of the software selects the area's that will be Armed/Disarmed during the 'Auto Arm/Disarm' period.

1. Select the areas to be armed and type them in the 'Areas' field.
2. Select the 'Warning Period'. This is a time (in minutes) when the control panel will warn anyone

who may be in the premises that an auto arm is about to take place.

NOTE: The warning time is additional to the Auto-arm time. E.g. if the auto arm time is 22:00, a warning time of 15 minutes will added to this , so the actual panel arm time will become 22:15. If the panel must arm at 22:00, but a 15 minute warning time is also needed, the auto arm time should be selected as 21:45.

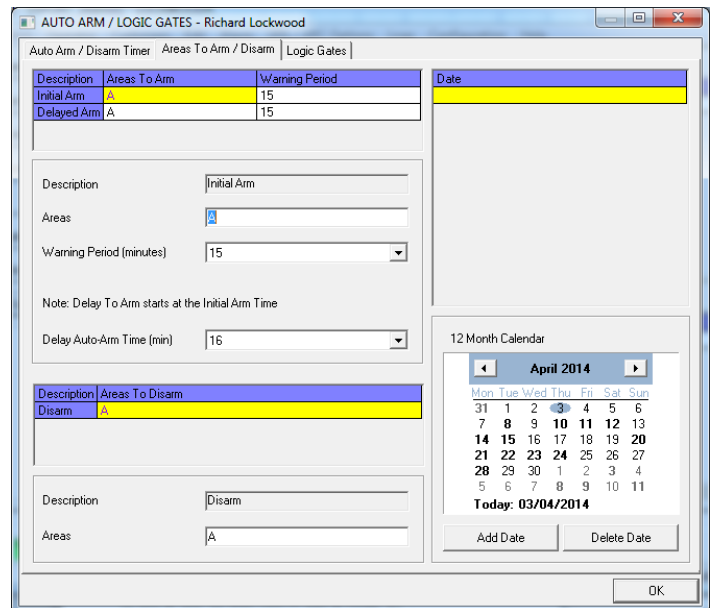
3. Select the 'Delay to Arm' time. This time is used if a person in the premises needs to delay the auto-timer. If a code is entered on the control panel during the warning period time, the auto timer can be delayed. E.g. If the warning period is set to 15 minutes, and the Delay Auto-Arm Time is set to 20 minutes. Then a user will have a further 5 minutes before the Auto-Arm begins.

NOTE: If a delay auto arm time is needed, it is recommended that his time is set to 1 minute more than the Warning period. The delay auto timer must always be set higher than the Warning Period.

4. Select the areas to disarm for the Auto-Disarms programmed previously. These are usually the same as the areas that have been selected to Arm.

5. The '12 month calendar' is used repetitive holidays that need to be repeated every year. For example this may be needed for national events, memorial days, birthdays etc.

Once all completed, exit the screen by clicking 'OK' and download the data to the control panel.



8.3 Programming Logic Gates

Logic Gates allow the use of 'logical operations' ('OR', 'AND' & 'NOT') to give greater control over how an output is activated. Rather than having an output activated following a 'burglary' alarm, it is possible to create an output that is activated, for example, when there is a 'burglary in area A' AND when area C is also armed.

This could be useful in a scenario where different offices are occupied in different areas, and do not require an external communicator or siren to signal an alarm in one area if other areas are still occupied.

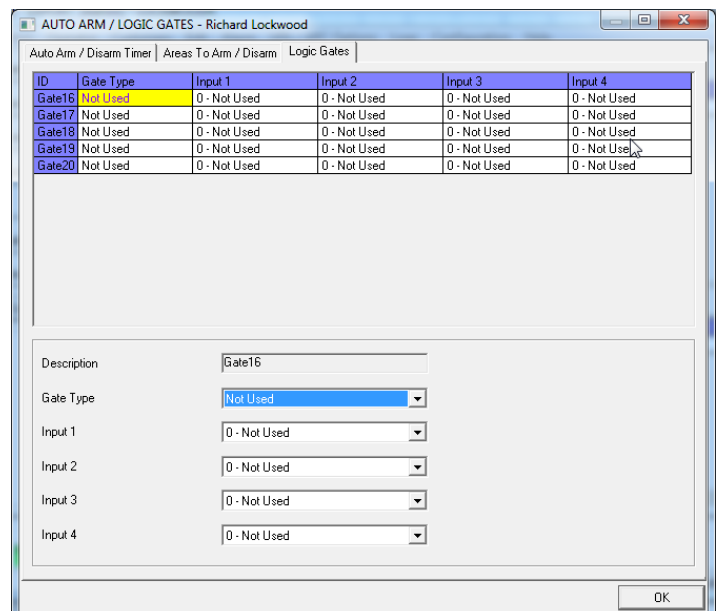
5 logic gates are available for programming. To program logic gates:

- 1.** Select the Logic Gates tab
- 2.** Select the gate type: 'AND', 'OR', 'NOT'
- 3.** Select the inputs (up to 4 can be selected). These are the input types of the control panel.
- 4.** Up to 5 logic gates can be programmed (Gates 16-20). These can only be programmed in the UDL software under 'Inputs/Outputs' button.

NOTE 1: Each gate can only be programmed with one 'logical operator'. For example, a gate can be programmed as A OR B OR C, but not A OR B AND C. If it is desirable to combine different logical operators, the logic gates will need to be split. Thus to obtain A **OR** B **AND** C the following logic can be used: Logic Gate 1 = A **OR** B; Logic Gate 2 = Logic Gate 1 **AND** C. The following example shows how to program the command:

{["Burglary Any" OR "Tamper Any"] AND "Ready C"}:

NOTE 2: Only Gates 16-20 can be programmed. Gates 1-15 are for future use



9. Faults and Troubleshooting

9.1 Device Fail / Active Faults

If a device on the Enforcer 32-WE system is not installed correctly or has been lost from the bus, a device fail will be present. An example of each fault is as follows:

- Failure on the panel = "Control Panel, Wireless Jamming Pnl"
- Keypad address 3 (1-3 available) failure = "Device 3, Device Fail Kpd"
- Tag Readers address 2 (1-3 available) failure = "Device 2, Device Fail Trd"
- Remote Input Expanders addresses 0 (0-4 available) = "RIX-00, Device Fail RIX"
- Remote Output Expanders address 0 = "ROX-00, Device Fail ROX"

If a 'location name' is entered for a device, the location will be displayed on the keypad instead of the address, for example instead of "Device 3" the Keypad will display "Entrance Corridor".

9.2 System Faults and Troubleshooting

9.2.1 Communications Faults

Fault	Description	Solution
MODEM FAULT	The panel is unable to see the Digi Modem	If the modem not present, ensure that "Disable Digi" option is set to 'YES' and "DOWNLOAD MODE" is set to 'NONE' or 'RS232'. If present, but not detected, check Digi Modem cable is connected correctly.
LINE FAULT	There is no telephone or GPRS line	a) Make sure to plug the PSTN modem into an analogue (conventional) telephone line. b) Make sure the SIM card is plugged in on the modem c) Make sure the GPRS signal is good enough.
CALL FAIL TO ARC	Call to the ARC has failed. NOTE This is a communication problem, which is rarely caused by an equipment fault. Is primarily related to the 'hand-shake' and 'kiss-off' frequency set up at the receiver.	Check ALL call details are programmed correctly. Ensure signalling format is correctly set for the ARC receiver.

9.2.2 RS485 Bus Problems

Fault	Description	Solution
DEVICE FAIL xxx xxx = ROX xxx = RIX xxx = Kpd xxx = Trd xxx = Pnl	Wired Device on the RS485 bus has been lost. Each Device is recognised by its own name such as: Output expander = ROX Input expander= RIX Keypad = Kpd Reader = Trd Control panel = Pnl	Identify device. Check the device is addressed correctly to match the programming. Check connections at the device, and the cabling to it. If the above are correct, re-boot the device, followed by a re-boot of the End Station.
485/COMMS LOST	Displayed on keypad that has not yet established communications with the control panel (End Station)	Part of the routine initialisation procedure. If this persists, check the display at other keypad(s) to confirm whether the device failure is at the keypad or complete system BUS failure. Temporarily install additional keypad.
Keypad display is BLANK	Keypad address does not match any keypad enabled in the panel.	Check the keypad address by pressing and holding [D] until the security code is required. Enter 2000 and set the keypad address. The Enforcer built in keypad address MUST always be set to [00]. Make sure that in the "Install Keypads and Readers" menu in Engineer mode -the keypad address set up correctly.

KEYS LOCKED OUT	a) More than one device connected at the same address. b) Too many incorrect key presses have been entered to creating 'Code Guessing' condition.	a) Correct addressing so that there are no overlaps. Then power the system down and back up again to correctly reinitialise. b) Wait 90 seconds for the keypad to be re-introduced onto the system.
-----------------	--	--

9.2.3 Detection Faults

Fault	Description	Solution
CASE TAMPER	Case tamper switch open	Ensure the switch is closed
Code Guessing	Up to 13 Invalid key presses have been entered or 3 invalid tags have been presented.	Press the x key to clear.

9.2.4 Power Supply Problems

Fault	Description	Solution
BATTERY FAULT xxx	Battery not present or Battery volts low	Note: This indication should be expected during recharge -after a mains failure.
BAT LOAD FAIL	Battery Load Test has failed	Only displays if option selected. Battery uncharged or capacity below specification – then it may need replacing.
BAT CRITICAL	Battery being disconnected	Protects the battery from deep discharge damage during extended mains failure. Note: The system is about to be powered down!
MAINS FAIL xxx	Mains supply failed	System detects that the mains frequency is out of specification, as well as voltage. Note: 'AC FAIL' timer operative
LOW VOLTS xxx	Power supply volts low	Battery volts below normal 'battery fault' level during a mains failure

9.2.5 Engineer Indications

Fault	Description	Solution
Engineer Access Denied	Access to Engineer menu NOT possible, as system is not fully disarmed.	Ensure that ALL areas are disarmed, using suitable user codes / tags at the appropriate keypads / readers.
Check Failed Input xxx	Input in fault on attempting to exit Engineer mode.	Applies to 24-hour tamper, or other input types that would generate an alarm condition if the system were returned to disarmed mode. This also applies to tamper faults on other input types. Check for the fault on input, or omit it in programming.
Error input Areas not accessible	An input has been programmed to an area for which no arming point is valid to disarm.	It would therefore be impossible to fully disarm the system after a tamper alarm on that input. Programming must be adjusted before exiting Engineer mode.
Error some Areas cannot be disarmed	Arming points have been programmed so it's possible to arm an area, but not disarm it.	Programming must be adjusted before exiting Engineer mode.

9.2.6 Wireless Faults

Fault	Description	Solution
U-01 (xx) WLs LOW BATT	Low battery on wireless keyfob (user) number 'xx'	Replace the battery on the keyfob mentioned
I-01 (xx) WLs LOW BATT	Low battery on wireless input number 'xx'	Replace the battery on the input device mentioned
B-01 (xx) WLs LOW BATT	Low battery on wireless bell number 'xx'	Replace the battery on the radio bell mentioned

I-01 (xx) WLs SUPERVN	Device on wireless input number 'xx' has not 'checked in'	Perform a walk test on the detector, and a diagnostic signal strength test and then try replacing the battery
B-01 (xx) WLs SUPERVN	Wireless bell number 'xx' has not 'checked in' within 20 minutes time	Test the siren, perform wireless signal strength diagnostic. Consider replacing the battery or relocating the siren.
- 01 (xx) CASE TAMPER	Tamper fault on input number 01 'xx' = any input number	Check the tamper switch on the detector and make sure the case is closed properly.
WLs TAMPER Bxx	Tamper fault on wireless bell number 'xx'	Check the tamper switch on the radio bell mentioned.
WLs JAMMING Pnl	Jamming fault on Enforcer 32-WE	Check no radio interference is in close proximity to the radio devices/panel.
WLs Supervn Fault	No 'supervision polls' were received for 20 minutes before the arming operation. Wireless Input or Bell input number will be shown so the problem is easily identified	Test the signal strength / battery on each of the wireless devices.
WLs Input / Input Type Mismatch	Wireless devices are learned on inputs but no input types have been programmed for them.	Program input type for each of the wireless devices learned in the PROGRAM INPUTS.

9.2.7 Errors When Arming

Fault	Description	Solution
Please leave via exit door	If the exit mode is programmed as Final Door, then the premises must be left through this door for the system to be armed.	Leave via the agreed exit route.
Exit Via...	If any follow detectors or door contacts are open during the arming procedure, a prompt will be displayed to close them.	Close all inputs.
Unable To Arm	A fault condition exists on the system. Details of the fault will scroll on the display.	Correct the problem if it is an input which is open, or call an engineer.
Alarm during the arming	Fail to arm time has been exceeded.	Leave the premises within the fail to arm time, increase the fail to arm time in 'timers' or disable this feature in system options.
Alarm during the arming procedure	Instant inputs have been activated.	During the arming procedure do not activate 'instant inputs'.

10. Event Types

	Custom	Default 1	Default 2	Default 3
Arm	x / ✓	✓	x	x
Disarm	x / ✓	✓	x	x
Special Arm/Dis	x / ✓	x	x	x
Sub Area/Sh.	x / ✓	✓	x	x
Sub Area/Sh.	x / ✓	✓	x	x
Burglary Alarm	x / Alarm Once /	Alarm All	Alarm All	Alarm All
Burglary	x / ✓	✓	✓	x
Fire	x / ✓	✓	✓	✓
Fire Restore	x / ✓	✓	✓	x
PA Alarm	x / ✓	✓	✓	✓
PA Restore	x / ✓	✓	✓	x
Medical	x / ✓	✓	✓	✓
Medical Restore	x / ✓	✓	✓	x
S-Area	x / ✓	✓	✓	x
Tamper	x / Tamper Once /	Tamper All	Tamper All	Tamper All
Tamper Restore	x / ✓	✓	✓	x
Bypass	x / ✓	✓	✓	✓
Bypass Restore	x / ✓	✓	✓	x
Technical	x / ✓	✓	✓	✓
Technical	x / ✓	✓	✓	x
AC	x / ✓	✓	✓	✓
Wireless Faults	x / ✓	✓	✓	✓
Telecom Status	x / ✓	x	x	x
Access Control	x / ✓	✓	x	x
Mask / Restore	x / ✓	✓	✓	✓
Special Log	x / ✓	x	x	x
Alarm Silenced	x / ✓	x	x	x
Tech Alarm	x / ✓	x	x	x
Information	x / ✓	x	x	x

11. EN 50131 Terminology

Enforcer 32-WE Language	EN50131 Language
ARM	Set
Disarm	Unset
Day or Disarmed Mode	Unset State (may be relevant to a specific area)
Personal Attack (PA)	Hold Up (HU)
Bypass	Inhibit
Unused	Isolated
Bell / External Sounder / SAB	External Warning Device (self-powered is assumed)
Internal Sounder / Speaker	Device combining internal warning device with audible indicator (using different tones and volumes)
Prox card, Tag, or wireless keyfob	Digital Key

12. Access Levels

- Level 1:** Access by any person; for example the general public.
- Level 2:** User access by an operator; for example customers (systems users).
- Level 3:** User access by an engineer; for example an alarm company professional.
- Level 4:** User access by the manufacturer of the equipment.

13. Factory Defaults

ENGINEER MENU	MENU	DEFAULTS
DATE & TIME	Year (00-99)	[07]
	Month (1-12)	[01]
	Day (1-31)	[11]
	Hours (0-23)	[00]
	Minutes (0-59)	[01]
	Summer Time Adjust	No [0]
LEARN WIRELESS DEVICES	Inputs 1 - 32	Available
	Bells 1 - 2	Available
PROGRAM INPUTS	Inputs 1 - 66	Unused
	Input In Area	A
	Common Input	No [0]
	Input Attributes	
	Chime	No [0]
	Allow Bypass	Yes [1]
	Double Knock	No [0]
	Combined Input	No [0]
	Normally Open	No [0]
	Mask Test	No [0]
	Non Activity Input	No [0]
	Special Log	No [0]
	Enter number	Input #
	Enter Location	—
INSTALL RIXs	RIX Address	[0]
	RIX Installed	No [0]
PROGRAM OUTPUTS	Endstation PGMs	
	BELL PGM	Bell Any [0014]
	STB PGM	Strobe Any [0016]
	PGM	Not Used [0000]
	PGM 1 - 4	Not Used [0000]
	ROX Module PGMs	
	ROX Installed	No [0]
	Keypad PGMs	
	PGM 1	Not Used [0000]
	Reader PGMs	
	PGM 1 - 2	Not Used [0000]
	User Outputs	
	User Output No	[01]
	User Output Type	Latched [0]
Output Name	—	
INSTALL KEYPADS/READERS	Device Address	[0]
	Device Type	Keypad
	Device Arms Area	[ABCD]
	Device Disarms	[ABCD]
	Device In Area	[ABCD]
	Device Name?	Device 0
	Enter Location	—
PROGRAM TIMERS	Entry Time 1	[030]
	Entry Time 2	[030]
	Exit Time	[020]
	Bell Time	[03]
	Bell Delay	[00]
	Strobe Time	[00]
	Number Re-Arms	[3]

	AC Fail Delay	[005]
	Final Door Delay	[005]
	Double Knock	[10]
	Delay Send Entry	[000]
	Line Fault Delay	[250]
	Arm Fail Time	[250]
	Guard Code Delay	[03]
	Fire Bell Time	[04]
	Arm Fail Warning	[00]
	NAT Day Timer	[00]
	NAT Hours Timer	[00]
	Pulsed Burglar Any	[005]
	Wireless Supervision Time	[02]
	Wireless Jamming Time	[100]
	Service Timer	[000]
CHANGE CODES	Change Duress Codes	1-10 Empty
	Change Master Manager Code	1234
	User In Area	[ABCD]
	User Arm Options	Disarm/Arm [0]
	Area Arm Choice	Yes [1]
	User Name	—
	Change Engineer Code	9999
VOLUME CONTROL	Entry	[4]
	Exit	[4]
	Alarm	[7]
	Fire	[7]
	Technical	[4]
	24 Hour	[4]
	Chime	[4]
	Code Stops Sound	Yes [1]
	Silent Tech Alert	No [0]
	Main Sounder All	No [0]
	Disable Call Fault	No [0]
SYSTEM OPTIONS	<i>Options</i>	
	Arm with Tamper	Yes [1]
	Arm if Modem Flt	Yes [1]
	Arm with Tec/Flt	Yes [1]
	Arm Fail = Alarm	No [0]
	Do Bat Load Test	No [0]
	Arm Acknowledge	Strobe Flash [1]
	Bypass on ReArm	No [0]
	Forced Arm	No [0]
	Tag Only Disarm	No [0]
	Quick Arm	No [0]
	Keypad PA Key	Bell+Signal [2]
	Manager Prog PA	Yes [1]
	Tag Disarm+Door	Yes [1]
	Keypad Fire Key	Yes [1]
	Arm with Spvn Flt	Yes [1]
	Keyfob on Entry	No [0]
	6 Digit Codes	No [0]
	<i>System Displays</i>	
	Area A,B,C,D Text	—
	Full Area Text	All Areas Armed
	Top Display Text	Enforcer 32WE
	Site Name	—

	Display If Armed	Yes [1]
	Display Alarms	Yes [1]
	Ready LED On	Yes [1]
	Display PAs	Yes [1]
	Display Silent PAs	Yes [1]
	Display Inputs	Yes [1]
	Disarm LED On	Yes [1]
	<i>Exit Options</i>	
	Exit Mode ABCD	Timed [0]
REVIEW LOGS	Panel Log	
	Access Control Log	
ENGINEER TESTS	Walk Test Areas	[ABCD]
	Soak Test	
	Soak Inputs	[--]
	Soak Days Left	[00]
	Initial Soak	[00]
	Bell Test	
	Battery Load Test	
	Test PGMs	
	Send Test Call	
	By-pass Fire PA	No [0]
DIAGNOSTICS	<i>Wireless Devices</i>	
	<i>Wired Devices</i>	
	<i>Communications</i>	
ENGINEER RESTORE OPTIONS	Restore Burglary	No [0]
	Restore PA	No [0]
	Restore Tamper	No [0]
	Restore Soak	No [0]
	Restore Faults	No [0]
	AntiCode Restore	No [0]
COMMUNICATIONS	<i>App Set Up</i>	
	Enable App	No [0]
	System ID	#####
	Cloud Password	—
	Security	Standard [0]
	App Password	—
	Poll Server	No [0]
	<i>Network Set Up</i>	
	Program GPRS	
	Program LAN	
	Program Wi-Fi	
	<i>ARC Signalling</i>	
	ARC Details	[1]
	Format	Not Used [254]
	Valid Areas	[A]
	Area ARC Account	No [0]
	One ARC Account	—
	Redials	[03]
	Time Out	[60]
	Test Calls	No [0]
	Event Types	Default 1 [0]
	Register To ARC?	
	<i>User SMS Signalling</i>	
	SMS Details	[1]
	User Mobile	—
	Valid Areas	[A]

	Redials	[09]
	Time Out	[99]
	Test Calls	No [0]
	Event Types	Default 1 [0]
	User SMS Common Message	Alarm System
	SMS Control Enable	
	SMS Arm	Yes [1]
	SMS Disarm	Yes [1]
	SMS Status	Yes [1]
	SMS Output	Yes [1]
	SMS No. Change	Yes [1]
	SMS Start UDL	Yes [1]
	Advanced Communications	
	Send Event UDL	[1]
	Modem Tel No	
	Send Alarms	No [0]
	Send Faults	No [0]
	Send Open/Close	No [0]
	Send Access/Ctrl	No [0]
ALARM RESPONSE	Area,Fire,Gas,PA,24 Hour Starts At	Signal Digi [3]
	Area,Fire,Gas,PA,24 Hour Stop At	Signal Digi [3]
OPTIONS UP/DOWNLOADING	Download by	RS-232 [2]
	Dial Mode Option	Auto-Answer [0]
	Dial In Options	Direct Dial [0]
	Number of Rings	Before AMC [05]
	Prefix Tel No	_
	Redials	[03]
	UDL Password	_
	Site Name	_
	UDL Priority	High [0]
PC CONNECT MENU	Select PC to dial	[1]
	Select Operation	Connect to PC [0]

14. Event Types (SIA and Contact ID codes)

Event	SIA code	CID code	Event Type Number	Default 1 (ARC) Full Reporting	Default 2 (ARC) No Arm/Disarm	Default 3 (ARC) No Arm/Disarm and Alarm Restorals	Default (SMS)
ARM							
Auto Arm	CA	3403	1	on			
Forced Arm	CF	3401	1				
Arm	CL	3401	1				
DISARM							
Disarm	OP	1401	2	on			
Auto Disarm	OA	1403	2				
(Special Arm/Disarm) ARM/DISARM WITH CODES 15 to 25							
Special Disarm	OP	1401	3				on
Special Arm	CL	3401	3				
SUBAREA / SHUNT ARM/DISARM							
Sub-Area Arm	CG	3402	4	on			
Shunt Closed		1402	4				
Sub-Area Disarm	OG	1402	5				
Shunt Opened		3402	5				
BURGLARY ALARM							
Burglary Alarm	BA	1130	7	all	all	all	once
Gas Alarm	GA	1151	7				
Entry/Exit alarm	BA	1134	7				
No Zone Activity - Sent	NA	1680	7				
24h Alarm	BA	1133	7				
Perimeter Alarm	BA	1131	7				
Keybox/Guard Zone Alarm		1250	7				
Flood Alarm	WA	1154	7				
Interior Alarm	BA	1132	7				
BURGLARY RESTORE							
Burglary Restore	BH	3130	9	all	all		
Gas Restore	GH	3151	9				
Entry/Exit Restore	BH	3134	9				
Day alarm restore	BH	3133	9				
Interior Alarm Restore	BH	3132	9				
Perimeter Restore	BH	3131	9				
Keybox Restore		3250	9				
Flood Alarm Restore	WH	3154	9				
Ward Alarm Restore	BH	3130	9				
FIRE ALARM							
Fire Alarm	FA	1110	10	on	on	on	on
Fire key pressed	FA	1110	10				
FIRE ALARM RESTORE							

Fire Alarm Restore	FH	3110	11	on	on		
Fire key Restore	FH	3110	11				
PA ALARM							
Duress Code	HA	1121	12	on	on	on	on
Keypad PA	PA	1120	12				
Radio fob PA	PA	1120	12				
PA Alarm	PA	1120	12				
Silent PA	HA	1122	12				
PA ALARM RESTORE							
PA Restore	PH	3120	13	on	on		
Silent PA Restore	HH	3122	13				
Keypad PA Restore	PR	3120	13				
MEDICAL ALARM							
Medical Alarm	MA	1100	14	on	on	on	on
MEDICAL RESTORE							
Medical Alarm Restore	MH	3100	15	on	on		
SUB-AREA ALARM/RESTOR							
Ward Alarm	BA	1130	16	on			
TAMPER ALARM							
Invalid Tag	JA	1461	17	all	all	all	
RS485 Fault	IA	1300	17				
Device Fail	ET	1333	17				
Tamper Alarm	TA	1137	17				
Tamper On Zone	TA	1144	17				
Code Guessing	JA	1461	17				
Case Tamper	TA	1137	17				
Siren Case Tamper	TA	1321	17				
Radio Tamper	TA	1337	17				
TAMPER RESTORE							
Tamper (Wired/Wireless) Restore	TH	3137	18	all	all		
Tamper On Zone Restore	TH	3144	18				
Case Tamper Restore	TR	3137	18				
Siren Case Tamper Restore	YH	3321	18				
BYPASS							
Zone Bypassed	BB	1570	19	on	on	on	
Zone Force (Bypassed) Armed		1570	19				
Fire Zone Bypassed	FB	1571	19				
24h Alarm Zone Bypassed	BB	1572	19				
RESTORE OF BYPASS							
Fire Zone Bypass Restore	FU	3571	20	on	on		
24h Alarm Zone Bypass Restore	BU	3572	20				
Zone Bypass Restore	BU	3570	20				
TECHNICAL							

Low Volts	AT	1302	21	on	on	on	
Battery Disconnect	YT	1311	21				
Battery Load Fail	YT	1309	21				
Fuse 1	IA	1300	21				
Fuse 2	IA	1300	21				
Fuse 3	IA	1300	21				
Fuse 4	IA	1300	21				
Fuse 5	IA	1300	21				
Fuse 6	IA	1300	21				
Fuse 7	IA	1300	21				
Fuse 8	IA	1300	21				
Battery Critical	YT	1302	21				
Wired Siren Fault	YA	1320	21				
TECHNICAL RESTORE							
Battery Connect	YR	3311	22	on	on		
Device Restored	ER	3333	22				
Fuse fail restore	IR	3300	22				
Detector Fault Restore	BJ	3324	22				
Wired Siren Fault Restore	YH	3320	22				
AC MAINS MISSING/RESTORE							
Mains Fail Fault	AT	1301	23	on	on	on	on
Restore of Mains Fault	AR	3301	23				
WIRELESS ALARM/RESTORE							
Radio low battery	XT	1384	24	on	on	on	
Radio supervision failure	UY	1381	24				
Radio hub jamming	XQ	1344	24				
Radio hub jam restore	XH	3344	24				
Radio Jamming restore	XH	3344	24				
Radio Supervision restore.	UJ	3381	24				
Radio low battery restore	XR	3384	24				
TELECOM STATUS							
Modem Failed		1330	25				
Modem Communication Fail		1350	25				
Input Line Fail	LT	1351	25				
Telecom Line Fault	LT	1351	25				
Input Line Restored	LR	3351	25				
Telecom Line Restored	LR	3351	25				
ACCESS CONTROL							
Door Left Open	DL	1426	26	on			
Door Forced	DF		26				
MASK ALARM/RESTORE							
Detector Masked	BT	1324	27	on	on	on	
Detector Masked Restore	BJ	3324	27				

SPECIAL LOG							
Zone Special Log Opened	UA	1146	28				
Zone Special Log Closed	UR	3146	28				
Zone Special Log Switcher Opened	UA	1146	28				
Zone Special Log Switcher Closed	UR	3146	28				
ALARM SILENCED							
Alarm Silenced	OR	1406	29		on		
Sub-Area Alarm Silenced	OG	1402	29				
TECHNICAL ALARM SILENCED							
Technical Alarm Silenced	OR	1406	30				
Technical Alarm in Sub-Area Silenced	OG	1402	30				
INFORMATION							
Engineer Access	LB	1627	31				
Engineer Exit	LX	1628	31				
System Restart		1305	31				
Logs Cleared		1621	31				
Engineer Reset	RN	3313	31				
Clean Started		1305	31				
Site Changed	YG	1306	31				
Logs nearly full		1623	31				
Input Walk Tested		1607	31				



Secure Holdings
Secure House
Braithwell Way
Hellaby
Rotherham
S66 8QY

Customer Support line (UK Only):
+44(0)845 6434 999 (local rate) or
+44(0)1709 535225

Hours: 8:00am - 6:30pm, Monday to Friday
Email: customer.support@pyronix.com
Website: www.pyronix.com

