



Enforcer 64

User Guide



Date: 26 February 2018
Document ID: 102017855 -V01

Copyright

Copyright © 2018 Pyronix All Rights Reserved.

Contains information owned by Pyronix and/or its affiliates. Do not copy, store, transmit or disclose to any third party without prior written permission from Pyronix.

Other product and company names may be trademarks or registered trademarks of other companies, and are the property of their owners. They are used only for explanation, without intent to infringe.

Intended purpose

This document provides information about using and managing the product after installation and commissioning.

Conventions

This document uses the following conventions:

▶ For more information...	A cross-reference to a related or more detailed topic.
---------------------------	--



Indicates a hazardous situation which, if not avoided, could result in death or serious injury.



Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.



Indicates an important situation which, if not avoided, may seriously impair operations.



Additional information relating to the current section.


Contact

Pyronix Ltd,
Secure House,
Braithwell Way,
Hellaby,
Rotherham,
S66 8QY,
UK

www.pyronix.com

Contents

Contents	iii
System Description	5
Introduction	5
HomeControl+ App	6
Operation	7
Getting Started	7
Operating the Panel	7
Arming the System	8
Disarming the System	9
Using the Keyfob	10
Locking the Keyfob	11
Quick Arming	11
Arming and Disarming with the Tag Reader	11
Access Control	12
Special Disarm Users	12
PyronixCloud	13
Setting up PyronixCloud on the Panel	13
Setting up the PyronixCloud	13
Setting Up The HomeControl+ App	14
HomeControl+ App Icons	17
Configuration	18
Chime Feature	18
PA from Keypad	18
Fire Alarm from Keypad	18
Master Manager Menu Options	19
Entering the Master Manager Menu	20
Bypass Inputs	20
Operate User Automation Outputs	21
Date & Time	22
Change Codes	23
User Codes	23
Proximity Tags	24
Keyfobs	25
Review Log	26
Setup App Data	27
Standard Security	27
High Security	28
SMS Phonebook	29
Walk Test	30
Bell Test	30
Allow Engineer Menu	31
Block Remote Arming	31
Block UDL	32
System Sounds Demo	32
Exit Master Manager Menu	33
Reference	34
Handover Form	34
SMS Commands	34



Inputs	36
Outputs	37
Users	38
Compliance	39
Notes	40

System Description

Introduction

The Enforcer is a wireless alarm system that has been designed with your security in mind; with quick and easy installation and minimal maintenance, the Enforcer protects your home with a multitude of unique features.

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

The Enforcer two-way wireless devices are fully operational when the system is armed. This makes your 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 your security.

The Enforcer has been engineered by Pyronix as a secure, reliable and easy to use wireless alarm system.

Battery Monitoring/Saving

Advanced technology preserves the battery life of each wireless device. The Enforcer panel also informs you in advance of when a battery needs replacing, giving you enough time to change the battery in the specific device before it stops working. This key feature keeps your environment fully protected, unlike other conventional systems.

High Security Encryption

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

User Friendly Keyfobs

The two-way wireless keyfob allows you to see the status of your Enforcer via three colour LEDs:

- System armed: A RED LED will illuminate.
- System disarmed: A GREEN LED will illuminate.
- System fault: An AMBER LED will illuminate (this will flash when the keyfob is unable to arm the system).
- Alarm activated: A flashing RED LED.

It is possible to allocate different functions to each keyfob, such as: arming or disarming different areas, activating outputs to control external devices (such as: gates), requesting the system status and activating PA (panic alarms).

Up to 32 wireless keyfobs can be added to your Enforcer. Each wireless keyfob has a unique ID, which can be reported to the ARC and HomeControl+ App. These are stored in the event log of the Enforcer individually.

User Automation Outputs

The Enforcer gives you the option to operate devices (such as: gates, lights, sprinklers,) via your keypad or remotely via your keyfob or HomeControl+ App.

HomeControl+ App and SMS notifications

Your Enforcer will provide you with real-time push notifications on your smart device or within the HomeControl+ App, such as: that your child has returned home from school, or a leakage of water in

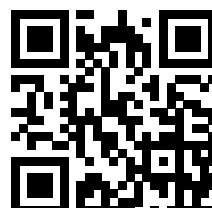
your property. You can also opt to receive these via SMS text messages, when a GPRS modem is connected to the panel.

HomeControl+ App

The Enforcer system can be remotely controlled using the HomeControl+ App. It allows you to arm and disarm the Enforcer, check the system status and bypass inputs. It also allows you to activate devices remotely, such as gates, lights, sprinklers and more. The HomeControl+ App and PyronixCloud communication is fully encrypted to the highest standard and no sensitive user data is stored on the PyronixCloud.



The HomeControl+ App is available in two versions: Android from Google Play Store and iOS from Apple store.













Operation

Getting Started

Operating the Panel

There are four different methods that can be used in arming or disarming your alarm: using a keypad, using a proximity tag, a keyfob or the HomeControl+ App on your smart device.

Table 1 - Button Operations

Button	Description
	Quickly exit a menu. Select Area A. Change case when entering text.
	Move back to the previous main menu item. Select Area B.
	Move back to the previous option in a sub-menu. Select Area C. Display additional information in the log. Delete letters or numbers when entering text. Enables chime feature.
	Scroll forwards in the log. Select Area D. Access the user menu. Press and hold to configure the keypad.
	Trigger PA (Panic Alarms) - only if enabled by an engineer.
	Trigger fire alarms - only if enabled by an engineer.
	Move from one option to another while in a sub-menu. Move through text.
	Select items and enter into a sub-menu or option.
	Enter a space when entering text.
	Scroll forwards in the main menu and sub-menus. When you have scrolled through all the options in a menu, returns to the previous menu level.

The Master Manager Menu allows you to setup specific features by asking you a series of setup questions:

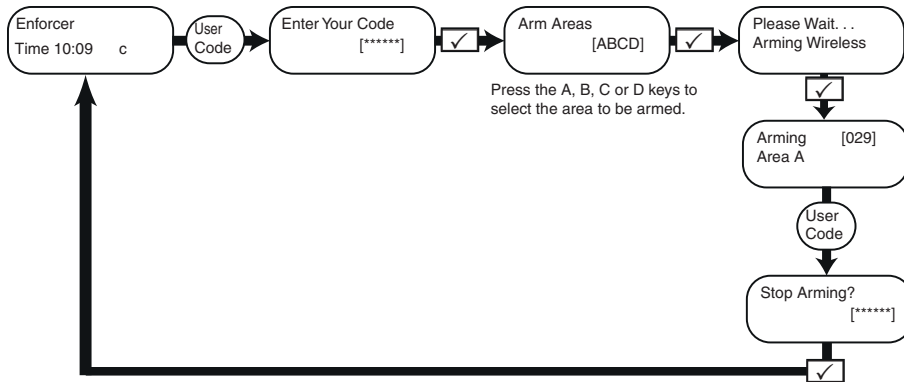
- Main menus are in capital letters and finish with a question mark, for example, **LEARN USER CODES KEYFOBS & TAGS?**.
- Sub-menus are in lower case letters and finish with a question mark, for example, **User Codes/Tags/Learn Keyfobs?**.
- Programmable options are in lower case letters and do not finish with a question mark, but instead: **Yes/No**, or other options, such as **User / Manager**.
- To navigate through the menu system, answer the questions in the main and sub-menus.

For example, if the question is: **LEARN USER CODES KEYFOBS & TAGS?**, pressing will take you into the sub-menu **User Codes/Tags/Learn Keyfobs?**, and pressing again will then take you into the programmable options of this sub-menu. If at this point you press , you will be taken out of the individual option. Continue to press and you will navigate through the sub-menus and eventually return to the main menu.

Arming the System

There are four ways that you can arm your system.

1. Enter your User Code on the keypad. The User Code needs to be programmed in the Master Menu.

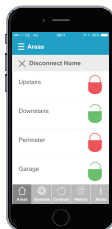


2. Present your tag and deselect any areas that are not to be armed, then press the button.




*Options 1 & 2 only function if 'Arm Area Choice' is selected as 'Yes' in the **Learn User Codes/Tags/Keyfobs?** menu. If selected as 'No', then all areas allocated to your user will arm.*

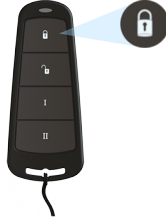
3. Open the HomeControl+ App on your smart device and sign into your system with your User Code and password details. Then touch the green (disarmed) padlock icons to turn them to red padlock icons and arm those areas.





For more information, contact your installer.

4. Press  and then release, the keyfob will arm the areas it has been assigned to by your installer. A red LED light will illuminate when the system is armed.

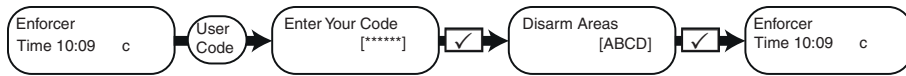


The keyfob buttons can be programmed in the Master Manager Menu **Learn User Codes/Tags/Keyfobs**.


Disarming the System

There are four ways that you can disarm your system.

1. Enter your User Code on the keypad. The User Code needs to be programmed in the Master Menu.



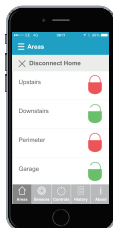
Press the A, B, C or D keys to select the area to be armed.

2. Present your tag and select any areas that are to be disarmed, then press the  button.




Options 1 & 2 only function if 'Arm Area Choice' is selected as 'Yes' in the **Learn User Codes/Tags/Keyfobs?** menu. If selected as 'No', then all areas allocated to your user will disarm.


- Open the HomeControl+ App on your smart device and sign into your system with your User Code and password details. Then touch the red (armed) padlock icons to turn them to green padlock icons and disarm those areas.



 For more information, contact your installer.



- Press  and then release, the keyfob will disarm the areas it has been assigned to by your installer. A green LED light will illuminate to indicate the system is disarmed.



 The keyfob buttons can be programmed in the Master Manager Menu **Learn User Codes/Tags/Keyfobs**.

Using the Keyfob



The wireless keyfob has four buttons that can be programmed to specific functions: no action, show status, arm area, disarm area, latch output, timed output and PA alarm activation. This can be customised to operate as desired (programmed in the function **Change Code**).

Button	Default configuration
	Programmed for 'Arm Area': one or more areas will be armed when pressed.
	Programmed for 'Disarm Area': one or more areas will be disarmed when pressed.

Button	Default configuration
I	Programmed for 'Status LED'. This displays the system status when pressed: <ul style="list-style-type: none"> • RED: Armed • GREEN: Disarmed • AMBER: Fault
II	No action.

Locking the Keyfob

All four buttons on the keyfob can be 'locked' to prevent you from accidentally pressing them.

To do this, press the two central keys together ( & I) or the two outer keys together ( & II).

A RED LED will flash to indicate that the fob has been locked. To unlock the keyfob press the same two keys together again and a GREEN LED will flash to indicate that it is now unlocked. Please note that locking the keyfob disables all LED indications.

Quick Arming

If you have chosen to program one of the keyfob buttons as 'Arm Area', you can then opt to 'quick arm' that area. When you press the button to arm the area, the panel will begin to count down your exit time (depending on what exit mode has been programmed by your engineer). Once this 'arming stage' begins, press the same button on the keyfob again and the system will arm immediately.

The disarm LED on the panel will turn off and a beep will sound to signal that the system has been armed. The RED LED on the keyfob will illuminate for a short time to confirm this.

Arming and Disarming with the Tag Reader

It is possible to arm and disarm your system using a tag wherever a reader is installed.

To lock and unlock doors using a tag reader, the door must have a magnetic lock that is connected to the door release output on the reader.

Arming

1. Present a valid tag to the reader.
2. The GREEN LED will illuminate on the external reader (or the disarm LED on the internal reader).
3. Remove the tag.
The door will unlock.
4. Present the same tag within 10 seconds and the system will arm and the door will lock displaying a RED LED.

Disarming

1. Present a valid tag to the reader and then remove it.
The status will be shown (the alarm symbol will illuminate to indicate that the system is armed on the internal reader, or the RED LED on the external reader).
2. Present the same tag again within 10 seconds and the system will disarm and the door will unlock.

Figure 1: External Tag Reader LEDs (arming shown)

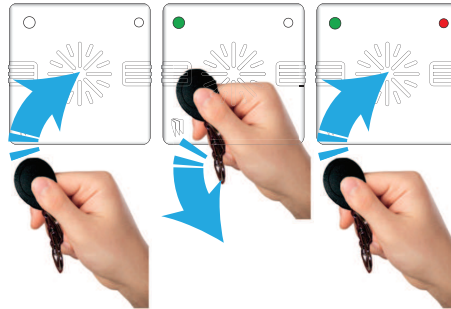








Table 2 - Internal Tag Reader LEDs

LED	Description
	Tag Area (present tag here)
	Ready LED (ready to arm)
	Alarm LED (shows alarms)
	Tamper LED (shows tamper alarms)
	Fault LED (shows system faults)
	Unset LED (shows system is disarmed)

Access Control

The readers can also be used for opening doors only, without the ability to arm or disarm. Please contact your installer for more information on this feature.



If the system fails to arm, a fault will display on the internal tag reader or a 'failed to arm' sound will activate on the external tag reader buzzer.

Special Disarm Users

The Enforcer uses Special Disarm Users, which are users that can signal disarm and special disarm. Special Disarm Users are programmed the same as standard users, and are numbers 15-25 in the **LEARN USER CODES KEYFOBS & TAGS?** menu.

PyronixCloud

Setting up PyronixCloud on the Panel

Check with your Engineer that the panel has been set up to allow communication between the panel and the cloud/app.

1. Press **D** and enter your User Code, then press .
The Master Manager Menu is displayed.
 2. Scroll to **SET UP APP?**, and press .
Enable App is displayed.
 3. Press **1** to enable the app and press .
System ID is displayed.
 4. Make a note of the System ID and press .
 5. Enter a secure password (max characters =16) for the PyronixCloud, and press .
 6. Press **0** to set Security to 'Standard' and press .
 7. Enter a secure password for the HomeControl+ App and press .
Poll Server is displayed.
 8. If required, choose a Poll Server setting and press .
It is recommended that **Poll Server** is set to **Yes**.
- For more information, see "Setting up the PyronixCloud" on page 13



When creating passwords, ensure that the password uses a variety of upper case, lower case, numbers and symbols – where applicable – to ensure the best security possible.

Setting up the PyronixCloud

Log on to www.pyronixcloud.com and create an account. A confirmation email will be sent to the registered email address. Once the link on the email is clicked, you are now set up on the PyronixCloud.

1. Enter the System ID and Cloud Password that was set up on the panel and click **Submit**.

Register New System

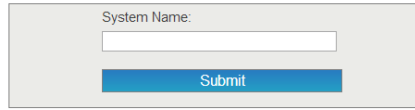
System ID:

Cloud Password:

2. Enter an appropriate System Name.


This will only be used by the Cloud, as you may want a different name on the App.

Register New System



A form titled "Register New System" with a text input field labeled "System Name:" and a blue "Submit" button below it.

3. The panel will now appear on 'View Systems' and 'System Polling' will be displayed on the right. The green tick shows that the system is connected.

Home (ABCDEFGH) [Edit](#) [Web Access](#) System Polling 

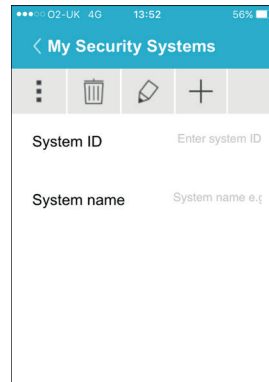
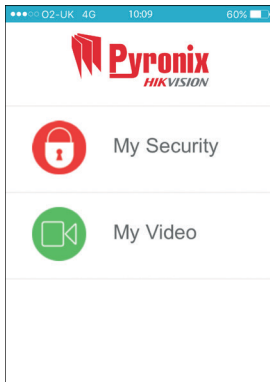
User	Device	Last Connected	Permission	Notifications
No User Apps Registered				

4. Set up the HomeControl+ app.

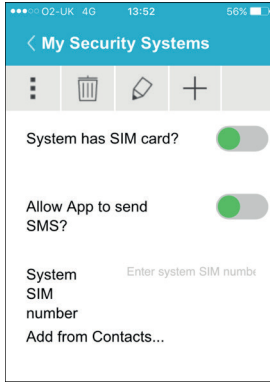
Setting Up The HomeControl+ App

Adding a Panel to the App

1. Open the HomeControl+ app and select **My Security**.
2. Select **+**, then enter the System ID and a System name for your reference.



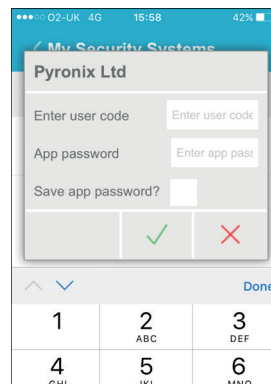
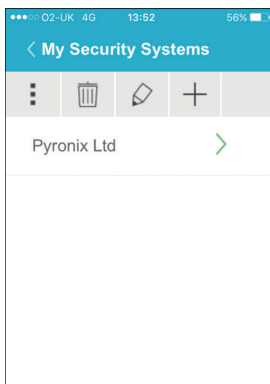
3. Enable and disable the relevant options and enter the SIM phone number used on the panel (in the format **+447777123456** for example).



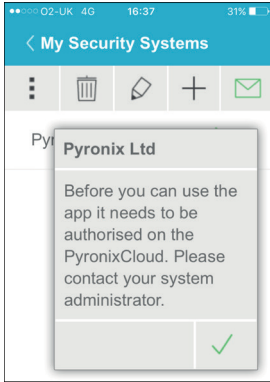
The SIM card and phone number options are only applicable when a DIGI-GPRS modem is installed. This allows the smart device to send SMS to the control panel in order to force the modem to poll the cloud. If the panel has been programmed to poll the cloud, these options are not applicable.

Connecting to a Panel

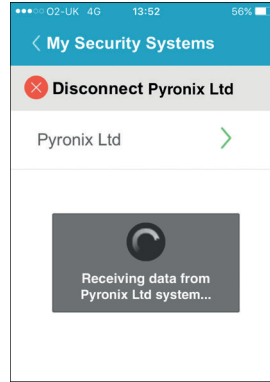
1. Open the HomeControl+ app and select the system.
2. Enter a valid User Code and the app password (as entered in the panel), then select the tick icon.



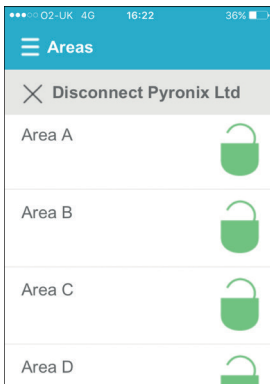
3. Ensure the HomeControl+ app is authorised on the PyronixCloud. Contact your engineer if the message below is displayed.



4. If connected successfully, **Connected to your system** will be briefly displayed and then the screen below will be displayed.
























5. To disconnect, select **X** next to **Disconnect**.



All new smart devices, when first connected, will be disabled by default. The cloud administrator will need to manually enable these devices before they will be able to connect to the panel. This is an additional security feature to prevent unauthorised access. A panel can only be claimed by one cloud administrator.

HomeControl+ App Icons

	My Security		Area unset
	My Video		Area set
	Settings		Area does not exist
	Delete		Unable to arm area
	Edit		Area cannot be armed
	Add system		Detector fault
	New notification		Area in alarm
	Notifications		Supervision fault
	Search		Output is off, or option is set to 'no'
	Refresh		Output is on, or option is set to 'yes'
	Disconnect from system		

Configuration

Chime Feature

This feature can be setup by your installer and is most commonly enabled for doors using the magnetic contact. When activated you will hear a 'chime' sound to alert you whenever the door is opened.

To disable the chime on the panel or keypad, close all doors that chime and press the **[C]** key until 'c' is no longer displayed on the screen.

Press the **[C]** key again to re-enable the chime.

PA from Keypad

If you require a PA (Panic Alarm), press and hold both the **[1]** and **[7]** keys or hold **[6]** for 2 seconds (by default) and a 'PA' alarm will be generated.



The PA feature, and the length of time the buttons must be held for, must be enabled by your engineer (silent or audible alarm options available).

Fire Alarm from Keypad

If you want to generate a fire alarm, perform one of the following actions:

- Press and hold both **[3]** and **[9]** for 2 seconds.
- Press and hold **[5]** for 2 seconds.



The fire alarm feature must be enabled by your engineer.

Master Manager Menu Options

Bypass Inputs	Disables any 24 hour input on the system for the current disarm period. NOTE: Inputs programmed as Entry Delay or PA cannot be bypassed
Operate User Outputs	Activates/deactivates user automation outputs that are used to remotely activate devices, such as electronic gates & lights.
Date & Time	Programs the date and time and enables the summer-time automatic adjustment. The timezone can also be changed in this menu.
Learn User Codes Keyfobs & Tags	Programs the User Codes, tags and learns keyfobs to the panel.
Review Log	The 'Review Log' function is used to view all operational information of the alarm system, such as arming/disarming information, access control and alarm activations etc.
Set Up App	To use the HomeControl+ app, this function must be enabled.
SMS Phonebook	If SMS is enabled, up to 10 mobile numbers can be programmed for the panel to send SMS alarms. Please discuss this feature with your installer if required.
Walk Test	The 'Walk Test' function allows the testing of all programmed inputs on the alarm system.
Bell Test	This function is used to test the external siren (wired and wireless) and strobe.
Allow Engineer Menu	If this function is enabled, the engineer will require authorisation from a Master Manager before an engineer can access the Engineer Menu.
Block Remote Arming	Blocks any attempt at arming the system remotely via the upload/download software.
Block UDL	Blocks any attempt at dialling into the system remotely via the upload/download software.
System Sounds Demo	This function demonstrates the sounds of the panel.
Exit Manager Mode	Exits the Master Manager Menu.



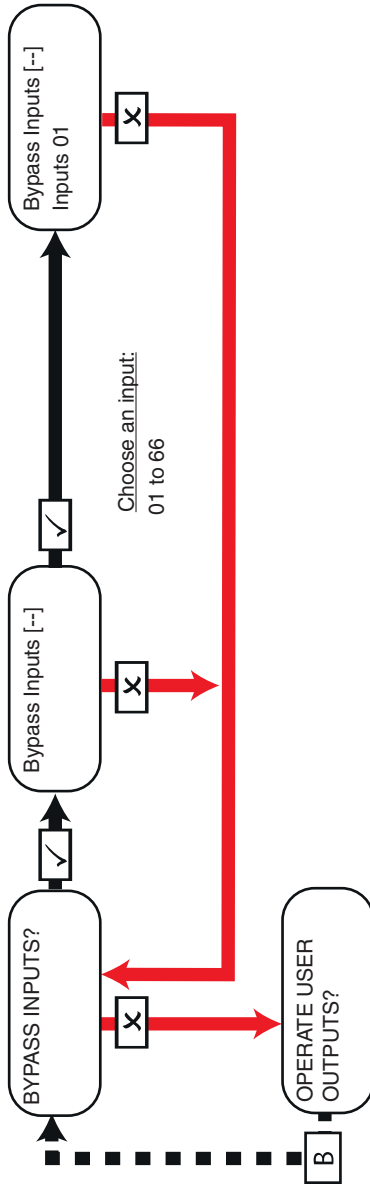
*Pressing the **A** key will exit the Master Manager Menu at any main menu option above. Make sure you change the default master manager code.*

Entering the Master Manager Menu

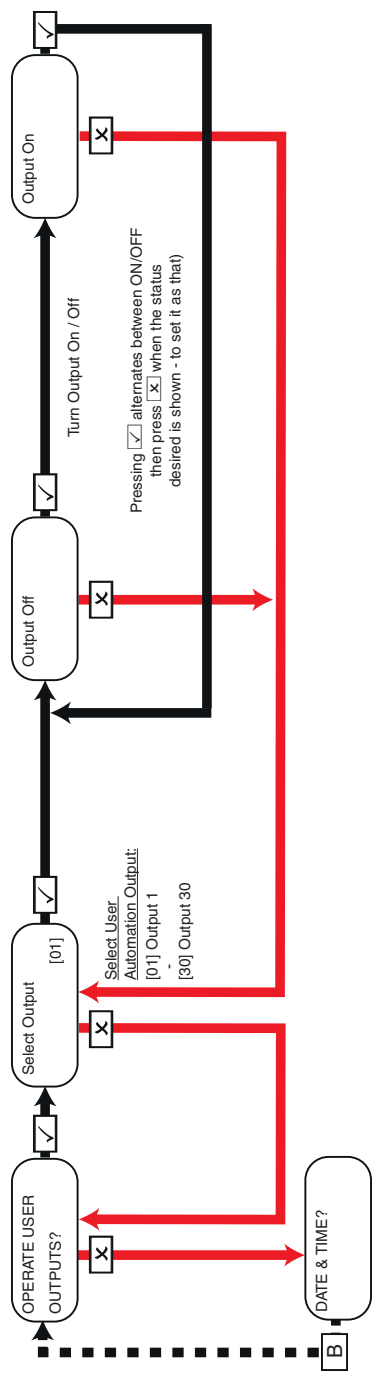
The default User Code is **1234**. We highly recommend that you change this code.



Bypass Inputs

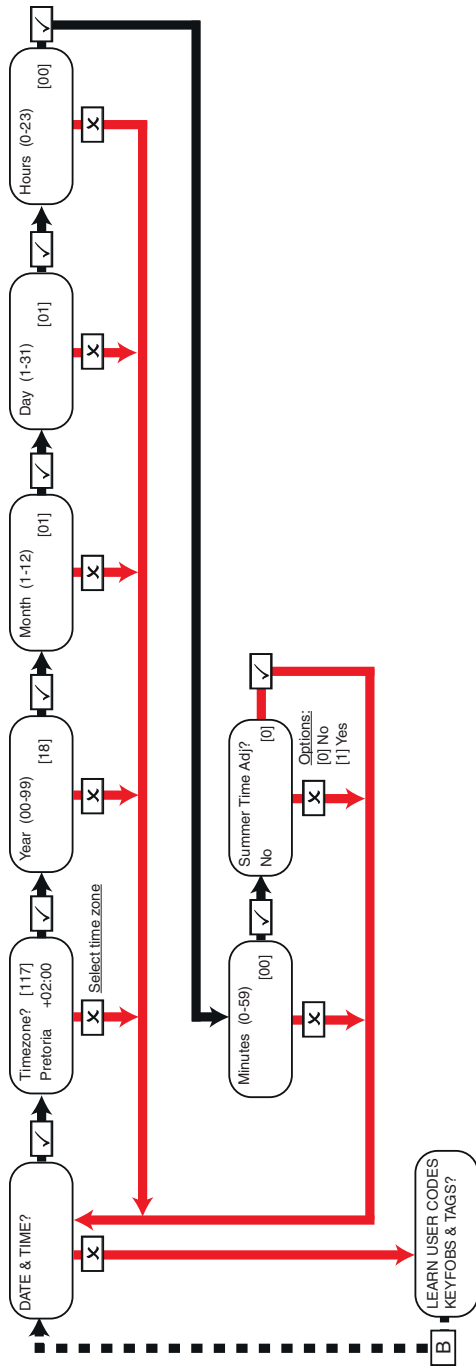


Operate User Automation Outputs



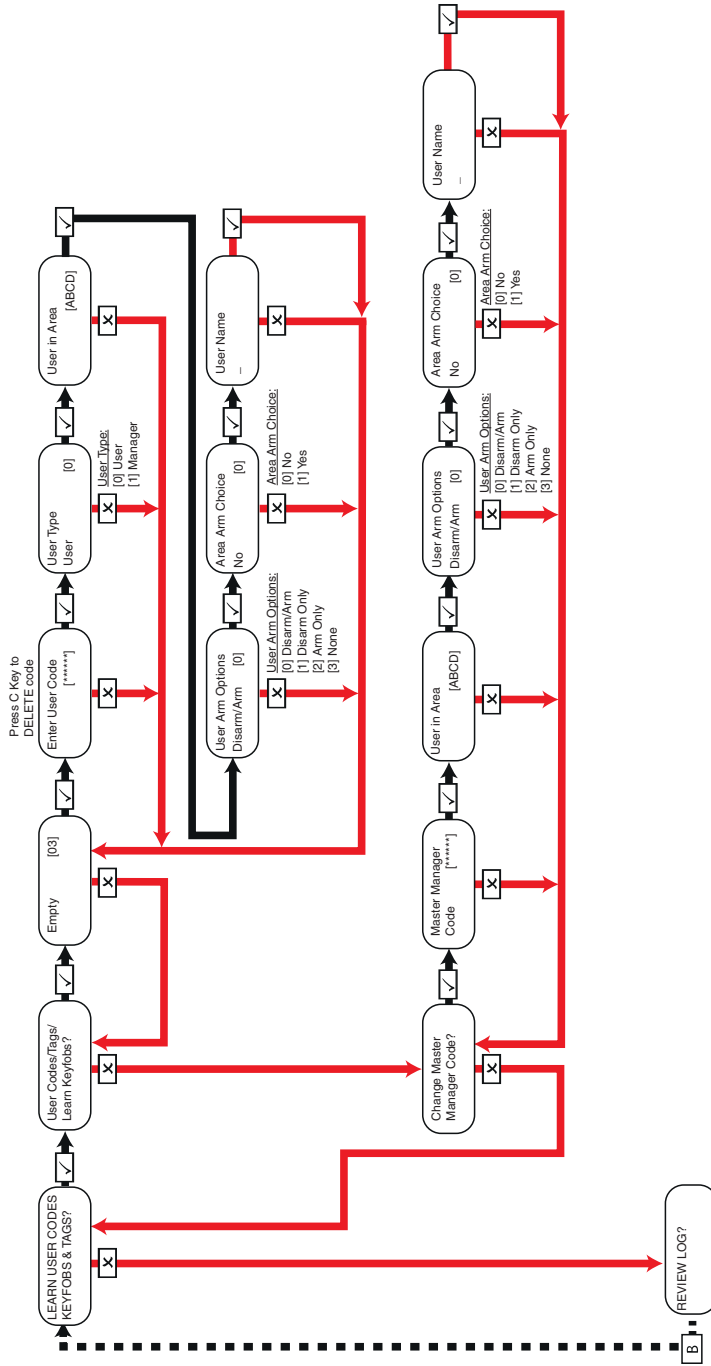
Date & Time

Date and Time are set automatically on most networks. You need to set the time manually when a PSTN modem is installed. GPRS is network dependant.



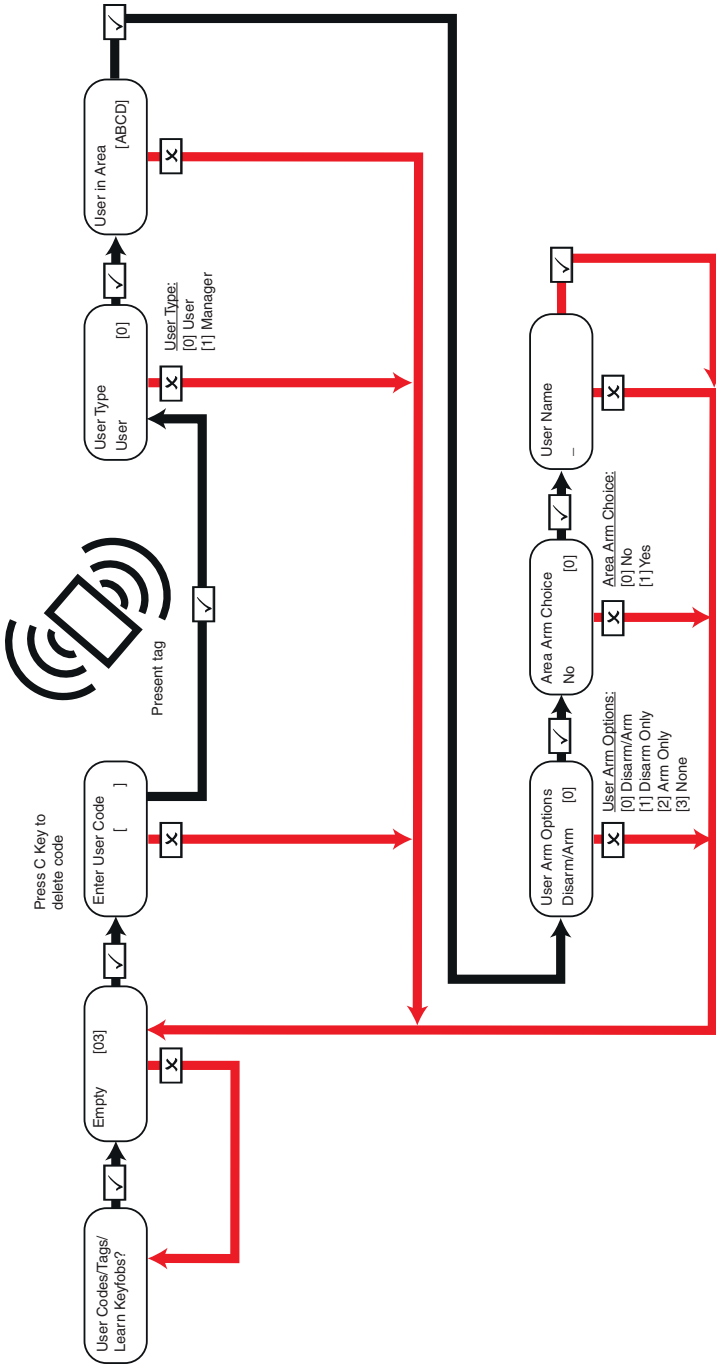
Change Codes

User Codes

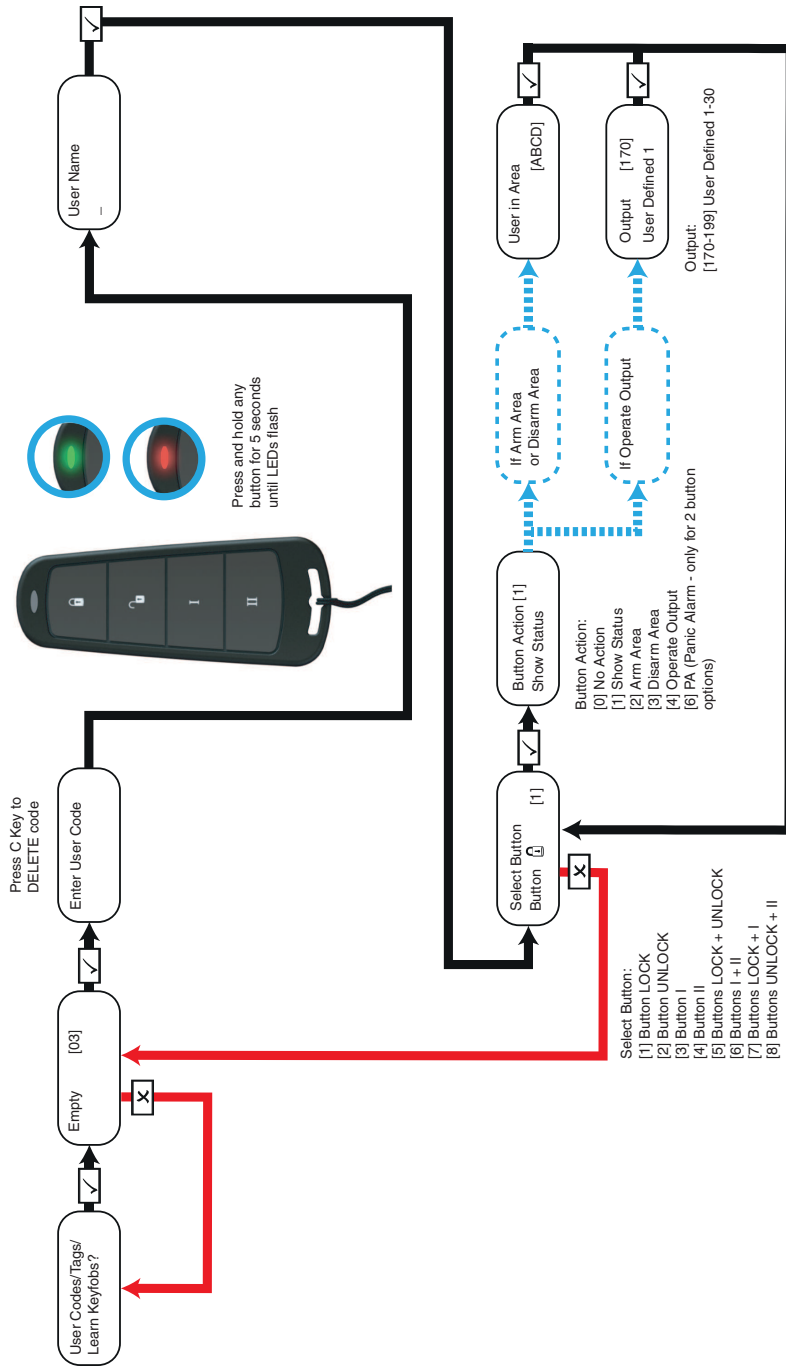


Proximity Tags

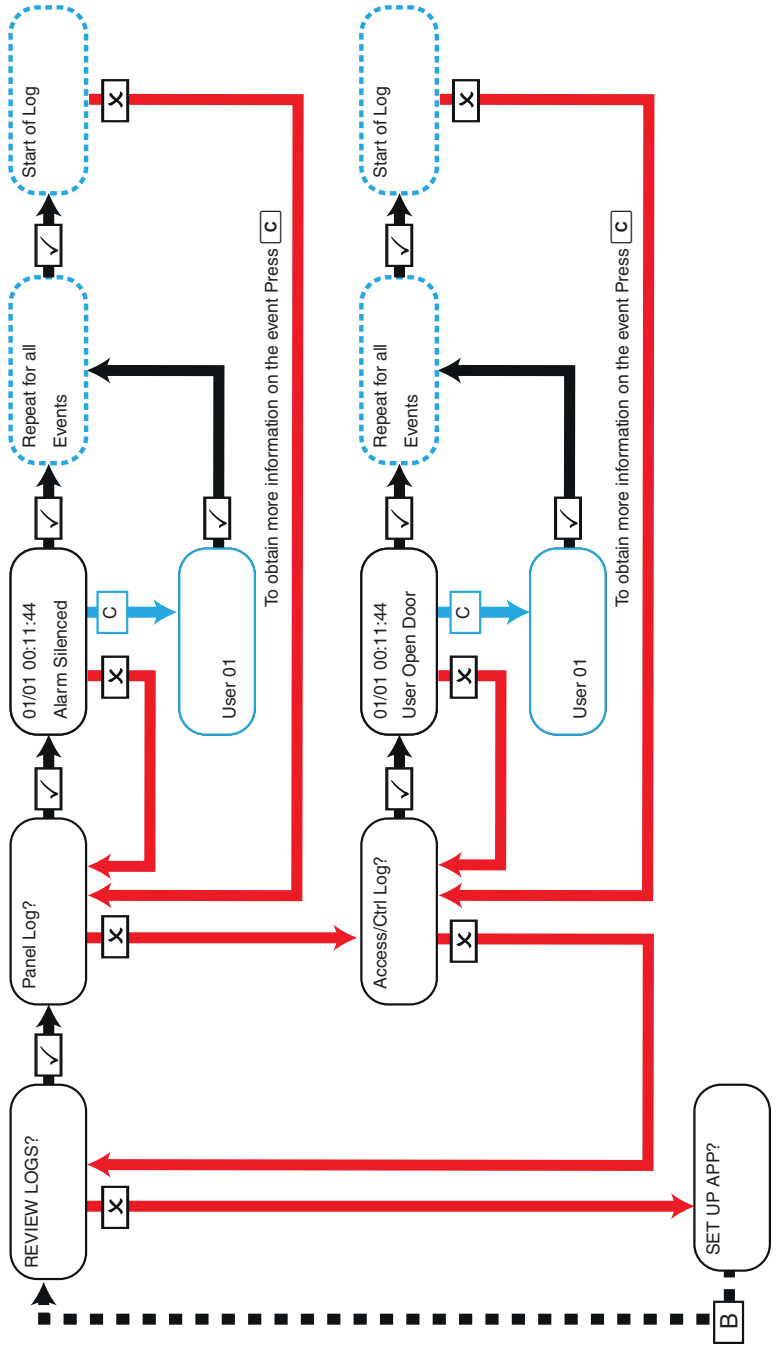
Arm Area Choice: If selected as 'Yes' you will be able to choose the area you wish to arm after you have entered your User Code or presented a valid tag. If selected as 'No', the Enforcer will automatically arm all areas the panel/code is assigned to.



Keyfobs

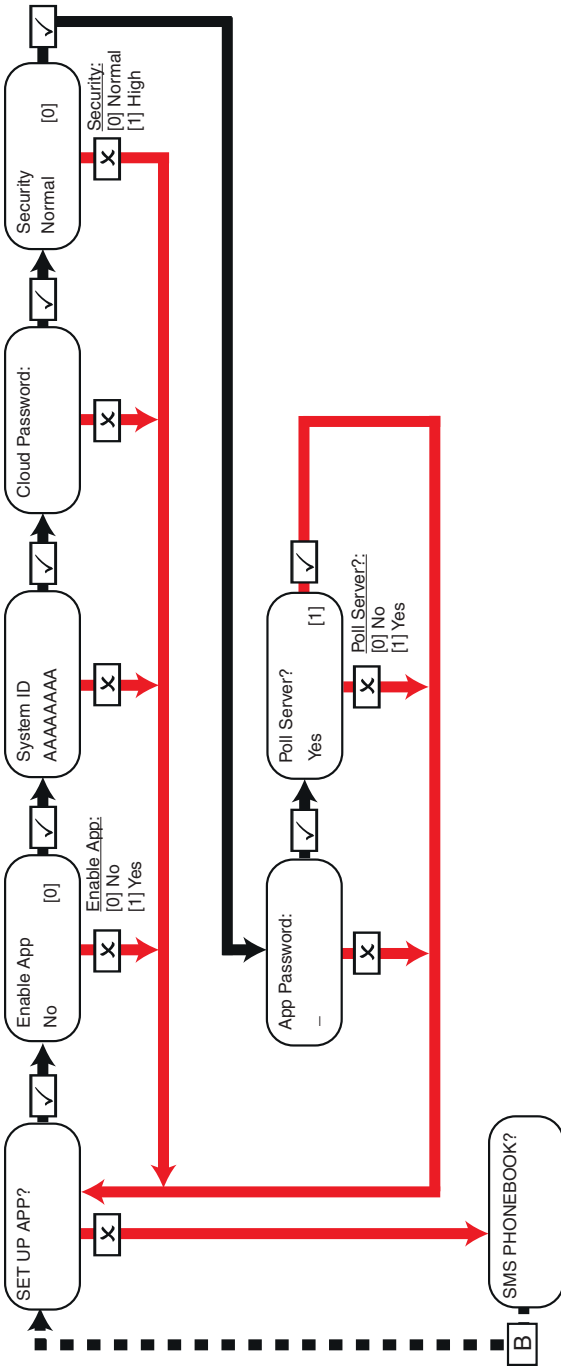


Review Log

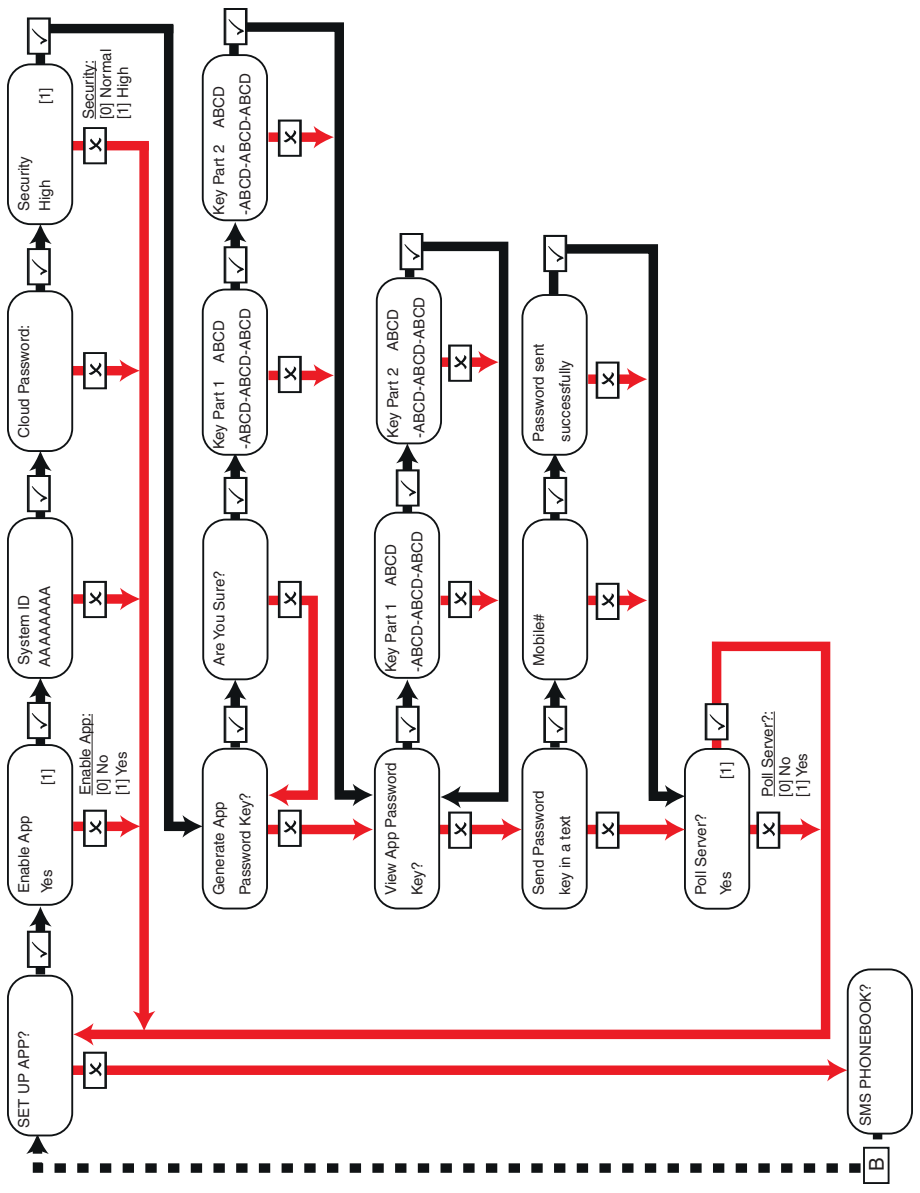


Setup App Data

Standard Security

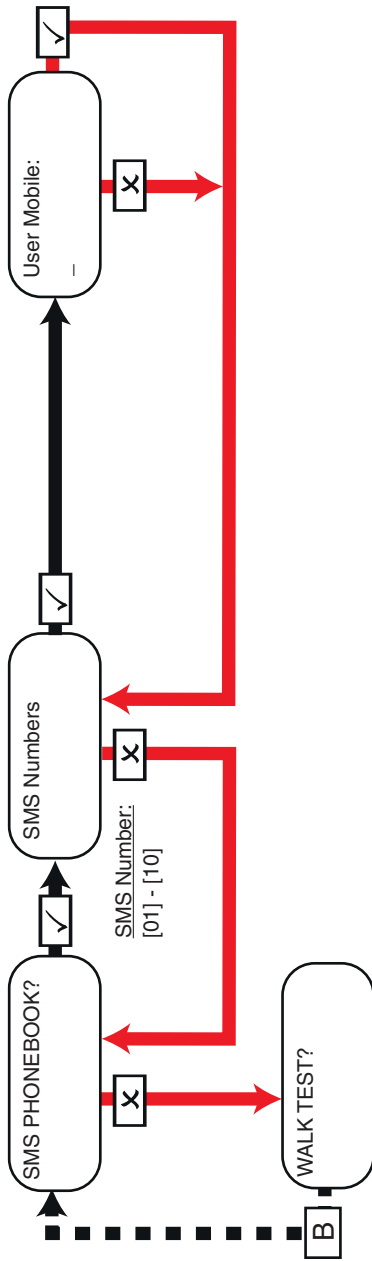


High Security



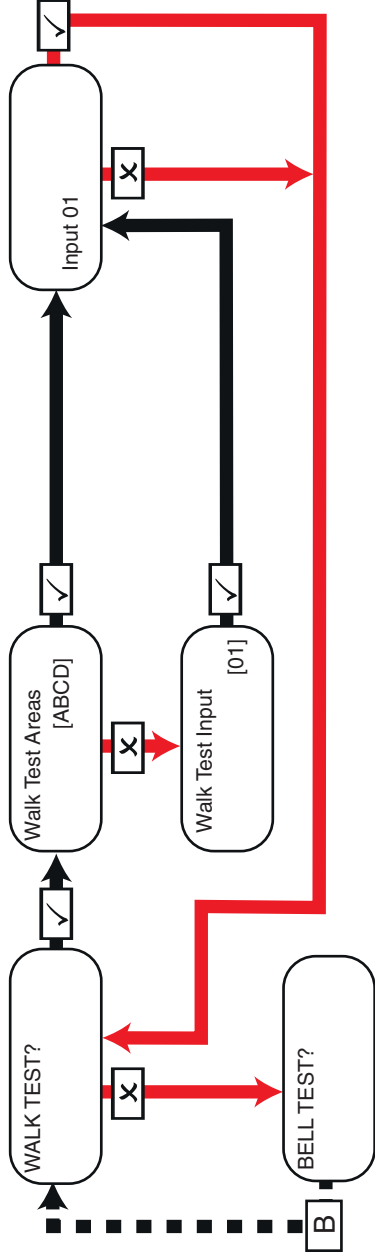
SMS Phonebook

Mobile numbers can be entered with or without an international dialling code (e.g. +44). If you need to enter an international dialling code to send the key to a foreign SIM card, use the **A** key to enter the '+' symbol.

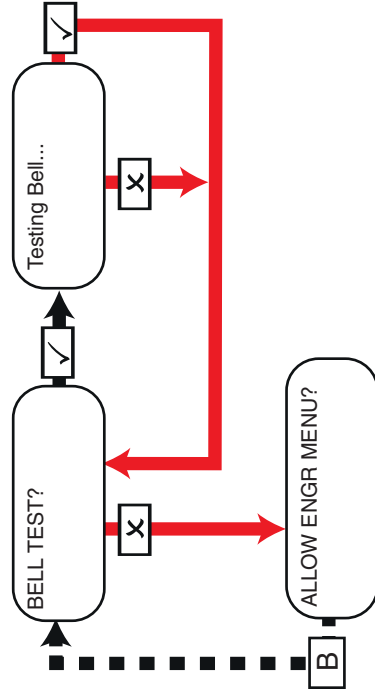


Walk Test

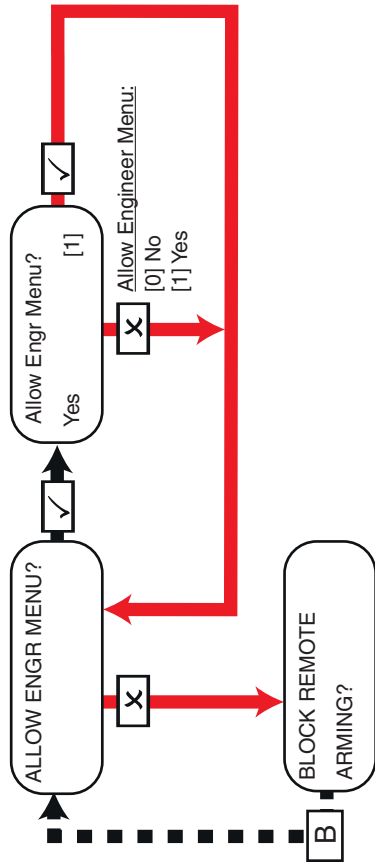
When walk testing areas, walk around to trigger all of the Inputs in the selected areas until the panel displays **Walk/Mask Test Inputs Completed**. When using the **Walk Test Input** option to choose a specific Input to test, the keypad will make an audible 'beep' each time the Input is triggered.



Bell Test

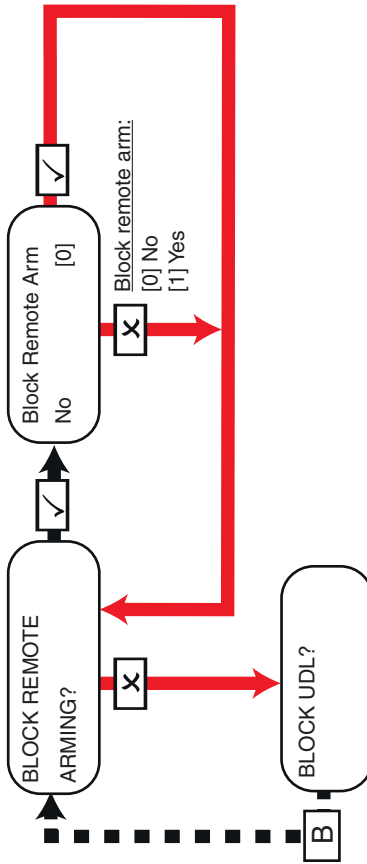


Allow Engineer Menu



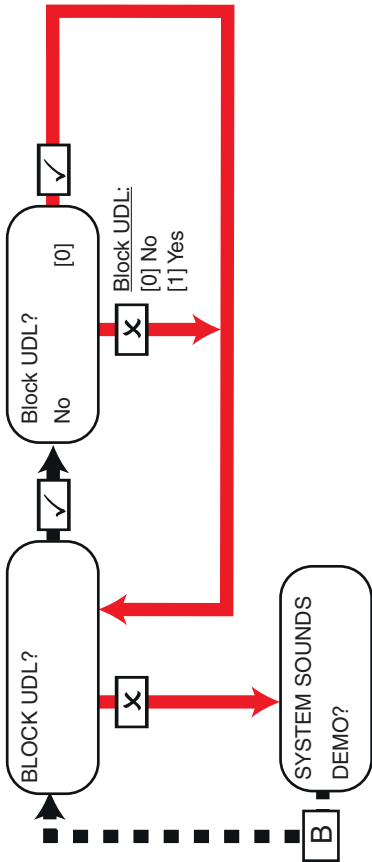
Block Remote Arming

This function will block any attempt made to arm or disarm via the UDL software if enabled.

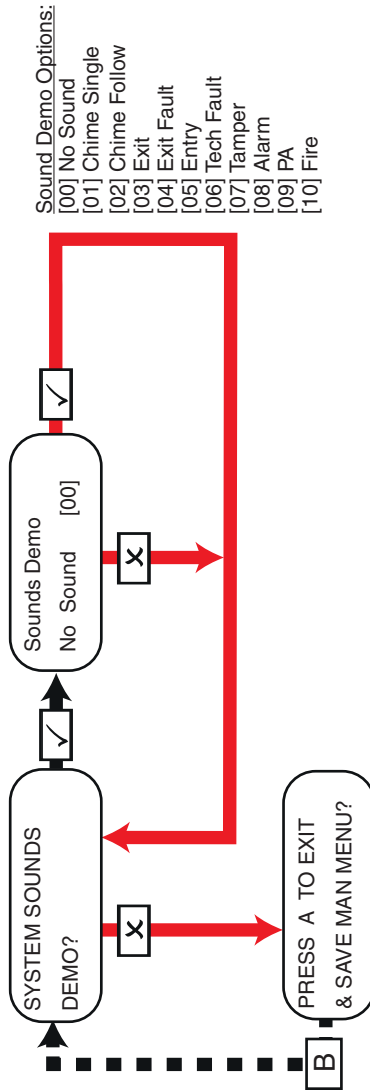


Block UDL

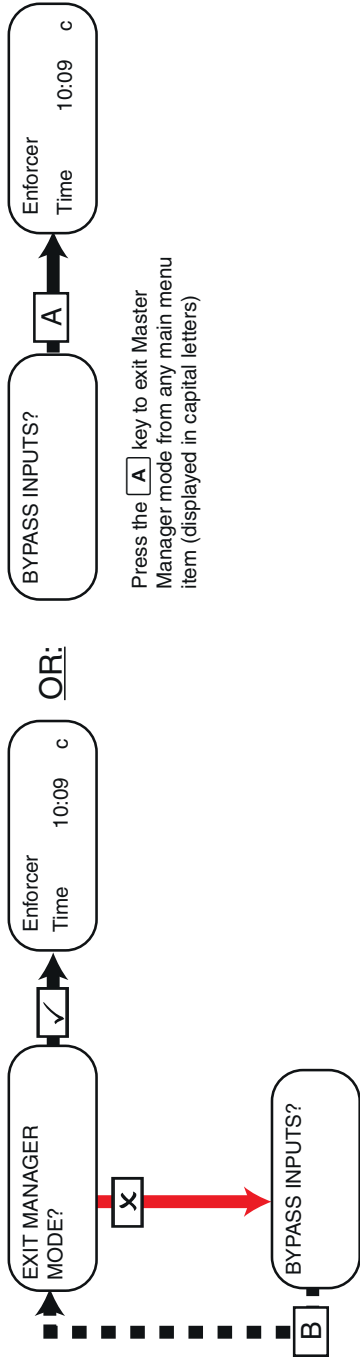
This function will block any attempt made to dial into the control panel to upload and download information if enabled.



System Sounds Demo



Exit Master Manager Menu



Press the **[A]** key to exit Master Manager mode from any main menu item (displayed in capital letters)

Reference

Handover Form

Alarm Company:	
Date of Installation:	
Site Reference:	
Engineer Name:	
Engineer Contact Number:	
Installed to Grade 2:	Yes / No
Environmental Class:	
Other Comments:	

SMS Commands

You can send SMS commands to the panel via your mobile phone.



All SMS commands must start with a valid User Code and are not case sensitive unless the utilised outputs are activated. If an SMS command is not recognised, the panel will send an 'incorrect command' message back to you.

Example SMS command send	Description	Example SMS command response
Arming via SMS text command		
1234 Arm A	1234 = User Code. Arm A = Will arm in Area A	Final Arm; Area A
1234 Arm ABCD	1234 = User Code. Arm ABCD = Will arm in Areas ABCD	Final Arm; Area ABCD
<i>NOTE: If no areas are specified then all areas will arm (default).</i>		
Disarming via SMS text command		
1234 Disarm A	1234 = User Code. Disarm A = Will disarm in Area A	Disarm; Area A
1234 Disarm ABCD	1234 = User Code. Disarm ABCD = Will disarm in Areas ABCD.	Disarm; Area ABCD

Example SMS command send	Description	Example SMS command response
<i>NOTE: If no areas are specified then all areas will disarm (default).</i>		
Arming with inputs bypassed via SMS text command		
1234 Arm A Bypass 4	1234 = User Code. Arm A Bypass 4 = Arms Area A and will bypass Input 4.	Input Bypass; Area A Input 04 Force Arm: Area A
1234 Arm A Bypass Kitchen	1234 = User Code. Arm A Bypass Kitchen = Arms Area A and will bypass the Input named Kitchen.	Input Bypass; Area A Kitchen Force Arm: Area A
Bypassing inputs via SMS text command		
1234 Bypass 6	1234 = User Code. Bypass 6 = In the next arming procedure, Input 6 will be bypassed.	Input Bypass; Area A Input 06
1234 Bypass Garage	1234 = User Code. Bypass Garage = In the next arming procedure, and will bypass the Input named Garage.	Input Bypass; Area A Garage
<i>NOTE: Output names have to be one word and spelled exactly as written in the panel e.g. 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>		
Checking the system status via SMS text command		
1234 Status	1234 = User Code. Status.	Area A Disarmed No Faults
Operating the user automation outputs via SMS text commands		
1234 Output 1 On	1234 = User Code. User Output 1 turns on.	OUTPUT 1 ON
1234 Output Garage-Door On	1234 = User Code output Garage-Door on = Turns output named as Garage-Door on.	OUTPUT Garage-Door ON
1234 Output Garage-Door Off	1234 = User Code output Garage-Door off = Turns output named as Garage-Door off.	OUTPUT Garage-Door OFF
<i>NOTE: Output names have to be one word and spelled exactly as written in the panel e.g. 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>		
<i>NOTE: The user automation outputs can also be activated via the keypad or the keyfob.</i>		
Checking the user automation outputs status via SMS text commands		
1234 Output 1	1234 = User Code. User Output 1 status check.	OUTPUT 1 ON or OUTPUT 1 OFF
1234 Output Garage-Door Status	1234 = User Code. Output Garage-Door status check.	OUTPUT Garage-Door ON or OUTPUT Garage-Door OFF
<i>NOTE: Output names have to be one word and spelled exactly as written in the panel e.g. 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>		
Changing a mobile number via SMS text commands		
1234 Change 07777888999 0787888999	1234 = User Code. Change number 07777888999 to number 0787888999	CHANGE 0787888999
<i>NOTE: Use the appropriate international dialling code (e.g. +44) when necessary (i.e. for foreign SIM cards). For example if you wanted to message a foreign SIM card at your holiday home abroad. When you send the SMS command, ensure you enter a space between the two mobile numbers.</i>		

Example SMS command send	Description	Example SMS command response
Start uploading/downloading via SMS text command		
1234 UDL	1234 = User Code. UDL = The panel 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 panel will make an outgoing data connection to the programmed PC1 number.	No response as the panel is already connected to the PC1

Inputs

Inputs	Input Name	Input Areas	Description	Inputs	Input Name	Input Areas	Description
1				34			
2				35			
3				36			
4				37			
5				38			
6				39			
7				40			
8				41			
9				42			
10				43			
11				44			
12				45			
13				46			
14				47			
15				48			
16				49			
17				50			
18				51			
19				52			
20				53			
21				54			
22				55			
23				56			
24				57			
25				58			
26				59			

Inputs	Input Name	Input Areas	Description	Input	Input Name	Input Areas	Description
27				60			
28				61			
29				62			
30				63			
31				64			
32				65			
33				66			

Outputs

Wired Outputs	Latched / Timed	Type	Action
PGM (Onboard)			
STB (Onboard)			
BELL (Onboard)			
PGM1 (KPD/TRD Address 1)			
PGM1 (KPD/TRD Address 2)			
PGM1 (KPD/TRD Address 3)			
PGM1 (ROX Address 0)			
PGM2 (ROX Address 0)			
PGM3 (ROX Address 0)			
PGM4 (ROX Address 0)			
PGM5 (ROX Address 0)			
PGM6 (ROX Address 0)			
PGM7 (ROX Address 0)			
PGM8 (ROX Address 0)			
PGM9 (ROX Address 0)			
PGM10 (ROX Address 0)			
PGM11 (ROX Address 0)			
PGM12 (ROX Address 0)			
PGM13 (ROX Address 0)			
PGM14 (ROX Address 0)			
PGM15 (ROX Address 0)			
PGM16 (ROX Address 0)			
PGM1 (RIX Address 0)			
PGM2 (RIX Address 0)			

Wired Outputs	Latched / Timed	Type	Action
PGM3 (RIX Address 0)			
PGM4 (RIX Address 0)			
PGM1 (RIX Address 1)			
PGM2 (RIX Address 1)			
PGM3 (RIX Address 1)			
PGM4 (RIX Address 1)			
PGM1 (RIX Address 2)			
PGM2 (RIX Address 2)			
PGM3 (RIX Address 2)			
PGM4 (RIX Address 2)			
PGM1 (RIX Address 3)			
PGM2 (RIX Address 3)			
PGM3 (RIX Address 3)			
PGM4 (RIX Address 3)			

Users

User	Name	Code/Tag/ Keyfob	User	Name	Code/Tag/ Keyfob	User	Name	Code/Tag/ Keyfob
1			26			51		
2			27			52		
3			28			53		
4			29			54		
5			30			55		
6			31			56		
7			32			57		
8			33			58		
9			34			59		
10			35			60		
11			36			61		
12			37			62		
13			38			63		
14			39			64		
15			40			65		
16			41			66		
17			42			67		
18			43			68		
19			44			69		

User	Name	Code/Tag/ Keyfob	User	Name	Code/Tag/ Keyfob	User	Name	Code/Tag/ Keyfob
20			45			70		
21			46			71		
22			47			72		
23			48			73		
24			49			74		
25			50			75		

Compliance

As per EN 50131-1 the Enforcer is capable of supporting all conditions A, B and C:

In Grades 1 & 2 I&HAS when an I&HAS or part thereof is in a set state:

- a. access to the supervised premises or part thereof, via an entry/exit route, shall be prevented, or
- b. opening the door to the entry/exit route shall initiate an entry procedure, or
- c. indication of the set/unset status shall be provided.

In Grades 3 & 4 I&HAS when an I&HAS or part thereof is in a set state:

- a. access to the supervised premises or part thereof, via an entry/exit route, shall be prevented, or
- b. opening the door to the entry/exit route shall initiate an entry procedure.

App HomeControl+ not certified IMQ-Security Systems.



EN50131-3:2009
 EN50131-1:2008+A1:2009
 Security Grade 2
 Environmental Class II



For electrical products sold within the European Community.

At the end of the electrical products useful life, it should not be disposed of with household waste. Please recycle where facilities exist. Check with your Local Authority or retailer for recycling advice in your country. When disposing of the product and accessories, the batteries must be removed and disposed of separately in accordance with the local regulations.



A series of 20 horizontal lines for writing, spaced evenly down the page.





CE