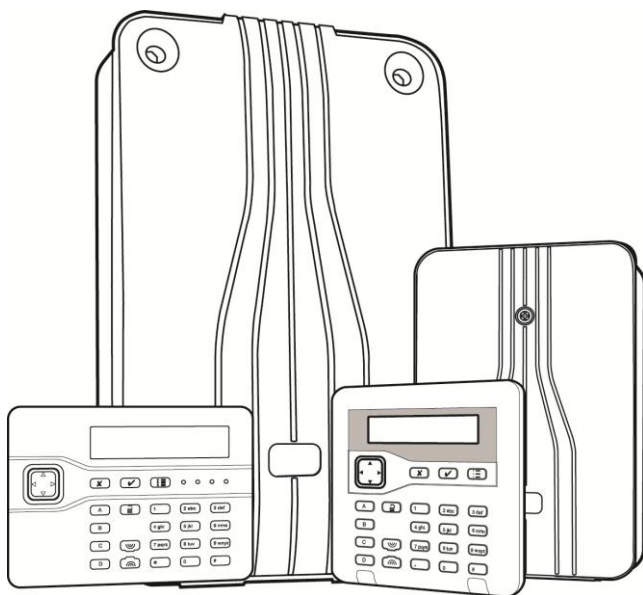


i-on30R/40H (Next Generation) Security System

Administration and User Guide



Issue 2

Control unit software version 5.01

EATON

Powering Business Worldwide

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation's ("Eaton") experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or other-wise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein. The information contained in this manual is subject to change without notice.

Compliance Statement

The i-on Next Generation control units are:

- Suitable for use in systems designed to comply with PD6662:2010 at Grade 2 and environmental class II.
- Suitable for use in systems designed to comply with the requirements of EN50131-3 at Grade 2 and environmental class II.
- Compliant with the requirements of EN50131-6:2008 at Grade 2 and environmental class II.

When an appropriate communicator is enabled, the control unit is compliant with EN 50136-1. It allows the alarm transmission system to meet the performance requirements of EN 50131-1:2006 ATS 2 provided that:

- a) The equipment is installed in accordance with the installation instructions.
- b) The communications link is functioning normally.

If the installer selects a non-compliant configuration, they must remove or adjust compliance labelling.



Warning: Mains voltages are present inside control unit. No user serviceable parts inside.

Contents

Compliance Statement.....	ii
Chapter 1: Introduction	1
About this guide.....	1
Part-setting and partitioned modes.....	1
Part-setting mode.....	1
Partitioned mode.....	2
System Components.....	3
The control unit.....	3
Detectors (zones).....	4
Outputs.....	5
Keypads.....	5
Proximity Tags.....	9
Remote controls.....	9
Radio Hold Up Alarms (HUA).....	9
About Users.....	10
User access codes.....	12
Installer access.....	13
Eaton SecureConnect™.....	13
Chapter 2: Setting and Unsetting	14
Introduction.....	14
Using a keypad.....	14
Setting the system.....	14
Quick-setting the system using a keypad.....	17
Unsetting the system using a keypad.....	18
Using a two-way keyfob-style remote control.....	19
Setting the system.....	20
Unsetting the system.....	20
Querying the set/unset status.....	20
Starting a Hold Up Alarm (HUA).....	21
Using a one-way remote control.....	21
Setting the system.....	22
Unsetting the system.....	22
Using a one-way radio keypad.....	23
Setting the system.....	23
Unsetting the system.....	24
Using SMS command messaging.....	24
Chapter 3: Managing Alarms	25
Alarm types and sounds.....	25
Other alarm actions.....	26
Speech messages.....	27
Silencing, acknowledging and resetting alarms.....	27
Installer resets.....	29
Accidental alarms.....	29
Viewing alerts.....	29
Chapter 4: User Menu Options.....	31
User Menu Map.....	31

Entering and exiting the user menu	33
Entering text.....	33
Omitting zones.....	34
Using shunt groups.....	35
About shunt groups.....	35
Activating or deactivating a shunt group	36
Managing users.....	36
Changing your access code or assigned devices	37
Adding users	37
Editing users	40
Deleting users	41
Viewing the log	41
User numbers.....	42
Testing the system	42
Testing sirens and sounders	42
Testing a wired keypad	43
Performing a walk test.....	44
Testing outputs.....	45
Testing remote controls	46
Testing user HUAs.....	47
Testing proximity tags	47
Testing ARC reporting.....	48
System configuration	49
Switching facilities on/off	49
Setting the date and time	50
Configuring calendar sets.....	50
Defining contacts	54
Editing outputs	55
Managing remote controls	57
Starting a call to Downloader.....	61
Switching outputs on/off	62
Using the About options	62
Generating a SecureConnect pairing code.....	63

Chapter 1: Introduction

About this guide

This guide explains how to operate and administer an i-on Next Generation alarm system as a user. The guide describes the devices you can use to carry out these tasks, how to perform functions such as setting and unsetting the system, how to manage alarms and the options available from the user menu to carry out tasks such as omitting zones, adding users and viewing the log.

This guide does not describe topics such as system installation, maintenance and installer menu options; these topics are covered in other guides that are available to installers.

Part-setting and partitioned modes

Depending on your requirements, your system may have been configured by the installer as a part-setting system or a partitioned system. These two modes are explained below.

Part-setting mode

In part-setting mode, the control unit can set in one of four ways: either full set or one of three part sets (part set B, C or D). Each zone can belong to one or more part sets.

When the system is full set, the control unit sets all zones, irrespective of the part set they belong to.

When the system is part set, the control unit sets only those zones that belong to the part set you have chosen to set. The installer defines which zones are in each part set. A part set may, for example, set all areas of the building except the delivery area, which would allow people to occupy the delivery area while the main part of the building is protected.

In a part-setting system, the system responds to just one keypad at a time.

Partitioned mode

Partitioned mode is useful if the system is installed at a site where it is necessary for different groups of users to have independent control to set and unset different areas of the building, such as certain offices in a building used by several companies. The maximum number of partitions is dependent on the type of control unit you are using.

The installer can allocate one or more zones to each partition, and users can set and unset each partition completely independently of all the others.

Individual users can be given access to one or more partitions. If a user has no access to a partition, he or she cannot set or unset that partition. In effect, partitions allow the system to be split into separate alarm systems.

A zone is armed only when ALL of the partitions that it belongs to are set. If you unset any of the partitions that a zone belongs to, the control unit will unset that zone. This allows, for example, the system to include areas such as lobbies that are shared by users belonging to different companies.

In addition, each partition can have a full-set level and one part-set level. Users can choose whether to set a partition to which they have access at full or part-set level. When the user chooses the part-set level, all zones that the installer has assigned the "Part Set" attribute are set, and the others remain unset.

For partitioned systems, you can use more than one keypad at the same time, provided that they are in separate partitions. Within each partition, the control unit responds to just one keypad at a time.

The installer can allocate keypads, sirens, sounders or outputs to any of the partitions.

System Components

An i-on Next Generation alarm system can contain many different types of device, depending on the requirements of the installation. Figure 1 and the following sections give an overview of key components of interest to users.

1. Two-button Hold Up Alarm long range.
2. Two-button Hold Up Alarm.
3. One-way remote control.
4. Two-way remote control.
5. Keypad (i-kp01) .
6. Keypad (KEY-K01, KEY-KP01, KEY-KPZ01 or KEY-RKPZ)
7. Keypad (i-RK01) one-way radio (arming) keypad.
8. Keypad (KEY-FKPZ) flush-mount keypad.
9. Door contact/universal transmitter.
10. Smoke detector.
11. Passive infra-red detector.
12. External siren/strobe.



Figure 1. Peripherals

The control unit

At the heart of an i-on alarm system is the control unit, which is often installed in a cupboard or elsewhere that is out of sight.

The control unit contains the main processing unit, the power supply and stand-by battery. The stand-by battery can keep the alarm system operational for several hours if the mains supply fails.

Several different control units are available. Each provides a different number of zones, outputs, users and other features. The control unit selected should match the requirements of the site.

Alarm communication

When the control unit detects an alarm, it starts an external sounder/strobe unit and operates sounders (such as the sounder in keypads).

If configured, the control unit can also communicate alarm information to an Alarm Receiving Centre (ARC) across the internet, or (depending on the hardware fitted) over a fixed-line or mobile telephone network.

Also depending on the hardware fitted and system configuration, the control unit may send alarm information by email, SMS text message, or to a specified telephone number using a pre-recorded speech message.

SMS command message control

If the control unit has appropriate hardware fitted, you can change or query the status of the alarm system using commands contained within SMS text messages sent from a mobile phone or other messaging device.

You can send SMS command messages to set/unset the system, activate/deactivate outputs, omit/un-omit zones or query the current status of the system.

For further information, please refer to the "SMS Command Messaging User's Guide".

Detectors (zones)

Detectors are the physical devices that detect alarm conditions. They include devices such as passive infra-red movement detectors, door contacts and smoke detectors. Each detector may use a wired or radio connection to the alarm system, depending on the type of detector.

In addition to fixed detectors, the control unit can monitor small portable Hold-Up Alarm (HUA) transmitters, which users can use to start alarms remotely. HUA transmitters are also known as Panic Alarms (PAs).

A zone is the lowest-level item within the intrusion system that can be set or unset, but since there is normally only one detector per zone, the terms "zone" and "detector" are often used interchangeably.

Outputs

The system provides "outputs", which can control external equipment such as lights, locking devices or other equipment, or communicate with an Alarms Receiving Centre (ARC).

The installer can configure "User Defined" outputs, which you can switch on or off from a keypad or remote control.

Keypads

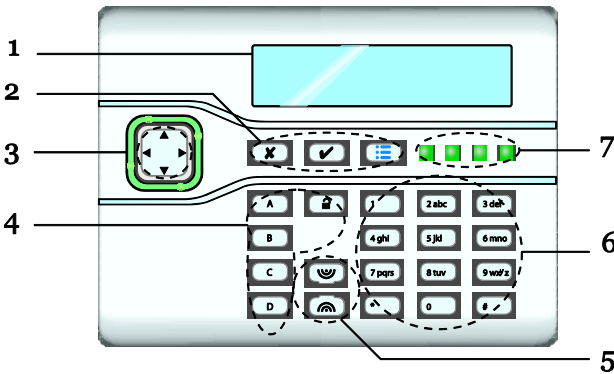
Keypads normally provide the main interface between users and the alarm system. They allow users to perform all functions, such as setting or unsetting the system and accessing the user menu options. Each alarm system can have one or more keypads up to a limit depending on the control unit used.

The i-on Next Generation range of alarm systems supports several different types and styles of keypad (Figure 2), including wired and radio (wireless) keypads.

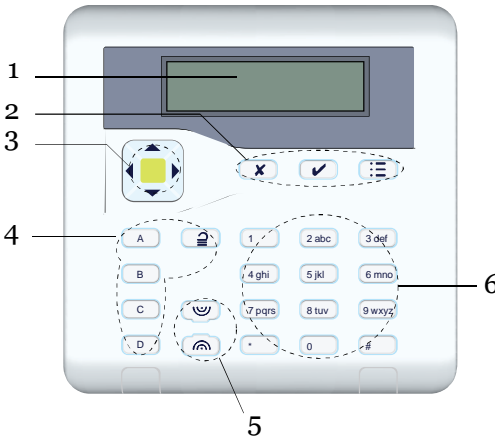
The keypads have keys to operate the system, and a two-line display to show you status information or options. Keypads also contain a sounder, which gives warning tones when the system is setting or unsetting, or when an alarm is detected.

Users identify themselves to the system by entering their unique access code at the keypad or by presenting a proximity tag (see page 8).

The following sections explain the main features of keypads.



i-kp01



KEY-K01

KEY-KP01

KEY-KPZ01

KEY-RKPZ

KEY-FKPZ (similar layout)

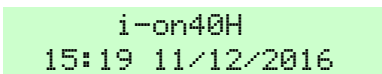
Figure 2. Keypad features (see the following sections)

LCD display

("1" on Figure 2.)

The LCD display shows messages and prompts to guide you through actions such as setting, unsetting, acknowledging alarms and using the user options.

When the system is idle (either while set or unset), the display shows the "standby screen". For example:



(The top line may show a name other than the control unit's model name.)

Programming keys

("2" on Figure 2.)

- ✓ Confirms an action, such as selection of an option or acknowledgement of an alarm.
- ✕ Exits an option or cancels a change.
- ☰ Displays the user menu or provides further information.

Navigation keys

("3" on Figure 2.)

The navigation keys have the following functions:

- ▲ In menus: scrolls up.
In text entry: moves the cursor left
- ▼ In menus: scrolls down.
In text entry: moves the cursor right.
- ▶ In menus: changes the value or displays further information.
In text entry: moves the cursor to the right.
- ◀ In menus: changes the value.
In text entry: deletes characters when editing names.

The navigation keys also glow red to draw your attention to special events.

Setting and unsetting keys


("4" on Figure 2.)

An installer can use the Installer menu to edit the details of the keypad and specify the action of the A, B, C and D keys. In a part-setting system, each key can either full set the system, set part set B, C or D, or operate an output. In a partitioned system, each key can either full set a partition, part set a partition, or operate an output.

For a KEY-K01, KEY-KP01, KEY-KPZ01 or KEY-RKPZ, A, B, C and D glow to show the set status. In a part-setting system, A glows if the system is full set, B glows if part set B is set, C glows if part set C is set, and D glows if part set D is set. In a partitioned system, A, B and C glow to show the set status of the partition controlled by the corresponding key. For example, if key A is used to part set partition 2, the key glows when partition 2 is part set.

An installer can use a link in the keypad or choose an option in the keypad's local menu to hide the set status shown by the keys to comply with EN50131.

To use A, B, C, D, enter your access code (or present your proximity tag) and press the key.

Pressing  and entering an access code (or presenting a proximity tag) unsets the system.

Hold Up Alarm (HUA) keys

("5" on Figure 2.)



Starts a Hold Up Alarm when both keys are pressed (if enabled by the installer).

Alpha/numeric keys

("6" on Figure 2.)

These are used for entry of text or access codes.

Set/Unset status LEDs

("7" on Figure 2.)

These LEDs (i-kp01 only) can show the set status of the system.

In a part-setting system, A glows if the system is full set, B glows if part set B is set, C glows if part set C is set, and D glows if part set D is set. In a partitioned system, A, B and C glow to show the set status of the partition controlled by the corresponding key. For example, if key A is used to part set partition 2, the key glows when partition 2 is part set.

An installer can use a link in the keypad to hide the set status shown by the keys to comply with EN50131.

Proximity Tags

A proximity tag is a small plastic token that contains a low-powered radio transmitter. Each tag contains a unique identity code and is assigned to a specific user.

When you present the tag within about 10mm from the front of a keypad that contains a proximity tag reader (or to a separate proximity tag reader), the reader senses the presence of the tag and reads its identity code.

If the control unit recognises the identity of the tag, it allows the user to access the system in the same way as if the user had entered a their access code.

Remote controls

Each user can be assigned a portable remote control to perform functions such as setting or unsetting the system or operating output devices from a distance. There are two types of remote control:

- The i-FB01 – This is a one-way remote control that has four buttons and a small LED that glows when it transmits a signal. See page 21 for details of how to operate this device.
- The FOB-2W – This is a two-way keyfob-style remote control that provides feedback to show you whether the alarm system has set or unset correctly. See page 19 for details of how to operate this device.

Radio Hold Up Alarms (HUA)

A radio HUA (Figure 3) is a two-button transmitter used to start a Hold Up Alarm (HUA), otherwise known as Panic Alarm or Personal Attack (PA).

To activate the transmitter, you must press both buttons at the same time. On some models, a third button acts as a lock, which prevents the HUA from accidentally operating when carrying it in your pocket.

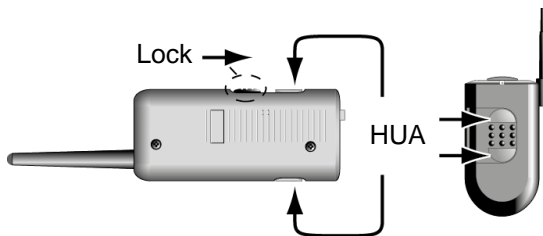


Figure 3. Radio HUA operation

About Users

A user is a person who is able to enter an access code at a keypad to perform an action, such as to set or unset the system, raise a duress alarm or gain access to the user options.

User options are available for carrying out tasks such as omitting zones, viewing the log, testing the system and switching outputs on or off. For a full list of available user options, please refer to the User Menu Map on page 31.

When the system is new, there is only one user: the default master user, who has full access to perform any action that a user is able to do and access all user options. The master user can add new users, and while doing so, specify the user's *type*, which determines the actions the user can carry out.

The control unit identifies each user by a unique *access code* (page 12), which contains 4 or 6 digits, depending on how the installer has set up the system.

The available user types are as follows:

- **Master user** – This user is able to carry out all user actions. A master user can, for example, set or unset the system and access all options in the user menus, including the ability to add or delete other users.

A master user can edit any user's name, and for all but other master users, edit a user's type and partitions.

In a partitioned system, all master users always belong to all partitions.

There is always (at least) one master user (User 001), which cannot be deleted by any user.

- **Admin** (partitioned system only) – This user is similar to a master user, but is limited to one or more partitions.

Admin users can set or unset the system and have access to most options in the user menu (see the User Menu Map on page 31). They can add, delete or edit other users (including admin users) belonging to the same partition(s), but cannot add, edit or delete master users. Admin users can assign other users to any of the partitions that the admin user belongs to.

- **Normal user** – A normal user can set and unset the system, but has access to a limited number of user options. A normal user can, for example, omit zones, change their own access code, add their own

proximity tag, view the log and operate outputs, but cannot add or delete users.

In a partitioned system, a normal user is assigned to one or more partitions, which are the only parts of the system that they can set and unset.

- **Partition user** (partitioned system only) – A partition user is similar to a normal user, but has the added restriction that they must set and unset their allocated partitions from keypads that are also assigned to those partitions.
- **Duress Code** – A duress code user can set or unset the system, but whenever the access code is used, the control unit notifies the Alarm Receiving Centre (ARC).

A duress code has no access to the user menu and cannot have a remote control or proximity reader tag.

Note: The Installer must program your system to provide this feature, and you must agree with your alarm installer and the ARC what action the ARC should take on receiving a duress message.

- **Guard** – A guard user can only unset the system when it is in alarm and set it again. A guard user has no access to the user menu.

In a partitioned system, a guard user can be allocated to one or more partitions, which are the only parts of the system that they can set and unset.

- **Set Only** – This type of user can set the system, but not unset it. A set-only user has no access to the user menu.

In a partitioned system, a set-only user can be allocated to one or more partitions, which are the only parts of the system that the user can set.

- **Shunt Code** – This type of user code is used only for activating and deactivating shunt groups (see page 35). When the user's access code or proximity tag is used, all zones in the shunt group assigned to this user are shunted.
- **Easy Set** – This type of user unsets or sets the whole system (for a part-setting system) or all partitions allocated to the user (in a partitioned system). When the user's access code, proximity tag or remote control is used:

- In a partitioned system, if any partition assigned to the user is currently set, all are unset. In a part-setting system, if the system is part set, the whole system is unset.
- In a partitioned system, if all partitions assigned to the user are currently unset, all are set (even if there are alerts present). No partitions are set if any has an active zone. In a part-setting system, if the whole system unset, the whole system is set.
- **Level-4** – This type of user can be created only by the installer. A level-4 user is able to update the firmware and language files at the control unit using the web interface.

A level-4 user cannot set or unset the system, and is able to use the user menu only to change their own name and access code (to access the web interface).

User access codes

To set or unset the system or access the user menu, a user must identify themselves either by entering a valid access code at the keypad or by presenting a proximity tag. Access codes and proximity tags are unique to each user and can be used interchangeably at any time.

Users can also use a remote control to set or unset the system, or to operate outputs (depending on how the system is configured).

By default, the access code for the default master user is 1234 (for four-digit access codes) or 123456 (for 6-digit access codes). **It is recommended that you change the default master user code as soon as possible after system installation (see page 40).**

Code lockouts

If a user has problems remembering their code, or has acquired an unrecognised proximity tag, they may try keying in their code or presenting the tag several times. If this happens four times in a row, the control unit locks all keypads for 90 seconds and starts a "Excess Keys" tamper alarm. If configured, the control unit also sends the event to the Alarms Receiving Centre (AC).

Once 90 seconds has elapsed, the keypads allow users to try again. If an incorrect code or tag is used again, the keypad lock them out for a further 90 seconds, and so on.

Installer access

The installer has their own access code to access the installer menu options for system configuration.

There is only one installer access code. It cannot be used to set or unset the system or to access the user options.

Note: The installer may be able to call into your control unit and program it remotely (e.g. using the Downloader software or web interface). Depending on how your installer has programmed the system, you may receive a phone call from the installer to request access.

Eaton SecureConnect™

Eaton SecureConnect allows you to monitor and control your alarm system over the internet from your phone or tablet. Using the app, you can, for example:

- View the status of your system.
- Receive notifications of alarms or set/unset actions (even when the app is not open).
- View camera images generated by an alarm or other event.
- Set and unset the system.
- Switch outputs on or off.

For details of how to install and use SecureConnect, please refer to the *SecureConnect App User Guide*.

Chapter 2: Setting and Unsetting

Introduction

Readying the system to start an alarm when someone moves into a protected area is called “setting” the system. Disarming the system so that people can move freely is called “unsetting” the system.

You can set and unset your system using a variety of different methods, depending on how the installer has configured your system. This chapter explains typical methods used.

Note: The control unit can monitor some detectors continuously, irrespective of whether the system is set or unset. For example:

- Fire and smoke detectors, flood sensors, Hold Up Alarm buttons or emergency exits.
- Monitors for machinery (for example freezers) or other type of “technical alarm”.

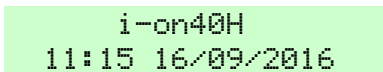
Using a keypad

This section explains how to set and unset your system from any keypad that has a display (including two-way radio keypads). If you are using a one-way radio keypad (which has no display), please refer to page 23.

Note: Please refer to page 6 for details of keypad features.

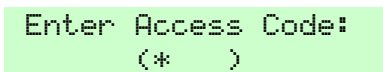
Setting the system

1. Make sure the display shows the standby screen; for example:



i-on40H
11:15 16/09/2016

2. Enter your access code or present your proximity tag to the keypad. If you enter your access code, the display shows a “*” for each digit:



Enter Access Code:
(*)

3. The bottom line shows the first setting option:

```
Setting Options  ↑  
A : Full Set
```

4. Press ▲ or ▼ followed by ✓ to select the option you require (refer to page 1 for details of part sets and partitions):

Full Set (part-setting system only)

To set the whole system.

Part Set B/C/D (part-setting system only)

To set part set B, C or D only.

Full Set All (partitioned system only)

To set all partitions fully. This is available only if all partitions are currently unset.

Part Set All (partitioned system only)

To part set all partitions. (This is available only if there are zones that the installer has given the Part Set attribute.)

Partitions (partitioned system only)

To choose the partition(s) to set, and whether to full set or part set those partitions.

5. If you selected *Partitions*:

- a) The bottom line shows the name of the first partition to which you have access and its current state (U = unset, S = full set, P = part set):

```
Partitions      ↑  
Partition 1    U
```

- b) Press ▲ or ▼ to select the partition you want to set.

- c) Press ► or ◀ to select the change you want:

```
Partitions      ↑  
Partition 2    U>S
```

“U>P” = change to part set

“U>S” = change to full set

“S>U” = change to unset

“P>U” = change to unset

Note: If a partition is full set, you cannot change it to part set or vice versa; you must unset the partition first.

Note: A zone is armed only when ALL of the partitions that it belongs to are set.

- d) Repeat steps b) and c) as required.
- e) Press ✓.

6. If you see a fault warning such as:

```
Tick to continue  
Batt 1 Low/Missing
```

- a) Press ✓ to override the warning and continue setting (if your installer has allowed this).
- b) Contact your installer for assistance.

7. You will hear a continuous exit tone (unless the system is configured for silent or instant setting).

If you have the final exit door open, or you trigger one of the detectors on your entry/exit route, the keypad gives an interrupted setting tone (this is normal).

The system sets when one of the following occurs, depending on how the system is configured:

- Immediately (instant set).
- After a specified period of time. You need to make sure you exit the premises before the exit timer expires. The bottom line shows the remaining time:

```
Setting:Partition 2  
23 to set
```

- When you have exited the premises and either pressed an exit-terminate button, closed the final door or operated a lock. The bottom line shows which of these methods is being used.

Note: You can press either the **⏏** or **✖** key to stop the system setting before it has set.

How do I know that the system is set?

When the system sets the keypad briefly shows:

```
System Set
```

After a short period, the standby screen is displayed. For example:

```
i-on40H  
11:15 16/09/2016
```

In a part-setting system, one of four LEDs (Figure 4) may glow to show which part of the system is set, unless disabled by the installer to meet appropriate standards.

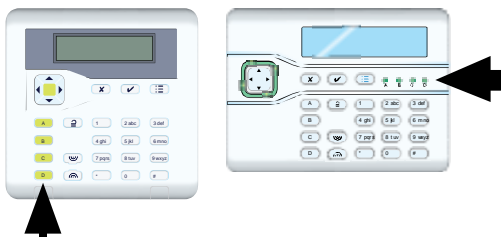


Figure 4. LED positions to indicate set/unset status

In addition, the installer may have configured the system to flash the strobe light briefly on the external siren/strobe unit when the system sets.

If the system does not set

If the system does not set, check the display to see if any zone is active. Normally, the system can set only when zones (other than those in the entry/exit route) are inactive. If there is more than one zone active, the display changes every three seconds to show each zone in turn.

Quick-setting the system using a keypad

Your installer may have enabled quick-setting, which removes the need to use an access code or proximity tag to start setting.

Note: To make the system comply with certain regulations, the installer may not be allowed to provide this facility.

To quick set (if enabled):

1. Press:
 - A – To set the system fully (part-setting system) or to set partition 1.
 - B – To set part set B (part-setting system) or to set partition 2.
 - C – To set part set C (part-setting system) or to set partition 3.
 - D – To set part set D (part-setting system) or to set partition 4.

2. You will hear a continuous exit tone (unless the system is configured for silent or instant setting). The system sets as described in step 7 on page 16.

Unsetting the system using a keypad

1. Enter through the entry route designated by the installer (this usually the same as you used to leave the premises). Do not stray from this route – you may cause an alarm.
2. Depending on how the system is configured, you may hear an entry tone. If you hear the tone, go directly to the keypad, since you will have limited time to unset the system before it generates an alarm.
3. Enter your access code or present your proximity tag to the keypad. If you enter your access code, the display shows a “*” for each digit:

```
Enter Access Code:  
(*  )
```

4. If you are using a partitioned system:
 - a) The bottom line shows the name of the first partition to which you have access and its current state (U = unset, S = full set, P = part set):

```
Partitions      ↑  
Partition 1    S
```

- b) Press ▲ or ▼ to select the partition you want to unset.
- c) Press ► or ◀ to select the change you want:

```
Partitions      ↑  
Partition 1    S>U
```

“U>P” = change to part set
“U>S” = change to full set
“S>U” = change to unset
“P>U” = change to unset

- d) Repeat steps b) and c) as required.
 - e) Press ✓.
5. The system unsets.

6. If you see a fault warning such as:

```
Tick to continue  
Batt 1 Low/Missing
```

- a) Press ✓ to acknowledge the warning.
- b) Contact your installer for assistance.

Using a two-way keyfob-style remote control

The two-way remote control (Figure 5) can be used to set and unset the system, query the current set/unset status of the system or operate a User-Defined output. Each remote control has a unique electronic identity and is assigned (page 37) to a specific user.

The remote control is designed to provide feedback about the current status of the system (if enabled by the installer). When you operate the buttons, the control unit sends back signals that light up one or more LEDs on the fob. These show whether your system has set, or if there has been an alarm while you have been away.

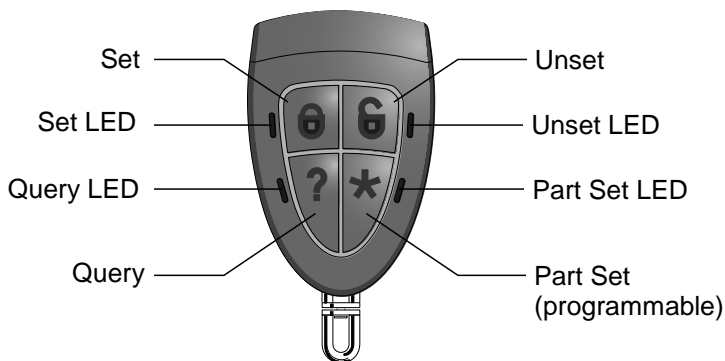


Figure 5. Two-way remote control buttons

In a partitioned system, the remote control can be used for only one partition (see page 37).

The installer can use a *2W Set Instant* option choose whether the remote control should set instantly or follow the configured exit mode (such as a timed set).

Operating the buttons

To ensure that the remote control does not accidentally operate while it is in your pocket, the buttons are deliberately slow to respond to pressure.

You must hold down the button you intend to press for at least three seconds to activate its function.

See page 57 for details of programming the * button.

Setting the system

1. Make sure the system is in standby.
2. Press and hold the Set or Part Set button, as required. The Set or Part Set LED flashes red three times.

If there is a fault (for example a zone is active), all four LEDs glow red for three seconds.
3. You will hear a continuous exit tone (unless the system is configured for silent or instant setting). The system sets as described in step 7 on page 16.
4. The Set or Part Set LED glows green for three seconds. This is your confirmation that the control unit has set the system.

Unsetting the system

Note: An administrator can disable the ability for remote controls to unset the system (see page 60).

To unset the system:

1. Enter through the entry route designated by the installer.
2. Depending on how the system is configured, you may hear an entry tone. If you hear the tone, you will have limited time to unset the system before it generates an alarm.
3. Press and hold the Unset button. The Unset LED flashes red three times.
4. The Unset LED glows green for three seconds. This is your confirmation that the control unit has unset the system.

Querying the set/unset status

1. Press and hold the Query button. The Query LED flashes red three times.
2. The Full Set, Part Set or Unset LED glows to show the current status of the system.

Starting a Hold Up Alarm (HUA)

A two-way remote control can be used to start a Hold Up Alarm if enabled by an installer and by a master or admin user (see page 61).

Note: Enabling this feature means that the system no longer complies with BS8243 or DD243.

To start a HUA from a two-way remote control:

1. Press and hold any two diagonally opposite buttons at the same time. All four LEDs flash red three times.
2. The control unit starts a hold up alarm and, if applicable, sends the alarms to the Alarms Receiving Centre (ARC).
3. All four LEDs glow green for three seconds. This is your confirmation that the control unit has generated the alarm.

Using a one-way remote control

The one-way remote control has four buttons and a small LED that glows when it transmits a signal (see Figure 6). The buttons can be programmed as required (see page 57), but by default, three of the buttons are used to set or unset the system.

Note that to prevent accidental operation the user must hold a button down for at least two seconds to ensure a transmission.

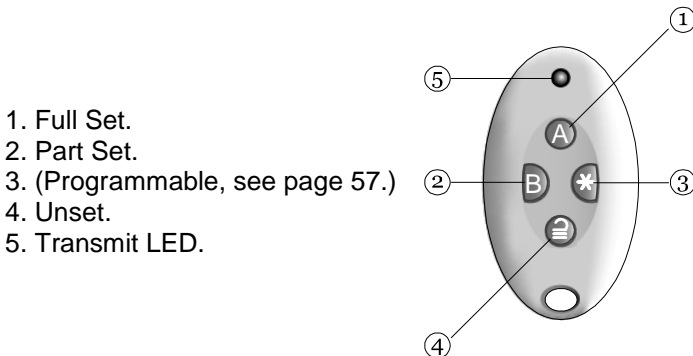


Figure 6. Default one-way remote control buttons

Each remote control has a unique electronic identity. You can assign (see page 37) only one remote control to each user.

Setting the system

1. Make sure the system is in standby.
2. Press the required button on the remote control. For example, Full Set (A) or Part Set (B).

In a partitioned system, the default action is to full set or part set all of the user's partitions.

3. You will hear a continuous exit tone (unless the system is configured for silent or instant setting). The system sets as described in step 7 on page 16.


If the system will not set

If one of the zones is active when you try to set the system, you will not hear the exit warning tone. Instead, you will hear a single beep.

Try pressing A again on your remote control. If set up by the installer, the system will omit the active detector and set. If the system does not set, you will need to go to a keypad and investigate why the system will not set.

Unsetting the system

Note: An administrator can disable the ability for remote controls to unset the system (see page 60).

1. Enter through the entry route designated by the installer.
2. Depending on how the system is configured, you may hear an entry tone. If you hear the tone, you will have limited time to unset the system before it generates an alarm.
3. Press  on your remote control.

Using a one-way radio keypad

A one-way keypad (Figure 7) does not have a display and can only transmit to the control unit (it cannot receive information back from the control unit).

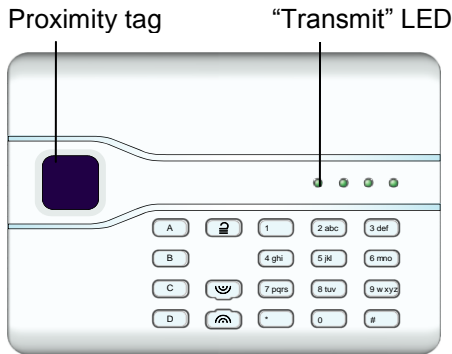


Figure 7. One-way radio keypad

The keypad cannot show the status of the system. The left-hand “Transmit” LED glows only to show that the keypad is sending a command to the control unit.

Setting the system

1. Make sure the system is in standby.
2. Enter a valid access code or present your proximity tag to the keypad.
3. Press:
 - A – To set the system fully (part-setting system) or to set partition 1.
 - B – To set part set B (part-setting system) or to set partition 2.
 - C – To set part set C (part-setting system) or to set partition 3.
 - D – To set part set D (part-setting system) or to set partition 4.
4. You will hear a continuous exit tone (unless the system is configured for silent or instant setting). The system sets as described in step 7 on page 16.

Unsetting the system

1. Enter through the entry route designated by the installer.
2. Depending on how the system is configured, you may hear an entry tone. If you hear the tone, go directly to the keypad, since you will have limited time to unset the system before it generates an alarm.
3. Enter your access code or present your proximity tag to the keypad.
4. Press **2**.

Using SMS command messaging

Using a mobile phone or other messaging device, you can send SMS messages to the control unit to set/unset the system, activate/deactivate outputs, omit/un-omit zones or query the current status of the system.

Please refer to the "SMS Command Messaging User's Guide" for further information.

Chapter 3: Managing Alarms

Alarm types and sounds

An alarm may occur for several different reasons. For example:


- A zone is triggered when the system is set (intruder alarm).
- The lid of the control unit or other device has been opened without the installer being logged in (tamper alarm).
- After entering the premises, a user has failed to unset the system in sufficient time.
- A fire detector is activated.
- A Hold-Up Alarm (HUA) device is activated.
- The mains supply has failed.
- There is a failure of a communications link from the control unit.

When an alarm occurs, the control unit normally activates internal sounders and, depending on severity, external siren/strobe units. Table 1 shows the default response for each type of alarm.

After an alarm, you will need to silence the sounders, acknowledge the alarm and reset the system (see "Silencing, acknowledging and resetting alarms" on page 26).

Table 1: Alarm sounds

Alarm	Sound	Cause
Intruder	Loud warbling tone from siren.	Normal alarm or entry route zone activated when system is set. 24-hour zone activated at any time.
Fire	Pulsing tone from sirens, internal sounders and wired keypads.	Fire zone activated at any time.

Hold Up	Loud warbling tone from siren.	HUA zone or radio Hold Up Alarm transmitter activated at any time.  Pressed on keypad. The installer must enable this feature.
Tamper	Loud warbling tone from siren.	Some part of the alarm system has been opened (tampered with). An alarm system cable has been cut or shorted. An incorrect user code has been entered too many times.
Technical	Quiet beeping once per second from wired keypads.	Technical alarm zone activated at any time. (Audible only when system is unset.)
Fault	Quiet beeping once per second from wired keypads.	A system fault detected by the control unit, such as a mains failure or communications line fault. See page 29.

Other alarm actions

In addition to sounding internal sounders and external siren/strobe units, the control unit may (depending on how the installer has configured the system) carry out other actions, such as to:

- Operate output devices, such as lights.
- Save recorded camera images.
- Send an alarm message to an Alarms Receiving Centre (ARC), who may decide to call the police or other security service to investigate the alarm.
- Send an alarm report by email or SMS text message to specified recipients.
- Send a pre-recorded speech message to specified phone numbers, as described next.

Speech messages

Note: This facility requires the control unit to have an appropriate communications module fitted.

As well as making an audible signal, the installer can configure the control unit to send a pre-recorded voice message to specified phone numbers when an alarm occurs. These messages can go to people nominated to monitor alarm calls.

If the control unit has Call Acknowledge enabled (ask the installer), a person receiving a speech message can control the link by pressing buttons on their telephone keypad. The commands available are as shown in Table 2.

Table 2: Speech message acknowledgement

Function	Key
End this call and let the control unit contact the other nominated persons for this alarm.	5
Play message again.	3
Clear down and do not call any of the other nominated persons for this alarm.	9

Note: When a recipient answers a speech message, there is a six-second delay before the control unit starts the message.

Silencing, acknowledging and resetting alarms

If there is an alarm, you will need to silence the sirens and sounders (if they are still running), acknowledge the cause of the alarm and reset the system.

Note:

- By default, sirens run for a maximum of 15 minutes. If this period has expired, the system may be silent, but you will still need to acknowledge and reset the alarm.
- See "Viewing alerts" on page 29 if the keypad is beeping approximately once per second.

To silence, acknowledge and reset an alarm:

1. **Make sure that it is safe to enter the premises.**
2. Enter your access code or present your proximity tag to the keypad. This silences the alarm (if the sirens and sounders are still operating).

Note: In a partitioned system, you can silence, acknowledge and reset an alarm only if it has been caused in a partition to which you have access.

3. The navigation key glows red and the bottom line of the display shows the first zone to alarm. For example:

```
Press tick to reset
Burg Z041 Alarm
```

OR, for example:

```
Call Installer
Tamper W1-04
```

The bottom line alternates once a second to show the name of the zone or device that generated the alarm. For example:

```
Press tick to reset
Back door
```

4. Press to indicate that you have acknowledged the alarm message. The system returns to standby and is ready to set again.
5. If the alarm message included "Press tick to reset" (see above), acknowledging the alarm also resets the system and the navigation key returns to its normal (green) state.

If the alarm message included "Call Installer" (see above) or "Call ARC", you will need to call the installer or ARC to reset the system (as described in the next section), although you will still be able to set and unset the system normally. The navigation key glows red until the alarm is reset.

Note:

- If the alarm was started by accident, see "Accidental alarms" on page 29.
- In a partitioned system, some tamper alarms may need to be silenced in more than one partition.

- The control unit saves alarm information in the log. See page 41 for details of how to view the log.

Installer resets

If the alarm requires an installer reset, there are several ways that this can be accomplished:

- The installer can visit your site and reset the system by entering the installer code and exiting the installer menu.
- If a suitable communicator is enabled, the ARC can send a signal to the control unit to allow you to reset the system yourself.
- If configured by the installer, the ARC can give you a special code for you to reset the system yourself. If this method is enabled, you will see a message similar to the following while acknowledging an alarm:

```
CALL ARC, Quote 4321  
*****
```

1. Note down the 4-digit number ("4321" in this example).
2. Press ✓ to clear the message. The display returns to normal.
3. Call the ARC and quote the 4-digit number.
4. If satisfied with your identity, the ARC provides a reset code.
5. Enter the reset code at the keypad to reset the alarm.

Accidental alarms

Your installer may have configured your system so that if you set off an alarm accidentally, you have an "Abort Time" (by default 120 seconds) in which to cancel the alarm. Go immediately to a keypad and enter your access code. If you do this within the Abort Time, the system will send an "Alarm Abort" message to the ARC (if used).

If the alarm is cancelled after the Abort Time, immediately call any ARC the control unit communicates with to notify them of the accident.

Viewing alerts

An alert is an event that is not directly related to an intrusion event, such as a low battery, a communications fault or an active "Technical Alarm" zone (which is often used to monitor equipment such as freezers).

An alert does not cause the external siren/strobe unit to operate or the keypads to give a continuous alarm sound. Instead, the navigation key on

keypads glow red if the system is unset, and keypads give a short "beep" approximately every second if the alert has not already been acknowledged.

To view the cause of the alert:

1. Make sure the system is unset and that the keypad shows the standby screen.
2. Before entering your access code, press ✓.
3. Enter your access code or present your proximity tag to the keypad.

The bottom line displays the most recent alert. For example:

```
Tick to continue  
Batt 1 Low/Missing
```

OR, for example:

```
Press tick to reset  
P1:Zone 041
```

The bottom line may alternate between displaying the zone number and name (if applicable).

4. Press ✓ to acknowledge that you have read the alert.
Repeat this step for any other alerts that may be active.
5. If you see a message similar to the following:

```
RESET FAULTS  
Z041 Zone 041
```

This indicates that the alert has been caused by a Technical Alarm zone type and the detector is still active. If you can, rectify the problem and repeat the procedure to reset the alert. Alternatively, press ✓ to continue (repeat the procedure when you have rectified the problem).

6. The standby screen is displayed and the beeping stops. The navigation key continues to glow red until the faults are rectified.

Chapter 4: User Menu Options

This chapter explains all options that are available to through the user menu. You can access the menu by pressing **≡**: and entering your user access code.

User Menu Map

This chapter shows all options in the user menu, and the availability depending on the user type. Some options may not be visible, depending on the hardware fitted.

<u>MENU Option</u>			Master Users	Admin Users	Normal Users	Partition Users	Level-4 Users
Omit Zones			✓	✓	✓	✓	
Shunt Group			✓	✓			
Users	Add User		✓	✓			
	Edit User	Name	✓	✓			✓
		Type (not U001)	✓	✓			
		Partitions (partitioned system)	✓	✓			
		App access	✓	✓	✓	✓	
		Code	✓	✓	✓	✓	✓
		Prox Tag	✓	✓	✓	✓	
		Remote	✓	✓	✓	✓	
	Hold Up Alarm	✓	✓	✓	✓		
Delete User		✓	✓				
View Log			✓	✓	✓	✓	
Test	Siren & Sounders	Ext. Radio Sirens	✓	✓			
		Wired Sirens	✓	✓			
		Loudspeakers	✓	✓			
		Wired Keypads	✓	✓			

User Menu Options

		KEY-RKPZ	✓	✓				
		Internal Sounders	✓	✓				
	Wired Keypad		✓	✓				
	Walk Test	Chime	✓	✓				
		System	✓	✓				
		Partitions	✓	✓				
		Zones	✓	✓				
	Outputs		✓	✓				
	Remotes		✓	✓				
	User HUAss		✓	✓				
	Prox Tags		✓	✓				
	ARC Reporting	Tel No 1	✓	✓				
		Tel No 2	✓	✓				
System Config	Facilities On/Off	Chime	✓	✓	✓	✓		
		Remote Access	✓					
		Level 4 Updates	✓	✓	✓	✓		
	Set Date & Time		✓					
	Calendar Set	Add Event		✓	✓			
		Edit Event	Event name	✓	✓			
			Event time	✓	✓			
			Event day	✓	✓			
			Ward/Partitions	✓	✓			
			Warning time	✓	✓			
			Warning tone	✓	✓			
		Delete event		✓	✓			
		Add Exception		✓	✓			
		Edit Exception	Exception Name	✓	✓			
	Exception Start Time		✓	✓				
	Exception Start Date		✓	✓				
	Exception End Time		✓	✓				
Exception End Date	✓		✓					
Delete Exception		✓	✓					
Contacts		✓						
Edit Outputs		✓	✓					
Remotes		✓	✓					

	Call Downloader	✓				
Outputs On/Off		✓	✓	✓	✓	
About	Panel	✓	✓			
	Cloud	✓	✓			
	Expanders	✓	✓			
	Keypads	✓	✓			
	Comms	✓	✓			
Pair App		✓	✓			

Entering and exiting the user menu

To access the user menu:

1. Make sure the display shows the standby screen. For example:

```
i-on40H
11:15 16/09/2016
```

2. Press ⏏ . The following is displayed:

```
Enter Access Code:
( )
```

3. Enter your access code. The first option is displayed:

```
MENU
Omit Zones
```

4. Press \blacktriangle or \blacktriangledown to scroll through the options, followed by \checkmark to select the option you require. Refer to the following sections for information about each option.
5. To leave the menu and return to the standby screen, press \times (if necessary several times).

Entering text

You can enter text at the keypad by pressing a key one or more times to obtain the letter you require. The letters of the alphabet appear on the keys in the same arrangement as on many mobile phones (see Figure 8). For example, to enter a "b", press the "2" key twice, or to enter an "f", press the "3" key three times. Wait a few moment before each new letter.

Press # to change between capitals and lower case letters. The cursor is an underline for small letters and a block for capitals.

Press ▲ to move the cursor left, or ▼ to move the cursor to the right.

Press ◀ to remove letters to the left of the cursor. Press ▶ to insert a space.

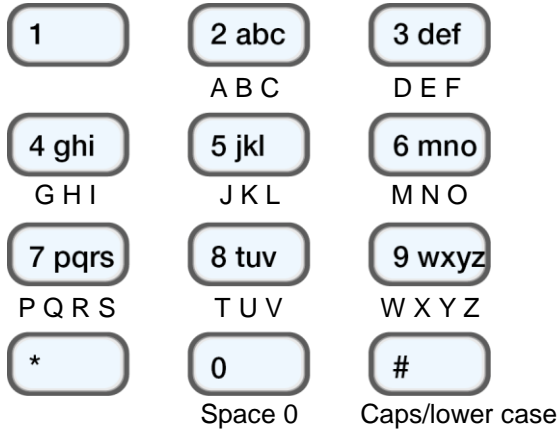


Figure 8. Letters assigned to keys

Omitting zones

This option allows you to omit one or more zones. Omitting a zone prevents it from generating an alarm if the zone is triggered while the system is set. For example, if a zone protects a garage door, you may want to omit the zone to enable the delivery of a parcel while the system is set.

Note: The control unit un-omits the zones when the system is unset. If you want to keep a zone omitted, you have to omit the zone again before you next set the system. Alternatively, use shunt groups (see the next section).

Note: You can omit only those zones that the installer has given the Omittable attribute.

To omit zones:

1. Select *Omit Zones*. The bottom line displays the first zone you can omit:

```
OMIT ZONES  
Zone 001      I
```

An "O" is displayed at the end of the line if the zone is Omitted. An "I" is displayed if the zone is Included.

2. Press ▲ or ▼ to display the zone you wish to omit, then ► to mark it for omission. Press ► again if you made a mistake and want the zone to be included.

Repeat this step for any other zones you wish to omit (or change to be included).

3. Press ✓ to store changes.

Using shunt groups

About shunt groups

A shunt group is a collection of zones that can be “shunted”. “Shunting” is another way of preventing a zone from causing an alarm. The difference between shunting and omitting a zone is the length of time that the control unit ignores the zone. When you omit a zone (see the previous section), the control unit ignores it for one setting/unsetting cycle. When you shunt a zone, the control unit ignores it until you unshunt it.

The installer sets up the shunt groups, each of which can consist of one or more zones. You should agree with the installer what zones need to go into each shunt group, and record that information. A zone can be in more than one shunt group.

Once the shunt groups are defined, there are three ways of shunting them:

- a) Master and admin users can use the *Shunt Groups* option to shunt all zones in selected shunt group. A master user can select any shunt group. In a partitioned system, an admin user can select any shunt group in the same partition as the admin user.
- b) A master user can use the *Users – Add User* option to add a Shunt Code user type and assign a shunt group to that user. When the code is used at a keypad, all zones in the shunt group are shunted. When the code is used again, the zones are unshunted.
- c) The installer can fit a key switch to a special zone, and link the zone to one or more shunt groups. Turning the key shunts all zones in the shunt groups. Turning the key again unshunts them.

When a user tries to set the system or a partition where zones are shunted, the keypad displays “Shunt Active tick to continue”. If the user presses ✓, the system continues to set.

Activating or deactivating a shunt group

A master or admin user can activate or deactivate a shunt group from a keypad as follows:

1. Select *Shunt Groups*. The first shunt group set up by the installer is displayed:

```
ACTIVE SHUNT GROUPS
Shunt Group 1 Yes
```

2. Press ▲ or ▼ to select the shunt group.
3. Use ► to change the setting to Yes (zones in shut group will be shunted) or No (zones will be unshunted).
4. Press ✓ to confirm the change.

Managing users

Selecting *Users* from the main menu has two functions, depending on your user type:

- a) If you are a normal or partition user, you can use the *Users* option to:
 - Change your access code.
 - Add or delete your own proximity tag, remote control or radio Hold-Up Alarm (HUA) transmitter.
 - In a partitioned system, specify the partitions that a two-way remote control can set, unset, etc. (not available for a one-way remote control).

These tasks are described in the next section.

- b) If you are a master or admin user, the *Users* option displays additional options that allow you to:
 - Add new users to the system, including the proximity tag, remote control and HUA transmitter allocated to each user (*Users – Add User*). See page 37.
 - Edit user details (*Users – Edit User*). See page 40.
 - Delete users (*Users – Delete User*). See page 41.

Changing your access code or assigned devices

This section applies if you are a normal or partition user. If you are a master or admin user, you will need to use *Users – Edit User* to carry out these tasks (page 40).

To change your access code or assigned devices:

1. Select *Users* from the main menu.
2. Press ▲ or ▼ followed by ✓ to select one of the following options (refer to "Adding users" on page 37 if you need information):

<i>Code</i>	To change your own access code.
<i>Prox Tag</i>	To add or delete your own proximity reader tag.
<i>Remote</i>	To add or delete your own remote control. If you are using a partitioned system and a two-way remote control, you can also use a <i>Remote Partition</i> option to specify the partition that the remote control can set, unset, etc. Use ▲ or ▼ to scroll through the partitions, and ► to choose Yes or No. Press ✓ on completion. You should delete your remote control if it has been lost.
<i>Hold Up Alarm</i>	To add or delete your own Hold-Up Alarm (HUA) device.

3. Follow the prompts.

Adding users

If you are a master or admin user, you can use *Users – Add User* to add new users. When adding a new user, you can:

- Specify the user's name, type, partitions and access code.
- Assign a proximity tag, remote control and radio Hold Up Alarm (HUA) transmitter. If you do not wish to assign these devices, each user can assign those devices to themselves at a later date using the *Users* option.

Each user can have only one proximity tag, remote control or HUA transmitter. No two users can have the same device.

A Duress user cannot have a remote control or HUA transmitter.

To add a new user:

1. Select *Users – Add User*.
2. The next available default user name is displayed:

```
Name :  
User 004
```

If you wish, edit this default name of the user (12 characters maximum). If required, please refer to page 33 for details of how to edit text. Press to continue.

3. The default user type is displayed (normal user):

```
User 004  
Normal User
```

Press or to select the user type (see page 10). Press to continue.

4. If you are using a partitioned system, and are adding a user other than a master user or Shunt Code user, you are prompted to specify the user's partitions:

```
USER 004  
Partition 1 Yes
```

By default, a new user belongs to all partitions. Press or to scroll through the partitions and to change the setting to Yes or No. Press to continue.

5. You are prompted to specify an access code for the user:

```
Assign Access Code  
( )
```

Enter an access code, or if you do not want to assign one. When prompted, enter the code a second time.

6. You are prompted to assign a proximity tag to the user:

```
Present Prox Tag to  
add to panel
```

Present an unallocated tag to the keypad until you see "Prox Tag added", or if you do not want to assign one.

Note: If you have a proximity tag that is already allocated, you can find out who it belongs to by using *Test – Prox Tag* (page 42).

7. For user types that can set the system, you can assign a remote control that is not already assigned to another user:

```
Press button to  
identify Remote
```

To assign a remote control, press any button on the remote control, then (if you are using a partitioned system), choose one partition to assign to the remote control.

If you do not want to assign a remote control, press ✓ at the above prompt.

Note: If you have a remote control that is already allocated, you can find out who it belongs to by using *Test – Remotes* (page 42).

8. For user types that can set the system, you can assign a radio HUA (Hold-Up Alarm) device:

```
Press both buttons  
to identify HUA
```

Press a button on an unallocated HUA transmitter until you see "HUA added", or ✓ if you do not want to assign one.

Note: If you have an HUA transmitter that is already allocated, you can find out who it belongs to by using *Test – Hold Up Alarms* (page 42).

Note: While you are registering a new HUA transmitter, the control unit will not respond to an alarm signal from any radio HUA it has already learnt.

9. If you are adding a Shunt Code user, press ▲ or ▼ followed by ✓ to select the shunt group to assign to the user:

```
User 005  
*Shunt Group 1
```

The * indicates the currently-selected shunt group.

10. The control unit confirms that the user has been added:

```
New User Added
```

Editing users

If you are a master or admin user, you can use *Users – Edit User* to:

- Change the name of existing users, and for users other than master users, also the user type (page 37) and allocated partitions. If you are an admin user, you can edit only those users who belong to the same partitions as you.
- Change your own access code.
- Add or delete your own proximity tag, remote control or HUA transmitter. If you want to delete another user's remote control, see "Deleting remote controls" on page 60.

Note: You cannot edit a user when the partition they belong to is set.

Note: If a user forgets their code, a master user or admin user must delete that user and recreate a new user with a new code.

To edit a user:

1. Select *Users – Edit User*.
2. Press ▲ or ▼ followed by ✓ to select the user you wish to edit. Alternatively, enter the user number (e.g. 004) and press ✓.
3. Press ▲ or ▼ followed by ✓ to select the option you require:

<i>Name</i>	To change the user name.
<i>Type</i>	To change the user type. You cannot change the type of a master user.
<i>Partitions</i>	To change the partitions that the user belongs to (partitioned systems only). You cannot change the partitions allocated to a master user, since master users always belong to all partitions. Every user must belong to at least one partition.
<i>App access</i>	To enable or disable use of the SecureConnect™ mobile app. Please refer to the <i>SecureConnect App User Guide</i> .
<i>Code</i>	To change your own access code.
<i>Prox Tag</i>	To add or delete your own proximity tag.
<i>Remote</i>	To add or delete your own remote control.
<i>Hold Up Alarm</i>	To add or delete your own HUA transmitter.

4. Follow the prompts. Please refer to "Adding users" on page 37 if you need information about how to use any of the above options.

Deleting users

If you are a master or admin user, you can use the *Users – Delete User* option to delete users.

Once you delete a user, the system does not respond to their access code. The control unit also deletes the identity of any proximity tag, remote control or HUA transmitter assigned to the user.

Note: You cannot delete User 001 (the default master user).

To delete a user:

1. Select *Users – Delete User*.
2. Press ▲ or ▼ followed by ✓ to select the user you wish to delete. Alternatively, enter the user number (e.g. 004) and press ✓.

You will see (for example):

```
DELETE User 004
Are you sure?
```

3. Press ✓ to delete the user (or ✕ if you have changed your mind).

Viewing the log

The control unit keeps a log of events such as alarms and setting/unsetting actions. You can view the log as follows:

1. Select *View Log* from the main menu.

The display shows the most recent event, for example:

```
*U001 Ptn 1 Unset
10:52:07 01/08/2016
```

When applicable, the event includes the associated user number (001 in the above example), as described in the next section.

2. If applicable, press ► to see a more detailed description of the event, such as the user name (rather than user number) associated with the event.

If you need information about a log event, please contact your installer.

3. Press ▼ to show older events, or ▲ to show more-recent events.
4. Press ✕ to finish viewing the log.

User numbers

The control unit identifies each user by a unique number as shown below.

Meaning	User Number	
	i-on30R	i-on40H
Action by installer	000	000
Action by default master user	001	001
Action by other added user	002-030	002-050
Quick Set (A/B/C/D key used)	031	051
Action by Level 4 user	032	052
Action by control unit	033	053
Keyswitch zone used to set/unset	034	054
Remote reset carried out by ARC	035	055
Action through Downloader software	036	056
Action through virtual keypad	037	057
Action through SMS command	040	060
Action through mobile app	041	061
Action through web interface	"Web"	"Web"

Testing the system

A master or admin user can use the *Test* option to test various components of the system, and to check the current owner of a proximity tag, remote control or HUA transmitter.

Testing sirens and sounders

To carry out the test:

1. Select *Test – Sirens & Sounders*.
2. Press ▲ or ▼ followed by ✓ to select the devices to test:
Ext. Radio Sirens External radio sirens and their strobes.

<i>Wired Sirens</i>	Wired sirens and their strobes.
<i>Loudspeakers</i>	Extension loudspeakers.
<i>Wired Keypads</i>	Sounders in wired keypads.
<i>KEY-RKPZ</i>	Sounders in KEY-RKPZ two-way radio keypads.
<i>Internal Sounders</i>	SDR-RINT internal radio sounders.

3. Press ▲ or ▼ to select whether to operate all sirens\sounders of the selected type, or (for partitioned system only) only those assigned to a specific partition. Press ► to switch the sirens\sounders on, and ► again to switch them off.
4. Press ✕ to finish the test.

Testing a wired keypad

Note: You can test only the keypad you are currently using (you cannot test a keypad remotely).

To carry out the test:

1. Select *Test – Wired Keypad*.

The bottom line of the display shows the keypad name and bus address. For example:

```
Press keys to test:  
KP 51 :Keypad K1-51
```

All four ABCD LEDs and LEDs around the navigation keys should glow red.

2. Press ▲, ▼, ► and ◀ in turn to test the navigation keys. Each time you press a key, the LEDs should change colour and the display show the key you pressed.
3. Press both HUA keys at the same time. The display should confirm that you pressed the HUA keys. An HUA alarm is not generated.
4. Press any other key to test it. The display should confirm the key you pressed.
5. Press ✕ to finish the test.

Performing a walk test

Master and admin users can use *Test – Walk Test* to test detectors without starting an alarm. Walking past motion detectors should be enough to trigger them. If you have detectors connected to doors or windows, you will have to open them to trigger those detectors.

During the test, if the detector is working, the control unit sounds a confirmation tone and indicates that the detector has passed the test.

Note: You cannot test wired HUA buttons, fire detectors, and 24-hour zones during a walk test. The control unit will always start an alarm if you activate those detectors.

To carry out the test:

1. Select *Test – Walk Test*. The following is displayed:

```
WALK TEST
Chime      Once
```

2. Press ◀ or ▶ to select one of the following:

Once Causes keypads and loudspeakers to chime only once for each zone that is triggered during the walk test.

On Generates a chime every time a zone is triggered.

Off Switches off chiming.

3. Press ▲ or ▼ followed by ✓ to select the method of testing:

System This option allows you to walk round the entire system and test all the zones.

Partitions (Partitioned systems only.) This option allows you to select one or more partitions, and test only the zones within those partitions.

Press ▲ or ▼ to scroll up or down the list of partitions, and ▶ to display “Yes” at the end of the bottom line to mark the partition as one you want to test.

Zones This option lets you select one or more individual zones, and test only those zones.

Press ▲ or ▼ to scroll up and down the list of zones. Press ▶ to display “Yes” at the end of the bottom line to mark the zone as one you want to test.

4. Press **✓** to begin the test.

The top line shows how many detectors remain to be tested. The bottom line provides a list of all the detectors ready for testing (press **▲** or **▼** to scroll through the zones):

```
10 Zone(s) to test
Zone 040
```

5. Walk round and trigger each detector in turn. If you have enabled *Chime*, the keypads and loudspeakers give a double-tone chime when you trigger a detector.

You can see which zones still need to be tested by pressing **▲** or **▼** to scroll through the zones: an "A" is shown at the end of the bottom line for each zone that has been tested. Alternatively, you can press **≡**: and scroll through the untested zones (press **≡**: again to continue with the test).

6. If you wish, you can press **✕** to finish the test early.
7. Once all zones are tested, you will see (for example):

```
All Zones tested
Zone 040          A
```

Testing outputs

Master and admin users can use *Test – Outputs* to test outputs the installer has configured as "User Defined". The outputs may be used to control external devices, such as lights or locking equipment.

Note: You can activate or deactivate user-defined outputs at any time (see page 62).

To carry out the test:

1. Select *Test – Outputs*.

The display shows the first in a list of any user-defined outputs allocated for your use. For example:

```
TEST O/P PAN>01 W
PORCH LIGHT      Off
```

The top line shows the address and type of the output. In the above example, the address is PAN>01 and the type is W (wired). The

bottom line shows the name of the output (which may be the same as the address) and whether the output is currently on or off.

2. Press ▲ or ▼ to select the output.
3. Press ► to switch the output on, and ► again to switch it off. Check that the output is working as expected. Outputs operated via radio may take several seconds to change state.
4. Press ✓ to end the test.

Testing remote controls

Master and admin users can use *Test – Remotes* to test remote controls.

To carry out the test:

1. Select *Test – Remotes*.

The following is displayed:

```
Press required  
Remote button
```

2. Press and hold a button on the device you wish to test until the transmit LED on the device flashes.

The keypad gives a double-beep confirmation tone and you will see the results of the test:

```
RM001,B1:User001  
Full Set All SS:9
```

The top line shows the number of the device, the button you pressed, and the name of the user the device is allocated to. The bottom line shows the function of the button and the strength of the signal. If the signal strength is less than 4, contact your installer.

3. Repeat step 2 for the other buttons. **Note:** If you wish to test the Hold-Up Alarm buttons, make sure you press them both at the same time.
4. Press ✓ to end the test.

Testing user HUAs

Master and admin users can use *Test – User HUAs* to test radio Hold-Up Alarm (HUA) devices.

To carry out the test:

1. Select *Test – User HUAs*.

The following is displayed:

```
Press both HUA  
buttons
```

2. Press and hold both HUA buttons on the device you wish to test until the transmit LED on the device flashes. If the device has a lock button, make sure you unlock the button before the test.

The keypad gives a double-beep confirmation tone and you will see the results of the test:

```
User: User002  
SS:9
```

The top line shows the name of the user the device is allocated to. The bottom line shows the strength of the signal. If the signal strength is less than 4, contact your installer.

3. Repeat step 2 for the other HUA devices.
4. Press ✓ to end the test.

Testing proximity tags

Master and admin users can use *Test – Prox Tags* to test proximity reader tags.

To carry out the test:

1. Select *Test – Prox Tags*.

The following is displayed:

```
TESTING PROX TAGS  
Present Tag to Panel
```

2. Hold the proximity tag against the front of the keypad.

The keypad gives a double-beep confirmation tone and you will see the results of the test:

```
TESTING PROX TAGS
User: User 001
```

The bottom line shows the name of the user the proximity tag is allocated to (or "Unknown" if the proximity tag is not recognised).

3. Repeat step 2 for the other proximity tags.
4. Press ✓ to end the test.

Testing ARC reporting

Master and admin users can use *Test – ARC Reporting* to test the connection to Alarms Receiving Centres (ARCs).

To carry out the test:

1. Select *Test – ARC Reporting*.

The following is displayed:

```
ARC REPORTING
Panel Ethernet
```

2. Use ▲ or ▼ to choose the communication method you want to test, then press ✓. The ARC may use Ethernet (*Panel Ethernet*), GSM or PSTN (the latter two require the control unit to have an appropriate plug-on module fitted).

Note: The installer may have configured more than one communication method to the ARC: Ethernet and GSM, or Ethernet and PSTN. The installer specifies which of the two methods has the highest priority. During normal operation, the control unit uses the method that has the highest priority, and uses the second method only if the first fails.

The following is displayed:

```
ARC REPORTING
Recipient A <Tel 1>
```

3. Use ▲ or ▼ to choose one of the two recipients selected by the installer. Each recipient is a separate telephone number or IP address to the ARC. Depending on how the installer has configured

communications, the second line or IP address may be used if the first fails to connect.

4. Press ✓ to start the test.

```
Test call started...
```

The keypad shows the progress of the call. Check with the ARC that the test call arrived. If the call fails, the display shows “Call failed”, followed by the reason.

System configuration

The *System Config* menu allows you to change some parts of the system to suit your particular needs.

Note: For normal and partition users, the *System Config* menu contains only the *Chime* and *Level 4 Update* options (see below).

Switching facilities on/off

System Config – *Facilities On/Off* can be used to switch the following facilities on or off:

- | | |
|-----------------------|---|
| <i>Chime</i> | Use this option to enable or disable the chimes that occur when a zone is triggered that has a Chime attribute (as set up by the installer). For most zone types, a chime occurs only when the system is unset. |
| <i>Remote Access</i> | <p>A master user can use this option to enable or disable remote access to the control unit from the web interface or Downloader software.</p> <p>Note: By default, this feature is off for security reasons. Make sure that any installer requesting access is your authorised installer. Switch off remote access once the installer has finished.</p> <p>Note: If you turn remote access off, you can still make the control unit start a call out to an installer who is using the Downloader software (see page 61).</p> |
| <i>Level 4 Update</i> | Use this option to enable or disable access to the control unit from the level-4 user. There can be only one level-4 user, which only the installer can create. |

The level-4 user is able to:

- a) Update the firmware and language files at the control unit using the web interface.
- b) Log into the user menu or web interface and change the level-4 user name and code.

The level-4 user cannot perform other tasks, such as to set or unset the system, omit zones, etc.

To switch facilities on or off:

1. Select *System Config – Facilities On/Off*.
2. Use ▲ or ▼ to choose the facility, then ► or ◀ to switch it on or off.
3. Press ✓.

Setting the date and time

Master and admin users can use *System Config – Set Date & Time* to set the date and time. You may need to do this if, for example, the control unit lost all power for an extended period of time.

Select the option, enter the date (dd/mm/yyyy) and then the time.

Note: The installer may have set up the control unit to obtain its time automatically from an SNTP server. The internal clock adjusts itself for daylight saving in Spring and Autumn.

Configuring calendar sets

Master and admin users can use *System Config – Calendar Set* to configure the control unit to set or unset the alarm system (or parts of it) at fixed times of day on a seven-day cycle. If the system is a part-setting system, you can use this option to full set or part set B, C or D. If the system is a partitioned system, this option allows you to full set or part set any collection of partitions.

There are two basic elements that you can program within the calendar set option: the “event” and the “exception”. An event defines an action (setting, part setting or unsetting) to occur regularly at set times and days. An exception defines periods such as holidays when you do not want the event to occur. The number of events and exceptions the control unit can store is dependent on the control unit model.

Hint: Set up exceptions first, and then the events.

Note:

- You cannot program an event to change the system/partition directly from one part set level to another. You must program an event to unset the system/partition first, and another event to set the system/partition to a different part set level. For example, if event A part sets the system (or a partition), you cannot program event B to full set the system. You must program event B to unset the system and then use event C to full set the system.
- If you create an event to unset a partition, and another event to set the same partition again, you must program the setting event to occur at least 10 minutes after the unsetting event.
- The control unit adjusts its clock in Spring and Autumn to allow for Summer Daylight Saving Time. At the Autumn change-over, avoid configuring any unset events to take place during the changeover time on the Sunday morning. For UK systems, this time is 01:00 to 02:00. For EU control units, this time is 02:00 to 03:00. If the control unit unsets any part of the system at these times, it will NOT set the system again when the clock changes back to Winter Time.

Manually setting and unsetting partitions does not alter the times programmed in calendar sets. If a user sets a partition that is due to be set by a calendar event, the partition remains set when the calendar event time is past. Likewise, if a user unsets a partition before a calendar event is due to unset the partition, the partition remains unset.

Add Event

Use *System Config – Calendar Set – Add Event* to create an event. When you select the option, the control unit will guide you through the following series of options:

- Event Name* Enter up to 12 characters or press ✓ to leave the default name. See page 33 for details of how to edit text.
- Event Time* Specify the time you want the event to occur, then ✓ to display the next prompt.
- The time “00:00” is midnight, at the beginning of a new day.
- Note that if you specify a start time that is less than 10 minutes from the current time shown by the control unit

User Menu Options

clock (that is, less than the period set by *Warning Time*), the event will not take action until the following day.

Event Days

Choose the days you want the event to occur.

Press ▲ or ▼ to scroll through each day of the week.
Press ◀ or ▶ to specify Yes or No.

Event Actions

In a partitioned system, press ▲ or ▼ to scroll through each partition, and ◀ or ▶ to select No (no action), Full (full set), Part (part set) or Unset.

In a part-setting system, select one of: Full Set, Part Set B (or C or D) or Unset.

Event Exceptions

Choose the exceptions (set up using *Add Exception*) that you want to apply to the event.

Press ▲ or ▼ to scroll through the list of programmed exceptions. Press ◀ or ▶ to specify Yes (the exception applies to the event) or No.

Warning Time

Specify the period (in minutes) you want the control unit to sound the warning tone before the start of a setting event. Enter between 1 and 30 minutes. The default is 10. There is no specific warning indication for an unset event.

The warning tone sounds at the keypads and loudspeakers allocated to the partition(s) specified in the event.

At the beginning of the warning time, the control unit activates any outputs of type Autosest Warning.

At the end of the period, the control unit stops the warning tone, sets the affected partition(s) without any delay and deactivates any outputs of type Autosest Warning.

Warning Tone

Press ▲ or ▼ to choose between Audible or Silent. When Silent, the control unit will NOT sound a warning tone for the event (although the warning timer will still operate).

If a warning tone is due from more than one event at the same time, and any of the tones is set to "Audible", the tone will be audible.

Edit Event

Use *System Config – Calendar Set – Edit Event* to edit individual parts of an event.

Delete Event

Use *System Config – Calendar Set – Delete Event* to delete an event.

Add Exception

Use *System Config – Calendar Set – Add Exception* to create an exception. During the time specified by the exception, none of the events that have the exception will take place. When you add an exception, the control unit guides you through the following steps:

- | | |
|----------------------|--|
| Name | Enter up to 12 characters or press ✓ to leave the default name. See page 33 for details of how to enter text. |
| Exception Start Time | Specify the time you want the exception to start, then ✓ to display the next prompt.
The time “00:00” is midnight, at the beginning of a new day. |
| Exception Start Date | Specify the date you want the exception to start (for example, 31/12 for 31 st December). |
| Exception End Time | Specify the time you want the exception to end. |
| Exception End Date | Specify the date you want the exception to end. |

Edit Exception

Use *System Config – Calendar Set – Edit Exception* to edit individual parts of an exception.

Delete Exception

Use *System Config – Calendar Set – Delete Exception* to delete an exception.

Deferring calendar setting

During the calendar set warning time, a user can interrupt the setting process. To do this, the user must enter the access code at a keypad (or present a prox tag), then do one of the following:

- Press ◀ or ▶ to see details of which partitions or part of the system is about to set.

- Press **X** to allow the setting event to proceed.
- Press **✓** to defer setting for 30 minutes. Note that for a partitioned system, the user must belong to the partition that is due to be set.
- Press the **≡** key to gain access to the setting menu to set another partition that is not involved in the current setting event. Note that if the user is allocated to a single partition, that partition may start setting immediately.

If a user defers a setting event, the control unit halts the warning timer, and defers setting 30 minutes from the start of the warning time. At that time, the control unit starts counting down the warning timer again. The user can defer setting in this way a total of three times. After the third deferral, the control unit sets the system.

Note that deferring setting does not defer any unsetting events.

Setting faults

If there is a fault that would normally prevent the system from setting, a calendar set event will also fail. Before the time of a setting event, the control unit starts the calendar set warning tone as usual, but at the setting time, the control unit will not set the system. The control unit will log the failure as “set fail”. At the same time, the control unit will activate any output programmed as type Set Fail.

Note that if an installer assigns zones the Force Set Omit attribute, the control unit will omit those zones if they are active during a scheduled setting event.

Defining contacts

Master users can use *System Config – Contacts* to edit the Contacts List, which is a list of up to 12 contacts (by default named Recipient A-L). Contacts are used for outgoing communications, such as those for reporting alarms by email, speech call or SMS message.

Each contact can have the following settings: *Name*, *Tel No 1*, *Tel No 2*, *Email Address* and *IP Address*.

Note:

- You cannot edit contacts that the installer has used for communications to an Alarms Receiving Centre (ARC).
- Unless you are sure of what you are doing, it is recommended that you liaise with your installer before editing the Contacts List.

To edit the Contacts List:

1. Select *System Config – Contacts*.

The first recipient (contact) you are able to edit is displayed:

```
CONTACTS
Recipient E
```

2. Press ▲ or ▼ followed by ✓ to select the recipient you want to edit.
3. Press ▲ or ▼ followed by ✓ to select one of the following options:

Name Select this to edit the name of the recipient. See page 33 for details of how to enter text.

Tel No 1 The first telephone number of the recipient.

Tel No 2 The second telephone number of the recipient.

Email The recipient's email address.

IP Address The recipient's IP address.

Press ✓ when you have finished editing the setting, and if required, select another setting to edit.

4. Press ✕ several times to exit.

Editing outputs

Master and admin users can use *System Config – Edit Outputs* to edit the on and off times of any output the installer has configured as "User Defined".

Note: Master, admin, normal and partition users can activate or deactivate user-defined outputs at any time (see page 62).

To edit an output:

1. Select *System Config – Edit Outputs*.

The first output you are able to edit is displayed:

```
EDIT O/P PAN>01 W
PORCH LIGHT >
```

The top line shows the address and type of the output. In the above example, the address is PAN>01 and the type is W (wired). The bottom line shows the name of the output.

2. Press ▲ or ▼ followed by ✓ to select the output you want to edit.
3. Press ▲ or ▼ followed by ✓ to select the setting to change:

Name You can edit the name of the output. See page 33 for details of how to enter text.

Latched Use ▲ or ▼ followed by ✓ to select Yes or No. When set to No, the output changes state when activated, but then returns to the normal state again after the period specified by *On Time* (see below). When set to Yes, the output changes state every time a user operates the output, or according to a schedule if you specify *On Time*, *Off Time* and *Days* (see below).

On Time/Off Time/Days

If *Latched* is set to No, use *On Time* to specify the number of seconds you want the output to remain active. If you specify zero seconds, the output will not operate.

You can use *On Time*, *Off Time* and *Days* to specify a schedule for the output to activate and deactivate automatically. Use *On Time* and *Off Time* to specify the time you want the output to activate and deactivate. Use *Days* to specify the days of the week you want the output to operate (use ▲ or ▼ to display each day, then ► or ◀ to choose Yes or No).

Note: If a user activates the output while it is deactivated, the output stays activated until the control unit reaches the next off time. If a user de-activates the output while it is activated, the output deactivates until the control unit reaches the next on time.

Leave *On Time*, *Off Time* and *Days* without values if you want the output to act as a simple on/off switch.

Press ✓ when you have finished editing *On Time/Off Time/Days*.

Managing remote controls

Master and admin users can use *System Config – Remotes* to specify the functions that can be carried out using remote controls. The *System Config – Remotes* menu contains the following options:

<i>Edit</i>	Used to edit the programming of the buttons, such as the buttons used to set or unset the system, or operate outputs.
<i>Delete</i>	Deletes a selected remote control.
<i>Delete All</i>	Deletes all remote controls.
<i>Unset</i>	Enables or disables the ability for all remote controls to unset the system.
<i>HUA Function</i>	Enables or disables the ability for remote controls to generate Hold-Up Alarms (HUAs).

These options are described next.

Editing the programming of the buttons

You can use *System Config – Remotes – Edit* to re-program buttons on a one-way remote control, or the “*” button on a two-way remote control, after the devices have been assigned to a user.

A button can be programmed to:

- Set a selected part set (part-setting system only).
- Part set a partition (partitioned system only).
- Operate an output configured as "User Defined" by the installer.
- Full set the whole system (one-way remote control only).
- Unset the whole system (one-way remote control only).
- Full set a partition (partitioned system, one-way remote control only).
- Unset a partition (partitioned system, one-way remote control only).

Note for one-way remote controls:

- If you have a part-setting (non-partitioned) system, you cannot reprogram the unset button.
- If you have a partitioned system, the unset button can only be used to unset some or all partitions allocated to the user.

To re-program the buttons on a remote control:

1. Select *System Config – Remotes – Edit*.

The following is displayed:

```
EDIT REMOTE
Press Remote button
```

2. **EITHER:**

- a) Press the button on the remote control you want to re-program. Hold down the button until you see the transmit LED flash.

OR (if you do not have the remote control):

- a) Press ✓ at the "Press Remote Button" prompt.
- b) Use ▲ or ▼ followed by ✓ to select the remote control you want to re-program.
- c) The display lists the first button on the remote control:

```
RM002: User 002
Button *
```

- d) Use ▲ or ▼ followed by ✓ to select the button you wish to re-program.

The top line of the display shows the identity of the remote control, the button you pressed or selected, and the name of the owner. For example:

```
RM002, *:User 002
*Part Set
```

3. Use ▲ or ▼ followed by ✓ to choose the function for the button:

Part Set (Two-way remote control only.) To set part set B/C/D (part-setting system), or to part set the partition assigned to the remote control (partitioned system). For a part-setting system, use ▲ or ▼ followed by ✓ to select the part set.

Output To operate a user-defined output. Use ▲ or ▼ followed by ✓ to select the output, then use ▲ or ▼ followed by ✓ to select the output mode:

- On – Switches the output on.
- Off – Switches the output off.

User Menu Options

- Toggle – Changes the state of the output each time you press the button.

Set/Unset (One-way remote control only.) To set or unset the system. Choose *Set* or *Unset*, then use ▲ or ▼ followed by ✓ to select the set/unsetting mode:

- Unset All – Unsets all partitions that the user belongs to.
- Unset Partitions – Unsets selected partitions that the user belongs to. After selecting this option, use ▲ or ▼ to scroll through the partitions and use ► or ◀ to choose whether the partition should be unset by the button. Press ✓ when you have finished.
- Part Set All (partitioned system) – Part sets all partitions that the user belongs to.
- Partitions (partitioned system) – Full sets or part sets selected partitions that the user belongs to. After selecting this option, use ▲ or ▼ to scroll through the partitions and use ► or ◀ to select No (do not set partition), Full (full set the partition) or Part (part set the partition). Press ✓ when you have finished.
- Full Set All (partitioned system) – Full sets all partitions that the user belongs to.
- Full Set (part-setting system) – Full sets the whole system.
- Part Set B\C\D (part-setting system) – Sets part set B, C or D.

Note: If you choose Unset, ask your installer whether the entry timer needs to be running before a user can unset using a remote control.

4. Press ✕ repeatedly to exit.

Deleting remote controls

You may want to delete a remote control if it is lost or you want to reassign it to another user. You must delete a remote control before you can reassign it to another user.

The *System Config – Remotes* menu provides two options for deleting remote controls:

Delete This allows you to delete a specific remote control (see below).

Delete All This deletes all remote controls that the system learnt. You should use this option only if you are sure you want to delete all remote controls.

To delete a specific remote control:

1. Select *System Config – Remotes – Delete*.

The following is displayed:

```
DELETE REMOTE
Press Remote Button
```

2. Press the button on the remote control you want to delete. Alternatively, if you do not have the remote control, press **✓**, then use **▲** or **▼** to choose the remote control, followed by **✓**.

The following is displayed:

```
DELETE REMOTE
Delete
```

3. Press **✓** to delete the remote control.

Enabling or disabling unsetting

You can use *System Config – Remotes – Unset* to enable or disable the ability for all remote controls to unset the system. By default, remote controls are able to unset the system, but you may want to change this for security reasons.

After selecting *Unset*, use **▲** or **▼** to select Enabled or Disabled, followed by **✓**.

Disabling *Unset* does not affect the ability for remote controls to set the system.

Enabling or disabling HUA functions

You can use *System Config – Remotes – HUA Function* to enable or disable the ability for a two-way remote control to generate Hold-Up Alarms (HUAs).

Note: The installer must first enable this feature by configuring "Basic" confirmation mode. Doing so means that the system does not comply with BS8243 or DD243.

After selecting *HUA Function*, use ▲ or ▼ to select Enabled or Disabled, followed by ✓.

See page 21 for details of how to generate an HUA using a two-way remote control.

Starting a call to Downloader

Master users can use *System Config – Call Downloader* to start a connection to the installer's Downloader software via a telephone connection or across an Ethernet network. The installer can use Downloader to configure your alarm system.

Depending on how the installer has configured your system, you may be asked to use *System Config – Call Downloader* to start the connection to Downloader. Alternatively, the installer may be able to start the connection, but this requires you to enable *System Config – Facilities On/Off – Remote Access* (page 49).

To start the connection:

1. Select *System Config – Call Downloader*.

The following is displayed:

```
CALL DOWNLOADER
Tel No 01
```

2. Press ▲ or ▼ to choose Tel No 01, Tel No 02, IP Address 1 or IP Address 2 (as specified by your installer), then press ✓. You do not need to know the actual telephone numbers or P addresses.

The keypad displays the following, followed by a series of progress messages:

```
Awaiting
Connection
```

Your system may be connected to Downloader for some time.

Press **X** if you decide you want to abandon the call.

3. When the installer has finished and the connection is broken, the display shows the standard standby screen. For example:

```
i-on40H
10:55 01/09/2016
```

Switching outputs on/off

Master and admin users can use *Outputs On/Off* to switch outputs on or off as follows:

1. Select *Outputs On/Off*.

The display shows the first in a list of any outputs allocated for your use. For example:

```
O/P PAN>01 W
PORCH LIGHT Off
```

The top line shows the address and type of the output. In the above example, the address is PAN>01 and the type is W (wired). The bottom line shows the name of the output (which may be the same as the address) and whether the output is currently on or off.

2. Press **▲** or **▼** to select the output.
3. Press **▶** or **◀** to switch the output on or off. Outputs operated via radio may take several seconds to change state.
4. Press **X** repeatedly to exit.

Using the About options

If you are a master or admin user, you can use the *About* option to find information about the system you are using. The *About* menu contains the following options:

Panel

This gives:

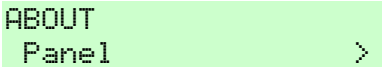
- The control unit model (e.g. i-on40H).
- The control unit's software (firmware) version number.
- Whether the control unit is in partitioned or part-setting mode.
- The installed languages and their versions.

<i>Cloud</i>	This gives information about the connection to the Eaton SecureConnect cloud, which your installer may need for support purposes.
<i>Expanders</i>	For each expander, this gives the expander's address, its type and the version of software (firmware) installed.
<i>Keypads</i>	For each keypad, this gives the keypad's address and the version of software (firmware) installed.
<i>Comms</i>	This gives information about the control unit's Ethernet connection and any plug-on communications module fitted. If required, please ask your installer for details about the information displayed (as documented in the Engineering Guide).

To use the *About* option:

1. Select *About*.

The following is displayed:

A screenshot of a menu option. The text 'ABOUT' is on the top line and 'Panel' is on the bottom line, both in a monospaced font. To the right of 'Panel' is a right-pointing chevron '>'. The entire text is highlighted with a light green background.

2. Press ▲ or ▼ followed by ✓ to select the option you require.
3. If applicable, press ▲ or ▼ followed by ✓ to select the sub-option.
4. If applicable, press ► or ◀ to display further information.
5. Press ✕ repeatedly to exit.

Generating a SecureConnect pairing code

You can use the *Pair App* option to generate a pairing code for the Eaton SecureConnect app. The app allows you to monitor and control your alarm system over the internet from your mobile phone or tablet.

The pairing code uniquely pairs your app with your panel and user code. This ensures that any actions you carry out using the app will affect only your panel, and are logged against your user code.

You are prompted to enter the code when you first open the app. The pairing code lasts for 15 minutes.

For details of how to use the app, please refer to the *SecureConnect App User Guide*.

SecureConnect is a trademark of Eaton.

www.touchpoint-online.com

Product Support (UK) Tel: +44 (0) 1594 541978

Available between:

08:30 to 17:00 Monday to Friday.

email: securitytechsupport@eaton.com

Part Number 12838021

21st February 2017