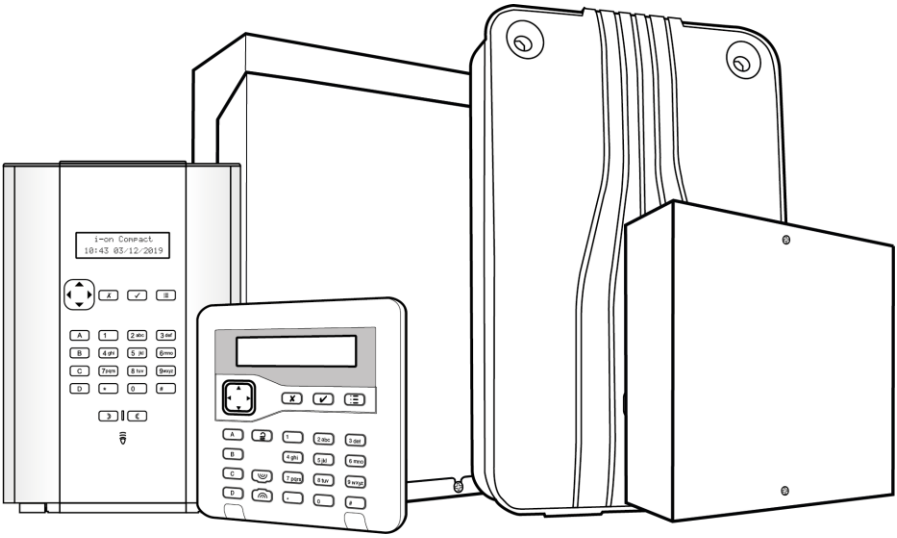
i-on Series
Security System

Administration and User Manual

for i-on Compact, i-on30R+, i-on40H+, i-onG2SM, i-onG3MM and i-onG3LM



Issue 4

Control unit software version 7.02.xx

© Eaton 2022

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 range of control units are:

- Suitable for use in systems designed to comply with PD6662:2010 at Grade 2, and environmental class II. The i-onG3MM is also designed to comply with PD6662:2017 at Grade 3.
- Suitable for use in systems designed to comply with the requirements of EN50131-3 at Grade 2, and environmental class II. The i-onG3MM is also designed to comply with the requirements of EN50131-3 at Grade 3.
- Compliant with the requirements of EN50131-6:2008 at Grade 2 and environmental class II. The i-onG3MM is also designed to comply with the requirements of EN50131-6:2008 at Grade 3 .

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 manual 1
Other publications 1
About Users 2
User types 2
User access codes 4
Code lockouts 5
Installer access 5
About part-setting and partitioned modes 5
Part-setting mode 5
Partitioned mode 6
About the web interface 7
Virtual Keypad 8
Chapter 2: Setting and Unsetting 9
Introduction 9
Using a keypad to set or unset the system 9
Setting the system 9
Quick-setting the system 12
Unsetting the system 13
Using a two-way keyfob-style remote control 14
Operating the buttons 15
Setting from a two-way remote control 15
Unsetting from a two-way remote control 15
Querying the set/unset status from a two-way remote control 16
Starting a hold-up alarm from a two-way remote control 16
Using a one-way remote control 16
Setting from a one-way remote control 17
Unsetting from a one-way remote control 18
Using a one-way i-RK01 radio keypad 18
Setting from an i-RK01 radio keypad 18
Unsetting from an i-RK01 radio keypad 19
Using a two-way KEY-RAS keypad 19
Setting from a KEY-RAS radio keypad 19
Unsetting from a KEY-RAS radio keypad 20
Using the SecureConnect™ app 20
Chapter 3: Managing Alarms 21
Alarm types and sounds 21
Other alarm actions 22
Speech messages 23
Silencing, acknowledging and resetting alarms 24
Installer resets 25
Accidental alarms 26
Viewing alerts 26
Chapter 4: User Menu Options 28
User Menu Map 28

Entering and exiting the user menu.....30
Entering text.....30
Omitting zones.....31
Using shunt groups.....32
About shunt groups.....32
Activating or deactivating a shunt group.....33
Managing users.....33
About users.....33
About the Users menu.....33
Adding users.....34
Editing users.....37
Deleting users.....39
Viewing the log.....40
Testing the system.....40
Testing sirens and sounders.....40
Testing a wired keypad.....41
Testing the on-board keypad.....42
Performing a walk test.....42
Testing outputs.....44
Testing remote controls.....44
Testing social-care or medical pendants.....45
Testing user HUDs.....46
Testing proximity tags.....46
Testing ARC reporting.....47
System configuration.....48
Switching facilities on/off.....48
Setting the date and time.....49
Configuring calendar sets.....49
Defining contacts.....53
Editing outputs.....54
Managing remote controls.....55
Connecting to a Wi-Fi network.....60
Switching outputs on/off.....61
Using the About options.....61
Pairing with the SecureConnect App.....62

Chapter 1: Introduction

About this manual

This manual provides full details of how to operate and administer an i-on alarm system as a user. The manual describes:

- The user types.
- The meaning of part-setting and partitioned modes.
- Detailed information about how to perform functions such as setting and unsetting the system.
- How to manage alarms.
- The options available from the user menu to carry out tasks such as omitting zones, adding users and viewing the log.

Other publications

If you are new to i-on alarm systems, you should read one of the following guides first:

- *i-on Compact User Guide.*
- *i-on Series User Guide (for i-on30R+, i-on40H+, i-onG2SM and i-onG3MM)*.

These provide an introduction to the key concepts and components of the alarm system, and how to carry out the most common day-to-day tasks.

Additional user guides are also available for other items, such as the KEY-RAS radio keypad. Your installer will be able to tell you which guides are available for the equipment installed at your site.

Other publications are available to installers − these describe topics such as system installation, maintenance and installer options.

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.
- Acknowledge and stop alarms.
- Raise duress alarms.
- Gain access to the user menu to carry out tasks such as to omit zones, view the log, test the system and switch outputs on or off. For a full list of available user options, please refer to the *User Menu Map* on page 28.

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 user types are described in the next section.

User types

Note: Some user types are available only if the system is configured as a partitioned (not part-setting) system. Please refer to page 5 for a description of part-setting and partitioned modes.

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 (if applicable).

  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 *User Menu Map* on page 28). 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** (not available for i-on Compact) – A duress code user can set or unset the system, but whenever the access code is used, the control unit can, for example, notify the Alarm Receiving Centre (ARC).

  A duress code has no access to the user menu and cannot have a remote, proximity reader tag or medial/social care pendant.

  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** (not available for i-on Compact) – 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** (not available for i-on Compact) – 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** (not available for i-on Compact) – This type of user code is used only for activating and deactivating shunt groups (see page

32). 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** (not available for i-on Compact) – 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.
- **BMS** – This is designed to give third-party systems permission to perform actions that would normally be performed by a normal user, such as setting and unsetting. A remote password is automatically generated and displayed when you create this user, which the third-party system requires.
- **Level-4** – This type of user can be created only by the installer, and is able to update the firmware and language files at the control unit using the web interface. There can be only one level-4 user.

  The 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).
- **Set/Unset** – This type of user can set and unset the system, change their own access code, add their own proximity tag and change their own remote-access password (which allows use of the virtual keypad).

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

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. Each access code is either 4 or 6 digits, depending on how the system is configured.

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

The access code of the first master user is defined by the installer during installation. **It is recommended that you change this user code as soon as possible after system installation (see page 37).**

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 an "Excess Keys" tamper alarm. If configured, the control unit also sends the event to the Alarms Receiving Centre (ARC).

Once 90 seconds has elapsed, the keypads allow users to try again. If an incorrect code or tag is used again, the keypad locks 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 web interface). Depending on how your installer has programmed the system, you may receive a phone call from the installer to request access.

About 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 next.

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 (unless the zone has the One Partition attribute 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 up to three part-set levels. Users can choose whether to set a partition to which they have access at full or a part-set level. When the user chooses a part-set level, all zones that the installer has assigned the appropriate "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.

About the web interface

This guide describes how to administer the control unit from a keypad. However, if the control unit is connected to the LAN, master users can also monitor and configure certain settings from the web interface (Figure 1), as the control unit has a built-in web server. Master users can carry out various operations, such as to view the status of the system, examine the log, create users, create calendar sets and view detector signal strengths.

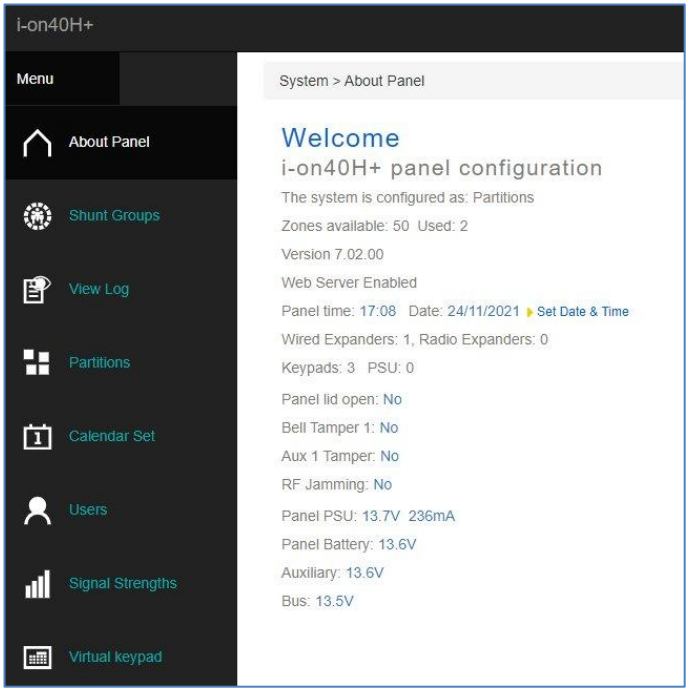


Figure 1 - Web Interface

You can access the web interface by entering the control unit's IP address in the address bar of a web browser, and then entering your user code and remote password in the login page displayed. Your remote password is defined using *User Menu – Users – Edit User*.

Before you can use the web interface, a Master User must enable remote access using *User Menu – System Config – Facilities On/Off – Remote Access*. The installer must also enable the web server in the Installer menu.

The *i-on Web Browser Interface Setup Guide* explains how to configure and use the system using the web interface.

Virtual Keypad

The virtual keypad (Figure 2) allows you to perform similar functions as available at a hardware keypad, including operation of user-defined outputs using the ABCD keys. The navigation and ABCD keys reflect the status of the system in the same way as for a hardware keypad.

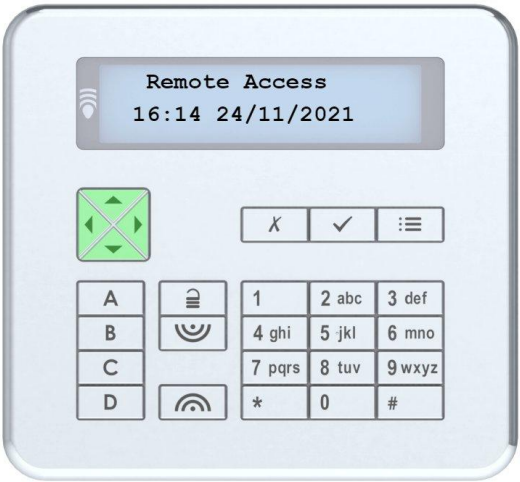


Figure 2 - Virtual Keypad

For installer and master users, the virtual keypad is access through a Virtual Keypad option in the web interface. For other users, the web interface is displayed directly after entering their user code and personal remote password in the login page of the web interface.

If a master user creates a new user and defines a remote password, it gives permission for the new user to access the virtual keypad. The new user can change the password using *User Menu – Users – Edit User* (if available to the user).

The virtual keypad can also be accessed through Eaton SecureConnect, as described in the *SecureConnect Installer's 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 devices or emergency exits.
- Monitors for machinery (for example freezers) or other type of “technical alarm”.

Using a keypad to set or unset the system

This section explains how to set and unset your system from any keypad that has a display (including the keypad built into an i-on Compact control unit). If you are using a radio keypad that has no display, please refer to page 18 (i-RK01) or to page 19 (KEY-RAS).

Note: Please refer to the *User Guide* if you need an overview of the purpose of the keypad keys.

Setting the system

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

```
      i-on40H+
 11:15 16/09/2019
```

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. Depending on how the system is configured, the bottom line may show the first of several setting options:

```
Setting Options    ↕
 A : Full Set
```

Press ▲ or ▼ followed by ✔ to select the option you require:

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.

Note: Please refer to page 5 for details of part sets.

Full Set All (partitioned system only)
To set all partitions fully. This is available only if all partitions are currently unset.

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

Note: Please refer to page 5 for details of partitions.

4. 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, PB/C/D = part set B/C/D is 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>PB/C/D” = change unset to part set B/C/D
   “U>S” = change unset to full set
   “S>U” = change set to unset
   “PB/C/D>U” = change part set B/C/D 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 (unless the zone has the One Partition attribute set).

d) Repeat steps b) and c) as required.

e) Press ✔.

5. 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.

You may see a setting fault (such as an active zone) that prevents you from setting the system. Normally, the system can set only when zones (other than those in the entry/exit route) are inactive.

6. 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 of the display 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 of the display shows which of these methods is being used. (Exit terminate and lock set are not available for i-on Compact.)

Note: You can press either the 🔒 or ✘ key to stop the system setting before it has set. (The 🔒 key is not available for i-on Compact.)

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 16/09/2019
```

In a part-setting system, one of the four ABCD keys (or one of the set/unset LEDs on a i-KP01) may glow to show which part of the system is set (Figure 1), unless disabled by the installer to meet appropriate standards.

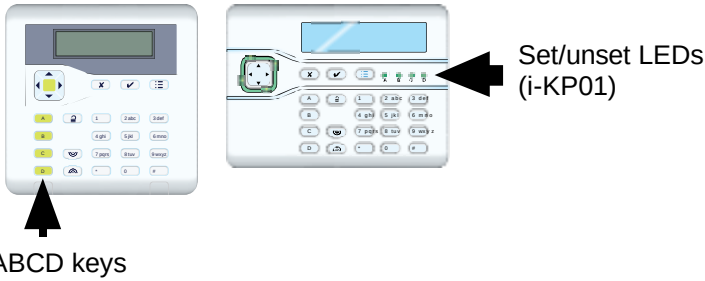


Figure 1. Keypad LED positions to indicate set/unset status

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

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 6 on page 11.

Unsetting the system

1. Enter through the entry route designated by the installer (this is 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, PB/C/D = part set B/C/D is set):

```
Partitions          ↕
 Partition 1      PB
```

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

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

```
Partitions          ↕
 Partition 1    PB>U
```

   "U>PB/C/D" = change unset to part set B/C/D
   "U>S" = change unset to full set

"S>U" = change set to unset
"PB/C/D>U" = change part set B/C/D 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 2) 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 34) 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.

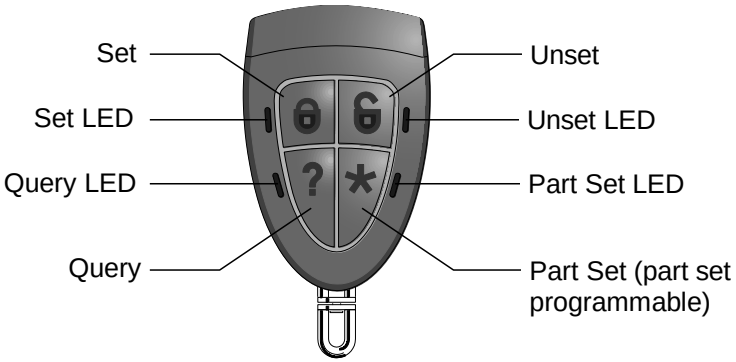


Figure 2. Two-way remote control buttons

In a partitioned system, the remote control can be used for only one partition.

The installer can use a *2W Set Instant* option to 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 56 for details of programming the * button.

Setting from a two-way remote control

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 6 on page 11.
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 from a two-way remote control

Note: The ability for remote controls to unset the system can be disabled (see page 59).

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 from a two-way remote control

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 from a two-way remote control

A two-way remote control can be used to start a hold-up alarm if enabled by an installer and in the user menu (see page 59).

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

To start a hold-up alarm 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 3). The buttons can be programmed as required (see page 56), but by default, 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.

1. Full Set.
2. Part Set (part-setting system).
3. (Programmable, see page 55.)
4. Unset.
5. Transmit LED.

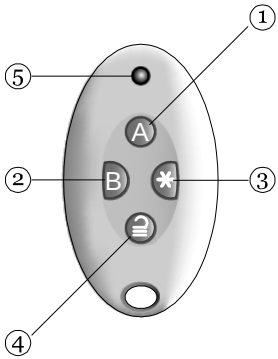


Figure 3. One-way remote control buttons

Each remote control has a unique electronic identity. You can assign (see page 34) only one remote control to each user.

Setting from a one-way remote control

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

   In a partitioned system, the default action for key A is to full set all of the user's partitions. Keys can be configured to part set specified partitions, if required.
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 6 on page 11.

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 from a one-way remote control

Note: The ability for remote controls to unset the system can be disabled (see page 59).

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 i-RK01 radio keypad

A one-way keypad (Figure 4) does not have a display and can only transmit to the control unit (it cannot receive information back from the control unit).

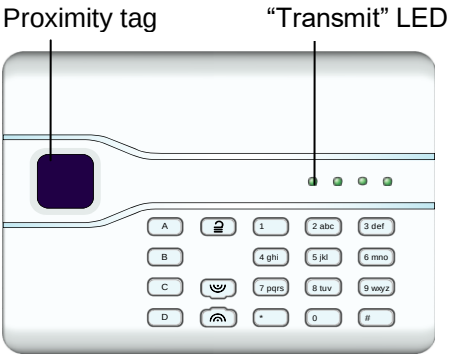


Figure 4. One-way radio keypad

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 from an i-RK01 radio keypad

1. Make sure the system is in standby.
2. Enter a valid access code or present your proximity tag to the keypad.
3. Press (these are the default actions):

   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 6 on page 11 (except there is no keypad display).

Unsetting from an i-RK01 radio keypad

1. Enter through the entry route designated by the installer.
2. 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 🔒.

Using a two-way KEY-RAS keypad

Note: Please refer to the *KEY-RAS User Guide* for full information about how to use the KEY-RAS.

A two-way KEY-RAS keypad (Figure 5) can transmit to the control unit and receive information back from the control unit. The keypad can show the current set/unset status of the system, and sound entry, exit and alarm sounds.

Figure 5. Two-way KEY-RAS radio keypad

Setting from a KEY-RAS radio keypad

1. Make sure the system is in standby.
2. Key in your access code, or press the ? key and present your proximity tag.

3. Press the appropriate ABCD key, as configured by your installer. The keys are normally configured as follows:
   - A − Sets the system fully. (For a partitioned system, only the partition the KEY-RAS is assigned to is set).
   - B, C or D − Sets part-set B, C or D.
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 6 on page 11 (except there is no keypad display).

   The key you pressed remains lit red, either for a few seconds or permanently while the system is set (depending on configuration). This indicates that setting was successful.

Unsetting from a KEY-RAS radio keypad

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.
2. Within the allocated time, key in your access code and press 🔒, or present your proximity tag.

   The entry tone stops and the system unsets.

   The ABCD keys remain lit green, either for a few seconds or permanently while the system is unset (depending on configuration). This indicates that unsetting was successful.

Using the SecureConnect™ app

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

- 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.

Please refer to the SecureConnect documentation for details about how to install and use the app.

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, social-care pendant or medical pendant 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 24).

Table 1: Alarm sounds

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

Hold Up	Loud warbling tone from sirens and internal sounders.	HUA zone or radio hold-up device transmitter activated at any time. Pressed on keypad. The installer must enable this feature.
Tamper	Loud warbling tone from sirens and internal sounders.	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 internal sounders.	Technical alarm zone activated at any time. This is known as an alert; see page 26. (Audible only when system is unset.)
Fault	Quiet beeping once per second from internal sounders.	A system fault detected by the control unit, such as a mains failure or communications line fault. This is known as an alert; see page 26.
Social Care	Chirp once per second at internal sounders for the first 30 seconds, then a louder chirp.	Social-care alert. **Note:** The first 30-second warning period allows a user to cancel the alert before it officially starts.
Medical	Loud chirp once per second at internal sounders. Strobe operates.	Medical alarm.

Other alarm actions

In addition to sounding internal sounders and external siren/strobe units, the system may (depending on configuration) 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. Depending on the hardware fitted, communication may be via a fixed-line telephone network, or over a mobile phone network, or across the internet (using the SecureConnect™ cloud service).
- 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 26 if the keypad is beeping approximately once per second.
- If an alarm occurs when the system is unset, the navigation key glows red.

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 in the normal way. 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. If the keypad has a display, 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 26.
- 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 40 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. Go through the procedure to acknowledge the alarm again, and at the above prompt, enter the reset code 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 internal sounders to give a continuous alarm sound. Instead, the navigation key on keypads glows red if the system is unset, and internal sounders give a short "beep" once or twice per second (depending on the type of alert) until the alert is acknowledged.

To view the cause of the alert (assuming the system is unset):

1. Press ✔ before entering your access code.
2. 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
    Tech Z000 Alarm
   ```

   The bottom line may alternate between displaying the zone number and name (if applicable).
3. Press ✔ to acknowledge and, if applicable, reset the alert.

   Repeat this step for any other alerts that may be active.

4. If you see a message similar to the following, it indicates that the alert has been caused by a Technical Alarm and the detector is still active:

```
RESET FAULTS
 Z041   Zone 041
```

   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

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.

Note: the user types marked * are not available for i-on Compact.

MENU Option			Master	Admin*	Normal	Partition*	Guard*	Set Only*	BMS	Duress*	Easy Set*	Shunt*	Level-4	Set/Unset
Omit Zones			✔	✔	✔	✔			✔		✔			
Shunt Group (not i-on Compact)			✔	✔										
Users	Add User		✔	✔										
	Edit User	Name	✔	✔									✔	
		Type (not U001)	✔	✔										
		Partitions (partitioned system)	✔	✔										
		Code	✔	✔	✔	✔			✔		✔		✔	✔
		Prox Tag	✔	✔	✔	✔					✔			✔
		Remote	✔	✔	✔	✔					✔			
		Social Care	✔	✔	✔	✔	✔	✔			✔			✔
		Medical	✔	✔	✔	✔	✔	✔			✔			✔
		Hold Up Device	✔	✔	✔	✔					✔			
		Remote Password							✔				✔	✔
		App access	✔	✔	✔	✔								
	Delete User		✔	✔										
View Log			✔	✔	✔	✔					✔			
Test	Siren & Sounders	Ext. Radio Sirens	✔	✔										
		Wired Sirens (not i-on Compact)	✔	✔										
		Loudspeakers (not i-on Compact)	✔	✔										
		On-board Sounder (i-on Compact)	✔	✔										
		Wired Keypads (not i-on Compact)	✔	✔										
		KEY-RKPZ	✔	✔										
		KEY-RAS	✔	✔										
		Internal Sounders	✔	✔										

	Wired Keypad (not i-on Compact)			✔	✔									
	Walk Test	Chime		✔	✔									
		System		✔	✔									
		Partitions		✔	✔									
		Zones		✔	✔									
	Outputs			✔	✔									
	Remotes			✔	✔									
	User HUDs			✔	✔									
	Prox Tags			✔	✔									
	ARC Reporting			✔	✔									
System Config	Facilities On/Off	Chime		✔	✔	✔	✔					✔		
		Remote Access		✔										
		Level 4 Update		✔	✔	✔	✔					✔		
		Activity Monitoring		✔	✔	✔	✔					✔		
	Set Date & Time			✔										
	Calendar Set (not i-on Compact)	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			✔	✔									
	Wi-Fi			✔	✔									
Outputs On/Off				✔	✔	✔	✔					✔		
About	Panel			✔	✔									
	Cloud			✔	✔									
	Expanders (not i-on Compact)			✔	✔									
	Keypads (not i-on Compact)			✔	✔									
	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 ▲ or ▼ to scroll through the options, followed by ✔ 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 ✘ (if necessary several times).

Entering text

You can use the numeric (0-9), * and # keys (see Figure 6) to enter numbers and text.

Press a key one or more times to obtain the letter you require. For example, to enter a "B", press the "2" key twice, or to enter an "C", press "2" three times. The bottom line of the display shows the character you are about to insert and the other characters available using that key. Wait a moment before each new letter.

Press # to change between capitals and lower case letters. Press 0 to enter a zero, space or other characters such as "&", "@" and "/".

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.

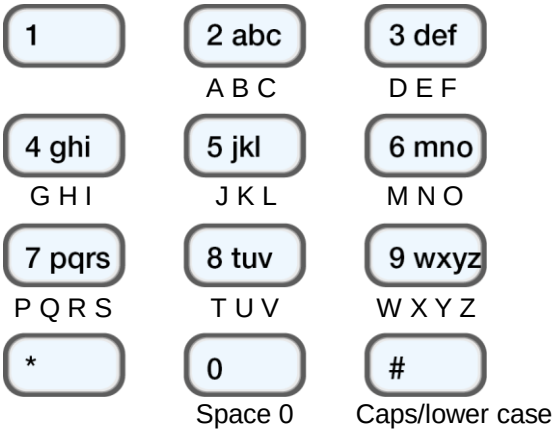


Figure 6. Letters assigned to keys

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. You may, for example, want to omit a zone that protects a garage to enable access while the system is set.

Note: The zone returns to normal operation 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

(Not available for i-on Compact.)

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

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.

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* (page 2), which determines the actions the user can carry out.

About the Users menu

If you are a master or admin user, you can use the *Users* option in the main menu to:

- Add new users to the system, including the devices they can use (*Users – Add User*). See the next section.
- Edit user details (*Users – Edit User*). See page 37.
- Delete users (*Users – Delete User*). See page 39.

If you are not a master or admin user, the *Users* menu does not contain *Add User*, *Edit User* and *Delete User* options. Instead, depending on your user type, it may include options from the *Edit User* menu that allow you to change your own details, such as your access code. For some user types,

the *Users* menu is not available at all. The menu map on page 28 shows the user types that have access to *Users* menu, and the options available. See page 38 for a description of each option.

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 (if applicable) and access code. Each user must have a unique access code.
- Assign a proximity tag, remote control, radio hold-up device, medical pendant and social-care pendant (depending on user type − a shunt code user can have only a proximity tag; duress and BMS users can have none of these devices).

  If you do not wish to assign these devices, most user types can assign the devices to themselves at a later date using the *Users* option (depending on user type – see the menu map on page 28).

  A user can have only one proximity tag, remote control, hold-up device, medical pendant or social-care pendant. No two users can have the same device.

  Note: The level-4 user can be created only by the installer. There can be only one level-4 user.

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 30 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 2 for a description of each user type). Press ✔ to continue.

4. If you are using a partitioned system, and are adding a user other than a master, shunt code or BMS 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 (except for duress and BMS users):

```
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 40).

7. You are prompted to assign a remote control to the user (except for shunt, duress and BMS users):

```
  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. The remote control must not be already assigned to another user.

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 40).

8. You are prompted to assign a social-care pendant (except for shunt, duress and BMS users):

```
  Press button on
Social Care Pendant
```

9. You are prompted to assign a medical pendant (except for shunt, duress and BMS users):

```
  Press button on
  Medical Pendant
```

10. You are prompted to assign a radio HUD (Hold-Up Device) (except for shunt, duress and BMS users):

```
Press both buttons
 to identify HUD
```

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

Note: If you have an HUD that is already allocated, you can find out who it belongs to by using *Test – User HUDs* (page 46).

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

11. 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.

12. You are prompted to enter a remote-access password:

```
SET REM. PASSWORD
```

If you want the user to be able to access the web interface (see page 7) or are defining a BMS user, enter a remote-access password of six or more characters, or press ✔ if you do not want to assign one.

If you define a password, the user can change it by logging into the User menu (if available to them), selecting *Edit User* and choosing to edit their own user settings.

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

```
New User Added
```

Editing users

Editing another user's details

To edit another user's details (such as the user's name or type), you must log in as a master or admin user and select *Edit User* from the *Users* menu. *Edit User* is available only if you have logged in as a master or admin user.

You can use *Edit User* to change a user's name, user type, allocated partitions (if applicable) and access to the SecureConnect app.

Note:

- Only master users can edit the details of other master users, and even then, only the name and app access settings can be changed.
- If you are an admin user, you can edit only those users who belong to the same partitions as you.
- If a user forgets their code, a master or admin user must delete that user and recreate a new user with a new code.
- You cannot edit a user when the partition they belong to is set.
- If you want to delete another user's remote control, see "Deleting remote controls" on page 58.

Editing your own user details

If you are a master or admin user, you can edit your own user details (such as your user code and allocated proximity tag) by selecting your user name in the *Users, Edit User* menu.

If you are not a master or admin user, the *Users, Edit User* menu is not available, but the *Users* menu may (depending on your user type) contain options to change your own user details. The menu map on page 28 shows the user types that have access to *Users* menu, and the options available.

You can (depending on your user type):

- Change your own access code.
- Add or delete your own proximity tag, remote control, hold-up device, medical pendant or social-care pendant.

- In a partitioned system, specify the partition that your two-way remote control can set, unset, etc. (not available for a one-way remote control).
- Enable or disable access to the SecureConnect app.
- Change your remote password.

Please refer to the following section for more details of the options.

Using the Users option
To edit user details:

1. Select *Users.*
2. If you are a master or admin user, select *Edit User*.

   Note: You can press * to alternate between displaying user numbers and names.
3. Press ▲ or ▼ followed by ✔ to select the user you wish to edit. Alternatively, enter the user number (e.g. 004) and press ✔.
4. Press ▲ or ▼ followed by ✔ to select the option you require:

Name	To change the user name.
Type	To change the user type. See page 2 for a description of each user type.
Partitions	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.
Code	To change your own access code.
Prox Tag	To add or delete your own proximity tag.
Remote	To add or delete your own remote control. If you are using a partitioned system and a two-way remote control, you can use the *Remote Partition* 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.

	Use *Delete Remote* to delete your remote control if it has been lost.
Hold Up Device	To add or delete your own hold-up device.
Medical Pendant	To add or delete your own medical pendant.
Social Care	To add or delete your own social-care pendant.
Remote Password	To change your own remote-access password to access the web interface, or to set the remote-access password for a BMS or level-4 user. This is available only if the user who added you gave you permission to access the web interface by specifying a remote password.
App access	To enable or disable use of the SecureConnect mobile app. This option is not available for users of type Set/Unset.

5. Follow the prompts. Please refer to "Adding users" on page 34 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, hold-up device, medical pendant or social-care pendant assigned to the user.

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

To delete a user:

1. Select *Users – Delete User*.

   Note: You can press * to alternate between displaying user numbers and names.

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 01/12/2019
   ```

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

2. If applicable, press ▶ to see additional information.

   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.

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, hold-up device, medical pendant or social-care pendant.

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.
Wired Sirens	Wired sirens and their strobes (not i-on Compact).
Loudspeakers	Extension loudspeakers, keypads and other internal sounders (not i-on Compact).
On-board Sounder	The control unit's internal sounder (i-on Compact only).

Wired Keypads	Sounders in wired keypads (not i-on Compact).
KEY-RKPZ	Sounder in KEY-RKPZ two-way radio keypads.
KEY-RAS	Sounder in KEY-RAS two-way radio keypads.
Internal Sounders	SDR-RINT internal radio sounders.

3. If applicable, 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

(Not available for i-on Compact.)

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.

Testing the on-board keypad

(i-on Compact only.)

To carry out the test:

1. Select *Test – On-board Keypad*. You will see:

```
Press keys to test:
_
```

   When you start the test, the LEDs around the navigation should all glow red, and A, B, C and D glow alternately. Every time you press a navigation key, the LEDs change colour.

2. Press ▲, ▼, ▶ and ◀ in turn to test the navigation keys. Each time you press a key, the display should 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.

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 a single chime for each zone that is triggered during the walk test.
Off	Switches off chiming.
On	Generates a chime every time a zone is triggered.

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*, there is 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 return to displaying all zones).

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 61).

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 output type is displayed for control units that have built-in radio and wired outputs. 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,S:User 001
Set Ptns>       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 social-care or medical pendants

Master and admin users can use *Test – Pendants* to test social-care or medical pendants.

To carry out the test:

1. Select Test – Pendants.

```
  Press button to
  identify Pendant
```

2. Press the button on the device you wish to test. The control unit gives a double-beep confirmation tone and you will see the results of the test:

```
User: User 002
Func: Medical   SS:9
```

The top line shows the name of the user the device is allocated to. The next line shows the function of the device, and the third line indicates the strength of the signal. If the signal strength is less than 4, contact your installer.

3. Repeat step 2 for the other buttons.

4. Press ✔ to end the test.

Testing user HUDs

Master and admin users can use *Test – User HUDs* to test radio hold-up devices.

To carry out the test:

1. Select *Test – User HUDs*.

   The following is displayed:

   ```
   Press both HUA
   buttons
   ```

2. Press and hold both 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 user hold-up 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 proximity tag sensor on 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

The *Test – ARC Reporting* option is available if the control unit uses a GSM or PSTN module to communicate alarms to an Alarms Receiving Centre (ARC).

Master and admin users can use *Test – ARC Reporting* to test the connection to the ARC.

To carry out the test:

1. Select *Test – ARC Reporting*.

   The following is displayed:

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

2. Use ▲ or ▼ to choose one of the two recipients selected by the installer. Each recipient uses a separate telephone number to the ARC. Depending on how the installer has configured communications, the second line may be used if the first fails to connect.

3. 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: The menu map on page 28 specifies the options available for each user type.

Switching facilities on/off

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

Chime	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.
Remote Access	Use this option to enable or disable remote access to the control unit from the web interface or SecureConnect. **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.
Level 4 Update	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 automatically or 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.
Activity Monitor	Setting this option to *On* enables social care activity monitoring. The installer can specify the zones to monitor for activity, the monitoring period, and the minimum period between activations. For example, if the monitoring period is 9am to 10pm, and the minimum period between activations is 2 hours, the control unit

will generate a "Social Inactivity" alert if no monitored zone activates over a period of 2 hours during 9am to 10pm.

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

You 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 the SecureConnect service. The internal clock adjusts itself for daylight saving in Spring and Autumn.

Configuring calendar sets

(Not available for i-on Compact.)

You 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 should not program an event to change the system/partition directly from one part set level to another. You should 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 01

part sets the system (or a partition), do not program event 02 to full set the system. Instead, program event 02 to unset the system and then use event 03 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 30 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 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 Autoset 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 Autoset 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 30 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 31st 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 that has a display (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 ✘ 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

You 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 speech call or SMS message.

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 30 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.

Note: The *Email* and *IP Address* settings are not used, as email addresses (for emailed alarms) and IP addresses (for ARC reporting over the internet) are configured and used by SecureConnect.

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

4. Press ✘ several times to exit.

Editing outputs

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

Note: User-defined outputs can be activated or deactivated at any time using *Outputs On/Off* (see page 61).

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 output type is displayed for control units that have built-in radio and wired outputs. 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 30 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

You 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:

Edit	Used to edit the programming of the buttons, such as the buttons used to set or unset the system, or operate outputs.
Delete	Deletes a selected remote control.
Delete All	Deletes all remote controls.
Unset	Enables or disables the ability for all remote controls to unset the system.

HUA Function 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 the A, B or * 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 (in a partitioned system, it part sets only the partition the remote control is assigned to).
- Operate an output configured as "User Defined" by the installer.
- Full set the whole system (one-way remote control only).
- Unset the whole system (partitioned system, one-way remote control only).
- Full set or part set selected partitions (partitioned system, one-way remote control only).
- Unset selected partitions (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. See *Unset, Unset All* and *Unset, Partitions* below.

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:

Note: If you have a partitioned system, the unset button can only be used to unset some or all partitions allocated to the user. See *Unset, Unset All* and *Unset, Partitions* below.

No Action For the button to have no action.

Part Set (two-way remote control only): To set part set B/C/D. For a partitioned system, it applies only to the partition assigned to the remote control. Use ▲ or ▼ followed by ✔ to select the part set. The * key cannot be used to unset or full set.

Set/Unset (one-way remote control only): To set or unset the system. Choose one of the following:

- *Unset, Unset All* (partitioned system) – Unsets all partitions that the user belongs to.
- *Unset, Partitions* (partitioned system) – 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.

- *Set, 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 PartB/C/D (part set the partition). Press ✔ when you have finished.
- *Set, Full Set All* (partitioned system) – Full sets all partitions that the user belongs to.
- *Set, Full Set* (part-setting system) – Full sets the whole system.
- *Set, 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.

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

4. Press ✘ repeatedly to exit.

Deleting remote controls

You may want to delete a remote control if 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 ✔.

   A message similar to the following is displayed:

   ```
   RM001:User 002
      Are you sure?
   ```

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

Connecting to a Wi-Fi network

You can use the *System Config – Wi-Fi* menu to connect the control unit to a Wi-Fi network. The menu is available only if a module that supports LAN communication via Wi-Fi is fitted, and the installer has enabled the option using the *Installer – System Options – User Options – User access – Wi-Fi Setup* option.

The Wi-Fi menu contains the following options:

Network

This option allows you to select the Wi-Fi network to use. The signal strength of each network is shown in brackets.

An asterisk (*) displayed next to a network name indicates that it is the selected network; it does not indicate connection status.

Enter the password when prompted; use:

- 1-9 keys to enter numbers and letters, as labelled on the keys. For example, use the “2” key to enter A, B, C or 2.
- # to change between upper/lower case.
- 0 to enter 0, space, or other character (e.g. “&”, “@” and “/”).
- The Menu key to show the password when entering.
- ▲ or ▼ to move the cursor left or right, ▶ to add a space, or ◀ to delete the previous character.

A "Connected" message is displayed if the connection is successful.

Note: The Network and WPS options are also available in the Installer menu.

WPS

Select this option if you want to connect using WPS. When you see “Waiting to connect”, press the WPS button at the router. If no connection is made within two minutes, the control unit cancels the procedure.

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 output type is displayed for control units that have built-in radio and wired outputs. 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 ✘ 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) and bootloader version number.
- The installed languages and their versions.
- Whether the control unit is in partitioned or part-setting mode (if applicable).

Cloud — This gives information about the connection to the SecureConnect.

Expanders	(Not available for i-on Compact.) For each expander, this gives the expander's address, its type and the version of software (firmware) installed.
Keypads	(Not available for i-on Compact.) For each keypad, this gives the keypad's address and the version of software (firmware) installed.
Comms	This gives information about any plug-on communications module fitted and the control unit's Ethernet connection. If required, please ask your installer for details about the information displayed (as documented in the *Configuration Guide*).

To use the *About* option:

1. Select *About*.

   The following is displayed:

```
ABOUT
 Panel                 >
```

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.

Pairing with the SecureConnect App

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

Note: *Pair App* is not available if *Cloud Access* is disabled in the Installer menu or if *App Access* is disabled in your user settings (see page 39). The option is also not available for users of type Set/Unset (see page 4).

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.

Please refer to the SecureConnect documentation for details of how to use the app.

SecureConnect is a trademark of Eaton.

www.myscantronic.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 14199506 24th January 2022