SigNET Series (100/200/300) User Guide

ELAB 1543

EUROPLEX TECHNOLOGIES

Centaur Alarms Limited

Warning: While this system is an advanced design integrated security system, it does not offer guaranteed protection against burglary, fire or other emergency. Any alarm system, whether commercial or domestic, is subject to compromise or failure to warn for a variety of reasons.

Therefore, good installation practices, thorough testing, and regular maintenance by the installation company and frequent testing by the user are essential to ensure continuous satisfactory operation of the system. It is recommended that the installation company offer a maintenance program and instruct the user with the correct procedure for use and testing of the system.

ELAB1543 SigNET Series User Guide, Issue 08, July 2009

Europlex Technologies [IRL] Ltd.
Clonshaugh Business and Technology Park,
Clonshaugh,
Dublin 17,
Ireland.

Tel: +353 (0) 1 2500500
Fax: +353 (0) 1 2500592

Europlex Technologies (UK) Limited
Innovation Centre,
Cranfield University Technology Park,
University Way, Cranfield,
Bedfordshire, MK43 0BT,
United Kingdom.
Tel. +44 (0) 8700 600 140
Fax. +44 (0) 8453 307 240

E-Mail: sales@europlex.ie
Company Web Site address: www.europlex.ie
Technical Support: tech@europlex.ie

Table of Contents

Introducing the SigNET System

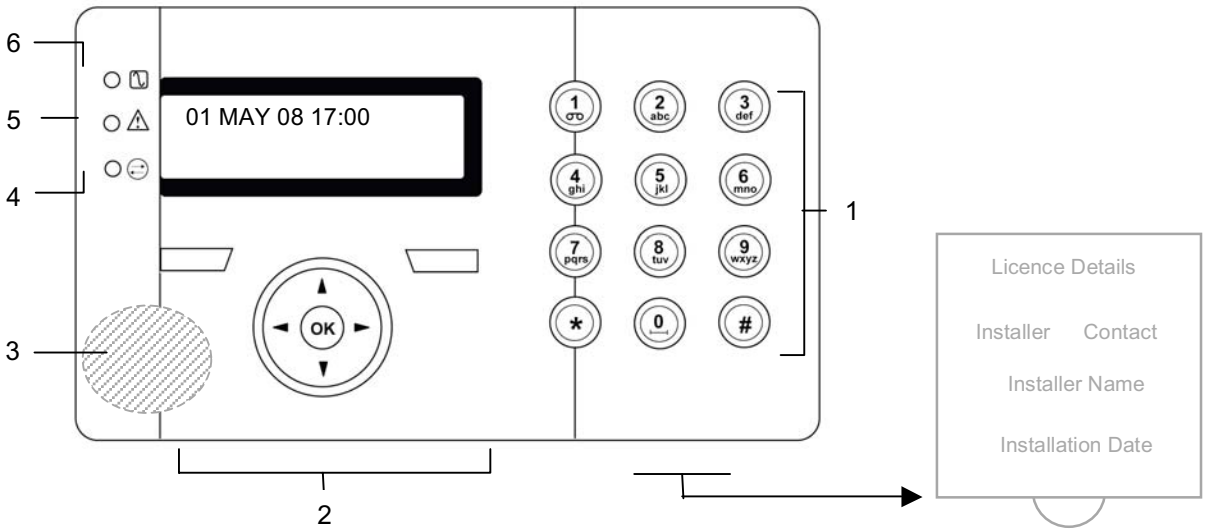
The SigNET Series 100/200/300 [herein referred to as SigNET systems] systems must be installed by qualified installation personnel. When the installation has been completed, the installer provides users with User Codes to set/arm or unset/disarm, and to configure the system as required. The SigNET 100 is a Grade 2 system where as the SigNET 200 / 300 series can be Grade 2 or 3 depending upon the installation – See Appendix G. All system are designed and built to Environmental class II indoor general.

Using the Keypad

The SigNET Keypad is a wall-mounted programming interface unit that allows users to enter User Programming menus (password protected), and to perform operational procedures on the system. The Keypad unit includes an integral front tamper switch and has a 2 line x 16-character display. Three LEDs provide information on AC power, system alerts, and communications status. The Keypad features easy-to-use navigation to assist in locating required programming options, and has two context sensitive soft keys (left and right) for selecting the required menu or program setting.

The SigNET Keypad may be factory fitted with a Portable ACE (PACE) proximity device reader and, optionally for European markets, a wireless module for the enrolment of wireless sensors.

Figure 1 – SigNET Keypad



1 Keypad

12 x alphanumeric keys for numeric and text data entry

2 Programming Keys

1 x multi-functional navigation key

2 x context sensitive programming keys (left and right)

3 Portable PACE Receiver Area

4 Comms LED

5 System Alert LED

6 AC Mains LED

Pull-down Information Tab

The installer contact and licence details are located on the pull down information tab at the rear of the unit

Table 1 – LED Status Indicators

LED	Description
AC Mains LED (green)	Indicates presence or failure of the Mains supply **FLASHING:** AC Mains fault detected **STEADY:** AC Mains OK
System Alert (yellow)	Indicates a system alert **FLASHING:** System Alert detected; display indicates the location and nature of the alert. If the system is SET, no indication of system alerts is given. **OFF:** No alert detected
Comms LED (red)	Indicates status of the E-BUS communications when in FULL ENGINEER/FULL INSTALLER programming

1.1 Using the Keypad Interface

Figure 2 – Keypad Interface

TOP LINE OF DISPLAY

In the normal state, displays the current date and time.

In Programming Mode, this line displays one of the following:

→ The programming feature to be selected

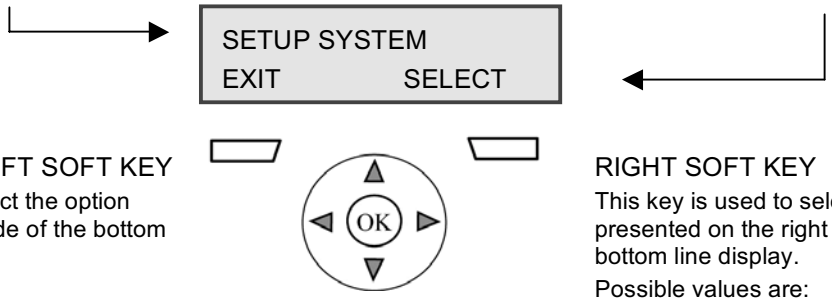
→ The current setting of the selected feature

During an alert condition, this line displays the nature of the current alert

BOTTOM LINE OF DISPLAY

In the normal state, this line is blank.

In Programming Mode, this line displays options available to the user. These options align over the left and right soft keys for selection as required.



LEFT SOFT KEY

This key is used to select the option presented on the left side of the bottom line display.

Possible values are:

→ EXIT to exit programming

→ BACK to return to previous menu

RIGHT SOFT KEY

This key is used to select the option presented on the right side of the bottom line display.

Possible values are:

→ SELECT to select the option displayed on the top line

→ ENTER to enter the data displayed on the top line

→ SAVE to save a setting

MULTI-FUNCTION NAVIGATION KEYS

OK — The OK button acts as a SELECT key for the menu option displayed on the top line and also as an ENTER/SAVE key for data display on the top line.

▶ — In Programming Mode, the right arrow key advances the user through the menus in the same way as pressing the SELECT option (right soft key).

In data entry mode, press this key to move the cursor one position to the right

◀ — In Programming Mode, the left arrow key returns the user to the previous menu level. Pressing this key when in the top menu level exits the user from programming.

In data entry mode, press this key to move the cursor one position to the left.

▲ — In Programming Mode, the up arrow key moves the user to a previous programming option in the same menu level. Continually press this key to scroll through all programming options available on the current menu level.

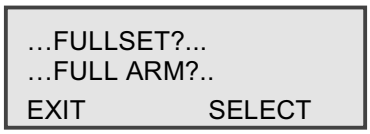
In alphanumeric mode, press this key over a lower case character to change the character to upper case.

▼ — In Programming Mode, the down arrow key moves the user to the next programming option in the same menu level. Continually press this key to scroll through all programming options available on the current menu level.

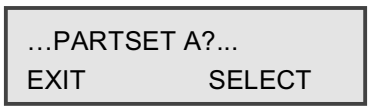
In alphanumeric mode, press this key over an upper case character to change the character to lower case.

User Operations on the System

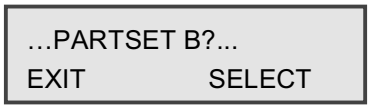
The following operations are available to users by entering a user code; these do not require menu navigation on the Keypad. User codes comprise 4, 5, or 6 digits, depending upon the programming grade of the system. See Appendix F for the number of variations per User Code.



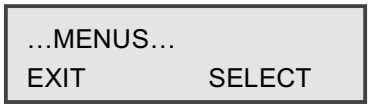
A user's permission rights, i.e. ability to see menus and options available on the SigNET system, are programmed by the installater. If users cannot see options described in this manual, they do not have rights to access such functionality.



When a code is entered, the digits display as asterixes and the left function key displays the QUIT option. This is for security reasons, so codes are not visible when entered.



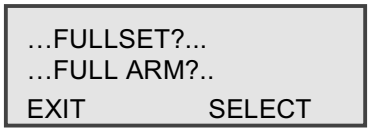
After entering a code, the following options are available: FULLSET/FULLARM, PARTSET A, PARTSET B, MENUS. Scroll these options by using the up/down arrow keys. An ellipsis (…) on accompanying graphics denotes when there is a choice of menu selection by scrolling.



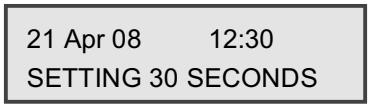
1.2 FULLSET/FULL ARM the System

The FULLSET/FULL ARM option provides the following functionality:

- Full protection to a building (opening of alarm zones activates alarm)
- Opening of entry/exit zones starts the entry timer. If the alarm is not unset/disarmed before the entry timer expires, the alarm is activated



To select the FULLSET/FULL ARM option, enter a valid user code, and press SELECT (right soft key). The second line displays the exit time and the buzzer sounds to indicate that the user should exit the building. When the system has been fully set, the LCD displays SYSTEM FULLSET/SYSTEM FULL ARM on the bottom line for approximately 10 seconds.

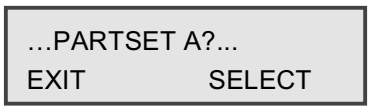


If the alarm fails to set/arm see Section 1.5, Fail to Set/Arm the System.

1.3 PARTSET A the System

The PARTSET A option provides the following functionality:

- Perimeter protection to a building while allowing free movement through the exit and access areas
- Exclusion of EXCLUDE A zones from protection
- Instant activation of alarm on selection of mode; by default there are no exit times associated with PARTSET A



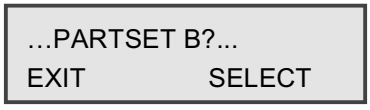
To select PARTSET A, enter a valid user code, scroll to the PARTSET A option and press SELECT (right soft key).

If the alarm fails to set/arm see Section 1.5, Fail to Set/Arm the System.

1.4 PARTSET B the System

The PARTSET B option provides the following functionality:

- Perimeter protection to a building while allowing free movement through the exit and access areas
- Exclusion of EXCLUDE B zones from protection
- Instant activation of alarm on selection of mode; by default there are no exit times associated with PARTSET B



To select PARTSET B, enter a valid user code, scroll to the PARTSET B option and press SELECT (right soft key).

Note Partset A and Partset B configuration modes are dependent upon how the system has been programmed.

1.5 Fail to Set/Arm the System

The system fails to set/arm if there is an open or fault condition detected on an alarm zone when the FULLSET/FULLARM or PARTSET A/B option is selected. The Keypad displays the zone number and description.

ZONE 1	OPEN
QUIT	FORCE

To set/arm the system, locate the zone and close or fix the fault. Repeat the FULLSET/FULLARM or PARTSET A/B operation.

1.6 Forced Set/Arm the System

The system can be forced to set/arm while an alarm zone is still open. This operation inhibits the open zone and sets/arms the system as normal.

…FORCED SET?...	
…FORCED ARM?..	
BACK	SELECT

If a user has the right to FORCE SET/FORCE ARM the system and an alarm zone is open, when the FULLSET/FULLARM or PARTSET option is selected, the Keypad buzzer beeps and the first line of the display indicates the open zone. The user is presented with the options to QUIT (left soft key) or FORCE (right soft key).

21 Apr 08	12:30
SETTING 30 SECONDS	

QUIT: Selecting this option aborts the attempt to set/arm the system and returns the user to User Programming.

21 Apr 08	12:30
SYSTEM FULLSET	
SYSTEM FULL ARM	

FORCE: Selecting this option inhibits the open zone and forces the system to set/arm.

1.7 Unset/Disarm the System

To UNSET/DISARM the system:

…UNSET?...	
…DISARM?…	
EXIT	SELECT

1. Enter a valid user code. The Keypad displays a prompt to unset/disarm the system.
2. To UNSET/DISARM the system, press SELECT (right soft key). The Keypad display indicates that the system is unset on the bottom line of the display for approximately five seconds. After this time has elapsed, the bottom line is cleared.

SYSTEM UNSET

3. If the alarm has been activated, entering the user code silences all bells and strobes and the message PANEL DISARMED displays on the Keypad for approximately five seconds.

PANEL DISARMED

4. The source of the alarm condition displays on the Keypad and the Alert LED flashes. The Keypad continues to display the alert until the alert is restored.

ALARM ZONE 2
FIRST ZONE

1.8 Restoring an Alarm Activation (Alert)

Alert conditions on the SigNET are indicated on the Keypad by a flashing yellow Alert LED and by activation of the buzzer. The Keypad indicates the location and nature of the alert condition. The ability of a user to restore alerts depends on the security grade setting of the system (in accordance with standards). An alert condition can only be restored once the fault or zone that caused the alert has been physically reset to its normal operating state; e.g. an open zone has been closed again or a severed EBUS connection re-established.

Users may be restricted from using the Restore feature if the installer chooses not to select 'Restore' within the User Rights menu for select users. Users who cannot restore an alert receive fault messages on the Keypad until the zone or fault condition is either inhibited or isolated.

ALARM ZONE 2
Sitting Room

Alarm conditions on the SigNET systems are indicated on the Keypad by a flashing yellow Alert LED (see Section 0, Using the Keypad) and by activation of the buzzer. The Keypad displays the location and nature of the alert condition.

Sitting Room	
QUIT	RESTORE

To restore an alert condition triggered by a zone opening:

1. Locate the open zone (displays on the Keypad) and restore the alarm sensor to its normal state by closing the door or window.
2. Enter a valid user code and select the RESTORE option (right soft key). The zone causing the alert displays on the top line.

ALL ALERTS
RESTORED

3. Press the right menu key to restore the alert. The message ALL ALERTS RESTORED displays and the flashing Alert LED turns off.

For system or communications type alert conditions (Mains failure or EBUS disconnect), locate the source of the alert condition and check that all wires and cables are properly connected.

For a tamper alert, ensure the lids on all enclosures and devices are correctly closed. If the physical fault cannot be restored to its normal operating state, contact the installater. The alarm system still operates by either inhibiting or isolating the fault condition.

Note

An Alert condition only displays on the Keypad when the system is UNSET/DISARMED. If the system is SET/ARMED when an alert condition occurs, the Keypad gives no indication of that alert condition until such time as the system is UNSET/DISARMED.

1.9 Coded Restore

The coded restore option is only available if the Security Grade of the system is set to Grade 3 or Engineer/Installer Configure. It provides the user with the ability to restore alert conditions that would normally only be available to the installer. To provide the user with this ability, it is necessary to protect this feature with a code.

To perform a coded restore on the system:

1. Ensure that the zone or fault that caused the alert condition has been physically restored to its normal operating state.
2. Contact the installer or the alarm receiving centre (ARC) before entering user programming and selecting the coded restore feature in the menus option. (Contact details should be available from the drop down label beneath the Keypad.)
3. Press SELECT on the Coded Restore option. A 6-digit reset code displays on the top line.
4. Provide 6-digit code to installer/ARC.
5. Receive newly generated code from installer/ARC.
6. Enter new code at the AUTH CODE prompt.
7. Press SELECT.

The message SYSTEM RESTORED displays on the top line of the display.

Note

The coded restore feature can only be operated from the Keypad. This feature is not accessible from the SigNET Series 200/300 web server browser.

1.10 Using 868MHz Wireless Fob

For European markets, if the optional 868MHz wireless receiver module is installed and configured on the Keypad or Controller and the user profile is configured for device and respective settings, the SigNET system enables functionality using an 868 MHz wireless fob. The installer configures the device and its settings, and users are instructed for activation of the device for the following commands:

- Set/Arm, Unset/Disarm
- Partset
- Clear Alerts/Restore
- X10 Functionality

Note

Forced set/arm with the RF fob: It is NOT possible to force set/arm the system with an RF fob even if the user assigned to the fob has this ability. Forced set/arm is only possible at the Keypad. This feature is not accessible from the SigNET Series 200/300 web server browser.

1.11 Using PACE

If a PACE reader is installed and configured on the SigNET Keypad, it is functional only with users of PACE-configured profiles.

If a Limited User's profile is configured for such device and functionality, once presented within 1cm of the Keypad's receiver area, the PACE enables set/arm and unset/disarm, denoted by the corresponding beeps.

If Manager and/or Standard Users' profiles are configured for such device and functionality, access to keypad is allowed using the PACE. Presentation of the device within 1cm of the Keypad's receiver area logs in the user and prompts menu options.

For additional security measures, installers have the option to set the PACE configurations to PIN and PACE. This prompts and requires user code following presentation of the PACE.

1.12 Using X10 Features

X10 is a technology that allows peripheral devices, such as lights, heaters, or appliances, to be controlled by the system and system events can be used to trigger outputs on the X10 devices. For example, a hall light could be configured to turn on when the front door of the house is opened. Alternatively, the function can be controlled directly at the Keypad.

The installer programs X10 settings and users are informed of the settings and the corresponding keys on the Keypad or the appropriate buttons of a configured 868MHz Wireless Fob.

On the keypad, turn an X10 feature on by pressing the hash (#) key and the feature number. The corresponding device turns on. To turn an X10 feature off, repeat the same keystrokes. The corresponding device turns off. The installer can fill in the following table for quick reference.

Table 2 – X10 Codes and Descriptions

Code #	Description
#0	
#1	
#2	
#3	
#4	
#5	
#6	
#7	
#8	
#9	

Note

X10 uses uni-directional communication and should not be used for critical devices because system interference can prevent the device from responding to the command.

1.13 Display Information

Whilst in any of the menus the * key can be used to toggle information for Zones / Area / Users / Doors / Outputs from the text description to the system number i.e. Front Door to Zone 1. Once the status has been changed then this will change the displayed information for all attributes.

User Menu Options

The following functions are available to users under MENUS on the Keypad.

In navigation mode following input of user code, the user selects one of a number of pre-defined programming options from a list. Pressing the up/down arrow keys scrolls the list of options available for selection. An ellipsis (…) on accompanying graphics denotes when there is a choice of menu selection by scrolling.

…INHIBIT…
EXIT SELECT

1.14 Inhibiting a Zone

Manager type users can manually inhibit zones on the system from the Keypad. Inhibiting a zone removes that zone from the system, silently disregarded, for one alarm set/arm period only.

…ZONES…
BACK SELECT

…ZONE1…
BACK SELECT

…INHIBIITED…
BACK SELECT

1. Press SELECT the INHIBIT option on the Keypad.
2. Scroll to the ZONES option and press SELECT (right soft key).
3. Scroll and select the required zone and toggle the setting from NOT INHIBITED to INHIBITED using the up/down arrow keys.
4. Press SELECT (right soft key) to exit user programming.

Note

Only the Alarm, Exit/Entry, Fire Exit and Line Zone types can be inhibited on the SigNET system. All other zone types are not displayed in the inhibit menus.

1.15 Isolating a Zone or Fault (Manager only)

Zones or faults on the system can be manually isolated from the Keypad. Isolation allows a zone to be removed from the system, silently disregarded, until it is set/armed for de-isolation by the user.

…ISOLATE…
EXIT SELECT

…ZONES…
BACK SELECT

…ZONE1…
BACK SELECT

…ISOLATED…
BACK SELECT

To isolate a zone:

1. Scroll to the ISOLATE option and press SELECT (right soft key).
2. Scroll to the ZONES option and press SELECT (right soft key).
3. A list of zones on the system displays. Select the required zone and toggle the entry from NOT ISOLATED to ISOLATED using the up/down arrow keys.
4. Press SELECT (right soft key) to exit User Programming.

1.16 Viewing Isolations

Any user can view zones or faults that have been manually isolated.

…ISOLATE…
EXIT SELECT

…VIEW ISOLATIONS…
BACK SELECT

ZONE1
Panic Button

To view isolations:

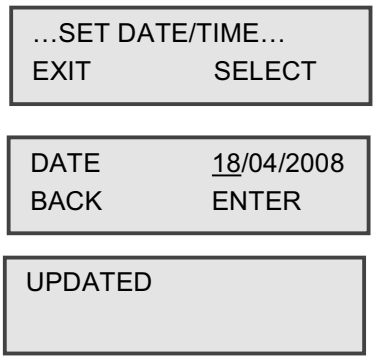
1. Scroll to the ISOLATE option and press SELECT (right soft key).
2. The display will give the user the option to view Isolations, to view press SELECT (right soft key).
3. A list of isolations will scroll on the system display, to quit from this press either of the two soft keys which will take system back to the View Isolation menu.

1.17 Set Date/Time

The date and time can be manually entered on the system (Manager type users). The time and date information displays on the Keypad to be used with time-related programming features.

To program the Date and Time:

1. Scroll to the SET DATE/TIME option and press SELECT (right soft key). The date displays on the top line, in format DD/MM/YYYY.
2. To enter a new date, press the required numeric keys. To move the cursor to the left and right, press the left and right arrow keys. Press ENTER (right soft key) to save the new date.
3. To enter a new time, press the required numeric keys. To move the cursor to the left and right, press the left and right arrow keys. Press ENTER (right soft key) to save the new time.

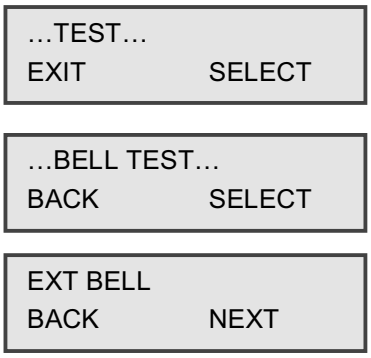


1.18 Perform Tests

Tests can be performed on the system to determine if bells, buzzers, and other audible devices operate correctly.

To perform a test on the system:

1. Scroll to the TEST option and press SELECT (right soft key).
2. Scroll and select BELL TEST, WALK TEST, or AUDIBLE OPTIONS.
3. When BELL TEST is selected, users may test each device by pressing NEXT for external bells, strobe, internal bells, or buzzer. The device sounds for each to verify it is operating correctly.
4. When WALK TEST is selected, users can test the operation of each alarm device by activating the device and listening for audible beeps at the Keypad.



1.19 Viewing the Event Log

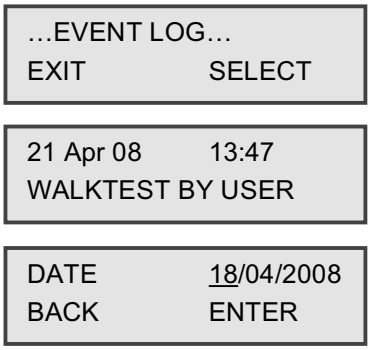
The most recent events on the system can be viewed by selecting the EVENT LOG option. The most recent events display on the bottom line with previous events displaying for one second in turn.

To view the event log on the Keypad:

1. Scroll to the EVENT LOG option and press SELECT (right soft key).

The Keypad displays the recent events on the system on the bottom line display for one second in turn.

2. To view an event from a particular date, enter the date with the numeric keys, in format DD/MM/YYYY.

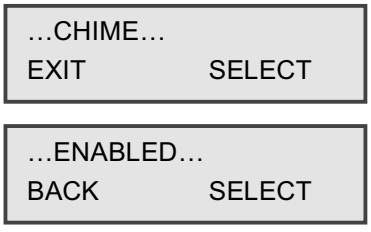


1.20 Enabling the Chime Function

The chime function can be enabled or disabled on all zones where the chime has been programmed as an audible alert feature.

To enable or disable the chime function:

1. Scroll to the CHIME option and press SELECT (right soft key).
2. Toggle between enable or disable for the chime function.



1.21 Creating System Users (Manager only)

In order to create a user for the system, the creator must be a Manager user type.

To create a user:

1. Scroll to the USERS option and press SELECT.
2. Scroll to ADD and press SELECT.

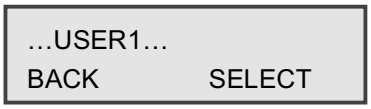
The system generates and displays next available user name.

3. Press SELECT for the default name and number, or enter a customized user name and press SELECT.
4. There are three types of users available: STANDARD USER, LIMITED USER, or MANAGER. Scroll to the preferred type and press SELECT. Note: user profiles may be changed at any time.

The system generates a default code for each new user. To change this code, overwrite the digits shown in the initial digits field.

5. Press SELECT to accept or enter a new user code and press SELECT.

The Keypad confirms that the new user has been created.



1.22 Changing a User Code

Users with profile rights to change their user code, may change codes.

Note, if the system is set for 5-digit user codes, a new 5-digit code must be entered. The system will not accept a code with fewer numbers than it is set to receive.

To change a user code:

1. Scroll to CHANGE CODE and press SELECT (right soft key).
2. A randomly generated user code appears.
3. Select new code, if acceptable. Or overwrite by entering the new user code and press ENTER (right soft key).
4. Confirm the new code, press SAVE (right soft key).
5. Press BACK (left soft key) to return to the previous screen to amend the code.

During the process if the display times out, the old code remains valid.

Note

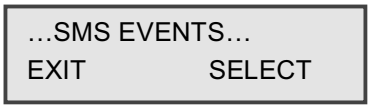
Where User Duress feature is enabled, consecutive user codes (i.e. 2906, 2907) are not permitted, as entering this code from the Keypad would activate a user duress event.

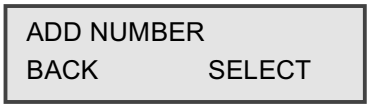
1.23 SMS EVENTS (Manager only)

The user can control the numbers used for SMS reporting and the events that are reported.

To Add a new SMS number:

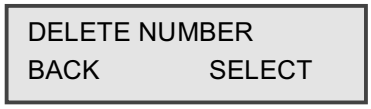
1. Scroll to SMS EVENTS and press SELECT (right soft key).
2. To add a new SMS number scroll to ADD NUMBER and press SELECT (right soft key).
3. The top line will then display SMS NUMBER briefly and then it will go black just leaving a curson on the left edge of the display. Use the keys on the keypad to enter into the telephone number that is required to receive the SMS message. Once the number has been entered then select ENTER (right soft key)
4. The system will automatically enable the SMS number and use the default settings for sending SMS status. (See Appendix C) for defaults. If the settings need to be changed then see EDIT SMS EVENTS.

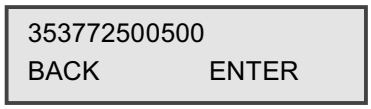




To delete an existing SMS number:

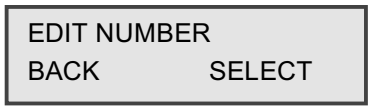
1. Within the SMS EVENTS option scroll to DELETE NUMBER and press SELECT (right soft key).
2. The first programmed number will be displayed, by using the up / down key the number to be deleted can be found. Once the number to be deleted is on the top line then select ENTER (right soft key) to delete the number.

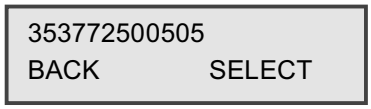


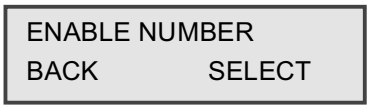


To edit a SMS number / change reported SMS EVENTS:

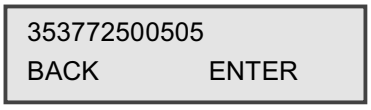
1. Within the SMS EVENTS option scroll to EDIT NUMBER and press SELECT (right soft key).
2. The first programmed number will be displayed, by using the up / down key the number to be edited can be found. Once the number to be edited is on the top line then press SELECT (right soft key) to edit the number.
3. A number of actions can be performed on this number – through the following menus ENABLE NUMBER / REPORTED EVENTS / SMS NUMBER
4. The ENABLE NUMBER allows the selected number to be enabled or disabled, to get these options press SELECT (right soft key).
    a. By using the up / down key either ENABLED or DISABLED can be selected, once the required option has been selected then press SELECT (right soft key).







5. The REPORTED EVENTS allows the user to edit which events will be reported to the selected SMS number, to get these options press SELECT (right soft key).
6. The first event will be displayed, by using the up / down key each event can be displayed. Once the required event to be edited is on the top line then press SELECT (right soft key) to enable/disable the event. If an event is enabled then it will be prefixed with a *.
7. The SMS NUMBER allows the selected number to be edited, to enter into this menu press SELECT (right soft key).
8. The ENABLE NUMBER allows the selected number to be enabled or disabled, to get these options press SELECT (right soft key).



9. The cursor will be under the first number, hence use the Left / Right keys to navigate along the number and then use the keypad to change the number as required. Once the required number is shown on the top line then press ENTER (right soft key).

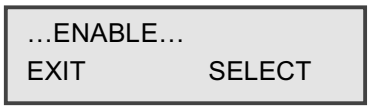
1.24 Grant Engineer/Installer/Manufacturer Access (Manager only)

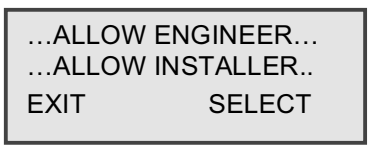
When engineer/installer or manufacturer access has been allowed, the Keypad displays the text ENGINEER ENABLE/INSTALLER ENABLE or MANUFACT ENABLE. Once access has been granted, the user cannot access the system until the engineer/installer has logged off.

To allow engineer/installer access:

1. Scroll to the GRANT ACCESS option and press SELECT (right soft key).
2. Select the ALLOW ENGINEER/ALLOW INSTALLER option (right soft key) and select ENABLED.

To disallow this access, follow the same path and toggle to DISABLED and press SELECT (right soft key).





Note

SigNET Series 100: Menu options on the SigNET 100 display allowing and disallowing Engineer/Installer Access only.

1.25 Door Control

Users with profile rights to Access control can control the status of any door on the system

To change a door status:

1. Scroll to DOOR CONTROL and press SELECT (right soft key).
2. Select the door that the state need to be changed on.
3. Select the status that the doors needs to be set to NORMAL / LOCKED / UNLOCKED and then press SELECT (right soft key).
4. Press BACK (left soft key) to return to the previous screen.

Note

SigNET Series 100: Does not support Door Control hence this menu will not be shown on a SigNET 100 controller

Appendix A: Standard User Settings

The operational features of the SigNET systems are described below. The installer informs users of their access rights assigned to each user profile. Depending on how the system has been programmed, users may have rights to all or some of these features.

Operation		User Profile Default	Description
FULLSET FULL ARM		Limited Standard Manager	The FULLSET/FULL ARM operation fully sets/arms the alarm system and provides full protection to a building (opening of any alarm zones activates the alarm). On selecting FULLSET/FULL ARM, the buzzer sounds and the Keypad display counts down the exit time period. Exit the building before this time period has expired. When the exit time period has expired, the system is set/armed and opening of entry/exit zones starts the entry timer. If the system is not Unset/Disarmed before the entry timer expires, the alarm is activated. To perform a FULLSET/FULL ARM, see Section 1.2.
PARTSET A		Standard Manager	The PARTSET A option provides perimeter protection to a building while allowing free movement through the exit and access areas. Zones that have been classified as **EXCLUDE A** remain unprotected in this mode. By default, there is no exit time; the system sets instantly on selection of this mode. An exit timer can be applied to this mode by enabling the Partset A timed variable. To perform a PARTSET A, see Section 1.3.
PARTSET B		Standard Manager	The PARTSET B option applies protection to all zones except those that have been classified as **EXCLUDE B**. By default there is no exit time; the system sets instantly on selection of this mode. An exit timer can be applied to this mode by enabling the Partset B timed variable. To perform a PARTSET B, see Section1.4.
FORCED SET FORCED ARM		Standard Manager	The FORCED SET/FORCED ARM option is presented on the Keypad display when an attempt is made to set/arm the system while an alarm zone is faulty or still open (the top line of the display shows the open zone). Selecting this option sets/arms the alarm and inhibits the zone for that period. To perform a FORCED SET/FORCED ARM, see Section 1.6.
UNSET DISARM		Limited Standard Manager	The UNSET/DISARM operation unsets/disarms the alarm. This menu option is only presented on the Keypad after an alarm has been activated and a valid user code has been entered. To UNSET/DISARM the system, see Section 1.7.
RESTORE		Standard Manager	The RESTORE operation restores an alert condition on the system and clears the alert message associated with that alert condition. An alert condition can only be restored after the zone(s) or fault(s) that triggered the alert condition have been restored to their normal operating state and the RESTORE option in user programming is selected for that zone. To RESTORE an alert, see Section 1.8.

Appendix B: User Configuration and Test Options

Operation		User Profile Default	Description
ISOLATE		Manager	Isolating a zone deactivates that zone until such time as the zone is de-isolated again. All zone types on the SigNET systems can be isolated. Use of this feature to deactivate faulty or open zones should be considered carefully; once a zone is isolated, it is ignored by the system and could be overlooked when setting/arming the system in the future, compromising the security of the premises. To isolate a zone, see Section 1.15.
INHIBIT		Standard Manager	Inhibiting a zone deactivates that zone for one alarm set period. Only alarm, entry/exit, fire exit and line zone types can be inhibited. This is the preferred method of deactivating a faulty or open zone as the fault or open condition is displayed on the Keypad each time the system is being set/armed to remind the user to attend to that zone. To inhibit a zone, see Section 1.14.
CHANGE CODE		Standard Manager	This menu option allows users to change their user codes. To change a user code, see Section 1.22.
GRANT ACCESS		Manager	This option allows users to grant access to manufacturer and engineer/installer programming. To grant access, see Section 1.24. (SigNET Series 100 allows only Engineer/installer Access.)
SET DATE / TIME		Standard Manager	Use this menu option to program the time and date on the system. Ensure the time and date information is accurate; these fields are presented in the event log when reporting system events. To set date or time, see Section 1.17.
TEST	 	Standard Manager	This menu option provides the following test features: 1. Bell test The bell test activates the external bells, strobe, internal bells, and buzzer in turn for 5 seconds to ensure their correct operation. 2. Walk test A walk test allows for testing of the operation of all alarm sensors on a system. When this option is selected, the Keypad displays the number of zones to test on the system. Activate each alarm sensor (by opening the door or window) and check for an audible beep at the Keypad. Isolated and inhibited zones are not included in the walk test. 3. Audible Options This option allows users to select which devices will activate during the walk test and which will be silent. To perform a test, see Section 1.18.
EVENT LOG		Standard Manager	This menu option displays the most recent event on the Keypad display. The event log details the time and date of each logged event. To view log, see Section 1.19.
CHIME		Standard Manager	All zones that have the CHIME attribute generate a short burst of audible tone on the Keypad buzzer when they are opened (while the system is unset/disarmed). This menu option allows for enabling or disabling of the chime feature on all zones. To enable or disable the chime feature, see Section 1.20.
SETUP SMS		Manager	This feature allows users to set up the SMS messaging service if a modem is installed on the system. For instructions on using the SMS feature, visit the downloads section of the Europlex web site at www.europlex-signet.com/downloads and download the SMS User Guide.
Door Control		Standard Manager	Allows a user to change the status of any door configured on the system, the door is selected then the status can be changed to any of the following states; Normal / unlocked / Locked. (Only available on SigNET 200 / 300 Series controllers)

Appendix C: SMS EVENTS

Event	Description
*Alarm	Alarm events
*Confirmed Alarm	Confirmed alarm events
Fault / Tampers	All system faults and Tamper events
Mode Changes	When the system is Set / Partset A / Partset B / Unset
Inhibit / Isolates	When any system event or zone is inhibited or isolated
Other events	These include the following; System power-up message User Code change Time change Engineer mode Man down test
Door	When any door events are triggered
Alarm restore	When any alarms are restored after unset
Fault restore	When any faults are restored after unset
*** This denotes that the event will be sent by SMS notification**	

Appendix D: AUTOMATIC INHIBITS

ACCESS CODES

For Grade 2 systems - after 10 unsuccessful attempts with the incorrect code the keypad will be disabled for 90 seconds, after a further 10 attempts with the incorrect code the keypad will be disabled for a further 90 seconds. Once a correct code has been entered it will reset the counter back to zero allowing for a further 10 attempts before disablement.

For Grade 3 systems - after 10 unsuccessful attempts with the incorrect code the keypad will be disabled for 90 seconds, after each further attempt with an incorrect code the keypad will be disabled for a further 90 seconds. Once a correct code has been entered it will reset the counter back to zero allowing for a further 10 attempts before disablement.

ZONES

When the UK & Commercial are selected the system will provide DD243 functionality, in this instance the system will inhibit zones under the following conditions;

- Entry zone will not cause an alarm signal to the central station and cannot be part of a confirmed alarm and hence will be effectively inhibited as required by DD243.
- If a single zone is trigged and another zone is not triggered within the confirmation time (30mins default) but the first zone is still trigged then the first zone will be automatically be inhibited and no further alarms will be trigged from this zone during the set period.

Appendix E: User Shortcuts

User shortcuts allow the user to enter their user code and then a number. This takes a user directly to the option rather than navigating through the menus.

Shortcut code	Description
00	Grant Engineer Access (this can only be used with a manager code)
1	UNSET system
2	FULLSET system
3	PARTSET A
4	PARTSET B

Appendix F: User Codes

The system supports 4, 5, 6, 7 or 8 PIN Digits for each user, the translation of how many logical combinations / variations can be found in the table below;

Table 3

NUMBER OF DIGITS	NUMBER OF VARIATIONS
4	10,000
5	100,000
6	10,000,000
7	10,000,000
8	100,000,000

All User Codes are valid, hence for a 4 digit code the numbers can be from 0000 through to 9999 with any combination allowed in between.

Appendix G: Zone Chart

System Name:
System Grade:

Zone #	Description