iconnect

Two-Way Wireless

Installation Manual

For quick installation information please refer to the iConnect Quick Start Installation Guide provided on our website: www.electronics-line.com

EL

UPGRADING
EVERYDAY
SECURITY

Table of Contents

1. Introduction 1
1.1. Documentation Conventions 1
1.2. Specifications 2
1.3. System Overview 3
1.4. Hardware Layout 4

2. System Installation 7
2.1. Pre-Installation Planning 7
2.2. Installation Procedure 8
2.3. Back Tamper 11
2.4. Internet Communication Setup 12

3. Basic System Operation 13
3.1. Front Panel Layout 13
3.2. Front Panel System Status LEDs 13
3.3. Front Panel Keypad and Wireless LCD Keypad 13
3.4. LCD Display 14
3.5. Audible Notification 15
3.6. Arming and Disarming 16
3.7. Additional Arming Options 18

4. Advanced System Operation 20
4.1. Menu Navigation 20
4.2. Cancel Report 20
4.3. Zone Bypassing/Unbypassing 21
4.4. User Codes 21
4.5. Follow-Me 23
4.6. Event Log 23
4.7. Service Menu 24

5. Telecontrol and Two-Way Audio 29
5.1. Incoming Calls 29
5.2. Outgoing Calls 31

6. Home Automation and PGM Control 33
6.1. Keypad Control 33
6.2. Keyfob Control 33
6.3. Telephone Control 33
6.4. Scheduling (not relevant to PGM) 34

7. Devices 35
7.1. Device Descriptors 35
7.2. Wireless Devices 35
7.3. Zones 36
7.4. Keyfobs 40
7.5. Wireless Keypads 41
7.6. Repeaters 41
7.7. Wireless Siren 41
7.8. Smartkeys 42

8. Entry/Exit Timers and System Tones 43
8.1. Entry/Exit Delay 43
8.2. Arm on Exit 43
8.3. Supplementary Entry Delay 43

8.4. Entry Deviation ... 43
8.5. Arming Tones ... 43
8.6. Home Automation Tones ... 44
8.7. System Trouble Tones ... 44
8.8. Tones Options ... 45

9. System Options ... 46
9.1. Swinger Setting ... 46
9.2. Code Lockout ... 46
9.3. Arm/Disarm Options ... 46
9.4. Panic Alarm ... 47
9.5. AC Loss Delay ... 48
9.6. Display Options ... 48
9.7. PGM Output Options ... 49
9.8. Guard Code ... 50
9.9. "No Arm" Indication ... 51
9.10. Jamming Detection ... 51
9.11. "No Motion" Time ... 51
9.12. Microphone/Speaker Options ... 51
9.13. Vocal Messages ... 52
9.14. Installer Access ... 52
9.15. Auto Log View ... 52
9.16. Daylight Savings ... 52
9.17. Standard Type ... 53
9.18. Battery Type ... 54
9.19. Report Fail Trouble ... 54
9.20. Immediate Arming from WUApp ... 54
9.21. T014A Standard ... 54
9.22. Alarm Memory Reset ... 54

10. Communications ... 55
10.1. System Reporting ... 55
10.2. Report Cycles ... 56
10.3. Vocal Message Dialer ... 57
10.4. Remote Programming ... 58
10.5. Service Call ... 59
10.6. Communications Options ... 60
10.7. GSM Options ... 61
10.8. TWA Event Report Options ... 63
10.9. Event Options for Central Station Reporting ... 64
10.10. Vocal Message Dialer Event Options ... 65

11. Internet Options ... 67
11.1. ELAS Connection Parameters ... 67
11.2. Control System Parameters ... 67
11.3. GPRS Network Parameters ... 68
11.4. LAN Network Parameters ... 68

12. Home Automation Programming ... 70
12.1. X10 Overview ... 70
12.2. HA Units ... 70
12.3. House Code ... 72
12.4. HA Control ... 72

13. System Initialization 73
13.1. Initialization 73
13.2. Default Program Restore 73
13.3. Clear User Codes 73
13.4. Clear Wireless Transmitters 73
13.5. Find Modules 73

Appendix A: Menu Structure 74

Appendix B: Transmitter Installation 81
PIR Detectors (EL-4755/EL-4755PI) 81
PIR Detectors (EL-4745/EL-4745PI) 84
Dual Magnetic Contact/Universal Transmitter (EL-4601DZ) 87
Universal Transmitter (EL-4602) 89
Vibration Detector (EL-4607) 90
Smoke Detector (EL-4703) 92
Keyfobs (EL-4714) 98
Keyfobs (EL-4711M/P) 99
Wireless LCD Keypad (EL-4727) 101
Gas Leak Detector (EL-4762) 102
Carbon Monoxide Detector (EL-4764) 105
Flood Detector (EL-4761) 109
Indoor Siren (EL-4723) 111
Outdoor Siren and Strobe (EL-4726T) 113
I/O Expander Module (EL-4770) 115
Transmitter Specifications 120

Appendix C: Web User Application 122

Appendix D: Event Table* 130

Appendix E: Zone Types 133

1. Introduction

This manual is designed to help you install the iConnect ② Control System[1]. We strongly urge you to read through this manual, in its entirety, before beginning the installation process so that you can best understand all that this security system has to offer. This manual is not intended for end user use. End users are encouraged to read the user manual provided with the system. If you have any questions concerning any of the procedures described in this manual please contact Electronics Line 3000 Ltd. at (+972-3) 963-7777.

1.1. Documentation Conventions

Throughout the manual, we have tried to include all of the operating and programming functions using a similar structure and order as they appear in the menu. A detailed explanation of how to navigate the Control System's menu is included in Menu Navigation. In order to simplify the procedures that appear in the rest of this manual, the following conventions are used:

Table 1-1: Documentation Conventions

Item…	**Description…**
Select…	Use the arrow keys to scroll through the options and press '√'.
From the Event Log Menu, select Clear Log.	Enter the main menu by pressing '√'and entering your user code. Using the arrow keys, navigate until you reach Event Log and press '√'. Using the arrow keys, navigate until you reach Clear Log and press '√'.
From the Service menu, select Set Time/Date, Set Date.	The same as above only this time you are navigating through three menu levels.
[7012]	The shortcut to a specific menu item from the main menu. In this case, this is the shortcut for Set Date. These appear in the procedures as an additional aid to menu navigation.
[#5]	A shortcut to a specific item in a sub-menu. For example, [#5] is the shortcut to Bell enable disable in the sub-menu that is opened once you have selected the detector you want to program.
'√'	The symbol on a key that appears on the keypad
5. Interface Test	The text that actually appears on the LCD display (bold).
☞ Due to the occurrence	Important note, please pay attention.
⚠ The iConnect ② Control System is …	Caution: description of a potentially hazardous situation.
Warning……Do not test with flame!	Warning: description of a potentially hazardous situation that is a threat to human life.
nsai EN 50131-1	EN Note – restrictions and settings demanded by the standard EN 50131-1

[1] The terms *Control System, Control Panel,* and *CP* refer to the same notion.

1.2. Specifications

General

Zones: 32 wireless zones, 2 hardwire zones (Zone 33-34), or zones 1 – 8 as wired zones, zones 9 – 32 as wireless and 2 hardwire zone (Zone 33, 34).

Wireless Keyfobs: 19 (Controlled or Non-controlled)

Wireless Keypads: up to 4

Wireless Repeaters: up to 4

Smartkeys: 12 (Controlled or Non-controlled)

Wireless I/O Zone Expanders: 2

Wireless Siren: up to 4

Wired Siren: 1

User Codes: 32

Arming Methods: Full, Part or Perimeter

Event Log: 1022 event capacity, time and date stamped

Weight: 1.350g

Dimensions: 270 x 222 x 50mm

Communications

Event Reporting Accounts: up to 6, including Central Station, Follow-Me, and Voice

Telephone Numbers: 6 event reporting accounts, RP Callback, Service Call

Communication Interface Options: GPRS/Ethernet or Ethernet/PSTN

Home Automation

Control Medium: Power-line carrier

Protocol: X10

HA Units: 16 individually addressed

Receiver

Type: Super-heterodyne, fixed frequency

Frequency: 868MHz, 433MHz (optional)

Data Encryption: SecuriCode™

Electrical[*]

Power Input: 230VAC, 50Hz

AC Current Consumption (GPRS Configuration): 30mA (alarm), 17mA (standby)

AC Current Consumption (Ethernet Configuration): 35mA (alarm), 17mA (standby)

DC Current Consumption (GPRS Configuration): 280mA (alarm), 130mA (standby)

DC Current Consumption (Ethernet Configuration): 330mA (alarm), 135mA (standby)

Maximum Auxiliary Output Current Rating : 50mA

Battery low: below 7.15V

Backup Battery Pack: 1 x 7.2V/1.8Ah Part No. BT5780

(6 x 1.2V Ni-MH rechargeable cells, size AA)

The maximum charging current for the BT-5780 is 5.4A

For EN-50131 standard, 1.5Ah battery is mandatory

Fuse Ratings: 63mA/250V for 230VAC – Part No. EF1063,

PGM Relay Output Contact Rating: 100mA (max. load)

Built-in Siren: 93dB @ 10ft

Tamper Switch: N.C.

Operating Temperature: 0-60°C /32-140°F

Complies with EN-50131-3 Grade 2 Class II
Power Supply Type A

Power connection to the unit should be according to the national electrical code for permanent installation.
The power supply should be fed from a readily accessible disconnect device.
If the unit is permanently wired to the mains power, use a 2-pole disconnect device (15A max.) and the wires should be min. 0.75mm^2 in a conduit of at least 16mm.
If the mains power is connected with a plug, the plug should be indicated as the disconnecting device and the socket shall be max. 2m from the Control System.
Batteries shall be provided by a distributor and replaced by authorized service personnel.
The backup battery pack should be replaced every five years.
Batteries should be stored in a cool, dry place.

[*] [*] The measurements are with fully charged battery. AC current was measured on fuse F1 and DC current was measured on fuse F2.

1.3. System Overview

The iConnect Control System is a full-featured 2-way wireless control system that is expected to provide a solution to the needs of most residential installations. This system has been developed based upon a design concept geared towards easy installation and use. With this in mind, the user interface is based on a simple, menu-driven model that suits the essential requirements of both the user and installer alike. You can program the iConnect Control System on-site using the on-Front Panel keypad or PC, or off-site via a PC using local programming option of the Remote Programmer.

Figure 1-1 shows the components that make up the system and the system's interaction with external communication networks for all the configurations.

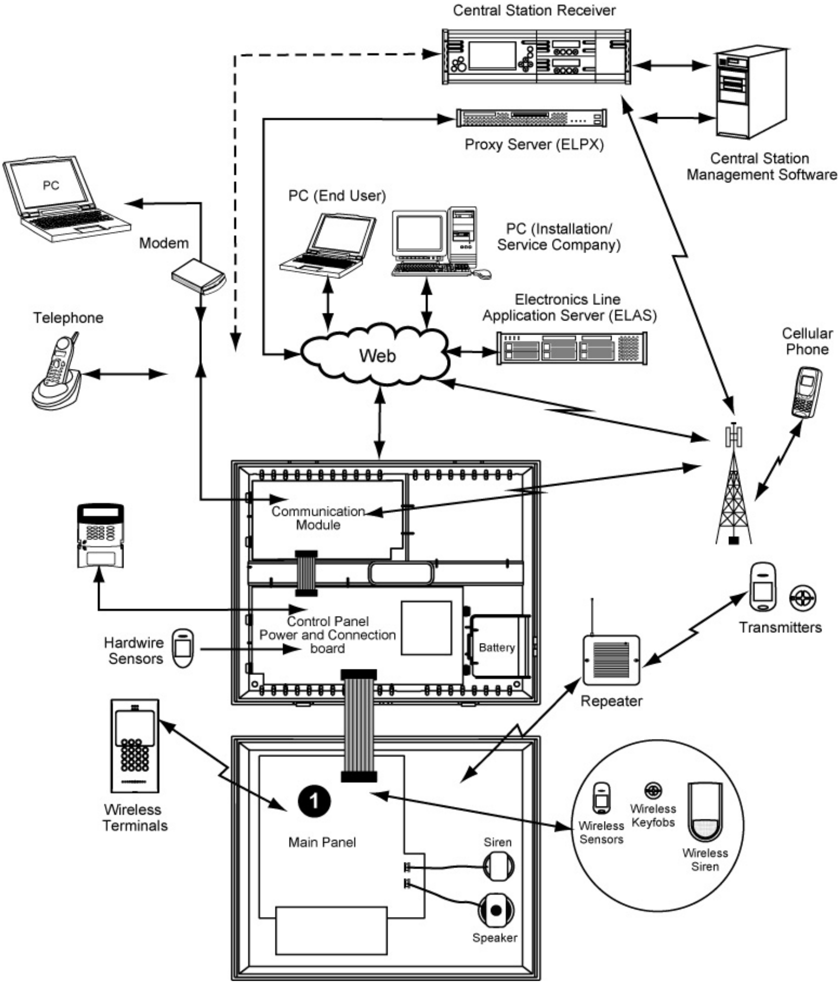


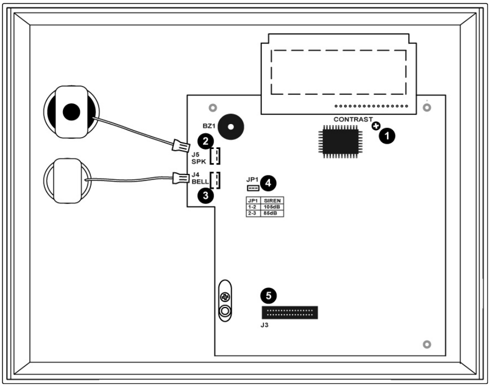
Figure 1-1: System Architecture

❶ See Figure 1-2

The system offers GPRS and Ethernet network connectivity, providing high-speed central station reporting via a GPRS or Ethernet interface.

The Electronics Line Application Server (ELAS) handles all communication between the system, service providers and web users enabling monitoring and control to be performed via the Web.

Central station communication and remote parameters programming and maintenance employ Ethernet, GPRS, GSM or standard PSTN communication. SMS messaging provides an innovative method used for both central station and Follow-Me user monitoring. Additionally, SMS messages can be sent to the iConnect Control System enabling the user to send commands to the system from anywhere on the planet.



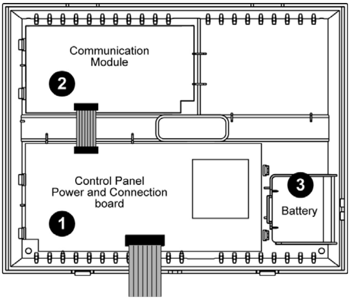
1. Contrast LCD
2. Speaker
3. Bell
4. Jumper for siren volume (see Table 1-2, Jumper Settings)
5. Flat Cable

Figure 1-2: Main Panel

The Main panel has connectors to the built-in Siren and the Speaker.

1.4. Hardware Layout

The aim of this section is to acquaint you with the various circuits that make up the system. Apart from the Main Panel, each peripheral module is available as an optional extra designed for installation inside the plastic housing.

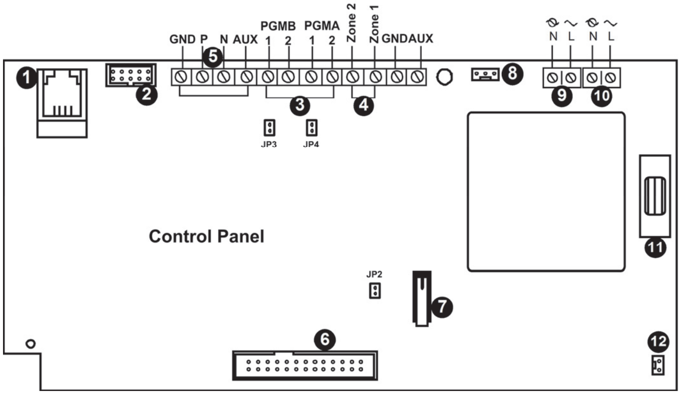


1. Power and Connection board
2. Communication module (GPRS + GSM + LAN)
3. Backup battery pack

Figure 1-3: System Layout

1.4.1. Power Supply and Connection Board

The Power and Connection Board is the brain of the system and connects to various peripheral modules using a number of interface connectors. Additionally the Power and Connection Board includes a programmable output, and hardwired zones input.



1. Interphone module connector
2. Flat-cable interface connector to communication module
3. Programmable relay output (100mA max. load) and jumpers for PGM control (JP3, JP4)
4. Wired detector zone (Zone 33, 34)
5. System bus terminal block (Wired Zone Module)
6. Flat-cable interface connector to Main board (LCD keypad, built-in speaker, microphone and siren)
7. Front tamper switch
8. Interface connector to Home Automation module
9. AC power terminal block
10. Home Automation module terminal block
11. AC power protection fuse
12. Backup battery connector and jumper for backup battery discharge protection (JP2)

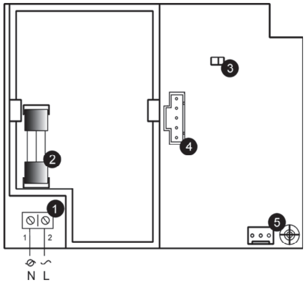
Figure 1-4: Power Supply and Connection Board

Table 1-2: Jumper Settings

JPI	Siren Strength (see Figure 1-2, Main Panel)	Installed: 105dB Removed: 85dB
JP2	Backup Battery Protection	Installed: Activated (If a continuous AC power outage occurs, the panel automatically disconnects the battery when its backup battery voltage drops to a certain level, in order to prevent "deep discharge" that may damage the battery) Remove: Disabled (The battery may be totally discharged during continuous AC failure; therefore battery replacement may be required.
JP3	PGM 1	Installed: Open Collector Removed: Dry Contact
JP4	PGM 2	Installed: Open Collector Removed: Dry Contact

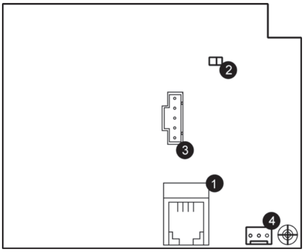
1.4.2. Home Automation Module

The Home Automation module provides the system with an interface to the power-line network, enabling control over 16 home automation units employing the X10 protocol via an external or internal Power-line Interface (PLI), depending on your system configuration. The illustrations below show the HA module used in the systems with internal PLI (for use in 220V, 50Hz A.C. power systems), and with external PLI (for use in 110V, 60Hz A.C. power systems).



1. Power-line terminal connections to Main Board (1 - Neutral; 2 - Live)
2. Fuse
3. LED Indicator
4. Flash programming connector
5. Interface connector to Main Board

Figure 1-5: Home Automation Module (Internal PLI Module)



1. External PLI connector
2. LED indicator
3. Flash programming connector
4. Interface connector to Main Board

Figure 1-6: Home Automation Module (External PLI Module)

☞ For external X10 PLI, we recommend to use the two-way TTL/CMOS interface such as XM10E module connected to the HA module with an RJ11 cable wired, as shown below.

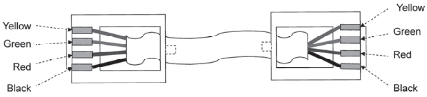


Figure 1-7: RJ11 wiring diagram

1.4.3. GPRS/LAN Communication Module

The GPRS/LAN Communication module enables the iConnect Control System to communicate to the WEB via cellular networks, perform remote firmware update, send or receive SMS messages, and implement cellular 2-way audio communication.

1.4.4. LAN/PSTN Module

The LAN/PSTN Communication module enables the iConnect Control System to communicate to the WEB via Ethernet, perform remote firmware update, and implement PSTN backup communication with event reporting and Two-Way Audio (TWA) control.

☞ Do not use VoIP phone lines for communication to the central monitoring station. In certain cases the system may not transmit alarm signals successfully over the VoIP network.

⚠ To reduce the risk of fire, use only No. 26AWG or larger telecommunication wire.

2. System Installation

The following chapter explains how to install the system and provides guidelines and tips on how to optimize the installation. It is recommended that you familiarize yourself with the various circuit boards that make up the system – see p. 4, 1.4 Hardware Layout.

2.1. Pre-Installation Planning

Before starting the installation procedure, it is worthwhile to draw a rough sketch of the building and determine the required position for the Control System and each wireless device.

When deciding on the placement for installation, consider the following:

- Mount the Control System in a location with easy access to telephone and power connections.
- Mount the Control System in a location that provides easy connection to the router.
- For best performance of the GPRS Communication module, the Control System should be mounted in a position where the GSM signal is strong.
- Refer to the following section in order to choose the optimal location for wireless devices in relation to the Control System.

2.1.1. Wireless Installation Guidelines

In order to optimize wireless communication, consider the following guidelines:

- Whenever possible, mount the Control System centrally in relation to wireless detectors.
- Avoid installation in close proximity to sources of high noise or radio frequency interference. For example, metal air conditioner/heater ducts and circuit breaker boxes.
- Minimize the distance between the Control System and transmitters.
- Minimize the number of obstacles between the Control System and transmitters.

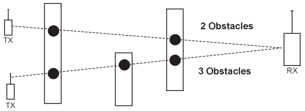


Figure 2-1: Minimizing Obstacles

- Metal based construction materials, such as steel reinforced concrete walls, reduce the range of radio transmissions.

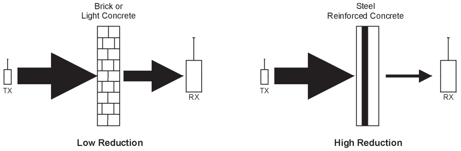


Figure 2-2: Considering Construction Materials

- The reduction of the RF signals' strength is directly proportional to the thickness of the obstacle, assuming that the obstacles are of identical material.

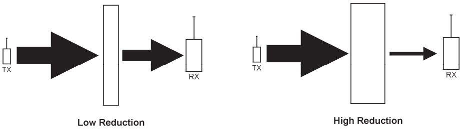


Figure 2-3: Considering Thickness of Obstacles

2.2. Installation Procedure

The iConnect ② Control System Kit consists of:

- Control System
- Quick Start Installation Guide
- Quick User Guide
- Mounting Guide
- Plastic bag with Cable Clamp, Cable Clamp screw, Housing Screw,

After unpacking the kit and making certain that you have all the necessary equipment, it is recommended that you install the system as follows:

STEP 1: Temporarily power up the system and install the SIM card.

STEP 2: Selecting language and defaults

STEP 3: Establishing an RF wireless network.

STEP 4: Register the transmitters.

STEP 5: Test the chosen mounting location.

STEP 6: Program the relevant Internet options.

STEP 7: Permanently install the Control System and transmitters.

2.2.1. Step 1 – Temporarily Power up the System and Install SIM Card

In order to register and test transmitters, it is necessary to temporarily power up the Control System before permanently installing it.

1. Remove the housing screw located at the bottom of the front cover as shown in Figure 2-4.
2. Insert a screwdriver between the front and back panels of the housing; carefully twist it to release the tabs.
3. Lift the front cover away from the back of the housing. You will notice that the front cover is attached to the back with two fastening bands and the hardwire LCD keypad's flat cable.

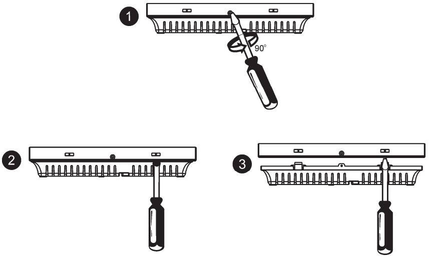


Figure 2-4: Opening the Housing

☞ The Control System is supplied without AC cable. Please use Standard Two-Pin European Plug cable only. For the Cable Clamp, use the screw and the washer supplied in your kit to replace the PCB screw.

4. Open the SIM card holder on the Communication Board, insert the SIM card.
5. Close the Housing.
6. Plug the Power AC cable into the wall outlet.

☞ In five minutes since power-up, the siren will sound. To silence the siren, enter your user code (default user code is 1234).

At this stage, do not connect the backup battery. Ignore any trouble conditions that may appear on the LCD Display (e.g. Low Battery)

2.2.2. Step 2: Selecting Language and Defaults

The Control System supports several languages. Upon power-up the control system automatically opens the language and default settings menu. Language and defaults settings must be defined before any configuration parameters are set or any transmitters registered.

To define language and defaults settings:

1. Press '√'.
2. Enter your Installer code (the default Installer code is 1111).
3. From the Programming menu, select Devices [971] (Programming, Initialize, Init. All).
4. Select the default setting and press '√'.
5. Select a language (Voice + LCD display) and press '√'.
6. Press '√' once more to restart the Control System.

2.2.3. Step 3 – Establishing an RF Wireless Network

In order to provide the best possible installation environment you need to establish an effective RF wireless network. RF wireless network establishment should be performed prior to any wireless device allocation in order to select the best RF channel according to the levels of background "noise" in the installation environment. This procedure helps the devices, once registered, to effectively deal with any high levels of background noise that may be generated by additional appliances operating at similar frequencies in the installation area.

To establish an RF wireless network:

1. Press '√'.
2. Enter your Installer code.
3. From the Programming menu, select Devices [9191] (Programming, Devices, RF Network Establishment).
4. Press '√'. The Control System scans several RF channels and selects the channel with lower "noise level".
5. When Save? is displayed on the Control System's LCD, press '√'.

☞ Network establishment must be performed prior to wireless device allocation.

If required, after the initial network is established, you can calibrate the receiver again only after deleting the network by selecting [9193] (Programming, Devices, RF Network, Delete Network).

2.2.4. Step 4 – Registering Transmitters

For the Control System to recognize a device, its transmitter must be registered. In general terms, transmitter registration means sending two transmissions from a device when the Control System is in Registration mode.

To register a device:

1. Press '√'.
2. Enter your Installer code.
3. Enter [91] (Programming, Devices) to enter the Devices menu.
4. Press the menu navigation keys (▲/▼), until the type of device you want to register appears on the LCD display (e.g. Zones or Keypads).
5. Press '√'.
6. Press the menu navigation keys (▲/▼), until the exact device you want to register appears on the LCD display (e.g. Zone 3 or Keypad 2).
7. Press '√'. If a device has not been registered at the chosen location, the Control System initiates Registration mode. During Registration mode, the system waits for two transmissions from the device.

   ☞ If a device has already been registered at the selected location, or in another location, the system will not initiate Registration mode.
8. Send two transmissions from the device – refer to each device's installation instructions in Appendix B for further details.
9. When Save? is displayed on the Control System's LCD, press '√'.

   The display automatically switches to the next option for that device. For example, pressing '√' to confirm Zone registration automatically moves you to the Zone Type option.
10. Continue entering other parameters for the chosen device.

2.2.5. Step 4 – Testing the Chosen Mounting Location

Once all of the transmitters are registered, it is recommended that you test the chosen mounting locations before permanently mounting the Control System and wireless devices. You can test the transmitter signal strength using the Test features.

To test transmitter signal strength:

1. Press '√'.
2. Enter your Installer code.
3. Enter [7042] (Service, Transmitters, TX Test) to initiate TX Test mode.
4. Activate the transmitter you wish to test; the transmitter's details appear on the Control System's LCD.
   Additionally, between one and four tones are sounded to indicate the transmitter's signal strength. If four tones are sounded, the transmitter is in the best possible location – see Transmitters for further information.
5. After you have tested each transmitter, press X to exit TX Test mode.

When using the GPRS Module, test the GSM signal strength.

To test the GSM signal strength:

1. Press '√'.
2. Enter your Installer code.
3. Enter [706] (Service, GSM Signal); the signal strength of the cellular network is displayed – see p. 27, 4.7.10 GSM Signal Strength for further information.
4. Check the RSSI (Received Signal Strength Indication) level of the installation environment using the system's RSSI meter.

To view the Environmental RSSI level reading:

- Enter [7044] (Service, Transmitters, Env. RSSI); the current RSSI level is displayed – see p.26, Environmental RSSI, for further information.

2.2.6. Step 5 – Programming Internet Options

Internet settings are mostly pre-programmed in the Control System's default settings. The only settings you need to program are the Control System's ID & Password (provided by the ELAS administrator). The following procedures explain how to program the Control System's ID (CPID) and Password. For further information regarding other Internet options and settings, see p. 67, 11 Internet Options.

To program the CPID:

1. Press '√'.
2. Enter your Installer code.
3. Enter [9573] (Programming, Communications, Internet, CPID).
4. Enter an ID using the alphanumeric keypad. The ID length must be six up to sixteen characters. The ID must begin with a letter.
5. Press '√'.

To program the Control System's password:

1. Press '√'.
2. Enter your Installer code.
3. Enter [9574] (Programming, Communications, Internet, CP Password).
4. Enter a password using the alphanumeric keypad.

   The password length must be six up to sixteen characters. The password must begin with a letter.
5. Press '√'.

2.2.7. Step 6 – Installing the Control System and Transmitters

Having chosen and tested the mounting location of the Control System and each transmitter, you are now ready to permanently install the system.

To permanently install the transmitters, refer to each device's installation instructions (in Appendix B of this manual or supplied individually with each product).

To install the Control System:

1. Disconnect AC power from the Control System.
2. Open the housing as explained in Step 1 – Temporarily Power up the System and Install SIM Card.
3. Remove the backup battery pack. If you want to install the Control System with back tamper, it is also necessary to disconnect the flat cable connecting the Main board to the front panel keypad and remove the Main board.
4. Place the Control System in position against the wall and mark the upper and lower mounting holes. If using the back tamper, also mark the hole for the back tamper screw.
5. Install wall anchors in the appropriate positions.
6. Thread any required cables through the wiring hole on the back cover (e.g. AC power, HA interface, Ethernet cable, and telephone line) and make any necessary wiring connections:
   a. Connect the power cable to the AC power input on the Main board.

      ⚠ Always connect AC power before connecting the battery pack. Batteries are supplied uncharged. When you first connect the battery, it is probable that the system will display a Low Battery condition. Allow the battery to charge for at least 18 hours before use.

   b. Connect the telephone line to the Telephone Line terminal block on the GPRS module (PSTN connector) – see p. 6, 1.4.3 GPRS/LAN Communication Module.
7. Mount the Control System to the wall using four screws and insert the back tamper screw if required – see p.11, 2.3 Back Tamper.

☞ The Control System must be mounted so that it shall withstand a force of at least three times its own weight.

8. Replace the Main Board and reconnect its peripheral modules.
9. Connect the flat cable connecting the Main board to the front panel keypad and replace the front cover's fastening bands.
10. Apply AC power.

    ⚠ Always connect AC power before connecting the battery pack. Batteries are supplied uncharged. When you first connect the battery, it is probable that the system will display a Low Battery condition. Allow the battery to charge for at least 18 hours before use.

11. Connect the battery pack to the connector on the Main Board.
12. Position the front cover's top holding hooks onto the back cover and snap the front cover closed.
13. After installing the Control System, perform the Find Modules function – see p. 73, 13.5 Find Modules.

2.3. Back Tamper

The back tamper switch is an optional feature that provides an extra safeguard in the event that the Control System is removed from the wall.

The back tamper switch is located on the rear side of the Control System's Main Board and is constantly depressed by the section of the back cover shown in Figure 2-5.

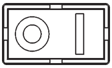


Figure 2-5: Perforated Back Tamper Release

For this feature to operate, you must insert a screw into the back tamper mounting hole – see p. 11, Step 6 – Installing the Control System and Transmitters. When the Control System is removed from the wall, the screw causes the perforated section of the plastic to break and remain attached to the wall. As a result, the back tamper switch is released and an alarm is generated.

2.4. Internet Communication Setup

After you have powered up the system, the GPRS or LAN startup sequence (depending on your Control System configuration) is initiated. During this sequence, the GPRS or Ethernet module receives the parameters programmed in the Control System's Internet Options – p. 67, 11 Internet Options. After the startup sequence is complete, the GPRS or LAN attempts to connect to the ELAS GPRS/LAN Proxy.

If the Control System is having difficulty connecting to ELAS, a trouble message is displayed. The following table summarizes the trouble messages for this case.

Table 2-1: ELAS Connection Trouble Message

LCD display	Trouble condition	Restored by
SIM CARD TROUBLE	SIM card not recognized or incorrectly programmed	Insertion of recognized SIM card or correct programming.
MEDIA LOSS LAN MODULE	LAN down	LAN restore
MEDIA LOSS GSM	Cellular network down	Cellular network restore
MEDIA LOSS GPRS MODULE	Wrong GPRS settings (APN, Password etc.) or loss of GPRS service	Correct GPRS settings or restored GPRS service
DEVICE TROUBLE LAN MODULE	Faulty Ethernet module	Replacement of faulty module
DEVICE TROUBLE GSM	Faulty GSM/GPRS module	Replacement of faulty module
DHCP ERROR	IP parameters cannot be set because of missing DHCP services	Change IP LAN settings or restored DHCP service
XML FAIL	Control panel fails to communicate with the XML Proxy	Successful communication with XML Proxy

In this case, check that the Control System's Internet Options are correctly programmed. If you still experience problems, the IP Protocol and GPRS settings must be checked.

To check the IP Protocol and GPRS/LAN settings:

1. For GPRS settings, open the system housing and make sure a SIM Card with GPRS support is on the GPRS module.
2. Close the Housing and enter your Installer code.
3. Enter [95112] (Programming, Communications, Accounts, Account 1, Protocol). If the setting is correct, you will see IP Protocol.
4. Exit this menu and Enter [95113] (Programming, Communications, Accounts, Account 1, Interface). If the setting is correct, you will see GPRS or LAN, respectively.

⚠ When using a SIM card with a PIN code, the installer has to make sure that the PIN code programmed in the Control System is the same as the SIM card's PIN code – see p. 62, 10.7.2 PIN Code.

3. Basic System Operation

The iConnect ② Control System is available with the LCD front panel configuration. Below you will find description of the LCD front panel layout.

3.1. Front Panel Layout

The front panel provides a detailed interface for operating and programming the system. The following diagram will familiarize you with the various elements of the front panel.

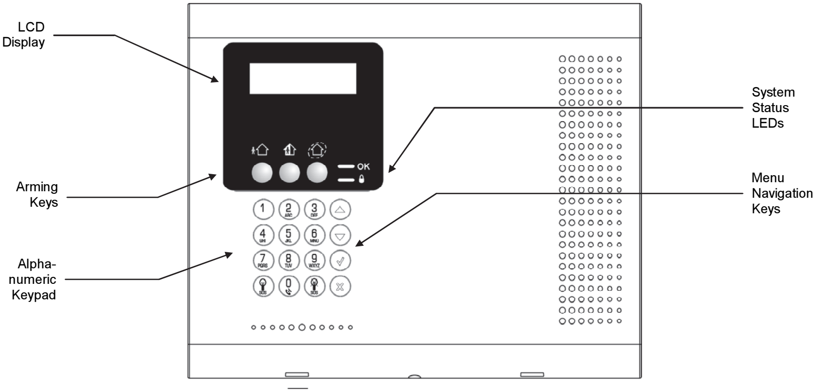


Figure 3-1: Front Panel

3.2. Front Panel System Status LEDs

The two LEDs, OK and Arm Status, provide essential information on the status of the system.

Table 3-1: OK LED Indication

OK LED Status	Meaning
Off	Both AC and Battery power are disconnected.
Green On	System Power Status is OK and there is System Trouble.
Green Flashing	Open Zone. Check that the windows and doors are closed and no movement is detected by the detectors within the protected area.
Yellow On	System Trouble.
Yellow Flashing (slow)	Backup battery low or low battery from transmitters.
Yellow Flashing (fast)	AC loss.
Yellow Intermittent On/Off	System Trouble in addition to AC loss/Low Battery.

Table 3-2: Arm Status LED Indication

🔒 LED Status	Meaning
Off	The system is disarmed.
Green On	The system is armed.
Red Flashing	An alarm has occurred. Alarm indication is cleared the next time you arm the system or view the relevant event in the event log.

☞ Alarm indication is not displayed after a silent panic alarm.

3.3. Front Panel Keypad and Wireless LCD Keypad

The alphanumeric keypad on the front panel enables you to perform various operation and programming tasks. Apart from the regular functions of a standard alphanumeric keypad, Full, Part, and Perimeter arming, Home Automation and PGM control, the keypad offers a number of special functions.

In addition to the front panel keypad, you can install up to four, individually addressed, Wireless LCD keypads. The layout of the Wireless LCD keypad is similar to the front panel keypad and most of the functionality is identical.

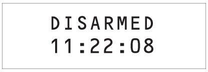
Table 3-3: Front Panel Keypad and Wireless LCD Keypad Functions

Key	Symbol used in the text of this manual	Special function
①	1	Used to enter symbols in descriptor editing.
⓪	0	Used to enter symbols in descriptor editing.
⊗	X	Used to cancel the current selection. Used to return to the previous menu level.
✓	'√'	Used to enter Menu mode. Used to select the current menu item. Used to signify the end of an entered value. Toggles status in Zone Bypass/Unbypass function.
💡 SOS	💡	Used to switch Home Automation units or PGM on. In descriptor editing, used to insert a space before the current character In phone number editing, used to enter "T", ",", "P", "+", "★", "#". In account number editing, used to enter Hexadecimal digits (A-F). Toggles item descriptors and default names. In the event log, toggles the time/date stamp. Toggles AM and PM when setting the time in 12hr format.
💡 SOS	⊠	Used to switch Home Automation units or PGM off In descriptor and phone number editing, used to delete the current character.
△	▲	Used to scroll backwards in the current menu level. For Global Chime and Message Center features, used to access shortcuts. ▲ + ▼ (Global Chime shortcut) ▲ + X (Record Message shortcut, front panel keypad only) ▲ + '√' (Play Message shortcut, front panel keypad only)
▽	▼	Used to scroll forwards in the current menu level. During standby, used to scroll through the list of system trouble conditions.

The Wireless LCD Keypad LEDs functionality is identical to those of the Front Panel keypad – see p. 13, 3.2 Front Panel System Status LEDs**Error! Reference source not found.** shows the layout of the LCD keypad:

3.4. LCD Display

The LCD display provides you with a detailed interface for operation and programming.



```
DISARMED
11:22:08
```

Figure 3-2: Typical Standby Display

3.4.1. Standby Mode

Standby mode can be defined as the state the system is in when it is disarmed and not in Menu mode. In Standby mode, the armed status, system status or banner are displayed. If system status is normal, the current time is displayed.

Table 3-4: Armed Status

Item…	Description…
DISARMED	The system is disarmed.
FULL ARMED	The system has been armed using the displayed arming method.
PART ARMED	
PERIMETER ARMED	
PART ARMED INST	The system has been armed using the displayed arming method with the Instant arm feature activated.
PERIM ARMED INST	
FULL ARMING	The system is in the process of arming (displayed during exit delay).
PART ARMING	
PERIMETER ARMING	
PART ARMING INST	The system is in the process of arming with the Instant arm feature activated.
PERIM ARMING INST	

Table 3-5: System Status

Item	Description
ZONES IN ALARM	Zones have been violated.
TAMPER ALARM	The system has been tampered with.
56 TO EXIT	The exit delay is counting down (56 seconds remaining).
11 TO DISARM	The entry delay is counting down (11 seconds remaining).
SYSTEM NOT READY	The system is not ready to arm, check that all doors and windows are closed.
KEYPAD LOCKED	Five unsuccessful attempts were made to enter a user code; the keypad is locked for 30 minutes.
SYSTEM TROUBLE	A trouble condition has been detected, press ▼ for further details.

3.5. Audible Notification

The following table is a summary of tones that audibly notify system status.

Table 3-6: Audible Notification

Status	Tones	Description
Positive Acknowledge	1 long tone.	The preceding action was accepted.
Negative Acknowledge	5 low tones.	The preceding action was not accepted (e.g. an incorrect user code entry).
Exit Delay/ Entry Delay	External Siren: 4 tones. Internal Siren: 4 tones or Continuous tones. Continuous tones quicken when there are 15 seconds remaining and quicken again when there are 5 seconds remaining.	The exit/entry delay is counting down. The number of tones sounded during each delay is determined in programming – see p. 43 8.5 Arming Tones.
Chime	2-tone modulated sequence (similar to a doorbell).	A zone with the Chime option enabled has been opened – see p. 38 7.3.5 Chime .
Arm	3-tone modulated sequence (low to high) sounded twice	The system has been armed using any of the arming methods.
Disarm	3-tone modulated sequence (high to low).	The system has been disarmed.
Home Automation	Rapid 2-tone modulated sequence.	An HA unit has been turned On or Off using a wireless keypad or keyfob – see p. 44 8.6 Home Automation Tones .
System Trouble	4 rapid tones sounded once per minute.	A trouble condition has been detected, press ▼ for further details. For Fire Trouble Tones, there is a programmable option to repeat fire-related trouble tones until the problem has been taken care of – see p. 45, 8.7.3 Fire Trouble Tones.

3.5.1. System Trouble Tones

In the event of system trouble, the iConnect ② Control System sounds a series of tones to alert the user. To silence these tones, press ▼ and scroll through the system trouble list displayed on the LCD. When the trouble condition is restored, it is removed from the system trouble list.

☞ For this feature to function, Trouble Tones must be enabled in programming – see p. 44, 8.7.1 System Trouble Tones.

System trouble tones are not sounded from 10:00pm to 7:00am so as not to disturb household members who may be asleep. However, you can program the system to immediately annunciate telephone trouble at all times – see p. 45, 8.7.2 Telephone Trouble Tones.

3.5.2. Vocal Message Annunciation

Certain versions of the iConnect ② Control System hardware support vocal annunciation of system status. If this feature is enabled in programming (see p. 52, 9.13 Vocal Messages), the system plays short messages to indicate arming, disarming, bypassed zones, system trouble, message waiting, and water alarm.

☞ The availability of the Vocal Message annunciation feature is hardware dependent.

3.5.3. Alarm Sounding Patterns

he following table summarizes the system's various alarm patterns.

Table 3-7: Alarm Patterns

Alarm	Alarm Pattern Description	Sounds
Burglary	ON (continuously)	Siren
Fire	ON - ON - ON, 1.5-second pause, ON - ON – ON...	Siren
Gas	ON - ON - ON - ON (short bursts), 5 second pause, ON - ON - ON - ON...	Siren
Medical	ON (continuously) – only applicable for MedicalEmergency alarm from zone	Siren
Flood/Environmental	4 rapid tones sounded once per minute (same as Trouble tones)	Buzzer

3.6. Arming and Disarming

The following section explains how to arm and disarm the Control System using the front panel keypad and wireless LCD keypad.

3.6.1. Arming

The iConnect Control System offers three arming modes that you can define to suit the application. Figure 3-4 illustrates the three arming modes. In each diagram, the protected area is shaded.

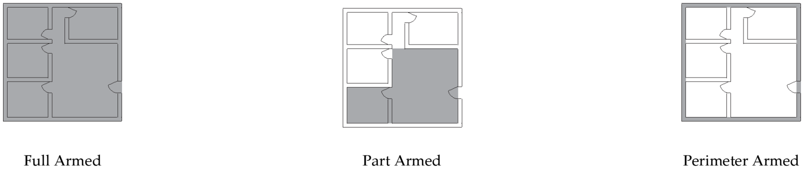


Figure 3-3: Arming Modes

The arming options are entirely flexible. You can program each detector to be included in any combination of the three arming modes – see p. 37, 7.3.2 Arm Set. Additionally, each arming mode has a separate exit and entry delay.

Below you can see another, more complicated example of how can the premises be divided. In this example, the garage is included in full + part + perimeter arming, the house perimeter zones are included in full + perimeter arming, and the house interior zones, in full arming only. So, part arming allows the user to arm the garage, perimeter arming is used to secure the house perimeter at nights, and the full arming is used when leaving the house. Figure 3-4 illustrates this example. In each diagram, the protected area is shaded.

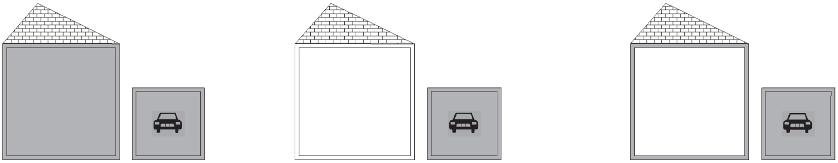


Figure 3-4: Arming Modes: Garage Example

3.6.2. Arming Keys

The Arming keys enable you to arm the system using any of the three arming methods: -- Full, Part and Perimeter.

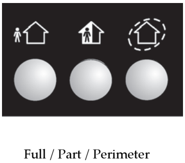


Figure 3-5: Front Panel and Wireless LCD Keypad Arming Keys

3.6.3. Full Arming

Full arming is designed for when the occupant vacates the premises.

To fully arm the system using the front panel keypad or Wireless LCD Keypad:

1. Check if the system is ready to arm.
2. Press the Full arming key on the keypad.
3. If One-Key Arming is disabled, enter your user code.

3.6.4. Part Arming

Part arming is designed for when the occupant intends to remain inside one part of the premises and secure another part.

To partially arm the system using the front panel keypad or Wireless LCD Keypad:

1. Check if the system is ready to arm.
2. Press the Part arming key on the keypad.
3. If One-Key Arming is disabled, enter your user code.

To partially arm the system using the hardwire LCD keypad:

1. Check if the system is ready to arm.
2. Press PART on the keypad.
3. Select Part arming.
4. If One-Key Arming is disabled, enter your user code.

3.6.5. Perimeter Arming

Perimeter arming is designed for when the occupant intends to remain inside the premises and secure the perimeter.

To arm the system's perimeter using the front panel keypad or Wireless LCD Keypad:

1. Check if the system is ready to arm.
2. Press the Perimeter arming key on the keypad.
3. If One-Key Arming is disabled, enter your user code.

To arm the system's perimeter using the hardwire LCD keypad:

1. Check if the system is ready to arm.
2. Press PART on the keypad
3. Select Perimeter arming.
4. If One-Key Arming is disabled, enter your user code.

3.6.6. Combination Arming

The system allows you to activate a combination of two arming methods. If you Perimeter arm the system, you may also activate Full or Part arming. Likewise, you can Perimeter arm the system after activating Full or Part arming. It is not important which arming mode you choose first.

☞ You can activate the second arming mode only during the exit delay of the first arming mode. When the first exit delay expires, you cannot activate a second arming mode.

For combination arming, perform the following procedure:

1. Check if the system is ready to arm.
2. Activate the first arming mode.
3. If One-Key Arming is disabled, enter your user code.
4. While the exit delay of the first arming mode is counting down, activate the second arming mode.
5. If One-Key Arming is disabled, enter your user code.

☞ It is not possible to activate Full and Part arming modes simultaneously. It is necessary to disarm first when changing from one arming mode to another arming mode.

The exit delays of the two arming modes are entirely independent. The moment an arming mode is activated, its exit delay begins to count down. The entry delay depends on which detector was tripped first. For example, if the detector is included in Full arming, the entry delay for Full arming counts down – see p. 37, 7.3.2 Arm Set. If the detector is included in both activated arming modes, the entry delay for Perimeter arming counts down.

☞ If, due to open zones, the system is not ready to activate the second arming mode then both arming methods are canceled. In this case, check that the relevant entrances are secured and start the entire arming sequence again.

Disarming cancels both active arming modes.

3.6.7. Disarming

When an entry/exit detector is tripped, the entry delay counts down; each arming method has its own entry delay.

To disarm the system:

Enter a valid user code, the system is disarmed.

☞ You can only disarm all the active arming modes.

3.7. Additional Arming Options

3.7.1. Forced Arming

Forced arming enables you to arm the system when the system is not ready. For example, if a door protected by a magnetic contact is open, you may arm the system on condition that the door will be closed by the end of the Exit delay. If the door is still open after the exit delay expires, an alarm is generated.

Two conditions enable you to perform Forced arming:

- Forced arming is enabled – see p. 46, 9.3.1 Forced Arm.
- The detector that is causing the System Not Ready condition is Force Arm enabled – see p. 38, 7.3.6 Force Arm.

3.7.2. Instant Arming

Instant arming is a feature that allows you to cancel the entry delay after Part or Perimeter arming the system. For this feature to function, it must be enabled in programming – see p. 47, 9.3.4 Instant Arming.

To instantly arm the system.

1. Check if the system is ready to arm.
2. Press the Part or Perimeter arming key on the keypad and enter your user code if One-Key Arming is disabled.
3. Press and hold down ▲ on your keypad until the message Instant Arming, OK? is displayed
4. Press '√'; the entry delay for the current arming period is canceled.

3.7.3. Disarming

When an entry/exit detector is tripped, the entry delay counts down; each arming method has its own entry delay.

To disarm the system:

Enter a valid user code, the system is disarmed.

3.7.4. Remote Arming/Disarming via SMS

You can arm and disarm the system remotely by sending the SMS commands from a cellular phone to the Cellular Communication Module (GPRS or Ethernet). Additionally, you can check the arm status of the system by sending an Arm Status request message.

Each SMS command contains the following elements:

✚ SMS Command Descriptor (up to 43 characters of free text)
✚ # (delimiter – separates the descriptor from the actual command)
✚ User Code (4 digits)
× Command (120=Disarm, 121=Full Arm, 122=Part Arm, 123=Perimeter Arm, 124=Full + Perimeter Arm, 125=Part + Perimeter Arm, 200=Arm Status)

The following example shows the format of an SMS command for arming the system:

+								+	+				×		
F	U	L	L		A	R	M	#	1	2	3	4	1	2	1

⚠ While the SMS Command Descriptor is optional, you must start the SMS command with the # symbol for the system to accept the command.

After an SMS command is executed by the system, you can program the system to return a confirmation message to the sender – see p. 62, 10.7.5 SMS Confirmation.

3.7.5. Arm Status Reply

On receiving an Arm Status request message, the system returns a status message to the sender. This message includes the system status and the descriptor of the user or the device used to arm/disarm the system.

The following example shows an Arm Status Reply message reporting that the system was fully armed by Master User.

F	U	L	L		A	R	M	E	D	-	M	A	S	T	E	R		U	S	E	R

3.7.6. Remote Arming/Disarming via DTMF

Using the Telecontrol feature, you can arm and disarm the system via the telephone with DTMF commands. For further information on the Telecontrol features, see p. 30, 5.1.5 Arm/Disarm DTMF Commands.

3.7.7. Remote Arming/Disarming via WUAPP

You can arm and disarm the system remotely using the WUAPP (Web User Application) – see p. 124, Arm/Disarm.

3.7.8. Alarm Activation

In the event of an emergency, the user can generate three kinds of alarms from the front panel keypad, wireless keypad or keyfobs.

To activate a SOS Panic alarm from the Keyfob (EL-4714):

- Press B1 and B2 buttons simultaneously.

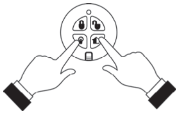


Figure 3-6: SOS Panic Alarm Activation (EL-4714)

To activate an SOS Panic alarm from the front panel keypad and the Wireless LCD Keypad:

- Press and hold down the SOS buttons simultaneously.

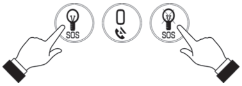


Figure 3-7: SOS Alarm Activation (Front Panel Keypad/Wireless LCD Keypad)

To activate a Fire alarm from the front panel keypad or hardwire LCD keypad:

- Press and hold down buttons 1 and 3 simultaneously.

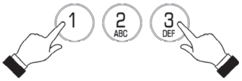


Figure 3-8: Fire Alarm Activation

To activate a Medical alarm from the front panel keypad or hardwire LCD keypad:

- Press and hold down buttons 4 and 6 simultaneously.

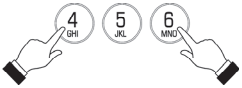


Figure 3-9: Medical Alarm Activation

4. Advanced System Operation

Besides the basic arming functions described in the previous chapter, you can access additional functions via the menu. This chapter describes these functions and the menu navigation procedure.

4.1. Menu Navigation

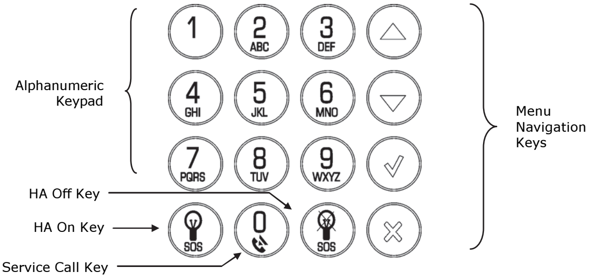


Figure 4-1: On-board Keypad Layout

The Front Panel/LCD keypads' friendly, menu-driven interface is designed to facilitate operation and provide a gentler learning curve for first-time users. You can navigate through the menus using the arrow navigation keys (▲/▼) and make simple yes/no decisions using the '√'and X keys.

For example, perform the following procedure to navigate to Service, Interface Test.

1. Press '√' to enter Menu mode.
2. Enter an authorized user code; the first menu item, 1. Cancel Report, is displayed.
3. Press ▼ until 7. Service is displayed.
4. Press '√' to enter the Service menu.
5. Press ▼ until 3. Test is displayed.
6. Press '√' to choose the displayed function.

☞ Press the 'X' key to return to the previous menu level. Press this key when you are in the main menu to exit Menu mode.

As an alternative to scrolling through menu options, you may enter a function’s shortcut once you have entered Menu mode. Shortcut numbers appear in square brackets in the procedures throughout this manual.

4.1.1. Menu Mode Timeout

Menu mode automatically terminates a certain amount of time after the last keystroke. The duration of this timeout depends upon which code is used to enter the menu. Usually the Menu Mode Timeout is two minutes but if you enter menu mode using the Installer code, the timeout is extended to fifteen minutes.

4.2. Cancel Report

This feature allows the user to cancel false alarms. Cancel Report behavior depends on time when it is performed. If the user selects Cancel Report:

- …before the alarm/restore message is sent, all the pending alarm or restore messages in the queue are aborted and marked "Cancelled" in the event log.
- …within 5 minutes since an alarm, a Cancel Report event and the user number are sent to the Central Station;
- …at the moment when the event is being reported (communication in progress), the event reporting is not cancelled;

☞ Non-alarm events (system trouble, arm/disarm etc.) are not aborted by Cancel Report.

To activate cancel report:

- From the main menu, select Cancel Report. [1].

4.3. Zone Bypassing/Unbypassing

When a detector is bypassed, it is ignored by the system and does not generate an alarm when triggered.

To bypass or unbypass a detector:

1. From the Bypass Zones menu, select Bypass/Unbyp. [21].
2. Using the arrow keys, scroll to the detector you want to bypass or unbypass.
3. Press '√' to change the bypass status.
4. Press X; Save Changes? is displayed.
5. Press '√' to confirm the changed bypass status.

To unbypass all detectors.

1. From the Bypass Zones menu, select Unbypass All [22].
2. Press '√'; all detectors are unbypassed.

☞ All bypassed zones are automatically unbypassed when the system is disarmed.

A Fire zone cannot be bypassed.

4.4. User Codes

The Control System supports up to 32 individual user codes. Each of these codes is four digits long. Most system operations require you to enter a valid user code. The ability to perform an operation is defined by your user code's authorization level. These authorization levels are pre-defined for each code as explained below.

☞ Codes 1-29 can be edited only by the Master code.

The Installer code, Guard Code and the Central Station TWA Code can be edited only by the installer.

Code 1: Master Code

The Master code is the highest user authorization level. With the Master code, you can edit all other user codes except the Installer code, the Guard code and the Central Station TWA Code. Additionally, the Master code grants access to the Event Log, the Service menu and Home Automation Schedule programming. The Master code is a "controlled" code. Arming and disarming using this code causes the Control System to notify the central station with an Arm/Disarm event message*.

⚠ The default Master code is 1234. Change this code immediately after installing the system!

*Codes 2-19: Controlled Codes**

When you use a controlled user code for arming and disarming, the Control System notifies the central station with an Arm/Disarm event message.

Codes 20-25: Non-controlled Codes

Non-controlled codes do not cause the Control System to send Arm/Disarm event messages to the central station. The Control System sends a Disarm message only if you use this code to disarm the system after an alarm occurrence.

Codes 26-27: Limited Codes

A Limited code enables the user to issue a code that is valid for one day only. This code automatically expires 24 hours after it has been programmed. These codes are "controlled" in that their use for Arm/Disarm is notified to the central station.

Code 28: Duress Code

The Duress code is designed for situations where the user is being forced to operate the system. This user code grants access to the selected operation, while sending a Duress event message to the central station.

* Only if arm/disarm reporting is enabled during System Programming

Code 29: Telecontrol Code

The Telecontrol code is designed to enable the user to perform a number of tasks via their telephone using DTMF commands. Using this code, the user can call their system to arm and disarm, turn on and off Home automation units, activate and deactivate the PGM output, cancel siren activation or establish Two-Way Audio communication.

Code 30: Central Station TWA Code

The Central Station TWA code is designed to enable the central station operator to establish Two-Way Audio communication with the Control System after an alarm. This code is valid for use for the first ten minutes after an alarm has occurred. This code can only be used for this specific purpose and does not grant access to any additional system functions such as disarming.

Code 31: Guard Code

Guard Code is an option that allows a security guard to check the premises in case of an alarm.

Code 32: Installer Code

The Installer code grants access to the Programming menu and the Service menu. Additionally, this code enables you to view and clear the Event Log.

⚠ The default Installer code is 1111. Change this code immediately after installing the system!

4.4.1. Editing User Codes

To edit a user code:

1. From the main menu, select User Codes [4].
2. Select the code you want to edit.
3. From the code's sub-menu, select Edit Code [#1]; the 4-digit code is displayed with the cursor flashing on the first digit.
4. Edit the code.
5. Press '√'; the new code is stored in the memory.

☞ If you enter a code that is identical to an existing user code, the Control System sounds an error tone and the new code is not accepted.

4.4.2. Deleting User Codes

To delete a user code:

1. From the main menu select, User Codes [4].
2. Select the code you want to delete.
3. From the code's sub-menu, select Edit Code [#1]; the 4-digit code is displayed with the cursor flashing on the first digit.
4. Enter 0000.
5. Press '√'; the code is deleted.

☞ The Installer and Master codes cannot be deleted.

4.4.3. User Code Descriptors

Each user code can be assigned a 16-character descriptor. These descriptors help to identify users in the event log and in SMS Follow-Me messages.

To edit a code descriptor:

1. From the main menu, select User Codes [4].
2. Select a code.
3. From the code's sub-menu, select Descriptor [#2].
4. Edit the descriptor using the alphanumeric keypad.
5. Press '√' when you have finished editing.

4.5. Follow-Me

The Follow-Me feature is designed to notify the user that certain events have occurred. The events that are sent to the Follow-Me telephone number are those events that the user is authorized to view in the event log; events that can be viewed only by the installer are not sent to the Follow-Me number – see p. 130, Appendix D: Event Table. If using the TWA Follow-Me feature, the audio channel is opened after alarm events only.

To edit the Follow-Me number:

1. From the main menu, select Telephone, Follow-me Number # [51].
2. Enter a telephone number for Follow-Me communication. If using the SMS Follow-Me feature, this number must be for a cellular phone with the capability to receive SMS messages.

☞ You may only access Follow-Me programming if the protocol for Account 3 is programmed as SMS or TWA Follow-Me.

4.6. Event Log

The event log records the last 1022 events the system has undergone. The log uses the FIFO (First In, First Out) method, automatically erasing the oldest event when the log is full.

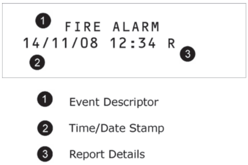
To view the event log:

1. From the Event Log menu, select View Log [61]; a summarized version of the most recent event is displayed. Press the 💡 key to view the time/date stamp or the device/user number on the second row of the display.
2. Use the arrow keys to scroll through the events.
3. When you have finished viewing, press X to exit the log.

The event log displays the following information for each event:

- The event descriptor – a brief description of the event that occurred.
- The zone where the event occurred.
- Time/date stamp – the exact time the event occurred.
- Report details – a single character indicating whether the event was reported to the central station. The options available are R: Report Sent, F: Report Failed, C: Report Canceled or N: No Report.

Figure 4-2 shows the detailed event log entry for a Fire alarm on November 14th 2008. The event was successfully reported to the central station.



```
 FIRE ALARM
14/11/08 12:34 R
```

Figure 4-2: Detailed Event Log Display

4.6.1. Event Log Authorization Levels

Every event that occurs is recorded in the event log. However, certain events are intended for the installer only. Those events include various service messages that are of little interest to the regular user. The View Log function requires you to enter either the Master or Installer code. The events that are displayed depend on which code you use to enter the log – see p.130, Appendix D: Event Table.

4.6.2. Clearing the Event Log

The Clear Log function erases all events from the log. After performing this function, a Clear Log event is recorded in the log. The Clear Log function is accessible using the Installer code only.

To clear the event log:

1. From the Event Log menu, select Clear Log [62]; the OK? confirmation message is displayed.
2. Press '√'; the log is cleared -- See p.130, Appendix D: Event Table.

For certain versions of the iConnect Control System software, the Clear Log function may be disabled.

4.7. Service Menu

The Service menu is accessible using either the Installer or Master code. This menu includes various functions that enable you to test the system effectively.

4.7.1. Set Time & Date

The time and date are used to time stamp events in the event log. Additionally the time is also displayed on the LCD display.

To set the time:

1. From the Service menu, select Set Time/Date, Set Time [7011].
2. Enter the current time.
3. Press '√'; the time is modified.

To set the date:

1. From the Service menu, select Set Time/Date, Set Date [7012].
2. Enter the current date.
3. Press '√'; the date is modified.

The format of the time and date is defined in the System Options – see p.48, 9.6.3 Time/Date Format. If you are setting the time in 12hr format, use the 💡 key to toggle between AM and PM.

4.7.2. Message Center

The iConnect Control System Message Center is designed to allow the user to record a short message that may be played back later by another user. After a message is recorded, Message Waiting is displayed on the LCD until the message is played back. If the Vocal Message option is enabled, the Message Waiting vocal message is sounded.

Recording a new message automatically overwrites all the previous messages in the Message Center.

To play back a recorded message:

- From the Service menu, select Messages, Play Message [7021].

To record a message:

1. From the Service menu, select Messages, Record Message [7022].
2. Press '√' to start recording the message.
3. Record your message. The message may be up to twenty seconds long.

   Time left out of the 20 seconds' timeout is displayed on the LCD.
4. Press '√' to stop recording; the message is automatically played back and OK? Is displayed.
5. Press '√' to save your recording.

The Record and Play options can also be accessed via a convenient shortcut without needing to enter a valid user code.

To play back a recorded message via a keypad shortcut:

From Standby mode, press ▲ then '√'.

To record a message via a keypad shortcut:

From Standby mode, press ▲ X then √. On the keypad, both LEDs flash in tandem during recording.

4.7.3. Wireless Siren Test

To test the wireless siren:

From the Service menu, select WL Siren Test [7031]; the external siren is sounded briefly.

4.7.4. Siren Test

To test the Control System's built-in siren:

From the Service menu, select Siren Test [7032]; the Control System's built-in siren is sounded briefly.

4.7.5. Interface Test

The Interface test enables you to check if the speaker, LEDs and LCD are functioning correctly.

To test the system interface:

From the Service menu, select Interface Test [7033]; a short sequence of chimes are sounded from the speaker, all LEDs flash and the LCD is tested on all connected LCD keypads.

4.7.6. Walk Test

To initiate Walk Test mode:

1. From the Service menu, select Walk Test [7034]; a list of registered detectors appears.
2. Trigger each detector; when the system receives a successful transmission from a detector, the detector is removed from the list.
3. When all the detectors are removed from the list, End Walk Test is displayed.
4. Press X to exit Walk Test mode.

4.7.7. Snapshot Test

The Snapshot Test enables you to check if the video verification detector cameras are functioning correctly

To test the video verification detector cameras:

1. From the Service menu, select Test and then Snapshot Test [7035]; a list of registered detectors appears.
2. Select a detector from the list and press √; a snapshot of the monitored area in taken and the results can be viewed in the Web User Application.
3. Repeat the test for each installed detector.
4. Press X to exit Snapshot Test mode.

4.7.8. Transmitters

The Transmitters menu offers a number of utilities that serve as a valuable aid during installation.

TX List

The TX List is a scrollable inventory of all registered transmitters and their last reported status.

To view the TX list:

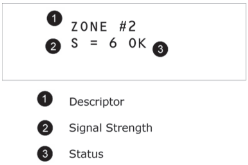
1. From the Service menu, select Transmitters, TX List [7041]; the first transmitter on the list is displayed.
2. Using the arrow buttons, scroll through the transmitter list.
3. When you have finished viewing, press X to exit the list.

The TX list displays the following information for each transmitter:

- The zone/device number or descriptor. Press the 💡 key to toggle the display.
- The signal strength of the last received transmission.
- An abbreviation indicating the last received status of the transmitter – see Table 4-1.

Table 4-1: Transmitter Status Abbreviations

Item…	Description…
OK	The transmitter is functioning correctly
TA	Tamper condition
BT	Battery low
OS	The transmitter is out of synchronization
NA	The transmitter is inactive – see p. 36, 7.2.3 Supervision Time



```
ZONE #2
S = 6 OK
```

Figure 4-3: TX List Display

In most cases, an "out of synchronization" condition indicates that an unauthorized attempt at grabbing the transmission has occurred – i.e. a previous transmission has been recorded and sent by somebody trying to violate the system.

TX Test

TX Test enables you to identify transmitters and test their signal strength. In TX Test mode, each time a transmission is received, the activated transmitter is displayed. If you enter this function using the Master code, a chime is sounded every time a transmission is received. If you enter this function using the Installer code, a sequence of tones in combination with subsequent LED flashes indicate the transmitter's signal strength – see Table 4-2.

This feature helps you to determine the best location to install a transmitter.

The lowest recommended signal strength for any installed transmitter is 2. If the received signal strength is lower than 2, relocate the transmitter.

Table 4-2: Signal Strength Tones

Signal Strength	Tones	LED Flash
1	1 Tone	1
2	2 Tones	2
3	3 Tones	3
4	4 Tones	4

To initiate TX Test mode:

1. From the Service menu, select Transmitters, TX Test [7042].
2. Activate a transmitter; the transmitter's details are displayed.
3. When you have finished, press X to exit TX Test mode.

RF Link Test

RF Link Test enables you to measure the RF noise levels between a selected transmitter and the system's receiver.

To view RF Link level reading:

1. From the Service menu, select RF Link Test [7043]; the first transmitter on the list is displayed.
2. Using the arrow buttons, scroll through the list and select a transmitter.
3. Press '√' and activate the selected transmitter, e.g. press keyfob button. The RF noise levels of the selected transmitter and the system's receiver are displayed.
4. When you have finished, press X to exit RF Link Test mode.

Environmental RSSI

Environmental RSSI Test enables you to measure the RF noise level of the systems environment. The Control System will start measuring the RSSI level every second, and it will display the result on the LCD.

RSSI level can jump momentarily when a detector is activated. It doesn't mean that the receiver is noisy.

To view the Environment RSSI level reading:

1. From the Service menu, select ENV. RSSI [7044]; the RF noise of the system's environment is displayed.
2. When you have finished, press X to exit the Environmental RSSI Test mode.

4.7.9. Audio Volume

To adjust the sensitivity of the microphone and the volume of the speaker:

1. Establish a two-way audio connection – see 5.1.4 Telecontrol Call Procedure.
2. From the Service menu, select Audio Volume [705].
3. Using the arrow keys on the Front Panel keypad, adjust the setting according to the following table.

Table 4-3: Voice Level Adjustment

Key…	Function
1	Increases microphone sensitivity
4	Reduces microphone sensitivity
3	Increases speaker volume
6	Reduces speaker volume

4. Press '√'; the new settings are stored in the memory.

4.7.10. GSM Signal Strength

You can measure the GSM signal strength. This function enables you to calculate the optimal location to install the Control System with the Cellular Communication Module.

To view the GSM signal strength reading:

- From the Service menu, select GSM Signal [706]; the signal strength of the cellular network is displayed.

Table 4-4: GSM Signal Level

Reading	Meaning
8-9	Reception is good
5-7	Reception is acceptable
Less than 5	Reception is unacceptable

☞ In severe cases of low GSM signal consider using external GSM antenna.

4.7.11. Display Version

To display the system's software and hardware versions:

From the Service menu, select Version [707]; the hardware (HW) and software (SW) versions are displayed.

4.7.12. Enable Programming

The Enable Programming command enables a user with Master code authorization to grant access to system programming. This feature is relevant only if the Installer Access and/or the RP Access options are programmed as "User Initiated" – see p. 52, 9.14 Installer Access and p. 59, RP Access Options.

To grant access to the installer or Remote Programmer:

From the Service menu, select Enable Prog. [708]; a 30-minute time window is opened during which the Installer Code is valid or RP communication may be established.

4.7.13. Global Chime

The Chime feature causes the Control System's built-in siren to ring when specific zones are triggered. Using the Global Chime option, you can enable or disable this feature for all zones that are defined as Chime enabled – see p.38, 7.3.5 Chime.

To enable or disable Global Chime:

1. From the Service menu, select Global Chime [709].
2. Select either Enabled or Disabled.
3. Press '√' when the desired setting is displayed.

☞ Though the Service menu is accessible to the Master and Installer only, Global Chime can also be accessed via a convenient shortcut without needing to enter a valid user code. To access the Global Chime option from Standby mode, press ▲ then ▼ .

4.7.14. Remote Firmware Update

The Remote Firmware Update command enables a user with Master code authorization to initiate the update. This feature is relevant only if the Remote Firmware Update mode is programmed as "User Initiated" – see p. 63, 10.8.4 Remote Firmware Update

To initiate Remote Firmware Update:

From the Service menu, select, SW Update [710]; a 24-hours time window is opened during which the Remote Firmware Update may be performed.

4.7.15. IP Display

When using Ethernet connection, you can view the LAN IP address of the Control System, i.e. the address that your home router has assigned to the Control System.

To display the IP Address:

From the Service menu, select IP Display [711]; the LAN IP address of the Control System is displayed.

5. Telecontrol and Two-Way Audio

The iConnect ② Control System offers a range of Telecontrol features that provide remote access via the telephone. These features include Two-Way Audio, remote arming/disarming and cancel siren activation. This chapter explains these features and their operating procedures.

Telecontrol features can be separated into two fundamental groups; incoming and outgoing calls. These groups differ in their associated features.

5.1. Incoming Calls

The Control System can receive incoming calls from either the user or central station operator. Users may use this feature as a convenient way of contacting their family, operating their system or to check their home when they are away. Additionally, the monitoring service can contact the user in the event of an emergency or use this feature for listen-in alarm verification.

For any of the incoming Telecontrol features to function, Telecontrol must be enabled in the Communication Options section of the Programming menu – see p. 61, 10.6.8 Incoming Calls.

5.1.1. User Code Verification

To prevent unauthorized attempts to connect with the Control System, there are two user codes designed for use with the Telecontrol features. The Telecontrol code enables the user to establish communication with the Control System at any time. Additionally, the Central Station TWA Code is used exclusively for Two-Way Audio alarm verification and is only valid for a ten-minute period following an alarm – see p. 21, 4.4 User Codes.

5.1.2. Incoming Calls via PSTN

In the case of PSTN communication, the Control System often shares a line with regular telephone handsets, an answering machine or a fax machine. It is therefore important that the Control System distinguish between calls so that it knows when to pick up the relevant call. For this purpose the iConnect ② Control System employs a double call method.

To connect to the Control System using the double call method:

1. Dial the telephone number of the line connected to the Control System.
2. Wait for two or three rings and hang-up.
3. Wait at least five seconds and dial the number again; on the second ring, the Control System picks up and sounds two DTMF tones.

5.1.3. Incoming Calls via a Cellular Network

The Cellular Communication module has its own individual telephone number and therefore, the double call method is not needed. In this case, the user or central station operator may call the Control System directly.

5.1.4. Telecontrol Call Procedure

The following procedure explains how to make a Telecontrol call. The conditions and procedure differ when using PSTN or Cellular Communication. For further information, see the entire section 5.1 Incoming Calls.

To make a Telecontrol call:

1. Call the Control System either using the double call method (PSTN) or directly (Cellular/PSTN); when the Control System picks up, two DTMF tones are sounded.
2. Enter the Telecontrol code (Code 29) on your telephone within 15 seconds.

   ☞ Do not enter your user code until you hear the two DTMF tones. Any digits entered before the tones are sounded are disregarded by the system.

3. A DTMF tone is sounded to indicate that the system is ready to receive commands.

   The following DTMF commands are available:

   o Press "2" for Two-Way Audio.

   If the TWA mode is defined as "Simplex" (see p. 61, 10.6.11, TWA Mode.), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "1" on your telephone. To switch back to Listen mode, press "0" on your telephone.

☞ During the TWA session, you can adjust the speaker volume using the arrow buttons.

- Press "3" to fully arm the system.
- Press "4XX" to turn HA unit #XX ON.
- Press "430" to activate PGM output (Unit 30/31)
- Press "5XX" to turn HA unit #XX OFF.
- Press "530" to deactivate PGM output (Unit 30/31)
- Press "6" to disarm the system.
- Press "9" to cancel the siren.

☞ The Arm/Disarm, Home Automation, PGM on/off, and Siren canceling can also be executed at any time during a Two-Way Audio session.

Error beeps (three tones) sound in case of a wrong command.

To clear the last command, press "*" or "#".

- The duration of the call is determined by the TC/VM Timeout -- see p. 61, 10.6.9 Telecontrol/Vocal Message Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, press "7" on your telephone. This command restarts the timeout.

4. To disconnect before the end of the timeout, press "*" then "#" on your telephone.

5.1.5. Arm/Disarm DTMF Commands

During a Telecontrol call, you can arm and disarm the system remotely using the DTMF commands (see above). When arming the system in this way, the system is armed immediately without an exit delay.

5.1.6. HA and PGM DTMF commands

During a Telecontrol call, you can turn On and Off the Home Automation units using the DTMF commands "4XX" (HA unit #XX On) and "5XX" (HA unit #XX Off). PGM unit is defined as HA Unit 30. You can activate and deactivate PGM using the DTMF commands "430" (PGM On) and "530" (PGM Off).

5.1.7. Siren Cancel ("Bell Cancel")

The siren is muted during Two-Way Audio communication. At the end of the call, the siren is re-activated (if the Siren Cut-Off has not yet expired). During the call, pressing "9" on your telephone cancels the re-activation of the siren.

5.1.8. Central Station Two-Way Audio

Central Station Two-Way Audio is an alarm verification feature that enables the central station operator to establish Two-Way Audio communication with the Control System within ten minutes of an alarm.

To make a Central Station TWA call:

1. Call the Control System either using the double call method (PSTN) or directly (Cellular); when the Control System picks up, two DTMF tones are sounded.
2. Enter the Central Station TWA code (Code 30) on your telephone within 15 seconds.

☞ Do not enter your user code until you hear the two DTMF tones. Any digits entered before the tones are sounded are disregarded by the system.

3. If the TWA mode is defined as "Simplex" (see p. 61, 10.6.11 TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "1" on your telephone. To switch back to Listen mode, press "0" on your telephone.
4. The duration of the call is determined by the TC/VM Timeout -- see p. 61, 10.6.9 Telecontrol/Vocal Message Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, press "7" on your telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, press "*" then "#" on your telephone.

5.2. Outgoing Calls

The iConnect ② Control System can make Two-Way Audio calls to the user or central station in the event of an alarm. This feature is designed for medical, panic alarms, and for alarm verification.

5.2.1. Service Call

The Service Call feature enables the user to establish a two-way audio connection with the central station operator. For further information on how to program this feature, see p. 59, 10.5 Service Call.

To initiate a Service Call:

Press and hold down the Service Call key for a few seconds.

The Control System starts to dial.

If the TWA mode is defined as "Simplex" (see p. 60, 10.6.11 TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). The operator may switch to Speak mode, by pressing "1" on their telephone. Pressing "0" switches back to Listen mode.

5.2.2. TWA Alarm Reporting

In the event of Burglary, Fire and Medical alarms, the Control System is able to report the events and then stay on the line after acknowledgment is received (ACK 2). This allows the operator to verify the alarm or provide assistance in the event of an emergency.

For this feature to function, you must enable Two-Way Audio for both the account and the event group.

The sequence for Two-Way Audio during alarm reporting is as follows:

1. An alarm event is sent to the central station and acknowledgment is received (ACK 2).
2. If Two-Way Audio is enabled for the account and event group, the Control System stays on the line and opens the audio channel.
3. If the TWA mode is defined as "Simplex" (see p. 61, 10.6.11 TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). The operator may switch to Speak mode, by pressing "1" on their telephone. Pressing "0" switches back to Listen mode.
4. The duration of the call is determined by the TC/VM Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, the operator presses "7" on their telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, the operator presses "*" then "#" on their telephone.

If multiple events are sent, the Control System sends all the events before opening the audio channel.

☞ When using the SIA protocol for event reporting, this feature functions in "listen-in" mode only.

5.2.3. Two-Way Audio after Vocal Messages

If Two-Way Audio is enabled for a Vocal Message account, the user can open the audio channel by pressing "2" on their telephone after the system has played all of the event messages.

The sequence for Two-Way Audio after a vocal message is as follows:

1. An event occurs and the Control System calls the telephone number of the first Voice Report Account chosen.
2. When the user answers the call, the Home ID message and the relevant event message are played.
3. If Two-Way Audio is enabled for the Voice Report account, the user presses "2" on their telephone to open the audio channel.
4. The duration of the call is determined by the TC/VM Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, the user presses "7" on their telephone. This command restarts the timeout.
5. To disconnect before the end of the timeout, the user presses "*" then "#" on their telephone.

5.2.4. TWA Follow-Me

The TWA Follow-Me feature is designed to establish a Two-Way Audio connection with the user in the event of an alarm. For this feature to function, the account's protocol must be defined as TWA Follow-Me.

The sequence for a Two-Way Audio Follow-Me call is as follows:

1. An alarm occurs.
2. The Control System dials the programmed telephone number and sounds two DTMF tones when you pick up the call.
3. Press "2" on your telephone; the Control System opens the audio channel.

   ☞ If you press "9" to answer the call, the Control System simultaneously cancels the siren when opening the audio channel.
4. If the TWA mode is defined as "Simplex", (see p. 60, 10.6.11 TWA Mode), the audio channel opens in Listen mode (microphone active/speaker mute). To switch to Speak mode, press "1" on your telephone. To switch back to Listen mode, press "0" on your telephone.
5. The duration of the call is determined by the TC/VM Timeout. Ten seconds before the timeout expires, two short DTMF tones are sounded. To extend the call, press "7" on your telephone. This command restarts the timeout.
6. To disconnect before the end of the timeout, press "*" then "#" on your telephone.

6. Home Automation and PGM Control

The purpose of this chapter is to explain the various methods used to control X10 Home Automation (HA) units installed around the home and PGM output. The PGM is a programmable output that is triggered according to specific system status conditions, or by remote command sent via PSTN, GSM, Ethernet, keyfob, keypad, or RP as explained below. For further information on the X10 protocol and the choice of options that are available in programming, see p. 70, 12 Home Automation Programming.

6.1. Keypad Control

Using the front panel keypad or the Wireless LCD Keypad, you can control HA units and PGM output with the dedicated Home Automation keys – see Figure 6-1.

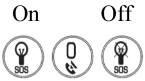


Figure 6-1: Home Automation Keys (Front Panel keypad or Wireless LCD Keypad)

To control HA units or PGM output via the front panel keypad or the Wireless LCD Keypad:

1. Press one of the two Home Automation keys on the keypad (On or Off).
2. Enter the number of the required HA unit in two-digits (01-16, or 30, 31 for PGM output); the command is sent to the HA unit or PGM.

To control HA units via the menu on the keypad (not relevant to PGM):

1. From the main menu, select Home Automat. [3]; HA Unit #1 is displayed.
2. Use the arrow keys to scroll to the unit you want to control.
3. Press '√' to select the HA unit.
4. Use the arrow keys to toggle the ON/OFF command.
5. Press '√' to select the command.
6. Scroll to the next unit you want to control or press X to exit this feature.

6.2. Keyfob Control

You can control up to two different HA units or PGM using any of the four button keyfobs registered to the system. For further information on how to assign keyfob buttons to HA units or PGM, see p. 40, 7.4.2 Keyfob Button Assignment.

6.3. Telephone Control

You can send On and Off commands to HA units or PGM output using SMS messages sent from a cellular phone to the Cellular Communication module. Alternatively, the HA unit or PGM can be controlled by using DTMF commands during Telecontrol call (either to the cellular or PSTN communication modules). For this feature to function correctly, Telephone control must be enabled for the specific HA units you want to control (see p. 71, 12.2.6 Telephone Control), and/or for PGM respectively – see p. 49, 9.7.1 Output Trigger.

6.3.1. DTMF command

Using the Telecontrol feature, you can turn on and off the HA units and PGM output via the telephone with DTMF commands. For further information on the Telecontrol features, see p. 29, 5 Telecontrol and Two-Way Audio and p. 30, 5.1.6 HA and PGM DTMF commands.

6.3.2. SMS Command Format

Each SMS command contains the following elements:

- SMS Command Descriptor (up to 43 characters of free text)
- # (delimiter – separates the descriptor from the actual command)
- User Code (4 digits)
- Command (0=Off, 1=On)
- Device Number (HA Units: 01-16, or 30, 31 for PGM output)

The following example shows the format of an SMS command to switch on a water boiler controlled by HA unit 8.

+									+	+				×	×	
B	O	I	L	E	R		O	N	#	1	2	3	4	1	0	8

While the SMS Command Descriptor is optional, you must start the SMS command with the # symbol for the system to accept the command.

6.3.3. SMS Confirmation Message Format

After an SMS command is executed, the system can return a confirmation SMS message to the sender. This message includes the descriptor of the HA unit or PGM descriptor and the command that was sent. For further information on how to enable this feature, see p. 62, 10.7.5 SMS Confirmation.

The following example shows the confirmation message the sender receives for the sample command from the previous section.

B	O	I	L	E	R	-	O	N

6.4. Scheduling (not relevant to PGM)

Scheduling allows you to program the Control System to send On/Off commands to HA units at specific times. You can also program the days of the week that the schedule is active. Scheduling is also available in the WUAPP (Web User Application) – see p. 129, Automation

6.4.1. On Time

To edit an HA unit's "On" Time:

1. From the main menu, select HA Schedules [8].
2. Select a HA unit.
3. From the HA unit's sub-menu, select On Time [1].
4. Enter a time (HH:MM).

6.4.2. Off Time

To edit an HA unit's "Off" Time:

1. From the main menu, select HA Schedules [8].
2. Select a HA unit.
3. From the HA unit's sub-menu, select Off Time [2].
4. Enter a time (HH:MM).

6.4.3. Weekly Schedule

To program the days of the week that the schedule is active:

1. From the main menu, select HA Schedules [8].
2. Select a HA unit.
3. From the HA unit's sub-menu, select Schedule [3].
4. Use keys 1 to 7 to toggle the days on and off.

Table 6-1: Weekly Schedule

Key	Value	Key	Value
1	Sunday	5	Thursday
2	Monday	6	Friday
3	Tuesday	7	Saturday
4	Wednesday		

7. Devices

This chapter explains how to register devices to the system and define programming options for each device. For further information on devices, please refer to the installation instructions included with each device.

7.1. Device Descriptors

You can assign a 16-character descriptor to each device. These descriptors help identify the devices when you operate and program the system.

To edit a device descriptor:

1. From the Programming menu, select Devices [91].
2. Select a device type.
3. From the device's sub-menu, select Descriptor.
4. Edit the descriptor using the alphanumeric keypad.
5. Press '√' when you have finished editing.

7.2. Wireless Devices

7.2.1. Registering Wireless Devices

For the system to recognize individual devices, each device must be registered to the system. For example, if the device is a wireless transmitter, registration enables the system to identify the source of a received transmission. Each device has an individual encrypted ID code. Registering the device to the system familiarizes the system with this code.

☞ It is not necessary to register hardwire detectors connected to Zones 33-34.

To register a device to the system:

1. From the Programming menu, select Devices [91].
2. Select the type of transmitter you want to register. For example, if you want to register a wireless detector to a zone, select Zones.
3. Select the specific device you want to register (for example, Zone 4); the system initiates Registration mode. During Registration mode, the system waits for two transmissions from the device.

   ☞ If a device has already been registered at the selected location, the system will not initiate Registration mode. If the device has already been registered at another location, attempts to register it are ignored by the system. Zones 1-32 are intended for wireless detectors by default, unless the zones 1 to 8 are programmed as wired zones connected to the Wired Zone Module.
4. Register the device – refer to each device's installation instructions in Appendix B for further details.
5. When two transmissions have been received, Save? is displayed.
6. Press '√' to confirm registration, or 'X' to cancel.

7.2.2. Deleting and Deactivating Wireless Devices

When you want to remove a device from the system, you have to delete and deactivate the device. It is important to delete and deactivate unused devices for two reasons. Firstly, you have to delete a device from the system before you can register a new transmitter in its place. Secondly, if the device is a wireless detector, it is important to deactivate the device so that the system will not react to the transmitter's failure to send supervision signals.

To delete and deactivate a device:

1. From the Programming menu, select Devices, [91].
2. Select the type of wireless device you want to delete.
3. Select the specific device you want to delete.
4. From the device's sub-menu, select Delete.
5. Deactivate the device – refer to each device's deactivation instructions in Appendix B for further details
6. Press '√' to confirm; the device is deleted from the system.

7.2.3. Supervision Time

The detectors in Electronics Line 3000's supervised wireless range send a supervision signal approximately 20 minutes after its last transmission. If the system does not receive supervision signals from a specific transmitter, the transmitter is regarded as inactive.

The amount of time after which a transmitter is considered inactive is called the Supervision Time. There is a separate supervision time for general transmitters and devices that are registered to Fire zones.

To program the Supervision Time for general transmitters:

1. From the Programming menu, select Devices, Superv. Time, General [9171].
2. Enter a supervision time between 02:00 and 23:59 hours.

To program the Supervision Time for transmitters registered to Fire zones:

1. From the Programming menu, select Devices, Superv. Time, Fire [9172].
2. Enter a supervision time between 02:00 and 23:59 hours.

7.3. Zones

The iConnect 2 Control System supports Electronics Line 3000's supervised wireless range of transmitters that includes various PIR detectors, magnetic contacts and smoke detectors. All these transmitters send supervision signals to the Control System's receiver in order to indicate that the transmitter is functional.

The iConnect 2 Control System includes 33-34 security zones. Zones 1-32 are intended for wireless detectors by default, unless the zones 1 to 8 are programmed as wired zones connected to the Wired Zone Module. Only one detector can be registered to each zone.

Zone 33-34 are on-board hardwire zones. These zones are programmed in the same way as the wireless zones with the exception of registration and deletion.

This section explains the programming exclusive to detectors. For information on registration, descriptor editing, and deletion, see p. 35, 7.1, 7.2.1, 7.2.2. The zone menu is displayed according to the zone type (see below).

Most of the programming options are identical for hardwire and wireless zones with the following exceptions:

Wireless Zones 1-32

- Register (see: p. 35, 7.2.1 Registering Wireless Devices)
- Delete (see: p. 35, 7.2.2 Deleting and Deactivating Wireless Devices)
- Repeater (see: p. 39, 7.3.9 Repeater)

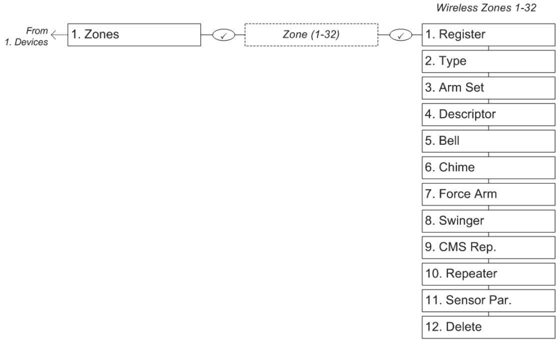


Figure 7-1: Wireless Zone Menu

Wired Zones 33-34

- Loop Type (see p. 39, 7.3.11, Loop Type (Wired zone 33-34 only)
- Loop Response (see p. 39, 7.3.12, Loop Response (hardwire zones 33-34 only)

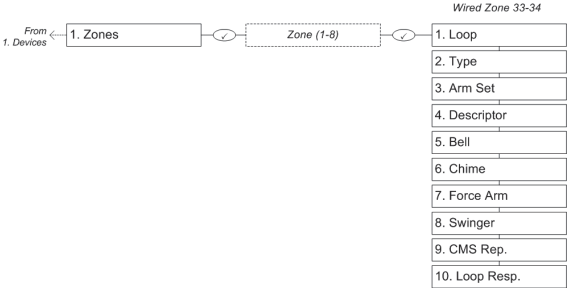


Figure 7-2: Wired Zone Menu

7.3.1. Zone Type

The zone type defines the type of alarm the system generates when the detector is tripped.

To program a zone type:

1. From the Programming menu, select Devices, Zones [911].
2. Select the detector you want to program.
3. From the detector's sub-menu, select Zone Type [#02].
4. Select one of the following zone types:

- Normal
- Entry/Exit
- Follower
- Panic
- Medical
- Fire
- 24H
- 24Hr-X (future option)
- Gas
- Flood
- Environmental
- No Motion
- Arm/Disarm
- Crash and Smash
- Not Used

For a detailed explanation on the function of each zone type, see p. 133, Appendix E: Zone Types.

7.3.2. Arm Set

The Arm Set option allows you to define the arm methods in which the zone is included.

Each zone can be assigned to Full Arming and/or to Part and/or Perimeter Arming in any combination.

To program the Arm Set option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Arm Set [#03]; the zone's current Arm Set setting is displayed.

Table 7-1: Arm Set Options

Arm Set	Description
1 (F)	The zone is included in Full arming.
2 (P)	The zone is included in Part arming.
3 (PE)	The zone is included in Perimeter arming.

4. Use the keys 1, 2 and 3 to toggle the current setting.

☞ It is not necessary to program this option for Panic, Medical, Emergency, Fire, 24Hr, Gas, Flood and Environmental zones.

7.3.3. Descriptor

For information on device descriptor editing, see p. 35, 7.1 Device Descriptors.

7.3.4. Bell (Siren)

Each zone can be programmed to activate the siren when triggered or to generate a silent alarm where only a message is sent to the central station.

To program the Bell option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Bell [#05]; the zone's current Bell setting is displayed.
4. Select either Enabled or Disabled.

☞ Fire zones always activate the siren regardless of what is programmed for this option.

> If the bell is disabled for Panic zones, this also disables all forms of alarm indication from the on-board keypad in the event of a Panic alarm.
>
> If the Bell option is enabled for Environmental or Flood zones, the system sounds trouble tones from the keypad.

7.3.5. Chime

When Chime is enabled, triggering the zone when the system is disarmed causes the internal siren to chime.

To program the Chime option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Chime [#06]; the zone's current Chime setting is displayed.
4. Select either Enabled or Disabled.

7.3.6. Force Arm

Force arming enables you to arm the system when the system is not ready. For example, a door that is protected by a magnetic contact is open. You may arm the system on condition that the zone is defined as Force Arm enabled. This door must be closed by the end of the Exit delay otherwise an alarm is generated. If the magnetic contact's zone is defined as Force Arm disabled, the system will not be ready to arm until you close the door.

To program the Force Arm option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Force Arm [#07]; the zone's current Force Arm setting is displayed.
4. Select either Enabled or Disabled.

☞ For the Force Arm feature to function, you must also enable Force Arming in System Options -- see p. 46, 9.3.1 Forced Arm.

7.3.7. Swinger

A zone defined as Swinger enabled can generate only a limited number of alarms during a specific time period. The Swinger setting is defined in System Options – see p.46, 9.1 Swinger Setting.

To program the Swinger option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Swinger [#08]; the zone's current Swinger setting is displayed.
4. Select either Enabled or Disabled.

☞ Do not enable the Swinger option for zones that are always active (Panic, Medical Emergency, Fire, 24-hr, Gas, Flood and Environmental zones).

7.3.8. CMS (Central Monitoring Station) Reporting

There is an option to enable or disable central monitoring station reporting for each burglary zone specifically. If enabled, the alarms are reported in the ordinary way, i.e. after the wireless siren delay; if disabled, alarms from this zone are not reported to the Central Station.

☞ This parameter is relevant only to Burglary zones used as Normal, Entry/Exit, Follower, or 24 hours type.

To program the CMS Reporting option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select CMS Rep. [#09]; the zone's current CMS Rep. setting is displayed.
4. Select either Enabled or Disabled.

7.3.9. Repeater

The repeater is an additional module that extends the range of the wireless transmitters. For a detector to use the repeater to relay transmissions to the system, you must define the Repeater option for its zone.

To program the Repeater option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Repeater [#10]; the zone's current Repeater setting is displayed.
4. Select either No Repeater or Use Repeater.

☞ Do not register the same transmitter to more than one repeater or mis-operation will occur.

7.3.10. Sensor Parameters

For a number of 2-Way detectors (e.g. Video Verification PIR Detector EL-4755 and 4755PI) you can define specific parameters through the control system. These parameters can be set in order to define how the device acts according to the zone in which it has been installed

To program the sensor parameter option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Sensor Par. [#11]; the zone's current Sensor Parameter setting is displayed.
4. Define the parameters according to the relevant device.
5. Press X, to exit the sensor parameters menu.

7.3.11. Loop Type (Wired zone 33-34 only)

This option enables you to determine the zone's loop type.

To program the Loop Type option:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Loop [#01]; the zone's current Loop type setting is displayed.
4. Select either N.O., N.C. or E.O.L.R.

7.3.12. Loop Response (hardwire zones 33-34 only)

The loop response determines how long a zone needs to be opened for the control system to generate an alarm. The following loop response options are available:

- Slow Loop (150ms) – used typically for PIR detectors, magnetic contacts, etc.
- Fast Loop (50ms) – designed for use with shock detectors

To set loop response:

1. From the Programming menu, select Devices, Zones [911].
2. Select the zone you want to program.
3. From the zone's sub-menu, select Loop Resp. [#10]; the zone's current Loop response is displayed.
4. Select Slow Loop or Fast Loop.

7.4. Keyfobs

The iConnect ② Control System supports two types of keyfob transmitter, EL-4711M/P and EL-4714. You can register up to 19 keyfobs to the system. Figure 7-3 illustrates these transmitters and the functions assigned to their buttons. For information on registration, deletion and deactivation, see p. 35, 7.2. Wireless Devices. For descriptor editing, see p. 35, 7.1 Device Descriptors.

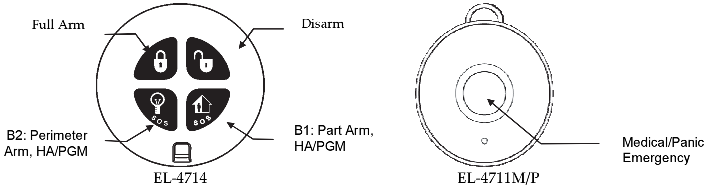


Figure 7-3: Keyfob Button Assignments

The following sections explain the programming options exclusive to the EL-4714 keyfob transmitter. These programming options are not relevant to the EL-4711M/P.

☞ For panic Alarm activation with the keyfob, see p. 19, 3.7.8, Alarm Activation.

7.4.1. Keyfob Type

You can define each registered keyfob as Controlled or Non-controlled. A Controlled keyfob causes the system to send arm/disarm event messages to the central station. Non-controlled keyfobs never send arm messages and send a disarm message only if the system is disarmed after an alarm occurrence.

To program a keyfob type:

1. From the Programming menu, select Devices, Keyfobs [912].
2. Select the keyfob you want to program.
3. From the keyfob's sub-menu, select Type [#2]; the current setting is displayed.
4. Select Controlled or Non-controlled.

7.4.2. Keyfob Button Assignment (EL-4714)

The EL-4714 includes two buttons (B1 and B2) that you can program individually.

☞ The default functions for B1 is part arming and for B2 , perimeter arming.

Alternatively, you can program these buttons to control a specific HA unit or PGM output.

To program buttons B1 and B2:

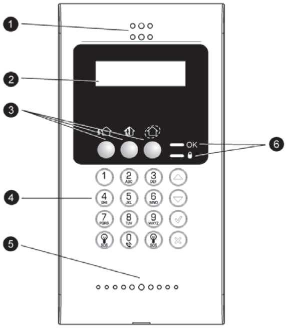
1. From the Programming menu, select Devices, Keyfobs [912].
2. Select the keyfob you want to program.
3. From the keyfob's sub-menu, select either B1 Assign [#4] or B2 Assign [#5].
4. Select the HA unit you want the button to control (01-16, or 30, 31 for PGM output) or enter 00 to program the button's default function; then press '√'.

7.4.3. SOS Panic Alarm Activation (EL-4714)

Using the four-button keyfob, you can activate an SOS Panic alarm by pressing two buttons simultaneously.

7.5. Wireless Keypads

The system supports up to four wireless keypads, including the EL-4727 Wireless LCD Keypad. For information on descriptor editing and deletion, see p. 35, 7.1 Device Descriptors, and p. 35, 7.2.2 Deleting and Deactivating Wireless Devices. The EL-4727 Wireless LCD Keypad's LED functionality is described in Appendix B**Error! Reference source not found.**.



1. Speaker
2. LCD Display
3. Arming Keys
4. Keypad
5. Microphone (optional)
6. System Status LEDs

Figure 7-4: EL-4727 Wireless LCD Keypad

Table 7-2: EL-4727 System Status LEDs

OK LED Status	🔒 LED Status	Meaning
Off		The system is disconnected from all power sources.
On - Green		The keypad is powered by AC and the battery is not low.
Flashing Yellow (slowly)		Local backup battery low.
Flashing Yellow (fast)		Wireless LCD Keypad AC loss.
	Off	The system is disarmed.
	On - Green	The system is armed.
	Flashing Red	An alarm has occurred. This alarm indication is reset when the system is armed using any of the three arming methods.

☞ Alarm indication is not displayed after a silent panic alarm.

For Panic Alarm activation using the Wireless LCD Keypad, see p. 19, 3.7.8 Alarm Activation

7.6. Repeaters

Repeaters are designed to extend the wireless range of the Control System. Up to four repeaters may be registered to the system with a maximum of 32 transmitters associated with each receiver. Repeater is a future option that is not available in the current firmware.

7.7. Wireless Siren

The Control System sends alarm and arm status information to the wireless siren's receiver. This requires that you register the Control System to the wireless siren's receiver. For information on registration and deletion, see p. 35, 7.1 Device Descriptors, and p. 35, 7.2.2 Deleting and Deactivating Wireless Devices.

7.7.1. Wireless Siren Delay

The Wireless Siren Delay is the period of time during which the wireless siren is not sounded after an alarm is triggered by Normal, Follower or 24Hr zones. This feature is implemented only when the system is not fully armed. During the Wireless Siren Delay, the Control System's built-in siren is sounded but the alarm report is not sent until the delay has expired. This gives the user enough time to disarm in the event that the alarm was accidentally triggered during Part or Perimeter arming. If the user disarms the system during the Siren Delay, an alarm event is not reported to the central station.

To program the Wireless Siren Delay time:

1. From the Programming menu, select Devices, Siren, WL Siren Delay [9152].
2. Enter a Siren Delay time (00-63 seconds), then press '√'.

7.7.2. Siren Cut-Off

The Siren Cut-Off is the period of time the sirens are activated after an alarm has occurred. You may program a Siren Cut-Off time in the interval between ten seconds to twenty minutes.

To program the Siren Cut-Off time:

1. From the Programming menu, select Devices, Siren, Cut-Off [9153].
2. Enter a Siren Cut-Off time MM:SS (00:10 - 20:00), then press '√'.

7.7.3. Wired Siren

When the system generates an audible alarm, both the wired built-in siren and the wireless siren are sounded. This option allows you to disable the alarm from the Control System's built-in siren. If disabled, the Control System's built-in siren may still be used to sound arm/disarm and entry/exit tones.

To program the Wired Siren option:

1. From the Programming menu, select Devices, Wired Siren [9154].
2. Select Enabled or Disabled.

7.8. Smartkeys

Smartkeys enable the user to arm and disarm the system without needing to enter a code. You can register up to 12 smartkeys to the system. For information on registration and deletion, see p. 35, 7.2. Wireless Devices. For descriptor editing, see p. 35, 7.1 Device Descriptors.

☞ Smartkey function existence is model dependant.

7.8.1. Smartkey Type

You can define each registered smartkey as Controlled or Non-controlled. A Controlled smartkey causes the system to send arm/disarm event messages to the central station. Non-controlled smartkeys never send arm messages and send a disarm message only if the system is disarmed after an alarm occurrence.

To program the smartkey type:

1. From the Programming menu, select Devices, Smartkeys [918].
2. Select the smartkey you want to program.
3. From the smartkey's sub-menu, select Type [#2]; the current setting is displayed.
4. Select Controlled or Non-controlled.

8. Entry/Exit Timers and System Tones

This chapter explains how to program the time of the Entry/Exit delays and the tones sounded by the built-in siren and wireless siren during Exit/Entry Delays, arming, disarming, home automation operation and when a trouble condition is present.

8.1. Entry/Exit Delay

The Entry/Exit delay timers determine the amount of time the user has to arm or disarm the system before an alarm is activated.

You can program separate Entry and Exit delays for each arming method.

To program Exit delay timers:

1. From the Programming menu, select Entry/Exit, Exit Delays [921].
2. Select the Exit delay you want to program: Full [#1], Part [#2] or Perimeter [#3].
3. Enter a delay time (000-255 seconds), then press '√'.

To program Entry Delay timers:

1. From the Programming menu, select Entry/Exit, Entry Delays [922].
2. Select the Entry Delay you want to program: Full [#1], Part [#2] or Perimeter [#3].
3. Enter a delay time (000-255 seconds), then press '√'.

8.2. Arm on Exit

The Arm on Exit feature cancels the unnecessary remainder of the Exit delay that continues to count down after the user has vacated the premises. This feature automatically arms the system when an Entry/Exit zone is closed during the Exit delay.

To program the Arm on Exit option:

1. From the Programming menu, select Entry/Exit, Arm On Exit [923].
2. Select Enabled or Disabled.

8.3. Supplementary Entry Delay

The Supplementary Entry Delay is a pre-alarm feature that is employed in the event that the system is not disarmed during the entry delay. When the entry delay expires, the Control System's built-in siren is sounded during an additional entry delay period. At the end of the supplementary entry delay, the system generates a full alarm condition; the wireless siren is sounded and an alarm event is reported to the central station.

To program the Supplementary Entry Delay setting:

1. From the Programming menu, select Entry/Exit, Supp. Ent. Delay [924].
2. Select Enabled or Disabled.

8.4. Entry Deviation

Entry Deviation is a pre-alarm feature employed in the event that a detector defined with the Normal zone type is opened during the entry delay. In this case, the Control System's built-in siren is sounded until the end of the entry delay period. Failure to disarm by the end of the entry delay causes the system to generate an alarm.

To program the Entry Deviation setting:

1. From the Programming menu, select Entry/Exit, Ent. Deviation [925].
2. Select Enabled or Disabled.

8.5. Arming Tones

Arming tones are the tones sounded by the Control System's built-in siren and/or the wireless siren when arming and disarming the system. Each set of tones can be enabled or disabled according to the requirements of the installation.

8.5.1. Exit Delay Tones

To program tones sounded by the wireless siren during the Exit delay:

1. From the Programming menu, select Tones, Exit Tones, WL Siren [9311].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren during the Exit delay:

1. From the Programming menu, select Tones, Exit Tones, Siren [9312].
2. Select No Tones, Four Tones or Continuous Tones.

8.5.2. Entry Delay Tones

To program tones sounded by the wireless siren during the Entry Delay:

1. From the Programming menu, select Tones, Entry Tones, WL Siren [9321].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren the Entry Delay:

1. From the Programming menu, select Tones, Entry Tones, Siren [9322].
2. Select No Tones, Four Tones or Continuous Tones.

8.5.3. Arming Tones

To program tones sounded by the wireless siren on arming:

1. From the Programming menu, select Tones, Arm Tones, WL Siren [9331].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren on arming:

1. From the Programming menu, select Tones, Arm Tones, Siren [9332].
2. Select Enabled or Disabled.

8.5.4. Disarming Tones

To program tones sounded by the wireless siren on disarming:

1. From the Programming menu, select Tones, Disarm Tones, WL Siren [9341].
2. Select Enabled or Disabled.

To program tones sounded by the built-in siren on disarming:

1. From the Programming menu, select Tones, Disarm Tones, Siren [9342].
2. Select Enabled or Disabled.

8.6. Home Automation Tones

Home Automation tones are sounded when you control HA units using keypads or keyfob transmitters.

To program built-in siren Home Automation tones:

1. From the Programming menu, select Tones, HA Tones [935].
2. Select Enabled or Disabled.

8.7. System Trouble Tones

System trouble tones are sounded to provide an audible indication that a system trouble condition exists. On hearing these tones the user is then able to determine which trouble condition is present from the front panel keypad. For additional information, see p. 15, 3.5.1 System Trouble Tones.

8.7.1. Trouble Tones

The Trouble Tones option allows you to enable or disable audible trouble annunciation.

To program the Trouble Tones option:

1. From the Programming menu, select Tones, Trouble Tones [936].
2. Select Enabled or Disabled.

8.7.2. Telephone Trouble Tones

Most trouble tones are not sounded between 10:00pm and 7:00am so as not to disturb the user late at night. Telephone trouble, however, may be an attempt to sabotage the system by cutting the telephone wires. For this reason, you can program telephone trouble tones to sound at all times.

To program the Telephone Trouble Tones option:

1. From the Programming menu, select Tones, Tel. Trb. Tones [937].
2. Select Immediate or Delayed.

8.7.3. Fire Trouble Tones

The Fire Trouble Tones option is a feature designed to repeat fire-related trouble tones until the problem has been taken care of. If this feature is enabled, fire trouble tones will be repeated 3½ hours after the user has manually silenced the tones if the trouble condition has not been restored.

To program the Fire Trouble Tones option:

1. From the Programming menu, select Tones, Fire Trb. Tones [938].
2. Select Enabled or Disabled.

☞ It is not necessary to program the Telephone Trouble Tones and Fire Trouble Tones options if the Trouble Tones option is programmed as disabled.

8.8. Tones Options

8.8.1. Tones Output

The Tones Output option enables you to determine whether the tones sounded when arming and disarming are sounded by the Control System's built-in siren or its built-in speaker.

To program the Tones Output option:

1. From the Programming menu, select Tones, Tones Options, Tones Output [9391].
2. Select Siren or Speaker.

8.8.2. Control Panel Speaker Volume

The Control Panel Speaker Volume option determines the volume level of the tones sounded by the control panel speaker.

To program the Control Panel Speaker Volume option:

1. From the Programming menu, select Tones, Tones Options, CP Speaker Vol. [9392].
2. Select High, Medium, Low or Mute.

☞ It is not necessary to program the Speaker Volume option if "Siren" is selected for the Tones Output option.

8.8.3. Wireless Keypad Speaker Volume

The Wireless Keypad Speaker Volume option determines the volume level of the tones sounded by the Wireless Keypad speaker.

To program the Wireless Keypad Volume option:

1. From the Programming menu, select Tones, Tones Options, KP Volume [9392].
2. Select the Wireless Keypad (1-4) that you want to program.
3. Select High, Medium, Low or Mute.

9. System Options

As the name suggests, System Options are settings that affect the entire system. This chapter offers explanations and programming instructions for each of these options.

9.1. Swinger Setting

A detector defined as Swinger enabled can generate only a limited number of alarms during a specific time period or during an arming period. The following options are available:

- One alarm per arming period
- One alarm per hour
- One alarm per day
- One alarm per week
- No swinger

To program the Swinger setting:

1. From the Programming menu, select System Options, Swinger [9401].
2. Select a Swinger setting from the list.

9.2. Code Lockout

The Code Lockout option locks the keypad for 30 minutes if five unsuccessful attempts are made to enter the user code.

To program the Code Lockout setting:

1. From the Programming menu, select System Options, Code Lockout [9402].
2. Select Enabled or Disabled.

☞ During the 30-minute lockout period, you can still arm and disarm the system using keyfobs and smartkeys. If one key arming is enabled, you may still arm the system using the keypads.

9.3. Arm/Disarm Options

The options offered in this section relate to arming and disarming the system.

9.3.1. Forced Arm

Forced arming enables you to arm the system when the system is not ready. This option allows you to enable or disable Forced arming for the entire system. Additionally, you can enable or disable Forced arming for each individual zone. For further information, see p. 38, 7.3.6 Force Arm.

To program the Forced Arm setting:

1. From the Programming menu, select System Options, Arm/Disarm, Forced Arm [94031].
2. Select Enabled or Disabled.

9.3.2. One-Key Arming

You can arm the system by pressing any of the three arming keys on the keypad. If One-Key Arming is enabled, the system does not prompt you for a user code.

To program the One-Key Arming setting:

1. From the Programming menu, select System Options, Arm/Disarm, One-Key Arming [94032].
2. Select Enabled or Disabled.

9.3.3. Supervised Arm

The Supervised Arm option is a feature designed to supervise a wireless device activity before you arm the system. If the system has not received a transmission from a detector during the interval defined for this option, all arming methods that include that detector will not be available. Medical, Panic, Fire, Gas, Flood, and Environmental zones are not included in this supervision and do not affect the system's ability to arm.

Press ▼ to check which detector is causing the "System Not Ready" condition.

To make the required arming method available, activate the detector. PIR detectors have a three-minute delay between transmissions.

If activating the detector does not help, there may be a problem with the detector. You can bypass the faulty detector's zone to allow system arming until the problem is remedied – see p. 21, 4.3 Zone Bypassing/Unbypassing.

☞ Zone bypassing is valid for one arming period only. All bypassed zones are automatically unbypassed when the system is disarmed.

To program the Supervised Arm interval:

1. From the Programming menu, select System Options, Arm/Disarm, Superv. Arm [94033].
2. Enter a Supervised Arm interval (001-255 minutes or 000 to disable the Supervised Arm option).

☞ Do not program a Supervised Arm interval that is less than the detector's supervision time.

9.3.4. Instant Arming

Instant arming is a feature that allows you to cancel the entry delay after arming the system – see p. 18, 3.7.2 Instant Arming. The feature is designed for use in situations where the system's perimeter is armed and nobody is expected to enter the premises from outside during the armed period.

To enable/disable the Instant Arm option:

1. From the Programming menu, select System Options, Arm/Disarm, Instant Arming [94034].
2. Select Enabled or Disabled.

9.3.5. Keyfob Disarm

The Keyfob Disarm option enables you to determine whether it is possible for the user to disarm the system using their keyfob at all times or during the entry delay only.

☞ This feature can be applied only after the system has been fully armed.

1. From the Programming menu, select System Options, Arm/Disarm, KF Disarm [94035].
2. Select Always or On Entry.

9.3.6. Supervised Arm Mode

For the Supervised Arm option, you can choose whether the Control System waits for a transmission of all the devices included in this supervision, or from at least one of them – see p. 47, 9.3.3 Supervised Arm.

To program the Supervised Arm mode:

1. From the Programming menu, select System Options, Arm/Disarm, Super Arm Mode [94036].
2. Select All Reg. Devices or Any Reg. Devices.

9.4. Panic Alarm

SOS Panic alarms generated from the front panel, keypads or keyfobs can be defined as either audible or silent.

To program the Panic Alarm setting:

1. From the Programming menu, select System Options, Panic Alarm [9404].
2. Select Audible or Silent.

9.5. AC Loss Delay

The AC Loss Delay is the amount of time that has to elapse before an AC Loss report is sent to the central station. If AC power is restored before the event message is sent, the event message is canceled and will not be sent. You can program an AC Loss Delay to be between 1 and 255 minutes after the system first senses the AC loss condition. Alternatively you can program a random AC Loss Delay.

The AC Restore message is also sent using the same method described above. AC Restore is reported only if the AC Loss report was sent.

To program the AC Loss Delay:

1. From the Programming menu, select System Options, AC Loss Delay [9405].
2. Enter a delay time (001-255 minutes) or enter 000 if you require the system to choose a random AC Loss Delay, and then press '√'.

9.5.1. Random AC Loss Delay

In the event of AC loss, an event message is sent to the central station between 15 and 30 minutes after the AC loss condition is sensed. The system chooses this delay at random in order to prevent the central station being inundated by simultaneous AC Loss reports in the event of a regional power cut.

9.6. Display Options

The following options relate to the information the system displays on the front panel keypad and the LCD keypad.

9.6.1. Arm Status Display

The Arm Status Display includes the current arm status and any trouble conditions that may exist within the system. You can program the system to display this information at all times, only for two minutes, or only for 30 seconds after arming or disarming the system.

To program the Arm Status Display options:

1. From the Programming menu, select System Options, Display, Arm Status [94061].
2. Select Display Always, Display 2 Min, or Display 30 sec.

9.6.2. Banner

The Banner is the 16-character text that you can program to appear on the top row of the LCD display. This text replaces the arm status if it is programmed to display for two minutes or 30 seconds only – see p.48, 9.6.1 Arm Status Display.

To edit the Banner text:

1. From the Programming menu, select System Options, Display, Banner [94062].
2. Edit the Banner text using the alphanumeric keypad, then press '√'.

☞ The system never displays the Banner text if the Arm Status Display option is programmed as Always.

9.6.3. Time/Date Format

This option determines the format in which the time and date are displayed.

The following options are available:

- DD/MM/YY, 24Hr
- DD/MM/YY, 12Hr
- MM/DD/YY, 24Hr
- MM/DD/YY, 12Hr

To program the Time/Date format:

1. From the Programming menu, select System Options, Display, Time Format [94063].
2. Select the required format from the options available.

9.6.4. Supervision Loss Indication

This option enables you to select whether the system trouble display will indicate transmitter supervision loss to the user.

To program the Supervision Loss Indication setting:

1. From the Programming menu, select System Options, Display, SV Loss Ind. [94064].
2. Select Enabled or Disabled.

9.7. PGM Output Options

PGM (1-2) and are programmable outputs that are triggered according to specific system status conditions, or by remote command sent via PSTN, GSM, keyfob, keypad, or RP.

9.7.1. Output Trigger

The Output Trigger option determines the conditions that activate and deactivate the PGM output.

To program the Output Trigger:

1. From the Programming menu, select System Options, PGM Options [9407].
2. Select a PGM Output.
3. Select Output Trigger [#1].
4. Select an Output Trigger option from the following table.

Table 9-1: PGM Output Trigger Options

Trigger Option	Activated by…	Deactivated by…
PGM Not Used	The PGM output is disabled	
Full Arm	System "Full" armed	System disarmed or PGM Cut-off
Perimeter Arm	System "Perimeter" armed	
Part Arm	System "Part" armed	
Arm Status	Any arming method	
Power Trouble	AC Loss or Low Battery conditions	AC restore or Battery restore
Tel. Line Trouble	Telephone line supervision trouble	Telephone line restore
System Trouble	System trouble condition	System trouble restore
Medical	Medical alarm	Any arming method, system disarmed or PGM Cut-off
Burglary	Burglary alarm	
Fire Alarm	Fire alarm	
Zone Status*	Open zones (steady) Bypassed zones (pulsing)	All zones closed and no zones bypassed
Entry/Exit	Entry/Exit delay follower	
Siren	Built-in siren follower	
WL Siren	Wireless siren follower	
Telecontrol	Remote PGM activation (PSTN/GSM/keyfob/keypad/RP, or via Internet in ELAS versions 321 and above)	

☞ For certain trigger options, deactivation may be determined by the PGM Cut-off -- see p. 50, 9.7.4 PGM Cut-off. If the PGM Cut-off is programmed as 000 (continuous activation), the PGM output shall remain activated until it is toggled by the relevant change in system status.

9.7.2. Output Type

The Output Type option determines whether the PGM output produces a steady or pulsed output.

To program the Output Type:

1. From the Programming menu, select System Options, PGM Options [9407].
2. Select a PGM Output.
3. Select Output Type [#2].
4. Select Steady or Pulsed.

☞ The Zone Status, Siren and WL Siren trigger options have a fixed Output Type; there is no need to program an Output Type for these options.

* Zone Status functions only when the system is disarmed.

9.7.3. Polarity

You can determine the polarity of the PGM output from the following two options:

- Active High: The output is normally off and is switched on when activated.
- Active Low: The output is normally on and is switched off when activated.

To program the Polarity:

1. From the Programming menu, select System Options, PGM Options [9407].
2. Select a PGM Output.
3. Select Polarity [#3].
4. Select Active High or Active Low.

9.7.4. PGM Cut-off

The PGM Cut-off is the duration for which the PGM is activated. Certain Output Trigger types are deactivated after the PGM Cut-off time has expired– see, 9.7.2, Output Type. For those Output Trigger types that are not affected by the PGM Cut-off, there is no need to program this option.

If, for example, Output Trigger option is set to Full Arm, and PGM Cut-off time is 060 seconds; then PGM is activated by Full Arming and deactivated by disarming or by PGM Cut-off Time, whichever comes first. If this option is set to "000" (Continuous activation), PGM is activated by Full Arming, and deactivated by disarming.

To program the PGM Cut-off time:

1. From the Programming menu, select System Options, PGM Options [9407].
2. Select a PGM Output.
3. Select PGM Cut-off [#4].
4. Enter a PGM Cut-off time (001-255 seconds or 000 for continuous activation), then press '√'.

9.8. Guard Code

Guard Code is an option that allows a security guard to check the premises in case of an alarm and to perform basic functions such as view log etc.

After two minutes since an alarm occurs, the Guard Code becomes active and the security guard can enter the premises and disarm the system using this code. Installer codes authorization also extends to allow arming and disarming. Guard Code is active within five minutes since the system is armed. After five minutes, the Guard code is revoked, and the installer code regular authorization is restored.

Guard code is also active when the system is disarmed.

☞ When the Guard Code option is enabled, the Guard Code Control [94221] and Guard code report [94222] options must be disabled.

To program the Guard Code:

1. From the Programming menu, select System Options, Guard Code. [9408].
2. Select Enabled or Disabled.
3. Edit the User Code 31 (see p. 22, 4.4.1 Editing User Codes).

☞ When the Guard Code is disabled, it is not valid even if programmed with a value other than 0000.

9.8.1. Guard Code Control

Guard Code Control option sets the Guard control value based on account #1, but in reversed order (e.g., the account #1 is set to 88881234, then the Guard Code is set to 4321).

☞ When the Guard Code Control option is enabled, the Guard Code option [9408] must be disabled.

The installer may use hex digits in the account number; the Guard Code will then be set to 0000.

If the automatically calculated Guard Code is the same number as an existing user code, it will be set to 0000.

To program the Guard Code Control option:

1. From the Programming menu, select System Options, Guard Code CT, Guard Code Ctr. [94221].
2. Select Enabled or Disabled.

☞ Clear Users function also clears the Guard Code even if the Guard Code Control is set as Enabled.

9.8.2. Guard Code Report

Guard Code Report option allows reporting of the Arm/Disarm events (including Disarm after an Alarm) to the Central Station even if the Arm/Disarm event group reporting is disabled – see p. 64, 10.9.1 Event Reporting.

☞ When the Guard Code Report option is enabled, the Guard Code option [9408] must be disabled.

To Activate the Guard Code Control option:

1. From the Programming menu, select System Options, Guard Code, Guard Code CT, Guard Code Rep [94222].
2. Select Enabled or Disabled.

9.9. "No Arm" Indication

The "No Arm" indication is a feature designed to inform the central station that the system has not been armed for a specified period of time.

To define the "No Arm" indication interval:

1. From the Programming menu, select System Options, No Arm Ind. [9409].
2. Select 1 Week, 2 Weeks, 3 Weeks, 4 Weeks or Disabled.

☞ The No Arm event message is an unclassified event. This means that it does not belong to any event group. If the No Arm option is programmed with any option other than "Disabled", the event message will be sent.

9.10. Jamming Detection

The system is able to detect RF Jamming that is usually caused by an intruder attempting to compromise the security system.

To program the Jamming Detection setting:

1. From the Programming menu, select System Options, Jamming Det. [9410].
2. Select Enabled or Disabled.

9.11. "No Motion" Time

The No Motion feature is designed to monitor the activity of disabled or elderly people. If a detector defined as "No Motion" (see p. 37, 7.3.1 Zone Type) has not detected within a pre-defined period of time, a No Motion event message is sent to the central station.

To program the No Motion time:

1. From the Programming menu, select System Options, No Motion [9411].
2. Enter the No Motion time value between 00:00 and 72:00. To disable the No Motion feature, enter 00:00. Press '√'.

9.12. Microphone/Speaker Options

In addition to the built-in microphone and speaker, the iConnect ② Control System Control System supports an external microphone/speaker unit called Interphone. The Microphone/Speaker option allows you to choose which microphone and speaker are in use. You can choose one mic./speaker (internal or external) to function exclusively or both may function simultaneously.

To program the Microphone/Speaker option:

1. From the Programming menu, select System Options, Mic./Speaker [9412].
2. Select Internal, External or Internal & External.

9.13. Vocal Messages

The Vocal Messages option allows you to enable/disable vocal annunciation of system status. When this feature is enabled, the system plays a short message to announce events such as arming and disarming.

To program the Vocal Messages option:

1. From the Programming menu, select System Options, Vocal Message [9413].
2. Select Enabled or Disabled.

☞ The availability of the Vocal Message annunciation feature is hardware dependent.

9.14. Installer Access

The Installer Access option determines if the Installer code can access the system at all times or only after the Master code provides authorization with the Enable Programming command – see p.27, 4.7.12 Enable Programming.

To program the Installer Access option:

1. From the Programming menu, select System Options, Install. Access [9414].
2. Select Always or User Initiated.

9.15. Auto Log View

Auto Log View is a future option that is not available in the current firmware. The default setting for this option is disabled. Electronics Line 3000 recommends that you do not change this setting.

9.16. Daylight Savings

Using the Daylight Savings option, the system is able to automatically adjust its clock twice a year according to the national adjustment to Daylight Saving Time.

Two options are available:

- Europe – the clock is adjusted forward 1hr on the last Sunday in March at 1am, the clock is adjusted back 1hr on the last Sunday in October at 1am.
- USA– the clock is adjusted forward 1hr on the second Sunday in March at 2am, the clock is adjusted back 1hr on the first Sunday of November at 2am.

To program the Daylight Savings option:

1. From the Programming menu, select System Options, Daylight Savings [9416].
2. Select Europe, USA or Disabled.

9.17. Standard Type

By choosing one of the existing security standards you can change the Control System behavior accordingly.

To set the standard type:

1. From the Programming menu, select System Options, Standard Type [9417].
2. Select Regular, EN-50131 or Skafor.

9.17.1. EN-50131 Standard Type

Settings the Standard type to EN-50131 changes some of the Control System settings as described below.

Arm Prevention for EN-50131

The system cannot be armed in the following cases:

- Media Loss, Supervision Loss, or Device Trouble condition in all Active Communication[1] modules -- GPRS and/or GSM, and/or PSTN[2];
- Trouble condition (Transmitter Out of Synch, Supervision Loss, or Zone Trouble) from any Zone, including Fire, Gas, Flood, and Environmental;
- Entry/Exit Trouble - System not ready is displayed on the Control System's LCD.

In an attempt to remotely arm the system the remote arming device is notified as follows:

- When arming by SMS – an SMS message "Command refused" is sent to the cellular phone;
- When arming by DTMF – a negative error tone is sounded;
- When arming from WUApp – System not Ready message is displayed.

Tamper Behavior for EN-50131

Opening of any tamper switch while the Control System is disarmed causes the Control System to send an alert. If the EN-50131 standard is chosen, the siren is not activated in this case. For other standards (Skafor, Regular), the siren is activated.

Number of Events from Single Source for EN-50131

The EN-50131 standard requires that the system avoid multiple events being generated from a single source. The number of repeated events from the same source during any Arm or Disarm period is limited to three. Two kinds of event types are defined for each device: Alarm/Tamper event and fault/trouble event. Every device can have maximum of three events from each type registered in the log. After the third event from the same source, no more events are sent to CS. Counters are reset each time the system is armed or disarmed.

EN-50131 Required Settings

To meet the requirements of the EN-50131 standard:

- Set Supervision Time to 2 hours – see p.36, 7.2.3 Supervision Time;
- Set Supervised Arm to 20 minutes – see p. 47, 9.3.3 Supervised Arm;
- Set Entry Delay to 45 sec. maximum – see p. 43, 8.1 Entry/Exit Delay;
- Set Arm Status Display to 30 sec. -- see p. 48, 9.6.1 Arm Status Display;
- Set Entry/Exit Trouble to "Enabled"

[1] Active communication module is a module used for events reporting.

[2] If there is only one communication module (GPRS, PSTN, or GSM), any communication trouble prevents the Control System from arming.

9.18. Battery Type

The battery type must be defined according to the battery supplied with the system (for example, if the battery sticker reads 1500 mAh, choose 1.5 Ah, if 3000 mAh, choose 3.0 Ah).

To program the battery type:

1. From the Programming menu, select System Options, Battery Type [9418].
2. Select the battery type.

9.19. Report Fail Trouble

If the Report Fail Trouble option is enabled, failure to report an event displays System Trouble on the LCD display. Report Fail Trouble is displayed after the control system has exhausted all message attempts and report cycles when trying to report the event. To restore a System Trouble condition caused by failure to report, press ▼ until you have scrolled through the entire system trouble list. If the Report Fail Trouble is disabled, failure to report an event does not cause a system trouble condition.

To program the Report Fail Trouble option:

1. From the Programming menu, select System Options, Rep. Fail Trb. [9419].
2. Select Enabled or Disabled.

9.20. Immediate Arming from WUApp

If immediate arming from WUApp is enabled, all WEB Arm commands received are executed immediately regardless of the programmed Exit Delay – see p. 43, 8.1 Entry/Exit Delay. If disabled, the ARM commands will be executed with the programmed Exit Delay.

1. From the Programming menu, select System Options, WEB Immed. Arm [9420].
2. Select Enabled or Disabled.

9.21. T014A Standard

To turn on the T014A functionality, perform the following procedure:

☞ For this functionality to function, the EN-50131 standard must be chosen.

1. From the Programming menu, select System Options, T014A, Enable T014A [94211].
2. Select Enable or Disable.

To reset messages:

1. From the Programming menu, select System Options, T014A, Message Reset [94212].

   The system Prompts: "Messages Reset OK?"
2. Press "'√'" to reset the messages.

9.22. Alarm Memory Reset

The Alarm Memory Reset feature enables the installer to enable or disable the alarm reset procedure. This procedure, if enabled, ensures that once an armed control system has been disarmed all alarm LED indicators are automatically deactivated (reset).

To set the alarm memory reset feature; perform the following procedure:

1. From the Programming menu, select System Options, Al. Mem. Reset [9422].
2. Select Enable or Disable.

10. Communications

This section explains how to determine the way the Control System communicates via the GPRS, GSM, Ethernet and PSTN modules to the Central Station and to the user.

10.1. System Reporting

The Control System supports six report accounts for central station and user reporting. Each account has its own telephone number and communications options. The first account is always primary, every other account (that is not a voice report) may be chosen as primary or backup. Each primary account may have one, several, or no backup accounts at all. The order of calling is the following:

1. First, the Control System calls all the primary accounts, in ascending order. In case a primary account report fails, the Control System calls the backup accounts.
2. After that, the system calls the Voice Report accounts – see p. 57, 10.3 Vocal Message Dialer.

☞ If account is set as Backup after Voice Report account, reports to this account will be discarded. It is Installer responsibility to program primary and backup accounts in proper order. To ensure proper functionality, Installer will not be able to set Account 1 as Voice Report or Backup.

10.1.1. Telephone Number

To edit an account's telephone number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (1-6).
3. From the account's sub-menu, select Phone Number [#1].
4. Enter up to 16 digits. Use the 💡 key to enter "★", "#", "," (pause), "T" (switch to DTMF tone dialing), "P" (switch to pulse dialing) or "+" (international code). Use the 🚫 key to delete one character at a time. Press '√'.

10.1.2. Protocol

To program an account's communication protocol:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (1-6).
3. From the account's sub-menu, select Protocol [#2].
4. Select a protocol from the options available.

☞ Set account 1 to IP protocol if you use GPRS communication. Account number 3 is designed for use with the Follow me feature. It is the only telephone number that can be programmed by the user.

10.1.3. Communication Interface

For each account, you can choose whether the system employs PSTN, GSM, Ethernet (LAN), or GPRS communication.

To program an account's communication interface:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program account (1-6).
3. From the account's sub-menu, select Interface [#3].
4. Select PSTN, GSM, LAN, or GPRS (GPRS or LAN is used only for the first account).

10.1.4. Two-Way Audio

The Two-Way audio option determines whether Two-Way Audio is enabled for the account. For further information, see p. 31, 5.2.2 TWA Alarm Reporting.

To program the Two-Way Audio option for an account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (1-6).
3. From the account's sub-menu, select Two-Way Audio [#4].
4. Select Enabled or Disabled.

10.1.5. Account Number (not available for voice report)

To edit an account number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (1-6).
3. From the account's sub-menu, select Account Number [#5].
4. Enter up to eight digits. Enter leading zeros for account numbers of less than eight digits. Use the 💡 key to enter hexadecimal digits. Press '√' .

☞ If the programmed protocol is Contact ID, "A" is not a valid entry in the account number.

10.1.6. Call Attempts (not available for voice report)

The Call Attempts option determines the number of times the system tries to call a telephone number before moving on to the next number in sequence.

To program the number of call attempts for an account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (1-6).
3. From the account's sub-menu, select Call Attempts [#6].
4. Enter a value between 01 and 15. Press '√'.

10.1.7. Account Type (not available for voice report)

To program the account type for an account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (2-6).
3. From the account's sub-menu, select Account Type [#7].
4. Select Primary or Backup.

☞ Account 1 is by default set as a primary account.

10.2. Report Cycles

The system's attempts to report events are organized in cycles. A report cycle is a set of call attempts – see p. 56, 10.1.6 Call Attempts (not available for voice report). If the system does not succeed in sending a report to any of the telephone numbers, it tries to dial the entire report cycle again until it sends a successful report. You can determine the number of times the system attempts to dial this sequence by programming the Report Cycle option.

To program the number of Report Cycles:

1. From the Programming menu, select Communications, Accounts, Report Cycles [9517].
2. Enter a value between 01 and 15. Press '√'.

In the example illustrated in Figure 10-1, Account 1 is programmed with 2 call attempts, Account 2 is programmed with 3 call attempts and the number of report cycles programmed is 3.

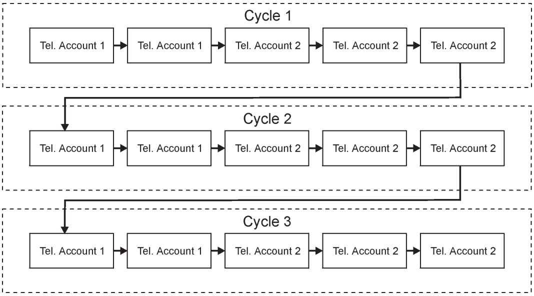


Figure 10-1: Typical Report Cycle Sequence

10.3. Vocal Message Dialer

The Vocal Message Dialer is a feature that calls the user's telephone number when specific events occur and plays pre-recorded messages. These calls are made after the system has reported the events to the central station. Additionally, in the event of an alarm, the user is able to establish a Two-Way Audio connection on receiving the vocal message in order to check the premises.

The system supports up to five Voice Report accounts. Each account has its own telephone number, communication interface and Two-Way Audio options.

The types of event that are reported using the Vocal Message Dialer feature are determined in VM Event Options – see p. 65, 10.10 Vocal Message Dialer Event Options.

If one of these events occurs, the Control System dials the phone numbers of the Voice Report Account.

The sequence for a vocal message call is as follows:

1. An event occurs and the Control System calls the telephone number of the first Voice Report Account chosen.
2. When the user answers the call, the Home ID message and the relevant event message are played.
3. The user presses 1 on their telephone; if there are additional events to report the next message is played.
   Otherwise, "No Further Messages" is announced.

   -or-

   If Two-Way Audio is enabled for the Voice Report account, the user may open the audio channel by pressing 2 on their telephone. If the user does not want to open the audio channel they may press "*" then "#" on their telephone to hang up.

If the call is not answered or the TC/VM Timeout (see p. 61, 10.6.9 Telecontrol/Vocal Message Timeout) expires before the message is acknowledged by the user pressing 1, the Control System calls the next Voice Report Account telephone number.

☞ The availability of the Vocal Message Dialer feature is hardware dependent.

10.3.1. Telephone Number

To edit a Voice Report Account account's telephone number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (2-6).
3. From the account's sub-menu, select Phone Number [#1].
4. Enter up to 16 digits. Use the 💡 key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialing), "P" (switch to pulse dialing) or "+" (international code). Use the ⊗ key to delete one character at a time. Press '√' when you have finished editing.

10.3.2. Protocol

To program voice report protocol:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (2-6).
3. From the account's sub-menu, select Protocol [#2].
4. Select Voice Report.

10.3.3. Communication Interface

For each Vocal Message account, you can choose whether the system employs cellular or PSTN communication.

To program a Voice Report Account's communication interface:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (2-6).
3. From the account's sub-menu, select Interface [#3].
4. Select GSM or PSTN.

10.3.4. Two-Way Audio

The Two-Way audio option determines whether Two-Way Audio is enabled for the Voice Report Account. For further information, see p. 31, 5.2.3 Two-Way Audio after Vocal Messages.

To program the Two-Way Audio option for a Voice Report Account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select the account you want to program (2-6).
3. From the account's sub-menu, select Two-Way Audio [#4].
4. Select Enabled or Disabled.

10.3.5. Home ID

The Home ID is a short message that is played at the beginning of a vocal message call in order to identify the system to the user. For example, at the beginning of the vocal message call, the message "Michael's House" will be played before the event messages.

To play back the Home ID message:

- From the Programming menu, select Communications, Accounts, Home ID, Play Message [95181].

To record a Home ID message:

1. From the Programming menu, select Communications, Accounts, Home ID, Record Message [95182].
2. Press '√' to start recording the message.
3. Record your message. The message may be up to ten seconds long.
4. Press '√' to stop recording; the message is automatically played back and OK? is displayed. Press '√' to save your recording.

10.4. Remote Programming

Electronics Line 3000's Remote Programmer (RP) and WEB Remote Programmer software enable you to operate and program the system from a PC either on-site or from a remote location. The software provides a comprehensive interface to the iConnect ② Control System designed to facilitate programming. There are 3 access levels available: Supervisor (full access), Technician (limited access to the program, a technician is not able to view or change user codes or the RP access code), and Operator (access to user operations, such as arming and disarming the system).

10.4.1. Remote Programmer

PC to Control System Connection Methods

You can connect to the Control System from a PC using one of three methods:

- Direct Call: The RP calls the site, the system picks up and RP communication is established.
- Callback: The RP calls the site, the system picks up then hangs up. The system then calls the Callback telephone number to establish a connection.
- Serial Connection: The RP connects directly via the USB port on the communication module (this method requires installation of the Control System USB Driver).

The following programming options relate to the method in which the Remote Programmer software connects with the system.

Callback Telephone Number

RP Callback is a security feature that helps ensure that remote programming is only performed by authorized personnel. When the Remote Programmer contacts the Control System, the Control System hangs up and calls the Callback telephone number.

To edit the Callback telephone number:

1. From the Programming menu, select Communications, Remote Prog., Call-Back # [9521].
2. Enter up to 16 digits. Use the 💡 key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialing), "P" (switch to pulse dialing) or "+" (international code). Use the ⊗ key to delete one character at a time. Press '√' when you have finished editing.

☞ If there is no Callback telephone number programmed, RP Callback is disabled and the system connects to the Remote Programmer software using the "direct call" method.

RP Passcode

The RP passcode is a six-digit code that grants access to remote programming. When establishing an RP connection, the passcode programmed in the RP customer file on the PC must be identical to the system's RP passcode.

To edit the RP passcode:

1. From the Programming menu, select Communications, Remote Prog., RP Passcode [9522].
2. Enter six digits, then press '√'.

RP Communication Interface

For remote programming, the iConnect ② Control System can employ GPRS, GSM, Ethernet, or PSTN communication.

To program the RP communication interface:

1. From the Programming menu, select Communications, Remote Prog., RP Interface [9523].
2. Select PSTN or GSM (GPRS and LAN are relevant for the WEB RP only).

RP Access Options

Options are available to enable, disable or limit access to remote programming.

To program RP Access Options:

1. From the Programming menu, select Communications, Remote Prog., RP Access [9524].
2. Select an RP access option from the following table.

Table 10-1: RP Access Options

Access option	Description
Always Enable	Up/downloading is always possible.
During Disarm	The system must be disarmed in order to establish a connection.
Disable	Up/downloading is disabled.
User Initiated	The user must perform Enable Programming from the Service menu in order to establish a connection – see p.27, 4.7.12 Enable Programming.

10.4.2. WEB Remote Programmer (Relevant only when using ELAS connection)

Electronics Line 3000's WEB-based Remote Programmer (WEB RP) allows the installer or service provider to operate and program the system via the WEB using ELAS database to get the list of supported Control Systems. To access WEB RP, the installer must enter user name and password.

10.5. Service Call

The Service Call feature is designed to enable the user to call the monitoring service at the push of a button. When the user presses the up arrow key button ▲ and then presses and holds down the Service Call button ☎ for a few seconds, a two-way audio connection with the central station is established.

10.5.1. Service Call Telephone Number

To edit the Service Call telephone number:

1. From the Programming menu, select Communications, Service Call, Phone Number [9531].
2. Enter up to 16 digits*. Use the 💡 key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialing), "P" (switch to pulse dialing) or "+" (international code). Use the ⌫ key to delete one character at a time. Press '√' when you have finished editing.

10.5.2. Service Call Interface

For the Service Call feature, you can choose whether the system employs cellular or PSTN communication.

To program the Service Call interface:

1. From the Programming menu, select Communications, Service Call, Interface [9532].
2. Select either GSM or PSTN.

10.6. Communications Options

10.6.1. Line Monitor

The Line Monitor feature monitors the PSTN telephone line. If a problem is detected with the line, a Media Loss event is registered in the log.

To program the Line Monitor setting:

1. From the Programming menu, select Communications, Comm. Options, Line Monitor [95401].
2. Select Enabled or Disabled.

10.6.2. Periodic Test Interval

The Periodic Test is a test transmission the system sends to notify the central station that its reporting capability is fully functional.

Two options are available for the Periodic Test:

- You can program the system to send a Periodic Test message according to a chosen time interval. This time interval can be between 1 and 254 hours (approximately 10 days).
- The system calculates automatically the time the Periodic Test is sent according to the last four digits of the account number. Automatically calculated tests can be sent daily, weekly or monthly according to the Auto Interval option – see p. 60, 10.6.4 Auto Interval. This feature is designed to avoid overflow of test reports to the central station at any given time.

☞ The Periodic Test event message is an unclassified event. This means that it does not belong to any event group. If the Periodic Test Interval is programmed with any value other than 000, the event message will be sent.

To program the Periodic Test Interval:

1. From the Programming menu, select Communications, Comm. Options, Test Interval [95402].
2. Enter the test interval (001-254 hours) or 255 for an automatically calculated test interval, then press '√'.

To disable the Periodic Test:

- Program the Periodic Test Interval as 000.

10.6.3. First Test

If the Periodic Test Interval is programmed as 001-254 hours, you must also program the time that the first Periodic Test is sent.

To program the First Test Time:

1. From the Programming menu, select Communications, Comm. Options, First Test [95403].
2. Enter a time (HH:MM), then press '√'.

10.6.4. Auto Interval

The Auto Interval option determines the frequency of automatically calculated periodic test messages.

To program the Auto Interval:

1. From the Programming menu, select Communications, Comm. Options, Auto Interval [95404].
2. Select Daily, Weekly or Monthly.

10.6.5. Call Timeout

The Call Timeout is the amount of time the system waits for the first acknowledgement (ACK1) from the central station when reporting using the PSTN. If ACK1 is not received during this time, the system regards the call as a failed dialing attempt.

To program the Call Timeout:

1. From the Programming menu, select Communications, Comm. Options, Call Timeout [95405].
2. Enter a time (001-255 seconds), then press '√'.

10.6.6. ACK. Timeout

The ACK Timeout is the amount of time the system waits for the second acknowledgement (ACK2) from the central station when reporting using the PSTN. If ACK2 is not received during this time, the system regards the call as a failed dialing attempt.

To program the ACK Timeout:

1. From the Programming menu, select Communications, Comm. Options, ACK Timeout [95406].
2. Enter a time (001-255 seconds), then press '√'.

10.6.7. RDM Period

Remote Diagnostics and Maintenance (RDM) session is a feature that is designed to enable automated maintenance of installed Control Systems. During a maintenance session, the Control System automatically dials the RP Callback number and connects to the RDM server. The time interval between maintenance sessions is called the RDM period.

To program the RDM period:

1. From the Programming menu, select Communications, Comm. Options, RDM Period [95407].
2. Enter the required RDM period (001-255 days or 000 to disable RDM communication).

10.6.8. Incoming Calls

This option determines whether the Control System is able to receive incoming Telecontrol/Two-Way Audio calls.

To program the Incoming Calls option:

1. From the Programming menu, select Communications, Comm. Options, Incoming Call [95408].
2. Select Enabled or Disabled.

10.6.9. Telecontrol/Vocal Message Timeout

The Telecontrol/Vocal Message Timeout (TC/VM Timeout) determines the duration of a Telecontrol, Two-Way Audio or Vocal Message call. In the case of a Telecontrol or Two-Way Audio call, when the time out expires, the system automatically disconnects unless the call is manually extended by the operator. For Vocal Message calls, if the time out expires and the user has not acknowledged the message, the system attempts to call the next Voice Report account's telephone number. During a Vocal Message call, the timeout is reset each time a message is acknowledged.

To program the Telecontrol/Vocal Message Timeout:

1. From the Programming menu, select Communications, Comm. Options, TC/VM Timeout [95409].
2. Enter a time (001-255 seconds), then press '√'.

10.6.10. Speed Dial Timeout

The Speed Dial timeout (SPD DIAL TMO) determines the duration of a Speed Dial call. When the timeout expires, the system automatically disconnects unless the call is manually extended by the operator.

To program the Speed Dial Timeout:

1. From the Programming menu, select Communications, Comm. Options, Spd Dial TMO [95410].
2. Enter a time: (00:00 — 99:59), then press '√'.

10.6.11. TWA Mode

The Two-Way audio features offer a choice of two operation modes:

- Duplex – both parties may speak at once just like a regular telephone.
- Simplex – one party may speak while the other party listens.

To program the TWA mode option:

1. From the Programming menu, select Communications, Co
2. mm. Options, TWA Mode [95411].
3. Select Duplex or Simplex.

10.7. GSM Options

10.7.1. GSM RX Report

The GSM RX Report is a feature that periodically reads the GSM signal strength of the Cellular Communication module – see p. 27, 4.7.10 GSM Signal Strength. This reading occurs at the times programmed for the Periodic Test – see p. 60, 10.6.2 Periodic Test Interval, and p. 60, 10.6.3 First Test. This means that each time the periodic test is sent, the system also sends a GSM signal strength report to the central station. The system also enters the GSM signal strength in the event log.

> ☞ If the Periodic Test is disabled, the GSM RX Report feature will not function. The GSM RX report belongs to the Peripherals event group – see p. 64, 10.9 Event Options for Central Station Reporting. If this event group is disabled, the GSM signal strength is still recorded in the event log.

To program the GSM RX Report option:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, GSM RX Report [954121].
2. Select Enabled or Disabled.

10.7.2. PIN Code

The PIN (Personal Identity Number) is a four-digit code that protects the SIM card from unauthorized use if lost or stolen.

When using a SIM card with an activated PIN code, the installer has to make sure that the PIN code programmed in the Control System is the same as the SIM card's PIN code. The PIN code should be programmed in the system before inserting the SIM card in the GSM module.

To program the PIN code:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, PIN Code [954122].
2. Edit the four-digit PIN code, then press '√'.
3. Power up the Control System to apply the new PIN Code definition.

> ☞ The new PIN code takes effect only after the System is powered up.

If a wrong PIN code was programmed in the system, a System Trouble is generated, PIN Code Error message is displayed, and GSM communication of any kind is not available. In this case, the SIM card must be reactivated.

To reactivate a SIM card:

1. Program the correct PIN code in the Control System (see above), then disconnect the Control System from all the power sources.
2. Remove the SIM card from the GSM module and insert it into a cellular phone.
3. Turn on the cellular phone and enter the correct PIN code.
4. Re-install the SIM card into the Control System and apply power.

10.7.3. SMS Center

To edit the SMS Center telephone number:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, SMS Center [954123].
2. Enter up to 16 digits. Use the 💡 key to enter "*", "#", "," (pause), "T" (switch to DTMF tone dialing), "P" (switch to pulse dialing) or "+" (international code). Use the ⊠ key to delete one character at a time. Press '√' when finished.

10.7.4. SMS Command

The SMS Command option enables you to enable or disable the ability to send commands to the system via SMS. For further information on SMS commands, see p. 18, 3.7.4 Remote Arming/Disarming via SMS and p. 33, 6.3 Telephone Control.

To enable/disable SMS commands:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, SMS Command [954124].
2. Select Enabled or Disabled.

10.7.5. SMS Confirmation

After an SMS command is executed by the system, a confirmation message is returned to the sender's mobile phone. You can enable or disable this feature using this option.

To enable/disable SMS confirmation:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, SMS Confirm [954125].
2. Select Enabled or Disabled.

10.7.6. GSM Media Loss Time

The GSM Media Loss Time is a feature that is designed to control the amount of GSM media loss events registered in the log and sent to the central station.

If, for a period defined in GSM ML Time parameter, the GSM signal has always been below the lower threshold, a Media Loss event is registered in the log and sent to the central station.

The GSM Media Loss event is sent to the central station via PSTN only.

If, for a period defined in GSM ML Time parameter, since GSM media restore is detected, the GSM signal has always been above the upper threshold, GSM Media Restore is registered in the log and sent to central station.

To disable the GSM Media Loss feature (cancel the GSM Media Loss events) enter 000.

To program the GSM Media Loss Time:

1. From the Programming menu, select Communications, Comm. Options, GSM Options, GSM ML Time. [954126].
2. Enter time (003-255 minutes or 000 to disable), then press '√'.

10.8. TWA Event Report Options

10.8.1. TWA Event Report

The TWA Event Report is an event report that is sent to the central station to indicate that Two-Way Audio communication is about to commence. If enabled, the system sends the Contact ID event code 606000 before establishing Two-Way Audio communication.

☞ This option affects Contact ID only. If using SIA, a TWA event report is always sent together with the TC/VM timeout, regardless of the configuration for this option.

To program the TWA Event option:

1. From the Programming menu, select Communications, Comm. Options, TWA Event Rept. [95413].
2. Select Enabled or Disabled.

10.8.2. TWA Time Report

If the TWA Time Report option is enabled, the last three digits of the TWA Event Report are replaced with the amount of seconds programmed for the TC/VM Timeout – p. 61, 10.6.9 Telecontrol/Vocal Message Timeout. For example, if the TC/VM Timeout is programmed as 120 seconds, the Contact ID event code to be sent for the TWA Event Report will be 606120.

To program the TWA Time Report option:

1. From the Programming menu, select Communications, Comm. Options, TWA Time Rept. [95414].
2. Select Enabled or Disabled.

10.8.3. Incoming Number

Incoming number feature allows the installer to program up to three high-priority telephone numbers so that the user would be able to use Telecontrol/2-way audio over GSM during a GPRS session. If the Control System recognizes the incoming call as a high-priority call, the GPRS session will be suspended.

To program/edit the Incoming Number:

1. From the Programming menu, select Communications, Comm. Options, Incoming #. [95415].
2. Select the telephone number you want to edit (1-3).
3. Enter up to 16 digits. Use the 💡 key to enter "★", "#", "," (pause), "T" (switch to DTMF tone dialing), "P" (switch to pulse dialing) or "+" (international code). Use the ⊗ key to delete one character at a time. Press '√' when you have finished editing.

10.8.4. Remote Firmware Update

Electronics Line 3000's Remote Firmware Update feature allows the Installer or service provider to perform firmware update from a remote PC using WEB communication.

☞ Before performing the firmware update, locally disarm the system and make sure that there are no AC LOSS or BATTERY LOW conditions.

To setup the firmware update mode:

1. From the Programming menu, select Communications, Comm. Options, Rem. SW Update [95416].
2. Select the Remote Firmware Update mode from the following table:

Table 10-2: Remote FW Update

Access option	Description
Always Enable	Update is always possible.
Disable	Firmware update is not allowed.
User Initiated	The user must perform SW Update from the Service menu in order to establish a connection – see p. 28, 4.7.14 Remote Firmware Update.

10.8.5. PSTN Country

In order to meet the requirements of local telecommunications authorities, default telephone line parameters have been chosen for a number of different countries.

To program the PSTN Country:

1. From the Programming menu, select Communications, Comm. Options, PSTN Country [95417].
2. Select your country from the options available.

☞ Electronics Line 3000 offers custom telephone line parameter settings for countries that do not appear in the list of pre-defined options. If your country does not appear among the available options, select the option Custom Settings.

10.8.6. Dial Tone Wait

This option determines whether the system dials only when the dial tone is present or if the dialing is initiated regardless of the dial tone.

To program the Dial Tone Wait option:

1. From the Programming menu, select Communications, Comm. Options, Dial Tone Wait [95418].
2. Select Enabled or Disabled.

10.9. Event Options for Central Station Reporting

System events are divided into a number of different event groups. This division allows you to enable or disable reporting or Two-Way Audio for a specific group of events.

The different event groups are as follows:

- Burglary [#1]
- Fire [#2]
- Open/Close (arm/disarm) [#3]
- Service [#4]
- Power [#5]
- Peripherals [#6]
- RF Jamming [#7]
- Medical

10.9.1. Event Reporting

You can enable or disable event reporting per Event Group. This allows you to filter the type of events that are reported to the central station.

To enable or disable reporting for an event group:

1. From the Programming menu, select Communications, Event Options [955].
2. Select an Event Group.
3. From the event group's sub-menu, select Report [#1].
4. Select Enabled or Disabled.

10.9.2. Restore Reporting

For each event group, you can determine whether restore messages will be sent.

To enable or disable restore reporting for an event group:

1. From the Programming menu, select Communications, Event Options [955].
2. Select an event group.
3. From the event group's sub-menu, select Report Restore [#2].
4. Select Enabled or Disabled.

10.9.3. Two-Way Audio

For Burglary, Fire and Medical event groups, there is an additional option that enables Two-Way Audio for that event group – see p. 31, 5.2.2 TWA Alarm Reporting.

To enable/disable Two-Way Audio for an event group:

1. From the Programming menu, select Communications, Event Options [955].
2. Select an Event Group (Burglary, Fire or Medical).
3. Select TWA [#3].
4. Select Enabled or Disabled.

10.10. Vocal Message Dialer Event Options

Events reported using the Vocal Message Dialer are divided into event groups that correspond with the pre-recorded event messages. This allows you to enable or disable the Vocal Message feature for a specific group of events. For further information on this feature, see p. 57, 10.3 Vocal Message Dialer.

The vocal message event groups and their associated system events are as follows:

Burglary [#1]

- Alarm from Zone (excluding Gas and Environmental zones)
- Zone Tamper
- Tamper
- Duress

Fire [#2]

- Zone Fire Alarm
- User Activated Fire Alarm

Panic [#3]

- Zone Panic Alarm
- User Activated Panic Alarm

Medical [#4]

- Zone Medical Alarm
- Zone Medical Alarm
- User Activated Alarm
- No Motion

Arm [#6]

- Full Arm
- Part Arm
- Perimeter Arm

Disarm [#7]

- Disarm
- Disarm after Alarm

Water [#8]

- Zone Water Alarm (Flood)

System Trouble [#5]

- Battery Low
- Transmitter Low Battery
- AC Loss
- Media Loss
- Device Trouble
- Communication Trouble
- Transmitter Out of Synch.
- Control System Transmitter Out of Synch.
- Supervision Loss
- Zone Trouble
- FM Jamming

To enable/disable the vocal message for an event group:

1. From the Programming menu, select Communications, VM Event Opt. [956].
2. Select an event group.
3. Select Enabled or Disabled.

11. Internet Options

The following options concern the configuration of the GPRS and Ethernet Communication Modules. In most cases, the Internet options will be pre-programmed as defaults and you will not be required to change any of the settings apart from the CPID and password for each customer.

11.1. ELAS Connection Parameters

The following parameters, required to connect Control System to ELAS, are set by ELAS administrator.

11.1.1. Proxy Address

To edit the Proxy Address:

1. From the Programming menu, select Communications, Internet, Proxy Address [9571].
2. Enter the Proxy Address IP provided by your ELAS administrator. Use the "1" key to enter ".", 💡 key to insert and the ⊗ key to delete one character at a time. Press '√' when finished.

11.1.2. XML Proxy Port

To edit the XML Proxy Port:

1. From the Programming menu, select Communications, Internet, XML Proxy Port [9572].
2. Enter the XML Proxy Port provided by your ELAS administrator. Use the "1" key to enter ".", 💡 key to insert and the ⊗ key to delete one character at a time. Press '√' when finished.

11.2. Control System Parameters

The following parameters, required to connect Control System to ELAS, should be provided by your ELAS administrator.

11.2.1. CP ID

To edit the Control System ID:

1. From the Programming menu, select Communications, Internet, CP ID [9573].
2. Enter the unique Control System ID provided by your ELAS administrator to connect the Control System to ELAS. Use the "1" key to enter ".", 💡 key to insert and the ⊗ key to delete one character at a time. The ID length must be six up to sixteen characters. Press '√' when finished.

11.2.2. CP Password

To edit the Control System Password:

1. From the Programming menu, select Communications, Internet, CP Password [9574].
2. Enter the Control System Password provided by your ELAS administrator to connect the Control System to ELAS. Use the "1" key to enter ".", 💡 key to insert and the ⊗ key to delete one character at a time. The password length must be six up to sixteen characters. Press '√' when finished.

11.2.3. ELAS Connection On/Off

To enable/disable ELAS connection option:

1. From the Programming menu, select Communications, Internet, ELAS Connect [9575].
2. Select Enabled or Disabled.

11.3. GPRS Network Parameters

The following parameters, required to program your GPRS connection, should be provided by the cellular provider.

11.3.1. APN

To edit the APN name of your GPRS connection:

1. From the Programming menu, select Communications, Internet, GPRS Options, APN [95761].
2. Enter the APN name provided by the cellular provider. Use the "1" key to enter ".", 💡 key to insert and the ☒ key to delete one character at a time.

11.3.2. User Name

To edit the User name of your GPRS connection (optional setting provided by the cellular provider):

1. From the Programming menu, select Communications, Internet, GPRS Options, User Name [95762].
2. Enter the User Name provided by the cellular provider. Use the "1" key to enter ".", 💡 key to insert and the ☒ key to delete one character at a time.
3. Press '√' when you have finished editing.

11.3.3. Password

To edit the Password of your GPRS connection (optional setting provided by the cellular provider):

1. From the Programming menu, select Communications, Internet, GPRS Options, Password [95763].
2. Enter the Password provided by the cellular provider. Use the "1" key to enter ".", 💡 key to insert and the ☒ key to delete one character at a time.

11.3.4. GPRS Write TMO

To edit the GPRS Write TMO of your GPRS connection:

1. From the Programming menu, select Communications, Internet, GPRS Options, GPRS Write TMO [95764].
2. Enter the GPRS Write TMO (015 -255 seconds). Press '√' when finished.

11.4. LAN Network Parameters

The following options concern the configuration of the Ethernet. All of the information required for programming these options should be provided by the network administrator.

There are two methods of programming the IP settings:

- Automatic IP settings (DHCP) – when using a DHCP server, the server provides all of the configuration settings automatically.
- Manual IP settings – you must enter the relevant IP addresses, Gateway and Subnet Mask, taking into consideration your router settings.

11.4.1. LAN IP Address

To edit the LAN IP address:

1. From the Programming menu, select Communications, Internet, LAN Options, LAN IP Address [95771].
2. Enter an IP address. Press the 💡 key as many times as necessary to select "." and the ☒ key to delete one character at a time.

☞ When you choose to use DHCP, set the IP address and Gateway values to "0", and the subnet mask to 255.255.255.000 (or another value according to your router's settings); if not, insert the IP Address, Subnet Mask, and Gateway. Press '√' when you have finished editing.

11.4.2. Subnet Mask

To edit the subnet mask:

1. From the Programming menu, select Communications, Internet, LAN Options, Subnet Mask [95772].
2. Enter the Subnet Mask. Press the 💡 key as many times as necessary to select "." and the ☒ key to delete one character at a time.

11.4.3. Gateway

To edit the Gateway address:

1. From the Programming menu, select Communications, Internet, LAN Options, Gateway [95773].
2. Enter the Gateway's IP address. Press the 💡 key as many times as necessary to select "." and the ✖ key to delete one character at a time.

11.4.4. DNS Server

To edit the DNS Server address:

1. From the Programming menu, select Communications, Internet, LAN Options, DNS Server [95774].
2. Enter the DNS Server's IP address. Press the 💡 key as many times as necessary to select "." and the ✖ key to delete one character at a time.

11.4.5. LAN Write TMO

To edit the LAN Write TMO:

1. From the Programming menu, select Communications, Internet, LAN Options, LAN Write TMO [95775].
2. Enter the LAN Write TMO. Press the 💡 key as many times as necessary to select "." and the ✖ key to delete one character at a time.

11.4.6. Trouble Conditions

The testing and status options of the Internet connection status should provide the installer with the exact source of the problem when the Control System is not capable of reporting via LAN. See p. 130, Appendix D: Event Table.

12. Home Automation Programming

This chapter explains the programmable options for the system's home automation features. The Home Automation module is an add-on optional extra that you can install inside the Control System's plastic housing.

☞ The iConnect System's home automation features require the use of an external power-line interface when used in an 110V/60HZ power system.

12.1. X10 Overview

The Control System's home automation feature employs the X10 protocol and this enables compatibility with a wide variety of readily available home automation products.

Before you can start programming the system's Home Automation features, you should be familiar with the basic concept behind X10 automation.

X10 is a protocol that enables you to send commands and other data over regular existing power lines. This means that, using an X10 transmitter (the Control System's Home Automation module), you can send On/Off commands to X10 receivers (lamp and appliance modules) that are plugged into electricity outlets around the home. From here on, we will refer to these X10 receivers as "HA units".

Each HA unit has two codes that are used for identification. These codes are known as the House code and the Unit code and are usually defined by adjusting the dials that appear on the X10 unit. In Figure 12-1, the HA unit is set to House A, Unit 3.

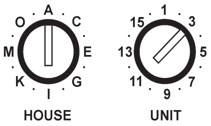


Figure 12-1: HA Unit Dials

The Control System supports sixteen HA units on one House code. To ensure that the Home Automation features function correctly, you must abide by the following guidelines.

- The House code must be the same on each HA unit.
- The House code on the HA units must be identical to the House code programmed in the Control System's memory – see p.72, 12.3 House Code.

12.2. HA Units

The following sections explain the programming options available for HA units.

12.2.1. Scheduling (not relevant to PGM)

Scheduling allows you to program the Control System to send On/Off commands to an HA unit at specific times. For information on programming the On Time, Off Time and Schedule for each HA unit, see p. 34, 6.4 Scheduling.

12.2.2. On by Zone

The On by Zone feature allows you to choose two zones that activate the HA unit when triggered. When either one of these zones is triggered, the system sends an On command to the HA unit according to the unit's programmed Pulse Time – see p. 72, 12.2.8 Pulse Time. For example, you have a magnetic contact installed above the front door. When the door is opened, the hall light is lit.

To select the detectors that activate an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select On by Zone [#04].
4. Enter up to two zone numbers.

12.2.3. On by Arm

The On by Arm feature activates the HA unit when the system is armed using any of the arming methods. The amount of time the HA unit is activated is determined by the Pulse Time – see p. 72, 12.2.8 Pulse Time. If the Pulse Time is programmed as "Toggle", disarming the system switches the HA unit off.

To program the On by Arm feature:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select On by Arm [#05].
4. Select Enabled or Disabled.

12.2.4. On by Alarm

On by Alarm is a feature designed for use with X10 sirens. When an alarm occurs, the HA unit (i.e. siren) is activated for the duration of the siren cutoff – see p. 42, 7.7.2 Siren Cut-Off. The X10 siren sounds a continuous pattern for intrusion/panic alarms and a pulsed pattern for fire alarms.

To program the On by Alarm feature:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select On by Alarm [#06].
4. Select Enabled or Disabled.

☞ If an HA unit is programmed to be activated by the On by Alarm feature, program all other operation modes (On by Arm, Randomize, etc.) as disabled.

Do not program more than one HA unit to be activated by the On by Alarm feature. If more than one siren is required, set all sirens with the same House and Unit code.

12.2.5. Keyfob Control

Each keyfob (EL-4714), offers control of up to two individual HA units. This programming option allows you to enable or disable this feature per HA unit.

To program the keyfob control option for an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select KF Ctrl [#07].
4. Select Enabled or Disabled.

12.2.6. Telephone Control

Via SMS or DTMF, you can send commands to the system in order to control various HA units. This option allows you to enable or disable this feature for each HA unit.

To program the telephone control option for an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select TEL Ctrl [#08].
4. Select Enabled or Disabled.

12.2.7. Randomize

When the system is fully armed between the hours 9:00pm and 6:00am, the Randomize feature turns HA units on and off at random. This gives the impression that the house is occupied and acts as a deterrent against potential intruders.

To program an HA unit to be included in the Randomize feature:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select Randomize [#09].
4. Select Enabled or Disabled.

12.2.8. Pulse Time

The Pulse Time determines the manner in which an HA unit responds to the On command. You can program each HA unit switch on momentarily. This means that, on receiving the On command, the unit will be switched on for a programmed amount of time. For example, you can program the hall light to switch on for 1 minute and automatically switch itself off. Alternatively, the HA unit can be programmed to toggle on and off.

To program the Pulse Time for an HA unit:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select Pulse Time [#10].
4. Select 5 sec, 30 sec, 1 min, 2 min or Toggle.

12.2.9. Descriptor

You can assign a 16-character descriptor for each HA unit. These descriptors help the user to identify the various HA units installed around the home.

To edit an HA unit descriptor:

1. From the Programming menu, select HA Programming, HA Units [961].
2. Select an HA unit (01-16).
3. From the HA unit's sub-menu, select Descriptor [#11].
4. Edit the descriptor using the alphanumeric keypad.

12.3. House Code

The House code is part of the identification code of each HA unit. For the Home Automation features to function correctly, the House code on each HA unit must be identical to the House code programmed in the system's memory.

To program the system House code:

1. From the Programming menu, select HA Programming, House Code [962].
2. Using the arrow keys, select a House code from the options available (A-P).

12.4. HA Control

The HA Control option allows you to enable or disable all Home Automation features for the entire system.

To program the Home Automation setting:

1. From the Programming menu, select System Options, HA Control [963].
2. Select Enabled or Disabled.

☞ PGM output is not affected by HA Control parameter. Remote activation of PGM is possible, even when HA control is disabled, as long as the PGM output trigger is defined as Telecontrol – see p. 49 9.7.1 Output Trigger.

13. System Initialization

The Initialization menu offers a number of options that enable you to reset the system. This menu is particularly useful when re-installing a Control System at a new site. The Initialization function clears the entire system. This restores programming defaults, clears the log, user codes and the transmitter register. Options are also available that enable you to clear a specific section of the system's memory separately.

13.1. Initialization

The Initialization function clears the entire system and resets factory defaults. If your system does not include multi-default and multi-language support, skip steps 2 and 3 of the following procedure.

To initialize the Control System:

1. From the Programming menu, select Initialize, Init All [971]; the system prompts you for confirmation.
2. For firmware versions that include multi-default and multi-language support, select the set of programming defaults that you want to load.
3. For firmware versions that include multi-default and multi-language support, select the required interface language. Factory programming defaults are restored, the event log is cleared, ser codes and wireless transmitters are deleted.

☞ During system initialization, recorded vocal messages (Message Center and Home ID) are not deleted.

13.2. Default Program Restore

Loading the system's default program enables you to restore the factory-set programming defaults.

To load the default program:

- From the Programming menu, select Initialize, Load Defaults [972]; the system prompts you for confirmation.

13.3. Clear User Codes

Clear User Codes deletes all programmed user codes and restores the default Master and Installer codes.

To clear user codes:

- From the Programming menu, select Initialize, Clear Users [973]; the system prompts you for confirmation.

13.4. Clear Wireless Transmitters

The Clear Wireless Transmitters function enables you to delete all registered transmitters at once.

To clear the transmitter register:

- From the Programming menu, select Initialize, Clear Wireless [974]; the system prompts you for confirmation.

13.5. Find Modules

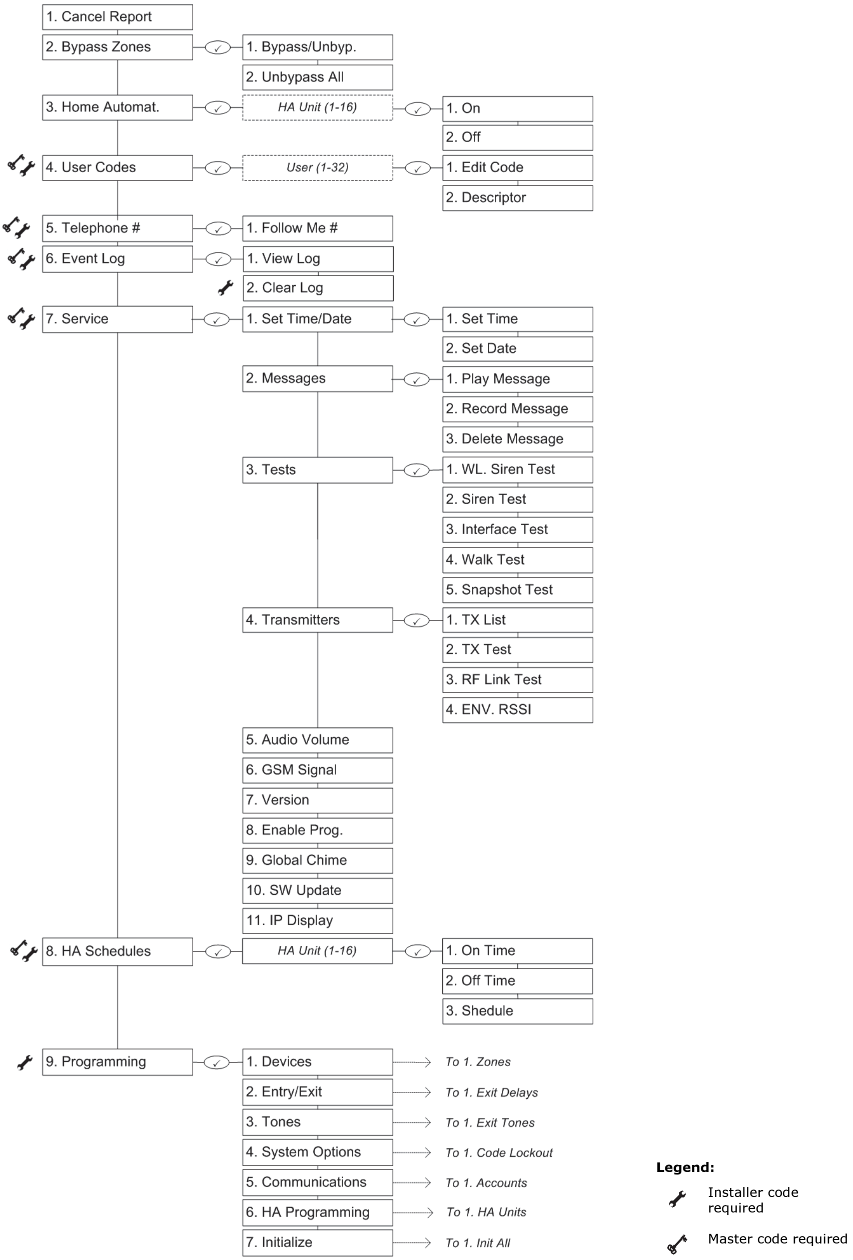
The Find Modules function runs a diagnostic test that identifies the modules that are connected to the system bus. With this information, the system knows which add-on modules should be present, enabling supervision for those modules.

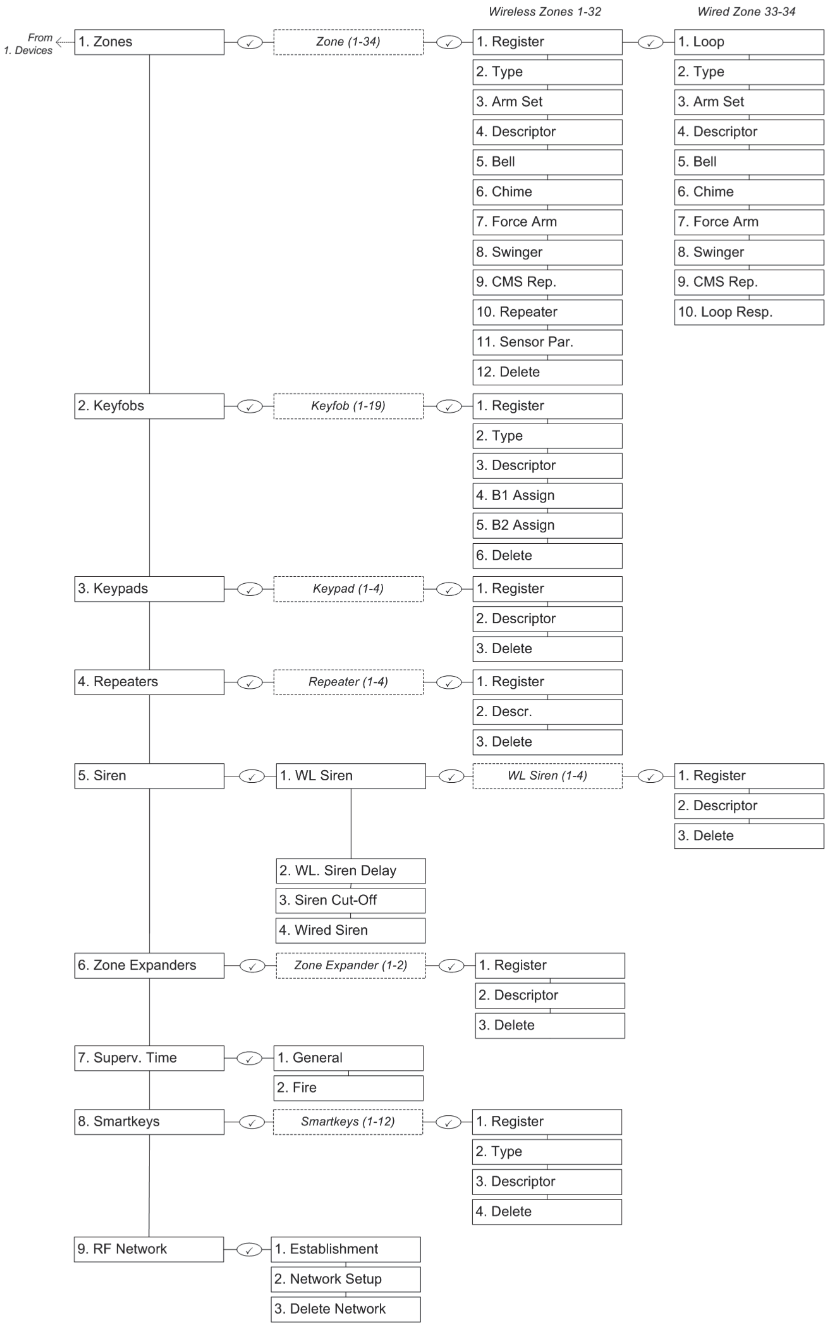
To run the Find Modules test:

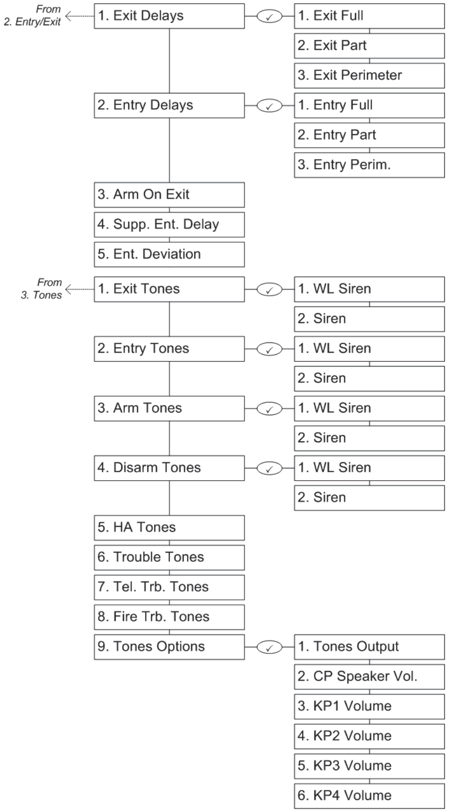
1. From the Programming menu, select Initialize, find Modules [975]; the system prompts you for confirmation.
2. Press '√' to confirm; the system begins to search for the connected modules. At the end of the search, the modules that are present are displayed and the system asks if you want to save the displayed list.

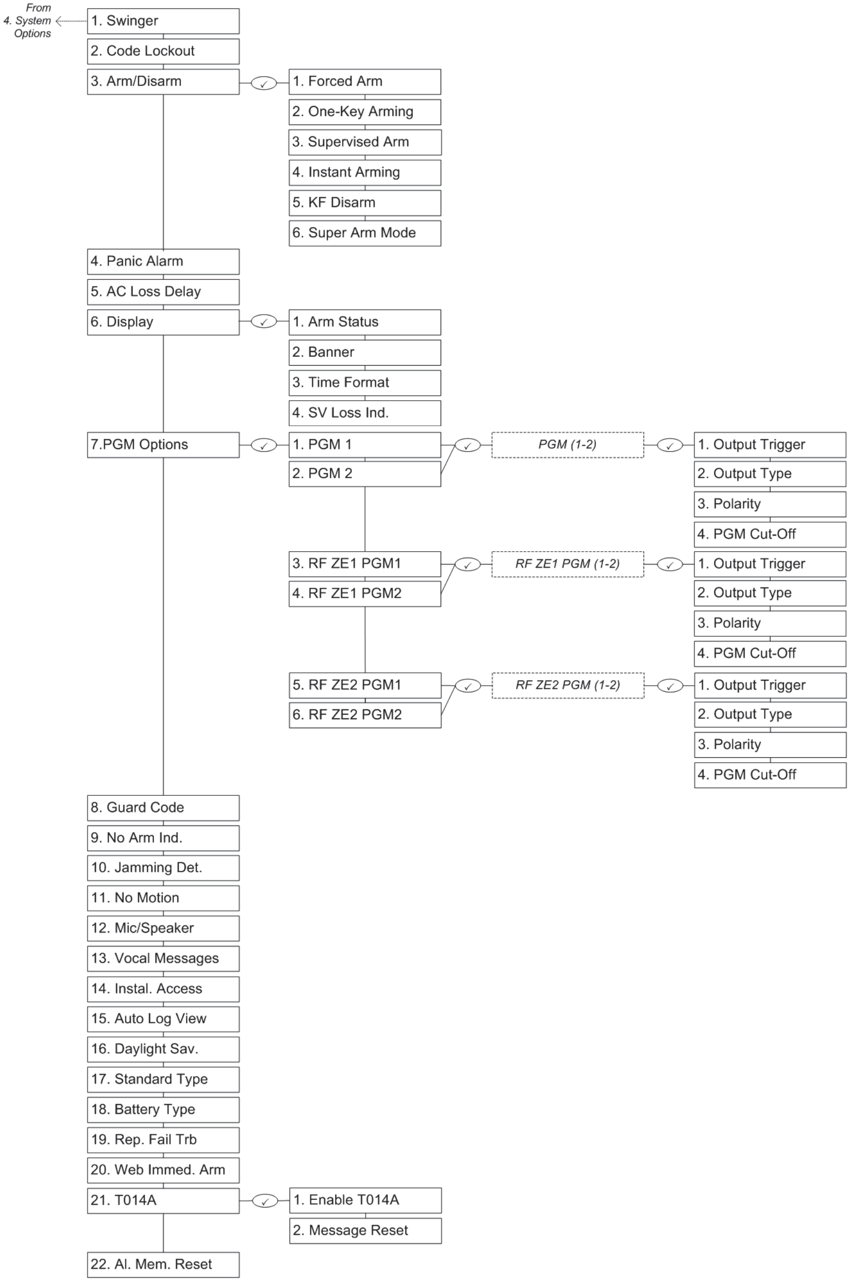
☞ If a connected module is not included in the list, check the wiring connections and run this test again.

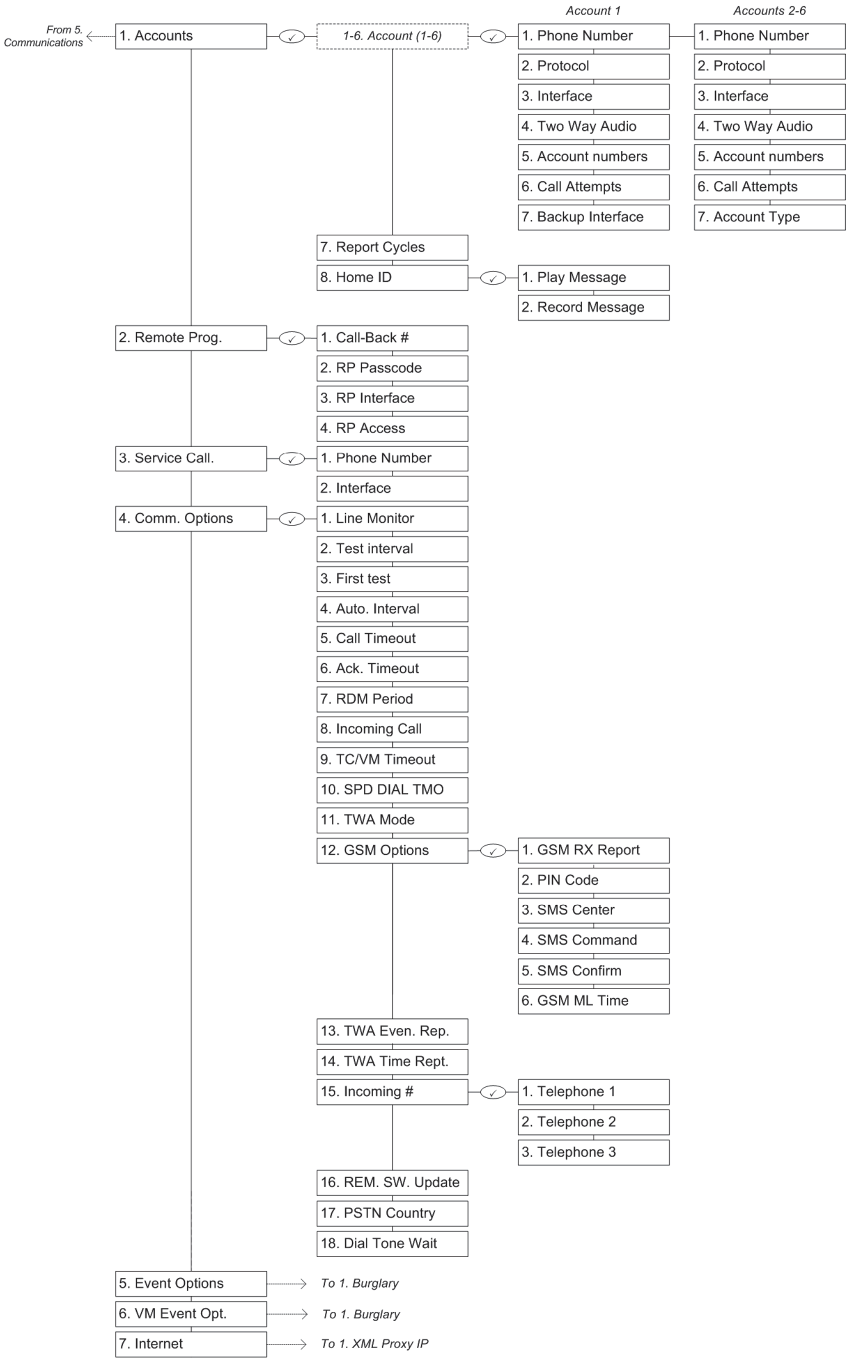
Appendix A: Menu Structure

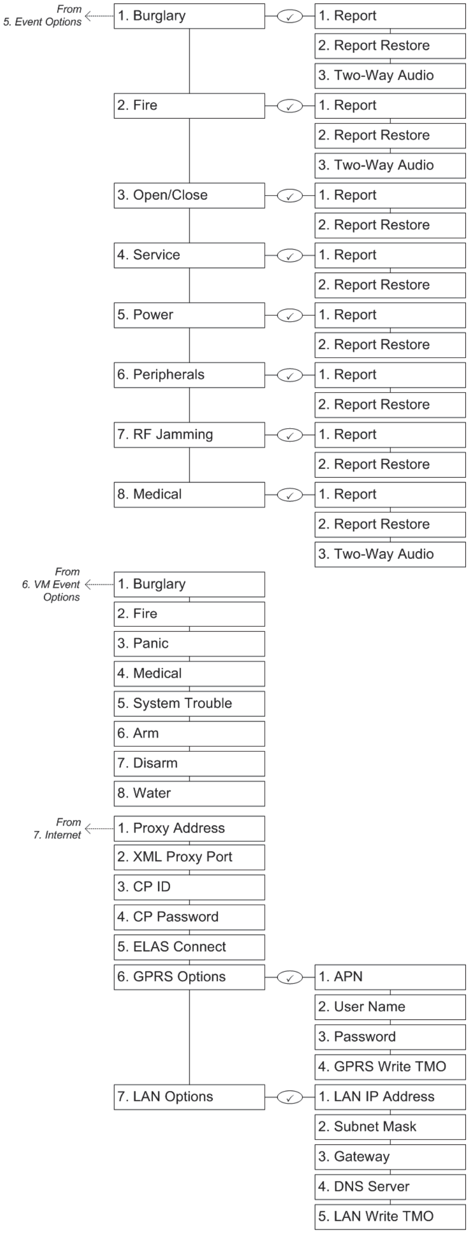


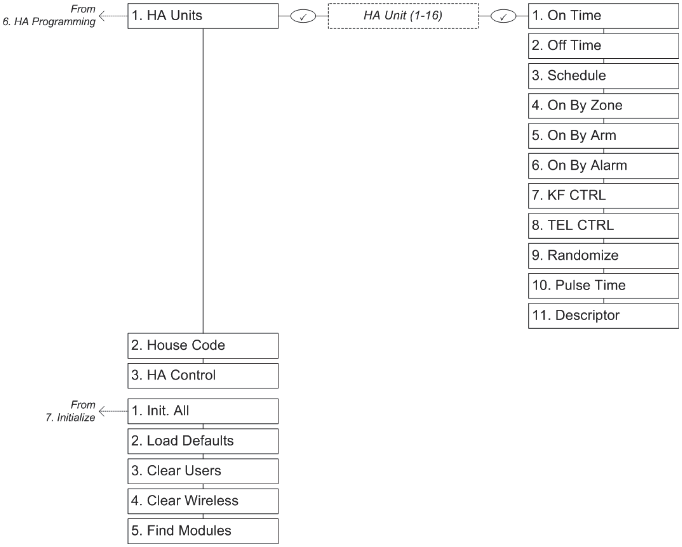

Wireless Zones 1-32
Wired Zone 33-34
From
1. Devices
1. Zones
Zone (1-34)
1. Register
2. Type
3. Arm Set
4. Descriptor
5. Bell
6. Chime
7. Force Arm
8. Swinger
9. CMS Rep.
10. Repeater
11. Sensor Par.
12. Delete
1. Loop
2. Type
3. Arm Set
4. Descriptor
5. Bell
6. Chime
7. Force Arm
8. Swinger
9. CMS Rep.
10. Loop Resp.
2. Keyfobs
Keyfob (1-19)
1. Register
2. Type
3. Descriptor
4. B1 Assign
5. B2 Assign
6. Delete
3. Keypads
Keypad (1-4)
1. Register
2. Descriptor
3. Delete
4. Repeaters
Repeater (1-4)
1. Register
2. Descr.
3. Delete
5. Siren
1. WL Siren
WL Siren (1-4)
1. Register
2. Descriptor
3. Delete
2. WL. Siren Delay
3. Siren Cut-Off
4. Wired Siren
6. Zone Expanders
Zone Expander (1-2)
1. Register
2. Descriptor
3. Delete
7. Superv. Time
1. General
2. Fire
8. Smartkeys
Smartkeys (1-12)
1. Register
2. Type
3. Descriptor
4. Delete
9. RF Network
1. Establishment
2. Network Setup
3. Delete Network


From
2. Entry/Exit
1. Exit Delays
✓
1. Exit Full
2. Exit Part
3. Exit Perimeter
2. Entry Delays
✓
1. Entry Full
2. Entry Part
3. Entry Perim.
3. Arm On Exit
4. Supp. Ent. Delay
5. Ent. Deviation
From
3. Tones
1. Exit Tones
✓
1. WL Siren
2. Siren
2. Entry Tones
✓
1. WL Siren
2. Siren
3. Arm Tones
✓
1. WL Siren
2. Siren
4. Disarm Tones
✓
1. WL Siren
2. Siren
5. HA Tones
6. Trouble Tones
7. Tel. Trb. Tones
8. Fire Trb. Tones
9. Tones Options
✓
1. Tones Output
2. CP Speaker Vol.
3. KP1 Volume
4. KP2 Volume
5. KP3 Volume
6. KP4 Volume


From
4. System
Options
1. Swinger
2. Code Lockout
3. Arm/Disarm
1. Forced Arm
2. One-Key Arming
3. Supervised Arm
4. Instant Arming
5. KF Disarm
6. Super Arm Mode
4. Panic Alarm
5. AC Loss Delay
6. Display
1. Arm Status
2. Banner
3. Time Format
4. SV Loss Ind.
7.PGM Options
1. PGM 1
2. PGM 2
PGM (1-2)
1. Output Trigger
2. Output Type
3. Polarity
4. PGM Cut-Off
3. RF ZE1 PGM1
4. RF ZE1 PGM2
RF ZE1 PGM (1-2)
1. Output Trigger
2. Output Type
3. Polarity
4. PGM Cut-Off
5. RF ZE2 PGM1
6. RF ZE2 PGM2
RF ZE2 PGM (1-2)
1. Output Trigger
2. Output Type
3. Polarity
4. PGM Cut-Off
8. Guard Code
9. No Arm Ind.
10. Jamming Det.
11. No Motion
12. Mic/Speaker
13. Vocal Messages
14. Instal. Access
15. Auto Log View
16. Daylight Sav.
17. Standard Type
18. Battery Type
19. Rep. Fail Trb
20. Web Immed. Arm
21. T014A
1. Enable T014A
2. Message Reset
22. Al. Mem. Reset


From 5. Communications
1. Accounts
1-6. Account (1-6)
Account 1
1. Phone Number
2. Protocol
3. Interface
4. Two Way Audio
5. Account numbers
6. Call Attempts
7. Backup Interface
Accounts 2-6
1. Phone Number
2. Protocol
3. Interface
4. Two Way Audio
5. Account numbers
6. Call Attempts
7. Account Type
7. Report Cycles
8. Home ID
1. Play Message
2. Record Message
2. Remote Prog.
1. Call-Back #
2. RP Passcode
3. RP Interface
4. RP Access
3. Service Call.
1. Phone Number
2. Interface
4. Comm. Options
1. Line Monitor
2. Test interval
3. First test
4. Auto. Interval
5. Call Timeout
6. Ack. Timeout
7. RDM Period
8. Incoming Call
9. TC/VM Timeout
10. SPD DIAL TMO
11. TWA Mode
12. GSM Options
1. GSM RX Report
2. PIN Code
3. SMS Center
4. SMS Command
5. SMS Confirm
6. GSM ML Time
13. TWA Even. Rep.
14. TWA Time Rept.
15. Incoming #
1. Telephone 1
2. Telephone 2
3. Telephone 3
16. REM. SW. Update
17. PSTN Country
18. Dial Tone Wait
5. Event Options
To 1. Burglary
6. VM Event Opt.
To 1. Burglary
7. Internet
To 1. XML Proxy IP


From
5. Event Options
1. Burglary
1. Report
2. Report Restore
3. Two-Way Audio
2. Fire
1. Report
2. Report Restore
3. Two-Way Audio
3. Open/Close
1. Report
2. Report Restore
4. Service
1. Report
2. Report Restore
5. Power
1. Report
2. Report Restore
6. Peripherals
1. Report
2. Report Restore
7. RF Jamming
1. Report
2. Report Restore
8. Medical
1. Report
2. Report Restore
3. Two-Way Audio
From
6. VM Event
Options
1. Burglary
2. Fire
3. Panic
4. Medical
5. System Trouble
6. Arm
7. Disarm
8. Water
From
7. Internet
1. Proxy Address
2. XML Proxy Port
3. CP ID
4. CP Password
5. ELAS Connect
6. GPRS Options
1. APN
2. User Name
3. Password
4. GPRS Write TMO
7. LAN Options
1. LAN IP Address
2. Subnet Mask
3. Gateway
4. DNS Server
5. LAN Write TMO


From
6. HA Programming
1. HA Units
✓
HA Unit (1-16)
✓
1. On Time
2. Off Time
3. Schedule
4. On By Zone
5. On By Arm
6. On By Alarm
7. KF CTRL
8. TEL CTRL
9. Randomize
10. Pulse Time
11. Descriptor
2. House Code
3. HA Control
From
7. Initialize
1. Init. All
2. Load Defaults
3. Clear Users
4. Clear Wireless
5. Find Modules

Appendix B: Transmitter Installation

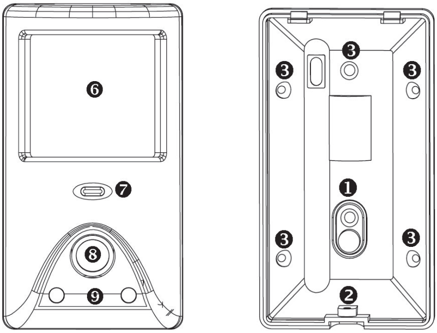
PIR Detectors (EL-4755/EL-4755PI)

The EL-4755 and EL-4755PI are intelligent 2-Way wireless PIR camera detectors designed for use with the iConnect Control System.

Each iConnect Control System (up-to-32-zone) can support up to eight PIR camera detectors.

All these detectors implement a feature to combat the problem of multiple transmissions, which drastically reduce the life of the batteries. After each transmission, there is a four-minute delay during which further transmissions will not be sent. When batteries need replacing, the detector sends a low battery indication to the Control System. The EL-4755PI is designed for pet installations and provides good immunity to nuisance alarms caused by pets and animals.

Detectors that meet the EN-50131 standard, have a three-minute delay between transmissions.



1. Tamper switch and mounting tab
2. Fastening screw hole
3. Mounting holes
4. Battery holders
5. Antenna
6. PIR Detector
7. Indicator LED
8. Camera Lens
9. IR LEDs

Figure B- 1: PIR Detector Outer Casing, Front & Back Views – EL-4755/4755PI

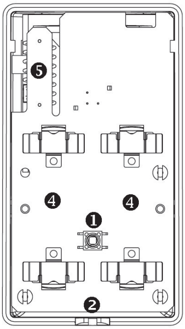


Figure B- 2: PIR Detector with Cover Removed – EL4755/4755PI

Consideration before Installation

- Select a location from which the pattern of the detector is most likely to be crossed by a burglar, should there be a break in.
- Do not place bulky objects in front of the detector.
- Avoid a location that comes in direct contact with radiators, heating/cooling ducts or air conditioners.
- Do not place the detector in front of windows subject to direct sunlight or drafts.

Pet Immunity Guidelines (EL-4755PI)

It is expected that the EL-4755PI will eliminate false alarms caused by:

- Animals up to 36kg/80lbs
- Several small rodents
- Random flying birds.

☞ The weight of the animal should only be used as a guide, other factors such as the length and color of fur also affect the level of immunity.

For maximum pet immunity the following guidelines are recommended:

- Mount the center of the detector at a height of 2.0m.
- Do not aim the detector at stairways that can be climbed by an animal.
- Avoid a location where an animal can come within 1.8m (6') of the detector by climbing on furniture, boxes or other objects.

Registration Procedure

The EL-4755/4755PI must identify itself to the iConnect ② Control System as follows

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'
2. Unscrew the casing back
3. Insert the supplied batteries into their battery holders. The detector will send a transmission, which if successfully received by the system will generate a confirmation sound. If no confirmation sound is heard, send another transmission by pressing and releasing the tamper switch of the device.
4. After the detector is successfully registered the display shows: Save? Press '√' to confirm and continue entering other parameters for the chosen device.

☞ To delete a PIR detector from the system refer to the Quick Installer manual.

Parameter Setting Procedure

As a 2-Way detector, the EL-4755/4755PI parameters can be modified only from the iConnect ② Control System.

Go to the main menu and select [9]>[1]>[1]>[11] (Programming > Devices > Zones > Sensor Par) and define the parameters according to the following table:

Table B- 1: Parameter Settings (EL-4755/EL-4755PI)

Sensor Par.	Parameter
LED	ENABLED/DISABLED
PULSE	1, 2 – The pulse counter determines the amount of beams that need to be crossed before the sensor will produce an alarm, with 1 being more sensitive:
ALARM DELAY	1–20 minutes (3) – The delay between reporting detections to the main unit
CAMERA RESOLUTION	VGA (640X480), QVGA (320X240), QVGA (160X120)
COLOR	COLOR, B&W (Black and White)
COMPRESSION	HIGH, LOW (more/less distortion)
FLASH	ENABLED, DISABLED
# OF PICTURES	1–9; 1–5 VGA (3)
	For Future Use
PICTURE DELAY	0–480 MS (480)
USER MONITOR	ENABLE, DISABLE
ZONE ASSIGNMENT	00-00-00-000 – Movement detection in any of the up-to-four specified zones triggers the camera to take a picture.
*Default in bold	

Web Interface Access

Transmitted pictures are visible through the web interface:

1. Access the supplied IP through your smart phone (iPhone) or web browser
2. Input access credentials
3. Click "Video" to view captured still pictures and configure settings.

Installation Procedure

To install PIR detectors:

☞ Before permanently mounting the detector, test the transmitter from the exact mounting position. If necessary, improve the position of the transmitter. The recommended height is 2.2m (6.6 ft).

1. If the unit is screwed together, unscrew the casing back.
2. Knock out the mounting holes of the mounting bracket and attach it to the wall, as appropriate.

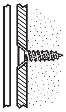


Figure B- 3: Mounting Screw Position

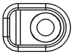


Figure B- 4: Rear Tamper Release

3. To use the rear tamper switch, insert a screw into the rear tamper mounting hole located in the lower center of the bracket. When the bracket is removed from the wall, the screw causes the tamper release to break away from the bracket and the rear tamper switch is released
4. Attach the screw provided in the detector kit to the bottom of the mounting bracket.

Operation Modes

Warm-up Time

The detector will need to warm up for the first 90 seconds after applying power.

Walk Test Mode

A walk test is performed in order to determine the lens coverage pattern of the detector. Walk Test mode cancels the delay time between detections, enabling you to perform an efficient walk test.

To walk test the detector:

1. Set the iConnect ② Control System to Walk test mode (Quick key 7>03>4).
2. Walk across the scope of the detector according to the detection pattern selected.
3. Confirm that the LED activates and deactivates accordingly. Wait for ten seconds after each detection before continuing the test.
4. After completing the walk test set the system to normal operation mode.

To test the detector camera:

1. Set the iConnect ② Control System to camera test mode (Quick key 7>03>5). Confirm with '√'.
2. If more than one PIR camera zone is defined, select a defined zone and press '√'.
3. In the displayed: SNAPSHOTS, choose the number (1-9) of snapshots to be taken and press '√' to transmit the snapshots.

LED Indication

The LED indicator is lit every time a transmission is made. The LED can be enabled / disabled by programming.

Battery Replacement

In case of a low battery (2.5VDC or less), the detector low battery condition is reported to the system and low battery message is displayed.

To replace the battery:

1. Unscrew the casing back.
2. Remove the spent batteries and replace them.
3. Re-attach the casing front and remount unit.

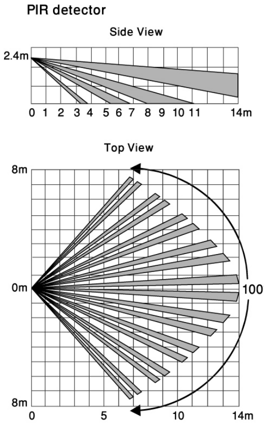


Figure B- 5: Lens Coverage – EL-4755

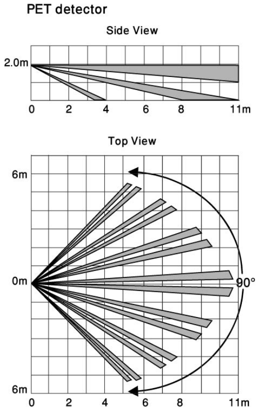


Figure B- 6: Lens Coverage – EL-4755PI

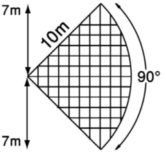


Figure B- 7: Camera Lens Coverage (Top View) – EL-4755/EL-4755PI

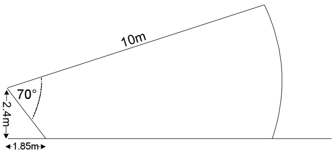


Figure B- 8: Camera Lens Coverage (Side View) – EL-4755

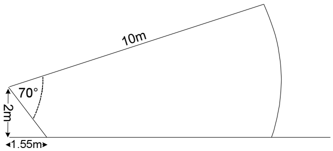


Figure B- 9: Camera Lens Coverage (Side View) – EL-4755PI

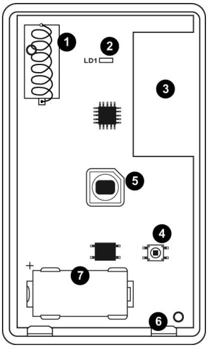
EL-4755/4755PI complies with EN-50131 2-2 Grade 2 Class II Power Supply Type C.

PIR Detectors (EL-4745/EL-4745PI)

The EL-4745 and EL-4745PI are intelligent 2-Way wireless PIR detectors designed for use with the iConnect ② Control System. All of these detectors implement a feature to combat the problem of multiple transmissions, which drastically reduce the life of the batteries. After each transmission, there is a four-minute delay during which further transmissions will not be sent. When batteries need replacing, the detector sends a low battery indication to the Control System.

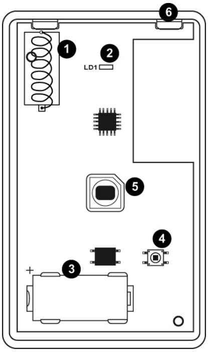
Detectors that meet the EN-50131 standard, have a three-minute delay between transmissions.

The EL-4745PI is designed for installations prone to nuisance alarms caused by pets or small animals.



1. Antenna
2. LED
3. Battery compartment
4. Tamper switch
5. Pyro sensor
6. PCB Release tab
7. Optional Battery compartment

Figure B- 10: PIR Detector with Cover Removed – EL-4745



1. Antenna
2. LED
3. Battery compartment
4. Tamper switch
5. Pyro sensor
6. PCB Release tab

Figure B- 11: PIR Detector with Cover Removed – EL-4745PI

Considerations before Installation

- Select a location from which the pattern of the detector is most likely to be crossed by a burglar, should there be a break in.
- Do not place bulky objects in front of the detector.
- Avoid a location which comes in direct contact with radiators, heating/cooling ducts, mirrors and air conditioners.
- Do not place the detector in front of windows subject to direct sunlight or drafts.

Pet Immunity Guidelines (EL-4745PI)

It is expected that the EL-4745PI detector will eliminate false alarms caused by:

- Animals up to 36kg/80lb (EL-4745PI)
- Several small rodents
- Random flying birds

☞ The weight of the animal should only be used as a guide, other factors such as the length and color of fur also affect the level of immunity.

For maximum pet immunity the following guidelines are recommended:

- Mount the center of the unit at a height of 2.0m (6.5')
- Do not aim the detector at stairways that can be climbed by an animal.
- Avoid a location where an animal can come within 1.8m (6') of the detector by climbing on furniture, boxes or other objects.

Registration Procedure

The EL-4745PI must identify itself to the iConnect 2 Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'
2. Detach the mounting bracket from the detector.
3. Open the battery compartment door.
4. Remove the isolator that separates the battery from the contacts on the battery holder. The detector will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard, send another transmission by pressing and releasing the tamper switch of the device.
5. After the detector is successfully registered the display shows: Save? Press '√' to confirm and continue entering other parameters for the chosen device.

☞ An additional battery can be placed inside the detector (EL-4745). To insert the additional battery open the front cover and place the battery. Pay attention to the polarity.

Installation Procedure

To install PIR detectors:

☞ Before permanently mounting the detector, test the transmitter from the exact mounting position. If necessary, improve the position of the transmitter. The recommended height is 2.2m (6.6 ft).

1. Knock out the mounting holes of the mounting bracket and attach it to the wall.
2. To use the rear tamper switch, insert a screw into the rear tamper mounting hole located in the center of the bracket. When the bracket is removed from the wall, the screw causes the tamper release to break away from the bracket and the rear tamper switch is released
3. Align the pins on the mounting bracket with the slots on the detector's base, attach the EL-4745PI to the bracket and slide it down while gently pressing it to fit to its place.
4. Attach the screw provided in the detector kit to the bottom of the mounting bracket.

Operation Modes

Warm-Up Time

The detector will need to warm up for the first 90 seconds after applying power.

Walk Test Mode

A walk test is performed in order to determine the lens coverage pattern of the detector. Walk Test mode cancels the delay time between detections, enabling you to perform an efficient walk test.

To perform a Walk Test:

1. Set the iConnect ② Control System to Walk test mode (Quick key [7034]).
2. Walk across the scope of the detector according to the detection pattern selected.
3. Confirm that the LED activates and deactivates accordingly. Wait for ten seconds, after each detection, before continuing the test.
4. After completing the walk test set the system to normal operation mode.

LED Indication

The LED indicator is lit every time a transmission is made. The Led can be enabled / disabled by programming.

☞ LED should only be disabled after successfully walk testing the detector.

Parameters Setting Procedure

As a 2-Way detector, the EL-4745PI parameters can be modified only from the iConnect ② Control System.

In comparison to other detectors the EL 4745PI has dedicated parameters that can be modified under quick key 9>1>1>11

- LED Enable: On/Off (Default: On)
- Pulse count: The pulse counter determines the amount of beams that need to be crossed before the detector will produce an alarm.
- Alarm Delay: The delay between reporting detections to the main unit.

Battery Replacement

In case of a low battery (2.5 VDC or less), the detector low battery condition is reported to the system and low battery message is displayed.

To replace the battery:

Open the battery compartment door located on the back cover, replace the battery, and close the compartment door. Attach the EL-4745PI to the bracket and slide it down while gently pressing it to fit to its place.

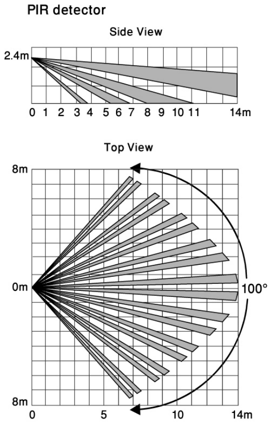


Figure B- 12: Lens Coverage Diagrams EL-4745

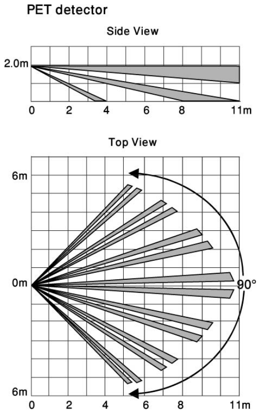
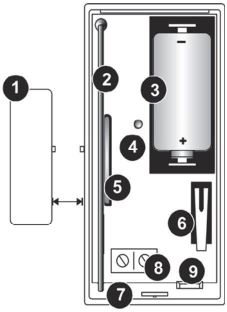


Figure B- 13: Lens Coverage Diagrams EL-4745PI

EL-4745 complies with EN-50131 2-2 Grade 2 Class II Power Supply Type C

Dual Magnetic Contact/Universal Transmitter (EL-4601DZ)

The EL-4601DZ is a 2-Way wireless device that can be defined either as a magnetic contact, a universal transmitter or both in combination. The EL4601DZ is for use with the iConnect Control System. When batteries need replacing, the EL-4601DZ sends a low battery indication to the Control System.



1. Magnet
2. Antenna
3. Battery Holder
4. LED Indicator
5. Reed switch
6. Tamper Switch
7. Location of Wiring Knockout
8. PCB Release Tab
9. Terminal Block

Figure B- 14: EL-4601DZ (Cover Off)

Registration Procedure

The EL-4601DZ must identify itself to the iConnect Control System as follows:

1. Set the system to registration mode.
    - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
    - Select a zone and press '√'.
2. Open the detector housing by inserting a small screwdriver at the bottom of the unit between the front and back cover and twist the screwdriver to release the cover.
3. Remove the divider separating the battery from the contacts on the battery holder. The detector will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the device.

☞ Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized.

4. As soon as 'Save?' appears press '√'.

Parameter Settings

As a 2-Way detector, the EL-4601DZ parameters can be modified only from the iConnect ② Control System.

The parameter settings can be defined as follows:

1. Go to the main menu and select [9]>[1]>[1]>[11] (Programming > Devices > Zones>Sensor Par.)
2. Select the Sensor Type (Magnetic, Universal or Magnetic + Universal)
3. Define Second Zone (1-32) for dual Magnetic + Universal configuration.

☞ By default the EL-4601DZ is registered as a Magnetic Contact. The Universal Transmitter can function in the same zone or can be assigned to a separate zone. If assigned to a separate zone any receiver already assigned to the selected zone will be deleted. For dual configuration each zone should be configured exclusively.

4. Press'√' to confirm.

Installation Procedure

Once the detector has been registered mount the detector as follows:

☞ Before permanently mounting the unit, test the transmitter from the exact mounting position. If necessary, improve the position of the transmitter. The alarm is generated by magnet removal at 24 (+/- 0.5) mm and is cleared by magnet approach at 22 (+/- 0.5) mm

1. Open the detector housing.
2. Remove the PCB by pressing the PCB release tab.

☞ When handling the PCB, do not apply pressure on the antenna.

3. Mount the back cover using two screws and replace the PCB. Use ISO 7050 (ST3.5 x 22) or similar countersunk screws so that the screw head will not touch the PCB.

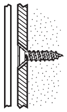


Figure B- 15: Mounting Screw Position

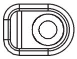


Figure B- 16: Rear Tamper Release

☞ The upper screw is also used for back tamper. When the detector is removed from the wall, the screw causes the tamper release to break away from the back cover and the rear tamper switch is released.

4. Knockout the wiring hole in the back cover.
5. Thread the wires through the wiring hole.
6. Connect the terminal block.
7. Test the transmitter, making certain that the LED is lit during transmission.
8. Open the magnet housing.
9. Mount the back cover of the magnet using two screws.

☞ Make sure that the guideline on the magnet is correctly aligned with the guideline on the transmitter. Do not install the magnet further than 1cm from the transmitter.

10. Test the transmitter, making certain that the LED is lit when opening the door/window and again when closing.
11. Close the front covers of the transmitter and the magnet.

Deleting the Dual Magnetic Contact/Universal Transmitter

To delete the EL-4601DZ from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones).
   - Select a zone and press '√'
2. Press >12 > '√'.

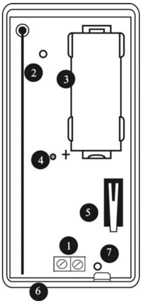
☞ For dual configuration (Magnetic + Universal) both magnetic and universal zones will be deleted.

3. Open the detector and take out the battery.
4. Press the tamper switch. While the tamper switch is being pressed insert the battery.
5. Within five seconds open the tamper and close it again.

EL-4601DZ complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

Universal Transmitter (EL-4602)

The EL-4602 is a 2-Way universal transmitter that includes a single output for use in a wide range of wireless applications. When batteries need replacing, the EL-4602 sends a low battery indication to the Control System.



1. Terminal Block
2. Antenna
3. Battery Holder
4. LED Indicator
5. Tamper Switch
6. Location of Wiring Knockout
7. PCB Release Tab

Figure B- 17: EL-4602 (Cover Off)

Registration Procedure

The EL-4602 must identify itself to the iConnect ② Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'.
2. Open the transmitter housing by inserting a small screwdriver at the bottom of the unit between the front and back cover and twist the screwdriver to release the cover.
3. Remove the divider separating the battery from the contacts on the battery holder. The transmitter will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the device.

☞ Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized

4. As soon as 'Save?' appears press '√'.

Installation Procedure

After the transmitter has been registered mount the transmitter as follows:

☞ Before permanently mounting the unit, test the transmitter from the exact mounting position. If necessary, improve the position of the transmitter.

1. Open the transmitter housing.
2. Remove the PCB by pressing the PCB release tab.

☞ When handling the PCB, do not apply pressure on the antenna

3. Mount the back cover using two screws and replace the PCB. Use ISO 7050 (ST3.5 x 22) or similar countersunk screws so that the screw head will not touch the PCB.

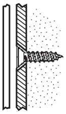


Figure B- 18: Mounting Screw Position

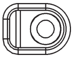


Figure B- 19: Rear Tamper Release

☞ The upper screw is also used for back tamper. When the transmitter is removed from the wall, the screw causes the tamper release to break away from the back cover and the rear tamper switch is released.

4. Knockout the wiring hole in the back cover.
5. Thread the wires through the wiring hole.
6. Connect the terminal block.
7. Test the transmitter, making certain that the LED is lit during transmission.
8. Close the front cover of the transmitter.

EL-4602 complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C.

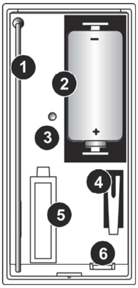
Deleting a Universal Detector

To delete a Universal detector from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones).
   - Select a zone and press '√'
2. Press >12 >√.
3. Open the detector and take out the battery.
4. Press the tamper switch. While the tamper switch is being pressed insert the battery.
5. Within five seconds open the tamper and close it again.

Vibration Detector (EL-4607)

The EL-4607 is a 2-Way wireless vibration detector for use with the iConnect ② Control System.



1. Antenna
2. Battery Holder
3. LED Indicator
4. Tamper Switch
5. Piezo Electric Sensor
6. PCB Release Tab

Figure B- 20: EL-4607 (Cover Off)

Registration Procedure

The EL-4607 must identify itself to the iConnect ② Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'.
2. Open the detector housing.
3. Remove the divider separating the battery from the contacts on the battery holder. The detector will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the device.

☞ Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized.

4. As soon as 'Save?' appears press '√'.

Parameter Settings

As a 2-Way detector, the EL-4607 parameters can be modified only from the iConnect ② Control System.

The parameter settings can be defined as follows:

1. Go to the main menu and select [9]>[1]>[1]>[11] (Programming > Devices > Zones>Sensor Par.)
2. Select Sensitivity and define the parameter accordingly (1 – 100); 1 being the lowest, 100 the highest.
3. Press'√' to confirm.

Installation Procedure

After the detector has been registered, mount the unit as follows:

☞ Before permanently mounting the unit, test the detector from the exact mounting position. If necessary, relocate the detector to a better position.

1. Open the detector housing.
2. Remove the PCB by pressing the PCB release tab.

☞ When handling the PCB, do not apply pressure on the antenna.

3. Mount the back cover using two screws and replace the PCB. Use ISO 7050 (ST3.5 x 22) or similar countersunk screws so that the screw head will not touch the PCB.

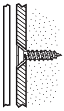


Figure B- 21: Mounting Screw Position

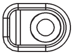


Figure B- 22: Rear Tamper Release

☞ The upper screw is also used for back tamper. When the detector is removed from the wall, the screw causes the tamper release to break away from the back cover and the rear tamper switch is released.

4. Test the detector, making certain that the LED is lit during transmission.
5. Close the front cover of the detector.

Testing the Vibration Detector

Once you have mounted the detector, test the detector's sensitivity, as follows:

1. With the tamper switch open, strike the protected door or window at the furthest point away from the detector with a screwdriver handle or cushioned tool; the LED color indicates the sensitivity level of the detector. Refer to following table:

Table B- 2: LED Sensitivity Level (EL-4607)

LED	Sensitivity Level
Red	Under-sensitive indication
Green	Normal sensitivity (recommended)
Orange	Over-sensitive indication

2. If required, adjust the Sensitivity parameter.
3. Repeat the sensitivity test until you achieve the required sensitivity level.
4. After you have adjusted the Sensitivity parameter, repeat the test once more.
5. Close the front cover of the detector.

Deleting a Vibration Detector

To delete a vibration detector from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones).
   - Select a zone and press '√'
2. Press >12 >√.
3. Open the detector and take out the battery.
4. Press the tamper switch. While the tamper switch is being pressed insert the battery.
5. Within five seconds open the tamper and close it again.

Smoke Detector (EL-4703)

The EL-4703 is a single station, photoelectric smoke detector with a built-in supervised wireless transmitter.

When sufficient smoke is detected, or the test feature is operated, the detector will sound its alarm horn and the transmitter will send an ALARM message. The Alarm output in the receiver will remain activated until the alarm condition clears.

The smoke alarm base lock discourages unauthorized removal of the smoke alarm by requiring a screwdriver to remove the alarm from the base.

The smoke alarm provides the following signals to the control panel:

- Alarm
- Alarm restore
- Low battery
- Tamper
- Supervision

⚠ WARNINGS:

This smoke detector is designed for use in a single residential unit only, which means that it should be used inside a single family home or apartment. It is not meant to be used in lobbies, hallways, basements, or another apartment in multi-family buildings, unless there are already working detectors in each family unit. Smoke detectors, placed in common areas outside of the individual living unit, such as on porches or in hallways, may not provide early warning to residents. In multi-family buildings, each family living unit should set up its own detectors.

This detector is not to be used in non-residential buildings. Warehouses, industrial or commercial buildings, and special purpose non-residential buildings require special fire detection and alarm systems. This detector alone is not a suitable substitute for complete fire detection systems for places where many people live or work, such as hotels or motels. The same is true of dormitories, hospitals; nursing homes or group homes of any kind, even if they were once single - family homes. Please refer NFPA 101, the Life Safety Code, NFPA71, 72A, 72B, 72C, 72D, and 72E for smoke detector requirements for fire protection in buildings not defined as "households".

Selecting a Location

Smoke detectors should be installed in accordance with the NFPA Standard 74 (National Fire Protection Association, Batterymarch Park, Quincy, MA 02169). For complete coverage in residential units, smoke detectors should be installed in all rooms, halls, storage areas, basements, and attics in each family living unit. Minimum coverage is one detector on each floor and one in each sleeping area and attics in each family living unit. Minimum coverage is one detector on each floor and one in each sleeping area.

- Install a smoke detector in the hallway outside every separate bedroom area. Two detectors are required in homes with two bedroom areas.
- Install a smoke detector on every floor of a multi-floor home or apartment.
- Install a minimum of two detectors in any household.
- Install a smoke detector inside every bedroom.
- Install smoke detectors at both ends of a bedroom hallway if the hallway is more than 40 feet (12 meters) long.
- Install a smoke detector inside every room where one sleeps with the door partly or completely closed, since smoke could be blocked by the closed door and a hallway alarm may not wake up the sleeper if the door is closed.
- Install basement detectors at the bottom of the basement stairwell.
- Install second-floor detectors at the top of the first-to-second floor stairwell.
- Be sure no door or other obstruction blocks the path of smoke to the detector.
- Install additional detectors in your living room, dining room, family room, attic, utility and storage rooms.
- Install smoke detectors as close to the center of the ceiling as possible. If this is not practical, put the detector on the ceiling, no closer than 4 inches (10 cm) from any wall or corner.
- If ceiling mounting is not possible and wall mounting is permitted by your local and state codes, put wall-mounted detectors between 4 and 6 inches (10 ~ 15 cm) from the ceiling.
- If some of your rooms have sloped, peaked, or gabled ceilings, try to mount detectors 3 feet (0.9 meter) measured horizontally from the highest point of the ceiling.

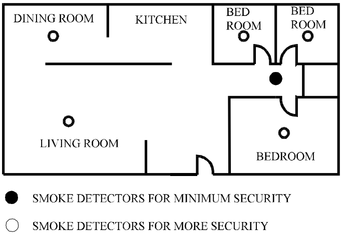

DINING ROOM
KITCHEN
BED ROOM
BED ROOM
LIVING ROOM
BEDROOM
● SMOKE DETECTORS FOR MINIMUM SECURITY
○ SMOKE DETECTORS FOR MORE SECURITY

Figure B- 23: Locations for placing smoke detectors for single residence with only one sleeping area

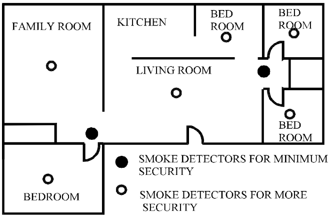

FAMILY ROOM
KITCHEN
BED ROOM
BED ROOM
LIVING ROOM
BED ROOM
BEDROOM
● SMOKE DETECTORS FOR MINIMUM SECURITY
○ SMOKE DETECTORS FOR MORE SECURITY

Figure B- 24: Locations for placing smoke detectors for single-floor residence with more than one sleeping area

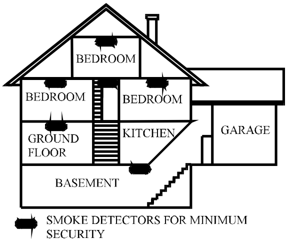


Figure B- 25: Location for placing smoke detectors for a multi-floor residence

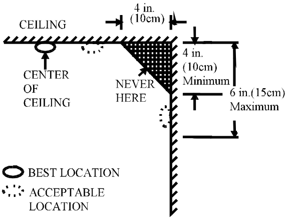


Figure B- 26: Recommended best and acceptable locations to mount smoke detectors

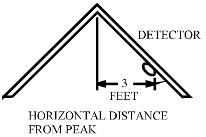


Figure B- 27: Recommended location to mount smoke detectors in rooms with sloped, gabled, or peaked ceiling

⚠ CAUTION:

(As required by the California State Fire Marshall)

"Early warning fire detection is best achieved by the installation of fire detection equipment in all rooms and areas of the household as follows: (1) A smoke detector installed in each separate sleeping area (in the vicinity, but outside of the bedrooms), and (2) Heat or smoke detectors in the living rooms, dining rooms, bedrooms, kitchens, hallways, attics, furnace rooms, closets, utility and, storage rooms, basements and attached garages."

For your information, NFPA Standard 74, Section 2-4 reads as follows:

"2-4.1.1 Smoke detectors shall be installed outside of each separate sleeping area in the immediate vicinity of the bedrooms and on each additional story of the family living unit including basements and excluding crawl spaces and unfinished attics.

The provisions of 2-4.1.1 represent the minimum number of detectors required by this standard. It is recommended that the householder consider the use of additional smoke detectors for increased protection for those areas separated by a door from the areas protected by the required smoke detectors under 2-4.1.1 above. The recommended additional areas are living room, dining room, bedroom(s), kitchen, attic (finished or unfinished), furnace rooms, utility room, basement, integral or attached garage, and hallways not included in 2-4.1.1 above. However, the use of additional detectors remains the option of the householder." We recommend complete coverage and use of additional smoke detectors.

Where to Install Your Smoke Detectors in Mobile Homes and RVs

Mobile homes and RVs built after about 1978 were designed and insulated to be energy-efficient. In mobile homes and RVs built after 1978, smoke detectors should be installed as described above. Older mobile homes and RVs may have little or no insulation compared to current standards. Outside walls and roofs are often made of non-insulated metal, which can transfer thermal energy flow from outdoors. This makes the air right next to them hotter or colder than the rest of the inside air. These layers of hotter or colder air can keep smoke from reaching a smoke detector. Thereby, install smoke detectors in such units only on inside walls. Place them between 4 and 6 inches (10 ~ 15 cm) from the ceiling. If you are not sure how much insulation is in your mobile home or RV, then install the detector on an inside wall. If the walls or ceiling are unusually hot or cold, then install the detector on an inside wall. Install one detector as close to the sleeping area as possible for minimum security, or install one detector in each room for security. Before you install any detector, please read the following section on "Where not to install your smoke detectors".

Where Not to Install Your Smoke Detectors

False alarms occur when smoke detectors are installed where they will not work properly. To avoid false alarms, do not install smoke detectors in the following situations:

- Combustion particles are by-products of something burning. Do not install smoke detectors in or near areas where combustion particles are present, such as kitchens with few windows or poor ventilation, garages where there may be vehicle exhaust, near furnaces, hot water heaters and space heaters.
- Do not install smoke detectors less than 6 meters (20 feet) away from places where combustion particles are normally present, like kitchens. If a 20-foot distance is not possible, e.g. in a mobile home, try to install the detector as far away from the combustion particles as possible, preferably on the wall. To prevent false alarms, provide good ventilation in such places.

⚠ Never try to avoid false alarms by disabling the detector.

- Do not mount smoke detectors in the path of fresh air intake. The flow of fresh air in and out can drive smoke away from the smoke detector; thus reducing its efficiency.
- Near paint thinner fumes.
- In close proximity to an automobile exhaust pipe; this will damage the detector.
- In damp or very humid areas or near bathrooms with showers. Moisture in humid air can enter the sensing chamber, then turns into droplets upon cooling, which can cause false alarms. Install smoke detectors at least 3 meters (10 feet) away from bathrooms.
- In very cold or very hot areas, including unheated buildings or outdoor rooms. If the temperature goes above or below the operating range of smoke detector, it will not work properly. The temperature range for your smoke detector is 4°C to 38°C (40°F to 100°F).

- In very dusty or dirty areas, dirt and dust can build up on the detector's sensing chamber, to make it overly sensitive.
- Additionally, dust or dirt can block openings to the sensing chamber and keep the detector from sensing smoke.
- Near fresh air vents or very drafty areas like air conditioners, heaters or fans. Fresh air vents and drafts can drive smoke away from smoke detectors.
- Dead air spaces are often at the top of a peaked roof, or in the corners between ceilings and walls. Dead air may prevent smoke from reaching a detector.
- In insect-infested areas. If insects enter a detector's sensing chamber, they may cause a false alarm. Where bugs are a problem, get rid of them before putting up a detector.
- Near fluorescent lights, electrical "noise" from fluorescent lights may cause false alarms. Install smoke detectors at least 1.5 meters (5 feet) from such lights.

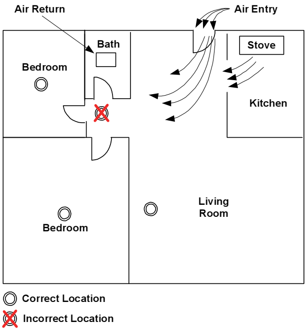


Figure B- 28: Recommended Smoke Detector Locations

The smoke detector is to be mounted on the ceiling or on the wall, if necessary. Since the smoke detector is a single-station type, it cannot be linked to other detectors.

Do not connect the smoke detectors to any other alarm or auxiliary device. Connecting anything else to this detector will prevent it from working properly.

Read the "Where to Install Your Smoke Detector" and "Where Not to Install Your Smoke Detectors" sections in this Manual before installing. To install the detector, perform the following steps.

Registration Procedure

The EL-4703 must identify itself to the EL wireless system receivers as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'.
2. Open the detector housing.
3. Insert the batteries into compartment. The detector will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the device.

   Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized.
4. As soon as 'Save?' appears, press '√'

Installation Procedure

1. Select the installation location.
2. Remove locking pin securing the mounting bracket to the unit.
3. Remove the mounting bracket from the unit by rotating it counterclockwise.

4. Use the bracket as a template for marking the mounting holes
5. Using an appropriate drill, drill two holes at the marks and insert anchors.
6. Using screws (supplied) attach the bracket to the wall.
7. Line up the side slot of the bracket and the detector. Push the detector onto the mounting bracket and turn it clockwise to fix it into place.
8. Insert the locking pin in order to secure the mounting bracket to the detector.
9. Pull the detector outward to make sure it is securely attached to the mounting bracket.

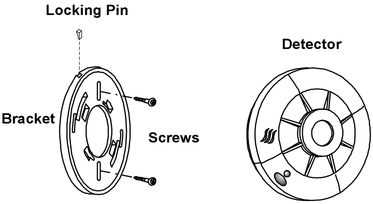


Figure B- 29: Smoke Detector Installation

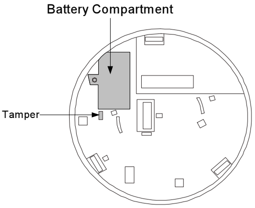


Figure B- 30: Batteries Compartment/Tamper

⚠ This detector is not suitable for installation in a hazardous location, as defined in the national electrical code. Do not use detector in an outlet controlled by a wall switch.

Deleting a Smoke Detector

To delete a smoke detector from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones).
   - Select a zone and press '√'
2. Press >12 > '√'.
3. Open the detector and take out the battery.
4. Press the tamper switch. While the tamper switch is being pressed insert the battery. Within five seconds open the tamper and close it again

Testing Your Smoke Detector

To be sure that detector is working correctly test the detector weekly by performing the following procedure:

Use your finger to firmly press the test button. If the detector is functioning correctly, the alarm horn sounds. To stop the alarm horn, press the test button again. If the detector fails to test properly, have it repaired or replaced immediately.

If the alarm horn begins to beep once every 35 seconds, it means that the detector’s batteries are weak. Replace the batteries immediately. Keep fresh batteries on hand for this purpose.

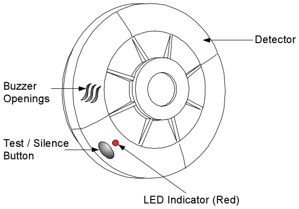


Figure B- 31: Testing the Smoke Detector

☞ Cooking smoke or a dusty furnace (sometimes called “friendly fires”) can cause the alarm to sound. If this happens, open a window or fan the air to remove the smoke or dust. The alarm will turn off as soon as the air is completely clear. Do not disconnect the batteries from the detector. This will cancel your protection from fire.

Red Indicator

When the red LED indicator flashes once in 30 seconds, it indicates the detector is under normal operation. When the red LED flashes very frequently and an audible alarm sounds simultaneously, it indicates that the detector senses smoke.

☞ The red LED behaves according to one of the following set modes:

Mode 1: The red LED indicator will not reset automatically at the end of an alarm event. This means that after the smoke chamber is cleared, the audible alarm will stop automatically, but the red LED indicator will continue to flash, until it is manually restored by the user. To restore – press the test button for 2-3 seconds, the LED will stop flashing.

Mode 2 (Default): The red LED will reset automatically at the end of an alarm event.

The user can check to which mode the detector is defined and switch between modes.

- To check the mode, press the Test button. The red LED will light up. If the red LED lights up continuously the detector is in Mode 1. If the red LED is blinking the detector is in Mode 2.
- To switch from one mode to another, press the Test button for 8 seconds. The buzzer will sound and the red LED will change its behavior either from a continuous light to a blinking light or from a blinking light to a continuous light.

Taking Care of Your Smoke Detector

To keep your detector in good working condition, you must test the detector weekly, according to the “Testing Your Smoke Detector” section.

Cleaning the Smoke Detector

1. Clean the housing with a dry or damp cloth to remove dust and dirt. If necessary, open the smoke chamber and clean the interior of the detector.
2. Remove the detector from the detector base.
3. Remove the batteries.
4. Using a flat screwdriver release the smoke detector cover.
5. Using a flat screwdriver lift the smoke chamber housing slightly.
6. Use a fine paintbrush to remove dirt from the chamber.
7. After cleaning, close the smoke chamber, fix the housing and remount the detector on the ceiling.

☞ Do not forget to change the batteries!

Battery Replacement

Replace the detector batteries once a year or immediately when the low battery “beep” signal sounds once every 35 seconds. The low-battery "beep" should last at least 30 days before the batteries die out completely.

☞ If false alarms keep coming from the detector, you should check whether the detector’s location is adequate. Refer to section “WHERE TO INSTALL SMOKE DETECTORS.” Have your detector moved if it is not located properly. Clean the detector as described above.

⚠ WARNINGS! LIMITATIONS OF SMOKE ALARMS

Wireless smoke alarms are very reliable, but may not work under all conditions. No fire alarm provides total protection of life or property. Smoke alarms are not a substitute for life insurance.

Smoke alarms require a source of power to work.

This smoke alarm will not operate and the alarm will not sound if batteries are dead or not installed properly.

Smoke alarms may not be heard. A sound sleeper or someone who has taken drugs or alcohol may not awaken if the alarm is installed outside a bedroom. Closed or partially closed doors and distance can block sound. This alarm is not designed for the hearing impaired.

Smoke alarms may not always activate and provide warning early enough. Smoke alarms only activate when enough smoke reaches the alarm. If a fire starts in a chimney, wall, roof, on the other side of closed doors, or on a different level of the property enough smoke may not reach the alarm for it to alarm.

Smoke alarms are a significant help in reducing loss, injury and even death. However, no matter how good a detection device is, nothing works perfectly under every circumstance and we must warn you that you cannot expect a smoke alarm to ensure that you will never suffer any damage or injury.

☞ Smoke detectors are not to be used with detector guards unless the combination has been evaluated and found suitable for that purpose

Keyfobs (EL-4714)

The EL-4714 is a keyfob transmitter designed for use with the iConnect Control System. The EL-4714 is a four-button keyfob transmitter that offers a number of functions including arm, disarm and SOS Panic.

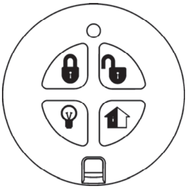


Figure B- 32: EL-4714

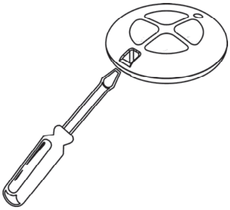


Figure B- 33: Opening the EL-4714's Casing

Keys Operation and LED Indication

Table B-3: Keys Operation (EL-4714)

Key	Operation
🔒 :	Full Arm
🔓 :	Disarm
🏠 :	Part Arm, HA/PGM
💡 / 🏠 :	Perimeter Arm, HA/PGM
💡 + 🏠 :	Panic alarm (Press and hold down)

Table B-4: LED Indication (EL-4714)

LED	Indication
Green:	Operation successful
Flashing green for 4 seconds:	Operation fail
Flashing Red for 4 seconds :	Low battery
Flashing amber for 4 seconds:	Out of range
Green:	Operation successful

Registration Procedure

The keyfob must identify itself to the iConnect ② Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[2] (Programming > Devices > Keyfobs)
   - Select a Keyfob (1-19) and press '√'.
2. Press one of the buttons on the Keyfob, making sure that the Keyfob's green LED lights up when the button is pressed.

☞ A flashing red LED indicates a communication problem between the Keyfob and the system.

3. As soon as 'Save?' appears press '√'.

☞ During registration, maintain a minimum 1 meter distance between the keyfob and panel.

Deleting a Keyfob

To delete a Keyfob from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[2] (Programming > Devices > Keyfobs).
   - Select a Keyfob (1-19) and press '√'
2. Press >6 > '√'.
3. Press 💡 + 🔓 for two seconds until the red led stops flashing
4. Press 🔒 + 🏠 for two seconds until the red led stops flashing.

Battery Replacement

If the LED blinks during transmissions, this indicates that the battery is low and need replacing.

☞ Batteries must be replaced within seven days of receiving a low battery indication. The estimated battery life is 2 years (avg. 4 activations per day).

To replace the battery:

1. Insert a small screwdriver into the pry-off slot. Carefully twist the screwdriver to separate the front and back of the casing.
2. Observing correct polarity, replace the battery.
3. Close the casing making sure that the front and back click shut.

⚠ Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

EL-4714 complies with EN-50131 Grade 2 Class II Power Supply Type C.

Keyfobs (EL-4711M/P)

The EL-4711M/P is a keyfob transmitters designed for use with the iConnect ② Control System. The EL-4711M/P is a one-button transmitter that generates a Medical/Panic alarm when pressed. The transmitter is water resistant and can be worn around the neck. Its large button makes it ideal for elderly or sight-impaired users.

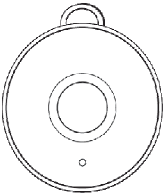


Figure B- 34: EL-4711M/P

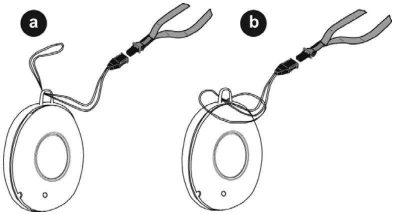


Figure B- 35: Inserting the Cord (EL-4711M/P)

LED Indication

Table B-5: LED Indication (EL-4714)

LED	Indication
Red (fast flash for 4 seconds)	Outgoing transmission.
Green	Operation successful
Amber	Low battery

Registration Procedure

The keyfob must identify itself to the iConnect 2 Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[2] (Programming > Devices > Keyfobs)
   - Select a Keyfob and press '√'.
2. Press one of the buttons on the Keyfob, making sure that the Keyfob's green LED lights up when the button is pressed.

> A flashing red LED indicates a communication problem between the Keyfob and the system.

3. As soon as 'Save?' appears press '√'.

> During registration, maintain a minimum 1 meter distance between the keyfob and panel.

Deleting a Keyfob

To delete a Keyfob from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[2] (Programming > Devices > Keyfobs).
   - Select a Keyfob (1-19) and press '√'
2. Press >6 > '√'.
3. Press and hold the Keyfob button for at least eight seconds. The initial red LED flashing indicates the Keyfob is attempting to contact the system. After the flashing stops, a red/green flashing LED begins and when it stops, the keyfob unregistration has succeeded.

Battery Replacement

If the LED blinks during transmissions, this indicates that the battery is low and need replacing.

> Batteries must be replaced within seven days of receiving a low battery indication. The estimated battery life is 2 years (avg. 4 activations per day).

To replace the battery:

1. Insert a small screwdriver into the pry-off slot. Carefully twist the screwdriver to separate the front and back of the casing (1-2).
2. Observing correct polarity, replace the battery (3-4).
3. Close the casing making sure that the front and back click shut (5).

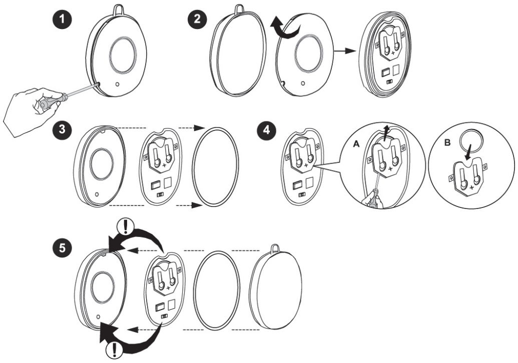


Figure B- 36: Replacing the EL-4714's batteries

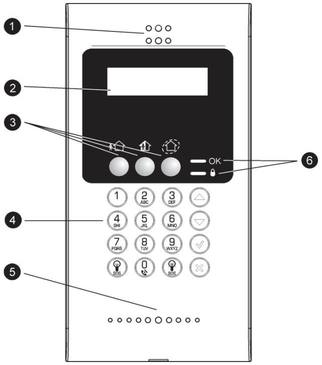
⚠ Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

EL-4714M/P complies with EN-50131 Grade 2 Class II Power Supply Type C.

Wireless LCD Keypad (EL-4727)

The EL-4727 is a 2-Way wireless keypad with LCD display used to remotely program and operate the ② Control System. The keypad's functionality is identical to the keys on the iConnect ② Control System front panel.

☞ Programming mode can be established either from a keypad or from the main panel, but not simultaneously.



1. Speaker
2. LCD Display
3. Arming Keys
4. Keypad
5. Microphone (optional)
6. System Status LEDs

Figure B- 37: Keypad front layout

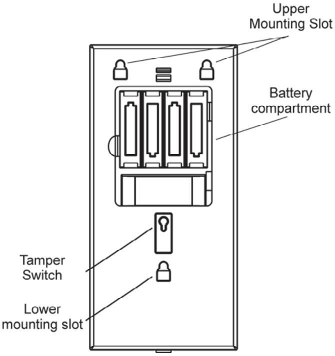


Figure B- 38: Keypad back layout

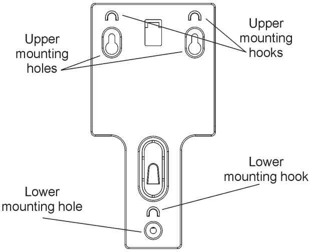


Figure B- 39: Keypad mounting bracket

LED Indication

Table B-6: LED Indication (EL-4727)

🔒 LED:		OK LED:	
Off:	System disarmed	Green:	Power OK
Green:	System armed	Yellow:	System trouble
Flashing red:	Alarm	Flashing green:	Open zone
		Flashing yellow:	(Slow) Low battery, (Fast) AC loss

Registration Procedure

The EL-4727 keypad must identify itself to the system receiver. This is done by registering the keypad to the iConnect Control System as follows:

1. Release the mounting bracket.
2. Open the battery compartment and insert the batteries. Pay attention to the correct polarity.
3. Set the system to registration mode
    - Go to the main menu and select [9]>[1]>[3] (Programming > Devices > Keypads)
    - Select a keypad (1-4)
4. Press the keypad's tamper switch.
5. As soon as 'Save?' appears on the Control System's LCD screen, press '√'

Installation Procedure

After the keypad has been registered to the system mount the keypad on the wall using the supplied mounting bracket.

☞ 1. Before mounting the keypad test the keypad communication with the system. To do so, try to arm the system using one of the arming buttons on the wireless keypad.

2. Minimum mounting distance between the wireless keypad and the panel is 1.5m.

To mount the keypad:

1. Release the mounting bracket
2. Attach the mounting bracket to the wall using the supplied screws.
3. Attach the wireless keypad to the mounting bracket by sliding it down.
4. If required attach the housing screw at the bottom of the front cover.

Deleting a Keypad

To delete a wireless keypad from the system:

1. Set the system to Delete mode.
    - Go to the main menu and select [9]>[1]>[3] (Programming > Devices > Keypads).
    - Select keypad (1-4) > '√'
2. Press >'√'.
3. Take out the keypad batteries.
4. While the back tamper switch is being pressed insert the batteries.
5. Within five seconds open the tamper and close it once again

Replacing Batteries

When the battery needs to be replaced the yellow OK LED will flash.

To replace the battery:

1. Remove the keypad from the wall.
2. Open the battery compartment.
3. Pull out the battery and replace it with a new one. Pay attention to the polarity when inserting the new batteries
4. Close the battery compartment, and place the keypad back to its place

Gas Leak Detector (EL-4762)

The EL-4762 is a 2-Way Wireless Gas Leak Detector used to detect mixtures of air and combustible gases (Natural Gas, Methane, Propane and Butane). Upon detecting the presence of gas, the unit emits an alarm and notifies the control panel.

Selecting a Location

The 2-Way Wireless Gas Leak Detector will function effectively if installed in the correct location. Consider the following before mounting the gas alarm:

- Methane (Natural) Gas: Methane is lighter than air, therefore the greatest concentration of gas is found right below the ceiling, and therefore the Wireless Gas Leak Detector should be installed on the wall, approximately 30 cm (12”) below the ceiling.
- Butane Gas: Propane and Butane are heavier than air, therefore the greatest concentration of gas is found right above the floor level. The Wireless Gas Leak Detector should therefore be installed about 30cm (12”) above the floor. Do not mount in a location where the gas alarm could be damaged by dirt, liquids, etc.

☞ Do not install the detector on the ceiling or on the floor.

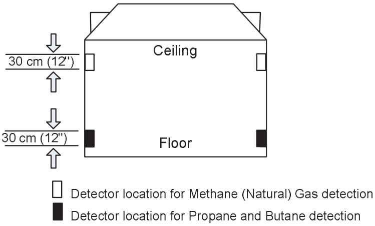

30 cm (12")
Ceiling
30 cm (12")
Floor
□ Detector location for Methane (Natural) Gas detection
■ Detector location for Propane and Butane detection

Figure B- 40: Gas leak detector installation location

- Install the detector in close proximity to every gas-operated appliance.

Do not:

- Install the gas detector directly on any gas appliance.
- Install the gas detector in sealed or closed compartments or in an area where a wall or a closed door can obstructs the flow of gas to the gas alarm.
- Install the gas detector in locations where fans, open doors, open windows etc. may prevent gas from reaching the detector.
- Install the gas detector in any room where aerosols or ammonia are used (e.g. bathrooms).

Installation Procedure

1. Remove the mounting bracket from your unit according to the illustrations below.
2.

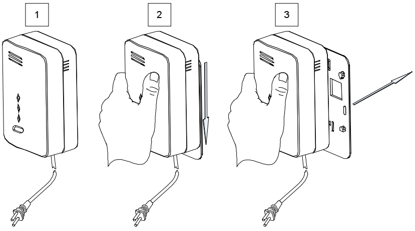


Figure B- 41: Gas leak detector installation procedure (#1)

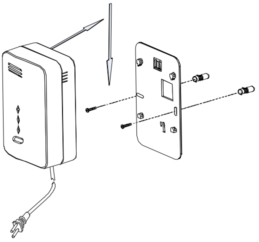


Figure B- 42: Gas leak detector installation procedure (#2)

3. Hold the Mounting bracket against the wall as a template and mark the locations for the 2 mounting holes.
4. Using a 3/16-inch (5 mm) drill bit, drill two holes at the marks and insert wall plugs.
5. Secure the mounting bracket to the wall.
6. Line up the side slot of the bracket and the detector. Push the detector onto the mounting bracket and fix it. Pull the detector outwards to make sure that it is securely attached to the mounting bracket.
7. Connect the detector power cable to the wall power outlet.

Registration Procedure

The EL-4762 must identify itself to the iConnect 2 Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'
2. Ensure that the detector power cable is plugged into the wall power outlet. (Wait 3 minutes for the power-on process to complete)
3. Press the TEST button for 3 seconds to send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard, repeat this step.
4. After the detector is successfully registered the display shows: Save? Press '√' to confirm.
5.

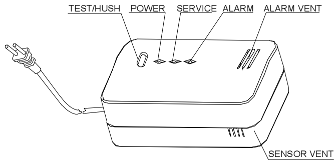


Figure B- 43: Gas leak detector registration procedure

LED & Buzzer Indication

Table B-7: LED & Buzzer Indication (EL-4762)

LED	LED Status	Buzzer	Meaning
Green (Power)	Flashing (for 4 minutes)		Warm up (the status between Power -Up and Normal operation)
	On		Normal Condition (Power On)
RED (Alarm)	Flashing	Sequential Alarm Sound	Alarm
Orange (service)	On		Malfunction/ detector interruption

Testing the Detector

To test the detector (do not test when detector is at warm up mode), press the Test Button.

•The red and orange LED's will flash and a sound will be heard

Muting the Detector

You can partially mute the detector in an event of alarm by pressing the Test Button. The Red LED will continue to flash and a short sound will be heard every 16 seconds.

Detector Malfunctioning

A malfunctioning unit is indicated by beep-sounding on and off sequentially, i.e., beeping for 3 seconds with 3 seconds delay between two beeps. If this occurs, unplug the detector from the power source for 10 seconds and then plug the unit again. Should the unit beep intermittently, DO NOT use this detector. Send the malfunctioning unit for servicing.

Taking Care of the Detector

You have to maintain the detector frequently to ensure it working properly. Few tips are provided for you to take care of your detector:

1. Use a vacuum cleaner to clean the air vents occasionally to keep them free of dust.
2. Push the Test button on your detector to test its operating function once every week.

Actions to take when Alarm Sounding

In case of harmful levels of gas being detected, your detector will go into a continuous full alarm. Try to take the following necessary actions immediately or evacuate the building:

- Widely open doors and windows
- Disconnect electrical appliances
- Avoid open fire
- Repair the gas leak by a professional gas repairer

Actions to take after the Problem Is Corrected

Once the problem about the gas presence in the premises has been corrected, the alarm of the detector should be off. After waiting for 10 minutes, push the Test button to test the detector so that you can make sure that the detector is working properly again.

Carbon Monoxide Detector (EL-4764)

The EL-4764 is a 2-Way Wireless Carbon Monoxide Detector (CO) used to detect the buildup of Carbon Monoxide. Upon detecting the CO gas, the unit emits an alarm and notifies the control panel.

Things you should know about Carbon Monoxide

Carbon monoxide, also known as "CO" by the chemical form, is considered to be a highly dangerous poisonous gas, because it is colorless, odorless, tasteless and very toxic. In general, biochemistry phenomena have shown that the presence of CO gas inhibits the blood's capacity to transport oxygen throughout the body, which can eventually lead to brain damage.

In any closed space (home, office, recreational vehicle or boat) even a small accumulation of CO gas can be quite dangerous.

Although many products of combustion can cause discomfort and adverse health effects, it is CO gas which presents the greatest threat to life.

Carbon monoxide is produced by the incomplete combustion of fuels such as natural gas, propane, heating oil, kerosene, coal, charcoal, gasoline, or wood. The incomplete combustion of fuel can occur in any device which depends on burning for energy or heat such as furnaces, boilers, room heaters, hot water heaters, stoves, grills, and in any gasoline powered vehicle or engine (e.g. generator set, lawnmower). Tobacco smoke also adds CO to the air you breathe.

When properly installed and maintained, your natural gas furnace and hot water heater do not pollute your air space with CO. Natural gas is known as a "clean burning" fuel because under correct operating conditions, the combustion products are water vapor and carbon dioxide (CO2), which is not toxic. The products of combustion are exhausted from furnaces and water heaters to the outside by means of a fuel duct or chimney.

Correct operation of any burning equipment requires two key conditions:

- An adequate supply of air for complete combustion.
- Proper venting of the products of combustion from the furnace through the chimney, vent or duct to the outside.

Typical carbon monoxide gas problems are summarized here:

- Equipment problems, due to defects, poor maintenance, damaged and cracked heat exchangers
- Collapsed or blocked chimneys or flues, dislodged, disconnected or damaged vents
- Downdraft in chimneys or flues. This can be caused by very long or circuitous flue runs, improper location of flue exhaust or wind conditions
- Improper installation or operation of equipment, chimney or vents
- Air tightness of house envelop/inadequate combustion of air
- Inadequate exhaust of space heaters or appliances
- Exhaust ventilation/fireplace competing for air supply

Potential sources of carbon monoxide in your home or office include clogged chimney, wood stove, wood or gas fireplace, automobile and garage, gas water heater, gas appliance, gas or kerosene heater, gas or oil furnace and cigarette smoke.

Selecting a Location

Since CO gas moves freely in the air, the suggested location is in or as near as possible to sleeping areas of the home, 30 cm (12 inch) below the ceiling . For maximum protection, a CO detector should be located outside the primary sleeping areas or on each level of your home.

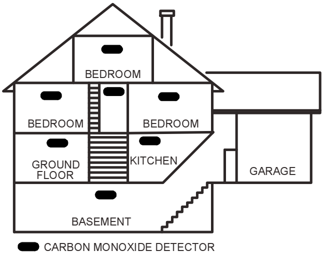


Figure B- 44: Carbon Monoxide detector installation location

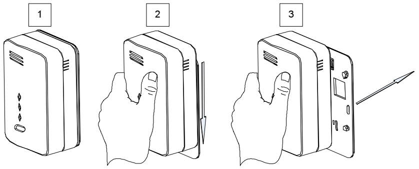
This device is not suitable for installation in a hazardous location, as defined by the US National Electrical Code.

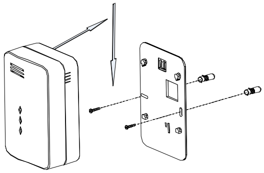
Do not place the detector in the following areas:

- Where the temperature may drop below 4°C (39°F) or exceed 38°C (100°F).
- Near paint thinner fumes
- Within 1.5 meter (5 feet) of open flame appliances such as furnaces, stoves and fireplaces
- In exhaust streams from gas engines, vents, flues or chimneys
- Do not place in proximity to an automobile exhaust pipe; this will damage the detector

Installation Procedure

1. Remove the mounting bracket from your unit according to the illustrations below.





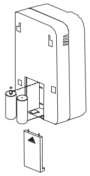


Figure B- 45: CO2 detector installation procedure (#1)

Figure B- 46: CO2 detector installation procedure (#2)

Figure B- 47: CO2 detector installation procedure (#3)

2. Hold the Mounting bracket against the wall as a template and mark the locations for the 2 mounting holes.
3. Using a 5 mm (3/16-inch) drill bit, drill two holes at the marks and insert wall plugs.
4. Secure the mounting bracket to the wall.
5. Open the battery cover by pushing down on the battery snaps.
6. Insert the batteries (supplied) into the battery compartment. Pay attention to the correct battery polarity (+) (-) and close the battery compartment
7. Line up the side slot of the bracket and the detector. Push the detector onto the mounting bracket until a click is heard.
8. Pull the detector outwards to make sure that it is securely attached to the mounting bracket.

Registration Procedure

The EL-4764 must identify itself to the iConnect ② Control System as follows:

1. Set the system to registration mode.
    - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
    - Select a zone and press '√'
2. Ensure batteries are in place (as per Installation instructions above). The detector will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard, send another transmission by pressing and releasing the tamper switch of the device.
3. After the detector is successfully registered the display shows: Save? Press '√' to confirm.

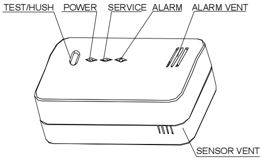


Figure B- 48: CO2 detector registration procedure

LED & Buzzer Indication

Table B-8: LED & Buzzer Indication (EL-4764)

Led Color	LED Status	Buzzer	Meaning
Green (Power)	Flashing On and Off every 30 seconds		Normal condition
RED (Alarm)	Flashing	Sequential Alarm Sound	Alarm
Orange (service)	Flashing On and Off	Sequential Alarm Sound	Internal self test fail - service required
All LED's	Flashing	3 beeps for a period of 3 seconds	Test mode

☞ Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized.

Testing And Resetting Your Detector

A green power light indicates that power is supplied. To test the detector, press the Test button. The detector will beep intermittently and the three LEDs will flash. Release the Test button. The beep and the three LEDs will stop and the green LED remains on or flashes every 60 seconds.

Muting Your Detector

You can partially mute the detector in an event of alarm by pressing the Test Button. The Red LED will continue to flash and a short beep will be heard every 16 seconds.

Detector Malfunctioning

A malfunctioning unit is indicated by beep-sounding on and off sequentially, i.e., beeping for 3 seconds with 3 seconds delay between two beeps. If this occurs, remove the batteries from the unit for 10 seconds and then install them again. Should the unit again beep intermittently, DO NOT use this detector. Send the malfunctioning unit to the manufacturer for servicing.

Taking Care Of Your Detector

You have to maintain the detector to ensure proper operation:

1. Use a vacuum cleaner to clean the air vents occasionally to keep them free of dust.
2. Press the Test button on your detector to test its operation once every week.

Actions to Take When Alarm Sounding

In case of harmful levels of CO gas being detected, your detector will go into a continuous full alarm. Try to take the following necessary actions immediately:

- If there is anyone experiencing the effects of carbon monoxide poisoning such as headache, dizziness, nausea or other flu-like symptoms, call your fire department or emergency service department right away. You should evacuate all the people in the premises immediately. Do a head count to check that everybody is present.
- Do not re-enter the premises until the problem has been corrected and the CO gas has been dispersed out and a safe level is reached.
- If no symptoms exist, immediately ventilate the home by opening windows and doors. Turn off fuel burning appliances and call a qualified technician or your utility company to inspect and repair your problem before restarting appliances.
-

⚠ WARNING

Normally an activation of the detector indicates the presence of CO gas. However, the CO gas can be extremely fatal, if it is not detected. The source of the CO gas may come from several possible situations, please refer to the list of sources of carbon monoxide in the beginning of this section.

⚠ CAUTION

This detector will only indicate the presence of CO gas at the detector. However, you have to be aware that the CO gas may be present in other areas in the premises.

Actions to Take After The Problem is Corrected

Once the problem of the CO gas presence in the premises has been corrected, the detector alarm should be off. After waiting for 10 minutes, push the Test button to test the detector, and by that, being confident that the detector is working properly again.

Technical Information

The Carbon Monoxide Detector is engineered to be able to provide alarm sounds based on the UL standards due to various exposure times at different level of carbon monoxide concentrations.

According to the Underwriters Laboratories Inc. the carbon monoxide concentrations and exposure time standards for the alarms have been established and specified below:

A full alarm is activated under the following conditions:

- Between 60 and 90 minutes at exposures of 70 ppm
- Between 10 and 30 minutes at exposures of 150 ppm
- Between 4 and 10 minutes at exposures of 400 ppm

⚠ WARNING AND LIMITATION

This detector may not alarm at low carbon monoxide levels. The Occupational Safety and Health Association (OSHA) has established that continuous exposure levels of 30 ppm should not be exceeded in an 8 hours period. Individuals with a medical problem may consider more sensitive detection devices.

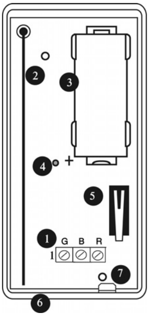
The CO gas detector is not suitable as a smoke or fire detector. This detector is not suitable to install in a hazardous location, as defined in the National Electrical Code.

This detector will not work without power. EL's Carbon Monoxide Detector will not work if the batteries are removed for any reason. Additionally, carbon monoxide must reach the detector for the proper performance of CO gas detection.

Carbon monoxide detectors may wear out because they contain electronic parts that fail at any time (see the section "Testing Your Detector").

Flood Detector (EL-4761)

The EL-4761 is a 2-Way flood detector for use with the iConnect ② Control System. The wireless flood detector is a fully supervised detector used to detect the presence of water-based liquids at any desired location, such as basements or water tanks. The detector is comprised from 2 parts: Wireless transmitter and flood detector which are connected by 2.4m cable. In the event of flooding or leakage, the EL-4761 notifies the control System after detecting the presence of water for a period of at least 20 seconds.



1. Terminal Block
2. Antenna
3. Battery Holder
4. LED Indicator
5. Tamper Switch
6. Location of Wiring Knockout
7. PCB Release Tab

Figure B- 49: EL-4761 (Cover Off)

Registration Procedure

The EL-4761 must identify itself to the iConnect ② Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones)
   - Select a zone and press '√'.
2. Open the transmitter housing.
3. Remove the divider separating the battery from the contacts on the battery holder. The transmitter will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the device.

   ☞ Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode for a few minutes until the battery voltage level is stabilized
4. As soon as 'Save?' appears press '√'.

Flood Detector Mounting Location

The flood detector should be placed in a position where water will accumulate rapidly in the event of flooding.

After selecting the mounting location:

1. Attach the flood detector in horizontal position near the floor with the 2 pins facing downwards using the enclosed screws or double-sided sticker.

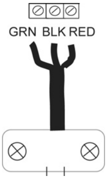


Figure B- 50: EL-4761 Flood Detector

2. Secure the flood detector cable to the wall.

   ☞ It is recommended to place the flood detector cable inside metal or plastic pipes

Installation Procedure

After the transmitter has been registered mount the transmitter as follows:

☞ Before permanently mounting the unit, test the transmitter from the exact mounting position. If necessary, improve the position of the transmitter. The alarm is generated by pressing the tamper switch.

1. Open the transmitter housing.
2. Remove the PCB by pressing the PCB release tab.

☞ When handling the PCB, do not apply pressure on the antenna.

3. Mount the back cover using two screws and replace the PCB. Use ISO 7050 (ST3.5 x 22) or similar countersunk screws so that the screw head will not touch the PCB.

☞ The upper screw is also used for back tamper. When the transmitter is removed from the wall, the screw causes the tamper release to break away from the back cover and the rear tamper switch is released.

4. Knockout the wiring hole in the back cover.
5. Thread the wires through the wiring hole.
6. Connect the terminal block.
7. Test the transmitter, making certain that the LED is lit during transmission.
8. Close the front cover of the transmitter.

Deleting a Flood Detector

To delete a flood detector from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[1] (Programming > Devices > Zones).
   - Select a zone and press '√'
2. Press >12 >√.
3. Open the detector and take out the battery.
4. Press the tamper switch. While the tamper switch is being pressed insert the battery.
5. Within five seconds open the tamper and close it again.

Indoor Siren (EL-4723)

The EL-4723 is a 2-Way Wireless Indoor Siren for use with the iConnect Control System. In the event of an alarm the control system activates the siren. The Wireless Indoor Siren is sounded until the end of the control-system-programmed siren cutoff.

Location of the Siren

Consider the following before mounting the siren:

- Choose a suitable mounting location for the siren.
- The siren should be mounted on a flat surface in a highly visible position for maximum deterrence against potential intruders.
- Before permanently mounting the siren, test the reception from the exact mounting position.

☞ Always wear ear protectors when installing indoor/outdoor sirens

Registration Procedure

The EL-4723 must identify itself to the iConnect Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[5]>[1] (Programming > Devices > Siren>WL Siren)
   - Select a siren from the list (1-4) and press '√'.
2. Release the mounting bracket captive locking screw.

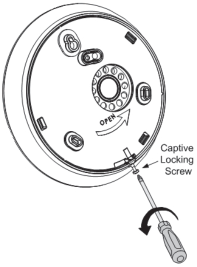


Figure B- 51: Releasing the locking screw

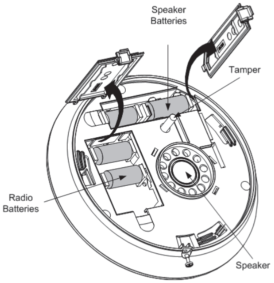


Figure B- 52: Inserting the batteries

3. Open the housing – lift the front cover away from the rear housing.
4. Insert the batteries while paying attention to polarity.

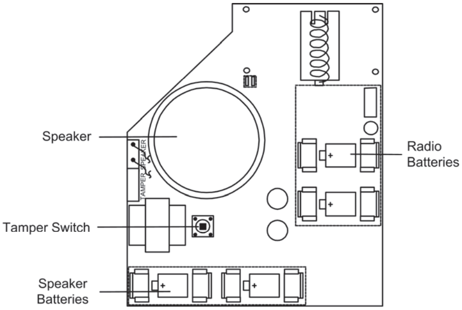


Figure B- 53: Inserting the batteries (#2)

5. The siren will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the siren.
6. As soon as 'Save?' appears press '√'.

Installation Procedure

After the siren has been registered mount the unit as follows:

1. Place the back cover in position against the wall and mark the upper and lower mounting holes.
2. Install wall anchors in the appropriate positions.
3. Attach the back cover to the wall using supplied screws.

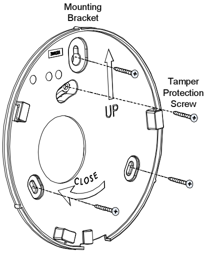


Figure B- 54: Attaching the mounting bracket

4. Mount the siren to the mounting bracket by turning the siren clockwise.
5. Secure the captive locking screw.

Testing the Siren

Once the siren has been registered test the unit according to the following testing procedure:

To perform a siren test:

1. Go to the main menu and select [7]>[0]>[3]>[1] (Service> Tests> WL Siren Test).
2. Select a siren from the list (1-4) and press '√'. The selected Siren is sounded briefly.

Deleting a Siren

To delete a siren from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[5] (Programming > Devices > Siren)
   - Select a siren from the list (1-4) and press '√'.
2. Press >3>'√'. Upon the 'OK' confirmation request, press '√'
3. Open the siren and take out the battery.
4. Press the tamper switch. While the tamper switch is being pressed insert the battery. Within five seconds open the tamper and close it again.

Outdoor Siren and Strobe (EL-4726T)

The EL-4726T is a 2-Way Wireless Outdoor Siren Strobe for use with the iConnect Control System. In the event of an alarm the control system activates the siren and strobe. The Wireless Siren is sounded until the end of the control-system-programmed siren cutoff. After the siren cutoff has expired, the strobe continues to flash until the system is disarmed.

Location of Siren Strobe

Consider the following before mounting the siren strobe:

- Choose a suitable mounting location for the siren strobe.
- The siren strobe should be mounted on a flat surface in a highly visible position for maximum deterrence against potential intruders.
- Before permanently mounting the siren strobe, test the reception from the exact mounting position.

Always wear ear protectors when installing indoor/outdoor sirens

Registration Procedures

The EL-4726T must identify itself to the iConnect Control System as follows:

1. Set the system to registration mode.
   - Go to the main menu and select [9]>[1]>[5]>[1] (Programming > Devices > Siren>WL Siren)
   - Select a siren from the list (1-4) and press '√'.
2. Open the screw cover by applying thumb pressure on the screw cover lower part.
3. Open the cover screw and lift the front cover away from the rear housing.
4. Open the battery housing cover
5. Insert the batteries while paying attention to polarity.

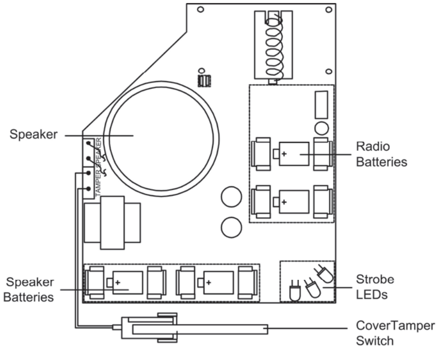


Figure B- 55: Inserting the batteries

6. The siren will send a transmission. If the transmission is successfully received by the system it will play a confirmation sound. If no confirmation sound is heard send another transmission by pressing and releasing the tamper switch of the siren.
7. As soon as 'Save?' appears press '√'.

Installation Procedure

After the siren strobe has been registered mount the unit as follows:

1. Place the back cover in position against the wall and mark the upper and lower mounting holes.
2. Install wall anchors in the appropriate positions.
3. Attach the back cover to the wall using supplied screws.
4. Mount the siren strobe to the mounting bracket.
5. Close the battery housing cover and replace the front cover. Pay attention to the tamper switch.
6. Secure the cover screw and replace the screw cover.

Testing the Siren Strobe

Once the siren strobe has been registered test the unit according to the following testing procedure:

To perform a siren strobe test

1. Go to the main menu and select [7]>[0]>[3]>[1] (Service> Tests> WL Siren Test).
2. Select a siren from the list (1-4) and press '√'. The selected siren is sounded briefly.

Deleting the Siren Strobe

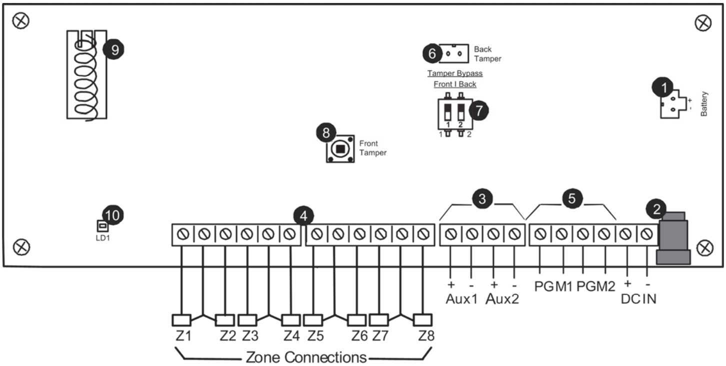
To delete a siren strobe from the system:

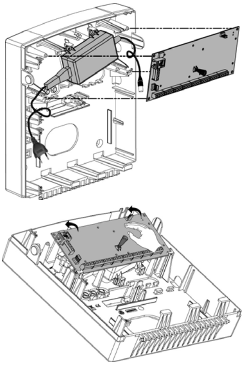
1. Set the system to Delete mode.
2. Go to the main menu and select [9]>[1]>[5] (Programming > Devices > Siren).
3. Press >5, and press '√'. Upon the 'OK' confirmation request, press '√'
4. Open the siren strobe and take out the batteries.
5. Press the tamper switch. While the tamper switch is being pressed insert the batteries. Within five seconds open the tamper and close it again.

I/O Expander Module (EL-4770)

The 2-Way Wireless I/O Expander Module (EL-4770) is an extension module enabling wired devices to be connected to the iConnect ② Control System (SW versions 305 and above). The iConnect ② Control System supports up-to two 2-Way Wireless I/O Expander Modules. Each 2-Way Wireless I/O Module supports 8 hardwired zone inputs, 2 auxiliary outputs and has the capability to control up to 2 PGM devices. Each output or PGM device can be operated in a response to a wide variety of system events.

The 2- Way Wireless I/O Expander Module is installed outside the Control System in its own dedicated plastic unit equipped with case open and wall removal tamper protection. The Wireless I/O Module is also provided with its own power supply and backup battery.





1. Backup battery connector
2. Power input jack (by external AC/DC adaptor)
3. Auxiliary parallel outputs (Aux1-2) for powering detection devices
4. Zone inputs (loop type configurable in programming)
5. Programmable outputs (PGM): dry contact
6. Back tamper switch connector
7. Tamper bypass dip switch
8. Front case tamper switch
9. Antenna (868 or 433)
10. LED indicator

Figure B- 56: I/O Expander Module circuit board and plastic unit

Table B-9: LED Indication

LED	State	Description
Red	On	AC and batteries OK
	Flashing	AC trouble
	Off	Power not present
Orange	Flashing	Low battery
Green/Red (tamper open)	Flashing	Green – Signal reception Red – Signal transmission

Box & Wall Tamper

Box and wall tamper switches provides extra protection. If the plastic unit is opened the front tamper switch is released and an alarm is generated. In the event that the plastic unit is removed from the wall, the screw causes the perforated section of the plastic and attached tamper mechanism metal plate to break and remain attached to the wall. As a result, the back tamper switch is released and an alarm is generated.

The front tamper switch is located on the front of the circuit board and is depressed via a spring when the front plastic cover is closed. The back tamper switch is located on the rear side of the back panel and is constantly depressed.

Attach the tamper hole to the wall during mounting and attach the tamper connector and lead to the main panel.

Set the Tamper dipswitch SW1 according to your tamper protection preferences, see Tamper Bypass section, below.

Tamper Bypass

The circuit board provides an option to bypass the front and back tamper, as shown in the following table:

Table B-10: Tamper Bypass Settings

Dipswitch SW1	Setting	Description
	ON	Tamper bypass is in effect. Use this setting during programming and if no back tamper has been connected.
	OFF	(Default): No tamper bypass is in effect. Use this option when back tamper is connected to the system.

Choosing the Mounting Location

Before you mount the 2-Way Wireless I/O Expander Module plastic unit, study the premises carefully for the best possible coverage and yet easily accessible to devices and accessories. Consider the following before mounting the 2-Way Wireless I/O Expander Module plastic unit:

- Centrality of location among all the detection devices and transmitters
- Proximity to an uninterrupted AC power supply
- Distance from sources of interference, such as direct heat sources, electrical noise such as computers, televisions etc., large metal objects, which may shield the transmission antenna
- Dryness

Mounting the I/O Expander Module

The 2-Way Wireless I/O Expander module unit consists of back and front panels and features plastic click-mounting for all internal components.

1. Separate the sub-assemblies by pressing the circular locking plastic brackets on either side to release the front cover (see below).

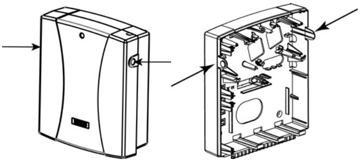


Figure B- 57: Box clip release

2. Remove the circuit board and if required open knock outs for the entry of input and power wires.
3. Hold the mounting bracket against the wall as a template and mark the locations for the mounting holes (4 mounting holes and an additional optional hole for securing the tamper protection bracket item).

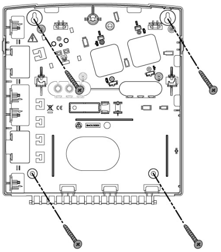


Figure B- 58: Mounting screw template

4. Drill the desired mounting holes and place the screw anchors.

☞ Do not permanently mount the plastic unit at this point of the installation

Wiring the I/O Expander Module

AC Adaptor and Circuit Board

The 2-Way Wireless I/O Expander Module is powered by an AC/DC Adaptor 100-240V, 50/60Hz/14.4V,1.5A. Connection to AC power supply must be permanent and connect through the mains-fuse terminal block (see below).

⚠ Caution

AC wiring should be done by a certified electrician

1. Connect the AC adapter to the main fuse terminal block (see below).

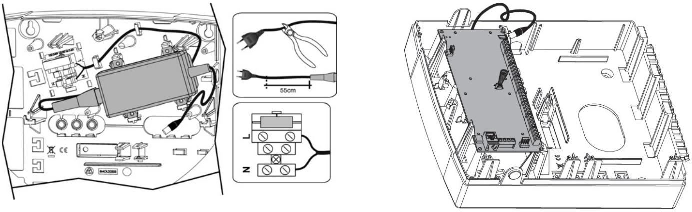


Figure B- 59: AC adapter and circuit board placement

2. Reinstall the circuit board and connect the power source plug to the power input jack on the circuit board.

⚠ Caution

Do not connect to main AC power at this point of the installation

3. Wire all input and output peripherals as described in the following sections.

Zone Input Wiring

The 2-Way Wireless I/O Expander Module supports 8 hardwired zones (defined in the iConnect ② Control System) that can be defined as Normally Open, Normally Closed, End of Line Double End of Line resistor zones. Zone connection configuration must be defined accordingly at each zone's programming parameters.

Auxiliary Output (AUX) Wiring

The 2-Way Wireless I/O Expander Module includes 2 auxiliary outputs (12±2VDC 1000mA). Use the auxiliary output terminals to power PIRs, glass-break detectors, smoke detectors, audio switches, photoelectric systems and/or any device that requires a 9VDC power supply.

☞ The total power from the AUX terminals should not exceed 1000 mA

Programmable Output (PGM) Wiring

The 2-Way Wireless I/O Expander Module enables the iConnect ② Control System to control PGM devices. The PGM is a programmable output that is triggered according to specific system status condition.

Connect a PGM device to the PGM output. PGM control configuration must be defined accordingly at each PGM's programming parameters.

Backup Battery Connection

Insert the backup battery into its place and connect the lead connector to the backup battery jack on the circuit board.

⚠ Caution

The circuit board is designed to work with all approved 12VDC,7Ah sealed lead batteries as a backup for the primary power supply in time of main power failure.

The circuit board is designed with reverse polarity protection on the battery charging circuit. However, prolonged improper connection of the battery to the circuit board will result in damage.

The battery is not supplied with the 2-Way Wireless I/O Expander Module.

The rechargeable battery should be charged for at least 72 hours.

Battery presence is checked every 10 seconds.

There is a risk of explosion if a battery is replaced with an incorrect type.

Dispose of used batteries according to the proper instructions.

Battery in product shall be replaced every 3-5 years. No maintenance is needed.

The power should remain disconnected until all connections have been made and checked for accuracy.

Completing the Installation

To complete the installation:

1. Mount the 2-Way Wireless I/O Expander Module back panel to the wall using affixing screws.
2. Connect the 2-Way Wireless I/O Expander Module to the AC mains power.

⚠ Caution

When the circuit board is powered on, mains voltage is present on the main PCB.

To prevent risk of electric shock, disconnect all power (AC transformer and battery) before servicing.

Under no circumstances should mains power be connected to the PCB other than through the main terminal block.

A readily accessible disconnection device shall be incorporated in the building installation wiring.

For continued protection against risk of fire, replace fuses only with fuses of the same type and rating.

3. Before closing the front cover and securing the locking screw, proceed to Registering the 2-Way Wireless I/O Expander Module, below.

Registering the I/O Expander Module

The 2-Way Wireless I/O Expander Module must identify itself to the iConnect ② Control System as follows:

1. Set the control system to registration mode.
   - Go to the main menu and select [9]>[1]>[6] (Programming > Devices > Zone Expanders)
   - Select a 2-Way Wireless I/O Expander Module from the list (1-2) and press '√'.
2. With the plastic unit cover open send a transmission by pressing and releasing the tamper switch of the Wireless I/O Expander Module. The 2-Way Wireless I/O Expander Module will send a transmission to the control system. If the transmission is successfully received by the control system it will play a confirmation sound.
3. As soon as 'Save?' appears press '√'.
4. Close the 2-Way Wireless I/O Expander Module front cover and secure the locking screw.

Deleting the I/O Expander Module

To delete a 2-Way Wireless I/O Expander Module from the system:

1. Set the system to Delete mode.
   - Go to the main menu and select [9]>[1]>[6] (Programming > Devices > Zone Expanders).
   - Select a 2-Way Wireless I/O Expander Module from the list (1-2) and press '√'.
2. Press >3, and then press '√'. Upon the 'OK' confirmation request, press '√'
3. Open the plastic unit (see Figure 5 1 and Figure 6 1) and disconnect the main AC power.
4. Press the tamper switch. While the tamper switch is being pressed connect the power. Within five seconds open the tamper and close it again.

Transmitter Specifications

The technical specifications for the transmitters that appear in this appendix are listed below. All transmitters are available in 868, or 433MHz (optional) FM frequencies.

El-4755 PIR
Frequency: 868* or 433MHz
Power: 3.6VDC AA Lithium Battery (x 2)
Current Consumption: 200mA (capture with flash), 42µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 14 x 14m
Pulse Count: 1 or 2
LED Indicator: Selectable
Digital Adaptive Temperature Compensation
RFI Immunity: According to EN 50130-4
Operating Temperature: 0 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 62 x 50mm

* Complies with EN-50131 2-2 Grade 2 Class II, Power Supply Type C

El-4755PI PIR
Frequency: 868* or 433MHz
Power: 3.6VDC AA Lithium Battery (x 2)
Current Consumption: 200mA (capture with flash), 42µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 11 x 11m
Pulse Count: 1 or 2
LED Indicator: Selectable
Digital Adaptive Temperature Compensation
RFI Immunity: According to EN 50130-4
Operating Temperature: 0 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 62 x 50mm

* Complies with EN-50131 2-2 Grade 2 Class II, Power Supply Type C

El-4745 PIR
Frequency: 868* or 433MHz
Power: 3.6V ½ AA Lithium Battery (Optional x 2)
Current Consumption: 30mA (transmission), 35µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 14 x 14m
Pulse Count: 1 or 2
LED Indicator: Selectable
Digital Adaptive Temperature Compensation
RFI Immunity: According to EN 50130-4
Operating Temperature: 0 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 62 x 50mm

* Complies with EN-50131 2-2 Grade 2 Class II, Power Supply Type C

El-4745PI PIR
Frequency: 868* or 433MHz
Power: 3.6V ½ AA Lithium Battery (Optional x 2)
Current Consumption: 30mA (transmission), 35µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 11 x 11m
Pulse Count: 1 or 2
LED Indicator: Selectable
Digital Adaptive Temperature Compensation
RFI Immunity: According to EN 50130-4
Operating Temperature: 0 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 62 x 50mm

* Complies with EN-50131 2-2 Grade 2 Class II, Power Supply Type C

EL-4601DZ Magnetic Contact/ Universal Transmitter
Frequency: 868* or 433MHz
Power: 3.6VDC ½ AA Lithium Battery
Current Consumption: 25mA (transmission), 10µA (standby)
RFI Immunity: According to EN 50130-4
Operating Temperature: 0-60°C

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL-4602 Universal Transmitter
Frequency: 868* or 433MHz
Power: 3.6VDC ½ AA Lithium Battery
Current Consumption: 25mA (transmission), 10µA (standby)
RFI Immunity: According to EN 50130-4
Operating Temperature: 0-60°C

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL-4607 Vibration Detector
Frequency: 868* or 433MHz
Power: 3.6VDC ½ AA Lithium Battery
Current Consumption: 25mA (transmission), 10µA (standby)
RFI Immunity: According to EN 50130-4
Alarm Delay During Normal Operation: Approx. 4 minutes
Operating Temperature: 0-60°C

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL-4703 Smoke Detector
Frequency: 868* or 433MHz,
Power:2xCR123 3V Lithium battery
Average Standby Current: 0.04mA
Test Current: 55mA
Alarm Current: 55mA
Peak Trouble Pulse Current: 4.73mA
Peak Pulse Current: 0.074mA
Alarm Sound Level: Exceeds 85dB at 3m (10 feet)
Operating Temperature: -10°C to 40°C (14°F - 104°F)
Dimensions: Diameter: 148 x 53mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL-4714 Keyfob
Frequency: 868* or 433MHz
Power: 3V Lithium Battery, Type CR2032
Current Consumption: 16mA (transmission), 0.2µA (standby)
RFI Immunity: According to EN 50130-4
Operating Temperature: 0-60°C

*Complies with EN- Grade 2 Class II Power Supply Type C

EL-4611M/P Keyfob
Frequency: 868* or 433MHz
Power: 3V Lithium Battery, Type CR2032
Current Consumption: 16mA (transmission), 0.2µA (standby)
RFI Immunity: According to EN 50130-4
Operating Temperature: 0-60°C

*Complies with EN- Grade 2 Class II Power Supply Type C

EL-4727 Wireless LCD Keypad
Frequency 868* or 433MHz
Power: 4x1.5V Lithium AA batteries
Current consumption: up to 100mA (transmission),
50µA (standby)
Operating temperature: 0°C to 60°C (32°F to 140°F)
Dimensions: 214 x 110 x 35mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL- 4762 Gas Leak Detector
Frequency: 868* or 433MHz
Power: AC120V/AC230V (model dependant)
Signal Volume: Approx. 85 dB at a distance of 3 meters
Operating Temperature: 0°C to 40°C (32°F to 122°F)
Storage Temperature: -20°C to 60°C (-4°F to 140°F)
Dimensions: 140 X 80 X 49 mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL- 4764 Carbon Monoxide Detector
Frequency: 868* or 433MHz
Power: 2 x CR 123, 3V Lithium Battery
Current Consumption: 20 µA (standby), 30mA (Alarm)
Signal Volume: Approx. 85 dB at a distance of 3 meters
Operating Temperature: 4°C to 38°C (39°F to 100°F)
Storage Temperature: -20°C to 60°C (-4°F to 140°F)
Dimensions: 140 X 80 X 49 mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL- 4761 Flood Detector
Frequency: 868* or 433MHz
Power: 3.6VDC ½ AA Lithium Battery
Current Consumption: 25mA (transmission),
40µA (standby)
RFI Immunity: According to EN 50130-4
Operating Temperature: 0-60°C
Dimensions: 65 x 30 x 25mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL-4723 Indoor Siren
Frequency: 868* or 433MHz
Power: 4 X CR123, 3V Lithium Battery (2 batteries for the Radio Transceiver, 2 batteries for the Speaker)
Current Consumption: 25mA (transmission), 40µA (standby)
Siren Output: Approx. 85dB @ 1m
Operating Temperature: -25°C to 60°C (-4°F to 140° F)
Dimensions: Ø183 x 51 mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL-4726 Outdoor Siren/Strobe
Frequency: 868* or 433MHz
Power: 4 X CR123, 3V Lithium Battery (2 batteries for the Radio Transceiver, 2 batteries for the Speaker)
Current Consumption: 25mA (transmission), 40µA (standby)
Siren Output: Approx. 105dB @ 1m
Operating Temperature: -25°C to 60°C (-4°F to 140° F)
Dimensions: 340 x 222 x 73mm

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

EL- 4770 I/O Expander Module
Frequency: 868* or 433MHz
Power Input: AC/DC Adaptor 100-240V,50/60Hz/14.4VDC,1.5A
Current Consumption: Typical: 40 mA; 65mA maximum
Rechargeable Standby Battery: 12VDC±2VDC up to 7Ah, typical
Auxiliary Power Outputs: 12VDC@1000mA, maximum (from all AUX terminals)
PGM Relay Output Dry Contact Rating: Dry contact – 1A@30VDC,0.5A@25VDC
Number of Zones: 8
Zone Loop Type: N.C. / N.O. / E.O.L. (Programmed at the Control System)
Tamper Protection: Front cover and back tamper (N.C.)
RF immunity: According to EN50130-4
Operating temperature: -10°C to 40°C (14°F to 104°F)
Storage temperature: -20°C to 50°C (-4°F to 122°F)
Usage: Indoor
Dimensions (Plastic Case): 290 x 254 x 97 mm (11.2 x 9.7 x 3.6 inch)

*Complies with EN-50131 2-6 Grade 2 Class II Power Supply Type C

Lithium Batteries

⚠ Fire, explosion and severe burn hazard!

When handling lithium batteries follow the listed precautions:

- Do not recharge.
- Do not deform or disassemble.
- Do not heat above 212°F (100°C) or incinerate.

☞ Due to the occurrence of voltage delay in lithium batteries that have been in storage, the batteries may initially appear to be dead. In this case, leave the unit in Test mode or Radio mode for a few minutes until the battery voltage level is stabilized.

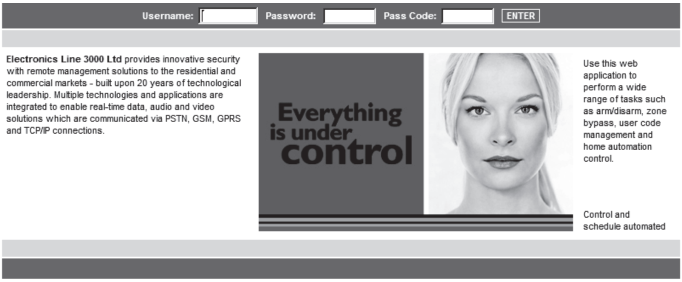
Appendix C: Web User Application

The Web Application provides a full interface to all of the system's user functions. Via the Web, the end user can perform a wide range of tasks such as arm/disarm, zone bypass, user code management and home automation control. You can also access the Web User Application from your cellular phone or PDA using the WAP protocol.

Log In Page

This application is usually part of the service provider's Web site and requires the end user to log in to gain access to the page.

To enter the Web Application, on your browser enter the Web page address supplied by your WEB service provider and press Go. You will see the Login Page.



Electronics Line 3000 Ltd provides innovative security with remote management solutions to the residential and commercial markets - built upon 20 years of technological leadership. Multiple technologies and applications are integrated to enable real-time data, audio and video solutions which are communicated via PSTN, GSM, GPRS and TCP/IP connections.

Use this web application to perform a wide range of tasks such as arm/disarm, zone bypass, user code management and home automation control.

Control and schedule automated

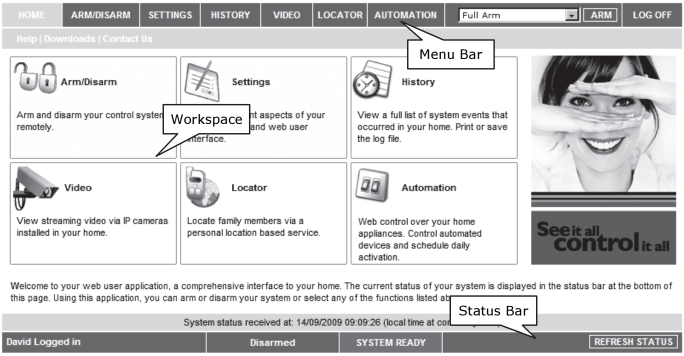
Figure C- 1: Login Page

To login to the Web Application, enter your user name and password supplied by your WEB service provider, and the passcode which is your User Code, then click the Enter button.

⚠ For your system security reasons, you must change the password immediately at first login. You can change your password on the Change Password page that is accessible from the Settings menu. Your new password should be no less than six characters and must start with a letter.

The Main Page

After logging in, your system's home page (Main Page) is displayed.



Arm and disarm your control systen remotely.

nt aspects of your and web user nterface.

View a full list of system events that occurred in your home. Print or save the log file.

View streaming video via IP cameras installed in your home.

Locate family members via a personal location based service.

Web control over your home appliances. Control automated devices and schedule daily activation.

Welcome to your web user application, a comprehensive interface to your home. The current status of your system is displayed in the status bar at the bottom of this page. Using this application, you can arm or disarm your system or select any of the functions listed ab

System status received at: 14/09/2009 09:09:26 (local time at co

David Logged in | Disarmed | SYSTEM READY

Figure C- 2: The Main Page

When using the Smartphone application service, the main page looks the following way:

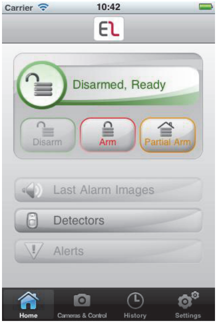


Figure C- 3: The Main Page (Smartphone Application)

Menu Bar

The Menu Bar includes the Main Menu, arm/disarm options list and the Log Off button. The Main Menu offers links to various pages in the Web Application. Use the Logoff button on the right side menu to properly close the session.The following options are available from the Main Menu:

- Home – pressing the Home button allows the user to return to the Main page at any time
- Automation – allows control or scheduling of automated lights and appliances.
- Video – provides access to view streaming video from IP cameras.
- My Account – offers various options including user code and contact management, event log viewing and zone bypass.
- Help – offers online explanations on how to use the Web Application plus FAQ and customer support options.

Status Bar

The Status bar displays information on your system's status and the name of the user currently logged in. Above the status bar, the time when the system status display was last updated is shown. This information is displayed according to the local time at the control system. When logging into the WUApp with a GPRS Control System, the system status refreshes automatically, and can be refreshed manually as well. To refresh the current system status, click the Refresh Status button on the right-hand side of the Status bar.

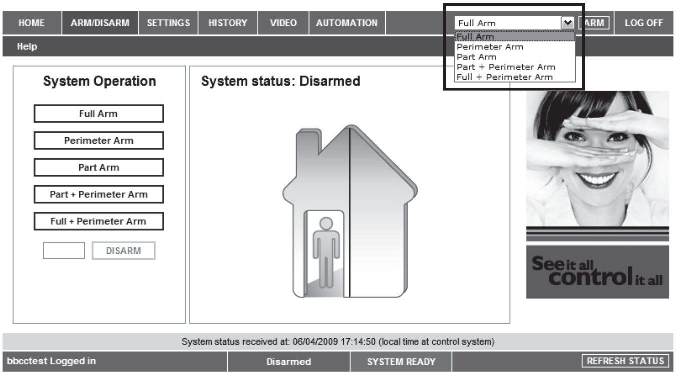
Workspace

The workspace offers additional links to the following pages of the application: Users and Codes, History, Automation, Alerts, Change Password, Video. When you choose a page, either from the Main Menu, or from the workspace, the page is displayed in the workspace. For example, if you choose Automation from the Main Menu, a list of automated appliances is displayed in the workspace.

☞ SMS alerts relate only to SMS sent from ELAS (WEB User Application).

Options Available from Main Page

Arm/Disarm



System status: Disarmed

System status received at: 06/04/2009 17:14:50 (local time at control system)

bbcctest Logged in

Figure C- 4: Arm/Disarm Page

You can arm and disarm the system using the Arm/Disarm drop-down box (upper-right part of the page) or using the buttons in the System Operation Area.

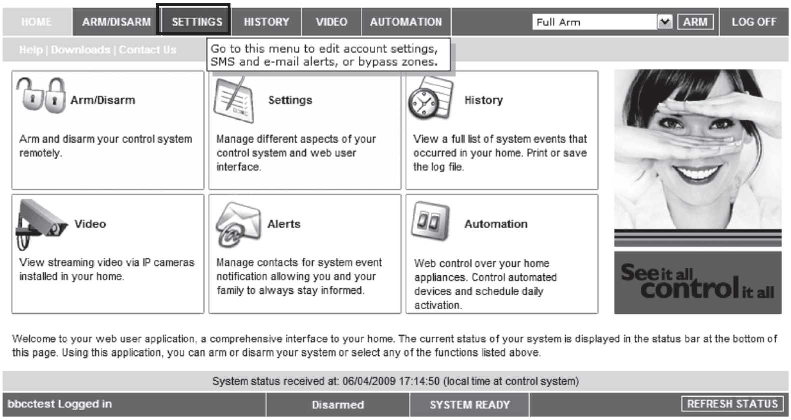
The Web Application allows you to arm and disarm your system via the Web Application using any of the available arming methods. It is important to note that when you arm using the Web application, the system is armed with the programmed delay.

1. On the Status Bar below on the page you can see the current status of the system (in our example it is Disarmed and System Ready, which means that the system and all the detectors are working properly and there are no events to report).
2. It is possible to check if there were alarms in the system – see p. 129, History.

System Users and Codes

In this area you can add, delete, or change users and the User Codes for your system (for example, add codes for family members).

1. On The Main Page menu, click Settings.



Go to this menu to edit account settings, SMS and e-mail alerts, or bypass zones.

Arm and disarm your control system remotely.

Manage different aspects of your control system and web user interface.

View a full list of system events that occurred in your home. Print or save the log file.

View streaming video via IP cameras installed in your home.

Manage contacts for system event notification allowing you and your family to always stay informed.

Web control over your home appliances. Control automated devices and schedule daily activation.

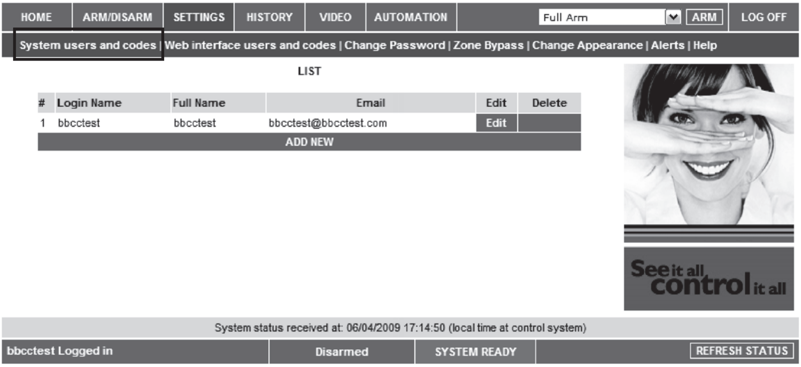
Welcome to your web user application, a comprehensive interface to your home. The current status of your system is displayed in the status bar at the bottom of this page. Using this application, you can arm or disarm your system or select any of the functions listed above.

System status received at: 06/04/2009 17:14:50 (local time at control system)

bbcctest Logged in

Figure C- 5: Settings Button

2. Click System Users and Codes, the following page appears:


HOME
ARM/DISARM
SETTINGS
HISTORY
VIDEO
AUTOMATION
Full Arm
ARM
LOG OFF
System users and codes | Web interface users and codes | Change Password | Zone Bypass | Change Appearance | Alerts | Help
See it all control it all
REFRESH STATUS

LIST

#	Login Name	Full Name	Email	Edit	Delete
1	bbcctest	bbcctest	bbcctest@bbcctest.com	Edit	

ADD NEW

System status received at: 06/04/2009 17:14:50 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY

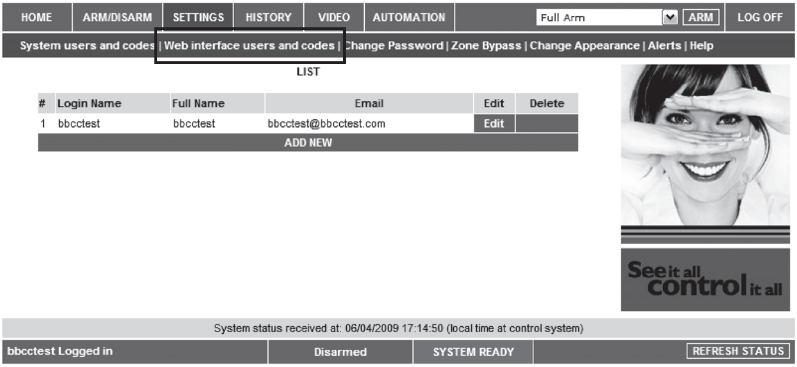
Figure C- 6: System Users and Codes Page

Web Interface Users and Codes

The Users and Codes page provides a useful tool for managing your system's users. From this page you can add, edit and delete users as required. You can even issue temporary (limited) codes to guests that will expire after 24 hours.

For further information on user codes and their various uses, see p. 21, 4.4 User Codes.

On The Main Page menu, click Settings, then Web Interface Users and Codes, the following page appears:


HOME
ARM/DISARM
SETTINGS
HISTORY
VIDEO
AUTOMATION
Full Arm
ARM
LOG OFF
System users and codes | Web interface users and codes | Change Password | Zone Bypass | Change Appearance | Alerts | Help
See it all control it all
REFRESH STATUS

LIST

#	Login Name	Full Name	Email	Edit	Delete
1	bbcctest	bbcctest	bbcctest@bbcctest.com	Edit	

ADD NEW

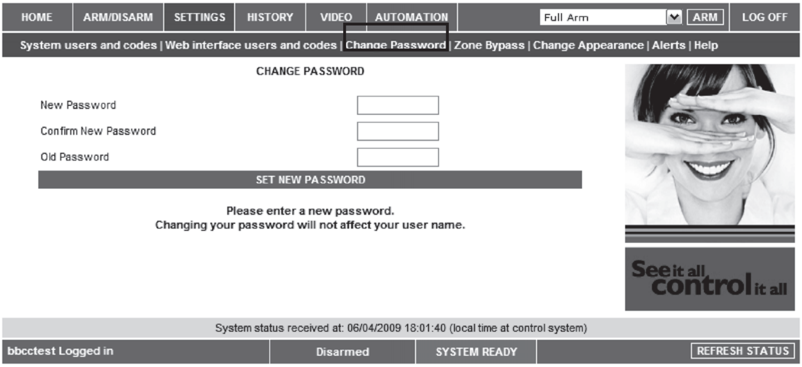
System status received at: 06/04/2009 17:14:50 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY

Figure C- 7: Web Interface Users and Codes Page

Change Password

Click Settings then Change Password to change the password you use to login to the Web Application.


HOME
ARM/DISARM
SETTINGS
HISTORY
VIDEO
AUTOMATION
Full Arm
ARM
LOG OFF
System users and codes | Web interface users and codes | Change Password | Zone Bypass | Change Appearance | Alerts | Help
See it all control it all
REFRESH STATUS

CHANGE PASSWORD

New Password

Confirm New Password

Old Password

SET NEW PASSWORD

Please enter a new password.
Changing your password will not affect your user name.

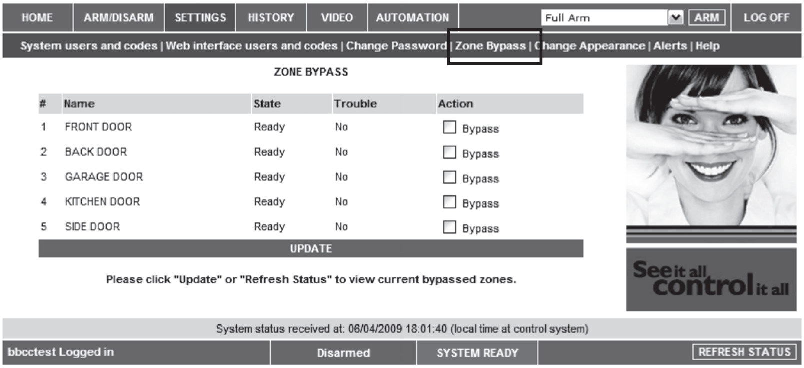
System status received at: 06/04/2009 18:01:40 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY

Figure C- 8: Change Password Page

Zone Bypass

On The Main Page menu, click Settings then Zone Bypass to bypass certain zones in your home that you don't want to receive event messages from – see p. 21, Zone Bypassing/Unbypassing. Select the checkboxes for the zones you want to bypass.


HOME
ARM/DISARM
SETTINGS
HISTORY
VIDEO
AUTOMATION
Full Arm
ARM
LOG OFF
System users and codes | Web interface users and codes | Change Password | Zone Bypass | Change Appearance | Alerts | Help
See it all control it all
REFRESH STATUS

ZONE BYPASS

#	Name	State	Trouble	Action
1	FRONT DOOR	Ready	No	□ Bypass
2	BACK DOOR	Ready	No	□ Bypass
3	GARAGE DOOR	Ready	No	□ Bypass
4	KITCHEN DOOR	Ready	No	□ Bypass
5	SIDE DOOR	Ready	No	□ Bypass

UPDATE

Please click "Update" or "Refresh Status" to view current bypassed zones.

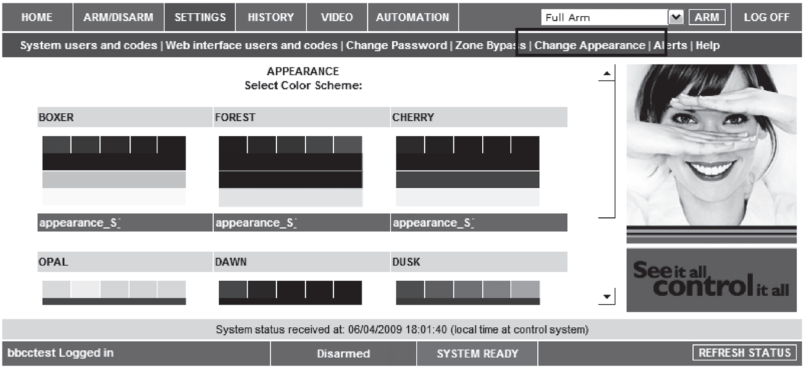
System status received at: 06/04/2009 18:01:40 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY

Figure C- 9: Zone Bypass Page

Change Appearance

On The Main Page menu, click Settings then Change Appearance to change the color scheme of your account.



System status received at: 06/04/2009 18:01:40 (local time at control system)

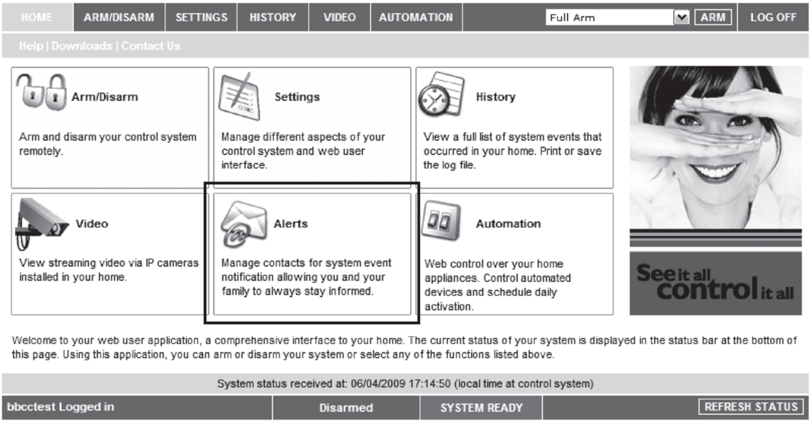
Figure C- 10: Change Appearance Page

Alerts

The Alerts page allows you to enter the details of contacts you wish to be informed when events occur in your system. For example, you can enter your own email address and/or cellular phone number so that you will receive email or SMS notification in the event of an alarm.

This area allows you to program where to send the alerts on home events (arming, disarming, alarm etc.) The events can be reported via email or your cellular phone.

1. On The Main Page menu, click the Alerts area.



Arm and disarm your control system remotely.

Manage different aspects of your control system and web user interface.

View a full list of system events that occurred in your home. Print or save the log file.

View streaming video via IP cameras installed in your home.

Manage contacts for system event notification allowing you and your family to always stay informed.

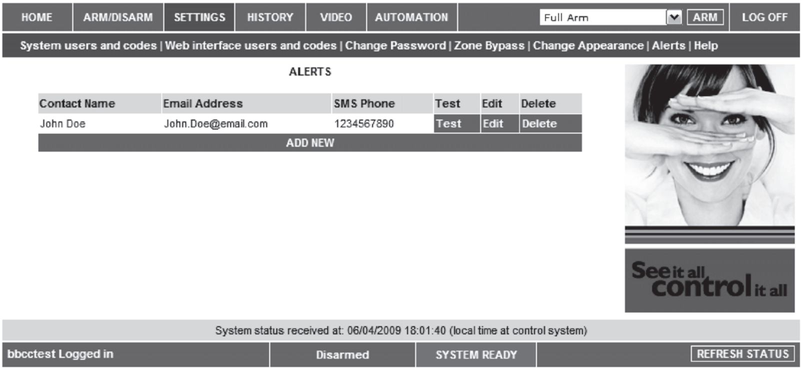
Web control over your home appliances. Control automated devices and schedule daily activation.

Welcome to your web user application, a comprehensive interface to your home. The current status of your system is displayed in the status bar at the bottom of this page. Using this application, you can arm or disarm your system or select any of the functions listed above.

System status received at: 06/04/2009 17:14:50 (local time at control system)

Figure C- 11: Alerts Area

The following page appears:


HOME
ARM/DISARM
SETTINGS
HISTORY
VIDEO
AUTOMATION
Full Arm
ARM
LOG OFF
System users and codes | Web interface users and codes | Change Password | Zone Bypass | Change Appearance | Alerts | Help
See it all control it all
REFRESH STATUS

ALERTS

Contact Name	Email Address	SMS Phone	Test	Edit	Delete
John Doe	John.Doe@email.com	1234567890	Test	Edit	Delete

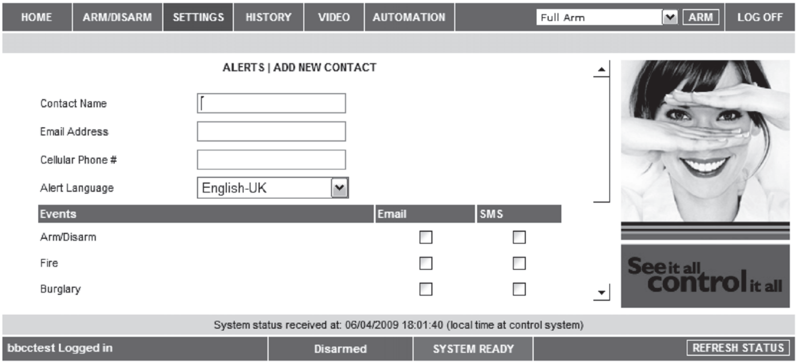
ADD NEW

System status received at: 06/04/2009 18:01:40 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY

Figure C- 12: Alerts Page

2. Press Add new to add email addresses or cellular telephone numbers for the alert messages.



ALERTS | ADD NEW CONTACT

Contact Name

Email Address

Cellular Phone #

Alert Language: English-UK

Events	Email	SMS
Arm/Disarm	□	□
Fire	□	□
Burglary	□	□

System status received at: 06/04/2009 18:01:40 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY

Figure C- 13: Add New Contact Page

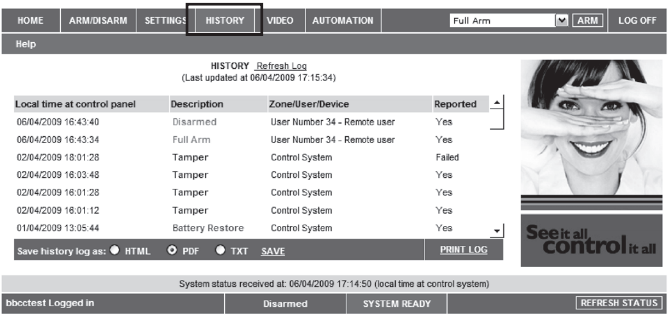
3. In the Contact Name field, enter the name of the contact to receive alerts.
4. In the Email Address field, enter the email address for email alerts.
5. In the Cellular Phone # field, enter the cellular phone number for SMS alerts.
6. To start receiving the events messages, in the area below, select the checkboxes according to the event type and message type you prefer (email or SMS).
7. Test the alerts you have programmed by clicking the Test button on the Alerts page near the newly added alert.

History

The History page enables you to view the system's event log. The events are arranged in a table that offers the advantage of allowing you to view a large number of events at once. In addition to viewing the event log, you may also save the log to a file (HTML, PDF or RTF) or print the log.

For further details on how to use the Web Application, refer to the Help menu included in the application.

- On The Main Page menu, click History, the following page appears:



HISTORY Refresh Log
(Last updated at 06/04/2009 17:15:34)

Local time at control panel	Description	Zone/User/Device	Reported
06/04/2009 16:43:40	Disarmed	User Number 34 - Remote user	Yes
06/04/2009 16:43:34	Full Arm	User Number 34 - Remote user	Yes
02/04/2009 18:01:28	Tamper	Control System	Failed
02/04/2009 16:03:48	Tamper	Control System	Yes
02/04/2009 16:01:28	Tamper	Control System	Yes
02/04/2009 16:01:12	Tamper	Control System	Yes
01/04/2009 13:05:44	Battery Restore	Control System	Yes

Save history log as: ● HTML ○ PDF ● TXT SAVE PRINT LOG

System status received at: 06/04/2009 17:14:50 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY | REFRESH STATUS

Figure C- 14: History Page

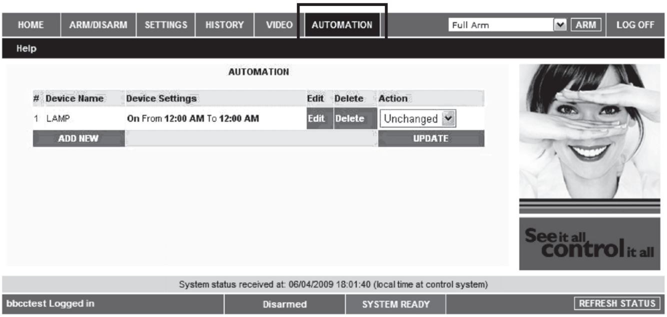
You can save or print the LOG from this page.

Automation

The Web Application allows you to control and schedule automated lights and appliances in your home. The application offers a comprehensive interface that enables you to view the settings for all of your automated devices at once. Additionally, you can add, edit or delete devices from the comfort of your PC.

Discuss this capability with your security service provider to determine if it is applicable to your system – see p. 33 Home Automation and PGM Control.

- On The Main Page menu, click Automation, the following page appears:



AUTOMATION

#	Device Name	Device Settings	Edit	Delete	Action
1	LAMP	On From **12:00 AM** To **12:00 AM**	Edit	Delete	Unchanged
	ADD NEW				UPDATE

System status received at: 06/04/2009 18:01:40 (local time at control system)

bbcctest Logged in | Disarmed | SYSTEM READY | REFRESH STATUS

Figure C- 15: Automation Page

You can program turning the HA units on/off at specific hour/day of the week.

Video

Using 2-way video verification PIR detectors (EL-4755/EL-4755PI) installed in your home, the Web Application enables you to view video images over the Web in order to check your home and family while you are away.

Discuss this capability with your security service provider to determine if it is applicable to your system.

Appendix D: Event Table*

Burglary

Description	🔧	Restore	SIA	Contact ID	Address Field
Alarm from Zone			NBA	1130	Device Number
Zone Alarm Restore	◆	◆	NBR	3130	Device Number
Zone Bypassed			NUB	1570	Device Number
Zone Unbypassed	◆	◆	NUU	3570	Device Number
Zone Tamper			NTA	1137	Device Number
Zone Tamper Restore	◆	◆	NTR	3137	Device Number
Zone Panic Alarm			NPA	1120	Device Number
Zone Panic Restore	◆	◆	NPR	3120	Device Number
Panic Alarm			NPA	1120	Device Number
Tamper			NTA	1137	Device Number
Tamper Restore	◆	◆	NTR	3137	Device Number
Duress			NHA	1121	—
Bell Cancel	◆		NBC	1521	User Number
Disarm after Alarm			NOR	1458	User Number
Water Alarm			NWA	1154	Device Number
Water Alarm Restore	◆	◆	NWH	3154	Device Number
Environmental Alarm			NUA	1150	Device Number
Environmental Alarm Restore	◆	◆	NUH	3150	Device Number
Exit Error	◆	◆	NEE	1457	User Number
Crash and Smash			….	….	….

Fire

Fire Alarm			NFA	1110	Device Number
Fire Alarm Restore	◆	◆	NFR	3110	Device Number
Gas Alarm			NGA	1151	Device Number
Gas Alarm Restore	◆	◆	NGH	3151	Device Number

Open/Close

Full Arm			NCL	3401	User Number
Part Arm			NCG	3456	User Number
Perimeter Arm			NCG	3441	User Number
Disarm (entire system)			NOP	1401	User Number

* 🔧 = Events that are displayed in the event log only when viewed by the installer.

Service

Description	🔧	Restore	SIA	Contact ID	Address Field
Edit User Code	◆		NJV	1462	User Number
Delete User Code	◆		NJX	3462	User Number
System Programming	◆		NLB	1627	—
End System Programming	◆		NLX	1628	—
Remote Programming	◆		NRB	1412	—
End Remote Programming	◆		NRS	3412	—
Walk Test	◆		NTS	1607	User Number
End Walk Test	◆		NTE	3607	—
Set Time	◆		NJT	1625	User Number
Set Date	◆		NJD	1625	User Number
Clear Log			NLB	1621	User Number

Power

Battery Low			NYT	1302	Device Number
Battery Restore		◆	NYR	3302	Device Number
Transmitter Low Battery			NXT	1384	Device Number
Transmitter Battery Restore		◆	NXR	3384	Device Number
AC Loss			NAT	1301	Device Number
AC Restore		◆	NAR	3301	Device Number
Power up (user-log)		◆	NRR	3301	Device Number

Peripherals

Media Loss			NLT	1351	Device Number
Media Loss Restore	◆	◆	NLR	3351	Device Number
Device Trouble			NET	1330	Device Number
Device Trouble Restore	◆	◆	NER	3330	Device Number
Transmitter Out of Synch.			NUT	1341	Device Number
Transmitter Re-synch.	◆	◆	NUR	3341	Device Number
CP Transmitter Out of Synch.			NUT	1341	Device Number
CP Transmitter Re-synch.	◆	◆	NUR	3341	Device Number
Supervision Loss			NUS	1381	Device Number
Supervision Restore	◆	◆	NUR	3381	Device Number
GSM Signal Level	◆		NYY	1605	Signal Level (0-9)
Zone Trouble			NBT	1380	Device Number
Zone Trouble Restore	◆	◆	NBJ	3380	Device Number

RF Jamming

FM Jamming			NXQ	1344	Device Number
FM Jamming Restore	◆	◆	NXH	3344	Device Number

Medical

Medical Alarm			NMA	1100	Device Number
Medical Alarm Restore	◆	◆	NMR	3100	Device Number
No Motion			NNA	1102	Device Number

Unclassified Events

Description	🔧	Restore	SIA	Contact ID	Address Field
Periodic Test	◆		NRP	1602	—
No Arm	◆		NCD	1654	—
Cancel Report			NOC	1406	—

Address Field

The address field provides additional information regarding the event. This information is forwarded as numeric data according to the following tables.

DEVICE NUMBER	
Value	Description
00	Control System
01-33	Zones
41-59	Keyfobs
65	Home Automation Module
77-80	Repeaters
81-84	Wireless Keypads
91	Front Panel Keypad
92-98	Hardwire Keypads
110	Wireless Siren
242	Communication Module
243	PSTN Communication Interface
244	Cellular Communication Interface
245	Ethernet Communication Interface
249	GPRS Communication Interface

USER NUMBER	
Value	Description
00	Control System
01-32	Users
34	Remote Access
41-59	Keyfobs
61-76	Smartkeys
81-84	Wireless Keypads
91	Front Panel Keypad
92-98	Hardwire Keypads

Appendix E: Zone Types

Normal

A Normal zone is active when the system is armed. This zone generates a Burglary alarm instantly when triggered. Normal zones are designed for detectors installed inside the protected site or doors/windows that are never used to enter the premises.

Event Group: Burglary

Entry/Exit

When the system is armed, Entry/Exit zones initiate the entry delay when triggered. If the system is not disarmed by the time the entry delay expires, a Burglary alarm is generated. These zones are designed for detectors protecting the entrance to the protected site

Event Group: Burglary

Follower

If an Entry/Exit zone is triggered first, Follower zones do not generate an alarm when triggered during the entry delay. If the system is not disarmed by the end of the entry delay, the Follower zone generates an alarm. A Follower zone instantly generates an alarm if triggered when the entry delay is not active. These zones are designed for detectors protecting the area in which a keypad has been installed or the area crossed in order to reach the keypad.

Event Group: Burglary

Panic

Panic zones are always active. When a Panic zone is triggered, a Panic alarm is generated. This zone type is designed for panic buttons that may be pressed in a robbery situation. If the Bell option is disabled for Panic zones, in addition to the siren not sounding, all forms of alarm indication from the keypad are also disabled.

Event Group: Burglary

Medical

Medical zones are always active. When triggered, Medical zones generate a Medical alarm. These zones are used typically with panic buttons that may be pressed in the event of a Medical.

Event Group: Medical

Fire

Fire zones are always active. When triggered, Fire zones generate a Fire alarm. These zones are designed for use with smoke detectors and panic buttons that may be pressed in the event of a fire. A Fire zone always activates the siren even if the Bell option is programmed as disabled. Fire alarms sound a pulsating siren to distinguish them from other alarms.

Event Group: Fire

24Hr

24Hr zones are always active. When triggered, 24Hr zones generate a Burglary alarm. These zones are used for applications that require constant protection.

Event Group: Burglary

24Hr-X

The 24Hr-X zone is a future option that is not available in the current firmware.

Event Group: Not applicable

Gas

Gas zones are always active. In the event of a gas leak, these zones generate a Gas alarm. Gas zones are typically used with methane/propane/butane or carbon monoxide gas detectors. Gas alarms sound a distinctive siren pattern to easily distinguish them from other alarms. A gas alarm causes the siren to sound until the alarm is restored; the siren cut-off does not apply to gas alarms.

Event Group: Fire

Flood

Flood zones are always active. When triggered, Flood zones generate a Water alarm. These zones are designed for use with EL-4761 flood detectors.

Event Group: Burglary

Environmental

Environmental zones are always active. When triggered, these zones generate an Environmental alarm. These zones are designed for applications that monitor environmental conditions such as temperature or humidity. If the Bell option is enabled for Environmental zones, the system sounds trouble tones from the keypad. These tones are sounded until the user presses ▼ on their keypad. Environmental alarms are not affected by the expiry of the siren cut-off.

Event Group: Burglary

No Motion

No Motion zones are used to monitor the activity of disabled or elderly people. If a No Motion zone has not been triggered within a pre-defined period of time (0 to 72 hours), a No Motion event message is sent to the central station.

Event Group: Medical

Arm/Disarm

The Arm/Disarm zone is a future option that is not available in the current firmware.

Event Group: Not applicable

Crash and Smash

This zone type can be used in cases where the alarm system, is positioned at the entrance of the premises. If a burglar breaks the door and smashes the alarm system, during the entry delay time and before a confirmed break-in event can be sent, a suspected break-in alarm event is sent to the monitoring station.

Event Group: Burglary

Not Used

This zone type is a future option that is not available in the current firmware.

Event Group: Not applicable

Electronics Line 3000 Ltd. Limited Warranty

EL and its subsidiaries and affiliates ("Seller") warrants its products to be free from defects in materials and workmanship under normal use for 24 months from the date of production. Because Seller does not install or connect the product and because the product may be used in conjunction with products not manufactured by the Seller, Seller cannot guarantee the performance of the security system which uses this product. Sellers' obligation and liability under this warranty is expressly limited to repairing and replacing, at Sellers option, within a reasonable time after the date of delivery, any product not meeting the specifications. Seller makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. In no case shall seller be liable for any consequential or incidental damages for breach of this or any other warranty, expressed or implied, or upon any other basis of liability whatsoever. Sellers obligation under this warranty shall not include any transportation charges or costs of installation or any liability for direct, indirect, or not be compromised or circumvented; that the product will prevent any persona; injury or property loss by intruder, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection. Buyer understands that a properly installed and maintained alarm may only reduce the risk of intruder, robbery or fire without warning, but is not insurance or a guaranty that such will not occur or that there will be no personal injury or property loss as a result. Consequently seller shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning. However, if seller is held liable, whether directly or indirectly, for any loss or damage arising from under this limited warranty or otherwise, regardless of cause or origin, sellers maximum liability shall not exceed the purchase price of the product, which shall be complete and exclusive remedy against seller. No employee or representative of Seller is authorized to change this warranty in any way or grant any other warranty.

WARNING: This product should be tested at least once a week.

CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to local regulations.

Contacting Electronics Line 3000 Ltd.

International Headquarters:

Electronics Line 3000 Ltd.
14 Hachoma St., 75655
Rishon Le Zion, Israel
Tel: (+972-3) 963-7777
Fax: (+972-3) 961-6584

All rights reserved.

No part of this document may be reproduced in any form without prior written permission from the publisher.