



infinite
broadband

CONTROL PANEL

INSTALLATION MANUAL



Electronics Line 3000 Ltd.

Infinite Broadband Installation Manual - Version 1.00
Catalog Number: Z10408A (7/06)

All data is subject to change without prior notice.

Hereby, Electronics Line 3000 Ltd. declares that this control panel is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.



Table of Contents

Chapter One: Introduction.....	5
1.1: Documentation Conventions.....	5
1.2: Specifications.....	6
1.3: System Overview.....	6
1.4: Hardware Layout.....	8
Chapter Two: System Installation.....	12
2.1: Pre-Installation Planning.....	12
2.2: Installation Procedure.....	13
2.3: Back Tamper.....	16
2.4: Installing Hardwire LCD Keypads.....	16
2.5: Ethercom Startup Sequence.....	18
2.6: Installing IP Cameras.....	18
Chapter Three: Basic System Operation.....	22
3.1: Front Panel Layout.....	22
3.2: System Status LEDs.....	22
3.3: Alphanumeric Keypad.....	23
3.4: LCD Display.....	23
3.5: Arming/Disarming.....	24
3.6: Remote Arming/Disarming via SMS.....	26
3.7: Front Panel Alarm Activation.....	27
Chapter Four: Advanced System Operation.....	28
4.1: Menu Navigation.....	28
4.2: Stop Communications.....	28
4.3: Sensor Bypassing/Unbypassing.....	29
4.4: User Codes.....	29
4.5: Follow Me.....	31
4.6: Event Log.....	31
4.7: Service Menu.....	32
Chapter Five: Web Access.....	37
5.1: Logging In.....	37
5.2: Web Application Interface.....	37
Chapter Six: Two-Way Audio.....	39
6.1: Incoming Calls.....	39
6.2: Outgoing Calls.....	40
6.3: Siren Silencing.....	41
Chapter Seven: Home Automation Control.....	42
7.1: Keypad Control.....	42
7.2: Keyfob Control.....	42
7.3: SMS Control (future availability).....	42
7.4: Scheduling.....	43
Chapter Eight: Devices.....	45
8.1: Device Registration.....	45
8.2: Device Descriptors.....	45
8.3: Device Deletion.....	46
8.4: Supervision Time.....	46
8.5: Re-Synchronization.....	46
8.6: Zones.....	47
8.7: Keyfobs.....	50
8.8: Keypads.....	51
8.9: Repeaters.....	51
8.10: External Siren.....	52
Chapter Nine: Entry/Exit Timers and Arming Tones.....	53
9.1: Entry/Exit Delay.....	53
9.2: Arm on Exit.....	53
9.3: Arming Tones.....	53
9.4: System Trouble Tones.....	55
9.5: Tones Options.....	55

- Chapter Ten: System Options 57
 - 10.1: Swinger Setting 57
 - 10.2: Code Lockout 57
 - 10.3: Forced Arm 57
 - 10.4: HA Control..... 58
 - 10.5: Panic Alarm..... 58
 - 10.6: One-Key Arming..... 58
 - 10.7: Supplementary Entry Delay..... 58
 - 10.8: Entry Deviation 58
 - 10.9: AC Loss Delay 59
 - 10.10: Arm Status Display..... 59
 - 10.11: Banner..... 59
 - 10.12: PGM Output 60
 - 10.13: Guard Code (for future use)..... 61
 - 10.14: Time/Date Format 61
 - 10.15: “No Arm” Indication 61
 - 10.16: Jamming Detection 62
 - 10.17: “No Motion” Time 62
- Chapter Eleven: Communications..... 63
 - 11.1: Accounts 63
 - 11.2: General Account Options 65
 - 11.3: Remote Programming 66
 - 11.4: Service Call 67
 - 11.5: SMS Center..... 68
 - 11.6: Communications Options 68
 - 11.7: Two-Way Audio Options 70
 - 11.8: GSM RX Report 71
 - 11.9: Event Options..... 71
- Chapter Twelve: Internet Options 73
 - 12.1: Ethercom..... 73
 - 12.2: ELAS 74
 - 12.3: I’m Alive Timers..... 75
- Chapter Thirteen: Home Automation Programming..... 77
 - 13.1: X10 Overview 77
 - 13.2: HA Units 77
 - 13.3: House Code 80
 - 13.4: SMS Confirmation 80
- Chapter Fourteen: System Initialization 81
 - 14.1: Initialization 81
 - 14.2: Default Program Restore 81
 - 14.3: Clear User Codes..... 81
 - 14.4: Clear Wireless Transmitters 81
 - 14.5: Find Modules..... 82
- Appendix A: Menu Structure 83
- Appendix B: Transmitter Installation 90
 - PIR Sensors (EL-2600/EL-2600PI/EL-2645/EL-2645PI) 90
 - Magnetic Contact (EL-2601)..... 93
 - Universal Transmitter (EL-2602) 94
 - Glassbreak Sensor (EL-2606)..... 95
 - Smoke Detector (EL-2603) 98
 - Keyfobs (EL-2611/EL-2614)..... 98
 - Wireless Keypads (EL-2620/EL-2640)..... 99
 - Transmitter Specifications..... 101

Chapter One: Introduction

This manual is designed to help you install the *infinite Broadband* control panel. 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) 918-1333.

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 panel's menu is included in section 4.1: Menu Navigation. In order to simplify the procedures that appear in the rest of this manual, the following conventions are used:


This...	Means...
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 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 sensor you want to program.
✓	The symbol on a key that appears on the keypad
4. Speaker Test	The text that actually appears on the LCD display (bold italics).
	Important note, please pay attention.

Table 1.1: Documentation Conventions

1.2: Specifications

General

Zones: 32 wireless zones (1 transmitter per zone), 1 hardwire zone (Zone 33)
Wireless Keyfobs: 8 (Controlled or Non-controlled)
Wireless Keypads: 4
Wireless Repeaters: 4
Hardwire LCD Keypads: 2 (INFINITE-KPD/L) or 3 (INFINITE-KPD/S)
User Codes: 32
Arming Methods: Full, Part or Perimeter
Event Log: 256 event capacity, time and date stamped

Communications

Accounts: 3 (8-digit account number)
Telephone Numbers: 3 regular, RP** Callback and Service Call (16-digits each)
Communication Interface Options: Ethernet 10BT, PSTN or GSM (optional expansion module required)

Home Automation

Control Medium: Power-line carrier
Protocol: X10
HA Units: 16 individually addressed

Receiver

Type: Super-heterodyne, fixed frequency
Frequency: 868.35, 433.92 or 418MHz FM
Data Encryption: SecuriCode™

Electrical

Power Input: 230VAC, 50Hz
Backup Battery Pack: 7.2V/3Ah
(6 x 1.2V Ni-MH rechargeable cells, size AA)
Fuse Ratings: 63mA/250V (AC protection fuse),
1A/250V (battery protection fuse)
PGM Relay Output Contact Rating: 100mA (max. load)
Internal Sounder: 95dB
Tamper Switch: N.C.
Operating Temperature: 0-60°C

1.3: System Overview

infinite Broadband is a full-featured wireless control panel 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 *infinite Broadband* on-site using the on-board LCD keypad or off-site via a PC using the RP up/downloading software.



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. 0.75mm² 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 panel.

Batteries shall be provided by a distributor and replaced by authorized service personnel.

Batteries should be stored in a cool, dry place.

** RP = Remote Programmer

The system offers secure TCP/IP network connectivity, providing high-speed central station reporting via a broadband 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. Backup communication is provided by the ethercom's on-board PSTN dialer and the GSM cellular communications module. The panel's home automation capabilities provide a wealth of features. The Home Automation module interfaces with X10 units over the AC premises wiring and provides the user with appliance and lighting control via a number of different media.

The following diagram shows the components that make up the system and the system's interaction with external communication networks.

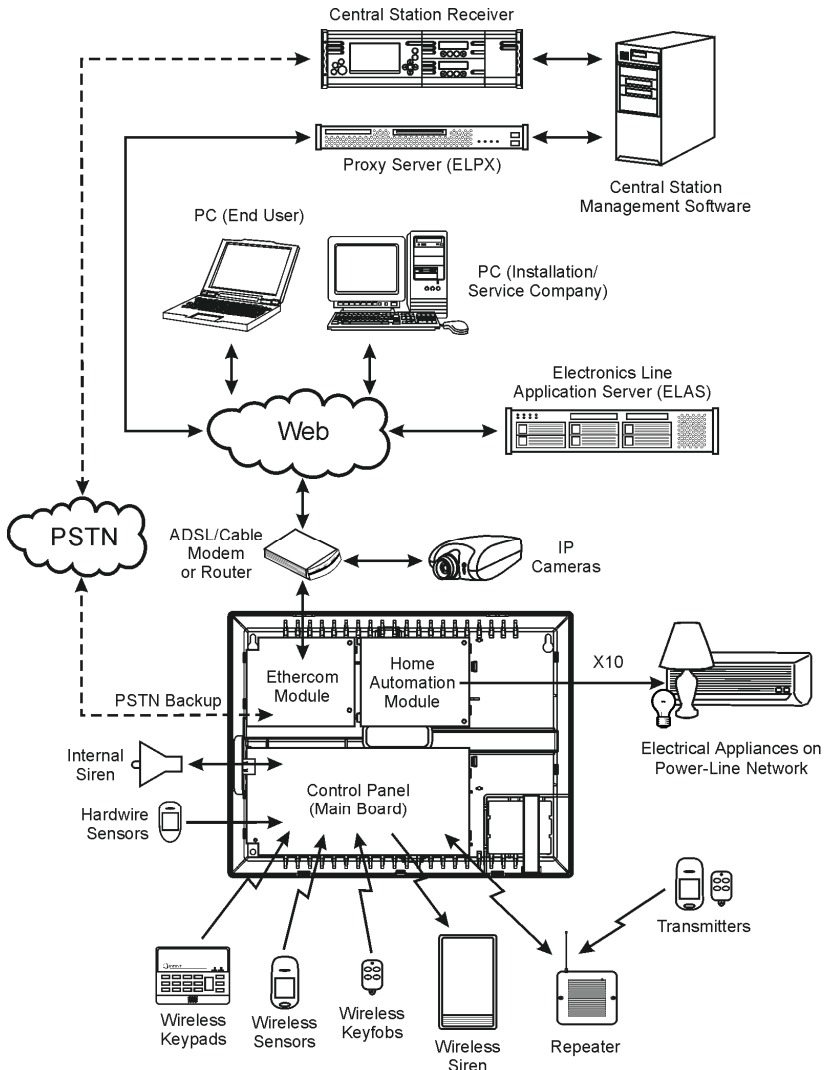


Figure 1.1: System Architecture

1.4: Hardware Layout

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

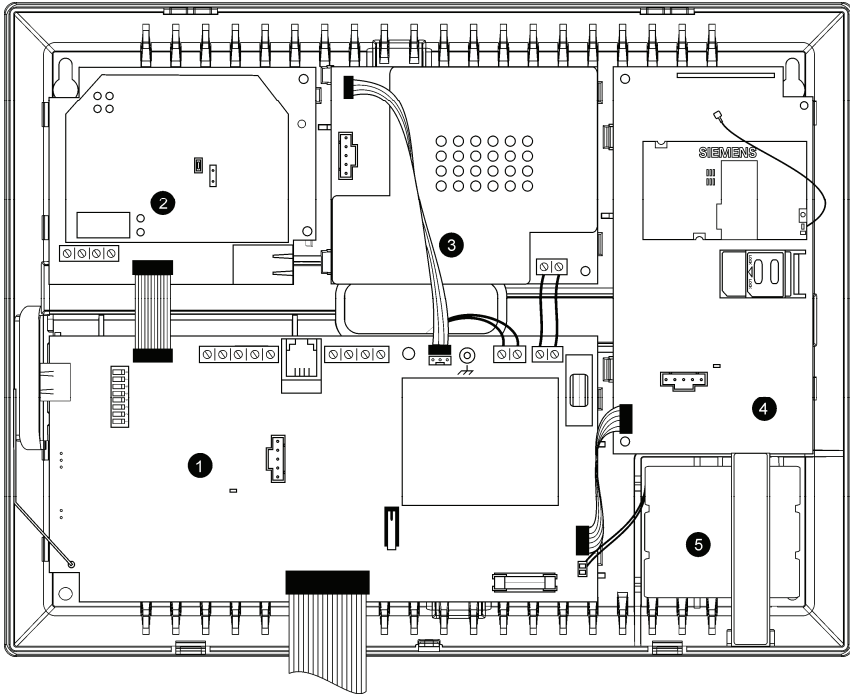


Figure 1.2: System Layout

1. Main Board
2. Ethernet module
3. Home Automation module (optional)
4. Cellular communications module (future option)
5. Backup battery pack

1.4.1: The Main Board

The Main Board is the brain of the system and connects to various peripheral modules using a number of interface connectors. Additionally, the Main Board includes a programmable output, a hardwire zone input, an external microphone/speaker connection and a serial port for PC programming.

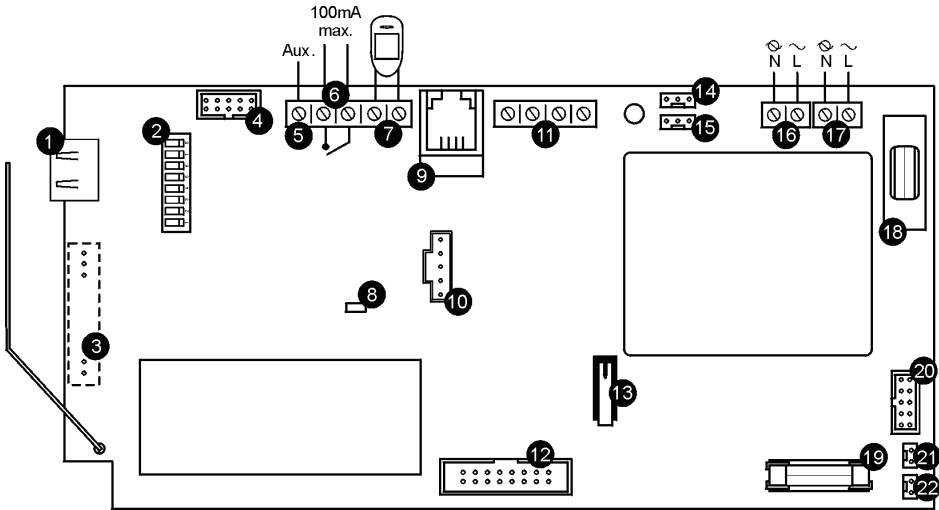


Figure 1.3: Main Board

1. USB port for connection to PC
2. DIP-switch for flash programming
3. Connector for on-board transmitter
4. Flat-cable interface connector to Ethercom module
5. Auxiliary power output (AC Operated: 10-15V, Battery Operated: 6-8V)
6. Programmable relay output (100mA max. load)
7. Hardwire zone (Zone 33)
8. Status LED
9. Interphone module connector
10. Flash programming connector for main board
11. Hardwire LCD keypad terminal block
12. Flat-cable interface connector to LCD keypad, internal speaker, internal microphone and internal siren
13. Front tamper switch
14. Interface connector to Home Automation module
15. Programming keypad connector
16. AC power terminal block
17. Home Automation module terminal block
18. AC power protection fuse
19. Backup battery protection fuse
20. Flat-cable interface connector to GSM cellular communications module
21. Backup battery connector
22. Additional backup battery connector

1.4.2: Ethercom Module

The Ethercom module provides the system with the ability to report over TCP/IP and an additional standard dialer for backup communication via the Public Switched Telephone Network (PSTN).

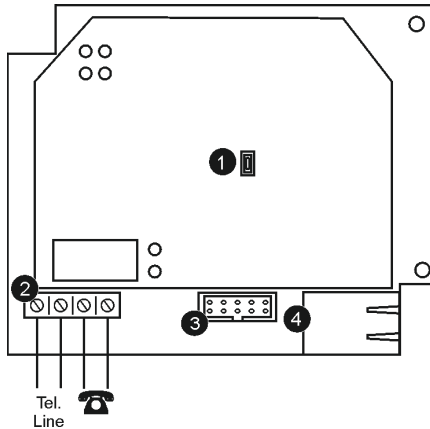


Figure 1.4: Ethercom Module

1. Reset button
2. Telephone line terminal block
3. Flat-cable interface connector to Main Board
4. RJ45 Ethernet Port

1.4.3: 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.

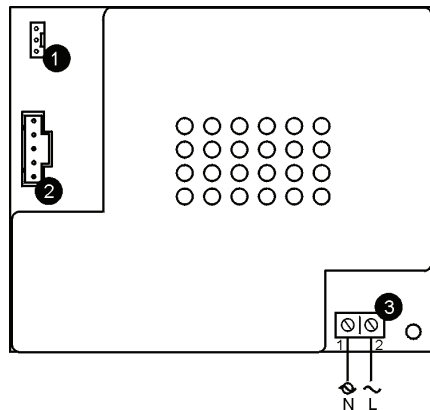


Figure 1.5: Home Automation Module

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

1.4.4: Cellular Communications Module (future option)

The Cellular Communications module enables the control panel to communicate via GSM cellular networks. This offers the ability to send or receive SMS messages, perform up/downloading and implement cellular 2-way voice applications.

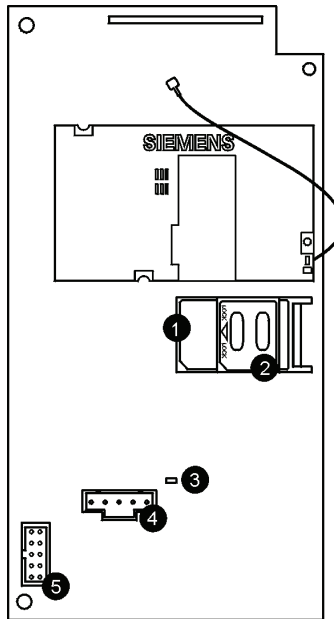


Figure 1.6: Cellular Communications Module

1. SIM card holder
2. SIM card release
3. Status LED
4. Flash programming connector
5. Flat-cable interface connector to Main Board

Chapter Two: 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 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 panel and each wireless device.

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

- Mount the control panel in a location with easy access to network, telephone and power connections.
- If installing with the GSM Cellular Communications module (future option), the control panel 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 panel.

2.1.1: Wireless Installation Guidelines

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

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

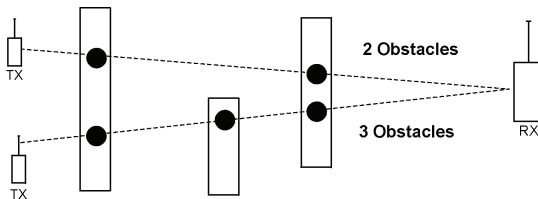


Figure 2.1: Minimizing Obstacles

- Metal based construction materials, such as steel reinforced concrete walls, wire lath plaster walls and metal foil back wallpaper, reduce the range of radio transmissions.

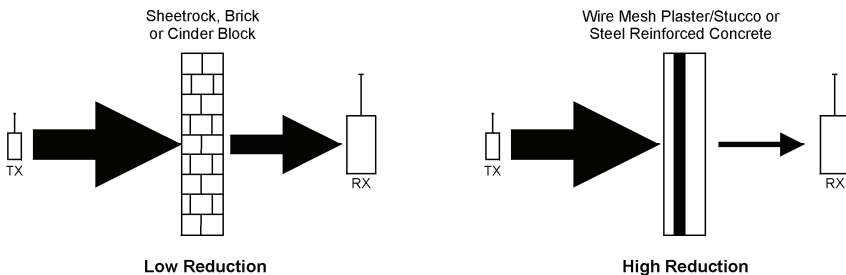


Figure 2.2: Considering Construction Materials

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

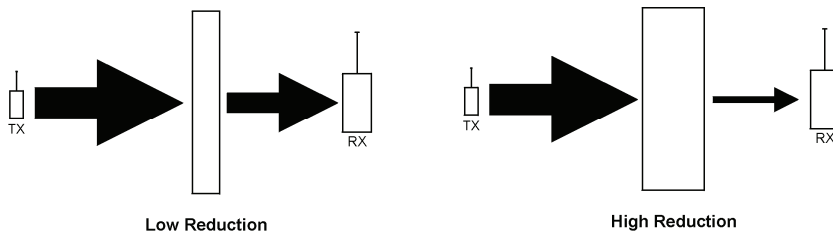


Figure 2.3: Considering Thickness of Obstacles

2.2: Installation Procedure

It is recommended that you install the system as follows:

- Unpack the kit and make certain that you have all the necessary equipment.
- Open the housing.
- Temporarily power up the system.
- Register the transmitters.
- Test the signal strength of the transmitters from the chosen location.
- Program the relevant Internet options (CP ID and Password).
- Permanently mount the control panel and transmitters.

2.2.1: Opening the Housing

To open the housing:

1. Remove the housing screw located at the bottom of the front cover.
2. Using a screwdriver carefully press the release tabs as shown in Figure 2.4.
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 keypad's flat cable.

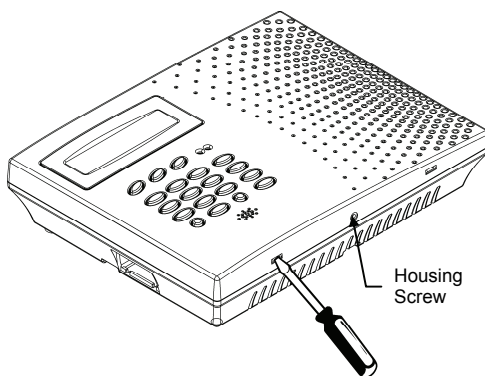


Figure 2.4: Opening the Housing

2.2.2: Powering Up the System

In order to register and test transmitters, it is necessary to temporarily power up the system before installing the control panel. At this stage, do not connect the backup battery.

Thread the power cable through the wiring hole on the back cover and connect the cable to the AC power input on the Main board. For the exact location of the AC power input, see section 1.4.1: The Main Board. Close the front cover and apply AC power.

At this stage, ignore any trouble conditions that may appear on the LCD display (e.g. Low Battery).

2.2.3: Registering Transmitters

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

To register a device:

1. Press ✓ .
2. Enter your Installer code (the default Installer code is **1111**).
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.
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 panel initiates Registration mode. During Registration mode, the system waits for two transmissions from the device.
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 panel’s LCD, press ✓ .



Pressing X returns you to the previous menu level. Press X when you are in the Main menu (Menu Level 1) to exit menu mode.

2.2.3: Testing Transmitter Signal Strength

Once all of the transmitters are registered, place them in the chosen mounting location and test the transmitter signal strength using the TX Test feature – see 4.7.6: *Transmitters for further details.*

To test transmitter signal strength.

1. Press ✓ .
2. Enter your Installer code.
3. Enter **7062** (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 panel’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.
5. After you have tested each transmitter, press X to exit TX Test mode.

2.2.4: Testing GSM Signal Strength

If installing with the GSM Cellular Communications module (future option), test the GSM signal strength using the system’s RSSI (Received Signal Strength Indication) meter. For further information, see 4.7.8: GSM Signal Strength.

To test the GSM signal strength:

1. Press ✓ .
2. Enter your Installer code.
3. Enter **708** (Service, GSM Signal); the signal strength of the cellular network is displayed.

2.2.5: Programming Internet Options

Internet settings are mostly pre-programmed in the control panel's default settings. The only settings you need to program are the control panel's ID & Password (provided by the ELAS system administrator). The following procedures explain how to program the Control Panel ID and Password. For further information regarding other Internet options and settings, see Chapter Twelve: Internet Options.

To program the control panel's ID (CPID):

1. Press ✓ .
2. Enter your Installer code.
3. Enter **95728** (Programming, Communications, Internet, ELAS, CPID).
4. Enter a six-character password using the alphanumeric keypad. The password must begin with a letter.
5. Press ✓ .

To program the control panel's password:

1. Press ✓ .
2. Enter your Installer code.
3. Enter **95729** (Programming, Communications, Internet, ELAS, Password).
4. Enter a six-character password using the alphanumeric keypad. The password must begin with a letter.
5. Press ✓ .

2.2.6: Installing the Control Panel

To install the control panel:

1. Disconnect AC power.
2. Open the housing – see 2.2.1: *Opening the Housing*.
3. Disconnect the flat cable connecting the main panel to the keypad.
4. Detach the front and back covers by unfastening the bands that connect them.
5. Remove the backup battery pack. If you want to install the control panel with back tamper, it is also necessary to remove the Main board. Figure 2.5 (below) shows the control panel with the Main board and the battery pack removed.

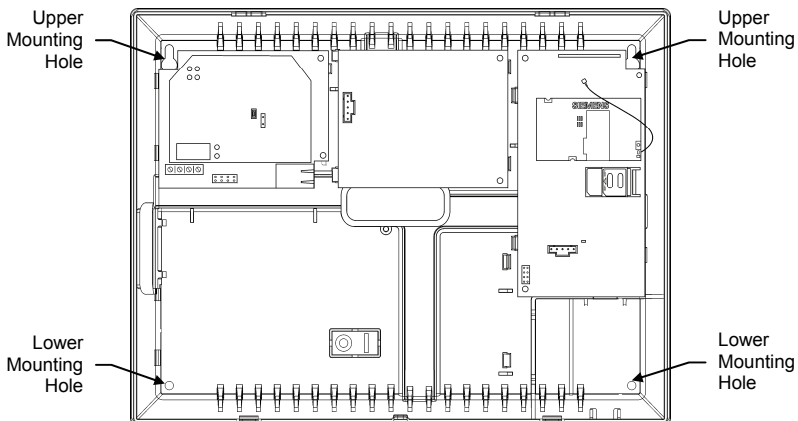


Figure 2. 5: Back Cover (Main Board and Battery Pack removed)

6. Place the control panel in position against the wall and mark the upper and lower mounting holes.
7. Install wall anchors in the appropriate positions.
8. Thread any required cables through the wiring hole on the back cover (e.g. network cable, telephone line, HA automation interface, AC power).
9. Connect the telephone line to the Telephone Line terminal block on the Ethercom module.
10. Plug the network cable into the RJ45 Ethernet Port and then into your Cable/ADSL modem or router.
11. Mount the control panel to the wall using four screws.
12. Replace the Main Board and reconnect its peripheral modules.
13. Connect the flat cables and fastening bands to the front cover.
14. 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.*

15. Connect the battery pack to the connector on the Main Board.
16. Position the front cover's top holding hooks onto the back cover and snap the front cover closed.

2.3: Back Tamper

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

The back tamper switch is located on the rear side of the control panel's Main Board and is constantly depressed by the section of the back cover shown in Figure 2.6.

For this feature to operate, you must insert a screw into the back tamper mounting hole – see section 2.2.6: *Installing the Control Panel*. When the control panel 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.

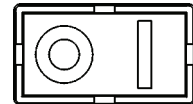


Figure 2.6: Perforated Back Tamper Release



The availability of the back tamper switch is dependent on the hardware version of the control panel.

2.4: Installing Hardwire LCD Keypads

The system supports hardwire LCD keypads that may be installed up to 300m from the control panel.

To install hardwire LCD keypads.

1. Disconnect all power, both AC and battery, from the control panel.
2. Remove the back cover of the keypad. To do so, press the two snaps (located at the bottom of the keypad) using a small flat-head screwdriver and carefully pull the back cover away from the front of the housing.

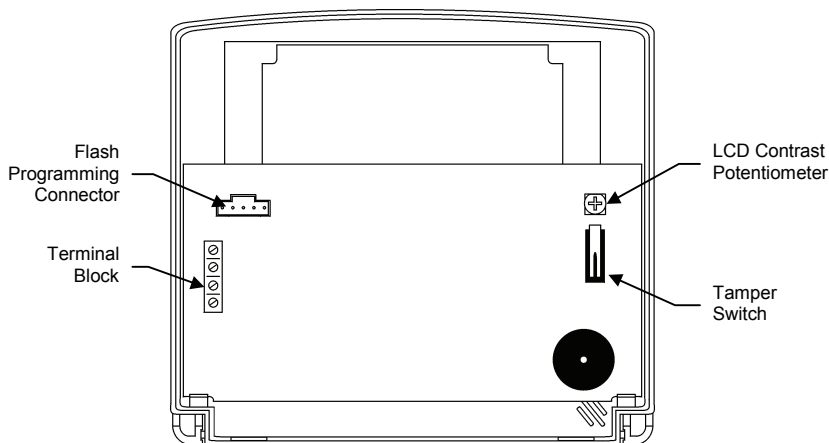


Figure 2.7: Hardwire LCD Keypad (back cover off)

3. Place the back cover of the keypad in position against the wall and mark the upper and lower mounting holes.
4. Install wall anchors in the appropriate positions.
5. Thread the cable from the control panel through the wiring hole on the back cover and attach the back cover to the wall using four screws.
6. Connect the terminal block on the keypad to the appropriate terminal block on the control panel's main board as shown in Figure 2.8.

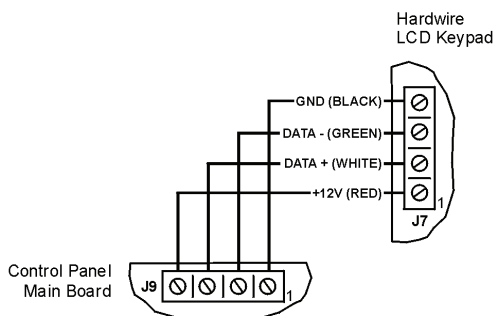


Figure 2.8: Connections for Hardwire LCD Keypad

7. Reapply power to the control panel.
8. Set the keypad address as follows:
 - a. Make certain the keypad's tamper switch is open.
 - b. On the keypad, press keys 1, 3 and 5 simultaneously.
 - c. Use the arrow keys (\blacktriangle / \blacktriangledown) to select the keypad address.
 - d. Press \checkmark .
9. Position the front cover's top holding hooks onto the back cover and snap the front cover closed.
10. After installing hardwire keypads, perform the Find Modules function – see 14.5: *Find Modules*.

2.5: Ethercom Startup Sequence

After you have installed and powered up the system, the Ethercom startup sequence is initiated. During this sequence, the Ethercom module receives the parameters programmed in the control panel's Internet Communication options – see *Chapter Twelve: Internet Options*. After the startup sequence is complete, the Ethercom attempts to connect to the ELAS remote server. The following table explains the messages that are displayed on the LCD during this sequence.

This...	Means...
EC STATE STARTING UP	The Ethercom module is receiving parameters from the control panel.
EC STATE CONNECTING ELAS	The Ethercom module is attempting to connect to the ELAS. When a successful connection is established, this message disappears.

Table 3.4: Ethercom Startup Display

If the Ethercom is having difficulty connecting to the ELAS, the message **Connecting ELAS** continues to be displayed. In this case, check that the control panel's Internet Options are correctly programmed – see *Chapter Twelve: Internet Options*. If you still experience problems, the IP Status utility in the Service menu may help in diagnosing the problem – see 4.7.12: *IP Status*.

2.6: Installing IP Cameras

IP cameras installed on the protected site may be accessed by the user via the Web Application – see 5.2: *Web Application Interface*.

For a list of supported IP cameras, please contact your distributor.

To enable video monitoring using IP cameras, the following steps are required:

- Port forwarding must be configured on the router to allow the user outside access to the IP camera.
- An administrator must enter the camera's IP address and port in the control panel's record in the ELAS database.

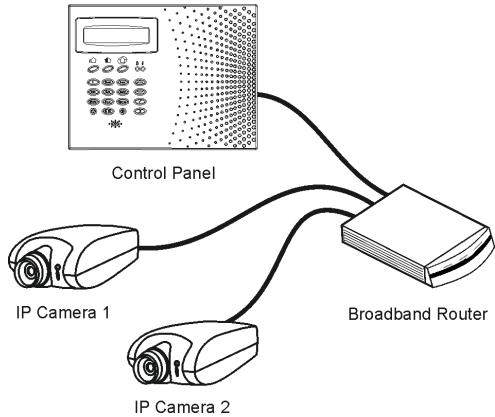


Figure 2.9: Typical IP Camera Installation

2.6.1: Port Forwarding

The Broadband Router has an IP address that allows data to be sent and received over the Internet. The IP address is divided into ports. These ports are effectively the path through which the data is sent or received allowing multiple tasks to be performed simultaneously via the router.

When a few IP network devices are connected to the router, to ensure a connection to the correct device you must configure the router's "Port Forwarding" options. This allows data has reached the router (with an external IP address) to reach its required destination on the internal network (i.e. behind the router).

2.6.2: IP Camera Installation

The following section describes the procedure for installing an IP camera. The exact procedure may differ according to the router and camera used. Nevertheless, the instructions below shall provide you with general guidelines that are common in most applications.

To install an IP camera:

1. Connect the camera's Ethernet port to the router.
2. Connect the camera to the power supply via the camera's power jack; the camera waits to automatically receive an internal IP address. When the camera receives an IP address, the camera indicates that it has connected (for example, a green flashing LED – refer to the camera manufacturer's installation instructions for further details).
3. Install the software provided with the IP camera on the PC that you are going to use to configure the camera settings.
4. Use the installation software to search for the IP camera on the LAN, if the search is successful, you will be able to determine the camera's IP address. Write down the camera's IP address for reference purposes - *you will need the camera's IP address when configuring the router.*
5. To access the camera's configuration interface, open your Internet browser, enter the IP address of the camera in the address bar and press Enter.
6. On the camera's security settings page, program a user name and password. When the user wants to access the camera from the *infinite Broadband Web Application*, they need to enter their user name and password for authentication purposes.

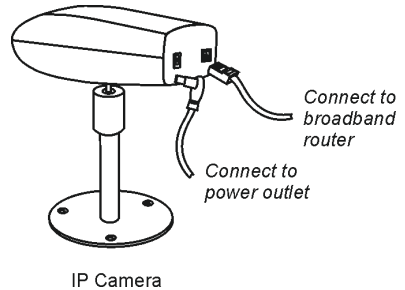
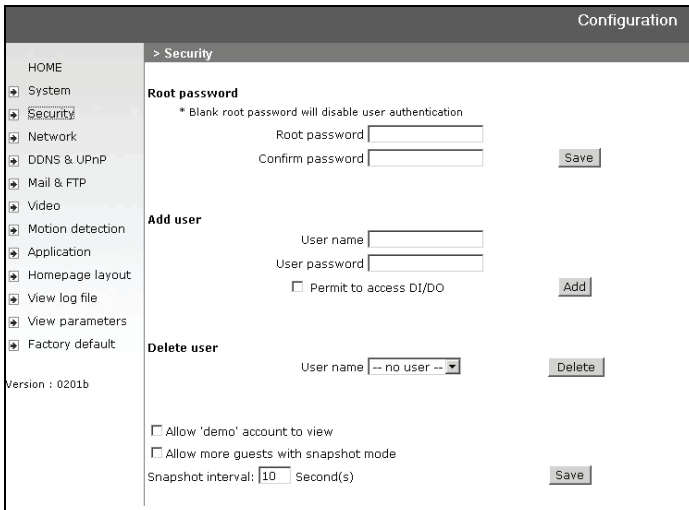


Figure 2.10: Connecting the IP Camera



The screenshot shows the 'Configuration' interface of an IP camera, specifically the 'Security' settings page. The left sidebar contains a navigation menu with options: HOME, System, Security (selected), Network, DDNS & UPnP, Mail & FTP, Video, Motion detection, Application, Homepage layout, View log file, View parameters, and Factory default. The main content area is titled '> Security' and includes the following sections:

- Root password:** A note states '* Blank root password will disable user authentication'. Below are input fields for 'Root password' and 'Confirm password', followed by a 'Save' button.
- Add user:** Input fields for 'User name' and 'User password', a checkbox for 'Permit to access DI/DO', and an 'Add' button.
- Delete user:** A dropdown menu for 'User name' (currently showing '-- no user --') and a 'Delete' button.
- At the bottom, there are checkboxes for 'Allow 'demo' account to view' and 'Allow more guests with snapshot mode', and a 'Snapshot interval' set to '10' seconds with a 'Save' button.

Figure 2.11: Example of IP Camera Security Settings Page

- On the camera's network configuration settings page, edit the settings for the ports that the IP camera uses during operation. The number of ports that the camera requires differs according to the camera used.

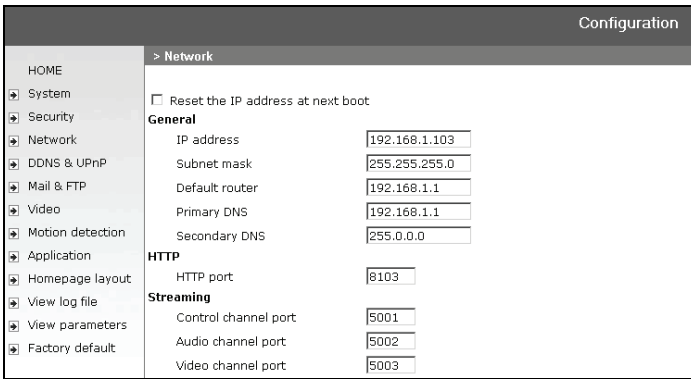
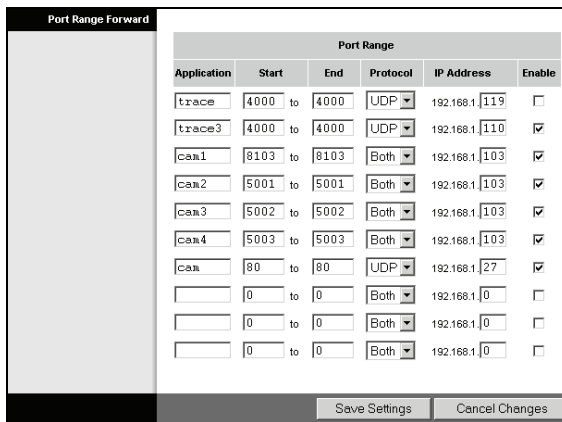


Figure 2.12: Example of IP Camera Network Settings Page

In most cases, the ports that are required by the IP camera are pre-configured as default. If you are installing one IP camera, you do not usually have to edit these settings (unless there is another network device using the same ports). However, if you are installing more than one camera, it is necessary to choose different ports for each camera.

- Using the router's configuration interface, edit the port forwarding setup – *further information refer to the manufacturer's instructions supplied with the router.* The port forwarding setup allows you to create “rules” that the router uses for port forwarding – *for further details see 2.6.1: Port Forwarding.*



Port Range Forward						
Port Range						
Application	Start	End	Protocol	IP Address	IP Address	Enable
trace	4000	to 4000	UDP	192.168.1	119	<input type="checkbox"/>
trace3	4000	to 4000	UDP	192.168.1	110	<input checked="" type="checkbox"/>
cam1	8103	to 8103	Both	192.168.1	103	<input checked="" type="checkbox"/>
cam2	5001	to 5001	Both	192.168.1	103	<input checked="" type="checkbox"/>
cam3	5002	to 5002	Both	192.168.1	103	<input checked="" type="checkbox"/>
cam4	5003	to 5003	Both	192.168.1	103	<input checked="" type="checkbox"/>
cam	80	to 80	UDP	192.168.1	27	<input checked="" type="checkbox"/>
	0	to 0	Both	192.168.1	0	<input type="checkbox"/>
	0	to 0	Both	192.168.1	0	<input type="checkbox"/>
	0	to 0	Both	192.168.1	0	<input type="checkbox"/>

Figure 2.12: Example of Router Port Forwarding Configuration Page

Configure port forwarding rules using the following guidelines:

- Create a separate rule for each port that is used by each camera.
- In the “Start” and “End” fields (sometimes labeled “Private” and “Public”), enter the same port number in both fields. For example, if the HTTP Port is 8103, enter “8103” in both fields.
- Select the Protocol as “Both” (i.e. use both UDP and TCP protocols).
- Enter the IP address that was automatically allocated to the IP camera – *see step 4 of this procedure.*

For further information on how to install an IP camera and configure the router, refer to the manufacturer’s instructions that are supplied with both products.

Chapter Three: Basic System Operation

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 on the front panel.

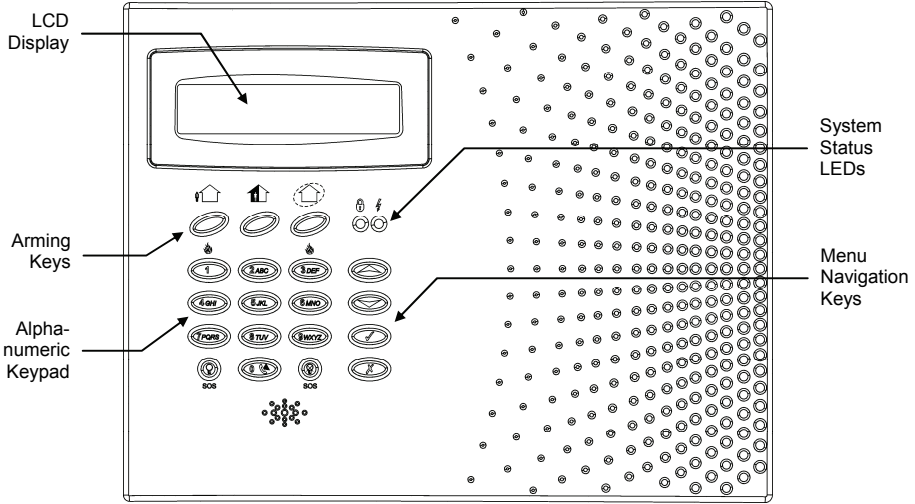


Figure 3.1: Front Panel

3.2: System Status LEDs

The two LEDs, Armed and Power, provide essential information on system status.

If the Armed LED is...	It means...
Off	The system is disarmed.
On	The system is armed.
Flashing	An alarm has occurred. Alarm indication is cleared the next time that an arming sequence is initiated or after the relevant event has been viewed in the event log.

Table 3.1: Armed LED Indication



Alarm indication is not displayed after a silent panic alarm.

If the Power LED is...	It means...
Off	Both AC and Battery power are disconnected.
On	System Power is OK.
Flashing (slow)	Backup battery low or low battery from transmitters.
Flashing (fast)	AC loss.

Table 3.2: Power LED Indication



In the event of AC loss and battery low, the green LED indicates the AC loss condition.

3.3: Alphanumeric 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, the keypad offers a number of special functions. These functions are listed in the following table.

Key	Special function
1	Used to enter symbols in descriptor editing.
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.
💡	Used to switch Home Automation units on. In descriptor editing, used to insert a space before the current character. In phone number editing, used to enter “*”, “T”, “,”, “P”, “+” 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.
⊗💡	Used to switch Home Automation units off. In descriptor and phone number editing, used to delete the current character.
⬆	Used to scroll backwards in the current menu level
⬇	Used to scroll forwards in the current menu level. During standby, used to scroll through the list of system trouble conditions.

Table 3.3: Keypad Functions

3.4: LCD Display

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

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.



Figure 3.2: Typical Standby Display

This...	Means...
DISARMED	The system is disarmed.
FULL ARMED	The system has been armed using the displayed arming method.
PART ARMED	
PERIMETER ARMED	
FULL ARMING	The system is in the process of arming (displayed during exit delay).
PART ARMING	
PERIMETER ARMING	

Table 3.4: Armed Status

This...	Means...
ZONES IN ALARM	Zones have been violated.
TAMPER ALARM	The system has been tampered with.
EXIT NOW 056	The exit delay is counting down (56 seconds remaining).
DISARM NOW 011	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.

Table 3.5: System Status

3.4.2: System Trouble Tones

In the event of system trouble, the *infinite Broadband* 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 9.4.1: 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 9.4.2: Telephone Trouble Tones.

3.5: Arming/Disarming

The following section explains how to arm and disarm the control panel using the LCD keypad.

The *infinite Broadband* offers three arming modes that you can define to suit the application. Figure 3.3 illustrates the three arming modes. In each diagram, the protected area is shaded.

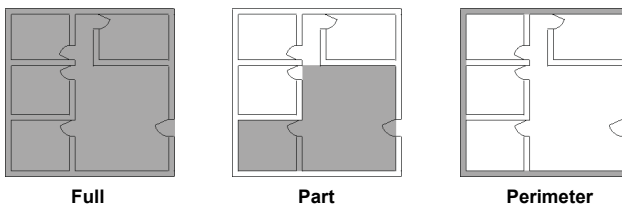


Figure 3.3: Arming Modes

The arming options are entirely flexible. You can program each sensor to be included in any combination of the three arming modes – see section 8.6.2: Arm Set. Additionally, each arming mode has a separate exit and entry delay.

The arming functions are only available while the system is in Standby mode.

3.5.1: Arming Keys

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

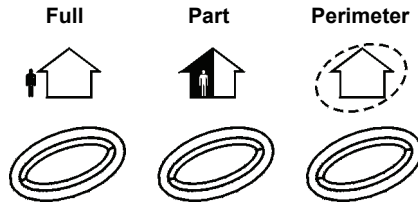


Figure 3.4: Arming Keys

3.5.2: Full Arming

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

To fully arm the system:

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.

3.5.3: 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:

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.

3.5.4: 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:

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.

3.5.5: Combination Arming

The system allows you to activate a combination of two arming modes. 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 during the exit delay of the first arming mode. If the first exit delay expires, you cannot activate a second arming mode.

To arm the system using two arming modes:

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 sensor was tripped first. For example, if the sensor is included in Full arming, the entry delay for Full arming counts down – see 8.6.2: *Arm Set*. If the sensor 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.

3.5.6: 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 section 10.3: *Forced Arm*.
- The sensor that is causing the System Not Ready condition is Forced Arm enabled – see section 8.6.5: *Force Arm*.

3.5.7: Disarming

When a sensor is tripped, the entry delay counts down; each arming method has its own entry delay.

To disarm the system:

- Enter a valid user code.

3.6: Remote Arming/Disarming via SMS

You can arm and disarm the system remotely by sending the SMS commands from a cellular phone to the optional cellular communications module.

Each SMS command contains the following elements:

- ① SMS Command Descriptor (up to 43 characters of free text)
- ② # (delimiter – separates the descriptor from the actual command)
- ③ User Code (4 digits)
- ④ Command (120=Disarm, 121=Full Arm, 122=Part Arm, 123=Perimeter Arm, 124=Full + Perimeter Arm, 125=Part + Perimeter Arm)

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

①					②	③				④					
F	u	i	i		A	r	m	#	1	2	3	4	1	2	0



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

3.7: Front Panel Alarm Activation

In the event of an emergency, the user can generate two kinds of alarm from the front panel.

To activate an SOS alarm:

- Press both Home Automation keys simultaneously.

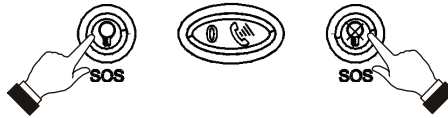


Figure 3.5: SOS Alarm Activation

To activate a Fire alarm:

- Press keys 1 and 3 simultaneously.

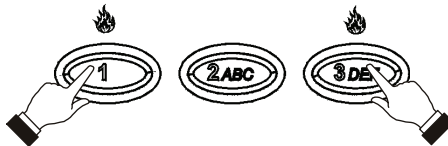


Figure 3.6: Fire Alarm Activation

To activate a Medical alarm:

- Press keys 4 and 6 simultaneously.



Figure 3.7: Medical Alarm Activation

Chapter Four: 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

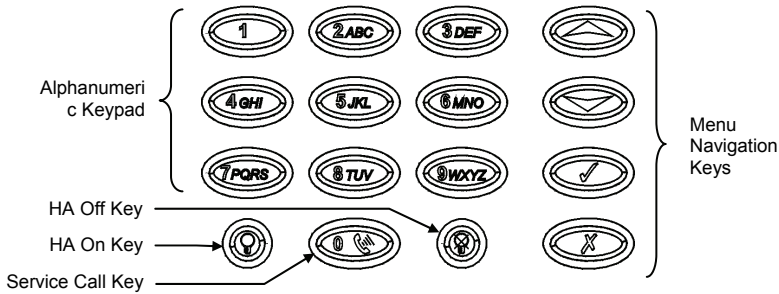


Figure 4.1: On-board Keypad Layout

The LCD keypad's 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 menu navigation keys (▲/▼) and make simple yes/no decisions using the ✓ and X keys.

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

1. Press ✓ to enter Menu mode.
2. Enter an authorized user code; the first menu item, **1. Stop Comm.**, is displayed.
3. Press ▼ until **7. Service** is displayed.
4. Press ✓ to enter the Service menu.
5. Press ▼ until **4. Speaker Test** is displayed.
6. Press ✓ to choose the displayed function.

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.



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.

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: Stop Communications

To stop communications:

- From the main menu, select Stop Com. [1]; all pending messages are canceled.

4.3: Sensor Bypassing/Unbypassing

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

To bypass or unbypass a sensor:

1. From the Bypass Zones menu, select Bypass/Unbyp. [21].
2. Using the arrow keys, scroll to the sensor 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 sensors:

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



All bypassed zones will be automatically unbypassed when the system is disarmed. Zones defined as "Fire" cannot be bypassed.

4.4: User Codes

The control panel 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.

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 panel 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 panel notifies the central station with an Arm/Disarm event message .

Codes 20-25: Non-controlled Codes

Non-controlled codes do not cause the panel to send Arm/Disarm event messages to the central station. The panel 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: User TWA Code

The User TWA code is designed to enable the user to establish Two-Way Audio communication with the control panel at any time from a remote location telephone. This code can only be used for this specific purpose and does not grant access to any additional system functions such as disarming.

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 panel 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.



The use of codes 29 and 30 require system support for PSTN or GSM communication (GSM communication is a future option that is not currently available).

Code 31: Guard Code (for future use)

The Guard Code is a future option that is not available in the current firmware.

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: Modifying User Codes

To modify a user code:

1. From the main menu select, User Codes [4].
2. Select the code you want to modify.
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. Modify 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 panel sounds an error tone and the new code is not accepted.

Codes 1-29 can be modified only by the Master code. The Installer code, Guard code and the Central Station TWA code can be modified only by the installer.

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.

To modify 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. Modify the descriptor using the alphanumeric keypad.
5. Press ✓ when you have finished the entry.

4.5: Follow Me

The Follow Me feature is designed to notify the user that certain events have occurred. This notification can be an SMS text message or Two-Way Audio connection over PSTN. Additional Follow Me notification may be sent to the email addresses programmed using the Web Access application.

To edit the Follow Me number:

1. From the main menu, select Follow Me [5].
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 256 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.

Figure 4.2 shows the event log entry for a burglary alarm at 11:34am on November 14th 2004. The event was successfully reported to the central station.

The event log displays the following information for each event:

- ① The Event – a brief description of the event that occurred.
- ② Default descriptor – the zone, device or user number (where applicable).
- ③ Time/date stamp – the exact time and date that the event occurred.
- ④ 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 or **N**: No Report.
- ⑤ Descriptor – the zone, device or user descriptor (where applicable).

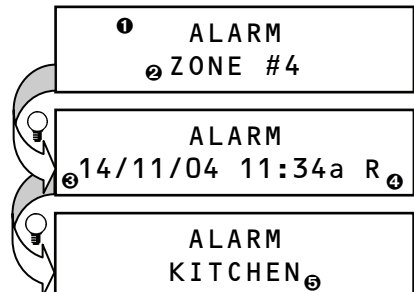


Figure 4.2: Event Log Display

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.

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.



For certain versions of the infinite Broadband 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 system effectively.

TO THE INSTALLER

Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system.

The installer should assume the responsibility of developing and offering a regular maintenance program to the user as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts. Recommendations must be included for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

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 10.14: Time/Date Format. If you are setting the time in 12hr format, use the ♀ key to toggle between AM and PM.

4.7.2: External Siren Test

To test the external siren:

- From the Service menu, select Ext. Siren Test [702]; the external siren is sounded briefly.

4.7.3: Internal Siren Test

To test the internal siren:

- From the Service menu, select Int. Siren Test [703]; the internal siren is sounded briefly.

4.7.4: Speaker Test

To perform a Speaker test:

- From the Service menu, select Speaker Test [704]; a short sequence of chimes are sounded from the speaker.

4.7.5: Walk Test

To initiate Walk Test mode:

1. From the Service menu, select Walk Test [705]; a list of registered sensors appears.
2. Trigger each sensor; when the system receives a successful transmission from a sensor, the sensor is removed from the list.
3. When all the sensors are removed from the list, **End Walk Test** is displayed.
4. Press **X** to exit Walk Test mode.

4.7.6: Transmitters

The Transmitters menu offers two choices that serve as valuable aids during installation. The first choice, 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 [7061]; 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 transmitter's descriptor.
- The signal strength of the last received transmission.
- An abbreviation indicating the last received status of the transmitter – see *Table 4.1*.



- ❶ Descriptor
- ❷ Signal Strength
- ❸ Status

Figure 4.3: TX List Display

This...	Means...
OK	The transmitter is functioning correctly
TA	Tamper condition
BT	Battery low
OS	The transmitter is out of synchronization
NA	The transmitter is non-functional – see section 7.4: Supervision Time

Table 4.1: Transmitter Status Abbreviations



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.

The second utility, 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 are sounded indicating the transmitter's signal strength – see *Table 4.2*. This feature helps you to determine the best location to install a transmitter.

Signal Strength	Tones
0-2	1 Tone
3-5	2 Tones
6-8	3 Tones
8-9	4 Tones

Table 4.2: Signal Strength Tones

To initiate TX Test mode:

1. From the Service menu, select Transmitters, TX Test [7062].
2. Activate a transmitter; the transmitter's details are displayed.
3. When you have finished, press **X** to exit TX Test mode.

4.7.7: Audio Volume

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

1. Establish a two-way audio connection.
2. From the Service menu, select Audio Volume [707].
3. Adjust the setting according to the following table.

Press...	To...
1	Increase microphone sensitivity
4	Reduce microphone sensitivity
3	Increase speaker volume
6	Reduce speaker volume

Table 4.3: Voice Level Adjustment

4. Press **✓**; the new settings are stored in the memory.

4.7.8: GSM Signal Strength

You can measure the GSM signal strength using the system's RSSI (Received Signal Strength Indication) meter. This function enables you to calculate the optimal location to install the control panel with the Cellular Communications module (future option).

To view the GSM signal strength reading:

- From the Service menu, select GSM Signal [708]; the signal strength of the cellular network is displayed.

This Reading...	Means...
8 to 9	The location is good
5 to 7	The location is acceptable
Less than 5	Unacceptable – <i>choose another location!</i>

Table 4.4: GSM Signal Strength

4.7.9: Display Version

To display the system's software and hardware versions.

- From the Service menu, select Version [709]; the hardware (HW) and software (SW) versions are displayed.

4.7.10: Enable Remote Programming

The system offers various remote programming access options that are explained in section 11.3.4: RP Access Options. If “User Initiated” RP access is selected, communication may be established only if the user manually enables remote programming.

To manually enable remote programming.

- From the Service menu, select Enable RP [710]; a 30-minute time window is opened during which RP communication may be established.

4.7.11: Global Chime

The Chime feature causes the internal 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 8.6.4: Chime.

To enable or disable Global Chime:

1. From the Service menu, select Global Chime [7 11].
2. Select either Enable or Disable.
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 ▼.

4.7.12: IP Status

The IP Status sub-menu includes various tests that enable you to check the status of the LAN connection.

To perform an IP Status test:

1. From the Service menu, select IP Status [712]; the first test, IP Parameters, is displayed.
2. Press ✓ to perform an IP Parameters test.
3. Press ✓ to run the next test in the IP Status menu or X to exit.

The tests included in the IP Status sub-menu are as follows:

- IP Parameters [71201]
- ELAS Parameters [71202]
- DHCP [71203]
- Network [71204]
- Authentication [71205]
- ELAS [71206] – *future availability*
- “I’m alive” [71207]
- Last ELAS Task [71208]
- Last Event Reported [71209]
- Security [71210] – *future availability*

The following table explains problems that may be the cause of an IP Status test failure.

Test	Failure message	Possible cause
IP Parameters	BAD	Problem with IP parameters – check that all Ethercom settings are correctly programmed (see 12.1: Ethercom)
ELAS Parameters	BAD	Problem with ELAS parameters – check that all ELAS settings are correctly programmed (see 12.2: ELAS)
DHCP	FAILED	Failure to connect to DHCP server – check DHCP settings (see 12.1.1: DHCP Server).
Network	TROUBLE	Problem with the network connection – check that the network cable is connected or replace the cable.
Authentication	FAILED	Authentication failed when the control panel attempted to connect to the ELAS – check the Control Panel ID and Control Panel Password (see 12.2.6: Control Panel ID and 12.2.7: Control Panel Password)
I'm Alive	FAILED	Temporary problem experienced when connecting to the ELAS.
Last ELAS Task	FAILED	Temporary problem experienced when connecting to the ELAS.
Last Event Reported	FAILED	Temporary problem experienced when connecting to the ELAS.

Table 4.5: Possible Causes for IP Status Test Failure

Chapter Five: Web Access

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.

5.1: Logging In

This application is usually part of the service provider's Web site and requires the end user to log in order to gain access to the page.



A horizontal form with four input fields: 'Username:', 'Password:', 'Pass Code:', and 'ENTER'. Each field is a simple rectangular box.

Figure 5.1: Log In Fields

To log in to the Web Application:

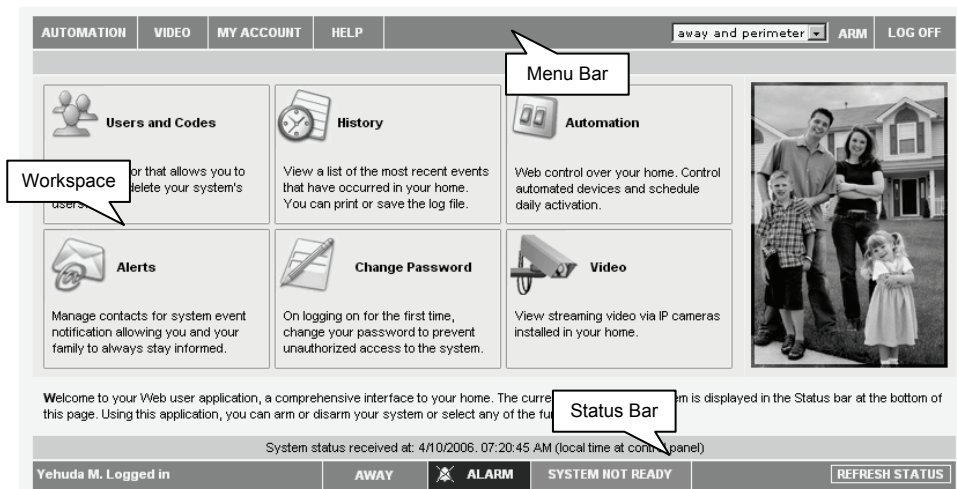
1. Enter a user name, password and the control panel's Master user code. The user name and password, that is entered here, is provided by the service provider.
2. Click Enter.



When logging in for the first time, you should change the password. You can do so from the Change Password page that is accessible from the My Account menu. Your new password should be no less than six characters and must start with a letter.

5.2: Web Application Interface

After logging in, the system's home page is displayed. The following screen shot shows the home page and explains the main elements of the web application's interface.



The screenshot shows a web application interface with a dark grey header. The header contains navigation tabs: 'AUTOMATION', 'VIDEO', 'MY ACCOUNT', and 'HELP'. On the right side of the header, there is a dropdown menu showing 'away and perimeter', and buttons for 'ARM' and 'LOG OFF'. Below the header is a main content area with a grid of six tiles. Each tile has an icon and a title: 'Users and Codes' (with a group of people icon), 'History' (with a clock icon), 'Automation' (with a remote control icon), 'Alerts' (with an envelope icon), 'Change Password' (with a pencil icon), and 'Video' (with a camera icon). Each tile contains a brief description of its function. To the right of the grid is a large photograph of a family (a man, a woman, and two children) standing in front of a house. Below the grid is a 'Workspace' section with a paragraph of text. At the bottom of the page is a 'Status Bar' with a dark background and white text. The status bar displays 'Yehuda M. Logged in', 'AWAY', 'ALARM' (with a siren icon), 'SYSTEM NOT READY', and a 'REFRESH STATUS' button. A 'Menu Bar' callout points to the header area, and a 'Status Bar' callout points to the bottom status bar.

Figure 5.2: Banner and Status Display

5.2.1: Menu Bar

The Menu Bar includes the Main Menu, arm/disarm options and the “Log Off” button. The Main Menu offers links to various pages in the Web Application.

The following options are available:

- 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.

5.2.2: Workspace

The workspace is where the various pages of the application are displayed. For example, if you choose Automation from the Main Menu, a list of automated appliances is displayed in the workspace. After logging in, the workspace provides convenient links to some of the more popular features.

5.2.3: Status Bar

The Status bar displays information on the system’s status and the name of the user currently logged in. Above the status bar, the time that the system status display was last updated is shown. This information is displayed according to the local time at the control panel. To receive the current system status, click the Refresh Status button on the right-hand side of the Status bar.

For further information on how to use the Web Application, refer to the Help menu included in the application.

Chapter Six: Two-Way Audio

The *infinite Broadband* control panel offers a range of Two-Way Audio features that can be used for applications such as alarm verification and assistance in the event of an emergency. This chapter explains these features, their operation procedures and programmable options.

Two-Way Audio communication can be separated into two fundamental groups; incoming and outgoing calls. These groups differ in their associated audio features.

6.1: Incoming Calls

The control panel 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 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 Two-Way Audio features to function, Incoming TWA must be enabled in the Communication Options section of the Programming menu.

6.1.1: User Code Verification

To prevent unauthorized attempts to connect with the control panel, there are two user codes designed for use with the Two-Way Audio feature. The User TWA code enables the user to establish Two-Way Audio communication at any time. The Central Station TWA Code is only valid for a ten-minute period following an alarm.

6.1.2: Incoming Calls via PSTN

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

To connect to the control panel using the double call method:

1. Dial the telephone number of the line connected to the control panel.
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 panel picks up and sounds two DTMF tones.

6.1.3: Incoming Calls via a GSM Cellular Network

The Cellular Communications Module (future option) 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 panel directly.

6.1.4: Two-Way Audio Call Procedure

The following procedure explains how to make a Two-Way Audio call. The conditions and procedure differ when using POTS or Cellular communication. For further information, read sections 6.1.1, 6.1.2. and 6.1.3 above.

To make a Two-Way Audio call:

1. Call the control panel either using the double call method (PSTN) or directly (Cellular); when the control panel picks up, two DTMF tones are sounded.
2. Enter the User TWA or Central Station TWA code 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 11.7.4: 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 TWA 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.

6.2: Outgoing Calls

The *infinite Broadband* control panel can make Two-Way Audio calls to the user or central station in the event of an alarm. This feature is designed for applications such as alarm verification, panic and personal emergency.

6.2.1: Service Call

The Service Call feature enables the user to establish a two-way audio connection with the security service provider (if this function is supported by the service provider). For further information on how to program this feature, see section



Figure 6.1:
Service Call Key



When using the Web RP application to program the system, you can always access the control panel in order to view programming parameters regardless of the RP Access options detailed above. However, if you wish to download any programming parameter modifications to the control panel, this action is limited by the RP Access option.

11.4: Service Call.

To initiate a Service Call:

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

If the TWA mode is defined as “Simplex” (see 11.7.4: 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

6.2.2: TWA Alarm Reporting

In the event of an alarm, the control panel is able to report the events and then stay on the line after ACK 2 (Kiss-Off) is received. 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 panel stays on the line and opens the audio channel.
3. If the TWA mode is defined as “Simplex” (see 11.7.4: 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 call is terminated by the expiration of the TWA Timeout.

If multiple events are sent, the control panel 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.

6.2.3: 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 panel dials the user’s telephone number and sounds two DTMF tones when you pick up the call.
3. Press any key on the telephone; the control panel opens the audio channel.



If you press 9 to answer the call, the control panel simultaneously cancels the siren when opening the audio channel.

4. If the TWA mode is defined as “Simplex”, (see 11.7.4: 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 TWA 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.

6.3: Siren Silencing

The siren is silenced during Two-Way Audio communication subsequent to an alarm. At the end of the call, the siren is re-activated (if the Siren Cut-Off has not yet expired). You can cancel the re-activation of the siren by pressing “9” on your telephone during the call.

Chapter Seven: Home Automation Control

The purpose of this chapter is to explain the various methods used to control X10 Home Automation (HA) units installed around the home or business. These devices are programmable switches that can be used to perform a variety of functions, such as: lighting on/off control and appliance on/off control. The control panel supports a total of 16 output devices.

For further information on the X10 protocol and the choice of options that are available in programming, see Chapter Thirteen: Home Automation Programming.

7.1: Keypad Control

Using either the LCD or the wireless keypad, you can control HA units with the dedicated Home Automation keys – see *Figure 7.1*.

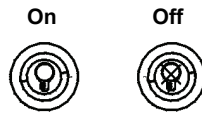


Figure 7.1: LCD Keypad Home Automation Keys

To control HA units via the 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); the command is sent to the HA unit

7.2: Keyfob Control

You can control up to two different HA units using any of the four button keyfobs registered to the system. For further information on how to assign keyfob buttons to HA units, see section 8.7.2: Button Assignment.

7.3: SMS Control (*future availability*)

You can send On and Off commands to HA units using SMS messages sent from a cellular phone to the cellular communications module. For this feature to function correctly, SMS control must be enabled for the specific HA units you want to control – see section 13.2.6: SMS Control.

7.3.1: SMS Command Format

Each SMS command contains the following elements:

- ① SMS Command Descriptor (up to 43 characters of free text)
- ② # (delimiter – separates the descriptor from the actual command)
- ③ User Code (4 digits)
- ④ Command (0=Off, 1=On)
- ⑤ Device Number (HA Units: 01-16)

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

①							②	③				④	⑤			
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.

7.3.2: SMS Confirmation Message Format

After an SMS command is executed by the system, a message is returned to the sender – see 13.4: *SMS Confirmation*. This message includes the HA unit’s descriptor and the command that was sent.

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
---	---	---	---	---	---	---	---	---

7.4: Scheduling

Scheduling allows you to program the panel 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.

7.4.1: On Time

To edit an HA unit’s “On” Time:

1. From the main menu, select HA Schedules [8].
2. Select an HA unit.
3. From the X10 unit’s sub-menu, select On Time [#1].
4. Enter a time (HH:MM).
5. Press ✓ when the desired setting is displayed.

7.4.2: Off Time

To edit an HA unit’s “Off” Time:

1. From the main menu, select HA Schedules [8].
2. Select an HA unit.
3. From the HA unit’s sub-menu, select Off Time [#2].
4. Enter a time (HH:MM).
5. Press ✓ when the desired setting is displayed.

7.4.3: 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 an 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.

Press...	To toggle...
1	Sunday
2	Monday
3	Tuesday
4	Wednesday
5	Thursday
6	Friday
7	Saturday

Table 7.1: Weekly Schedule

5. Press ✓ when the desired setting is displayed.

Chapter Eight: Devices

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

8.1: Device Registration

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 sensors connected to Zone 33.

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 sensor 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 required location, the system will not initiate Registration mode. If the device has already been registered at another location, attempts to register are ignored by the system

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.

8.2: Device Descriptors

You can assign a 16-character descriptor to each device except the siren. 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. Select the specific device you wish to edit.
4. From the device's sub-menu, select Descriptor.
5. Edit the descriptor using the alphanumeric keypad.
6. Press **✓** when you have finished editing.

8.3: Device Deletion

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

To delete a device:

1. From the Programming menu, select Devices, [91].
2. Select a device type.
3. Select the exact device you want to delete
4. From the device's sub-menu, select Delete.
5. Press ✓ to confirm; the device is deleted.

8.4: Supervision Time

The sensors in Electronics Line 3000's supervised wireless range send a supervision signal approximately one hour after its last transmission. If the system does not receive supervision signals from a specific transmitter, the transmitter is regarded as having a supervision failure and requires service. The amount of time after which a transmitter is considered as having a supervision failure 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 [9161].
2. Enter the Inactive Time between 4:00 and 23:59 hours.



It is recommended that the system be set for the maximum time period to minimize occurrences of false supervision failure indications.

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

1. From the Programming menu, select Devices, Superv. Time, Fire [9162].
2. Enter a supervision time between 02:00 and 23:59 hours.

8.5: Re-Synchronization

Transmissions whose encrypted codes are out of synchronization are rejected by the system. This can happen because of the unique encrypted transmission method used should an attempt be made to compromise the system. For example, it is not possible to arm or disarm the system using a keyfob that is out of synchronization. In the event that a transmitter's coded message is out of synchronization, it is possible to re-synchronize the transmitter and restore normal operation.

To re-synchronize transmitters:

1. From the Programming menu, select Devices, TX Re-synch [917]; a 10-minute time window is opened.
2. During the 10-minute time window, if a transmission is received that is out of synchronization, the transmitter is re-synchronized.

8.6: Zones

The *infinite Broadband* includes 33 security zones. Zones 1-32 are intended for wireless sensors. One sensor can be registered to each wireless zone. The system supports Electronics Line's supervised wireless range of transmitters that includes various PIR sensors, magnets, glass break sensors, and flood detectors. All these transmitters send supervision signals to the panel's receiver in order to indicate that the transmitter is functional.

Zone 33 is an on-board hardware zone. This zone is programmed in the same way as the wireless zones with the exception of registration and deletion.

This section explains the sections of programming exclusive to sensors. For information on registration, descriptor editing and deletion, see sections 8.1, 8.2 and 8.3, respectively.

8.6.1: Zone Type

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

To program a zone type:

1. From the Programming menu, select Devices, Zones [911].
2. Select the sensor you want to program.
3. From the sensor's sub-menu, select Zone Type [#02].
4. Select a zone type from Table 8.1.

Zone Type	Description
Normal	When the system is armed, this zone instantly generates a burglary alarm when triggered.
Entry/Exit	When the system is armed, this zone initiates the entry delay when triggered. If the system is not disarmed by the time the entry delay expires, a burglary alarm is generated.
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 a burglary alarm if the entry delay is not active.
Panic	Panic zones are always active, regardless of whether the system is armed or not. When a Panic zone is triggered, a Panic alarm is generated.
Personal Emergency	Personal Emergency zones are always active. When triggered, these zones generate an Emergency alarm.
Fire	These zones are always active. When a fire sensor is triggered, the zone generates a Fire alarm.
24Hr	This zone type produces a burglary alarm when triggered, even when the system is disarmed.
24Hr-X (future use)	The 24Hr-X zone is a future option that is not available in the current firmware.
Gas	These zones generate a Gas alarm in the event of a gas leak. Gas zones are always active.
Flood	Flood zones are designed for use with water sensors and generate a water alarm when triggered. Flood zones are always active.
Environmental	These zones are designed for environmental sensors that check temperature, humidity etc. Environmental zones are always active.
No Motion	No motion zones are used to monitor the activity of disabled or elderly people – see 10.17: “No Motion” Time.
Not Used	This zone type disables the sensor output. All alarm transmissions from the sensor are ignored though the sensor may still be used to activate HA units in Home Automation applications.

Table 8.1: Zone Type Options

8.6.2: Arm Set

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

To program the Arm Set option:

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

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.

Table 8.2: Arm Set Options

4. Use the keys 1, 2 and 3 to toggle the current setting.
5. Press ✓ when the desired setting is displayed.



It is not necessary to program this option for Panic, Personal Emergency, Fire and 24Hr zones.

8.6.3: 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 Enable or Disable.
5. Press ✓ when the desired setting is displayed.



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.

8.6.4: 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, Sensors [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 Enable or Disable.
5. Press ✓ when the desired setting is displayed.

8.6.5: 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 Enable or Disable
5. Press ✓ when the desired setting is displayed.



For the Force Arm feature to function, you must also enable Force Arming in the System options (see 10.3: Forced Arm).

8.6.6: 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.

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 Enable or Disable.



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

8.6.7: Repeater

The EL-2635 repeater is an additional module that extends the range of the wireless transmitters. For a sensor to use the repeater to relay transmissions to the system, you must define the Repeater option for its zone as "Use Repeater".

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 [#09]; the zone's current Repeater setting is displayed.
4. Select either No Repeater or Use Repeater.
5. Press ✓ when the desired setting is displayed.

8.7: Keyfobs

The *infinite Broadband* supports two types of keyfob transmitter, EL-2611 and EL-2614. You can register up to eight keyfobs to the system. Figure 8.1 illustrates these transmitters and the functions assigned to their buttons. For information on registration, descriptor editing and deletion, see sections 8.1, 8.2 and 8.3, respectively.

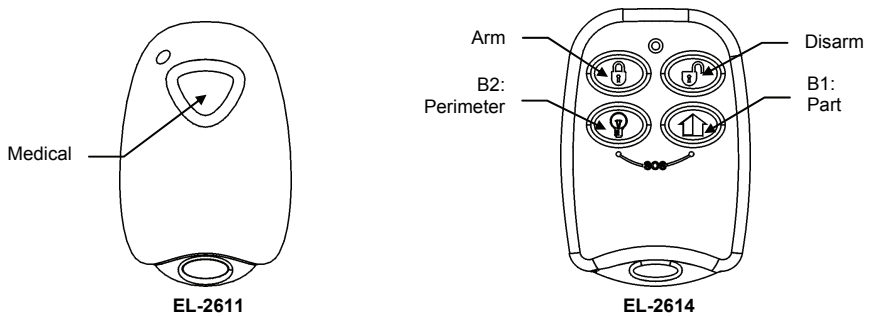


Figure 8.1: Keyfob Button Assignments

The following sections explain the programming options exclusive to the EL-2614 keyfob transmitter. These programming options are not relevant to the EL-2611. The latter product is factory preset to only send Personal Emergency alarms.

8.7.1: 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 either Controlled or Non-controlled.
5. Press ✓ when the desired setting is displayed.

8.7.2: Button Assignment

The EL-2614 includes two buttons (B1 and B2) that you can program individually. The default functions for B1 and B2 offer different arming methods. Alternatively, you can program these buttons to control a specific HA unit.

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 enter 00 to program the button's default function.

The default functions are as follows:

B1: Part arming

B2: Perimeter arming

8.7.3: SOS Panic Alarm Activation (EL-2614)

Using the four-button keyfob, you can activate an SOS Panic alarm by pressing two buttons simultaneously. Figure 8.2 illustrates how to activate an SOS Panic alarm on the EL-2614 wireless keyfob.

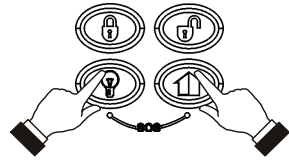


Figure 8.2: SOS Panic Alarm Activation

8.8: Keypads

Up to four wireless keypads are supported by the system. With the exception of the Cancel key, operation is identical for both EL-2620 and EL-2640 keypads. For information on registration, descriptor editing and deletion, see sections 8.1, 8.2 and 8.3, respectively.

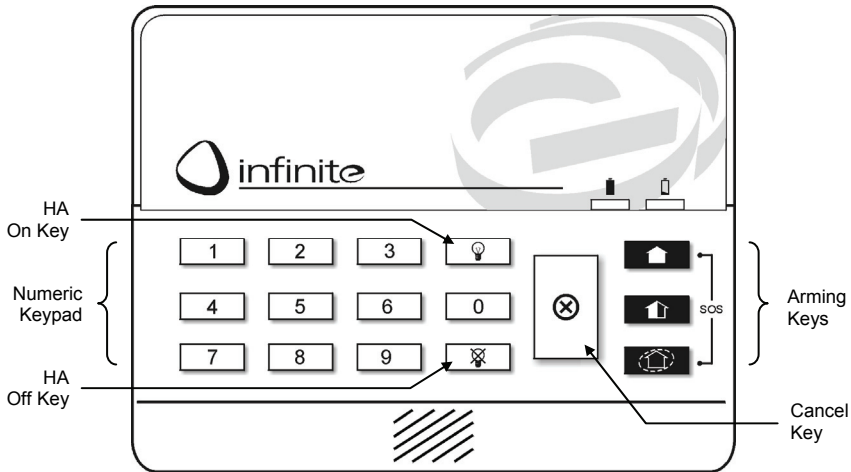


Figure 8.3: EL-2620 Keypad Layout

8.8.1: Keypad SOS Panic Alarm Activation

Using any of the wireless keypads, you can activate an SOS Panic alarm by pressing the Full and Perimeter arming keys simultaneously. Figure 8.4 illustrates how to activate an SOS Panic alarm on the EL-2620 wireless keypad.

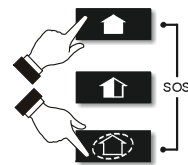


Figure 8.4: SOS Panic Alarm Activation (EL-2620)

8.9: Repeaters

Repeaters are designed to extend the wireless range of the control panel. Up to four repeaters may be registered to the system with a maximum of eight transmitters associated with each repeater. For information on registration, descriptor editing and deletion, see sections 8.1, 8.2 and 8.3, respectively.

8.10: External Siren

In addition to the control panel's internal siren, the system also supports a one-way external wireless siren. The control panel may include an optional on-board transmitter that sends alarm and arm status information to the wireless siren's receiver. This transmitter must be registered to the siren's receiver.

To register the on-board transmitter to the siren's receiver:

1. Set the siren's receiver to Registration mode – *refer to the siren's installation instructions for further information.*
2. Activate the siren using the External Siren Test feature – *see 4.7.2: External Siren Test.*
3. Activate the siren again; the on-board transmitter is registered to the siren's receiver.

8.10.1: Siren Type

The control panel supports both 1-way and 2-way sirens. For this feature to function correctly, you must define the siren type in programming.

To program the siren type:

1. From the Programming menu, select Devices, Siren, Ext. Siren Type [9152].
2. Select 1-Way Siren, 2-Way Siren (future availability) or No Ext. Siren if no siren is installed.

8.10.2: Siren (and Alarm Reporting) Delay

The Siren Delay is the period of time during which, only the internal siren is sounded and an 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 event message is not sent to the central station.

To program the Siren Delay time:

1. From the Programming menu, select Devices, Siren, Siren Delay [9153].
2. Enter a Siren Delay time (000-063 seconds).
3. Press ✓ when the desired setting is displayed.

8.10.3: Siren Cut-Off

The Siren Cut-Off is the period of time the siren is activated after an alarm has occurred. You may program a Siren Cut-Off time of between 001-254 seconds. If the Siren Cut-Off is programmed as 255 (continuous), the external siren will continue to sound until its internal cut-off time expires. In this case, the control panel's internal siren will sound for 255 seconds.

To program the Siren Cut-Off time:

1. From the Programming menu, select Devices, Siren, Cut-Off [9154].
2. Enter a Siren Cut-Off time (001-254 seconds).
3. Press ✓ when the desired setting is displayed.

Chapter Nine: Entry/Exit Timers and Arming Tones

This chapter explains how to program the time of the Entry/Exit delays and the tones sounded by the two sirens during Exit/Entry delays, arming and disarming.

9.1: 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. When these timers count down, the internal siren sounds a series of tones throughout the delay.

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).
4. Press ✓ when the desired setting is displayed.

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).
4. Press ✓ when the desired setting is displayed.

9.2: 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 Enable or Disable.
3. Press ✓ when the desired setting is displayed.

9.3: Arming Tones

Arming tones are the tones sounded by the siren when arming and disarming the system. Each set of tones can be enabled or disabled according to the requirements of the installation.

9.3.1: Exit Delay Tones

To program external siren tones during the Exit delay:

1. From the Programming menu, select Tones, Exit Tones, External Tones [9311].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

To program internal siren tones during the Exit delay:

1. From the Programming menu, select Tones, Exit Tones, Internal Tones [9312].
2. Select No Tones, Four Tones or Continuous Tones.
3. Press ✓ when the desired setting is displayed.

9.3.2: Entry Delay Tones

To program external siren tones during the Entry delay:

1. From the Programming menu, select Tones, Entry Tones, External Tones [9321].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

To program internal siren tones during the Entry delay:

1. From the Programming menu, select Tones, Entry Tones, Internal Tones [9322].
2. Select No Tones, Four Tones or Continuous Tones.
3. Press ✓ when the desired setting is displayed.

9.3.3: Arming Tones

To program external siren tones on arming:

1. From the Programming menu, select Tones, Arm Tones, External Tones [9331].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

To program internal siren tones on arming:

1. From the Programming menu, select Tones, Arm Tones, Internal Tones [9332].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

9.3.4: Disarming Tones

To program external siren tones on disarming:

1. From the Programming menu, select Tones, Disarm Tones, External Tones [9341].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

To program internal siren tones on disarming:

1. From the Programming menu, select Tones, Disarm Tones, Internal Tones [9342].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

9.3.5: Home Automation Tones

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

To program internal siren Home Automation tones:

1. From the Programming menu, select Tones, HA Tones [935].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

9.4: 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 LCD keypad on the front panel. For additional information, see 3.4.2: System Trouble Tones.

9.4.1: 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.
3. Press ✓ when the desired setting is displayed.

9.4.2: 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.
3. Press ✓ when the desired setting is displayed.

9.4.3: 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 shall 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.
3. Press ✓ when the desired setting is displayed.



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

9.5: Tones Options

9.5.1: Tones Output

The Tones Output option enables you to determine whether the tones sounded when arming and disarming are sounded by the control panel'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 [939].
2. Select Siren or Speaker.

9.5.2: Speaker Volume

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

To program the Speaker Volume option:

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



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

Chapter Ten: 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.

10.1: Swinger Setting

A sensor 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 sounding and report* per arming period
- One alarm sounding and report* per hour
- One alarm sounding and report* per day
- One alarm sounding and report* per week

To program the Swinger setting:

1. From the Programming menu, select System Options, Swinger [9401].
2. Select a Swinger setting from the above list.
3. Press ✓ when the desired setting is displayed.

10.2: 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 Enable or Disable.
3. Press ✓ when the desired setting is displayed.



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

10.3: 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 section 8.6.5: Force Arm.

To program the Forced Arm setting:

1. From the Programming menu, select System Options, Forced Arm [9403].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

* Both the alarm and its restore report are permitted.

10.4: 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 [9404].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

10.5: 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 [9405].
2. Select Audible or Silent.
3. Press ✓ when the desired setting is displayed.

10.6: 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, One-Key Arming [9406].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

10.7: 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 internal 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 external siren is sounded and the central station is notified.

To program the Supplementary Entry Delay setting:

1. From the Programming menu, select System Options, Supp. Entry Delay [9407].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

10.8: Entry Deviation

Entry Deviation is a pre-alarm feature employed in the event that a sensor defined with the "Normal" zone type is opened during the entry delay. In this case, the internal 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 System Options, Entry Deviation [9408].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

10.9: 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 cancelled 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 [9409].
2. Enter a delay time (001-255 minutes) or enter 000 if you require the system to choose a random AC Loss Delay.
3. Press ✓ when the desired setting is displayed.

10.9.1: 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.

10.10: 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 or only for two minutes after arming or disarming the system.

To program the Arm Status Display options:

1. From the Programming menu, select System Options, Arm Status Display [9410].
2. Select Always or Display 2 Min.
3. Press ✓ when the desired setting is displayed.

10.11: 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 only – see 10.10: *Arm Status Display*.

To edit the Banner text:

1. From the Programming menu, select System Options, Banner [9411].
2. Edit the Banner text using the alphanumeric keypad.
3. Press ✓ when you have finished editing.



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

10.12: PGM Output

The PGM is a programmable dry contact relay output that is triggered according to specific system status conditions.

10.12.1: 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, Output Trigger [94121].
2. Select an Output Trigger option from the following table.
3. Press ✓ when the desired setting is displayed.

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
Personal Emergency	Personal Emergency 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	
Internal Bell	Internal siren follower	

Table 10.1: PGM Output Trigger Options

* Functions only when the system is disarmed.



For certain trigger options, deactivation may be determined by the PGM Cut-off (see 10.12.4: 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.

10.12.2: 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, Output Trigger [94122].
2. Select Steady or Pulsed.
3. Press ✓ when the desired setting is displayed.



The Zone Status and Internal Bell trigger options have a fixed Output Type; there is no need to program an Output Type for these options.

10.12.3: 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 Output Type:

1. From the Programming menu, select System Options, PGM Options, Polarity [94123].
2. Select Active High or Active Low.
3. Press ✓ when the desired setting is displayed.

10.12.4: 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 *Table 10.1: PGM Output Trigger Options*. For those Output Trigger types that are not affected by the PGM Cut-off, there is no need to program this option.

To program the PGM Cut-off time:

1. From the Programming menu, select System Options, PGM Options, PGM Cut-off [94124].
2. Enter a PGM Cut-off time (001-255 seconds or 000 for continuous activation).
3. Press ✓ when the desired setting is displayed.

10.13: Guard Code (for future use)

The Guard Code 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.

10.14: Time/Date Format

This option determines the format in which the time and date are displayed in the user interface. 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, Time Format [9414].
2. Select the required format from the options available.
3. Press ✓ when the desired setting is displayed.

10.15: “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. [9415].
2. Select the required interval from the options available (1-4 weeks).
3. Press ✓ when the desired setting is displayed.

10.16: Jamming Detection

The system is able 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. [9416].
2. Select Enabled or Disabled.
3. Press ✓ when the desired setting is displayed.

10.17: “No Motion” Time

The No Motion feature is designed to monitor the activity of disabled or elderly people. If a sensor defined as “No Motion” (see 8.6.1: 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 [9417].
2. Select 6 Hours, 12 Hours, 24 Hours, 48 Hours, 72 Hours or Disabled.
3. Press ✓ when the desired setting is displayed.

Chapter Eleven: Communications

The *infinite Broadband* control panel's main communication channel is provided by the Ethercom module. All system events are forwarded via the Web over TCP/IP to the ELAS application server which handles routing both to service providers (e.g Security and Fire monitoring services) and to users via email or text message. Additionally, users are able to monitor and control the system from their PC or other Web-enabled devices.

The Ethercom's on-board PSTN dialer provides a back-up communication channel along with the optional GSM cellular communications module (future option). These modules are also used for various Two-Way Audio applications.



For firmware versions that do not support the GSM cellular communications module, do not select any of the cellular communication options in programming.

When using the Ethercom, the account configuration is as follows:

- Account 1 (Ethercom)
 - Telephone Number: Not necessary (leave blank)
 - Protocol: IP Protocol
 - Communication Interface: Ethernet 10BT (LAN)
- Account 2 (PSTN backup)
 - Telephone Number: Enter the Central Station telephone number
 - Protocol: SIA or Contact ID
 - Communication Interface: PSTN
- Account 3 (optional)
 - Telephone Number: Enter the Central Station telephone number
 - Protocol: SIA, Contact ID, SMS SIA or Follow Me
 - Communication Interface: PSTN or GSM

In addition to the Account configuration options, you must also program the Internet options for the Ethercom module – see *Chapter Twelve: Internet Options*.

11.1: Accounts

The control panel supports three customer accounts. Each account has its own communications options. An explanation of each of these options is included in this section.

11.1.1: Telephone Number

To edit an account's telephone number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select an account.
3. From the account's sub-menu, select Telephone # [#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.
5. Press ✓ when you have finished editing.

11.1.2: Account Number

To edit an account number:

1. From the Programming menu, select Communications, Accounts [951].
2. Select an account.
3. From the account's sub-menu, select Account # [#2].
4. Enter up to eight digits. Enter leading zeros for account numbers of less than eight digits.
5. Press ✓ when you have finished editing.

11.1.3: Protocol

To program an account's communication protocol:

1. From the Programming menu, select Communications, Accounts [951].
2. Select an account.
3. From the account's sub-menu, select Protocol [#3].
4. Select a protocol from the options available.
5. Press ✓ when the desired setting is displayed.



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.

11.1.4: Communication Interface

For each account, you can choose the type of communication the system employs when reporting.

To program an account's communication interface:

1. From the Programming menu, select Communications, Accounts [951].
2. Select an account.
3. From the account's sub-menu, select Interface [#4].
4. Select either LAN (Account 1 only), PSTN or GSM.
5. Press ✓ when the desired setting is displayed.

11.1.5: Call Attempts

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 an account.
3. From the account's sub-menu, select Call Attempts [#5].
4. Enter a value between 01 and 15.
5. Press ✓ when the desired setting is displayed.

11.1.6: Two-Way Audio

The Two-Way audio option determines whether Two-Way Audio is enabled for the account. For further information, see section 6.2.2: TWA Alarm Reporting.

To program the number of call attempts for an account:

1. From the Programming menu, select Communications, Accounts [951].
2. Select an account.
3. From the account's sub-menu, select TWA [#6].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

11.2: General Account Options

The options included in this section concern event reporting via POTS and GSM for all three accounts.

11.2.1: Call Continue

When reporting an event, the system attempts to report to Account 1. If the system fails in its attempt to report the event, it attempts to report to Account 2 then Account 3, respectively. If the Call Continue feature is active, the control panel sends a duplicate report to the accounts that are selected.

To program the Call Continue option:

1. From the Programming menu, select Communications, Accounts, Call Continue [9514]; the current Call Continue setting is displayed.

Press...	To...
1	Toggle Account 1 in the Call Continue sequence.
2	Toggle Account 2 in the Call Continue sequence.
3	Toggle Account 3 in the Call Continue sequence.

Table 10.1: Call Continue Options

2. Use keys 1, 2 and 3 to toggle the account numbers.
3. Press ✓ when the desired setting is displayed.



If Account 1 is programmed as TCP/IP protocol/LAN interface, Account 2 functions as backup only and cannot be programmed to send a duplicate report.

11.2.2: Report Cycles

The system's attempts to report events are organized in cycles. A report cycle is a set of call attempts. If the system does not succeed in sending a report to any of the accounts, it tries the entire report cycle until it succeeds. You can determine the number of times the system attempts this sequence by programming the Report Cycle option.

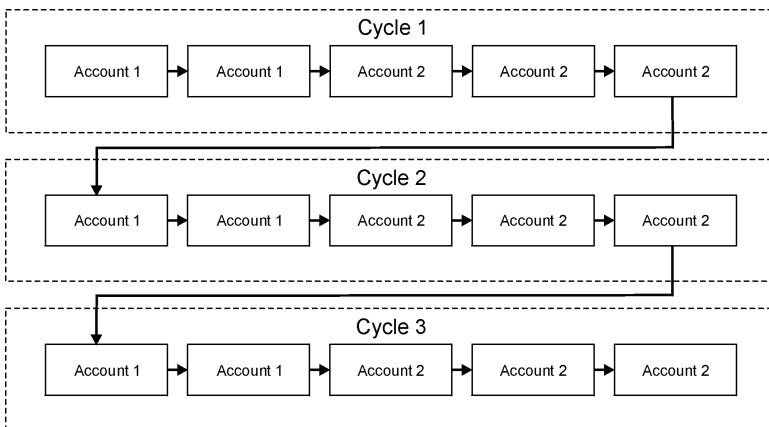


Figure 11.1: Typical Report Cycle Sequence

In the example illustrated in Figure 11.1, 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.

To program the number of Report Cycles:

1. From the Programming menu, select Communications, Accounts, Report Cycles [9515].
2. Enter a value between 01 and 03.
3. Press ✓ when the desired setting is displayed.

11.3: Remote Programming

Electronics Line 3000's Remote Programmer (RP) software enables 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 *infinite Broadband* control panel designed to facilitate programming.

You can connect to the panel from a PC using one of the following methods:

- Web RP: A version of the RP software that establishes communication with the control panel over the Web via the ELAS.
- 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 Main board's 9-pin serial port (this method requires that you install the optional Serial Interface board).

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

11.3.1: 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 panel, the panel hangs up and calls the Callback telephone number.

To edit the Callback telephone number:

1. From the Programming menu, select Communications, Remote Prog., Callback # [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.
3. 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.

11.3.2: 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 up to six digits.
3. Press ✓ when you have finished editing.

11.3.3: RP Communication Interface

Along with remote programming via the Web, the *infinite Broadband* can also employ either cellular or PSTN communication.

For PSTN communication, the RP uses a double call method so that the line can be shared with regular telephone handsets, an answering machine or fax. The Cellular Communications Module has its own individual telephone number for data transfer and therefore, the double call method is not needed. In this case, the RP calls the control panel directly.

To program the RP communication interface:

1. From the Programming menu, select Communications, Remote Prog., RP Interface [9523].
2. Select either LAN, PSTN or GSM.

11.3.4: 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.

Access option	Description
Always	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 RP from the Service menu in order to establish a connection – see 4.7.10: <i>Enable Remote Programming</i> .

Table 10.2: RP Access Options



When using the Web RP application to program the system, you can always access the control panel in order to view programming parameters regardless of the RP Access options detailed above. However, if you wish to download any programming parameter modifications to the control panel, this action is limited by the RP Access option.

11.4: 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 and holds down the Service Call button (0) for a few seconds, a two-way audio connection is established with the central station.

11.4.1: 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.
3. Press ✓ when you have finished editing.

11.4.2: 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 PSTN or GSM.

11.5: SMS Center

To edit the SMS Center telephone number:

1. From the Programming menu, select Communications, SMS Center [954].
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.
3. Press  when you have finished editing.

11.6: Communications Options

11.6.1: Line Monitor

The Line Monitor feature monitors the PSTN telephone line. If a problem is detected, 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 [9551].
2. Select Enable or Disable.

11.6.2: 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 sends a weekly test and calculates automatically the time the Periodic Test is sent according to the last four digits of the account number. This feature ensures that the central station is not inundated by test reports at any given time.



Do not select the Automatic Periodic Test Interval option if Account 1 is programmed to report using the IP Protocol over the LAN.

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 shall be sent.

To program the Periodic Test Interval:

1. From the Programming menu, select Communications, Comm. Options, Test Interval [9552].
2. Enter the test interval (001-254 hours) or 255 for an automatically calculated weekly test interval.
3. Press ✓ when the desired setting is displayed.

To disable the Periodic Test:

- Program the Periodic Test Interval as 000.

11.6.3: 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 [9553].
2. Enter a time (HH:MM in 24hr format).
3. Press ✓ when the desired setting is displayed.

11.6.4: 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 module. 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 [9554].
2. Enter a time (001-255 seconds).
3. Press ✓ when the desired setting is displayed.

11.6.5: 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 module. 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 [9555].
2. Enter a time (001-255 seconds).
3. Press ✓ when the desired setting is displayed.

11.6.7: 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 [9556].
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.

11.6.8: 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 [9557].
2. Select Enable or Disable.

11.7: Two-Way Audio Options

The *infinite Broadband* control panel offers a number of Two-Way Audio features that can be used in various applications. This section explains the programming options that control the mode in which these features function. For further information on Two-Way Audio, see

11.7.1: Incoming Two-Way Audio

This option determines whether the user/central station operator can establish Two-Way Audio communication with the control panel.

To program the Incoming Two-Way Audio setting:

1. From the Programming menu, select Communications, Comm. Options, Incoming TWA [95581].
2. Select Enable or Disable.

11.7.2: Two-Way Audio Timeout

The Two-Way Audio Timeout is the duration of a Two-Way Audio call. When the time out expires, the system automatically disconnects unless the call is manually extended by the operator.

To program the Two-Way Audio Timeout:

1. From the Programming menu, select Communications, Comm. Options, TWA Timeout [95582].
2. Enter a time (001-255 seconds).
3. Press ✓ when the desired setting is displayed.

11.7.3: Microphone/Speaker Options

In addition to the built-in microphone and speaker, the control panel supports an external microphone speaker unit. The Microphone/Speaker options allow you to choose which microphone and speaker shall function during Two-Way Audio communication. You can choose one mic./speaker (internal or external) to function exclusively or both may function simultaneously.

To program the Microphone/Speaker options:

1. From the Programming menu, select Communications, Comm. Options, Mic./Speaker [95583].
2. Select one of the available options.

11.7.4: TWA Mode

The Two-Way audio features offer a choice of two operating 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, Comm. Options, Two-Way Audio, TWA Mode [95584].
2. Select Duplex or Simplex.
3. Press ✓ when the desired setting is displayed.

11.8: GSM RX Report

The GSM RX Report is a feature that periodically reads the GSM signal strength of the Cellular Communications module (future option)— see 4.7.8: *GSM Signal Strength*.

This reading occurs at the times programmed for the Periodic Test – see 11.6.2: *Periodic Test Interval* & 11.6.3: *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 11.9: Event Options. 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 RX Report [9559].
2. Select Enable or Disable.

11.9: Event Options

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 [#8]

11.9.1: 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/disable reporting for an event group:

1. From the Programming menu, select Communications, Event Options [956].
2. Select an event group.
3. From the event group's sub-menu, select Report [#1].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

11.9.2: Restore Reporting

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

To enable/disable restore reporting for an event group:

1. From the Programming menu, select Communications, Event Options [956].
2. Select an event group.
3. From the event group's sub-menu, select Report Restore [#2].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

11.9.3: Two-Way Audio

For the Burglary, Fire and Medical event groups, there is an additional option that enables Two-Way Audio – see 6.2.2: *TWA Alarm Reporting*.

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

1. From the Programming menu, select Communications, Event Options [956].
2. Select an event group (Burglary, Fire or Medical).
3. Select TWA [#3].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

Chapter Twelve: Internet Options

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 control panel ID and password for each customer.

12.1: Ethercom



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

There are two methods to program the IP settings:


- Automatic IP settings (DHCP) – when using a DHCP server, the server provides all of the configuration settings automatically.
- Manual IP settings – if the DHCP server option is programmed as “0.0.0.0”, you must enter the IP Address, Gateway, Netmask and DNS Server manually.

12.1.1: DHCP Server

To edit the IP address of the DHCP server:




1. From the Programming menu, select Communications, Internet, Ethercom, DHCP Server [95711].
2. Enter the DHCP server’s IP address. Use the  key to enter “.” and the  key to delete one character at a time.

If you are not using DHCP, program this option as “0.0.0.0”. If the DHCP server’s IP address is unknown, you can program the system to broadcast a request for a DHCP server from the Internet service provider. To do so, program this option as “255.255.255.255”.

3. Press  when you have finished editing.




12.1.2: IP Address

To edit the IP address:

1. From the Programming menu, select Communications, Internet, Ethercom, IP Address [95712].
2. Enter an IP address. Use the  key to enter “.” and the  key to delete one character at a time.
3. Press  when you have finished editing.

12.1.4: Netmask

To edit the netmask:

1. From the Programming menu, select Communications, Internet, Ethercom, Netmask [95713].
2. Enter the netmask. Use the  key to enter “.” and the  key to delete one character at a time.
3. Press  when you have finished editing.

12.1.3: Gateway

To edit the Gateway address:

1. From the Programming menu, select Communications, Internet, Ethercom, Gateway [95714].
2. Enter the Gateway's IP address. Use the $\text{\textcircled{0}}$ key to enter "." and the $\text{\textcircled{X}}$ key to delete one character at a time.

12.1.5: DNS Server

To edit the DNS server address:

1. From the Programming menu, select Communications, Internet, Ethercom, DNS Server [95715].
2. Enter the DNS Server's IP address. Use the $\text{\textcircled{0}}$ key to enter "." and the $\text{\textcircled{X}}$ key to delete one character at a time.
4. Press \checkmark when you have finished editing.

12.2: ELAS

The following options are related to communication between the Ethercom to the ELAS.

- Web service URL
- Control Panel ID
- Password

The Web service URL includes a number of elements that have been divided into several programming options. These are shown below in Figure 11.1.



Figure 11.1: Example of Web Service URL

12.2.1: Site Head

To edit the Site Head:

1. From the Programming menu, select Communications, Internet, ELAS, Site Head [95721].
2. Enter the Site Head (domain name or IP address) using the alphanumeric keypad.
3. Press \checkmark when you have finished editing

12.2.2: Site Tail

To edit the Site Tail:

1. From the Programming menu, select Communications, Internet, ELAS, Site Tail [95722].
2. Enter the Site Tail using the alphanumeric keypad.
3. Press \checkmark when you have finished editing

12.2.3: Path

To edit the Path:

1. From the Programming menu, select Communications, Internet, ELAS, Path [95723].
2. Enter the path using the alphanumeric keypad.
3. Press ✓ when you have finished editing.

12.2.4: File

To edit the file:

1. From the Programming menu, select Communications, Internet, ELAS, File [95724].
2. Enter the file name. Use the ⓪ key to enter "." and the ✕ key to delete one character at a time.
3. Press ✓ when you have finished editing.

12.2.5: HTTP Port

To edit the HTTP Port:

1. From the Programming menu, select Communications, Internet, ELAS, HTTP Port [95725].
2. Enter the HTTP port. Use the ⓪ key to enter "." and the ✕ key to delete one character at a time.
3. Press ✓ when you have finished editing.

12.2.6: Control Panel ID

To edit the control panel ID:

1. From the Programming menu, select Communications, Internet, ELAS, CPID [95726].
2. Enter the control panel ID using the alphanumeric keypad.
3. Press ✓ when you have finished editing.

12.2.7: Control Panel Password

To edit the control panel password:

1. From the Programming menu, select Communications, Internet, ELAS, Password [95727].
2. Enter a six-character password using the alphanumeric keypad. The password must begin with a letter.
3. Press ✓ when you have finished editing.

12.3: I'm Alive Timers

"I'm Alive" is a periodic supervision signal transmitted from the Ethercom to the ELAS. Two timers determine how often the "I'm Alive" signal is sent. The first timer determines the "I'm Alive" interval when the control panel is disarmed. The second timer determines the length of the interval when the control panel is armed. The following options enable you to program the initial settings for these timers.

12.2.9: "I'm Alive" During Disarm

To program the "I'm Alive" during disarm timer:

1. From the Programming menu, select Communications, Internet, Alive Disarm [9573].
2. Enter a time (001-255 seconds).
3. Press ✓ when you have finished editing.

12.2.9: “I’m Alive” During Arm

To program the “I’m Alive” during arm timer:

1. From the Programming menu, select Communications, Internet, Alive Arm [9574].
2. Enter a time (001-255 seconds).
3. Press ✓ when you have finished editing.

Chapter Thirteen: 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 panel's plastic housing. The *infinite Broadband* control panel's home automation features require the use of an external X10 power-line interface.

13.1: X10 Overview

The control panel'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 AC power lines. This means that, using an X10 transmitter, you can send On/Off commands to X10 receivers (lamp and appliance modules) that are plugged into electrical outlets around the home. From here on, we shall 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 13.1, the HA unit is set to House A, Unit 3.

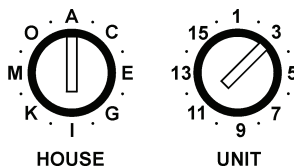


Figure 13.1: HA Unit Dials

The control panel 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 panel's memory – see section 13.3: House Code.

13.2: HA Units

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

13.2.1: Scheduling

Scheduling allows you to program the panel to send On/Off commands to an HA unit at specific times. The Scheduling section of Home Automation programming is identical to that described in Chapter Seven: Home Automation Control. For further information on programming the On Time, Off Time and Schedule for each HA unit, see section 7.4: Scheduling.

13.2.2: 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 13.2.8: *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 sensors 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 [#4].
4. Enter up to two zone numbers.
5. Press ✓ when the desired setting is displayed.

13.2.3: 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 13.2.8: *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 [#5].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

13.2.4: 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 8.10.3: *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.

13.2.5: Keyfob Control

Each EL-2614 keyfob, 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 Control [#6].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

13.2.6: SMS Control

Via SMS, 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 SMS 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 SMS Control [#7].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

13.2.7: Randomize

When the system is fully armed between the hours 21:00 and 06:00, 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 [#8].
4. Select Enable or Disable.
5. Press ✓ when the desired setting is displayed.

13.2.8: 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 [#9].
4. Select 5 sec, 30 sec, 1 min, 2 min or Toggle.
5. Press ✓ when the desired setting is displayed.

13.2.9: 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 modify 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 [#0].
4. Modify the descriptor using the alphanumeric keypad.
5. Press ✓ when you have finished modifying the descriptor.

13.3: 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. Select a House code from the options available (A-P).
3. Press ✓ when the desired setting is displayed.

13.4: 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 HA Programming, SMS Confirm. [963].
2. Select Enable or Disable.
3. Press ✓ when the desired setting is displayed.

Chapter Fourteen: 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 panel 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.

14.1: Initialization

The Initialization function clears the entire system and resets factory defaults.

To initialize the control panel:

1. From the Programming menu, select Initialize, Init All [971]; the system prompts you for confirmation.
2. Press ✓ to confirm; factory programming defaults are restored, the event log is cleared, user codes and wireless transmitters are deleted.

14.2: Default Program Restore

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

To load the default program:

1. From the Programming menu, select Initialize, Load Defaults [972]; the system prompts you for confirmation.
2. Press ✓ to confirm; factory programming defaults are restored.

14.3: Clear User Codes

Clear User Codes deletes all programmed user codes and restores the default Master and Installer codes.

To clear user codes:

1. From the Programming menu, select Initialize, Clear Users [973]; the system prompts you for confirmation.
2. Press ✓ to confirm; all user codes are deleted and default codes are restored.

14.4: Clear Wireless Transmitters

The Clear Wireless Transmitters function enables you to delete all registered transmitters at once.

To clear the transmitter register:

1. From the Programming menu, select Initialize, Clear Wireless [974]; the system prompts you for confirmation.
2. Press ✓ to confirm; the transmitter register is cleared.

14.5: Find Modules

The Find Modules function runs a diagnostic test that identifies the modules and keypads 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.

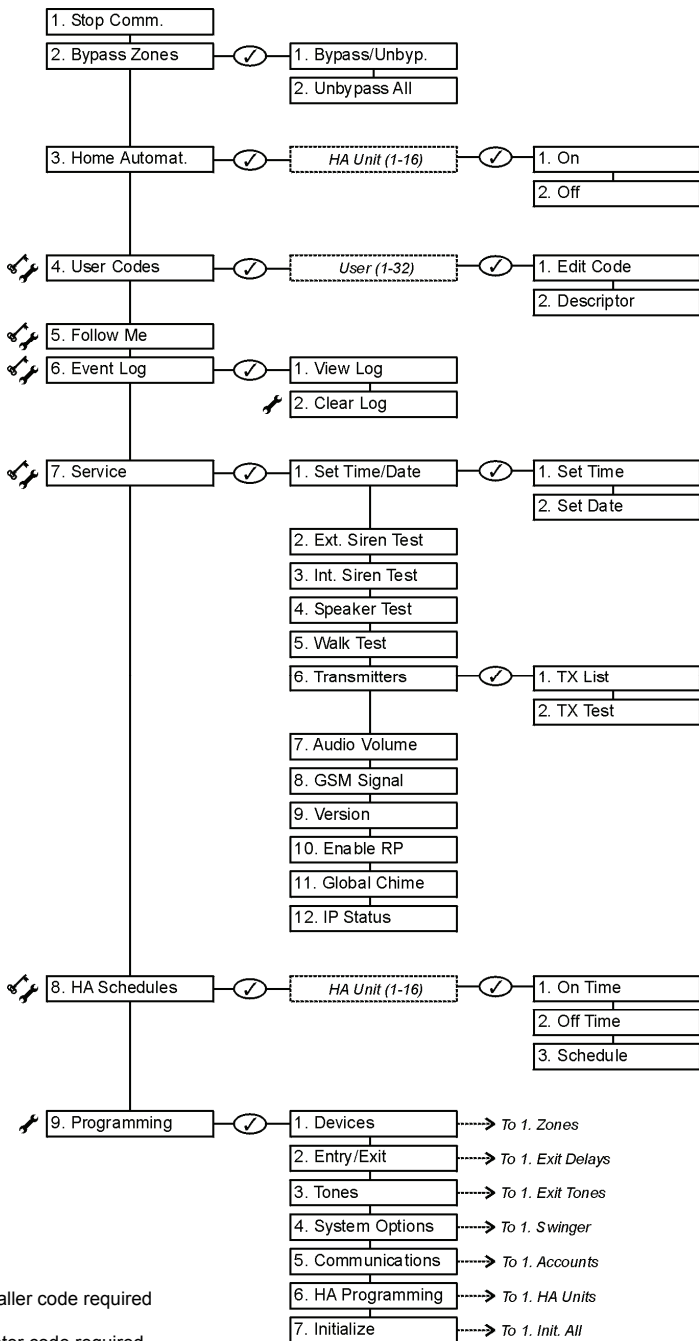
To run the Find Modules test:

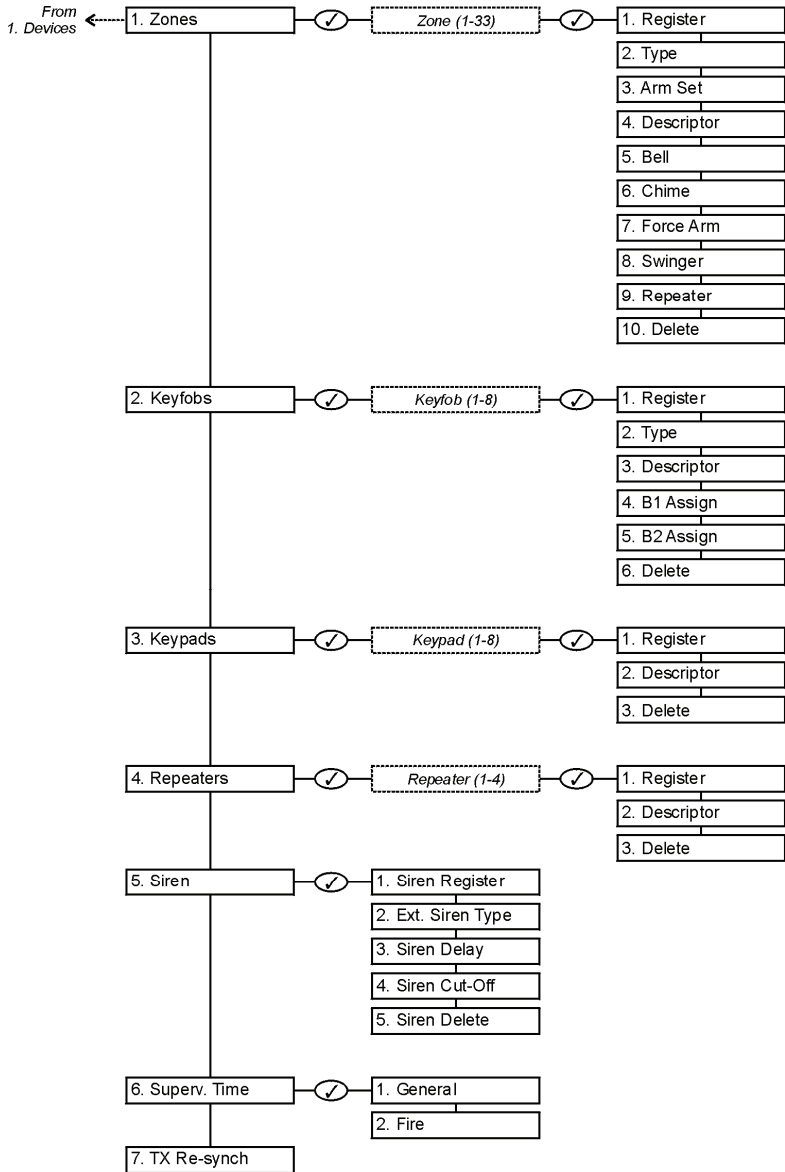
1. From the Programming menu, select Initialize, find Modules [975]; the system prompts you for confirmation.
2. Press ✓ to confirm; the system begins to search for the connected modules. At the end of the search, the modules that are present are displayed and the system asks if you want to save the displayed list.
3. Press ✓ ; the list is saved.

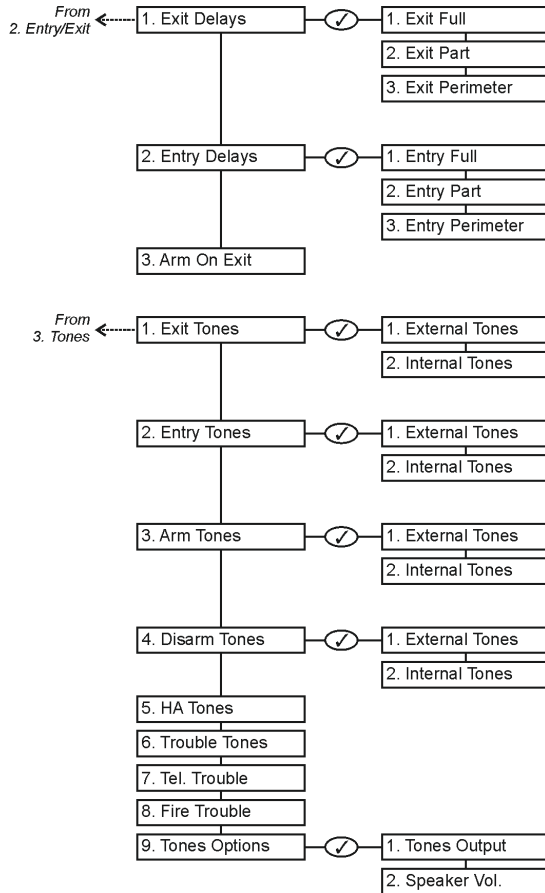


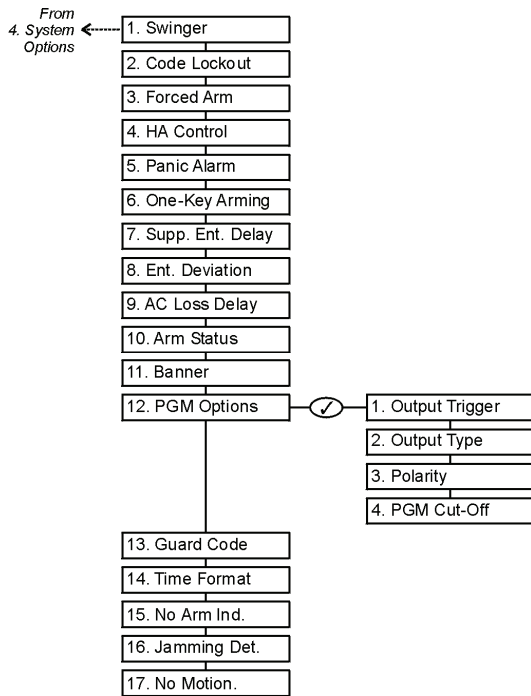
If a connected module is not included in the list, check the wiring connections and run this test again.

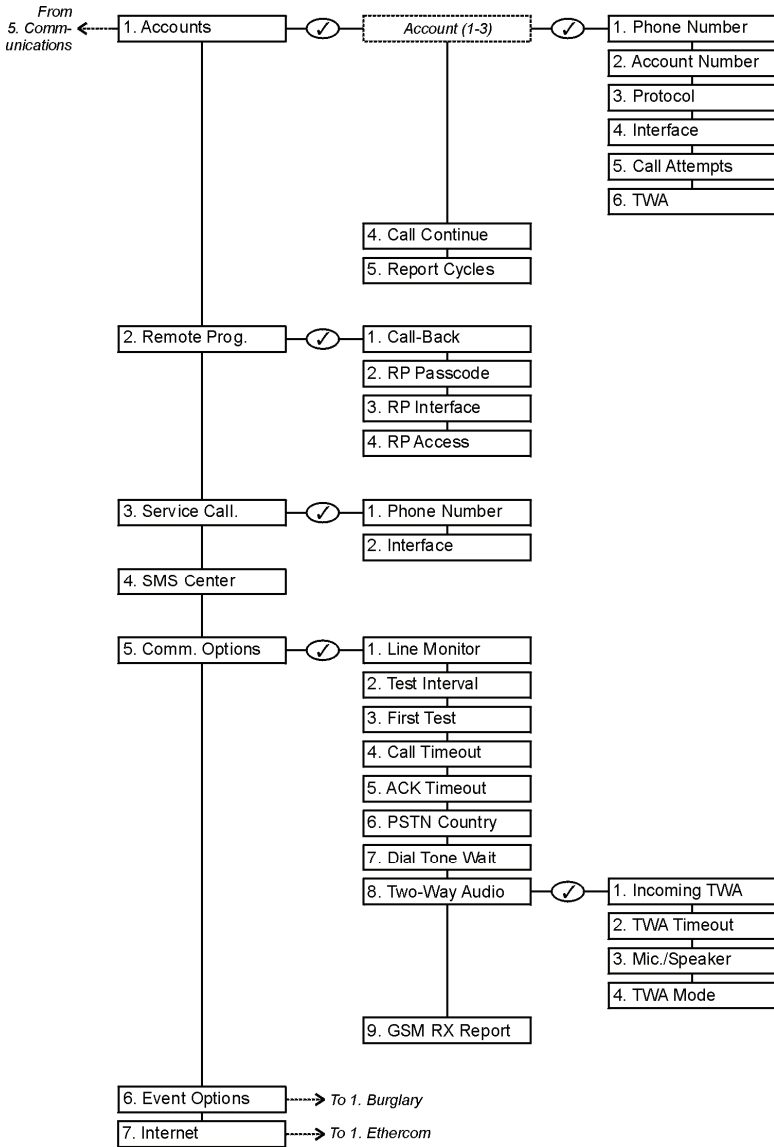
Appendix A: Menu Structure

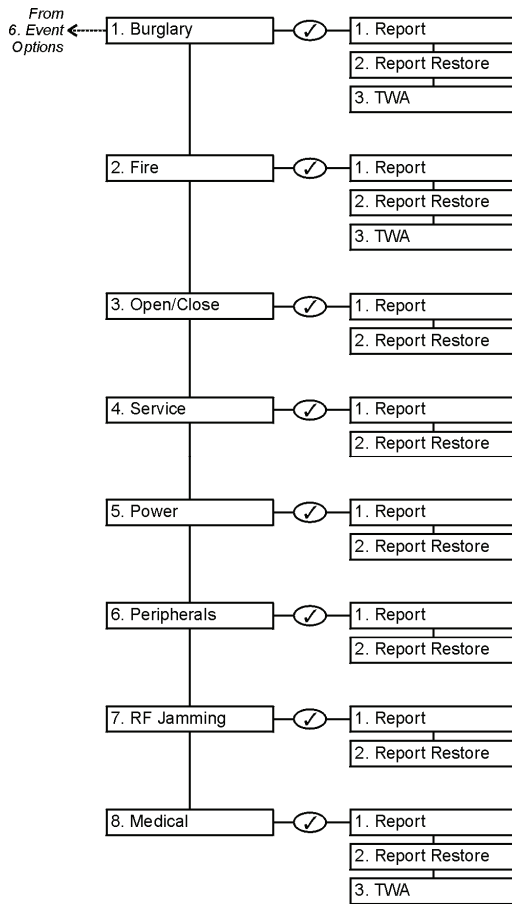


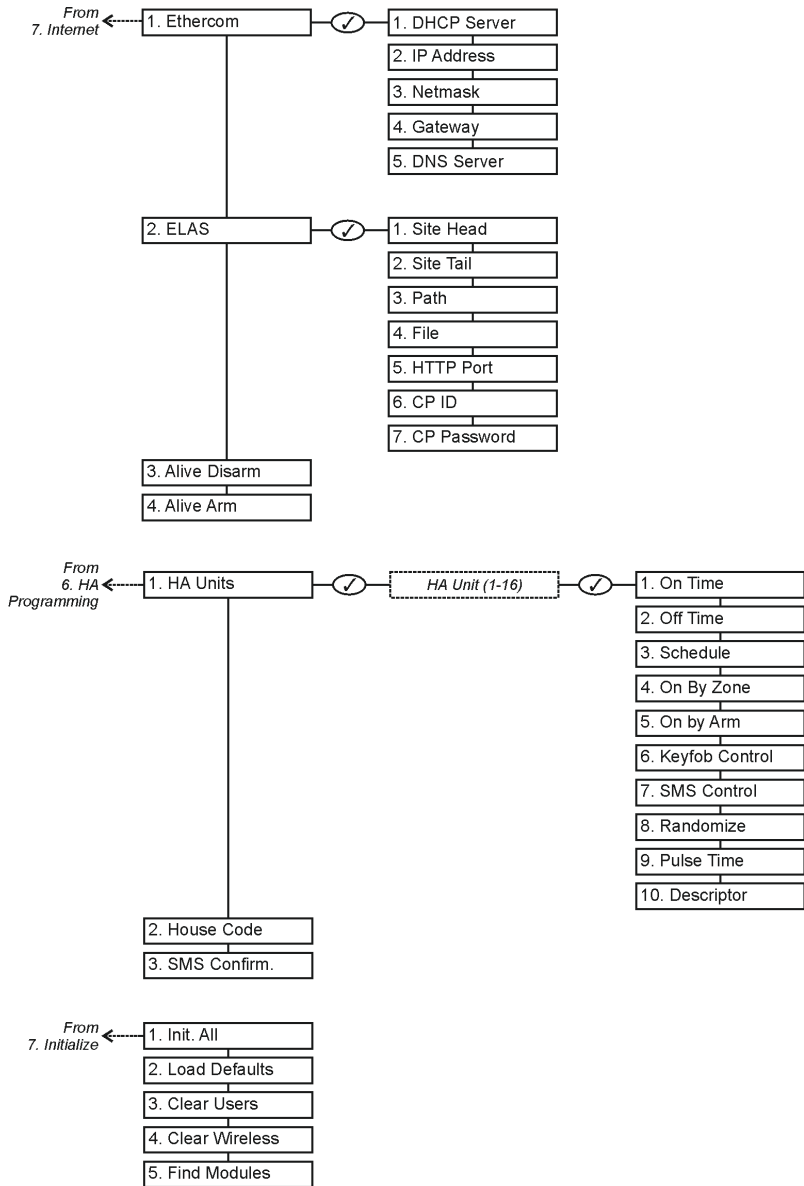












Appendix B: Transmitter Installation

PIR Sensors (EL-2600/EL-2600PI/EL-2645/EL-2645PI)

The EL-2600, EL-2600PI, EL-2645 and EL-2645PI are intelligent wireless PIR sensors for use with the *infinite Broadband* system. All of these sensors 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.

The EL-2600PI and EL-2645PI are designed for installations prone to nuisance alarms caused by pets or small animals.

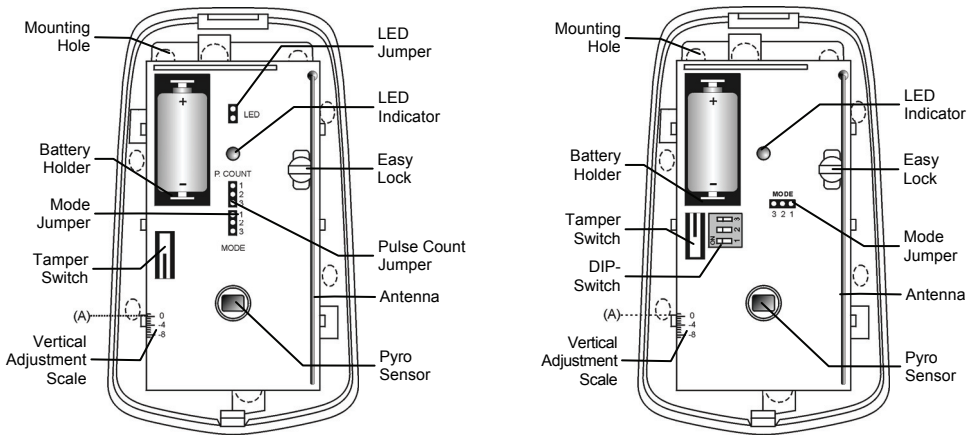


Figure B.1: PIR Sensors with Cover Removed – EL-2600/EL-2600PI (left) and EL-2645/EL-2645PI (right)

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.
- Select an appropriate installation height from Table B1.

Lens	Mounting Height
Standard	2.2m (6.6')
Long Range	2m (6.5')
Curtain	1m (3.25')
EL-2600PI	2m (6.5')
EL-2645PI	2m (6.5')

Table B.1: Recommended Mounting Height

Pet Immunity Guidelines (EL-2600PI/EL-2645PI)

It is expected that the EL-2600PI and EL-2645PI will eliminate false alarms caused by:

- Animals up to 22kg (EL-2600PI)
- Animals up to 45kg (EL-2645PI)
- 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 2m with the PCB vertical setting at -4.
- Set the pulse counter to 2.
- 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 of the detector by climbing on furniture, boxes or other objects.

Installation Procedure

To install PIR sensors:

1. Open the housing by removing the front cover. To do so, insert a screwdriver in the release slot (located at the bottom of the detector between the front and back cover). Turn the screwdriver 90° to release the cover.
2. Remove the PCB by turning counter-clockwise and removing the Easy Lock – *do not touch the face of the pyro sensor!*
3. Apply battery power by removing the isolator that separates the battery from the contacts on the battery holder.
4. Place the Mode jumper over pins 2 & 3 (Radio Mode); the LED flashes.



Install the Mode jumper only after applying battery power.

5. From the Programming menu, select Devices, Zones [911].
6. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When **Save?** appears on the control panel's LCD display, press ✓.
7. Remove the Mode jumper and place it over one pin for storage.
8. Choose an appropriate mounting height from Table B.1 and test the transmitter from the exact mounting position before permanently mounting the unit.
9. Knock out the mounting holes and attach the base to the wall.
10. Mount the PCB at the required vertical adjustment and replace the PCB screw.
11. Write the number of the zone on the sticker provided. Affix the sticker inside the front cover for future reference and replace the front cover.

Warm-Up Time

The detector will need to warm up for the first 90 seconds after applying power.

Pulse Counter

The pulse counter determines the amount of beams that need to be crossed before the detector will generate an alarm. To set the pulse counter, refer to tables B.2 and B.3.

Adaptive Pulse Count (EL-2645/EL-2645PI)

Using the Adaptive pulse count feature, the detector chooses between 1 or 2 pulses based on its analysis of the received signal.

Vertical Adjustment

To position the PCB, turn the Easy Lock counter-clockwise and slide the PCB up or down to the required setting using the vertical adjustment scale. The detector's coverage area is 14m x 14m (EL-2600/EL-2645) or 12m x 12m (EL-2600PI/EL-2645PI) when the PCB is positioned at 0. Slide the PCB up towards the -8 position to decrease the coverage area bringing the beams closer to the mounting wall.

Jumper Position	Pulse Count
Pins 1&2	1
Pins 2&3	2
Jumper Removed	3

Table B.2: Pulse Count Jumper (EL-2600/EL-2600PI)

Switch 2	Switch 3	Pulse Count
OFF	OFF	1
ON	OFF	2
ON	ON	3
OFF	ON	Adaptive

Table B.3: Pulse Count Setting (EL-2645/EL-2645PI)

Walk Test Mode

A walk test is performed in order to determine the lens coverage pattern of the detector – see *Figure B.2*. Walk Test mode cancels the delay time between detections, enabling you to perform an efficient walk test.

To perform a Walk Test.

1. Place the Mode jumper over pins 1 & 2.
2. Walk across the scope of the detector according to the detection pattern selected.
3. Confirm that the LED activates and deactivates accordingly. Wait five seconds after each detection before continuing the test.
4. After completing the walk test, remove the jumper and place it over one pin for storage – see *Mode Jumper Safeguard*.

LED Indication

The LED indicator is lit twice every time a transmission is made. To enable or disable LED indication, refer to Table B.4 below.

LED Indication	EL-2600/EL-2600PI	EL-2645/EL-2645PI
Disabled	Remove LED Jumper	DIP-Switch 1 OFF
Enabled	Install LED Jumper	DIP-Switch 1 ON

Table B.4: LED Indication Settings



The LED should only be disabled after successfully walk testing the detector.

Mode Jumper Safeguard

During normal operation, the Mode jumper should be placed over one pin for storage. When the mode jumper is placed over two pins, the detector is either in Radio or Walk Test Mode. As a precaution, these modes are limited to three minutes. After three minutes have expired, the detector switches back to normal operation. If this happens, you can reset a mode by removing and replacing the mode jumper.

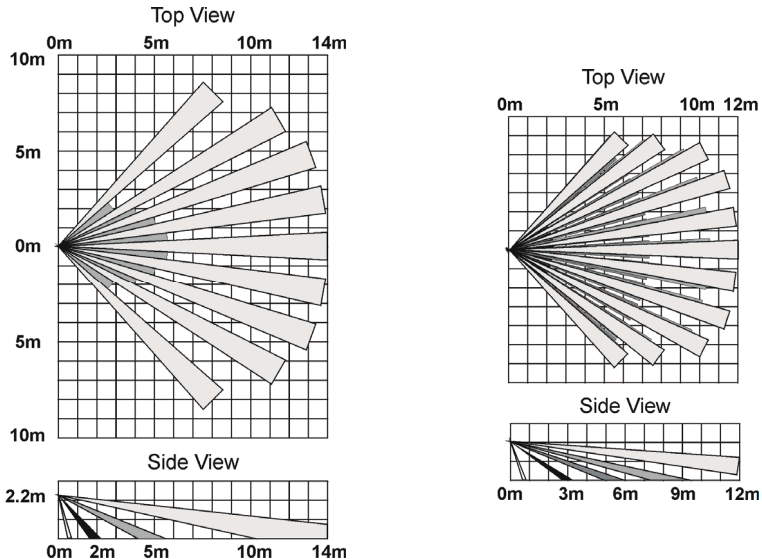


Figure B.2: Lens Coverage Diagrams EL-2600/EL-2645 (left) and EL-2600PI/EL-2645PI (right)

Magnetic Contact (EL-2601)

The EL-2601 is a magnetic contact designed for installation on doors and windows.

Installation Procedure

To install magnetic contacts.

1. To open the housing, insert a small screwdriver at the bottom of the unit between the front and back cover and twist the screwdriver to release the cover.
2. Remove the divider separating the battery from the contacts on the battery holder. When you apply power and the Tamper switch is open, the EL-2601 enters Test mode during which a transmission is sent every few seconds. You can terminate Test mode by closing the Tamper switch. Test mode is automatically terminated after approximately five minutes.

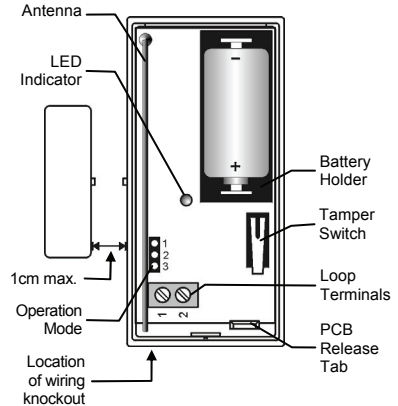


Figure B.3: EL-2601 (cover off)



When handling the PCB, do not apply pressure on the antenna.

3. From the Programming menu, select Devices, Zones [911].
4. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When **Save?** appears on the control panel's LCD display, press \checkmark .
5. After registration, press the EL-2601's tamper switch to terminate Test mode.
6. Before permanently mounting the unit, test the transmitter from the exact mounting position.
7. To remove the PCB, press the PCB release tab and carefully lift the board and slide the board away from the back cover.
8. The EL-2601 is able to operate in three modes: Magnetic Switch, Universal Transmitter or a combination of the two. If connecting a wired contact loop (N.C.), connect the terminal block as follows: 1 - Alarm; 2 - GND. For this purpose, a wiring knockout is provided in the back cover.
9. 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 – see Figure B.4.
10. To open the magnet's housing, insert a small screwdriver into one of the pry-off slots located at either end of the magnet's back cover and lift to separate from the front cover.
11. 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.

Jumper Position	Operation Mode
Pins 1&2	Universal Transmitter
Pins 2&3	Magnetic Switch
Jumper Removed	Magnetic Switch/ Universal Transmitter

Table B.2: Operation Mode Jumper

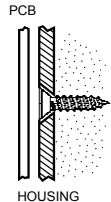


Figure B.4: Mounting Screw Position



Do not install the magnet further than 1cm from the transmitter.

12. Test the transmitter, making certain that the LED is lit when opening the door/window and again when closing.
13. Close the front covers of the transmitter and the magnet.

Universal Transmitter (EL-2602)

The EL-2602 is a universal transmitter that includes a single output for use in a wide range of wireless applications.

Installation Procedure

To install universal transmitters:

1. To open the housing, insert a small screwdriver at the bottom of the unit between the front and back cover and twist the screwdriver to release the cover.
2. Remove the divider separating the battery from the contacts on the battery holder. When you apply power and the Tamper switch is open, the EL-2602 enters Test mode during which a transmission is sent every few seconds. You can terminate Test mode by closing the Tamper switch. Test mode is automatically terminated after approximately five minutes.
3. From the Programming menu, select Devices, Zones [911].
4. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When **Save?** appears on the control panel's LCD display, press ✓.
5. After registration, press the EL-2602's tamper switch to terminate Test mode.
6. Before permanently mounting the unit, test the transmitter from the exact mounting position.
7. To remove the PCB, press the PCB release tab, carefully lift the board and slide the board away from the back cover.

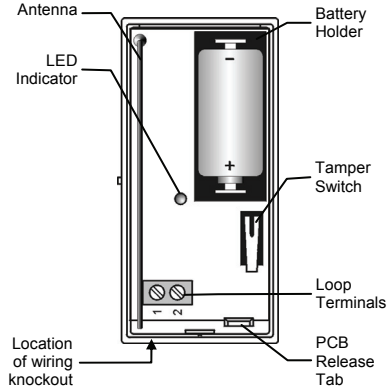


Figure B.5: EL-2602 (cover off)



When handling the PCB, do not apply pressure on the antenna.

8. Knockout the wiring hole in the back cover.
9. Thread the wires through the wiring hole.
10. Mount the back cover to the wall 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 – see *Figure B.4*.
11. Connect the terminal block as follows: 1 - Alarm; 2 - GND.
12. Test the transmitter, making certain that the LED is lit during transmissions.
13. Close the front cover of the EL-2602.

Glassbreak Sensor (EL-2606)

The EL-2606 is an intelligent acoustic glassbreak sensor with an incorporated wireless transmitter.

Mounting Considerations

The EL-2606 acoustic sensor is omnidirectional, providing 360° coverage. The coverage is measured from the sensor to the point on the glass farthest from the sensor. The sensor can be mounted as close as 1m from the glass.

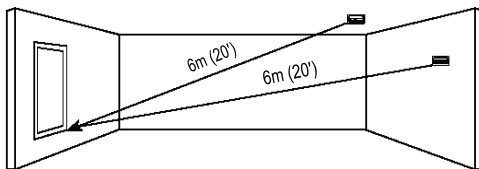


Figure B.6: Acoustic Sensor Range Measurement (plate, tempered, laminated and wired glass)

Sensor range:

- If mounting on the ceiling, the opposite wall or adjoining walls, the maximum range is 6m for plate, tempered, laminated and wired glass.
- For armor-coated glass, the maximum range is 3.65m.

Minimum recommended glass size:

- 0.3m x 0.6m

Glass thickness:

- Plate: 2.4mm to 6.4mm
- Tempered: 3.2mm to 6.4mm
- Wired: 6.4mm
- Laminated: 3.2mm to 6.4mm

For best detection:

- The sensor must always be in direct line of sight of all windows to be protected.
- If mounting on the wall, try to install the sensor directly opposite the protected window. If this is not possible, adjoining side walls are also a good location.
- If mounting on the ceiling, install the sensor 2-3m into the room.
- Avoid installing in rooms with lined, insulating or sound deadening drapes.
- Avoid installing in rooms with closed wooden window shutters inside.
- Avoid installing in the corners of a room.

The EL-2606 is best suited to rooms with moderate noise.



The sensor may not consistently detect cracks in the glass, bullets which break through the glass or glass breaking around corners and in other rooms. Glassbreak sensors should always be backed up by interior protection.

For best false alarm immunity:

- Locate the sensor at least 1.2m away from noise sources (televisions, speakers, sinks, doors, etc.).
- Avoid rooms smaller than 3m x 3m and rooms with multiple noise sources.
- Do not use where white noise, such as air compressor noise, is present (a blast of compressed air may cause a false alarm).
- Do not define the zone as 24hr. It is recommended to register the EL-2606 to a perimeter arming group that arms the perimeter doors and windows of the premises.
- Avoid humid rooms – the EL-2606 is not hermetically sealed. Excess moisture can eventually cause a short and a false alarm.

Areas to avoid:

- Glass airlocks and glass vestibule areas
- Noisy kitchens
- Residential car garages
- Small utility rooms
- Stairwells
- Small bathrooms
- Other small acoustically live rooms

For glass break protection in such applications, use shock sensors on the windows or window frames connected to an EL-2602 universal transmitter.

Installation Procedure

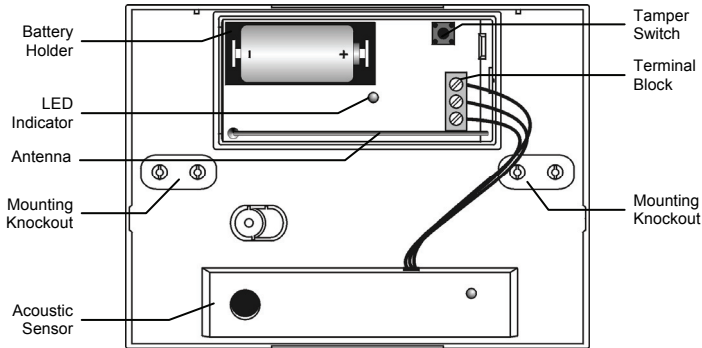


Figure B.7: EL-2606 (cover off)

1. Open the housing using a small flat-head screwdriver to separate the base from the cover.
2. Remove the insulator separating the battery from the contacts on the battery holder. When you apply power and the Tamper switch is open, the EL-2606 enters Test mode during which a transmission is sent every few seconds. You can terminate Test mode by closing the Tamper switch. Test mode is automatically terminated after approximately five minutes.
3. From the Programming menu, select Devices, Zones [911].
4. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When **Save?** appears on the control panel's LCD display, press ✓.
5. After registration, press the EL-2606's tamper switch to terminate Test mode.
6. Choose a suitable mounting location according to the guidelines in the previous section.
7. Before permanently mounting the unit, test the acoustic sensor and the transmitter from the exact mounting position. For further information on testing the acoustic sensor, refer to the following section, Testing Procedures.
8. Knock out the required mounting holes on the back cover.
9. Mount the unit to the wall using the mounting screws provided.
10. Write the number of the zone on the sticker provided and affix the sticker inside the front cover for future reference.
11. Close the front cover making sure that it snaps shut.

Testing Procedure

The Pattern Recognition Technology™ of the EL-2606 ignores most of the sounds that could cause a false alarm (including glass-break testers). In order to test the EL-2606, you must set the unit to Test mode. In Test mode, processing of the upper and lower frequencies is disabled. This means that the EL-2606 is only listening for mid-range frequencies reproduced by the glassbreak tester. It's these mid-range frequencies that determine the sensor's range.

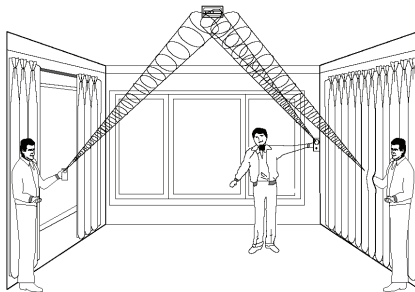


Figure B.8: Testing the EL-2606



In Normal mode, the tester will not activate the sensor unless held directly over the sensor.

Test the sensor using the Electronics Line GBS7 or Sentrol 5709C hand-held tester.

1. If using the 5709C tester, set the tester to tempered glass. The 5709C tester has a different setting for each type of glass. The tester should always be set for tempered or laminated glass (either is correct and both have the same range) unless the installer is certain that all the glass to be protected is plate glass.
2. Hold the tester speaker directly on top of the sensor and activate the tester; the sensor generates an alarm and then enters test mode for one minute. When in test mode, the LED on the sensor flashes continuously. You can extend the test mode time by firing the tester at the sensor at least once a minute.



Each time the sensor generates an alarm, it also goes into Test mode for one minute.

3. Hold the tester near the surface of the glass and aim the tester at the EL-2606. If drapes or blinds are present, test with the hand-held tester behind the closed drapes or blinds.
4. Hold down the test button. When the LED on the sensor goes solid momentarily, the glass is within detection range.
5. If the LED does not go solid, but simply continues blinking, re-position the sensor closer to the protected windows and retest. This may require adding additional sensors in order to achieve adequate coverage. It is very rare that the sensor will not activate within its stated range of coverage. In this case check the battery in the hand-held tester. A new tester battery is likely to restore the range.
6. Test mode automatically terminates approximately one minute after the last activation of the hand-held tester.



Room acoustics can artificially extend the range of a glassbreak sensor. The specified range of the EL-2606 has been established for worst-case conditions. While the sensor is likely function at the extended range, it may miss a minimum output break or room acoustics may be changed at some future time bringing sensor range back into normal 6m conditions. Do not exceed the rated range of the sensor regardless of what the tester shows!

Hand Clap Test

The Hand Clap test enables you to test the EL-2606 while in Normal mode. This test checks the sensors power supply, microphone and circuit board.

To perform a Hand Clap test

- Clap your hands loudly under the sensor; the LED flashes twice but an alarm is not generated.

Smoke Detector (EL-2603)

The EL-2603 is a brand-name smoke detector with an integrated Electronics Line 3000 transmitter.

Installation Procedure

The following procedure explains the installation of the EL-2603 wireless smoke detector and its registration to the receiver. For further information regarding the smoke detector's location, test procedures, maintenance and specifications, refer to the manufacturer's installation instructions provided with this product.

To install smoke detectors:

1. Open the cover by lifting the opening tab while firmly holding the base with your other hand.
2. Push the cover backwards to separate the cover from the base.
3. Install a 9V battery into the detector's battery snap.
4. Insert the Test jumper; the EL-2603 enters Test mode and the LED flashes every few seconds.
5. From the Programming menu, select Devices, Zones [911].
6. Select the zone to which you want to register the transmitter; the system initiates Registration mode. When **Save?** appears on the control panel's LCD display, press ✓.
7. After registration, remove the Test jumper and place it over one pin for storage.
8. Before permanently mounting the unit, test the transmitter from the exact mounting position.
9. Attach the mounting base to the ceiling using the screws provided.
10. Replace the cover onto its hinges and close the cover until it snaps together with the base.

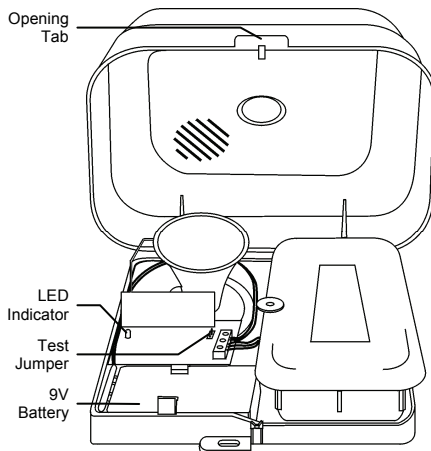


Figure B.9: EL-2603 (cover open)

Keyfobs (EL-2611/EL-2614)

The EL-2611 and EL-2614 are keyfob transmitters that are supported by the *infinite Broadband* system.

Registration Procedure

To register keyfobs:

1. From the Programming menu, select Devices, Keyfobs [912].
2. Select the keyfob you want to register; the system initiates Registration mode.
3. Press a button, making sure that the keyfob's LED lights up when the button is pressed.
4. Press the same button again. When **Save?** appears on the control panel's LCD display, press ✓.

EL-2611

The EL-2611 is a one-button transmitter that generates a Medical Emergency 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.

When the battery is low, the EL-2611's LED flashes during transmission and a Low Battery signal is sent to the receiver. When either of these two indications are observed, replace the unit.

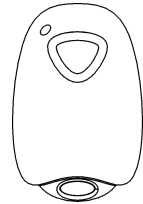


Figure B.10: EL-2611



Figure B.11: EL-2614

EL-2614

The EL-2614 is a four-button keyfob transmitter that offers a number of functions including arm, disarm and SOS Panic.

When the battery is low, the EL-2614's LED flashes during transmission and a Low Battery signal is sent to the receiver. When either of these two indications are observed, replace the batteries.

To replace the batteries:

1. Insert a small screwdriver into the pry-off slot – see *Figure B.12* Carefully twist the screwdriver to separate the front and back of the casing.
2. Observing correct polarity, replace the batteries (3V lithium, size: CR1225).
3. Close the casing making sure that the front and back click shut.

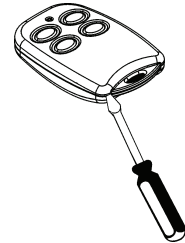


Figure B.12: Opening the EL-2614's Casing

Wireless Keypads (EL-2620/EL-2640)

The EL-2620 and EL-2640 are one-way wireless keypads primarily designed as additional arming stations, including three arming keys that enable Full, Part or Perimeter arming modes. Pressing the Full and Perimeter buttons simultaneously generates an SOS panic alarm. Additionally, the keypad may be used to control Home Automation modules.

The EL-2620 also includes an additional Cancel key, ☉, that clears the keypad in the event that a key is pressed by mistake while entering a code, for example. This key causes the keypad to disregard what was previously entered enabling the user to start again.

Registration Procedure

To register wireless keypads:

1. From the Programming menu, select Devices, Keypads [914].
2. Select the keypad you want to register; the system initiates Registration mode.

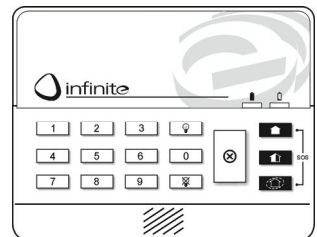


Figure B.13: EL-2620

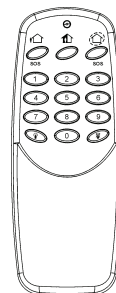


Figure B.14: EL-2640

3. Press a button on the keypad making sure that a LED lights up when the button is pressed.
4. Press the same button again. When **Save?** appears on the control panel's LCD display, press ✓.

Battery Replacement (EL-2620)

Every time a key is pressed, one of the battery status LEDs is lit. When the battery needs to be replaced, the red Low Battery LED is lit.

To replace the battery:

1. Insert a small screwdriver into the pry-off slots at the bottom of the unit and twist to remove the back cover.
2. Observing correct polarity, replace the battery (9V, alkaline).
3. Replace the back cover making sure that the two covers click shut.

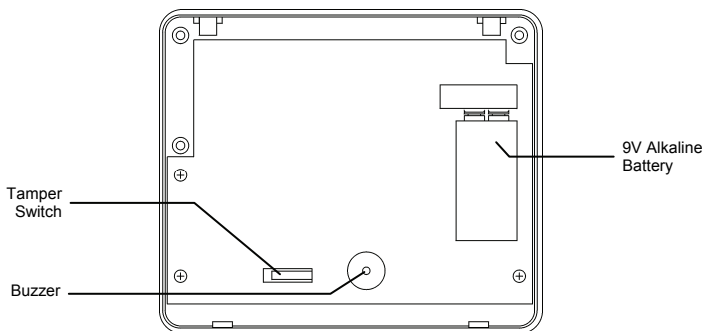


Figure B.15: EL-2620 (back cover off)

Battery Replacement (EL-2640)

When the battery is low, the EL-2640's LED flashes during transmission.

To replace the battery:

1. Remove the battery cover located at the rear of the unit. To do so, press the release tab using a small screwdriver and lift the cover away from the EL-2640's plastic housing.
2. Observing correct polarity, replace the battery (9V, alkaline).
3. Replace the battery cover making sure that it clicks shut.

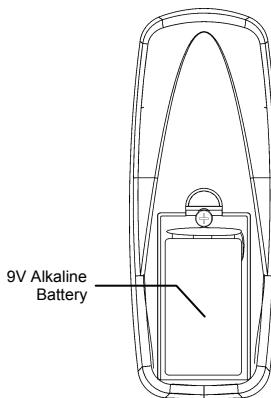


Figure B.16: EL-2640 (battery cover off)

Transmitter Specifications

The technical specifications for the transmitters that appear in this appendix are listed below. All transmitters are available in 868.35, 433.92 or 418MHz FM frequencies.

EL-2600

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 30mA (transmission)
6µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 14 x 14m
Pulse Count: 1, 2 or 3 Jumper Selectable
LED Indicator: Jumper Selectable
Adaptive Temperature Compensation
RFI Immunity: 30V/m
Operating Temperature: -10 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 60 x 45mm

EL-2600PI

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 30mA (transmission),
6µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 12 x 12m
Pulse Count: 1, 2 or 3 Jumper Selectable
LED Indicator: Jumper Selectable
Adaptive Temperature Compensation
RFI Immunity: 30V/m
Operating Temperature: -10 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 60 x 45mm

EL-2645

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 30mA (transmission)
12µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 14 x 14m
Pulse Count: 1, 2, 3 or Adaptive
LED Indicator: Selectable
Adaptive Temperature Compensation
RFI Immunity: 30V/m
Operating Temperature: -10 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 60 x 45mm

EL-2645PI

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 30mA (transmission),
12µA (standby)
Pyroelectric Sensor: Dual Element
Maximum Coverage: 12 x 12m
Pulse Count: 1, 2, 3 or Adaptive
LED Indicator: Selectable
Adaptive Temperature Compensation
RFI Immunity: 30V/m
Operating Temperature: -10 to 60°C
Fire Protection: ABS Plastic Housing
Dimensions: 110 x 60 x 45mm

EL-2601/EL-2602

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 25mA (transmission)
10µA (standby)
Loop Input Voltage Range: 0-15VDC/AC
(peak to peak)
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 65 x 30 x 25mm

EL-2603

Antenna: Built-in Internal Whip
Current Consumption: 30mA (transmission),
20µA (standby)
Power: 9V Alkaline Battery
RFI Immunity: 40V/m
Operating Temperature: 0 to 60°C
Dimensions: 138 x 118 x 44mm

EL-2606

Antenna: Built-in Whip
Power: 3.6V ½ AA Lithium Battery
Current Consumption: 25mA (transmission)
30µA (standby)
Microphone: Omni-directional electret
Maximum Range: 6m (plate, tempered,
laminated and wired glass)
3.65m (armor-coated glass)
RFI Immunity: 20V/m
Operating Temperature: 0 to 50°C
Dimensions: 80 x 108 x 43mm

EL-2611

Antenna: Built-in Whip
 Power: Non-replaceable battery
 RFI Immunity: 40V/m
 Operating Temperature: 0 to 60°C
 Dimensions: 60 x 40 x 15mm

EL-2614

Antenna: Built-in Whip
 Power: 2 x 3V Lithium Battery
 Size CR1225
 Current Consumption: 16mA (transmission)
 2µA (standby)
 RFI Immunity: 40V/m
 Operating Temperature: 0 to 60°C
 Dimensions: 62 x 42 x 15mm

EL-2620

Antenna: Printed on PCB
 Current Consumption: 26mA (transmission)
 2µA (standby)
 Power: 9V Alkaline Battery
 RFI Immunity: 40V/m
 Operating Temperature: 0 to 60°C
 Dimensions: 130 x 110 x 28mm

EL-2640

Antenna: Printed on PCB
 Current Consumption: 25mA (transmission)
 3µA (standby)
 Power: 9V Alkaline Battery
 RFI Immunity: 40V/m
 Operating Temperature: 0 to 60°C
 Dimensions: 128 x 49 x 27mm

**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 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.

ELECTRONICS LINE Ltd (EL3K) - LIMITE DE GARANTIE

ELECTRONICS LINE (EL3K) LTD ET SES FILIALES garantit ses produits pièces et main-d'oeuvre, dans le cadre d'une utilisation et d'un entretien normal, pour une période de (Produits radio – 12 mois, Centrales 2 Ans, Détecteurs bi-technologie 2 Ans, Détecteurs IR filaires 3 Ans) A partir de la date de vente.

L'obligation d'EL3K se limite, suivant ses conditions et dans le cadre de la garantie, à l'échange ou à la réparation sans frais de tout produit reconnu défectueux. En cas de panne, contacter le professionnel qui a effectué l'installation du système de sécurité et qui l'entretient régulièrement. Afin d'exercer la garantie, l'utilisateur ou l'acheteur doit renvoyer le produit à EL3K. en port payé avec assurance. Après réparation ou échange, EL3K prend à sa charge les frais de réexpédition du(des) produit(s) sous garantie. EL3K ne peut en aucun cas, être tenu pour responsable, des actions entreprises pour le démontage et la réinstallation des produits.

Cette garantie ne s'applique pas si l'appareil, ou l'un de ses sous-ensembles, a été réparé ou entretenu par un tiers en dehors d'un service de maintenance agréé par ELECTRONICS LINE. De même, la garantie est invalidée si le produit a été installé de manière incorrecte, s'il en a été fait mauvais usage, s'il a été transporté sans ménagements, altéré, endommagé ou s'il a subi une catastrophe naturelle. Enfin, la garantie ne s'applique pas non plus, dans le cas où les numéros de série figurant normalement sur l'appareil ont été altérés, rendus illisibles ou effacés.

Il n'est donné aucune garantie expresse ou implicite de qualité marchande ou d'adéquation à un usage particulier. Toute action concernant le non respect de toute garantie, incluant mais ne se limitant pas à toute garantie implicite de qualité marchande, doit être engagée durant les six mois courant après la fin de la période de garantie. EL3K ne sera en aucune façon tenu responsable envers qui que ce soit de tout dommage indirect ou accessoire résultant du non respect de ceci ou toute autre garantie, expresse ou implicite, ou de tout autre élément de responsabilité sur une base quelconque, même si la perte ou le dommage résulte de la négligence ou d'une faute de la part d' EL3K.

Electronics Line n'est en aucun cas responsable de l'augmentation du prix de vente du produit, de toute perte ou dommage direct, indirect, accidentel, consécutif ou provenant d'un défaut du produit. PAR VOIE DE CONSEQUENCE, E.L. N'ENCOURRA AUCUNE RESPONSABILITE POUR UN QUELCONQUE DOMMAGE CORPOREL, DOMMAGE MATERIEL OU AUTRE PERTE QUI POURRAIT ETRE INVOQUEE POUR CAUSE DE NON DELIVRANCE D'UNE ALARME PAR LE PRODUIT. La garantie mentionnée ci-dessus ne pourra être étendue, réduite ou modifiée. Aucune obligation ou responsabilité ne pourront être imputées à EL3K. pour tout conseil technique ou service lié à la commande de marchandises par l'acheteur.

Cette garantie remplace toute autre garantie ou obligation précédente. Elle est la seule garantie faite par EL3K Il n'est admis aucune extension, ni amendement des dispositions de la présente garantie, que ce soit sous forme écrite ou verbale. EL3K ne reconnaît, ni n'autorise, qui que ce soit à agir en son nom afin de modifier ou d'appliquer toute autre garantie ou responsabilité relative aux produits.

EL3K RECOMMANDE D'EFFECTUER CHAQUE SEMAINE UN TEST DU SYSTEME.

Avertissement : en dépit des tests effectués fréquemment, le système peut ne pas fonctionner correctement. Cette défection peut être due, mais ne se limite pas, aux événements suivants : sabotage, interruption des liaisons électriques ou de communications. EL3K ne fait aucune déclaration selon laquelle les produits qu'il vend ne pourront pas être mis en péril ou en échec; selon laquelle ces produits empêcheront tout risque de dommage corporel ou de perte de propriété en cas de cambriolage, de vol, d'incendie ou autre; ou selon laquelle ces produits fourniront en toutes circonstances une alarme ou une protection appropriée. Un système d'alarme correctement installé et entretenu ne peut prétendre à d'autres fins que de limiter les risques de cambriolage, de vol, d'incendie ou de tout autre événement susceptible de se produire et qu'il ne constitue nullement une assurance ou une garantie contre la survenance d'un tel. Par conséquent, l'installateur doit à son tour avertir son client afin que ce dernier prenne toutes les précautions nécessaires à sa sécurité, incluant mais ne se limitant pas à : fuir les locaux et appeler la police ou les pompiers, afin de limiter les risques de dommages corporels et/ou matériels.

EL3K n'assure ni les biens, ni la sécurité de la famille de l'utilisateur ou de ses employés, et limite sa responsabilité pour toute perte ou dommage y compris tous dommages indirects ou accessoires au prix de vente d'origine de son produit, indépendamment de la cause de cette perte ou dommage. Au cas où l'utilisateur souhaiterait obtenir une couverture plus complète, EL3K obtiendra, à la seule charge de l'utilisateur, une assurance complémentaire en sus de la propre police d'assurance de l'utilisateur, pour un coût qui sera déterminé par l'assureur d'EL3K sur demande écrite de l'utilisateur, expédiée par courrier recommandé avec accusé de réception à l'adresse du siège social d'EL3K et à réception du paiement par l'utilisateur de la prime annuelle d'assurance.

Certains pays ou états interdisent la limitation de durée de garantie implicite ainsi que l'exclusion ou limitation de tous dommages indirects ou accessoires, et appliquent des mesures différentes concernant la limitation de responsabilité pour les fautes lourdes ou ordinaires, et il se peut donc que les limitations ou exclusions précédentes ne s'appliquent pas à votre cas. La présente garantie vous confère des droits légaux spécifiques et il se peut que vous bénéficiiez d'autres droits, différents selon les pays ou états.



Electronics Line

Electronics Line USA

5637 Arapahoe Avenue
Boulder, CO 80303
Tel: (800) 683-6835
Fax: (303) 938-8062

Electronics Line 3000 Ltd.

2 Granit St.
Kiryat Arie Industrial Zone
POB 3253
Petah Tikva 49130 Israel
Tel: (+972-3) 918-1333
Fax: (+972-3) 922-0831

Electronics Line UK

Unit 7, Leviss Trading Estate
Station Road, Stechford
Birmingham B33 9AE
Tel: (+44-121) 789-8111
Fax: (+44-121) 789-8055

Electronics Line France

Zi 61 Rue du Marche Rollay
94500 Champigny Sur Marne
Tel: (+33-1) 45.16.19.20
Fax: (+33-1) 45.16.19.29
www.sectec.fr

www.electronics-line.com

