GUARDPOST 4G

WIRELESS SECURITY SYSTEM
WITH 4G MONITORING
& TWO WAY VOICE

MADE IN AUSTRALIA

THE WORLD'S SMARTEST WIRELESS INTRUDER ALARM SYSTEM

Installation, Programming & Operation Manual

Rev 1.3

CORPORATION

www.ness.com.au

National Customer Service Centre
Ph: 1300 551 991
techsupport@ness.com.au

Quality
ISO 9001
NSW Head Office only

MADE IN AUSTRALIA

Ness Guardpost 4G
Installation, Programming & Operation Manual
Rev 1.3

Document Part No: 890-488
November 2023

For the products:
106-305S Guardpost 4G

WARNINGS & NOTICES

Ness Corporation manufacturing processes are accredited to ISO9001 quality standards and all possible care and diligence has been applied during manufacture to ensure the reliable operation of this product. However there are various external factors that may impede or restrict the operation of this product in accordance with the product's specification.

These factors include, but are not limited to:

1. Erratic or reduced radio range (if radio accessories are installed). Ness radio products are sophisticated low power devices, however the presence of in-band radio signals, high power transmissions or interference caused by electrical appliances such as Mains Inverters, Wireless Routers, Cordless Phones, Computers, TVs and other electronic devices may reduce radio range performance. While such occurrences are unusual, they are possible. In this case it may be necessary to either increase the physical separation between the Ness receiver and other devices or if possible change the radio frequency or channel of the other devices.

2. Unauthorised tampering, physical damage, electrical interruptions such as mains failure, electrical spikes or lightning.

3. Solar power inverters are a known source of electrical interference. Please ensure that this product and all associated cabling is installed at least 3 metres away from a solar power inverter and its cabling.

WARNING: Installation and maintenance to be performed only by qualified service personnel.

CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries in accordance with local regulations.

CONTENTS

GUARDPOST FEATURES

- 4G dialler with SMS/Audio/Contact ID/ArmorIP/CSV reporting

- Two-Way-Voice monitoring and remote arm/disarm

- SMS remote arm/disarm

- SMS remote programming

- Onboard PIR for 15m x 15m coverage plus optional external devices

- Supports up to 24 supervised and encrypted radio devices

- Supports Ness radio PIRs, radio reed switches, radio smoke detector, radio keys

- Scrolling LED display for easy to read visual display

- Voice annunciation for status, events & user instructions

- Dual Home modes for zoned arming

- Strobe light differentiation for arm/disarm

- Onboard 124dBM siren for an extra loud audible deterrent

- Extensive event memory accessed via the scrolling LED display

- Front panel push-button adjustment for voice & internal beeps volume control

- Sophisticated power management for long battery life

- Solar cell charging support

- Proprietary encryption algorithm for secure comms between radio devices and Guardpost

- Radio Jamming / Radio Substitution detection

- Auxiliary outputs for optional external sirens, strobe and radio key AUX operation

INTRODUCTION

Guardpost is a fully self contained security system including an on-board motion sensor, loud siren, and wireless receiver for remote sensors and Arm/Disarm radio keys.

Guardpost's onboard 4G dialler gives it complete independence from landlines and allows reporting in Contact ID format back to base, audible voice reporting to any telephone, SMS reporting to mobile phones, SMS arming/arming/programming and even Two Way Voice communications for alarm verification and user safety.

Guardpost not only visually reports all events to the user via its large, bright alphanumeric display, it actually speaks to the user to report events and advises on the action to take.

Guardpost uses the latest microprocessor technology ensuring the highest level of security and dependability. The wireless radio keys utilise proprietary encryption algorithms for highest security.

Detection devices such as wireless passive infrared detectors and wireless reed switches also offer a high level of security through the use of programmable supervision techniques and constant monitoring of their battery condition.

Guardpost also helps resolve the growing issue of manpower when it comes to installation. Minimal programming is required allowing a comprehensive system to be installed in under one hour and a basic system in minutes.
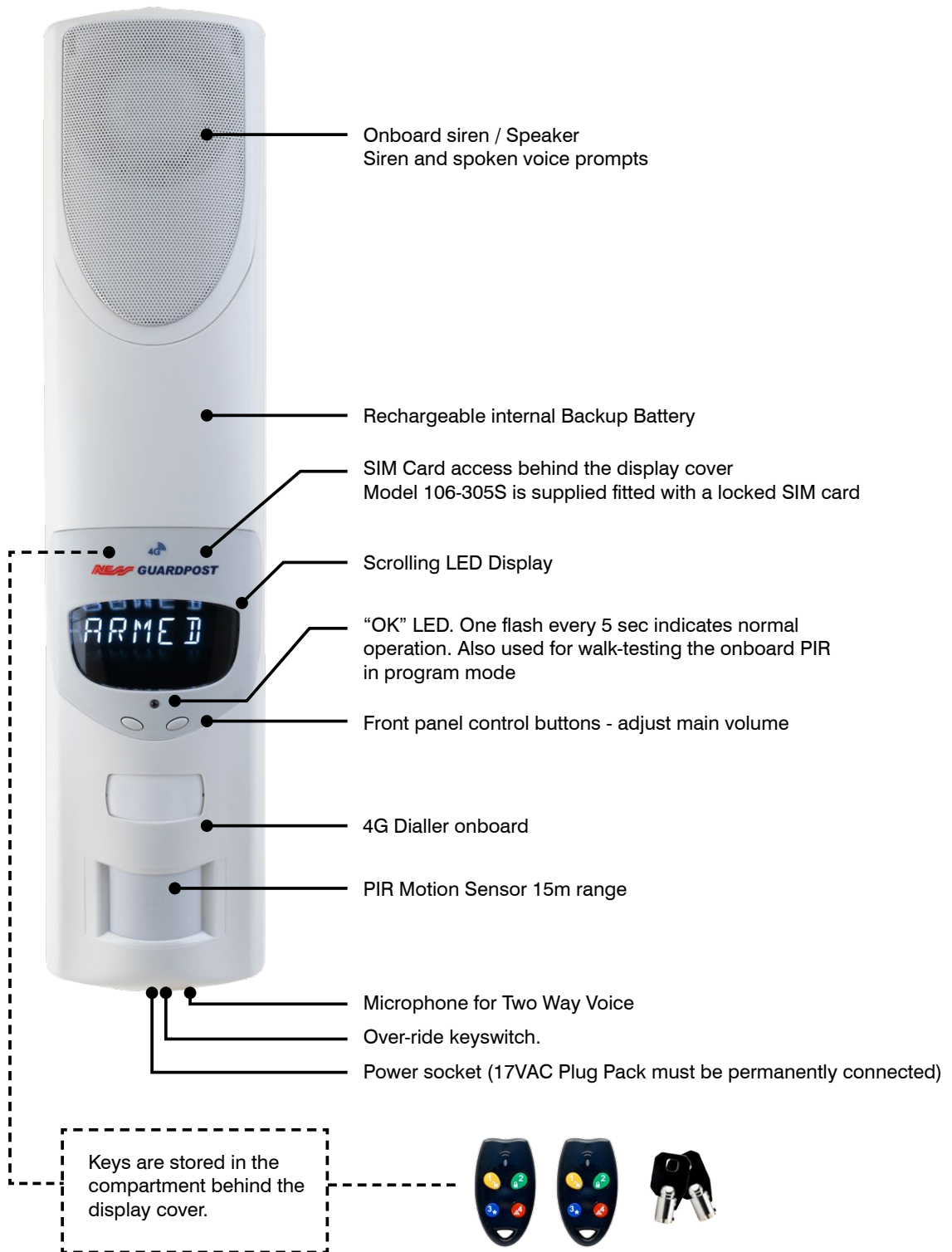
Guardpost is made in Australia by Ness Corporation to world class standards using the latest surface mount technology and state of the art in-circuit probe testers, together with strict process controls and adherence to an ISO9001 Quality Assurance Program, ensuring a quality product and a long service life.

COMPATIBILITY

Guardpost is compatible with Ness one-way radio transmitters.

PRODUCT OVERVIEW

Onboard siren / Speaker
Siren and spoken voice prompts

Rechargeable internal Backup Battery

SIM Card access behind the display cover
Model 106-305S is supplied fitted with a locked SIM card

Scrolling LED Display

"OK" LED. One flash every 5 sec indicates normal
operation. Also used for walk-testing the onboard PIR
in program mode

Front panel control buttons - adjust main volume

4G Dialler onboard

PIR Motion Sensor 15m range

Microphone for Two Way Voice

Over-ride keyswitch.

Power socket (17VAC Plug Pack must be permanently connected)

Keys are stored in the
compartment behind the
display cover.
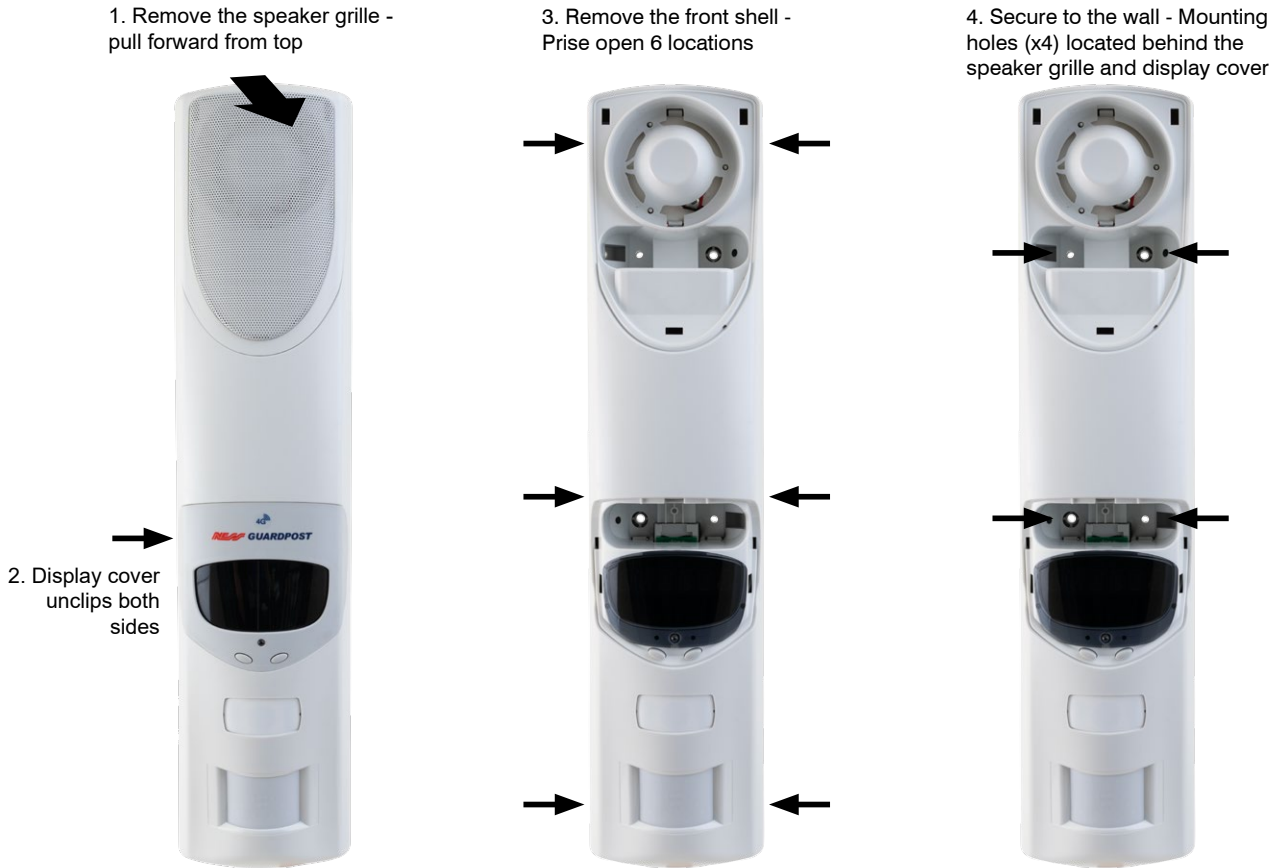
Guardpost is supplied with:

2 x Radio keys
2 x Over-ride keys
1 x 17VAC Plug Pack
2 x 3k3 resistors
1 x Wire loom & installation kit
1 x Ness SIM Card (some models)

INSTALLATION

The front cover forms a secure clamshell when Guardpost is installed. The unit must be removed from the wall before attempting to remove the front shell.
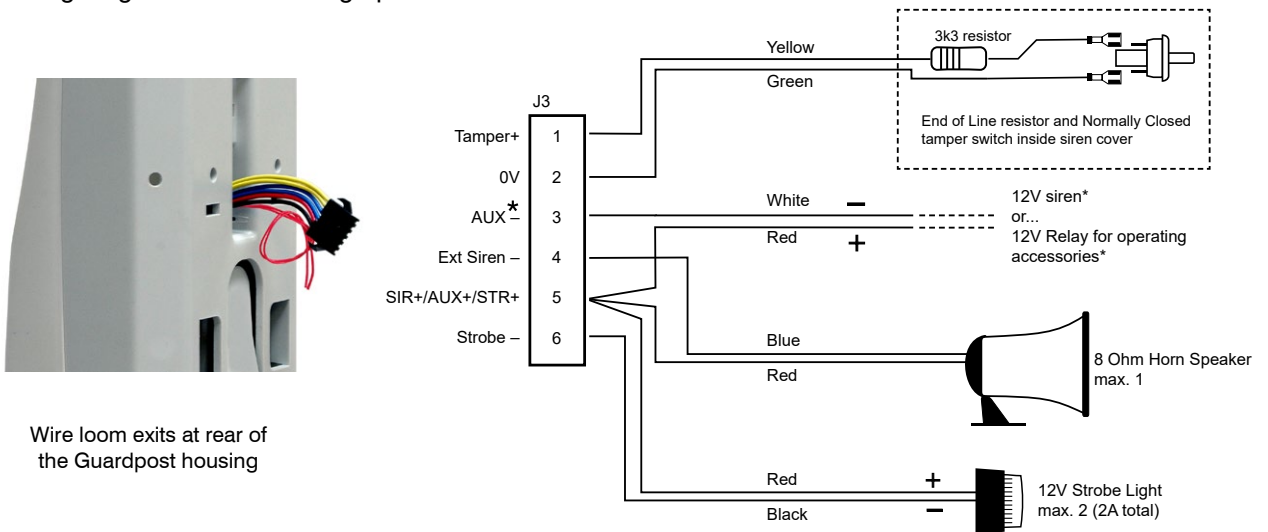
Screw mounting holes are provided for either flat wall mounting or corner mounting.

Guardpost should be mounted in a position which provides a clear field of view for the onboard PIR.

1. Remove the speaker grille - pull forward from top

2. Display cover unclips both sides

3. Remove the front shell - Prise open 6 locations

4. Secure to the wall - Mounting holes (x4) located behind the speaker grille and display cover

WIRING

Wiring diagram for connecting optional external sirens and strobe.

Wire loom exits at rear of the Guardpost housing

J3		
Tamper+	1	Yellow
0V	2	Green
AUX* −	3	White
Ext Siren −	4	Red
SIR+/AUX+/STR+	5	
Strobe −	6	Blue / Red

3k3 resistor

End of Line resistor and Normally Closed tamper switch inside siren cover

12V siren*
or...
12V Relay for operating accessories*

8 Ohm Horn Speaker max. 1

Red +
Black −
12V Strobe Light max. 2 (2A total)

* AUX output follows the siren output or can be operated by the AUX button on radio keys.
See AUXOUT programming, page 21

FLYING LEADS

| Red	AC	Optional External 17VAC power input and solar power input
Red	AC	

SIM CARD INSTALLATION

Your Guardpost may be supplied with a factory-fitted Ness (locked) SIM card or if you have a non-locked Guardpost 4G you can install your own standard SIM card as shown below.

Ness SIM cards must be activated online at www.activate.ness.com.au

If using a third party SIM card ensure that it's not PIN locked.
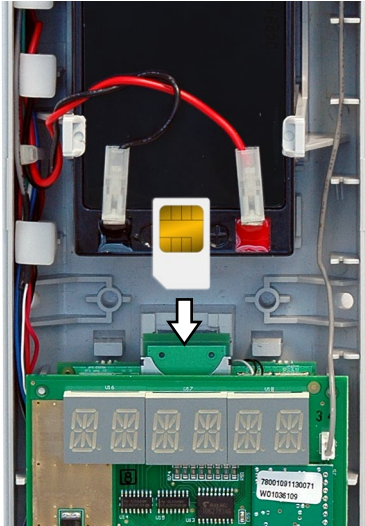
IF YOUR PANEL WAS SUPPLIED WITH A NESS SIM it must be used with the SIM provided.

The NESS SIM card provided must be activated for the dialler to operate. To activate go to **activate.ness.com.au**

If your panel is an unlocked model supplied without a Ness SIM the information above is not relevant.

The SIM slot is located above the LED display.

If your unit does not have a factory-fitted SIM, insert your own SIM card prior to fitting the cover.

Standard size SIM card required.

CELLULAR STATUS LED

The cellular comms status LED is visible in the compartment behind the display cover.

The LED indicates cellular network status.

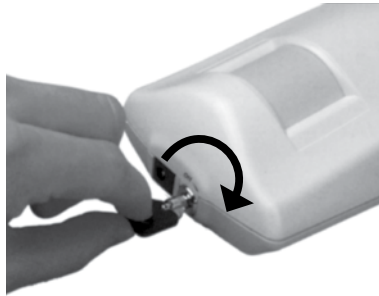Also see the CELL SIG cellular signal strength option, page 22.

Cellular Network status LED

LED OFF	4G dialler disabled
One flash per second	Network is not active
One flash every 3 seconds	Network OK

STARTUP

After mounting the Guardpost, plug in and turn on the AC plug pack. **The Plug Pack must remain permanently connected.**

To power-up the unit, turn the main keyswitch clockwise to the ON position.

The display will show the firmware revision number.

When the unit is powered-up it briefly allows entry into PROGRAM mode. See page 15.

Guardpost then enters the previous operational mode.

If the unit was in ARMED, HOME, or HOME 2 mode, it will show the mode on the display for 30 seconds. During this period triggers from the main PIR are ignored, allowing it time to settle.

Then the unit resumes normal operation in the mode displayed. This process will occur silently, without the usual arming sounds.

RADIO KEYS

The 4 button radio key is used for Arm, Disarm and Panic and also has an additional AUX button which can be programmed to operate the SG4 AUX output or add the optional 100-099 AUX Receiver for home automation functions such as lighting control or operating motorised garage doors.

DISARM

ARM

AUX

PANIC/ DURESS

ONBOARD AUX OUTPUT, See page 6

OPTIONAL AUX RECEIVER
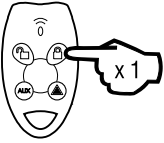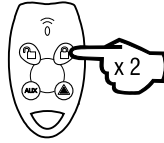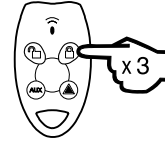
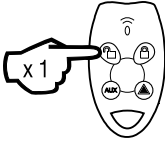Relay output to:
- Garage door controller
- Lighting
- Sprinkler systems
- Almost any electrical device

USER OPERATION

The system can be in one of four user modes, DISARMED, HOME, HOME 2 and ARMED.

From the DISARMED mode, an ON press enters ARMED mode, a second ON press enters HOME mode, and a third ON press enters HOME 2 mode (provided devices are programmed for these modes), as detailed in the following sections.

USER OPERATION MODES	ARMED	HOME	HOME2	DISARMED
HOW TO OPERATE USER MODES	x 1	x 2	x 3	x 1
DISPLAYS AND AUDIBLE FEEDBACK				
SCROLLING DISPLAY	ARMED Displayed for the duration of exit delay.	HOME Displayed for the duration of exit delay.	HOME 2 Displayed for the duration of exit delay.	OFF Displayed for 5 seconds.
OK LED	OFF	1 Flash every 2 seconds	Double Flash every 2 seconds	1 Flash every 5 seconds
VOICE	"ARMED" *	"HOME" *	"HOME TWO" *	"DISARMED" *
SIREN	INTERNAL SIREN# 1 chirp at start of exit delay* and 1 chirp at end of exit delay. EXTERNAL SIREN: 1 chirp at start of exit delay (if enabled).	INTERNAL SIREN# Home arming tone.	INTERNAL SIREN# Home2 arming tone.	INTERNAL SIREN# 3 chirps. EXTERNAL SIREN: 3 chirps (if enabled).
STROBE LIGHT (If installed)	Flash for 2 seconds.	Flash for 5 seconds.	Flash for 5 seconds.	Flash for 4 seconds.

* If the V-ARM option is enabled.

If the V-ARM option is disabled.

Note: At least one device must be programmed as HOME or HOME 2 for the system to allow arming in those modes.

ARM/DISARM BY SMS
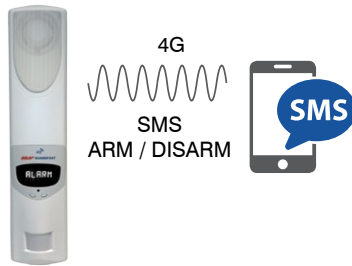
Guardpost supports remote programming by SMS (see page 26-28) and remote arming/disarming by SMS.

To arm/disarm Guardpost by SMS you must know the mobile phone number of the Guardpost's SIM card and the client account number.

SMS Commands

TO ARM	CCCC,arm
TO DISARM	CCCC,disarm

CCCC is the 4 digit client account number. (see page 21)

Examples

To ARM a Guardpost which has the client account number 1234:

Send this SMS to the Guardpost   1234,arm

Guardpost will reply with   Unit 1234: Armed

To DISARM the Guardpost:

Send this SMS to the Guardpost   1234,disarm

Guardpost will reply with   Unit 1234: Disarmed

Hints & Tips

The Arming and Disarming commands can be abbreviated "a" and "d" meaning you can simply send   1234,a   to Arm and   1234,d   to Disarm.

If you send an SMS in the wrong format, Guardpost will respond with:

Unit CCCC: Command error.

The SMS format requires a comma between each command and no spaces.

NOTES
- SMS commands must not include spaces.

- Arm/Disarm commands are not case sensitive.

- The dialler must be enabled to allow operation by SMS.

- SMS reply messages are sent to the mobile phone which sent the SMS commands - which can be any mobile phone.

- IMPORTANT NOTE.
  Guardpost may not respond to SMS commands immediately if the 4G module is in sleep mode.
  The state of the 4G module is dependent on the power management mode.
  See page 24.

RADIO DEVICE ALLOCATION

Guardpost supports up 24 Ness one-way radio devices including the main detector onboard.

This provides up to 23 radio allocations for any combinations of remote devices including radio keys, radio PIRs, radio reed switches, radio smoke detectors, radio keypad.

At least one radio key must be programmed.

Up to 23 additional devices

FRONT PANEL CONTROL BUTTONS

The font panel buttons adjust main volume for voice and beeps. Press the Left Button to select; press the Right Button to step through the volume levels (the last value selected becomes the new programmed value).

Selected options and values are announced by voice as well as displayed. The display extinguishes after a short period of inactivity.

LEFT BUTTON	RIGHT BUTTON
Adjust MAIN VOLUME - Press x 1	Main Volume 1 – 4

In Program mode, pressing the Left Button allows stepping backwards through the various options and devices.

MAIN MOTION DETECTOR

- The onboard PIR (SENSOR 1) conserves power using a lock-out timer after each detection.
- When disarmed, the lockout time is 4 minutes. When armed, the lockout time is 5 seconds between activations.
- The detection coverage of the onboard PIR can be walk-tested when the PULSE or RANGE options are selected in program mode. The main unit OK LED serves as the onboard PIR's alarm indicator when walk testing.

GUARDPOST MODE	MAIN PIR LOCKOUT TIME
DISARMED*	4 minutes
ARMED, HOME, HOME2	5 seconds
PULSE or RANGE is selected in Program mode	0 seconds to allow walk test

* Unless the onboard PIR is configured as CHIME

ALARM DISPLAYS

Intruder Alarms will sound the internal and external (if fitted) sirens and strobe flashes. The siren will turn off after the programmed siren time and the strobe will flash for 1 hour or 12 hours if the system is running on mains power.

Press the OFF button on a programmed Radio Key to cancel the alarm and disarm the GUARDPOST.

When disarming after an alarm, Guardpost will indicate an alarm has occurred by voice and by display. This warning may indicate that an intruder is still present. The source of the alarm is then displayed for 5 minutes, and logged to the event memory.

Intruder alarms are not indicated when the system is in ARMED, HOME or HOME 2 modes.

A time stamp is appended to each of the following alarm messages displayed when displayed. For example, if the alarm occurred within 24 hours, the time stamp is appended as: ... < 2 HRS < 15 MIN < AGO; for events older than 24 hours: ... < 1 DAY < 13 HRS < AGO.

DISPLAY	DESCRIPTION
ALARM < SENSOR < 1	ALARM from the onboard detector
ALARM < SENSOR < 2-23	ALARMS from radio devices such as radio PIRs, radio reed switches.
TAMPER < SIREN < BOX	SIREN TAMPER In ARMED mode, sound a full alarm & report to the central monitoring station when applicable. In HOME, HOME 2 or DISARMED modes, sound a low-volume warning sound & report. The warning will sound again for further Tamper deactivation/ reactivations. Arming and Disarming will clear the display.
TAMPER < SENSOR < 2-23	A Sensor has reported a tamper alarm. In ARMED mode, sound a full alarm & report to the central monitoring station when applicable. In HOME, HOME 2 or DISARMED modes, sound a low-volume warning sound & report. The warning will sound again for further Tamper deactivation/reactivations. Arming and Disarming will clear the display.
PANIC < KEY < 1-23	PANIC ALARM from a radio key or fixed radio panic button or radio medical key. On silencing a PANIC alarm (OFF button), the status display indicates which key caused the alarm.
MEDIC < KEY < 1-23	PANIC ALARM from a medical key. During the alarm the display will show "PRESS < OFF < TO < CANCEL < MEDIC < ALARM". On disarming, the status display indicates which key caused the alarm.
RADIO < JAMMED	Radio jamming signal detected. If a radio signal is detected in the operating bandwidth of the Guardpost the unit will go into ALARM mode if enabled.
RADIO < TAMPER	TAMPER Radio message that is not an original message has been received. (If RADSUB = ON). 1. A code that is a retransmitted code of an original message has been received to try to defeat the system. 2. 20 multiple messages have been received by the system to crack the encryption. Arming/Disarming the system will reset the count.

SYSTEM DISPLAYS

System troubles are indicated in the DISARMED mode. When DISARMING after a trouble alarm the GuardPost will display the type of trouble alarm with a time stamp.

The message will be displayed for 5 minutes.

DISPLAY	DESCRIPTION
BATTRY < KEY BATTRY < PANIC	A radio key or radio panic button has a low battery. The battery should be replaced. Some transmitters are sealed units designed to last for many years. These units should be replaced for new.
BATTRY < SENSOR < 2-23	A radio radio PIR or radio reed switch has a low. The battery should be replaced.
FAIL < SENSOR < 2-23	A supervision signal has not been received within the programmed supervision interval. (See the program option SUPVIS). Check that the sensor is present and working correctly. This only applies to supervised sensors.
OPEN < SENSOR < 2-23	A REED SWITCH is open on ARMING A reed switch detector programmed for Check mode operation was unsealed when entering ARMED, HOME or HOME 2 modes. The detector should be checked to ensure that it has sealed. A warning tone will sound at the end of EXIT DELAY when ARMED.
LOW < MAIN < BATTRY	MAIN BATTERY LOW The main unit battery is periodically load tested. A low battery condition is cleared immediately when mains power goes from off to on, or when battery passes load test.
FAULT < MAIN < BATTRY	MAIN BATTERY FAULT The main unit battery failed load-test immediately following recharge cycle. The alarm can be cleared by switching the over-ride switch off then on.
DIALER < RADIO < FAIL	DIALLER RADIO FAIL Guardpost was not able to communicate with the optional radio dialler. (If installed).

EVENT LOG

System alarm events are logged in memory and displayed with the time elapsed since the alarm occurred. Multiple alarms from the same device are logged only once, with the time stamp updated for each new repeat alarm.

In DISARMED mode, press OFF to step through the log. Once all logged alarms have been displayed, pressing OFF will clear the display. Pressing OFF again will redisplay the first event in the log, etc.

Entries in the log will cleared only when the cause of the alarm has been rectified, or when power is turned off using the key switch.

The alarm event log will store up to 5 events. If the log is full, logging a new event causes the oldest event to be discarded. Events older than 100 days will be discarded.

A time stamp is appended to each event when displayed. For example, if the alarm occurred within 24 hours, the time stamp is appended as: ... < 2 HRS < 15 MIN < AGO; for events older than 24 hours: ... < 1 DAY < 13 HRS < AGO.

POWER MANAGEMENT

Guardpost employs sophisticated power management software to maximise main battery life and increase the time between charging.

Guardpost can be operated in FULL TIME MAINS mode, BATTERY ONLY mode or SOLAR CELL charge mode.

In Full Time Mains Mode, Guardpost constantly trickle charges the main battery. **This is the default mode. The plug pack must be permanently connected.**

Battery Only mode and Solar Cell modes are low current modes designed to consume the minimal power by shutting down non-essential circuits and by the use of sleep/wake cycles. See the programming option POWER for more information.

In power conservation modes Guardpost can be operated for up to 1 month without recharging. In this case, Guardpost will initiate fast-charging mode for 24 hours once the mains charger is connected.

The OK light will remain on during fast charging only.

LOAD TEST

A battery test is performed by briefly applying a simulated load on power-up, every 24 hours, on disarming and 3 hours after the completion of a recharge cycle (only if mains was on at the end of recharge cycle, and no siren activity occurred after recharge period).

ALARMS

If a low battery is detected when mains is on, no alarm is displayed or reported, but the battery is recharged for 24 hours.

If a low battery is detected and mains is off, a LOW < MAIN < BATTRY alarm is displayed and reported if enabled, and the battery is recharged for 24 hours when mains comes on. When mains comes on, the alarm condition is immediately cleared and restored.

If a low battery is detected after the completion of a recharge cycle, a FAULT < MAIN < BATTRY alarm is displayed and unconditionally reported. If the battery passes a subsequent load test, this condition is restored.

SOLAR CHARGING

Guardpost has onboard support for power supply and charging by solar cells.

• Solar cell power input connects to the AC red wires for the solar connections.

• Select SLR-30, SLR-1H or SLR-2H power management mode.

• A 12V 10W-20W solar panel is recommended with max power output of 17.6V.

Guardpost makes efficient use of available solar power by switching between fast charge and float charge while monitoring the battery capacity at all times.

See Power Management Mode, page 24.

PROGRAMMING

1 Enter program mode
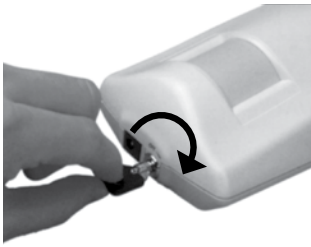
To enter program mode, turn on the main keyswitch.

The software revision number is briefly displayed.

2 To learn the first Radio Key

If the unit has no radio keys learned, the display will show LEARN KEY 1 until a radio key is learned.

Guardpost requires at least one radio key to be active before you can proceed with further programming.

Press Panic on the first radio key to learn the radio key.

The new device will be added to the next available slot, the new slot number is displayed and provides options to configure the new device."

Successful learning=beep, beep, beep-beep

3 To learn additional Radio Keys

If the Guardpost already has a radio key programmed it flashes LEARN and waits 10 seconds to receive a radio key message.

The procedure for learning additional radio keys is slightly different.

This requires the keyswitch to be turned on then *immediately* press and hold Panic on a new radio key for 8 seconds.

You may find it easier to hold down Panic while turning on the keyswitch. This eliminates any lag in sending the signal.

> Turn off the keyswitch > Press Panic on another radio key > Turn on the keyswitch > Continue to hold Panic for at least 8 seconds.

The display flashes READY and is waiting for a LEARN message from another new device.

At this step the system will exit program mode if a signal is not received within 10 seconds.

4 To learn other radio devices

When th display is flasdhing READY, send the Learn Signal from the new radio device.

See next page. How to send a LEARN signal.

5

The display will show the new Key or Sensor number.

New devices are added to the next available vacant slot.

6

Press the ON button on a valid radio key to view the sub-menu options for the device. See page 18 for sub-menu options for radio keys and radio devices.

Press OFF to return to LEARN.

Press ON to flash READY and learn another device, or press OFF to step through devices and program options.

PROGRAMMING

How to send a Learn Signal from radio devices

RADIO KEYS	Press PANIC for 8 seconds.	
RADIO PIRS RADIO SMOKE DETECTORS RADIO KEYPAD	Insert the battery.	
RADIO REED SWITCHES	UNENCRYPTED DEVICES Check Mode: Close the reed switch. (Move the magnet towards). Non-Check Mode: Open the reed switch. (Move the magnet away).	ENCRYPTED DEVICES Check Mode: Insert the battery with the reed switch closed. (Magnet on the reed switch). Non-Check Mode: Insert the battery with the reed switch open. (Magnet away from the reed switch).
	Reed Switch devices (door/window sensors) may be learned as a Checked device. This means the door or window needs to be closed before the system can be armed. If the sensor is not closed on arming the system will announce and display the sensor number. When learning devices, the OK LED turns on when Check mode operation is successfully programmed.	

Error Tone

When learning device an ERROR TONE could mean:

POSSIBLE CAUSE	REMEDY
1. The device is already programmed	Remove the battery from this device to prevent it sending signals while you program other devices.
2. The device is not compatible with the Guardpost (possibly a different radio protocol).	Check with your Ness branch.
3. The device might be too close to the Guardpost.	When enrolling/learning radio devices maintain at least 2m separation from the Guardpost to prevent errors caused by excessive signal strength.

Deleting a Radio Key or Sensor

The sub-menu for each enrolled radio key and sensor includes the option to ERASE. To delete the device select ERASE and press PANIC to store the selection. The display will then show LEARN, giving the user the option of reprogramming a new device into this particular slot. This allows a faulty device to be replaced while keeping the same slot number.

Programming Notes

• All programming is performed using an enrolled radio key.
• To prevent learning the wrong device, start programming with the batteries removed from all devices on site. Once a device is learned remove its battery until all devices are learned.
• Each time a programming change is made, the new value is stored immediately in non-volatile memory.
• Guardpost will flash FULL if an attempt is made to program a device when no slot is available. It will allow programmed devices to be viewed in sequence and erased if desired.
• A key cannot be used to erase itself. A device cannot be programmed more than once. Guardpost will give a long warning beep if either are attempted.
• Guardpost will automatically exit PROGRAM mode after 10 minutes of inactivity.

PROGRAMMING

Navigation in program mode

KEY 1 --- SENS 1 RANGE PULSE SIGNAL ...
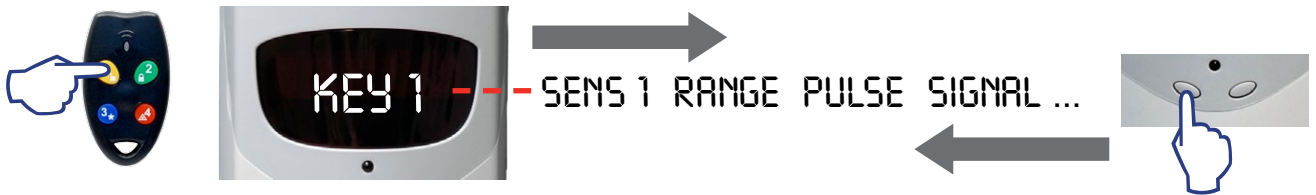
Press the OFF button on a valid radio key to step forward through the programming menu.

The LEFT front panel button cycles BACKWARD through the programming menu.

RANGE --- LOW HIGH

The currently programmed value will flash.

Press the ON button to cycle through the sub-menu options for a programming option.

RANGE --- LOW HIGH

The currently programmed value will flash.

Press the PANIC button to store the currently displayed value. The new value will then flash to indicate it is programmed.

To exit program mode

P-EXIT

Select P-EXIT from the programming menu.

Then press the ON button to exit program mode.

Otherwise Guardpost will automatically exit PROGRAM mode after 10 minutes of inactivity.

PROGRAMMING OPTIONS

KEY 1-23	RADIO KEYS

	Sub-menu
	KEY Enables the radio key for use as a user key with Arm, Disarm, Panic, Aux **(DEFAULT)**
	DURESS User key with PANIC button programmed for "DURESS" operation
	MEDIC Medical help key (behaves like Duress alarm)
	BELL [not used]
	NO PAN PANIC button disabled (except in Program mode); used for control of independent radio switch, e.g. garage door control
	ERASE Deletes the programmed radio key

SENS 1	ONBOARD PIR

	Sub-menu
	ALARM Active when ARMED, inactive when DISARMED **(DEFAULT)**
	HOME Active when ARMED mode or HOME mode
	HOME 2 Active when ARMED, HOME or HOME 2 modes
	FIRE 24 hour alarm, always active
	CHIME Chime* when DISARMED, inactive when ARMED, HOME or HOME 2 modes
	ACHIME ALARM/CHIME Alarm when ARMED, chime** when DISARMED, inactive when in HOME or HOME 2 modes
	HCHIME HOME/CHIME Alarm when ARMED mode, chime** when in HOME mode, inactive when in HOME 2 or DISARMED modes
	H2CHIM HOME 2/CHIME Alarm when ARMED mode, chime** when in HOME or HOME 2 modes, inactive when in DISARMED mode
	SILENT Active when ARMED, only does dialler reporting when triggered, no siren
	EXCLUD Disables the onboard PIR

SENS 2-23	RADIO DEVICES 2-23

Optional sensors can be any combination of up to 22 radio PIRs, radio reed switches, radio smoke detectors, radio keypad.	**Sub-menu**
	ALARM Active when ARMED, inactive when DISARMED **(DEFAULT)**
	HOME Active when ARMED mode or HOME mode
	HOME 2 Active when ARMED, HOME or HOME 2 modes
	FIRE 24 hour alarm, always active.
	CHIME* Chime when DISARMED, inactive when ARMED, HOME or HOME 2 modes
	ACHIME** Alarm when ARMED, chime when DISARMED, inactive when in HOME or HOME 2 modes
	HCHIME** Alarm when ARMED mode, chime when in HOME mode, inactive when in HOME 2 or DISARMED modes
	H2CHIM** Alarm when ARMED mode, chime when in HOME or HOME 2 modes, inactive when in DISARMED mode
	SILENT Active when ARMED, only does dialler reporting when triggered, no siren.
	ERASE Erase this device
	* Chime tone (no Dialler report or event logging)
	** Warning tone (no Dialler report or event logging)

PROGRAMMING OPTIONS

RANGE	ONBOARD PIR RANGE
	Sub-menu LOW Low range 8m **(DEFAULT)** HIGH High range 14m The onboard PIR can be walk-tested while this menu item is displayed.

PULSE	ONBOARD PIR PULSE COUNT
	Sub-menu 1 PULS 1 pulse count **(DEFAULT)** 2 PULS 2 pulse count 3 PULS 3 pulse count 4 PULS 4 pulse count The onboard PIR can be walk-tested while this menu item is displayed.

SIGNAL	RADIO SIGNAL STRENGTH CHECK
Check the signal strength of your radio keys and radio devices. Note: OK light indicates onboard PIR trigger.	**Sub-menu** SEND DEVICE Waiting for device message SENS 2-23 / LEVL 1-9 Detector received at signal strength level shown KEY 1-23 / LEVL 1-9 Key received at signal strength level shown Guardpost registers the first device received and displays the signal strength (1-9), and beeps a corresponding number of times. • Press ON to activate Signal Check • For a key, press PANIC; for a detector, activate the detector • Listen to beeps, view display • Press OFF to exit Signal Check • Press ON to re-activate Signal Check

RADJAM	RADIO JAMMING ALARM
	Sub-menu ON Enabled OFF Disabled **(DEFAULT)** SILENT Dialler report only (no local siren, display or logging). Limit of 10 reports; limit cleared on arming. Use for transparent monitoring of radio interference. When RADJAM is enabled Guardpost will generate a chime in modes DISARMED, HOME, HOME 2 if it receives a continuous source of Radio Frequency Interference (RFI). In ARMED mode the system will go into a full alarm mode.

RADSUB	RADIO MESSAGE SUBSTITUTION ALARM
	Sub-menu ON Enabled OFF Disabled **(DEFAULT)** When RADSUB is enabled Guardpost will generate a CHIME alarm in DISARMED or HOME or HOME 2 modes, and a full alarm in ARMED modes if it senses an intentional radio message substitution.

SUPVIS	RADIO SUPERVISION INTERVAL
	Sub-menu OFF Disabled **(DEFAULT)** 1 HR 4 HRS 8 HRS 16 HRS 24 HRS If enabled, a system alarm will occur if a valid supervisory message has not been received from supervised radio within the programmed interval.

PROGRAMMING OPTIONS

LOKOUT	ALARM LOCKOUT
	Sub-menu ON Enabled OFF Disabled **(DEFAULT)** Alarm lockout prevents multiple sirens sounding due to an alarm from the same device. The external siren will not sound again until the system is disarmed with the Disarm/Unlock button. The internal siren will always sound unless the lockout option is on and then the internal siren will behave like an external siren.

ENTRY	ENTRY DELAY TIME
Entry delay time applies to all enrolled devices.	**Sub-menu** 5 SEC **(DEFAULT)** 10 SEC 15 SEC 20 SEC 25 SEC 30 SEC Entry Delay Time allows time to disarm the system once a detector is activated. Guardpost is normally armed/disarmed by radio keys from outside the protected area but in some situations you may want to disarm from inside the premises.

EXIT	EXIT DELAY TIME
Exit delay time applies to all enrolled devices.	**Sub-menu** 5 SEC **(DEFAULT)** to 60 SEC in 5 second steps Exit Delay Time allows time to exit the premises once the system is armed. All radio devices are inactive during Exit Delay.

SIREN	SIREN RUN TIME
	Sub-menu 1 MIN 2 MIN 3 MIN 4 MIN 5 MIN **(DEFAULT)** Sets the run time in minutes for the internal and optional external siren (if fitted).

CHIRPS	EXTERNAL SIREN CHIRPS
External Siren ARMING: 1 Chirp DISARMING: 3 Chirps	**Sub-menu** ON Enabled **(DEFAULT)** OFF Disabled This option enables arm/disarm chirps for the external siren. External Siren Chirp applies only to Arming/Disarming. HOME or HOME 2 modes never chirp.

V-ARM	VOICE ANNUNCIATION FOR ARMING/DISARMING
When V-ARM is disabled the internal speaker will chirp on arming and disaming. **Internal Siren** ARMING: 1 Chirp DISARMING: 3 Chirps	**Sub-menu** ON Enabled **(DEFAULT)** OFF Disabled This option enables voice annunciation of Arrming and Disarming.

PROGRAMMING OPTIONS

V-ALRM	VOICE ANNUNCIATION FOR ALARMS
	Sub-menu ON Enabled **(DEFAULT)** OFF Disabled Enables voice annunciation of Alarm events.

V-BATT	VOICE ANNUNCIATION FOR BATTERY ALARMS
	Sub-menu ON Enabled **(DEFAULT)** OFF Disabled Enables voice annunciation of low battery events.

V-FALT	VOICE ANNUNCIATION FOR SYSTEM FAULTS
	Sub-menu ON Enabled **(DEFAULT)** OFF Disabled Enables voice annunciation of system faults.

AUX OUT	AUX OUTPUT
	Sub-menu OFF Disabled for radio keys **(DEFAULT)** In this case the AUX output follows the siren output TOGGLE AUX button on a valid radio key Toggles the AUX output PULSE AUX button on a valid radio key Pulses the AUX output Enables operation of the AUX output. See page 6, Wiring of the external outputs.

OPEN	OPEN/CLOSE REPORTS
Applicable when using central station, Audible or SMS monitoring.	**Sub-menu** OFF All disabled **(DEFAULT)** ON Open/Close Reports enabled (sent at end of exit delay) RESTOR Alarm Restores enabled RES+OC Alarm Restores and Open/Close Reports enabled Open and Close reporting options.

LOWBAT	LOW BATTERY REPORTING
Applicable when using central station, Audible or SMS monitoring.	**Sub-menu** NONE No low battery reporting **(DEFAULT)** MAIN Report low main battery SENSOR Report low detector batteries (including Fixed Panic Buttons) ALL Report low main unit and detector batteries Low Battery reporting options.

CLIENT	CLIENT ACCOUNT NUMBER
Applicable when using central station monitoring. Four digit client account number. Allowable range. 0000-FFFF Digits can be hexadecimal, but 'A' is not allowed for protocol compatibility.	• Press ON to view the programmed client account number. The first digit will flash. • Press ON to step through values for the first digit. • Press PANIC to store the digit. The second digit will now flash. • Repeat for the remaining digits. • Press PANIC to store the last digit, and first digit will flash. • Repeat programming procedure to make corrections, or press OFF to return to top level

PROGRAMMING OPTIONS

PHONE 1	TELEPHONE NUMBER 1
Applicable when using central station, audible or SMS monitoring. The dialler is disabled if PHONE 1 or PHONE 2 are blank. When the dialler is disabled the Guardpost will also not accept SMS operation or programming commands. 20 digits maximum.	Telephone number 1 is used for reporting alarms to a central monitoring station, audible voice reporting or SMS reporting to a mobile phone. • Press ON to view programmed phone number, which be displayed in successive 6-digit segments, after which the first segment will be displayed with the first digit will be flashing. • Press OFF to leave the number unchanged and step to the next option. • Press ON to step through values for the first digit: • Press PANIC to store the first digit. The second digit will flash. • Repeat for each digit (the display will scroll left after the fourth digit is entered). • Press ON to store the last digit, then press OFF, which returns to PHONE 1 • Press OFF to step to next option, or repeat procedure to make corrections. • The phone number can be deleted by reprogramming each digit with a PAUSE. Allowable digits <table><tr><td>-</td><td>PAUSE</td></tr><tr><td>0-9</td><td>digits 0-9</td></tr><tr><td>*</td><td>STAR</td></tr><tr><td>H</td><td>HASH</td></tr><tr><td>+</td><td>Dials the international access prefix</td></tr></table>

PHONE 2	TELEPHONE NUMBER 2
Applicable when using central station, audible or SMS monitoring. The dialler is disabled if PHONE 1 or PHONE 2 are blank. When the dialler is disabled the Guardpost will also not accept SMS operation or programming commands. 20 digits maximum.	Telephone number 2 is used as a secondary phone number for reporting alarms to a central monitoring station, audible voice reporting or SMS reporting to a mobile phone. • Press ON to view programmed phone number, which be displayed in successive 6-digit segments, after which the first segment will be displayed with the first digit will be flashing. • Press OFF to leave the number unchanged and step to the next option. • Press ON to step through values for the first digit: • Press PANIC to store the first digit. The second digit will flash. • Repeat for each digit (the display will scroll left after the fourth digit is entered). • Press ON to store the last digit, then press OFF, which returns to PHONE 1 • Press OFF to step to next option, or repeat procedure to make corrections. • The phone number can be deleted by reprogramming each digit with a PAUSE. Allowable digits <table><tr><td>-</td><td>PAUSE</td></tr><tr><td>0-9</td><td>digits 0-9</td></tr><tr><td>*</td><td>STAR</td></tr><tr><td>H</td><td>HASH</td></tr><tr><td>+</td><td>Dials the international access prefix</td></tr></table>

CELL SG	CELLULAR SIGNAL STRENGTH
Range 0-9 0, low signal 9, best signal	Indicates cellular signal strength.

ABORT	DIALLER ABORT DELAY
Applicable when using central station, Audible or SMS monitoring.	**Sub-menu** 0 SEC 5 SEC **(DEFAULT)** ... to 60 SEC in 5 second steps Dialler abort delay gives the opportunity to abort sending an alarm message to the central monitoring station within the programmed time (i.e. to cancel a false alarm).

PROGRAMMING OPTIONS

MEDIC	MEDICAL KEY ABORT DELAY
Applicable when using central station, Audible or SMS monitoring.	**Sub-menu** 0 SEC 5 SEC 10 SEC 15 SEC 20 SEC **(DEFAULT)** ... to 60 SEC in 5 second steps Medical key abort delay gives the opportunity to abort sending an alarm message to the central monitoring station within the programmed time (i.e. to cancel a false alarm).

T-CALL	DIALLER TEST CALLS
Applicable when using central station or SMS monitoring. Test calls are automatically disabled when SMS or Audible reporting is set. ┌─────────────┐ **T-Call must be OFF** if Audible reporting (AUD) mode is enabled. └─────────────┘	**Sub-menu** OFF Test calls disabled **(DEFAULT** when DIALER = SMS or AUDIBLE**)** 1 DAY 7 DAY **(DEFAULT** when DIALER = Contact ID**)** 14 DAY 30 DAY This option enables periodic test reports. Depending on the chosen Dialler Reporting Format, test reports are sent to the central station by Contact ID or SMS. **Test reports are usually not required when using ArmorIP or CSV "polled reporting" formats.** CONTACT ID Reporting: Test calls are sent to the central monitoring station. SMS Reporting: Test calls are sent to PHONE1 & PHONE2 by SMS.

DIALER	DIALLER REPORTING FORMAT
Internet reporting formats (ArmorIP & CSV) are available in Guardpost V2.3 and later.	**Sub-menu** OFF Dialler is disabled CID CONTACT ID reporting to a central station **(DEFAULT)** SMS SMS reporting to a mobile phone AUD AUDIBLE reporting to a mobile phone AIPTCP ArmorIP TCP reporting ⎤ AIPUDP ArmorIP UDP reporting Internet Reporting Formats CSVTCP CSV TCP reporting ⎦ This option sets the Guardpost reporting method via the 4G dialler.

PROGRAMMING OPTIONS

POWER	POWER MANAGEMENT MODE
Guardpost power management options ensure long battery life under various power supply scenarios.	**Sub-menu** AC-ON AC mode, Cellular module is on all the time **(DEFAULT)** BATT Battery mode, Cellular module 24 hours wake-up when mains is off BAT-30 Battery mode, Cellular module 30 min wake-up when mains is off BAT-1H Battery mode, Cellular module 1 hour wake-up when mains is off BAT-2H Battery mode, Cellular module 2 hour wake-up when mains is off SLR-30 Solar Cell charge mode, Cellular module 30 min wake-up SLR-1H Solar Cell charge mode, Cellular module 1 hour wake-up SLR-2H Solar Cell charge mode, Cellular module 2 hours wake-up AC-ON **(DEFAULT)** In this mode Guardpost should be permanently powered by mains plug pack. The backup battery will provide at least two days normal run in case of AC failure. Cellular module will be ON all the time in this mode and GUARDPOST will receive SMS messages instantly. BATT Cellular module will be turned off if no activity. Cellular module will be turned on once every 24 hours for 2 minutes to check SMS remote Arm/Disarm command if there is no event report within the whole 24 hours period. AC should be plugged in for charging for 24 hours when battery is low. BAT-30 Cellular module will be turned on every 30 minutes for 2 minutes to check SMS remote Arm/Disarm command. AC should be plugged in for charging for 24 hours when battery is low. BAT-1H Cellular module will be turned on every 1 hour for 2 minutes to check SMS remote Arm/Disarm command. AC should be plugged in for charging for 24 hours when battery is low. BAT-2H Cellular module will be turned on every 2 hours for 2 minutes to check SMS remote Arm/Disarm command. AC should be plugged in for charging for 24 hours when battery is low. Note 1: For the above battery modes, if AC is connected, the Cellular module will be turned on automatically so that GUARDPOST can receive remote SMS Arm/Disarm instantly. SLR-30/ SLR-1H/ SLR-2H Solar Cell charge mode. In this mode, the backup battery is charged by solar cells. To keep system current low, the Cellular module will be turned off when there is no activity, and will be turned on every 30 minutes/ 1 hour/ 2 hours for 2 minutes to check SMS remote Arm/Disarm command.

DEFALT	RESET FACTORY DEFAULTS
	Sub-menu ALL Erases all programmed devices and defaults all options OPTION Defaults all option values except radio keys and radio devices KEY Erases all radio keys SENSOR Erases all radio detectors and defaults SENSOR 1 (main PIR) Erase devices and/or default options as required. If ALL or KEY is selected, GUARDPOST will jump to the start of PROGRAM mode, displaying LEARN / KEY 1.

P-EXIT	EXIT PROGRAM MODE

PROGRAMMING OPTIONS SUMMARY

Program Option Name	SMS Program Option No. (XX)	Value (YY)	Description	Default	Page No.
KEY 1-23	N/A	KEY, DURESS, MEDIC, BELL, NO PAN, ERASE	Options for learning radio keys	None	18
SENS 1	N/A	ALARM, HOME, HOME 2, FIRE, CHIME, ACHIME, HCHIME, H2CHIM, SILENT, EXCLUD	Options for the onboard sensor	ALARM	
SENS 2-23	N/A	ALARM, HOME, HOME 2, FIRE, CHIME, ACHIME, HCHIME, H2CHIM, SILENT, EXCLUD	Options for the optional radio devices 2-23	ALARM	
RANGE	01	00, 01	Onboard PIR range. 00 = Low, 01 = High	LOW	19
PULSE	02	01, 02, 03, 04	Onboard PIR pulse count.	1 PULS	
SIGNAL	N/A	–	Radio devices signal strength check	–	
RADJAM	N/A	ON, OFF, SILENT	Radio jamming alarm	OFF	
RADSUB	N/A	ON, OFF	Radio message substitution alarm	OFF	
SUPVIS	03	00, 01, 04, 08, 16, 24	Supervision time in hours. 00 = Supervision disabled	OFF	
LOKOUT	04	00	Alarm Lockout. 00 = Disabled, 01 = Enabled	OFF	20
ENTRY	05	05, 10, 15, 20, 25, 30	Entry delay in seconds	5 sec	
EXIT	06	05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	Exit delay in seconds	5 sec	
SIREN	07	01, 02, 03, 04, 05	Siren time in minutes	5 min	
CHIRPS	08	00, 01	External Siren Chirps. 00 = Disabled, 01 = Enabled	ON	
V-ARM	N/A	ON, OFF	Voice annunciation for arming/disarming	ON	
V-ALRM	N/A	ON, OFF	Voice annunciation for alarms	ON	21
V-BATT	N/A	ON, OFF	Voice annunciation for battery alarms	ON	
V-FALT	N/A	ON, OFF	Voice annunciation for system faults	ON	
AUX OUT	16	OFF, TOGGLE, PULSE	Enables AUX output via external wire loom	OFF	
OPEN	09	00, 01, 02, 03	Open Close Reports. 00 = Disabled, 01 = ON, 02 = RESTOR, 03 = RES+OC	OFF	
LOWBAT	10	00, 01, 02, 03	Low Battery Reporting. 00 = NONE, 01 = MAIN, 02 = SENSOR, 03 = ALL	NONE	
CLIENT	CL1	Up to 4 digits	Client account number	0000	
PHONE 1	PH1	Up to 20 digits	Telephone No. 1 for reporting alarms by CID, SMS or AUD	none	22
PHONE 2	PH2	Up to 20 digits	Telephone No. 2 for reporting alarms by CID, SMS or AUD	none	
CELL SIG	N/A	–	Indicates cellular signal strength 0=no signal, 9=best signal		
ABORT	11	00, 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	Dialler Abort delay in seconds.	5 sec	
MEDIC	12	00, 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	Medical Key Abort delay in seconds.	20 sec	23
T-CALL	13	00, 01, 07, 14, 30	Test Call interval in days. 00=Test Calls disabled	OFF (7 DAY when dialler = CID)	
DIALER	14	00, 01, 02, 03, 04, 05	Dialler reporting format 00 = Contact ID (CID), 01 = SMS, 02 = Audible, 03 = ArmorIP TCP, 04 = ArmorIP UDP, 05 = CSV TCP	CID	
POWER	15	01, 02, 03, 04, 05, 06, 07, 08	AC-ON, BATT, BAT-30, BAT-1H, BAT-2H, SLR-30, SLR-1H, SLR-2H	AC-ON	24
DEFALT	N/A	ALL, OPTION, KEY, SENSOR	Reset factory defaults	N/A	
P-EXIT	N/A	–	Press the ON button on your radio key to exit program mode.	N/A	
Only available by SMS	V		Request current programmed options. Guardpost replies with the current values of all programmed options	N/A	–

Options numbers marked "N/A" are not available for programming by SMS.

PROGRAMMING BY SMS

4G

SMS
Programming

Many Guardpost programming options can be programmed remotely by SMS message. Some programming can only be performed locally by radio key.

To program a Guardpost by SMS you must know the mobile phone number of the Guardpost's SIM card and the client account number.

SMS Programming Commands

SMS programming commands are sent to the Guardpost in this format:

CCCC,PXX=YY,E

CCCC	Client account number	4 digits
P	Precedes each program option 01 to 15 Not required for PH1, PH2 & CL1	Must be UPPERCASE
XX	Program option number	01 - 15, PH1, PH2, CL1
YY	Value	
E	End of message	Must be UPPERCASE

The Guardpost will reply with a confirmation SMS:

Unit CCCC: PXX=YY, Programmed

If you send an SMS in the wrong format, Guardpost will respond with:

Unit CCCC: Command error.

The SMS format requires a comma between each command and no spaces.

PROGRAMMING BY SMS

NOTES

- SMS programming messages must not include spaces.

- Some commands must be sent in uppercase.

- Up to 7 options can be sent in one SMS message.

- To delete a phone number, send a hyphen '-' in place of a phone number.

- SMS acknowledgement messages are sent to the mobile phone which sent the SMS commands - which can be any mobile number. However if PHONE 1 or PHONE 2 are blank the dialler will not send messages of any type.

Examples

To program ENTRY delay to be 10 seconds. In these examples the Guardpost's client account number is 1234:

Send this SMS to the Guardpost   1234,P05=10,E

Guardpost will reply with   Unit 1234: P05=10, programmed

Up to 7 general programming options can be programmed in one SMS message. (PH1, PH2 and CL1 must be sent separately.)
For example:

To program multiple options in one message   1234,P05=10,P06=20,P08=01,E

Guardpost will reply with   Unit 1234: P05=10,P06=20,P08=01, programmed

To program example PHONE1 to be 9123 1234.

Send this SMS to the Guardpost   1234,PH1=91231234,E

Guardpost will reply with   Unit 1234: PH1=91231234, programmed

To program example PHONE1 to be 9123 1234 and PHONE2 to be 92220011.

Send this SMS to the Guardpost   1234,PH1=91231234,PH2=92220011,E

Guardpost will reply with   Unit 1234: PH1=91231234,PH2=92220011, programmed

To program example CLIENT account number to be 2468.

Send this SMS to the Guardpost   1234,CL1=2468,E

Guardpost will reply with   Unit 1234: CL1=2468, programmed

To delete PHONE1.

Send this SMS to the Guardpost   1234,PH1=-,E

Guardpost will reply with   Unit 1234: PH1=, programmed

To request a summary of all current program options.

Send this SMS to the Guardpost   1234,V,E

Guardpost will reply with   Unit 1234: P01=00,P02=03,
P03=24,P04=00,P05=05,P06=05,
P07=05,P08=01,P09=00,P10=00,
P11=00,P12=20,P13=07,P14=01,
P15=01,PH1=91231234,PH2=.....

PROGRAMMING BY SMS

SMS program options summary

These options are available for programming by SMS. See page 25 for the full programming options table.

See page 30 for PROGRAM OPTIONS FOR INTERNET SETTINGS.

Program Option Name	SMS Program Option No. (XX)	Value (YY)	Description	Default	Page No.
RANGE	01	00, 01	Onboard PIR range. 00 = Low, 01 = High	LOW	19
PULSE	02	01, 02, 03, 04	Onboard PIR pulse count.	1 PULS	
SUPVIS	03	00, 01, 04, 08, 16, 24	Supervision time in hours. 00 = Supervision disabled	OFF	
LOKOUT	04	00	Alarm Lockout. 00 = Disabled, 01 = Enabled	OFF	20
ENTRY	05	05, 10, 15, 20, 25, 30	Entry delay in seconds	5 sec	
EXIT	06	05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	Exit delay in seconds	5 sec	
SIREN	07	01, 02, 03, 04, 05	Siren time in minutes	5 min	
CHIRPS	08	00, 01	External Siren Chirps. 00 = Disabled, 01 = Enabled	ON	
OPEN	09	00, 01, 02, 03	Open Close Reports. 00 = Disabled, 01 = ON, 02 = RESTOR, 03 = RES+OC	OFF	21
LOWBAT	10	00, 01, 02, 03	Low Battery Reporting. 00 = NONE, 01 = MAIN, 02 = SENSOR, 03 = ALL	NONE	
ABORT	11	00, 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	Dialler Abort delay in seconds.	5 sec	22
MEDIC	12	00, 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	Medical Key Abort delay in seconds.	20 sec	23
T-CALL	13	00, 01, 07, 14, 30	Test Call interval in days. 00=Test Calls disabled	OFF (7 DAY when dialler = CID)	
DIALER	14	00, 01, 02, 03, 04, 05	Dialler reporting format 00 = Contact ID (CID), 01 = SMS, 02 = Audible, 03 = ArmorIP TCP, 04 = ArmorIP UDP, 05 = CSV TCP	CID	
POWER	15	01, 02, 03, 04, 05, 06, 07, 08	01 = AC-ON, 02 = BATT, 03 = BAT-30, 04 = BAT-1H, 05 = BAT-2H, 06 = SLR-30, 07 = SLR-1H, 08 = SLR-2H	AC-ON	24
AUXOUT	16	00, 01, 02	00 - Disabled, 01=Toggle, 02=Pulse	OFF	21
CLIENT	CL1	Up to 4 digits	Client account number	0000	21
PHONE 1	PH1	Up to 20 digits	Telephone No. 1 for reporting alarms by CID, SMS or AUD	none	22
PHONE 2	PH2	Up to 20 digits	Telephone No. 2 for reporting alarms by CID, SMS or AUD	none	
Only available by SMS	V		Request current programmed options. Guardpost replies with the current values of all programmed options	N/A	–

CENTRAL STATION REPORTING OPERATION
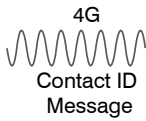
If enabled, Guardpost reports alarms to a central monitoring station via the 4G cellular network in Contact ID/ArmorIP or CSV formats.

There are 2 phone numbers, a primary number PHONE1 and a secondary number PHONE2. Reports are usually sent on the primary number but if the dialler is unsuccessful in connecting, it will dial the secondary number.

A client account number is allocated by the monitoring company to identify the customer. The client account number must be programmed into the system.

GUARDPOST transmits the next message on the queue, and if no acknowledge is received from the monitoring station, GUARDPOST re-transmits the message for a total of 10 attempts before displaying a dialler fault. Then, it will try again in 5 minutes, then, another 4 times every 1 hour. If still unsuccessful, GUARDPOST ceases transmitting until a new event occurs and raises a system alarm.

Contact ID Reporting Format

Contact ID reporting format takes the form:

SSSS 18 Q XYZ GG CCC E

SSSS	4 digit Client Account number
18	Uniquely identifies this format as Contact ID
Q	Event qualifier (1 = New alarm or Open; 3 = Restore or Close)
XYZ	Event code (hexadecimal)
GG	Group code. (always 00)
CCC	Sensor/key ID + offset, or Type number (decimal)
E	Error check

Contact ID reporting table

Program Option	Event Code (XYZ)	Offset + device ID, or Type number (CCC)
SENS 1-23 = ALARM SENS 1-23 = HOME SENS 1-23 = HOME 2 SENS 1-23 = ACHIME SENS 1-23 = HCHIME	130 Burglary	0 + ID
SENS 1-23 = FIRE	133 24 hour	50 + ID
Always enabled (unless auto-excluded at power-up)	137 Siren box tamper (Main unit)	106
Always enabled	383 Tamper (Sensor)	350 + ID
KEY 1-23 = KEY	120 Panic by user	300 + ID
KEY 1-23 = DURESS	121 Duress by user	400 + ID
KEY 1-23 = MEDICAL	101 Medical pendant	650 + ID
RADJAM = ON or		
RADSUB = ON	355 Radio jamming	105
SUPVIS not = OFF	355 Radio supervision poll fail (Device)	200 + ID Detector
500 + ID Fixed Panic Button		
LOWBAT = MAIN LOWBAT = ALL	302 Main unit low battery	107
LOWBAT = SENSOR LOWBAT = ALL	384 Radio device low battery	0 + ID
Always enabled	309 Main unit battery test fail	108
OPEN = ON	401 Open/Close with user ID	0 + ID
Always enabled	406 Cancel of alarm message	0 + ID

CENTRAL STATION REPORTING OPERATION

Internet Reporting (ArmorIP/CSV)

Available in Guardpost Rev2.4 and later

ArmorIP/CSV cellular internet settings such as IP address, Domain name, IP port number, APN name, etc. **can only be programmed via SMS text message.**

See P26-27 for SMS Programming instructions.

PROGRAM OPTIONS VIA SMS FOR ARMOR-IP / CSV

PI1	IP Address 1, Primary, up to 15 digits
PI2	IP Address 2, Secondary, up to 15 digits
PP1	Port number 1, Primary, up to 5 digits
PP2	Port number 2, Secondary, up to 5 digits
PAP	APN name, up to 30 digits
PD1	Domain name 1, Primary, up to 30 digits
PD2	Domain name 2, Secondary, up to 30 digits
PTM	ArmorIP Poll Time, 1 digit 0 = disabled 1 = 1 hour 2 = 2 hours 3 = 4 hours 4 = 8 hours 5 = 24 hours
PUN	Username for CSV, up to 10 digits
PWD	Password for CSV, up to 10 digits

ARMORIP/CSV PROGRAMMING FORMAT
CCCC,PXX=Y,E

CCCC	4 digit Client Account number
PXX	P must be upper case
XX	XX program option, 2 digits
Y	String value of program option
E	End of SMS program message

ARMOR-IP PROTOCOL AND FORMAT

If SIM data is enabled, the CELLULAR module will allow a GUARDPOST 4G to report alarms on internet to a central monitoring station which has IP receiver.

IP addresses/Domain name/Port number
There are two sets of IP addresses/domain name/port number to be programmed into GUARDPOST 4G via SMS, Primary and secondary. Reports are usually sent to the primary set of IP address/domain name/port number, but if the dialler is unsuccessful in connecting or reporting to IP receiver, it will be sent to the secondary set. Domain name and IP address are alternative. If both domain name and IP address are programmed, only domain name will be used.

APN – Access Point Name
APN is required for some cellular modules.

Different cellular network and SIM provider has different APN name as below:
Telstra APN – "telstra.internet"
Optus APN – "internet"
Vodafone – "vfinternet.au"

As default, GUARDPOST 4G will set up APN name automatically for one of three Australia cellular networks as per the SIM inserted to the cellular module. However, APN name can be programmed via SMS to overwrite the above three default APN name if needed.

IP settings, such as IP address, Domain name, IP port number, APN name, etc. can only be programmed via SMS text message. See 12.1.4 Internet Settings Program and 12.2.2 View of Internet Options for details.

GUARDPOST 4G allows two types of data format in IP reporting: ArmorIP and CSV.

ArmorIP Protocol and format

The Armor IP Protocol uses standard UDP and TCP protocols over IP data packets, often referred to as UDP/IP and TCP/IP respectively.

The data format of the ArmorIP protocol is broken down into fields or tokens where a field contains a two letter identifier and then the field data. All data that is sent using the ArmorIP protocol is ASCII. The STX (0x02) Start of Text and ETX End of Text (0x03) values are used to delimit the fields with the field type immediately following the STX for that filed. The complete packet is encapsulated in a SOT (0x01) start of transmission and EOT (0x04) End of Transmission sequence.

Example 1:
SOT STXAC00001234ETX STXSQ00000003ETX STXDF-CIDETX STXDD123418113000001FETX STX ET13:21:07 10/06/21ETX STXXP2a4eETX STXPNMezzoGuardian ETX STXPTSMARTLINKETX STX PV00.00.21ETX EOT

The example above is a non-encrypted message sent for Account Number 1234, it is a Contact ID Message, and the event is an zone alarm by sensor 1

AC00001234 – AC, Account Number, 00001234
SQ00000003 – SQ, Sequence Number, 00000003
DFCID – DF, Data Format in DD packet, CID for Contact ID
DD123418113000001F – DD, Data, 123418113000001F
This is Contact ID report data, account number 1234, zone alarm event 130, sensor 1 triggered.

Note: The SUM digit (Last Digit in DD) will always be sent as 'F' this is for legacy support of an existing IP solution that is being replaced

ET13:21:07 10/06/21 – ET, Event Time, 13:21:07, 10/06/21
XP2a4e – XP, Panel Poll Time, 2a4e hex number in seconds
PNMezzoGuardian – PN, Panel Name, MezzoGuardian
PTSMARTLINK – PT, Panel Type, SMARTLINK
PV00.00.21 – PV, Application Version, 00.00.21

CSV PROTOCOL AND FORMAT

CSV IP Alarm messaging consists of sending a standard ASCII string within a standard TCP/IP data frame using fields separated by commas, the first two fields of the message between header and trailer are reserved to specify the username, password (authentication) and the next two fields allocated for the alarm server device ASD ID (identifier account number) and lastly the message. (Alarm message). A Device manufacturer could use their own data format or a well-known industry standard dial up alarm formats like Contact ID, SIA to describe message their content. Please note CSV IP Alarm data fields are comma separated values (CSV)

[Name],[Password],[ASDID],[Message]

Example 1:
CSV data packet with username and password for authentication as below:

Username,Password,1234,18113001003

Up to 10 digits username and password for authentication.

Example 2:
CSV data packet without username and password for non-authentication as below:

,,1234,18113001003

The Contact ID message 1234 18113001003 would have been decoded by the CMS as
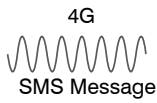1234 = Account
181 = new event
130 = burglary event type
01 = area
003 = zone

Acknowledgement from CSV Receiver
After received a message, the CSV Receiver will reply with the same message to the sender for acknowledgement.

SMS REPORTING OPERATION

If enabled, Guardpost reports alarms by SMS to up to two mobile phones via the Cellular network.

There are 2 phone numbers, a primary number PHONE1 and a secondary number PHONE2.

Guardpost will send an SMS to PHONE1 and PHONE2 if the phone number is programmed.

SMS Reporting Format

Unit [Client number]: [Alarm event]

Example

Unit 1234: Alarm sensor 1

This means Guardpost with the client account number 1234 an alarm from sensor 1.

SMS Reporting Table

Client Number (yyyy)	Event Message	Device ID (xx)	Description
0000 – FFFF	Alarm sensor	1 – 23	Alarm triggered by sensor xx from unit yyyy
0000 – FFFF	Siren tamper	N.A.	Alarm triggered by Siren box tamper from unit yyyy
0000 – FFFF	Tamper sensor	1 – 23	Alarm triggered by sensor xx tamper from unit yyyy
0000 – FFFF	Panic key	1 – 23	Panic alarm triggered by key xx from unit yyyy
0000 – FFFF	Duress key	1 – 23	Duress alarm triggered by key xx from unit yyyy
0000 – FFFF	Medical key	1 – 23	Medical alarm triggered by key xx from unit yyyy

AUDIBLE REPORTING OPERATION

If enabled, Guardpost reports alarms by audible message to up to two telephones via the cellular network.

Audible Report

Guardpost is able to report alarms to one or two telephone/mobile phones via the cellular network with audible messages, such as "ALARM FROM SENSOR ONE", "MEDICAL ALARM KEY TWO", "PANIC ALARM KEY THREE" etc. Multiple voice messages will be played if more than one event occurs while reporting.

There are 2 phone numbers, a primary number PHONE1 and a secondary number PHONE2. Reports are usually sent on the primary number but if the dialler report is not acknowledged, it will dial the secondary number. Telephone numbers must be programmed into the system.

If no acknowledge is received from the number called, GUARDPOST re-try for a total of 10 attempts before displaying a dialler fault. Then, it will try again in 5 minutes, then, another 4 times every 1 hour. If still unsuccessful, GUARDPOST ceases transmitting until a new event occurs and raises a system alarm.

ACKNOWLEDGE

Press key '9' on the receiving telephone to acknowledge the audible report. Guardpost will then hang up the call.

Or press '*' to acknowledge the audible report and start Two-Way-Voice monitoring. See page 34, Two Way Voice Monitoring.

TWO-WAY-VOICE MONITORING

Guardpost Two-Way-Voice (TWV) monitoring allows an operator or customer to listen and talk to Guardpost when alarm events happen.

Communications at the Guardpost is via the built-in microphone and speaker.

When an alarm event occurs and dialler report ends, or, when Two-Way-Voice is enabled via SMS, the operator/customer can start two-way-voice monitoring to listen to the area in which Guardpost is installed.

The operator can conduct a two way voice conversation with the premises. No user intervention is required at the Guardpost and all communications is "hands-free".

Two-Way-Voice monitoring can be initiated by one of three methods.

TWO-WAY-VOICE TIMING

- 3 minutes time out for call back after dialler report has finished
- 90 seconds time out for phone key commands after a call has been connected.
- A Two Way Voice communications session will time out after 3 minutes.
- Multiple call back is allowed within 90 seconds after a call has been terminated using "99".

DIRECT START AFTER EVENT

Direct start of Two-Way-Voice monitoring can only be used if Cellular audible reporting is enabled (AUDIBLE).

While the Guardpost voice message is annunciating, press ✳ (star) on your phone to acknowledge the audible report. This will start Two-Way-Voice monitoring in listen mode.

CALL BACK AFTER EVENT

You can always phone the Guardpost to start Two-Way-Voice monitoring after a dialler report has ended in any dialler mode (CID, SMS and AUDIBLE).

1 Call back the Guardpost after a dialler report has finished. Continuous beeps will be heard indicating that Two-Way-Voice is ready to start.

2 Press ✳ ✳ on your phone to start Two-Way-Voice in listen mode.

CALL BACK ENABLED BY SMS

This method of initiating Two Way Voice requires an SMS request to be sent to the Guardpost. In this example the Guardpost's client account number is 1234.

1 Send this SMS to the Guardpost `1234,TWV Request`   T must be uppercase.
(Shortcut. You can omit "WV Request" and send only 1234,T)

Guardpost will reply with `Unit 1234: TWV Enabled`

2 Once you receive the SMS reply you have 3 minutes to phone the Guardpost and start two-way-voice communications.. Continuous beeps will be heard indicating that Two-Way-Voice is ready to start.

3 Press ✳ ✳ on your phone to start Two-Way-Voice in listen mode.

TELEPHONE COMMANDS

Press ✳ ✳ to start TWV.
Press ✳ to acknowledge an Audible alarm report.

TELEPHONE COMMANDS DURING A TWO-WAY-VOICE SESSION.

Press 1 to talk
Press 2 to listen
Press 7 to reset/extend time. (Two Way Voice times out after 3 minutes.)
Press 3 to increase Guardpost microphone gain
Press 6 to decrease Guardpost microphone gain
Press 9 9 to hang up

REMOTE ARM/DISARM DURING TWO-WAY-VOICE

The Guardpost can be remotely armed/disarmed during a two way voice session.

Press 8 # to arm
Press 0 # to disarm

"Armed" or "Disarmed" will be heard then two-way-voice will continue in LISTEN mode.

An attempt to arm/disarm the panel when it is already armed or disarmed will result in 2 seconds silence then two-way-voice will continue in LISTEN mode.

DIALLER LISTEN-IN FUNCTION

The "Dialler Listen-in " feature is a useful installer's tool for diagnosing dialler operation in Contact ID reporting mode.

To enable dialler listen-in press the left front panel control button for 2 seconds.

Listen-in will be enabled for 3 minutes.

Dialler communications will be heard from the internal speaker.

Note: Ignore the display/voice of VOLUME while holding left button.

DIALLER SWINGER SHUTDOWN

To prevent excessive calls charges in the event of repeated alarms, dialler alarm reports are limited to a maximum of 20 reports between Arm/Disarm, or a 24 hour period.

In addition, the runaway shutdown feature limits the number of times an alarm from a particular device will be sent to the monitoring station. After 3 alarms have been sent, no further alarms for that device will be sent until the system is Disarmed and Armed.

This applies to all reporting formats - Contact ID, SMS and Audible.

TROUBLESHOOTING

ERROR CODE OR SYMPTOMS	POSSIBLE CAUSE(S)	SOLUTION
DIALER SIM FAULT	SIM related faults such as: • SIM not inserted or inserted properly. • SIM is locked with a pin. • SIM is not activated. • SIM has no credit to make/receive calls.	• Insert SIM • Check the SIM operation by testing it in a mobile phone handset.*
DIALER MODULE FAULT	Cellular module related issues such as • Cellular signal is too low. • Network related failure. • Communication issues between the on-board cellular module and the panel.	• Check cellular signal strength - make sure it is greater than level 2. • Check the network coverage by testing the SIM in a mobile handset*
DIALER FAIL	• Dialler report was not delivered • Dialler report did not get acknowledged, Example, an audible message was not acknowledged after reporting 10 times.	• Reset the unit using the override key or trigger and acknowledge a new alarm.
ARM/DISARM OR PROGRAM BY SMS NOT WORKING	• SIM unable to receive SMS. • SIM is full or with many messages. • All dialler functions including operation by SMS is disabled if PHONE 1 and PHONE 2 are blank.	• Check that the SIM card can receive SMS by testing it in a handset.* • Make sure all messages on the SIM card are deleted. • Make sure PHONE 1 or PHONE 2 are programmed.
SMS NOT REPORTING	• SIM unable to send SMS. • All dialler functions are disabled if PHONE 1 and PHONE 2 are blank. • Only main alarm events are reported by SMS. Alarms reported are: Sensor Alarm/Tamper, Siren Tamper Key Panic/Duress/Medical.	• Check that the SIM card can send SMS by testing it in a handset.* • Make sure PHONE 1 or PHONE 2 are programmed.
AUDIBLE NOT REPORTING	• SIM unable to call a number. • Only main alarm events are reported by Audible. Alarms reported are: Sensor Alarm/Tamper, Siren Tamper Key Panic/Duress/Medical.	• Check that the SIM card can make calls by testing it in a handset.*
TEST ALARM NOT WORKING	• The test alarm created is too short.	• Give abort time to expire before disarming • Connect mains power or set power mode to mains.
SENSOR FAIL	• Radio sensor faulty. • Radio sensor battery abnormally low or faulty. • Supervision time too short.	• Test sensor operation. • Adjust supervision time.

*Ness locked SIMs cannot be tested in other devices

SPECIFICATIONS

SYSTEM	
ONBOARD PIR	15m PIR motion sensor
ONBOARD SIREN	124dBM
COMMUNICATOR	4G Module, type: CAT 1: Bands supported: 4G: 2100 (B1), 1800(B3), 850(B5), 900(B8), 700(B28) MHz 3G: 2100(B1), 850(B5) ,900(B8) MHz Other support: VoLTE
BATTERY	12 Volt 3.2Ah SLA provides internal power in low-current modes / provides backup power in Mains mode
USER INTERFACE	
DISPLAY	6 Character scrolling LED
VOICE FEEDBACK	Onboard voice + language options
OPERATION	Arm / Disarm / Panic / Programming by radio keys Arm / Disarm by SMS messaging
EVENT LOG	Last 5 events with voice announcement
SETUP	
SYSTEM PROGRAMMING	Local programming by radio keys Self learning of radio devices by local programming Off site programming by SMS messaging
RADIO DEVICES	
DEVICES SUPPORTED	Up to 24 Ness Radio Keys or Radio Devices including the onboard PIR
RADIO SECURITY	Proprietary encryption and supervision Radio jamming detection Radio substitution detection
RADIO RX/TX	Ness integrated receiver for radio device signals
RADIO FREQUENCY	304Mhz / 868MHz depending on local requirements
INPUTS / OUTPUTS	
EXTERNAL WIRE LOOM	RED/BLACK. Strobe output: 12V strobe light, max. 2 RED/BLUE. Siren output: 8 Ohm horn speaker, max. 1 RED/WHITE. Internal siren output: 12V screamer, max. 1 YELLOW/GREEN. Tamper input: 3k3 end of line (resistor supplied) RED/RED FLYING LEADS. External input for hardwired 17VAC supply or solar panel supply
EXTERNAL POWER	17VAC Plug Pack supplied for periodic battery charging or for full-time power External input for hardwired 17VAC supply, (see External Wire Loom) External input for solar panel power supply, (see External Wire Loom)
PHYSICAL	
DIMENSIONS, MAIN UNIT	515(h) x 112(w) x 80mm(d)
COMPLIANCE	
APPROVALS	RCM, CE

REVISIONS

Document Rev 1.2 Feb2023
• Removed reference to 'GSM'
• P15, modified instructions for learning radio keys

Document Rev 1.3 Nov2023
• p23, Deleted 'Audible' from T-call definition, Added ArmorIP reporting options
• p23, Internet reporting formats (ArmorIP & CSV) are available in Guardpost firmware v2.3 and later.
• p25, Added ArmorIP reporting options
• p28, SMS program options summary, corrected options for Power.
• p30, Added Program options VIA SMS for ArmorIP/CSV

NOTES

NESS

CORPORATION