



EN 50131-1
EN 50131-3
EN 50131-6
EN 50131-10
EN 50136-1
EN 50136-2
EN 50130-4
EN 50130-5
CEB T014



GameOver



SMARTLIVING
Anti-intrusion control panels and security systems

USER'S MANUAL



INIM Electronics s.r.l. (Seller, Our, Us) warrants the original purchaser that this product shall be free from defects in materials and workmanship under normal use for a period of 24 months. As INIM Electronics s.r.l. does not install this product directly, and due to the possibility that it may be used with other equipment not approved by Us; INIM Electronics s.r.l. does not warrant against loss of quality, degradation of performance of this product or actual damage that results from the use of products, parts or other replaceable items (such as consumables) that are neither made nor recommended by INIM Electronics. Seller obligation and liability under this warranty is expressly limited to repairing or replacing, at Seller's option, any product not meeting the specifications. In no event shall INIM Electronics s.r.l. be liable to the purchaser or any other person for any loss or damage whether direct or indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party caused by defective products or otherwise arising from the incorrect or otherwise improper installation or use of this product.

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage arising from improper maintenance or negligence
- damage caused by fire, flood, wind or lightning
- vandalism
- fair wear and tear

INIM Electronics s.r.l. shall, at its option, repair or replace any defective products. Improper use, that is, use for purposes other than those mentioned in this manual will void the warranty. Contact Our authorized dealer, or visit our website for further information regarding this warranty.

INIM Electronics s.r.l. shall not be liable to the purchaser or any other person for damage arising from improper storage, handling or use of this product.

Installation of this Product must be carried out by qualified persons appointed by INIM Electronics. Installation of this Product must be carried out in accordance with Our instructions in the product manual.

The information contained in this document is the sole property of INIM Electronics s.r.l. No part may be copied without written authorization from INIM Electronics s.r.l.

All rights reserved.

Hereby INIM Electronics s.r.l. declares that the SmartLiving series of intrusion-control panels, the Air2 series of devices and the SmartLinkAdv product are in compliance with the essential requirements and other relevant provisions of Directive 1999/5/CE.

Moreover, INIM Electronics s.r.l. also declares that all other devices mentioned in this manual are in compliance with the essential requirements and other relevant provisions of Directive 2004/108/CE.

The full declarations of conformity can be found at URL:

www.inim.biz/certifications

The devices described in this manual, depending on the settings selected during the installation phase and the implementation of the concepts illustrated in this guide, allow you to create an Intrusion Detection and Hold-up Alarm System (I & HAS) compliant with EN 50131-1: 2006 + A1: 2009, safety grade 3 (at highest) and an alarm transmission system (ATS) compliant with EN 50136-1: 2012 in category ATS6 (at highest SP6 or DP4).

The devices described are compliant with European standards EN 50131-3: 2009 (in reference to control and indicating equipment - CIE), EN 50131-6: 2008 + A1: 2014 (in reference to power supplies - PS), EN 50131- 10: 2014 and EN 50136-2: 2013 (in reference to transceivers on supervised sites - SPT).

As a support to the design, planning, operation, installation, commissioning and maintenance of intrusion alarm systems installed in buildings, the following regulatory documents should be consulted: CEI 79-3 and CEI CLC / TS 50131-7.

Depending on the State where the components described are installed, certified compliance with local laws and regulations may be required.

Warranty

Limited warranty

Copyright

European Directive compliance

Leading-edge systems (DM37/08)

Table of contents

Warranty	2
Limited warranty	2
Copyright	2
European Directive compliance.	2
Leading-edge systems (DM37/08)	2
Table of contents	3
Chapter 1 General information	5
1-1 Manufacturer's details	5
1-2 Description of the product and various models	5
1-3 Environmental Conditions	6
1-4 Products certified and conforming to directives	6
1-5 Manuals	7
1-6 Operator Qualifications.	7
1-7 Access Levels	8
1-8 Conventions – Glossary	8
Chapter 2 The SmartLiving System.	9
2-1 Introduction	9
2-2 The Technologies.	10
2-3 Keypads	10
2-4 Reader - nBy.	18
2-5 User Codes	20
2-6 Keys	21
2-7 Multi-system access.	22
2-8 Telephone functions.	22
2-9 WEB / e-mail functions.	23
2-10 AlienMobile Application	23
2-11 Inim Cloud	23
2-12 Arming scenarios.	25
2-13 Videosurveillance.	25
Chapter 3 Shortcuts	26
3-1 Keypad shortcuts.	26
3-2 Shortcut with code.	27
3-3 Key and Reader shortcuts.	27
3-4 Shortcut list	28
3-5 Shortcut on event	28
Chapter 4 Voice functions	29
Chapter 5 Using the system.	30
5-1 Managing alarms	30
5-2 Arming and disarming partitions	32
5-3 Voice box and intercom functions	34
5-4 Activations	35
5-5 View.	36
5-6 Activation of outputs	40
5-7 Change date and time	41

5-8	Keypad settings	42
5-9	Change PIN	43
5-10	Change telephone numbers	44
5-11	Teleservice request	44
5-12	Overtime request	44
5-13	Thermostat	45
5-14	Teleservice via Nexus	46
5-15	Codes	47
5-16	Timer programming	48
5-17	Listen-in	49
5-18	Partition status enquiry	49
5-19	Commands over-the-phone	50
5-20	Alien function keys	51
5-21	Using the SmartLAN/G	53
5-22	Using AlienMobile application	55
5-23	Photo frame	56
5-24	Graphic maps	56
5-25	Alarm clock and memo	57
5-26	Camera access	58
5-27	Use of the Inim Cloud	59
Appendix A	Glossary	62
Appendix B	Shortcuts at default	67
Appendix C	Fault signals	68
	Notes	71

Chapter 1

GENERAL INFORMATION

Manufacturer's details 1-1

Manufacturer: INIM Electronics s.r.l.
 Production plant: Centobuchi, via Dei Lavoratori 10
 63076, Monteprandone (AP), Italy
 Tel: +39 0735 705007
 Fax: +39 0735 704912
 e-mail: info@inim.biz
 Web: www.inim.biz

The persons authorized by the manufacturer to repair or replace the parts of this system have authorization to work on INIM Electronics brand devices only.

Description of the product and various models 1-2

Description: Intrusion control panel
 Models: SmartLiving 505
 SmartLiving 515
 SmartLiving 1050, SmartLiving 1050/G3,
 SmartLiving 1050, SmartLiving 1050/G3,
 SmartLiving 10100L, SmartLiving10100L/G3

Standards applied: EN 50131-1:2006 + A1:2009,
 EN 50131-3:2009,
 EN 50131-6:2008 + A1:2014,
 EN 50131-10:2014,
 EN 50136-1:2012,
 EN 50136-2:2013,
 EN 50130-4:2011 + A1:2014,
 EN 50130-5:2011,
 CEB T014:2013-04 (ed.3)

Certifying body: IMQ S.p.A.
 Safety grade: 2 or 3 (in accordance with configurations)
 ATS Categories: up to SP6 or DP4 (in accordance with configurations)

The following table describes the main features of the various models of the control panels:

Table 1-1: Control panel - Main Features

SmartLiving Control panel models		505	515	1050 1050/G3 1050L 1050L/G3	10100L 10100L/G3
Total terminals		5	15	50	100
Terminals on panel	total	5		10	
	configurable as inputs	5		10	
	configurable as rollerblind/shock	2			
	configurable as outputs	0		5	
Total zones		10	30	100	200
Outputs on control-panel motherboard	total	3			
	relay	1			
	open-collector output	2			
Partitions		5		10	15

Table 1-1: Control panel - Main Features

SmartLiving Control panel models	505	515	1050 1050/G3 1050L 1050L/G3	10100L 10100L/G3
Keypads (JOY, nCode/G, Concept/G, Alien, Aria)	5		10	15
Voice memo slots	5		10	15
FLEX5 expansions	5	10	20	40
nBy Readers	10		20	30
Sounderflashers (Ivy-B, Hedera)	10			
Air2-BS200 Transceivers	10		20	30
Digital keys and wireless command devices	50		100	150
Possible key combinations	4294967296			
IB100 isolators	15			
Nexus dialer	1			
Codes	30		50	100
Scenarios	30			
Timers	10			20
Recordable Events	500		1000	
Programmable events	10		30	50

Environmental Conditions

1-3

The Joy/GR, Joy/MAX, Aria/HG, nCode/G, Concept/G, Alien/S, Alien/G, IB100, FLEX5, Nexus and nBy/X peripheral devices are for indoor installation only and operate best under the following environmental conditions:

- **Temperature:** from -10° to +40°C
- **Maximum humidity:** 75% (without condensation)
- **Environmental class:** II

The nBy/S reader is suitable for outdoor installation and operates best under the following conditions:

- **Temperature:** from -25° to +70°C
- **Maximum humidity:** 93% (without condensation)
- **Protection grade:** IP 34
- **Environmental class:** IV

Products certified and conforming to directives

1-4

The SmartLiving control panels and devices described in this manual are IMQ certified - Sistemi di sicurezza (IMQ S.p.A.) and conform to the above mentioned standards, when duly programmed, as described in .



The control panel enclosure is capable of housing the following certified items:

- INIM Electronics switching-power supply
- Motherboard (IN082 or IN088)
- SmartLogos30M voice board (accessory item)
- FLEX5/U input/output expansion board (accessory item)
- AUXREL32 relay board (accessory item)
- SmartLAN/SI and SmartLAN/G LAN interface boards (accessory items)
- GSM Nexus and Nexus/G communicators (optional)
- IB100/RU BUS isolator board (accessory item)
- ProbeTH thermal-probe kit for battery-charge optimization (accessory item)
- TamperNO tamper-protection kit (accessory item)
- Backup battery, 12V @ 7, 9 or 17Ah (depending on the control panel)
- Motherboard (IN082 and IN088) integrated Type B notification apparatus

The control panel compliance is also guaranteed when connected to the following certified devices:

- FLEX5/P input/output expansion boards
- Joy/MAX, Joy/GR, Aria/HG, Concept/G, nCode/G, Alien/G, Alien/S keypads
- nBy/S outdoor-mount proximity readers
- nBy/X universal-mount proximity readers
- IB100/RP BUS isolator
- Self-powered IB100/A BUS isolator

- nCard access-control card for proximity readers
- Tag for nKey or nBoss proximity readers
- Self-powered sounderflashers for outdoor installation: Ivy, Ivy-F, Ivy-M, Ivy-FM, Ivy-B, Ivy-BF, Ivy-BM, Ivy-BFM
- Wireless devices AIR2, AIR2-BS200 (transceiver), Air2-IR100 (PIR detector), Air2-MC100 (magnetic contact)
- SmartLinkAdv/GP, SmartLinkAdv/G, SmartLinkAdv/P communicators

Manuals 1-5

Installer's manual 1-5-1

The installer's manual (not included in the package) can be purchased from your retailer. You should read it carefully through in order to become familiar with all the components and operating procedures of the SmartLiving system.

In order to provide adequate protection, the installer must adhere to all the manufacturer's guidelines relating to the active and passive security devices of this system.

Installation and programming guide 1-5-2

The guide, supplied with each control panel, provides all the instructions and illustrations necessary for fast installation and programming of the SmartLiving system. It provides step by step descriptions of the procedures required for the system wiring, the various connections and first powerup. It also provides a table for the peripheral addressing process and a quick guide indicating default parameters and values and how to program/change them directly from the keypad.

User's Manual (this manual) 1-5-3

DCMUINEOSLIVINGE 6.40
MANUAL CODE REVISION

It is advisable that the installer reads through the User's Manual which is supplied with the control panel. Once the system has been installed, the user manual must given to the users for consultation. The user must fully understand all the system functions and the configuration settings.

It is the installer's responsibility to inform the system users that, regardless of its capabilities, an intrusion alarm system is not a substitute for the necessary precautions building occupants must take to prevent intrusion.

Operator Qualifications 1-6

Installer 1-6-1

The installer is the person (or group of persons) who sets up and programs the entire security system in accordance with the purchaser's requirements and in respect of the safety laws in force. As the only individual in contact with system users, it is the installer's responsibility to instruct them on how to use the security system properly.

Under normal circumstances, the installer is not allowed to arm/disarm the system without previous authorization from the user. All the system partitions must be disarmed before accessing the parameter programming phase.

The access code of the installer is a level 3 access code.

User 1-6-2

The users are the occupants of the building where this intrusion control panel is installed. Only authorized users can access and operate the system.

Thanks to the extreme flexibility of the system, the most common operations can be carried out without authorization. This operating method must be expressly requested by the main user, as it considerably lowers the security level of the system and may cause false alarms, accidental arm/disarm operations, etc.

A system access code can be associated with each user. The programming process allows you to define the code hierarchy:

- **User**
- **Manager**
- **Master**

Each code, in accordance with its assigned level in the system-hierarchy (the "User" being the lowest level), is capable of carrying out the following operations on all other codes that are hierarchically inferior:

- enable/disable
- change PIN
- change several programming parameters

If the system programming complies with security grade 3 of EN 50131, some partition arming or delete memory operations, requested from a keypad, may be authorized by the entry of a level 3 code (installer code) as well as by a user code.

Access Levels 1-7

The normative defines the following system-access levels, regardless of system-access limitations:

- **Level 1** - access by any person (e.g. passer-by)
- **Level 2** - access by a user
- **Level 3** - access by the installer or maintenance operator access (authorized by a level 2 user)
- **Level 4** - manufacturer access

Conventions – Glossary 1-8

In order to understand the terminology used in this manual and improve your knowledge of this system and its operating procedures, read carefully through the Technical Terminology – Glossary (refer to *Appendix A, Glossary*).

The appendix contains the definitions of technical terms commonly used in the field of security, therefore, relevant to the SmartLiving system.

Chapter 2

THE SMARTLIVING SYSTEM

Introduction

2-1

INIM Electronics wishes to thank you for choosing this SmartLiving intrusion control system. Its advanced technology and user-friendly operations provide an extremely high level of protection combined with ease-of use.

INIM Electronics recommends that all parts of this manual be read thoroughly before starting up SmartLiving system. Once you have become accustomed to the day-to-day operations, your installer will explain and if required, program the advanced functions provided by the system.

A typical system comprises:

- SmartLiving control panel
- intrusion detection devices (PIR or microwave detectors, magnetic contacts, linear beam detectors, etc.)
- system control peripherals: proximity readers, keypads
- alarm signalling devices which generally signal the events detected by the system (sounders, flashers, etc.)

The keypad is an extremely flexible peripheral device which allows users to manage the system with ease. The graphic display shows all the necessary information and provides an advanced user-interface based on icons for instant and clear indications relating to the operations to be performed. All users have PINs which allow them to access and control the system via the keypad in accordance with their permitted access level.

Advanced voice technology guides you through the operations by means of clear voice prompts which explain the operations you must undertake.

nBy readers (2 versions available: nBy/S wall-mount and By/X flush-mount) allow you to access and control the system. Although these devices are not as flexible as keypads, they provide a quick and easy way of carrying out day-to-day operations such as arming and disarming the system. Authorized digital-key users can operate the system in accordance with their programmed access level (enabled functions, etc.) by holding the key in front of the proximity key reader.

All SmartLiving control panels are capable of managing INIM's "Air2" two-way wireless system. This system integrates wireless devices (detectors, keyfobs, etc.) into the hardwired environment.

SmartLiving control panels are capable of managing various event types (alarms, faults, tamper, code/key identification, arm/disarm operations, etc.) and event-response actions (audible/visual signalling, telephone calls, SMS text messages over the GSM network and, with the addition of the optional SmartLAN/G board, e-mails with attachments). The calls can be:

1. report calls to alarm receiving centres - via the most widely used reporting protocols.
2. voice calls to contact numbers - using advanced voice technology to inform contact persons of the active alarm condition.

Events can also be announced on JOY/MAX, Aria/HG and Alien keypads.

The SmartLiving intrusion control panel also provides automatic features, such as:

- arm and disarm operations set up on a weekly basis
- simple yet useful access-control functions which allow the system to deny access to specific keys/codes at certain times
- preset activation/deactivation of household devices (building automation) such as courtesy lights
- other similar automatic facilities.



The Technologies

2-2

Expertise in the arena of total security and a commitment to precision and high quality allow INIM's R & D professionals to deliver excellence in design technology and dependability through time.

EASY4U

2-2-1

This user-friendly tool provides an interesting array of graphic features and functions. All SmartLiving intrusion control panels are controlled by keypads equipped with 96x32 pixel graphic displays. The four-line alphanumeric display screen (16 characters per line) can be edited or used to view the icons associated with various customized user-operations. The keypad shortcuts allow time-consuming sequences to be transformed into simple keystroke actions. They can be used for a variety of tasks and make operations less tedious and less error-prone. In this way, INIM has eliminated the repetitive sequences of keystrokes required by other systems available on the market. The use of customizable graphic-objects, which indicate the system status, helps users to understand what is happening on the system.



Besides accepting various commands (Away Arm, Stay Arm, Disarm, etc.), the nBy reader also allows users to manage the "shortcuts" programmed on the keypad.

The Joy/MAX, Aria/HG and Alien keypads both have built-in nBy proximity readers.

VOIB

2-2-2

This is an acronym for **Voice Over Inim-Bus**. VOIB technology allows the system to manage end-to-end digitized voice transmissions at extremely high-speed over the IBUS. Voice transmissions can be carried to all points of the IBUS. The JOY/MAX, Aria/HG and Alien keypads have built-in microphones and speakers for message recording and playback. The 30 minute capacity voice board allows each event to be associated with a message. Voice digitizing and compression allow the signal to be transmitted in data packets over the bus to recipient keypads where it is announced. Voice digitizing and the characteristics of the I-BUS allow end-to-end "noise-immune" voice transmissions without the need of any additional wiring.



Keypads

2-3

The keypad allow users to manage all aspects of the security system. SmartLiving control panels are capable of managing keypads with the following features:

Table 2-1: Keypads - functions

Models	Joy/MAX	Joy/GR	Aria/HG	Aria/W	nCode/G	Concept/G	Alien/S	Alien/G	
Graphic display	Monochromatic 96x32						65536 colour touch screen		
							4.3 inches 480x272	7 inches 800x480	
Keys	23 (in soft rubber)				23 (touch)		No		
Signalling LEDs	4						No		
Buzzer	Yes								
Terminals	2		No		1		No	2	
Microphone	Yes	No	Yes	No				Yes	
Speaker	Yes	No	Yes	No				Yes	
Built-in proximity reader	Yes	No	Yes	No				Yes	
Temperature sensor	Yes	No	Yes	No				Yes	
Backlight activated by proximity sensor	No				Yes		No		
Brightness sensor	No		Yes		No				
Tamper protection	Yes								
Wireless	No			Yes		No			
Keypad lock-out	No					Yes			
USB port	No						Yes		
SD card	No						Max. 32 GByte		

The various keypad models have different functions, enclosures and key access. The keys on Joy keypads are protected a cover, whereas, the keys of the nCode/G, Aria and Concept/G keypads are on view. The Concept/G is a touch-screen keypad. Alien keypads are not equipped with keys but instead have a colour touch screen that allows access to the system via touch or touch-screen pen (supplied with Alien/G).

The installer assigns the partitions and portions/sections of the system that users, with assigned codes, will have access to via the keypad in use.

It is possible to extend the use of some of the system shortcuts to users without assigned codes. In this way, SmartLiving control panels add further operating modes to that of the traditional user menu which is only accessible after code entry.

It is possible to use the shortcuts at the keypads (refer to "Shortcuts" in the Glossary) associated with keys **F1** **F2** **F3** **F4**. Generally, intrusion control panels do not allow access to the system via keypad without code entry. However, by means of the shortcuts associated with keys **F1**, ..., **F4** it is possible to enable building occupants to access and operate on the system without code entry.

The Alien touch screen user interface provides shortcuts such as the activation of scenarios, and also applications such as device settings, which can be activated by the buttons displayed on the screen without code entry.

The installer must program the shortcuts to suit the system requirements and explain how they are used. For example, it may be useful to allow all the building occupants to arm the system without code entry, as this operation increases the level of system security. However, operations which lower the level of system security should be reserved for code users only (thus allowing identification of users who disarm the system). Under normal circumstances, operations which increase system security can be allowed without valid-code entry whereas, operations which lower system security (Disarm, Delete Alarm/Tamper memory, Deactivate Alarm/Tamper outputs) should be allowed only after valid-code entry.

JOY/MAX, Aria/HG and Alien keypads also provide a programmable chronothermostat function. This function allows you to set up zone management (one zone per keypad) of the heating/air-conditioning system.

The temperature is read by a built-in temperature sensor. The hysteresis is fixed at 0.4°C.

The Concept/G keypad provides a further two options relating to direct user access.

A special feature allows activation of the backlight of the display and keys when users approach the keypad. This is achieved through a proximity sensor which can be

activated by pressing keys **1** and ***** simultaneously and deactivated by pressing **1** and **#**.

The other option, block/unblock keypad, can be achieved by pressing key ***** for 3 seconds. If the block keypad option is enabled, the display will show the icon opposite.

The Aria/W wireless keypad provides all the necessary functions for control and management of a SmartLiving installation equipped with an Air2 system, which it can interface with through the Air2-BS200 transceiver. It integrates all the functions of a hard-wired keypad and provides a graphic icon display.

It is equipped with an accelerometer which provides both anti-tamper and "wakeup" from stand-by functions, whereas the brightness sensor controls the display and key brightness optimally with respect to the surrounding environment. Moreover, it has an automatic shutdown function in the event of loss of wireless connection.

The Alien keypad screen

The brightness and contrast of the backlit-graphic LCD (96 x 32 pixel) can be adjusted by way of the respective options on the user menu (refer to *paragraph 5-8 Keypad settings*).

It is divided into four lines which continually provide information regarding the status of the system and control panel, without need of user-code entry.

- 1° line:
- 2° line:
- 3° line:
- 4° line:

KEYS



SHORTCUTS



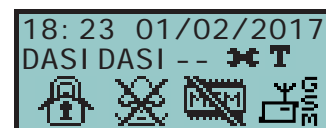
CHRONOTHERMOSTAT

CONCEPT/G ACCESS



WIRELESS TERMINALS








2-3-1



The following table describes the messages which are shown on the keypad display, in accordance with the actual status of the control panel:

- Standby - shown when the control panel is functioning normally and there are no alarm, tamper or fault events present on the system.
- Zone alarm or tamper - shown when the control panel detects or signals violation on a zone, both in the event of intrusion or detection of a lost device
- Maintenance - shown when the control panel is in maintenance mode for repair or programming purposes

Table 2-2: Display visualization

Display line	Control panel status		
	Standby	Alarm or tamper	Maintenance
1	<p>18: 23 01/02/2017</p> <p>The first line of the display shows the date and time.</p>	<p>Panel T03</p> <p>If at least one of the keypad partitions has saved an alarm or tamper event to the memory, the first line of the screen will flash the descriptions of the zones concerned every 3 seconds.</p> <p>Note</p> <p>Open zones are signaled by blinking on the red LED .</p>	<p>K03 Service</p> <p>If the control panel is in Service mode, a string will be shown indicating the address of the keypad in use (in the figure, the keypad is at address 3).</p>
	<p>18: 23 PM 25.9</p> <p>If you are using a keypad with temperature sensor, the date and room temperature will alternate on the screen every 3 seconds.</p>	<p>Mainten K03 P05</p> <p>If you are using a keypad with temperature sensor, the string will also show the address of its built-in proximity reader (in the figure, the reader is at address 5).</p>	
	<p>Panel T03</p> <p>If the "View open zones" control-panel option is enabled, the descriptions of zones that are not in standby status when the keypad partitions disarm will be shown in sequential order approximately every 3 seconds.</p> <p>Panel T03</p> <p>Any auto-bypassable zones will be shown in white on black background.</p>	<p>Panel T03</p> <p>Mainten K03 P05</p> <p>If the control panel is in Service mode and at least one of the keypad partitions has saved an alarm or tamper event to the memory, the above-described strings will alternate on the display.</p>	
2 left	<p>DASI DASI --</p> <p>The left side of the second line shows the characters that indicate the current status of the partitions the keypad is assigned to:</p> <ul style="list-style-type: none"> • D = partition disarmed • A = partition armed in Away mode (interior and perimeter zones armed) • S = partition armed in Stay mode (perimeter zones armed) • I = partition armed in Instant mode (perimeter zones armed with no delay) • - = partition does not belong to the keypad <p>In the case of the SmartLiving 505 or 515, 5 characters indicating the status of partitions 1 to 5 will be shown. In the case of the SmartLiving 1050 or 1050L, 10 characters indicating the status of partitions 1 to 10 will be shown.</p> <p>The display of the SmartLiving 10100L model, alternates at 3 second intervals, between 10 characters, indicating the status of partitions 1 to 10, and 5 characters indicating the status of partitions 11 to 15.</p>	<p>DASI DASI --</p> <p>D SI DASI --</p> <p>In the event of a partition alarm or tamper memory, the red LED  on the keypad and the characters corresponding to the partitions concerned will blink.</p>	<p>The line is the same as when the control panel is in standby condition.</p>
	<p>SCENARIO 001</p> <p>If the "Show scenario" control panel parameter is active, the left side of the second line on the screen will display the current scenario.</p>		
2 right	<p>DASI DASI --  T</p> <p>The right side of the second line allows you to view several icons which provide visual information regarding the system. For a detailed description of these icons refer to <i>Table 2-3: Information icons</i>.</p>		
3	<p>   </p>		
4	<p>Lines three and four on the display are occupied by the icons which correspond to the shortcuts assigned to the function keys F1 Fn, ..., F4 Fn.</p> <p>If no shortcuts are programmed on the keypad function keys, the respective spaces on the display will remain empty.</p>		

The blinking status of characters relating to the partition statuses which appears on the screens of Aria/W keypads is not in fact a blink but is the solid negative image of the character.

Note

The icons which appear on the right side of the second line, provide information regarding the system, therefore, their presence or status (fixed or flashing) depends on the status they must signal:

Table 2-3: Information icons

Icon	Signalling	Joy, Aria/HG, nCode, Concept	Aria/W	Alien
Telephone line	Telephone line busy	Solid		Solid
	Telephone line down	Blinking		Blinking
Peripheral Loss	At least one peripheral (keypad, reader, expansion) is not responding properly.	Solid		Solid
	All the peripherals in the system configuration are responding properly, however, loss of a peripheral has been detected and cleared (Peripheral Loss memory).	Animated	Solid	Blinking
Answerphone	Answerphone function enabled	Solid		Solid
Teleservice	Teleservice enabled	Solid		Solid
Key	False key	Blinking	Solid	Blinking
Tamper disabled	The tamper protection on the Alien keypad is disabled			Solid
Peripheral tamper	At least one peripheral (keypad, reader, expansion) is in tamper status (enclosure open or device dislodged).	Solid		Solid
	All peripherals are properly placed and all enclosure covers are closed, however, tamper was previously detected and cleared (Tamper memory).	Animated	Solid	Blinking
Control panel Tamper	The Control panel is in tamper status (enclosure open or device dislodged).	Solid		Solid
	The Control panel is properly placed and the enclosure is closed, however, panel tamper has been detected and cleared (Panel tamper memory).	Animated	Solid	Blinking
Call on Nexus	The Nexus/G communicator is engaged in a call	Solid		Solid
Sending SMS	The Nexus/G dialler is sending an SMS text message	Solid		Solid
LAN	A SIA-IP event report is being sent through the LAN	Solid		Solid
	The LAN board cannot be found	Blinking		Blinking
SIA-IP on Nexus	An event is being transmitted through the Nexus/G in SIA-IP reporting format or a teleservice request is being sent over the GPRS network.	Solid		Solid
Thermostat: Winter mode	The keypad thermostat option is enabled in Winter mode (Heating).	Solid		Solid
Thermostat: Summer mode	The keypad thermostat option is enabled in Summer mode (Air-conditioning).	Solid		Solid
Thermostat: Heating/Air-conditioning	Heating/Air-conditioning On.	Solid		Solid

If duly programmed by the installer, the icon will be shown when Teleservice is enabled.

Note

The backlight can be programmed from the keypad Aria in accordance with the measured ambient-brightness. The keypad manages two different brightness settings:

- Day
- Night

These settings can be programmed via the "Keypad" section in the User menu.

ARIA BACKLIGHTING

Using the keys 2-3-2

The following section describes how the keys are normally used. Some of the keys may have specific functions which will be indicated when necessary.

Table 2-4: The keypad keys

Keys	Name	Typical application
	Number keys	Used to type in User PINs
	OK	Confirms the selected item (parameter, etc.)
	UP, DOWN	These keys allow you to scroll the menu lists and/or adjust graphically displayed parameters (for example, keypad or volume adjustment).
	LEFT, RIGHT	These keys allow you to scroll along the parameters or data being viewed (for example, when viewing partitions in the events log or when selecting partitions in the arm/disarm menu).
	C	This key allows you to step back on the open menu without confirming the selected options (parameters, etc.) or, after entering a user PIN and pressing , to run through the 3 user-menus (refer to <i>paragraph 2-5 User Codes</i>).
	ESC	This key exits the user menu definitely without confirming any selected items (parameters, etc.).
	ENABLE	Enables options (refer to <i>paragraph 5-4 Activations</i>)
	DISABLE	Disables options
	F1, F2, F3, F4 or function keys	Activate the shortcuts which correspond to the associated icons. Can be used also as Emergency keys (refer to <i>paragraph 2-3-3 Emergency functions</i>).

Emergency functions 2-3-3

The control panel provides 3 special functions which can be activated from the keypad:

- Fire Emergency
- Ambulance Emergency
- Police Emergency

Activation of these keys will generate the associated events and actions (e.g. activation of outputs and calls).

To activate an emergency request, press and hold for 3 seconds the required key combination and wait for the confirmation beep, as follows:

Table 2-5: Emergency keys

Emergency	Combination keys	Alien keys
Fire		
Ambulance		
Police		

If any two function keys are pressed at the same time, the functions relating to the icons associated with the keys will not be activated.

Note

Visual signals on the keypad LEDs 2-3-4

The following table describes the signals on the LEDs of the Joy, nCode, Aria and Concept keypads, or the icons which represent them on the display of the Alien keypad.

Table 2-6: Keypad LEDs

LED/Icon activation	Red	Yellow	Blue	Green
OFF Icon not present	All the keypad partitions are disarmed.	No faults present.	Open zones on the keypad partitions.	Primary power failure (230V a.c.)
ON Icon on solid	At least one of the keypad partitions is armed.	At least one fault is present.	All the zones on the keypad partitions are in standby status: Ready to arm.	Primary power OK (230V a.c.)
Slow blinking (ON: 0.5sec OFF: 0.5sec)	All the keypad partitions are disarmed. Memory of alarm/tamper on at least one of the keypad partitions or memory of a system alarm is present.	No faults present. At least one of the zones belonging to the keypad partitions is either disabled (inhibited) or is in Test status	All the zones belonging to the keypad partitions are in standby status. An unplayed voice message is present in the memo box.	
Fast blinking (ON: 0.15sec OFF: 0.15sec)	At least one of the keypad partitions is armed. Memory of alarm/tamper on at least one of the keypad partitions or memory of a system alarm is present.	At least one fault is active and at least one zone belonging to the keypad partitions is either disabled (inhibited) or is in Test status.	Open zones on the keypad partitions. An unplayed voice message is present in the memo box.	

The list of faults signaled on the yellow fault LED can be found in the table in *Appendix C, Fault signals*.

Following is the list of events which cause the Red System Alarm LED to blink:

- Open panel tamper
- Dislodged panel tamper
- Expansion tamper
- Keypad Tamper
- Reader Tamper
- Expansion Loss
- Keypad Loss
- Reader Loss
- False key

If the "False key" event is configured as a "Silent event", the red LED will not blink.

"FALSE KEY"

If this option is enabled, the status of the partitions will be hidden. If a valid code is entered at a keypad, the real-time status will be indicated on the keypad concerned for 30 seconds. Additionally:

"50131STATHIDDEN"

- If the partitions are armed, the status of the system will be hidden from non-authorized users.
 - Red keypad LED Off
 - Yellow keypad LED Off
 - Green keypad LED On solid
 - Status icons not present
 - Alarm and Tamper memory hidden
 - If a particular event occurs more than 5 times when the partitions are armed, it will not be signaled as having occurred more than 5 times. This is due to the limitation placed on the counter of each event. The counters will reset to zero each time all the partitions are disarmed.
- If the partitions are DISARMED:
 - The LEDs will function normally.
 - Status icons present
 - Alarm and Tamper memory visible

Emergency status

In the event of a keypad configuration or communication error between the system peripherals, the display will show one of the templates opposite.

If you are using an Alien user interface, the above-mentioned information will be shown on the bottom bar on the home page.

If this occurs, you must contact your installer immediately and get the fault cleared.

2-3-5

```
- JOY/MAX -
FW RELEASE X.YZ
NO COMMUNICATION
K01 P14
```

```
- JOY/MAX -
FW RELEASE X.YZ
NOT ENROLLED
K01 P14
```

Alien keypad

Alien is a colour touch-screen user interface. Two versions are available, the 4.3 inch Alien/S model and the 7 inch Alien/G model. The screen displays the dialogue boxes and coloured icons related to all the control panel functions and signals. As required, the Alien touch screen immediately shows the buttons required for the activation of the functions related to the specific situation.

By just tapping the screen you can activate one of the scenarios (programmed by the installer on the control panel), access information relating to the various parts of the system (zones, outputs, etc.) or view the events log.

The structured graphics control provides ample room for customization, with skin and background selection and image gallery slideshow management. You can also control the screen brightness, contrast and image transparency.

The Alien keypad has a built-in microphone and speaker for voice functions.

A temperature sensor indicates the room temperature on the screen and activates the Chronthermostat functions.

The built-in proximity reader reads tags and cards and allows easy access to the system without the need of code entry.

The Alien keypad has a USB interface and an SD card slot (up to 32GB) for storing photos and images.

The Alien user-interface provides the following user applications:

- photo-frame application, that allows viewing of slide-shows of all the images contained in the SD-card
- graphic maps for the supervision of the entire system monitored by the SmartLiving control panel through a graphic layout containing images, icons and buttons visualized on the display
- alarm and memo functions, programmable directly by the user, which generate audible signals and display popups

2-3-6



The Alien keypad screen

2-3-7

Access to the Alien keypad functions is achieved by tapping the respective buttons displayed on the screen.

Although the functions provided by the different versions of the Alien keypads are they same, the devices differ in screen size and the layout of the icons and buttons.

Following is the description of the Alien/S screen layout; the presence of the various elements described depends on the activated functions and the accessed window:

Table 2-7: Alien - screen

<p>A Data and Time of the SmartLiving control panel. If the control panel is in Service status, this field will show the address of the Alien and its built-in reader.</p>	
<p>B Keypad LED icons (<i>Table 2-6: Keypad LEDs</i>).</p>	
<p>C Temperature read by the thermometer of the Alien user interface.</p>	
<p>D Icon which indicates the presence of an SD card in the card slot. After the entry of a valid user code, the Logout key which appears will allow you to close the session.</p>	
<p>E Section for active functions, with the buttons for access to the Alien user interface, its applications and the SmartLiving system. The home page of the Alien/S (shown in the figure) shows the function buttons indicated in <i>Table 5-3: Alien menu</i>. In the Alien/G, these buttons are shown in a section on the left and are always visible regardless of the active function.</p>	
<p>F String showing the arming status of the control panel, in accordance with the active scenario or status of the partitions. If a keypad partition changes its arming status in relation to the active scenario, or when the control panel is in service/maintenance mode, this string will show the characters which indicate the real arming status of the partitions, as described in <i>Table 2-2: Display visualization</i>.</p>	
<p>G Tapping this section on the display opens (for 3 seconds) a window containing a list of the active scenarios. If required by programming (<i>paragraph 5-8 Keypad settings</i>), it may request entry of a valid code.</p>	
<p>H System information icons, as described in <i>Table 2-3: Information icons</i>.</p>	
<p>I If you are inside a section, this field will show the following buttons which may cover the information buttons:</p> <ul style="list-style-type: none"> • Back level This key allows you to step back to the previously active function. • Home Button, present only on the Alien/S model, which allows you to go directly to the home page. 	

Further visualizations displayed on the Alien screen depend on the section/page being accessed by means of the buttons. The layout of such pages depends on the functions and buttons available and how they are used (*paragraph 5-20 Alien function keys*).

There are also alerts which the control panel activates automatically and that appear as pop-ups during the following events:

- **Zone alarm or tamper**
If any of the keypad partitions has alarm or tamper event memory, a pop-up will appear showing:
 - an "ALARM" warning and the description of the zone which generated the alarm or tamper signal
 - the **Disarm** button, to disarm all the armed partitions that the code and keypad in use have in common
 - the **Stop alarms** button, to deactivate the outputs activated by the alarm signal
 - the **Clear call queue** button, to cancel the calls in the outgoing call queue
 - the **Home** button provides direct access to the home page
- Activation of the **entry time**
- Activation of the **exit time**
If an entry or exit time is activated, a pop-up will appear showing:
 - a string indicating the remaining seconds of the running entry/exit time
 - the **Disarm** button, to disarm all the armed partitions that the code and keypad in use have in common
 - the **Scenarios** button, to access the scenarios available for activation
 - the **Home** button provides direct access to the home page



- icon which appears when you tap the display and the keypad is blocked due to 5 consecutive entries of an invalid code.



- icon which is shown when you tap the display and the keypad is blocked due to 5 consecutive entries of an invalid code.

Touching the "Settings" option on the home page for at least 7 seconds disables the sensitivity of the display for 20 seconds. During this interval, the "CLEAN SCREEN" message is shown to indicate that it is possible to clean the screen.

CLEANING THE DISPLAY

Touching any part of the screen for 50 seconds will restore touch screen sensitivity.

REBOOTING

Signalling on the Buzzer

2-3-8

Keypads equipped with buzzers provide you with audible signals, that is, if the sound has not been switched off.

If the keypad has voice function capacity, the buzzer will also signal incoming intercom calls from another keypad.

The buzzer signals the running entry, exit and pre-arm times (refer to *Appendix A, Glossary*) of enabled partitions. The activation these signals can be set up by means of the keypad options described in *paragraph 5-8 Keypad settings*.

If the control panel is duly programmed, the keypads will be able to generate alarm signals on the buzzer.

Table 2-8: Signalling and types of signal

Signalling	Type of signal
Button pressed	Single pulse (beep)
Entry time running	8 pulses + 5 second pause
Exit time running	3 pulses + 5 second pause; 4 short pulses + 5 second pause during the final 20 seconds of the exit Time
Pre-arm time running	1 pulse + 5 second pause
Activation of the output connected to terminal "T1" on the keypad	Continuous audible signal for the entire duration of output activation
Intercom call	Two-tone pulse
Alarm	Fast pulses

Reader - nBy

2-4

SmartLiving intrusion control panels can manage nBy/S and nBy/X readers and also the built-in readers of JOY/MAX, Aria/HG and Alien keypads.

The proximity reader is the easiest way for users to interact with the SmartLiving intrusion control system.

The wall-mount nBy/S model can be attached to any flat surface by means of two screws, it is IP34 rated and therefore suitable for outdoor use.

It is equipped with a buzzer and 4 LEDs:

- **F1** - Red
- **F2** - Blue
- **F3** - Green
- **F4** - Yellow

The Universal flush-mount nBy/X (**Patent Pending**) has been especially designed to integrate with all brands of cover plates.

It is equipped with 4 LEDs (red, blue, green and yellow).

Readers do not provide the same extent of system control as keypads, however, these devices are quick and easy-to-use and are extremely useful when carrying out day-to-day operations (arm/disarm partitions, etc.).

Readers are usually located near the main entry/exit points of the protected building. These devices allow system access to valid keys only. The system readers are capable of recognizing a large number of keys, each characterized by customized parameters. Each reader is enabled to operate on specific partitions, whereas each key is enabled to operate only on the partitions the user is allowed to control. Therefore, if a key is held in the vicinity of a reader, it will be possible to control only the partitions which the two devices have in common.

Each reader can be programmed with up to 4 shortcuts (one per LED).

Each key can be programmed with up to 4 shortcuts.

Unlike most traditional readers (which generally carry out arm/disarm operations only), nBy readers also manage a series of useful shortcut commands. For example, it is possible to associate two shortcuts to the red and blue LEDs for arm and disarm operations, and a shortcut to the green LED for gate control, and yet another to the yellow LED for "Clear call queue" operations.

The buzzer signals the running Entry, Exit and Pre-arm time of the reader partitions (refer to *paragraph 2-3-8 Signalling on the Buzzer*).



Signalling on the reader LEDs 2-4-1

The LEDs have two distinct operating in modes:

1. When no key is present at the reader (refer to *Table 2-9: Reader LEDs with no key at reader*), the LEDs will indicate the current status of the associated shortcut.
2. When a key is present at the reader (refer to *Table 2-10: Reader LEDs with key at reader*), the LEDs will indicate (in rapid succession) the available shortcuts.

Table 2-9: Reader LEDs with no key at reader

LED	Red	Blue	Green	Yellow
OFF (All LEDs Off)	All the reader partitions are disarmed. No alarm/tamper memory on the reader partitions or system tamper memory.			
ON / OFF (in accordance with the associated shortcut)	The scenario associated with the arming-shortcut of the red LED is active/inactive. The output associated with the output-activation shortcut of the red LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the blue LED is active/inactive. The output associated with the output-activation shortcut of the blue LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the green LED is active/inactive. The output associated with the output-activation shortcut of the green LED is active/inactive. Faults are present/not present.	The scenario associated with the arming-shortcut of the yellow LED is active/inactive. The output associated with the output-activation shortcut of the yellow LED is active/inactive. Faults are present/not present.
Intermittent blinking (ON: 2.3sec OFF: 0.1sec)	At least one Reader-partition is armed.			
Slow blinking (ON: 0.5sec OFF: 0.5sec)	The reader partitions are disarmed. Alarm/tamper memory on at least one of the reader partitions, or system tamper memory.	The scenario associated with the last key used is active.		
Fast blinking (ON: 0.15sec OFF: 0.15sec)	At least one Reader-partition is armed. Alarm/tamper memory on at least one of the reader partitions, or system tamper memory.			

Table 2-10: Reader LEDs with key at reader

LED	Red	Blue	Green	Yellow
OFF (no light)	Request to arm ALL the partitions common to both the key and reader.			
ON (only one LED On)	Request to activate the shortcut associated with the red LED on the reader or the first shortcut of the key	Request to activate the shortcut associated with the blue LED on the reader or the second shortcut of the key	Request to activate the shortcut associated with the green LED on the reader or the third shortcut of the key	Request to activate the shortcut associated with the yellow LED on the reader or the fourth shortcut of the key
ON (All the LEDs On)	Request to activate the shortcut associated with the key.			
Fast blinking (ON: 0.15sec OFF: 0.15sec one LED only)	If the shortcut associated with the red LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the blue LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the green LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.	If the shortcut associated with the yellow LED is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.
Fast blinking (ON: 0.15sec OFF: 0.15sec ALL LEDs)	If the shortcut associated with the key is an arming operation, one of the partitions concerned is not-ready-to-arm due to zones which are not in standby status.			

If a key is present, all operations (arm, disarm, etc.) will apply only to the partitions common to both the key and reader.

Note

If this option is enabled and there are no keys present at the reader, the reader LEDs will be Off.

"50131READERLEDOFF"

User Codes

2-5

Each User Code comprises a PIN for identification purposes and a group of parameters which determine its rank in the system code hierarchy and the operations the user is entitled to perform.

The PIN is made up of 4, 5 or 6 digits that the user must enter in order to allow identification.

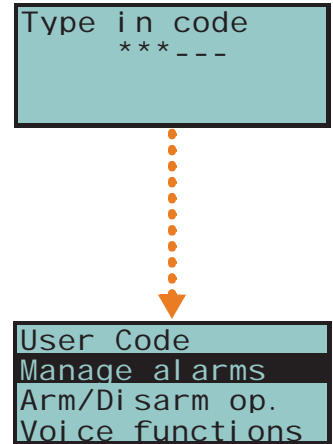
The PIN of the only user code enabled at default is 0001. The PINs of the successive codes are 0002, 0003, etc.

The PINs of user codes can be changed by the installer or by other hierarchically superior code. The installer provides the system users with default user PINs which they must change immediately to PIN codes of their choice.

Each user code has the following parameters, to be programmed by the installer or by other user codes of hierarchically superior level.

- The **partitions** the user can control.
If a user code is entered at a keypad, the user can control only the partitions which are common to both the code and keypad concerned. For example, if a code enabled on partitions 1, 2, 3, 4 and 5 is entered at a keypad which enabled on partitions 4, 5, 6 and 7, it will be able to operate on partitions 4 and 5 only.
- The **type of user code**.
Each code can be assigned a specific level in the system hierarchy:
 - User
 - Manager
 - Master
 Each code, in accordance with its assigned level in the system-hierarchy (the "User" being the lowest level), is capable of carrying out the following operations on all other codes that are hierarchically inferior:
 - enable/disable
 - change PIN
 - change several programming parameters
- The **ways of accessing the user menu**.
Each code can access its customized menu in 3 different ways (refer to *paragraph 2-5-1 Ways of accessing the user menu*).
- The **commands over the phone**.
This option enables access to the system via remote telephone. If this option is enabled, the User can send commands to the control panel over-the-phone. Commands can be sent during calls to/from the control panel. After a valid PIN entry on the telephone keypad the user can activate specific shortcuts (refer to *Chapter 3 - Shortcuts*). This method of entering commands will affect the code partitions only.
- **Timer Restriction** (codes limited to a timeframe)
If a code is associated with one of the timers, it will be able to operate the system only when the timer is On.
- The **group of outputs which can be activated/deactivated manually**
After accessing the Outputs ON/OFF section (user menu) you can activate/deactivate the duly programmed outputs.
- The **menu sections** the user can access (refer to *paragraph 2-5-1 Ways of accessing the user menu, point 1.*)
- **Customized shortcuts**.
Each code can be programmed to manage:
 - up to 12 customized (personal) shortcuts assigned to keys **F1** Fn, ..., **F4** Fn
 - up to 10 customized (personal) shortcuts assigned to keys **0** ↵, ..., **9** wxyz
 These shortcuts are available to the code user only after accessing the user menu.

Note



Ways of accessing the user menu

2-5-1

In order for code users to access their user menus, they must first validate their codes.

This can be done by typing-in the code PIN and pressing **OK**.

If the installer has enabled the "Fixed length" option on a user code, the user must first press **OK** and then type-in their PIN.

"FIXED LENGTH"

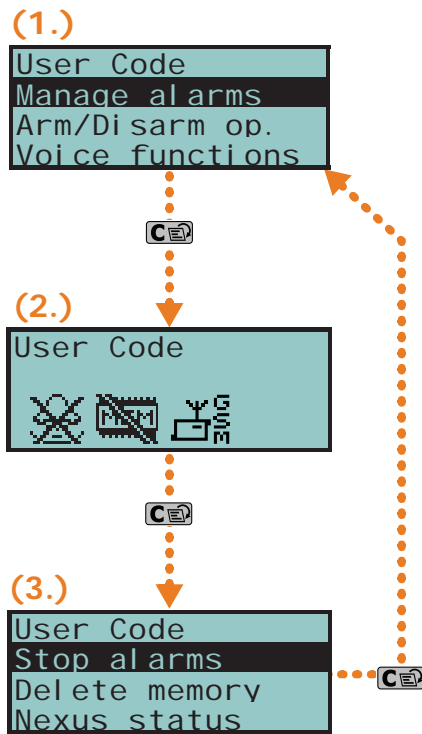
At this point, there are 3 different ways of allowing first-access to the user menu, depending on the system setup, as follows:

1. The user can access the menu directly, as shown in the figure opposite (1.); by means of keys and , the user can select the desired menu section and then press for access. Following is a the list of available user-menu sections:

- Manage alarms
- Arm/Disarm op.
- Voice functions
- Activations
- View
- Outputs ON/OFF
- Set date/time
- Keypad settings
- Change PIN
- TelephoneNumbers
- Teleservice req.
- Overtime request
- Thermostat
- Nexus Nexus
- Codes
- Timers

2. The keypad deletes the shortcut icons associated with keys **F1 Fn**, ..., **F4 POU** and replaces them with the customized shortcut icons associated with the code, as illustrated opposite (2.). Keys **F1 Fn**, ..., **F4 POU** and **0**, ..., **9 wxyz**, will allow the user to select the desired shortcut.

3. You can access a descriptive menu of the customized shortcuts assigned to keys **F1 Fn**, ..., **F4 POU**, as shown opposite (3.). To activate the user shortcut, use keys and to select the description then press .



These methods, show how you can access the menu after code validation, in other words, on first access. At this point, each time you press key , 3 different objects will appear, select the one that applies to the operation concerned and then continue.

Keys 2-6

The SmartLiving system is capable of managing INIM's contact-free digital-keys, which are available in three versions:

- **nKey, nBoss** - tag fro proximity readers
- **nCard** - proximity card
- **Air2-KF100** - remote control key



Each key is unique and is identified by a random code selected from over 4 billion code combinations. During the installation phase, each key is enrolled on the system in order to allow it to operate.

Each key is characterized by the following parameters (programmed by the installer) in accordance with the requirements of the key user.

- **Partitions** - user codes can control only the partitions they are assigned to. If a key is used at a reader, it can operate only on the partitions the two devices have in common. For example, if the key controls partitions 1, 3, and 5 and the reader controls partitions 1, 2 and 6, the key can operate on partition 1 only, as it is the only partition the key and reader have in common. If a button on the remote-control is pressed, the user will be allowed access only to the partitions the device is assigned to.
- Up to 4 **Shortcuts**.
- A **Timer** can be set up to restrict the use of a key. A key associated with a timer will only be accepted by the system during the timeframe set for the timer involved.
- The **Patrol** option is usually enabled on keys used by security personnel or night watchmen who must patrol the protected premises at regular intervals. This type of key does not allow the user to select the "Arm Type". When a key with this attribute is recognized, the system will perform the following operations:
 1. Disarm the partitions common to the key and reader concerned.
 2. Activate the respective Patrol Time for the partitions concerned.
 3. Re-arm the partitions (as before) when the Patrol Time expires.



If the patrol key is held in the vicinity of the reader while the Patrol Time is still running (for example, if the inspection ends ahead of time), the Patrol Time will end immediately and the partitions will arm as before.

- The **Service** (maintenance) option allows keys to deactivate instantly any outputs associated with zone and partition alarm/tamper events (on the Partitions the key and reader have in common). This type of key can select the reader shortcuts and its customized (personal) shortcuts.

Air2-KF100 Wireless keyfobs 2-6-1

The KF100 remote-control has 4 buttons which can each be programmed with a shortcut (ask your installer for details). The graphic-choice feature allows you to identify the buttons by numbers or icons.

The remote-control also provides 4 button-associated LEDs and a confirmation LED. As a result of two-way communications with the BS200 transceiver, the KF100 remote-control imparts audible and visual feedback signals (beep and LED signals) which notify the user of the outcome of requested operations.

Table 2-11: Feedback signals provided by KF100 wireless remote-control

Key	Icon	LED 1	LED 2	LED 3	LED 4	Buzzer signal	Operation
F1		1 flash				beep	Activates shortcut 1
F2			1 flash			beep	Activates shortcut 2
F3				1 flash		beep	Activates shortcut 3
F4					1 flash	beep	Activates shortcut 4
F2 + F3			1 flash	1 flash		beep	Block/Unblock remote-control device
Any				4 flashes	4 flashes		Remote-control device blocked

If an operation is successful, but the corresponding LED fails to light, it is an indication that the battery is low. The battery must be replaced before it runs out completely.

Note

Table 2-12: Control panel signals over wireless keyfob

Feedback from panel	Confirmation LED - green	Confirmation LED - red	Buzzer signal
Command not received		1 flash	
Operation not done		4 flashes	bop
Operation done	3 flashes		long beep

Multi-system access 2-7

Users can access several systems using the same code/key/remote-control device. The user code, key or remote-control device must be enrolled separately on the control panels concerned, and can be programmed with different attributes and functions in accordance with the requirements of each specific system.

The keys and codes provide the systems with random codes (for keys) or PINs (for codes) which the system associates with the respective attributes and functions programmed by the installer. For example, a user key/code may be enabled on partitions 1 and 2 on system A, on partitions 7, 8 and 9 on system B and on partitions 4 and 5 on system C.

This operating method is possible for all keys and codes.

Telephone functions 2-8

The SmartLiving control panel events can be programmed to trigger report calls to an Alarm receiving Centre (via digital dialler) and also voice calls and SMS messages to contact numbers.

The SmartLiving control panel also accepts commands over-the-phone. Shortcut commands can be sent during calls to/from the control panel, after valid PIN entry on the telephone keypad.

The commands can be activated by keys "0" to "9" on the telephone keypad, which the system associates with various shortcut actions. Each code can be programmed with customized shortcuts, such as: arm, disarm, activate/deactivate outputs, delete alarm memory, etc.

If the system is equipped with a SmartLogos30M voice board, the code shortcuts assigned to keys "0" to "9" will be announced over-the-phone, in order to facilitate operations.

Additionally, the Listen-in function allows you to eavesdrop on the protected premises by means of the keypad microphones.

When a user requests an operation, via a correctly formatted SMS message or voice call to the SIM card of the Nexus, the control panel will activate the respective shortcut and send confirmation (feedback) of the successfully implemented command.

WEB / e-mail functions

The SmartLAN/G board guarantees complete access to the functions of the SmartLiving system either by means of the user and installer codes. The control panels can be reached and configured even when the computer in use is not equipped with INIM software. An Internet connection is necessary either through a PC or the AlienMobile app for smartphones and tablets.

All SmartLAN/G equipped SmartLiving control panels are capable of sending event associated e-mails (SmartLAN/G is an optional accessory board).

The e-mail text, subject, attachments and recipients must be edited by your installer. No changes whatsoever should be made to the e-mail structure. Each e-mail can be associated with a subject, a text body (in a format capable of containing a direct link to a website or to an IP addressable device such as an IP camera) and an attachment document/file.

For a description of a typical e-mail format, refer to *paragraph 5-21-1 e-mail*.

In addition to e-mails, the SmartLAN/G board allows you to interface with the control panel from any computer or mobile phone device (PDA, mobile phone, etc.) via any Internet browser. The SmartLAN/G board integrates a web-server which allows users to operate the control panel from remote locations without the need of authentication.

For web-server access and use, refer to *paragraph 5-21-2 Access to and use of the Web interface*.

2-9



AlienMobile Application

INIM Electronics now offers SmartLiving control panel users the Alien Mobile application for smartphones and Android or Apple tablets, in two different versions:

- **AlienMobile** - free App with basic functions
- **AlienMobile+** - purchasable App with advanced functions

The application can be downloaded from an on-line application store (Play store or Apple app store).

The user, via smartphone or tablet can monitor up to 5 SmartLiving control panels by means of an interface similar to the one described in this manual for the Alien keypad or for the web-server interface of the SmartLAN/G board.

It is the installer's task to prepare the control panel for direct connection to the devices which use the Alien Mobile application and to configure the application for use with the system to be monitored and, finally, to provide end-users with all the necessary access data.

For instructions for use and access to the system via Alien Mobile refer to *paragraph 5-22 Using AlienMobile application*.

2-10



Inim Cloud

2-11

The INIM Electronics Cloud service provides SmartLiving users with a further mode of intrusion panel management via Internet.

The connection of control panels to the Cloud service is achieved via a web interface (the AlienMobile+ App or any browser) without any need to configure the network on which the control panel is installed. In particular, it is not necessary to program a router to perform port-forwarding and the like in order to reach the control panel.

Intervention with regard programming relating to network operations is not required on SmartLAN cards, since these cards are programmed by default with DHCP enabled (option to automatically assign an IP address to the devices on the network).

In order to allow use of the Cloud service, the user must have their own account at www.inimcloud.com, registered as "User".



After login, the user will have access to a customized web interface which provides all the tools required for supervision of all the control panels registered by the user.

Following is the description of the home page; the presence of each of the following elements described depends on the activated functions and the page you are accessing:

Table 2-13: Inim cloud - home page

A	Button for the selection of one of the registered control panels and description of the selected control panel.	
B	Buttons for access to the sections relating to the selected control panel (paragraph 5-27 Use of the Inim Cloud)	
C	Description of the main user and supervisor. The symbol indicates Cloud ownership.	
D	Buttons for quick viewing	
E	Buttons for user profile management	
F	Section for the display of all the ongoing alarms and alarm memories	
G	Text section relating to the button pressed	

Present at all times in the upper right corner are the buttons for viewing and editing the profile of the user and control panel registered to the cloud. Editing can be done after data has been unlocked by clicking on the respective icon .

In order to use the Inim Cloud services, registration must be carried out also by the user. For the procedure relating to Cloud registration please refer to *paragraph 5-27-1 Registering a control panel to the user account*.

The Inim Cloud service provides three different user levels, relating to a single control panel. The ratings may be different in your profile, depending on the control panel:

- **Supervisor**, corresponds to the installer who registered the control panel to cloud and who can, by means of Web interface, supervise the system and who can, through the SmartLeague software, change its programming.
- **Admin**, corresponds to the first user who registers the control panel to their own cloud profile and who can, through a web interface, supervise the system. And who can, by accessing their own profile (*Table 2-13: Inim cloud - home page, E*), delete the control panel from their own account or that of other users. Furthermore, can pass the title of "Admin" to another user.
- **User**, is the user who registered the control panel to their own cloud profile and who can, through a web interface, supervise the system. And who can, by accessing their own profile (*Table 2-13: Inim cloud - home page, E*), delete the control panel from their own account.

USER LEVELS

The "ownership" attribute allows a user to delete a control panel from the supervisor's account. It can be assigned both the installer and the end user by the installer during registration of the control panel to cloud.

OWNERSHIP

Therefore, if "owner" is the user, they can enable/disable other users and the installer who supervises the system.

If, instead, the installer is the "owner" they can enable/disable themselves and the "Admin" user.

The deletion of a control panel from the profile of a user, supervisor or not, including your own profile, determines the complete deletion of the control panel from cloud.

Note

Arming scenarios

2-12

A scenario is a preset arming configuration which applies various operating modes to the SmartLiving security system partitions (the scenarios are programmed by the installer in accordance with user requirements).

For example, if all the occupants are leaving the building, you can apply a scenario that arms all the partitions and activates the outputs which closes the rollerblinds and switches off the lights. On returning to the building, you can apply a scenario that disarms some of the partitions (those required) and activates an output which switches on the garden lights.

Following the activation of a scenario, it is also possible to change the status of several outputs simultaneously or change the value of the voltage supplied to the outputs and thus change, for example, the brightness of any lights with this capability.

The installer will set up the and make available the scenarios which best suit user requirements. Users can activate the scenarios via keypads, readers, remote-control devices and over-the-phone by means of shortcut commands (refer to *Chapter 3 - Shortcuts*). Scenarios can also be activated via a browser with an web interface for mobile phones or PCs, or through the Alien Mobile application by accessing the "Scenarios" section (*paragraph 5-2 Arming and disarming partitions*).

If the "Show scenario" control panel parameter is active, the left side of the second line on the screen will display the current scenario.

"SHOW SCENARIO"

If you are using an Alien keypad, the "View partition status" option (refer to *paragraph 3-3-3 Remote-control shortcuts*) will allow you to select the visualization mode of the operating status on the bottom bar of the display:

"VIEW PARTITION STATUS"

- Single partition - the characters relating to the operating status of the partitions will be shown, as described in *Table 2-2: Display visualization*
- Single scenario - the description of the active scenario will be shown

Additionally, tapping the bottom bar on the home page will open (for 3 seconds) a window containing a list of the active scenarios. If required by programming (*paragraph 5-8 Keypad settings*), it may request entry of a valid code.

Videosurveillance

2-13

The SmartLAN/G board supports JPEG and MJPEG streaming for surveillance cameras, viewable as a full video or snapshot.

The SmartLiving control panel is capable of managing two types of IP cameras (or "webcams"), which use one URL address for video viewing:

- static cameras
- cameras with Onvif protocol, which allow user interaction thanks to remote control capabilities and pre-programmed audio/video profiles

The visualization of the shots (images or video) is achieved by accessing the URL address of the camera. It can be done via web browser or AlienMobile application, through the "Camera" section, or by means of the cameras configured inside the graphic maps.





The user can view the image flow or video in real-time and, solely through the Alien web-interface, view the image recordings which precede and follow the occurrence of an event.

Chapter 3

SHORTCUTS

Keypad shortcuts

3-1

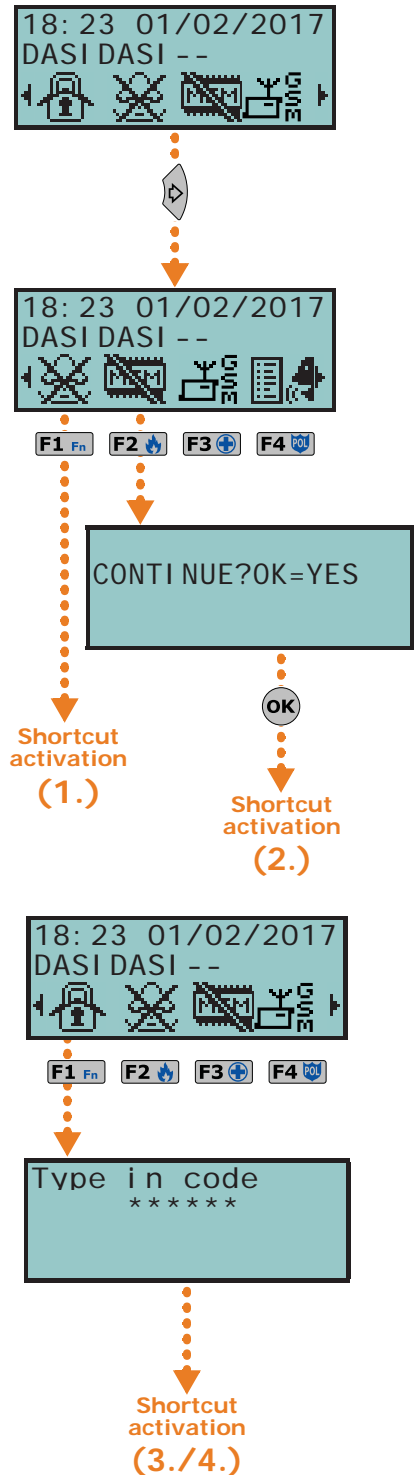
The installer can program each Joy, Aria/HG, nCode and Concept keypad with up to 12 shortcuts associated with 4 function keys **F1 Fn**, **F2 Fn**, **F3 Fn**, **F4 Fn**. The shortcuts are identified by icons which appear on the lower part of the display. Arrows to the right and left of the icons indicate that keys , , will allow you to view and use other shortcuts (if programmed).

The 12 keypad shortcuts can be activated in 4 different ways, as follows.

1. **By ALL.** Pressing the respective key **F1 Fn**, ..., **F4 Fn** will activate the shortcut instantly without code entry. The shortcut will affect all the keypad partitions.
2. **By ALL with confirmation request.** Pressing the respective key **F1 Fn**, ..., **F4 Fn** will prompt the system to ask you if you want to continue or not. If you press **OK** the shortcut will activate instantly, if you press **CE** or **Esc** the operation will be abandoned. This method protects against accidental operations. The shortcut will affect all the keypad partitions.
3. **Code users only.** Press the respective key **F1 Fn**, ..., **F4 Fn**, then enter a valid code, the shortcut will activate after code recognition. The shortcut will affect the partitions common to both the keypad and code.
4. **Code users only when activation of the shortcut lowers system security.** If a shortcut involves a scenario that completely disarms a partition, or switches a partition from Away mode to Stay mode, the security of your system will obviously be at risk, therefore, the system will request code entry. The shortcut will affect the partitions common to both the keypad and code.

To activate a shortcut, press the key which corresponds to the shortcut icon: **F1 Fn**, ..., **F4 Fn**. The system will either activate the shortcut instantly (case 1.) or will request confirmation (case 2.) or code entry (cases 3. and 4.) before carrying out the operation.

Alien user interfaces do not have function keys **F1 Fn**, **F2 Fn**, **F3 Fn**, **F4 Fn**, nor do they provide access to certain functions via shortcuts. However, the screen provides buttons which, with a single tap, activate functions and applications. For further details refer to *paragraph 5-20 Alien function keys*.




Shortcut with code

3-2

Besides the shortcuts provided by keys **F1_{Fn}**, **F2_{Fn}**, **F3_{Fn}**, **F4_{Fn}**, each user code can have as many as 22 customized (personal) shortcuts.

Users will be able to access their code-shortcuts only after validating their PINs (refer to *paragraph 2-5-1 Ways of accessing the user menu*). Each code can be programmed to manage:

- Up to 12 shortcuts can be activated by keys **F1_{Fn}**, ..., **F4_{Fn}** and identified by explicit icons.
- Up to 10 shortcuts can be activated by keys **0_{xyz}**, ..., **9_{xyz}**. If a code is enabled to operate the system over-the-phone, these shortcuts will also be available on the telephone number-keys.

Entry of a code associated with shortcut no.9:  at a keypad with the speaker, prompts the voice announcement of all the shortcuts assigned to the number keys.

Via Keypad

1. Validating your PIN
2. Access the user menu, using the method described in *paragraph 2-5-1 Ways of accessing the user menu* at point 2.
3. Press the key **F1_{Fn}**, ..., **F4_{Fn}** which corresponds to the shortcut icon or press the key **0_{xyz}**, ..., **9_{xyz}** which is assigned to the shortcut.

If the installer has enabled the "Fixed length" option on a user code, the shortcut assigned to **F12** will activate as soon as the user types-in their PIN without need of touching any other key.

"FIXED LENGTH"

Over-the-phone

1. Establish communication with the control panel.
2. Type in your code followed by "#".
3. Listen to the voice prompts regarding the available shortcuts.
4. Press the number key which corresponds to the required shortcut.

Key and Reader shortcuts

3-3

nBy/S and nBy/X Reader shortcuts

3-3-1

Hold a valid key in the vicinity of the reader, as soon as the reader accepts the key, a series of visual signals on the reader LEDs will indicate the various shortcuts.

When the required shortcut is indicated, remove the key to activate the corresponding shortcut action.

The visual signals on the Reader LEDs are as follows (refer to *Table 2-10: Reader LEDs with key at reader*).

1. **Red LED on for 3 seconds** - shortcut associated with the red LED of the reader or first shortcut of the key
2. **Blue LED on for 3 seconds** - shortcut associated with the blue LED of the reader or second shortcut of the key
3. **Green LED on for 3 seconds** - shortcut associated with the green LED of the reader or third shortcut of the key
4. **Yellow LED on for 3 seconds** - shortcut associated with the yellow LED of the reader or fourth shortcut of the key
5. **All LEDs on for 3 seconds** - first shortcut associated with the user key
6. **All LEDs off for 3 seconds** - disarm all the partitions.
7. If the key is not removed, the reader will run through the entire sequence again starting from the red LED. Selection of the desired shortcut (indicated by a specific LED) will not occur until the key is removed.


If, during this phase, any of the partitions are armed, the LED sequence will start at point 6.

If the installer has enabled option "50131ReadLedOFF", the reader LEDs will be off, therefore, if you wish to activate a shortcut, you must:

1. Wave the key across the sensitive area of the reader: the LEDs will signal the respective status for 30 seconds.
2. During this 30 second period, hold a valid key in the vicinity of the reader in order to generate the shortcut, as previously described.

"50131READERLEDOFF"

Shortcuts on the built-in readers of keypads

Users must hold their digital keys in the vicinity of the built-in reader (the position of the reader is indicated by ) , instead, on the Alien keypad it is positioned on the lower right-hand corner of the frontplate).

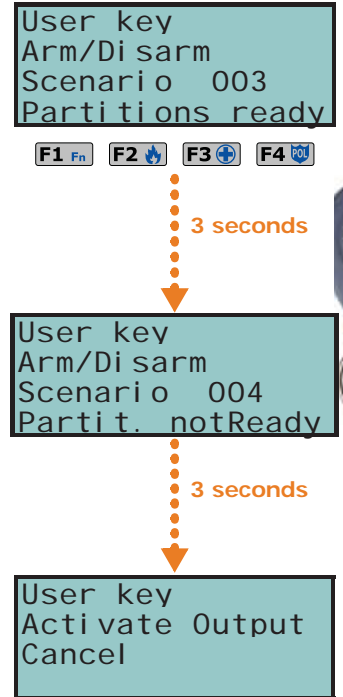
The key and reader shortcuts will flash one-by-one at 3 second intervals on the keypad display. When the required shortcut is indicated, remove the key to activate the corresponding action.

The shortcuts appear on the display in the following order:

1. Description of the first reader shortcut for 3 seconds
2. Description of the second reader shortcut for 3 seconds
3. Description of the third reader shortcut for 3 seconds
4. Description of the fourth reader shortcut for 3 seconds
5. Description of the fourth reader shortcut for 3 seconds
6. "Disarm" (disarms all the partitions) for 3 seconds
7. Then back to point 1. and run through the sequence until the user removes the key, thus selecting the shortcut described in the moment key is removed.

If, during this phase, any of the partitions are armed, the LED sequence will start at point 6.

3-3-2



Remote-control shortcuts

To activate the installer-programmed shortcuts assigned to the 4 keys **F1**, ..., **F4** on the remote-control device, simply push the button which corresponds to the desired command. The successful outcome of the operation will be signaled by audible and visual feedback (refer to *Table 2-11: Feedback signals provided by KF100 wireless remote-control*).


3-3-3

Shortcut list

3-4

For the complete list of shortcuts refer to the table in *Appendix B, Shortcuts at default*. Shortcuts 0 to 8, shown in the table, carry out the specified actions instantly.

Shortcut 9  can be activated over-the-phone only (telephone shortcut).

Shortcut 17  can be activated over-the-phone or at a keypad.

All other shortcuts (from 10 to 16 and from 18 to 37) provide direct access to specified sections in the user menu, therefore, can be activated at keypads only.

Shortcut on event

3-5

The shortcuts on events are control panel functions which are triggered (activated) by the occurrence of an event.

The definition of these functions and their triggers can be achieved only through appropriate programming of the SmartLiving control panel by the installer and cannot be done by the user.

Chapter 4

VOICE FUNCTIONS

If the SmartLiving control panel is equipped with a SmartLogos30M voice board, you will be able to take advantage of all the voice functions provided by the JOY/MAX, Aria/HG and Alien keypads, including the over-the-phone voice guide.

Your installer will program the voice messages you require:

- for event-associated calls
- for event-associated announcements on the keypad at address 1

All keypads with voice functions provides a voice memo-box for the recording and playback of messages. This handy function will allow you to leave messages for other users who have access to the keypad; refer to *paragraph 5-3 Voice box and intercom functions*. You can record, play and delete messages at your own discretion.

The presence of a new memo in the memo-box will be indicated on the blue LED on the keypad, as described in *Table 2-6: Keypad LEDs*.

The SmartLogos30M voice board provides a total of 60 seconds memo time (shared by all the voice-capable keypads in the system).

15 memo slots are available.

Note

Chapter 5

USING THE SYSTEM

This chapter describes all the operations users can carry out with or without authorization (user PIN entry). The tools and methods which allow access the system operations are as follows.

The system can be accessed:

- via **Keypad - Joy, Aria, nCode/G, Concept/G**
in which case the user can operate the system in two ways:
 1. by means of shortcuts (refer to *paragraph 3-1 Keypad shortcuts*);
 2. by means of access codes via the user menu (refer to *paragraph 2-5 User Codes* and *paragraph 3-2 Shortcut with code*). Users have various ways of viewing their personal menus (refer to *paragraph 2-5-1 Ways of accessing the user menu*). However, this chapter describes only the procedures starting from the menu with visual information relating to the sections described at point 1 in *paragraph 2-5-1 Ways of accessing the user menu*.
- via **Keypad Alien**
in this case, users are provided with buttons, displayed on the screen, that with a single tap activate functions and applications. For further details refer to *paragraph 5-20 Alien function keys*.
- via **Reader (nBy, built-in reader on keypads)**
The proximity-key reader provides users with only one way of accessing the system, as described in *paragraph 3-3 Key and Reader shortcuts*.
- Over-the-phone
During a call from/to the control panel after valid code (PIN) entry.
- Via **Command Zone**
After violation of a duly-programmed zone which sends a command to the control panel.
- Via **Wireless remote-control device**
by means of keys **F1**, ..., **F4**, as described in *paragraph 2-6-1 Air2-KF100 Wireless keyfobs*.
- Via **Web**
by means of the integrated web-server on the SmartLAN/G (if installed) via any browser (refer to *paragraph 5-21-2 Access to and use of the Web interface*).
- Via **AlienMobile Application**
In this case, users are provided with buttons, on the screen of their smartphones, which activate functions and applications from remote locations (refer to *paragraph 5-22 Using AlienMobile application*).
- Via **Inim Cloud**
by means of a browser, the user can access a customized web interface which provides all the registered control panels (refer to *paragraph 2-11 Inim Cloud* and *paragraph 5-27 Use of the Inim Cloud*).

Managing alarms

5-1

This paragraph describes the actions users can take during typical alarm and tamper conditions:

- **Stop alarms** - deactivates instantly the outputs activated by zone/partition alarm and tamper events and system tamper events.
The system tamper events are:
 - Open panel
 - Dislodged panel
 - Peripheral tamper (expansion, keypad, reader)
 - Peripheral loss (expansion, keypad, reader)
- **Clear call queue** - clears the outgoing call queue and stops any ongoing calls.
- **DeleteAlarm mem.** - implements a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.

Via Keypad

Method 1

Activate the shortcuts associated with keys **F1**, ..., **F4** shown on the display, with or without code entry:

- The shortcut which is assigned to "Alarm menu" menu operations (shortcut n.13: allows you to view the respective section. You can select one of the following options, using keys and and activate it by means of the **OK** key:
 - **Stop alarms**
 - **Clear call queue**
 - **DeleteAlarm mem.**
- The following shortcuts activate the associated commands:
 - Shortcut n.2: "Stop alarms"
 - Shortcut n.3: "Clear call queue"
 - Shortcut n.4: "DeleteAlarm mem.";

Method 2

Access the "Alarm management" section (user menu) by means of a valid PIN. Follow the instructions described in **Method 1**.

Via Alien touch screen

Access the "Menu" section by tapping , type-in the user code and then access the "Actions" section.

This section contains a list of control panel commands which can be activated by tapping **ON**, commands such as:

- **Stop alarms**
- **Clear call queue**
- **Clear alarm memory**

Via Reader

Hold a valid key in the vicinity of the reader until the reader LEDs or display indicates "Stop alarms" (shortcut n.2), "Clear call queue" (shortcut n.3) or "DeleteAlarm mem." (shortcut n.4).

Over-the-phone

Type-in the PIN of a user code followed by **#** (the user code must be enabled to operate the system over-the-phone), then press the key (from **0** to **9**) which the installer has programmed to activate "Stop alarms" (Shortcut n.2), "Clear call queue" (shortcut n.3) or "DeleteAlarm mem." (shortcut n.4).

Via Wireless remote-control device

Push the respective button on the remote-control device and verify the outcome of the requested operation, as described in *paragraph 2-6-1 Air2-KF100 Wireless keyfobs*.

Via Web and AlienMobile

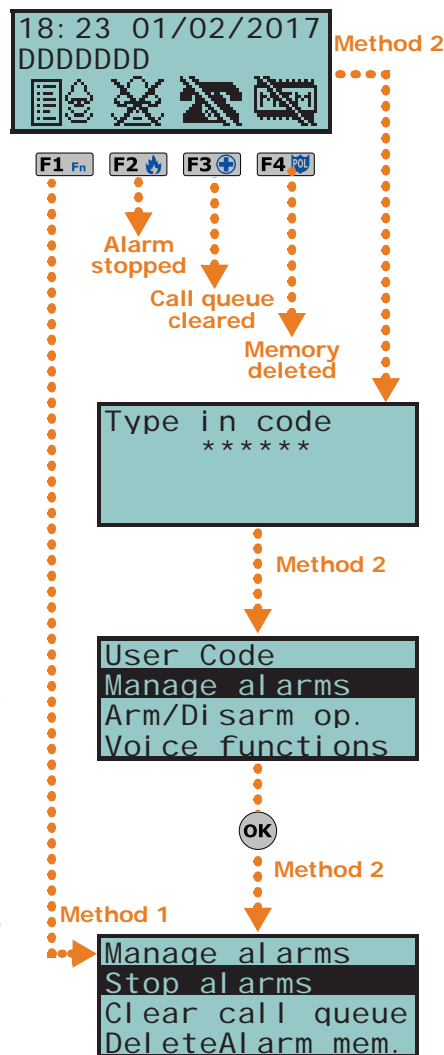
First access the "Intrusion" section, then the "Partitions" section.


This section contains the list of partitions the user can control, the **SET** button opens a window containing a list of commands for the partition. The **RESET** button deletes the alarm memory and, if allowed, also tamper memory.

Via Inim Cloud

Viewing and management of alarms by means of access to the cloud is possible in the following ways:

- If alarms or alarm memories relating to any of the registered control panels are present, they will be listed in the dedicated section in the centre of the page (*Table 2-13: Inim cloud - home page, F*). Alongside each of them you will find an **Ok** button that will allow you to confirm display of the alarm event.
- The **Events** button provides access to the viewing of all the events of the selected control panel. The alarm events can be identified by the icon.
There is also a button to confirm the visualization of all the ongoing alarms.



- The button for quick viewing  (Table 2-13: Inim cloud - home page, D) opens a window containing a list of the last 4 alarm events. This window also provides a button that accesses the events sections of the selected control panel. When required, this button shows the number of alarm events of all the registered control panels for which viewing has not been confirmed.

Arming and disarming partitions



You can arm/disarm the system partitions via keypad, reader, over-the-phone, zone command, wireless command, Internet, as follows.

If you request an arm-partition command at a keypad (for one or more partitions) and not all the zones involved are in standby status (thus execution of the command would generate an instant alarm), the keypad will provide a list of the zones concerned.

You can scroll the list and check the zones which are not in standby status (open zones). If you wish to implement the command, the visualized zones will generate an instant alarm.

If you request an arm-partition command at a keypad (for one or more partitions) and conditions (programmed by the installer) which lower the security of the system are present, the keypad will provide a list of the conditions concerned, as shown in the figure opposite.


You can scroll the list and view the conditions which lower the security of the system.

If you wish to implement the command, you must use a keypad and press . Arming the system under such circumstances will generate a "Forced arming" on partition event. This event highlights the fact that partitions were armed when conditions which lowered the security of the system were present (for example, "Low battery" or "Mains failure"). If, however, the installer included the "LossTamp.ongoing" event in the list of conditions which lower security, and this condition is active, you can cancel the operation by pressing .

Via Keypad






Method 1

Activate the shortcuts associated with keys , ...,  (shown on the display) with or without code entry:

- The shortcut that is assigned to "Arm/Disarm" operations (shortcut n.1: ) applies the pre-set scenario.

If the shortcut is activated by the entry of a code PIN with the "Fixed Length" attribute, and if all the partitions the user controls are disarmed, they will switch status and arm; likewise, if all the partitions the user controls are armed they will switch status and disarm.

- The shortcut assigned to "Arm/Disarm Menu" (shortcut n.12: ) allows you to view the respective section and arm (in Stay or Away mode) or disarm each partition separately.

- Select the desired partition, using keys  and .
- Select the required operating mode for the selected partition, using keys  and .
- Once you have set up the required operations for all the partitions, press .

Method 2

Access the "Arm/Disarm" section of the user menu by means of a valid code PIN. Follow the instructions described in **Method 1**.

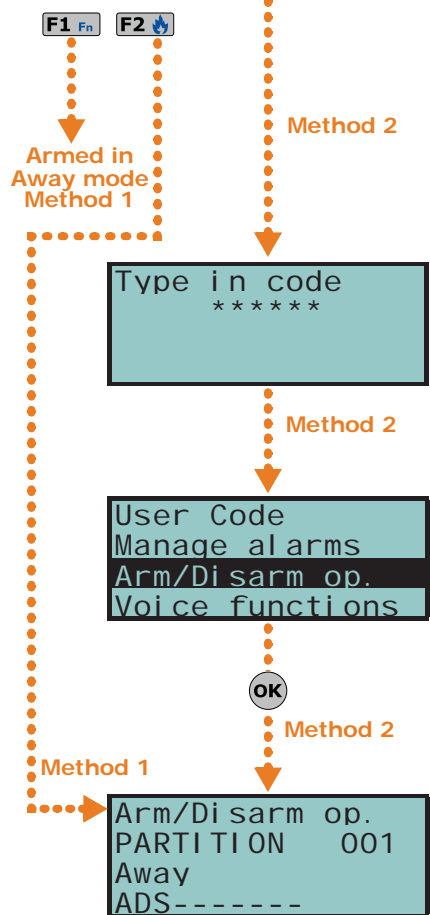
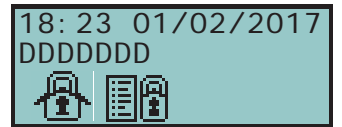
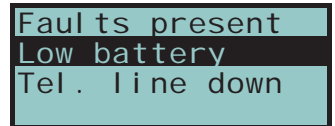
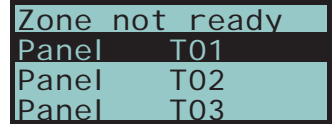
Method 3



While the entry time is still running (refer to "Entry time" in *Appendix A, Glossary*), type in a valid code (the code must have access to the "Arm/Disarm" section of the user menu), the partitions the code and keypad concerned have in common will disarm instantly.

Via Alien touch screen

The Alien keypad allow users to activate the programmed scenarios and also set up the arming mode of the partitions they control (have access to):

5-2



- Access the “Scenarios” section by tapping . This section provides a list of the scenarios which can be activated by means of the **ACTIVATE** button.
- Access the “Intrusion” section by tapping , type-in the user code and then access the “Partitions” section. This section displays the partitions separately. You can scroll and select a partition by means of the right/left scroll keys and then select the arming mode by means of up/down keys. To apply the selected arming mode tap **OK**.

Via Reader

Hold a valid key in the vicinity of the reader and remove it when “Arm/Disarm” (shortcut n.1) is indicated on the LEDs (the system will apply the preset scenario).

Over-the-phone

Type in a valid code PIN followed by “#”. Press the number key (from “0” to “9”) associated with the “Arm/Disarm” shortcut (shortcut n.1) in order to apply the pre-set scenario.

Via Command Zone

Under normal circumstances, a command zone comprises a mechanical key-lock or call point which activates an electrical contact wired to the command zone. In accordance with how the command zone is configured, it is possible to:

- arm the partitions the zone belongs to
- disarm the partitions the zone belongs to
- switch the status of the partitions (arm any disarmed partitions and disarm any armed partitions, refer to “Switch Zone” in *Appendix A, Glossary*)
- arm the partitions the zone belongs to when the command zone is violated, and disarm the partitions the zone belongs to when it restores to standby

Via Wireless remote-control device

Push the respective button on the remote-control device and verify the outcome of the requested operation, as described in *paragraph 2-6-1 Air2-KF100 Wireless keyfobs*.





Via Auto-arm operations

If a partition is associated with a timer which controls automatic-arming operations, it will arm when the timer switches ON and disarm when the timer switches OFF. Users who are enabled to control Auto-arm operations (refer to *paragraph 5-4 Activations*) must:

- activate the timer associated with the Auto-arm operations
- enable the Auto-arm option for the partitions concerned

Via Web and AlienMobile

Access to the system via web browser and mobile phone allows users to activate the programmed scenarios and also set up the arming mode of the partitions the users controls:

- Access “Scenarios” section This section provides a list of the scenarios which can be activated by means of the **ACTIVATE** button. The description of the current scenario is displayed on the bar on the bottom left of the screen.
- First access “Intrusion” the section and then the “Partitions” section. This section contains the list of partitions the user can control, the **SET** button opens a window containing the buttons for the arming mode settings.
 - **AWAY** arming mode arms the perimeter and internal zones and the icon becomes 
 - **STAY** arming mode arms the perimeter zones of the partition and the icon becomes 
 - **INSTANT** arming mode arms the partition in instant mode and the icon becomes 
 - **DISARM** disables the partition and the icon becomes 

The button indicating the active arming mode will be highlighted by a different colour to the other buttons.

Via Inim Cloud

The Inim cloud allows users to activate the programmed scenarios and also set up the arming mode of the partitions of the selected control panel:



- Access the “Scenarios” section by pressing . This section provides a list of the scenarios which can be activated by means of the **ACTIVATE** button. By clicking on the arrow button relating to a scenario you can view the status of all the partitions involved in the scenario. The description of the current scenario can be viewed on the home page.
- Access the “Partitions and Zones” section by pressing . This section contains a list of all the partitions available for the user and the respective buttons for a zones list and arming mode.

Voice box and intercom functions

5-3

Voice communication during keypad-to-keypad intercom calls is one-way, therefore, only one person should speak while the other listens. The user who wishes to speak must activate the intercom function on the keypad they are using.

The voice functions are:

- **Record** - starts the recording phase of the memo in the memo-box of the keypad you are working on.
- **Playback** - starts the playback phase of the message in the memo-box of the keypad you are working on.
- **Delete** - deletes the memo in the memo-box of the keypad you are working on.
- **Intercom** - allows voice communication with another voice-capable keypad.

Via Keypad

Method 1

Activate the shortcuts associated with keys , ..., (shown on the display) with or without code entry:

- The shortcut assigned to the “Voice functions menu” (shortcut n.14:) allows you to view the “Voice functions” section. Select the required function by means of keys and then press .
- **Record/Playback** - the operation time-out (expressed in seconds) will be signaled by a counter and a progress bar on the display. If you wish to interrupt the record/playback operation manually, press , otherwise, it will end automatically when the pre-set time-out expires. You can adjust the volume during the playback phase using keys and .
- **Delete** - this operation must be confirmed by pressing .
- **IntercomCall** - the display provides the list of keypads you can call. Use and to select the keypad you wish to contact, then press to start the call. The recipient keypad will emit an audible signal to indicate the incoming call and the display will appear as shown in the figure. The recipient can press to answer the call or to reject it. Both the caller and the call recipient can end the call by pressing . The volume can be adjusted during the listen phase by pressing keys and .
- The “IntercomCall” shortcut (shortcut n.11:) allows you to view the previously described “Intercom call” section.

Method 2

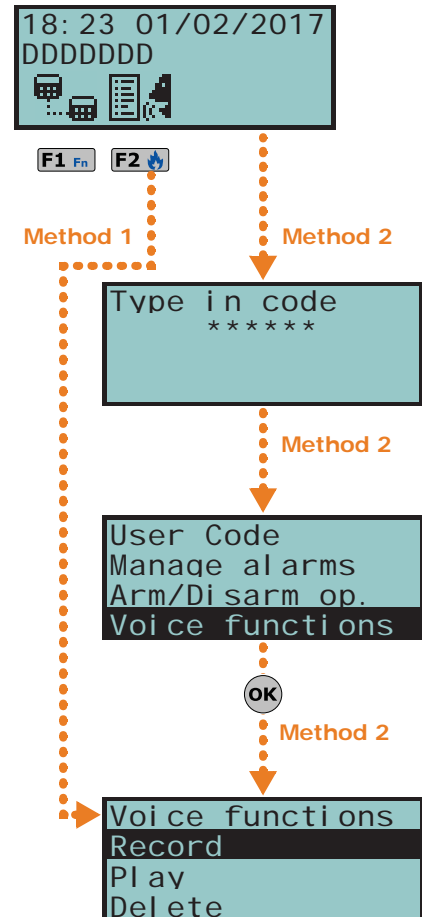
Access the “Voice functions” section of the user menu by entering a valid PIN code. Follow the instructions described in **Method 1**.

Via Alien touch screen

When accessing the voice functions via the Alien touch screen, first access the “Apps” section by tapping the button then access the “Voice functions” section. Following is a list of the sections relating to each function which can be activated by tapping the respective **ON** button:

- **Record**
- **Play**
- **Delete**
- **Intercom**

The sections accessed through the touch screen reproduce the same voice functions as those previously described for keypads with keys.



Activations

5-4

The activation/deactivation of the SmartLiving system peripherals and elements (described in the following section) enables them to operate in accordance with their settings (activation) or disables their functions completely (deactivation). The user has full control over activation/deactivation of the SmartLiving system peripherals and elements.

The following section describes the consequences of activation/deactivation.

- **Zone** - disabled zones cannot generate alarms (bypassed).
- **Auto-arm operations** - can be activated/deactivated separately on each single partition. If this option is enabled on a partition, it will arm and disarm in accordance with the On/Off settings of the respective timer.
- **Codes** - deactivated (disabled) codes cannot access the system. Activation/Deactivation can be achieved only on hierarchically inferior codes (refer to *paragraph 2-5 User Codes*).
- **Keys** - deactivated (disabled) keys cannot access the system.
- **Keypads** - deactivated (disabled) keypads do not permit code entry (or access to the menu), therefore, they cannot manage shortcuts. However, the LEDs and display will be refreshed.
- **Readers** - deactivated (disabled) readers cannot provide access to the system, therefore, cannot accept keys or generate commands. However, the LEDs will indicate the current status of the system.
- **Timers** - activated timers (On) manage their associated elements (partitions, codes, keys) in accordance with their settings. Deactivated timers cannot time-manage their associated elements, therefore, they will function in accordance with Timer Off status.

All the timers will be activated automatically when you exit the programming session. You must deactivate timers which are not used for system control purposes.

Note

- **Dialler** - a deactivated (disabled) dialler cannot send voice or digital calls. However, if duly programmed, it will be able to manage incoming calls.
- **Answerphone function** - if activated (enabled), the control panel will answer incoming calls with the prerecorded voice message ("Answerphone message").
- **InternetTeleser.** - if activated when the Answerphone option is enabled, the control panel will answer incoming calls with the prerecorded voice message.
- **Teleservice** - if activated (enabled), the installer will be able to access the system via modem. The teleservice call allows the installer to work on the control panel parameters. Teleservice operations involve a request from you and the installers acceptance, therefore, this option needs to be enabled only when required.

Note






If the "Answerphone" and "Teleservice" functions are both enabled, the control panel will give incoming-call priority to the teleservice call. After picking up the call, the control panel will allow the installer-company modem 30 seconds to establish communication. If the modem fails to communicate within this period, the control panel will play the pre-recorded "Answerphone" voice message.

- **Internet access** - If this option is enabled, and the system is equipped with a SmartLAN/G board, the control panel will allow user-authorized access to the system via LAN/Internet. If this option is disabled, the control panel will allow user-authorized access to the system via teleservice (if authorized).
- **Enable install.** - If enabled, the Installer PIN will be accepted by the system and the installer will have access to the Installer menu. If disabled, entry of the installer PIN will generate an "Invalid Code" event and the installer will be denied access to the respective menu.
- **Sync IP2RX** - if activated, the control panel will send a specific string to the IP2RX software in order to allow its identification.
- **Cloud registration**- this section allows the SmartLiving panel to access INIM Electronics cloud service (*paragraph 5-27 Use of the Inim Cloud*).

Via Keypad

Method 1

Activate the shortcuts associated with keys **F1 Fn**, ..., **F4 BOL** (shown on the display) with or without code entry:

- The shortcut assigned to the "Activations menu" (shortcut n.15: ) allows you to view the respective section in the user menu, where you can:
 1. Use keys  and  followed by **OK** to select the category of elements you wish to activate/deactivate (zones, codes, etc.).
 2. Use keys  and  followed by **OK** to select the single element you wish to activate/deactivate.

3. Use to activate the selected element or to deactivate it.

Other shortcuts which provide direct access to sub-sections of the "Activations" section are:

- Shortcut n.19 () accesses "Activations/Zones"
- Shortcut n.22 () accesses "Activations/Answerphone"
- Shortcut n.23 () accesses "Activations/Teleservice"
- Shortcut n.24 () accesses "Activations/Codes"
- Shortcut n.25 () accesses "Activations/Keys"
- Shortcut n.26 () accesses "Activations/Timers"
- Shortcut n.27 () accesses "Activations/Auto-arm"

Method 2

Access the "Activations" section of the user menu by means of a valid code PIN. Follow the instructions described in **Method 1**.

Via Alien touch screen

Access the "Menu" section by tapping , type-in the user code and then access the "Activations" section.

Here are listed the sections relating to the elements you can activate by tapping the **ACTIVATE** button.

Each section presents its own elements arranged in list form. Each element is associated with two buttons - **ON** for activation and **OFF** for inhibition, and an icon which changes in accordance with the status:

- - activated/enabled
- - deactivated/disabled

Via Web and AlienMobile

First access the "Intrusion" section, then the "Zones" section.

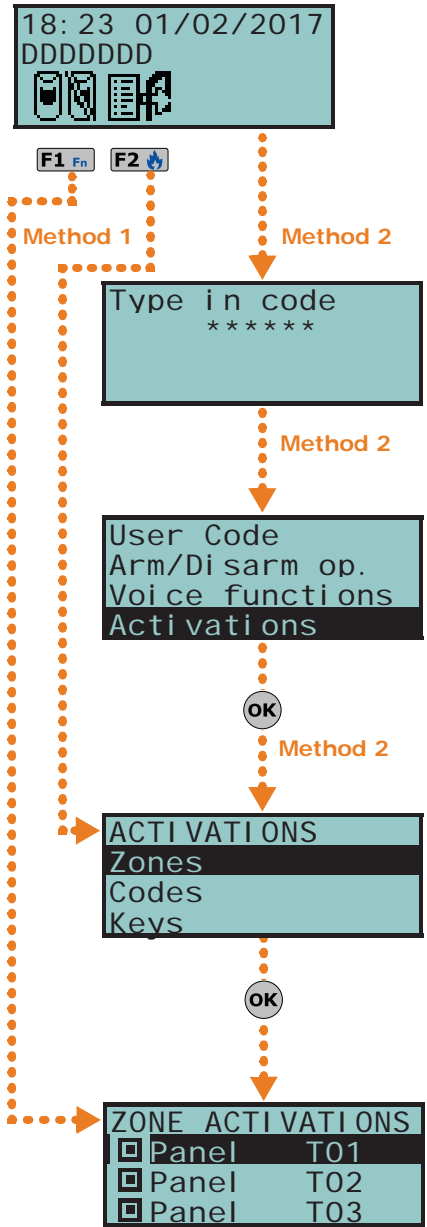
"Zones" section contains a list of the zones available to the user, and each zone provides the following keys:

- **ON** - enables the zone and the corresponding icon becomes
- **OFF** - inhibits the zone and the corresponding icon becomes

Via Inim Cloud

Using the button access the "Partitions and Zones" section. This section contains a list of the partitions of the selected control panel.

By clicking on the relative arrow key, it is possible to list the zones for each partition and change the enabled status of each of them.



View 5-5

This section allows you to view the events log and the current status of some of the system peripherals and elements.

The "Events log", "Alarms log", "Faults log" and "Arm/Disarm op." allow you to view the start and end of the corresponding events in chronological order.

The "Nexus status" section shows (on the display) some of the parameters of the Nexus dialler.

The "System voltage" section allows you to view the respective voltage panel.

The "Zone Status" section shows the status of the zone (**Standby, Alarm, Shorted, Tamper**) and its inhibited status (**Unbypassed** - capable of generating alarms, or **Bypassed** - incapable of generating alarms).

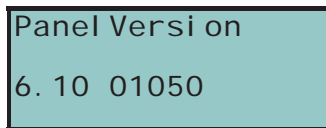
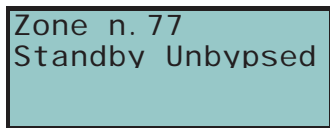
The "Faults" section allows you to view current faults only (refer to *Appendix C, Fault signals*).

The "Panel version" section allows you to view the firmware version and model of your SmartLiving control panel.

When viewing the wireless zones, the last line on the display indicates the level of signal strength on a scale of 0 to 7; the higher the value the better the signal.

If you access the control panel via browser, it will be possible to view the status of:

- Partitions
- menu
- outputs
- timer
- events log



Via Keypad

Method 1

Activate the shortcuts associated with keys **F1 Fn**, ..., **F4** (shown on the display) with or without code entry:

- Shortcut n.28 (🔑📄) accesses "View/Events log"
- Shortcut n.29 (🔑🚨) accesses "View/Alarms log"
- Shortcut n.30 (🔑⚠️) accesses "View/Faults log"
- Shortcut n.31 (🔑🔒) accesses "View/Arm/Disarm op."

User access to the information in the "Logs" is filtered. For example, a user can view only the zone alarms relating to the partitions the code and keypad concerned have in common.

Use key 📶 or 📶 to scroll the chronological events list.

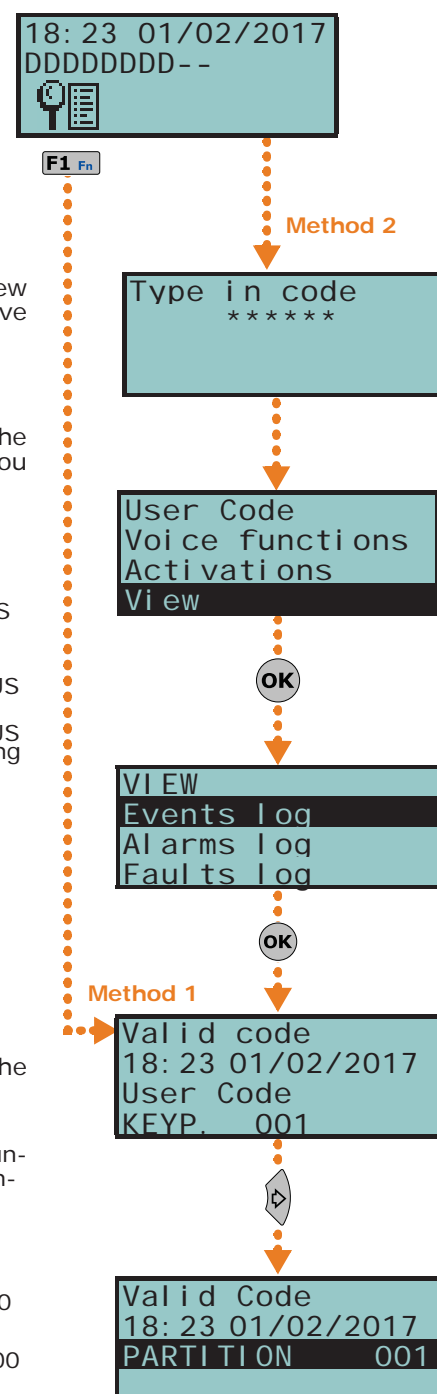
For some events, key 📶 allows you to view the partitions details. For example, the details of an "Arm" command will show the code and keypad concerned and, if you press 📶, the list of partitions involved.

- Shortcut n.16 (🔑📶) accesses "View/NexusStatus":
 - 1° line: GSM network provider (Wind, Tim, Vodafone, etc.), on the left side and BUS connections on the right side of the string:
 - if nothing appears, it means that the Nexus/G is connected to the BUS
 - if the letter "G" appears, it means that the Nexus/G is connected to the BUS and that the GPRS service is available
 - if the letter "C" appears, it means that the Nexus/G is connected to the BUS and that a teleservice request (TCP connection) or SIA-IP event report is being sent
 - if "--" appears, it means that the Nexus is connected to the BUS
 - 2° line: GSM signal reception (value between 1 and 100)
 - 3° line: balance, at the last operation (expressed in the local currency)
 - 4° line: faults present - access the "View-Faults" section for details.

- Shortcut n.32 (🔑🔋) accesses "View/System voltage"
- Shortcut n.33 (🔑🏠) accesses "View/Zone status"

Use keys 📶 and 📶 to scroll the list of accessible zones. The display shows the following zone parameters:

- 1° line: zone description
- 2° line: zone status ("Standby", "Alarm", "Short", "Tamper"), its activation status ("unbypassed" - capable of generating alarms, or "bypassed" - incapable of generating alarms)
- 3° line: various indications depending on the device type:
 - wireless zone; wireless signal reception level
 - level of smoke present in the smoke detection chamber of the Air2-FD100 smoke detector, expressed in mdB/m
- 4° line: level of contamination present in the smoke detection chamber of Air2-FD100 smoke detector (%)



It is advisable to clean the detector when the value exceeds 90%.

Note





- Shortcut n.36 () accesses "View/Faults"

Method 2




Access the "View" section of the User menu by means of a valid PIN. Follow the instructions described in **Method 1**.

Via Alien touch screen

It is possible to view the status of the system elements through the various section the user has access to:

- Access the "Intrusion" section by tapping the  button, enter the user code. The following sections will be available:
 - "Zones" - the zones are listed in this section along with their status icons (positioned to the left of each zone description):
 -  - green spot - standby status
 -  - red spot - alarm status
 -  - yellow triangle - fault/tamper

Each zone is associated with two buttons, **ON** for activation and **OFF** for inhibition, and an icon which changes in accordance with the status:

 -  - activated/enabled
 -  - deactivated/disabled
 - "Events Log" - all the events saved to the log are displayed one at a time. However, the up/down keys will allow you to scroll the entire list of events. Each event shows the relative details and, where possible, allows you to view the partitions involved by means of the **PARTITIONS** button.
- Access the "System" section by tapping the  button, enter the user code. The following sections will be available:
 - "Faults" - this section allows you to view all the faults present on the system and, where possible, the fault details by means of the **DETAILS** button.
 - "Voltage" - this section allows you to view the control panel power-supply voltage.
 - "GSM info" - this section allows you to view the parameters of the Nexus GSM communicator.

Via Web and AlienMobile

Access to the system via web browser and mobile phone allows users to view other parts of the system through their respective sections:

- **Partitions**
- **Zones**
- **Commands**

Following is a table showing the meaning of the various icons positioned at the side of the description of the element displayed:

Table 5-1: Viewing via web browser and mobile device

Section		Icon		
	Partitions/ Zones		Disarmed	Armed/Disarmed status of partition/zone
			Armed in Away mode	
			Armed in Stay mode	
			Armed in instant mode	
	Zones		Disarmed	Partition/Zone alarm status
			Standby	
			Alarm	
			Tamper or fault	
			An alarm or tamper event in memory	
			Zone shorted	
	Timers		Zone active	Zone activation status
			Zone deactivated	
Timers		Activated	Timer status	
		Deactivated		

Section	Icon		
		Activated	Output status
		Deactivated	

- **Events log** - first access the "Intrusion" section then the "Events log". A window will appear which provides buttons to indicate the number of events to be viewed, starting from the last. Once accessed, this section provides a list of events with the respective details and the relative **PARTITIONS** button which, if pressed, opens a window containing a list of the partitions involved in the event.
- **System info** - the "System" section provides the following sub-sections:
 - "Faults list" - a window showing a list of the faults present on the system.
 - "Voltage" - this window allows you to view the control panel power-supply voltage.
 - "GSM info" - this window allows you to view the parameters of the Nexus GSM communicator.



Via Graphic maps

The visualization of the status and supervision of the SmartLiving system and its parts can be done through the graphic maps, function which can be accessed through the Alien keypad or web interface.

Refer to *paragraph 5-24 Graphic maps*.

Via Inim Cloud

The web interface of the cloud allows visualization of the status and the supervision of the elements of the SmartLiving system in different ways:

- The home page (accessible also by means of the button) provides, in the bottom centre section of the page (*Table 2-13: Inim cloud - home page, G*), the immediate display of the following elements of the selected control panel:
 - Current scenario (with access to all the programmed scenarios)
 - Active outputs (with access to all the "Smart Home" outputs)
 - Status of the thermostat (with access to the "Climate" section)
 - Armed partitions
 - Bypassed zones

- The buttons for access to the sections of the selected control panel (Table 2-13: *Inim cloud - home page, B*). For further information refer to paragraph 5-27 *Use of the Inim Cloud*.
- The buttons for quick viewing of the events of all the registered control panels (Table 2-13: *Inim cloud - home page, D*):

- opens a window containing a list of the last 4 fault events.
- opens a window containing a list of the last 4 events on the control panel and cloud.

These windows also provide a button that accesses the events section of the selected control panel. Where necessary, these buttons show the number of events of all the registered control panels not yet viewed.

Activation of outputs

5-6

This section allows you to activate/deactivate manually the outputs the code is enabled to work on.

You can activate/deactivate low-power open-collector or relay outputs and view their status by means of the respective icons.

You can activate/deactivate high-power relay outputs and view their supplied voltage and relative power factor (cosφ).

You can view the supplied voltage of dimmer outputs and manage their settings by means of the scroll bar.

Via Keypad

Method 1

Activate the shortcuts associated with keys **F1** , ..., **F4** (shown on the display) with or without code entry:

- The shortcut assigned to “Output control” (shortcut n.21:) , allows you to view the “Outputs ON/OFF” section of the user menu where you can:
 1. Use keys and to select the output you wish to activate/deactivate.
 2. Press to activate the selected output or to deactivate it. If the output is a dimmer output, you can increase or decrease its power supply by means of keys and .
- The shortcut assigned to the “Activate outputs” operation (shortcut n.5:) will activate the output when the respective button is pressed.
- The shortcut assigned to the “Deactiv. outputs” (shortcut n.6:) will deactivate the output when the respective button is pressed.

Method 2

Access the “Outputs ON/OFF” section of the user menu by typing-in a valid PIN.

Follow the instructions described in **Method 1**.

Via Alien touch screen

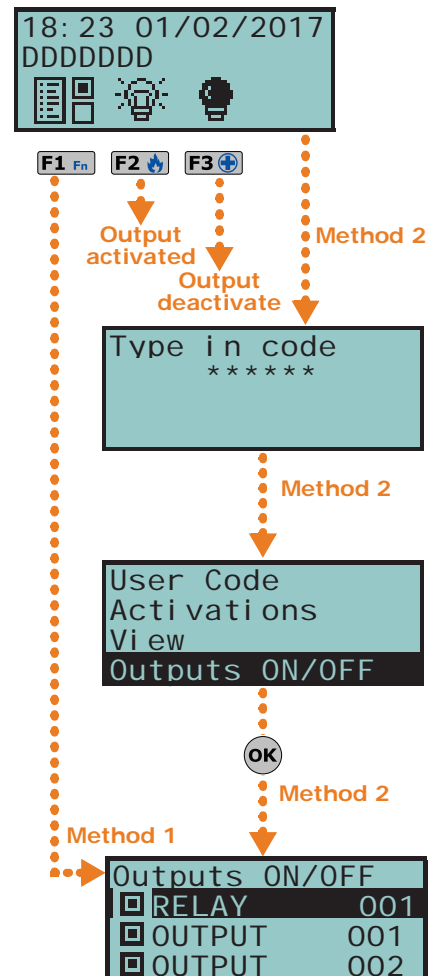
Access the “Commands” section by tapping the button, then select the required sub-section:

- “Home automation” - accesses the outputs of the home automation system without the need of code entry.
- “Intrusion” - accesses the outputs of the intrusion control system after typing-in a valid user code.

The available outputs are listed in both sections.

The activatable outputs are associated with two buttons, **ON** for activation and **OFF** for deactivation, and an icon which changes accordingly:

- - output activated
- - output deactivated



High-power relay outputs and dimmer outputs have a scroll bar for the visualization of their supplied power/current, together with the numerical value and power factor (cosφ). These values can be adjusted using the "+" and "-" keys.

Via Reader

Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Activate outputs" (shortcut n.5) or "Deactiv. outputs" (shortcut n.6).

Over-the-phone

Type-in the PIN of a user code followed by "#" then press the key (from "0" to "9") which the installer has programmed to trigger "Activate outputs" (shortcut n.5) or "Deactiv. outputs" (shortcut n.6).

Via Wireless remote-control device

Push the respective button on the remote-control device and verify the outcome of the requested operation, as described in *paragraph 2-6-1 Air2-KF100 Wireless keyfobs*.

Via Web and AlienMobile

Access the "Commands" section.

This section provides a list of the control panel outputs and two buttons:



- **ON** to activate the output, when activated the corresponding icon becomes
- **OFF** to deactivate the output, when deactivated the corresponding icon becomes
- a scroll bar for adjustments to the power/current supplied to the high-power relay outputs and dimmer outputs (viewable through the web interface only).

Via Inim Cloud



Using the button, access the "Smart Home" section

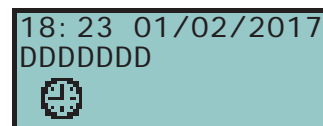
This section contains a list of the outputs of the selected control panel. A button is available for the activation/deactivation of each output (On/Off).

In the case of a dimmer output, a scroll bar is available for the adjustment of the supplied power/voltage.

Change date and time 5-7

This option allows you to set the date and time in accordance with the selected format.

Via Keypad



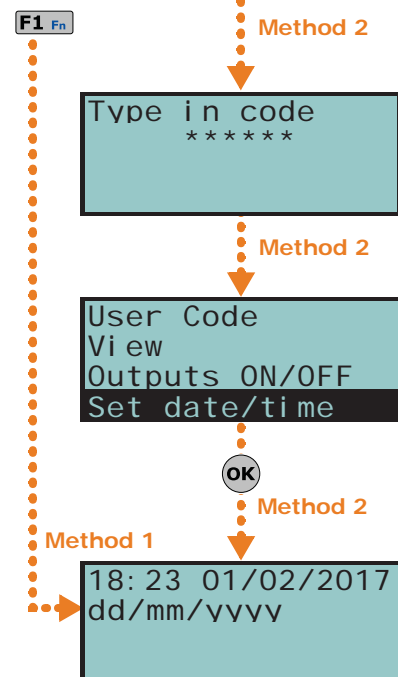
Method 1

Activate the "Date/Time" shortcut (shortcut n.35), associated with one of the keys **F1**, ..., **F4** shown on the display, with or without code entry, to access the user menu at the "Set date/time" section.

1. Use keys and to select the programming field you wish to change (hour, minutes, etc.).
2. Use keys and to change the selected field.
3. Press **OK** to save the setting.

Method 2

Access the "Keypad date/time" section on the User menu by means of a valid PIN. Follow the instructions described in **Method 1**.



Via Alien touch screen

Access the "Settings" by tapping the button, type-in a valid user code, then access the "Date/Time - Change PIN - Tel. Numbers" section.

This section allows you to access and change the date and time of the control panel clock. Changes can be made using the left/right and up/down scroll keys and confirmed by the **OK** key.

Keypad settings

5-8

This option allows you to configure the displays and buzzers of the keypads which access to the SmartLiving system.

The parameters which are available depend on the type of keypad.

- **Brightness** - for the adjustment of the brightness of the display backlight and key LEDs when any key is pressed (duration 20 seconds).
- **Standby brightness** - for the adjustment of the brightness of the display backlight and key LEDs when the keypad is in standby status.
- **Contrast** - for the adjustment of the black/white contrast.
- **Volume** - for the adjustment of the buzzer volume.
- **Keypad options:**
 - **Temperature off** - if enabled, the temperature value read by the built-in temperature sensor will not be shown (only on temperature-sensor equipped keypads).
 - **NoExitTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Exit time.
 - **NOEntryTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Entry time.
 - **Beep on output** - if enabled, the buzzer will emit audible signals during partition Exit time.
 - **Disable chime** - if enabled, the buzzer will not emit audible signals when a bell zone is violated.
 - **LED OFF in standby** - If enabled, in the event of inactivity on the keypad for at least 40 seconds, the respective LEDs will go off.

These settings apply only to the keypad you are working on, and will be saved even in the event of panel shutdown.

Via Keypad

Method 1

Activate the shortcut assigned to "Keypad settings" (shortcut n.18:), associated with one of the following keys **F1 Fn**, ..., **F4 Fn** shown on the display, with or without code entry, to access the "Keypad settings" section of the user menu.

1. Use and , followed by **OK** to select the parameters to be programmed.
2. Use keys and to increase or decrease the value of the selected parameter. To activate the selected option press , to deactivate it press .
3. Press **OK** to save.

Method 2

Access the "Keypad settings" section of the user menu by typing-in a valid code PIN. Follow the instructions described in **Method 1**.

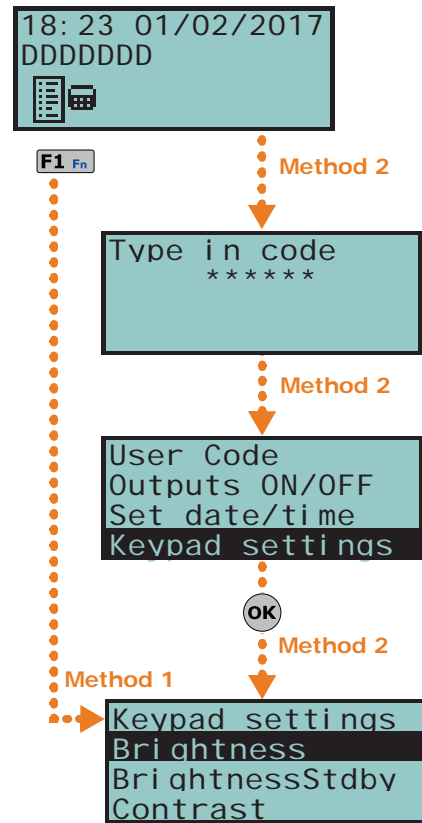
Via Alien touch screen

Access the "Settings" section by tapping the button , type-in a valid user code and then access the "Alien" section.

This section will allow you to view the firmware version of the keypad in use on the connected control panel and change the parameter settings of the keypad you are working on.

The settings will be saved even in the event of control-panel shutdown.

- **Transparency** - for the adjustment of the transparency effect
- **Brightness** - for the adjustment of screen brightness when touched (duration 45 seconds)
- **Standby brightness** - for the adjustment of screen brightness when the keypad is in standby status
- **Volume buzzer** - for buzzer loudness adjustment
- **Volume voice** - for the adjustment of the speaker loudness
- **Skin** - for the selection of one of the skins for the Alien touch screen
- **Delay photof.** - waiting time before the automatic startup of the photoframe application during standby status
- **Photo int.** - interval between the display of photos used by the photoframe application



- **Language** - for the selection of the language used by the Alien touch screen interface
- **Temperature adjustment** - for the adjustment of the temperature shown on the display
- **View partitions** - for the visualization of the operating status of the partitions on the bottom bar of the display
- **Exit time** - enables/disables the audible signal during exit time
- **Entry time** - enables/disables the audible signal during entry time
- **Bell** - enables/disables the audible signal for the bell function
- **Temperature** - enables/disables the visualization of the temperature on the display
- **Tamper** - enables/disables the device tamper function (Alien/G only)
- **Maps** - enables/disables the automatic start up of the graphic maps application when the keypad is in stand-by
- **Show scenario with code** - enables/disables the request for user-code entry when the user taps the lower bar on the home page to view the active scenarios.
- **Emergency lights** - if enabled, the keypad brightness will increase to the maximum value during mains power-cut events and will remain so until the mains power restores to normal

If the SmartLiving control panel is in maintenance status, a list of the following parameters will be shown:

- **Keypad address**
- **Keypad address** - this is the address of the Alien keypad and its integrated reader
- **Tamper** - enables/disables the device tamper protection (for Alien/G this option is shown also when the control panel is not in maintenance status); if tamper is disabled, the upper tool bar on the home page will show the icon:



You can select the parameter by means of "+" and "-". To confirm changes and exit the section tap **SAVE**.

English is the default language of the Alien keypad.

Note

Change PIN 5-9

This section allows you to change the User Code PIN you used for access and also the PINs of other users with a lower rank in the system hierarchy (refer to *paragraph 2-5 User Codes*).

In order to be EN50131 compliant, all PINs must have 6 figures.

Via Keypad

Method 1

Activate the shortcut assigned to the "Change PIN" (shortcut n.34: *****3**) and associated with one of the following keys **F1 Fn**, ..., **F4 Fd** shown on the screen, with or without code entry, to access the "Change PIN" section of the User Menu, where it is possible to:

1. Use keys and followed by to select the user code you wish to change.
2. Type-in the new PIN (4, 5 or 6 digits) using keys **0**, ..., **9 wxyz** then press .
3. Type-in the new PIN again using keys **0**, ..., **9 wxyz** and press to save.

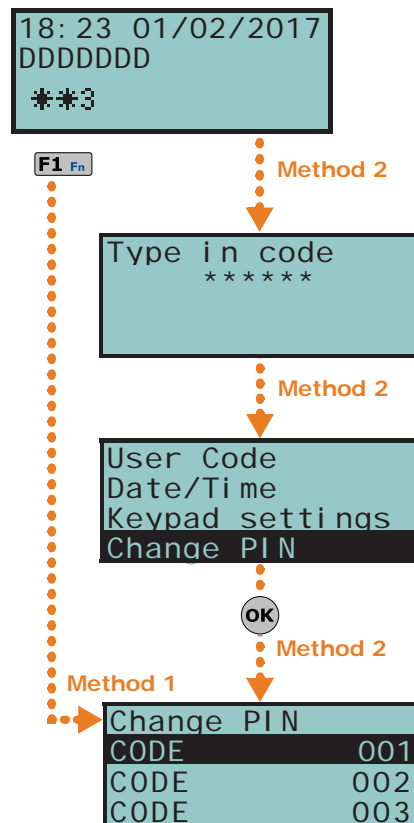
Method 2

Access the "Change PIN" section of the user menu by typing-in a valid code PIN. Follow the instructions described in **Method 1**.

Via Alien touch screen

Access the "Settings" section by tapping , enter a valid user code, then go to "Date/Time - Change PIN - Tel. Numbers" section, select "Change PIN".

Select the code you desire from those available on the list. The next step is to change the code using the screen buttons, tap **OK** to confirm.



Change telephone numbers

Users can change the contact numbers used by the dialler of the SmartLiving control panel.

Only contact numbers with at least one partition in common with the entered PIN and keypad in use will be shown.

Via Keypad

Access the phonebook:

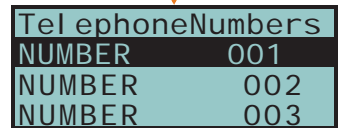
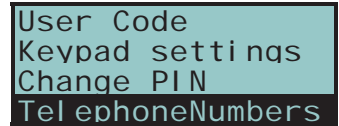
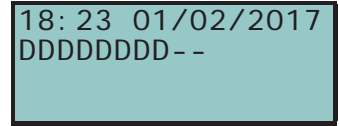
1. Use keys and to select the required phone number then press ; each programming field accepts a 20 digit phone number.
2. Use keys and to select the field you wish to change, then use the number keys (1..9, etc.) to edit the number. The following characters are also accepted: ", " (= 2 second pause), "*" and "#".
3. Press to confirm and exit.

Via Alien touch screen

Access the "Settings" section by tapping , enter a valid user code, then go to "Date/Time - Change PIN - Tel. Numbers", then to the "Tel. Numbers" section.

Select the telephone number you desire from those available on the list. The next step is to change the number using the screen buttons, tap **OK** to confirm.

5-10



Teleservice request

This command sends a call to the installer company.

Your installer must enable control panel option "Num15ForTeleserv", otherwise this function will not be available.

Via Keypad

Method 1

Activate the shortcut assigned to the "Teleservice req." (shortcut n.8:)

Method 2

Access the "Teleservice request" section of the user menu by typing-in a valid code PIN.

Via Alien touch screen

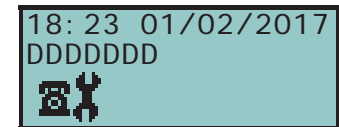
Access the "Menu" section by tapping , type-in the user code and then access the "Actions" section.

This section contains a list of control panel commands which can be activated by tapping **ACTIVATE**, among them is the "Teleservice".

Via Reader

Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Teleservice Request" (shortcut n.8).

5-11

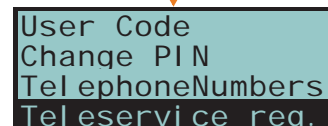


F1 Fn

Method 2



Method 2



Method 1

Service call activated

Overtime request

5-12

This operation can be carried out under the following conditions only.

- The partition concerned must be timer-controlled.
- The auto-arm option must be enabled (refer *paragraph 5-4 Activations*).

Each overtime request postpones the auto-arming operation by 30 minutes.

Via Keypad

Method 1

Activate the shortcut assigned to the "Overtime" (shortcut n.7:).

Method 2

Access the "Overtime req." section of the user menu by typing in a valid code PIN.

Via Alien touch screen

Access the "Menu" section by tapping , type-in the user code and then access the "Actions" section.

This section contains a list of control panel commands which can be activated by tapping **ON**, amongst which "Overtime request".

Via Reader

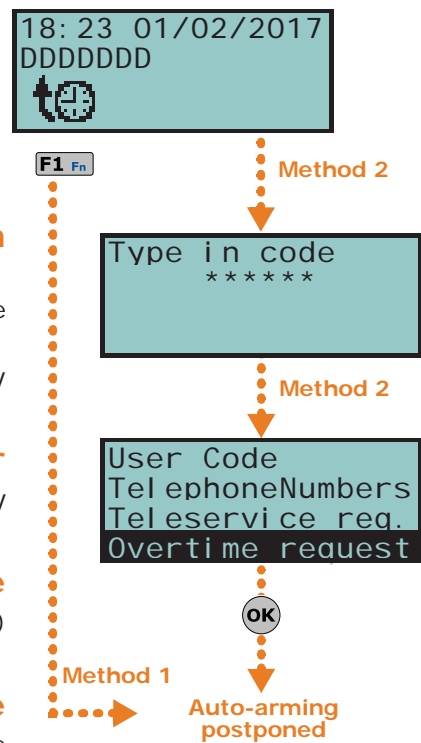
Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Overtime" (shortcut n.7).

Over-the-phone

Type-in the PIN of a user code followed by "#", then press the key (from "0" to "9") which the installer has programmed to activate "Overtime" (shortcut n.7).

Via Wireless remote-control device

Push the respective button on the remote-control device and verify the outcome of the requested operation, as described in *paragraph 2-6-1 Air2-KF100 Wireless keyfobs*.



Thermostat

5-13

The "Thermostat" function, provided by keypads with temperature sensor, manages the heating or air-conditioning system in accordance with its setting.

- - **Summer/Cooling**: when the sensor detects that the temperature has risen above the value set by the user, the output connected to the air-conditioning system will activate (indicated on the display by).
- - **Winter/Heating**: when the sensor detects that the temperature has fallen below the value set by the user, the output connected to the heating system will activate (indicated on the display by .

This function provides 5 operating modes for the user to choose from:

- **Off** - the thermostat is off; the output associated with the heating or air-conditioning system is deactivated.
- **Manual** - the temperature set by the user is valid for 24 hours per day, for 7 days per week.
- **Daily** - the temperature set by the user is valid during the selected hours for 7 days per week.
- **Weekly** - the temperature set by the user is valid during the selected hours on specific days of the week.
- **Antifreeze** - this is a forced operation. If the temperature drops below 5°C, the output connected to the heating system will activate.

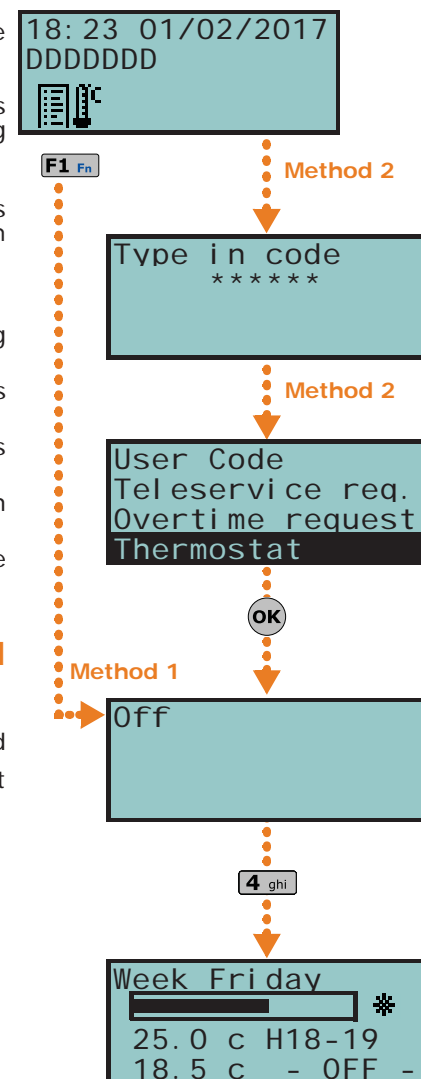
Via Keypad

Method 1

Activate the shortcut assigned to the "Thermostat" (shortcut n.37:) , associated with one of the following keys **F1 Fn**, ..., **F4 P0** (shown on the display), with or without code entry, to access the "Thermostat" section of the user menu.









1. Use the number keys to select the operating mode of the thermostat:

- **1** ., - thermostat Off
- **2** abc - "Manual"
- **3** def - "Daily"
- **4** ghi - "Weekly"
- **5** jkl - "Antifreeze"



The display will show the:

- 1° line: operating mode of the thermostat and day of the week
- 2° line: pre-set temperature bar and "Summer/Winter" operating mode icon
- 3° line: temperature setting and operating hours
- 4° line: temperature reading and the status of the heating system/air-conditioning system (ON/OFF)


2. Select the operating mode ("Summer/Winter") of the thermostat using .
3. Select the temperature, using keys  and .
4. Select the timeframe, using  and .
5. Select the day of the week, using  and .
6. Press  to confirm and exit.

Method 2

Access the "Thermostat" section of the user menu by typing-in a valid code PIN.

Follow the instructions described in **Method 1**.

Via Alien touch screen

Access the "Climate" section by tapping .

This is the section relative to the operating mode of the thermostat.

Selecting **Back** accesses a page containing the buttons of the 5 operating modes available.

Select the button which corresponds to the section you require, then set the parameters of the selected operating mode. You can change the temperature using "+" and "-", and also the timeframe and day (where available) by means of the arrow keys.

The Summer/Winter button will allow you to select the respective season.

The icons corresponding to the thermostat options are displayed of the upper tool bar on the home page.

Via AlienMobile

On accessing the "Climate" section you will find a list of all the keypads configured with the thermostat function. If there is only one keypad, you will immediately access the thermostat configuration page.

Each listed keypad will show:

- keypad description
- thermostat operating mode
- the temperature read by the keypad
- **View** button for access to the thermostat configuration described in the Alien keypad section

Via Inim Cloud

Using the  button, access the "Climate" section

The "Climate" section will allow you to select one of the keypads configured with the thermostat function. Once selected, the screen will show:

- the temperature read by the keypad
- the temperature set on the thermostat
- thermostat operating mode

Teleservice via Nexus

5-14

Requests for teleservice can be made over the GSM network by means of the "Nexus Teleserv." option.

This option allows the installer to carry out remote programming operations over the GPRS network.

This is a service provided by the installer company with the user's collaboration.

Note

Via Keypad

Access the "Nexus Teleserv." section of the user menu by typing-in a valid code PIN.

User Code
Overtime request
Thermostat
Nexus Nexus

Via Alien touch screen

Access the "Menu" section by tapping , type-in the user code and then access the "Actions" section.

This section contains a list of control panel commands which can be activated by tapping **ON**, amongst which Nexus teleserv." option.





Codes 5-15

The user menu provides a section for the programming of the parameters of hierarchically lower user codes (refer to *paragraph 2-5 User Codes*).

The parameters which can be changed in this section are also available in other sub-sections.

Via Keypad

Access the "Codes" section of the user menu by typing-in a valid code PIN.

1. Use keys  and  followed by **OK** to select the user code you wish to change.
2. Use keys  and  followed by **OK** to select the parameter you wish to change.
3. Change the parameter then press **OK** to save the changes.











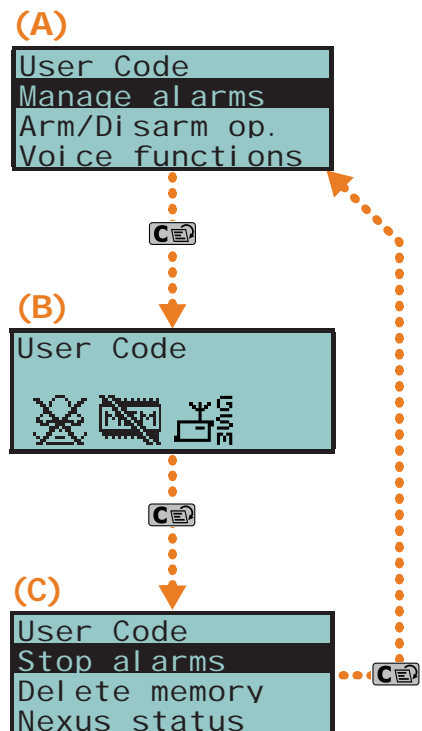
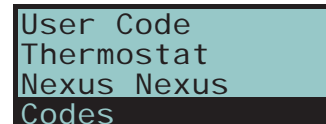
- **Description**: edit field for the code description.
- **Partitions** - select the partitions the user code is assigned to. Press , to enable the partition and  to disable it.
- **Options** - use  and  to enable/disable the code options.
 - **Partition filter** - if this option is enabled, the code will be able to change the parameters only of codes with a lower rank in the system hierarchy whose partitions are amongst the partitions assigned to the code being programmed. For example, if a code is configured as "Master" with "Partition filter" and is assigned to partitions 1, 3, 5 and 7, it will be able to enable/disable or change the PIN of a "User" code assigned to partitions 1 and 5 but not the PIN of a "User" code assigned to partitions 1, 2, and 3.
 - **Text menu** and **User menu** - the combination of these two options allows immediate visualization of the menu screens on the keypad displays after acceptance of a valid user PIN. Refer to the following table.

Table 5-2: Combinations "text menu" and "user menu"

Case	Text menu	User menu	Description
A	Disabled	Enabled	Accesses the user-menu (shown as a list of operations the user is enabled to perform); at this point the user can scroll the list using  and  and select the required option.
B	Disabled	Disabled	Visualization of the user-icons associated with function keys F1  , ..., F4  ; at this point the user can press the required function key and activate the associated shortcut.
C	Enabled	Disabled	Shows the descriptions of the personalized user-icons associated with function keys. The descriptions of the shortcuts are shown in place of their associated icons. The user can use  and  to scroll the list of shortcut descriptions and select the desired shortcut, which can be activated by means of the OK key.
D	Enabled	Enabled	The same as "C"



In all methods of access (A, B and C), the  key allows you to access/view the other cases in succession, see figure.

Note





- **AnnounceShortcut** - if enabled on a voice capable keypad, the descriptions of all the shortcuts assigned to the code and associated with the number keys will be announced after acceptance of the entered PIN.
- **Remote access** - if enabled, the code PIN can be used to operate the system from any remote telephone. If the code PIN is entered on a remote telephone keypad, only the shortcuts associated with keys 0 to 9 can be used to:
 - Arm/Disarm
 - Stop alarms
 - Clear call queue
 - Delete memory
 - Activate Output

- Deactiv. Output
- Listen-in
- Arming status





Any other type of command will have no effect.

- **Patrol** - if enabled, the code will be able to disable the system for the pre-set "Patrol time".
- **Fixed length** - if enabled, after typing in a PIN and without pressing the **OK** key, the user will be able to activate the shortcut associated with function key "F12", programmed via the "F1/4KeyShortcuts", described later.
If this shortcut is number 1 ("Arm/disarm") and all the partitions assigned to the user code in question are disarmed, the command will arm them, otherwise it will disarm them.
A user code with this option enabled has access to its own menu only after pressing the **OK** key followed by PIN entry.
- **F1/4KeyShortcuts** - this section allows you to configure up to 12 shortcuts associated with keys **F1 Fn**, ..., **F4 P00**. After valid PIN entry the keypad will show the icons that correspond to keys **F1 Fn**, ..., **F4 P00** and which are associated with these shortcuts. The respective shortcut will activate when the corresponding key is pressed.
- **0/9 Key shortcuts** - this section allows you to configure up to 10 shortcuts associated with keys **0**, ..., **9 wxyz**. After PIN acceptance, the code user can activate the shortcut by pressing the respective number key.

To assign the shortcuts to the function keys, work through the following steps.

1. Use keys  and  to select the key you wish to associate with the shortcut then press **OK**.
 2. Press **OK** then, using keys  and , select the shortcut you wish to associate with the function key from the "Type" list.
 3. Press **OK** to confirm and exit.
 4. If the shortcut is associated with "Arm/Disarm" operations, the application will ask you to select a scenario. If the associated shortcut is "Activate output" or "Deactiv. output", the application will ask you to select the output.
- **ActivatableOutputs** - this section allows the user to enable/disable the outputs the code is allowed to control manually:

User menu, Outputs ON/OFF **OK**.

1. Use keys  and  to select the desired output.
 2. Use keys  and  to enable/disable manual control of the output for the code concerned.
 3. Press **OK** to confirm and exit.
- **Timers** - this section allows you to assign a timer to the code. The code will be operative only at the pre-set times.
 - **Type** - this section allows you to assign a level (rank) in the system hierarchy to the selected code.
 - **Enablements** - this section allows you to enable/disable access to the various sections of the user menu.
The programming steps are identical to those of "Outputs ON/OFF".

Timer programming

5-16

This section allows the programming of all the timers the user has access to.

You can program two "ON" times and two "OFF" times for each day of the week.

A timer can be associated with:

- a **Partition** - if the timer is enabled and the partition is enabled for automatic-arming operations (refer to *paragraph 5-4 Activations*), the partition will arm when the timer switches ON and disarm when the timer switches OFF.
- a **Code** - if the timer is enabled, the code will be authorized to operate on the system only when the timer is active (ON).
- a **Key** - if the timer is enabled, the key will be authorized to operate on the system only when the timer is active (ON).

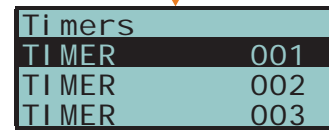
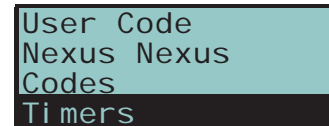
If you wish to associate a timer with a partition or a code, you must access the respective section in the user menu. The association of timers with keys must be done by the installer during the programming phase.

Via Keypad

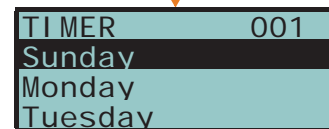
Access the "Timers" section of the user menu by typing-in a valid code PIN.

1. Use keys and to select the Timer then press .
2. Using the same keys, select the day of the week.
3. Select an activation or a restoral of the timer.
4. Set the selected time (expressed in hours and minutes) by means of keys and then, using keys and select the number.
5. Press to confirm and exit.

It is possible to programme only timer activation or timer reset.
Enter "--:--" in the field you do not wish to program.



Note



Listen-in

5-17

This function can be activated over-the-phone only.

Users communicating with the control panel over-the-phone can activate the Listen-in function and eavesdrop on the protected premises. This is made possible by the microphones on voice-capable keypads which have at least one partition in common with the entered telephone code.



Shortcut n.10 must be assigned (by your installer) to one of the number keys relating to the code that generates this operation.

Over-the-phone

Type-in the PIN of a user code followed by "#", then press the key (from "0" to "9") which the installer has programmed to activate "Listen-in" (shortcut n.10). The control panel will open a listen-in channel between the users telephone and the first voice-capable keypad with at least one partition on common with the entered code. During the listen-in phase, the user can open a voice-communication channel with another keypad by pressing the number key which corresponds to the address of the selected keypad. Also in this case, the selected keypad must have at least one partition in common with the entered code.

Press "*", to end the listen-in phase and step back to the voice-announced Shortcut menu.

Partition status enquiry

5-18

This function can be activated over-the-phone only.

The Partition status enquiry function allows users to listen to voice announcements regarding of the armed/disarmed status of the partitions during telephone communications with the control panel, or by activating the corresponding shortcut from a voice-capable keypad. The control panel will announce the armed/disarmed status of the partitions the entered PIN is assigned to.

If you activate this shortcut from a keypad, the control panel will announce the armed/disarmed status of the partitions the entered PIN is assigned to, regardless of the partitions assigned to the keypad.

Note

The user code must be enabled (by the installer) to activate shortcut n.17 via keys , ..., or the number keys relative to the code.



Over-the-phone

Type-in the PIN of a user code followed by "#" then press the key (from "0" to "9") which the installer has programmed to activate "Arming status" (shortcut n.17). The control panel will announce (in order) the descriptions of the partitions the entered PIN is assigned to and their current armed/disarmed status.

Press "*", to step back to the main menu to listen to all the voice announcements relating to the shortcuts assigned to the entered PIN.

Via Keypad

After entering a valid user-code PIN, press the key which is assigned to the "Arming status" shortcut (shortcut n.17). The control panel will announce (in order) the descriptions of the partitions the entered PIN is assigned to and their current armed/disarmed status.

Commands over-the-phone 5-19

Panel to user calls 5-19-1

Your installer will instruct you as to which events generate voice calls. Event report calls will be sent to the programmed contact numbers of your choice when the event occurs and, in most cases, also when it ends.

During the call, the call recipient can:

- press "*" to go to the next message or, if there is only one message, end the successful call.
- Type-in a valid PIN followed by "#" and access the customized shortcuts assigned to the code. The control panel will activate the voice guide which will announce the available shortcuts and the number keys to press. The respective shortcut will activate when the key indicated by the voice guide is pressed.

User to panel calls 5-19-2

If the "Answerphone" function (refer to *paragraph 5-4 Activations*) is enabled, users can call the control panel from any remote telephone and send commands to the system (refer to *paragraph 3-2 Shortcut with code*) and/or activate Listen-in sessions (refer to *paragraph 5-17 Listen-in*) in the following way.

1. Dial the control panel telephone number.
2. Allow the phone to ring for the pre-established number of rings. The control panel will answer and will play message n.216.
3. Type in your PIN followed by "#".
4. The control panel will activate the voice function which will announce the available shortcuts and the number keys to press.
5. As soon as the selected number is pressed on the telephone keypad, the control panel will activate the corresponding shortcut.

If the system is equipped with a Nexus dialler, the user can operate on the control panel via voice call to the SIM card of the Nexus. If duly configured (by the installer), the user will receive feedback (SMS text message or ring) from the Nexus relating to successfully implemented commands.

SMS text message to the user 5-19-3

If the system is equipped with a duly programmed Nexus dialler, the user may receive SMS text messages signalling that events have occurred.

If an event (which has been duly configured by the installer) occurs or restores, the control panel will send notification to the programmed users via SMS.

SMS text message to the control panel 5-19-4

If the system is equipped with a duly programmed Nexus dialler, the user can operate on the control panel by sending SMS text commands to SIM card of the Nexus.

Users who wish to activate a command via SMS text must enter the command details as follows:

<xxxxxx> <SMS Text>

where:

- <xxxxxx> stands for the PIN of a control panel user
- a blank space must be keyed in after PIN entry
- <SMS Text> which is the command identifier - this parameter must be provided by your installer.

If duly configured (by the installer), the user will receive feedback (SMS text message or ring) from the Nexus relating to successfully implemented commands.

The SmartLiving control panel is programmed with five predefined default commands:

SMS TEXT AT DEFAULT

- Balance enquiry relating to the SIM card of the Nexus

If the following SMS text message is sent:

<xxxxxx> CREDIT BALANCE

where <xxxxxx> stands for the user's PIN - the user will receive an SMS text message indicating the remaining credit (balance).

- Status enquiry relating to the Nexus

If the following SMS text message is sent:

<xxxxxx> STATUS

where <xxxxxx> stands for the user-access PIN - the user will receive an SMS text message indicating the:

- device name and firmware revision
- GSM network provider
- GSM signal reception level
- device tamper status
- BUS status
- Balance (remaining credit)

- Inhibition (using the "EXC" or "ESC" command) or activation (using the "INC" command) of the control panel zones

If the following SMS text message is sent:

<xxxxxx> EXC <zone description>

where:

- <xxxxxx> is the PIN of a control-panel user coded, followed by a blank space
- "EXC" (or "ESC" or "INC") is the command to be implemented on the zone, followed by a space
- <zone description> is the name zone to be inhibited or activated

Alien function keys

5-20

The Alien touch screen user interface provides a function key menu similar to that of the web server of the SmartLAN/G board and the Alien Mobile application. The keys are visualized as icons which activate the respective functions when tapped on the Alien touch screen and Alien Mobile application or, in the case of the web server, when clicked by means of the mouse.

The following table provides a description of the function keys displayed on the home page. The home page of the Alien/S, coincides with the page that is displayed when the user has not activated any function or application, or has simply not touched the display for at least 45 seconds. The keys coincide with those present in the section on the right-hand side of the display of the Alien/G.

Some of these keys activate their assigned functions after entry of a user code that opens a session, which is closed by tapping "Logout" button on the top right of the Home page or after 45 seconds inactivity on the keypad.

In the case of the web interface and the Alien Mobile application, this page is displayed after the user access is achieved through a valid login operation.

Table 5-3: Alien menu

Icon/key		Function		
		Alien keypad	Web interface	AlienMobile
	SCENARIOS	Accesses the section containing the list of programmed scenarios which can be activated. No code required for access. Refer to <i>paragraph 5-2 Arming and disarming partitions.</i>		
		Depending on programming, the activation of scenarios may require code entry.	/	User code is required if it is not registered in the "Settings - Control panel" section.
	COMMANDS	Accesses a section containing the list of outputs which can be activated. Refer to <i>paragraph 5-6 Activation of outputs.</i>		
		The outputs are divided in two sections: <ul style="list-style-type: none"> "Domotic", outputs for the management of home automation No code requested "Intrusion" outputs programmed through the intrusion-control system User code required. 	/	User code is required if it is not registered in the "Settings - Control panel" section. Available for AlienMobile+ only.
	INTRUSION	Accesses a section where you can view and change the status of parts of the intrusion-control system: <ul style="list-style-type: none"> "Partitions" - where you can view and change the status of the partitions. "Zones" - where you can view and changes the status of the zones. "Events Log" - where you can view the events log. Refer to paragraphs 5-1, 5-2 and 5-5.		
		User code required.	<ul style="list-style-type: none"> The "Partitions" section allows you to reset the partition alarm memory. After obtaining access to the "Events Log" section, it is necessary to indicate the number of events to be viewed. 	
			Also available in the "Timer" section where it is possible to view the timers and their status. Refer to <i>paragraph 5-5 View.</i>	User code is required if it is not registered in the "Settings - Control panel" section.
	MENU	Accesses two sections: <ul style="list-style-type: none"> "Actions" - containing a list of the control panel commands in the event of alarm or tamper events or requests for teleservice and overtime. Refer to paragraphs 5-1, 5-11, 5-12 and 5-14. "Activations" - where it is possible to view and enable the activations described in <i>paragraph 5-4 Activations.</i> User code required. 	Not present	Not present
	CAMERAS	Not present	Accesses two sections: <ul style="list-style-type: none"> "Real-time" - where the configured cameras are listed "Records", that allow you to view the snapshots recorded after the occurrence of an event. Refer to <i>paragraph 5-26 Camera access.</i>	You access a section containing the list of cameras configured in the AlienMobile "Settings" section. Refer to <i>paragraph 5-26 Camera access.</i> Available for AlienMobile+ only
	SETTINGS	Accesses the sections for the settings of the keypad and the SmartLiving control panel: <ul style="list-style-type: none"> "Alien" - provides information regarding the setting-up of the Alien touch screen interface you are using. It shows the model, firmware revision and the address of the keypad and built-in reader. Furthermore, it allows you to modify the screen by means of the + and - keys. Refer to <i>paragraph 5-8 Keypad settings.</i> "Date/Time", "Change PIN", "Tel.Numbers" - these sections allow you to change the date and time on the control panel clock, the user PINs and the contact phone numbers saved to the memory. Refer to paragraphs 5-7, 5-9 and 5-10. "Installer" - this section allows access to the installer menu after entry of a valid installer PIN, thus putting the control panel in programming mode. "View Joy" - this section allows you to work on the Alien keypad as if it were a Joy keypad. Tap the ALIEN button to step back to the standard mode. User code required. Installer code required for the "Installer". 	Accesses a section where it is possible to: <ul style="list-style-type: none"> select the language of the web interface select the home page of the web interface, from the menu pages and the first graphic map send a test email from the SmartLAN to an indicated recipient upgrade the web server interface open a section that shows the meanings of the icons used by the web interface 	You can access the following sections: <ul style="list-style-type: none"> "General", where you can change the settings on the AlienMobile application "Panel", where you can configure the SmartLiving control panel associated with the home page in question and enter the data for the Inim Cloud. "Camera", where you can configure the cameras viewable in the "Cameras" section. "Help", where you can view the user's guide. Refer to <i>paragraph 5-22 Using AlienMobile application</i> and to <i>paragraph 5-26 Camera access.</i>

Table 5-3: Alien menu

Icon/key		Function		
		Alien keypad	Web interface	AlienMobile
	SYSTEM	Accesses a section where it is possible to view the system parts: <ul style="list-style-type: none"> List of ongoing faults Power-supply voltage of the control panel Information relating the GSM communications board Refer to <i>paragraph 5-5 View</i> .		
		User code required.	/	
	APPS	Accesses the applications of the Alien touch screen interface: <ul style="list-style-type: none"> "Photo frame" - application that starts a slideshow of the images contained in the inserted SD-card (see <i>paragraph 5-23 Photo frame</i>). "Voice functions" - accesses a section where it is possible to activate the control panel voice board functions or the "Intercom" function. Refer to <i>paragraph 5-3 Voice box and intercom functions</i>. "Maps" - accesses the system by means of the graphic maps (refer to <i>paragraph 5-24 Graphic maps</i>). "Alarm clock", "Memo" - application for the programming and activation of audible signalling and popups on the Alien keypad (refer to <i>paragraph 5-25 Alarm clock and memo</i>). No code requested	Not present	Not present
	KEYPAD	Not present	Section for remote access to a keypad. Refer to <i>paragraph 5-21-2 Access to and use of the Web interface</i> .	Not present
	SMS	Not present		Accesses a section where it is possible to send the SMS commands and change their settings. User code is required if it is not registered in the "Settings - Control panel" section. In order to use this section, the control panel requires installation of a Nexus GSM dialer, which need not be connected to the Internet. Available for AlienMobile+ only. Refer to <i>paragraph 5-22-1 SMS commands</i> .
	CLIMATE	Accesses the thermostat functions section No code requested	Not present	Accesses the list of keypads configured with the thermostat function Available for AlienMobile+ only
		Refer to <i>paragraph 5-13 Thermostat</i> .		
	MAPS	Section contained in "Apps".	Accesses the system through the graphic maps.	Not present
		Refer to <i>paragraph 5-24 Graphic maps</i> .		

Using the SmartLAN/G 5-21

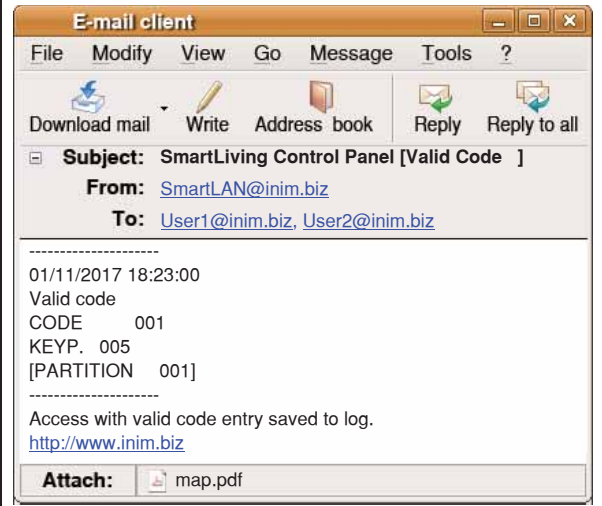
e-mail 5-21-1

The event-related e-mail sent to the user via the SmartLAN/G board must be programmed entirely by the installer.

Below is an example of an e-mail associated with a "Valid Code" event.

Table 5-4: E-mail parameters

Option	Example	
Subject	SmartLiving control panel [Valid code]	Text, edited by the installer, associated with the respective event (in square brackets).
Sender	SmartLAN@inim.biz	Parameters set by the installer
Recipient	User1@inim.biz, User2@inim.biz	
Message text	----- 01/11/2017 18:23:00 Valid code CODE 001 KEYP. 005 [PARTITION 001] -----	The first part of the e-mail shows the date and time of the event (when saved to the events log) and any relative details.
	Access with valid code entry saved to log.	Optional text Link to an Internet website or IP address (if applicable).
	http://www.inim.biz	
Attachment	map.pdf	Document/file sent with the e-mail



Access to and use of the Web interface 5-21-2

The security of the connection with the computer is guaranteed by integrated cryptography. The security of the connection of mobile-phone devices is guaranteed by the SSL protocol used for HTTPS connections.

Following is a description of the method of access to the interface which allows remote management of the control panel.

LOGIN

1. Type in the IP address on the navigation bar of the browser.
If you wish to use HTTPS protocol, simply add the letter "s" to the "http" prefix (for example: "http://192.168.1.92" would become "https://192.168.1.92").
2. At this point the control panel will display the access page template which requires the following data (provided by the installer):
 - Username
 - Password
 - Code (user code valid for the control panel)
If the installer code is entered, it will be accepted only if the Teleservice function is enabled (*paragraph 5-4 Activations*).
3. Press "Login" to start the connection.

Access will be denied in the following cases:

- the entered PIN is not recognized
- the entered PIN does not belong to any partition
- the entered PIN is not enabled
- the entered PIN is associated with a timer and the timer concerned is OFF.
- The "Internet Access" option from the Activations section in the User menu is not enabled

If the connection is successful, the browser will show the home page of the web-server interface and the main menu. The menu provides the function keys listed in *Table 5-3: Alien menu*.

MENU

In addition to the keys on the home page, the following buttons will help you navigate through the various sections:

NAVIGATION

- **HOME** - positioned to the right on the lower tool bar, takes you directly to the home page
- **MENU** - positioned to the right on the lower bar, opens a list of buttons/links to the sections of the web interface and also the logout button
- **LOGOUT** - present in the "MENU" list, effects user logout operations and returns to the login form fields.

Once web-interface consultation is over, it is advisable to end the session started after login, with a "logout" operation, this will avoid unauthorized access to the system via the browser.

ATTENTION!



The lower tool bar of each section always shows the firmware version and model of the SmartLiving control panel in use and also the current arming scenario.

INFO

The "Keypads" section contains a replica of one of the keypads connected to SmartLiving control panel. This section allows you to use the replica keypad, with its keys, display and LEDs, to operate on the system after access from remote locations.

KEYPADS

Besides the keypad buttons (described in *paragraph 2-3-2 Using the keys*) there are also other buttons:

-  , to access the start page of the web interface
-  , key to open a window for the selection of the keypad to be replicated from those connected to the control panel

Using AlienMobile application

5-22

The Alien Mobile application may be utilized by SmartLiving control panel users who have Internet connection.

CONNECTING TO THE INTERNET

Once the application has been downloaded to the tablet or smartphone, the user can enter the connection parameters (provided by the installer), in the "Settings - Control panel" section of the application (refer to *Table 5-3: Alien menu*).

- IP address and connection port of the control panel
- User details (username, password and user code)
- Type of SmartLAN board used for web access




If you wish, you can enter a password in "Settings - General" section of the application (refer to *Table 5-3: Alien menu*), that will be requested each time the application starts (the "Request password" option must be enabled).

PASSWORD

Once the application starts and the password is entered, the home page will show the main menu with the function keys listed in *Table 5-3: Alien menu* in reference to the first control panel configured.

MENU

Table 5-5: AlienMobile - home page

A	Firmware version, type and description of the SmartLiving control panel.	
B	Mobile connection icon: <ul style="list-style-type: none"> •  Mobile data •  WiFi 	
C	Section for the active functions, with access buttons to the application and the SmartLiving system. The home page of the Alien/G (shown in the figure) shows the function buttons indicated in <i>Table 5-3: Alien menu</i> .	
D	Scroll keys	
E	Button to restart an arming status reading on the control panel (only AlienMobile+) and string showing the ongoing scenario.	
F	Button for quick viewing of cloud events.	
G	Page indicator (only AlienMobile+). If you are inside a section, this field will show the following buttons: <ul style="list-style-type: none"> • Back level This button allows you to step back to the previous level of the active function. • Home Button which allows you to go directly to the home page. 	

By tapping on the scroll-buttons, or lightly swiping from either left or right, you will be able to navigate through the various pages, each referring to a different configured SmartLiving control panel.

You can add a new page for the configuration of a new control panel by tapping the right scroll-button after the last configured control panel and by confirming the request.

ADD OR DELETE A CONTROL PANEL

You can configure up to 5 control panels with the AlienMobile+, whereas the AlienMobile allows you to configure only one.

To delete a page swipe it lightly from bottom to top and then confirm deletion.

Otherwise, you can go to the respective section "Settings - Control panel" and tap the **Delete** button.

For control panels registered to the Inim Cloud service, the AlienMobile+ application also provides a key that accesses the event viewing section.

If necessary, this button indicates the number of events not yet viewed,

The events that can trigger these notifications are those for which the “push” option has been enabled (*paragraph 5-27 Use of the Inim Cloud*). In this case, the device used (smartphone or tablet) will notify the user of the arrival of a notification even when the application is closed.

CLOUD NOTIFICATIONS

SMS commands 5-22-1

The Nexus dialer board allows the control panel to receive commands sent by the user via GSM, and in particular via SMS.

When a user requests an operation, via a correctly formatted SMS message to the SIM card of the Nexus, the control panel will activate the respective shortcut and send confirmation (feedback) of the executed command.

The “SMS” section of the AlienMobile+ application allows the commands programmed on the control panel to be sent via SMS.

This section of the application can be used also when the control panels are not connected to the Internet.

Here you can find the list of the programmed SMS commands inserted in the smartphone you are using.

The following buttons are available:

- **SEND**, button to send the SMS message to the control panel, in order to activate the related command.
- **Add**, button to add an SMS command to the list. Once pressed, a window appears with the following strings that must be edited:
 - “Description”, string that can be customized by the user
 - “Command text”, string that must to be consistent with the control panel programming
- **Synchronize**, button to download all SMS commands from the control panel to the smartphone.
- **Nexus number**, button to enter the phone number of the control panel GSM board.



Photo frame 5-23



“Photo frame” is an Alien keypad application that plays a slideshow of images.

The image files must be stored in the folder “images” under root on the micro SD card which is inserted in the appropriate slot on the Alien keypad. Visualization image file format: JPG, GIF and BMP.

For optimum visualization, it is advisable to keep the size of each file below 500 kbytes.

Note

There are two ways of starting Photo frame:

- From the Alien keypad - access the “Apps” section by tapping the button , then tap the “Photo frame” button.
- Automatically, if the value set for the “Delay photo” parameter is different from “Disabled”. In order to change this parameter and others of the Alien keypad and the application, access the “Settings” section by tapping the button , type-in a user code and then access the “Alien” section (see *paragraph 5-8 Keypad settings*). The slideshow can be stopped by simply tapping the screen, which then returns to the home page.

Graphic maps 5-24

The SmartLiving supervision functions are based on graphic maps which can accessed by the end-user through an Alien keypad or web interface.

The graphic maps are linked together in a tree structure that allows you to view the status of every part of the security system status and interact with it through the icons shown.

The Alien keypad manage up to 10 maps (versions previous to 2.00 manage up to 5 maps) and the web interface as many as 20 maps. Each map supports up to 20 objects/ buttons represented by icons.

The type of icon used and its function as a default button is described in the following table. It is possible to change these functions during the programming phase and associate each icon with a descriptive string or even make use of customized icons.

The Graphic map functions require installation of a micro-SD board. If this board is not installed the **MAPS** button will show the message "no SD-card" and the application will not start.

Note

Table 5-6: Graphic map icons at default

Subject	Icon	Key	Subject	Icon	Key	
Link		Link to the Alien home page	Scenario		Scenario active /	
		Map link			Scenario inactive	After a valid code entry you can activate the scenario
Partition		Partition armed in Away mode	Ongoing fault		Scenario active	Accesses the faults viewing section
		Partition armed in Away mode			Scenario inactive	
		Partition armed in Instant mode	Thermostat		Thermostat disabled	Accesses the reader thermostat management section
		Partition disarmed			Thermostat set to manual mode	
		Partition alarm/tamper memory			Thermostat set to daily mode	
Zone		Zone shorted/tamper Zone alarm/tamper memory		Thermostat set to weekly mode		
		Zone in stand-by status		Thermostat set to antifreeze mode		
		Zone in alarm status	Reset partitions		After a valid code entry you can deactivate immediately the outputs relative to alarm and tamper events and clears the alarm and tamper memory	
		Zone disabled/bypassed	Clear call queue		After a valid code entry you can clear the call queue completely and interrupt any ongoing call.	
Output		Output activated	Stop alarms		After a valid code entry you can deactivate instantly the outputs activated by zone/partition alarm and tamper events and system tamper events.	
		Output deactivated	View events log		After a valid code entry you can access the events log	

Alarm clock and memo

5-25

The Alien keypad provides applications which allow the user to manage the events which when they occur activate a signal that is both audible and visual (in the form of popups on the display).

Programming or activation of the alarm and memo events are of no consequence to the programming or regular functioning of the SmartLiving control panels and its peripherals.

Note

The "Alarm clock" and "Memo" functions in the "Apps" section access lists that provide all the events and, for each, provide buttons for activation (**ON**, **OFF**) and programming (**SET**).

Each event can be programmed with:

- description
- day of the week, by selecting the respective button in the upper part of the "When?" section
- time, by changing the field selected with the arrows

For "Memo" events only, you can also program:

- additional text
- day of the week or alternatively a specific date in the lower part of the "When?" section
- a second time, in the "When?" section, by selecting **Time 1**
- if a specific date is programmed, you will be able to set a regular interval (periodicity) in the lower part of the "When?" section and a time pattern (cadence) by tapping on the OFF button until you obtain the desired value.
- audible signals and images that correspond to the memo

Touching the "Alarm clock" or "Memo" button for at least 5 seconds will delete all the programming in the section concerned.

When the properly programmed and activated event occurs, a window similar the one shown will appear. the OFF button stop the signalling, whereas the SNOOZE button interrupts the signal for 5 minutes before signalling again.



Camera access

5-26


The user can view the video recording made by the IP cameras through the Alien interface, the web browser, the AlienMobile application ("AlienMobile+" version) or keypad.

Via Graphic maps

Access to the graphic maps allows direct viewing on the display or screen associated with the "Camera" object.

A window (predefined by the installer) will appear in place of the object concerned and will show the video recording shot by the camera in real-time.

The type of video playback (snapshots in sequence or filmstrip) depends on the type and make of the camera.

From the Alien keypad, access the "Apps" section by tapping the  button, followed by the "Maps" button.

Via the web browser, access the "Graphic Maps" section.

Once access has been obtained, navigate through the tree structure until you reach the map containing the camera.



Via Web

Access the "Camera" section.

Two sections are available:

- "Real-time" - allows you to view the configured cameras and relative video recordings in real-time.
Each camera has a box that shows:



- information regarding the camera (description, make, time, date, etc.
- snapshots taken in real-time
- **Snapshots** button - allows you to view the recorded footage in snapshot sequence
- **Video** button - allows you to view the recorded footage in video format
- "Records" - allows you to view recorded footage after the occurrence of an event. Each box provides:
 - information regarding the event that triggered the video recording (description, time, date)
 - first snapshot of the recorded sequence
 - **View** button - allows you to view the recorded camera footage in specific snapshot sequence (the snapshots which immediately precede and follow the occurrence of the event)

Depending on the type and make of camera, it may be possible to use the pan, tilt and zoom (PTZ) commands for viewing or select one the preset for viewing or operating modes provided by the camera.

Via AlienMobile

The AlienMobile+ application allows you not only to access viewing of recorded footage, but also to add or configure the cameras you have access to.

Cameras can be configured or added to those available through the "Settings, Cameras" section.



In this section you can select the camera by simply navigating through the corresponding pages using the right/left arrow keys, or add a new camera by tapping the right arrow key after the last configured camera.

Inside the open page, you can select the camera type and change a series of parameters which vary depending on the type and make of camera in use.

You must tap the **Save** button in order to confirm and save any changes.

The "Cameras" section on the home page shows a list of cameras included.



You can obtain direct access to one of the configured cameras either by tapping the







View button, or by first tapping the  button (which allows simultaneous viewing of the footage of all the configured cameras) and then tapping the corresponding box.

Once the camera is accessed you can view the recorded footage in real-time and interact with the camera functions supported by the type and make of the camera.

Use of the Inim Cloud

5-27






The web interface of the cloud allows you to navigate by means of buttons that access the sections relating to selected control panel (Table 2-13: Inim cloud - home page, B). Status viewing and supervision of the elements on the SmartLiving system is achieved via the available buttons.


-  , button for access to the home page (paragraph 5-5 View)
-  , button for access to the programmed arming scenarios (paragraph 5-2 Arming and disarming partitions)
-  , button for access to the management section of the comprised partitions and zones (paragraph 5-2 Arming and disarming partitions and paragraph 5-4 Activations)
-  , button for access to the management section of the outputs (paragraph 5-6 Activation of outputs)
-  , button for access to the management section of the air conditioning systems connected to the keypad thermostats (paragraph 5-13 Thermostat)
-  , button for access to the section where the control panel devices are listed, each showing their firmware revision, supply voltage, enabled status and other details.

SECTION ACCESS BUTTONS

These devices are divided into categories:








- Control panel
- Keypads
- Readers
- Expansions
- Sounderflashers
- Nexus

-  , button for access to the events log of the selected control panel. The events are listed in chronological order and, in addition to viewing, reset, search, download and storage operations are also available for each event. The event type can be identified by an icon:
 -  , alarm events. Confirmation of the viewing operation is also available for these events (✓).
 -  , alarm events. Confirmation of the viewing operation is also available for these events (✓).
 -  , other control panel events
-  , button for access to the section where you set up notifications for the events of the selected control panel. The events are grouped into 5 categories:
 - alarms
 - generic messages
 - faults
 - Arm/Disarm op.
 - programming

There is a list of notification recipients for each type of event and it is possible to add others via the  button by specifying:

 - name
 - phone number for the voice call
 - phone number for the SMS message
 - email address
 - enable the “push” notification for AlienMobile+ users

The web interface of the cloud has several buttons for the management of the displayed objects:

-  , button to start a search through the listed events
-  , button to download the data displayed via a .csv file
-  , button to view the events log of the selected control panel.
-  , button to store the displayed data. The data will be transferred in the “Archive” section, reachable by means of the  button in the upper right corner of the same section. In this section, it is possible to view, reset or permanently delete the listed data.
-  , button to confirm the visualization of all the ongoing alarms
-  , button to refresh the web page

OTHER BUTTONS

Registering a control panel to the user account

5-27-1

After creating your Inim Cloud service account, the user can request the registration of a new control panel to those they have access to via the web interface (*Table 2-13: Inim cloud - home page, A*).

The control that the user wants to register to their account must first be registered to the Cloud service by an installer.

Note

Clicking on the button that manages your profile (*Table 2-13: Inim cloud - home page, D*), accesses a page where you can set the parameters of your account and those of registered control panels. In the lower section, below the list of control panels, you have the “New INIM system” section.

1. The **Add** button will allow you start the registration process. The Cloud service will send an OTP (One Time Password) number consisting of 6 digits to the user. This number has a limited time duration of 15 minutes.
2. From an LCD keypad, access the “Activations” section of the User menu, and then “Cloud enrollment”. From an Alien keypad, access the “Menu” section, then “Activations”, then “Cloud enrollment”.
3. Enter the OTP password and wait for the outcome of the registration. The outcome of the procedure will be shown with one of the following messages:

- "Account created!": the control panel has been successfully registered to Cloud
- "Communicat.Error": generic communication error.
The possible causes may be:
 - no Internet connection
 - date of manufacture of the control panel is earlier than dd/mm/yyyy
 - date/time of control panel different, ahead or behind the exact date/time by more than 15 minutes
- "Already enrolled": the control panel is already registered to Cloud
- "Bad/expired OTP": the entered password is incorrect or expired
- "Panel notEnabled": the control panel cannot be registered to Cloud.

Appendix A

GLOSSARY

These are 4, 5 or 6 digit PINs which allow the building occupants (users) to access the system. Each code can be programmed to control specific functions only, and to operate the system to suit the requirements of the Main user.

Code types

- **Installer code:** assigned to the installer of the security system
- **User code:** assigned to the end-users of the system

Detection of non-authorized entry into the protected building. More specifically, activation of a detector.

In the event of:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

The red LEDs on the system keypads and readers go On each time one of the previously-mentioned events occur. This visual warning signal is held even after the event ends (alarm memory), in order to warn you that an event occurred during your absence. This visual warning signal will be held until you clear the event memory (refer to Delete Memory).

This is a private service that monitors premises protected by intrusion control systems equipped with digital communicators or voice dialers.

Alarm Receiving Centres receive alarm reports from monitored systems and take all the necessary actions to protect the occupants of the protected premises.

The "Answerphone" function, if enabled by the user, allows the control panel to answer incoming calls after a pre-set number of rings. The control panel will pick-up and play the recorded answer message.

During the call, the recipient can type-in a valid PIN (enabled for over-the-phone control) and access the authorized functions.

User operations on one or more partitions. These generally indicate also the status of the partitions. Under normal circumstances, the zones of armed partitions can generate alarms. Under normal circumstances, the zones of disarmed partitions cannot generate alarms. The system generates tamper alarms even when partitions are disarmed.

You can enable/disable the Auto-arm function on each separate partition.

If the auto-arm option is enabled on a timer-controlled partition, the partition will arm/disarm in accordance with the ON/OFF settings of the timer.

This is the secondary power source of the system. If primary (230 Vac) power failure occurs, the battery will take over.

A list of outgoing event-associated calls the control panel must send to programmed contact numbers.

Enabled users can clear the call queue manually.

The Cloud is a web service that provides data storage space ("cloud storage") that, by means of any Internet connection, is accessible at any time and from any place. The data are then shared over the network, along with the resources to process them ("cloud computing") with all users who have a valid access.

The Cloud provider guarantees therefore that the user has both the resources for the processing and editing of data, and data synchronization that can be accessed and modified by multiple users without the risk of being lost.

Violation of a zone with this configuration will not generate an alarm but will trigger the associated Timer (Entry time). If the user does not disarm the partition/s within the set "Entry time", the system will generate an alarm.

For example, the zone that monitors the main door of a building is usually configured as a Delayed Entry Zone, in order to give building occupants time to enter the building and disarm the partition without generating an alarm.

Violation of a zone with this configuration will not generate an alarm but will trigger the associated Timer (refer to Exit time).

For example, the zone that monitors the main door of a residence or building is usually configured as a delayed exit zone, in order to give occupants time to leave the partition after an arming operation. If the user does not leave the zone within the set "Exit time", the system will generate an alarm.

ACCESS CODES

ALARM

ALARM OR TAMPER MEMORY

ALARM RECEIVING CENTRE (ARC)

ANSWERPHONE

ARM/DISARM

AUTO-ARM

BACKUP BATTERY

CALL QUEUE

CLOUD

DELAYED ENTRY ZONE

DELAYED EXIT ZONE

This is an explicit user-command which ends signalling on the red keypad/reader LEDs of the following events:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper (keypads, expansions, readers)
- peripheral loss (keypads, expansions, readers)
- false key

If you delete the alarm/tamper memory, the visual signals on the red reader/keypad LEDs will clear.

This device allows the control panel to send report calls to Alarm Receiving centres (ARC). SmartLiving control panels provide a built-in digital dialler which supports all the most widely used protocols.

The time (expressed in minutes or seconds) that the system allows the user to disarm the partition after zone violation. If the system is not disarmed within the set time it will generate an alarm.

Each partition can be programmed with its own Entry time.

An operative status recognized by the system.

For example: detector alarm, mains failure, blown fuse, user-code recognition, etc., are all events recognized by the control panel.

Each event (e.g. mains failure) can be associated with an activation event (when the event occurs) and a restoral event (when the event ends).

Each event can be programmed to generate the following actions:

- activation of one or more outputs
- transmission of one or more e-mails
- send one or more SMS messages
- activation of one or more voice calls
- activation of one or more digital calls

This is the non-volatile portion of the memory the panels saves events to. The events are saved in chronological order with the following details:

- event description - with details regarding new events and restorals
- information regarding the user or the cause of event
- event location
- event date and time

The events log can be viewed by the system users and the installer.

Partition events (zone alarms, partition alarms, arm/disarm operations, recognized codes and keys, etc.) can be viewed by users with at least one partition in common with the event element.

For example, if a user arms several partitions from a keypad, the events log will show:

- description of the event - "Arm request"
- description of the code and partitions involved
- description (label) of the keypad involved
- date and time of the request

A short period (expressed in minutes or seconds) during which the user must disarm the partition after violation (for example, after opening the front door) otherwise the system will generate an alarm.

Each partition can be programmed with its own Exit time.

These boards can be used to increase the number of terminals (zones or outputs) and/or the size of the system (in order to extend it over a larger area). Expansion boards can be connected to the system via the I-BUS.

A condition which indicates that a system component is not working properly.

Some faults can jeopardize the performance of the entire system. Mains failure (230V a.c.), telephone line-down and low battery are typical faults.

A map is a graphic representation of part of the area supervised by the security system and identified by an image file. The entire system can be represented by maps which can be linked together.

Each map can contain objects represented by icons. These icons are capable of changing status in accordance with the objects they represent and can operate as activation buttons for specific functions.

The user, by means of access to a graphic map, can view the supervised area and also access the security system functions.

An object can be:

- Partition
- Zone
- Output
- Map link
- Key

A device which allows the control panel to make telephone calls over the GSM network and also allows users to interact with the control panel over-the-phone or by means of SMS text messages.

DELETE ALARM/TAMPER MEMORY

DIGITAL DIALER

ENTRY TIME (OR ENTRY DELAY)

EVENT

EVENTS LOG (OR EVENTS MEMORY)

EXIT TIME (OR EXIT DELAY)

EXPANSION BOARDS

FAULT

GRAPHIC MAP

GSM DIALER

This is the two-way communication line (4 wires only) which connects the peripheral devices (keypads, readers, expansions, etc.) to the control panel.

The 4 easily identifiable wires, on the control panel motherboard and on the expansions, are:

- “+” power 12 Volt
- “D” data
- “S” data
- “-” Ground

A bypassed (disabled) zone cannot generate alarms. Activation/Deactivation of zones can be carried out manually by users or, under certain circumstances, automatically by the control panel.

The Installer code is generally a 4, 5 or 6 digit PIN which allows the installer to access the system Programming Menu and check or change the system parameters either from a keypad or via the respective software programme, on condition that all the system partitions are disarmed.

List of system functions and respective parameters accessed via keypad.

This menu allows the installer to program, check and change nearly all of the system parameters. The installer menu can be accessed from any keypad after entry of a valid installer PIN, and on condition that all the system partitions are disarmed, or can be accessed via a computer equipped with the SmartLeague software.

A zone that monitors the inside of the protected building.

For example, the interior zones of an office building are the zones that monitor offices and entrance points.

If a partition that a zone belongs to is armed in Stay mode, it will be unable to generate alarms.

A camera is an electronic instrument that records bidirectional images in sequence. It is part of a telesurveillance system supervised by an intruder control panel.

The IP camera (or “webcam”) transmits video images to an URL address, for direct viewing or for storage of the recorded material.

A portable control device (card or keyfob) which allows the authorized user to access the system. The key must be held in the vicinity of the reader in such a way to allow the system to read it and permit access to authorized operations.

Each key is programmed with:

- A random code selected from over 4 billion possible combinations.
- A label (usually the name of the user).
- The partitions it controls (arms, disarms, etc.).
- A group of pre-set parameters which allow the key user to operate the system in accordance with the authorized access level (for example, a key can be programmed to arm or disarm the system only at certain times of the day).

This device allows users to access and control the system. Keypads can be connected to the system via the I-BUS.

The keypad allows users to access and control the partitions which are common to both the code and keypad in use. The user can arm/disarm partitions, view the status of the zones, stop visual and audible signalling devices, etc.

A generic magnetic-contact is a detector/sensor based on a magnet which, when placed near the sensor, provokes the mechanical closure of an electrical contact.

An electrical output point connected to a signaling or control device activated/deactivated by the control panel in response to programmed events.

Signaling that may be associated with a state of emergency perceived by the user and signaled to the intrusion control panel by means of a button or the activation of a shortcut.

This type of signalling generates an event which activates the programmed outputs and calls. This type of signalling does not activate the red LEDs on the keypads and readers nor is it visualized on the keypad displays.

A group of zones.

A partition identifies a group of zones that belong to a spatial or logical portion of the protected premises. For example, a partition may comprise all the zones that protect the downstairs partition of a house (spatial partition), or all the entrances of an office building (logical partition).

This refers to the status of a partition as requested by the user.

The user can carry out the following operations.

- **Disarm** - this operation disables the partition completely. In this way, none of the zones belonging to the partition can generate alarms.
- **Away mode** - this operation enables the interior and perimeter zones of the partition. In this way, all of the zones of the partition can generate alarms.
- **Stay mode** - this operation enables only the perimeter zones of the partition. In this way, only the perimeter zones of the partition can generate alarms.
- **Instant mode** - this operation enables the partition perimeter zones only and annuls delays. In this way, violation of the perimeter zones of the partition will generate instant alarms.
- **Hold** - this operation forces the partition to hold its current status.

A periodic inspection of the protected premises carried out by authorized security staff.

A zone that monitors the entrance points of the protected building.

Perimeter zones are usually direct entrance points such as doors and windows. For example, the front door of an apartment and windows that allow access from outside.

I-BUS

INHIBITION - DEACTIVATION OF A ZONE

INSTALLER CODE

INSTALLER MENU

INTERIOR ZONE

IP CAMERA

KEY

KEYPAD

MAGNETIC CONTACT

OUTPUT

PANIC

PARTITION

PARTITION ARM/ DISARM OPERATIONS

PATROL

PERIMETER ZONE

Devices connected to the control panel via the I-BUS.

SmartLiving control panels manage the following peripherals:

- Keypads (Joy, Aria, nCode, Concept, Alien)
- Proximity Readers (nBy)
- Expansions (Flex5)
- Transceiver (Air2-BS200)
- Sounderflasher (Ivy-B)
- Isolators (IB100)
- GSM dialer (Nexus)

The period (expressed in minutes) before an automatic arming operation.

For example, if a partition is set to arm automatically at 10:30 with a Pre-arm time of 5 minutes, all the partition keypads and readers will initiate an audible countdown at 10:25 in order to warn users of the forthcoming arming operation.

Each partition can be programmed with its own Pre-arm time.

The area to be protected.

Identifies the building or part protected by the intrusion control system, generally, a house or office.

Under normal circumstances, the mains power supply (230Vac) 50 Hz (110V a.c. 60Hz in some countries).

Usually connected to a switching power supply or transformer (depending on the model) that provides the stabilized voltage to the system and the charge source to the batteries.

This device allows users to access and control the system. The system readers are connected to the control panel via the I-BUS.

The readers allows users to arm/disarm the partitions which are common to both the reader and key in use (refer to Shortcuts). The key (TAG) must be held in the vicinity of the reader in such a way to allow the system to read it and permit access to authorized operations. Although readers provide a more limited access to the system, they are easiest way of carrying out day-to-day operations (arm, disarm, etc.).

A pre-set arming configuration which applies various operating modes to the system partitions.

The shortcuts are control panel functions which, in a single operation, provide a fast way of carrying out specific operations which would normally require a series of activations.

They can be activated by the end-user (at keypads, on codes typed in at keypads or on remote telephones, at readers or on keys) or on the occurrence (activation) of an event.

Optical smoke detectors are equipped with sampling chambers (based on light scattering mass - Tyndall effect). They are capable of sensing the presence of smoke particles and thus detecting a fire in its early stages.

These detectors have low power absorption during standby. The current absorption increases during alarm status and thus signals the danger of fire to the control panel.

The "supervision time" is the interval during which the wireless-system devices (in general wireless detectors in permanent placements) must signal to the control panel that they are operating in the network. If a wireless device fails to signal before the "supervision time" expires, it will be classified as "Lost" and the control panel will trigger a "peripheral-loss" fault event.

Detection of a serious condition that jeopardizes the operating capacity of the device concerned and thus puts the system at risk.

Tamper conditions are detected by tamper switches connected to the system zones, keypads, readers, expansions and control panel. Generally, these events are triggered by system violation such as unauthorized opening of a keypad cover.

These are calls sent to programmed contact numbers when specific events start and end (restoral).

This is a service provided by the installer company with the user's collaboration. The installer connects to the control panel over-the-phone or via a GPRS or Internet connection and, in this way, can check and/or change the control panel programming data.

A zone with this attribute cannot generate alarms (activate audible and visual signalling devices). However, any alarm events which occur will be saved to the events memory.

If zones are not operating properly, the "Test" option will allow the installer to check them without the risk of generating false alarms

A logical entity for automatic time-management of programmed peripherals or elements.

SmartLiving control panels provide 10 timers.

Transceiver-equipped devices

In two-way wireless systems, all the devices are equipped with transceivers. In one-way wireless systems, the main unit is equipped with a receiver module whereas the peripheral devices are equipped with transmitters.

PERIPHERALS

PRE-ARM TIME

PREMISES

PRIMARY POWER SOURCE

READER

SCENARIO

SHORTCUTS

SMOKE DETECTORS

SUPERVISION

TAMPER

TELEPHONE ACTIONS

TELESERVICE

TEST ZONE

TIMERS

TRANSCEIVER

Each code is programmed with:

- A 4, 5 or 6 digit PIN which allows access the system.
- A label which identifies the user (usually the user's name).
- The group of partitions it controls (arms, disarms, etc.).
- A group of pre-set parameters which allow the operator to work on the system in accordance with its authorized access level (for example, a code can be enabled to consult the events log but not to change the date and time).
- A hierarchical level, that may allow the user to change to parameters of codes on a lower level in the system hierarchy.
 - User (the lowest level)
 - Manager
 - Master

List of functions available to the user after entry of a valid code at the keypad.

This device allows the control panel to send voice calls to programmed contact numbers.

In SmartLiving control panels the voice dialler function is provided by the SmartLogos30M board (accessory item).

If the system is equipped with a SmartLogos30M voice board, all keypads with voice functions present in the system configuration will allow users to record memos. Messages can be recorded, played and deleted as required.

Software application that allows you to view web contents over the Internet.

Software application that processes web page requests from a web browser.

The SmartLAN/G network board has an integrated web server that provides the browser with a web interface for the management and supervision of the SmartLiving system.

An intrusion control system whose devices (detectors, keypads, keyfobs) communicate with the control panel over radio waves.

Usually, only the control panel of wireless-systems is mains powered (220Va.c.) while, the wireless devices are battery powered. The battery life is of utmost importance in the design layout and operational capacity of these systems.

An electrical input point used for the management/supervision of signals coming from an intrusion detection device.

USER CODE

USER MENU

VOICE DIALER

VOICE MEMO

WEB BROWSER

WEB SERVER

WIRELESS

ZONE

Appendix B


SHORTCUTS AT DEFAULT






n.	Icon	description	function	parameter
1		Arm/Disarm	Applies a pre-set scenario	which scenario
2		Stop alarms	Immediately deactivates the outputs relative to zone/partition alarm and tamper events and system tamper events.	
3		Clear call queue	Cancel the entire call queue and stops ongoing calls (if any).	
4		Delete memory	Carries out a "Stop alarms" operation and, at the same time, deletes memory of system and partition alarm and tamper events.	
5		Activate Output	Activates one of the programmed outputs.	Output
6		Deactiv. output	Deactivates one of the programmed outputs.	Output
7		Overtime	Delays auto-arming time of partitions by 30 minutes.	
8		Teleservice req.	Sends a call to the Installer company number (Teleservice number).	
9		Voice menu	Plays a recorded voice message which announces the shortcuts assigned to the number keys.	User code
10		Listen-in	Allows eavesdropping over-the-phone by means of a microphone located on suitably placed keypad.	Keypad
11		Intercom Call	Accesses the user menu section: Voice functions/intercom Call	
12		Arm/disarm menu	Accesses the user menu section: Arm/Disarm	
13		Alarm menu	Accesses the user menu section: Manage alarms	
14		Voice func. menu	Accesses the User Menu section: Voice functions	
15		Activations menu	Accesses the user menu section: Activations	
16		View Nexus status	Accesses the user menu section: View/Nexus status	
17		Arming status	Provides voice information regarding the armed/disarmed status of the partitions.	
18		Keypad sett. menu	Accesses the user menu section: Keypad settings	
19		ZoneBypass menu	Accesses the user menu section: Activations/Zones	19

n.	Icon	description	function
20		Voice memo	Accesses the User Menu section: Voice functions
21		Output control	Accesses the user menu section: Outputs ON/OFF
22		Enab.answer-phone	Accesses the user menu section: Activations/Answerphone
23		Enab.teleservice	Accesses the user menu section: Activations/Teleservice
24		Enable codes	Accesses the user menu section: Activations/Codes
25		Enable keys	Accesses the user menu section: Activations/Keys
26		Enable timers	Accesses the user menu section: Activations/Timers
27		Enab. auto-arm	Accesses the user menu section: Activations/Auto-arming
28		View events log	Accesses the user menu section: View/Events log
29		View alarm log	Accesses the user menu section: View/Alarms log
30		View faults log	Accesses the user menu section: View/Faults log
31		View arm ops log	Accesses the user menu section: View/Arm/Disarm op.
32		ViewSystemStatus	Accesses the user menu section: View/System status
33		View zone status	Accesses the user menu section: View/Zone status
34		Change PIN	Accesses the user menu section: Change PIN
35		Time/Date	Accesses the user menu section: Time/Date
36		View faults	Accesses the user menu section: View/Faults
37		Thermostat menu	Accesses the user menu section: Thermostat
38		Panic	Activates a "Panic" event

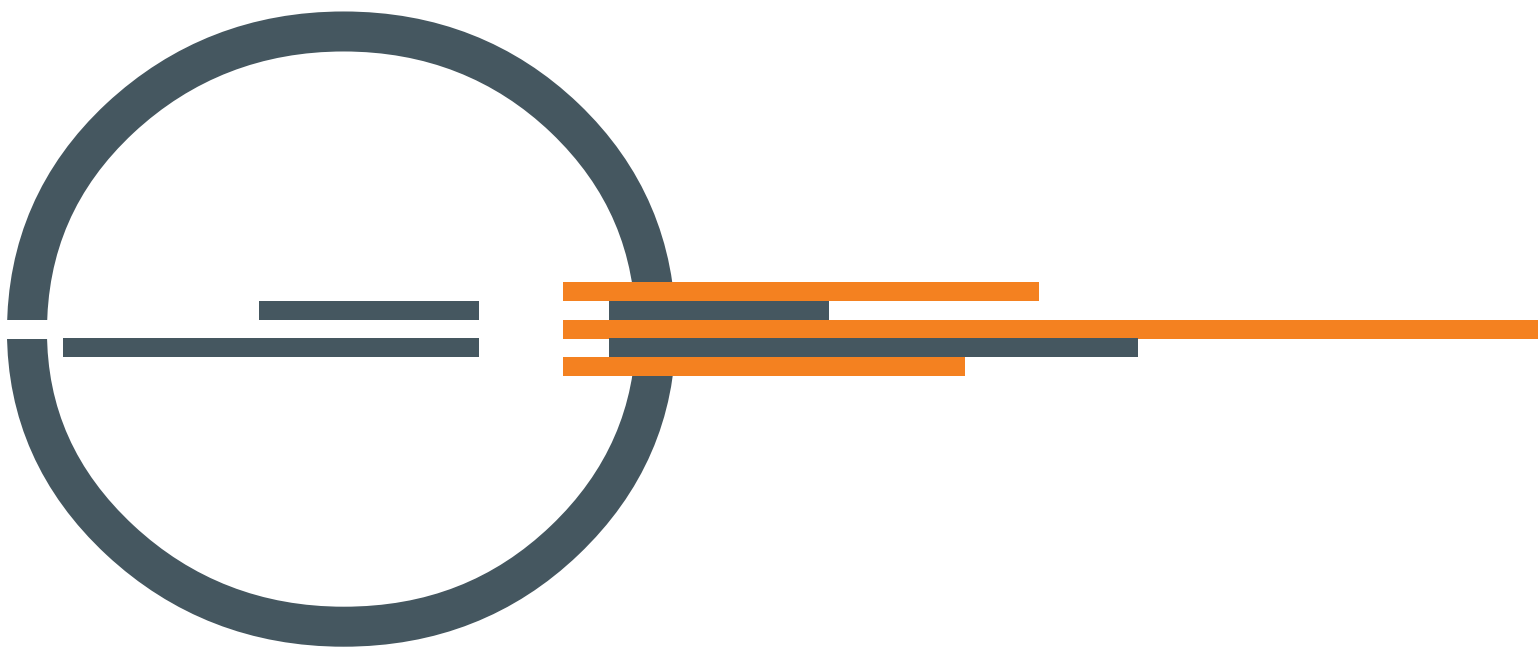
Appendix C

FAULT SIGNALS

The following table shows the system faults which are signaled on the yellow LED on the keypad  :

FAULT	Message on the User menu, "View/Faults"	Probable cause	Note
Zone fuse blown	Zone fuse fault	Excessive current draw on the "+AUX" terminals of the control panel	
BUS fuse blown	IBUS fuse fault	Excessive current draw on the "+" terminal of the control panel	
Backup battery inefficient or not connected	Low battery	The backup battery of the control panel is almost empty or disconnected.	
Primary power-source loss	Mai ns fai lure	The primary power source voltage (230 Vac) has failed or has been disconnected	
The PSTN landline is unavailable	Tel. li ne down	Trouble on the PSTN landline	
Interference	Jammi ng	Wireless transmission is poor	
Wireless detector battery low	Low battery WLS	The battery of at least one wireless detector is running out	For "Low WLS battery" and "WLS zone loss" signalling, access the user menu, go to "View/Faults", press  to view the list of devices involved.
Wireless detector not operative	WLS zone loss	At least one wireless detector is not operating	
Nexus GSM dialer faults	Nexus fault / Low signal	The GSM network signal is insufficient	Select "Nexus fault" then press the  button to access the list of current faults.
	Nexus fault / GSM module fault	The GSM module of the Nexus dialer is not operating properly. Call your Installer company	
	Nexus fault / SIM commun. fault	The SIM card does not respond or is not present. The SIM card PIN is not disabled.	
	Nexus fault / Low Credit	The credit left on the SIM card is below the minimum credit threshold.	
	Nexus fault / Provider Unavailable	The GSM network provider of the SIM in use is unavailable.	
Nexus fault /GPRS conn. lost	NEXUS/G detects problems on GPRS network communications		
IP connection loss	IP conn. lost	The verification of the IP connection fails.	
Device loss or tamper in progress	LossTamp. ongoing	One of the following events has occurred: <ul style="list-style-type: none"> • Control panel open • Dislodged panel • Expansion tamper • Keypad tamper • Reader tamper • Sound.flash.Tamp • Expansion loss • Keypad loss • Reader loss • Sound.flash.Loss 	
Faults on IVY-BUS sounderflasher	Sounder faults / Horn fault	A defect/damage has been detected on the horn/sounder.	Select "Sounder faults" then click on the  button to access the list of devices which have at least one fault present. Select the sounderflasher concerned then click on the  button to access the list of current faults on the device.
	Sounderflasher faults / LowBatt. Soundfl.	A low-voltage value has been detected on the sounderflasher battery. If the voltage drops below 10V, the device will inhibit the sounder and activate only the flasher (in the event of an alarm). If the voltage drops below 8V, the device will inhibit both the sounder and the flasher.	
	Sounderflasher Faults / Battery resist.	An excessive internal resistance has been detected on the sounderflasher battery. This type of deep fault indicates corrosion inside the battery, therefore, the battery must be replaced.	
Violation of zones with faults	Faults on zones	Violation has occurred on one or more zones with the "Fault zone" option enabled.	
Contaminated smoke sensor	Detector dusty	The smoke chamber of at least one of the Air2-FD100 smoke detectors is contaminated by dirt or dust.	Press  to access the list of zones involved.

Notes



ISO 9001 Quality Management
certified by BSI with certificate number FM530352

Centobuchi, Via Dei Lavoratori 10
63076 Montepandone (AP) ITALY
Tel. +39 0735 705007 _ Fax +39 0735 704912

info@inim.biz _ www.inim.biz