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 T031

GameOver

Prime
Anti-intrusion control panels and security systems

User's manual

inim ELECTRONICS

Warranty

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 of 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.

Limited 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.

Copyright

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.

RED European Directive compliance

Hereby INIM Electronics s.r.l. declares that the following devices are in compliance with the essential requirements and other relevant provisions of Directive 2014/53/UE.

Prime240L, Prime120L, Prime060S, Aria/HG, Joy/MAX, Quadra/P, nBy/S, nBy/X, Alien/GB and variants, Alien/SB and variants, Air2-BS200/50 and variants, Air2-KF100, Air2-MC100B and variants, Air2-MC200B and variants, Air2-UT100, Air2-FD100, Air2-Hedera-F and variants, Air2-Aria/B and Air2-Aria/N, AIR2-XIR200W, AIR2-XDT200W, AIR2-DT200TB and variants, SmartLinkAdv/GP, SmartLinkAdv/G

All the devices mentioned here above can be used in all EU countries without restrictions.

The full declarations of conformity can be found at URL: www.inim.biz

Leading-edge systems (DM37/08)

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.

WEEE

Informative notice regarding the disposal of electrical and electronic equipment (applicable in countries with differentiated waste collection systems)

The crossed-out bin symbol on the equipment or on its packaging indicates that the product must be disposed of correctly at the end of its working life and should never be disposed of together with general household waste.

The user, therefore, must take the equipment that has reached the end of its working life to the appropriate civic amenities site designated to the differentiated collection of electrical and electronic waste. As an alternative to the autonomous-management of electrical and electronic waste, you can hand over the equipment you wish to dispose of to a dealer when purchasing new equipment of the same type. You are also entitled to convey for disposal small electronic-waste products with dimensions of less than 25cm to the premises of electronic retail outlets with sales areas of at least 400m2, free of charge and without any obligation to buy.

Appropriate differentiated waste collection for the subsequent recycling of the discarded equipment, its treatment and its environmentally compatible disposal helps to avoid possible negative effects on the environment and on health and favours the re-use and/or recycling of the materials it is made of.

Table of contents

About this manual

MANUAL CODE

DCMUINE0PRIMEE

VERSION

1.40

USER'S MANUAL

This manual contains instructions relating to the user interface (keypad) of the Prime system, its functions and how to use them.

This manual is supplied with every control panel and must be given to the end-user for consultation. It is the duty of the installer to ensure that the end-user fully understands how the system works and is aware of the configuration set by the installer.

0-1 Terminology

CONTROL PANEL, SYSTEM, DEVICE

The main supervisory unit or any constituent parts of the Prime intrusion control system.

LEFT, RIGHT, BEHIND, ABOVE, BELOW

Refer to the directions as perceived by the operator when directly in front of the mounted device or computer screen.

QUALIFIED PERSONNEL

Persons whose training, expertise and knowledge of the products and laws regarding security systems, are able to create, in accordance with the requirements of the purchaser, the most suitable solution for the protected premises.

SELECT

Click on a specific item on the interface (drop-down menu, options box, graphic object, etc.).

PRESS

Click on a video button, or push a key on the control-panel keypad.

0-2 Graphic conventions

Note

The notes contain important information relating to the text.

ATTENTION!

The "Attention" prompts indicate that total or partial disregard of the procedure could damage the device or its peripherals.

Chapter 1 General information

1-1 Manufacturer's details

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.

1-2 Description of the product and various models

DESCRIPTION	anti-intrusion control panel
MODELS	Prime060S, Prime060L, Prime120L, Prime240L
COMPLIANCE	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 T031:2014-12 (ed.1)
SECURITY RATING	3
ATS CATEGORIES	up to SP6 or DP4 (in accordance with configurations)

The Prime system

Chapter 2

A typical Prime system comprises:

- a Prime 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 the most complete and versatile device for managing the system: the graphic display shows all the necessary information and provides an icon-based user interface for the immediate and clear identification of the operations to be carried out.

Together with the keypad, the system can also be managed by proximity readers, which represent a fast, easy-to-use interface for the most frequent daily operations, i.e. arming/ disarming operations. Authorized digital-key users can operate the system in accordance with the functions they are enabled to control by holding the key in front of the proximity key reader.

All control models are capable of managing a wireless system (wireless devices, remote-control keys, etc.), which can be easily integrated with a hardwired system.

Prime control panels are capable of managing various event types (not only alarms but also faults, tamper, code/key identification, arm/disarm operations, etc.) and event-response actions such as audible/visual signalling and messages (voice calls, SMS text messages and e-mails with attachments or push notifications).

The Prime also provides home-automation functions, such as programmed arm/disarm operations, access control, output activation/deactivation.

Telephone functions 2-1

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

By calling a Prime control panel or receiving a voice call from it, you can enter the PIN of a user code on the telephone keypad and activate commands via the scenarios.

The commands can be activated by keys "**0**" to "**9**" on the telephone keypad, which the system associates with various shortcut actions once the code PIN has been accepted. 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.

2-2 Voice functions

If the Prime control panel is equipped with a SmartLogos30M voice board, you will be able to take advantage of all the telephone and voice functions provided by the keypads equipped with loudspeakers.

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 5-4 Voice memo and intercom functions*. You can record, play and delete messages at your own discretion.

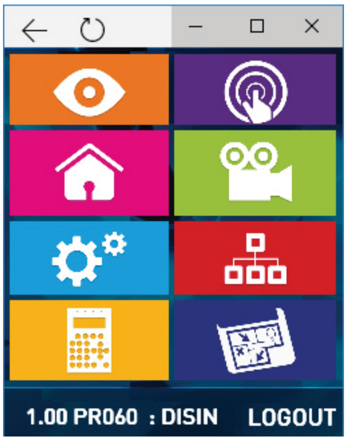
The presence of a new memo in the memo-box will be indicated by blinking on the blue LED on the keypad, as described in *Table 6-7: Keypad LEDs*.

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

Note

15 memo slots are available.

2-3 WEB / e-mail functions



The PrimeLAN board provides full access to the Prime system functions both via user and installer codes even when INIM software is not installed on the computer in use. An Internet connection is necessary either through a PC or the AlienMobile app for smartphones and tablets.

All Prime control panels equipped with the optional PrimeLAN board are capable of sending control-panel event associated e-mails.

The e-mail text, subject, attachments and recipients must be edited by your installer. For a description of a typical e-mail, refer to *paragraph 8-3-6 Partition status enquiry.*

In addition to e-mails, the PrimeLAN 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 PrimeLAN 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 8-3-6 Partition status enquiry*.

2-4 AlienMobile Application

INIM Electronics now offers Prime 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 Prime 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 PrimeLAN board.

It is the installer's task to prepare the control panel for direct connection to the devices which use the AlienMobile 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 regarding use and access to the system via AlienMobile, refer to the application manual.

Inim Cloud 2-5

The INIM Electronics Cloud service provides Prime system users with a further method 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.

No network programming is required on the Prime network boards, as these boards are programmed by default with the DHCP enabled (option that allows to automatically assign an IP address to the devices on the network).

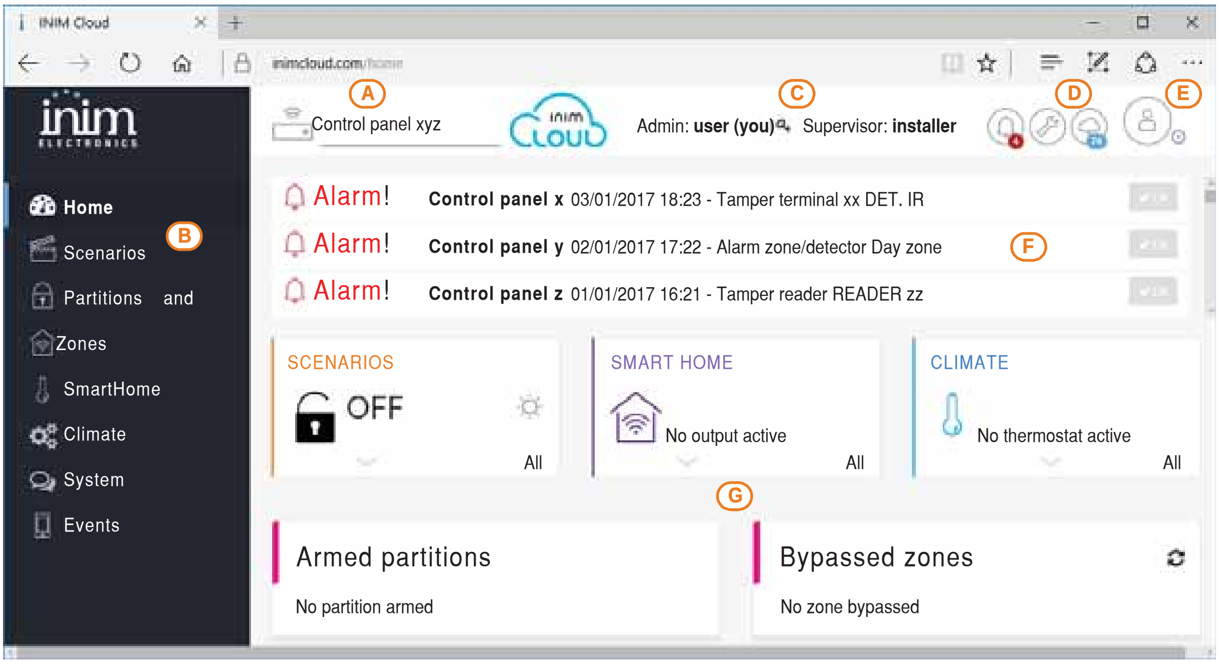
In order to allow use of the Cloud service, the user must have their own account at www.inimcloud.com, registered as“User”.

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 2-1: 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
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



Admin: **user (you)** Supervisor: **installer**

Alarm! **Control panel x** 03/01/2017 18:23 - Tamper terminal xx DET. IR

Alarm! **Control panel y** 02/01/2017 17:22 - Alarm zone/detector Day zone

Alarm! **Control panel z** 01/01/2017 16:21 - Tamper reader READER zz

SCENARIOS: OFF — All

SMART HOME: No output active — All

CLIMATE: No thermostat active — All

Armed partitions: No partition armed

Bypassed zones: No zone bypassed

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. Changes to the data of a control panel can be made by clicking-on and unlocking the respective 🔒. icon.

In order to use the Inim Cloud services, registration must be carried out also by the user.

For registration of an installation and use of the Cloud service refer to the Inim Cloud user manual.

Videosurveillance 2-6

The PrimeLAN board provides support for JPEG and MJPEG streams for surveillance cameras and allows users to retrieve and view video recordings and snapshots.

The Prime 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.

2-7 Versatility of the Prime system

Prime control panels, in addition to the traditional functions typical of an intrusion detection system, provide users with additional accessory functions, which do not necessarily concern the scope of intrusion control, such functions provide for the use of devices alternative to those available.

For example, it is possible to schedule switching ON/Off of lights at specific times; chronothermostat functions; access to control functions; Arm and Disarm operations via buttons and also program actions that follow a logical sequence of events/situations and much more.

Therefore, the manufacturer suggests that you contact your installer and request the possibility to evaluate the feasibility of these options

Prime users

Chapter 3

User Codes

3-1

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 user code n. 1 is "0001" at default. The PINs of the successive user codes are "0002", "0003", etc. up to "0050" for the Prime060S and Prime060L control panel models and "0100" for Prime120L and Prime240L.

Note

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 code 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 **way of accessing the user menu**.
  Each User code can access its customized menu in 3 different ways (refer to *paragraph 3-2 Methods 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 entry of a valid PIN on the telephone keypad the user can activate the required shortcut (refer to *paragraph 4-2 Shortcut with code*). This method of entering commands will affect the code partitions only.
- **Time restriction of code operability**
  If a code is associated with one of the timers, it will be able to operate the system only when the timer is On.
- **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 has access to (refer to *paragraph 3-2 Methods of accessing the user menu, Mode A*).
- **Customized shortcuts**.
  Each code can be programmed to manage:
    - up to 12 customized shortcuts assigned to keys F1 Fn, ..., F4 POL
    - up to 10 customized shortcuts assigned to keys 0 ␣, ..., 9 wxyz
      These shortcuts are available to the code user only after accessing the user menu.

3-2 Methods of accessing the user menu

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 the **OK** button.

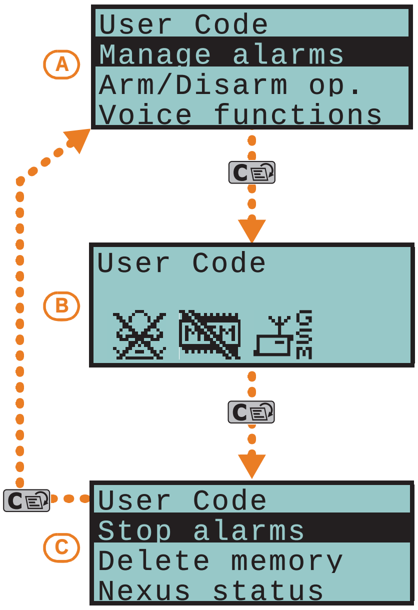
FIXED LENGTH

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

At this point, there are 3 different methods that allow first access to the user menu, depending on how the system has been programmed, as follows:

METHOD A

The user accesses the user menu directly:



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

The user can select the desired option from the menu by means of buttons ▲ and ▼ and by pressing the **OK** button.

METHOD B

The keypad deletes the icons of the shortcuts assigned to buttons F1 Fn, ..., F4 POL and replaces them with the icons that relate to the personal shortcuts of the code.

The user can activate the desired shortcut selected from those set on buttons F1 Fn, ..., F4 POL and 0 ␣, ..., 9 wxyz.

METHOD C

The user can access a descriptive menu of the customized shortcuts assigned to buttons F1 Fn, ..., F4 POL. To activate the shortcut, the user must first select the description of the required shortcut, by means of buttons ▲ and ▼, then press **OK**.

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

3-3 Multi-system access

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.

Shortcuts

Chapter 4

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 divided into three categories:

- immediate command shortcuts, which activate functions instantly
- service shortcuts, that provide direct access to Prime system data
- direct access shortcuts, that provide direct access to sections of the user menu on the keypad

They can be activated by the user or by the occurrence (activation) of an event.

The method of activation of a shortcut depends on the device being used (keypad with LCD display, code typed-in at a keypad or remotely via telephone, reader, key or wireless key) and the category it belongs to.

Table 4-1: Shortcut list

Shortcut			on keypad			on code		on reader	on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over-the-phone			
Arm / Disarm	Applies a pre-set scenario	which scenario	1		`Arm/Disarm`	Available	Available	Available	Available	Available Activate scenario
Stop alarms	Immediately deactivates the outputs relating to alarm and tamper events		2		`Stop alarms`	Available	Available	Available	Available	Not available
Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).		3		`Clear call queue`	Available	Available	Available	Available	Not available
Delete memory	Implements a “Stop alarms” operation and at the same time deletes memory of system and partition alarm and tamper events.		4	MEM	`Delete memory`	Available	Available	Available	Available	Available
Activate output	Activates one of the programmed outputs.	which output	5		`Activate Output`	Available	Available	Available	Available	Available
Deactivate output	Deactivates one of the programmed outputs.	which output	6		`Deactiv. output`	Available	Available	Available	Available	Available
Overtime	Delays auto-arming time of partitions by 30 minutes.		7		`Overtime`	Available	Available	Available	Available	Not available
Teleservice request	Sends a call to the Installer company number (Teleservice number).		8		`Teleservice req.`	For future use	For future use	For future use	For future use	Not available
StartVoiceNotifier	Plays a recorded voice message which announces the shortcuts assigned to the number keys.	User code	9		`Voice menu`	Available (only for number keys)	Available	Not available	Not available	Not available
Listen-in	Allows listen-in over-the-phone by means of a keypad microphone.	Keypad	10		`Listen-in`	Not available	Available	Not available	Not available	Not available
Intercom Call	Accesses the user menu section: Voice functions/intercom Call		11		`Intercom Call`	Available	Not available	Not available	Not available	Not available
Arm / Disarm menu	Accesses the user menu section: Arm/Disarm		12		`Arm/Disarm menu`	Available	Not available	Not available	Not available	Not available
Alarm management menu	Accesses the user menu section: Manage alarms		13		`Alarm menu`	Available	Not available	Not available	Not available	Not available
Voice functions menu	Accesses the User Menu section: Voice functions		14		`Voice func. menu`	Available	Not available	Not available	Not available	Not available

Table 4-1: Shortcut list

Shortcut			on keypad			on code		on reader	on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over-the-phone			
Activations menu	Accesses the user menu section: Activations		15		`Activations menu`	Available	Not available	Not available	Not available	Not available
Nexus status menu	Accesses the user menu section: View/Nexus status		16		`Nexus status menu`	Available	Not available	Not available	Not available	Not available
Arming status	Provides voice information regarding the armed/disarmed status of the partitions.		17		`Arming status`	Available	Available	Not available	Not available	Not available
Keypad settings	Accesses the user menu section: Keypad settings		18		`Keypad sett.menu`	Available	Not available	Not available	Not available	Not available
Zone activations menu	Accesses the user menu section: Activations/Zones		19		`ZoneBypass menu`	Available	Not available	Not available	Not available	Not available
Voice memo	Accesses the User Menu section: Voice functions		20		`Voice memo`	Available	Not available	Not available	Not available	Not available
ON/OFF output menu	Accesses the user menu section: Outputs ON/OFF		21		`Output control`	Available	Not available	Not available	Not available	Not available
Enable/Disable answerphone	Accesses the user menu section: Activations/Answerphone		22		`Enab.answerphone`	Available	Not available	Not available	Not available	Not available
Enable teleservice	Accesses the user menu section: Activations/Teleservice		23		`Enab.teleservice`	For future use	Not available	Not available	Not available	Not available
Enable codes	Accesses the user menu section: Activations/Codes		24		`Enable codes`	Available	Not available	Not available	Not available	Not available
Enable keys	Accesses the user menu section: Activations/Keys		25		`Enable keys`	Available	Not available	Not available	Not available	Not available
Enable timers	Accesses the user menu section: Activations/Timers		26		`Enable timers`	Available	Not available	Not available	Not available	Not available
Enable auto-arming	Accesses the user menu section: Activations/Auto-arming		27		`Enab. auto-arm`	Available	Not available	Not available	Not available	Not available
View events log	Accesses the user menu section: View/Events log		28		`View events log`	Available	Not available	Not available	Not available	Not available
View alarms log	Accesses the user menu section: View/Alarms log		29		`View alarm log`	Available	Not available	Not available	Not available	Not available
View faults log	Accesses the user menu section: View/Faults log		30		`View faults log`	Available	Not available	Not available	Not available	Not available
View arm/disarm operations	Accesses the user menu section: View/Arm/Disarm op.		31		`View arm ops log`	Available	Not available	Not available	Not available	Not available
View system status	Accesses the user menu section: View/System status		32		`ViewSystemStatus`	Available	Not available	Not available	Not available	Not available
View zone status	Accesses the user menu section: View/Zone status		33		`View zone status`	Available	Not available	Not available	Not available	Not available
Change PIN code	Accesses the user menu section: Change PIN		34		`Change PIN`	Available	Not available	Not available	Not available	Not available
Time/Date	Accesses the user menu section: Keypad date/time		35		`Time/Date`	Available	Not available	Not available	Not available	Not available
View faults	Accesses the user menu section: View / Faults ongoing		36		`View faults`	Available	Not available	Not available	Not available	Not available
Thermostat menu	Accesses the user menu section: Thermostat		37		`Thermostat menu`	Available	Not available	Not available	Not available	Not available
Panic	Activates a “Panic” event	which panic event	38	PANIC	`Panic`	Available	Available	Available	Available	Not available
Zone bypass	Bypasses one of the configured zones	which zone	Not available			Not available	Not available	Not available	Not available	Available
Unbypass zone	Unbypasses one of the configured zones	which zone	Not available			Not available	Not available	Not available	Not available	Available

Table 4-1: Shortcut list

Shortcut			on keypad			on code		on reader	on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over-the-phone			
Disable code	Disables one of the configured codes	which code	Not available			Not available	Not available	Not available	Not available	Available
Enable code	Enables one of the configured codes	which code	Not available			Not available	Not available	Not available	Not available	Available
Disable key	Disables one of the configured keys	which key	Not available			Not available	Not available	Not available	Not available	Available
Enable key	Enables one of the configured keys	which key	Not available			Not available	Not available	Not available	Not available	Available
Activate thermostat	Activates the thermostat of one of the keypads in the selected operating mode	Keypad which mode	Not available			Not available	Not available	Not available	Not available	Available
Deactivate thermostat	Deactivates the thermostat of one of the keypads	Keypad	Not available			Not available	Not available	Not available	Not available	Available
Dimmer up	Increases the voltage value on a dimmer output by 5%	which output	Not available			Not available	Not available	Not available	Not available	Available
Dimmer down	Decreases the voltage value on a dimmer output by 5%	which output	Not available			Not available	Not available	Not available	Not available	Available

Keypad shortcuts

The installer can program each LCD keypad with up to 12 shortcuts associated with 4 function keys F1 Fn F2 F3 F4. 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 in cases when there are more than 4 function keys.

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

A- **By ALL**.
Pressing the respective key F1 Fn, ..., F4 will activate the shortcut instantly without code entry. The shortcut will affect all the keypad partitions.

B- **By ALL with confirmation request**.
Pressing the respective key F1 Fn, ..., F4 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 C or Esc the operation will be abandoned. This method protects against accidental operations. The shortcut will affect all the keypad partitions.

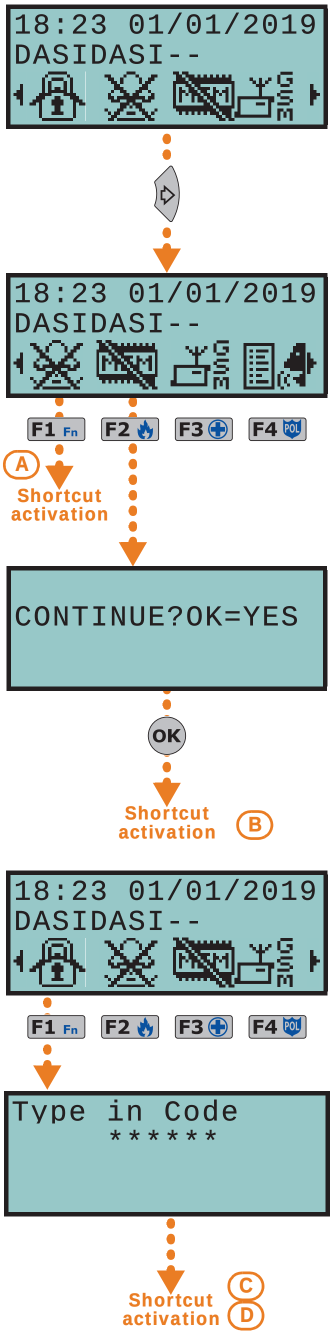
C- **Code users only**.
After pressing the respective key F1 Fn, ..., F4, a valid code entry will be required, the shortcut will activate after code recognition. The shortcut will affect the partitions common to both the keypad and code.

D- **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 that is associated with the shortcut icon: F1 Fn, ..., F4. The system will either activate the shortcut instantly (case *A*), or will request explicit confirmation (case *B*), or will request code entry (cases *C* and *D*).

Alien user interfaces do not have function keys F1 Fn F2 F3 F4, 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 6-7 Operations via an Alien keypad*.

4-1



4-2 Shortcut with code

Besides the keypad shortcuts provided by keys F1 Fn F2 F3 F4 POL, 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 3-2 Methods of accessing the user menu*). Each code can be programmed to manage:

- Up to 12 shortcuts can be activated by keys F1 Fn, ..., F4 POL and identified by explicit icons.
- Up to 10 shortcuts can be activated by keys 0 ␣, ..., 9 wxyz. If a code is enabled to operate the system over-the-phone, these shortcuts will also be available on the telephone number-keys.

Via keypad

1. Validating your PIN
2. Access the user menu, using the method described in *paragraph 3-2 Methods of accessing the user menu*, Method B.
3. Press the key F1 Fn, ..., F4 POL which corresponds to the shortcut icon or press the key 0 ␣, ..., 9 wxyz which is assigned to the shortcut.

FIXED LENGTH

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.

Over-the-phone

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

4-3 Key and Reader shortcuts

4-3-1 nBy/S and nBy/X Reader shortcuts

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 7-2: 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.

READER LED OFF

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.

Shortcuts on keypad integrated readers 4-3-2

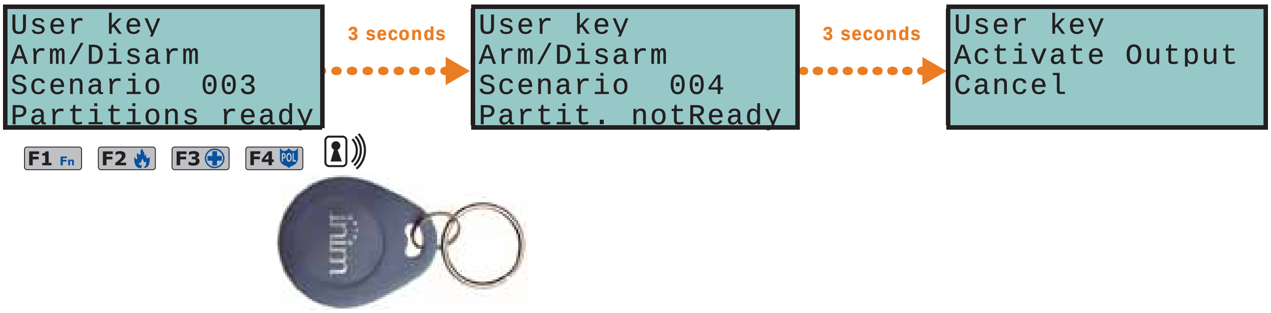
Users must hold their digital keys in the vicinity of the integrated reader (the position of the reader is indicated by the ⓘ symbol, instead, on the Alien keypad it is positioned on the lower right-hand corner of the frontplate).

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 key shortcut for 3 seconds
6. The “Disarm” string, to disarm all the partitions
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.



```
User key
Arm/Disarm
Scenario  003
Partitions ready
```

```
User key
Arm/Disarm
Scenario  004
Partit. notReady
```

```
User key
Activate Output
Cancel
```

Remote-control shortcuts 4-3-3

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 7-3: Feedback signals provided by wireless keys*).

Shortcut on event 4-4

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 Prime control panel by the installer and cannot be implemented by the user.

Chapter 5 Using the Prime system

The Prime system can be accessed in the following ways:

- via **keypad with a display (LCD)** (**Joy**, **Aria**, **nCode/G**, **Concept/G**).
  In which case the user can operate the system in two ways:
  - through shortcuts (refer to *paragraph 4-1 Keypad shortcuts*);
  - through the user code/menu (refer to *paragraph 3-2 Methods of accessing the user menu*).

  Refer to *paragraph 6-6 Operations from LCD keypads*.
- Via **Alien keypad**
  in this case, the display provides the user with buttons, that with a single tap activate functions and applications. For further details refer to *paragraph 6-7 Operations via an Alien keypad*.
- Via **proximity reader** (**nBy/S**, **nBy/X**, built into the keypad)
  in this case it is necessary to use a valid key and there is only one way of accessing the system, as described in *paragraph 7-3 Reader and key operations*.
- Via **telephone**
  during a call from/to the control panel itself or via an SMS message and valid code entry (PIN).

  Refer to *paragraph 8-3 Operations via telephone*.
- Via **remote-control device**
  by pressing keys **F1**, ..., **F4**, as described in *paragraph 7-2-1 Wireless keys (remote-control keys)*.
- Via **Web**
  by means of the integrated web-server on the PrimeLAN board (if installed) through any browser (refer to *paragraph 9-2 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).
- Via **Inim Cloud**
  by means of a browser, the user can access a customized web interface which provides all the registered control panels.

5-1 Managing alarms

The Prime control panel will signal an alarm if one of the following events occurs:

- Zone alarm, when violation of a zone is detected.
- Zone tamper, when tamper (opening, dislodgement or delinquency) is detected on a device that is connected to the terminals
- Peripheral tamper, when tamper (opening, dislodgement or delinquency) is detected on one of the devices connected to the BUS (keypad, reader, expansion, sounder, GSM communicator)
- Peripheral loss, when communication between the system and a peripheral device connected to the BUS stops suddenly
- Control panel tamper, when tamper (opening, dislodgement or delinquency) is detected on the control panel itself

In each of the following cases, the control panel will start the programmed alarm signalling such as the activation of outputs, sounders, the sending of messages (SMS, email, push notifications) or telephone calls.

These events will be saved to the events log.

The typical operations the user must perform in the event of alarms and/or tamper conditions are:

- Stop the ongoing alarms by deactivating the outputs related to the system alarm and tamper events.
- Cancel the entire call queue and stop ongoing calls (if any).
- Delete the alarm and tamper memories.

These operations can be carried out through:

- LCD Keypad (*paragraph 6-6-1 Alarm management*)
- Alien keypad (*paragraph 6-7-2 Alarm management*
- Proximity readers (*paragraph 7-3-1 Alarm management*)
- Keyfobs (*paragraph 7-3-1 Alarm management*)
- Telephone (*paragraph 8-3-1 Alarm management*)
- Web browser (*paragraph 9-3-1 Alarm management*)
- AlienMobile Application
- InimCloud

Arming and disarming partitions 5-2

The operating status of partitions can be changed by users who are authorized to access them.

Through the appropriate user access sections for Prime system management, it is possible to request the following commands:

- **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 perimeter zones only and annuls delays. In this way, all the perimeter zones of the partition will generate instant alarms.
- **Hold** - this operation forces the partition to hold its current status.

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.

Note

When arming partitions, all the zones must be in stand-by status (not violated) and no faults must be present.

Arming the system when zones are violated or faults are present 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").

Appropriate programming of the control panel can however prevent the arming of partitions in the presence of causes of reduced security.

These operations can be carried out through:

- LCD Keypad (*paragraph 6-6-2 Arming commands and scenarios*)
- Alien keypad (*paragraph 6-7-3 Arming commands and scenarios*
- Proximity readers (*paragraph 7-3-2 Arming commands and scenarios*)
- Keyfobs (*paragraph 7-3-2 Arming commands and scenarios*)
- Telephone (*paragraph 8-3-2 Arming commands and scenarios*)
- Web browser (*paragraph 9-3-2 Arming commands and scenarios*)
- AlienMobile Application
- InimCloud
- Auto-arm

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 (refer to *paragraph 5-5 Activations*). Users who are authorized to control Auto-arm operations must:

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

5-3 Arming scenarios

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

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.

These operations can be carried out through:

- LCD Keypad (*paragraph 6-6-2 Arming commands and scenarios*)
- Alien keypad (*paragraph 6-7-3 Arming commands and scenarios*
- Proximity readers (*paragraph 7-3-2 Arming commands and scenarios*)
- Keyfobs (*paragraph 7-3-2 Arming commands and scenarios*)
- Telephone (*paragraph 8-3-2 Arming commands and scenarios*)
- Web browser (*paragraph 9-3-2 Arming commands and scenarios*)
- AlienMobile Application
- InimCloud

5-4 Voice memo and intercom functions

The user can access the voice functions exclusively via keypads equipped with a speaker and microphone.

The functions are:

- Recording of a message in the memo-box of the keypad you are working on.
- The playback of the message in the memo-box of the keypad you are working on.
- The deletion of the message in the memo-box of the keypad you are working on.
- Voice communication with another keypad.

RECORD / PLAYBACK

The operation time-out (expressed in seconds) will be signalled by a counter and a progress bar on the display. If you wish to stop the record/playback operation manually, press **OK**, otherwise, it will end automatically when the pre-set time-out expires.

DELETE

This operation must be confirmed by pressing **OK**.-

INTERCOM CALL

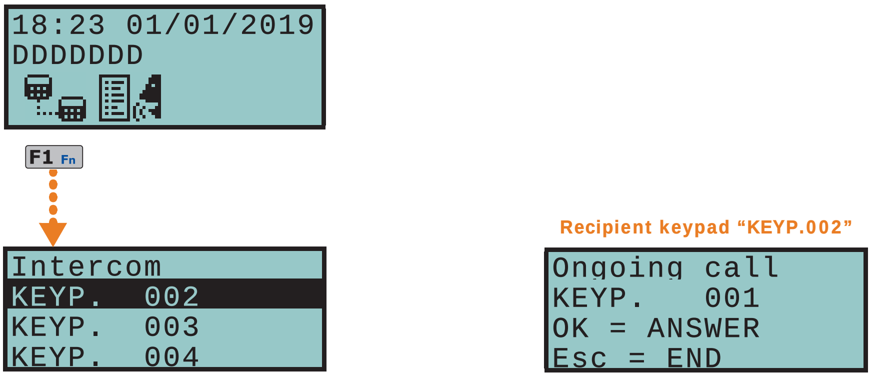
Voice communication during keypad-to-keypad intercom calls is one-way, therefore, only one person can speak while the other listens. The user who wishes to speak must activate the intercom function on the keypad they are using.

The display shows a list of the keypads the user can communicate with; select the desired keypad then press **OK** to start the call.

The buzzer on the selected keypad will signal the incoming call. The call recipient can press**OK** to answer the call or **Esc** to reject it.

Both the caller and the call recipient can end the call by pressing **Esc**.

Caller keypad "KEYP.001"



```
18:23 01/01/2019
DDDDDDD
```

```
Intercom
KEYP.   002
KEYP.   003
KEYP.   004
```

Recipient keypad "KEYP.002"

```
Ongoing call
KEYP.    001
OK = ANSWER
Esc = END
```

These operations can be carried out through:

- LCD Keypad (*paragraph 6-6-3 Voice memo and intercom functions*)
- Alien keypad (*paragraph 6-7-4 Voice memo and intercom functions*

Activations 5-5

The activation (and deactivation) of the various elements of the Prime system allows them to operate normally in accordance with their programming (= activation) or disable their functions completely (= deactivation).

The user can activate or deactivate the following elements:

- **Zone** - deactivated (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 3-1 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.

Note

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.

- **Dialer** - a deactivated (disabled) dialer cannot send voice or digital calls. However, if duly programmed, it will be able to manage incoming calls.
- **PSTN/GSM Answerphone** - if activated (enabled), the control panel will answer incoming calls (on the PSTN landline and GSM network) with the prerecorded "Answerphone" message.
- - If activated (enabled), the Installer PIN will be accepted by the system and the installer will have access to the Installer menu. If deactivated (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 (enabled), the control panel will send a specific string to the IP2RX software in order to allow its identification.
- **Registration**- this section allows the Prime panel to access INIM Electronics cloud service.

The activations of the elements can be carried out from:

- LCD Keypad (*paragraph 6-6-4 Activations*)
- Alien keypad (*paragraph 6-7-5 Activations*
- Web browser (*paragraph 9-3-3 Viewing and activations*)
- AlienMobile Application
- InimCloud

Outputs management 5-6

The user can activate/deactivate manually the outputs the user code in question is authorized to work on.

It is possible to activate/deactivate low-power open-collector or relay outputs and view their status by means of the respective icons.

It is possible to activate/deactivate high-power relay outputs and view their supplied voltage and relative power factor (cosφ).

It is possible to view the supplied voltage of dimmer outputs.

The activations of the outputs can be implemented via:

- LCD Keypad (*paragraph 6-6-6 Outputs management*)
- Alien keypad (*paragraph 6-7-7 Outputs management*
- Proximity readers (*paragraph 7-3-3 Outputs management*)

- Keyfobs (*paragraph 7-3-3 Outputs management*)
- Telephone (*paragraph 8-3-3 Activation of outputs*)
- Web browser (*paragraph 9-3-3 Viewing and activations*)
- AlienMobile Application
- InimCloud

5-7 Change code PIN

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 3-1 User Codes*).

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

This operation can be done through:

- LCD Keypad (*paragraph 6-6-9 Change code PIN*)
- Alien keypad (*paragraph 6-7-10 Change code PIN*

5-8 Change telephone numbers

Users can edit the contact numbers used by the dialer of the Prime control panel.

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

This operation can be done through:

- LCD Keypad (*paragraph 6-6-10 Edit telephone numbers*)
- Alien keypad (*paragraph 6-7-11 Edit telephone numbers*

5-9 Overtime request

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

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

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

This operation can be done through:

- LCD Keypad (*paragraph 6-6-11 Overtime request*)
- Alien keypad (*paragraph 6-7-12 Overtime request*
- Proximity readers (*paragraph 7-3-4 Overtime request*)
- Keyfobs (*paragraph 7-3-4 Overtime request*)
- Telephone (*paragraph 8-3-4 Overtime request*)

5-10 Thermostat

The "thermostat" function of Prime control panels makes it possible to manage boilers or air conditioners via keypads equipped with thermometers.

There are two operating modes:

☀ ☀

- **Summer / Air-Conditioning**
  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 of the day for 7 days per week.
- **Weekly** - the temperature set by the user is valid during the selected hours of the day 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.

This function can be managed from the:

- LCD Keypad (*paragraph 6-6-12 Thermostat*)
- Alien keypad (*paragraph 6-7-13 Thermostat*
- AlienMobile Application
- InimCloud

Listen-in 5-11

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 the installer) to one of the number keys relating to the code that will generate this operation (refer to *paragraph 8-3-5 Listen-in*).

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

Partition status enquiry 5-12

During a telephone communication with the control panel or by accessing a keypad with an LCD display with voice functions, the user can listen to the status of arming/disarming the partitions.

The control panel will announce the armed/disarmed status of the partitions the entered PIN is assigned to.

This operation can be implemented through:

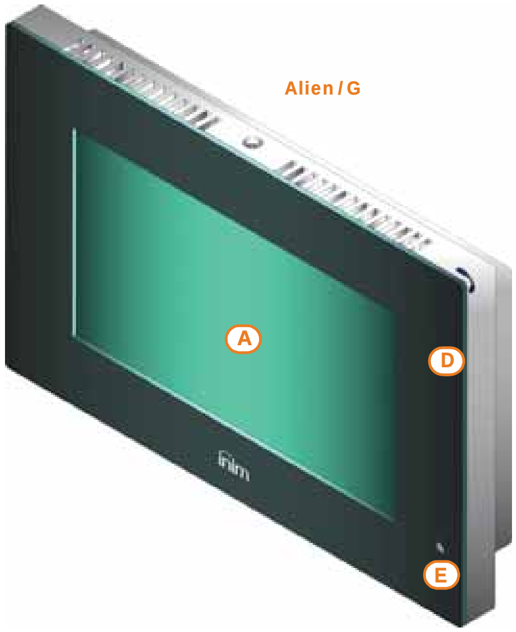
- LCD Keypad (*paragraph 6-6-15 Partition status enquiry*)
- Telephone (*paragraph 8-3-6 Partition status enquiry*)

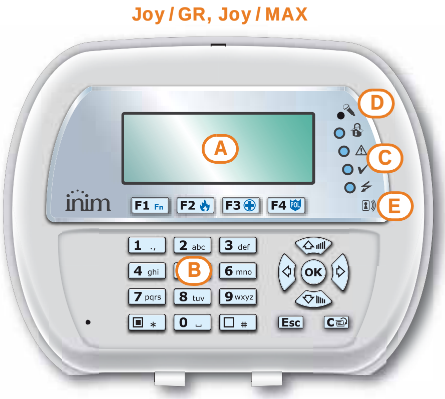
Chapter 6 Keypads

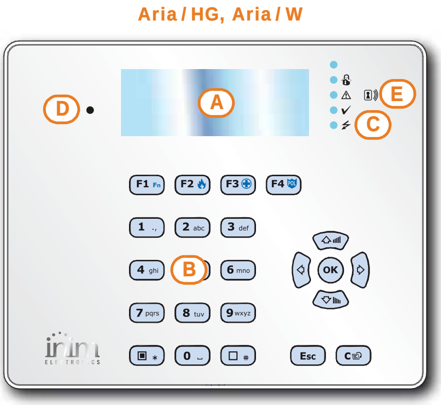
The various keypad models can be distinguished by their functions, external design and accessibility to the keys. These features are indicated in the following table:

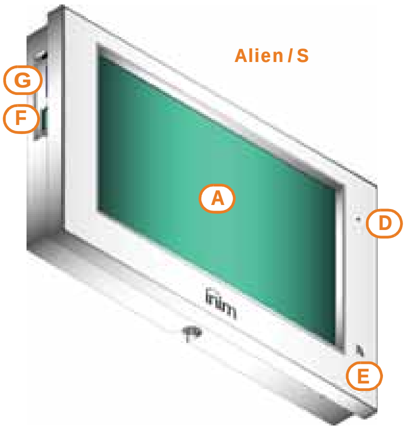
Table 6-1: Keypads - functions

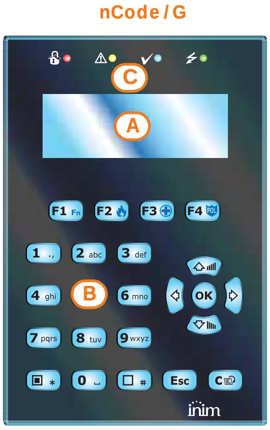
Models		Joy/MAX	Joy/GR	Aria/HG	Aria/W	nCode/G	Concept/G	Alien/S	Alien/G
A	Graphic display	LCD 96x32						65536 colour touch screen	
								4.3 inches 480x272	7 inches 800x480
B	Keys	23 (in soft rubber)					23 (touch)	No	
C	Signalling LEDs	4						No	
D	Microphone	Yes	No	Yes	No			Yes	
E	Built-in proximity reader	Yes	No	Yes	No			Yes	
F	USB port	No						Yes	
G	SD card	No						Max. 32 GByte	
	Buzzer	Yes							
	Terminals	2			No	1		No	2
	Speaker	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		

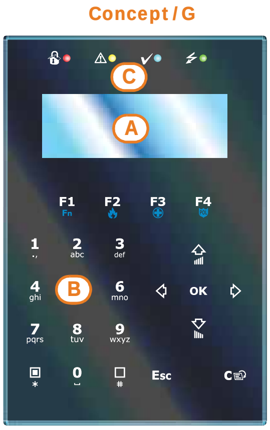












The keypad is the most complete and versatile device for system management.

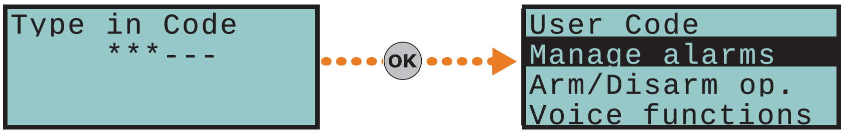
For each keypad the installer assigns the partitions it belongs to and the sections of the system that user codes can access through it.

The graphic display shows the necessary information and provides a user-interface based on a user menu and icons for the operations to be performed.

ACCESSING THE KEYPAD

Each user, who enters a valid PIN code on the keypad that is recognized by the control panel, can be enabled to operate on the system or on part of it.

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 the **OK** button.



```
Type in Code
     ***---
```

```
User Code
Manage alarms
Arm/Disarm op.
Voice functions
```

SHORTCUT

It is possible to extend the use of some of the system shortcuts to users without assigned codes.

By means of the keypads it is possible to use the shortcut functions associated with the keys F1 Fn F2 F3 F4, these operations are usually reserved for authorized users (users with assigned codes).

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.

CHRONO-THERMOSTAT

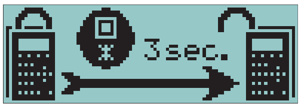
If a keypad is equipped with a thermostat, it can also be programmed to control the programmable chronothermostat function. This function allows you to set up zone management (one zone per keypad) of the heating/air-conditioning system.

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

CONCEPT/G

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.

WIRELESS TERMINALS

The Aria/W wireless keypad provides all the necessary functions for the control and management of a Prime installation equipped with an Air2 system, which it can interface with through the Air2-BS200 transceiver.

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.

BACKLIGHTING

The backlight of Air/W keypads can be programmed from the keypad in accordance with the measured ambient brightness. The keypad manages two different brightness settings:

- Day
- Night

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

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

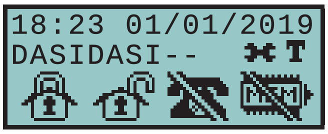
Graphics management provides ample room for customization, with skin and background selection and image rotation. You can also control the screen brightness, contrast and image transparency.

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 Prime control panel through a graphic layout containing images, icons and buttons on the display
- alarm and memo functions, programmable directly by the user, which generate audible signals and display popups

6-1 Keypad displays

6-1-1 LCD keypad

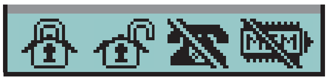

18:23 01/01/2019
DASIDASI-- ✖ T

The screens of LCD keypads (96 x 32 pixel) are backlit, it is possible to adjust the screen brightness and contrast via the respective options on the user menu (refer to *paragraph 6-6-8 Keypad settings*).

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

- **Stand-by** - indicates the control panel is functioning normally and there are no alarm, tamper of fault events present on the system.
- **Alarm** or **Zone tamper** - indicates that the control panel has detected trouble on a zone, such as zone violation (intrusion) or detection of a lost device
- **Maintenance** - indicates that the control panel is in maintenance mode for repair or programming purposes

Table 6-2: Display visualization

<table>
<tr><th rowspan="2">Line</th><th colspan="3">Control panel status</th></tr>
<tr><th>Stand-by</th><th>Alarm or tamper</th><th>Maintenance</th></tr>
<tr><td rowspan="3">1</td><td>18:23 01/01/2019
The first line of the display shows the date and time.</td><td rowspan="2">Panel T03
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.
Note
Open zones are signalled by blinking on the red LED . 🔒</td><td>K03 Service
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).</td></tr>
<tr><td>18:23 PM 25.4°
If the keypad is equipped with a thermostat, the date and room temperature will alternate on the screen every 3 seconds.</td><td>Mainten K03 P05
If you are using a keypad with an integrated proximity reader, the string will also show the address of its reader (in the figure, the reader is at address 5).</td></tr>
<tr><td>Panel T03
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.
Panel T03
Any auto-bypassable zones will be shown in white on black background.</td><td colspan="2">Panel T03
Mainten K03 P05
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.</td></tr>
<tr><td rowspan="2">2
left</td><td>DASIDASI--
The left side of the second line shows the characters that indicate the current status of the partitions the keypad is assigned to:
• D = partition disarmed
• A = partition armed in Away mode
• S = partition armed in Stay mode
• I = partition armed in Instant mode
• - = partition does not belong to the keypad
In the case of the Prime060S and Prime060L, the display will show 10 characters indicating the status of partitions 1 to 10.
In the case of the Prime120L and Prime240L, the display will show 10 characters, which alternate at 3 second intervals, indicating the status of partitions 1 to 10 and then 5 characters indicating the status of partitions 11 to 15.</td><td>DASIDASI--
D SIDASI--
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. 🔒</td><td>The line is the same as when the control panel is in standby condition.</td></tr>
<tr><td colspan="3">SCENARIO 001
If the “Show scenario” control panel parameter is active, the left side of the second line on the screen will display the current scenario.</td></tr>
<tr><td>2
right</td><td colspan="3">DASIDASI-- ✖ T
On the second line, on the right side, you can see several icons which provide system information.
For a detailed description of these icons refer to <i>Table 6-4: Information icons</i>.</td></tr>
<tr><td>3
4</td><td colspan="3">
Lines three and four on the display are occupied by the icons which correspond to the shortcuts assigned to function keys F1 Fn , ..., F4 .
If no shortcuts are programmed on the keypad function keys, the respective spaces on the display will remain empty.</td></tr>
</table>

Note

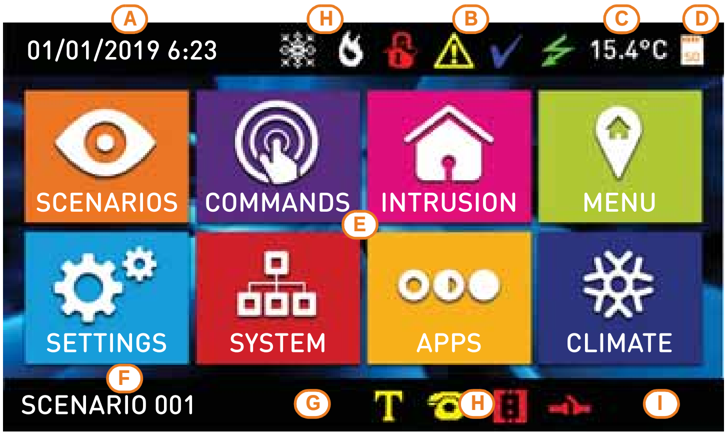
What appears on the display of Air/W keypads as the flashing of the characters that indicate the operating statuses of the partitions, is not actually true flashing but is in fact the solid negative image of the characters themselves.

The Alien keypad screen 6-1-2

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 6-3: Alien - screen

A	Data and Time of the Prime control panel. If the control panel is in Service status, this field will show the address of the Alien and its built-in reader.	 A H B C D 01/01/2019 6:23 15.4°C SCENARIOS COMMANDS INTRUSION MENU E SETTINGS SYSTEM APPS CLIMATE F SCENARIO 001 G H I
B	Keypad LED icons (*Table 6-7: Keypad LEDs*).	
C	Temperature read by the thermometer of the Alien user interface.	
D	Icon which indicates the presence of an SD card in the card slot. After entering a valid user code, the **Logout** that appears will allow you to close the session.	
E	Section for the active functions, with buttons for access to the Alien user interface, to its applications and to the Prime system. The home page of the Alien/S (shown in the figure) shows the function buttons indicated in *Table 6-19: Alien keypad menu*. In the Alien/G, these buttons are shown in a section on the left and are always visible regardless of the active function.	
F	String showing the arming status of the control panel, in accordance with the active scenario or status of the partitions. If a partition to which the keypad belongs changes its status with respect to what is programmed for the active scenario, or in the event that the control panel enters maintenance mode, this string will show the characters relating to the status of the partitions, as described in *Table 6-2: Display visualization*.	
G	Tapping this section on the display opens (for 3 seconds) a window containing a list of the active scenarios. If required by programming (*paragraph 6-6 Operations from LCD keypads*), it may request entry of a valid code.	
H	System information icons, as described in *Table 6-4: Information icons*.	
I	If you are inside a section, this field will show the following buttons which may cover the information buttons: • **Prev. level** This key allows you to step back to the previously active function. • **Home page** 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 6-7-1 Alien function keys*).

POP-UP

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 the code and keypad in use have in common
  - the **Stop alarms** button, to deactivate the outputs activated by the alarm signal
  - **Clear call queue** button, to cancel the calls in the outgoing call queue
  - the **Home** button to access the home page directly
- 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 the code and keypad in use have in common
  - the **Scenarios** button, to access the scenarios available for activation
  - the **Home** button to access the home page directly
- **Keypad locked**,icon which appears when you tap the display and the keypad is locked due to 5 consecutive entries of an invalid code.
- **Reader locked**, icon which appears when you hold a key in the vicinity of a reader which has been locked due to 5 consecutive attempts to use an invalid key.

CLEANING THE DISPLAY

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

REBOOTING

Touching any part of the screen for 50 seconds will reboot the keypad.

6-1-3 Status icons on display

The icons that appear on the second line, on the right side of the LCD screen or on the top and bottom bars of the Alien display, provide system information, therefore, their appearance or status (fixed or flashing) depends on the status they must report:

Table 6-4: Information icons

Icon	Signalling	Joy, Aria/HG, nCode, Concept	Aria/W	Alien
Telephone line	Telephone line busy	T **Solid**		T **Solid**
	Telephone line down	T **Blinking**		T **Blinking**
Lost	At least one peripheral device is not responding	⊡ **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 (for future use)	✖ **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 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	A telephone call is in progress via the Nexus communicator	TY **Solid**		TY **Solid**
Sending SMS	An SMS text message is being sent through the Nexus/G dialer	SMS **Solid**		SMS **Solid**
LAN	A SIA-IP event report is being sent through the LAN	品 **Solid**		品 **Solid**
	The LAN board cannot be found	品 **Blinking**		品 **Blinking**
SIA-IP on Nexus	A SIA-IP event report is being sent through the Nexus	IPY **Solid**		IPY **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**

Note

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

Using the keys 6-2

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 6-5: The keypad keys

Keys	Name	Typical application
1 ., 2 abc 3 def 4 ghi 5 jkl 6 mno 7 pqrs 8 tuv 9 wxyz 0 ␣	**Number keys**	Used to type in User PINs
OK	**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	**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 **OK**, to scroll through the 3 user-menus (refer to *paragraph 3-1 User Codes*).
Esc	**ESC**	This key exits the user menu definitely without confirming any selected parameters, etc.
▣ *	**ENABLE**	This key enables options (refer to *paragraph 6-6-4 Activations*)
□ #	**DISABLE**	Disables options
F1 Fn F2 🔥 F3 ⊕ F4 POL	**F1, F2, F3, F4 or function keys**	These keys activate the shortcuts associated with the icons. They can also be used as Emergency keys (refer to *paragraph 6-2-1 Emergency functions*).

Emergency functions 6-2-1

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 an hold for 3 seconds the required key combination and wait for the confirmation beep, as follows:

Table 6-6: Emergency keys

Emergency	Key combinations	Alien keys
Fire	F1 Fn + F2 🔥	👁
Ambulance	F1 Fn + F3 ⊕	◎
Police	F1 Fn + F4 POL	🏠

Note

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.

6-3 Visual signals on the keypad LEDs

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 6-7: 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 (230V a.c.) is present
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 bypassed (disabled) or in Test status. PSTN or GSM communicator is disabled.	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 B, 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

FALSE KEY

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

HIDE STATUS

If “Hide status” 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 in question for 30 seconds. Additionally:

- 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

Signalling on the Buzzer 6-4

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 of enabled partitions. The activation these signals can be set up by means of the keypad options described in *paragraph 6-6-8 Keypad settings*.

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

Table 6-8: Signalling and types of signal

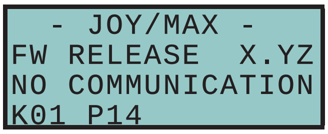
Signalling	Type of signal
Button pressed	Single pulse (beep)
Entry time running	8 pulses + 5 second pause
Exit time running	3 pulses + 5 second pause; 4 short pulses + 5 second pause during the final 20 seconds of the exit Time
Pre-arm time running	1 pulse + 5 second pause
Activation of the output connected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

Emergency status 6-5

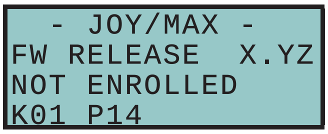
In the event of a keypad configuration or communication error between the system peripherals, the display will show one of the templates opposite.

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.



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



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

Operations from LCD keypads 6-6

Alarm management 6-6-1

The actions that can be performed from the keypad in the event of alarm and tamper events are:

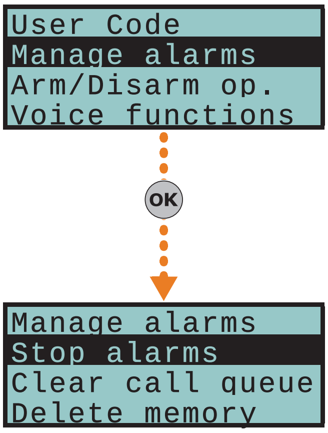
- Stop alarms
- Clear call queue
- Delete memory

The user can operate via the keypad in two ways:

- activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry:
- access the "Alarm management" section (in the user menu) by entering of valid PIN.

Table 6-9: Shortcut for the management of alarms from a keypad

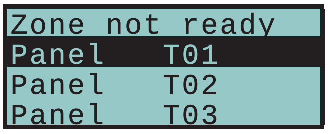
Shortcut			User menu section	Operation
Alarm management menu	**n.13**		Manage alarms	Access the section with the list of available operations.
Stop alarms	**n.2**		Stop alarms	Deactivates instantly the outputs activated by alarm and tamper events
Clear call queue	**n.3**		Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).
Delete memory	**n.4**		Delete memory	Performs a "Stop alarms" operation and, at the same time, deletes memory of system/ partition alarm and tamper events.



```
User Code
Manage alarms
Arm/Disarm op.
Voice functions
```

```
Manage alarms
Stop alarms
Clear call queue
Delete memory
```

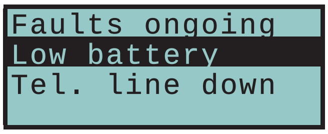
6-6-2 Arming commands and scenarios



```
Zone not ready
Panel    T01
Panel    T02
Panel    T03
```

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.



```
Faults ongoing
Low battery
Tel. line down
```

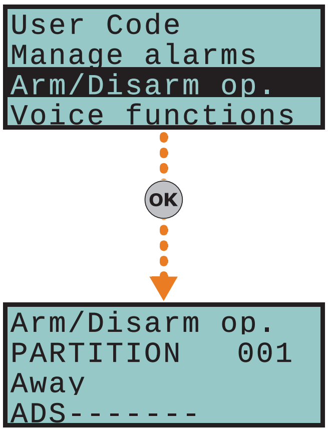
If you request an arm-partition command at a keypad (for one or more partitions) and conditions (programmed by the installer) which lower the security of the system are present, the keypad will provide a list of the conditions concerned, as shown in the figure opposite.

The user can scroll through the list to see the causes of reduced security, then decide whether or not to force the arming command.

The user can operate via the keypad in two ways:

- activate the shortcuts associated with keys F1 Fn, ..., F4 POL, shown on the display (with or without code entry) of the "Arm/Disarm" type (shortcut no. 1) that will apply the programmed 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.
- Access the "Arm/Disarm" section in the user menu. In this section it is possible to select the arm or disarm mode for each partition individually:



```
User Code
Manage alarms
Arm/Disarm op.
Voice functions
```

```
Arm/Disarm op.
PARTITION   001
Away
ADS-------
```

1. Select the desired partition, using keys ◁ and ▷.
2. Select the required operating mode for the selected partition, using keys △ and ▽.

- **"D"**, to disarm.
- **"A"**, to arm in Away mode (entire system armed)
- **"S"**, to arm in Stay mode (system partially armed).
- **"I"**, to arm in Instant mode (no delays)
- **"N"**, not to change the operating status.

3. Once you have set the arming modes on all the partitions, press **OK**.

ENTRY TIME WINDOW

If during the entry time a code is entered, and if the code is authorized to access the "Arm/Disarm" section of the user menu, the partitions common to the code and keypad will disarm immediately.

Table 6-10: Shortcut for Arm/Disarm partition operations from a keypad

Shortcut			User menu section	Operation
Arm/Disarm	**n.1**	🔒	/	Activate the scenario selected from those available.
Arm/Disarm menu	**n.12**	☰🔒	Arm/Disarm op.	Accesses the section containing the list of partitions which the user can access and change the operating status.

SHOW SCENARIO

If the control panel "Show scenario" (or "View scenario" on keypad) option is active, the left side of the second line on the screen will display the current scenario.

6-6-3 Voice memo and intercom functions

The voice functions available at the keypad are:

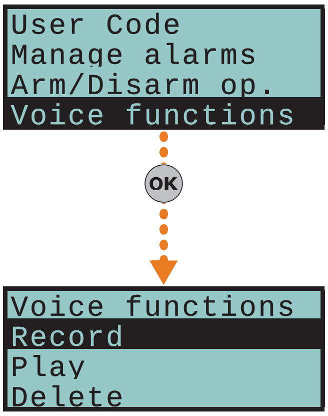
- Record message in the voice memo box
- Playback message in the voice memo box
- Delete message in the voice memo box
- Voice communication with another keypad.

The user can operate via the keypad in two ways:

- activate the shortcuts associated with keys F1 Fn, ..., F4 POL (shown on the display) with or without code entry.

- access the "Voice functions" section of the user menu by entering a valid PIN code.

You can adjust the volume during the playback phase using keys ⇧ and ⇩.


User Code
Manage alarms
Arm/Disarm op.
Voice functions

Voice functions
Record
Play
Delete

Table 6-11: Shortcut for voice function from a keypad

Shortcut			User menu section	Operation
Voice functions menu	**n.14**		Voice functions	Access the section with the list of available operations.
			Record	Record message in the voice memo box
			Play	Playback message in the voice memo box
			Delete	Delete message in the voice memo box
Intercom Call	**n.11**		Intercom	Intercom call

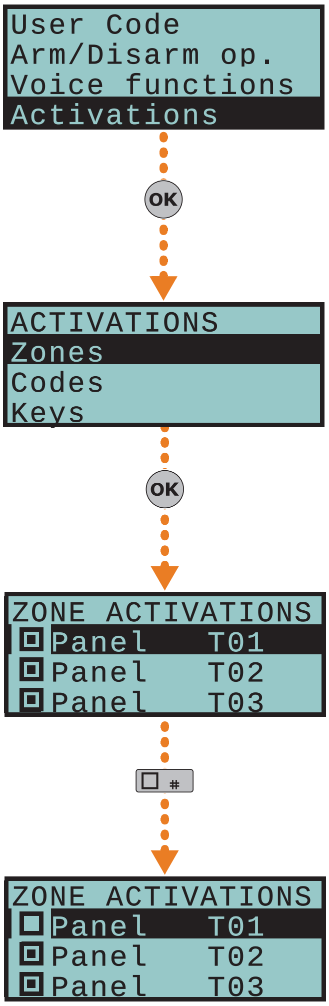
Activations

6-6-4

The user can implement activations via the keypad in two ways:

- activate the shortcuts associated with keys F1 Fn, ..., F4 (shown on the display) with or without code entry:
- access the "Activations" section of the user menu by entering a valid code PIN.

In this section it is possible to activate the selected element by means of the ▣ * button or deactivate it by means of the □ # button.


User Code
Arm/Disarm op.
Voice functions
Activations

ACTIVATIONS
Zones
Codes
Keys

ZONE ACTIVATIONS
▣Panel T01
▣Panel T02
▣Panel T03

ZONE ACTIVATIONS
□Panel T01
▣Panel T02
▣Panel T03

Table 6-12: Shortcut for activations from a keypad

Shortcut			User menu section	Operation
Activations menu	**n.15**		Activations	Access the section with the list of available elements.
Zone activations menu	**n.19**		Zones	List of zones
Enable / Disable answerphone	**n.22**		Answerphone	"Answerphone" function
Enable teleservice	**n.23**		Teleservice	For future use
Enable codes	**n.24**		Codes	List of codes
Enable keys	**n.25**		Keys	List of keys
Enable timers	**n.26**		Timers	List of timers
Enable auto-arming	**n.27**		Auto-arm	Auto-arm single partition

6-6-5 View

From the keypad, the user can view the current status of some of the system elements:

- the events log (alarms, faults, arm/disarm operations, etc.), which shows the chronology with which the events occurred and were restored
- the status of the Nexus GSM communicator
- the control panel power-supply voltage, its firmware version and model
- the electrical status of the zones (stand-by, alarm, short-circuit, tamper) and their bypassed status
- activation status of the outputs
- activation status of the timers
- any faults present (refer to *Appendix B, Fault signals*)

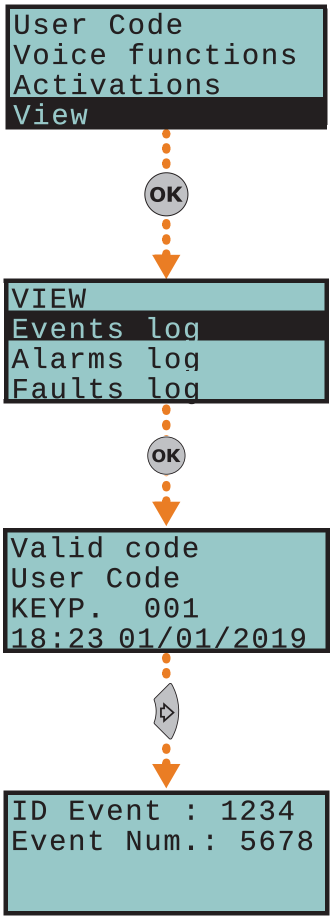
To view these statuses:

- activate the shortcuts associated with keys F1 Fn, ..., F4 POL (shown on the display) with or without code entry:
- access the “View” section of the User menu by entering a valid PIN.

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

Press keys ▲ and ▼ to scroll the chronological events list.

For some events, pressing the ► button will allow you to view the respective details.



```
User Code
Voice functions
Activations
View
```

```
VIEW
Events log
Alarms log
Faults log
```

```
Valid code
User Code
KEYP.  001
18:23 01/01/2019
```

```
ID Event : 1234
Event Num.: 5678
```

Table 6-13: Shortcut for viewing from a keypad

Shortcut			User menu section	Operation
			View	Access the section with the list of items that can be viewed.
View events log	n.28		Events log	Events log
View alarms log	n.29		Alarms log	Alarms log
View faults log	n.30		Faults log	Faults log
View arm/disarm operations	n.31		Arm/Disarm ops.	Arm/Disarm log
Nexus status menu	n.16		Nexus status	Status of Nexus GSM communicator
View system status	n.32		System status,	
			Batt	the voltage measured on the battery
			Pow.	the control panel power supply voltage
			Aux x	the voltage measured on terminal “AUX x”
			I-BUS	the voltage measured on terminal “+” of the I-BUS
View zone status	n.33		Zone status	Zone status
View faults	n.36		Faults ongoing	Ongoing fault
			PanelVersion	the firmware version and the control panel model

NEXUS STATUS

Table 6-14: View Nexus status on the keypad

Line	Display	View
1	`TELECOM      C G`	• Mobile network provider (on the left side) • "--" means that the Nexus is connected to the BUS • "C" means that data transfer is in progress • data network technology (on the right side) G, GPRS service 3G, UMTS service H, HSPA service
2	`GSM signal    01`	GSM signal reception (value between 1 and 100)
3	`Remaining cred.`	balance, at the last operation (expressed in the local currency)
4	`No signal`	Faults present, in this case it is necessary to access the "View-Faults" section for details.

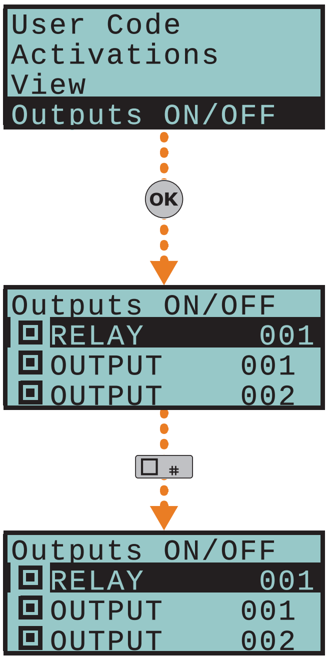
ZONE STATUS

Table 6-15: View zone status from keypad

Line	Display	View
1	`FD living room`	Zone description
2	`Standby Unbypsed`	Zone status ("Standby", "Alarm", "Short-circuit", "Tamper") and its activation status ("unbypassed" - capable of generating alarms, or "bypassed" - incapable of generating alarms)
3	`Lev.07 000 mdB/m`	Indications that vary depending on the device type: • wireless zone; level of wireless signal reception (from 0 to 7) • Air2-FD100 smoke detector; level of wireless signal and level of smoke present in the sensing chamber, expressed in mdB/m
4	`Dust level 000%`	Level of contamination present in the smoke detection chamber of Air2-FD100 smoke detector (%)

Outputs management

6-6-6



User Code
Activations
View
Outputs ON/OFF

Outputs ON/OFF
▣ RELAY 001
▣ OUTPUT 001
▣ OUTPUT 002

Outputs ON/OFF
▣ RELAY 001
▣ OUTPUT 001
▣ OUTPUT 002

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

The user can implement output activations via the keypad in two ways:

- activate the shortcuts associated with keys F1 Fn, ..., F4 POL (shown on the display) with or without code entry:
- access the "Outputs ON/OFF" section of the user menu by entering a valid PIN.

Once the output has been selected, it can be activated by the ▣ * key and deactivated by the □ # key.

If the output is a dimmer output, you can increase or decrease its power supply by means of keys ▣ * and □ #.

Table 6-16: Shortcut for output activations from a keypad

Shortcut			User menu section	Operation
ON/OFF output menu		▤	`Outputs ON/OFF`	Access the section with the list of available outputs
Activate output	**n.5**	💡		Activates the output programmed for the shortcut
Deactivate output	**n.6**	💡		Deactivates the output programmed for the shortcut

Change date and time

6-6-7

The keypads have a section where you can set the date and time of the control panel and the format.

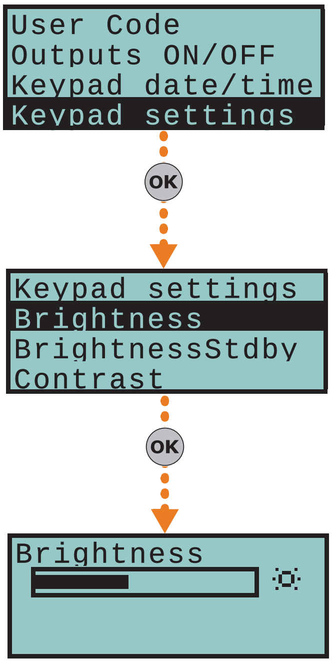
The user can operate via the keypad in two ways:

- activate the "Date/Time" shortcut (shortcut n.35), associated with one of the keys F1 Fn, ..., F4 POL shown on the display, with or without code entry

- access the “Keypad date/time” section on the user menu after entering a valid code.

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.

6-6-8 Keypad settings


User Code
Outputs ON/OFF
Keypad date/time
Keypad settings

Keypad settings
Brightness
BrightnessStdby
Contrast

Brightness

The keypads have a section for the programming of the displays and buzzers of the keypads which access to the Prime system.

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

- **Brightness** - the intensity of the backlight of the display and key LEDs, when a key is pressed and for the following 20 seconds.
- **Standby brightness** - the intensity of the backlight of the display and key LEDs when the keypad is in stand-by status.
- **Contrast** - black/white contrast adjustment.
- **Volume** - intensity of buzzer loudness.
- **Keypad options**:
  - **Temperature off** - if enabled, the temperature value read by the built-in temperature sensor will not be shown (only for temperature-sensor equipped keypads).
  - **NoExitTimeSignal** - if enabled, the buzzer will not emit an audible signal during partition exit time.
  - **NOEntryTimeSignal** - if enabled, the buzzer will not emit an audible signal during partition entry time.
  - **Beep on output** - if enabled, the buzzer will emit an audible signal during activation of keypad terminal T1, when this is programmed as an output.
  - **Disable Chime** - if enabled, the buzzer will not emit an audible signal when a bell zone is violated.
  - **LED Off in standby** - if enabled, this option switches of the relative LEDS after at least 40 seconds of inactivity on the keypad.

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

The user can operate via the keypad in two ways:

- by activating the “Date/Time” shortcut (shortcut n.18), associated with one of the keys F1 Fn, ..., F4 POL shown on the display, with or without code entry
- access the “Keypad settings” section of the user menu by typing-in a valid code PIN.

1. Use keys △ 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.

6-6-9 Change code PIN

To change user code PIN via keypad, the user can operate in two ways:

- activate the “Change PIN” shortcut (shortcut n.34), associated with one of the keys F1 Fn, ..., F4 POL shown on the display, with or without code entry
- access the “Change PIN” section of the user menu by typing-in the current code PIN.

1. Use keys △ and ▽ followed by **OK** to select the code to be changed.
2. Type-in the new PIN (4, 5 or 6 digits) using keys 0 ␣, ..., 9 wxyz then press **OK**.
3. Type-in the new PIN again using keys 0 ␣, ..., 9 wxyz and press **OK** to save.

6-6-10 Edit telephone numbers

To change the telephone numbers from the keypad, access the user menu in the "Telephone Numbers" section by entering your PIN code.

Access the phonebook:

1. Use keys ▲ and ▼ to select the required phone number then press **OK**; 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 ., , etc.) to edit the number. The following characters are also accepted: "," (= 2 second pause), "*" and "#".
3. Press **OK** to confirm and exit.

6-6-11 Overtime request

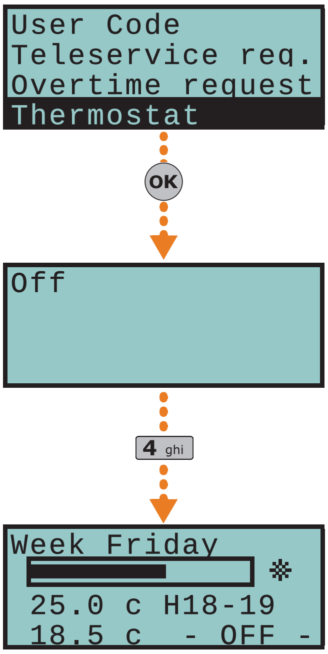
The overtime request via keypad can be activated in two ways:

- activate the "Overtime" shortcut (shortcut n.8), associated with one of the keys F1 Fn, ..., F4 POL shown on the display, with or without code entry
- access the "Overtime req." section of the user menu by typing in a valid code PIN.

6-6-12 Thermostat

The "thermostat" function can be controlled via keypad in two ways:

- activate the "Thermostat menu" shortcut (shortcut n.37), associated with one of the keys F1 Fn, ..., F4 POL shown on the display, with or without code entry
- access the "Thermostat" section of the user menu by typing-in a valid code PIN.


User Code
Teleservice req.
Overtime request
Thermostat

OK

Off

4 ghi

Week Friday
❄
25.0 c H18-19
18.5 c - OFF -

Table 6-17: Thermostat ON

Line	Display	View
1	Week Friday	operating mode of the thermostat and day of the week
2	❄	pre-set temperature bar and "Summer/Winter" operating mode icon
3	25.0 c H18-19	temperature setting and operating hours
4	18.5 c - OFF -	temperature reading and the status of the heating system/air-conditioning system (ON/OFF)

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"
2. Select the operating mode ("Summer/Winter") of the thermostat using 6 mno.
3. Select the temperature, using keys ▲ and ▼.
4. Select the timeframe, using ◄ and ►.
5. Select the day of the week, using ▣ * and □ #.
6. Press **OK** to confirm and exit.

6-6-13 Code Management

The user menu provides a section for the programming of the parameters of hierarchically-lower user codes (refer to *paragraph 3-1 User Codes*).

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

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

1. Use keys ▲ and ▼ followed by **OK** to select the code to be changed.
2. Use keys ▲ and ▼ followed by **OK** to select the parameter to be changed.
3. Change the parameter then press **OK** to save the changes.

CODE PARAMETERS

- **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 options for each code.
  - **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 code. Refer to the following table.

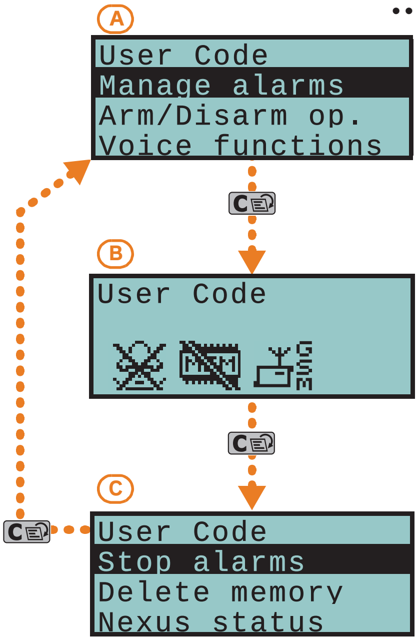


Table 6-18: Combinations “text menu” and “user menu”

Case	Text menu	User menu	Description
A	Disabled	Enabled	Access to 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 Fn, ..., F4 POL; 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 shortcut descriptions will be shown instead of the shortcut icons, at this point the user can use ▲ and ▼ to scroll the list of shortcut descriptions and select the 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 C key allows you to access/view the other cases in succession, see figure.

  - **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 code.
  - **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
    - Deactivate 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”, to be 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.
    If this option is enabled, the user of the code concerned can access their menu only after pressing **OK** and typing-in their PIN.
- **F1/4KeyShortcuts** - this section allows you to configure up to 12 shortcuts associated with keys F1 Fn, ..., F4 POL. After valid PIN entry the keypad will show the icons that correspond to keys F1 Fn, ..., F4 POL 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 from the "Type" list the shortcut you wish to associate with the function key.
3. Press **OK** to confirm and exit.
4. If the shortcut is associated with "Arm/Disarm" operations, the system will ask you to select a scenario. If the associated shortcut is "Activate output" or "Deactiv. output", the system will ask you to select an output.

- **ActivatableOutputs** - this section allows the user to enable/disable the outputs the code is allowed to control manually:

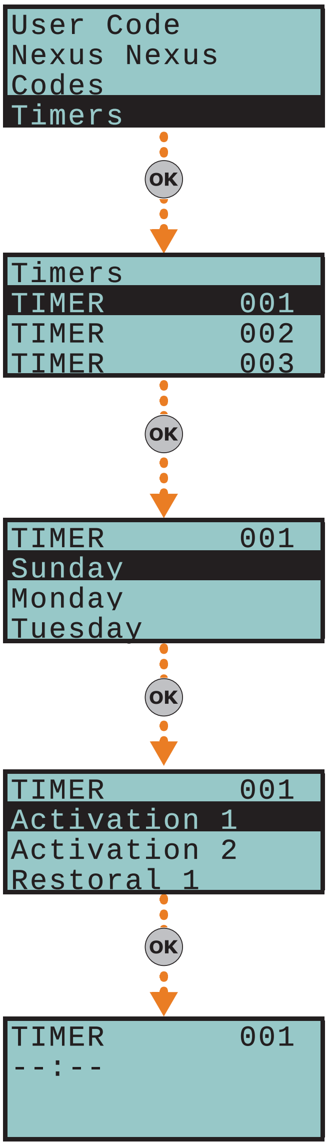
User menu, `Outputs ON/OFF` .

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

6-6-14



```
User Code
Nexus Nexus
Codes
Timers
```

OK

```
Timers
TIMER          001
TIMER          002
TIMER          003
```

OK

```
TIMER          001
Sunday
Monday
Tuesday
```

OK

```
TIMER          001
Activation 1
Activation 2
Restoral 1
```

OK

```
TIMER          001
--:--
```

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 6-6 Operations from LCD keypads*), 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.

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 **OK**.
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 **OK** to confirm and exit.

It is possible also to program timer activation only or timer reset only.

If you do not wish to program the timer activation or restoral setting, enter "--:--" in the field you do not wish to program.

6-6-15 Partition status enquiry

The user code must be enabled (by the installer) to activate shortcut n.17 via keys F1 Fn, ..., F4 POL or the number keys.

After entering a valid user-code, press the key which is assigned to the shortcut. The keypad sequentially replicates the description of the partition and its armed/disarmed status.

Note

The control panel replicates the armed/disarmed status of the code partitions and disregards the keypad partitions.

6-7 Operations via an Alien keypad

6-7-1 Alien function keys

The Alien keypad user-interface is shown as a menu of function keys. The keys are visualized as icons which activate the respective functions when tapped on the touch screen.

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.

Table 6-19: Alien keypad menu

Icon/key		Function	Code required
👁	**SCENARIOS**	Accesses the section containing the list of programmed scenarios which can be activated. Refer to *paragraph 6-7-3 Arming commands and scenarios*.	No code required for access. Depending on programming, the activation of scenarios may require code entry.
◎	**COMMANDS**	Accesses a section containing the list of outputs which can be activated. Refer to *paragraph 6-7-7 Outputs management*. The outputs are divided in two sections: • "Domotics", outputs for the management of home automation • "Intrusion" outputs programmed through the intrusion-control system	• "Domotics", no code required • "Intrusion", code required.
⌂	**INTRUSION**	Accesses a section where you can view and change the status of parts of the intrusion-control system: • "Partitions" - where you can view and change the status of the partitions. • "Zones" - section where you can view and changes the status of the zones. • "Events Log" - section where you can view the events log. Refer to paragraphs *6-7-2*, *6-7-3* and *6-7-6*.	User code required.
📍	**MENU**	Accesses two sections: • "Actions" - which lists the control panel commands in the event of alarm, tamper or overtime requests. Refer to paragraphs , *6-7-2* and *6-7-12*. • "Activations" - where it is possible to view and enable the activations described in *paragraph 6-7-5 Activations*.	User code required.
⚙	**SETTINGS**	Accesses the sections for the settings of the keypad and the Prime control panel: • "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 *paragraph 6-7-9 Keypad settings*. • "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 *6-7-8*, *6-7-10* and *6-7-11*. • "Installer" - this section allows access to the installer menu after entry of a valid installer PIN, thus putting the control panel in programming mode. • "Alphanumeric keypad" - this section allows you to work on the Alien keypad as if it were an LCD keypad. Tap the **ALIEN** button to step back to the standard mode.	User code required. Installer code required for the "Installer".
品	**SYSTEM**	Accesses a section where it is possible to view the system parts: • List of ongoing faults • Power-supply voltage of the control panel • Information relating the GSM communications board Refer to *paragraph 6-7-6 View*.	User code required.

Table 6-19: Alien keypad menu

Icon/key		Function	Code required
●●●	**APPS**	Accesses the applications of the Alien touch screen interface: • "Photo frame" - application that starts a slideshow of the images contained in the inserted SD-card (see *paragraph 6-8 Photo frame*). • "Voice functions" accesses a section where it is possible to activate the control panel voice board functions or the "Intercom" function. Refer to *paragraph 6-7-4 Voice memo and intercom functions*. • "Maps" - for access to the system by means of the graphic maps (refer to *Chapter 10 , Graphic maps*). • "Alarm clock", • "Memo" - application for the programming and activation of audible signalling and popups on the Alien keypad (refer to *paragraph 6-9 Alarm clock and memo*).	No code requested
❄	**CLIMATE**	Accesses the thermostat functions section Refer to *paragraph 6-7-13 Thermostat*.	No code requested

Alarm management 6-7-2

The typical operations the user must perform in the event of alarms and/or tamper conditions are:

- Stop the ongoing alarms by deactivating the outputs related to the system alarm and tamper events.
- Cancel the entire call queue and stop ongoing calls (if any).
- Delete the alarm and tamper memories.

To perform these operations, it is necessary to access the "Menu" section, enter the user code and then access the "Actions" section.

This section contains a list of control panel commands which can be activated by means of the **ACTIVATE** button.

Arming commands and scenarios 6-7-3

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):

In the case of arming requests in conditions of reduced security (partitions not ready or faults present) the keypad will show the list of causes of reduced security.

SCENARIOS

- Access "Scenarios" section This section provides a list of the scenarios which can be activated by means of the **ACTIVATE** button.

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, the system may request entry of a valid user code ("Show scenario with code",*paragraph 6-7-9 Keypad settings*).

PARTITIONS

- Access the "Intrusion" section, 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 buttons and then select the arming mode by means if up/down buttons.

- **"D"**, to disarm.
- **"A"**, to arm in Away mode (entire system armed)
- **"S"**, to arm in Stay mode (system partially armed).
- **"I"**, to arm in Instant mode (no delays)
- **"N"**, not to change the operating status.

To apply the selected arming mode , press the **OK** button.

Voice memo and intercom functions 6-7-4

When accessing voice functions via the Alien touch screen, first access the "Apps" section and then the "Voice functions" section.

Following is a list of the sections relating to each function which can be activated by pressing the respective **ON** button:

- Record message in the voice memo box
- Playback message in the voice memo box
- Delete message in the voice memo box
- Voice communication with another keypad.

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

6-7-5 Activations

To activate (and deactivate) the elements of the Prime system via the Alien keypad, access the “Menu” section, enter the user code and then access the “Activations” section.

Here are listed the sections relating to the elements you can activate by pressing 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

6-7-6 View

The Alien keypad has sections for displaying the current status of all system elements.

The “Activations” (*paragraph 6-7-5 Activations*) and “Commands” (*paragraph 6-7-7 Outputs management*) sections allow the display of the status of the activatible elements and the outputs. To these you can add other elements reachable through other sections:

- the events log (alarms, faults, arm/disarm operations, etc.), which shows the chronology with which the events occurred and were restored
- the status of the Nexus GSM communicator
- the control panel power-supply voltage, its firmware version and model
- the electrical status of the zones (stand-by, alarm, short-circuit, tamper) and their bypassed status
- any faults present (refer to *Appendix B, Fault signals*)

Access the “Intrusion” section and enter the user code. The following sections will be available:

PARTITIONS

- In the “Partitions” section, the partitions are listed and show their arming status, which can be changed, as described in *paragraph 6-7 Operations via an Alien keypad*.

The “View partition status” option (refer to *paragraph 6-7-9 Keypad settings*) will allow you to select the visualization mode of the operating status on the bottom bar of the screen:

- “Single partition” - the characters relating to the operating status of the partitions will be shown, as described in *Table 6-2: Display visualization*
- “Single scenario” - the description of the active scenario will be shown

ZONES

- In the “Zones” section, the zones are listed in this and show their status icons (positioned to the left of each zone description):
  - 🟢, green spot - stand-by 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

- In the “Events Log” section, all the events saved to the log are displayed one at a time, however, the up/down buttons 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 and enter the user code. The following sections will be available:

ONGOING FAULT

- The “Faults” 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

- The “Voltage” section allows you to view the control panel power-supply voltage.

NEXUS

- The “GSM info” section allows you to view the parameters of the Nexus GSM communicator.

Table 6-20: View Nexus status via Alien keypad

Line	View
1	• Mobile network provider (on the left side) • "--" means that the Nexus is connected to the BUS • "C" means that data transfer is in progress • data network technology (on the right side) G, GPRS service 3G, UMTS service H, HSPA service
2	GSM signal reception (value between 1 and 100)
3	balance, at the last operation (expressed in the local currency)
4	Presence of ongoing faults

Via Graphic maps

The visualization of the status and monitoring of the Prime system and its parts can also be achieved through the graphic maps accessible through the "Maps" section contained in the "Apps" section.

Refer to *Chapter 10 , Graphic maps*.

6-7-7 Outputs management

The Alien keypad allows you to activate/deactivate manually the outputs the code is enabled to work on.

Access the "Commands" section, then select the required sub-section:

- "Home automation", for access to the outputs of the home automation system, code entry not required.
- "Intrusion", for access to the outputs of the intrusion control system, code entry required.

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

The 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 "-" buttons.

6-7-8 Change date and time

The Alien keypad has a section that allows you to set the date and time in accordance with the selected format.

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

Changes can be made using the left/right and up/down scroll buttons and confirmed by the **OK** button.

6-7-9 Keypad settings

Access the "Settings" section, 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)
- **Stand-by brightness** - for the adjustment of screen brightness when the keypad is in stand-by status
- **Volume buzzer** - for buzzer loudness adjustment
- **Volume voice** - for speaker loudness adjustment
- **Skin** - for the selection of one of the skins available for the Alien keypad screen
- **Delay photo.** - waiting time before the automatic startup of the photoframe application during stand-by 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 keypad
- **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, in the event of mains power failure the keypad will increase brightness to its maximum value and will hold this status until the mains power restores to normal

If the Prime 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 opposite.

You can select the parameter by means of **+** and **-** buttons. To confirm changes and exit the section press the **SAVE** button.

Note

English is the default language of the Alien keypad.

6-7-10 Change code PIN

To change the PINs of the user codes via the Alien keypad, access the "Settings" section, enter a valid user code, then go to the"Date/Time - Change PIN - Change Tel. Numbers" section and select "Change PIN".

Select the code you desire from those available on the list. The next step is to change the code by means of the buttons on the screen and confirm changes by pressing the **OK** button.

6-7-11 Edit telephone numbers

To edit telephone numbers via the the Alien keypad, access the "Settings" section, enter a valid user code, go to the"Date/Time - Change PIN - Change 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 edit the number using the screen buttons and confirm changes by pressing the **OK** button.

6-7-12 Overtime request

Overtime requests via Alien keypads can be activated through the "Menu" section after entering a valid user code and accessing the "Actions" section.

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

6-7-13 Thermostat

The Alien keypad Thermostat" functions can be managed via the "Climate" section.

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

Press the **Back** button accesses a page containing buttons for the selection of the 5 operating modes available.

- Manual
- Day mode
- Week
- Antifreeze
- OFF

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 the **+** and **-** buttons, 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.

Photo frame 6-8

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

The image files must be stored in the "images" folder in the root directory of Micro SD card which is inserted in the appropriate slot on the Alien keypad. Visualization image file format: JPG, GIF and BMP.

Note

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

There are two ways of starting Photo frame:

- via Alien keypad, by accessing the "Apps" section, and pressing the "Photo frame" button;
- automatically, if the value set for the "Delay photo" option is different from "Disabled".
  To change this setting and other Alien keypad and application settings, access the "Settings" section, type-in a valid user code then access the "Alien" section (refer to *paragraph 6-7-9 Keypad settings*).

The slideshow can be stopped by simply tapping the screen, which then returns to the home page.

Alarm clock and memo 6-9

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).

Note

The programming and activation of the clock and memo events are of no consequence to the programming or regular functioning of the Prime control panels and its peripherals.

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:

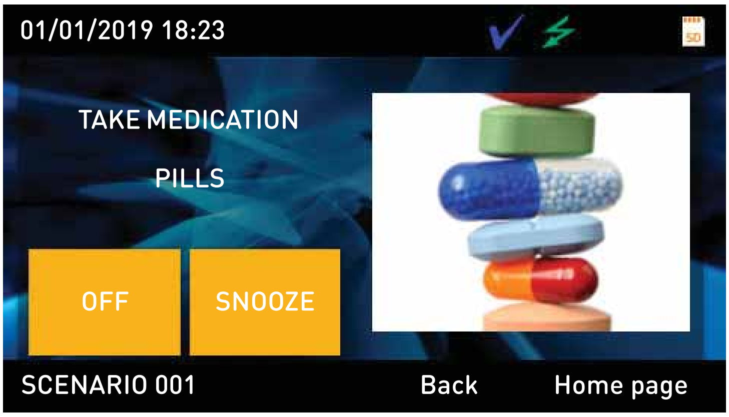
- description
- day the week, by selecting the respective button in the upper part of the "When?" section
- time, by changing the field selected with the arrows

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 stops the signalling, whereas the **SNOOZE** button interrupts the signal for 5 minutes before signalling again.



01/01/2019 18:23

TAKE MEDICATION

PILLS

Chapter 7 Readers and Keys

7-1 Proximity readers

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

Readers (also referred to as proximity readers) have 4 LEDs:

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

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).

If the keypad is equipped with a buzzer, the latter will signal the running entry, exit and pre-arm times on the enabled reader partitions (refer to *paragraph 6-4 Signalling on the Buzzer*).

7-1-1 Signalling on reader LEDs

The LEDs have two distinct operating modes:

- when no key is present at the reader (refer to *Table 7-1: Reader LEDs with no key at reader*), the LEDs will indicate the current status of the associated shortcut.
- when a key is present at the reader (refer to *Table 7-2: Reader LEDs with key at reader*), the LEDs will indicate (in rapid succession) the available shortcuts.

Table 7-1: 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 7-2: 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.			

Note

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

READER LED OFF

If the installer has enabled the "LED Off reader" option (or "50131LedOFFLett." on keypads option), the reader LEDs will remain Off when there is no key in the vicinity of the reader (in order to hide the armed status of the partitions).

7-2 Keys

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

- tags for proximity readers
- cards for proximity readers
- keyfobs (remote-control keys)

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

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

- The **partitions** the user can control. 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. The system will allow the key to operate the system only when the Timer is active. In this way, the user will be unable to access the system at all other times.
- The "**Patrol**" option, usually enabled on keys used by security personnel or night watchmen who must patrol the protected premises. 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:
  - Disarm the partitions common to the key and reader concerned.
  - Activate the respective Patrol Time for the partitions concerned.
  - 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 which 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.

7-2-1 Wireless keys (remote-control keys)

The wireless keys have 4 buttons which can each be programmed with a shortcut. The graphic-choice feature allows you to identify the buttons by numbers or icons.

The wireless keys also have 4 button-associated LEDs and a confirmation LED. Thanks to two-way communication (transceiver), the LEDs and buzzer on the remote-control keys provide users with feedback signals that notify them of the successful outcome or failure of the requested operation:

Table 7-3: Feedback signals provided by wireless keys

Button	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

Note

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.

Table 7-4: 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

7-3 Reader and key operations

7-3-1 Alarm management

The operations that users can perform via proximity readers or keys, in relation to alarm and/or tamper events, depend on the programming of the associated shortcuts.

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), “Delete call memory” (shortcut n.4).

Via Wireless key

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 7-2-1 Wireless keys (remote-control keys)*.

7-3-2 Arming commands and scenarios

Via a reader or key it is possible to activate the programmed scenarios for the associated shortcuts:

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).

Via Wireless key

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 7-2-1 Wireless keys (remote-control keys)*.

Outputs management 7-3-3

The activations and deactivations that users can perform via proximity readers or keys depend on the programming of the associated shortcuts.

Via Reader

Hold a valid key in the vicinity of the reader until the reader LEDs or display indicates "Activate output" (shortcut n.5), "Deactivate output" (shortcut n.6).

Via Wireless key

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 7-2-1 Wireless keys (remote-control keys)*.

Overtime request 7-3-4

The overtime request via proximity reader or key is possible through one of the appropriately programmed associated shortcuts.

Via Reader

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

Via Wireless key

Push the respective button on the wireless key and verify the outcome of the requested operation, as described in *paragraph 7-2-1 Wireless keys (remote-control keys)*.

Chapter 8 Commands over-the-phone

8-1 Use of telephone calls

8-1-1 Panel to user calls

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 the "*****" button on the telephone keypad and go to the next message or, if there is only one message, end the successful call.
- type-in a valid PIN code followed by "**#**" and access the shortcuts programmed for 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.

8-1-2 User to control panel calls

If the "Answerphone" function is enabled (refer to *paragraph 5-5 Activations*), the user can call the control panel from any remote telephone and send commands to the system (refer to *paragraph 4-2 Shortcut with code*) and/or activate a listen-in session (refer to *paragraph 5-11 Listen-in*).

1. Dial the control panel telephone number.
2. The control panel will answer after the programmed number of rings and will play message n.216: "Enter valid code followed by #".
3. Type in your PIN followed by "**#**".
4. The control panel will announce the available shortcuts and the number keys to press.
5. Press the number key that corresponds to the required command.

If the system is equipped with a Nexus GSM dialer, the user can operate on the control panel through a simple call to the telephone number of the SIM inserted into 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.

8-2 Use of SMS text messages

8-2-1 SMS text message from panel to user

If the system is equipped with an appropriately programmed Nexus GSM dialer, the user may receive an SMS text message signalling an event that has 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.

8-2-2 SMS text message from user to panel

If the system is equipped with a duly programmed Nexus GSM dialer, the user can operate on the control panel by sending a command via SMS text to the 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.

SMS TEXT AT DEFAULT

By default, commands are predefined and can be modified by the installer:

- "**CONNECT**" for a request for remote assistance via SMS text (future use).
- "**CREDIT**" - for balance enquiries relating to the SIM card of the Nexus, the user will receive an SMS text indicating the remaining credit.
- "**STATUS**" - for status enquiries relating to the Nexus, the user will receive an SMS text indicating the:
  - device name and firmware revision
  - GSM network provider
  - GSM signal reception level
  - device tamper status
  - BUS status
  - Balance (remaining credit)
  - scenario active (if present)
- "**EXC**" (or "**ESC**"), to inhibit the control panel zones
- "**INC**", to activate the control panel zones

For the last two commands, the message text must be:

<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

Operations via telephone 8-3

Alarm management 8-3-1

The operations that can be performed via the keypad in the event of alarm or tamper are:

- Stop alarms
- Clear call queue
- Delete memory

Type-in the PIN of an authorized user followed by "**#**" on the telephone keypad, then press the key (from "**0**" to "**9**") which the installer has programmed to "Stop alarms" (Shortcut n.2), "Clear call queue" (Shortcut n.3), "Delete memory" (macro n.4).

Arming commands and scenarios 8-3-2

Type in an authorized 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.

Activation of outputs 8-3-3

Type-in the PIN of an authorized user code followed by "**#**" on the telephone keypad, then press the key (from "**0**" to "**9**") which the installer has programmed to activate "Activate output" (Shortcut n.5) or "Deactivate output" (Shortcut n.6).

Overtime request 8-3-4

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

8-3-5 Listen-in

Type-in the PIN of an authorized user code followed by “**#**” on the telephone keypad, 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 session and step back to the voice-announced Shortcut menu.

8-3-6 Partition status enquiry

Type-in the PIN of an authorized user code followed by “**#**” on the telephone keypad, 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 in order to listen to the voice messages relative to the shortcuts available for the authenticated code.

How to use the PrimeLAN

Chapter 9

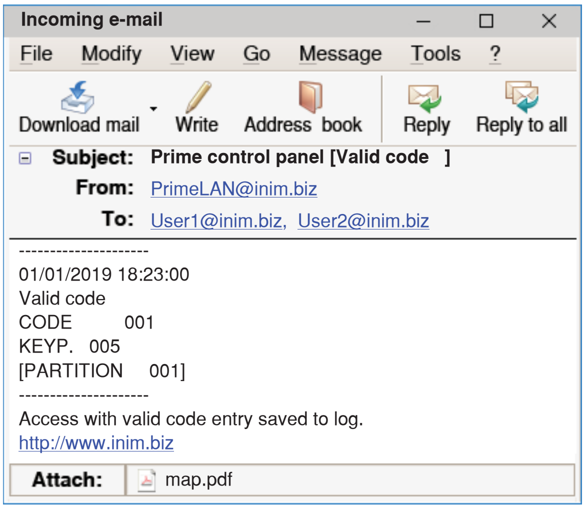
e-mail

9-1

The event-related e-mail sent to the user via the PrimeLAN board can be programmed entirely by the installer.

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

Table 9-1: E-mail parameters

Parameter	Example		
Subject	Prime control panel [Valid code]	Text, edited by the installer, associated with info about the respective event.	 Incoming e-mail File Modify View Go Message Tools ? Download mail Write Address book Reply Reply to all **Subject:** Prime control panel [Valid code] **From:** PrimeLAN@inim.biz **To:** User1@inim.biz, User2@inim.biz -------------------- 01/01/2019 18:23:00 Valid code CODE 001 KEYP. 005 [PARTITION 001] -------------------- Access with valid code entry saved to log. http://www.inim.biz **Attach:** map.pdf
Sender	PrimeLAN@inim.biz	Parameters set by the installer	
Recipient	User1@inim.biz, User2@inim.biz		
Message text	-------------------- 01/01/2019 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

9-2

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.

LOGIN

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

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):
   - Password
   - Code (user code valid for the control panel)
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.

MENU

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 9-2: Menu via web server*.

NAVIGATION

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

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

ATTENTION!

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.

INFORMATION

In each section, the firmware revision and the Prime panel type are always visible on the lower bar together with the current arming scenario.

9-3 Sections of the web interface

The user interface of the PrimeLAN web server appears as a menu of function keys represented by icons.

The table below is a description of the function keys on the menu present on the home page, each one corresponding to a different section.

None of these sections, like any operation that can be activated by the web server, requires the entry of a valid code, other than the one already entered during login.

Table 9-2: Menu via web server

Icon/key		Section
	SCENARIOS	Accesses the section containing the list of programmed scenarios which can be activated. Refer to *paragraph 9-3-2 Arming commands and scenarios*.
	COMMANDS	Accesses a section containing the list of outputs which can be activated. Refer to *paragraph 9-3-3 Viewing and activations*.
	INTRUSION	Accesses a section where you can view and change the status of parts of the intrusion-control system: • "Partitions" - section where you can view the status of the partitions, change the arming status and implement reset of partition alarm memory. • "Zones" - section where you can view and changes the status of the zones. • "Events Log" - section where you can view the events log. After obtaining access to this section, it is necessary to indicate the number of events to be viewed. • "Timer" - section where you can view the timers and their statuses. Refer to paragraphs *9-3-1*, *9-3-2* and *9-3-3*.
	CAMERAS	Accesses two sections: • "Real-time" - section where the configured cameras are listed • "Records" - section where you can view the snapshots recorded after the occurrence of an event. Refer to *paragraph 10-1 Camera access*.
	SETTINGS	Accesses a section where it is possible to: • 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 PrimeLAN to a recipient • upgrade the web server interface • open a section that shows the meanings of the icons used by the web interface
	SYSTEM	Accesses a section where it is possible to view the system parts: • List of ongoing faults • Power-supply voltage of the control panel • Information relating the GSM communications board Refer to *paragraph 9-3-3 Viewing and activations*.

Table 9-2: Menu via web server

Icon / key		Section
	KEYPAD	Section for remote access to a keypad. Refer to *paragraph 9-3-5 Remote keypads*.
	MAPS	Accesses the system through the graphic maps. Refer to *Chapter 10 , Graphic maps*.

Alarm management 9-3-1

In the event of alarm and tamper, the user can intervene by deleting the alarm and tamper memories.

To do this you must 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.

Arming commands and scenarios 9-3-2

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

- 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 a list of commands for the partition.

Table 9-3: Activations via web

Button		Function
SET		opens a window with the buttons for setting the arming mode
	AWAY	Arms the selected partition in Away mode
	STAY	Arms the selected partition in Stay mode
	INSTANT	Arms the selected partition in Instant mode
	DISARM	Disarms the selected partition

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

Viewing and activations 9-3-3

Through the PrimeLAN web browser it is possible to view the status of various elements of the Prime system and to change their activations by means of the available buttons.

Table 9-4: Viewing via web

Section		Icon	Status
🏠	Partitions/Zones	🔓	Disarmed
		🔒	Armed in Away mode
		🔒	Armed in Stay mode
		🔒	Armed in instant mode
		⏻	Stand-by
		🔔	Alarm
		⚠	Tamper or fault
		M	An alarm or tamper event in memory
	Zones	⚡	Zone shorted
		✓	Zone active
		⊗	Zone deactivated
	Timer	⏱	Activated
		⏱	Deactivated
◎		💡	Output status
		💡	

Table 9-5: Activations via web

Section		Button	Function
🏠	Zones	ON	Enables zone
		OFF	Disables zone
◎		ON	Activates output
		OFF	Deactivates output
		bar	scroll bar for adjustments to the power/current supplied to the high-power relay outputs and dimmer outputs

- **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** - accessing the "System" section provides the following sub-sections:
  - "Faults list" - this 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 viewing of the Prime system status and the monitoring of its parts can be done through the graphic maps function, accessible through an Alien keypad or web interface.

Refer to *Chapter 10 , Graphic maps*.

Camera access 9-3-4

The web interface allows the user to view the image stream or video in real time and the image recordings which precede and follow the occurrence of an event.

This is possible through the "Cameras" section, where the camera shots configured through the appropriate programming of the PrimeLAN board can be viewed.

Two sections are available:

REAL-TIME

- "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

RECORDINGS

- "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.

Remote keypads 9-3-5

The "Keypads" section of the web interface of a Prime control panel provides access to the replication of one of the keypads connected to the 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.

Besides the keypad buttons (described in *paragraph 6-2 Using the keys*) there are also other buttons:

- 🏠, to access the home page of the web interface
- 🖩, to open a window for the selection of the keypad to be replicated

Chapter 10 Graphic maps

The Prime monitoring 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 can manage up to 10 maps (revisions below 2.00 can manage up to 5 maps) and the web interface up to 20. 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.

Note

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

Via Alien

Access the “Apps” section, then the “Maps” section.

Via Web browser

Access the “Graphic maps” section in the home page.

Table 10-1: Graphic map icons at default

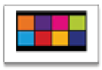
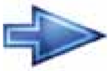
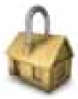
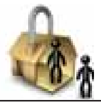
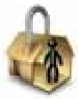
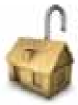
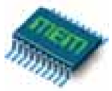
Subject	Icon		Button
Link			Link to the Alien home page
			Map link
Partition		Partition armed in Away mode	After a valid code entry a window will open where you can select the arming mode you wish to apply.
		Partition armed in Away mode	
		Partition armed in Instant mode	
		Partition disarmed	
		Partition alarm/tamper memory	

Table 10-1: Graphic map icons at default

Subject	Icon		Button
Zone	⚠	Zone shorted/tamper Zone alarm/tamper memory	After a valid code entry the zone will change its activation status
	●	Zone in stand-by status	
	●	Zone in alarm status	
	☒	Zone disabled/bypassed	
Output	💡	Output activated	Output switches status
	💡	Output deactivated	
Scenario	🏠	Scenario active	/
	🏠	Scenario inactive	After a valid code entry you can activate the scenario
Ongoing fault	FAULT	Scenario active	Accesses the faults viewing section
	FAULT ⚠	Scenario inactive	
Thermostat	❄	Thermostat disabled	Accesses the reader thermostat management section
	❄ M	Thermostat set to manual mode	
	❄ 24h	Thermostat set to daily mode	
	❄ W	Thermostat set to weekly mode	
	❄ fr	Thermostat set to antifreeze mode	
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
Clear call queue	☒ ☎		After a valid code entry you can clear the call queue completely and interrupt any ongoing call.
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.
View events log	LOG		After a valid code entry you can access the events log

10-1 Camera access

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

Once the map application has started, navigate through the tree structure until you reach the map where the camera is.

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, image streaming or video) depends on the type and make of the camera.

Glossary

Appendix A

ALARM

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

ALARM OR TAMPER MEMORY

In the event of:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper
- peripheral loss
- 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).

ALARM RECEIVING CENTRE (ARC)

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.

ANSWERPHONE

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.

ARM / DISARM

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.

AUTO-ARM

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.

BACKUP BATTERY

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

Prime control panels use 12V sealed lead batteries. The battery housing determines the maximum size of the battery and therefore, its power-storage capacity. Prime control panels can be equipped with lead batteries @12V 7, 9 or 17Ah. The control panel monitors the battery continuously and keeps it is under constant charge (from Mains).

BYPASS - ZONE DEACTIVATION

A bypassed (disabled) zone cannot generate alarms. Each zone can be bypassed/unbypassed manually by the system users, or automatically by the control panel. Automatic bypass operations can take place only when the zone is configured as "Auto-bypassable" and the conditions that regulate auto-bypass operations are in effect (refer to Zone Attributes – Auto-bypassable).

CALL QUEUE

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

Enabled users can clear the call queue manually.

CLOUD

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.

CODE

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**:	used by the installer company technician
• **User code**:	assigned to the building occupants

DEFAULT SETTINGS

A group of operating parameters set at the factory by the manufacturer. The purpose of these settings is to reduce the work of the installer during the installation phase.

The installer can restore the system to “Default Settings” if necessary.

DELAYED ENTRY ZONE

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.

DELAYED EXIT ZONE

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.

DELETE ALARM / TAMPER / FAULT MEMORY

This is an explicit user-command which ends signalling on the red and yellow LEDs on keypad and readers for the following events:

- Zone Alarm
- terminal tamper
- open panel or dislodged panel
- peripheral tamper
- peripheral loss
- false key
- ongoing fault
- memory fault

If a user deletes the alarm/tamper memory, the visual signals on the reader/keypad LEDs will clear.

If the settings for norm. 50131 compliance are active, the keypads may, in addition, require entry of a level 3 access code code (installer code) for the deletion of fault memories.

DIGITAL DIALER

This device allows the control panel to send report calls to Alarm Receiving centres (ARC).

Prime control panels provide a built-in digital dialer.

DIMMER

Operating mode of specific terminals configured as “outputs” which, when the respective option is selected, allows adjustment of the power supply to the connected load (for example a lamp) during certain events.

ENTRY TIME (OR ENTRY DELAY)

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

Each partition can be programmed with its own Entry time.

EVENT

An operative status recognized by the system.

For example: detector alarm, mains failure (230V~), blown fuse, user-code recognition, etc., are all events recognized by the control panel.

Each event is 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
- activation of an output scenario
- 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
- activation of shortcut functions

EVENTS LOG (OR EVENTS MEMORY)

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

EXIT TIME (OR EXIT DELAY)

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.

EXPANSION BOARDS

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.

FAULT

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~), telephone line-down and low battery are typical faults.

GRAPHIC MAP

A map is an 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
- Button

GSM DIALER

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.

I-BUS

A proprietary 4-conductor bidirectional digital high-speed communication line used to connect its peripherals 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

INSTALLER CODE (ACCESS LEVEL 3)

The installer code is generally characterized by a PIN (4, 5 or 6 digits) through which the installer, by entering it on a keypad or using in the software program (provided that all the system partitions are disarmed) has access to the programming menu and can check and change all the system parameters.

In accordance with EN 50131 grade 3 security, the installer code is a level 3 access code.

INSTALLER MENU

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, on condition that all the system partitions are disarmed, or can be accessed via a PC equipped with the Prime software program.

INTERIOR ZONE

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.

IP CAMERA

A camera is an electronic instrument that records bidimensional images in sequence. It is part of a camera surveillance system monitored by a 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.

The Prime control panel manages the following types of IP cameras:
- static cameras
- cameras with Convict protocol, that allow user interaction thanks to remote control of the lens (ZTL) and pre-programmed audio/video profiles

ISOLATOR

The isolators are peripherals that allow you to increase the extension and the functional integrity of the BUS.

The functions they provide are:
- galvanic isolation of the entire BUS between input and output
- regeneration of the communication signals
- detection of operating anomalies towards the output branch

KEY

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).

KEYPAD

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.

MAGNETIC CONTACT

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

MAINTENANCE

If you wish to carry out maintenance work on the control without generating false alarms (tamper and intrusion), you must put the control panel in "Maintenance" mode. The control panel in must also be in "Maintenance" mode during the keypad and reader addressing process. The other functions of the control panel are still available (arm/disarm operations, events, calls, etc.).

OUTPUT

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

The terminal the device is connected to must be configured as an "output".

Outputs are usually connected to audible or visual signalling devices but can be used for other purposes such as: switching on lights or opening doors/gates.

OUTPUT SCENARIOS

This is the configuration of the activation mode of several outputs at the same time.

For each output, it is possible to set up the digital status (On - Off) or the analogue status (1 - 100 for dimmer type outputs and analogue expansion outputs).

The Prime control panel provides 50 output scenarios, each with a maximum of 10 outputs.

PANIC

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.

PARTITION

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).

PARTITION ARM/ DISARM OPERATIONS

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 perimeter zones only and annuls delays. In this way, all the perimeter zones of the partition will generate instant alarms.
- **Hold** - this operation forces the partition to hold its current status.

PATROL

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

Patrol staff can disarm each partition for the pre-set time only (programmable separately for each partition). The partitions concerned will rearm-as-before automatically when the pre-set time expires. Persons involved in periodic security inspections require codes with the "Patrol" attribute.

PERIMETER ZONE

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.

PERIPHERALS

Device for management and use of the system, external to the control panel.

These are devices connectible to the control panel by I-BUS as well as wireless devices.

Prime control panels manage the following peripherals on the IBUS:

- Keypads (Joy, nCode, Concept, Alien, Aria/HG)
- Proximity Readers (nBy)
- Expansions (Flex5)
- Transceiver (Air2-BS200)
- Sounder/flasher (Ivy-B)
- GSM dialer (Nexus)
- Isolators (IB200)

The following wireless devices can be added, and are recognized by the control panel as peripheral devices:

- Keypads (Air2-Aria/W)
- Sounders (Air2-Hedera)

PRE-ARM TIME

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.

PREMISES

The installation site.

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

PRIMARY POWER SOURCE

The primary source of electrical power to the system is normally @ 230V~ 50 Hz (115V60Hz in some American states).

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.

READER

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

By means of the readers, each user can arm/disarm the partitions which are common to both the key and reader in use and can activate shortcuts (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.).

SCENARIO

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

SHORTCUT

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.

SMOKE DETECTORS

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.

SUPERVISION

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.

TAMPER

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.

TELEPHONE ACTIONS

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

TELESERVICE

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.

TERMINAL

Screw terminal for the connection of zones (detection devices) or outputs (command/ signalling devices).

TIMER

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

Prime control panels manage 40 timers.

Each timer can be programmed to manage:

- Two activation times (ON) and two deactivation times (OFF) on preset days of the week.
- 15 timer-slot exceptions. Each exception refers to a specific interval of one or more days, which can be programmed with an ON and OFF Time.

The timers can be used for different purposes:

- If a timer is associated with a partition, the system will arm and disarm the partition automatically at set times of the day.
- If a timer is associated with a code, the latter will be allowed to access the system only when the timer is On.
- If a timer is associated with a key, the latter will be allowed to access the system only when the timer is On.
- If the “Timer xxx” event is assigned to an output, the latter will activate/deactivate the connected device in accordance with the On/Off settings of the timer.

No matter how they are employed, the timers must always be enabled by the user.

TRANSCEIVER

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.

USER CODE

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

USER MENU

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

VOICE DIALER

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

In Prime control panels the voice dialer is provided by the SmartLogos30M board (to be installed on the control panel).

VOICE MEMO

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.

WEB BROWSER

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

WEB SERVER

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

The PrimeLAN board has an integrated web server that provides the browser with a web interface for the management and supervision of the Prime system.

WIRELESS

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

Usually, in wireless systems, only the control panel is mains powered (230V~), whereas the system peripherals are battery powered. The battery life is of utmost importance in the design layout and operational capacity of these systems.

ZONE

An electrical input point used for the management/supervision of signals coming from an intrusion detection device. The terminal the zone is connected to must be configured as an “input” zone.

Zones are usually connected to a single device, however, it is possible (if the zone is duly wired and configured) to connect more than one device. If a zone is connected to more than one device it is impossible to identify the alarm-trigger device in the event of an alarm.

Fault signals

Appendix B

The faults listed below are the faults that may be shown when accessing the user menu:

`View, Faults ongoing, Faults log`

Fault	Signalling on keypad		Occurs when...	Restores when ...	Control panel event
Battery fault	`Low battery`		The backup battery is low (voltage below 10.4V)	The backup battery is charged (voltage above 11.4V)	Yes
AC Mains failure	`Mains failure`		The primary power supply 230V~ fails	The primary power supply 230V~ is restored	Yes
Telephone line down	`Tel. line down`		The land line is not working	The land line restores	Yes
Jamming	`Jamming`		Wireless interference detected	Wireless interference cleared	Yes
Low battery on wireless zone	`Low WLS`	([a])	The battery of a least one wireless detector must be replaced	All the wireless detectors are running with sufficient power	Yes
Wireless zone loss	`WLS zone loss`		Loss of at least one wireless detector has been signaled (monitoring time exceeded)	All the wireless detectors are present	Yes
Nexus GSM dialer faults	`Nexus fault`	([b])	One of the faults below is present	None of the faults below are present	No
Insufficient cover	`No signal`		The GSM network signal is insufficient	/	No
GSM module communication fault	`GSM module fault`		The GSM module of the Nexus dialer is not functioning properly.	/	No
SIM communication fault	`SIM commun.fault`		The SIM card does not respond or is not present. The SIM card PIN is not disabled.	/	No
Low credit	`Low credit`		The credit remaining on the SIM card inserted in the Nexus is below the minimum credit threshold.	/	Yes
Provider unavailable	`ProviderUnavail.`		The GSM network provider of the SIM in use is unavailable.	/	No
GPRS connection lost	`IP conn. lost`		NEXUS detects connection problems on GPRS network	/	No
Nexus/3GP battery inefficient	`Low battery`		The buffer battery of the Nexus/3GP module is inefficient or missing	The backup battery is charged	No
Contaminated smoke sensor	`Detector dusty`	([a])	The smoke chamber of at least one of the Air2-FD100 smoke detectors is contaminated by dirt or dust.	The contamination level of all detectors is below the programmed threshold	Yes
Violation of zones with faults	`Faults on zones`		Violation has occurred on one or more zones with the "Fault zone" option enabled.	All zones with the "Fault zone" option active have reset	No
Faults on BUS sounder/flasher	`Sounder faults`	([c])	One of the faults below is present	None of the faults below are present	No
Horn damaged	`Horn fault`		A defect/damage has been detected on the horn/sounder.	/	No
Sounder/flasher battery low	`Sounder lowBatt.`		A low-voltage value has been detected on the sounder/flasher 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.	/	No
Internal resistance of the sounder/flasher battery too high	`Battery battery`		An excessive internal resistance has been detected on the sounder/flasher battery. This type of deep fault indicates corrosion inside the battery, therefore, the battery must be replaced.	/	No
Internal resistance of battery too high	`Int. Resistance`		The internal resistance of the battery has exceeded the $R_{i\ max}$ value.	The internal resistance of the battery returned to below the $R_{i\ max}$ value.	Yes
Short-circuit on battery	`Battery shorted`		A short-circuit condition has been detected on the battery connection terminals	The short-circuit condition is no longer present	Yes
Battery disconnected	`Battery disconn.`		The buffer battery is disconnected	The buffer battery is connected	Yes
Power-supply overload	`PwSupplyOverload`		Output overload is detected on the power-supply unit	The electrical load returns below the allowed limit	Yes

Fault	Signalling on keypad	Occurs when...	Restores when ...	Control panel event
Overheating on power-supply unit	PwSupply Overheat	The temperature of the power-supply unit has exceeded the allowed limit	The temperature of the power-supply unit is normal	Yes
Dispersion to earth	Earth fault	Leakage to ground is present	The leakage to ground condition is no longer detected	Yes
Overvoltage on Aux x	Overvoltage "x"	A voltage of over 14.5V has been detected on terminal "**+AUX**"	The normal voltage on the terminal has been restored.	Yes
Overvoltage on BUS power supply	Overvolt. BUS	A voltage of over 14.5V has been detected on the "**+**" terminal of the I-BUS	The normal voltage on the terminal has been restored.	Yes
Undervoltage on Aux x	Undervoltage "x"	A voltage below 9.8V has been detected on the "**+AUX**" terminal	The normal voltage on the terminal has been restored.	Yes
Undervoltage on BUS	Undervoltage BUS	A voltage below 9.8V has been detected on the "**+**" terminal of the I-BUS	The normal voltage on the terminal has been restored.	Yes
Short-circuit on Aux x	Short circuit ?x?	Short-circuit has been detected on the "**+AUX x**" terminal	The short-circuit is no longer present.	Yes
Short-circuit on BUS power supply	Short circuit BUS	A short-circuit has been detected on the "**+**" terminal of the I-BUS	The short-circuit is no longer present.	Yes
Overload on Aux x	Overload ?x?	A load of over 1.5A has been detected on the "**+AUX**" terminal	The terminal restores to normal.	Yes
Overload on BUS power supply	Overload BUS	A load of over 3.5A has been detected on the "**+**" terminal of the I-BUS	The terminal restores to normal.	Yes
Communication with power supply failed	NoCommunPwSupply	The power supply unit is not communicating with the control panel	Communication between the power supply unit and the control panel restores.	Yes
Low battery on wireless keypad	Low batt.WLS keypad ([a])	The battery of a least one wireless keypad must be replaced	All the wireless keypads are running with sufficient power	No
Open-panel tamper	Control panel open	The control-panel enclosure is removed	The front of the control-panel is replaced	Yes
Dislodged-panel tamper	Dislodged panel	The control-panel enclosure is detached from the wall	The control-panel enclosure is reattached to the wall	Yes
I/O Expansion tamper	Expansion tamper	An expansion board signals tamper conditions	Tamper conditions clear on all the system expansion boards	Yes
Keypad Tamper	Keypad tamper	A keypad signals tamper conditions	Tamper conditions clear on all the system keypads	Yes
Reader Tamper	Reader tamper	A reader signals tamper conditions	Tamper conditions clear on all the system readers	Yes
Sounder flasher tamper	Sound.flash.Tamp	A sounder/flasher connected to the BUS signals tamper	All the sounder/flashers connected to the BUS reset	Yes
Nexus tamper	Nexus tamper	The GSM dialer Nexus signals tamper	Tamper conditions clear on the Nexus	Yes
I/O expansion loss	Expansion loss	An expansion board cannot be found on the BUS	All expansion boards can be found on the BUS	Yes
Keypad Loss	Keypad loss	A keypad cannot be found on the BUS	All keypads can be found on the BUS	Yes
Reader Loss	Reader loss	A reader cannot be found on the BUS	All readers can be found on the BUS	Yes
Sounder/flasher loss	Sound.flash.Loss	A sounder/flasher cannot be found on the BUS	All sounder/flashers can be found on the BUS	Yes
Nexus loss	Nexus loss	The control panel is unable to communicate the Nexus 100	Communication between the control panel and the Nexus restores	Yes
Internet connection loss	IP conn. lost	The IP connectivity test is enabled and the test result in negative (failed).	A connection attempt has been successful.	Yes

a. Press the **OK** button to access the list of devices affected by the fault.
b. Press the **OK** button to access the list of the ongoing faults.
c. Press the **OK** button to access the list of sounder/flashers that have at least one fault present. Select the sounder/flasher to access the list of current faults on the device.

ISO 9001 Quality Management
certified by BSI with certificate number FM530352

Centobuchi, via Dei Lavoratori 10
63076 Monteprandone (AP), Italy
Tel. +39 0735 705007 _ Fax +39 0735 704912

info@inim.biz _ www.inim.biz