



EN 50131-1
EN 50131-3
EN 50131-6
EN 50131-10
EN 50130-4
EN 50130-5
EN 50136-1
EN 50136-2
CEB T031



PRIME

Anti-intrusion control panel and security systems



User's manual



Warranty

Inim Electronics S.r.l. warrants that this product shall be free of defects in material and workmanship for a period of 24 months from the date of production.

In consideration of the fact that Inim Electronics does not install directly the products here indicated, and due to the possibility they may be used with other products not manufactured by Inim Electronics, Inim Electronics cannot guarantee the performance of the security installation. Seller obligation and liability under this warranty are expressly limited to repairing or replacing, at seller's option, any product not meeting its stated specifications. In no case can Inim Electronics be held responsible or liable by the buyer or any other person for any loss or damage, direct or indirect, 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 these products.

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover misuse or neglect, damage caused by fire, flood, wind, lightning, vandalism or wear and tear.

Inim Electronics shall, at its option, repair or replace any defective products. Improper use, that is, use for purposes other than those mentioned herein will void this warranty. For further details regarding this warranty contact the authorized dealer.

Limited Warranty

Inim Electronics S.r.l. shall not be liable for any damage caused by improper use of this product.

The installation and use of the products indicated herein must be carried out by authorized persons only. Moreover, the installation procedure must be carried out in full respect of the instructions provided in this manual.

Simplified EU declaration of conformity

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/EU:

- Prime 500L, Prime 240L, Prime120L, Prime060L, Prime060

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

The full text of the EU declaration of conformity is available at the following Internet address: www.inim.biz.

Leading-edge systems (DM 37/08)

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 + A2:2017 + A3:2020 and EN 50131-5-3:2017, safety grade 2 (at highest) and an alarm transmission system (ATS) compliant with EN 50136-1:2012 + A1:2018 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 50131-6:2017 (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.

Processing of personal data

Prime control panels, by attributing them to installers and users registered with the Inim Cloud service, can be managed through dedicated web pages and/or apps available to both the installer and the end user.

In order to allow management of the control panel via Inim Cloud an explicit request is required from the users to whom the control panel is to be associated.

As soon as a control panel is connected to a LAN or a GSM/LTE network, it will be available on the Inim Cloud, however, until the association is explicitly requested by a user the data exchanged are:

- purely technical (in order to allow an association to a user in the future) and do not include any personal data
- always encrypted
- free from any correlation with personal data that may already be present in the Inim Cloud

The control panel events log becomes available only after associating the control panel with the users and can be viewed chronologically from the moment of such an association.

If you do not want to manage the control panel via Inim Cloud and/or do not want to allow, in a preventive way, any type of connection to Inim Cloud, it is necessary to request the intervention of the installer who, through appropriate programming, will prevent the aforementioned connection.

Table of contents

Chapter 1 General information	5
1.1 Manufacturer's details	5
1.2 Registered patents	5
1.3 Operator Qualifications	5
1.4 Access Levels	6
1.5 Manuals	6
1.6 Documents for the users	6
1.7 About this manual	6
1.8 Copyright	7
1.9 Terminology	7
1.10 Graphic conventions	7
Chapter 2 The Prime system	8
2.1 Description of products	8
2.2 The Technologies	9
2.3 Voice functions	9
2.4 Telephone functions	10
2.5 WEB / e-mail functions	10
2.6 Videosurveillance	11
2.7 The service Inim Cloud	11
2.8 Inim Home application	11
2.9 The Marilyn More voice system	12
2.10 Flexibility of the Prime system	13
Chapter 3 User of the Prime system	14
3.1 User Codes	14
3.2 Access to user menu	15
3.3 Multi-system access	15
Chapter 4 Shortcut	16
4.1 Keypad shortcuts	18
4.2 Shortcut with code	19
4.3 Key and Reader shortcuts	20
4.3.1 Shortcuts on external readers	20
4.3.2 Shortcuts on readers integrated	20
4.3.3 Remote-control shortcuts	21
4.4 Shortcuts on event	21
Chapter 5 Use of the Prime system	22
5.1 Managing alarms	22
5.2 Arming and disarming partitions	23
5.3 Arming scenarios	24
5.4 Voice memo	25
5.5 Activations	26
5.6 Outputs management	27
5.7 Change code PIN	27
5.8 Change telephone numbers	27
5.9 Connection to a LAN/Wi-Fi network	28
5.10 Overtime request	28
5.11 Thermostats	28
5.12 Listen-in	29
5.13 Partition status enquiry	29
5.14 Graphic maps	30
Chapter 6 Using the keypads	32
6.1 Keypad displays	34
6.1.1 The LCD keypad screen	34
6.1.2 Touch-screen keypad displays	35
6.2 Status icons on screen	37
6.3 Use of the keys	38
6.3.1 LCD keypad buttons	38
6.3.2 Keys of touch-screen keypads	38
6.3.3 Emergency functions	39
6.4 LED signalling	40
6.5 Signalling on the Buzzer	41
6.6 Operations from LCD keypads	41
6.6.1 Managing alarms	41
6.6.2 Arming commands and scenarios	42
6.6.3 Voicebox and intercom functions	43
6.6.4 Activations	43
6.6.5 View	44
6.6.6 Outputs management	45
6.6.7 Change date and time	46
6.6.8 Keypad and display settings	46
6.6.9 Change PIN codes	47
6.6.10 Change telephone numbers	47
6.6.11 Connection to a LAN network	47
6.6.12 Network connection test	48
6.6.13 Overtime request	48

6.6.14	Thermostats management	49
6.6.15	Code Management	49
6.6.16	Timer programming	51
6.6.17	Partition status enquiry	52
6.7	Operations via touch-screen keypad	52
6.7.1	Managing alarms	52
6.7.2	Arming commands and scenarios	52
6.7.3	Voicebox and intercom functions	52
6.7.4	Activations	53
6.7.5	View	53
6.7.6	Outputs management	55
6.7.7	Change date and time	55
6.7.8	Touch-screen display settings	55
6.7.9	Change code PIN	56
6.7.10	Change telephone numbers	56
6.7.11	Overtime request	56
6.7.12	Thermostats management	57
6.7.13	Photo frame	57
6.7.14	Alarm clock and memo	57
6.7.15	Graphic maps via touch-screen keypad	58
Chapter 7	Use of proximity readers and digital keys	59
7.1	Proximity readers	59
7.1.1	Signalling on reader LEDs	59
7.2	Keys	60
7.3	Remote-control keys	61
7.4	Reader and key operations	61
7.4.1	Managing alarms	61
7.4.2	Arming commands and scenarios	62
7.4.3	Outputs management	62
7.4.4	Overtime request	62
7.4.5	Operations via remote-control keys	62
7.4.6	Use of remote-controls with low battery	62
Chapter 8	Commands over the phone	63
8.1	Use of phone calls	63
8.1.1	Panel to user calls	63
8.1.2	User to control panel calls	63
8.2	Use of SMS text messages	63
8.2.1	SMS text message from panel to user	63
8.2.2	SMS text message from user to panel	64
8.3	Operations via telephone	64
8.3.1	Managing alarms	64
8.3.2	Arming commands and scenarios	64
8.3.3	Activation of outputs	65
8.3.4	Overtime request	65
8.3.5	Listen-in	65
8.3.6	Partition status enquiry	65
Chapter 9	Use of the web server	66
9.1	Sections of the web interface	66
9.2	Access to and use of the Web interface	67
9.3	Operations via web server	68
9.3.1	Managing alarms	68
9.3.2	Arming commands and scenarios	68
9.3.3	Viewing and activations	68
9.3.4	Camera access	70
9.3.5	Remote keypads	70
9.3.6	Graphic maps via web server	70
9.4	e-mail	71
Appendix A	Glossary	72
Appendix B	Fault signals	77

Chapter 1 General information

1.1 Manufacturer's details

Manufacturer: Inim Electronics S.r.l.
Production plant: Centobuchi, via Dei Lavoratori 10
63076 Montepreandone (AP), Italy
Tel.: +39 0735 705007
Fax: +39 0735 734912
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 only on devices marketed under the brand Inim Electronics.

1.2 Registered patents

The Prime series of control panels include technology covered by the following patents:

- **Input/Output Terminals:** terminals "T1" and "T2" on-board the control panel can be configured by the installer as either input or output zones.
- **nBy/X proximity reader:** this reader has been especially designed to flush-mount to all models of light switch boxes.
- **Learn zone balancing:** under opportune conditions, this option allows the installer to start the process of automatic learning of the balancing of all the system zones, thus eliminating the task of entering the value of each zone in separately.

1.3 Operator Qualifications

Installer

The installer is the person (or group of persons) who sets up and programs the entire security system in accordance with the purchaser's requirements and in respect of the safety laws in force. It is the responsibility of the installer to instruct the user on how to use the security system properly.

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

The access code of the installer is a level 3 access code (see "Access Levels").

User

The user or users are the occupants of the premises where the Prime anti-intrusion system is installed. The users can arm and disarm the system or parts of it after valid authentication.

As a result of the extreme flexibility of the system, the most frequent operations can be carried out without prior authorization. This operating method must be expressly requested by the purchaser who must be made aware of the risks that this way of operating entails (false alarms, accidental arm/disarm operations, etc).

Each user is associated with a system access code. The code programming process allows you to define the code hierarchy:

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

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

- enable/disable
- change PIN
- change some of the programming parameters

1.4 Access Levels

Specific legislation defines the following levels of access to the control panel, distinct from the limitations of system usability:

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

1.5 Manuals

The manuals which are not supplied with the apparatus can be ordered, making reference to their respective codes, or downloaded from www.inim.biz.

Installation and programming guide

The guide, supplied with each control panel, provides all the instructions and illustrations necessary for fast installation and programming of the Prime system.

This leaflet provides a quick guide to first startup, together with the wiring diagrams for the necessary connections, a table for the peripheral addresses, a quick guide to system programming as well as the default values of the programming parameters.

Installation manual

The installation manual contains the technical specifications of all the system components and the instructions for their installation, including instructions with wiring diagrams for the various modules.

It also contains the instructions for system commissioning

It is the responsibility of the installer to follow all the manufacturer's instructions in order to ensure proper functioning of the system and, at the same time, to comply with all the warnings relating to the active and passive security of the installation.

Programming manual

The Programming manual contains instructions for the configuration and programming of the Prime system, as well as the descriptions of all the parameters and options, regardless of the means chosen for the programming process (keypad, software, etc.).

It also contains the instructions for commissioning, maintenance and troubleshooting procedures.

Software program

The Prime/STUDIO software manual contains the description of the software and the instructions for its installation and use.

It is the responsibility of the person who programs the Prime system to follow the instructions carefully and to ensure they have complete knowledge of the software in order to proceed swiftly and properly with the configuration and programming procedures.

User's manual (this manual)

This manual contains instructions relating to the user interface of the Prime control panel, its functions and use.

Supplied with every control panel, this manual must be given to the user who must be aware of and have fully understood all the system functions as well as the configuration set by the installer.

1.6 Documents for the users

Declarations of Performance, Declarations of Conformity and Certificates concerning to Inim Electronics S.r.l. products may be downloaded free of charge from the web address www.inim.biz, getting access to Extended Access and then selecting 'Certifications' or requested to the e-mail address info@inim.biz or requested by ordinary mail to the address shown in this manual.

Manuals can be downloaded free of charge from the web address www.inim.biz, after authentication of credentials and by directly by accessing the page of each product.

1.7 About this manual

Manual code: DCMUINE0PRIMEE

Revision: 170

1.8 Copyright

The information contained in this document is the sole property of Inim Electronics S.r.l.. Copying, reprinting or modification of this document, in part or as a whole, is not permitted without prior authorization in writing from Inim Electronics S.r.l.. All rights reserved.

1.9 Terminology

Panel, control panel, device

Refer to the main supervisory unit and any constituent parts of the Prime security system.

Left, Right, Behind, Above, Below

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

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 element of the interface (drop-down menu, options box, graphic object, etc.).

Press

Means click-on a video button or push a key on the control-panel keypad.

1.10 Graphic conventions

The following images represent the display of a control panel with an LCD screen and relative signalling. For other types of displays, it is necessary to refer exclusively to the notifications which are shown and not to the image shown:



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.

DANGER!



The DANGER warnings indicate that total or partial disregard of the procedure could injure the operator or persons in the vicinity.

Chapter 2 The Prime system

A typical Prime system comprises:

- a Prime control panel
- alarm signalling devices and, generally, the events detected by the system (wireless sounders, visual-audible signalling devices, etc.)
- wireless intrusion-detection devices (PIR or microwave detectors, magnetic contacts, linear beam detectors, etc.)
- system control peripherals: proximity readers, wireless keypads

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 immediate and clear identification of the operations to be carried out.

Besides the keypad, the system can also be managed via proximity readers which provide an interface for fast execution of the most frequent daily operations, i.e. arming and disarming. Users in possession of electronic keys can activate the functions they are enabled to control by holding the key in the vicinity of the proximity key reader.

All models of the control panel manage a wireless system for the deployment of wireless and remote-control devices.

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).

Moreover, the Prime has automation functions, such as programmed arming and disarming, access control, activation and deactivation of outputs, suitably categorized (signaling devices, gates, light points, roller shutters, sprinklers, air conditioners, household appliances, etc.).

2.1 Description of products

Description Models and Functions

anti-intrusion control panel

Prime060S, Prime060L, Prime120L, Prime240L, Prime500L

Table 2.1: Control panels - main features

Control panel models	Prime060S	Prime060L	Prime120L	Prime240L	Prime500L
Total terminals	60		120	240	500
Total zones	120		240	480	1000
Outputs on control-panel motherboard			15		
Partitions	10		20	30	
Keypads	10		15		30
Voice memo slots			10		
Expansions			100		
Proximity readers			60		
Sounder/flashers			10		
Wireless transceiver	20			30	
Digital keys and wireless command devices			150		500
Possible key combinations			4294967296		
Isolators			16		
Temperature probes			15		
Home-automation modules			30		
Wi-Fi boards			1		
GSM, GPRS, UMTS, HSPA and LTE communicator			1		
Codes	50		100		500

Control panel models	Prime060S	Prime060L	Prime120L	Prime240L	Prime500L
Scenarios	50				
Timers	40				
Recordable Events	4000				
Programmable events	60				

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 grade

3

ATS categories

up to SP6 or DP4 (in accordance with configurations)

2.2

The Technologies

EASY4U



This user-friendly tool provides an interesting array of graphic features and functions.

All Prime intrusion control panels are controlled by keypads equipped with 96x32 pixel graphic displays. The four-line alphanumeric display screen (16 characters per line) can be edited or used to view the icons associated with various customized user-operations.

The use of customizable graphic-objects, which indicate the system status, helps users to understand what is happening on the system.

The keypad shortcuts allow time-consuming sequences to be transformed into simple keystroke actions. They can be used for a variety of tasks and make operations less tedious and less error-prone. In this way, INIM has eliminated the repetitive sequences of keystrokes required by other systems available on the market.

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

VOIB



This is an acronym for "Voice Over Inim-bus".

VOIB technology allows the system to manage end-to-end digitized voice transmissions at extremely high-speed over the IBUS. Voice transmissions can be carried to all points of the IBUS.

Keypads that provide a built-in microphone and speaker allow recording and playback of messages of the control panel.

The 30 minute capacity voice board allows each event to be associated with a message. Voice digitizing and compression allow the signal to be transmitted in data packets over the bus to recipient keypads where it is announced. Voice digitizing and the characteristics of the I-BUS allow end-to-end "noise-immune" voice transmissions without the need of any additional wiring.

2.3

Voice functions

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

The installer can program the voice messages that will be played:

- for calls associated with events
- on the control panel in correspondence to events

Each keypad 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 (see "Voice memo"). 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, as described in "LED signalling".

The SmartLogos30M voice board provides a total of 60 seconds for voice messages.

Note

The maximum number of voicemail slots is 10.

2.4 Telephone functions

For each of the events recognized by the Prime control panel, it is possible to activate report calls to Alarm receiving Centres (via digital dialer), as well as voice calls and SMS messages to specific contact numbers.

By calling the Prime control panel or receiving a call from it (via voice dialer), it is possible to enter a valid code PIN and activate shortcut commands and customized automatic functions.

The shortcuts are available on keys "0" to "9" of the phone keypad after entry of a valid code PIN. Each code can be programmed with customized shortcuts, such as: arm or disarm the system, activate or 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.

Furthermore, It is possible to activate the listen-in function which allows the user to listen to the sounds picked up by the microphone of the keypads located on the protected premises..

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

2.5 WEB / e-mail functions



The PrimeLAN board provides full access to the Prime system functions both for user and installer codes even when Inim Electronics software is not installed on the computer in use. An Internet connection is necessary via a PC or through the Inim Home 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, recipients and attachments must be programmed by your installer ("e-mail").

In addition to the 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 "Use of the web server".

2.6 Videosurveillance

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 “web cams”) which use one URL address for the viewing of videos:

- 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 recordings (images or videos) is achieved by accessing the URL address of the camera. It can be done via web browser or Inim Home 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 The service Inim Cloud



The Inim Electronics Cloud service provides users of INIM anti-intrusion control panels with an additional management mode via the internet.

The connection of control panels to the Cloud service is achieved via a web interface 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 control panel network boards, as these boards are programmed by default with the DHCP enabled (option that allows the automatic assignment of an IP address to devices on the network).

User access to the service can only take place after proper registration on the www.inimcloud.com site, which returns credentials.

At this point you can have access in the following modes:

- via a web browser, using a customized web interface which provides tools to supervise all the registered control panels
- via Inim Home, an application that allows you to supervise the system with all its functions and to receive all the desired notifications through “push” type notifications
- via voice assistant, using the Marilyn More home-automation and anti-intrusion alarm system

For the use of Inim Cloud refer to the service manual, available at www.inimcloud.com, by logging into your account.

2.8 Inim Home application



Inim Home is an App dedicated to end users for the remote control of their installations via smart phone or tablet. The application allows you to view and manage all the features of the system:

- visualization of:
 - status of the partitions (armed / disarmed)
 - status of the scenarios
 - presence of faults
 - status of the detectors (in alarm / stand-by / tamper / bypassed)
 - events log
 - status of the thermostats
 - status of the control panel and peripheral devices
- commands for:
 - arm / disarm partitions
 - apply scenarios

- bypass / unbypass detectors
- activate single outputs and output groups

Following the appropriate setup implemented by the installer, the Inim Home App groups the outputs (lighting activations, gate control, management of motorized roller shutters, household appliances) and presents them in a coherently categorized way to the user. Inside each category of activations/outputs, the user can create their own groups, choose which elements to add to favourites in order to have easy access on the home page relating to their system and thus adapt the app to each specific need.

Also available is interaction with videocameras for real-time video verification. Inim Home allows you to associate one or more videocameras to a detector and display on your smartphone the real-time video from the videocameras activated in the event of an alarm on the detector in question. If cameras with ONVIF standard are used it is possible to control the PTZ movements of the camera as well as view multiple cameras simultaneously.

Inim Home is generally used through the Inim Cloud service and, therefore, the user must create their own account on the www.inimcloud.com website. By taking advantage of the potential of the Cloud, the user can receive push notifications regarding alarms, faults, arming/disarming operations and the status of the connection. It is also possible to use Inim Home in direct connection with control panels, without going through the Cloud, however, in this case it is not possible to obtain push notifications.

Inim Home is therefore available in two versions:

- Inim Home, which interfaces with the Inim Cloud service
- Inim Home P2P, which allows connection to the control panels via direct point-to-point connection.

For the use of Inim Home, please refer to the application manual, available at www.inim.biz or to the App itself.

2.9

The Marilyn More voice system



The Marilyn More home automation and anti-intrusion system, based on the Inim Electronics anti-intrusion control panels, is integrated with the most widely used smart speakers and smartphones with voice assistant (GoogleHome, Amazon Alexa, ect.).

The user of the control panel interfaces with the system using voice commands, thus being able to carry out system management and supervision operations.

The Marilyn More system is an accessory to the Inim Electronics Cloud service. It is therefore necessary that the user has their own account at website www.inimcloud.com and has registered in their profile the control panels they want to operate.

The operations available from the voice assistant are:

- **Scenarios management**
A scenario is a system configuration through which it is possible to arm/disarm the partitions of the security system and activate one or more outputs when it is used. The scenario applied, such as the arming status of the system or part of it, can be notified to the user and via this can be modified.
- **Outputs management**
The user can manually activate or deactivate the outputs their code is enabled to operate as well as query their status.
- **Inputs management**
The user can query the voice assistant for information about the enabled/disabled status of the inputs, zones, detectors and devices connected to the control panel and which monitor the system. Additionally, the user can change the operating status of the control panel signaling inputs.
- **Thermostats management**
This function allows the user to manage the heating and air-conditioning systems connected to the control panel, through activation or shutdown operations and notification requests.

The possibility of using each function is linked to the features of the system, to its programming and to the configuration of the voice functions, which must be duly programmed before they can be used.

Note

Inim Electronics is committed to guaranteeing the widest compatibility with the functions of the Google and Amazon voice assistants, however the possibility is not excluded that the suppliers of the voice systems introduce limitations or particular operating characteristics in such a way as to modify the experience with Marilyn More. It should be noted that any such changes do not depend on the will of Inim Electronics.

Google Home is a trademark of **Google LLC**.

Amazon, Alexa and its related logos are registered trademarks of **Amazon.com, Inc.** or affiliates.

For the use of Inim Cloud refer to the manual of the service, available at www.inim.biz.

2.10 Flexibility of the Prime system

Prime control panels, in addition to the typical functions offered by anti-intrusion systems, also provide users with accessory functions which do not necessarily involve the purpose of anti-intrusion, such functions provide for the use of devices alternative to those available.

For instance, it is possible to schedule the ON/Off times of lights; access 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

Chapter 3 User of the Prime system

3.1 User Codes

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".

Note

For security reasons all the system default codes must be changed. The installer must provide each of the system users with a code PIN that must be changed immediately to a code PIN 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.
When a code is entered at a keypad, the user will be allowed to operate only the partitions which are enabled for both the code and keypad in use. For example, if a code enabled on partitions 1, 2 and 3 is entered at a keypad which enabled on partitions 2, 3 and 4, it will be able to operate on partitions 2 and 3 only.
- **User type**
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 some of the programming parameters
- The **way of accessing the user menu**.
Each code can access its customized menu in 3 different ways (see "Access to user menu").
- The **commands over the phone**.
Authorization to issue commands from a phone. 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 phone keypad the user can activate the required shortcut (see "Shortcut with code") This method of entering commands will affect the code partitions only.
- **Time limitation of code operativity**
If a code is associated with one of the timers, it will be able to access and operate on the system only when the timer is On.
- **Group of outputs which can be activated/deactivated manually**
After accessing the Domotic commands section (user menu) you can activate/deactivate the appropriately programmed outputs.
- The **menu sections** the user has access to (see "Access to user menu", Mode "A").
- **Customized shortcuts**.
Each code can be programmed to manage:

- up to 12 customized (personal) shortcuts assigned to keys **F1**, ..., **F4**
 - up to 10 customized (personal) shortcuts assigned to keys **0**, ..., **9**
- These shortcuts are available to the code user after accessing the user menu.

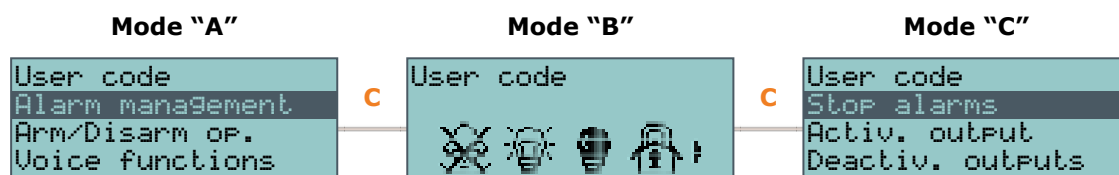
3.2 Access to user menu

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:



Mode "A"

The user accesses the user menu directly:

- Alarm management
- Arm/Disarm op.
- Voice functions
- Activations
- View
- Home-automation commands
- Set date/time
- Keypad settings
- Change PIN
- TelephoneNumbers
- Settings
- Overtime request
- Thermostat
- Codes
- Timers

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

Mode "B"

The keypad deletes the icons of the shortcuts assigned to buttons **F1**, ..., **F4** 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**, ..., **F4** and **0**, ..., **9**.

Mode "C"

The user can access a descriptive menu of the customized shortcuts assigned to buttons **F1**, ..., **F4**. 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.

3.3 Multi-system access

A user in possession of a key or a PIN (code) or a wireless remote-control device can manage one or more systems using the same key or the same PIN. 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 3, 4 and 5 on system B and on partitions 4 and 5 on system C.

This operating method is possible for all keys and codes.

Chapter 4 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 divided into three categories:



- immediate command shortcuts, which activate functions instantly
- service shortcuts, that provide direct access to the 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 phone, readers, keys or wireless remote-control keys) and the category it belongs to.

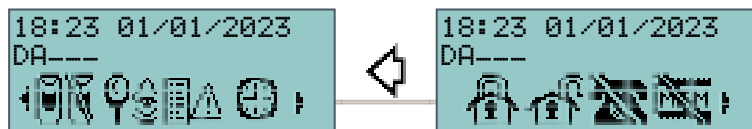
Shortcut			on keypad			on code		on reader		on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over the phone	stand alone	via keypad		
Arm/Disarm	Applies a pre-set scenario	which scenario	1		Arm/Disarm	Available	Available	Available	Available	Available	Available Activate scenario
Stop alarms	Shortcut that deactivates instantly the outputs relative to alarm and tamper events and deletes the partition and system alarm and tamper memories.		2		Stop alarms	Available	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	Available	Not available
Delete memory	Deletes memory of system and partition alarm and tamper events.		4		Delete memory	Available	Available	Available	Available	Available	Available
Activate output	Activates one of the programmed outputs.	which output	5		Activ. output	Available	Available	Available	Available	Available	Available
Deactivate output	Deactivates one of the programmed outputs.	which output	6		Deactiv. output	Available	Available	Available	Available	Available	Available
Overtime	Delays partition auto-arming time by 30 minutes.		7		Over time	Available	Available	Available	Available	Available	Not available
Settings menu	Accesses the user menu section: Settings	Reference code (on reader and key)	8		Settings menu	Available	Not available	Not available	Available	Available	Not available
StartVoiceNotifier	Plays a recorded voice message which announces the shortcuts assigned to the number keys.		9		Voice menu	Available (only for number keys)	Available	Not available	Not available	Not available	Not available
Listen-in	Allows listen-in sessions via phone by means of a microphone on one of the available keypads.	Keypad	10		Listen-in	Not available	Available	Not available	Not available	Not available	Not available
Intercom Call	Accesses the user menu section: Voice functions/ Intercom	Reference code (on reader and key)	11		Intercom call	Available	Not available	Not available	Available	Available	Not available
Arm/Disarm menu	Accesses the user menu section: Arm/Disarm op.	Reference code (on reader and key)	12		Arm/Disarm menu	Available	Not available	Not available	Available	Available	Not available
Alarm management menu	Accesses the user menu section: Alarm management	Reference code (on reader and key)	13		Alarm menu	Available	Not available	Not available	Available	Available	Not available
Voice functions menu	Accesses the user menu section: Voice functions	Reference code (on reader and key)	14		Voice func. menu	Available	Not available	Not available	Available	Available	Not available

Shortcut			on keypad		on code		on reader		on keys	on event
description	function	parameter	n.	Icon	String	via keypad	over the phone	stand alone	via keypad	
Activations menu	Accesses the user menu section: Activations	Reference code (on reader and key)	15		Activations menu	Available	Not available	Not available	Available	Available Not available
Sol-2G/3G/4G status menu	Accesses the user menu section: View / Sol-2G/3G/4G status	Reference code (on reader and key)	16		Sol-2G/3G/4G status menu	Available	Not available	Not available	Available	Available Not available
Arming status	Plays a voice announcement regarding the armed/disarmed status of partitions.	Reference code (on reader and key)	17		Arming status	Available	Available	Not available	Not available	Not available Not available
Keypad settings	Accesses the user menu section: Keypad settings	Reference code (on reader and key)	18		Keypad sett.menu	Available	Not available	Not available	Available	Available Not available
Zone activations menu	Accesses the user menu section: Activations / Zones	Reference code (on reader and key)	19		ZoneBypass menu	Available	Not available	Not available	Available	Available Not available
Voice memo	Accesses the user menu section: Voice functions	Reference code (on reader and key)	20		Voice memo	Available	Not available	Not available	Available	Available Not available
ON/OFF output menu	Accesses the user menu section: Home-automation commands	Reference code (on reader and key)	21		Output control	Available	Not available	Not available	Available	Available Not available
Enable/Disable answerphone	Accesses the user menu section: Activations / Answerphone	Reference code (on reader and key)	22		Enab. answerphone	Available	Not available	Not available	Available	Available Not available
Activate output scenarios	Activate one of the programmed output scenarios	which scenario	23		Output scenario	Available	Available	Not available	Not available	Not available Not available
Enable codes	Accesses the user menu section: Activations / Codes	Reference code (on reader and key)	24		Enable codes	Available	Not available	Not available	Available	Available Not available
Enable keys	Accesses the user menu section: Activations / Keys	Reference code (on reader and key)	25		Enable keys	Available	Not available	Not available	Available	Available Not available
Enable timers	Accesses the user menu section: Activations / Timers	Reference code (on reader and key)	26		Enable timers	Available	Not available	Not available	Available	Available Not available
Enable auto-arming	Accesses the user menu section: Activations / Auto-arming	Reference code (on reader and key)	27		Enab. auto-arm	Available	Not available	Not available	Available	Available Not available
View events log	Accesses the user menu section: View / Events log	Reference code (on reader and key)	28		View events log	Available	Not available	Not available	Available	Available Not available
View alarms log	Accesses the user menu section: View / Alarms log	Reference code (on reader and key)	29		View alarm log	Available	Not available	Not available	Available	Available Not available
View faults log	Accesses the user menu section: View / Faults log	Reference code (on reader and key)	30		View faults log	Available	Not available	Not available	Available	Available Not available
View arm/disarm operations	Accesses the user menu section: View / Arm/Disarm op.	Reference code (on reader and key)	31		View arm ops log	Available	Not available	Not available	Available	Available Not available
View system status	Accesses the user menu section: View / System status	Reference code (on reader and key)	32		ViewSystemStatus	Available	Not available	Not available	Available	Available Not available
View zone status	Accesses the user menu section: View / Zone status	Reference code (on reader and key)	33		View zone status	Available	Not available	Not available	Available	Available Not available
Change PIN code	Accesses the user menu section: Change PIN	Reference code (on reader and key)	34		Change PIN	Available	Not available	Not available	Available	Available Not available
Time/Date	Accesses the user menu section: Set date/time	Reference code (on reader and key)	35		Time/Date	Available	Not available	Not available	Available	Available Not available
View faults	Accesses the user menu section: View / Faults present	Reference code (on reader and key)	36		View faults	Available	Not available	Not available	Available	Available Not available

Shortcut			on keypad			on code		on reader			
description	function	parameter	n.	Icon	String	via keypad	over the phone	stand alone	via keypad	on keys	on event
Thermostat menu	Accesses the user menu section: Thermostat	Reference code (on reader and key)	37		Thermostat menu	Available	Not available	Not available	Available	Available	Not available
Panic	Activates a "Panic" event	which panic event	38		Panic	Available	Available	Not 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	Not available	Available
Unbypass zone	Unbypasses one of the configured zones	which zone			Not available	Not available	Not available	Not available	Not available	Not available	Available
Disable code	Disables one of the configured codes	which code			Not available	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	Not available	Available
Disable key	Disables one of the configured keys	which key			Not available	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	Not available	Available
Activate thermostat	Activates the thermostat in the selected operating mode	which thermostat which mode			Not available	Not available	Not available	Not available	Not available	Not available	Available
Deactivate thermostat	Deactivates the thermostat	which thermostat			Not available	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	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	Not available	Available

4.1 Keypad shortcuts

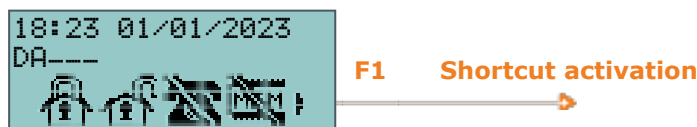
The installer can program each LCD keypad with up to 12 shortcuts associated with 4 function keys **F1**, **F2**, **F3**, **F4**. The shortcuts are identified by icons which appear on the lower part of the display. The presence of arrows to the far right and left of the icons indicate that by pressing keys **Q**, **P**, the user can access other shortcuts in cases where there are more than 4 on the keypad.



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

A. By ALL.

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



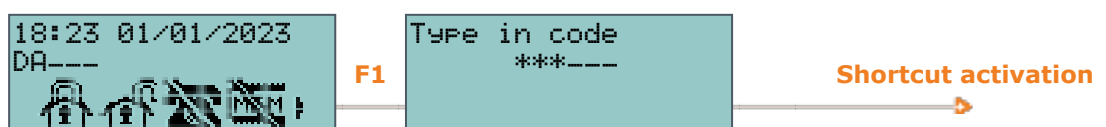
B. Code users only.

After pressing the respective key **F1**, ..., **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.

C. By code users only when activation of the shortcut lowers system security.

("Requires authorization in the event of lowered security").

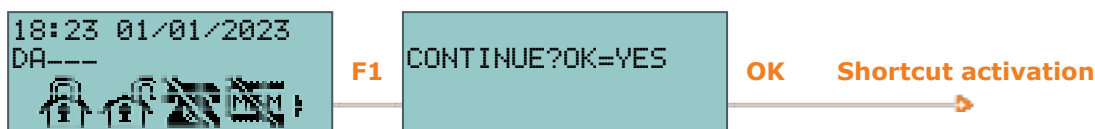
If a shortcut involves a scenario that completely disarms a partition, or switches a partition from Away mode to Stay mode, the security of the system will obviously be lowered, therefore, the system will request code entry. The shortcut will affect the partitions common to both the keypad and code.



D. By ALL with confirmation request.

Pressing the respective key **F1**, ..., **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.



To activate the desired shortcut, press the button **F1**, ..., **F4** that corresponds to the icon that identifies the shortcut. The system will activate the shortcut instantly (case A), or will request explicit confirmation (case D), or will request code entry (cases B and C).

touch-screen keypads do not have function keys **F1**, **F2**, **F3**, **F4**, nor do they provide access to certain functions via shortcuts. However, they provide buttons on the display which, with a single tap, activate functions and applications. For further details refer to "Keys of touch-screen keypads".

Table 4.1: Default shortcuts from the keypad

Shortcut	Icon	Description	Operation	Confirm
Arm in Away mode	n.1	AWAY	Arms all the system partitions.	No confirmation or valid code entry required.
Disarm the system	n.37	DISARM	Disarms all the system partitions.	Valid code entry required.
Clear call queue	n.3	Clear call queue	Cancels the entire call queue and stops ongoing calls (if any).	Valid code entry required.
Delete memory	n.4	Delete memory	Deletes memory of system and partition alarm and tamper events.	Valid code entry required.
Zone activations menu	n.19	Zone activations menu	Accesses the user menu section: Activations / Zones	Valid code entry required.
View alarms log	n.29	View alarm log	Accesses the user menu section: View / Alarms log	No confirmation or valid code entry required.
View faults	n.36	View faults	Accesses the user menu section: View / Faults present	No confirmation or valid code entry required.
Time/Date	n.35	Time/Date	Accesses the user menu section: Set date/time	Valid code entry required.
Voice functions menu	n.14	Voice func. menu	Accesses the user menu section: Voice functions	No confirmation or valid code entry required.
Intercom Call	n.11	Intercom Call	Accesses the user menu section: Voice functions / Intercom	No confirmation or valid code entry required.
Thermostat menu	n.37	Thermostat menu	Accesses the user menu section: Thermostat	No confirmation or valid code entry required.
Keypad settings	n.18	Keypad sett. menu	Accesses the user menu section: Keypad settings	No confirmation or valid code entry required.

4.2 Shortcut with code

Besides the keypad shortcuts provided by the function keys **F1**, **F2**, **F3**, **F4**, 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 (see "Access to user menu"). Each code can be programmed to manage:

- up to 12 shortcuts can be activated by keys **F1**, ..., **F4** and identified by explicit icons
- up to 10 shortcuts can be activated by keys **0**, ..., **9**. 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 mode described in the paragraph "Access to user menu", Mode "B".

3. Press the key **F1**, ..., **F4** which corresponds to the shortcut icon or press the key **0**, ..., **9** 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 (via a telephone call to or from 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 Shortcuts on external readers

The user must hold the electronic key in the vicinity of the reader, as soon as the reader recognizes the key, the relevant LEDs will light to indicate the various shortcuts.

When the required shortcut is indicated, the user must move the key away from the reader to activate the required shortcut.

The lighted sequence on the Reader LEDs is as follows (see also "Signalling on reader LEDs"):

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 moved away.


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

LEDs not enabled

If the installer has enabled option "50131ReadLedOFF", the reader LEDs will be off, therefore, to select and activate a shortcut, it is necessary to:

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

4.3.2 Shortcuts on readers integrated

To activate a shortcut the user must hold their digital key in the vicinity of the reader-integrated on the keypad (the position of the reader is indicated by the  symbol, instead on the Alien keypad it is positioned in the lower right-hand corner of the front plate).

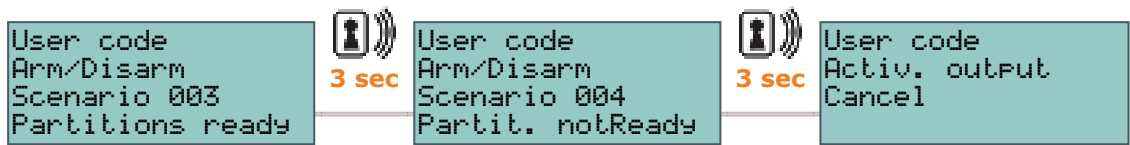
As soon as the key is recognized, the reader display will show, one-by-one at 3 second intervals, the shortcuts available on the reader and on the key. When the required shortcut is indicated, the user must move the key away from the reader to activate the required shortcut.

The shortcuts appear on the display in the following order:

1. Description of the first reader shortcut for 3 seconds
2. Description of the second reader shortcut for 3 seconds
3. Description of the third reader shortcut for 3 seconds
4. Description of the fourth reader shortcut for 3 seconds

5. Description of the fourth reader shortcut for 3 seconds
6. The "Disarm" string, to disarm all the partitions
7. Then, starting at point 1., the system will run through the sequence again until the user moves the key away in order to select the shortcut indicated at the time.

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



4.3.3 Remote-control shortcuts

To activate the shortcuts programmed by the installer on the 4 remote-control buttons, the user simply needs to press the button which corresponds to the desired shortcut. The successful outcome of the operation will be signalled by the buzzer and LEDs on the remote control itself (see "Remote-control keys").

Super keys

Furthermore, if the "super keys" function is enabled, by pressing and holding the button for at least 2 seconds, until a second beep is emitted, you can activate a shortcut different from the one associated by simply pressing the button.
In this way you can have up to 8 different shortcuts on each remote-control key.

4.4 Shortcuts on event

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 Use of the Prime system

The Prime system can be accessed and operated in the following ways:

- via **keypad with a display (LCD)** (Joy, nCode/G, Aria/HG, Concept/G and Air2-Aria/W)
In this case the user can operate the system in two ways:
 - by means of shortcuts (see "*Keypad shortcuts*")
 - by entering a valid code that accesses the respective user menu (see "*Access to user menu*")
Refer to "*Operations from LCD keypads*".
- Via **touch-screen display** (Alien)
in this case, users are provided with buttons, displayed on the screen, that with a single tap activate functions and applications. For further details refer to "*Operations via touch-screen keypad*".
- Via **proximity reader** (nBy external or integrated)
in this case it is necessary to use a valid key and there is only one way of accessing the system, as described in "*Reader and key operations*".
- Via **remote-control device**
by pressing the keys, as described in "*Operations via remote-control keys*".
- via **telephone**
during a call from/to the control panel or via an SMS message and valid code entry (PIN). Refer to "*Operations via telephone*".
- Via **web server**
by means of the integrated web-server on the PrimeLAN board (if installed) through any browser (see "*Use of the web server*").
- from **Inim Cloud**
by means of a browser, the user can access a customized web interface which provides all the registered control panels.
- Via **Inim Home application**
in this case the user has remote functions and applications.
- Via **Marilyn More voice assistant**
by means of voice commands.

5.1 Managing alarms

The 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 act of delinquency) is detected on one of the devices connected to the BUS (reader, wireless receiver)
- Peripheral loss, when sudden loss of one of the devices connected to the BUS occurs
- Loss of or tamper on a wireless device
- 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
-  touch-screen display
-  proximity reader
-  keyfobs (remote-control keys)
-  telephone
-  web server
-  Inim Cloud
-  Marilyn More voice assistant

5.2 Arming and disarming partitions

The operating status of partitions can be changed by users who are authorized to access them. Via the appropriate user access sections for management of the system, it is possible to request the following commands:

- **Disarm** - this operation disables the partition completely. During this status, none of the zones belonging to the partition can generate alarms.
- **Away mode** - this operation enables the interior and perimeter zones of the partition. During this status, all of the zones belonging to the partition can generate alarms.
- **Stay mode** - this operation enables only the perimeter zones of the partition. During this status, all the zones belonging to the partition, with the exception of interior zones, can generate alarms.
- **Instant mode** - this operation enables the perimeter zones only and annuls delays. During this status, all the zones belonging to the partition, with the exception of the interior zones, can generate instant alarms with no entry-time delay.
- **Hold** - this operation forces the partition to hold its current status.

When a partition is armed, generally the zones belonging to it 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 "AC 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
-  touch-screen display
-  proximity reader
-  keyfobs (remote-control keys)
-  telephone
-  automatic arming/disarming
-  Violation of a command zone
-  web server
-  Inim Cloud

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 (see "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

Via "command" zone

The zones of an installation of Prime control panels can be suitably programmed according to needs. The programming of these also defines the "type".

A "command" type zone, if violated, does not generate alarms but executes the command it is assigned to.

Prime control panels manage the following commands:

- "Disarm" zone: if activated, it will disarm all the partitions it belongs to.
Zones configured in this way can be used to disarm partitions by means of a keyswitch.
- "Arm" zone: if activated, it will arm all the partitions it belongs to.
For example, keyswitches are usually configured as command zones.
- "OnArm/OffDisarm zone" zone: if activated, it will generate an arm-partitions command and, the instant it restores to standby, a disarm-partitions command. The command will affect only the partitions the zone belongs to.
Zones configured in this way can be used to arm/disarm partitions by means of a keyswitch.
- "Switch" zone: if activated when all the partitions it belongs to are disarmed, it will arm all the partitions. If activated when even one of the partitions it belongs to is armed, it will disarm all of its partitions. The command will affect only the partitions the zone belongs to.
Zones configured in this way can be used to arm/disarm partitions by means of a keyswitch.
- "Patrol" zone: if activated, it will have a patrol function in all the partitions it belongs to.









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 one or several outputs simultaneously.

The installer will program the system and make available the scenarios which best suit user requirements.

The user can activate the scenarios via:

-  LCD keypad
-  touch-screen display
-  proximity reader
-  keyfobs (remote-control keys)
-  telephone
-  web server
-  Inim Cloud
-  Marilyn More voice assistant

5.4 Voice memo

The user can access the voice functions exclusively via control panels equipped with SmartLogos30M voice boards and via keypads with speakers and microphones.

The functions are:

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

**Record /
Playback**

Delete

Intercom call

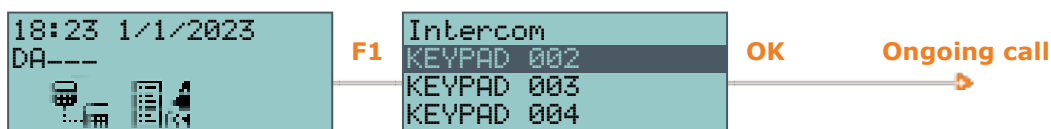
The operation time-out (expressed in seconds) will be indicated by a counter and a progress bar on the display. If you wish to stop the record/playback operation manually, press **OK**, otherwise, it will end automatically when the pre-set time-out expires.

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

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 in use.

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

Caller keypad "001"





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.

Recipient keypad "002"



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

These operations can be carried out through:

-  LCD keypad
-  touch-screen display

5.5 Activations

The activation (or 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 "User Codes").
- **Keys** - deactivated (disabled) keys cannot access the system.
- **Outputs** - each output programmed for the user code used for access can be enabled or disabled for activation by the user.
- **Keypads** - deactivated (disabled) keypads do not allow 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 recognize keys. 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

On exiting the programming session, all the timers will be activated automatically. It is the task of the user to 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.
- **InternetTeleser.** - if activated when the Answerphone option is enabled, the control panel will answer incoming calls with the prerecorded voice message.
- **Internet access** - If this option is enabled, and the system is equipped with a PrimeLAN module, the control panel will allow user-authorized access to the system via LAN/Internet. If this option is disabled, the control panel will allow user-authorized access to the system via teleservice (if authorized).
- **Enable installer** - If activated, the Installer PIN will be accepted and the installer will have access to the Installer menu, if not activated, entry of the installer PIN will generate an "Invalid Code" event and the installer will be denied access to the respective menu.
- **Registration to Inim Cloud** - this section allows the control panel to access Inim Electronics Cloud service.

The activations of the elements can be carried out from:

-  LCD keypad
-  touch-screen display
-  web server
-  Inim Cloud

5.6 Outputs management

Output scenarios

Enablement of outputs

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

For low-power open collector (OC) or relay outputs, it is possible to activate or deactivate the output and view the status by means of the respective icons.









A scenario is a configuration of the statuses of several outputs (activation type, supplied voltage, composite actions on roller shutters).

By activating one of these scenarios, the user can change the status of multiple outputs at the same time or pilot the roller shutters to programmed positions. Activation can also be automatic, combined with the activation or reset of a control panel event.

Users, via the activation menu on the keypad they can access, can also enable the outputs programmed for their code ("*Activations*").

If an output is disabled it will immediately go into its stand-by status. On re-enablement, it will remain in stand-by status until the activation condition occurs again.

The activations of the outputs can be implemented via:



-  LCD keypad
-  touch-screen display
-  proximity reader
-  keyfobs (remote-control keys)
-  telephone
-  web server
-  Inim Cloud
-  Marilyn More voice assistant

5.7 Change code PIN

This section allows the user to change the code PIN used for accessing the system and also the PINs of other users with a lower rank in the system hierarchy (see "*User Codes*").

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

This operation can be done through:



-  LCD keypad
-  touch-screen display

5.8 Change telephone numbers

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

Only contact voice-contact numbers with at least one partition in common with the entered user code and keypad in use will be shown.

This operation can be done through:

-  LCD keypad
-  touch-screen display

5.9 Connection to a LAN/Wi-Fi network

The Prime control panel can connect to a LAN network, both cabled via an Ethernet port, or via Wi-Fi through the optional PrimeWiFi module, and therefore have access to a local or Internet network.

Connectivity to the LAN network is subject to the configuration of the network itself. The manufacturer strongly recommends that you contact the network administrator for the correct configuration.

The connection of the control panel and configuration of its settings can be carried out by the user from the user menu, which can be accessed via:

-  LCD keypad
-  touch-screen, after accessing the "Settings - Alphanumeric display" section from the home page ("*Keys of touch-screen keypads*") that operates as an LCD keypad

5.10 Overtime request

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






- The partition concerned must be timer-controlled.
- The Auto-arm partition option must be enabled (see "*Activations*")

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

Note

Only 3 consecutive overtime requests are possible, for a maximum delay of 1 hour and 30 minutes.

This operation can be done via:

-  LCD keypad
-  touch-screen display
-  proximity reader
-  keyfobs (remote-control keys)
-  telephone

5.11 Thermostats

The "thermostat" function of Prime control panels makes it possible to manage boilers or air conditioners from keypads equipped with thermometers or thermal probes managed by the system.

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 each hour of the day and for every day of the week.
- **Daily** - the user sets the temperature for each hour of the day, the setting is valid for every day of the week.
- **Weekly** - the temperature set by the user is valid during the selected hours on specific days of the week.
- **Antifreeze** - this is a forced operation. If the temperature drops below 5°C, the output connected to the heating system will activate.

This function can be managed from the:

- LCD keypad
- touch-screen display
- Inim Cloud
- Inim Home application
- Marilyn More voice assistant

5.12 Listen-in

During a telephone communication with the control panel, the user can activate the Listen-in function and listen to sounds coming from premises with control panels that have at least one partition in common with the code used over-the phone.



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 "*Listen-in*").

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

5.13 Partition status enquiry

During a telephone communication with the control panel, the user, after entering a valid code, can access a control panel with voice functions and enquire about the armed/disarmed status of the partitions.

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

This operation can be done through:

- LCD keypad
- telephone


















5.14 Graphic maps










The Prime provides monitoring functions based on graphic maps which the user can access through a touch-screen keypad or web-browser.

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


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.

Table 5.1: Graphic map icons at default

Subject	Icon	Button
Link		Link to the home page of the touch-screen keypad
		Map link
Partition		After a valid code entry a window will open where you can select the arming mode you wish to apply.
		
		
		
		
Zone		After a valid code entry the zone will change its activation status
		
		
		
Output		Output switches status
		
Scenario		/
		After a valid code entry you can activate the scenario
Ongoing fault		Accesses the faults viewing section
		

Subject	Icon		Button
Thermostats		Thermostat disabled	Accesses the reader thermostat management section.
		Thermostat set to manual mode	
		Thermostat set to daily mode	
		Thermostat set to weekly mode	
		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			After a valid code entry you can access the events log

The user can reach the graphic maps through:

-  touch-screen display

-  web server

Chapter 6 Using the 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.

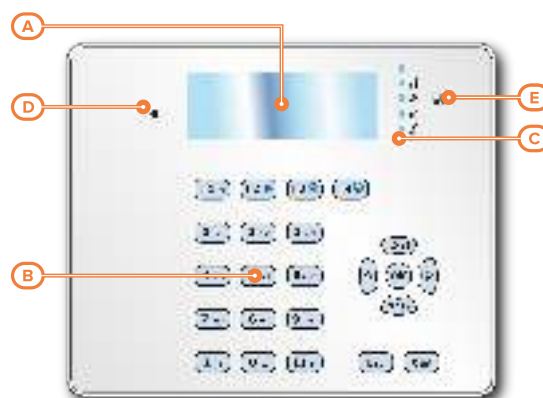
Table 6.1: Control panels - keypads functions

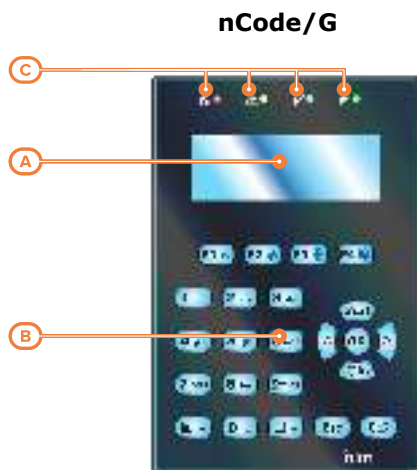
Models	Joy/MAX	Joy/GR	Aria/HG	Air2-Aria/W	nCode/G	Concept/G	Alien/S	Alien/G
[A] Graphic display	LCD192x64	LCD192x64	LCD192x64	LCD192x64	LCD192x64	LCD192x64	65536 colour touch screen 4.3 inches 480x272	65536 colour touch screen 7 inches 800x480
[B] Keypad	23 (in soft rubber)	23 (in soft rubber)	23 (in soft rubber)	23 (in soft rubber)	23 (in soft rubber)	23 (touch)	No	No
[C] Signalling LED	4	4	4	4	4	4	No	No
[D] Microphone	Yes	No	Yes	No	No	No	Yes	Yes
[E] Proximity reader	Yes	No	Yes	No	No	No	Yes	Yes
[F] USB port	No	No	No	No	No	No	Yes	Yes
[G] SD card	No	No	No	No	No	No	Max. 32 GByte	Max. 32 GByte
Buzzer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Terminals	2	2	2	No	1	1	No	2
Speaker	Yes	No	Yes	No	No	No	Yes	Yes
Temperature sensor	Yes	No	Yes	No	No	No	Yes	Yes
Backlight activated by proximity sensor	No	No	No	No	No	Yes	No	No
Brightness sensor	No	No	Yes	Yes	No	No	No	No
Tamper protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wireless	No	No	No	Yes	No	No	No	No
Keypad lock-out	No	No	No	No	No	Yes	Yes	Yes

Joy



Aria/HG/Air2-Aria/W

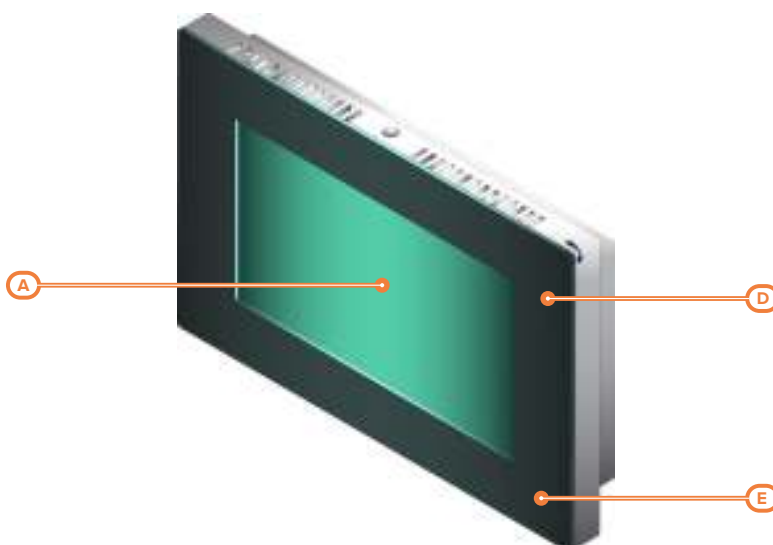
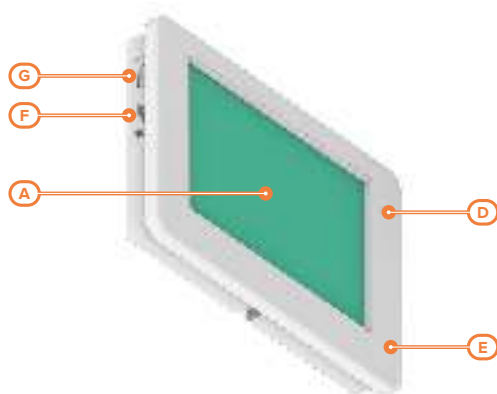




Alien/S



Alien/G



The keypad is the most complete and versatile device for system management. The installer assigns the partitions and portions/sections of the system that users with codes have access to via the keypad in use.

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.

Each user, who enters a 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 menus, they must first have their codes validated. This can be done by typing-in the code PIN and pressing the **OK** button.



Accessing the keypad

Shortcut

It is possible to extend the use of some of the system shortcuts to users without assigned codes. LCD keypads allow use of shortcut functions associated with the function keys **F1**, **F2**, **F3**, **F4**, these operations are usually reserved for authorized users (users with assigned codes). Also touch-screen keypads provide shortcuts, such as the activation of scenarios and applications, such as the setting-up of the keypad itself, which can be activated without code entry by the buttons displayed on the screen.

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 an integrated temperature sensor. The hysteresis is fixed at 0.4°C.

Soft-touch keypads

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, lock/unlock 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 Air2-Aria/W wireless keypad provides all the functions for the control and management of the Prime control panel via the Air2 system, which it interfaces with through the transceiver integrated into the control panel or through an optional Air2-BS200 transceiver. It is equipped with an accelerometer which provides both anti-tamper and "wake-up" 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

Air2-Aria/W wireless keypad) allow the user to set the keypad backlight to suit the measured ambient lighting conditions. The keypad manages two different brightness settings:

- Day
- Night

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

Touch-screen keypads

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 keypad functions is achieved by tapping on 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 keypad 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
- wake-up alarms and reminders that generate audible signals and screen popups directly programmable by the user



6.1 Keypad displays

6.1.1 The LCD keypad screen

The backlit graphic LCD screen measures 96 x 32 pixels and allows brightness and contrast adjustment via the relative section in the user menu (refer to 'Keypad settings'). Open zones are signalled by blinking on the red LED.

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 or 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

display	control panel status		
	Stand-by	Alarm or tamper	Maintenance
1st line	<div>18:23 01/01/2023</div> <p>The first line of the display shows the date and time.</p> <div>18:23 25.4°</div> <p>If the keypad is equipped with a thermostat, the date and room temperature will alternate on the screen every 3 seconds.</p>	<div>T03 Control Panel</div> <p>If at least one of the keypad partitions has an alarm or tamper memory, the first line of the screen will flash the descriptions of the zones involved every 3 seconds.</p> <p>Note Open zones are signalled by blinking on the red LED.</p> 	<div>18:23 01/01/2023</div> <div>K03 Service</div> <p>If the control panel is in maintenance mode, a string will be shown indicating the address of the keypad in use (in the figure, the keypad at address 3).</p> <div>Mainten K03 P05</div> <p>If you are using a keypad with an integrated proximity reader, the string will also show the reader address (in the figure, the reader at address 5).</p>
	<div>T03 Control Panel</div> <p>If the "View open zones" control-panel option is enabled, approximately every 3 seconds the descriptions of zones that are not in stand-by status will be shown in sequential order when the keypad partitions are disarmed.</p> <div>T03 Control Panel</div> <p>Any auto-bypassable zones will be shown in negative.</p>	<div>T03 Control Panel</div> <div>Mainten K03 P05</div> <p>If the control panel is in maintenance mode and at least one of the keypad partitions has saved an alarm or tamper event to the memory, the above-described strings will alternate on the display.</p>	
2nd line left	<div>DA SIDASI--</div> <p>The left side of the second line shows the characters that indicate the current status of the partitions the keypad is assigned to:</p> <ul style="list-style-type: none"> D = partition disarmed A = partition armed in Away mode S = partition armed in Stay mode I = partition armed in Instant mode - = partition does not belong to the keypad <p>In the case of the Prime060S and Prime060L, the display will show 10 characters indicating the status of partitions 1 to 10.</p> <p>In the case of the Prime120L, Prime240L and Prime500L, 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.</p>	<div>DA SIDASI--</div> <div>D SIDASI--</div> <p>In the event of Alarm or Tamper memory, the red LED on the keypad and the characters corresponding to the partitions concerned will blink.</p>	The line remains unchanged with respect to the stand-by status
	<div>Scenario 001</div> <p>If the "Show scenario" option of the control panel is enabled, the description of the active scenario will be shown on the left side of the second line of the display.</p>		
2nd line right	<div>DA SIDASI--</div> <p>The right side of the second line shows several icons which provide visual information regarding the system.</p>		
3rd and 4th line	 <p>Lines three and four on the display are occupied by the icons which correspond to the shortcuts assigned to function keys "F1", ..., "F4". If no shortcuts are programmed on the keypad function keys, the respective spaces on the display will remain empty.</p>		

Note

The visual aspect of the characters that represent the armed status of partitions on the screen of the Air2-Aria/W keypad is not that of blinking but rather that of characters in negative.

6.1.2

Touch-screen keypad displays

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 window that has been accessed:



[A]	Date and Time of the Inim Electronics control panel. If the control panel is in 'maintenance' mode, this field will show the address of the Alien and its integrated reader.
[B]	Keypad LED icons ("LED signalling"). Temperature read by the thermometer on the Alien.
[C]	Icon which indicates the presence of an SD card in the card slot. After entering a valid user code, the Logout button appears, which will allow you to exit the open session.
[D]	Section for active functions, with the buttons for access to the control panel, its applications and the Inim Electronics system. The home page of the Alien/S shows the function buttons ("Keys of touch-screen keypads").
[E]	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: <ul style="list-style-type: none">• 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
[F]	Tapping this section on the screen opens a window (for 3 seconds) containing a list of the active scenarios. If required by programming, it may request entry of a valid code.
[G]	System information icons ("Status icons on screen")
[H]	If the user is working inside a section, this field will show the following buttons which may cover the information icons: <ul style="list-style-type: none">• Back This button allows the user to step back to the previously active function.• Home page Button which allows the user to go directly to the home page.

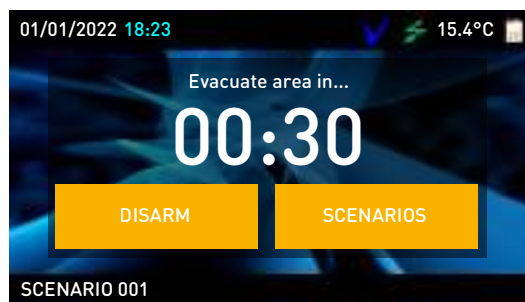
Further viewing on the touch-screen display depends on the section/page being accessed by means of the buttons. The layout of these pages depends on the functions and buttons available and how they are utilized by the user.

Pop-up

There are also visualizations that the control panel activates automatically and appear as pop-ups when the following events occur:



- **Zone alarm or tamper**
If any of the keypad partitions has alarm or tamper event memory, a pop-up window 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**, this icon appears when the user taps the display and the keypad is locked due to 5 consecutive invalid code entries.
- **Reader locked**, this icon appears when the user holds 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



Rebooting



















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.

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

6.2 Status icons on screen

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 display, provide system information, therefore, their appearance or status (fixed or flashing) depends on the status they are reporting:

Table 6.2: Information icons

Icon		Signalling	
Telephone line		Solid	Telephone line busy
		blinking	Telephone line down
Peripheral Loss		Solid	At least one peripheral device is not responding
		animated / blinking	All the peripherals in the system configuration are responding properly, however, loss of a peripheral has been detected and cleared (Peripheral Loss memory).
Answerphone		Solid	Answerphone function enabled
			
Key		blinking	False key
			
Tamper disabled		Solid	The tamper protection on the Alien keypad is disabled
			
Peripheral tamper		Solid	At least one peripheral (keypad, reader, expansion) is in tamper status (enclosure open or dislodged)
		animated / blinking	All peripherals are properly positioned and all enclosure covers are closed, however, tamper signalling has occurred on one or more of them (tamper memory).
Control panel Tamper		Solid	The Control panel is in tamper status (enclosure open or device dislodged).
		animated / blinking	The Control panel is properly positioned and the enclosure is closed, however, open-panel signalling has occurred (panel tamper memory).
Call on GSM		Solid	A phone call is in progress on the GSM communicator
			
Sending SMS		Solid	An SMS text message is being sent through the GSM communicator
			

	Icon		Signalling	
LAN			Solid	A SIA-IP event report is being sent through the LAN
			blinking	The LAN board cannot be found
SIA-IP over GSM			Solid	A SIA-IP event report is being sent through the GSM communicator
Thermostat: Winter mode			Solid	The keypad thermostat option is enabled in Winter mode (Heating).
Thermostat: Summer mode			Solid	The keypad thermostat option is enabled in Summer mode (Air-conditioning).
Thermostat: Heating/Air-conditioning			Solid	Heating/Air-conditioning On.

6.3 Use of the keys

6.3.1 LCD keypad buttons

The following section describes the typical usage of the keys. Some of the keys may have specific functions which will be indicated when necessary.

Table 6.3: The keypad keys

Buttons	Name	Typical application
1 ., 2 abc 3 def 4 ghi 5 jkl 6 mno 7 pqrs 8 tuv 9 wxyz 0 _	Number keys	These keys are used to input data into the system.
OK	OK	Used to confirm a choice, a selection or the value of a parameter
	Up, Down	These keys allow you to scroll the menu lists and/or make parameter adjustments to graphical elements (for example, keypad or volume adjustment).
	Left, Right	These keys allow you to scroll along the parameters or data being viewed (for example, when viewing partitions in the events log or when selecting partitions in the arm/disarm menu).
	C	This key allows you to step back while navigating a user menu without confirming any parameters or selections or, after entering a user PIN and pressing OK , to pass through the 3 screens of the user-menu (refer to "User of the Prime system")
Esc	Esc	This key exits the user menu definitely without confirming any of the selected parameters, etc.
	Enable	This key enables options (see "Activations")
	Disable	This key disables options.
F1 F2 F3 F4	F1, F2, F3, F4 or function keys	These keys activate the shortcuts associated with the icons. They can also be used as "Emergency Keys" (see "Emergency functions").





6.3.2 Keys of touch-screen keypads

The 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 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.

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 6.4: Touch-screen keypad menu

Icon/key		Function	Code required
	SCENARIO	Accesses the section containing the list of programmed scenarios which can be activated. Refer to " <i>Arming commands and scenarios</i> ".	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 " <i>Outputs management</i> ". The outputs are divided in two sections: <ul style="list-style-type: none"> "Home automation", outputs for the management of the home "Intrusion" outputs programmed through the anti-intrusion system 	"Home automation", no code required "Intrusion", code required.
	INTRUSION	Accesses a section where you can view and change the status of parts of the anti-intrusion system: <ul style="list-style-type: none"> 'Partitions', section where the user can view and change the status of the partitions. 'Zones', section where the user can view and change the status of the zones. 'Events Log', section where the user can view the events log. Refer to paragraphs " <i>Managing alarms</i> ", " <i>Arming commands and scenarios</i> " and " <i>View</i> ".	User code required.
	MENU	Accesses two sections: <ul style="list-style-type: none"> 'Actions', which lists the control panel commands in the event of alarm, tamper or overtime requests. Refer to paragraphs "<i>Managing alarms</i>" and "<i>Overtime request</i>". "Activations" - where it is possible to view and enable the activations described in "<i>Activations</i>". 	User code required.
	SETTINGS	Accesses the sections for the settings of the keypad and the Prime control panel: <ul style="list-style-type: none"> "Alien" - provides information regarding the settings of the keypad the user is working on. It shows the model, firmware revision and the address of the keypad and built-in reader. Furthermore, it allows the user to modify the viewing mode of the display by changing the available screen options by means of the + and - keys. Refer to "<i>Touch-screen display settings</i>". "Date/Time", "Change PIN", "Tel.Numbers" - these sections allow you to change the date and time on the control panel clock, the user PINs and the contact phone numbers saved to the memory. Refer to paragraphs "<i>Change date and time</i>", "<i>Change code PIN</i>" and "<i>Change telephone numbers</i>". "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 the user to work on the touch-screen keypad as if it were an LCD keypad. Tap the HOME button to step back to the standard mode. 	User code required. Installer code required for the "Installer".
	SYSTEM	Accesses a section where it is possible to view the system parts: <ul style="list-style-type: none"> List of ongoing faults Power-supply voltage of the control panel Information on the GSM communications module Refer to " <i>View</i> ".	User code required.
	APPS	Accesses the keypad applications: <ul style="list-style-type: none"> "Photo frame" - application that starts a slideshow of the images contained in the inserted SD-card (see "<i>Photo frame</i>"). "Voice functions" - accesses a section where the user can activate the control panel voice board functions. Refer to "<i>Voicebox and intercom functions</i>". "Maps" - for access to the system by means of the graphic maps (see "<i>Graphic maps</i>"). "Alarm clock" "Memo" - application for the programming and activation of audible signalling and popups (Refer to "<i>Alarm clock and memo</i>"). 	No code requested
	CLIMATE	Accesses the thermostat functions section Refer to " <i>Thermostats management</i> ".	No code requested

6.3.3 Emergency functions




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

- Fire Emergency
- Ambulance Emergency
- Police Emergency

Activation of any of these emergency keys will generate the associated events, output actions 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 6.5: Emergency keys

Key combinations	Icon/key	Emergency
F1 + F2		Fire
F1 + F3		Ambulance
F1 + F4		Police

Note





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

6.4

LED signalling

The following table shows the signalling on the 4 LEDs common to the control panel frontplates, keypads with LCD screen and icons on the touch-screen display that represent them.

Table 6.6: Frontplate LEDs

LED/Icon activation	Red 	Yellow 	Blue 	Green 
OFF Icon not present	All the partitions of the control panel/keypad are disarmed.	No faults present.	Open zones on the control panel/keypad partitions.	Primary power failure (230V a.c.)
ON Icon on solid	At least one of the control panel/keypad partitions is armed.	At least one fault is present.	All the zones on the keypad partitions are in stand-by status: Ready to arm	Primary power (230V a.c.) is present
Slow blinking (ON: 0,5sec OFF 0,5sec)	All the partitions of the control panel/keypad are disarmed. Memory of alarm/tamper on at least one partition or memory of a system alarm is present.	No faults present. At least one zone belonging to the control panel/keypad partitions that is either disabled (inhibited) or is in Test status. PSTN or GSM communicator is disabled.	All the zones belonging to the control panel/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 control panel/keypad partitions is armed. Memory of alarm/tamper on at least one partition or memory of a system alarm is present.	At least one fault is active and at least one zone belonging to the control panel/keypad partitions is either inhibited (disabled) or is in Test status.	Open zones on the control panel/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 "*Fault signals*".



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

- Open panel tamper
- Dislodged panel tamper
- Keypad Tamper
- Reader Tamper
- Keypad Loss
- Reader Loss
- Sounder/flasher tamper/loss
- Home-automation module tamper/loss
- GSM/2G/3G/4G communicator tamper/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 the installer has enabled the "Hide status" option (or "50131StatHidden" on keypad), the status of the partitions will not be shown. If a valid code is entered, the real-time status of the system will be shown for 30 seconds.

Additionally:

- If the partitions are ARMED, the current status of the system will be hidden from non-authorized persons.
 - Red LED Off
 - Yellow LED Off
 - Green LED On
 - Status icons not present
 - Alarm and Tamper memory hidden
 - If the same event occurs more than five times when the partitions are armed, the event in question will not be signaled further by the control panel. This is due to the fact that each event has a counter which, during armed status, increases by 1 each time it occurs; only when all the partitions disarm will the counter reset.
- When partitions are DISARMED:
 - the LEDs function normally
 - status icons are present
 - alarm and tamper memories are visible

6.5 Signalling on the Buzzer

The buzzers on and keypads provide users with audible signals, as long as the volume is turned up.

The buzzer signals the running entry, exit and pre-arm times of enabled partitions. Activation of these signals can be set up by means of the keypad options described in "*Keypad and display settings*".

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

Table 6.7: 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

6.6 Operations from LCD keypads

6.6.1 Managing alarms

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**, ..., **F4** (shown on the display) with or without code entry
- access the "Alarm management" section of the user menu by typing in a valid code PIN.



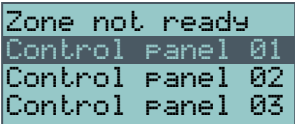
Table 6.8: Shortcut for the management of alarms from a keypad

Shortcut			User menu section	Operation
Alarm management menu	n.13		Alarm management	Access the section with the list of available operations.
Stop alarms	n.2		Stop alarms	Deactivates instantly the outputs relative to zone/partition alarm and tamper events and deletes the partition and system alarm and tamper memories.
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	Deletes memory of system and partition alarm and tamper events.

6.6.2 Arming commands and scenarios

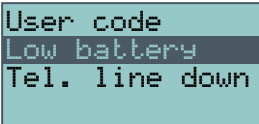
If you issue an arm-partition command at a keypad (for one or more partitions) and not all the zones involved are in stand-by status (thus execution of the command will generate an instant alarm), the keypad will provide a list of the zones concerned.

You can scroll the list and check the zones which are not in stand-by status. If you wish to implement the command, the visualized zones will generate an instant alarm.



If you issue 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.

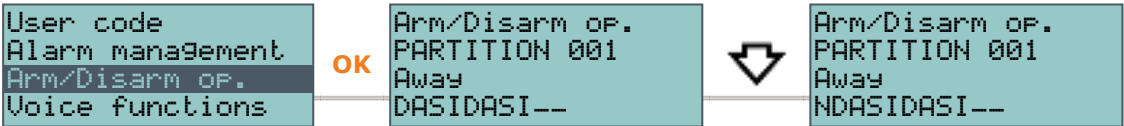
The user can scroll through the list to see the causes of reduced security, then decide whether or not to force the arming command.



The user can operate via the keypad in two ways:

- Activate the shortcuts associated with keys **F1**, ..., **F4**, 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:
 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

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 6.9: 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 “View scenario” control-panel option is enabled (or “View scenario” on keypad, enabled at default), the left side of the second line on the keypad display will show the description of the active scenario.

6.6.3

Voicebox and intercom functions

The voice functions available at the Prime control panel with SmartLogos30M voiceboard are:

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

The user can operate on the keypad in two ways:

- activate the shortcuts associated with keys **F1**, ..., **F4** (shown on the display) with or without code entry
- access the “Voice functions” section of the user menu by entering a valid PIN code (section not available if the voiceboard is not installed)

The volume can be adjusted during the playback phase by means of keys  and .

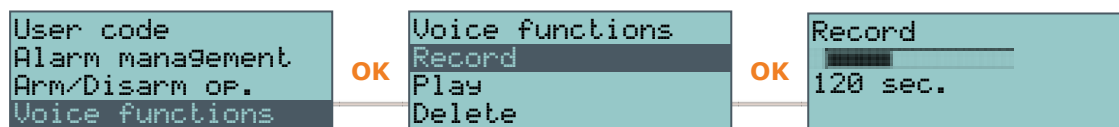




Table 6.10: Shortcut for voice function from a keypad

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 voicemail message
	Delete	Delete voicemail message
Intercom Call n.11	 Intercom	Intercom call

6.6.4

Activations

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

- activate the shortcuts associated with keys **F1**, ..., **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 .



Table 6.11: 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 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 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 (see "*Fault signals*")
- the firmware revision and the control panel model
- the sunrise and sunset times of the current day

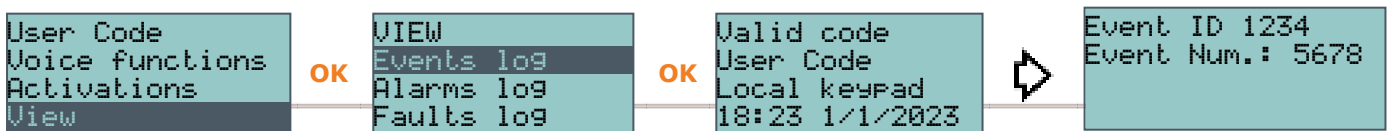
To view these statuses:

- activate the shortcuts associated with keys **F1**, ..., **F4** (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.

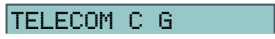



**Table 6.12: Shortcut for viewing from a keypad**

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

Shortcut		User menu section	Operation
GSM Menu status	n.16	 Sol-2G/3G/4G status	Status of GSM communicator
View system status	n.32	 System status	
		Batt.	the voltage measured on the battery
		Pow.	the control panel power supply voltage
		Aux.	the voltage measured on terminal "AUX"
		I-BUS	the voltage measured on terminal "+" of the I-BUS
View zone status	n.33	 Zone status	Zone status
View faults	n.36	 Ongoing faults	Ongoing faults
		PanelVersion	the firmware version and the control panel model


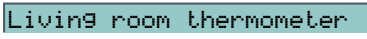

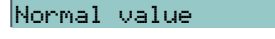

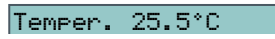
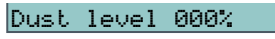
GSM status

Table 6.13: View GSM status from keypad

Line	Display	View
1		<ul style="list-style-type: none"> mobile network provider (on the left side) "--" indicates that the GSM card is present in the control panel "C" means that data transfer is in progress data network technology (on the right side) <ul style="list-style-type: none"> G, GPRS service 3G, UMTS service H, HSPA service 4G, LTE service
2		GSM signal reception (value between 1 and 100)
3		Credit balance, at the last operation (expressed in the local currency)
4		Faults present, in this case it is necessary to access the "View-Faults" section for details.

Zone status

Table 6.14: View zone status from keypad

Line	Display	Generic zone	Wireless zone	Smoke detector	Thermal probe
1	 	Zone description			
2	 	Zone status ("Standby", "Alarm", "Short-circuit", "Tamper") and its activation status ("unbypassed" - capable of generating alarms, or "bypassed" - incapable of generating alarms)		"Normal value" or "Threshold exceeded" respectively if the temperature is below the alarm threshold or not.	
3	 	-	Level of wireless signal (from 0 to 7)	Level of wireless signal and level of smoke present in the sensing chamber, expressed in mdB/m	Temperature read by the probe connected to the terminal with precision of a tenth of a degree centigrade
4		-	-	Level of contamination present in the smoke detection chamber of a smoke detector (%)	-



6.6.6

Outputs management

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

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

- activate the shortcuts associated with keys **F1**, ..., **F4** (shown on the display) with or without code entry
- access the "Domotic commands" 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 .

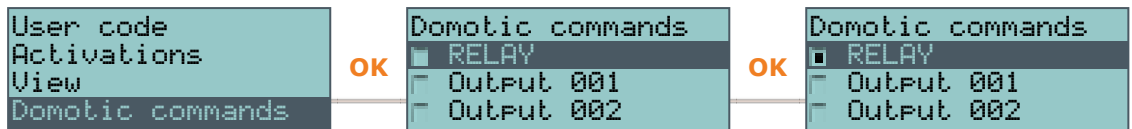


Table 6.15: Shortcut for output activations from an LCD keypad

Shortcut		User menu section	Operation
ON/OFF output menu	n.21	Domotic commands	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

6.6.7 Change date and time

The keypads provide a section for the control panel date and time setting and its 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**, ..., **F4** shown on the display, with or without code entry
- access the “Set date/time” section of the user menu by entering a valid PIN.
 1. Use keys and to select the programming field to be changed (hour, minutes, etc.).
 2. Use keys and to make any changes in the selected field.
 3. Press **OK** to save the setting.

6.6.8 Keypad and display settings

The keypads provide a section for the settings of the keypad display and buzzer and also for the buzzer of the control panel.

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

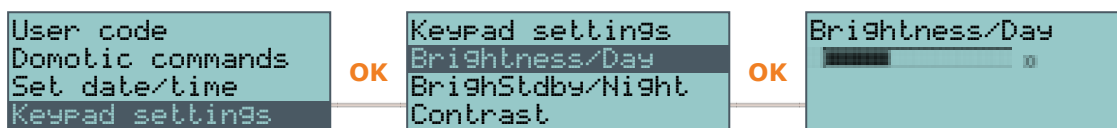
- **Brightness/Day** - for the adjustment of the backlight brightness of the display and key LEDs, when any key is pressed and for the following 20 seconds, in “Day” mode.
- **BrighStdby/Night** - for the adjustment of the backlight brightness of the display and key LEDs, when the keypad is in Standby and in “Night” mode.
- **Contrast** - for the adjustment of the black/white contrast.
- **Volume** - intensity of buzzer loudness.
- **Keypad options:**
 - **Temperature off** - if enabled, the temperature value read by the integrated temperature sensor will not be shown (only for temperature-sensor equipped keypads).
 - **NoExitTimeSignal** - if enabled, the buzzer will not emit audible signals during partition Exit time.
 - **NoEntryTimeSign.** - if enabled, the buzzer will not emit audible signals during partition Entry time
 - **Beep on output** - if enabled, the buzzer will emit an audible signal during activation of terminal T1, when it is programmed as an output.
 - **Chime** - if enabled, the buzzer will not emit audible signals when a chime zone is violated.
 - **LED Off in stand-by** - 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 "Keypad settings menu" shortcut (shortcut n.18), associated with one of the keys **F1**, ..., **F4** shown on the display, with or without code entry
- access the "Keypad settings" section of the user menu by entering a valid PIN.
 1. Use keys \leftarrow and \rightarrow followed by **OK** to select the parameter to be programmed.
 2. Use keys \leftarrow and \rightarrow to increase or decrease the value of the selected parameter. To activate the selected option press \blacksquare , to deactivate it press \square .
 3. Press **OK** to save.



6.6.9 Change PIN codes



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**, ..., **F4** 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 \leftarrow and \rightarrow 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** then press **OK**.
 3. Type-in the new PIN again using keys **0**, ..., **9** and press **OK** to save.

6.6.10 Change 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 contacts list:

1. Use keys \leftarrow and \rightarrow to select the required phone number then press **OK**; each programming field accepts a 20 digit phone number.
2. Use keys \leftarrow and \rightarrow to select the field to be edited, then use the number keys (**1**, ect.) to edit the number. Accepts also "," (= 2 second pause), "*" and "#".
3. Press **OK** to confirm and exit.

6.6.11 Connection to a LAN network

The connection of the control panel and the configuration of the parameter settings can be done through the user menu. It is necessary to enter the user code PIN, access the "Settings" section, then the "IP Par.and Wi-Fi" section.

This section provides the following sub-sections:

- **Wi-Fi Networks** - by pressing the **OK** button the control panel will start scanning for available networks, those found will be listed in order in accordance with their signal strength. At this point the user can select a network and make the connection using the **OK** button, after entering the respective password, if required.



- **Parameters:**

- **Enable DHCP** - if enabled, the IP connection parameters will be obtained automatically, in accordance with DHCP protocol.
- **Enable Wi-Fi** - if enabled, the PrimeWiFi module will activate for the Wi-Fi connection.
- **Test Internet** - if enabled, the control panel will automatically carry out an Internet connection test every 5 minutes, if failed, the system will force the restart of the Wi-Fi connection.

Once the option has been selected, it is enabled using the "■" button and disabled using "□". The **OK** button confirms any changes to the options.

- **IP Parameters** - this section is for the network parameter settings (IP address, subnet mask, gateway, DNS, communication port).

1. Use keys \leftarrow and \rightarrow to select the parameter then press **OK**.
2. Using the "left" and "right" arrow keys select the field you wish to change then, by means of the number keys, edit the number.
Insert the octets inclusive of zeros (e.g.: 192168001010 per 192.168.1.10).
3. Press **OK** to confirm and exit.

After modifying these parameters, and in general, on exiting the "Settings" menu item, the control panel may restart completely.

6.6.12

Network connection test

You can start the Internet/Cloud connectivity test via your user menu, by entering your code PIN and accessing the "Settings" section, then the "Connection test".

This test starts the following checks in succession:

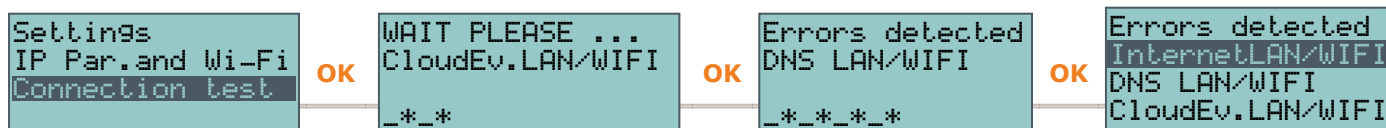
- Internet connection test via LAN/Wi-Fi network
- Internet connection test via GSM communicator
- DNS resolution test via LAN/Wi-Fi network
- DNS resolution test via GSM communicator
- Cloud "Events" channel connection test via LAN/Wi-Fi network
- Cloud "Events" channel connection test via GSM communicator
- Cloud "Commands" channel connection test via LAN/Wi-Fi network
- Cloud "Commands" channel connection test via GSM communicator

During the execution of the test, the first line of the display will show the wording 'Wait' while the second line of the display shows the description of the test currently in progress.

On completion of each test, the keypad display shows the test result on the fourth line:

- an asterisk ("*") if the test is completed successfully;
- a dash ("-") if the test fails.

On completion of all the tests, if communication is successful, the following message will be shown on the first two lines: "Test carried out successfully" otherwise the generic wording "Errors detected Press OK" will be shown. When the **OK** button is pressed, any failed tests will be listed.



Note

If the Ethernet connector is disconnected or if the Sol-2G/3G/4G GSM communicator is not present or does not respond, or if there is a GSM communicator model without IP communication capacity, the tests relating to these communication channels will not be carried out.
If a PrimeLAN module is present on the control panel, the test relating to the LAN channels will be started regardless of whether the Ethernet connector is connected or not to a network.

6.6.13

Overtime request

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



- activate the “Overtime” shortcut (shortcut n.7), associated with one of the keys **F1**, ..., **F4** 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.

6.6.14 Thermostats management

The control panel “thermostat” function on keypads equipped with a thermometer or thermal probe, that are part of the system, can be managed from any of the system keypads:



- activate the “Thermostat” shortcut (shortcut n.37), associated with one of the keys **F1**, ..., **F4** shown on the display, with or without code entry
 - access the “Thermostat” section of the user menu by typing-in a valid code PIN.
1. Select one of the thermal probes that the keypad you are using has access to.
 2. Use the number keys to select the operating mode of the thermostat:
 - “1” - thermostat Off
 - “2” - “Manual”
 - “3” - “Daily”
 - “4” - “Weekly”
 - “5” - “Antifreeze”

Table 6.16: LCD keypad thermostats

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)

3. Select the operating mode (“Summer/Winter”) of the thermostat by means of the **6** button.
4. Select the temperature, using keys and .
5. Select the time frame, using and .
6. Select the day of the week, using and .
7. Press **OK** to confirm and exit.



6.6.15 Code Management

The user menu provides a section for the programming of the parameters of hierarchically-lower user codes (see “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.

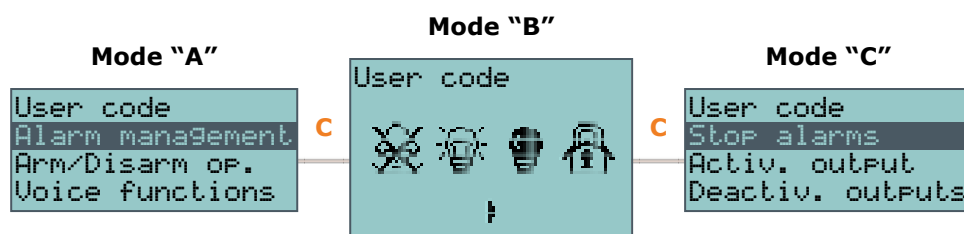
Code parameters

- **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, and 5, 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 6.17: Combinations "text menu" and "user menu"

Mode	Text menu	User menu	View
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 , ..., F4 ; at this point the user can press the required function key and activate the associated shortcut.
C	Enabled	Disabled	Shows the descriptions of the personalized user-icons associated with function keys. The 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	As per mode "C"



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

- **AnnounceShortcut** - if enabled on a voice capable keypad, the descriptions of all the shortcuts assigned to the code and associated with the number keys will be announced after acceptance of the entered PIN.
- **Remote access** - if enabled, the code PIN can be used to operate the system from any remote phone.
If the code PIN is entered on a remote phone 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
- **Patrol** - if enabled, the code will have the attributes of a "Patrol" code.
- **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**, ..., **F4**.
After valid PIN entry the keypad will show the icons that correspond to keys **F1**, ..., **F4** 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**.
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 Δ and ∇ to select the key you wish to associate with the shortcut then press **OK**.
 2. Press **OK** then, using keys Δ and ∇ , select from the "Type" list the shortcut to be associated 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 the user to select a scenario. If the associated shortcut is "Activate output" or "Deactiv. output", the system will ask the user to select an output.
- **ActivatableOutputs** - this section allows the user to enable/disable the outputs the code is allowed to control manually:
User menu, Home-automation commands
 1. Use keys Δ and ∇ to select the desired output.
 2. Use keys \blacksquare and \square to enable/disable manual control of the output for the code concerned.
 3. Press **OK** to confirm and exit.
 - **Timers** - this section allows the user to assign a timer to the code. The code will be operative only at the pre-set times.
 - **Type** - this section allows the user 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".

6.6.16

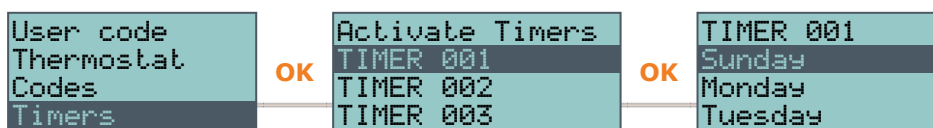
Timer programming

This section allows the programming of all the timers the user has access to.
The user 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 (see "Activations"), the partition will arm when the timer switches ON and disarm when the timer switches OFF.
- a **Code** - if the timer is enabled, the code will be authorized to operate on the system only when the timer is active (ON).
- a **Key** - if the timer is enabled, the key will be authorized to operate on the system only when the timer is active (ON).

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

1. Access the "Timers" section of the user menu by typing-in a valid code PIN.
2. Use keys Δ and ∇ to select the Timer then press **OK**.
3. Using the same keys, select the day of the week.
4. Select an activation or a restoral of the timer.
5. Set the selected time (expressed in hours and minutes) by means of keys \diamond and \pounds then, using keys Δ and ∇ select the number.
6. Press **OK** to confirm and exit.



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

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

6.6.17

Partition status enquiry



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

After entering a valid user-code, press the key which is assigned to the shortcut. The description of the area and its armed/disarmed status will be reproduced in sequence.

Note

The status of the areas belonging to the code only is reproduced without considering the areas to which the keypad belongs.

6.7

Operations via touch-screen keypad

6.7.1

Managing alarms

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.

6.7.2

Arming commands and scenarios

The touch-screen keypad allows users to activate the programmed scenarios and also set up the arming mode of the partitions the users 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", "Touch-screen display settings").

Partitions



Access the "Intrusion" section, type-in the user code and then access the "Partitions" section.

This section displays the partitions separately. The user can scroll and select a partition by means of the right/left scroll buttons and then select the arming mode by means of 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.

6.7.3

Voicebox and intercom functions



To access the voice functions via the touch screen keypad, you must 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 accessed by tapping the relative **ON** button:

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

6.7.4



Activations



To activate (and deactivate) the elements of the Prime system via the touch-screen 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

6.7.5

View

The touch-screen keypad provides sections for the visualization of the current status of all system elements.

The "Activations" (*"Activations"*) and "Commands" (*"Outputs management"*) sections allow the display of the status of the activatable elements and the outputs. It is possible to add other elements to these which can be reached 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 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 (see *"Fault signals"*)

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



Partitions

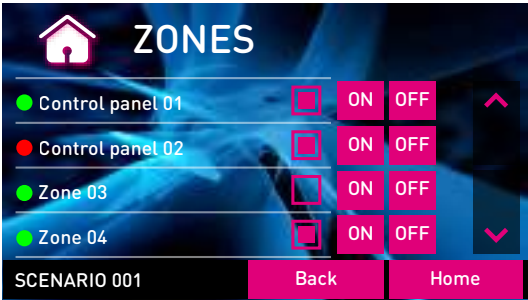
In the "Partitions" section, the partitions are listed and show their arming status, which can be changed, as described in *"Arming commands and scenarios"*.




The availability of the keypad parameter "View area status" (see *"Touch-screen display settings"*) will allow the user to select the visualization mode of the operating status on the bottom bar of the screen:

- "Single partition" - the characters relating to the armed status of the partitions will be shown, as described in *"Keypad displays"*
- "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”, all the events saved to the log are displayed one at a time, however, the up/down buttons will allow the user 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

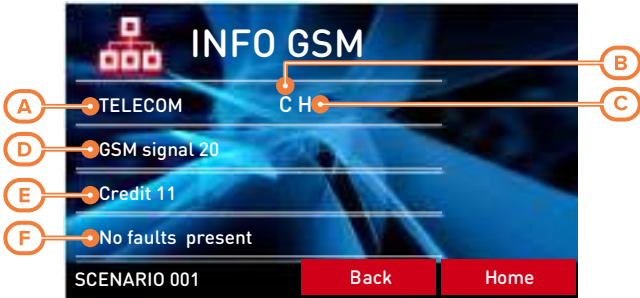
The “Faults” section allows you to view all the faults present on the system and, where possible, the fault details by means of the **DETAILS** button.

Voltage

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

GSM

The “GSM info ” section allows you to view the parameters of the GSM communicator:



[A]	Mobile network provider
[B]	“--” means that the communicator is connected to the BUS. “C” means that data transfer is in progress.
[C]	Data network technology: <ul style="list-style-type: none">• G, GPRS service• 3G, UMTS service• H, HSPA service• 4G, LTE service
[D]	GSM signal reception (value between 1 and 100)
[E]	Credit balance, at the last operation (expressed in the local currency)
[F]	Presence of ongoing faults

Via Graphic maps



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

Refer to "*Graphic maps*".

6.7.6

Outputs management





From a touch-screen keypad it is possible to activate/deactivate manually the outputs the code is enabled to work on.

Access the "Commands" section, where the following sections are available:

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

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 ($\cos\phi$). These values can be adjusted using the **+** and **-** buttons.

6.7.7

Change date and time



The touch-screen keypad has a section where the user can set the date and time of the control panel and the required date/time format.

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

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

6.7.8

Touch-screen display settings



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

This section allows the user to view the firmware version of the control panel and change the parameter settings of the keypad in use.

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 for the touch-screen
- **Delay photof.** - waiting time before the automatic startup of the photoframe application during standby status
- **Photo int.** - interval between the display of photos used by the photoframe application
- **Language** - for selection of the language used by the control panel

- **View partitions** - for the viewing mode 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 status
- **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
- **Keypad address**
Keypad address - this is the address of the Alien keypad and its integrated reader
- **Tamper** - enable/disable detection of tamper on the device (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.

Select the parameter using the up/down scroll keys and change it by means of the **+** and **-** buttons. To confirm changes and exit the section press the **SAVE** button.

Note

English is the default language of the Alien keypad.

6.7.9

Change code PIN



To change user code PINs via the touch-screen keypad, access the "Settings" section, enter a valid user code, then go to the "Date/Time - Change PIN - Change tel. num." section, then to the "Change PIN" section.

Select the code 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.

6.7.10

Change telephone numbers



To edit telephone numbers via the touch-screen keypad, access the "Settings" section, enter a valid user code, then go to the "Date/Time - Change PIN - Change tel. num." section, then to the "Change tel. num." section.

In this section it is necessary first to select the required telephone number 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.

6.7.11

Overtime request



Overtime requests via the touch-screen keypad can be activated by accessing the "Menu" section, entering a valid user code and then accessing the "Actions" section.

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

6.7.12

Thermostats management



The "Thermostat" function of the Prime control panel is managed via the "Climate" section.

By accessing the section for the selection of one of the thermal probes (keypad or isolated) which the keypad has access to. Then successively going to the section relating to the operating mode of the thermostat:

- Manual
- Daily
- Weekly
- 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 time frame 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.

6.7.13

Photo frame

"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.

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 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 keypad and application settings, access the "Settings" section, type-in a valid user code then access the "Alien" section (see "*Touch-screen display settings*").

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

6.7.14

Alarm clock and memo

The touch-screen keypads have applications that allow the user to manage events that, when necessary, activate both an audible and visual signalling, in the form of a pop-up notification on the screen.

Note

The programming and activation of the clock and memo events are of no consequence to the programming or regular functioning of the control panel 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, the user 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 activation of the appropriately programmed event occurs, a window will appear similar to the one shown here. The **OFF** button deactivates signalling, whereas the **SNOOZE** button defers it for 5 minutes.

6.7.15

Graphic maps via touch-screen keypad



Access the “Apps” section, then the “Maps” section, here it is possible to access the maps programmed for the keypad in use.

The touch-screen keypad can manage up to 10 maps and the Web interface up to 20 maps. Each map supports up to 20 objects/buttons represented by icons.

Note

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

Chapter 7 Use of proximity readers and digital keys

7.1 Proximity readers

Prime control panel can manage nBy readers, and also the built-in readers in the 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 (see "*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, the LEDs will indicate the current status of the associated shortcut.
- when a key is present at the 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 the reader partitions are disarmed.			
(All LEDs Off)	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)s	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 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 stand-by 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 stand-by 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 stand-by 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 stand-by 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 stand-by 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 contact-free electronic keys, which Inim Electronics offers 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 system programming phase, the installer enrolls each key on the control panel in order to allow the system to recognize it when it is used.

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

- The **partitions** it is enabled to 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** (8 shortcuts for remote controls with "super keys" function).
- 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 they were before being disarmed 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.

7.3 Remote-control keys

Remote-control keys have 4 buttons the functions of which can be programmed from the control panel.

It is possible to associate a control-panel shortcut to each button, the shortcut can be activated by pressing the button and confirmed by a beep from the remote-control buzzer.

Super keys

If the “super keys” function is enabled, by pressing and holding the button for at least 2 seconds, until a second beep is heard, you can activate a shortcut different from the one associated with simply pressing the key.

In this way you can have up to 8 different shortcuts on each remote-control key.

Signalling

The remote-controls have 5 LEDs, 4 of which are associated with buttons and the other is 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	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
F1 for 2 seconds	1 flash				2 beeps	Activates shortcut 5 (“super key”)
F2 for 2 seconds		1 flash			2 beeps	Activates shortcut 6 (“super key”)
F3 for 2 seconds			1 flash		2 beeps	Activates shortcut 7 (“super key”)
F4 for 2 seconds				1 flash	2 beeps	Activates shortcut 8 (“super key”)
F2 + F3		1 flash	1 flash		beep	Block/Unblock remote-control device
F3 + F4			1 flash	1 flash	beep	Enrolling
Any			3 flashes	3 flashes		Remote-control device blocked

Note

Failure of the LED to light, after pressing the corresponding button and the successful execution of the command, is an indication that the wireless battery is running 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

7.4 Reader and key operations

7.4.1 Managing alarms

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

Hold a valid key in the vicinity of the reader and select the LED or description corresponding to a shortcut such as:

- “Stop alarms” (shortcut n.2)
- “Clear call queue” (shortcut n.3)
- “Delete memory” (shortcut n.4)

7.4.2 Arming commands and scenarios

Via a reader it is possible to activate the programmed scenarios for the associated shortcuts:
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).

7.4.3 Outputs management

The activations and deactivations of outputs via proximity readers depend on the appropriate programming of the shortcuts associated with them.

Hold a valid key in the vicinity of the reader and select the LED or description corresponding to a shortcut such as:

- "Activate output" (shortcut n.5)
- "Deactivate output" (shortcut n.6).

7.4.4 Overtime request

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

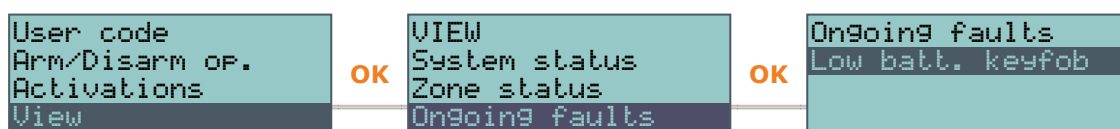
Hold a valid digital key in the vicinity of the reader until the reader LEDs or display indicates "Overtime" (shortcut n.7).

7.4.5 Operations via remote-control keys

Press the key on the remote control to which the shortcut relating to the requested operation is associated and verify the outcome of the operation, as described in "Remote-control keys".

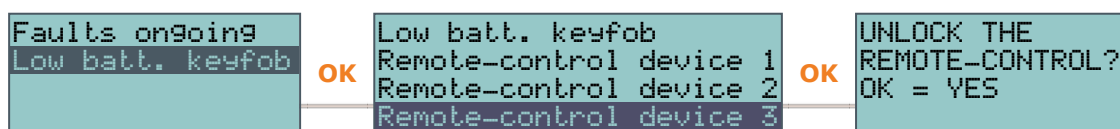
7.4.6 Use of remote-controls with low battery

A remote control can signal the low battery condition to the control panel. This condition is recognized by the control panel as a fault, consequently the yellow LED on the keypads will activate and the list of ongoing faults will be updated (see "LED signalling" and "Fault signals"):



In this case, if provided for in the programming, the remote control may have the arming option disabled.

The user can force this condition by requesting a rehabilitation of the remote control, which can be reached from the 'Faults present' menu indicated above, by selecting the remote control concerned



If **OK** is selected again at this point, the control panel will compare the partitions to which the user code, keypad and remote control belong and if this check results positive, the remote control will finally be enabled for arming/disarming operations even when the battery is low.

Chapter 8 Commands over the phone

8.1 Use of phone calls

8.1.1 Panel to user calls

The installer will instruct the user 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 phone 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 (see "*Activations*") is enabled, the user can call the control panel from any remote phone and send commands to the system and/or activate Listen-in sessions.

1. Call the control panel.
2. The control panel will answer after the programmed number of rings and will play message "Enter valid code followed by #".
3. Type in your PIN followed by "#".
4. The control panel will activate the voice function which will announce the available shortcuts and the number keys to press.
5. As soon as the selected number is pressed on the telephone keypad, the control panel will activate the corresponding shortcut.

If the system is equipped with a GSM communicator, the user can send commands to the control panel also by phoning the number of the SIM card inside the device. If appropriately configured (by the installer), the user will receive an SMS text message or a feedback ring from the GSM communicator confirming the successful outcome the command.

8.2 Use of SMS text messages

8.2.1 SMS text message from panel to user

If the Prime control panel is equipped with a GSM communicator, users can receive SMS text notification of events.

If an event (appropriately programmed by the installer) occurs or restores, the control panel will send an SMS text notification to the programmed contact numbers.

8.2.2 SMS text message from user to panel

If the Prime control panel is equipped with a GSM communicator, users can send commands to the control panel via SMS text messages to the number of the SIM card inserted in the device. 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 appropriately configured (by the installer), the user will receive an SMS text message or a feedback ring from the GSM communicator confirming the successful outcome the command.

SMS text at default

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

- **"CREDIT"** - for balance enquiries relating to the SIM card of the GSM communicator, the user will receive an SMS text indicating the remaining credit.
- **"STATUS"** - for status enquiries relating to the GSM communicator, the user will receive an SMS text containing 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

8.3 Operations via telephone

8.3.1 Managing alarms

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 phone 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).

8.3.2 Arming commands and scenarios

Type in an enabled 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.

8.3.3 Activation of outputs

Type-in the PIN of a code enabled for phone use followed by “#” then press the key (from “0” to “9”) which the installer has programmed to activate the shortcut, for example:

- “Activate output” (shortcut n.5)
- “Deactivate output” (shortcut n.6).
- “Activate scenario of outputs” (shortcut n.23)

8.3.4 Overtime request

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 user on the phone and the control panel itself.

Press “*”, to end the Listen-in phase 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.

Chapter 9 Use of the web server

If used, the PrimeLAN network module provides the user of the Prime control panel the following services:

- interaction with the control panel via any browser thanks to an integrated web server
- sending e-mails with attachments in relation to the control panel events






9.1 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 9.1: Menu via web server

Icon	Section	Function
	SCENARIOS	Accesses the section containing the list of programmed scenarios which can be activated. Refer to " <i>Arming commands and scenarios</i> ".
	COMMANDS	Accesses a section containing the list of outputs which can be activated. Refer to " <i>Viewing and activations</i> ".
	INTRUSION	Accesses a section where you can view and change the status of parts of the anti-intrusion system: <ul style="list-style-type: none"> • "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 the user 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 " <i>Managing alarms</i> ", " <i>Arming commands and scenarios</i> " and " <i>Viewing and activations</i> ".
	CAMERAS	Accesses two sections: <ul style="list-style-type: none"> • "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 " <i>Camera access</i> ".
	SETTINGS	Accesses a section where it is possible to: <ul style="list-style-type: none"> • select the language of the web interface • select the home page of the web interface, from the menu pages and the first graphic map • send a test email from the PrimeLAN to a recipient • upgrade the web server interface • open a section that shows the meanings of the icons used by the web interface

Icon	Section	Function
	SYSTEM	<p>Accesses a section where it is possible to view the system parts:</p> <ul style="list-style-type: none"> List of ongoing faults Power-supply voltage of the control panel Information relating the GSM communications board <p>Refer to "<i>Viewing and activations</i>".</p>
	KEYPAD	<p>Section for remote access to a keypad.</p> <p>Refer to "<i>Remote keypads</i>".</p>
	MAPS	<p>Accesses the system through the graphic maps.</p> <p>Refer to "<i>Graphic maps via web server</i>".</p>

9.2 Access to and use of the Web interface

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://192.168.1.98" would become "https://192.168.1.98").
2. At this point the control panel will display the access page 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 code is not active, that is, it has been disabled by the user
- 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 "*Sections of the web interface*".

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.

Warning

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

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

9.3 Operations via web server

9.3.1 Managing alarms

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.

9.3.2 Arming commands and scenarios

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 9.2: 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.

9.3.3 Viewing and activations

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

Table 9.3: Viewing via web






















Section	Icon/Button	Status
 - Partitions / Zones		Disarmed
		Armed in Away mode
		Armed in Stay mode
		Armed in instant mode
		Stand-by
		Alarm
		Tamper or fault
		An alarm or tamper event in memory
 - Zones		Zone shorted
		Zone active
		Zone deactivated
 - Timers		Activated
		Deactivated
		Output status
		

Table 9.4: 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



System info



First access the “Intrusion” section and then the “Events log” section. 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.

The “System” section provides the following sub-sections:

- “Faults list” - a window showing a list of the faults present on the system.
- “Voltage” - this window allows you to view the control panel power-supply voltage.
- “GSM info” - this window allows you to view the parameters of the GSM communicator.

Via Graphic maps



The visualization of the status and supervision of the system and its parts can be done through the graphic maps, accessible through web interface.

Refer to "*Graphic maps via web server*".

9.3.4

Camera access



Real-time

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:

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

- information regarding the camera (description, make, time, date, etc.
- snapshots taken in real-time
- **Snapshots** button - allows you to view the recorded footage in snapshot sequence
- **Video** button - allows you to view the recorded footage in video format

Records

The "Recordings" section allows you to view recorded footage after the occurrence of events (appropriately programmed). 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.

9.3.5



Remote keypads



The "Keypads" section of the web interface of a 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 "*LCD keypad buttons*") 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

9.3.6

Graphic maps via web server



Camera access

The graphic maps, once properly programmed, can be accessed by any user with a device equipped with a web browser.

These maps are accessible through the "Graphic maps" section of the web-server menu.

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.

Note

Access to the cameras is allowed only via a web browser and not via maps on the touch keypad.

9.4 e-mail

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

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

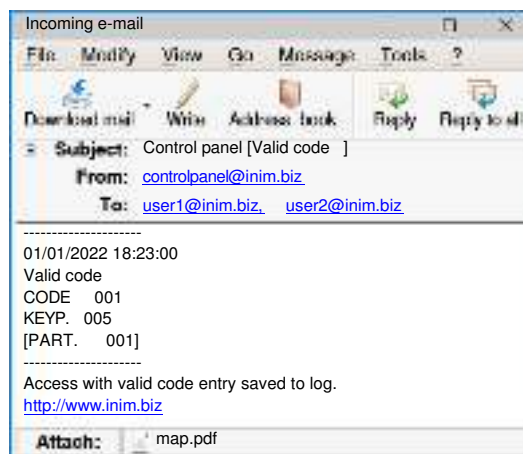


Table 9.5: E-mail parameters

Parameter	Example	
Subject	Control panel [Valid code]	It consists of a text, edited by the installer, with information regarding the event associated with the e-mail.
Sender	centrale@inim.biz	Parameters set by the installer
Recipient	User1@inim.biz, User2@inim.biz	
Message text	----- 1/01/2023 6:23:00 PM Valid code CODE 001 KEYPAD 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

Appendix A Glossary

Alarm	Detection of non-authorized entry into the protected building. More specifically, activation of a detector.
Alarm cycles	A parameter generally associated with zones. This value determines the number of alarm events a zone can generate before the partitions it belongs to disarm. This value (number of alarm events) resets to zero when the zone partitions re-arm or reset. If a zone is allowed to generate an unlimited number of alarm events, it is classified as a "repetitive" zone.
Alarm or Tamper Memory	In the event of: <ul style="list-style-type: none"> • Zone Alarm • terminal tamper • open panel or dislodged panel • peripheral tamper (keypads, expansions, readers) • peripheral loss (keypads, expansions, readers) • false key <p>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).</p>
Alarm Receiving Centre (ARC)	This is a private service that monitors premises protected by anti-intrusion 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. When a partition is armed, generally the zones belonging to it can generate alarms. When a partition is disarmed, the zones belonging to it cannot generate alarms. The system generates tamper alarms even when partitions are disarmed.
Astronomical clock	Function of the control panel that allows it to automatically determine sunrise and sunset times through the geographical coordinates of the system, without using a twilight sensor.
Auto-arm	The user 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. The control panel monitors the battery continuously and keeps it 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 <ul style="list-style-type: none"> • Installer code: assigned to the installer of the security system • User code: assigned to the end-user of the security system
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	<p>This is an explicit user-command which ends signalling on the red and yellow LEDs on keypad and readers for the following events:</p> <ul style="list-style-type: none"> • Zone Alarm • terminal tamper • open panel or dislodged panel • peripheral tamper (keypads, expansions, readers) • peripheral loss (keypads, expansions, readers) • false key • ongoing fault • memory fault <p>If a user deletes the alarm/tamper memory, the visual signals on the reader/keypad LEDs will clear.</p> <p>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.</p>
Digital telephone dialer	<p>This device allows the control panel to send report calls to Alarm Receiving centres (ARC).</p> <p>Prime control panels provide a built-in digital dialer.</p>
Dimmer	<p>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.</p>
Entry time (or Entry delay)	<p>The time (expressed in minutes or seconds) that the system allows the user to disarm the partition after zone violation. If the system is not disarmed within the set time it will generate an alarm.</p> <p>Each partition can be programmed with its own Entry time.</p>
Event	<p>An operative status recognized by the system.</p> <p>For example: detector alarm, mains failure (230V~), blown fuse, user-code recognition, etc., are all events recognized by the control panel.</p> <p>Each event is associated with an activation event (when the event occurs) and a restoral event (when the event ends).</p> <p>Each event can be programmed to generate the following actions:</p> <ul style="list-style-type: none"> • activation of one or more outputs • activation of an output scenario • transmission of one or more e-mails • send one of more push notifications • 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)	<p>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:</p> <ul style="list-style-type: none"> • event description - with details regarding new events and restorals • information regarding the user or the cause of event • event location • event date and time <p>The events log can be viewed by the system users and the installer.</p> <p>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.</p> <p>For example, if a user arms several partitions from a keypad, the events log will show:</p> <ul style="list-style-type: none"> • 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)	<p>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.</p> <p>Each partition can be programmed with its own Exit time.</p>
Expansion	<p>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.</p>
Fault	<p>A condition which indicates that a system component is not working properly.</p> <p>Some faults can jeopardize the performance of the entire system. Typical faults are Mains failure (230V ~), telephone line down, low battery.</p>
Fault zone	<p>Violation of this type of zone will generate the zone alarm event and concur with the signalling of faults (yellow LED on the keypad).</p>
Graphic map	<p>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.</p> <p>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.</p> <p>The user, by means of access to a graphic map, can view the supervised area and also access the security system functions.</p> <p>An object can be:</p> <ul style="list-style-type: none"> • Partition • Zone • Output • Map link • Button
GSM Dialer	<p>A device which allows the control panel to make phone 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.</p>

Hold-up Zone (or panic zone or silent zone)	Activation of a zone with this configuration generates an immediate alarm even when the partition it belongs to is disarmed. The outputs and programmed calls will be activated, but the alarm will not be signaled on the red LEDs on the keypads and readers or on the keypad displays. Under normal circumstances zones with this attribute are activated manually (using hidden buttons or similar devices) in situations of duress (armed robbery, etc.).
Home Automation	It is the combination of technologies, devices and services intended to improve the quality of life in the home and more generally in anthropized environments. This highly interdisciplinary area requires the contribution of different technologies and skills, including design, information technology and electronic engineering. Home automation devices and/or modules often have elements of contact with anti-intrusion systems as they can be distributed in residential environments, as is the case with anti-intrusion peripherals and can therefore be easily integrated. Typical home automation modules are air quality meters, electricity meters, motorized roller shutter actuators, wind speed meters.
I-BUS	This is the two-way communication line (4 wires only) which connects the peripheral devices (keypads, readers, expansions, etc.) to the control panel. The 4 easily identifiable wires, on the control panel motherboard and on the expansions, are: <ul style="list-style-type: none"> • “+” 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, and on condition that all the system partitions are disarmed.
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 device that captures two-dimensional images in sequence. It is part of a telesurveillance system monitored by an anti-intrusion panel. The IP camera (or “webcam”) transmits video images to an URL address, for direct viewing or for storage of the recorded images. The Inim Electronics control panel manages the following types of IP cameras: <ul style="list-style-type: none"> • static cameras • cameras with Onvif 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	The control panel must always be placed in “Maintenance” mode before the installer starts work on the system, otherwise the system will generate false alarms (tamper and intrusion). The control panel 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	Electrical output point for the activation/deactivation (by the control panel) of a signalling device or activation 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).
Panic	Signalling that may be associated with a state of emergency perceived by the user and signalled to the anti-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	<p>This refers to the status of a partition as requested by the user. The user can carry out the following operations.</p> <ul style="list-style-type: none"> • Disarm - this operation disables the partition completely. During this status, none of the zones belonging to the partition can generate alarms. • Away mode - this operation enables the interior and perimeter zones of the partition. During this status, all of the zones belonging to the partition can generate alarms. • Stay mode - this operation enables only the perimeter zones of the partition. During this status, all the zones belonging to the partition, with the exception of interior zones, can generate alarms. • Instant mode - this operation enables the perimeter zones only and annuls delays. During this status, all the zones belonging to the partition, with the exception of the interior zones, can generate instant alarms with no entry-time delay. • Hold - this operation forces the partition to hold its current status.
Patrol	<p>A periodic inspection of the protected premises carried out by authorized security staff.</p> <p>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.</p>
Perimeter Zone	<p>A zone that monitors the entrance points of the protected building.</p> <p>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.</p>
Peripherals	<p>Device connectible to the control panel via I-BUS.</p> <p>Inim Electronics control panels manage the following peripherals:</p> <ul style="list-style-type: none"> • Keypads • Proximity readers • Expansions • Transceivers • Sounder/flashers • GSM communicators • Isolators <p>The following wireless devices can be added, and are recognized by the control panel as peripheral devices:</p> <ul style="list-style-type: none"> • Keypads • Sounder/flasher
Power supply station	<p>The power-supply station is a device for powering loads and recharging a lead acid battery.</p> <p>It is equipped with a switching power-supply module capable of generating a nominal voltage of 12V included in a metal box that can also contain rechargeable batteries. MARIO</p>
Pre-arm time	<p>The period (expressed in minutes) before an automatic arming operation.</p> <p>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.</p> <p>Each partition can be programmed with its own Pre-arm time.</p>
Premises	<p>The area to be protected.</p> <p>Generally identifies the place of installation of the anti-intrusion system. generally, a house or office.</p>
Primary power source	<p>The primary source of electrical power to the system is normally @ 230V~ 50 Hz (115V60Hz in some American states).</p> <p>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.</p>
Reader	<p>This device allows users to access and control the system. The system readers are connected to the control panel via the BUS.</p> <p>Readers are usually located near the main entry/exit points of the protected building. These devices allow system access to valid keys only. The system readers are capable of recognizing a large number of keys, each characterized by customized parameters. Each reader is enabled to operate on specific partitions, whereas each key is enabled to operate only on the partitions the user is allowed to control. Therefore, if a key is held in the vicinity of a reader, it will be possible to control only the partitions which the two devices have in common.</p> <p>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.).</p>
Scenario	<p>A pre-set arming configuration which applies various operating modes to the system partitions.</p> <p>The control panels have different scenarios programmable by the installer in accordance with the needs of the user.</p>
Shortcuts	<p>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.</p> <p>They can be activated by the user (at keypads, on codes typed in at keypads or on remote phones, at readers or on keys) or on the occurrence (activation) of an event.</p> <p>The shortcuts that can be activated by the user allow direct access to the user menu sections and various operations which normally require several steps inside the user menu.</p>
Smoke detector	<p>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.</p> <p>These detectors have low power absorption during stand-by. The current absorption increases during alarm status and thus signals the danger to the control panel.</p>
Supervision	<p>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.</p>
Tamper (or act of delinquency)	<p>Detection of a serious condition that jeopardizes the operating capacity of the device concerned and thus puts the system at risk.</p> <p>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.</p>
Telephone actions	<p>These are calls sent to programmed contact numbers when specific events start and end (restoral).</p>
Teleservice	<p>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.</p>
Terminal	<p>Screw terminal for the connection of zones (detection devices) or outputs (activation/ signalling devices).</p>

Timers	A logical entity for automatic time-management of programmed peripherals or elements. 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ◦ 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 Inim Electronics control panels the telephone 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, each voice-capable keypad in the system configuration will allow users to record voice messages. Messages can be recorded, played and deleted as required.
Web browser	Software application that allows the user to view web contents over the Internet.
Web server	Software application that processes web page requests from a web browser. The PrimeLAN network board has an integrated web server that provides the browser with a web interface for the management and supervision of the system.
Wireless	An anti-intrusion system whose devices (detectors, keypads, keyfobs) are not connected to the control panel by wires but by electromagnetic 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 appropriately 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.
Zone Alarm	The conditions which generate a zone alarm, on the understanding that the zone belongs to several partitions, are as follows: the zone must detect violation and all the partitions it belongs to must be armed. Zone alarms trigger activation of audible and visual signalling devices (sounders, flashers, reader/keypad LEDs, etc.) and generate voice and digital calls. Zone alarm events automatically generate partition alarm events on all the partitions the zone belongs to. A violated zone will not generate alarms if: <ul style="list-style-type: none"> • it belongs to several partitions and one of them is disarmed • it is inhibited • it is in test status (the event will be saved to the events log only) • it an "interior" zone, and one of the partitions it belongs to is armed in Stay or Instant mode

Appendix B Fault signals

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	The backup battery is charged	Yes
AC Mains failure	Mains failure	The primary power supply 230V~ fails	The primary power supply 230V~ is restored	Yes
Telephone line trouble	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 battery 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 (a)	Loss of at least one wireless detector has been signaled (monitoring time exceeded)	All the wireless detectors are present	Yes
GSM communicator faults	[[[Undefined variable Product/Dispositivi.Modulo GSM_GPRS]]] fault (b)	One of the faults below is present	None of the faults below are present	Yes
Insufficient cover	No signal	The GSM network signal is insufficient	/	No
GSM module communication fault	GSM module fault	The GSM module of the 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 left on the SIM card 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	The communicator detects connection problems on GPRS network	/	Yes
Sol-2G/3G/4G battery inefficient	Low battery	The buffer battery of the Sol-2G/3G/4G module is inefficient or missing	The backup battery is charged	No
Contaminated smoke sensor	Detector dusty (a)	The smoke chamber of at least one or more 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	Zone faults (a)	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.	/	No
Internal resistance of the sounder/flasher battery too high	Battery resist.	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 returns 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	Voltage dispersion to earth has been detected.	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 the "+AUX x" terminal	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
Low voltage on AUX x	Low voltage "x"	A voltage below 9.8V has been detected on the "+AUX x" terminal	The normal voltage on the terminal has been restored.	Yes
Undervoltage on BUS	Undervoltage BUS	A voltage below 9.8V detected on the "+" terminal of the I-BUS	The normal voltage on the terminal has been restored.	Yes
Short-circuit on +AUX x	ShortCircuit"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 x" terminal	The terminal restores to normal.	Yes
Overload on BUS power supply	Overload BUS	A load 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 fails to communicate with the control panel	Communication between the power supply unit and the control panel restores.	Yes
Low battery on wireless keypad	Low battery WLS keypad (a)	The battery of a least one wireless keypad must be replaced	All the wireless keypads are running with sufficient power	No
Panel tamper	PanelTamper	The frontplate of the control panel has been opened or the control panel has been detached from the wall	The frontplate of the control panel has been closed or the control has been reattached to the wall	Yes
I/O Expansion tamper	Expansion tamper	A sounder/flasher connected to the BUS signals tamper	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	An expansion board on the BUS signals tamper conditions	All the sounder/flashers connected to the BUS reset tamper	Yes
Sol-2G/3G/4G tamper	Sol-2G/3G/4G tamper	The GSM communicator signals tamper conditions	Tamper conditions clear on the communicator	Yes
Home-automation module tamper	HomAut.mod tamp.	One of the home-automation modules has been tampered.	Tamper conditions clear on all the system home-automation modules	Yes
Tamper on the power-supply station	PowerStationTamp	One of the power-supply stations has been tampered.	Tamper conditions clear on all the power stations	Yes
I/O expansion loss	Expansion tamper	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 device connected to the BUS is not present	All expansion boards can be found on the BUS	Yes
Sol-2G/3G/4G loss	Sol-2G/3G/4G loss	The control panel cannot find the GSM communicator	The communicator can be found on the BUS	Yes
Home-automation module loss	HomAut. mod loss	One of the home-automation modules is not present.	All home-automation modules can be found on the BUS	Yes
Power-supply station loss	PowerStationLoss	One of the power-supply stations is not present	All the power-supply stations can be found on the BUS	Yes
Internet connection loss	IP conn.Lan lost	The IP connectivity test is enabled and the test result in negative (failed).	A connection attempt has been successful.	Yes
GSM connection loss	IP conn.GSM lost	The GSM connectivity test is enabled and the test result in negative (failed).	A connection attempt has been successful.	Yes
Low battery on keyfob	Low batt. keyfob	One of the keyfobs in the configuration signals low battery voltage	All the keyfobs have effective battery voltage.	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.

Notes

Notes

Notes

Disposal of the product



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.



Information about disposal of batteries and accumulators (applicable in Countries with separate collection systems)

This marking on batteries and/or their manual and/or their packaging, indicates that batteries of this products, at the end of their working life, should not be disposed of as unsorted municipal waste, but must be object of a separate collection. Where marked, the chemical symbols Hg, Cd o Pb indicate that the battery contains mercury, cadmium or lead above the reference levels of the directive 2006/66/EC. If batteries are not properly disposed of, these substances, together with other ones contained, can cause harm to human health and to the environment. To protect human health and the environment, to facilitate treatment and recycling of materials, separate batteries from other kind of waste and use the collection scheme stated in your area, in accordance to current laws. Before disposing of the above, it's appropriate to remove them from their holders avoiding to damage them or causing short circuits.



Evolving Security

Inim Electronics S.r.l.

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

info@inim.biz _ www.inim.biz

ISO 9001 Quality Management
certified by BSI with certificate number FM530352



DCMUINE0PRIMEE-170-20230714