

English

intelbras

User manual

AMT 8000 LITE
AMT 8000 PRO



AMT 8000 LITE and AMT 8000 PRO

Alarm center

Congratulations, you have just acquired a product with Intelbras quality and security.

The wireless alarm centers AMT 8000 LITE and AMT 8000 PRO have advanced technology and are easy to program. They can be connected to all series 8000 devices by exchanging encrypted information for greater system security. Both models have an integrated siren and 16 partitions. The system features differentials such as high-performance (bidirectional) wireless device communication with a range of up to 1000 meters without barriers and direct targeting, GPRS, GSM, Ethernet/Wi-Fi and telephone line connections¹ to provide greater ease for monitoring reporting to 2 IPs (monitoring companies), 2 telephone numbers (monitoring company) plus the Intelbras Cloud connection, initially using the random remote access password indicated together on the QR Code label that also contains the MAC.

The alarm centers, AMT 8000 LITE and AMT 8000 PRO, have remote firmware update, using Ethernet communication for the execution of download the firmware version. In addition to this option, the alarm center can also be updated by using the BootLoader feature. For this, it is necessary to have the **Atualizador** (Updater) 8000 software previously installed on your computer.

¹ Phone line (FXO 8000 module card required) and Wi-Fi only for AMT 8000 PRO.



ATTENTION: this product comes with a factory default password. For your security, it is imperative that you change it as soon as you install the product and ask your technician about the configured passwords, which users have access and the recovery methods.



This equipment must be connected to a power outlet that has grounding (three pins), in accordance with the electrical installation standard ABNT NBR 5410, to ensure user safety against electric shocks.

Care and safety

- » Follow all instructions in the manual for installation and handling of the product.
- » Carry out the installation in environments that are not susceptible to factors such as rain, fog and water splashes.
- » Wireless communication technology, when exposed to environments with high power radiation, may suffer interference and have its performance impaired. Example: locations near TV towers, AM/FM radio stations, amateur radio stations, etc.
- » Do not install the alarm center and its accessories near radio frequency equipment such as routers, repeaters and/or Wi-Fi signal amplifiers. The alarm center and its devices must maintain a minimum distance of 2 meters from these equipment.
- » Do not install the alarm center facing air conditioning or heating equipment.
- » Do not expose directly to sunlight.
- » Only clean the external part of the device, using only a damp cloth (do not use chemical solvents).
- » Do not subject the device to excessive pressures or knocks/drops.
- » Check whether the installation site, the indicator LED of the devices flashes green when activated.
- » Avoid installation on metallic surfaces so as not to attenuate the transmission signal between system devices.
- » The installation and configuration of the alarm center and the other products that make up this system must be carried out by a qualified professional.
- » Perform periodic tests on it, in order to validate weather conditions, battery level and other factors, so that the site monitored by the system is always able to operate correctly.
- » LGPD - General Law for the Protection of Personal Data: this product does not process any personal data.

Summary

1. Technical specifications	6
2. Features of the alarm centers, AMT 8000 LITE and AMT 8000 PRO	7
3. AMT 8000 LITE and AMT 8000 PRO Accessories	7
3.1. GPRS module XG 2G, GSM XG 3G and GSM XG 4G	7
3.2. Communication module via telephone line – FXO 8000	8
4. Installation of the alarm center and its peripheral devices	9
4.1. Alarm center power supply (full range 90 and 265 Vac)	11
4.2. Battery	11
4.3. XG 2G/XG 3G/XG 4G module	12
4.4. FXO 8000 Phone Module	12
4.5. AMT 8000 LITE and AMT 8000 PRO alarm center	13
5. Operation	13
5.1. Description of XAT 8000 LCD keyboard indications	13
5.2. Exhibition of problems	13
5.3. Description of the LED signaling on the alarm center boards	13
5.4. Partitioning	14
5.5. Alarm center activation/deactivation	14
5.6. Menu	16
5.7. Remote update	19
6. Programming	19
6.1. Wi-Fi Provisioning	19
6.2. Connection to the AMT 8000 PRO Wi-Fi network	19
6.3. Programming mode	20
6.4. Wireless devices (register/delete)	22
6.5. Wireless sensor functions	27
6.6. Remote control key functions	29
6.7. Wireless keyboard functions	31
6.8. Siren functions	33
6.9. Update	40
6.10. Passwords	41
6.11. Quick configurations for monitoring	44
6.12. Configurations of zones	48
6.13. Program the partitioning of the alarm center	52
6.14. Timings	53
6.15. Alarm center time configurations	54
6.16. Time zone	56
6.17. Periodic test	57
6.18. Automatic activation	57
6.19. Monitoring configurations	61

6.20. Activation/deactivation of functions80

6.21. Time for sending of AC failure.83

6.22. System reset84

6.23. Programming quick reference.84

6.24. Approval102

Warranty Terms103

1. Technical specifications

Product	Monitored alarm center
Communication	AMT 8000 LITE Ethernet (100 Mbps and Full Duplex) AMT 8000 PRO Ethernet (100 Mbps and Full Duplex) / Wi-Fi 2,4GHz (IEEE 802.11b/g/n)
Wi-Fi Provisioning	AMT 8000 PRO
Integrated siren	Audible power of 100 decibels at 1 (one) meter
AC Power Supply	90 to 265 V (it is recommended to use a cable with gauge ≥ 1 mm)
DC Power Supply	5.7 coming from the AMT 8000 LITE/PRO source
Battery	3.7 Vdc 2.000 mA rechargeable battery (included with the alarm control panel)
Operating temperature	-10 °C to 50 °C @ 90% humidity
Weight	568 grams (with battery)
Dimensions (W x H x D)	About the product: 170 x 211 x 81 mm With individual packaging: 177 x 216 x 82 mm
Average power ¹	AMT 8000 LITE: 5.2 Watts
	AMT 8000 LITE + XG: 8.1 Watts
	Antenna type: indoor Antenna gain: 0 dBi
Wireless communication frequency AMT 8000 LITE/PRO/Accessory	915 to 928 MHz via internal antenna, power 18 dBm
Modulation	DSSS BPSK 40 Kbps
Optional devices ²	XAC 8000 remote control
	REP 8000 Range RF Amplifier
	XAT 8000 Wireless Keyboard
	XAS 8000 wireless magnetic sensor
	Universal Transmitter TX 8000
	IVP 8000 EX wireless passive infrared sensor
	IVP 8000 Pet Wireless Passive Infrared Sensor
	Wireless passive infrared sensor IVP 8000 Pet Cam
	GPRS XG 2G Module
	GSM XG 3G Module
	GSM XG 4G Module
	FXO 8000 module
	XSS 8000 Wireless Siren
	PGM 8000 wireless actuator

¹ **Conditions:** maximum power verified with the alarm control panel activated, with registered peripherals (keyboards/sensors/sirens) and with the means of communication connected and operating together with the alarm center. In some operations, consumption may vary according to the number of peripherals operating in the security system and their exchange of information (Stand by mode - continuous).

² **Optional devices:** FXO 8000 module compatible only with the AMT 8000 PRO model, for more information, consult the website www.intelbras.com.br.

Attention: Intelbras wireless systems are tested with the highest standards of demand and bring high reliability, however, due to the use/installation in varied scenarios, some considerations must be taken into account:

- » Transmitters/receivers may be disturbed by radio signals, natural interference, location of device operation, weather issues and other adversities that affect data transmission regardless of the frequency or technology used, since the transmission medium is adverse and different from place to place.
- » Device receivers/transmitters have an internal processing time, and only receive the necessary data for communication between them after this particular time for the system.
- » Wireless devices should be tested regularly to determine if there are any sources of interference and to protect against occasional failures.

2. Features of the alarm centers, AMT 8000 LITE and AMT 8000 PRO

- » Capacity for 16 partitions with independent activation/deactivation.
- » Allocation of zones according to the desired partitions.
- » Wireless signal receiver/transmitter integrated into the alarm center operating at a frequency of 915 to 928 Mhz.
- » Support 2 SIM card mobile phone with XG 2G, XG 3G or XG 4G module installed.
- » Quad band GPRS modem: compatible with most national GSM operators for AMT 8000 LITE and AMT 8000 PRO operating with XG 2G, XG 3G and XG 4G module (sold separately).
- » Event reporting:
 - » **AMT 8000 LITE:** event reporting via Ethernet connection, GPRS connection (with XG 2G module installed - sold separately), GSM connection (with XG 3G module installed - sold separately) and GSM connection (with XG 4G module installed - sold separately).
 - » **AMT 8000 PRO:** event reporting via Ethernet/Wi-Fi connection, via telephone line (with FXO 8000 module installed - sold separately), GPRS connection (with XG 2G module installed - sold separately), GSM connection (with module XG 3G installed - sold separately) and GSM connection (with XG 4G module installed - sold separately).
- » Remote access to the alarm center via application.
- » Use in conjunction with all wireless devices in the 8000 line.
- » Capacity for visualization and programming of parameters by up to 16 XAT 8000 keyboards.
- » Built-in wired siren plus 16 XSS 8000 wireless sirens.
- » Capable of connecting up to 98 XAC 8000 controllers with user identification.
- » Capacity for connecting up to 64 wireless sensors from the 8000 line.
- » Remote programming via Ethernet, GPRS and GSM.
- » Capacity for connecting up to 04 REP 8000 RF amplifiers. Programming for up to 97 passwords including duress with configurable permissions.
- » Monitorable by Contact-ID protocol.
- » Supervision of sensors, wireless sirens, keypads, PGMs and repeaters.
- » Low battery detection of wireless devices.
- » Internal buffer for 512 events.
- » Remote firmware update via Ethernet connection.

3. AMT 8000 LITE and AMT 8000 PRO Accessories

The AMT 8000 LITE and AMT 8000 PRO alarm centers can have various accessories grouped together to compose the monitoring and security system, with the accessories responsible for communication and monitoring, the sound warning, LCD keyboard and various sensors, for better adequacy and composition of the necessary protection system.

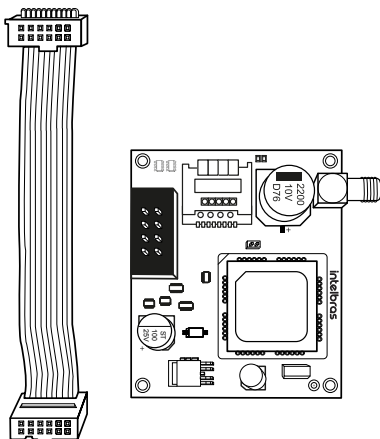
3.1. GPRS module XG 2G, GSM XG 3G and GSM XG 4G

Optional dedicated accessory for data transmission via GPRS / GSM for communication, configuration and event reporting between user and/or monitoring company with the AMT 8000 LITE and AMT 8000 PRO security system.

Features

- » It supports up to two SIM card type chips.
- » 2G GPRS communication with XG 2G module, 2G/3G communication with XG 3G module and 4G communication with XG 4G module.
- » External antenna with 0 dBi gain.
- » Reports events to 2 IP destinations (monitoring company) plus the Intelbras cloud.
- » Connections with DNS destinations.
- » Power supply from the AMT 8000 LITE or AMT 8000 PRO alarm center.

The following figure presents an illustrative image of the XG 2G, XG 3G and XG 4G modules:



GPRS module XG 2G, GSM XG 3G and GSM XG 4G

Obs.: XG 2G, XG 3G and XG 4G modules are compatible with most national GPRS / GSM operators with 2G, 3G and 4G technology.

3.2. Communication module via telephone line – FXO 8000

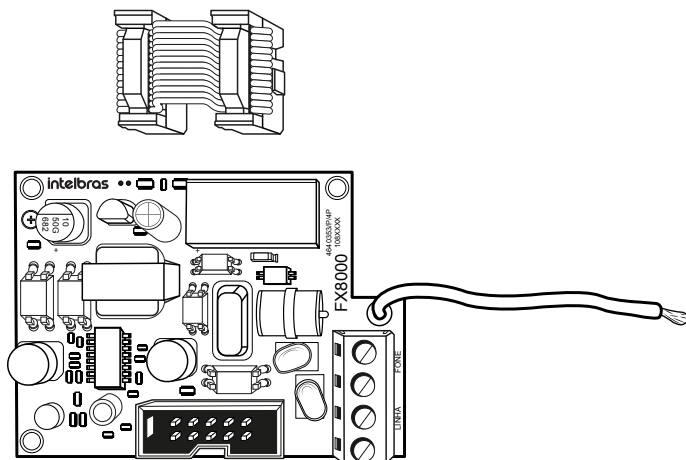
Dedicated optional accessory for data transmission via telephone line for communication and event reporting to the monitoring company with the AMT 8000 security system, in addition to dialing up to 5 personal telephones and issuing, through the telephone line, the sound of a siren.

Attention: the FXO 8000 module is only compatible with the AMT 8000 PRO alarm center.

Features

- » Up to 7 programmable phone addresses.
- » DTMF type dialing mode.
- » Telephone line cut/interruption check.
- » Contact-ID communication protocol.
- » Power supply from the AMT 8000 alarm center.

The following figure shows an illustrative image of the FXO 8000 module:



FXO 8000 Phone Line Module

4. Installation of the alarm center and its peripheral devices

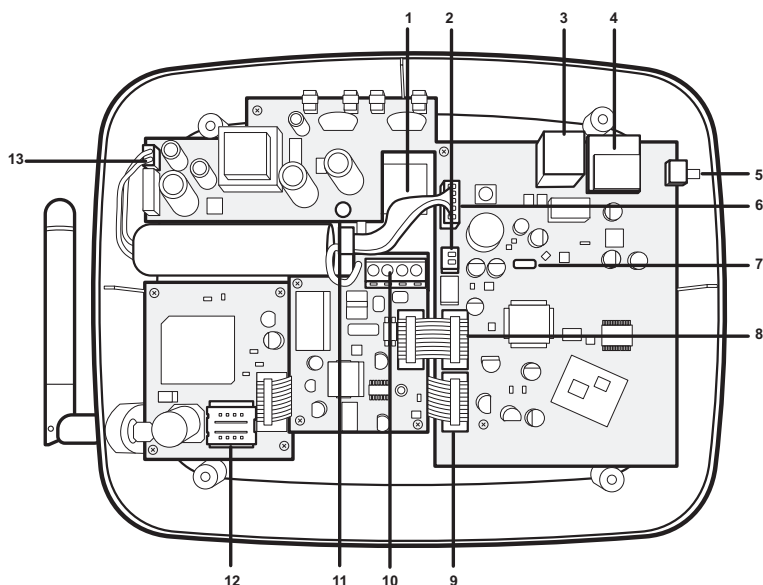
Attention: only connect the central to the mains and battery after installing all the equipment and peripheral devices.

Open the product box and then open the alarm center cabinet cover by removing the screws, where you will be able to see two plates, that is, its basic configuration contains the AMT 8000 LITE or AMT 8000 PRO alarm center plate and its respective power supply and the rechargeable battery that comes with the alarm center.

You can purchase the XG 2G, XG 3G and XG 4G modules for the AMT 8000 LITE alarm center and the XG 2G, XG 3G, XG 4G and FXO 8000 modules for the AMT 8000 PRO, and these boards have their respective interconnection cables with the alarm center.

The AMT 8000 LITE and AMT 8000 PRO alarm center have only wireless zones, as well as other accessories (keyboard, sirens, etc.) are connected to the alarm center via a wireless signal, with only the AC power and Ethernet cables connected to alarm center.

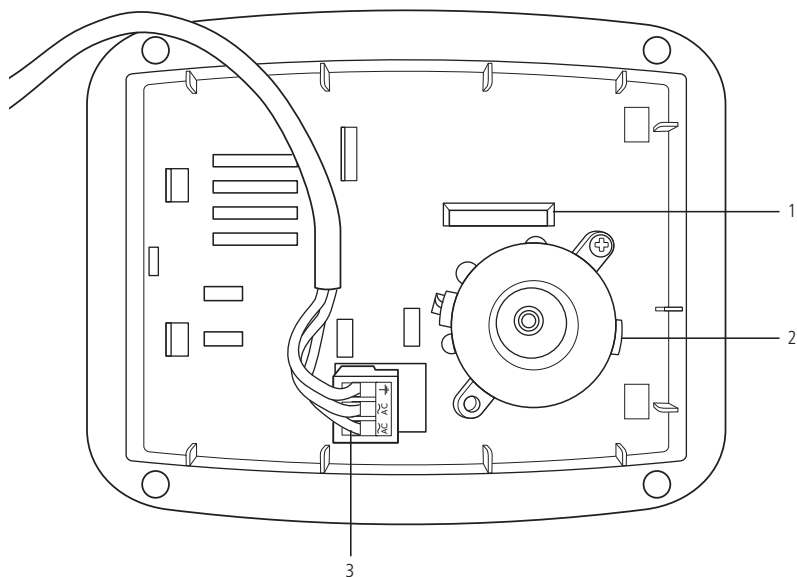
The following image illustrates the alarm center with all the devices that can be physically connected:



AMT 8000 LITE/PRO alarm control

1. Opening for passing the Ethernet cable and telephone line (AMT 8000 PRO compatibility).
2. Integrated siren connection.
3. Connector for Ethernet network cable.
4. Wi-Fi Module (AMT 8000 PRO compatibility).
5. Button for registering wireless devices.
6. Connector for power supply flat cable.
7. Micro-USB type connector for updating the alarm control panel's firmware.
8. Connector for FXO 8000 module flat cable (AMT 8000 PRO compatibility).
9. Connector for flat cable of XG 2G, XG 3G and XG 4G modules.
10. Connector for connecting the telephone line and telephone (AMT 8000 PRO compatibility).
11. FXO 8000 board ground point (AMT 8000 PRO compatibility).
12. Connector for SIM 1 and SIM 2 card.
13. Input connector for battery connection.

Note: XG 2G, XG 3G and XG 4G modules are compatible with most national GSM operators with 2G, 3G and 4G technology.



1. Tamper-proof switch.
2. Integrated siren.
3. Connector for AC power.

Caution: be careful not to invert the position of the ground wire.

Attention: the AMT 8000 LITE and AMT 8000 PRO alarm control panels do not have an auxiliary output to power other devices and no connection point on the control panel boards (control panel or source) should be used for this functionality, as in addition to damaging the alarm control panel and its accessories, it may damage the devices that are connected because the alarm panels operate with different voltages.

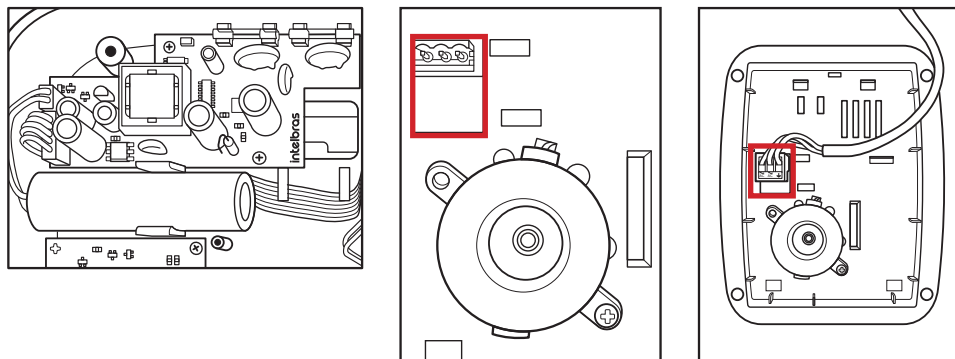
4.1. Alarm center power supply (full range 90 and 265 Vac)

The alarm center is equipped with a full range switching power supply that works with input voltages of 90 and 265 Vac without the need for a voltage selector switch. In this way, even if there is some voltage variation in the electrical network, the alarm center will continue to function normally (as long as the voltage is in the range of 90 to 265 Vac).

There are two alarm center protection fuses on this board. If you need to change it, use new ones of the same value (250 V/400 mA).

To connect the AC electrical grid input and also to ground, it is recommended to use a three-pin cable with a gauge of 1 mm or greater.

The output for the alarm center board is 5.7 Vdc and 1.7 A.



AMT 8000 LITE/PRO power supply

Connect the ground terminal of the source as shown in the image above to the ground of the local electrical installation.

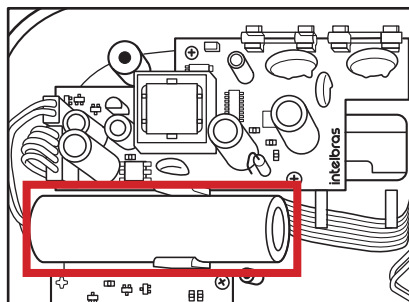
If the local electrical installation does not have grounding, install a grounding bar and connect the connection terminal to the alarm center to carry out the correct grounding.

Attention: it is mandatory that the grounding connection be done on the alarm center so that there is greater protection against lightning and overload by the electrical grid. If this connection is not made, the alarm center will work normally, but it will be unprotected against overloads

The warranty does not cover possible damage caused by lightning to the alarm center or any other equipment connected to it.

4.2. Battery

The AMT 8000 LITE and AMT 8000 PRO alarm panels have an internal rechargeable 3.7 Vdc battery with a capacity of 2.000 mA. The battery connector is located on the power supply board and is used to connect the battery to the alarm system. To connect the battery to this connector, use the cable that comes with it, as shown in the figure below.



Rechargeable battery for AMT 8000 LITE and AMT 8000 PRO alarm center

The alarm centers have protection against inversion of polarity and short circuit in the battery and protection to prevent the battery from being damaged in the event of a failure in the electrical grid (if the battery voltage is below 2.8 V, the control unit will turn off so as not to damage the battery).

Attention: the battery can take up to 12 hours to complete its first charge cycle.

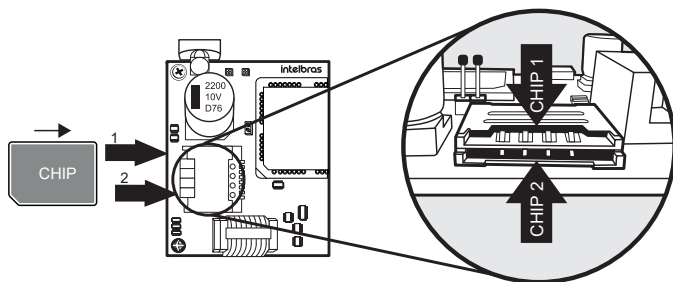
Battery duration:

- » Approximately 4 hours reporting events via GPRS/Ethernet + built-in siren on constant fire;
- » Approximately 13 hours reporting events via GPRS (only hourly periodic test and with integrated siren in stand by);
- » Approximately 17 hours reporting events via ETH (only hourly periodic test and with integrated siren in stand by).

Attention: if battery replacement is necessary, please contact our authorized service network or an authorized reseller.

4.3. XG 2G/XG 3G/XG 4G module

In the modules XG 2G, XG 3G and XG 4G there are two slots to be allocated two chips (SIM card) overlapping one over the other, with chip 1 being above chip 2. When installing the chips, leave their metallic contacts facing downwards and insert them to the end of the slot for the correct allocation of the chips.

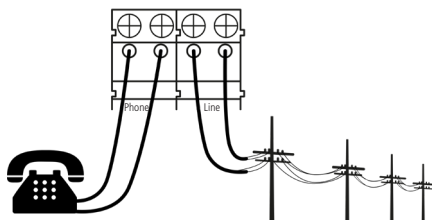


Chip allocation on the module

4.4. FXO 8000 Phone Module

Check if the cable for connection to the alarm center is correctly connected, and its installation should only be done with the alarm center turned off to avoid damage to the equipment and the installer.

In the FXO 8000 module there is a Line terminal, where it must be connected to the main telephone line (two wires), connecting the Phone output (two wires) to the other telephone devices contained in this same line and as can be seen in the following image:



Telephone line connection plan on the FXO 8000 module

Attention: the FXO 8000 module is only compatible with the AMT 8000 PRO alarm center.

This connection is necessary so that, in the case of reporting events or remote accesses, the alarm center does not run out of communication or have it interrupted if other telephones on the same circuit start/are in operation. In this case, at the time of event reporting, the other phones will be inoperative, as the alarm center will be occupying the line.

4.5. AMT 8000 LITE and AMT 8000 PRO alarm center

The AMT 8000 LITE and AMT 8000 PRO alarm centers have an integrated wired siren, tamper switch against violation, and if the tamper switch is opened/violated, the integrated siren plus the registered sirens will go off and send the corresponding event if the function Problems that generate trigger is enabled (see section *Problems that generate trigger*).

Ethernet and AC power supply cables must be routed through the hole located on the back of the alarm center.

The installation of the alarm centers can be on different surfaces, always placing them in a vertical position with a height between 1.80 and 2.20 meters and using double-sided tape or screws (not included) to fix the base and after attaching the alarm center, fitting and checking that there was correct placement so that there are no falls and damage and directing the wires in the dedicated areas.

5. Operation

Once the installation is complete, turn on the control unit by connecting it to the local electrical grid and to the rechargeable battery.

Obs.: to turn on the AMT 8000 LITE and AMT 8000 PRO alarm centers, it is necessary that they are connected to the AC network, otherwise the alarm centers will not turn on, even if the batteries are connected. In the event of an AC power outage, the alarm centers will be maintained by the battery and when the AC network returns, the batteries will be recharged.

5.1. Description of XAT 8000 LCD keyboard indications

At the top of the LCD display are located the indication icons described below:

- » : if this icon is flashing, it indicates that a problem has been detected.
- »  will light whenever there is trigger in the siren.
- » **P:** with the icon accessed, the alarm center is in programming mode.
- » **Battery:** indicates the battery status of the alarm center.

5.2. Exhibition of problems

The occurrence of problems is described as follows:

On the XAT 8000 keyboard, the icon  will be blinking.

If any problems are detected, press the up or down arrow keys on the XAT 8000 keyboard to view them. To end the display, press the *Exit* key.

Obs.:

- » If the function Indication of problems by siren on activation/deactivation and Siren beep on activation/deactivation are enabled and if a problem is detected, 1 long beep will be emitted on activation and 2 long beeps on deactivation.
- » To clear the keyboard after shots, just press the *Exit* key.

5.3. Description of the LED signaling on the alarm center boards

alarm center base plate LEDs

LED	Status/event	Signaling ¹
LED1/LED2	Disconnected from the Ethernet network	LED off
LED1/LED2	Connected with the Ethernet network ¹	LED blinking constantly
LED3	Alarm center off	LED off
LED3	Alarm center on	LED blinking
LED3	Alarm center on and registering devices	LED accessed

¹ This status does not mean that the system is connected to the monitoring servers. To view the connection status, observe through the Menu function (see section *Connections*).

GPRS XG 2G/ XG 3G board LEDs

LED	Status/event	Signaling ¹
LED1, LED2	Power supplied (on on the CPU board)	LED1 and LED 2 constantly accessed
LED1, LED2	Chip (SIM1 or SIM2) looking for connection	Only the corresponding accessed LED
LED1	Chip 1 (SIM1) connected to servers	LED blinking once (connected to server 1), LED blinking twice (connected to server 2)
LED2	Chip 2 (SIM2) connected to servers	LED blinking once (connected to server 1), LED blinking twice (connected to server 2)

¹ This status does not mean that the system is connected to the monitoring servers. To view the connection status, observe through the Menu function (see section Connections).

5.4. Partitioning

Using this feature through the control panel's programming, it is possible to divide it into up to 16 partitions with independent activation and deactivation and associate any of the 64 wireless zones to any of the partitions. It is also allowed to program passwords giving specific permissions for these partitions.

This function is useful in offices, homes or other places in the same building that need more alarm panels, because with partitioning, the panel is divided and each partition operates individually, as if it were an independent alarm center.

The 16 partitions can be controlled via keyboard, remote control, software and applications compatible with the AMT 8000 LITE and AMT 8000 PRO alarm centers, as one partition can be activated or deactivated without influencing the other.

When the system is partitioned, zones and any of the other wireless devices on the 8000 Line can be partitioned as shown below (for more information, see section 6.10. Configuration of zones).

- » **Common:** The zone does not belong to any of the partitions. It will only be activated when all partitions are activated and will be deactivated whenever one of the sixteen partitions is deactivated.

Example: in an office divided by two professionals, one room is defined for Partition 01, and another for Partition 02 and the reception as the common zone. That way, even if one of the people leaves and activates his partition, the reception will remain deactivated and will only be activated when the other partition is also activated.

- » **Partition (01 to 16):** wireless devices registered in zones defined to belong to any of the 16 partitions will have access or be influenced by the chosen partition.

Example: in a gallery comprising 8 rooms, each room will have its own independent partition with specific zones, with independent activation and deactivation. In this scenario, each partition can have independent sirens and keyboards or share devices between partitions (common sirens and keyboards).

- » **Partial:** zones selected for this option remain inactive during *Partial mode* wakeup regardless of the partition associated with it.

Example: assuming that for partition 01, consisting of zones 01 to 10, only zones 01 to 05 are enabled as *Partial mode*. When executing the command for the *Partial mode* option for a given partition, in this case, partition 01, if someone passes in the sector where sensors 01 to 05 are located, the control panel will not trigger - zones where the occupants of the place will be present and during activation of *Partial mode* do not trigger, since if someone passes through sensors 06 to 10, the control panel will trigger for partition 01, indicating such triggered sectors, being signaled by sirens and sending events to monitoring/applications, if used.

Obs.: during full partition activation - outside of *Partial mode*, all zones in the partition will trigger.

5.5. Alarm center activation/deactivation

The alarm center can be activated and/or deactivated in different ways, depending on the defined settings. For any of the ways to activate the system, with the exit time different from zero, after entering the password, the keyboard will emit beeps at intervals of 1 second. In the last five seconds of the delay, these beeps will become faster to indicate that the exit delay is at an end. At the end of the exit time, the siren will emit a sound (if programmed) indicating that the alarm center is activated.

Attention: » For some programming of the alarm center and also to activate it, it is necessary to use the 4-digit master password, indicated on the QR code label inside the alarm center. This password can be changed as discussed in the fields below.

- » If the switchboard system is reset, it will no longer use the random passwords that are linked together with the QR code label pasted inside the switchboard and will use password 1234 as the master password and password 878787 as access remote until they are changed again.

Obs.: » If there is a mistake in entering the password, press the Back key and enter the password again.

- » When the control panel or partition receives the command to activate and any of the zones is open, a fault/error will be generated (long beep on keypads) and it will only be possible to activate the control panel when all zones are closed in the case of a complete or non-partitioned system, or in the case of partitioned systems with the zones of the respective partitions closed. To activate the control panel with open zones, see section General configurations 1.

Activation / deactivation in non-partitioned systems

Full mode activation

To fully activate the system, enter a valid password on the XAT 8000 keyboard, for example the master password. To find out if the alarm center is activated, just slide the keyboard cover and view the message, if the alarm center is activated, the message will be shown: *Alarm activated*, otherwise *Alarm deactivated* will be shown.

Activation through a key

If the *One-Key Activation* function is enabled (see section General configurations 1), pressing and holding the active key until the keypad emits a confirmation beep (+/- 3 seconds) will activate the system in *Full* mode. The exit timing will be started in order to leave the protected area. At the end of the exit delay, the system will be activated in *Full* mode (all partitions). This procedure does not allow to deactivate the system.

Obs.: if a common keyboard is used, all partitions will be activated in the case of a partitioned alarm center. In case of keyboard with permissions for partitions, only the partition where this keyboard has permission will be activated.

System deactivation

To deactivate the system enter a valid password, for example the master password. After entering the password, the control panel will be completely deactivated and the *Deactivated alarm* information will be displayed.

Zones, which must be passed through to reach the keyboard, must be programmed as timed for entry or as followers so the alarm does not go off immediately when the keyboard access path is breached/accessed. After entering the area protected by a timed zone for entry, the entry timing will start and the user must enter a valid password on the keyboard before the delay expires, to avoid triggering the alarm and reporting the corresponding events. See section *Zone Functions* to define as timed.

Activation/deactivation by remote control

To activate/deactivate the system by remote control, it is necessary that it is registered in the control panel, as described in section 6.4. *Wireless devices (register/delete)*.

The control leaves the factory configured so that button 1 only deactivates the alarm center, button 2 only activates it and button 3 is disabled. The remote control will have the same permissions as the password of the user it is associated with (user 00 to 97).

Activation / deactivation on partitioned systems

Before trying to carry out the following operations, it is necessary to program the alarm center for one of these conditions and to do so, consult the section 6. *Programming*.

Activation by master password or full password

If you are using the master password or a full password (which has permission to activate/deactivate more than one partition), there are two ways of activation:

- » **All partitions:** enter the password, the exit timing will start and at the end, all partitions will be activated.
- » **Desired partition only:** press the *Activate key + Partition (01 to 16) + Password*. The exit timing will start and at the end, the partition chosen in the range (01 to 16) will be activated.

With the partitioned alarm, when entering the Master password or FULL PERMISSION USER password, if any partition is activated, it will deactivate the activated partitions and will not activate pending partitions.

Activation in Partial mode

Activation in *Partial* mode allows you to partially activate the system, that is, it is possible to select some zones to remain deactivated while others remain activated. For example, it is possible to activate the external zones while the internal zones remain deactivated, allowing people to circulate inside the property without triggering the alarm. But, if someone tries to break into the place through an activated zone, the alarm will go off normally.

In this mode, the zones selected for *Partial* mode remain disabled and the other zones will be activated normally.

To activate *Partial* mode, enter *Partial + Password*. The exit timing will begin and the keyboard will beep at 1 second intervals. In the last 5 seconds of the timing, these beeps will become faster to indicate that the exit time is at an end. To activate, in *Partial* mode, a specific partition with a password with permission for more than one partition, use the sequence *Activate + Partial + Partition (01 to 16) + Password*.

Obs.: only master password and passwords with permission to enable Partial mode enabled can activate the system in Partial mode.

Deactivation by master password or full password

If you are using the master password or a full password (which has permission to activate/deactivate all partitions), there are two forms of deactivation:

- » **All partitions:** type the password and all partitions will be disabled.
- » **Desired partition only:** press *Deactivate key + Partition (01 to 16) + Password* and the chosen partition in the range (01 to 16) will be deactivated.

Zones, which must be passed through to reach the keyboard, must be programmed as timed for entry or as followers so the alarm does not go off immediately when the keyboard access path is breached/accessed. After entering the area protected by a timed zone for entry, the entry timing will start and the user must enter a valid password on the keyboard before the delay expires, to avoid triggering the alarm and reporting the corresponding events. See section *Zone Functions* to define as timed.

Activation/deactivation by specific user password

Specific passwords can be programmed to activate/deactivate a Partition (between 01 to 16). In this case, just enter the password to activate/deactivate the corresponding partition.

Upon activation, the exit timing will start and the partition will be active at the end of the programmed time.

Upon deactivation, the keyboard must be accessed through a timed zone if necessary and the password entered before the end of the programmed time so that there is no triggering and event reporting.

Activation/deactivation by remote control

To activate/deactivate the system by remote control, it is necessary that it is registered in the alarm center, as described in section 6.4. *Wireless devices (register/delete)*.

The control leaves the factory configured so that button 1 only deactivates the alarm center, button 2 only activates it and button 3 is disabled. The remote control will have the same permissions as the password of the user it is associated with (user 00 to 97).

synchronization

5.6. Menu

The alarm center has the *Menu* function to facilitate the visualization of the status and the execution of some commands. When accessing one of the options, if you want to return to the *Main* menu, press the *Back* or *Exit* key to direct you to the initial screen.

Bypass

Through this function it is possible to temporarily cancel one or more zones. With this function, zones that are bypassed (suffer bypass) during the next activation will not generate triggers in the system if they are violated.

After the system is deactivated, zones that were bypassed will revert to their normal configuration. Only the master password user and users with bypass permission can temporarily cancel a zone.

This function must be programmed at most 30 seconds before the system is activated, otherwise the operation will be canceled.

The procedure for temporarily canceling a zone is as follows:

1. With the system off and out of programming mode, press the *Menu* key;
2. With the marker in the bypass position, press the *Enter* key;
3. Through the numeric and directional keys on the keyboard, select which zones will have the bypass active (01 to 64);
4. Press the *Enter* key to confirm the cancellation of the selected zones;
5. Type in the master password or a password with permission to cancel zones;
6. If an invalid password is entered, the message *Incorrect password error* will be displayed and the keypad will continue to display the zones to be canceled until a valid password is entered or it exceeds the time of 30 seconds. If a password is entered without permission to cancel, the message *No permission to cancel sensor* will be displayed and the operation will be canceled immediately;
7. To cancel the operation, press the *Exit* key before entering the password.

To cancel a zone more than 30 seconds before activation, enter in the programming mode (*Enter + Password*) using a password with permission for bypass and perform steps 1 through 4. The next time the system is activated, the bypass will be performed, even if the user who performed the activation does not have permission to bypass.

Open sensors

In normal operation mode, the XAT 8000 keyboard will display the status of the alarm center and if there are any open zones.

To view currently open zones, press the *Menu* key and then access *Open sensors* and press the *Enter* key.

Outside the programming mode, if *1 + Enter* is pressed, zones 1 to 10 will be displayed. *2 + Enter* displays zones 11 through 20, and so on, up to the key *7*, which displays zones 61 through 64.

The status of the sensors in their respective zones will be displayed, distributed in divisions of 10 zones. To change the group of zones press the arrow keys down or up, for example to access zones 41 to 50 press the down key on the keyboard until the number 4 appears in front of the first square, making the number 1 referring to zone 41 and so on, making the number 5 referring to zone 50.

Group 1 will represent zones 1-10, group 2 zones 11-20, and so on, up to zones in group 7, thus demonstrating the status of zones 1-64.

To facilitate the interpretation of this way of identifying the status of the zones (open or closed), next to the number of the sensor, a square will be displayed, which according to its marking will be the status of the zone:

- » Empty square (□) closed/unviolated zone.
- » Filled square (■) open/violated zone.

Trigger sensors

When the alarm center is active, sensors that are violated (disregarding canceled-bypass sensors) will generate triggers and report events, and the display screen will show the information of the trips that alternate with the information of the status of the alarm center (alarm activated or alarm deactivated).

When pressing *Menu*, with the directional keys leave the marker on *Trigger sensor* and press *Enter* key. Through the directional keys navigate between the sensors/zones of the alarm center to check which sensors generated the trigger.

- » Empty square (□) closed/unviolated zone.
- » Filled square (■) open/violated zone.

Partitions

The partitions enabled on the control panel will be displayed (see the section 6.13. *Program the partitioning of the alarm center* and its respective status.

When pressing *Menu*, with the directional keys leave the marker on *Partitions* and press *Enter* key. Through the directional keys navigate between the partitions of the alarm center to check their status.

- » **Activated:** The partition is activated.
- » **Deactivated:** The partition is deactivated.

Connections

The status of connections for reporting events via IP to monitoring services will be shown.

In the *Cloud* menu of the keyboard, the alarm centers will have only one option filled in, that is, ETH or GPRS. However, priority will be given to communication via ETH.

When pressing *Menu*, with the directional keys leave the marker on *Connections* and press *Enter* key.

- » **Wi-Fi:** empty square (□): not connected to the destination / filled square (■): connected to the destination.
- » **Eth:** empty square (□): not connected to the destination / filled square (■): connected to the destination.
- » **2G/3G:** empty square (□): not connected to the destination / filled square (■): connected to the destination.

Eth: IP1 ■ IP2 □

2G/3G/4G: IP1 □ IP2 □

Status viewing function of IP1/IP2 connections. In this example, IP1 is connected via Ethernet network cable

Obs.:

- » XG 2G module covers 2G technology only, XG 3G module covers both 2G and 3G technology, and XG 4G module covers both 2G and 4G technology. When the XG 3G or XG 4G module is used, the communication technology chosen will depend on the availability of signal coverage by the operator in the region where the exchange is located.
- » Wi-Fi connection available only for the AMT 8000 PRO model.

See the section *Connections* to define addresses of priorities and routings.

- » **Cloud:** will display if the alarm center is connected to the Intelbras Cloud server via ETHERNET or 2G/3G/4G. This server allows communication between the alarm centers and the remote access via application.
- » **Eth:** empty square (□): not connected to Intelbras Cloud / filled square (■): connected to Intelbras Cloud.
- » **2G/3G/4G:** empty square (□): not connected to Intelbras Cloud / filled square (■): connected to Intelbras Cloud.

2G/3G/4G

It will display the operator's signal level in percentage, where square 1 represents a level less than or equal to 10% and square 0 represents 100%. The filled mark corresponds to the active signal and the empty mark to no signal, referring to the level in 10 divisions.

When pressing *Menu*, with the directional keys leave the marker on *2G/3G/4G Signal* and press *Enter* key.



Illustration of GSM network signal level function

Obs.: when the GPRS / GSM function is disabled, disregard this function.

Wireless signal

It will display the signal level in percentage of the wireless devices registered in the alarm center.

When pressing *Menu*, with the directional keys leave the marker on *Wireless signal* and press *Enter* key.

The signal level will be displayed on the keyboard, compared to the color of the LED indicator of the registered devices, as below:

- » **Orange color:** signal level between 1 and 2
- » **Green color:** signal level between 5 and 10

Wireless signal can be viewed from the following devices:

- » **Sensors:** devices registered in the alarm center at addresses 01 to 64. To visualize the signal of the sensors with the marker on it, press *Enter* and then, with the directional keys, toggle between the sensors.
- » **Keyboards:** devices registered in the alarm center at addresses 01 to 16. To visualize the signal of the keyboards with the marker on it, press *Enter* and then, with the directional keys, toggle between the keyboards.
- » **Sirens:** devices registered in the alarm center at addresses 01 to 16. To visualize the signal of the sirens with the marker on it, press *Enter* and then, with the directional keys, toggle between the sirens.
- » **Repeaters:** devices registered in the alarm center at addresses 01 to 04. To visualize the signal of the repeaters with the marker on it, press *Enter* and then, with the directional keys, toggle between the repeaters.
- » **Actuators:** devices registered in the alarm center at addresses 01 to 16. To visualize the signal of the PGM 8000 actuators with the marker on it, press *Enter* and then, with the directional keys, toggle between the actuators.

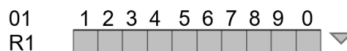
The signal level in percentage will be displayed, where number 1 represents a level less than or equal to 10% and square 0 represents 100%. The filled mark corresponds to the active signal and the empty mark to no signal, referring to the level in 10 divisions.

The wireless device that is carrying out the communication directly with the alarm center will be identified with the letter C and the device that is passing through the range RF amplifier (REP 8000 repeater) will be identified with the letter R.

Ex.: sensor 01 communicating directly with the alarm center.



Ex.: sensor 01 communicating with repeater 01:



Obs.: the repeaters will be identified from R1 (repeater 1) to R4 (repeater 4).

To return the option *Wireless signal* and to check the signal from other devices press the *Back* or *Exit* key to go to the initial screen.

Obs.: the signal level that appears on the keyboard for each of the devices, refers to the last communication that it carried out.

Address MAC

It will display the MAC address of the alarm center. The MAC address will display with 12 digits between numbers and letters. Through this address the alarm center will connect to on-line *on-line servers*.

Alarm center version

It will display the alarm center version.

Keyboard version

It will display the version of the keyboard used.

Test Mode

It will perform the wireless signal test of the keyboard used with the registered alarm center. When pressing *Menu*, with the directional keys leave the marker on *Test* mode and press *Enter* key.

The test will start, showing the information *Signal test* and at the end the result, which can be *Excellent*, *Good*, *Weak* or *No response* in case of loss of communication with the alarm center.

Obs.: the signal level that appears on the keyboard for each of the devices, refers to the last communication that it carried out.

Battery voltage

It will display the keyboard battery voltage level.

5.7. Remote update

The AMT 8000 LITE and AMT 8000 PRO alarm centers have remote firmware updating, and in the case of availability of new firmware versions, it is not necessary to use recorders or connect to computers to be updated, downloading the new version through the Ethernet connection. When performing the version update, the registration of wireless devices or saved configurations will not be lost.

Attention: updating the control panel's firmware version is a programming process and it is recommended that it be done by a qualified professional, with access to the AMT 8000 alarm control panel's programming mode and the control panel must be connected to the cloud server (necessary commands contained in item 6. *Programming*).

6. Programming

The alarm center has several programmable parameters, which makes it versatile, allowing to optimize the operation for each need.

These configurations are stored in EEPROM type memory, thus avoiding the need for frequent reprogramming or in case it is turned off.

To program these parameters, it is necessary to use two special passwords, called master password (the control panel initially has a random master password indicated on the QR code label inside the cabinet) and installer password (factory default: 9090). We recommend that they be modified during installation to increase system security, as this will prevent unauthorized persons from changing the alarm center settings (see section 6.10. *PasswordsPasswords*).

6.1. Wi-Fi Provisioning

The provisioning of the alarm center aims to allow it to communicate via Wi-Fi with customer devices that need to perform remote access via an app or programming software for smartphones and computers, even if the center is not connected to the internet. With this resource, it will be possible to access the alarm center and perform all the necessary configurations.

Enable Wi-Fi Provisioning

To activate this function, with the control panel turned on, press the wireless device registration key for 7 seconds, the LED will start flashing quickly to indicate that the alarm center is in provisioning mode and this mode will remain for 5 minutes, if not performed. access to the alarm center it will cancel provisioning and return to normal operation, if there is a connection to the alarm center it will remain in provisioning mode until the remote connection is terminated by the user.

6.2. Connection to the AMT 8000 PRO Wi-Fi network

The alarm center will create a Wi-Fi network and it will appear on the devices with ssid AMT8000PRO plus the MAC number (EX: AMT8000PRO-XXXXXXXXXX). The access password to the Wi-Fi network created by the alarm center is the same used for remote access + 00 at the end (EX: 87878700).

Obs.: the IP range of 192.168.4.1 will be distributed by the alarm center, and it is not possible to change it.

Access to the alarm center via AMT Remote Mobile

To execute the access via AMT Remote Mobile, select the Local IP connection option and enter the IP 192.168.4.1 plus the remote access password available on the QR Code label (EX: 878787).

Access to the alarm center via Desktop programmer software

To access via Desktop software, on the client's editing screen, enter the IP 192.168.4.1 in the option *IP address for connection via ethernet/wi-fi* plus the remote access password available on the QR Code label (EX: 878787).

Attention: the remote access password is available on the QR Code label along with the MAC address on the alarm center

6.3. Programming mode

Using the XAT 8000 wireless keyboard

When accessing the programming mode, edit or view any programming on the keyboard, if the sequence or password is accepted, 2 confirmation beeps will be emitted, otherwise, a long error beep will be emitted, in which case the insertion of the password must be started or the command again.

Enter in programming mode

When pressing the *Enter* key on the initial screen, the message *Prog. password* will be displayed, indicating that the alarm center is waiting for the entry of the master password or the installer password.

Enter in programming mode with the installer password



Enter in programming mode with the master password

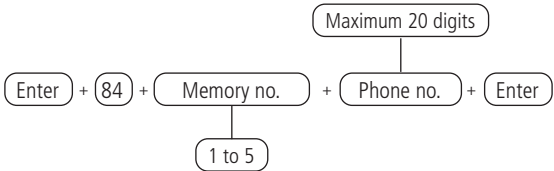


After entering the password, the *P* icon on the display will be lit, indicating that the alarm center is in programming mode.

- Obs.:** » If you want to cancel typing a sequence before finishing, keep the Back key pressed until you receive the confirmation beep or press the Exit key and restart typing from the beginning of the sequence indicated in the manual.
- » To cancel entering a password, press the Exit key or press and hold the Back key for three seconds.
 - » To exit programming mode, type the master password or the installer password (same password used to access programming mode).
 - » If the keyboard is not operated for three minutes, the alarm center will exit the programming mode and when accessed, the keyboard will be directed to the initial screen.
 - » There is no need to exit programming mode to execute the next command allowed by the password.

Direct editing/programming command

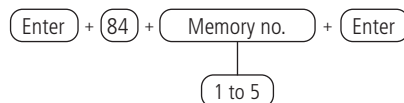
In programming mode, the command will be entered by directly typing its entire extension and at the end pressing *Enter* key to save the command and proceed to another one, as for example:



Obs.: some commands can be entered both by direct editing/programming mode or by editing/programming mode with visualization.

Editing/Programming command with visualization

In programming mode, some commands can be entered in parts, so the first part of the command will be entered first and shown on the first line of the display and the value to be edited/viewed will be shown on the second line of the display. If the alarm center memory referring to the typed command is empty, the second line will be erased. To edit, for example, the telephone number using the LCD keyboard, place the cursor in the desired position using the keyboard arrows and type the telephone number, then press *Enter* key to save the command and proceed to another one.



If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: some commands can be entered both by direct editing/programming mode or by editing/programming mode with visualization.

Bit editing command

In programming mode, some commands are entered with a special editing mode, which simplifies data entry and allows you to view the current programming.

On the XAT 8000 keyboard, numbers from 1 to 10 will be displayed according to the function on the display, representing the respective keys. Below each number there will be a square indicating the status of the function: filled marker (■ enabled function) or empty marker (□ disabled function). To enable/disable the function, press the corresponding key on the keyboard. After the configuration is finished, press *Enter* key to save this command and proceed to another command.

If the *Back* key or any invalid key is pressed, the changes will be discarded, the keypad will exit edit mode, and wait for the next programming sequence.

If you only want to view the configuration, press the *Back* or *Exit* and no programming will be changed

Cancel the typing of a command

If you want to undo typing a command or its contents before finishing, press the *Back* key or the *Exit* key.

Erase a digit or cancel the typing of a password

Press the *Back* key and the digit before the cursor will be deleted. To delete the entire sequence, press the *Exit* key or press and hold the *Back* key for 3 seconds.

Insert a pause between digits

Press the *Down Arrow* key on the XAT 8000.

Insert characters

Attention: it is not allowed to insert letters with an accent and some characters are available from version 0.28 of the keyboard.

Press the key corresponding to the desired letter or character. The following table demonstrates the available options.

Table of characters
Correspondence of the alphanumeric keyboard keys

0	Espaço	=	-	+	0	\	_	0
1	.	:	;	,	@	'	1	
2	a	b	c	2				
3	d	e	f	3				
4	g	h	i	4				
5	j	k	l	5				
6	m	n	o	6				
7	p	q	r	s	7			
8	t	u	v	8				
9	w	x	y	z	9			
Activates	*	!	"	#	\$	%	&	
Panic	()	/	<>	?	^			
Partial	[]	'	[]		~			

Using the AMT Remote Mobile application (for mobile devices)

Through the application installed on a mobile device (smartphone/tablet – Android®/iOS) it is possible to access the programming menu of the alarm center, provided that the password used for access has permission to change the programming. It is necessary that the alarm center is connected to the internet via Ethernet connection, GPRS/GSM (XG 2G, XG 3G or XG 4G module added to the alarm center is required) or Wi-Fi provisioning enabled (function available for AMT 8000 PRO).

For more information about the AMT Remote Mobile application, access the link <http://www.intelbras.com>.

Obs.: it is necessary for the computer/remote access password to be enabled, see section 6.10. Passwords.

Using the programmer for computers

Through the software installed on a computer (Windows® system) it is possible to access the alarm center's programming menu, as long as the password used for access is registered. It is necessary that the alarm center is connected to the internet via Ethernet connection, GPRS/GSM (XG 2G, XG 3G or XG 4G module added to the alarm center is required) or Wi-Fi provisioning enabled (function available for AMT 8000 PRO).

Obs.: it is necessary for the computer/remote access password to be enabled, see section 6.10. Passwords.

It is necessary that the alarm center is connected to the internet via Ethernet connection, GPRS/GSM (XG 2G, XG 3G or XG 4G module added to the alarm center is required) or Wi-Fi provisioning is enabled (function available for AMT 8000 PRO).

Using the Intelbras Guardian application (for mobile devices)

Through the application installed on a mobile device (smartphone/tablet – Android®/iOS) it is possible to access the alarm center to activate and deactivate it, check the status of sensors/zones, send emergencies, among other functions. Through the application current events from the alarm center will be received, such as activations, triggers and other occurrences. For access it is necessary for the master password or any secondary password to be placed, taking into account that the permissions in the application will be the same as what the password has defined in the other accesses. It is necessary that the alarm center is connected to the internet via Ethernet or GPRS/GSM connection (XG 2G or XG 3G module added to the alarm center is required).

Provisioning

To enable provisioning mode, type:

(Enter) + (855) + (Enter)

The LED will blink quickly to indicate that the alarm center is in provisioning mode and this mode will remain for 1 minute, if access to the alarm center is not performed, it will cancel the provisioning and will return to normal operation, if there is a connection with the alarm center it will remain in the provisioning mode until the remote connection is concluded by the user. If you want to cancel the keyboard provisioning mode, press the *Exit* key.

6.4. Wireless devices (register/delete)

Attention!

If during the wireless device registration process the LED of the device flashes red, press the synchronization button of the device for 15 seconds (for the XAC 8000, keep the top 2 buttons pressed) and restart the registration process.

The AMT 8000 LITE and AMT 8000 PRO alarm centers already have an integrated wireless receiver for signal reception and transmission to sensors, keyboards and other devices.

The following table shows how many and which wireless devices can be registered in the alarm center.

Types of devices		Maximum number of devices	Addresses
Keyboards	XAT 8000	16	1 to 16
Controls	XAC 8000	98	00 to 97
	XAS 8000		
	IVP 8000 EX		
	IVP 8000 Pet		
Sensors	TX 8000	64	1 to 64
Sensor with photocheck	IVP 8000 Pet Cam	8	1 to 64
Sirens	XSS 8000	16	1 to 16
Range RF amplifier	REP 8000	4	1 to 04
Wireless actuator	PGM 8000	16	1 to 16

To facilitate the registration of devices, it is recommended that before their physical installation, the following steps are checked:

- » Check whether all devices have the battery correctly installed.
- » Leave the wireless devices close to the alarm center to carry out the correct registration and verify the correct addressing.
- » Carry out the registration of the keyboards first, to allow them to be used for registration of the other devices via programming.
- » The use of a maximum of 8 sensors with IVP 8000 Pet CAM photocheck per alarm center is recommended, however their registration can occur throughout the exclusive addressing range for sensors (01 to 64).

The mentioned wireless devices can be registered in two ways, the first using the synchronization key on the alarm center and the other through programming mode using the XAT 8000 keyboard, as described below.

Wireless device registration using the control unit's synchronization button

Press and release the alarm center synchronization key, LED 3 will light up continuously, indicating that the center is ready to register wireless devices. When completing the registration of all devices, press the alarm center synchronization button again and check that LED 3 has left Continuous mode (flashes indicating normal operation), showing that the control center has exited wireless device registration mode .

With the function active on the control panel, press the synchronization button for each device (if in doubt, consult the manual of the device to be registered), synchronization will be sequential, respecting the maximum limit of each device. For remote control, simply press any of its keys.

Maximum device capacity

- » 16 Wireless Keyboards
- » Remote controls 98
- » 64 wireless sensors
- » 16 wireless sirens
- » Wireless Actuator 16
- » RF Repeater 04

Attention: if it is not possible to register the device in the alarm center, reset it by pressing the synchronization button for approximately 10 seconds until the device's indicator LED flashes red twice, this process guarantees that the device will not be linked to any other system, the keyboard will display the message Keyboard unregistered and then the message Register keyboard, indicating that it can now be registered again. For more information, consult the user manual for each device.

Registration by keyboard command

The registration of devices by keyboard commands directs them to the desired addresses, respecting the maximum limit of devices per type.

It is necessary that the registration of the first keyboard is done through the control panel key (see section *Registration of wireless device by the synchronization button of the alarm center*).

» Change system language

Enter + 854 + 1 + Enter

- » 1 = 0: Portuguese
- » 1 = 1: Spanish
- » 1 = 2: English

Obs.: functionality available from version 1.0.1 of the XAT 8000 keyboard.

- » **Keyboards (addresses 01 to 16):** with the keypad to be registered next to the control panel, enter the following code and press the synchronization key on its back. Keyboard addressing will take place according to the inserted command, respecting the maximum limit of 16 devices of this type and after registering all of them, being added to the common partition. To change the partition of the keyboards, see section *Keyboard partition*.

To register wireless keyboards, type:

1 to 16
Enter + 620 + Keyboard no. + Enter + Activate wireless device

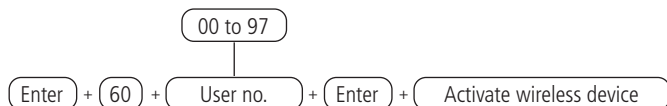
To erase wireless keyboards, type:

1 to 16
Enter + 720 + Keyboard no. + Enter

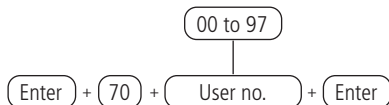
Obs.: after registering the keyboard, it will go into the process of updating messages, which takes approximately 50 seconds per keyboard and occurs on one keyboard at a time. If the process of updating the messages is interrupted, the keyboard will update them again as soon as it is opened again. In this case, it must remain open until the update has concluded.

- » **Remote controls (addresses 00 to 97):** with the control to be registered in hand, enter the code below on the keyboard and press any of its keys. The control addressing takes place according to the command entered, respecting the maximum limit of 97 devices.

To register remote controls, type:



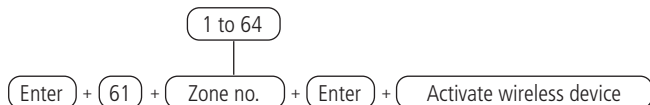
To erase remote controls, type:



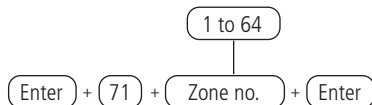
- » **Wireless sensors (addresses 01 to 64):** with the sensor to be registered in hand, enter the following code on the keyboard and press the synchronization button (if in doubt, consult the manual of the device to be registered). The sensor will be addressed according to the command entered, respecting the maximum limit of 64 devices.

Note: after pressing the sensor synchronization key, check whether the LED will flash green, indicating successful registration. If the LED flashes red, there has been an error and the process must be repeated.

To register wireless sensors, type:



To erase wireless sensors, type:

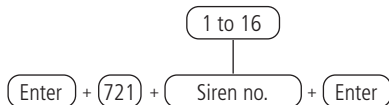


- » **Wireless sirens (addresses 01 to 16):** follows the same principle as the other devices. When necessary press the synchronization key on the back of the siren (remove the base for fixing on surfaces), after entering the code below, check if the LED will flash green, indicating success in the registration. If the LED flashes red, there has been a failure and the process must be repeated. Siren addressing will take place according to the command performed, respecting the maximum limit of 16 devices of this type and after registration, all will be added to the common partition. To change the partition of the sirens, see section *Siren partition*.

To register wireless sirens, type:



To erase wireless sirens, type:



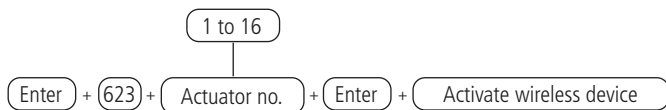
Attention: the integrated siren leaves the factory enabled and occupies position 00 of the alarm center and cannot be enabled/disabled by the registration and exclusion command of the wireless sirens. To disable/enable the integrated siren, refer to the topic *Enable/Disable Integrated Siren*.

- » **Wireless actuator (PGM addresses 01 to 16):** follows the same principle as the other devices. When necessary press the synchronization key on the back of the actuator (remove the base for fixing on surfaces), after entering the code below, check if the LED will flash green, indicating success in the registration. If the LED flashes red, there has been

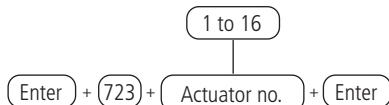
a failure and the process must be repeated. Actuator addressing will take place according to the command performed, respecting the maximum limit of 16 devices of this type and after registration, all will be added to the common partition. To change the partition of the actuators, refer to the section *PGM Partition*.

Obs.: so that the actuator activates the Relay, it must be supplied with a power of 12 to 24 Vdc or it must be connected in the 110/220 Vac AC network.

» To register wireless actuators, type:

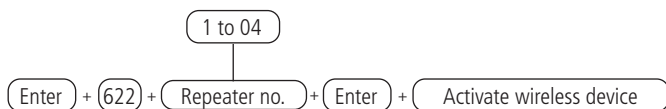


» To erase wireless actuators, type:

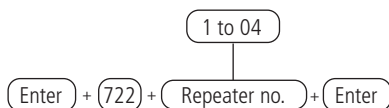


» **Range RF amplifier (repeater REP addresses 01 to 04):** follows the same principle as the other devices. When necessary press the synchronization key on the back of the repeater (remove the base for fixing on surfaces and turn on its power supply, for it to be started, the power supply must be turned on), after entering the code below, check if the LED will flash green, indicating success in the registration. If the LED flashes red, there has been a failure and the process must be repeated. The repeater addressing will take place according to the command performed, respecting its maximum limit of 4 devices.

To register the wireless repeater, type:



To erase the wireless repeater, type:



Change of route of the devices between the alarm center and the repeater

For a device to pass through the RF amplifier (Repeater REP 8000) it is necessary that the signal level of the repeater -> device be higher than the central signal level -> device. Otherwise, it will communicate directly with the alarm center without going through the repeater.

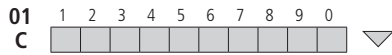
To check the signal intensity of the devices on the 8000 line, press the device synchronization key, where the LED indicator will show its status, and if the LED lights up in green, the signal is excellent, in orange the signal is intermittent the weak and red there is no communication (only for the XAT 8000 keyboard the status will be shown through a message on its own display).

Whenever you want to pass a device through a certain repeater, turn off the others to ensure that the device will pass through the route of the desired repeater, after the configuration you can turn on all the repeaters, this prevents the device from entering a route that does not this is what you want, if this happens, simply repeat the route change process.

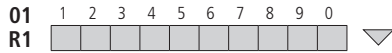
Route change by restarting devices

Remove the power supply from the device so that your communication passes through the repeater and after 3 seconds turn it on again (replace it), for the control it is not necessary to remove the battery, however, you must press the two first keys (open lock and closed lock) simultaneously and release. After the initialization time of the device (varies from 0 to 60 seconds depending on the type) start with your new route, to verify if the change of route has been carried out successfully, press the synchronization key and the keyboard will show the redirection of the devices , if the route has not been changed, repeat the battery extraction process. Another way to check the route of the device is through the option of signal level of the visualization devices in the menu of the keyboard. If the device is in direct communication with the alarm center, the position of the device plus the letter C will be shown, if the device is passing through the repeater, its position will be shown plus the letter R followed by the position of the repeater.

Ex.: sensor 01 communicating directly with the alarm center.



Ex.: sensor 01 communicating with repeater 01:



Route change by command

Attention: all devices, including the REP 8000 repeater, must be in version 2.0.0 or higher. For devices with a lower version, the route change prevails by restarting the devices.

Allows you to change the route using a keyboard command, so that the device searches for a new route, just access the programming mode with the installer password and execute the command for the device that will be described below.

Search for a new sensor route

Enter + 544 + ZZ + Enter

ZZ = 2 digit zone number

After executing the command, it is necessary to force a transmission from the device.

To force a transmission from the sensors, just press the synchronization button, but ideally, the sensor transmits without touching your hands so that there is no interference when looking for a new route search. To do this, just leave the sensor installed in its already defined location and generate a detection for the IVP's or an opening/closing of the XAS and TX. If the device has not changed the route, repeat the command and generate a new transmission from the device.

Search for a new Keyboard route

Enter + 545 + TT + Enter

TT = 2 digit keyboard number

After executing the command, it is necessary to force a transmission from the device.

Force a transmission from the keyboards press any of its key or press its synchronization button. If the device has not changed the route, repeat the command and generate a new transmission from the device.

Search for a new Siren route

Enter + 546 + SS + Enter

SS = 2 digit siren number

After executing the command wait for a new siren transmission that takes place every 4 seconds, if the device has not changed the route, repeat the command.

Search for a new PGM route

Enter + 547 + PP + Enter

PP = 2 digit PGM number

After executing the command, generate an activation of the PGM or press its synchronization button. To avoid interference when searching for a new route, press the PGM synchronization button and position it in the defined location and then execute the command for a new search, because when pressing the PGM synchronization button it will transmit to the alarm center every 3 seconds during the next initial 15 minutes.

Automatic route change of devices between the AMT 8000 LITE and AMT 8000 PRO Alarm centers with the REP 8000

Attention: all devices, including the REP 8000 repeater, must be in version 2.0.0 or higher. For devices with a lower version, the route change prevails by restarting the devices.

The devices automatic route change is a feature of the AMT 8000 LITE and AMT 8000 PRO alarm centers that allows the devices to search for a new route if there is no communication with the alarm center or with the repeater for 30 minutes if the device is already is communicating through a repeater. The remote control will always look for the best route.

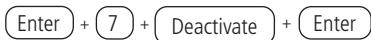
Example: if a sensor that is communicating directly with the alarm center is without communication for 30 minutes, the sensor starts a new route search, and when receiving the first response, either from the alarm center itself or from one of the 4 repeaters, the device starts to follow that route forever or until it goes another 30 minutes without communication on that new route. Route change can occur every 30 minutes as mentioned above. This process is repeated three times, that is, if the sensor is without communication with the alarm center for 30 minutes, it starts a new route search, if it does not find it, it will try a new route after 30 minutes and this process is repeated for 3 times, and if in three attempts the device does not get a new route it remains on the route it was on until it is restarted. Remembering that every 5 minutes the devices make a keep alive transmission and can restore communication on its initial route as long as it has been repositioned in a suitable place.

Attention: when starting a new route search, the device enters the route that responds first, this may cause it to enter a route with a lower signal than the other routes in the system.

Reset wireless devices

It will erase all registered wireless devices, including the keyboard used to perform the command. If you want to register again a device after the reset, you will need to physically delete it using the synchronization key and only after confirming its deletion, by indicating the LED, will it be possible to register again.

To erase all wireless devices, type:

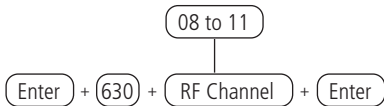


Obs.: if the Reset blocking is activated, it will not be possible to execute this function (see the section Blocks).

RF channel change

The AMT 8000 LITE and AMT 8000 PRO alarm centers have 4 RF communication channels, operating in the frequencies from 915 to 928 MHz and the channel used can be changed, if there are other devices using this same frequency in the location where the alarm centers are already located. thus causing interference.

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Attention: when changing the alarm center channel, all devices registered to it must have the synchronization key pressed to direct the device to the new channel, for control it is necessary to press the first two keys (lock opened and lock closed) simultaneously and release, otherwise they will not communicate with the alarm center.

6.5. Wireless sensor functions

Wireless sensor test

This function will test the sensors, and after entering the following command, when the sensors are activated, the sirens added to the partition in which the sensors are configured or siren 01 or the one with the lowest registered value, in the case of non-partitioned systems, will fire, indicating that the sensor is operating correctly.

To program this function, type:



For opening type sensors, the siren will be activated when the sensor opens and closes and for infrared type sensors, it will be activated at each activation, while the command is active.

To close the wireless sensor testing mode, press the *Exit* key, enter another programming sequence, or then enter the programmer password to exit the programming mode.

Zone tamper detection

To program this function, type:

Command to disable the tamper of the sensors:

(Enter) + (78) + (X) + (Enter)

X = Group zones 0 to 6

Command to disable the digital tamper of IVP 8000 EX

(Enter) + (79) + (X) + (Enter)

X = Group zones 0 to 6

Obs.: function available from version 2.0.0 of the sensor.

Restoration of the digital tamper of IVP 8000 EX sensor

(Enter) + (543) + (ZZ) + (Enter)

ZZ = 2 digit zone number

Obs.: function available from version 2.0.0 of the sensor.

Sensor firmware check

(Enter) + (641) + (ZZ) + (Enter)

ZZ = 2 digit zone number

Keyboard firmware check

(Enter) + (642) + (TT) + (Enter)

TT = 2 digit keyboard number

Siren firmware check

(Enter) + (643) + (SS) + (Enter)

SS = 2 digit siren number

Repeater firmware check

(Enter) + (644) + (RR) + (Enter)

RR = 2 digit repeater number

Remote control firmware check

(Enter) + (645) + (CC) + (Enter)

CC = 2 digit remote control number

PGM 8000 actuator firmware check

(Enter) + (646) + (PP) + (Enter)

PP = 2 digit PGM number

Obs.: function available for the devices starting from version 2.0.0. For devices with a version lower than 2.0.0, 0.0.0 will be displayed.

Device address identification

To identify in which position the device is registered in the alarm center, it is necessary that at least 1 XAT 8000 keyboard has been registered to the system with the display turned on.

To perform the address identification test, press and release the desired device's sync button and wait for the 2 keypad confirmation beeps. Soon after, a message will be displayed with the position of the device and also the partition, which it belongs to in case of partitioned systems.

Test example with non-partitioned alarm center sensor 01:

- » **1 display line:** The message P00 Located will be displayed
- » **2 display line:** The message Sensor 01 will be displayed

Obs.: for a partitioned system, P00 will be displayed for the common partition or P01 to P16 according to the partition the device belongs to.

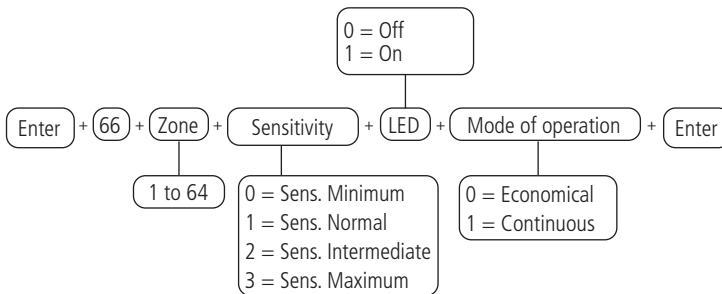
Adjustment of wireless infrared sensors

Attention: settings available for devices with firmware version lower than 3.0.0. For equal or higher versions consult the device manual for more information.

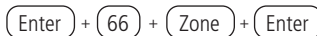
Registered wireless infrared sensors can be customized to operate in the best way, as described below:

- » **Sensitivity:** it will adjust so that the sensor detects correctly, according to the installation area, having the adjustment of 4 types of sensitivity, ranging from minimum, normal, intermediate and maximum (factory default sensitivity 2 = Intermediate Sens.). Although programming is allowed in the alarm center, it is not possible to change the sensitivity of the XAS 8000 and TX 8000 sensors.
- » **LED:** will define whether the transmission/detection LED of the sensor will turn on or remain off when any movement is detected (factory default *off*, only on during the first 15 minutes after battery insertion).
- » **Operation mode:** it will define how the sensor will detect movements, and in the case of operation in *Cost-saving* mode the sensor detects and once the sensor has triggered, it is necessary to wait a time of two minutes without movement for it to detect again. When in *Continuous* mode, the sensor detects continuously, as in wired sensors, that is, the sensor will trigger every time it detects movement, without waiting any time (factory default *cost-saving*). Although programming is allowed in the alarm center, it is not possible to change the *operating mode* of the XAS 8000 and TX 8000 sensors.

To program these sensor functions, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

For the *Sensitivity Programming*, *LED* and *sensor operation* to be effective, it is necessary that the sensor tamper activation, a trigger or a quick activation of the synchronization button of this sensor takes place.

6.6. Remote control key functions

The XAC 8000 control buttons leave the factory with the following functions:

- » **Button 1:** assemble (function 02).
- » **Button 2:** disassemble (function 03).
- » **Button 3:** disable (function 00).

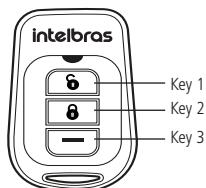
With the command and the indicative table below, it is possible to change the function of each of the keys on the remote control.

Obs.: some functions listed below are also associated with specific permissions such as password permissions.

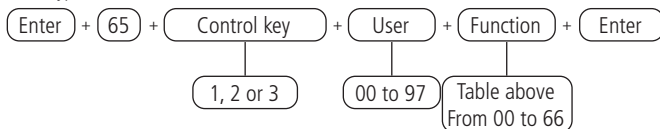
Use the following table to fill in the *Function* field to define functions for the remote control keys.

00	Disabled
01	Activate / Deactivate all partitions
02	Activate only all partitions
03	Deactivate only all partitions
04	Activate / Deactivate all partitions in <i>Partial</i> mode
05	Only assemble in <i>Partial</i> mode
06	Panic with siren
07	Silent panic
08	Fire panic
09	Medical emergency
10	N/A
11	Activate / Deactivate Partition 1 only
12	Activate / Deactivate Partition 2 only
13	Activate / Deactivate Partition 3 only
14	Activate / Deactivate Partition 4 only
15	Activate / Deactivate Partition 5 only
16	Activate / Deactivate Partition 6 only
17	Activate / Deactivate Partition 7 only
18	Activate / Deactivate Partition 8 only
19	Activate / Deactivate Partition 9 only
20	Activate / Deactivate Partition 10 only
21	Activate / Deactivate Partition 11 only
22	Activate / Deactivate Partition 12 only
23	Activate / Deactivate Partition 13 only
24	Activate / Deactivate Partition 14 only
25	Activate / Deactivate Partition 15 only
26	Activate / Deactivate Partition 16 only
27	N/A
28	N/A
29	N/A
30	N/A
31	Activate / Deactivate Partial mode Partition 1 only
32	Activate / Deactivate Partial mode Partition 2 only
33	Activate / Deactivate Partial mode Partition 3 only
34	Activate / Deactivate Partial mode Partition 4 only
35	Activate / Deactivate Partial mode Partition 5 only
36	Activate / Deactivate Partial mode Partition 6 only
37	Activate / Deactivate Partial mode Partition 7 only
38	Activate / Deactivate Partial mode Partition 8 only
39	Activate / Deactivate Partial mode Partition 9 only
40	Activate / Deactivate Partial mode Partition 10 only
41	Activate / Deactivate Partial mode Partition 11 only
42	Activate / Deactivate Partial mode Partition 12 only
43	Activate / Deactivate Partial mode Partition 13 only
44	Activate / Deactivate Partial mode Partition 14 only
45	Activate / Deactivate Partial mode Partition 15 only
46	Activate / Deactivate Partial mode Partition 16 only
51	PGM 01
52	PGM 02
53	PGM 03
54	PGM 04
55	PGM 05
56	PGM 06
57	PGM 07
58	PGM 08
59	PGM 09
60	PGM 10

61	PGM 11
62	PGM 12
63	PGM 13
64	PGM 14
65	PGM 15
66	PGM 16



To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

6.7. Wireless keyboard functions

Keyboard partition

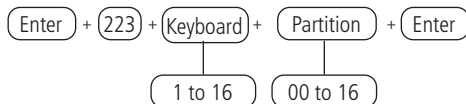
In factory default the keyboards can operate and view the status of all partitions. Through the following command it is possible to program the keyboard to operate only a specific partition.

When the keyboard is programmed for a specific partition, it will only be possible to view the status and operate the selected partition, therefore, if a password for another partition is entered or that has permission for more than one partition, the message *Keyboard error without permission* will be displayed.

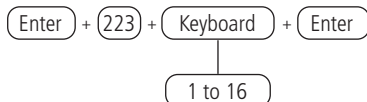
To activate the switch partition on which a keyboard is allowed using the master password or a password with permission for more than one partition, including the keyboard partition in question, simply enter the password or use the sequence *Activate + Partition + Password*.

It is possible to program/associate a keyboard (01 to 16) to one of the partitions (01 to 16), as described below.

To program this function, type:



To edit/view the programmed value, type:



After entering the command, define which partition the XAT 8000 wireless keyboard will belong to, being the address 00 for common keyboard and 01 to 16 for a specific partition and press *Enter* key to confirm. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: » All keyboards leave the factory programmed for common partition 00.

- » Even though the keyboard is partitioned, specific passwords are required to perform partition functions through it.
- » A keyboard can be registered in a single partition or be common to all, but a partition can have more than one keyboard (keyboards 01 to 16).

Ex.: Keyboards 01 and 02 can be registered in partition 01 and keyboards 03 and 04 in partition 02. What cannot be registered is keyboard 01 in partition 01 and then register this same keyboard 01 in partition 02, because if it is done so keyboard 01 will only belong to partition 02.

Editing XAT 8000 Keyboard Messages

Through this function it is possible to customize the name of the zones, users and wireless devices added to the alarm center. When an event occurs, the first line of the display will show predefined messages, indicating the event and the second line will show the programmed name (up to 14 digits).

The predefined messages are as follows:

Function	Description
Activation	Alarm center was activated
Deactivation	Alarm center was deactivated
Trigger	Trigger. The second line will indicate which zone
24-Hour trigger	24-Hour zone trigger The second line will indicate which zone
Panic	Trigger due to panic The second line will indicate which zone
Medical emergency	Trigger due to medical emergency The second line will indicate which zone
Fire	Trigger in fire zone The second line indicates which zone
Zone / sensor tamper	Tamper opening detected The second line will indicate which zone
Low battery	Wireless device with weak battery
Tamper devices	Violation of devices. The second line will indicate the device

Change messages

To edit / view the programmed messages use the table below as support to carry out the command:



Description	Message group	User, device or zone
Alarm center name	1	00
Users	2	00 to 99
Zones	3	1 to 64
Partitions	4	1 to 16
PGM	5	01 to 16
Keyboards	6	1 to 16
Sirens	8	1 to 16

After entering the command, the first line of the display will show the typed sequence and the second the previously programmed message. To edit the message, place the cursor in the desired position, use the keyboard arrows and successively press the desired key until the letter, character or number appears on the display.

To erase a digit, press the *Back* key and to cancel the operation, keep the *Back* key pressed for 3 seconds or press the *Exit* key.

To confirm the message change, press the *Enter* key.

Reset of messages

To return all programmed messages for display, type:



Obs.: returns all messages from the alarm center to the factory default according to the selected language.

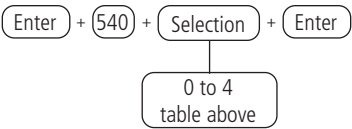
Panic Key

If the *Panic* key is pressed for 3 seconds, the siren will sound and the Audible Panic event will be reported to the monitoring company.

This key can assume the following configurations:

Function	Selection
Disabled	0
Audible panic	1
Silent panic	2
Fire panic	3
Medical emergency	4

To program this function, type:



To edit/view the programmed value, type:



After entering the command, define which function the *Panic* key will have, being the selection 0 as disabled, 1 as *Audible panic* (factory default), 2 as silent panic, 3 as fire panic and 4 as medical emergency and press the *Enter* key to confirm. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

6.8. Siren functions

Integrated siren

The alarm center has an integrated wired siren and this siren has a sound dispersion function to make it difficult to locate in case of a trigger. The integrated siren will always be common and the assembly and disassembly beep will always be emitted by it, the triggers that occur will be signaled both by the integrated siren and by the wireless sirens that are registered in the alarm center.

Enable/disable integrated siren



Use key 1 on the keyboard to enable the alarm center siren, so that the number 1 remains marked to enable and unmarked to disable the integrated siren, confirm with the *Enter* key. If you only want to view the configuration, press the *Back or Exit* key and no programming will be changed.

Enable/disable the integrated siren beep in the activation/deactivation of the system (function available from version 3.0.6)

As of version 3.0.6, it is possible to enable/disable the arm and disarm beep of the integrated siren. With this function activated, the beep will be emitted exclusively by the silent siren. For more details, see the topic *Enable the siren beep on activation/deactivation of the system*.

Note: *only the arming and disarming beep will be disabled in the integrated siren. In case of shots or emergencies, it will continue to function normally.*

To program this function, enter:



Use key 2 on the keyboard to enable/disable the function, so that the number 2 remains marked to disable and unchecked to enable the arm and disarm beep of the integrated siren, confirm with the *Enter* key. If you wish to only view the configuration, press the *Back/Exit* key otherwise the programming will be altered.

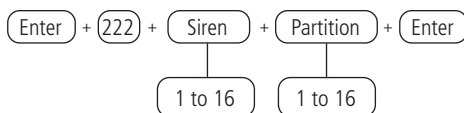
Starting with version 3.2.4, it is possible to adjust the volume of the integrated siren in 3 levels. When this function is enabled, the integrated siren will follow the volume already configured in the *Adjust beep on entry timing* field. To change the volume, see the *Adjust beep on entry timing* topic.

Enter + 541 + Enter

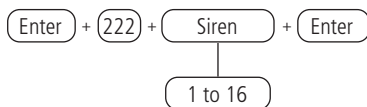
Wireless siren

Siren partition

To program this function, type:



To edit/view the programmed value, type:



After entering the command, define which partition the XSS 8000 siren will belong to, with address 00 being common (the siren will be triggered if an event is generated in any of the partitions) or from 01 to 16 (the siren will only be triggered if the partition it was defined for, generate some event) according to the desired partition and press the *Enter* key to confirm. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: a siren can be registered in a single partition or be common to all, however a partition can have more than one siren (sirens from 01 to 16).

Ex.: sirens 01 and 02 can be registered in partition 01 and sirens 03 and 04 in partition 02. What cannot be registered is siren 01 in partition 01 and then register this same siren 01 in partition 02, because if it is done this siren 01 will only belong to partition 02.

Enable the siren beep in system activation/deactivation

Activates / deactivates the beep emitted during activation / deactivation of the alarm center. During activation, the siren will emit 1 beep and during deactivation, the siren will emit 2 beeps. If a problem is detected and the *Siren problem indication* function is enabled, the siren will emit 1 long beep during activation and 2 long beeps during deactivation.

To program this function, type:



Use key 3 on the keyboard to enable the siren beep during system activation / deactivation, so that number 3 remains marked to enable and unmarked to disable the siren beep, then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

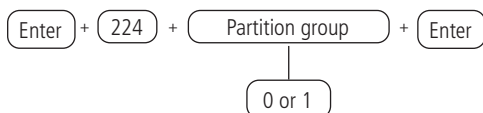
Obs.: » For partitioned or non-partitioned systems, only the integrated siren will be responsible for the activation/deactivation beep and follow the following behavior:

- » If the alarm center is not partitioned, only the integrated siren will beep on and off. If there are wireless sirens registered in the alarm center and the integrated siren is disabled from the system, the beep will be emitted by wireless siren 01 and if siren 01 is removed from the system, the beep will be emitted by siren 02 and so on.
- » The beep will only be emitted by the next siren if the previous siren is turned off or after the alarm center detects a supervisory fault.
- » If the alarm center is partitioned, when general activation/deactivation is performed or in more than one partition, the beep will be given on the integrated siren, or on the siren registered at the lowest value address (01) if the integrated siren is disabled.
- » If the system is partitioned, and only one partition with its own siren is activated, only that partition will emit the beep on activation/deactivation.
- » In the case of a partitioned system and with a siren without a partition defined for it, the beep will occur on the integrated siren, if the system does not have an integrated siren, there will be no activation/deactivation beep for this partition and no activation of the other sirens for this partition in case of triggers.

Enable the siren beep during activation/deactivation in a specific partition.

Selects which partitions the siren beep will be emitted during activation/deactivation of the alarm center when it is partitioned, customizing the siren registered for each partition. During activation, the siren will emit 1 beep and during deactivation, the siren will emit 2 beeps. If a problem is detected and the *Siren problem indication* function is enabled, the siren will emit 1 long beep during activation and 2 long beeps during deactivation.

To program this function, type:

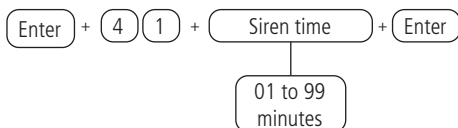


After entering the command, through the XAT 8000 keyboard, mark which partitions will have the siren beep activated, using the keyboard numbers to leave them marked referring to the partition. Select 0 for partition group from 1 to 10 and 1 for partitions from 11 to 16. After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back or Exit* key and no programming will be changed.

Siren time

The siren time leaves the factory programmed for 5 minutes. This is the time that the siren will be activated/sounding after a violation/intrusion occurs in an active partition/zone and can be changed to a time between 01 and 99 minutes.

To program this function, type:



Obs.: if 00 is programmed, an error beep will be emitted and the configuration will not be changed.

To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

PGM 8000 wireless actuator

The PGM outputs are programmable and can be used to activate devices such as: electric locks, spotlights, auxiliary sirens, buzzers or almost any device that uses electricity. The PGM output is activated whenever the programmed event occurs and can operate in the following modes:

- » **On/Off:** when the event occurs, the PGM will be turned on and will only be turned off when the event ceases.
- » **Pulsed:** when the programmed event occurs, the PGM will remain on for the programmed time from 1 to 8 seconds and then it will be turned off; regardless of whether the event has ceased or not.
- » **Timed:** when the scheduled event occurs, the PGM will remain on for the programmed time from 01 to 99 minutes and then it will be turned off; regardless of whether the event has ceased or not.

The events that can trigger the PGM outputs are:

Activation by applications:

- » **Non-partitioned alarm center:** PGMs can be controlled by application.
- » **Partitioned alarm center:** the PGMs can only be controlled if the App is accessed by the user with permission in the partition or with full permission. Even when programmed for other functions.

Activation by password (secondary passwords from 51 PGM01 to 66 PGM16):

- » **Non-partitioned alarm center:** in *On/off* mode, the corresponding PGM output will be turned on when the password is typed on the keyboard, and will only be turned off when the password is typed again. If it is in *Pulsed or Timed* mode, the PGM output will remain on for the programmed time whenever the password is typed, and can be deactivated by typing the password on the keyboard before the programmed time. If this function is disabled, the passwords will work as a common password, if enabled, the password will only work to trigger the PGM output.
- » **Partitioned alarm center:** the PGM will be triggered by the password regardless of whether it is linked to a partition or not.

Obs.: whenever the PGM is activated/deactivated by a password on the keyboard, it will issue two short confirmation beeps or will display the fault message *Actuator error not accessible* if the PGM activation/deactivation is not performed.

System activation:

- » **Non-partitioned alarm center:** activates the PGM output when the alarm center is activated.
- » **Partitioned alarm center:** activates the PGM output only with the activation of the partition to which the PGM belongs. If the PGM is common it will be activated with the activation of all partitions and deactivated with the deactivation of any partition.

System deactivation:

- » **Non-partitioned alarm center:** activates the PGM output when the alarm center is deactivated.
- » **Partitioned alarm center:** activates the PGM output only with the deactivation of the partition to which the PGM belongs. If the PGM is common, it will be activated with the deactivation of any of the partitions.

Medical emergency:

- » **Non-partitioned alarm center:** in case of medical emergency, the PGM will be turned on.
- » **Partitioned alarm center:** activates only the PGM output that belongs to the partition that generated the emergency. If the PGM is common, it will be activated with the emergency generated from any partition.

Event communication failure:

- » **Non-partitioned alarm center:** if there is a communication failure (in case the number of attempts to report events by the telephone is exceeded or communication with the monitoring software via IP is lost), the PGM output will be activated.
- » **Partitioned alarm center:** if there is a communication failure (in case the number of attempts to report events by the telephone is exceeded or communication with the monitoring software via IP is lost), the PGM output will be activated regardless of whether it is linked to a partition or not.

Telephone line cut (Function available only for AMT 8000 PRO):

- » **Non-partitioned alarm center:** if the telephone line is cut, the PGM output will be activated.
- » **Partitioned alarm center:** if the telephone line is cut, the PGM output will be activated regardless of whether it is linked to a partition or not.

Obs.: it is necessary that the telephone line cut sensor is activated.

Siren problem:

- » **Non-partitioned alarm center:** in the event of a problem with the wireless sirens, a supervisory fault will be generated and the PGM output will be activated.
- » **Partitioned alarm center:** in case of a problem with the wireless sirens, a supervisory fault will be generated and only the PGM output linked to the partition where the problem occurred will be activated. If the PGM is common, it will be activated with any siren supervision failure.

Obs.: the PGM will only be activated after a failure to supervise the wireless sirens.

Panic/Trigger (all panics and emergencies and all audible triggers):

- » **Non-partitioned alarm center:** turns on the PGM output when any type of emergency occurs, audible/silent panic or audible zone trigger.
- » **Partitioned alarm center:** turns on the PGM output when any type of emergency occurs, audible/silent panic or audible zone trigger referring to the partition to which the PGM belongs. If the PGM is common, it will be activated with the mentioned events from any of the partitions.

Silent trigger or panic (silent triggers and panics only):

- » **Non-partitioned alarm center:** turns on the PGM output when a Silent Trigger or Silent Panic occurs.
- » **Non-partitioned alarm center:** Turns on the PGM output when a silent trigger or silent panic occurs regarding the partition to which the PGM belongs. If the PGM is common, it will be activated with the silent panic activation or silent trigger from any partition.

Fire zone trigger:

- » **Non-partitioned alarm center:** in case of any fire event, the PGM will be turned on.
- » **Partitioned alarm center:** turns on the PGM output when any fire event occurs in the partition to which the PGM belongs. If the PGM is common, it will be activated with the fire event from any partition.
For example: it can activate a fire fighting system, activate a differentiated siren, activate emergency lights, etc.

Opening of zone 1:

- » **Non-partitioned alarm center:** whenever zone 1 is opened, the PGM will be turned on (for presence sensors, the PGM will be activated and deactivated whenever there is a detection and for opening sensors, the PGM will be activated on opening and deactivated on closing or after a time programmed if the sensor remains open).
- » **Partitioned alarm center:** whenever zone 1 is opened, the PGM will be turned on regardless of whether the PGM is linked to a partition or not.

Remote control (control registered in users from 51 PGM01 to 66 PGM16):

- » **Non-partitioned alarm center:** in *On/Off* mode, the corresponding PGM output will be turned on when the control is activated, and will only be turned off when the control is activated again. If it is in *Pulsed* or *Timed* mode, the PGM output will remain on for the programmed time whenever the control is activated and can be deactivated before ceasing the time by the control itself.
- » **Partitioned alarm center:** in this case, the operation will be the same as described for a non-partitioned alarm center, regardless of whether the user with which the control is registered has permission to partition or not. See item *Remote Control Key Functions*.

Obs.: whenever the PGM is activated/deactivated by the remote control, the LED will light up in green informing that the PGM has been activated or deactivated and in red in case of communication failure (non-activation/deactivation of the PGM).

Activation/deactivation by time:

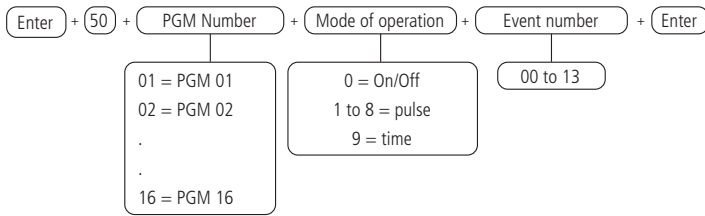
- » **Non-partitioned alarm center:** with this function, the PGM can be programmed for automatic activation and automatic deactivation for different days and times.
- » **Partitioned alarm center:** the PGM will be activated / deactivated at the scheduled time regardless of whether it is linked to a partition or not.

Open door actuation:

- » **Non-partitioned control panel:** activates the PGM output when the open door event is generated.
- » **Partitioned control panel:** activates only the PGM output that belongs to the partition that generated the open door event. If the PGM is common, it will be activated with the open door event of any partition.

Attention: for the PGM to be associated with a partition, refer to the topic *Association of the PGM 8000 actuator for a partition*.

To program the PGM function, type:



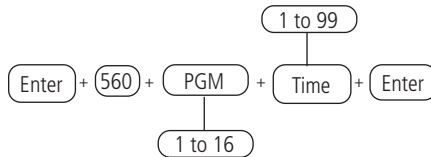
Event that activates the PGM:

00	External activation (applications)
01	Activation by password (passwords from 51 PGM01 to 66 PGM16)
02	System activation
03	System deactivation
04	Medical emergency:
05	Event communication failure
06	Telephone line cut (Function available only for AMT 8000 PRO)
07	Siren problem
08	Trigger
09	Silent trigger or panic
10	Fire zone trigger
11	Opening of zone 1
12	Remote control
13	Activation/deactivation by time
14	Open door actuation

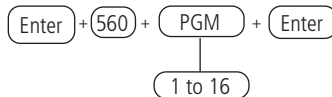
Scheduled time

Configure the time in minutes that the PGM will remain activated.

To program this function, type:



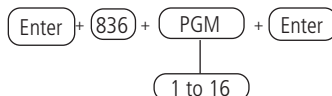
To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Days for Scheduled Automatic Activation of the PGMS

Select the days when Automatic Activation of the PGM will occur. Key 8 enables the function for programmed holidays.



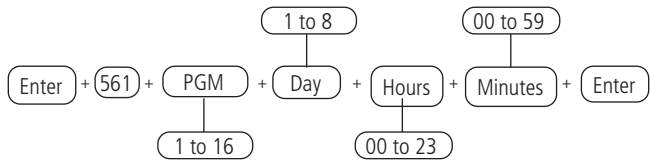
After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Use the keyboard keys to define the days for the automatic activation of the PGM to occur, so that the referring numbers, who wish to have the days enabled, remain marked and the days with the function disabled remain unmarked and then confirm with the *Enter* key.

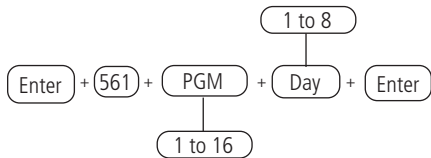
PGM automatic activation time

Selects the time that Automatic activation by partition will occur.

To program this function, type:

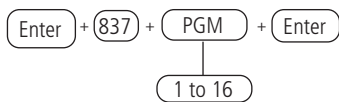


To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back* or *Exit* key and no programming will be changed

Days of the week for Scheduled Automatic Deactivation of the PGMS

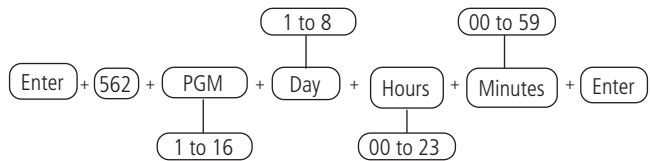


Use the keyboard keys to define the days for the automatic deactivation of the PGM to occur, so that the referring numbers, who wish to have the days enabled, remain marked and the days with the function disabled remain unmarked and then confirm with the *Enter* key.

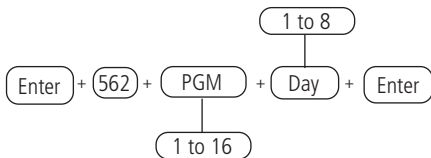
PGM automatic deactivation time

Selects the time that Automatic deactivation by partition will occur.

To program this function, type:



To edit/view the programmed value, type:



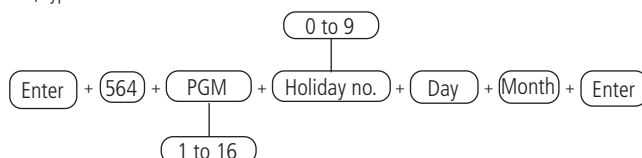
Holidays

The alarm center has 10 memories (0 to 9) to program dates that require a special time for Automatic activation and Automatic deactivation.

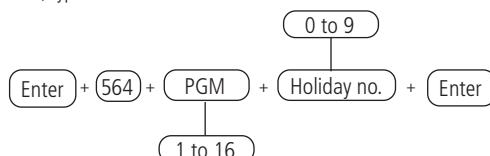
When the system date is the same as one of the programmed dates, the day of the week settings will be superimposed by the times programmed in the address of the commands described above, referring to the alarm center's automatic activation programming.

Define holidays for Automatic Activation / Automatic Deactivation

To program this function, type:



To edit/view the programmed value, type:



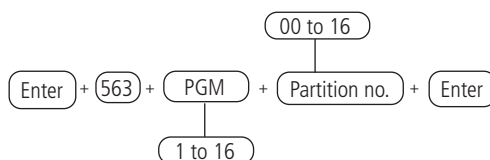
After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Obs.: to disable a holiday, program the date with the value 00 for Day and Month.

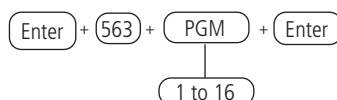
Association of the PGM 8000 actuator to the partition

With this function, it will be possible to associate the PGMS with the partitions of the alarm center, allowing a partition to have one or more PGMS (total of PGMS per alarm center - 16) and being able to be activated in different ways according to the operating mode configured for it.

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

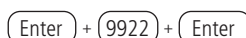
Obs.: a PGM can be registered in a single partition or be common to all, however a partition can have more than one PGM (PGM's from 01 to 16).

Ex.: PGM's 01 and 02 can be registered in partition 01 and PGM's 03 and 04 in partition 02. What cannot be registered is PGM 01 in partition 01 and then register that same PGM 01 in partition 02, because if it is done this, PGM 01 will only belong to partition 02.

6.9. Update

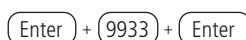
The AMT 8000 LITE and AMT 8000 PRO alarm panels have remote firmware updates, meaning that when new firmware versions are available, there is no need to use recorders or connect to computers. The panel simply needs to be connected to the Cloud via Ethernet to be updated. When the version is updated, the registration of wireless devices or saved settings will not be lost.

To download/verify a new version, type:



If there is a version for download, the information Download Wait will be displayed and it will start, which will take around 3 to 5 minutes. If the alarm center does not have a downloadable version, the display will show the *Alarm center is already updated*.

After the download time has elapsed, access the programming mode again and type:



The new version that was downloaded will be installed and records and alarm center settings will not be lost. To check the control panel firmware version, access *Menu* and with the directional keys access *Alarm center version* to be displayed.

Note: the control panels must be connected to the internet via Ethernet / Wi-Fi or 4G. Software download/update is not possible via GPRS 2G and 3G connection due to the connection's download speed and excessive consumption of the data package used.

Attention: 4G update (XG 4G module required) is available from version 3.2.4. The update process may take about 1 hour and will be completed automatically - after the download is complete, the control panel applies the update without any user intervention.

6.10. Passwords

Attention: » The control panel needs passwords to be operated/configured, and some passwords are created through the programming mode (secondary passwords, filtration) and the installer password has the factory default of 9090. In the case of the remote access password and the master password, to increase security, they are random passwords that are available on the QR Code label together with the MAC address of the alarm center.

» Before changing the installer password or the master password, make sure you have the new password well memorized or written down, because after exiting the programming mode, it will only be possible to access this mode again, through the new password. If the password is forgotten, see section 6.22. *System reset*.

Obs.: » For security reasons, do not reveal the master password to third parties.

- » If the master password is forgotten, perform the System Reset procedure with the installer password. This reset erases all alarm center settings except wireless devices and editable messages.
- » The alarm center cannot contain repeated passwords between users, including Master User, Installer and Remote Access and because of this, it does not allow programming repeated passwords.
- » If the alarm center is operating with a 4-digit password, no password can be equal to the first 4 digits of the remote access password.
- » » If the switchboard system is reset, it will no longer use the random passwords that are linked together with the QR Code label pasted inside the switchboard and will use password 1234 as the master password and password 878787 as access remote until they are changed again.

The alarm center has 96 secondary passwords and can be programmed for up to 16 partitions, that is, this would be similar to dividing the alarm center into 16 and commanding it through one or more keyboards or remote applications.

With the installer password, you have access to the programming mode and it is possible to change the installer password and the computer/remote access password, in addition to making the alarm center settings, but it is not allowed to activate and deactivate the alarm center, change the master password or secondary passwords.

Through the master password, it is possible to change the password itself, program and/or change the secondary passwords, activate or deactivate the entire alarm center or a specific partition.

Permissions of programming passwords

Password	Activation
Master (initially random, see QR Code label)	Create and delete secondary passwords
	Change master password
	Enable/disable permissions for secondary passwords
	Adjust date, time and day of the week
	Editing of XAT 8000 Keyboard Messages
Installer (default factory password: 9090)	Activate/deactivate the complete alarm center or partitioned (Partition 01 to 16)
	Perform all alarm center settings, except activate/deactivate the alarm center, change the master password and secondary passwords

Definition of passwords

Address	Password
00	Master password (initially random, see QR Code label)
01 to 96	Secondary passwords
	Users from 51 to 66 are PGM passwords. If there is no registered PGM, the passwords will have secondary user permission.
	User 51 PGM 01 user 52 PGM 02 and so on up to user 66 PGM 16.
97	Filtration password
98	Remote access computer password (initially random, see QR Code label)
99	Installer password (factory default 9090)

The secondary passwords plus the filtration password are divided into 9 groups, in accordance with the table below:

User group (GU)	Users from 1 to 10	User group (GU)	Users from 11 to 20	User group (GU)	Users from 21 to 30
0	Key 1 = user 1	1	Key 1 = user 11	2	Key 1 = user 21
	Key 2 = user 2		Key 2 = user 12		Key 2 = user 22
	Key 3 = user 3		Key 3 = user 13		Key 3 = user 23
	Key 4 = user 4		Key 4 = user 14		Key 4 = user 24
	Key 5 = user 5		Key 5 = user 15		Key 5 = user 25
	Key 6 = user 6		Key 6 = user 16		Key 6 = user 26
	Key 7 = user 7		Key 7 = user 17		Key 7 = user 27
	Key 8 = user 8		Key 8 = user 18		Key 8 = user 28
	Key 9 = user 9		Key 9 = user 19		Key 9 = user 29
	Key 0 = user 10		Key 0 = user 20		Key 0 = user 30
User group (GU)	Users from 31 to 40	User group (GU)	Users from 41 to 50	User group (GU)	Users from 51 to 60
3	Key 1 = user 31	4	Key 1 = user 41	5	Key 1 = user 51
	Key 2 = user 32		Key 2 = user 42		Key 2 = user 52
	Key 3 = user 33		Key 2 = user 43		Key 3 = user 53
	Key 4 = user 34		Key 4 = user 44		Key 4 = user 54
	Key 5 = user 35		Key 5 = user 45		Key 5 = user 55
	Key 6 = user 36		Key 6 = user 46		Key 6 = user 56
	Key 7 = user 37		Key 7 = user 47		Key 7 = user 57
	Key 8 = user 38		Key 8 = user 48		Key 8 = user 58
	Key 9 = user 39		Key 9 = user 49		Key 9 = user 59
	Key 0 = user 40		Key 0 = user 50		Key 0 = user 60
User group (GU)	Users from 61 to 70	User group (GU)	Users from 71 to 80	User group (GU)	Users from 81 to 90
6	Key 1 = user 61	7	Key 1 = user 71	8	Key 1 = user 81
	Key 2 = user 62		Key 2 = user 72		Key 2 = user 82
	Key 3 = user 63		Key 3 = user 73		Key 3 = user 83
	Key 4 = user 64		Key 4 = user 74		Key 4 = user 84
	Key 5 = user 65		Key 5 = user 75		Key 5 = user 85
	Key 6 = user 66		Key 6 = user 76		Key 6 = user 86
	Key 7 = user 67		Key 7 = user 77		Key 7 = user 87
	Key 8 = user 68		Key 8 = user 78		Key 8 = user 88
	Key 9 = user 69		Key 9 = user 79		Key 9 = user 89
	Key 0 = user 70		Key 0 = user 80		Key 0 = user 90
		User group (GU)	Users from 91 to 97		
		9	Key 1 = user 91		
			Key 2 = user 92		
			Key 3 = user 93		
			Key 4 = user 94		
			Key 5 = user 95		
			Key 6 = user 96		
			Key 7 = user 97		

Obs.: use the table above in the following programmings.

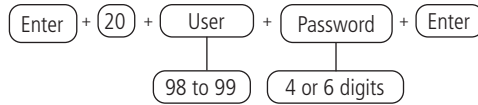
Programming of passwords using the installer password

Change the passwords using the installer password

With the installer password it is allowed to change only the installer password (User = 99) and that of the remote computer / access (User = 98). The password of user 98 always has 6 digits and does not depend on the configuration, now the password of user 99 can have 4 or 6 digits.

To use the 6-digit password, check the topic: *General configurations 1*.

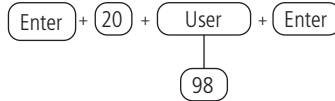
To program this function, type:



Erase the passwords using the installer password

The password of user 99 (installer) can only be changed and not erased. Now the password of user 98 can be erased.

To erase this password, type:



Programming of passwords using the master password

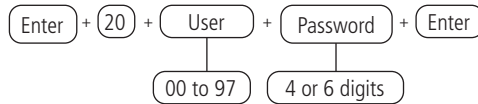
Change the passwords using the master password

With the master password it is possible to change the master password itself, register secondary passwords (master password - 00, secondary users - 01 to 96, duress password - 97).

Attention: users 51 to 66 are dedicated to the PGM, therefore these users will have the same permissions as the other secondary users, but if the PGM is registered in the alarm center and the PGM is configured to be activated by a password, the password will have exclusivity for PGM. EX.: User 51 PGM 01 user 52 PGM 02 and so on up to user 66 PGM 16.

To use the 6-digit password, check the topic *General configurations 1*, in this manual.

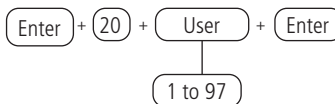
To program this function, type:



Erase the passwords using the master password

The password of master user - 00 can only be changed and not erased. Now the passwords of users 01 to 97 can be erased.

To program this function, type:



Permissions of passwords

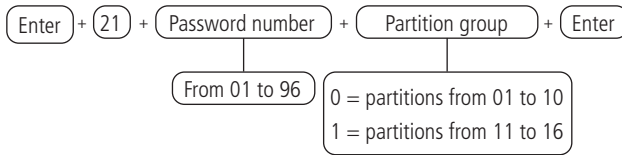
The secondary passwords that are created (01 to 96) will have permission to activate/deactivate the complete system and can be enabled to have the following accesses/permissions according to the needs of each installation.

- » **Partition:** passwords with this permission can only activate/deactivate partitions (01 to 16) previously selected via command.
- » **Activates only:** the selected passwords will be able to activate the system, but will not have permission to deactivate.
- » **Bypass:** initially, only the master password is allowed to perform temporary cancellation of zones (bypass), the passwords selected for this function will have permission to cancel zones at the time of system activation.
- » **Partial:** passwords with this function enabled can activate the control panel, leaving only the environment enabled where there are no zones that have been configured for *Partial* mode. Remembering that this function can be applied to both the partitioned and non-partitioned exchange.

These 4 permissions can be enabled simultaneously for any of the passwords 01 to 96, for example, the password of user 15 can have permission at the same time permission to only activate partition 01, activate in *Partial* mode and also to perform cancellation of partition 01 zones.

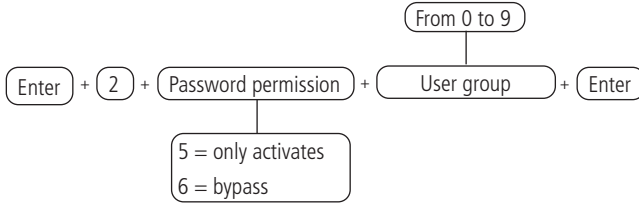
The commands to enable/disable the permissions described above are shown below:

Permission for partition



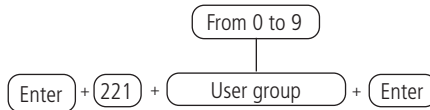
After entering the command, through the XAT 8000 keyboard, mark which partitions the password will have permission, using the keyboard numbers to leave marked referring to the partition. Select 0 for the group of partitions from 1 to 10 and 1 for partitions from 11 to 16. After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Permission to only activate or permission to bypass



Use the keys on the keyboard to enable the permissions to only activate and bypass for users from positions 01 to 96, so that the corresponding numbers that you want to have the function enabled remain marked on the display and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Permission for Partial mode



Use the keys on the keyboard to enable the permissions for partial mode for users from positions 01 to 96, so that the corresponding numbers that you want to have the function enabled remain marked on the display and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

6.11. Quick configurations for monitoring

This section briefly describes the processes for reporting of events to monitoring companies through telephone line channels, IP communication and GPRS connection.

For more details about these programmings, see section 6.16. Telephony and monitoring configurations.

Monitoring via phone line (only for AMT 8000 PRO model)

The alarm center can report events via telephone line channel (DTMF) - FXO 8000 module is required, for monitoring companies, for this reason the following commands must be programmed:

Obs.: the center only connects with 2.4 GHz routers (IEEE 802.11b/g/n, Wi-Fi compliant).

» Enter in programming mode with the installer password

Enter + Installer password (factory default: 9090)

» Program monitoring account

Enter + 15 + PP + Enter, where PP = partition from 01 to 16.

After the command, type the monitoring account number with 4 digits and press the *Enter* key to confirm.

» Program telephone number for the monitoring company

Enter + 10 + M + phone number of the monitoring company + Enter, where M = memory for telephone of 1 or 2

» Program the reporting mode as Regular IP

Enter + 17 + 4 0 0 + Enter

- » **Program the number of attempts for reporting an event in the factory default - up to 9 attempts**

Enter + 13 + T + Enter, where T = number of attempts from 1 to 9

- » **Program DTMF signal level**

If the factory standard DTMF level stored in the alarm center memory does not work, type the following command and test all options from 0 to 6 to check in which of them the best result is obtained.

Enter + 18 + Enter + N + Enter, where N = level from 01 to 6

- » **Exit from the programming mode with the installer password or then insert a new command**

Installer password (factory default: 9090).

Monitoring via Ethernet/Wi-Fi (Wi-Fi only for AMT 8000 PRO alarm center)

The alarm center can report events via IP communication to monitoring companies (Intelbras IP Receiver Software), for which the following commands must be programmed:

If you are using Wi-Fi connection before setting the monitoring options, program the following commands:

Obs.: the alarm center is connected only with 2.4 GHz routers.

- » **Enter in programming mode with the installer password**

Enter + Installer password (factory default: 9090)

- » **Insert name of the Wi-Fi network to be connected**

Enter + 850 + Enter + Insert name of the network + Enter

- » **Insert password of the Wi-Fi network to be connected**

Enter + 851 + Enter + Insert password of the network + Enter

- » **Enable Wi-Fi / define type of configuration of the network to be connected**

Enter + 852 + Enter + TP + Enter

- » **TP = type of configuration**

Selection	Type of configuration
0	Wi-Fi disabled
1	Wi-Fi enabled / in case of AC failure, operates on battery
2	Wi-Fi enabled / only with active AC network

Obs.: » After entering each command and confirming with the *Enter* key, two quick beeps should be heard, indicating that the programming was accepted, otherwise, there was an error.

» The network name and password must be entered exactly as it was defined in the router, considering uppercase and lowercase letters. To change between uppercase and lowercase, press the Deactivate key.

- » **Program monitoring account**

Enter + 15 + PP + Enter, where PP = partition from 01 to 16

After the command, type the monitoring account number with 4 digits and press the *Enter* key to confirm.

- » **Program the reporting mode.**

Enter + 17 + 4 + 0 + 0 + Enter

- » **Program communication priority (Ethernet only)**

Enter + 19 + 0 + Enter

- » **Program destination IP**

Enter + 801 + I + Enter, where I = 1 or 2 (destination IP 1 or destination IP 2)

After the command, type the IP number of the monitoring company (example: 192.168.001.100) and press the *Enter* key to confirm.

- » **Program IP network communication port**

Port 1 = *Enter + 802 + 1 + Port number with 4 digits + Enter*

Port 2 = *Enter + 802 + 2 + Port number with 4 digits + Enter*

- » **Program destination domain name (DNS)**

If you do not want to use DNS move to the next command, otherwise, type.

Enter + 803 + D + Enter, where D = 1 or 2 (DNS 1 or DNS 2)

After the command, type the DNS domain name and press the *Enter* to confirm.

» **Program monitoring options via IP**

Enter + 830 + Enter

After the command, using the keyboard keys, enable the desired option from 1 to 4, where:

- » **1:** enables the sending of events to the monitoring company 1.
- » **2:** enables the sending of events to the monitoring company 2.
- » **3:** enables the domain name (DNS) of the monitoring company 1.
- » **4:** enables the domain name (DNS) of monitoring company 2 and press the *Enter* key to confirm.

» **Program DHCP**

If you do not have a DHCP server or do not want to use this option, do not enable it and follow the next steps, where network mask, gateway, etc. will be added manually and not received from the connected network.

Enter + 831 + Enter

After the command, using the keyboard keys, enable option 1 (mark 1) and press the *Enter* key to confirm.

» **Program the network mask**

Enter + 8130 + Enter

After the command, type the network mask number and press the *Enter* key to confirm.

» **Program the gateway**

Enter + 8140 + Enter

After the command, type the gateway number and press the *Enter* key to confirm.

» **Program DNS servers for Ethernet**

Enter + 815 + S + Enter, where S = 1 or 2 (Server 1 or Server 2)

After the command, type the DNS1 server number and press the *Enter* key to confirm.

» **Program the Heartbeat Ethernet interval (link test)**

Enter + 816 + TTM + Enter, where TTM = time interval varying from 000 to 255 minutes (factory default:) 5 minutes)

» **Exit the programming mode with the installer password**

Installer password (factory default: 9090)

» **Check the connection to the IP Receiver service**

Press the *Menu* key, navigate through the arrow keys, access the *Connections* option and check if the mark for the *Eth* option: *IP1* and/or *IP2* is enabled. If yes, the alarm center is connected via Ethernet with the IP receiver software through the IPs that were enabled.

Monitoring by GPRS

The control panel can report events via 2G/3G/4G channel - an XG 2G/3G/4G module is required for monitoring companies. Sending events to monitoring companies will use the GPRS channel to send to IP addresses, as well as the Ethernet connection. The commands to be programmed are as follows:

Obs.: after entering each command and confirming with the *Enter* key, two quick beeps should be heard, indicating that the programming was accepted, otherwise, there was an error.

» **Enter in programming mode with the installer password**

Enter + installer password (factory default: 9090)

» **Program monitoring account**

Enter + 15 + PP + Enter, where PP = partition from 01 to 16

After the command, type the monitoring account number with 4 digits and press the *Enter* key to confirm.

» **Program the reporting mode.**

Enter + 17 + 4 + 0 + 0 + Enter

» **Program communication priority (2G/3G only)**

Enter + 19 + 1 + Enter

» **Program destination IP**

Enter + 801 + I + Enter, where I = 1 or 2 (destination IP 1 or destination IP 2)

After the command, type the IP number of the monitoring company 1 (example: 192.168.001.100) and press the *Enter* key to confirm.

» **Program IP network communication port**

Port 1 = Enter + 802 + 1 + Port number with 4 digits + Enter

Port 2 = Enter + 802 + 2 + Port number with 4 digits + Enter

» **Program destination domain name (DNS)**

If you do not want to use DNS move to the next command, otherwise, type.

Enter + 803 + D + Enter, where D = 1 or 2 (DNS 1 or DNS 2).

After the command, type the DNS domain name and press the *Enter* key to confirm.

» **Program monitoring options via IP**

Enter + 830 + Enter

After the command, using the keyboard keys, enable the desired option from 1 to 4, where:

- » **1:** enables the sending of events to the monitoring company 1.
- » **2:** enables the sending of events to the monitoring company 2.
- » **3:** enables the domain name (DNS) of the monitoring company 1.
- » **4:** enables the domain name (DNS) of monitoring company 2 and press the *Enter* key to confirm.

» **Enable the chip to be used**

Enter + 832 + Enter

After the command, use the keyboard keys to enable options 1 (chip 1), 2 (chip 2).

» **Program login**

Enter + 822 + O + Enter, where O = 1 or 2 (operator 1 or operator 2)

After the command, type the login (in accordance with the operator used) and then press the *Enter* key to confirm.

» **Program password**

Enter + 823 + O + Enter, where O = 1 or 2 (operator 1 or operator 2)

After the command, type the password (in accordance with the operator used) and then press the *Enter* key to confirm.

» **Program APN**

Enter + 824 + O + Enter, where O = 1 or 2 (operator 1 or operator 2)

After the command, type APN (in accordance with the operator used) and then press the *Enter* key to confirm.

» **To program the PIN (Personal Identification Number)**

If you want to use the PIN, perform the command presented in sequence, otherwise proceed with the next command.

If the PIN is incorrect, the chip will be blocked.

Enter + 825 + O + PIN Number with 4 digits + Enter, where O = 1 or 2 (operator 1 or operator 2)

» **GPRS Heartbeat interval (link test)**

Enter + 827 + TTM + Enter, where TTM = time interval of the Heartbeat from 000 to 255 minutes (default 005 minutes)

» **DNS Servers for GPRS**

Enter + 828 + S + Enter, where S = 1 or 2 (Server 1 or Server 2)

After inserting the command, type the DNS server code (in accordance with the server used) and then press the *Enter* key to confirm.

» **Interval between GPRS connection attempts**

Enter + 829 + TG + Enter, where TG = time interval of the reconnection attempts from 00 to 20 (default 00 minutes)

» **Exit the programming mode with the installer password**

Installer password (factory default: 9090)

» **Check the 2G/3G signal level**

Press the *Menu* key, navigate through the arrow keys, access the option *2G/3G Signal* and check the signal through the marks from 1 to 10.

» **Check the connection to the IP Receiver service**

Press the *Menu* key, navigate through the arrow keys, access the *Connections* option and check if the mark for the 2G/3G option: *IP1* and/or *IP2* is filled. If yes, the alarm center is connected via GPRS with the IP receiver software through the chips that were enabled.

6.12. Configurations of zones

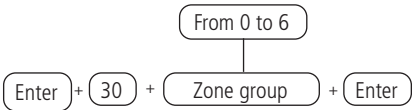
Zone configurations can be performed to adapt/define functionalities that best fit the alarm center operating environment. The following table demonstrates which group the zone is in, divided into 10 and the keyboard keys referring to each zone, according to the chosen group.

Group	Zones from 01 to 10	Group	Zones from 11 to 20	Group	Zones from 21 to 30
0	Key 1 = zone 1	1	Key 1 = zone 11	2	Key 1 = zone 21
	Key 2 = zone 2		Key 2 = zone 12		Key 2 = zone 22
	Key 3 = zone 3		Key 3 = zone 13		Key 3 = zone 23
	Key 4 = zone 4		Key 4 = zone 14		Key 4 = zone 24
	Key 5 = zone 5		Key 5 = zone 15		Key 5 = zone 25
	Key 6 = zone 6		Key 6 = zone 16		Key 6 = zone 26
	Key 7 = zone 7		Key 7 = zone 17		Key 7 = zone 27
	Key 8 = zone 8		Key 8 = zone 18		Key 8 = zone 28
	Key 9 = zone 9		Key 9 = zone 19		Key 9 = zone 29
	Key 0 = zone 10		Key 0 = zone 20		Key 0 = zone 30
Group	Zones from 31 to 40	Group	Zones from 41 to 50	Group	Zones from 51 to 60
3	Key 1 = zone 31	4	Key 1 = zone 41	5	Key 1 = zone 51
	Key 2 = zone 32		Key 2 = zone 42		Key 2 = zone 52
	Key 3 = zone 33		Key 3 = zone 43		Key 3 = zone 53
	Key 4 = zone 34		Key 4 = zone 44		Key 4 = zone 54
	Key 5 = zone 35		Key 5 = zone 45		Key 5 = zone 55
	Key 6 = zone 36		Key 6 = zone 46		Key 6 = zone 56
	Key 7 = zone 37		Key 7 = zone 47		Key 7 = zone 57
	Key 8 = zone 38		Key 8 = zone 48		Key 8 = zone 58
	Key 9 = zone 39		Key 9 = zone 49		Key 9 = zone 59
	Key 0 = zone 40		Key 0 = zone 50		Key 0 = zone 60
Group	Zones from 61 to 64				
6	Key 1 = zone 61				
	Key 2 = zone 62				
	Key 3 = zone 63				
	Key 4 = zone 64				

Enable / Disable zones

The zones that are not being used must be disabled so that they do not go off when the alarm center is activated using a remote control, or even if, when trying to activate the alarm center using a valid password, the keyboard emits an error beep indicating that the alarm center has open zones.

To program this function, type:



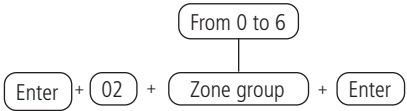
Use the keys on the keyboard to define the status of the zone, so that the referring numbers, who wish to have the zone active, remain marked and the zones that should remain inactive remain unmarked, then confirm with the *Enter* key.

Observation: all zones leave the factory enabled.

Partial Mode

When the system is activated in *Partial* mode, only the zones defined for this mode when being violated/activated will not generate a trigger. This mode is useful for activating zones in cases where you do not want to activate the entire system or the entire partition, such as only activating the external perimeter zones. Zones defined as *Partial* mode can belong to any partition on the switch.

To program, type:



Use the keys on the keyboard to define which zones will have *Partial* mode, so that the referring numbers, who wish to have the zone with *Partial*, mode, remain marked and the zones without the function remain unmarked and then confirm with the *Enter* key.

Observation: if the control panel is activated in Complete mode, all zones, including those defined as Partial mode will be activated, in the same way it will happen with the activation of partitions of the control panel, activating the zones defined as Partial.mode.

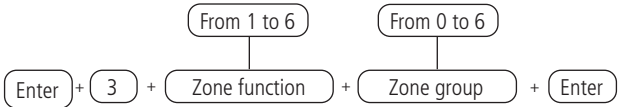
Zone Functions

The alarm center zones leave the factory configured as immediate, that is, when they are violated, they generate an immediate event/trigger, however they can be configured for the following functions:

- » **Timed zone for entry:** allows defining which zones will be timed when the alarm center is activated. If a timed zone is opened/violated with the control panel activated, the entry delay will start, being necessary to deactivate the system before the end of the delay for the alarm not to go off. If an untimed zone is opened prior to deactivation of the system, the trigger will be immediate. To set the time, refer to the *Entry Timing* section.
- » **Follower zone:** this configuration is only valid if used together with a timed zone with the alarm center activated. The zone can behave in two different ways:
 - » If someone enters a timed zone and then enters the follower zone, the behavior will be timed zone.
 - » If someone enters a follower zone without having previously passed through a timed zone, the behavior will be that of an immediate zone.
- » **24 Hour Zone:** In this configuration, the zone remains activated 24 hours a day, even when the system is turned off. It can be configured for audible or silent trigger. To define the trigger type, see section *Zone operating mode*.
- » **Panic zone:** this function is designed to call for help in a dangerous situation. The moment the zone is breached, the panic event will be reported to the monitoring company. It is possible to program this function in *Audible* or *Silent* mode. To define the trigger type, see section *Zone operating mode*.
- » **Medical panic zone:** when the zone is violated, the medical emergency event will be reported to the monitoring company, and the siren will beep for 1 second every 6 seconds.
- » **Fire zone:** has the function of monitoring fire sensors – use the TX 8000 universal transmitter to receive the signal from a wired fire sensor. The configured zone will remain active 24 hours a day. If the sensor detects a problem, the fire event will be reported to the monitoring company and the siren will emit pulsed tones. In most cases, fire sensors have normally open (NO) contacts and to configure the zone, be in this mode, see section *Zone operating mode*.

A zone can only be configured for one of the above functions. This way, if a zone is configured for more than one function, only the last selected function will be accepted. For example, if zone 2 is configured as a timed zone and then configured as a 24-hour zone, zone 2 will operate according to the last configuration made, in this case, a 24-hour zone.

To program this function, type:



Zone functions	
1	Timed
2	Follower
3	000 to 24 hours
4	Panic
5	Medical emergency
6	Fire

Use the keyboard keys to define the function of the zone, so that the referring numbers, who wish to have the zone with the given function, remain marked and the zones without the function remain unmarked, then confirm with the *Enter* key.

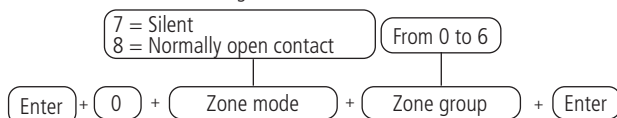
Obs.: each zone can have only one function and if programming is done in a zone already configured with another function, the last programming made will remain as operative

Zone operating mode

In conjunction with the settings of *Zone Functions* mentioned above, the zone can be configured for the following operating modes:

- » **Silent:** if there is a trip in a zone configured for *Silent* mode, the siren will not be activated, however the corresponding event will be sent to the registered security company/applications and the programmed personal telephones will be called.
- » **Normally open contact:** the zones leave the factory prepared for the use of sensors with normally closed contact (NC). If you want to use sensors with contact being normally open (NO), for example, fire sensors (through TX 8000), activate this operating mode in the control panel for the corresponding zone.

To set an operating mode for zones, use the following command:



Use the keyboard keys to define the zone mode, so that the referring numbers, who wish to have the zone with the certain mode, remain marked and the zones without the mode remain unmarked, then confirm with the *Enter* key.

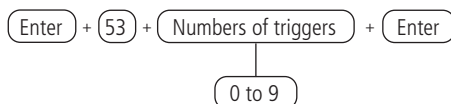
Obs.: the programming carried out in a sensor will only be effective after activating the tamper, tripping or when quickly activating its respective synchronization button.

Automatic zone cancellation

This function will temporarily cancel a zone if it triggers the programmed number of times, within the same activation. For example, with the number of triggers programmed to 4, the fourth time a sensor triggers while the system is activated, the corresponding zone will be bypassed and the corresponding event will be sent to the monitoring company.

When the system is deactivated, the zone will return to normal operation. If the number of triggers is programmed as 0, the function will be disabled.

To program this function, type:



To edit/view the programmed value, type:

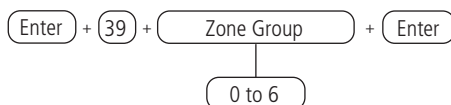


After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Open Door Zone (from version 3.0.5)

With this function enabled, if the zone remains open for the programmed time, the control panel sends the open door event to the monitoring and applications and, if programmed, can activate the PGM 8000 (see the PGM 8000 Wireless Actuator section). It only works when the control panel is deactivated.

To program this function, type:

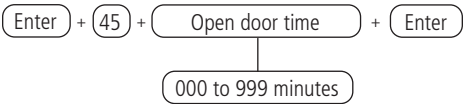


Use the keys on the keyboard to define which zones will have the open door function enabled, so that the numbers referring to the zones that will have the function enabled remain marked and the zones that should have the function disabled remain unmarked, and then confirm with the *Enter* key.

Door open time (from version 3.0.5)

This is the maximum time, in minutes, that the zone can remain open without triggering the open door alarm.

To program the time, enter:



To edit/view the scheduled time, type:



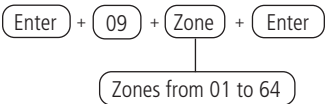
After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Entry on

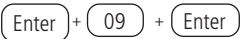
Entry on zone

This function allows you to program a zone to activate or deactivate the alarm center. The Zone ranges from 01 to 64. If you program 00, the Entry on function will be disabled.

To program this function, type:



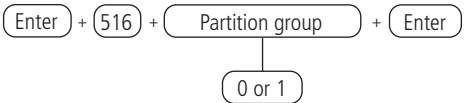
To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Entry on partition

Choose the partition that will be activated or deactivated through the On entry, factory default all partitions are enabled. For a non-partitioned system, keep at least partition 01 enabled.



After entering the command, through the XAT 8000 keyboard, mark which partitions will be activated by the entry on function, using the keyboard numbers to mark the partition. Select 0 for partition group from 1 to 10 and 1 for partitions from 11 to 16. After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Entry on activation and/or deactivation permission

It allows entry on only to activate the alarm center, only to deactivate the alarm center or both.



After the command, using keys 2 and 3 of the keyboard, enable the desired option, where:

- » **Key 2:** permission to activate;
- » **Key 3:** permission to deactivate and press the *Enter* key to confirm.

6.13. Program the partitioning of the alarm center

Enable the partitioning

To enable the partitioning of the alarm center (the alarm center can have up to 16 partitions with activation / deactivation and reporting of events independent) must be programmed.

(Enter) + (510) + (Enter)

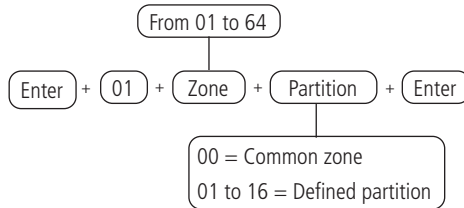
Use key *1* on the keyboard to enable the partitioning of the alarm center, so that number 1 remains marked to enable and unmarked to disable the partitioning and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Zone partition

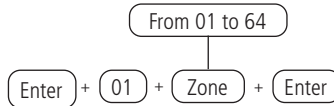
Once the system is partitioned, the zones can be divided as follows:

- » **Common Zone (default):** The zone does not belong to any of the partitions. It is only activated when all partitions are activated (activation by master password or total password) and deactivated whenever one of them receives the command to deactivate.
- » **Zone defined to one of the partitions:** zones thus defined will be activated/deactivated when the desired partition (01 to 16) is activated/deactivated or when the system is activated in *Partial* mode.

To choose which partition a certain zone (sensor) should belong to, program:



To edit/view the partition of programmed zones, enter:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: if zones are not defined for the partition, it will be inactive.

Partitions of passwords

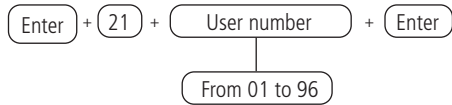
The secondary passwords that are created (01 to 96) leave the factory without permission to operate partitions. When enabling partitioning, it is necessary to select which partitions the user will have permission to Activate/Deactivate using the following command.



After entering the command, through the XAT 8000 keyboard, mark which partitions the password will have permission, using the keyboard numbers to leave marked referring to the partition. After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Attention: in addition to the aforementioned programming points, it is necessary that the user passwords are created / defined (topic *Passwords*) in addition to the registration of wireless controls for access (topic *Remote control*) and also to define the partitioning of keyboards (topic *Keyboard*) and sirens (topic *Wireless sirens*).

To edit/view the programmed value, type:



6.14. Timings

Input timing

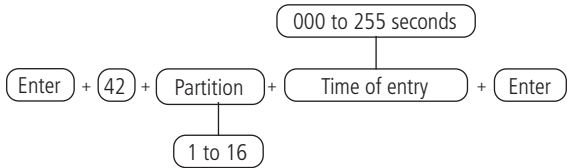
The entry timing is used when you want to have time to enter the protected environment and deactivate the alarm center without triggering the alarm (it is necessary to enable the zone as a delay, see section Functions of the zones).

When activated, if any sensor connected to the timed zone is triggered, the alarm center memorizes the violation and waits for the programmed time to trigger the alarm and will also emit beeps on the integrated siren every 1 second, and in the last 5 seconds of the timer, the beeps will be faster. The input timing beep can be disabled or have the volume adjusted to low, medium and high according to the need of the environment (see item *Volume adjustment on the built-in siren for entry timing*). Factory default disabled.

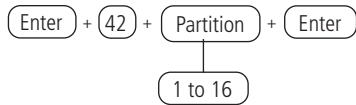
If the alarm center is not deactivated during this period, the alarm will be triggered even if the sensor has returned to normal.

This time is programmable from 000 (timing deactivated) up to 255 seconds. The timing leaves the factory programmed to 30 seconds (non-partitioned or partitioned system which is applied to all partitions). On non-partitioned systems program the entry time with the partition address being 01.

To program this function, type:



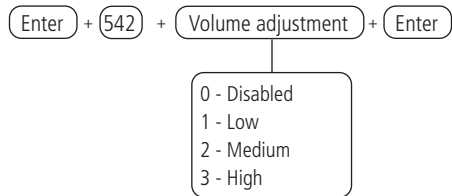
To edit/view the programmed value, type:



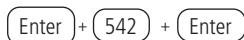
After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Adjustment of the beep in entry timing

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Exit timing

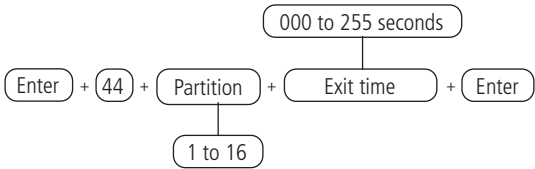
The exit timing is used when you want to activate the alarm center via the keyboard, and have time to leave the room before the alarm goes off.

This time is programmable from 000 (timing disabled) up to 255 seconds and leaves the factory programmed for 30 seconds. If the timing is programmed, when the alarm center is activated by the keyboard, it will emit beeps every 1 second, and in the last 5 seconds of the timing, the beeps will be faster.

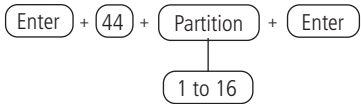
All zones in the partition to be programmed will be affected by the exit timing, except zones programmed as 24-hour, Panic, Medical Emergency or Fire.

The exit timing is valid only for activation of the alarm center via keyboard. When activation is done via remote control, the timing will always be zero (instantaneous). On non-partitioned systems program the exit timing with the partition address being 01.

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Disable output beep

This function allows you to disable only the output time beeps that are emitted by wireless keyboards (beeps are only emitted when the time is different from zero).

To program this function, type:



After entering the command, use key 8 to mark/enable this function and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

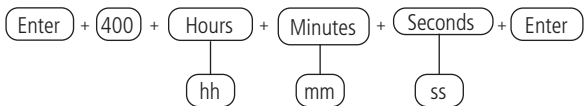
Obs.: this function is disabled at the factory and if programmed, it will be applied to all keyboards registered in the alarm center.

6.15. Alarm center time configurations

The alarm center has an internal clock and calendar and must be correctly programmed so that, in the event of an event, it is stored in the center buffer (last 512 events) with the correct date and time, for remote consultation through the monitoring / activation software. When the event is transmitted to the monitoring company, date and time will not be transmitted.

Clock

To program th clock, type:



To edit/view the programmed value, type:

(Enter) + (400) + (Enter)

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Calendar

To program the calendar, type:

(Enter) + (401) + (Day) + (Month) + (Year) + (Enter)

| | |

(DD) (MM) (YY)

To edit/view the programmed value, type:

(Enter) + (401) + (Enter)

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: if the clock and calendar are not programmed correctly, the alarm center will work normally, however the date and time of the events stored in the internal buffer will not correspond to the actual date and time and also the definition of holidays and automatic activation may not operate correctly.

Adjustment of the day of the week

Adjusts the current day of the week to align the current day of the month with the day of the week.

To program this function, type:

From 1 to 7
1 = Sunday
7 = Saturday

|

(Enter) + (402) + (Day of the week) + (Enter)

To edit/view the programmed value, type:

(Enter) + (402) + (Enter)

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Time interval for synchronization of date and time

When this function is enabled, the alarm center will synchronize the date and time with the server where the Intelbras IP Receiver software is installed (factory default 24-hour synchronization), for third-party software, they must be consulted. Synchronization will occur in the following situations:

- » In the programmed time interval.
- » The moment the alarm center is turned on in the electrical grid.
- » If the date and time are changed manually.
- » In case the connection to the server is lost.

To program this function, type:

From 000 to 255 hours
000 = disabled

|

(Enter) + (403) + (Time interval) + (Enter)

To edit/view the programmed value, type:

Enter + 403 + Enter

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

6.16. Time zone

When the alarm center is programmed to synchronize the date and time automatically, programming this field adjusts the time zone according to the region where the switchboard is installed. Time zone ranges from 00 (disabled) to 25, where 01 means GMT -1, 02 means GMT -2, and so on. Brasilia time is GMT -3.

To program, type the command below:

Enter + 405 + Time zone + Enter

00 - Disabled

01 - GMT -1

02 - GMT -2

03 - GMT -3

04 - GMT -4

05 - GMT -5

06 - GMT -6

07 - GMT -7

08 - GMT -8

09 - GMT -9

10 - GMT -10

11 - GMT -11

12 - GMT -12

13 - GMT 0

14 - GMT +1

15 - GMT +2

16 - GMT +3

17 - GMT +4

18 - GMT +5

19 - GMT +6

20 - GMT +7

21 - GMT +8

22 - GMT +9

23 - GMT +10

24 - GMT +11

25 - GMT +12

To edit/view the programmed interval, type:

Enter + 405 + Enter

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

6.17. Periodic test

This function is used to verify the integrity of the communication channel between the alarm center and the monitoring company.

If programmed, the *Periodic test* event will be periodically reported. Thus, if the monitoring company does not receive this event within the scheduled period, the communication channel can be considered inoperative.

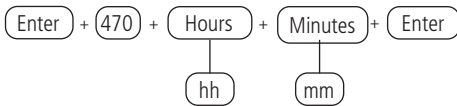
The *Periodic Test* function can operate in two modes:

- » **Time:** the periodic test event is sent once a day always at the scheduled time. If this mode is programmed, the time interval test will be skipped.
- » **Time interval:** the periodic test is sent at programmable time intervals from 1 to 255 hours.

Obs.: if you want to use the *Periodic Test by Time* together with the *Periodic Test by Time Interval*, the first event will be delivered at the time defined in the *Test by Time*, varying the delivery of the event according to the time programmed in the *Test by Time Interval*.

Periodic testing by time

To program this function, type:



To cancel the periodic test by time, type:



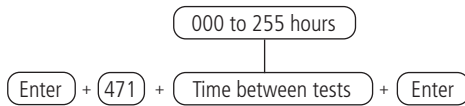
To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Periodic testing by time interval

To program this function, type:



Obs.: to deactivate the period test by time interval, program as 000.

To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

6.18. Automatic activation

With this function enabled, the alarm center will activate if all zones are closed and there is no movement in the room during the programmed time, at any time of the day, or after a programmed time. The time is programmable from 01 to 99 minutes (inactivity), that is, up to one hour and thirty-nine minutes, at any time of the day. In the case of partitioned switches, *Automatic activation*, when executed, will be performed on all partitions with the option of automatic activation of enabled partition. If you want to use the Automatic activation by partition, consult the topic *Programming partitioning of the alarm center*.

We present below examples of the use of automatic activation:

» **Example 1:**

In a place where there is no fixed time to activate the alarm center, we can program the *Automatic activation due to inactivity* to occur whenever all the sensors are closed, for example, for 50 minutes. This time must be chosen according to the local routine. If it is very busy, the time may be shorter. If there is little movement of people, the time must be longer, to prevent the alarm center from being activated at an undesired time.

» **Example 2:**

In an office, which closes every day at 6:00 pm, it can be programmed so that the *Programmed automatic activation* function only starts working from 6:00 pm. In this way, it is possible to reduce or eliminate the programmed idle time, without the risk of the alarm center being activated during the day.

The programmed automatic activation and due to inactivity can be used together. For example, if you want the alarm center to assemble automatically due to inactivity only after 10:00 pm.

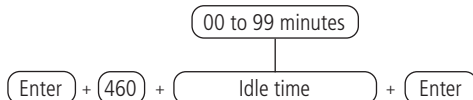
For this programming we have 3 examples that explain the Automatic activation of the alarm center, shown below, considering that the Programmed automatic activation will be at 10:00 pm and the idle time will be 10 minutes:

1. There was detection of a sensor (opening and closing) at 9:50 pm, so the alarm center will automatically activate at 10:00 pm.
2. There was detection of a sensor (opening and closing) at 9:55 pm, so the alarm center will automatically activate at 10:05 pm.
3. There was an opening of a sensor (only opening) at 9:59 pm and this sensor remained open until 10:30 pm, then the alarm center will automatically activate at 10:40 pm.

Automatic activation by inactivity

With this programmed function, the alarm center will be activated as soon as the defined time is made concrete so that the zones remain closed. The time must be inserted with two digits from 00 to 99 minutes. If 00 is typed, the Automatic Activation due to inactivity will be canceled.

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Programmed automatic activation and automatic deactivation

These functions allow activating and deactivating the system automatically at pre-programmed times, one for each day of the week and one more for holidays. To use the function, follow the procedure:

1. Select the days of the week on which Automatic activation will occur;
2. Select the days of the week for Automatic deactivation;
3. Program the desired times;
4. Adjust the system date and time;
5. Adjust the day of the week;

Obs.: for adjustment of the day of the week, consult the programming in the topic 6.15. Alarm center time configurations.

6. If you want to enable the automatic synchronization of date and time with the server (make sure that the latest version of Intelbras Receiver IP is being used so that the function takes effect correctly).

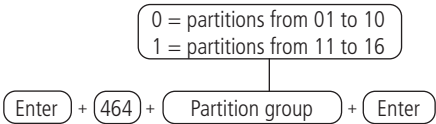
Use the following table referring to the following necessary programmings:

Key	Day of the week
Key 1	Sunday
Key 2	Monday
Key 3	Tuesday
Key 4	Wednesday
Key 5	Thursday
Key 6	Friday
Key 7	Saturday
Key 8	Holiday

Selection of automatic activation / automatic deactivation by partitions

Selects which partitions will have the programmed automatic activation and automatic deactivation function. Factory default, all partitions enabled.

To program this function, type:

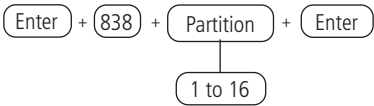


Use the keys on the keyboard to enable the function on partitions, partitions 01 to 10 are in partition group 0 and partitions 11 to 16 are in partition group 1, so that the numbers corresponding to the partitions you want have the function enabled remain marked on the display and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: if all partitions are selected, automatic activation will only occur if all zones of the alarm center are closed.

Days of the week for automatic activation

Select the days when Automatic Activation by partition will occur.



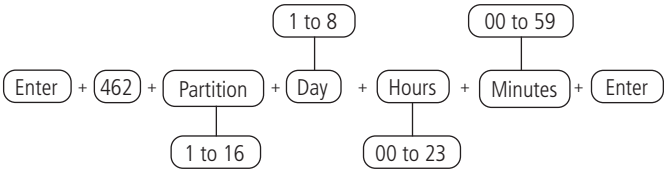
Use the keyboard keys to define the days for the automatic activation by partition to occur, so that the referring numbers, that you want to have the days enabled, remain marked and the days with the function disabled remain unmarked and then confirm with the *Enter* key.

Obs.: in the command above for a non-partitioned alarm center, use Partition = 01.

Automatic activation time

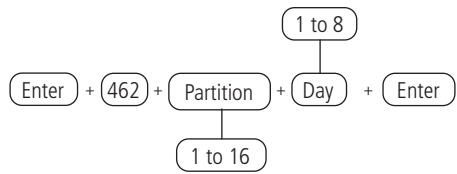
Selects the time that Automatic activation by partition will occur.

To program this function, type:



Obs.: in the command above for a non-partitioned alarm center, use Partition = 01.

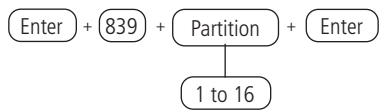
To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed

Days of the week for Automatic deactivation

Select the days when Automatic deactivation by partition will occur.



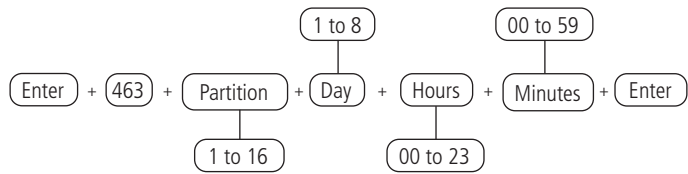
Use the keyboard keys to define the days for the automatic deactivation by partition to occur, so that the referring numbers, that you want to have the days enabled, remain marked and the days with the function disabled remain unmarked and then confirm with the *Enter* key.

Obs.: in the command above for a non-partitioned alarm center, use Partition = 01.

Automatic deactivation time

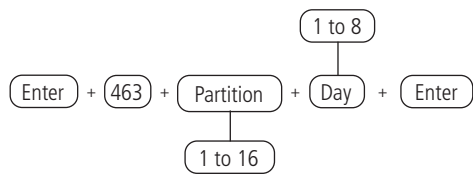
Selects the time that Automatic deactivation by partition will occur.

To program this function, type:



Obs.: in the command above for a non-partitioned alarm center, use Partition = 01.

To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Holidays

The alarm center has 10 memories (0 to 9) to program dates that require a special time for Automatic activation and Automatic deactivation.

When the system date is the same as one of the programmed dates, the day of the week settings will be superimposed by the times programmed in the address of the commands described above, referring to the alarm center's automatic activation programming.

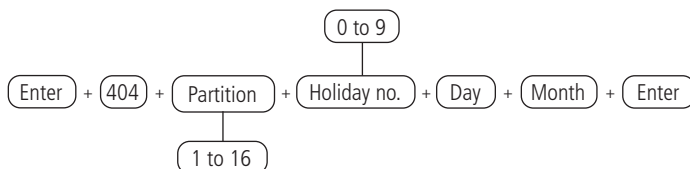
For the correct operation of this function, it is necessary to check whether the following scheduled automatic activation and automatic deactivation programmings are correctly enabled:

- » Days for programmed automatic activation.
- » Time of programmed automatic activation.
- » Days for programmed automatic deactivation.
- » Time of programmed automatic deactivation.
- » Adjustment of the day of the week
- » Time interval for synchronization of date and time.

Define holidays for Automatic Activation / Automatic Deactivation

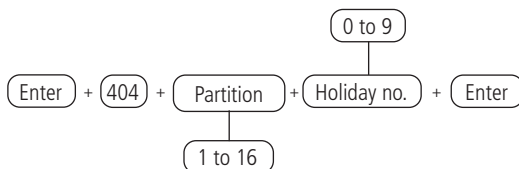
If the alarm center is partitioned, holidays can be defined by partition.

To program this function, type:



Obs.: » In the command above for a non-partitioned alarm center, use Partition = 01.

- » To disable a holiday, program the date with the value 00 for Day and Month.
- » To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: in the command above for a non-partitioned alarm center, use Partition = 01.

6.19. Monitoring configurations

The AMT 8000 LITE and AMT 8000 PRO alarm centers were especially developed to be monitored remotely, that is, a hired company can monitor in real time different events, for example:

- » System activation and deactivation.
- » Power outage (the power grid failure event will be reported according to the configured time, with the factory default being 1 minute. For more information, see the topic 6.21. *Time for sending of AC failure*).
- » System violation (trigger)
- » Violation of sensors (tamper)
- » Siren failure

When an event occurs, the alarm center will make contact with the monitoring company and will transmit via IP (Ethernet or 2G/3G) the event that occurred (internal buffer for 512 events)

Obs.: so that there may be monitoring via and 2G/3G it is necessary that the expander modules XG 2G or XG 3G be added to the alarm center.

Contact-ID Events

The alarm center leaves the factory with all events enabled (default Contact-ID).

See below the list of Contact-ID events.

Event	Standard code
Medical emergency	100
Fire alarm	110
Panic	120
Activation and deactivation under filtration	121
Silent panic	122
Zone trigger / zone restoration	130
24-Hour zone trigger	133
Silent trigger	146
AC network failure / AC network restoration	301
Low system battery / System battery restoration	302
System reset	305
Programming change	306
Battery absent / Battery restoration	311
Failure when communicating event	354
GPRS Keep Alive Failure	360
ETH Keep Alive Failure	361
Supervision failure / Supervision restoration	147
Tamper of expander devices / Restoration tamper of expander devices	145
Tamper sensors / Restoration tamper sensors	383
Low battery wireless device / Restoration battery device	384
System activation / deactivation.	401
Automatic activation / deactivation	403
Remote activation / deactivation	407
Activation through a key	408
Remote access	410
System activation/deactivation via Alexa	419
Partial activation of the system via Alexa	420
PGM activation/deactivation	422
PGM activation/deactivation via Alexa	435
Partial activation of the system	456
Incorrect password	461
RF Registration / exclusion	533
Registration / change / exclusion of password	534
Enable/disable zones	535
Zone bypass via Alexa	578
Zone bypass / zone bypass restoration	570
Periodic test	602
Manual testing	601
Request for maintenance	616
Event buffer reset	621
Date and time restarted	625

Obs.: some event codes may not be registered in all monitoring software. If necessary, register the corresponding comment, as these events facilitate the identification and solution of problems.

When an event occurs, the alarm center will inform the IP Receiver software of the corresponding device in the user/zone field, according to the following table:

Type of device	Index / initial address	Index / final address
Sensor / zone	001	064
Activation/deactivation by remote control	100	197
Activation / deactivation by keyboard	200	297
Keyboard failures	201	216
Siren failures	301	316
Amplifier failures	401	404
PGM 8000 wireless actuator	501	516

We present below examples of sending of *Contact-ID* events to devices:

- » **Sensor trigger in zone 01:** event 130 and user/zone is 001.
- » **Sensor trigger in zone 25:** event 130 and user/zone is 025.
- » **Sensor communication failure in zone 12:** event 147 and user/zone is 012.

- » **Sensor restoration in zone 64:** event 130 and user/zone is 064.
- » **Sensor tamper in zone 05:** event 383 and user/zone is 005.
- » **Registered siren tamper at address 09:** event 145 and user/zone is 309.
- » **Registered keyboard communication failure at address 01:** event 381 and user/zone is 201.

Enable / disable events

Note: this programming was removed from the keyboard starting with version 3.2.4 and is only available through the AMT Remote software or the AMT Remote Mobile app.

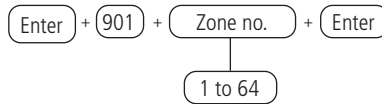
As it can be observed in the following commands, the event can be blocked if it is configured as 000 (it will not be sent to the Receiver IP) and enabled when registering FFF (it will be sent to the Receiver IP)

The tables below show the events and the respective default Contact-ID codes.

After inserting the command, insert the value 000 to disable or FFF to enable and press the Enter key to confirm. If you only want to view the configuration, press the Exit key and no programming will be changed.

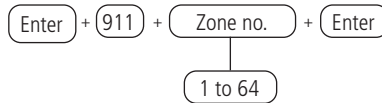
Opening type events		
Zone trigger		
Zone no.	Event	Contact-ID Code
1 to 64	Zone trigger	130

Use the table above to perform the event blocking / unblocking command.

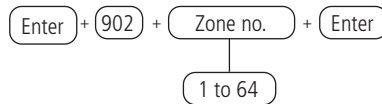


Restoration type events		
Zone trigger		
Zone no.	Event	Contact-ID Code
1 to 64	Restoration zone trigger	130

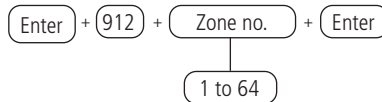
Use the table above to carry out the *Contact-ID* event change command for restoration of zones, as described below:



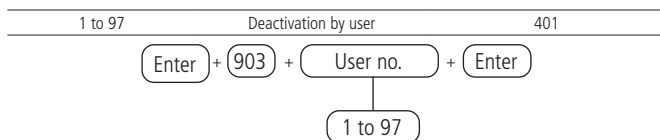
Opening type events		
Sensor tamper		
Zone no.	Event	Contact-ID Code
1 to 64	Sensor tamper	383



Restoration type events		
Sensor tamper		
Zone no.	Event	Contact-ID Code
1 to 64	Sensor tamper restoration	383



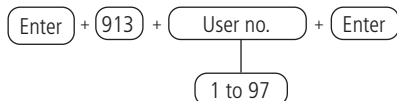
Opening type events		
Deactivation by user		
User no.	Event	Contact-ID Code



Restoration type events

Activation by user

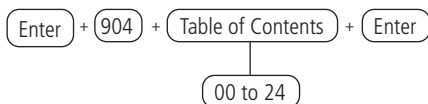
User no.	Event	Contact-ID Code
1 to 97	Activation by user	401



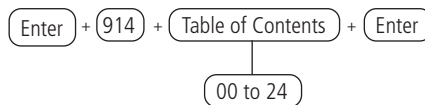
Opening type events

System events

Table of Contents	Internal event	Standard code
00	Low battery wireless device	384
01	N/A	
02	Supervision failure	147
03	Zone bypass	570
05	AC network failure	301
06	Low system battery	302
07	Battery absent	311
08	N/A	N/A
09	Remote deactivation	404
10	Automatic deactivation	403
11	N/A	
12	N/A	
13	System reset	305
14	Programming change	306
15	Failure when communicating event	354
16	Incorrect password	461
17	Remote access	410
18	Manual testing	601
19	Periodic test	602
20	Event buffer reset	621
21	Date and time restarted	625
22	Tamper of expander devices / Restoration tamper of expander devices	145
23	Tamper sensors / Restoration tamper sensors	383
24	Request for maintenance	616
25	AC failure wireless device	342
26	PGM activation	422
27	RF Registration	533
28	Registration / change of password	534



Restoration type events		
System events		
Table of Contents	Internal event	Standard code
00	Restoration low battery wireless device	384
01	N/A	N/A
02	Restoration supervision failure	147
03	Restoration zone bypass	570
05	AC network restoration	301
06	Low system battery restoration	302
07	Battery restoration	311
08	N/A	N/A
09	Remote activation	404
10	Automatic activation	403
11	Activation through a key	408
12	Activation under filtration	121
13	N/A	N/A
14	N/A	N/A
15	N/A	N/A
16	N/A	N/A
17	N/A	N/A
18	N/A	N/A
19	N/A	N/A
20	N/A	N/A
21	N/A	N/A
22	Tamper of expander devices	145
23	Sensor tamper	383
24	N/A	N/A
25	AC failure wireless device	342
26	PGM activation	422
27	RF Exclusion	533
28	Password exclusion	534



Push Events

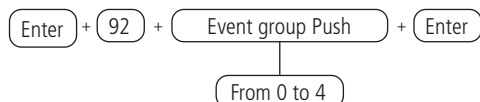
Notifications that will be sent to the Intelbras Guardian application when the corresponding event occurs with the alarm center, and it is necessary that the alarm center is connected to Internet (Ethernet, 2G/3G or 4G).

For further information about the application consult section *Using the Intelbras Guardian application (for mobile devices)*.

Event group (EV)	Event	Key	Key
0	ARME_DESARME_USUARIO (Assemble_Disassemble_User),	Key 1	Enabled
	N/A	Key 2	Enabled
	DISPARO_ZONA (Trigger_Zone),	Key 3	Enabled
	DISPARO_24H (Trigger 24 hours)	Key 4	Enabled
	DISPARO_SILENCIOSO (Silent_Trigger),	Key 5	Enabled
	DISPARO_EMERGENCIA_MEDICA (Trigger_Medical_Emergency),	Key 6	Enabled
	DISPARO_INCENDIO (Trigger_Fire),	Key 7	Enabled
	DISPARO_PANICO_AUDIVEL (Trigger_Audible_Panic),	Key 8	Enabled
	DISPARO_PANICO_SILENCIOSO (Trigger_Silent_Panic),	Key 9	Enabled
	TAMPER_SENSOR,	Key 0	Enabled

1	BATEIRA_BAIXA_SENSOR (Low_Battery_Sensor),	Key 1	Enabled
	N/A	Key 2	Enabled
	FALHA_SUPERVISAO_RF (RF_Supervision_Failure),	Key 3	Enabled
	BYPASS_ZONA (Zone_Bypass),	Key 4	Enabled
	BYPASS_AUTOMATICO (Automatic_Bypass),	Key 5	Enabled
	FALHA_REDE_ELETRICA (Electric_Grid_Failure),	Key 6	Enabled
	BATERIA_PRINCIPAL_BAIXA (Low_Main_Battery),	Key 7	Enabled
	BATERIA_PRINCIPAL_AUSENTE (Main_Battery_Absent),	Key 8	Enabled
	N/A	Key 9	Enabled
2	ARME_DESARME_REMOTO (Remote_Assembly_Disassembly),	Key 0	Enabled
	AUTO_ARME_DESARME (Automatic_Assembly_Disassembly),	Key 1	Enabled
	ARME_RAPIDO (Fast Assembly),	Key 2	Enabled
	ARME_DESARME_SOB_COACAO (Assembly_Disassembly_Under_Filtration),	Key 3	Enabled
	RESET_SISTEMA (System_Reset),	Key 4	Enabled
	PROGRAMACAO_ALTERADA (Changed Programming),	Key 5	Enabled
	FALHA_AO_COMUNICAR_EVENTO (Failure_when_communicating_event)	Key 6	Enabled
	SENHA_INCORRETA (Incorrect_Password)	Key 7	Enabled
	ACESSO_DOWNLOAD (Download_Access)	Key 8	Enabled
	TESTE_MANUAL (Manual_Test)	Key 9	Enabled
3	TESTE_PERIODICO (Periodic_Test)	Key 0	Enabled
	RESET_BUFFER_EVENTOS (Event_Buffer_Reset)	Key 1	Enabled
	RESET_DATA_HORA (Date_Time_Reset)	Key 2	Enabled
	N/A	Key 3	Enabled
	N/A	Key 4	Enabled
	SOLICITACAO_MANUTENCAO (Maintenance_Request)	Key 5	Enabled
	FALHA_REDE_ELETRICA_MOD_EXPANSOR (Electric_Grid_Failure_Expander_Module)	Key 6	Enabled
	ACTIVATION / DEACTIVATION_PGM	Key 7	Enabled
	RF REGISTRATION / EXCLUSION	Key 8	Enabled
	REGISTRATION / CHANGE / EXCLUSION OF PASSWORD	Key 9	Enabled
4	ENABLE_DISABLE_ZONE	Key 0	Enabled
	FALHA_KEEP_ALIVE_GPRS	Key 1	Enabled
	FALHA_KEEP_ALIVE_ETHERNET	Key 2	Enabled
	ARME_DESARME_VIA_ALEXA	Key 3	Enabled
	ARME_STAY_VIA_ALEXA	Key 4	Enabled
	ACIONAMENTO_PGM_VIA_ALEXA	Key 5	Enabled
	BYPASS_ZONA_VIA_ALEXA	Key 6	Enabled

Use the table above to disable / enable the sending of occurrences to the monitoring application, as described below:



Use the keys on the keyboard to enable the options of *Push* events, such that the corresponding numbers that you want to have the function enabled remain marked on the display and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Remote control generated panic events

User no. 0 to 97	Partitions																Event
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
User 1																	Partition 1
User 2																	Partition 0
User 3																	Partition 0

Obs.:

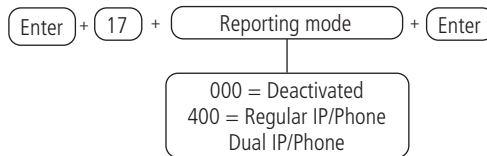
- » User registered only in a partition the panic event will arrive at the registered partition.
- » User registered for more than one partition the generated panic event will arrive at the partition 00.
- » User with no permission to the partition the panic event will arrive at the partition 00.

Reporting mode

The alarm center can be configured to report events to the monitoring company, through one of the modes describe below:

- » **Deactivated:** in this mode the alarm center will operate as a monitored alarm center, not reporting the events of the occurrences through no channel, only to applications, if used.
- » **Regular IP/phone:** in the occurrence of an event, the alarm center will send them through the available communication channels in the sequence: IP1, IP2, phone 1 and phone 2, until the event is sent or the number of attempts (standard of 9 attempts) is reached.
- » **Double IP/Phone:** uses IP1 and IP2. In the failure of IP1 the event will be reported to Phone 01 and in failure of IP2 the event will be reported to Phone 02, that is, if phones 01 and 02 are registered.

Obs.: reporting via telephone line available only for AMY 8000 PRO.



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Resending activation issues (feature available from version 3.0.6)

With the function enabled, whenever the system is activated, any problems (low battery, supervision failure, tamper violation, etc.) detected and not resolved are sent back to the monitoring company.

To program this function, type:



Use key 1 on the keyboard to enable or disable the troubleshooting function when activating the system, so that the number 1 remains marked to enable the function and unmarked to disable it, and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Blocking of the sending from partition 00 to the monitoring company

This function blocks the sending of partition 00. This value 00 is sent to the monitoring company when the alarm center is not partitioned or when it triggers a common zone to all partitions (Partition: 01 to 16). This function was created, as some event receivers used in monitoring companies do not recognize partition 00.

To program this function, type:



Use key 8 on the keyboard to enable the remittance blocking function of partition 00, so that the number 8 remains marked to enable and unmarked to disable the function, and then, confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Monitoring via telephone line

The alarm center has 7 memories for telephone, divided in the following way:

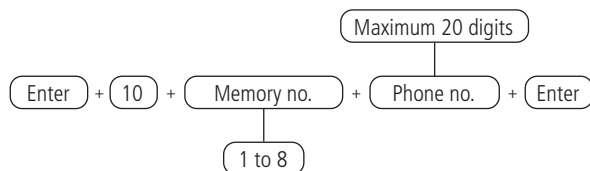
Memories 1 and 2	Monitoring company
Memories 4 to 8	Personal phones

Obs.: memory number 3 must not be used.

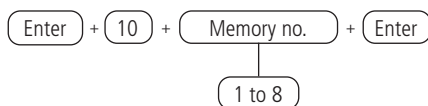
- » **Monitoting company:** phones for which the alarm center will call if it is configured as monitored and any event is generated.
- » **Personal phones:** in case of trigger or activation of the *Panic* function, the alarm center will call the programmed numbers and emit the sound of a siren for approximately 50 seconds.

Program / exclude and test phone numbers

To program the phones to be called (in case of occurrence of events, alarm or panic), type:

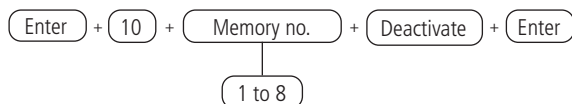


To edit/view the programmed value, type:

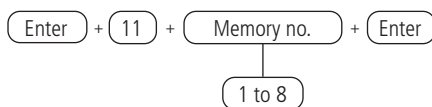


After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

To erase a previously programmed phone, type:



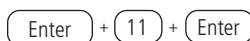
To test whether the phone number was programmed correctly, type:



Obs.: memory number 3 must not be used.

The alarm center will generate the manual test event and dial the phone selected to report this event (memories 1 and 2) and will call the personal phones (memories 4 to 8).

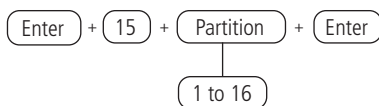
To interrupt the phone test, type:



Monitoring account

The monitoring account is the customer's identification in the monitoring company. Up to 16 accounts (one for each partition) containing 4 characters can be programmed.

To program this function, type:



After entering the command, enter the monitoring account code always with 4 digits and values from 0 to 9 or the letters B, C, D, E and F. If you only want to view the configuration, press the *Exit* key, no programming will be changed.

Obs.: if the AMT 8000 alarm center is not partitioned, use the partition as 01.

Reset of pending events

This command will cancel the sending of all non-transmitted events, however the events are still recorded and can be accessed via download. For example, if the system has been without a telephone line for some time, the event buffer can have up to 512 untransmitted events. If *Reset blocking* is activated, it will not be possible to execute this function (see section *Blocks*).

To program this function, type:

Enter + 16 + Enter

Number of attempts to report an event

Whenever an event is generated, the alarm center will call the monitoring company and, if it cannot send the event, it will make a new call and try to send the event again. The panel leaves the factory programmed for 9 attempts, this value can be changed respecting the limit of 1 to 9 attempts.

To program this function, type:

Enter + 13 + No. of attempts + Enter
1 to 9

To edit/view the programmed value, type:

Enter + 13 + Enter

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Generated DTMF signal level

It allows you to change the amplitude of the generated DTMF signal to solve communication problems in places where the line signal is very low. The adjustment of the DTMF level must be carried out in the place where the alarm center will operate, since the adjustment can vary from place to place and all options must be tested, starting with level 0 up to level 6, until the desired condition is obtained.

To program this function, type:

Enter + 18 + DTMF signal level + Enter
0 = level 0 (low)
1 = level 1
2 = level 2 (standard)
3 = level 3
4 = level 4
5 = level 5
6 = level 6 (high)

To edit/view the programmed value, type:

Enter + 18 + Enter

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Monitoring via Ethernet/Wi-Fi connection

Obs.: Wi-Fi connection available only for the AMT 8000 PRO alarm center and with 2.4 GHz routers.

The alarm center has a connection to report events and be accessed/controlled remotely through an Ethernet or Wi-Fi network for IP addresses.

- » **Ethernet:** an RJ45 cable must be installed in the alarm center with the Ethernet signal coming from a router, switch or directly from the signal received at the installation site. The alarm center, when connected via Ethernet, can also be accessed remotely through Intelbras applications.
- » **Wi-Fi:** with the Wi-Fi connection enabled on the alarm center, event reporting and connections will use this route, and for this, the alarm center installation site must have a router or device to send the signal with good quality (check the distance between the signal replicating device and the alarm center). The alarm center, when connected via Wi-Fi, can also be accessed remotely through Intelbras applications.

For the alarm center to be connected to a Wi-Fi network, the following commands must be executed:

To program or change the Wi-Fi network name, enter:

Enter + 850 + Enter

After entering the command, use the XAT 8000 keyboard keys to enter the name of the network you want to connect, paying attention to special characters if applicable and after changing the value, press the Enter key. If you only want to view the configuration, press the Exit key and no programming will be changed

Obs.: check if the network to be connected has special characters, numbers and different symbols in its name, which if not inserted can prevent the connection to the correct network.

To program or change the Wi-Fi network password, enter:

Enter + 851 + Enter

After entering the command, use the XAT 8000 keyboard keys to enter the password of the network you want to connect, paying attention to special characters if applicable and after changing the value, press the Enter key. If you only want to view the configuration, press the Exit key and no programming will be changed

Obs.: check if the network to be connected has special characters, numbers and different symbols in your password, which if not inserted they can impede the connection to the network.

To enable Wi-Fi, type:

Enter + 852 + Type of configuration + Enter

0 to 2

Selection	Type of configuration
0	Wi-Fi disabled
1	Wi-Fi enabled / in case of AC failure, operates on battery
2	Wi-Fi enabled / only with active AC network

To edit/view the programmed value, type:

Enter + 852 + Enter

After inserting the command, use the XAT 8000 keyboard keys to define the type of configuration of the network that will be connected.

Selection	Type of configuration
0	Wi-Fi disabled
1	Wi-Fi enabled / in case of AC failure, operates on battery
2	Wi-Fi enabled / only with active AC network

After selecting the type of configuration, press the Enter key to confirm. If you only want to view the configuration, press the Back/Exit key and no programming will be changed.

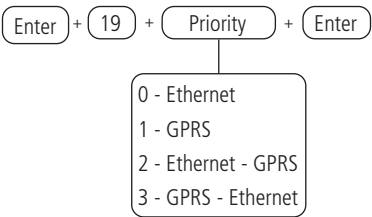
Obs.: if the alarm center is already connected to the network cable (Ethernet), the communication priority will be Ethernet and the Wi-Fi network will be the second option. In case of loss of communication via cable, the priority becomes the Wi-Fi connection. When using only the Wi-Fi network, this will be the priority.

To be able to establish the connection via Ethernet/Wi-Fi, the following configurations exposed below must be carried out:

Communication priority

Define the priority communication channel to transmit the generated events. If the priority channel fails, the alarm center will try to send the event through the next channel until it is sent or the number of attempts is reached. For example, if option 2 is selected, the alarm center will try to send the event via Ethernet. If it fails, it will try to send via GPRS and then via the phone line if any phone number is programmed.

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Monitoring options via IP

To send the events for monitoring, it is necessary to define the address(es) to which the events will be sent, it is necessary to enable the sending through this(ese) address(es) and select whether the IP address or domain name (DNS) will be used.

- » **Event transmission to IP1/DNS1:** filled marker ☒ = enabled, empty marker ☐ = disabled (it is necessary to program the address).
- » **Event transmission to IP2/DNS2:** filled marker ☒ = enabled, empty marker ☐ = disabled (it is necessary to program the address).
- » **IP1 or DNS1:** empty marker ☐ = the IP address will be used, filled marker ☒ = the domain name (DNS) will be used.
- » **IP2 or DNS2:** empty marker ☐ = the IP address will be used, filled marker ☒ = the domain name (DNS) will be used.

Key 1	Enable the sending of events to the monitoring company 1
Key 2	Enable the sending of events to the monitoring company 2
Key 3	Enable the domain name (DNS) of the monitoring company 1
Key 4	Enable the domain name (DNS) of the monitoring company 2

Use the table above to disable/enable the sending of events via IP addresses or DNS for monitoring purposes, as described below:

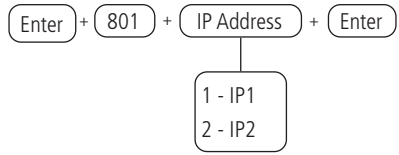


Use keys 1, 2, 3 and 4 on the keyboard to enable the monitoring options via IP, so that the corresponding numbers, who wish to have the function enabled, remain marked on the display and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Destination IP address

IP address of the computer that will receive events from the alarm center (monitoring company). Up to two addresses (IP1 and IP2) can be programmed, regardless of whether the communication channel used is Ethernet, WI-FI or GPRS, the report will be made to the same addresses. To receive events over the Internet, it is necessary to install the Intelbras IP Receiver software on the computer or use a monitoring software already compatible with the TCP/IP communication of the AMT 8000 LITE and AMT 8000 PRO alarm centers.

To program this function, type:



After the command, type the IP number of the monitoring company (example: 192.168.001.100) and press the Enter key to confirm. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: for correct functioning, the same destination IP addresses with the same port referring to IP1 and IP2 must not be added, otherwise it will cause blockages/failures in the event reporting.

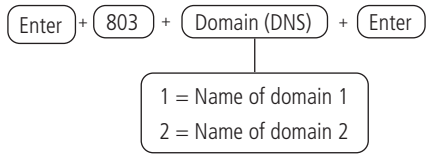
Destination Domain Name (DNS)

It allows you to program the address of the destination computer in DNS format (Domain Name System – ex.: nome.dominio.xx).

It is recommended to use DNS if the computer's Internet connection does not have a fixed IP.

Obs.: there are free services available on the internet that allow users to obtain subdomains, which point to IP addresses, which regularly change (e.g.: No-IP®, DynDNS®), but may not guarantee continued system operation. These services usually have long update times and can go through periods of instability and even temporary absence.

To program this function, type:



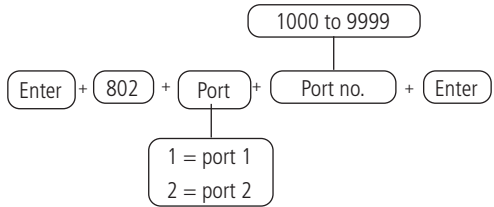
After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: for correct operation, the same destination DNS addresses with the same port referring to domains 1 and 2 must not be added, otherwise it will cause blockages/failures in the reporting of events.

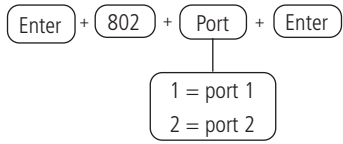
Port

The port is a number associated and mandatory to communication sections between applications in IP networks. This field defines the port to which the alarm center will connect, factory default 9009. Intelbras IP Receiver software must be configured to the same port. Some ports may be used by other applications, so choose one that is free, preferably above 1000.

To edit the communication port to be used, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: additional amounts may be charged by the service provider for the use of communication ports, so their availability and release/configuration costs must be consulted.

DNS servers for Ethernet

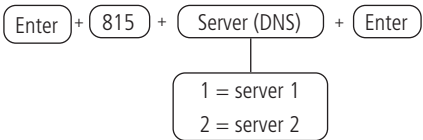
DNS server addresses available on the internet for name and domain resolution (eg: name.domain.xx).

It is recommended to adopt the servers provided by the internet provider itself. It is also possible to choose to use external and free DNS servers, as is the case with the service offered by the website www.opendns.com. The following table presents the IP addresses of the servers. In some cases, it is possible to use the addresses of primary servers as secondary servers and vice versa.

Company	DNS Servers	
	Primary or preferential (1)	Secondary or alternative (2)
Open DNS	208067222222	208067220220

Obs.: this information can be changed with no prior notice.

To program this function, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Local Ethernet Configurations

The following options configure the network properties on the alarm center, such as IP address, mask, gateway, etc., very similar to the configurations of a network card on a computer. These configurations allow the alarm center to connect to the Intelbras IP Receiver software and transmit events.

Visualization of the alarm center MAC

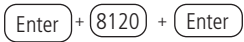
To view the alarm center MAC, perform the following procedure:

1. Press the *Menu* key, with the directional keys on the keyboard find the *End* option. *MAC.*, press the *Enter* key and the MAC address of the alarm center will be shown on the bottom line;

IP Address of the alarm center (connection by cable)

IP Address of the local network where the alarm center is connected. To view / edit the alarm center IP address, simply perform the following procedure:

1. To program/change the IP address of the alarm center, type:



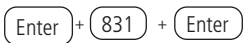
2. The current address will be shown, being the factory default *192.168.001.100*, to insert/change the address, type the new programming and press *Enter* key to confirm the programming;
3. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: the DHCP option shown below must be disabled to manually change the IP of the alarm center.

DHCP

With this mode enabled, the alarm center will automatically obtain the IP address from a DHCP server. In this mode, the alarm center may take a few seconds to make the connection(s) with the monitoring servers (IP1/IP2). If there is no *online* DHCP server, the alarm center will not be able to establish connections with the monitoring servers (on = enabled, off = disabled).

To program / activate the DHCP, type:



Use key 1 on the keyboard to enable the DHCP of the alarm center, so that number 1 remains marked to enable and unmarked to disable the DHCP and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: ADSL modems, for the most part, have the DHCP feature and to activate it, consult your equipment manual.

Network mask (connection by cable)

To view/edit the network mask of the alarm center, type:

Enter + 8130 + Enter

The current network mask will be shown, being the factory default 255.255.255.000, to insert/change the mask, type the new programming and press *Enter* key to confirm the programming. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: the DHCP option must be disabled for change.

Gateway (connection by cable)

To view/edit the gateway, type:

Enter + 8140 + Enter

The current gateway will be shown, being the factory default 192.168.001.001, to insert/change the gateway, type the new programming and press *Enter* key to confirm the programming; If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

IP Address of the alarm center (Wi-Fi connection)

IP Address of the local network where the alarm center is connected. To view / edit the alarm center IP address, simply perform the following procedure:

1. To program/change the IP address of the alarm center, type:

Enter + 8620 + Enter

2. The current address will be shown, being the factory default 192.168.001.100, to insert/change the address, type the new programming and press *Enter* key to confirm the programming;
3. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: the DHCP option that is shown below must be disabled to manually change the IP of the alarm center.

DHCP (Wi-Fi connection)

With this mode enabled, the alarm center will automatically obtain the IP address from a DHCP server. In this mode, the alarm center may take a few seconds to make the connection(s) with the monitoring servers (IP1/IP2). If there is no online DHCP server, the alarm center will not be able to establish connections with the monitoring servers (on = enabled, off = disabled).

To program / activate the DHCP, type:

Enter + 831 + Enter

Use key 1 on the keyboard to enable the DHCP of the alarm center, so that number 1 remains marked to enable and unmarked to disable the DHCP and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: ADSL modems, for the most part, have the DHCP feature and to activate it, consult your equipment manual.

Network mask (Wi-Fi connection)

To view/edit the network mask of the alarm center, type:

Enter + 8630 + Enter

The current network mask will be shown, being the factory default 255.255.255.000, to insert/change the mask, type the new programming and press *Enter* key to confirm the programming. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Obs.: the DHCP option must be disabled for change.

Gateway (Wi-Fi connection)

To view/edit the gateway, type:

Enter + 8640 + Enter

The current gateway will be shown, being the factory default 192.168.001.001, to insert/change the gateway, type the new programming and press *Enter* key to confirm the programming; If you only want to view the configuration, press the *Back* or *Exit* key and no programming will be changed

Ethernet Heartbeat interval (link test)

To check if the communication between the alarm center and the Intelbras Receiver IP software is working, the alarm center will send a message (known as Heartbeat or Keep alive) according to the programmed time interval. If the Intelbras IP Receiver does not receive this message within the programmed time interval, a fault event may be generated.

To program this function, type:

Enter + 816 + Interval + Enter
001 to 255 minutes

To edit/view the programmed value, type:

Enter + 816 + Enter

After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: in order to minimize network traffic, a time greater than 2 minutes is recommended for each test interval, and the factory default is 5 minutes.

Enable/disable Ethernet keep alive event (link test)

With this function enabled, the control panel monitors the Ethernet connection link with monitoring servers 1 and 2, and with the cloud. If enabled, the control panel will monitor the connection and generate ETH Keep Alive Failure and Restoration events. Otherwise, if disabled, the control panel will not monitor and will not generate the events.

To program/activate the Ethernet Keep Alive event, type:

Enter + 831 + Enter

Use key 5 on the keyboard to enable the Ethernet keep alive event on the control panel, so that the number 5 remains marked to enable and unmarked to disable, and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Note: the event will be generated 1 minute after the time defined in the Ethernet Heartbeat Interval (link test) command.

Example: if the link test interval is set to 5 minutes, the event will be generated 6 minutes after the failure is detected.

The following events will be reported:

Device	Event	Default code	Index (Zone/User)
IP 1 Eth	Keep Alive Eth Failure	361	001
IP 2 Eth			002
Cloud			003

Note: function available from version 3.0.5

Monitoring via GPRS (General Packet Radio Service) connection.

The alarm centers have connections to report events and be accessed/controlled remotely through the 2G/3G/4G cellular network, for this it is necessary to install the XG 2G, XG 3G or XG 4G module together with the AMT 8000 LITE and AMT 8000 PRO alarm centers.

To carry out communications via 2G/3G, the chip (SIM card) must be enabled for a plan with a data package. It is not necessary to enable the voice service. Consult the operator to acquire the most suitable plan for the traffic of information from the alarm center.

To be able to establish the connection, the following configurations must be carried out.

Shipping chip options and operation method

It is necessary to enable the chips installed in the alarm center to be used.

- » **Chip 1:** enables the use of the chip allocated in slot/position 1 on the XG 2G / XG 3G module. If no chip is enabled, the alarm center does not proceed with the connection to the operator's network.
- » **Chip 2:** enables the use of the chip allocated in slot/position 2 on the XG 2G / XG 3G module. If no chip is enabled, the alarm center does not proceed with the connection to the operator's network.

Use the following table to disable/enable alarm center configurations.

Key 1	Chip 1
Key 2	Chip 2

Use keys 1 and 2 on the keyboard to enable the chip and method options, so that the corresponding numbers, who wish to have the function enabled, remain marked on the display and then confirm with the *Enter* key. If you only want to view the configuration, press the Back/Exit key and no programming will be changed.

Login

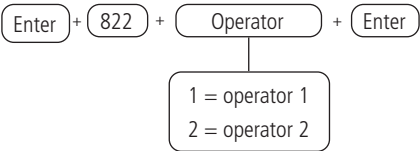
Login for connection in the 2G/3G network of the operator used. This field accepts letters and numbers and can contain up to 16 digits.

The default logins for some operators are listed below.

Operator	Login
TIM	tim
Claro	claro
Vivo	vivo
Oi	oi

Obs.: this information can be changed with no prior notice. For further information, consult the operator used in order to insert the right login.

To program this function, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Password

Password for 2G/3G connection in the network of the operator used. This field accepts letters and numbers and can contain up to 16 digits.

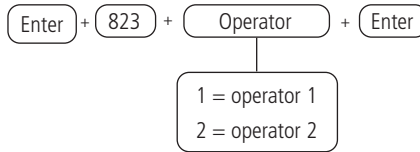
The default passwords for some operators are listed below.

Operator	Login
TIM	tim
Claro	claro

Vivo	vivo
Oi	oi

Obs.: this information can be changed with no prior notice. For further information, consult the operator used in order to insert the right password.

To program this function, type:



After the command, type the password (in accordance with the operator used) and then press the *Enter* key to confirm. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

APN - Access Point Name

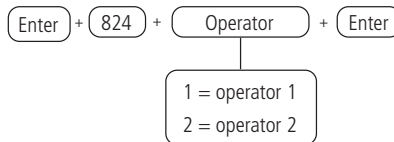
The APN is the name used to identify a GPRS service in the GSM mobile network. It defines the type of service that is provided in the data connection package. This field accepts letters and numbers and can contain up to 34 digits.

The default APNs for some operators are listed below.

Operator	APN
TIM	tim.br
Claro	generica.claro.com.br or claro.com.br
Vivo	zap.vivo.com.br
Oi	gprs.oi.com.br

Obs.: this information can be changed with no prior notice. For further information, consult the operator used in order to use the right APN.

To program this function, type:



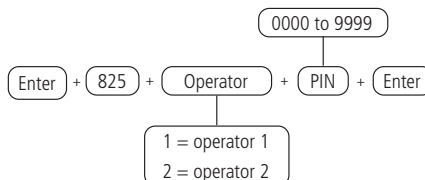
After the command, type the APN (in accordance with the operator used) and then press the *Enter* key to confirm. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

PIN (Personal Identification Number)

PIN is a chip identification, and if it is incorrect the chip will be blocked. If the PIN of the chip used is enabled, it will be necessary to inform it through the programming mode of the alarm center. As it is a password-type field, the visualization of its content on the LCD display is blocked.

It is also possible to configure the PIN code and permanently record it on the chip using a cell phone. In this case, the alarm center will not use this field, as the chip will already be released. Special attention is recommended for this option, as the chip will be able to establish Internet connections in any equipment that uses cellular technology.

To program, type:



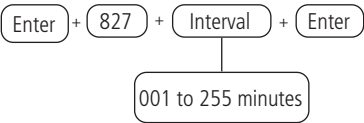
Obs.: to unlock a SIM card if you do not have access to the PIN, it must be inserted into a cell phone and the PUK code configured. If you do not have this code (or other codes such as PIN2 and PUK2), consult the operator of the chip used for further information.

GPRS Heartbeat interval (link test)

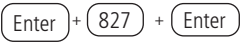
With the same function as the Ethernet Heartbeat Interval (link test), but relative to the GPRS channel.

To check if the communication between the alarm center and the Intelbras Receiver IP software is working, the alarm center sends a message (known as Heartbeat or Keep alive) according to the programmed time interval. If the Intelbras IP Receiver does not receive this message within the programmed time interval, a fault event may be generated.

To edit the link test interval, type:



To edit/view the programmed value, type:



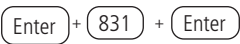
After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

Obs.: in order to minimize excessive data consumption, a time greater than 2 minutes is recommended for each test interval, and the factory default is 5 minutes.

Enable/disable GPRS keep alive event (link test)

With this function enabled, the control panel monitors the GPRS connection link with monitoring servers 1 and 2, and with the cloud. If enabled, the control panel will monitor the connection and generate GPRS Keep Alive Failure and Restoration events. Otherwise, if disabled, the control panel will not monitor and will not generate the events.

To program/activate the GPRS Keep Alive event, type:



Use key 6 on the keyboard to enable the GPRS keep alive event of the control panel, so that the number 6 remains marked to enable and unmarked to disable, and then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Note: the event will be generated 1 minute after the time defined in the *GPRS Heartbeat Interval (link test)* command.

Example: if the link test interval is set to 5 minutes, the event will be generated 6 minutes after the failure is detected.

The following events will be reported:

Device	Event	Default code	Index (Zone/User)
GPRS IP 1	GPRS Keep Alive Failure	360	001
GPRS IP 2			002
Cloud			003

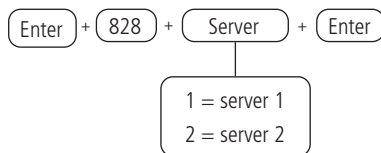
Note: function available from version 3.0.5

DNS Servers for GPRS

With the same function as DNS Servers for Ethernet, but relative to the GPRS channel.

If 000.000.000.000 or 255.255.255.255 is programmed, the cellular modem will automatically try to use the DNS provided by the operator.

To program/change the IP of the DNS servers type:



After inserting the command, type the DNS server code (in accordance with the server used) and then press the *Enter* key to confirm.

Obs.: the addresses suggested in the section, additional values can be charged by the service provider for use of communication ports, thus their availability and release / configuration costs must be consulted can be used, however it is recommended to use the addresses provided by the operator of the chip used.

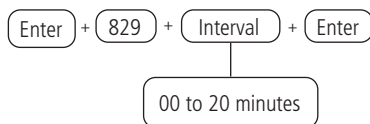
Interval between GPRS connection attempts

When there is a failure in the cellular modem connection (XG 2G, XG 3G or XG 4G) with the Intelbras IP Receiver software, the alarm center tries to make a new connection with it. This function will define the time between these attempts and it leaves the factory at zero (00 minutes).

This resource is mainly applied in installations that use prepaid plans and is intended to reduce the consumption of credits in constant situations of connection failures, unavailability of services by the operator or the Intelbras IP Receiver software (e.g. offline software).

Obs.: if you want connection attempts to be established without waiting time, program the value 00 (ZERO).

To program, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed.

Cloud Connection

The switchboard is already directed to Intelbras Cloud, initially using the random remote access password indicated together on the QR Code label that also contains the MAC.

To disable/enable the Cloud connection, type:

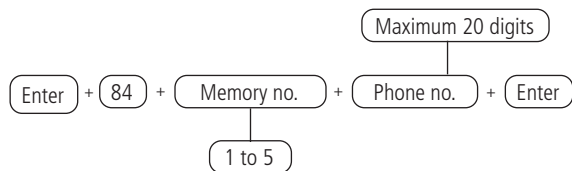


Use the 6 key on the keyboard to enable or disable the Cloud connection of the alarm center, so that the number 6 remains marked to disable and unmarked to enable the Cloud connection, then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Phone for GSM calls

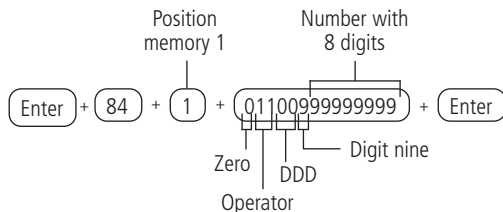
Configures the cell phone numbers that will receive calls via GSM from the alarm center (XG 2G, XG 3G or XG 4G module required). The alarm center has 5 (five) memory locations for registering telephone numbers. In case of trigger or activation of the Panic function, the alarm center will call the programmed numbers and emit the sound of a siren for approximately 50 seconds. This process is repeated twice.

To program this function, type:

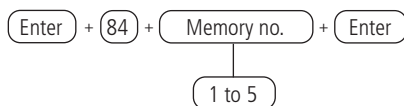


Obs.: enter the phone number to be programmed, starting with the operator, then the area code and finally the number always starting with the digit 9 (nine) – if it is a cell phone – followed by 8 (eight) more numbers.

Example:

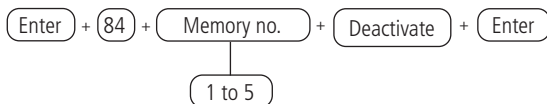


To edit/view the programmed telephones, type:



After changing the configured value, press the *Enter* key. To delete the registered number, press the Exit key until all digits are erased and then press the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

To exclude the programmed telephones, type:



6.20. Activation/deactivation of functions

The AMT 8000 LITE and AMT 8000 PRO alarm centers have several functions that can be activated or deactivated according to the needs of each installation. These functions are divided into 6 groups:

- » General configurations 1
- » General configurations 2
- » Blocks
- » General configurations 3
- » Events that generate triggers
- » Monitoring

General configurations 1

The parameters configured in this group of functions are described below:

- » **Partitioning:** with this resource, the alarm center can be divided as if there were up to 16 independent systems. For further information, consult section *Program the partitioning of the alarm center*.
- » **Activation through a key:** If this function is activated, it is possible to activate the system when pressing the Activate key for 3 seconds. All partitions will be activated in case of partitioned alarm center, if a common keyboard is used, and in the case of keyboard with permission in a specific partition, only this partition will be activated.

Obs.: this command does not permit the alarm center to be deactivated. For further information consult *Keyboard partition*.

- » **Siren beep during activation / deactivation:** activates / deactivates the beep emitted by the siren during activation / deactivation of the alarm center. During activation, the siren will emit a short beep and during deactivation, the siren will emit short beeps. If a problem is detected and the *Siren Problem Indication* function is enabled, a long beep will be emitted on activation and two long beeps on deactivation.
- » **Activation with open zones:** in the factory setting it is only possible to activate the system if all activated zones are closed. With this function enabled, the system can be active even if some zone is open. In this case, all zones must be closed when the exit timing ends so that a trigger does not occur.
- » **Password with 6 digits:** Increases the number of digits in the password from 4 to 6. The passwords programmed before the function was enabled remain the same and 00 must be typed at the end to complete the 6 digits of the password before being changed. While this function is enabled, the system will only accept the programming of 6-digit passwords.
- » **Remote control clean trigger:** allows the memorization of the triggers that occurred to be cleared even when the system is activated by remote control.

To program this function, type:

(Enter) + (510) + (Enter)

Key	Function
1	Partitioning
2	Activation through a key
3	Siren beep on activation/deactivation
4	Activation with open zones
5	Password with 6 digits
6	N/A
7	N/A
8	Trigger clean remote control

Use the keyboard keys to define the status of the function, so that the referring numbers, who wish to have the function active, remain marked and the functions that should remain inactive remain unmarked, then confirm with the *Enter* key.

General configurations 2

The parameters configured in this group of functions are described below:

- » **Silent panic by key 0:** if key 0 is pressed for 3 seconds, the siren will remain off and the event of *Silent Panic* will be reported to the monitoring company.
- » **Audible panic by key 2:** when activated, if key 2 is pressed for 3 seconds, the siren will be activated and the event of *Audible panic* will be reported to the monitoring company.
- » **Medical Emergency via key 5:** if key 5 is pressed for 3 seconds, the Medical Emergency event will be reported to the monitoring company and the siren will emit intermittent beeps lasting 1 second and a 6 second interval between beeps.
- » **Fire panic by key 8:** if key 8 is pressed for 3 seconds, the *Fire* event will be sent to the monitoring company and the siren will sound intermittently.
- » **Maintenance request via the Enter key:** by enabling this function, the user will be able to request equipment maintenance by pressing the *Enter* key for 3 seconds, eliminating the need to call the monitoring company/system installer.
- » **Trouble indication by siren:** if the functions *Indication of problems by siren on activation/deactivation* and *Siren beep on activation/deactivation* are enabled and if a problem is detected, a long beep will be emitted on activation and two long beeps on deactivation.
- » **Automatic cancellation due to zone opening:** in normal operation, the *Automatic zone cancellation* function works taking into account the number of triggers of the siren. With this function enabled, the cancellation becomes the number of times the zone is opened.

To program this function, type:

(Enter) + (511) + (Enter)

Key	Function
1	Silent panic through key 0
2	Audible panic through key 2
3	Medical emergency through key 5
4	Fire by key 8
5	Maintenance order by Enter key

6	N/A
7	Problem indication by siren
8	Automatic cancellation due to opening of zone

Use the keyboard keys to define the status of the function, so that the referring numbers, who wish to have the function active, remain marked and the functions that should remain inactive remain unmarked, then confirm with the *Enter* key.

Blocks

The parameters configured in this group of functions are described below:

- » **Reset blocking:** with this function active, all forms of reset are blocked.
- » **Remote control blocking:** all remote controls will be blocked and the activation/deactivation of the system can only be done through a password.
- » **Keyboard lock in case of incorrect password:** If an incorrect password is entered 4 times, the keyboard will be locked for 10 minutes and the incorrect password event will be sent to the monitoring company. If the function is disabled, the event will be sent, but the keyboard will continue to function normally.
- » **Blocking of the synchronism button for registration of wireless devices:** with this function active, it will not be possible to register wireless devices using the synchronism button, however, registration can still be performed via programming using the XAT 8000 keyboard, software or App. The other functions associated with this key continued to function normally.

To program this function, type:

(Enter) + (512) + (Enter)

Key	Function
1	Reset blocking
2	Remote control blocking
3	Keyboard lock in case of incorrect password
4	Blocking of the synchronism button for registration of wireless devices

Use the keyboard keys to define the status of the function, so that the referring numbers, who wish to have the function active, remain marked and the functions that should remain inactive remain unmarked, then confirm with the *Enter* key.

General configurations 3

The parameters configured in this group of functions are described below:

- » **Alarm control panel tamper:** when activated, the control panel generates a tamper fault in case of violation of the same and the wind is generated and, if programmed, it will trigger the siren, even if the system is deactivated (see section Problems that generate trigger).

To program this function, type:

(Enter) + (513) + (Enter)

Key	Function
Key 1	Alarm center tamper

Use key 1 on the keyboard to enable the control panel function, so that the number 1 remains marked to enable and unmarked to disable, then confirm with the *Enter* key. If you only want to view the configuration, press the *Back/Exit* key and no programming will be changed.

Monitoring

The parameters configured in this group of functions are described below:

- » **Real-time reporting:** In *Standard* mode, when a trigger in a zone occurs, the alarm center will send the trigger event only once to the monitoring company and send the trigger event stopped only when the system is deactivated. If real-time reporting is enabled, the alarm center will send the trigger and ceased trigger events, whenever the zone is opened or closed while the system is activated.
- » **Disables exit time beep:** this option will disable the beep that the keyboard emits during exit (after entering the password).

To program this function, type:

Enter + 514 + Enter

Key	Function
1	N/A
2	N/A
3	Real time reporting
4	N/A
5	N/A
6	N/A
7	N/A
8	Disables exit time beep

Use the keyboard keys to define the status of the function, so that the referring numbers, who wish to have the function active, remain marked and the functions that should remain inactive remain unmarked.

Problems that generate trigger

With this function enabled, sirens will go off if at least one of the following events is detected: supervision failure, device tampering, in addition to system intrusions. With the function disabled, only the corresponding event will be generated, but the siren remains off.

- » **Supervision fault:** the system has communication supervision with all wireless devices with the alarm center, and with the function active, the system will generate a fault if any of the devices loses communication.

When a supervision failure occurs, the sectors will be opened immediately if the partition is deactivated, if it is activated, the supervision failure event will be generated and the status of the sector will change to open, as soon as the partition is deactivated.

Obs.: the wireless devices of the 8000 line have a fixed device supervision time of 60 minutes and this time cannot be changed. During this time, if there is no communication with the alarm center, it will generate a Supervision failure.

- » **Tamper of wireless devices:** for all devices that have a tamper against removal from the installation site or opening them, and when the function is active (factory default activated), the system will generate a fault if any of the devices is violated.
- » **Do not generate trips:** if the function is enabled (factory default *deactivated*), even if the system is active, no fault trips will be generated.

To program this function, type:

Enter + 515 + Enter

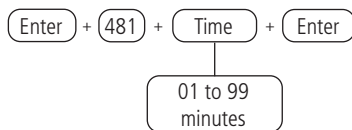
Key	Function
Key 1	N/A
Key 2	Supervision failure
Key 3	N/A
Key 4	N/A
Key 5	Tamper of devices
Key 6	Do not generate triggers

Use the keyboard keys to define the status of the function, so that the referring numbers, who wish to have the function active, remain marked and the functions that should remain inactive remain unmarked, then confirm with the *Enter* key.

6.21. Time for sending of AC failure

As soon as a failure in the electrical network is detected, the alarm center will wait for the programmed time to generate the corresponding event. If during this time the electrical grid is restored, no event will be generated. This time leaves the factory programmed for 1 minute and can be changed for up to 99 minutes.

To program this function, type:



To edit/view the programmed value, type:



After changing the configured value, press the *Enter* key. If you only want to view the configuration, press the *Exit* key and no programming will be changed

6.22. System reset

There are two types of reset, one temporary by hardware, and the other permanent by software (by programming mode). The *Temporary Reset* restarts the installer password to 9090 and the master password to 1234 for 1 minute, without erasing any programming made. The *Reset by programming mode*, in addition to returning the installer and master passwords (see topic 6.10. *Passwords*) to the factory defaults, it also erases all secondary passwords and all programming carried out.

If the *Reset Blocking* is activated, it will not be possible to perform a *System Reset* (see item 6.18. *Activation/deactivation of functions*).

Temporary reset of master and installer password

If you have forgotten the master password or the installer password, it will not be possible to enter the programming mode and access the alarm center settings/operations. If this occurs, there is a temporary reset for these passwords following this step:

1. With the alarm center on, press the wireless device registration key for approximately 15 seconds, when the LED flashes again, the alarm center will enter into temporary reset mode for 1 minute. During this time the master password will revert to 1234 and the installer password to 9090.

During this period, it will be possible to enter the programming mode and change the master password and/or the installer password (see topic 6.10. *Passwords*). If nothing is done during this period, the passwords will return to the same previously programmed values.

Reset by programming mode

The *Reset via programming mode*, erases all programming carried out on your alarm center and cancels the reporting of pending events.

To program this function, type:



Obs.: this command does not delete the wireless devices registered in the alarm center or the editable messages.

If you want to perform a single command to erase all the alarm center configurations, including registered wireless devices and editable messages, type:



Attention: this command will make the alarm center return to the factory default, so even the keyboard used to execute the command will lose its registration, and all programming must be redone.

6.23. Programming quick reference

This quick reference assumes that the alarm center is in programming mode and presupposes reading the complete manual and knowing the result of each function.

Enter in programming mode

When pressing the *Enter* key on the initial screen, the message *Prog. password* will be displayed, indicating that the alarm center is waiting for the entry of the master password or the installer password.

Provisioning

Enable provisioning by synchronism button

Press the wireless device registration key for 7 seconds, the LED will start flashing quickly to indicate that the alarm center is in provisioning mode and this mode will remain for 5 minutes, if not performed. access to the alarm center it will cancel provisioning and return to normal operation, if there is a connection to the alarm center it will remain in provisioning mode until the remote connection is terminated by the user.

Enable provisioning by keyboard

Enter + **855** + **Enter**

If you want to cancel the provisioning by keyboard mode, press the *Exit* key.

Wireless devices

Attention!

If during the wireless device registration process the LED of the device flashes red, press the synchronization button of the device for 15 seconds (for the XAC 8000, keep the top 2 buttons pressed) and restart the registration process.

Registration by synchronization key

Press and release the alarm center synchronization button, LED 3 will remain lit continuously, indicating that the alarm center is ready for registration of wireless devices. When completing the registration of all devices, press again the synchronization key on the alarm center and check if LED 3 has left Continuous mode (flashes indicating its normal operation), showing that the alarm center has left the wireless device registration mode.

With the function active on the alarm center, press the synchronization key for each device, the synchronization will be sequential, respecting the maximum limit for each device. For remote control just press any of its keys.

Maximum capacity of devices

- » Wireless keyboards 16
- » Remote controls 98
- » Wireless sensors 64
- » Wireless sirens 16
- » Wireless actuator 16
- » RF Repeater 4

Keyboard commands for wireless devices

» **Keyboard**

» **Change system language**

Enter + **854** + **I** + **Enter**

- » I = 0: Portuguese
- » I = 1: Spanish
- » I = 2: English

Obs.: functionality available from version 1.0.1 of the XAT 8000 keyboard.

» **Register wireless keyboard**

Enter + 620 + NT + *Enter* + Activate the keyboard by pressing the synchronization key

NT = keyboard number from 01 to 16.

» **Turn off wireless keyboards**

Enter + 720 + NT + *Enter*

NT = keyboard number from 01 to 16.

» **Partition of wireless keyboards**

Enter + 223 + NT + PP + *Enter*

NT = keyboard address from 01 to 16.

PP = Partition from 00 to 16 (00 = common keyboard, that is, the keyboard will have permission of access to all partitions of the alarm center).

» **Change messages**

Enter + GM + Activates + (User, device, partition or zone) + *Enter*

GM = group of messages from 1 to 8.

User, device, partition or zone = in the case of messages for zone 1 to 64, device from 01 to 16, partition from 01 to 16 and in the case of user from 00 to 99.

Description	Message group	User, device, partition or zone
Alarm center name	1	00
Users	2	00 to 99
Zones	3	01 to 64
Partitions	4	01 to 16
Keyboards	6	01 to 16
Sirens	8	01 to 16

» **Reset messages**

Enter + 1 + Deactivate + Enter

Obs.: returns all messages from the alarm center to the factory default according to the selected language.

» **Panic Key**

Enter + 540 + P + Enter

- » **P=0:** Disabled
- » **P=1:** Audible panic
- » **P=2:** Silent panic
- » **P=3:** Fire panic
- » **P=4:** Medical emergency

» **Remote control**

» **Register remote control**

Enter + 60 + NU + Enter + Activate the control by pressing one of the keys

NU = user number from 00 to 97.

» **Turn off remote control**

Enter + 70 + NU + Enter

NU = user number from 00 to 97.

» **Remote control firmware check**

Enter + 645 + CC + Enter

CC = Remote control number with 2 digits

» **Remote control key functions**

Enter + 65 + T + NU + FC + Enter

T = Control key from 1 to 3.

NU = user number from 00 to 97.

FC = function from 00 to 66 that will be linked to the selected control key (1 to 3).

00	Disabled
01	Activate / Deactivate all partitions
02	Activate only all partitions
03	Deactivate only all partitions
04	Activate / Deactivate all partitions in <i>Partial</i> mode
05	Only assemble in <i>Partial</i> mode
06	Panic with siren
07	Silent panic
08	Fire panic
09	Medical emergency
10	N/A
11	Activate / Deactivate Partition 1 only
12	Activate / Deactivate Partition 2 only
13	Activate / Deactivate Partition 3 only
14	Activate / Deactivate Partition 4 only
15	Activate / Deactivate Partition 5 only

16	Activate / Deactivate Partition 6 only
17	Activate / Deactivate Partition 7 only
18	Activate / Deactivate Partition 8 only
19	Activate / Deactivate Partition 9 only
20	Activate / Deactivate Partition 10 only
21	Activate / Deactivate Partition 11 only
22	Activate / Deactivate Partition 12 only
23	Activate / Deactivate Partition 13 only
24	Activate / Deactivate Partition 14 only
25	Activate / Deactivate Partition 15 only
26	Activate / Deactivate Partition 16 only
27	N/A
28	N/A
29	N/A
30	N/A
31	Activate / Deactivate Partial mode Partition 1 only
32	Activate / Deactivate Partial mode Partition 2 only
33	Activate / Deactivate Partial mode Partition 3 only
34	Activate / Deactivate Partial mode Partition 4 only
35	Activate / Deactivate Partial mode Partition 5 only
36	Activate / Deactivate Partial mode Partition 6 only
37	Activate / Deactivate Partial mode Partition 7 only
38	Activate / Deactivate Partial mode Partition 8 only
39	Activate / Deactivate Partial mode Partition 9 only
40	Activate / Deactivate Partial mode Partition 10 only
41	Activate / Deactivate Partial mode Partition 11 only
42	Activate / Deactivate Partial mode Partition 12 only
43	Activate / Deactivate Partial mode Partition 13 only
44	Activate / Deactivate Partial mode Partition 14 only
45	Activate / Deactivate Partial mode Partition 15 only
46	Activate / Deactivate Partial mode Partition 16 only
51	PGM 01
52	PGM 02
53	PGM 03
54	PGM 04
55	PGM 05
56	PGM 06
57	PGM 07
58	PGM 08
59	PGM 09
60	PGM 10
61	PGM 11
62	PGM 12
63	PGM 13
64	PGM 14
65	PGM 15
66	PGM 16

» Wireless sensors

» Register wireless sensors

Enter + 61 + ZZ + Enter + Activate the sensor by pressing the synchronization key
ZZ = zone to which the sensor from 01 to 64 will be linked.

» Turn off wireless sensors

Enter + 71 + ZZ + Enter

ZZ = zone to which the sensor from 01 to 64 will be unlinked.

» **Adjustment of wireless infrared sensors**

Attention: settings available for devices with firmware version lower than 3.0.0. For equal or higher versions consult the device manual for more information.

Enter + 66 + ZZ + S + L + M + Enter

ZZ = zone from 01 to 64

S = Sensitivity from 0 to 3, where 0 = Minimum Sensitivity / 1 = Normal Sensitivity / 2 = Intermediate Sensitivity / 3 = Maximum Sensitivity Maximum.

L = Sensor LED, where 0 = Off / 1 = On

M = Operation mode of the sensor, where 0 = Cost-saving / 1 = Continuous

Obs.: for the XAS 8000 and TX 8000 the Sensitivity, Sensor LED and Operation Mode settings are allowed by the alarm center, but only the LED configuration is accepted by XAS 8000 and by TX 8000.

» **Wireless sensor test**

Enter + 52 + Enter + Activate sensor

» **Disable tamper of the sensors**

Enter + 78 + X + Enter

X = Group zones 0 to 6

» **Disable digital tamper of IVP 8000 EX sensor**

Enter + 79 + X + Enter

X = Group zones 0 to 6

» **Restoration of the digital tamper of IVP 8000 EX sensor**

Enter + 543 + ZZ + Enter

ZZ = 2 digit zone number

» **Firmware visualization of the sensors**

Enter + 641 + ZZ + Enter

ZZ = 2 digit zone number

» **Integrated siren**

» **Enable/disable built-in siren**

Enter + 541 + Enter + tecla 1 + Enter

» **Enable/disable the built-in siren beep when activating/deactivating the system (Function available from version 3.0.6)**

Enter + 541 + Enter + 2 + Enter

» **Ajuste do volume da sirene integrada na ativação/desativação e disparos do sistema (função disponível a partir da versão 3.2.4)**

Enter + 541 + Enter + 3 + Enter

» **Wireless sirens**

» **Register wireless sirens**

Enter + 621 + NS + Enter + Activate the siren by pressing the synchronization key

NS = siren number from 01 to 16.

» **Turn off wireless sirens**

Enter + 721 + NS + Enter

NS = siren number from 01 to 16.

» **Siren firmware check**

Enter + 643 + SS + Enter

SS = Siren Number with 2 digits

» **Partition of wireless sirens**

Enter + 222 + NS + PP + Enter

NS = siren number from 01 to 16.

PP = Partition from 01 to 16 (00 = common address for all zones and 01 to 16 individual partitions of the alarm center).

» **Enable / disable the siren beep in system activation/deactivation**

Enter + 510 + Enter + Key 3 + Enter

» **Enable / Disable the siren beep by partition**

Enter + 224 + GP + Enter

GP = partition group, with partitions from 01 to 10 in group 0 and partitions from 11 to 16 in group 1.

» **Change siren time**

Enter + 41 + TS + Enter

TS = siren time from 01 to 99.

Obs.: factory default 5 minutes, and if 00 is placed in the command, error beep will be emitted.

» **Register Range RF Amplifier (REP 8000 repeater)**

Enter + 622 + NA + Enter + Activate the amplifier by pressing the synchronization key

NA = amplifier number from 01 to 04.

» **Turn off Range RF Amplifier (REP 8000 repeater)**

Enter + 722 + NA + Enter

NA = amplifier number from 01 to 04.

» **Repeater firmware check**

Enter + 644 + RR + Enter

RR = Repeater number with 2 digits

» **Register PGM 8000 Actuator**

Enter + 623 + NA + Enter + Activate the Actuator by pressing the synchronization key

NA = Actuator number from 01 to 16.

» **Turn off PGM 8000 Actuator**

Enter + 723 + NA + Enter

NA = Actuator number from 01 to 16.

» **PGM 8000 actuator firmware check**

Enter + 646 + PP + Enter

PP = 2 digit PGM number

» **PGM 8000 Actuator functions**

Enter + 50 + PGM + Enter + M + E + Enter

PGM = PGM number from 01 to 16.

M = mode of operation of PGM from 0 to 9 (0 = on/off, 1 to 8 = pulse and 9 = programmed time)

E = Event that activates the PGM 00 a 13

00	External activation (applications)
01	Activation by password (passwords from 51 PGM01 to 66 PGM16)
02	System activation
03	System deactivation
04	Medical emergency:
05	Event communication failure
06	NA
07	Siren problem
08	Trigger
09	Silent trigger or panic
10	Fire zone trigger
11	Opening of zone 1
12	Remote control
13	Activation/deactivation by time
14	Open door actuation

» **Programmed time for PGM 800 is activated**

Enter + 560 + PGM + T + Enter

PGM = PGM number from 01 to 16.

T = time from 01 to 99 minutes

» **Days for Scheduled Automatic Activation of PGM 8000 Actuator**

Enter + 836 + PGM + Enter

PGM = PGM number from 01 to 16.

After the command, using the keyboard keys, select the days of the week from 1 to 7, where 1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday and 8 = holiday and confirm with *Enter* key.

» **Time for Automatic Activation of PGM 8000 Actuator**

Enter + 561 + PGM + D + HH + MM + Enter

PGM = PGM number from 01 to 16.

D = day of the week from 1 to 7 (1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday and 8 for holidays).

HH = hours from 00 to 23

MM = minutes from 00 to 59

» **Days for Scheduled Automatic deactivation of PGM 8000 Actuator**

Enter + 837 + PGM + Enter

PGM = PGM number from 01 to 16.

After the command, using the keyboard keys, select the days of the week from 1 to 7, where 1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday and 8 = holiday and confirm with *Enter* key.

» **Time for Automatic deactivation of PGM 8000 Actuator**

Enter + 562 + PGM + D + HH + MM + Enter

PGM = PGM number from 01 to 16.

D = day of the week from 1 to 7 (1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday and 8 for holidays).

HH = hours from 00 to 23

MM = minutes from 00 to 59

» **Holidays for Automatic activation / automatic deactivation of PGM 8000 Actuator**

Enter + 564 + PGM + F + DD + MM + Enter

PGM = PGM number from 01 to 16.

F = holiday memory number from 0 to 9

DD = day from 01 to 31.

MM = month from 01 to 12

» **Association of the PGM 8000 actuator to the partition**

Enter + 563 + PGM + PP + Enter

PGM = PGM number from 01 to 16.

PP = Partition from 01 to 16.

» **Reset wireless devices**

» **Turn off all registered wireless devices**

Enter + 7 + Deactivate + Enter

Obs.: all wireless devices will be unregistered from the alarm center, including the keyboard itself used.

RF channel change

Enter + 630 + RF + Enter

RF = channels from 08 to 11

Attention: when carrying out the change of the alarm center channel, all devices registered to it (except remote control) must have the synchronization key pressed to direct the device to the new channel, otherwise they will not communicate with the alarm center.

Remote update

» **To download/verify a new version**

Enter + 9922 + Enter

If there is a version for download, the information *Download Wait* will be displayed and it will start, which will take around 3 to 5 minutes (variable according to the connection used). If the alarm center does not have a version for download, the display will show the *Alarm center is already updated. If there is any problem on the network or Internet where the alarm center is connected, the message will be displayed: Download Failure.*

» Install the download version

Enter + 9933 + Enter

The new version that was downloaded will be installed and records and alarm center settings will not be lost. To check the control panel firmware version, access *Menu* and with the arrow keys click on *Alarm center version* to be displayed.

Note: the control panels must be connected to the internet via Ethernet / Wi-Fi or 4G. Software download/update is not possible via GPRS 2G and 3G connection due to the connection's download speed and excessive consumption of the data package used.

Attention: 4G update (XG 4G module required) is available from version 3.2.4. The update process may take about 1 hour and will be completed automatically - after the download is complete, the control panel applies the update without any user intervention.

Passwords

» Programming of passwords 1 (exclusive programming of programmer user)

» Change passwords of users of positions 98 and 99

Enter + 20 + NU + SENHA + Enter

NU = user number 98 or 99.

PASSWORD = password to be programmed containing 4 or 6 digits.

» Erase user password of position 98.

Enter + 20 + 98 + Enter

Obs.: the password of position 99 cannot be erased.

» Programming of passwords 2 (exclusive programming of Master user)

» Change/create passwords of users of positions 00 to 97

Enter + 20 + NU + SENHA + Enter

NU = user number from 00 to 97.

PASSWORD = password to be programmed containing 4 or 6 digits.

» Erase passwords of users of positions 01 to 97

Enter + 20 + NU + Enter

NU = user number from 01 to 97.

Obs.: the password of position 00 cannot be erased.

» Password permission

» Define permission for password partition

Enter + 21 + NU + GP + Enter

NU = user number from 01 to 96.

GP = partition group, with partitions from 01 to 10 in group 0 and partitions from 11 to 16 in group 1.

» Define permission to only Activate or permission to bypass

Enter + 2 + P + GS + Enter + Select password + Enter

P = definition of permission, 5 only active and 6 permission to bypass.

GS = password group from 0 to 9, with group 0 goes from 01 to 10, group 1 from 11 to 20 and so on, closing with group 9 from 91 to 97.

» Define permission for *Partial* mode

Enter + 221 + GS + Enter + Select password + Enter

GS = password group from 0 to 9, with group 0 goes from 01 to 10, group 1 from 11 to 20 and so on, closing with group 9 from 91 to 97.

Zone configurations

» Enable / disable zones

Enter + 30 + Enter

G = zone group from 0 to 6

After inserting the command, through the keyboard keys enable / disable the zones corresponding to the group and press the *Enter* key to confirm.

» **Enable *Partial* mode**

Enter + 02 + Enter

G = zone group from 0 to 6

After inserting the command, through the keyboard keys enable / disable the zones corresponding to the group and press the *Enter* key to confirm. It is also necessary that passwords have the permission for *Partial* mode.

» **Zone functions**

Enter + 3 + F + G + Enter

F = functions of zones from 1 to 6.

G = zone group from 0 to 6

After inserting the command, through the keyboard keys enable / disable the zones corresponding to the group and press the *Enter* key to confirm.

Zone functions	
1	Timed
2	Follower
3	000 to 24 hours
4	Panic
5	Medical emergency
6	Fire

» **Zone operating mode**

Enter + 0 + MP + G + Enter

MP = mode of zones 7 or 8.

G = zone group from 0 to 6

After inserting the command, through the keyboard keys enable / disable the zones corresponding to the group and press the *Enter* key to confirm.

MP	Mode of operation
7	Silent
8	Normally open contact

» **Automatic zone cancellation**

Enter + 53 + N + Enter

N = number of triggers from 0 to 9

Open Door Zone (from version 3.0.5)

Enter + 39 + G + Enter

G = group of zones from 0 to 6

Door open time (from version 3.0.5)

Enter + 45 + T + Enter

T = 000 to 999 minutes.

Entry on

Enter + 09 + ZZ + Enter

ZZ = zones from 01 to 64

Entry on partition

Enter + 516 + GP + Enter

GP = partition group, with partitions from 01 to 10 in group 0 and partitions from 11 to 16 in group 1.

Entry on activation and/or deactivation permission

Enter + 518 + Enter

Key 2 - Permission to activate

Key 3 - Permission to deactivate

Partitioning

» Enable partitioning

Enter + 510 + Enter + Select option 1 + Enter

» Zone partition

Enter + 01 + ZZ + PP + Enter

ZZ = zone from 01 to 64

PP = Partition from 01 to 16.

» Define permission for password partition

Enter + 21 + NU + GP + Enter

NU = user number from 01 to 96.

GP = partition group, with partitions from 01 to 10 in group 0 and partitions from 11 to 16 in group 1.

Attention: in addition to the aforementioned programming points, it is necessary that the user passwords are created / defined (topic *Passwords*), the registration of wireless controls for access (topic *Remote control*) and the definition of the partitioning of keyboards (topic *Keyboard*) and sirens (topic *Wireless sirens*).

Timings

» Input timing

Enter + 42 + PP + TTS + Enter

PP = partition from 01 to 16 (non-partitioned center, use PP = 01)

TTS = time from 00 to 255 seconds.

» Adjustment of the beep in entry timing

Enter + 542 + Volume adjustment + Enter

0 - Disabled

1 - Low

2 - Medium

3 - High

» Exit timing

Enter + 44 + PP + TTS + Enter

PP = partition from 01 to 16 (non-partitioned center, use PP = 01)

TTS = time from 00 to 255 seconds.

» Disable output beep

Enter + 514 + Enter + Key 8 + Enter

Alarm center time configurations

» Clock

Enter + 400 + HH + MM + SS + Enter

HH = hours from 00 to 23

MM = minutes from 00 to 59

SS = seconds from 00 to 59.

» Calendar

Enter + 401 + DD + MM + AA + Enter

DD = day from 01 to 31.

MM = month from 01 to 12

YY = year from 00 to 99.

» Adjustment of the day of the week

Enter + 402 + D + Enter

D = day of the week from 1 to 7 (1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday).

» **Time interval for synchronization of date and time**

Enter + 403 + HHH + Enter

HHH = interval between synchronizations from 000 to 255 hours.

» **Time zone**

Enter + 405 + FF + Enter

FF = Time zone 00 - Disabled

01 - GMT -1
02 - GMT -2
03 - GMT -3
04 - GMT -4
05 - GMT -5
06 - GMT -6
07 - GMT -7
08 - GMT -8
09 - GMT -9
10 - GMT -10
11 - GMT -11
12 - GMT -12
13 - GMT 0
14 - GMT +1
15 - GMT +2
16 - GMT +3
17 - GMT +4
18 - GMT +5
19 - GMT +6
20 - GMT +7
21 - GMT +8
22 - GMT +9
23 - GMT +10
24 - GMT +11
25 - GMT +12

Periodic test

» **Enable periodic testing by time**

Enter + 470 + HH + MM + Enter

HH = hours from 00 to 23

MM = minutes from 00 to 59

» **Disable periodic testing by time**

Enter + 470 + Deactivate + Enter

» **Periodic testing by time interval**

Enter + 471 + HHH + Enter

HHH = hours from 000 to 255

Automatic activation / automatic deactivation and Automatic activation / automatic deactivation by partition

» **Enable automatic activation due to inactivity**

Enter + 460 + TM + Enter

TM = time from 00 to 99 minutes.

» **Selection of automatic activation / automatic deactivation by partitions**

Enter + 464 + GP + Enter

GP = Group of partitions 0 or 1 (0 = group of partitions from 01 to 10 and 1 = group of partitions from 11 to 16).

» **Define holidays**

Enter + 404 + PP + F (0 to 9) + DD + MM + Enter
PP = partition (non-partitioned center, use PP = 01)
F = holiday memory number from 0 to 9
DD = day of the month that will be holiday from 01 to 31
MM = month of the holiday from 01 to 12

» **Day of the week for Automatic activation**

Enter + 838 + PP + Enter
PP = partition from 01 to 16 (non-partitioned center, use PP = 01)
After the command, using the keyboard keys, select the days of the week from 1 to 7, where 1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday.

» **Automatic Activation Time**

Enter + 462 + PP + D + HH + MM + Enter
PP = partition from 01 to (non-partitioned center, use PP = 01)
D = day of the week from 1 to 7 (1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday).
HH = hours from 00 to 23
MM = minutes from 00 to 59

» **Days of the week for Automatic deactivation**

Enter + 839 + PP + Enter
PP = partition from 01 to 16 (non-partitioned center, use PP = 01)
After the command, using the keyboard keys, select the days of the week from 1 to 7, where 1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday.

» **Automatic Deactivation Time**

Enter + 463 + PP + D + HH + MM + Enter
PP = partition from 01 to 16 (non-partitioned center, use PP = 01)
D = day of the week from 1 to 7 (1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday).
HH = hours from 00 to 23
MM = minutes from 00 to 59

» **Define holidays for Automatic Activation / Automatic Deactivation**

Enter + 404 + PP + F + DD + MM + Enter
PP = partition from 01 to 16 (non-partitioned center, use PP = 01)
F = holiday memory number from 0 to 9
DD = day from 01 to 31.
MM = month from 01 to 12

Configurations for monitoring

» **Wi-Fi Connection (function available only for AMT 8000 PRO)**

- » **Insert name of the network to be connected**
Enter + 850 + Enter + Insert name of the network + Enter
- » **Insert password of the network to be connected**
Enter + 851 + Enter + Insert password of the network + Enter
- » **Enable / disable Wi-Fi**
Obs.: the alarm center is connected only with 2.4 GHz routers.
Enter + 852 + Enter + TP + Enter
TP = type of configuration.

Selection	Type of configuration
0	Wi-Fi disabled
1	Wi-Fi enabled / in case of AC failure, operates on battery
2	Wi-Fi enabled / only with active AC network

» **Program monitoring account**

Enter + 15 + PP + Enter, where PP = partition from 01 to 16

After the command, type the monitoring account number with 4 digits and press the *Enter* key to confirm.

» **Monitoring via phone line (function available only for AMT 8000 PRO)**

» **Program telephone number for the monitoring company**

Enter + 10 + M + phone number of the monitoring company + Enter, where M = memory for telephone of 1 and 2

» **Turn off phone**

Enter + 10 + M + Deactivate + Enter

M = memory for telephone of 1 and 2

» **Telephone testing**

Enter + 11 + M + Enter

M = memory for telephone from 1 to 8

Obs.: *memory number 3 must not be used.*

» **End telephone testing**

Enter + 11 + Enter

» **Program number of attempts to report an event**

Enter + 13 + T + Enter, where T = number of attempts from 1 to 9

» **Program DTMF signal level**

If the factory standard DTMF level stored in the alarm center memory does not work, type the following command and test all options from 0 to 6 to check in which of them the best result is obtained.

Enter + 18 + N + Enter

N = number of attempts from 0 to 6

» **Event reporting mode**

Enter + 17 + AAA + Enter

AAA = indicates in which mode the alarm center will operate, where 000: deactivated, 400: regular IP/Phone and 600: dual IP/Phone.

» **System activation issue forwarding**

Enter + 519 + Enter + key 1 + Enter

» **Blocking of the sending from partition 00 to the monitoring company**

Enter + 515 + Enter

After the command, using the keyboard keys, enable option 8 (mark 8) and press the *Enter* key to confirm.

» **Reset of pending events**

Enter + 16 + Enter

» **Program communication priority**

Enter + 19 + P + Enter

P = communication priority from 0 to 3, where 0 = Ethernet, 1 = 2G/3G, 2 = Ethernet/2G/3G, 3 = 2G/3G/Ethernet.

» **Program destination IP**

Enter + 801 + I + Enter, where I = destination IP 1 or 2

After the command, type the IP number of the monitoring company you hired (example: 192.168.001.100) and press the *Enter* key to confirm.

» **Program IP network communication port**

Enter + 802 + P + Enter

P = port that will be used for the alarm center to connect, where 1 = port 1 and 2 = port 2.

After the command, insert the port number with 4 digits.

Obs.: *this field defines the port to which the alarm center will be connected, factory standard: 9009. Intelbras IP Receiver software must be configured to the same port.*

Important: the same port of another manufacturer must not be used for this communication, as there is a possibility of conflict.

» **Program destination domain name (DNS)**

If you do not want to use DNS move to the next command, otherwise, type it.

Enter + 803 + D + Enter, D = 1 or 2 (DNS 1 or DNS 2)

After the command, type the DNS domain name and press the *Enter* key to confirm.

» **Program monitoring options via IP**

Enter + 830 + Enter

After the command, using the keyboard keys, enable the desired option from 1 to 4, where:

- » **1:** enable the sending of events to the monitoring company 1
- » **2:** enable the sending of events to the monitoring company 2
- » **3:** enable the domain name (DNS) of monitoring company 1
- » **4:** enable the domain name (DNS) of monitoring company 2 and press the *Enter* key to confirm.

» **Program DHCP**

If you do not have a DHCP server or do not want to use this option, execute the next option, otherwise, type the following command and also the next ones.

Enter + 831 + Enter

After the command, using the keyboard keys, enable option 1 (mark 1) and press the *Enter* key to confirm.

» **IP Address of the alarm center (connection by cable)**

Enter + 8120 + Enter

After the command, insert the IP address for the alarm center.

Obs.: *it will only be possible to edit / insert the address manually if the DHCP function is disabled, otherwise only the IP address of the alarm center will be exhibited.*

» **Program the network mask (connection by cable)**

Enter + 8130 + Enter

After the command, type the network mask number and press the *Enter* key to confirm.

» **Program the gateway (connection by cable)**

Enter + 8140 + Enter

After the command, type the network Gateway number and press the *Enter* key to confirm.

» **Program the DNS servers for Ethernet (connection by cable)**

Enter + 815 + S + Enter, where S = 1 or 2 (Server 1 or Server 2)

After the command, type the DNS1 server number and press the *Enter* key to confirm.

» **IP address of the alarm center (Wi-Fi connection only for AMY 8000 PRO)**

Enter + 8620 + Enter

After the command, insert the IP address for the alarm center.

Obs.: *it will only be possible to edit / insert the address manually if the DHCP function is disabled, otherwise only the IP address of the alarm center will be exhibited.*

» **Program the network mask (Wi-Fi connection only for AMY 8000 PRO)**

Enter + 8630 + Enter

After the command, type the network mask number and press the *Enter* key to confirm.

» **Program the Gateway (Wi-Fi connection only for AMY 8000 PRO)**

Enter + 8640 + Enter

After the command, type the network Gateway number and press the *Enter* key to confirm.

» **Program the DNS servers for Ethernet (Wi-Fi connection only for AMY 8000 PRO)**

Enter + 865 + S + Enter, where S = 1 or 2 (Server 1 or Server 2)

» **Program the Heartbeat Ethernet interval (link test)**

Enter + 816 + TTM + Enter, where TTM = time interval varying from 000 to 225 minutes (factory standard 5 minutes)

» **Enable/disable Ethernet keep alive event (link test)**

Enter + 831 + Enter

After the command, using the keyboard keys, enable option 5 (marking 5) and press the *Enter* key to confirm.

Note: *function available from version 3.0.5*

» **Program login**

Enter + 822 + O + Enter, where O = 1 or 2 (operator 1 or operator 2)

After the command, type the login (in accordance with the operator used) and then press the *Enter* key to confirm.

» **Enable chips**

Enter + 832 + Enter

After the command, use the keyboard keys to enable options 1 (chip 1) and 2 (chip 2).

» **Program password**

Enter + 823 + O + Enter, where O = 1 or 2 (operator 1 or operator 2)

After the command, type the password (in accordance with the operator used) and then press the *Enter* key to confirm.

» **Program APN**

Enter + 824 + O + Enter, where O = 1 or 2 (operator 1 or operator 2)

After the command, type APN (in accordance with the operator used) and then press the *Enter* key to confirm.

» **Program the PIN (Personal Identification Number)**

If you want to use the PIN, perform the command in sequence, otherwise proceed with the next command.

If the PIN is incorrect, the chip will be blocked.

Enter + 825 + O + PIN Number with 4 digits + Enter, where O = 1 or 2 (operator 1 or operator 2)

» **GPRS Heartbeat interval (link test)**

Enter + 827 + TTM + Enter, where TTM = time interval of the Heartbeat from 000 to 255 minutes (standard 005 minutes)

» **Enable/disable GPRS keep alive event (link test)**

Enter + 831 + Enter

After the command, using the keyboard keys, enable option 6 (marking 6) and press the *Enter* key to confirm.

Note: function available from version 3.0.5

» **DNS Servers for GPRS**

Enter + 828 + S + Enter, where S = 1 or 2 (Server 1 or Server 2)

After inserting the command, type the DNS server code (in accordance with the server used) and then press the *Enter* key to confirm.

» **Interval between GPRS connection attempts**

Enter + 829 + TG + Enter, where TG = time interval of the reconnection attempts from 00 to 20 (default 00 minutes)

» **Cloud Connection**

Enter + 512 + Enter

After the command, use the 6 key on the keyboard to enable or disable the cloud connection and press the *Enter* key to confirm.

Program the phone for GSM calls

» **Program options of the GPRS channel to enable chips**

Enter + 832 + Enter

After the command, use the keyboard keys, to enable options 1 (chip 1) and 2 (chip 2) and press the *Enter* key to continue.

» **Phone for GSM calls**

Enter + 84 + M + Phone number with up to 20 digits + Enter, where M = memory number varying from 1 to 5

The phone number must have a maximum of 20 digits and must be in the format: 0 + operator code + area code + phone number starting with the digit 9.

Contact-ID codes

» **Enable / Disable events**

Note: this programming was removed from the keyboard starting with version 3.2.4 and is only available through the AMT Remote software or the AMT Remote Mobile app.

As it can be observed in the following commands, the event can be blocked if it is configured as 000 (it will not be sent to the Receiver IP) and enabled when registering FFF (it will be sent to the Receiver IP)

After inserting the command, insert the value 000 to disable or FFF to enable and press the *Enter* key to confirm.

» **Enable / Disable Contact-ID code for zone opening type events**

Enter + 901 + ZZ + Enter

ZZ = zone from 01 to 64

» **Enable / Disable Contact-ID code for zone restoration type events**

Enter + 911 + ZZ + Enter

ZZ = zone from 01 to 64

» **Enable / Disable Contact-ID code for tamper opening type events**

Enter + 902 + ZZ + Enter

ZZ = zone from 01 to 64

» **Enable / Disable Contact-ID code for tamper restoration type events**

Enter + 912 + ZZ + Enter

ZZ = zone from 01 to 64

» **Enable / Disable Contact-ID code for deactivation events by users**

Enter + 903 + NU + Enter

NU = user number from 01 to 97

» **Enable / Disable Contact-ID code for activation events by users**

Enter + 913 + NU + Enter

NU = user number from 01 to 97

» **Enable / Disable Contact-ID code for opening type system events**

Enter + 904 + II + Enter

II = system event index from 00 to 26

Opening type events System events		
Table of Contents	Internal event	Standard code
00	Low battery wireless device	384
01	N/A	
02	Supervision failure	147
03	Zone bypass	570
05	AC network failure	301
06	Low system battery	302
07	Battery absent	311
08	N/A	N/A
09	Remote deactivation	404
10	Automatic deactivation	403
11	N/A	
12	N/A	
13	System reset	305
14	Programming change	306
15	Failure when communicating event	354
16	Incorrect password	461
17	Remote access	410
18	Manual testing	601
19	Periodic test	602
20	Event buffer reset	621
21	Date and time restarted	625
22	Tamper of expander devices / Restoration tamper of expander devices	145
23	Tamper sensors / Restoration tamper sensors	383
24	Request for maintenance	616
25	AC failure wireless device	342
26	PGM activation	422

» **Configure Contact-ID code for restoration type system events, type:**

Enter + 914 + II + Enter

II = system event index from 00 to 26

Opening type events System events

Table of Contents	Internal event	Standard code
00	Restoration low battery wireless device	384
01	N/A	N/A
02	Restoration supervision failure	147
03	Restoration zone bypass	570
05	AC network restoration	301
06	Low system battery restoration	302
07	Battery restoration	311
08	N/A	N/A
09	Remote activation	404
10	Automatic activation	403
11	Activation through a key	408
12	Activation under filtration	121
13	N/A	N/A
14	N/A	N/A
15	N/A	N/A
16	N/A	N/A
17	N/A	N/A
18	N/A	N/A
19	N/A	N/A
20	N/A	N/A
21	N/A	N/A
22	Tamper of expander devices	145
23	Sensor tamper	383
24	N/A	N/A
25	AC failure wireless device	342
26	PGM activation	422

» Configure event code *Push*

Enter + 92 + EV + Enter + Select the event + Enter

EV = event group from 0 to 4, where group 0 is from 01 to 10 and so on, up to group 4 which is from 31 to 35.

Event group (EV)	Event	Key	Key
0	ARME_DESARME_USUARIO (Assemble_Disassemble_User),	Key 1	Enabled
	N/A	Key 2	Enabled
	DISPARO_ZONA (Trigger_Zone),	Key 3	Enabled
	DISPARO_24H (Trigger 24 hours)	Key 4	Enabled
	DISPARO_SILENCIOSO (Silent_Trigger),	Key 5	Enabled
	DISPARO_EMERGENCIA_MEDICA (Trigger_Medical_Emergency),	Key 6	Enabled
	DISPARO_INCENDIO (Trigger_Fire),	Key 7	Enabled
	DISPARO_PANICO_AUDIVEL (Trigger_Audible_Panic),	Key 8	Enabled
	DISPARO_PANICO_SILENCIOSO (Trigger_Silent_Panic),	Key 9	Enabled
	TAMPER_SENSOR,	Key 10	Enabled
1	BATERIA_BAIXA_SENSOR (Low_Battery_Sensor),	Key 1	Enabled
	N/A	Key 2	Enabled
	FALHA_SUPERVISAO_RF (RF_Supervision_Failure),	Key 3	Enabled
	BYPASS_ZONA (Zone_Bypass),	Key 4	Enabled
	BYPASS_AUTOMATICO (Automatic_Bypass),	Key 5	Enabled
	FALHA_REDE_ELETRICA (Electric_Grid_Failure),	Key 6	Enabled
	BATERIA_PRINCIPAL_BAIXA (Low_Main_Battery),	Key 7	Enabled
	BATERIA_PRINCIPAL_AUSENTE (Main_Battery_Absent),	Key 8	Enabled
	N/A	Key 9	Enabled
	ARME_DESARME_REMOTO (Remote_Assembly_Disassembly),	Key 10	Enabled

2	AUTO_ARME_DESARME (Automatic_Assembly_Disassembly),	Key 1	Enabled
	ARME_RAPIDO (Fast Assembly),	Key 2	Enabled
	ARME_DESARME_SOB_COACAO (Assembly_Disassembly_Under_Filtration),	Key 3	Enabled
	RESET_SISTEMA (System_Reset),	Key 4	Enabled
	PROGRAMACAO_ALTERADA (Changed Programming),	Key 5	Enabled
	FALHA_AO_COMUNICAR_EVENTO (Failure_when_communicating_event)	Key 6	Enabled
	SENHA_INCORRETA (Incorrect_Password)	Key 7	Enabled
	ACESSO_DOWNLOAD (Download_Access)	Key 8	Enabled
	TESTE_MANUAL (Manual_Test)	Key 9	Enabled
	TESTE_PERIODICO (Periodic_Test)	Key 10	Enabled
3	RESET_BUFFER_EVENTOS (Event_Buffer_Reset)	Key 1	Enabled
	RESET_DATA_HORA Date_Time_Reset)	Key 2	Enabled
	N/A	Key 3	Enabled
	N/A	Key 4	Enabled
	SOLICITACAO_MANUTENCAO (Maintenance_Request)	Key 5	Enabled
	FALHA_REDE_ELETRICA_MOD_EXPANSOR (Electric_Grid_Failure_Expander_Module)	Key 6	Enabled
	ACTIVATION / DEACTIVATION_PGM	Key 7	Enabled
	RF REGISTRATION / EXCLUSION	Key 8	Enabled
	REGISTRATION / CHANGE / EXCLUSION OF PASSWORD	Key 9	Enabled
	ENABLE_DISABLE_ZONE	Key 0	Enabled
4	FALHA_KEEP_ALIVE_GPRS	Key 1	Enabled
	FALHA_KEEP_ALIVE_ETHERNET	Key 2	Enabled
	ARME_DESARME_VIA_ALEXA	Key 3	Enabled
	ARME_STAY_VIA_ALEXA	Key 4	Enabled
	ACIONAMENTO_PGM_VIA_ALEXA	Key 5	Enabled
	BYPASS_ZONA_VIA_ALEXA	Key 6	Enabled

» Activation / deactivation of functions

Enter + 51 + GF + Enter + FUNCTION + Enter

GF = group of functions from 0 to 5.

FUNCTION = key corresponding to the function.

Key	Group of functions 0	Group of functions 1	Group of functions 2	Group of functions 3	Group of functions 4	Group of functions 5
1	Partitioning	Silent panic through key 0	Blocking of reset	Tamper of alarm center	-	-
2	Activation through a key	Audible panic through key 2	Remote control blocking	-	-	Supervision failure
3	Siren beep on activation/deactivation	Medical emergency by key 5	Keyboard lock in case of incorrect password	Cutting of telephone line	Real time reporting	Cutting of telephone line
4	Activation with open zones	Fire by key 8	Blocking of the synchronism button for registration of wireless devices	-	-	-
5	Password with 6 digits	Maintenance order by Enter key	-	-	-	Tamper of devices
6	Trigger clean remote control	-	-	-	-	Do not generate triggers
7	-	Indication of problems by siren	-	-	-	-
8	-	Automatic cancellation due to opening of zone	-	-	Disable output beep	-

Time of sending of failures

» AC failure

Enter + 481 + TM + Enter

TM = time of sending of the failure from 01 to 99 minutes.

System reset

» Reset of the entire system except registration of wireless devices

Enter + 0000 + Enter

» Reset of the entire system (Programmings, messages and wireless devices)

Enter + 9999 + Enter

6.24. Approval



05326-18-00160

This equipment is not entitled to protection against harmful interference and may not cause interference in duly authorized systems. This is a product approved by Anatel, the approval number can be found on the product label, for queries visit the website: <https://www.gov.br/anatel/pt-br>.

Warranty Terms

It is expressly stated that this contractual guarantee is granted under the following conditions:

Name of client:

Client's signature:

Invoice No.:

Date of purchase:

Model:

Serial No.:

Retailer:

1. All parts, pieces and components of the product are guaranteed against any manufacturing defects that may arise, for a period of 1 (one) year - this being 90 (ninety) days of legal guarantee and 9 (nine) months of contractual guarantee -, counted from the date of purchase of the product by the Consumer, as stated in the invoice for the purchase of the product, which is an integral part of this Term throughout the national territory. This contractual guarantee includes the free exchange of parts, pieces and components that present a manufacturing defect, including the expenses with the labor used in this repair. This contractual guarantee includes the express exchange of products that present a manufacturing defect. If no manufacturing defect is confirmed, but rather defect(s) arising from improper use, the Consumer will bear these expenses.
2. Product installation must be done in accordance with the Product Manual and/or Installation Guide. If your product needs installation and configuration by a trained technician, look for a qualified and specialized professional, and the costs of these services are not included in the price of the product.
3. Once the defect is verified, the Consumer must immediately contact the nearest Authorized Service that appears in the list offered by the manufacturer – only these are authorized to examine and remedy the defect during the period of guarantee provided herein. If this is not respected, this guarantee will lose its validity, as the product will be violated.
4. In the event that the Consumer requests home care, he must go to the nearest Authorized Service to inquire about the technical visit fee. If the need to withdraw the product is found, the resulting expenses, such as transport and security for the return trip of the product, are the responsibility of the Consumer.
5. The warranty will completely lose its validity in the occurrence of any of the following hypotheses: a) if the defect is not manufacturing, but caused by the Consumer or by third parties outside the manufacturer; b) if damage to the product is caused by accidents, accidents, agents of nature (lightning, flooding, landslides, etc.), humidity, voltage in the electrical network (over-voltage caused by accidents or excessive fluctuations in the network), installation/use in disagreement with the user manual or arising from the natural wear and tear of parts, pieces and components; c) if the product has been influenced by a chemical, electromagnetic, electrical or animal nature (insects, etc.); d) if the serial number of the product has been adulterated or erased; e) if the device has been tampered with.
6. This guarantee does not cover loss of data, therefore, it is recommended, if applicable to the product, that the Consumer regularly backs up the data contained in the product.
7. Intelbras is not responsible for the installation of this product, and also for any attempts at fraud and/or sabotage in its products. Keep software updates and applications used up to date, if applicable, as well as the necessary network protections to protect against intrusions (hackers). The equipment is guaranteed against defects within its normal conditions of use, and it is important to be aware that, as it is an electronic equipment, it is not free from fraud and scams that could interfere with its correct functioning.
8. Properly dispose of your product after its useful life - deliver it to collection points for electrical and electronic products, at an authorized Intelbras technical assistance center or consult our website www.intelbras.com.br and support@intelbras.com.br or (48) 2106-0006 or 0800 7042767 for more information.

These being the conditions of this complementary Term of Guarantee, Intelbras S/A reserves the right to change the general, technical and aesthetic characteristics of its products without prior notice.

All images in this manual are illustrative.

Product benefited by the Information Technology Legislation.

intelbras



talk to us

Customer Support: ☎ (48) 2106 0006

Forum: forum.intelbras.com.br

Support via chat: chat.apps.intelbras.com.br

Support via e-mail: suporte@intelbras.com.br

Customer Service / Where to buy? / Who installs it? 0800 7042767

Produced by: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia BR 459, km 126, nº 1325 – Distrito Industrial – Santa Rita do Sapucaí/MG – 37538-400
CNPJ 82.901.000/0016-03 – www.intelbras.com.br | www.intelbras.com/en

02.26
Made in Brazil