English

intelbras

# User's manual

## AMT 8000

intelbras

# AMT 8000
## Alarm center

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

AMT 8000 Wireless Alarm Center has advanced technology and is easy to program. Due to its differentiated technology, the following unique wireless devices can be connected to this center: XAC 8000 remote control, XAS 8000 magnetic wireless sensor, IVP 8000 Pet passive wireless sensor, IVP 8000 Pet Cam passive wireless sensor, XSS 8000 wireless siren, wireless keypad for XAT 8000 alarm center, REP 8000 range RF amplifier and also the TX 8000 universal transmitter with all devices exchanging information with encryption, for greater system security. In addition to various security devices such as tamper against removal of the installation surface and violation of devices and with long battery life. This center has 16 partitions, 8 memories for phone numbers, *Panic* function, *Emergency*function, smart battery charger with protection against short circuit or polarity reversal, timing and sensor test function. The system has differentials such as high performance wireless device communication (bidirectional) with a range of up to 1000 meters without barriers and direct view, GPRS and GSM type connections, telephone line, Ethernet and Wi-Fi connection to provide greater ease for system monitoring and checking. Reports events to 2 IP destinations (monitoring companies). The center is already directed to the Intelbras Cloud using initially the random remote access password indicated along with the QR Code label that also contains the MAC.

AMT 8000 Center has remote firmware update, using Ethernet cable or Wi-Fi communication to download the most updated firmware version.

In addition to this option, the center can also be updated using the BootLoader feature. To do this, you need to have the *Atualizador 8000* software previously installed on your computer.

⚠ 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 Security

- Follow all instructions in the manual for product installation and handling.
- Perform the installation in environments not susceptible to factors such as rain, fog and splashes of water.
- Wireless communication technology, when exposed to environments with high power radiation, may suffer interference and have its performance impaired. Example: places near TV towers, AM/FM radio stations, amateur radio stations, etc.
- Do not install the control panel and its accessories near radio frequency equipment such as routers, repeaters and / or wi-fi signal amplifiers. The control panel and its devices must maintain a minimum distance of 2 meters from this equipment.
- Do not install the alarm center facing air conditioning or heating equipment.
- Do not expose directly to sunlight.
- Clean only the external part of the device, using only a damp cloth (do not use chemical solvents).
- Do not subject the device to excessive pressure or knocks/falls.
- Do not cover the device with adhesives, paper or inks.
- Check that at the installation site, the LED indicating the devices flash green when activated.
- Avoid installation on metal surfaces in order not to attenuate the transmission signal between the devices in the system.
- The installation, configuration of the center and the other products that make up this system must be performed by a qualified professional.
- Perform periodic tests on it in order to validate weather conditions, battery level and other factors, so that the site supervised by the system is always able to operate correctly.
- ATTENTION: this product comes with a factory default password. For your security, it is essential that you change it as soon as you install the product and ask your technician about the passwords set, which users have access and the recovery methods.
- LGPD - General Law for the Protection of Personal Data: this product does not process any personal data.

# Summary

1. Technical Specifications 10

2. AMT 8000 Alarm Center Features 11

3. AMT 8000 Accessories 12

3.1. XAG 8000, XAG 8000 3G and XG 4G modules (compatibility with XG 4G module from version 2.3.7) . . . . . . . . . . 12

Features . . . . . . . . . . 12

3.2. Communication module via telephone line - FXO 8000 . . . . . . . . . . 13

Features . . . . . . . . . . 13

4. Installation of the alarm center and its peripherals 14

4.1. Power supply for the alarm center (full range 90 and 265 Vac) . . . . . . . . . . 17

4.2. Battery. . . . . . . . . . . 18

4.3. XAG 8000, XAG 8000 3G and XG 4G modules. . . . . . . . . . . 18

4.4. FXO 8000 Phone Module. . . . . . . . . . . 19

4.5. AMT 8000 Alarm Center . . . . . . . . . . 20

5. Operation 20

5.1. Description of the XAT 8000 LCD keyboard indications. . . . . . . . . . . 20

5.2. Display of troubles . . . . . . . . . . 21

5.3. Description of the LEDs signaling on the alarm center boards . . . . . . . . . . 21

LEDs of alarm center baseplate . . . . . . . . . . 21

XAG 8000, XAG 8000 3G and XG 4G board LEDs . . . . . . . . . . 21

5.4. Partitioning . . . . . . . . . . 22

5.5. Activation/deactivation of the alarm center. . . . . . . . . . . 23

Activating/Deactivating on non-partitioned systems. . . . . . . . . . . 24

Activating/Deactivating on Partitioned Systems . . . . . . . . . . 25

5.6. Menu. . . . . . . . . . . 26

Bypass . . . . . . . . . . 26

Open Sensors . . . . . . . . . . 27

Trigger Sensors . . . . . . . . . . 28

Partitions . . . . . . . . . . 28

Connections . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .28

2G/3G/4G signal. . . . . . . . . . . . . . . . . . . . . . . . . . . . . .29

Wireless signal . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .30

Addr. MAC . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .31

Center version . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .31

Keyboard version . . . . . . . . . . . . . . . . . . . . . . . . . . . . .31

Test mode . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .31

Battery tens. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .31

5.7. Remote update . . . . . . . . . . . . . . . . . . . . . . . . . . . . .31

6. Programming 32

6.1. Programming mode . . . . . . . . . . . . . . . . . . . . . . . . . . .32

Using the XAT 8000 Wireless Keyboard . . . . . . . . . . . . . . . . .32

Using AMT Remote Mobile Application (for mobile devices) . . . . . . . . . . . . . .35

Using the AMT 8000 programmer (for computers) . . . . . . . . . . . . . . . . . . . . .35

Using Intelbras Guardian application (for mobile devices). . . . . . . . . . . . . . . .36

6.2. Wireless devices (register/delete) . . . . . . . . . . . . . . . . . . . . . .36

Wireless device registration by means of the alarm center synchronization button . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .37

Registering by keyboard command . . . . . . . . . . . . . . . . . . . . . . .39

Exchange of device routes between central and repeater . . . . . . . . . . . . . . . .42

Changing route by restarting devices. . . . . . . . . . . . . . . . . . . . . . .43

Route change by command (function available from firmware version 2.0.0 of the control unit and devices) . . . . . . . . . . . . . . . . . . . . . . . . .43

Automatic device route exchange between Alarm center and repeater (function available from firmware version 2.0.0 of the control panel and devices) . . . . .45

Reset wireless devices. . . . . . . . . . . . . . . . . . . . . . . . . . . . .46

Changing RF Channel . . . . . . . . . . . . . . . . . . . . . . . . . . . . .46

6.3. Wireless sensor functions . . . . . . . . . . . . . . . . . . . . . . . . . .47

Wireless sensor testing . . . . . . . . . . . . . . . . . . . . . . . . . . . .47

Zone tamper detection . . . . . . . . . . . . . . . . . . . . . . . . . . . .47

IVP 8000 EX sensor digital tamper reset . . . . . . . . . . . . . . . . . . . .48

Sensor firmware verification . . . . . . . . . . . . . . . . . . . . . . . . . .48

Device Address Identification. . . . . . . . . . . . . . . . . . . . . . . . . .48

  Adjusting Wireless Infrared Sensors . . . . . . . . . . . . . . . . . . . . . . . . . . .49
6.4. Functions of Remote Control Keys . . . . . . . . . . . . . . . . . . . . . . . . . . .50
6.5. Functions of Wireless Keyboard . . . . . . . . . . . . . . . . . . . . . . . . . . . .52
  Keyboard Partition. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .52
  Editing XAT 8000 keyboard messages . . . . . . . . . . . . . . . . . . . . . . . . . . .53
  Change messages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .54
  Resetting the messages. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .54
  Panic key . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .54
6.6. Siren functions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .55
  Siren Partition . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .55
  Enable siren beep on system activation/deactivation . . . . . . . . . . . . . . . . . .56
  Enabling the siren beep in the activation/deactivation on a specific partition . . .57
  Siren Time. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .58
  PGM 8000 Wireless actuator. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .58
  Scheduled time . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .63
  Days for Scheduled Self-Activation of PGMS . . . . . . . . . . . . . . . . . . . . . . .63
  PGM auto-activation time . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .63
  PGM auto deactivation time . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .64
  Holidays . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .65
  PGM 8000 Actuator Association to Partition . . . . . . . . . . . . . . . . . . . . . . .66
6.7. Update . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .66
6.8. Passwords . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .67
  Programming password permissions . . . . . . . . . . . . . . . . . . . . . . . . . . . .68
  Password programming using the installer password . . . . . . . . . . . . . . . . . . .70
  Password programming using the master password. . . . . . . . . . . . . . . . . . . . .71
  Password Permissions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .71
6.9. Quick setup for SMS monitoring and programming. . . . . . . . . . . . . . . . . . . .73
  Monitoring via phone line . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .73
  Monitoring via Ethernet/Wi-Fi . . . . . . . . . . . . . . . . . . . . . . . . . . . . .74
  Monitoring via GPRS. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .77
  Program SMS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .79

6.10. Zone settings . . . . . 80
- Enable/Disable zones . . . . . 81
- Partial mode (stay) . . . . . 81
- Zone Functions . . . . . 82
- Zone operation mode . . . . . 84
- Automatic zone cancellation . . . . . 84
- Alloy input (from version 1.9.2) . . . . . 85
- Alloy input partition . . . . . 85
- Permission to activate and / or deactivate the alloy input . . . . . 86

6.11. Programming the alarm center partitioning . . . . . 86
- Enable partitioning . . . . . 86
- Partitioning the zone . . . . . 86
- Password Partitions . . . . . 87

6.12. Timings . . . . . 88
- Input Timing . . . . . 88
- Output Timing . . . . . 89
- Disable Beep Out . . . . . 89

6.13. Alarm Center Time Settings . . . . . 90
- Clock . . . . . 90
- Calendar . . . . . 90
- Weekday adjustment . . . . . 91
- Time interval for date and time synchronization . . . . . 91
- Time zone command . . . . . 92

6.14. Periodic Test . . . . . 94
- Periodic test by time . . . . . 94
- Periodic test by time interval . . . . . 95

6.15. Autoactivation . . . . . 95
- Autoactivation by Inactivity . . . . . 96
- Programmed Autoactivation and Autodisactivation . . . . . 96
- Holidays . . . . . 99

6.16. Telephony and Monitoring Settings . . . . . . . . . . . . . . . . . . . . . . . . . . . . 101
Contact-ID Events . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 101
Push Events . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 108
Panic events generated by the remote control . . . . . . . . . . . . . . . . . . . . . . 110
Reporting Mode . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 110
Blocking the sending of partition 00 to the monitoring company . . . . . . . . . 111
Monitoring via phone line . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 112
Monitoring via Ethernet/Wi-Fi Connection . . . . . . . . . . . . . . . . . . . . . . . 116
Switch IP address (Wi-Fi connection) . . . . . . . . . . . . . . . . . . . . . . . . . . . 123
DHCP (Wi-Fi connection) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 123
Netmask (Wi-Fi connection) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 124
Gateway (Wi-Fi connection) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 124
Monitoring via GPRS (General Packet Radio Service) connection . . . . . . . . . 125
Cloud Connection . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 130
6.17. Functions via SMS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 130
Sending SMS messages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 130
Sending chip options and operating method . . . . . . . . . . . . . . . . . . . . . . 131
Select SMS events . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 131
Phone to SMS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 132
Remote operation by SMS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 133
Changing the Display Name of the Alarm Center . . . . . . . . . . . . . . . . . . . 134
6.18. Activation/deactivation of Functions . . . . . . . . . . . . . . . . . . . . . . . . . 135
General settings 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 135
General settings 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 136
Locks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 137
General settings 3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 138
Monitoring . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 138
Troubles that generate triggering . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 140
6.19. Time to send the AC fault . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 140
6.20. System Reset . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 141
Temporary Reset of Master and Installer Passwords . . . . . . . . . . . . . . . . . . 141
Reset by programming mode . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 142

6.21. Quick programming reference . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 142
Enter programming mode . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 142
Changing RF Channel . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 149
Remote update . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 149
Passwords . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 150
Zone configurations . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 151
Partitioning . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 153
Timings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 153
Alarm Center Time Settings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 153
Periodic Test . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 154
Autoactivation/autodeactivation and Autoactivation/autodeactivation per partition . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 154
Wi-Fi Connection . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 156
Settings for monitoring and SMS . . . . . . . . . . . . . . . . . . . . . . . . . . . . 156
Fault sending time . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 166
System Reset of the entire system except wireless device registration . . . . . 166

Warranty Term 167

# 1. Technical Specifications

| | |
|---|---|
| Product | Monitored alarm center |
| ETH Connection | 100 Mbps and Full Duplex |
| AC power | 90 to 265 V (we recommend the use of a cable with gauge ≥ 1 mm) |
| DC power | 5.7 V coming from XFT 8000 source |
| Battery | 3.7 Vdc rechargeable battery (supplied with alarm center) |
| Operating temperature | –10 °C to 50 °C @ 90% humidity |
| Weight | 568 grams (with battery and other accessories connected - XAG and FXO) |
| Dimensions (W × H × D) | of Product: 170 × 211 × 81 mm |
| | With individual packaging: 177 × 216 × 82 mm |
| Average power[1] | AMT 8000: 5.2 Watts |
| | AMT 8000 + FXO 8000: 5.8 Watts |
| | AMT 8000 + XAG 8000: 8.1 Watts |
| | AMT 8000 + FXO 8000 + XAG 8000: 8.2 Watts |
| | Antenna type: internal |
| | Antenna gain: 0 dBi |
| Wireless communication frequency AMT 8000/Accessories | 915 to 928 MHz via internal antenna, power 18 dBm |
| Modulation | DSSS BPSK 40 Kbps |
| Battery | 3.7 Vdc lithium rechargeable, internal |
| Optional[2] | XAC 8000 remote control |
| | REP 8000 Range RF Amplifier |
| | XAT 8000 Wireless Keyboard |
| | XAS 8000 Wireless Magnetic Sensor |
| | TX 8000 Universal Transmitter |
| | IVP 8000 Pet passive infrared wireless sensor |
| | IVP 8000 Pet Cam passive infrared wireless sensor |
| | FXO 8000 Telephone Line Module |
| | XAG 8000 GPRS Module |
| | XSS 8000 Wireless Siren |
| | XAG 8000 3G GSM Module |
| | XG 4G Module |
| | PGM 8000 Wireless Actuator |

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

[2] ***Optional:*** *for more information see the website* www.intelbras.com.br.

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

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

# 2. AMT 8000 Alarm Center Features

- Capacity for 16 partitions with independent activations/deactivations.
- Zone allocation according to the desired partitions.
- Wireless signal receiver/transmitter integrated into the alarm center operating with a frequency from 915 to 928 MHz.
- Support for two cell phone SIM cards with the XAG 8000 / XAG 8000 3G / XG 4G module installed.
- Quad-band GPRS modem: compatible with most national GSM operators for the AMT 8000 operating with the XAG 8000, XAG 8000 3G, and XG 4G modules (sold separately).
- Event reporting via Ethernet/Wi-Fi connection, telephone line (with the FXO 8000 module installed - sold separately), GPRS connection (with the XAG 8000 module installed - sold separately), GSM connection (with the XAG 8000 3G module installed - sold separately), and LTE connection (with the XG 4G module installed - sold separately).
- Use in connection with all wireless devices on the 8000 line.
- Ability to display and program parameters by up to 16 XAT 8000 keyboards.
- Ability to connect up to 16 XSS 8000 wireless sirens.
- Ability to connect up to 98 XAC 8000 controls with user identification.
- Ability to connect up to 64 wireless sensors of the 8000 line.
- Remote programming via fax/modem card, Ethernet, Wi-Fi, GPRS and GSM.
- Ability to connect 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, sirens and keyboards.
- Low battery detection of registered wireless devices.
- Internal buffer for 512 events.
- Remote firmware update through Ethernet or Wi-Fi connections.

# 3. AMT 8000 Accessories

AMT 8000 alarm center can have several accessories grouped to compose the monitoring and security system, with the accessories responsible for communication and monitoring, sound warning, LCD keyboard and several sensors, for better adequacy and composition of the necessary protection system.

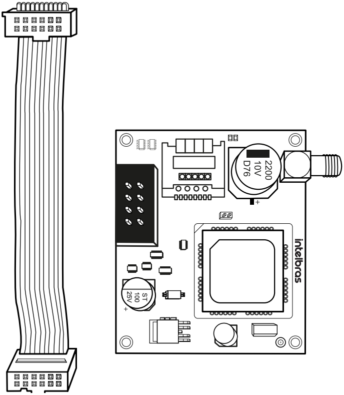
## 3.1. XAG 8000, XAG 8000 3G and XG 4G modules (compatibility with XG 4G module from version 2.3.7)

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

**Features**

- Supports up to two SIM card type chips.
- GPRS communication in 2G with the XAG 8000 module, 2G/3G/4G communication with the XAG 8000 3G module and 2G/4G communication with the 4G module.
- External antenna with 0 dBi gain.
- Reports events to 2 IP destinations (monitoring company) plus the Intelbras cloud.
- Operates with fixed or dynamic IP.
- Connections to DNS destinations.
- Power from the AMT 8000 alarm panel.

The following figure shows an illustrative image of the XAG 8000, XAG 8000 3G and XG 4G modules:



*GPRS XAG 8000 module, GSM XAG 8000 3G module and XG 4G module*

***Note:*** *the XAG 8000, XAG 8000 3G and XG 4G modules are compatible with most national GPRS / GSM operators with 2G, 3G and 4G technology.*

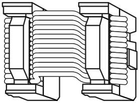
## 3.2. Communication module via telephone line - FXO 8000

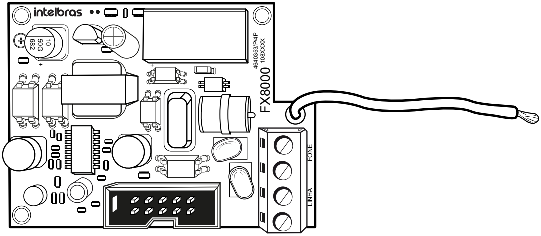
Optional accessory dedicated to data transmission via telephone line for communication and event reporting to a monitoring company with the AMT 8000 security system, in addition to dialing up to 5 personal phones and emitting the sound of a siren from the telephone line.

**Features**

- Up to 8 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 the illustrative image of the FXO 8000 module:





*FXO 8000 Telephone Line Module*

# 4. Installation of the alarm center and its peripherals

**Attention:** only connect the AMT 8000 alarm center to the mains and battery after the installation of all equipment and peripherals.

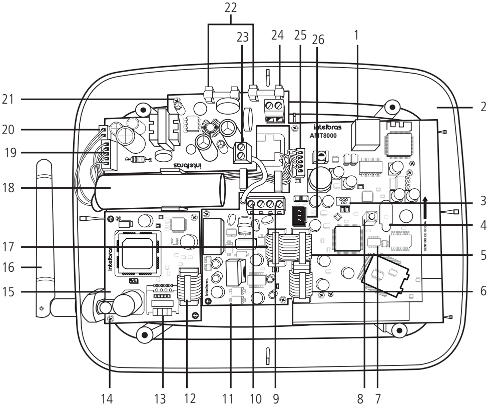
Open the product box and then open the cover of the AMT 8000 alarm center cabinet by removing the screws, where two plates can be seen, that is, its basic configuration contains the AMT 8000 alarm center board and its respective power supply and rechargeable battery that comes with the system.

telephone, GPRS and GSM, these cards with their respective interconnection cables with the AMT 8000 exchange.

If you choose the full configuration, 4 boards must be installed in the alarm center cabinet (the alarm center board, the source board, the telephone line module and the GPRS module or GSM module).

AMT 8000 alarm center has only wireless zones, as well as other accessories (keyboard, sirens, etc.) are connected to the alarm center via wireless signal, with only the AC power cables, telephone line and Ethernet network cable connected to the alarm center.

Image below illustrates the alarm center with all the devices that can be physically connected:


22
23
24
25
26
1
21
2
20
19
18
3
4
17
5
16
15
6
14
13
12
11
10
9
8
7
intelbras
AMT8000
intelbras
intelbras
intelbras
SENTIDO DE SOLDA

*AMT 8000 Alarm Center*

1. Connector for network cable (Ethernet).
2. CPU card of the AMT 8000 alarm center.
3. Mini-USB type connector for alarm center firmware update.
4. Alarm center CPU card indicator LED.
5. Alarm center board connector for interconnecting the FXO 8000 telephone line module.
6. Alarm control panel board connector to connect the XAG/XG module.
7. Pin-type connector (2×5-way) for firmware update of the alarm center.
8. Key for wireless device registration.
9. Input connector for telephone line.
10. Output connector for telephones.
11. CPU board for FXO 8000 telephone line module.
12. Connector for XAG/XG module flat cable.
13. Connector for SIM 1 card and SIM 2 card.

14. Connector for the external antenna of the XAG/XG module.
15. CPU card of the XAG 8000 GPRS module.
16. External GSM antenna (included with the XAG/XG module).
17. Connector for flat cable for the output of the telephone line signal to the alarm center board.
18. 3.7 V battery.
19. Flat cable connector for DC output from power supply.
20. Input connector for two-way battery cable.
21. XFT 8000 power supply board.
22. Protection fuses (2 x 250 Vac/400 mA).
23. Connector to connect the ground to the power supply (ground).
24. AC input of the power supply (switched full range - 90 to 265 Vac).
25. Flat cable input of the power supply.
26. Radio connector (future use).

**Attention:** the AMT 8000 alarm center does not have an auxiliary output to feed other devices and no connection point must be used on the alarm center cards (alarm center, GPRS card, telephone line card or source) for this functionality, because besides damaging the alarm center, it may damage the devices due to the alarm center operating at different voltages according to the circuit.

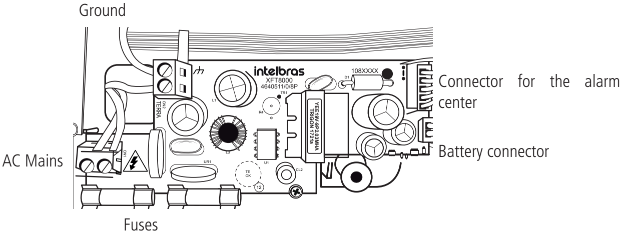
## 4.1. Power supply for the alarm center (full range 90 and 265 Vac)

Alarm unit is equipped with a full range switching source that works with the input voltage of 90 and 265 Vac without the need of a voltage selector switch. This way, even if some voltage variation occurs in the mains, the alarm unit will continue working normally (as long as the voltage is in the range of 90 to 265 Vac).

On this board there are two protection fuses of the unit. If you need to change, use new ones of the same value (250 V/400 mA).

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

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


Ground
intelbras
XFT8000
4640511/0/8P
108XXXX
CN2
TERRA
YEE19V-8P2.03MHA
TRIGON 1721a
Connector for the alarm center
Battery connector
AC Mains
Fuses

*XFT 8000 Power Supply*

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

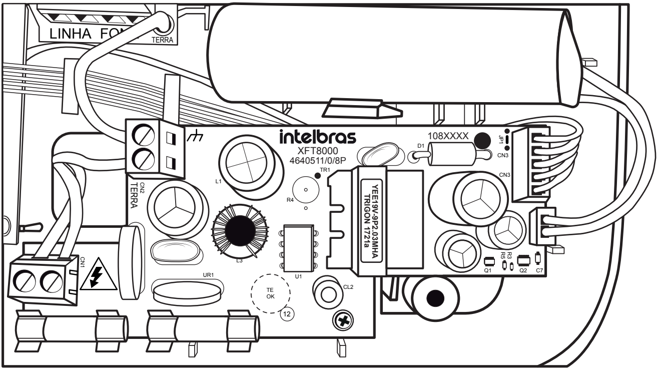
If the local electrical installation is not grounded, install a grounding bar and wire the connection terminal to the alarm center to perform the correct grounding.

**Attention:** it is mandatory to connect the grounding to the alarm center in order to have greater protection against lightning and overload by the mains and/or telephone line. If this connection is not made, the alarm center will function normally, but will be unprotected against overloads.

Warranty does not cover possible damages caused by lightning to the alarm center or to any other equipment connected to it.

## 4.2. Battery

AMT 8000 alarm center has an internal rechargeable battery of 3.7 Vdc and a capacity of 3,000 mA. The battery connector is located on the power supply board and is used to connect the battery to the alarm system. To wire the battery to this connector use the cable that comes with it, as shown below.


LINHA FO
TERRA
intelbras
XFT8000
4640511/0/8P
TR1
108XXXX
D1
JP1
CN3
CN3
CN2
TERRA
L1
R4
YEE19V-9P2.03MHA
TRIGON 1721a
L3
CN1
UR1
U1
TE
OK
12
CL2
Q1
R5
R3
Q2
C7

*Rechargeable battery for AMT 8000 alarm center*

Alarm center has protection against reverse polarity and short circuit in the battery.

The unit also has protection to prevent the battery from being damaged in the event of a mains failure.

If the voltage in the battery is below 2.8 V, the alarm center will switch off in order not to damage the battery.

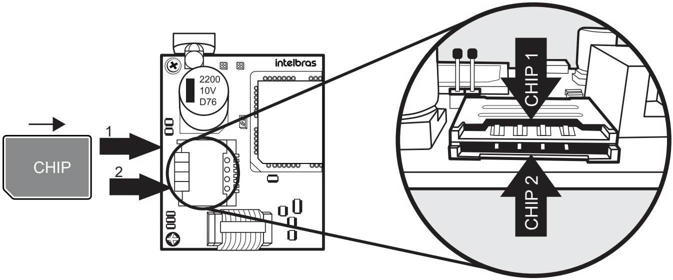
Battery life of 8 hours with Wi-Fi enabled and 16 hours with Wi-Fi disabled.

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

## 4.3. XAG 8000, XAG 8000 3G and XG 4G modules

Check that the cable for connection to the alarm center is correctly connected, passing under the board of the FXO 8000 telephone line module (if used), and its installation should be done only with the unit off, to avoid damage to the equipment and the installer.

In the XAG 8000, XAG 8000 3G and XG 4G modules there are two slots to accommodate two chips (SIM card) overlapping one another, with chip 1 above chip 2. When installing the chips, leave their metal contacts facing downwards and insert them to the end of the slot for correct allocation of the chips.

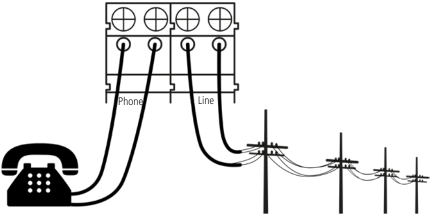


Chip allocation on the module

## 4.4. FXO 8000 Phone Module

Check that the cable for connection to the alarm center is correctly connected, and that it is only installed with the unit off, to avoid damage to the equipment and the installer.

In the FXO 8000 module there is the *Line* terminal, where the main telephone line (two wires) must be wired, connecting the *Phone* output (two wires) in the other telephone sets contained in this same line and as can be seen in the image below:



Wiring diagram of telephone line in the FXO 8000 module

This connection is necessary so that in case of reporting events or remote accesses, the alarm center is not without communication or has it interrupted if other phones of the same circuit enter/are in operation. In this case, when reporting events or remote access, the other phones will be inoperative, because the center will be occupying the line.

### 4.5. AMT 8000 Alarm Center

AMT 8000 alarm center has a tamper key against violation, and if this tamper switch is opened/violated, registered sirens will trigger and send the corresponding event if the *Problems that generate trigger* function is enabled (see section *Problems that generate trigger*).

Ethernet cables, AC power and telephone line should be directed through the hole located at the rear of the alarm center.

Alarm center can be installed on several surfaces, always placing it 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 securing the alarm center, fitting and checking that it has been placed correctly so that there are no falls and damage, and directing the wires in the dedicated areas.

## 5. Operation

Once the installation is finished, connect the alarm center to the local mains and the rechargeable battery.

***Note:*** to connect the AMT 8000 alarm center it is necessary that it is connected to the AC mains and the 5-way cable of the source is wired to the Source connector of the alarm center board, otherwise the alarm center will not power on even if the same is with battery. With the alarm center on and the battery connected, it will be recharged by the source and when the AC network is dropped the alarm center will be maintained by battery power.

### 5.1. Description of the XAT 8000 LCD keyboard indications

The following icons are located on top of the LCD display:

- ⚠**:** If this icon is flashing, it indicates that a trouble has been detected.
- 🔈**:** it will light up whenever there is a shot in the siren.
- **P:** with the icon lit, the center is in programming mode.
- **Battery:** indicates the battery status of the alarm center.

## 5.2. Display of troubles

The occurrence of troubles is described as follows:

On the XAT 8000 keyboard the ⚠ icon will flash.

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

***Note:***

- *If the  Indication of troubles by the siren in the activation/deactivation function and Beeping of the siren in the activation/deactivation are enabled and if any trouble is detected, 1 long beep will beep on activation and 2 long beeps on deactivation.*
- *To clear the keyboard after shooting, just press the* Exit *key.*

## 5.3. Description of the LEDs signaling on the alarm center boards

### LEDs of alarm center baseplate

| LED | Status/event | Signaling[1] |
|---|---|---|
| LED1/LED2 | Disconnected from the Ethernet network | LED off |
| LED1/LED2 | Connected to Ethernet network[1] | Flashing LED |
| LED3 | Center off | LED off |
| LED3 | Center on | Flashing LED |
| LED3 | Center on and registering devices | LED lit |

[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).

### XAG 8000, XAG 8000 3G and XG 4G board LEDs

| LED | Status/event | Signaling[1] |
|---|---|---|
| LED1, LED2 | Powered (connected to CPU board) | LED1 and LED2 constantly on |
| LED1, LED2 | Chip (SIM1 or SIM2) seeking connection | Only the corresponding LED is lit |
| LED1 | Chip 1 (SIM1) connected to servers | LED flashing 1 time (connected to server 1),<br>LED flashing 2 times (connected to server 2) |
| LED2 | Chip 2 (SIM2) connected to servers | LED flashing 1 time (connected to server 1),<br>LED flashing 2 times (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 alarm center programming you can split it into up to 16 independently activated and deactivated partitions and associate any of the 64 wireless zones with any of the partitions. You can also program passwords giving specific permissions to these partitions.

This function is useful in offices, residences or other places in the same building that need more alarm centers, because with the partitioning, the center is split 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 unit, because one partition can be activated or deactivated without influencing the other.

When the system is partitioned, the zones and any of the other wireless devices in the 8000 line can be split as shown below (for more information, refer to the section *6.10. Zone settings.*

» **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 reception as a common zone. This way, even if one of the people leaves and activates their partition, reception will still be disabled and will only be activated when the other partition is also activated.

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

**Example:** in a gallery composed of 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 (stay):** zones selected for this option remain inactive during activation in *Partial*mode independent of the partition associated with it.

**Example:** Assuming that for partition 01, composed of zones 01 to 10, only zones 01 to 05 are enabled as *Partial* mode. When the command for the *Partial* mode option is executed for a specific partition, in this case, partition 01, if someone passes the sector where sensors 01 to 05 are located, the alarm center will not fire - zones where the occupants will be present and during activation of the *Partial* mode they will not fire, if someone passes the sensors 06 to 10, the alarm center will fire for partition 01, indicating such sectors fired, being signaled by sirens and sending events for monitoring/ applications, if used.

**Note:** during the complete activation of the partition - outside the *Partial* mode (stay), all zones of the partition will trip.

## 5.5. Activation/deactivation of the alarm center

Alarm center can be activated and/or deactivated in different ways, depending on the settings defined. For any of the ways of activating the system, with the output time different from zero, after entering the password, the keyboard will beep at intervals of 1 second. In the last five seconds of the timer, these beeps will become faster to indicate that the output time is at the end. Once the output time is over, the siren will beep (if programmed) indicating that the alarm center is activated.

**Attention:** » For some programs 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 unit. This password can be changed as treated in the following fields.

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

***Note:*** » *If there is an error when typing the password, press the* Back *key and type the password again.*

» *When the alarm center or partition receives the command to activate and any of the zones are open, a fault/error will be generated (long beep on the keyboards) and it will only be possible to activate the alarm center when all zones are closed in the case of a full or non-partitioned system, or in the case of partitioned systems with the zones of the respective closed partitions. To activate the alarm center with open zones, refer to section* General settings 1.

### Activating/Deactivating on non-partitioned systems

*Activation in* Full *mode*

To enable the system completely, enter a valid password on the XAT 8000 keyboard, for example, the master password. To know if the alarm center is activated just slide the cover of the keyboard and display the message, if the alarm center is activated will be displayed the message: *Alarm activated*, otherwise *Alarm deactivated* will be displayed.

*Activation by a key*

If the *One Key Activation* function is enabled (see section *General settings 1*), keeping the active key pressed until the keyboard beeps ( + /- 3 seconds) will activate the system in *Full* mode. Exit time will be initiated to exit the protected area. At the end of the exit time, the system will be activated in *Full* mode (all partitions). This procedure does not allow you to deactivate the system.

**Note:** If a common keyboard is used, all partitions will be activated in the case of a partitioned alarm center. In the case of a keyboard with permissions for partitions, only the partition on which this keyboard has permission will be activated.

*Disabling the system*

To deactivate the system enter a valid password, for example, the master password. After entering the password, the alarm center will be completely disabled and the *Alarm Disabled* information will be displayed.

The zones, which must be passed until the keyboard is reached, must be programmed as entry timers or as followers so that the alarm not to be triggered immediately when the keyboard access path is violated/accessed. After entering the protected area by an entry time zone, the entry time will start and the user must enter a valid password on the keyboard before the time limit ends, to avoid triggering the alarm and reporting the corresponding events. Refer to the section *Zones functions* to set as timed.

*Remote control activation/deactivation*

To activate/deactivate the system by remote control, it must be registered with the alarm center, as described in section *6.2. Wireless devices (register/delete).*

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

### Activating/Deactivating on Partitioned Systems

Before attempting to perform the following operations you must program the unit for one of these conditions and to do so refer to 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 enable/disable 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 enabled.
- **Desired partition only:** press the *Active + Partition (01 to 16) + Password* key. 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 (stay)*

Activation in *Partial* mode allows you to partially activate the system, that is, you can select some zones to remain deactivated while others remain activated. For example, you can activate the external zones while the internal zones remain deactivated, allowing the circulation of people inside the building without triggering the alarm. But if someone tries to invade the property through a zone that is activated, the alarm will trigger normally.

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

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

***Note:*** only the master password and passwords with permission to enable the Partial mode (stay) can enable 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 enable/disable all partitions), there are two ways of deactivation:

- **All partitions:** enter the password and all partitions will be disabled.
- **Only desired partition:** press the *Disable + Partition (01 to 16) + Password* key and the chosen partition within the range (01 to 16) will be disabled.

The zones, which must be passed until the keyboard is reached, must be programmed as entry timers or as followers so that the alarm not to be triggered immediately when the keyboard access path is violated/accessed. After entering the protected area by an entry time zone, the entry time will start and the user must enter a valid password on the keyboard before the time limit ends, to avoid triggering the alarm and reporting the corresponding events. Refer to the *Zones functions* section to set as timed.

*Activation/deactivation by user-specific password*

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

On activation, the output time will start and the partition will be active at the end of the programmed time.

On deactivation, the keyboard must be accessed for a time zone if necessary and the password must be entered before the end of the programmed time in order to avoid triggering and reporting events.

*Remote control activation/deactivation*

To activate/deactivate the system by remote control, it must be registered with the alarm center, as described in section *Wireless devices (register/delete).*

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

## 5.6. Menu

Alarm center has a *Menu* function to make it easier to view the status and perform some commands. When accessing one of the options if you want to return to the *Main* menu press the *Back* or *Exit* key to go to the Home screen.

### Bypass

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

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

This function must be programmed no more than 30 seconds before the system is activated, otherwise the operation will be withdrawn.

Procedure for temporarily cancel a zone is as follows:

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

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

### Open Sensors

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

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

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

Status of the sensors in their respective zones will be displayed, distributed in divisions of 10 zones. To change the zone group press the directional 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 to 10, Group 2 the zones 11 to 20 and so on up to the zones in Group 7, thus demonstrating the status of zones 1 to 64.

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

- Square empty (☐) zone closed/non violated.
- Square filled (■) zone open/violated.

### Trigger Sensors

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

When pressing *Menu*, with the directional keys leave the marker in *Trigger Sens.* and press *Enter*. Use the directional keys to navigate between the sensors/zones of the alarm unit to check which sensors generated the trip.

- Square empty (☐) zone closed/non violated.
- Square filled (■) zone open/violated.

### Partitions

Enabled partitions will be displayed in the alarm center (see the section *6.11. Programming the alarm center partitioning* and their respective status.

When pressing *Menu*, with the arrow keys leave the marker in *Partitions* and press *Enter*. Use the arrow keys to navigate between the alarm center partitions to check their status.

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

### Connections

Connection status for reporting events via IP to monitoring services will be shown. The connection information for the 2G/3G/4G WI-FI is available from version 1.0.2 of XAT 8000 and 1.2.7 of the AMT 8000 control panel.

In the *Cloud* menu of the keyboard, the control panel will have only one option filled, that is, ETH or GPRS. However, communication via ETH will be a priority.

When pressing *Menu*, with the arrow keys leave the marker in *Connections* and press *Enter*.

- **WI-FI:** empty square (☐): not connected to the destination / filled square (■): connected to the destination.

- **Eth (using network cable):** empty square (☐): not connected to destination/ filled square (■): connected to destination.
- **2G/3G/4G:** empty square (☐): not connected to destination/filled square (■): connected to destination.

Eth: IP1 ■ IP2 ☐

2G/3G/4G: IP1 ☐ IP2 ☐

*IP1/IP2 connections status display function. In this example, IP1 is connected via Ethernet network cable*

***Note:*** *the XAG 8000 module covers only 2G technology, the XAG 8000 3G module covers both 2G and 3G technology, and the XAG 4G module covers both 2G and 4G technology. When using the module, the chosen communication technology will depend on the availability of signal coverage by the operator in the region where the exchange is located.*

Refer to the *Connections* section for setting priority addresses and directions.

- **Cloud:** Will display whether the center is connected to the Intelbras Cloud server via ETHERNET (network cable), via WI-FI or 2G / 3G. This server allows communication between AMT 8000 and remote access via application.
- **WI-FI:** empty square (☐): not connected to Intelbras Cloud / filled square (■): connected to Intelbras Cloud.
- **Eth (using network cable):** 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 signal

It will display the operator's signal level in percent, where square 1 represents level less than or equal to 10% and square 0 represents 100%. The filled mark corresponds to the active sign and the empty mark to the one without sign, referring to the level in 10 divisions.

When pressing *Menu*, with the arrow keys leave the marker in *2G/3G/4G signal* and press *Enter*.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
|---|---|---|---|---|---|---|---|---|---|
| ■ | ■ | ■ | ■ | ■ | ☐ | ☐ | ☐ | ☐ | ☐ |

*Illustration of the GSM network signal level function*

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

### Wireless signal

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

When pressing *Menu*, with the arrow keys leave the marker in *Wireless Signal* and press *Enter*.

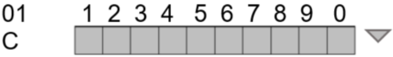
Wireless signal from the following devices may be displayed:

- **Sensors:** devices registered in the alarm center at 01 to 64 addresses. To view the signal of the sensors with the marker on it press *Enter* and then, with the arrow keys, switch between the sensors.
- **Keyboards:** devices registered in the alarm center at 01 to 16 addresses. To view the signal of the keyboards with the marker on it press *Enter* and then, with the arrow keys, switch between the keyboards.
- **Sirens:** devices registered in the alarm center at 01 to 16 addresses. To view the signal of the sirens with the marker on it press *Enter* and then, with the arrow keys, switch between the sirens.
- **Repeaters:** devices registered in the alarm center at 01 to 04 addresses. To view the signal of the repeaters with the marker on it, press Enter and then, with the arrow keys, switch between the repeaters.

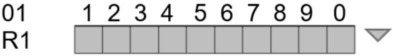
Signal level will be displayed in percentage, where the number 1 represents level less than or equal to 10% and the square 0 represents 100%. The filled mark corresponds to the active sign and the empty mark to the one without sign, referring to the level in 10 divisions.

Wireless device that is communicating directly with the center will be identified with the letter C and the device that is passing 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 the repeater 01:



***Note:*** repeaters will be identified from R1 (repeater 1) to R4 (repeater 4).

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

***Note:*** the signal level that appears on the keyboard for each of the devices refers to the last communication it made.

**Addr. MAC**

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

**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 center. When pressing *Menu*, with the arrow keys leave the marker in *Test* mode and press *Enter*.

The test will start, showing the *Signal test* information 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.

***Note:*** the signal level that appears on the keyboard for each of the devices refers to the last communication it made.

**Battery tens.**

It will display the battery level of the keyboard.

## 5.7. Remote update

AMT 8000 alarm center has remote firmware updates, and if new firmware versions are available, it is not necessary to use recorders or connect to computers to be updated by downloading the new version through Ethernet or Wi-Fi connections. When the version update is performed, the registration of the wireless devices or saved settings 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

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

These settings are stored in EEPROM type memory, thus avoiding the need for frequent reprogramming or if it is not fed.

To program these parameters, it is necessary to use two special passwords, called master password (the center initially has the 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 the installation to increase system security, as this will prevent unauthorized persons from changing the alarm center settings (see *6.8. Passwords section).*

## 6.1. Programming mode

### Using the XAT 8000 Wireless Keyboard

When accessing the programming mode, editing or viewing some 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 or command must be started again.

*Enter programming mode*

When you press the *Enter* key on the initial screen, the *Prog. Password* message will be displayed, indicating that the center is waiting for the master password or the installer password to be entered.

*Entering the programming mode with the installer password*

Enter + Installer password

*Entering the programming mode with the master password*

Enter + Master password

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

**Note:** » *If you wish to cancel the typing of a sequence before finishing, keep the* Back *key pressed until receiving the confirmation beep or press the* Exit *key and start typing again from the beginning of the sequence indicated in the manual.*

» *To cancel the typing of a password, press the* Exit *key or press and hold the* Back *key.*

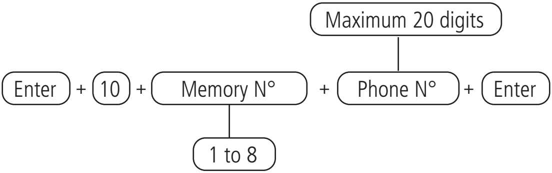
» *To exit programming mode, enter the* master password *or* installer password *(same password used to access programming mode).*

» *If the keyboard is left unoperated for three minutes, the alarm center exits programming mode and when accessed the keyboard is directed to the home screen.*

» *There is no need to exit the programming mode to execute the next command allowed by the password.*

*Direct editing/programming command*

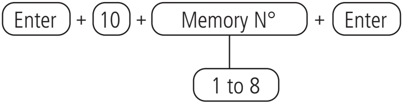
In programming mode, the command will be inserted by directly typing its entire extension and at the end pressing *Enter* to save the command and proceed to another, for example:



**Note:** Some commands can be entered either by the direct editing/programming mode or by the editing/programming mode with display.

*Editing/programming command with display*

In programming mode, some commands can be inserted in parts, so the first part of the command will be inserted 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 memory of the unit for the entered command is empty, the second line will be deleted. To edit, for example, the phone number using the LCD keyboard, place the cursor in the desired position using the arrow keys and enter the phone number, then press *Enter* to save the command and proceed to another.



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

***Note:*** Some commands can be entered either by the direct editing/programming mode or by the editing/programming mode with display.

### *Bit Editing Command*

In programming mode, some commands are entered with a special edit mode, which simplifies data entry and allows the display of the current programming.

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

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

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

### *Cancelling the typing of a command*

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

### *Delete a digit or cancel the typing 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 else hold down 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 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 center, provided that the password used for access has permission to change programming. The device must be connected to the Internet via Ethernet, Wi-Fi or GPRS (XAG 8000, XAG 8000 3G or XG 4G module added to the control panel is required).

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

***Note:*** it is required that the computer/remote access password is enabled, see 6.8. *Passwords* section.

### Using the AMT 8000 programmer (for computers)

Using the software installed on a computer (Windows® system) it is possible to access the programming menu of the center, provided that the password used for access is registered. It is necessary that the center is connected to the Internet (to use external network or via cloud) via Ethernet, Wi-Fi or GPRS connection (XAG 8000, XAG 8000 3G or XG 4G module added to the control panel is required).

***Note:*** it is required that the computer/remote access password is enabled, see 6.8. *Passwords* section.

### Using Intelbras Guardian application (for mobile devices)

Through the application installed on a mobile device (smartphone/tablet – Android®/iOS) you can access the alarm center to activate and deactivate it, check sensor/zone status, send emergencies, among other functions. Through the application will also receive current events from the alarm center, such as activations, triggers and other occurrences. For access, the master password or some secondary password must be placed, and the permissions in the application will be the same as the password defined in the other accesses. The device must be connected to the Internet via Ethernet, Wi-Fi or GPRS (XAG 8000 module added to the device is required).

## 6.2. Wireless devices (register/delete)

AMT 8000 alarm center already comes with the wireless receiver integrated to it in order to receive and transmit signal to sensors, keyboards and other devices.

Table below shows how many and which wireless devices can be registered in the alarm center.

| Types of devices | | Maximum devices | Addresses |
|---|---|---|---|
| Keyboards | XAT 8000 | 16 | 01 to 16 |
| Controls | XAC 8000 | 98 | 00 to 97 |
| Sensors | XAS 8000<br>IVP 8000 Pet<br>TX 8000 | 64 | 01 to 64 |
| Sensor with photochecking | IVP 8000 Pet Cam | 8 | 01 to 64 |
| Sirens | XSS 8000 | 16 | 01 to 16 |
| Range RF Amplifier | REP 8000 | 4 | 01 to 07 |

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

- » Check that all devices are correctly installed with the battery.
- » Leave the wireless devices near the alarm center to perform the correct registration and check the correct addressing.
- » First register the keyboards to allow them to be used to register the other devices via programming.

- It is recommended to use a maximum of 8 sensors with photochecking IVP 8000 Pet Cam per AMT 8000 alarm center, however their registration can occur during the entire address range exclusive to sensors (01 to 64).

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

### Wireless device registration by means of the alarm center synchronization button

Synchronization of devices using the synchronization button is the simplest method to add devices to the alarm center, however, in this method it is not possible to select the position that the device will occupy in memory. Each new device will occupy the first free position. To register a device in a specific position use the commands described in *Register by keyboard commands section.*

Press and release the synchronization button on the alarm center and wait for LED 3 located next to this button to be continuously lit, indicating that the center is ready for wireless device registration.

When the registration of all devices is complete, press the synchronization button of the alarm center again and check if LED 3 is back to the *Pulsed* mode (flashes indicating its normal operation), indicating that the system has left the wireless device registration mode.

Sensors, sirens and keyboards can be registered randomly, and each one will assume the addressing order according to its type.

- **Keyboards (addresses 01 to 16):** with the function active in the alarm center press the synchronization button on the keyboard, located at the back of same (remove the support for fixing on surfaces). The keyboard addressing will be according to the sequence performed, respecting the maximum limit of 16 devices of this type and after registration all of them, the common partition being added. To change the keyboards partition, see *Keyboards partition section.*

  To delete a registered keyboard in the alarm center, keep the synchronization key of the device pressed for 20 seconds, until the *Unlocked keyboard* information is shown on its display.

  **Note:** when physically erasing the keyboards, they must be erased from the memory of the alarm center via programming. Otherwise, a wireless device supervision failure will be generated.

- **Remote controls (addresses 00 to 97):** the control register follows the principle similar to keyboards, however any of the control keys can be used to perform the register. Each registered control will be associated to the user according to the registration sequence, being the first registered control address 00 (Master user) and the other controls assuming the addresses 01 to 97 (secondary users) that will have the same permissions as the users of the passwords that as factory default can activate and deactivate the complete system. The third key leaves the factory disabled and if you need to change any control settings, see *6.4. Functions of Remote Control Key.*

  To delete a control registered in the alarm center, press the keys in positions 1 and 2 (following vertical orientation) of the device for 10 seconds until the LED flashes twice in red.

  **Note:** when physically erasing controls, they must be erased from the memory of the alarm center via programming.

- **Wireless sensors (addresses 01 to 64):** follows the same principle as the other devices, however each sensor will be associated to a zone of the alarm center according to the registration sequence, starting with sensor 01 (corresponds to zone 01) up to sensor 64 (corresponds to zone 64). With the function active in the alarm center, press the synchronization key on each sensor that you want to synchronize according to its models:
  - **IVP 8000 Pet:** remove the protective cover from the battery compartment, press the synchronization key on it and check if the LED flashes green, indicating the success of the registration, in case of any failure the LED flashes red and the process must be repeated.
  - **IVP 8000 Pet Cam:** remove the back cover and press the synchronization key on it, check if the LED blinks green, indicating the success in the registration, in case of any failure the LED blinks red and the process must be repeated.
  - **XAS 8000/TX 8000:** press the synchronization key located on the back the same, check that the LED located on the front of the sensor blinks green, indicating success. If the LED blinks red there has been a failure and the process must be repeated.

  To delete a sensor registered in the alarm center, hold down the synchronization key on the device for 20 seconds until the LED flashes red twice.

  **Note:** when physically erasing sensors, they must be erased from the alarm center memory via programming.

- **Wireless sirens (addresses 01 to 16):** follow the same principle as the other devices, with the synchronization function active on the alarm center, press the synchronization key on the back of the siren (remove the base for fixing on surfaces) and check if the LED flashes green, indicating success in the registration, if the LED flashes red then process must be repeated. The addressing of the siren will be according to the sequence performed, respecting the maximum limit of 16 devices of this type and after the registration all being added the common partition. To change siren partition, see *Siren Partition* section.

  To delete a registered siren at the alarm center, keep the device synchronisation key pressed for 20 seconds until the LED flashes twice in red.

  **Note:** when physically erasing sirens, they must be erased from the memory of the alarm center via programming.

- **Range RF Amplifier (REP 8000 Repeater, addresses 01 to 04):** follow the same principle as the other devices, with the synchronization function active in the alarm center, press the synchronization key on the back of the repeater (remove the base for fixing on surfaces and turn on its power supply, because for it to initialize the source must be on) and check if the LED blinks green, indicating the success in the registration, if the LED blinks red there was some fault and the process must be repeated. The repeater addressing will be according to the sequence performed, respecting the maximum limit of 04 devices of this type.

  To delete a repeater registered in the alarm center, hold down the synchronization key on the device for 10 seconds until the LED flashes twice in red.

  ***Note:*** when erasing the repeater physically it is necessary to erase it from the memory of the alarm center via programming.

### Registering by keyboard command

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

It is necessary to register the first keyboard through the alarm center key (see *Cadastro de dispositivo sem fio pelo botão de sincronismo da central*section).

- **Keyboards (addresses 01 to 16):** with the keyboard to be registered near the alarm center, insert the following code and press the synchronization key at the back. The keyboard addressing will be according to the command entered, respecting the maximum limit of 16 devices of this type and after registration, all being added the common partition. To change the keyboards partition, see *Keyboard partition section.*

To register wireless keyboards, type:

01 to 16

Enter + 620 + Keyboard N° + Enter + Activate the wireless device

To delete wireless keyboards, type:

01 to 16

Enter + 720 + Keyboard N° + Enter

**Note:** *After registering the keyboard it will go into the process of updating messages, which takes approximately 30 seconds per keyboard and occurs in one keyboard at a time. If the message update process is interrupted, the keyboard will update them again as soon as it is opened again. In this case it should remain open until the update is finished.*

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

To register remote controls, type:

00 to 97

Enter + 60 + User N° + Enter + Activate the wireless device

To delete remote controls, type:

00 to 97

Enter + 70 + User N° + Enter

» **Wireless sensors (addresses 01 to 64):** follows the same principle as the other devices, but each sensor will be associated to a zone of the alarm center, according to the command performed.

To register wireless sensors type:

01 to 64

Enter + 61 + Zone N° + Enter + Activate the wireless device

- **IVP 8000 Pet:** remove the protective cover from the battery compartment, press the synchronization key on it and check if the LED flashes green, indicating the success of the registration, in case of any failure the LED flashes red and the process must be repeated.
- **IVP 8000 Pet Cam:** remove the back cover and press the synchronization key on it, check if the LED blinks green, indicating the success in the registration. If the LED blinks red there has been a failure and the process must be repeated.
- **XAS 8000/TX 8000:** press the synchronization key located on the back the same, check that the LED located on the front of the sensor blinks green, indicating success. If the LED blinks red there has been a failure and the process must be repeated.

To delete wireless sensors, type:

01 to 64

Enter + 71 + Zone N° + Enter

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

To register wireless sirens, type:

01 to 16

Enter + 621 + Siren N° + Enter + Activate the wireless device

To delete wireless sirens, type:

01 to 16

Enter + 721 + Siren N° + Enter

- **Range RF Amplifier (REP 8000 repeater, addresses 01 to 04):** follows the same principle as other devices. It is necessary to press the synchronization key on the back of the repeater (remove the base to fix it on surfaces and turn on the power supply of the repeater, because for it to initialize the source must be on), after typing the following code, check if the LED will flash green, indicating the success of the registration. If the LED blinks red there has been a failure and the process must be repeated. The repeater addressing will be according to the command performed, respecting the maximum limit of 04 devices of this type.

To register wireless repeater, type:

01 to 04

Enter + 622 + Repeater N° + Enter + Activate the wireless device

To delete wireless repeater, type:

01 to 04

Enter + 722 + Repeater N° + Enter

### Exchange of device routes between central and repeater

For a device to pass through the RF amplifier (Repeater REP 8000), the repeater signal level -> device must be greater than the central signal level -> device. Otherwise, it will communicate directly with the control panel without going through the repeater.

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

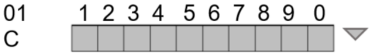
Whenever you want to pass a device through a specific repeater, turn off the others to ensure that the device will go through the desired repeater route.

After configuration, all repeaters can be turned on, this prevents the device from entering a route that is not the desired one. , if this happens, simply repeat the route change process.

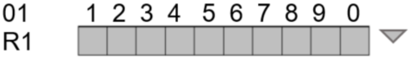
### Changing route by restarting devices

Remove the power from the device to have its communication pass through the repeater and after 3 seconds power it (replace the battery) again, for control it is not necessary to remove the battery, however, you need to press the first two keys (padlock open and padlock closed) simultaneously and release. After the device initialization time (varies from 0 to 60 seconds depending on the type) it starts with its new route, to check if the route change was carried out successfully press the synchronization key and the keyboard will display the new device route, if you have not changed the route, repeat the battery removal process. Another way to check the device's route is through the option to display the devices' signal level through the keyboard menu. If the device is in direct communication with the control unit, the position of the device will be shown plus the letter C, if the device is passing through the repeater, its position will be shown plus the letter R accompanied by the position of the repeater.

Ex.: sensor 01 communicating directly with the control unit:



Ex.: sensor 01 communicating with repeater 01:



### Route change by command (function available from firmware version 2.0.0 of the control unit and devices)

It allows the route change to be carried out by command via keyboard, so that the device searches for a new route, simply access the programming mode with the installer password and execute the command for the device that will be described below. The remote control will always look for the best route, which is why there is no command for it.

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

- **Search for new sensor route**

Enter + 544 + Zone + Enter
01 to 64

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

To force a transmission from the sensors, simply press the synchronization button, however, ideally, the sensor should carry out a transmission without hand contact so that there is no type of interference when searching for a new route. To do this, simply 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 its route, repeat the command and generate a new transmission from the device.

- **New route search Keyboards**

Enter + 545 + Keyboard + Enter
01 to 16

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

To force a keyboard transmission, press any key on the keyboard or press the synchronization button on the keyboard. If the device has not changed its route, repeat the command and generate a new transmission from the device.

- **Search for a new Sirens route**

Enter + 546 + Siren + Enter
01 to 16

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

- **Search for new PGM route**

Enter + 547 + PGM + Enter
01 to 16

After executing the command, activate the PGM or press the PGM 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, as when pressing the PGM synchronization button it will transmit to center every 3 seconds for the next initial 15 minutes.

### Automatic device route exchange between Alarm center and repeater (function available from firmware version 2.0.0 of the control panel and devices)

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

The automatic route change of devices is a feature that allows devices to search for a new route if they are left without communication with the alarm center or with the repeater for 30 minutes if the device is already communicating through a repeater. The remote control will always look for the best route.

Example: if a sensor that is communicating directly with the center remains without communication for 30 minutes, the sensor starts a new route search, and upon receiving the first response, whether from the center itself or from one of the 4 repeaters, the device starts to follow this route forever or until it remains without communication on this new route for another 30 minutes. Route changes can occur every 30 minutes as mentioned above. This process is repeated three times, that is, if the sensor is without communication with the 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 the device fails to find a new route after three attempts, 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.

- **Wireless actuator (PGM 8000 addresses 01 to 16):** follows the same principle as the other devices. If it is necessary to press the synchronization key on the back of the actuator (remove the base for fixing to surfaces), after entering the following code, check if the LED will flash green, indicating successful registration. If the LED flashes red there has been a failure and the process must be repeated. The actuator will be addressed according to the command made, respecting the maximum limit of 16 devices of this type and after registration, all being added to the common partition. To change the actuator partition, see the PGM Partition section.

  ***Note:*** *for the actuator to activate the Relay, it must be powered by a 12 to 24 VDC source or must be connected to the 110/220 Vac AC network.*

  - To register wireless actuators, enter:

01 to 16

Enter + 623 + Actuator No. + Enter + Activate the wireless device

  - Apagar atuadores sem fio digite:

01 a 16

Enter + 723 + Actuator No. + Enter

### Reset wireless devices

It will erase all registered wireless devices, including the keyboard used to perform the command. If you wish to re-register any device after the reset, it will be necessary to physically delete it by the synchronization key and only after confirmation of its deletion, by LED indication, it will be possible to re-register it.

To delete all wireless devices, enter:

Enter + 7 + Deactive + Enter

***Note:*** if the Reset Lock  is activated, it will not be possible to perform this function (see Bloqueiossection).

### Changing RF Channel

AMT 8000 alarm center has 4 RF communication channels, operating in the frequencies from 915 to 928 MHz and it is possible to change the channel used, if in the place where the system is located there are already other devices using this same frequency and thus causing interference.

To program this function, type:

08 to 11

Enter + 630 + RF Channel + Enter

To edit/view the programmed value, type:

Enter + 630 + Enter

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

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

## 6.3. Wireless sensor functions

### Wireless sensor testing

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

To program this function, type:

Enter + 52 + Enter

For open type sensors, the siren will be activated on opening and closing of the sensor and for infrared sensors, it will be activated on each activation while the command is active.

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

### Zone tamper detection

As of version 1.9.8 of the AMT 8000 control panel, the function to disable the tamper detection of the zone has been included.

To program this function, type:

Command to disable sensor tamper:

Enter + 78 + X + Enter

X = Zone group 0 to 6

Command to disable the digital tamper of the IVP 8000 EX

Enter + 79 + X + Enter

X = Zone group 0 to 6

***Note:*** *function available from version 2.0.0 of the sensor and version 2.0.0 of the AMT 8000 control unit.*

### IVP 8000 EX sensor digital tamper reset

Enter + 543 + ZZ + Enter

ZZ= 2-digit zone number.

***Note:*** *function available from version 2.0.0 of the sensor and version 2.0.0 of the AMT 8000 control unit.*

### Sensor firmware verification

Enter + 641 + ZZ + Enter

ZZ = 2-digit zone number

***Note:*** *function available for the control unit version from 2.0.3 and sensors from version 2.0.0. For sensors 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 to have at least 1 XAT 8000 keyboard registered to system with the display on.

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

Example of a test with sensor 01 of non-partitioned alarm center:

- » **1 line of the display:** Localized P00 message will be displayed
- » **2 line of the display:** Sensor 01 message will be displayed

**Note:** For partitioned system you will see P00 for common partition or P01 to P16 according to which partition the device belongs.

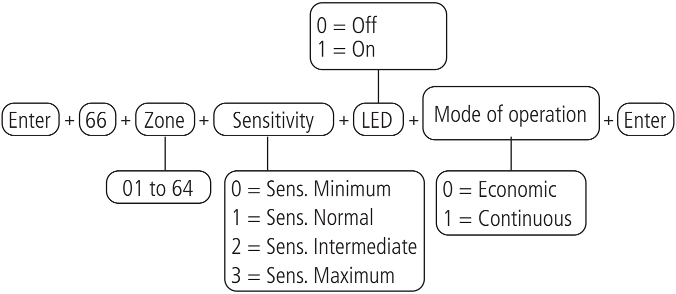
### Adjusting Wireless Infrared Sensors

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

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

- **Sensitivity:** will adjust so that the sensor detects correctly, according to the installation area, having the adjustment of 4 types of sensitivity, varying from the minimum, normal, intermediate and maximum (factory default sensitivity 2 = Intermediate Sens.). Although programming is permitted at the center, it is not possible to change the sensitivity of the XAS 8000 and TX 8000 sensors.
- **LED:** will set whether the LED of sensor transmission/detection will light up or remain off when any movement is detected (factory default *off*, only lighting for the first 15 minutes after battery insertion).
- **Operation mode:** it will define how the sensor will detect the movements, in case of operation in *Economy* mode the sensor detects and once the sensor has fired, 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 trip every time it identifies movement, without waiting any time (Economy factor). Although programming is permitted at the center, it is not possible to change the *operating mode* of the XAS 8000 and TX 8000 sensors.

To program these sensor functions, enter:



To edit/view the programmed value, type:

Enter + 66 + Zone + Enter

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

For the *Sensitivity Programming, LED and sensor operation* to be effective, it is necessary to trigger the sensor tamper, a trigger or a fast activation of the sensor synchronism button.

## 6.4. Functions of Remote Control Keys

The buttons on the XAC 8000 controls come out of the factory with the following functions:

- » **Button 1:** arm (function 02).
- » **Button 2:** disarm (function 03).
- » **Button 3:** disabled (function 00).

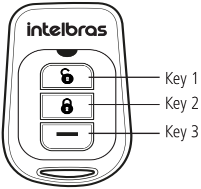
With the following command and indicative table it is possible to change the function of each remote control keys.

**Note:** some functions listed below are also associated with specific permissions as password permissions.

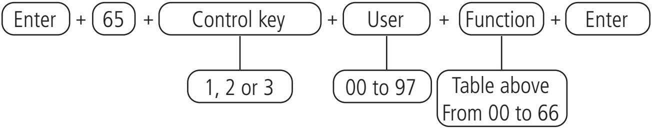
Use the following table to fill in the *Function* field to define functions for the remote control keys.

| | |
|---|---|
| 00 | Disabled |
| 01 | Atv/Dtv all partitions |
| 02 | Only activates all partitions |
| 03 | Only deactivates all partitions |
| 04 | Atv/Dtv all partitions in *Partial* mode (stay) |
| 05 | Arm only in *Partial* mode (stay) |
| 06 | Panic with siren |
| 07 | Silent panic |
| 08 | Fire panic |
| 09 | Medical emergency |
| 10 | N/A |
| 11 | Atv/Dtv only Partition 1 |
| 12 | Atv/Dtv only Partition 2 |
| 13 | Atv/Dtv only Partition 3 |

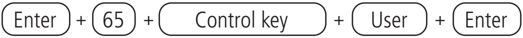
| | |
|---|---|
| 14 | Atv/Dtv only Partition 4 |
| 15 | Atv/Dtv only Partition 5 |
| 16 | Atv/Dtv only Partition 6 |
| 17 | Atv/Dtv only Partition 7 |
| 18 | Atv/Dtv only Partition 8 |
| 19 | Atv/Dtv only Partition 9 |
| 20 | Atv/Dtv only Partition 10 |
| 21 | Atv/Dtv only Partition 11 |
| 22 | Atv/Dtv only Partition 12 |
| 23 | Atv/Dtv only Partition 13 |
| 24 | Atv/Dtv only Partition 14 |
| 25 | Atv/Dtv only Partition 15 |
| 26 | Atv/Dtv only Partition 16 |
| 27 | N/A |
| 28 | N/A |
| 29 | N/A |
| 30 | N/A |
| 31 | Atv/Dtv *Partial* mode (stay) for Partition 1 only |
| 32 | Atv/Dtv *Partial* mode (stay) for Partition 2 only |
| 33 | Atv/Dtv *Partial* mode (stay) for Partition 3 only |
| 34 | Atv/Dtv *Partial* mode (stay) for Partition 4 only |
| 35 | Atv/Dtv *Partial* mode (stay) for Partition 5 only |
| 36 | Atv/Dtv *Partial* mode (stay) for Partition 6 only |
| 37 | Atv/Dtv *Partial* mode (stay) for Partition 7 only |
| 38 | Atv/Dtv *Partial* mode (stay) for Partition 8 only |
| 39 | Atv/Dtv *Partial* mode (stay) for Partition 9 only |
| 40 | Atv/Dtv *Partial* mode (stay) for Partition 10 only |
| 41 | Atv/Dtv *Partial* mode (stay) for Partition 11 only |
| 42 | Atv/Dtv *Partial* mode (stay) for Partition 12 only |
| 43 | Atv/Dtv *Partial* mode (stay) for Partition 13 only |
| 44 | Atv/Dtv *Partial* mode (stay) for Partition 14 only |
| 45 | Atv/Dtv *Partial* mode (stay) for Partition 15 only |
| 46 | Atv/Dtv *Partial* mode (stay) for Partition 16 only |



To program this function, type:


Enter
+
65
+
Control key
+
User
+
Function
+
Enter
1, 2 or 3
00 to 97
Table above
From 00 to 66

To edit/view the programmed value, type:


Enter
+
65
+
Control key
+
User
+
Enter

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

## 6.5. Functions of Wireless Keyboard

### Keyboard Partition

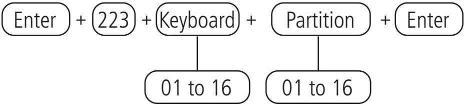
In the factory default keyboards can operate and view the status of all partitions. Using the following command you can program the keyboard to operate only one specific partition.

When the keyboard is programmed for a specific partition, you can only view the status and operate the selected partition, so if you enter a password for another partition or have permission for more than one partition, the *Keyboard error without permission* message will be displayed.

To activate the alarm center partition on which a keyboard is allowed using the master password or a password with permission for more than one partition, including the relevant keyboard partition, just enter the password or use the sequence *Activate + Partition + Password.*

In AMT 8000 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:


Enter
+
223
+
Keyboard
+
Partition
+
Enter
01 to 16
01 to 16

To edit/view the programmed value, type:

Enter + 223 + Keyboard + Enter

01 to 16

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

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

- » *Even if the keyboard is set to the partition, specific passwords are required to perform the 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

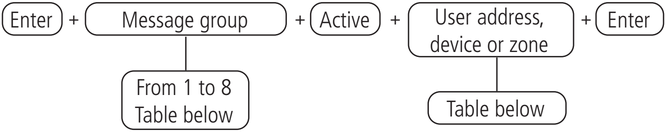
Through this function it is possible to customize the name of the zones, users and wireless devices added to the alarm center. When an event occurs, the first line of the display will display predefined messages indicating the event and the second line will display the programmed name (up to 14 digits).

Predefined messages are as follows:

| Function | Description |
|---|---|
| Activation | Alarm center has been activated |
| Deactivation | Alarm center has been deactivated |
| Trigger | Trigger The second line will indicate which zone |
| 24 Hour Trip | Trip a zone 24 hours. The second line will indicate which zone |
| Panic | Panic triggers. The second line will indicate which zone |
| Medical emergency | Triggers for medical emergency. The second line will indicate which zone |
| Fire | Triggers in a fire zone. The second line indicates which zone |
| Tamper zone/sensor | Tamper opening detected. The second line will indicate which zone |
| Low battery | Wireless device with low battery |
| Tamper devices | Device violation. The second line will indicate the device |

### Change messages

To edit/view the programmed messages use the following table to support the command:



| Description | Message group | User, device or zone |
|---|---|---|
| Name of the alarm center | 1 | 00 |
| Users | 2 | 00 to 99 |
| Zones | 3 | 01 to 64 |
| Partitions | 4 | 01 to 16 |
| PGM | 5 | 01 to 16 |
| Keyboards | 6 | 01 to 16 |
| Sirens | 8 | 01 to 16 |

After entering the command, the sequence entered will appear on the first line of the displayand the previously programmed message on the second. To edit the message, place the cursor in the desired position, use the arrow keys and successively press the desired key until the letter, character or number appears in the display.

To delete a digit press the *Back* key and to cancel the operation hold down the *Back* key for 3 seconds or press the *Exit* key.

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

### Resetting the messages

To return all messages scheduled for display, type:

Enter + 1 + Deactive + Enter

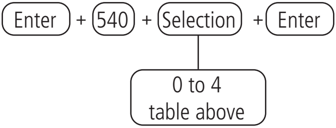
### *Panic* key

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

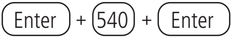
This key can assume the following settings:

| 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 will have the *Panic* key, 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 setting, press the *Back/Exit* and no programming will be changed.

## 6.6. Siren functions

The alarm center can have up to 16 wireless XSS 8000 sirens added, and if the center is partitioned, each of the 16 sirens can be associated to any of the partitions or remain in *Common* mode, in which case, if any partition/zone is intruded, it will be activated.

Below are the functions they can assume.

### Siren Partition

By factory default the sirens will trip and beep for activation/deactivation for all partitions. The following command can be used to program the siren to emit sound signals associated with a specific partition. When the siren is programmed for a specific partition, it will only fire if there are shots on this partition or if a common zone is fired. The Arm/Disarm beep will also only be emitted for the associated partition.

To program this function, type:

Enter + 222 + Siren + Partition + Enter
01 to 16 01 to 16

To edit/view the programmed value, type:

Enter + 222 + Siren + Enter
01 to 16

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

***Note:*** *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 siren beep on system activation/deactivation

Activates/deactivates the beep emitted by the siren on activation/deactivation of the alarm center. On activation, the siren will emit 1 beep and on deactivation, the siren will emit 2 beeps. If any trouble is detected and the *Indication of troubles by siren* function is enabled, the siren will emit 1 long beep on activation and 2 long beeps on deactivation.

To program this function, type:

Enter + 510 + Enter

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

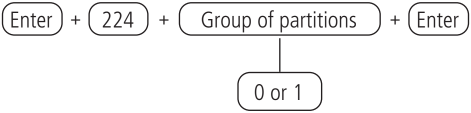
**Note:** » *For partitioned or non-partitioned systems, only one siren will be responsible for the activation/deactivation beep and follow the following behavior:*

- » *If the unit is not partitioned, only the siren registered at the lowest value address will beep for activation and deactivation. If there are more sirens registered at the unit and the siren of address 01 is removed from the system, the beeper will be emitted by siren 02 and so on.*
- » *The next siren will beep only if the previous siren is deleted or after the unit detects supervision failure.*
- » *If the unit is partitioned, when the general activation/deactivation is performed or in more than one partition, the beep will be given in the common siren, if it has one, or at the siren registered at the lowest address (01).*
- » *If the system is partitioned and only one partition with its own siren is activated, only one partition will be beep when the system is activated/deactivated.*
- » *In case of partitioned system and with siren without partition defined for it, beeping will take place on the common siren, if the system does not have common siren, beeping will not have activation/deactivation for this partition and neither will beeping of the other sirens for this partition in case of triggering.*

### Enabling the siren beep in the activation/deactivation on a specific partition

Select to which partitions the siren beep will be emitted in the activation/deactivation of center when the same is partitioned by customizing the registered siren for each partition. On activation, the siren will emit 1 beep and on deactivation, the siren will emit 2 beeps. If any trouble is detected and the *Indication of troubles by siren* function is enabled, the siren will emit 1 long beep on activation and 2 long beeps on deactivation.

To program this function, type:



After entering the command, using the XAT 8000 keyboard, mark which partitions will have the siren beep active, using the numbers on the keyboard to leave a mark on the partition. Select 0 for partition group 1 to 10 and 1 for partition 11 to 16. After changing the configured value, press the *Enter* key. If you only want to view the setting, press the *Back/Exit* key and no programming will be changed.

### Siren Time

Siren time leaves the factory programmed for 5 minutes. This is the time that the siren will be turned on/beeping after a violation/intrusion in any active partition/zone occurs and can be changed to a time between 01 to 99 minutes.

To program this function, type:

Enter + 4 1 + Siren Time + Enter

01 to 99 minutes

***Note:*** if 00 is programmed, error beep will be emitted and the setting will not be changed.

To edit/view the programmed value, type:

Enter + 4 1 + Enter

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

Para editar/visualizar o valor programado, digite:

Enter + 4 1 + 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.

### PGM 8000 Wireless actuator

PGM outputs are programmable and can be used to trigger devices such as: electric locks, floodlights, 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 stops.
- **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.

- **Time:** when the programmed 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 the event having stopped or not.

The events that can trigger PGM outputs are:

Triggered by apps:

- **Unpartitioned switch:** PGMs may be application controlled.
- **Partitioned Center:** PGMs can be controlled only if the App is accessed by the user with partition permission or with full permission. Even when programmed for other functions.

Password activation (secondary passwords from 51 PGM01 to 66 PGM16):

- **Unpartitioned Switch:** in On/Off mode, the corresponding PGM output will be turned on when the password is typed on the keyboard, and it will only be turned off when the password is typed again. If it is in Pulse or Time mode, the PGM output will remain on for the programmed time whenever the password is entered, and it can be disabled by entering the password on the keypad before the programmed time. If this function is disabled, passwords will work as a common password, if enabled, the password will only work to trigger the PGM output.
- **Partitioned switch:** PGM will be triggered by password regardless of whether it is linked to a partition or not.

  ***Note:*** *whenever the PGM is activated/deactivated by a password on the keyboard, it will emit two short beeps for confirmation or will display the fault message Actuator error not accessible if the activation/deactivation of the PGM is not carried out.*

System activation:

- **Non-partitioned control panel:** activates the PGM output when the control panel is activated.
- **Partitioned switch:** triggers the PGM output only with the activation of the partition to which the PGM belongs. If the PGM is common, it will be activated by activating all partitions and deactivated with deactivating any partition.

System deactivation:

- **Unpartitioned control panel:** activates the PGM output when the control panel is deactivated.

- **Partitioned switch:** triggers 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:

- **Unpartitioned Switch:** in case of a medical emergency, the PGM will be turned on.
- **Partitioned switch:** activates only the PGM output that belongs to the partition that generated the emergency. If PGM is common it will be activated with the generated emergency of any partition.

Event communication failure:

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

Cutting the phone line:

- **Unpartitioned Switch:** if the phone line is cut, the PGM output will be triggered.
- **Partitioned exchange:** if the telephone line is cut, the PGM output will be activated regardless of whether it is linked to a partition or not.

***Note:*** *the telephone line cut sensor must be activated.*

Siren problem:

- **Central não particionada:** em caso de problema com a sirene será gerado a falha de supervisão da mesma e a saída PGM será acionada.
- **Central particionada:** em caso de problema com a sirene será gerado a falha de supervisão e apenas a saída PGM atrelada a partição em que houve o problema será acionada. Se a PGM for comum será ativada com a falha de supervisão de qualquer sirene.

***Note.:*** *the PGM will only be activated after failure of Siren supervision.*

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

- **Unpartitioned Switch:** turns on the PGM output when any type of emergency, audible/silent panic or audible zone trigger occurs.

- **Partitioned Control Panel:** turns on the PGM output when any type of emergency, audible/silent panic or audible zone trip occurs concerning the partition that the PGM belongs to. If the PGM is common it will be activated with the events mentioned from any of the partitions.

Shot or silent panic (only shots and silent panics):

- **Unpartitioned Switch:** turns on PGM output when Silent Trigger or Silent Panic occurs.
- **Unpartitioned Switch:** turns on the PGM output when there is a silent trigger or silent panic referring to the partition that the PGM belongs to. If PGM is common it will be activated with silent panic trigger or silent trigger of any partition.

fire zone trigger:

- **Non-partitioned switch:** in case of any fire event, the PGM will be turned on.
- **Partitioned Control Panel:** turns on the PGM output when any fire event occurs in the partition that the PGM belongs to. If PGM is common it will be activated with fire event of any partition.

  For example: it can trigger a firefighting system, trigger a differentiated siren, trigger emergency lights, etc.

Opening Zone 1:

- **Non-partitioned switch:** 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 activate on opening and deactivate on closing or after time programmed if the sensor remains open).
- **Partitioned Control Panel:** whenever zone 1 is opened, the PGM will be turned on regardless of whether the PGM is pegged to a partition or not.

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

- **Non-partitioned control panel:** in On/Off mode, the corresponding PGM output will be turned on when the control is activated, and it will only be turned off when the control is activated again. If it is in Pulsed or Tempo mode, the PGM output will remain on for the programmed time whenever the control is activated and can be deactivated before the time limits by the control itself.
- **Partitioned control panel:** in this case, the operation will be the same as described for a non-partitioned control unit, regardless of whether the user in which

the control is registered has partition permission or not. See the item Remote control key functions.

***Note:*** *whenever the PGM is activated/deactivated by the remote control, it will light up the LED in green color informing that the PGM was activated or deactivated and in red color in case of communication failure (no activation/deactivation of the PGM).*

Switching on/off by time:

» **Unpartitioned Switch:** with this enable function, the PGM can be programmed to auto-activate and auto-deactivate for different days and times.

» **Partitioned switch:** the PGM will be switched on/off at the scheduled time regardless of whether it is linked to a partition or not.

**Attention:** for PGM to be associated with a partition, see the topic PGM 8000 actuator association for partition.

To program the PGM function, type:

Enter + 50 + PGM number + Operation mode + Event number + Enter

PGM number:
01 = PGM 01
02 = PGM 02
.
.
16 = PGM 16

Operation mode:
0 = On/Off
1 a 8 = pulse
9 = time

Event number:
00 to 13

Event that triggers the PGM:

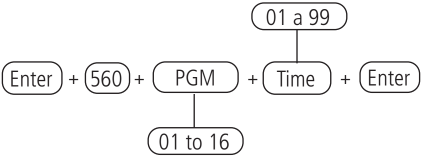
| | |
|---|---|
| 00 | Triggered by software and applications |
| 01 | Password activation (passwords from 51 PGM01 to 66 PGM16) |
| 02 | System activation |
| 03 | System deactivation |
| 04 | Medical emergency |
| 05 | Event communication failure |
| 06 | Cutting the phone line |
| 07 | Siren problem |
| 08 | Panic or shooting |
| 09 | Trigger or silent panic |

| | |
|---|---|
| 10 | Fire zone trigger |
| 11 | Zone 1 opening |
| 12 | Remote Control |
| 13 | Switching on/off by time |

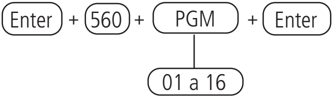
### Scheduled time

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

To program this function type:



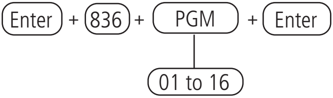
To edit/view the programmed value, type:



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 Self-Activation of PGMS

Selects the days on which the PGM Auto Activation will occur. Key 8 enables the function for programmed holidays.



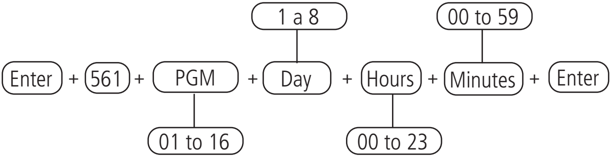
After changing the configured value, press the Enter key. If you only want to view the configuration, press the Exit key and no programming will be changed.

Use the keyboard keys to define the days for the PGM auto-activation to occur, so that the referring numbers, which want the days enabled, remain marked and the days with the function disabled remain unmarked and then confirm with the Enter key.

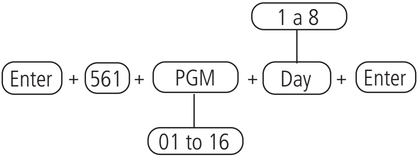
### PGM auto-activation time

Selects the time that Autoactivation per partition will take place.

To program this function, type:

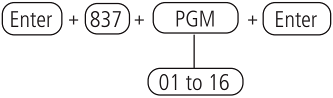

1 a 8
00 to 59
Enter
+
561
+
PGM
+
Day
+
Hours
+
Minutes
+
Enter
01 to 16
00 to 23

To edit/view the programmed value, type:


1 a 8
Enter
+
561
+
PGM
+
Day
+
Enter
01 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.

Days of the week for scheduled PGMS Auto-Deactivation:

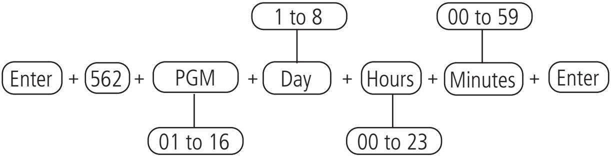

Enter
+
837
+
PGM
+
Enter
01 to 16

Use the keyboard keys to define the days for the PGM auto-deactivation to occur, so that the referring numbers, which want the days enabled, remain marked and the days with the function disabled remain unmarked and then confirm with the Enter key.

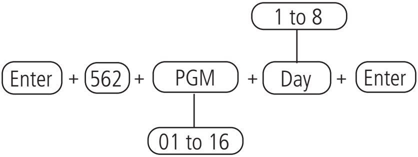
### PGM auto deactivation time

Selects the time that Auto-Disable by partition will occur.

To program this function, type:


1 to 8
00 to 59
Enter
+
562
+
PGM
+
Day
+
Hours
+
Minutes
+
Enter
01 to 16
00 to 23

To edit/view the programmed value, type:


1 to 8
Enter
+
562
+
PGM
+
Day
+
Enter
01 to 16

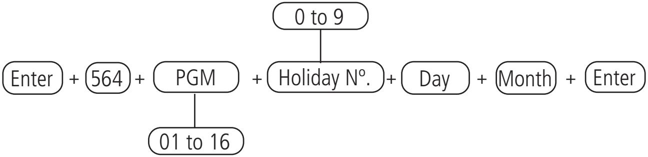
### Holidays

The control panel has 10 memories (0 to 9) to program dates that require a special time for Autoactivation and AutoDeactivation.

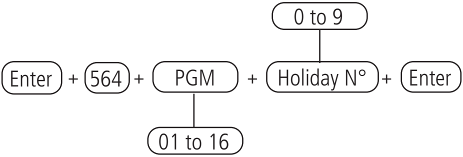
When the system date is equal to one of the programmed dates, the day of the week settings will be overridden by the times programmed in the address of the commands described above, referring to the alarm control panel's auto-activation programming.

*Set Holidays for Auto Activation/Auto Deactivation*

To program this function type:


0 to 9
Enter
+
564
+
PGM
+
Holiday Nº.
+
Day
+
Month
+
Enter
01 to 16

To edit/view the programmed value, type:


0 to 9
Enter
+
564
+
PGM
+
Holiday N°
+
Enter
01 to 16

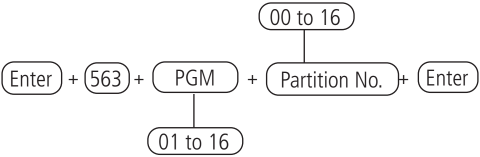
After changing the configured value, press the Enter key. If you only want to view the configuration, press the exit key and no programming will be changed.

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

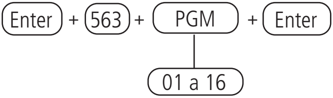
### PGM 8000 Actuator Association to Partition

With this function, it will be possible to associate the PGMS with the partitions of the switch, allowing a partition to have one or more PGMs (total of PGM per switch - 16) and which can 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.

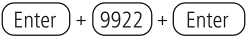
***Note:*** *a PGM can be registered in a single partition or be common to all, however a partition can have more than one PGM (PGM's from 01 to 16).*

*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.*

## 6.7. Update

The AMT 8000 control panel has remote firmware updates, meaning that when new firmware versions are available, there is no need to use recorders or connect to computers. The control 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/check a new version, type:



If there is a version to download, the *Download Wait* information will be displayed and it will start, which will take about 3 to 5 minutes (variable according to the connection used). If the alarm center does not have a version for download will be shown *Alarm center is already updated.*

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

Enter + 9933 + Enter

The new version that was downloaded will be installed and will not be lost records and programming of the alarm center. To check the firmware version of the alarm center, access *Menu* and with the arrow keys access *Version of the alarm center* to be displayed.

**Attention:** to download the firmware, the control panel must be connected to the Cloud via an Ethernet or Wi-Fi connection. Downloading/updating via a GPRS connection is not possible due to the connection's download rate and excessive consumption of the package used.

## 6.8. Passwords

**Attention:** » The alarm center to be operated/configured requires passwords, being some passwords are created through programming mode (secondary passwords, duress) and the installer password has the *9090*factory standard . In case of remote access password and master password for increased security are random passwords which are available on the QR Code label together with the MAC address of the alarm center.

» Before you change the installer password or the master password, make sure to have the new password well stored or noted, because after exiting the programming mode, you will only be able to access this mode again through the new password. If the password is forgotten, see *6.20. System reset section.*

***Note:*** » *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 deletes all alarm center settings except wireless devices and editable messages.*

» *Alarm center cannot contain repeated passwords between users, including Master User, Installer and Remote Access, and because of this it does not allow the programming of repeated passwords.*

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

The alarm center has 96 secondary passwords and can be programmed for up to 16 partitions, that is, it would be similar to divide the alarm center in 16 and command by 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 and computer/remote password, as well as perform the settings for the alarm center, but it is not allowed to activate and deactivate the alarm center, change the master password or the secondary passwords.

Using the master password, you can change your own password, program and/or change the secondary passwords, enable or disable the entire alarm center or a specific partition.

### Programming password permissions

| Password | Enabling |
|---|---|
| Master (initially random, see *QR Code* label) | Create and delete secondary passwords |
| | Change the master password |
| | Enable/disable secondary password permissions |
| | Adjust date, time and day of week |
| | Editing XAT 8000 keyboard messages |
| | Activate/deactivate the center completely or partitioned (Partition 01 to 16) |
| Installer (factory default password: *9090*) | Perform all settings of the alarm center, except enable/disable the 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 |
| 97 | Password of duress |
| 98 | Password of computer/remote access (initially random, see *QR Code* label |
| 99 | Installer password (*9090* factory standard) |

The secondary passwords plus the duress password are divided into 9 groups, according to the following table:

| **User group (GU)** | **Users of 1 to 10** | **User group (GU)** | **Users of 11 to 20** | **User group (GU)** | **Users of 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 of 31 to 40** | **User group (GU)** | **Users of 41 to 50** | **User group (GU)** | **Users of 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 of 61 to 70** | **User group (GU)** | **Users of 71 to 80** | **User group (GU)** | **Users of 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 of 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 |

***Note:*** use the table above in the programming below.

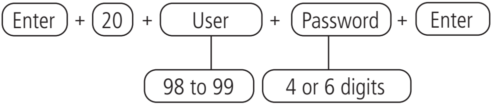
## Password programming using the installer password

### *Changing passwords using the installer password*

With the installer password it is allowed to change only the installer password (User = 99) and the computer/remote access password (User = 98). The user password 98 is always with 6 digits and does not depend on setting, but the user password 99 can be with 4 or 6 digits.

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

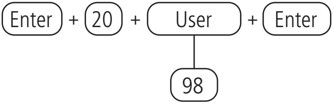
To program this function, type:



### *Delete passwords using the installer password*

The user password 99 (installer) can only be changed and not deleted. The user password 98 can be deleted.

To delete this password, enter:



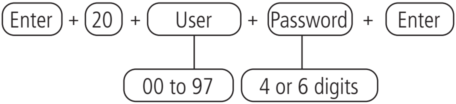
### Password programming using the master password

*Changing passwords using the master password*

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

To use 6-digit password, check the topic: *Configurações gerais 1*

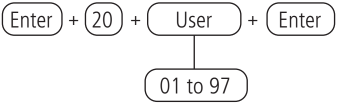
To program this function, type:



*Delete the passwords using the master password*

The master user password - 00 can only be changed and not deleted. User passwords 01 to 97 can be deleted.

To program this function, type:



### Password Permissions

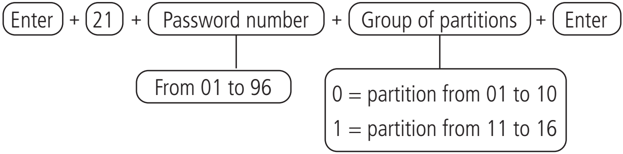
Secondary passwords that are created (01 to 96) will be allowed to enable/disable the entire system and can be enabled to have the following accesss/permissions according to the needs of each installation.

- **Partition:** passwords with this permission will only be allowed to enable/disable the partitions (01 to 16) previously selected via command.
- **Only active:** the selected passwords can enable the system, but will not be allowed to disable.
- **Bypass:** initially, only the master password is allowed to perform temporary zone cancellation (bypass), the passwords selected for this function will be allowed to cancel zones at the time of system activation.
- **Partial (stay):** passwords with this function enabled will be able to activate the control panel, leaving only the environment enabled where there are no zones that have been configured for Partial mode (stay). 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 from 01 to 96, for example, user 15's password can have at the same time permission to only enable partition 01, enable *Partial* mode (stay) and also perform zone override of partition 01.

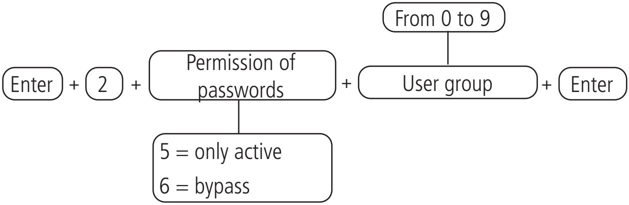
The commands to enable/disable the permissions described above are exposed below:

*Partition Permission*


Enter
+
21
+
Password number
+
Group of partitions
+
Enter
From 01 to 96
0 = partition from 01 to 10
1 = partition from 11 to 16

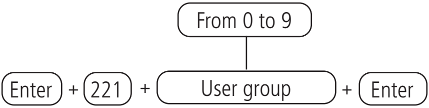
After entering the command, using the XAT 8000 keyboard, mark which partitions the password will be allowed to, using the numbers on the keyboard to leave marked for the partition. Select 0 for partition group 1 to 10 and 1 for partition 11 to 16. After changing the configured value, press the *Enter*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

*Permission to only activate or bypass permission*


From 0 to 9
Enter
+
2
+
Permission of passwords
+
User group
+
Enter
5 = only active
6 = bypass

Use the keys on the keyboard to enable permissions to activate and bypass only for users from positions 01 to 96, so that the corresponding numbers you 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 setting, press the *Back/Exit* key that no programming will be changed.

*Allowing for* Partial *mode (stay)*



Use the keys on the keyboard to enable permissions to stay for users from positions 01 to 96, so that the corresponding numbers you 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 setting, press the *Back/Exit* key that no programming will be changed.

## 6.9. Quick setup for SMS monitoring and programming

In this section the processes for reporting events for monitoring companies through the phone line channels, IP communication and GPRS connection are briefly described. The option to send SMS is also described.

For more details on these programming please refer to the *6.16. Telephony and Monitoring Settings* section.

### Monitoring via phone line

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

***Note:*** after inserting each command and confirming with the Enter key, two quick beeps must be heard, indicating that the programming was accepted, otherwise, there was some error.

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

*Enter + installer password* (factory default: *9090*)

» **Schedule monitoring account**

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

After the command, enter the 4-digit monitoring account number and press the *Enter* key to confirm.

» **Program phone number for monitoring company**

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

- **Program the reporting mode as Phone Adjust and Communication Protocol for Phone 1 and 2 as Contact-ID**

  *Enter + 17 + 1 + 0 + 0 + Enter*

- **Program the number of attempts to report 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 default DTMF level stored in the alarm center memory does not work, type the following command and test all the options from 0 to 6 to see which one gives the best result.

  *Enter + 18 + Enter + N + Enter, where N= level from 0 to 6*

- **Exit programming mode with the installer password or enter a new command**

  Installer password (factory standard: *9090*).

### Monitoring via Ethernet/Wi-Fi

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

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

***Note:*** the alarm center connects only with 2.4GHz routers.

- **Entering the programming mode with the installer password**

  *Enter + installer password* (factory default: *9090*)

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

  *Enter + 850 + Enter + Insert network name + Enter*

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

  *Enter + 851 + Enter + Insert network password + Enter*

- **Enable Wi-Fi/define type of network configuration 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 |

***Note:*** *» After inserting each command and confirming with the* Enter *key, two quick beeps must be heard, indicating that the programming was accepted, otherwise, there was some error.*

*» The network name and password must be entered exactly as it was defined in the router considering the upper and lower case letters. To change between upper and lower case, press the* Disable *key.*

» **Schedule monitoring account**

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

After the command, enter the 4-digit monitoring account number and press the *Enter* key to confirm.

» **Programming the reporting mode**

*Enter + 17 + 4 + 0 + 0 + Enter*

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

*Enter + 19 + 0 + Enter*

» **Program target IP**

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

After the command, enter 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 target domain name (DNS)**

If you don't want to use DNS, go 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 keys on the keyboard, 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 the 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 perform the next steps, where netmask, gateway, etc., will be added manually and not received from the connected network.

  *Enter + 831 + Enter*

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

- **Programming the network mask**

  *Enter + 8130 + Enter*

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

- **Programming the gateway**

  *Enter + 8140 + Enter*

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

- **Programming DNS Servers for Ethernet**

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

  After the command, enter 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 ranging from 000 to 255 minutes (factory default: *5 minutes*)

- **Exit programming mode with installer password**

  Installer password (factory standard: *9090*)

- **Check connection to IP Receiver service**

  Press the *Menu* key, navigate through the arrow keys, access the *Connections* option and check if the marking for the *Eth: IP1* and/or *IP2* is enabled. If so, the unit is connected via Ethernet with the IP receiver software through the IPs that have been enabled.

### Monitoring via GPRS

The control panel can report events via 2G/3G/4G channels (XAG 8000, XAG 8000 3G, or XG 4G module required) to monitoring companies. Events will be sent to monitoring companies using the GPRS channel to send messages to IP addresses, as well as the Ethernet connection. The commands to be programmed are as follows:

***Note:*** after inserting each command and confirming with the Enter key, two quick beeps must be heard, indicating that the programming was accepted, otherwise, there was some error.

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

*Enter + installer password* (factory default: *9090*)

» **Schedule monitoring account**

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

After the command, enter the 4-digit monitoring account number and press the *Enter* key to confirm.

» **Programming the reporting mode**

*Enter + 17 + 4 + 0 + 0 + Enter*

» **Program communication priority (2G/3G/4G only)**

*Enter + 19 + 1 + Enter*

» **Program target IP**

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

After the command, enter 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 target domain name (DNS)**

If you don't want to use DNS, go 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 keys on the keyboard, 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 the monitoring company 2 and press the *Enter* key to confirm.

- **Enable the chip to be used**

  *Enter + 832 + Enter*

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

- **Program login**

  *Enter + 822 + O + Enter*, where O = 1 or 2 (Operator 1 ou Operator 2)

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

- **Program password**

  *Enter + 823 + O + Enter*, where O = 1 or 2 (Operator 1 ou Operator 2)

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

- **Program APN**

  *Enter + 824 + O + Enter*, where O = 1 or 2 (Operator 1 ou Operator 2)

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

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

  If you wish to use the PIN, execute the command shown in the sequence, otherwise move to the next command.

  If the PIN is incorrect the chip will be locked.

  *Enter + 825 + O + PIN number with 4 digits + Enter*, where O = 1 or 2 (Operator 1 or Operator 2)

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

  *Enter + 827 + TTM + Enter*, onde TTM = Heartbeat interval time 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 entering the command, enter the DNS server code (according to the server used) and then press the*Enter* key to confirm.

» **Interval between GPRS connections attempts**

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

» **Exit programming mode with installer password**

Installer password (factory standard: *9090*)

» **Check the 2G/3G/4G signal level**

Press the *Menu* key, navigate through the arrow keys, access the *2G/3G/4G Signal* option and check the signal through the 1 to 10 markings.

» **Check connection to IP Receiver service**

Press the *Menu* key, navigate through the arrow keys, access the *Connections* option and check if the marking for the *2G/3G/4G:* option *IP1* and/or *IP2* is filled. If so, the unit is connected via GPRS with the IP receiver software through the chips that have been enabled.

### Program SMS

**Attention:** as of version 1.7.9, all functions related to SMS (sending and receiving) for the AMT 8000 central were removed.

Alarm center can send information messages via SMS to the programmed mobile phones. The commands to be programmed are as follows:

***Note:*** after inserting each command and confirming with the Enter key, two quick beeps must be heard, indicating that the programming was accepted, otherwise, there was some error.

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

*Enter + installer password* (factory default: *9090*)

» **Program GPRS channel options to enable chips and SMS sending/receiving**

*Enter + 832 + Enter*

After the command, use the keys on the keyboard to enable *1 (chip 1), 2 (chip 2), 3 (send SMS), 4 (receive SMS)* options and press the *Enter* key to confirm.

» **Select SMS events**

*Enter + 833 + Enter*

After the command, use the keys on the keyboard to enable *1, 2, 3, 4* options and press the *Enter* key to confirm.

- **Program phone to SMS**

  *Enter + 84 + M + Phone number with up to 20 digits + Enter*, where M = memory number ranging from 1 to 5.

  The phone number must be a maximum of 20 digits and in format: *0 + operator code + area code + phone number starting with the digit 9.*

- **Exit programming mode with installer password**

  Installer password (factory standard: *9090*).

- **Test to check if the SMS configuration worked**
  - **Test receiving SMS:** activate the alarm center and wait for the reception of the activation event by SMS.
  - **Test send SMS:** deactivate the alarm center manually and then send an SMS message using the mobile phone in the following way: *!Master Password A!*, if the master password is, for example, 1234 the command will be: *!1234A!*. Wait and check if the alarm center has been activated.

## 6.10. Zone settings

Zone settings can be made to suit/define features that best fit the alarm center's operating environment.

The following table shows in which group the zone is, being divided into 10 and the keys on the keyboard referring to each zone, according to the group chosen.

| Group | Zones 1 to 10 | Group | Zones 11 to 20 | Group | Zones 21 to 30 |
|---|---|---|---|---|---|
| 0 | Key 1 = zone 1<br>Key 2 = zone 2<br>Key 3 = zone 3<br>Key 4 = zone 4<br>Key 5 = zone 5<br>Key 6 = zone 6<br>Key 7 = zone 7<br>Key 8 = zone 8<br>Key 9 = zone 9<br>Key 0 = zone 10 | 1 | Key 1 = zone 11<br>Key 2 = zone 12<br>Key 3 = zone 13<br>Key 4 = zone 14<br>Key 5 = zone 15<br>Key 6 = zone 16<br>Key 7 = zone 17<br>Key 8 = zone 18<br>Key 9 = zone 19<br>Key 0 = zone 20 | 2 | Key 1 = zone 21<br>Key 2 = zone 22<br>Key 3 = zone 23<br>Key 4 = zone 24<br>Key 5 = zone 25<br>Key 6 = zone 26<br>Key 7 = zone 27<br>Key 8 = zone 28<br>Key 9 = zone 29<br>Key 0 = zone 30 |

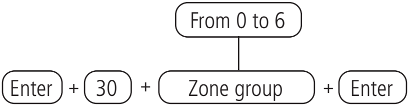
| Group | Zones 31 to 40 | Group | Zones 41 to 50 | Group | Zones 51 to 60 |
|---|---|---|---|---|---|
| 3 | Key 1 = zone 31 | 4 | Key 1 = zone 41 | 5 | Key 1 = zone 51 |
| | Key 2 = zone 32 | | Key 2 = zone 42 | | Key 2 = zone 52 |
| | Key 3 = zone 33 | | Key 3 = zone 43 | | Key 3 = zone 53 |
| | Key 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 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 fire when the alarm center is activated using a remote control, or when trying to activate the alarm center using a valid password, the keyboard beeps 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 numbers that you wish to have the zone active remain marked and the zones that should remain inactive remain unchecked, then confirm with the *Enter* key.

**Note:** All zones leave the factory enabled.

### *Partial* mode (stay)

When the system is activated in *Partial* mode (stay), only the zones defined for this mode when violated/activated will not generate triggering. 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 activating only the outer perimeter zones. Zones defined as *Partial* mode can belong to any alarm center partition.

To program, type:

From 0 to 6

Enter + 02 + Zone group + Enter

Use the keys on the keyboard to define which zones will have *Partial* mode (stay), so that the numbers that you want to have the zone with *Partial* mode, remain marked and the zones without the function remain unchecked, then confirm with the *Enter* key.

***Note:*** if the alarm center is activated in Full mode, all zones, including those defined as Partial mode, will be activated, so it will also happen with the center's partition activation, activating the zones defined as Partialmode.

### Zone Functions

The zones of the alarm center leave the factory configured as immediate, i.e. when are violated they generate the immediate event/fire, but can be configured for the following functions:

» **Timed zone for input:** allows you to define which zones will be timed when the alarm center is activated. If a timed zone is opened/violated with the center activated, the input timing will start and the system must be deactivated before the end of the timing for the alarm not to trigger. If a non-timed zone is opened before the system is deactivated, the alarm will trigger immediately. To set the time, refer to the *Input Timing* section.

» **Follower zone:** this setting is valid only if used in conjunction 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 passed through a timed zone before, the behavior will be immediate zone.

» **24 hour zone:** in this setting, the zone remains activated 24 hours a day, even when the system is deactivated. It can be configured for audible or silent triggering. To set the type of trip, see *Zone operation mode.*

» **Panic zone:** this function is designed to request help in a hazardous situation. The moment the zone is violated, the panic event will be reported to the monitoring company. You can program this function in *Audible* or *Silent* mode. To set the type of trip, see *Zone operation mode section.*

- **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. 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 contacts (NO) and to configure the zone, be in this mode, see *Zone operation mode section.*

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

To program this function, type:

Enter + 3 + Zone Functions + Zone group + Enter

Zone Functions: From 1 to 6

Zone group: From 0 to 6

| Zone Functions | |
|---|---|
| 1 | Timed |
| 2 | Follower |
| 3 | 24 Hour |
| 4 | Panic |
| 5 | Medical emergency |
| 6 | Fire |

Use the keys on the keyboard to define the function of the zone, so that the numbers that you want to have the zone with the given function remain marked and the zones without the function remain unchecked, then confirm with the *Enter* key.

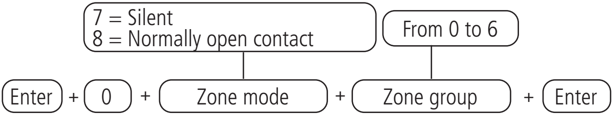
***Note:*** each zone can have only one function and if programming is done in a zone already configured with another function, the last programming done will remain operational.

### Zone operation mode

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

- **Silent:** If there is a trigger in a zone configured for *Silent*mode, the siren will not be triggered, but the corresponding event will be sent to the security company/registered applications and the programmed personal phones will be called.
- **Normally open contact:** zones leave the factory prepared for the use of normally closed contact (NC) sensors. If you wish to use sensors with normally open contact (NO), e.g. fire sensors (via TX 8000), activate this operating mode at the center for the corresponding zone.

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



Use the keys on the keyboard to define the zone mode, so that the reference numbers, which you wish to have the zone with the given mode, remain marked and the zones without the mode remain unchecked, then confirm with the *Enter* key.

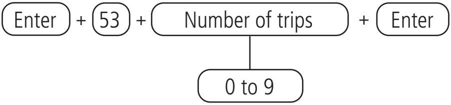
***Note:*** *The settings made on a sensor are only effective after the tamper has been activated, triggered or the respective synchronism button has been pressed quickly.*

### Automatic zone cancellation

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

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

To program this function, type:



To edit/view the programmed value, type:

Enter + 53 + Enter

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

### Alloy input (from version 1.9.2)

*Alloy input zone*

This function allows you to program a zone to activate or deactivate the control panel. The Zone ranges from 01 to 64. If you program 00, the Input On function will be disabled.

To program this function, type:

Enter + 0953 + Zone + Enter

Zones 01 to 64

To edit / view the programmed value, type:

Enter + 09 + Enter

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

### Alloy input 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.

Enter + 516 + Partition group + Enter

0 or 1

After entering the command, using the XAT 8000 keyboard, mark which partitions will be activated by the input input function, using the numbers on the keyboard to leave it marked for the partition. Select 0 for the partition group 1 through 10 and 1 for partitions 11 through 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 activate and / or deactivate the alloy input

Allows the input to only activate the control panel, only to disable the control panel or both.

Enter + 518 + Enter

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

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

## 6.11. Programming the alarm center partitioning

### Enable partitioning

To enable alarm center partitioning (the center can have up to 16 partitions with independent activation/deactivation and event reporting), it must be programmed:

Enter + 510 + Enter

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

### Partitioning the zone

When 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 full password) and deactivated whenever one of them receives the command to deactivate.
- **Zone set to one of the partitions:** The zones so set will be activated/deactivated when the desired partition (01 to 16) is activated/deactivated or when the system is activated in *Partial* mode (stay).

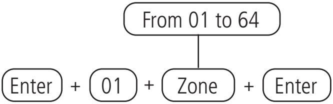
To choose which partition a particular zone (sensor) should belong to, program:

From 01 to 64

Enter + 01 + Zone + Partition + Enter

00 = Common zone
01 to 16 = Defined Partition

To edit/view the programmed zone partition, enter:

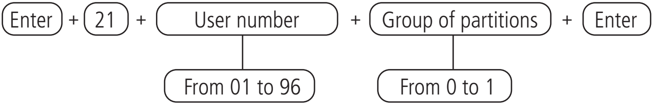

From 01 to 64
Enter
+
01
+
Zone
+
Enter

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

**Note:** If no zones are defined to the partition, it will be inactive.

### Password Partitions

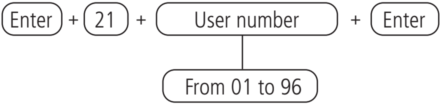
Secondary passwords that are created (01 to 96) leave the factory without permission to operate partitions. When enabling partitioning you must select which partitions you will be allowed to Enable/Disable using the following command.


Enter
+
21
+
User number
+
Group of partitions
+
Enter
From 01 to 96
From 0 to 1

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

**Attention:** besides the above mentioned programming points, user passwords must be created/defined (topic *Passwords*) besides registering wireless controls for access (topic *Remote controller*) and also define partitioning of keyboards (topic *Keyboard*) and sirens (topic *Wireless sirens*).

To edit/view the programmed value, type:


Enter
+
21
+
User number
+
Enter
From 01 to 96

## 6.12. Timings

### Input Timing

The input timing is used when you want to have a time to enter the protected environment and deactivate the unit without triggering the alarm (it is necessary to enable the zone as timed, see *Zone functions section*).

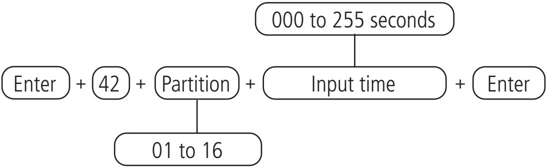
When it is activated, if any sensor connected to the timed zone is triggered, the unit stores the violation and waits for the programmed time to trigger the alarm. Therefore, if the unit is not deactivated during this period, the alarm will be triggered even if the sensor has returned to normal.

This time is programmable from 000 (timing deactivated) to 255 seconds. The timing leaves the factory programmed for 30 seconds (non-partitioned or partitioned system applying to all partitions). On non-partitioned systems, program the input time with the partition address being *01*.

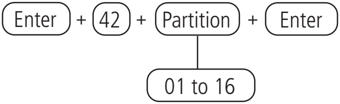
***Note:*** » The output beep on the keyboard exits the factory enabled mode and will not beep for security measure on the keyboard when counting the input time.

- » When the keyboard is closed and we activate the alarm center through the application AMT MOBILE V3 or GUARDIAN, even with the Output Beep function on the keyboard is enabled it will not emit the Beep.

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 setting, press the *Exit* key and no programming will be changed.

### Output Timing

Output timing is used when you want to activate the alarm center from the keyboard, and have time to leave the site before the alarm triggers.

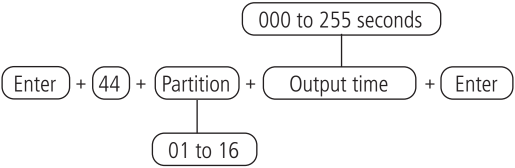
This time is programmable from 000 (timing deactivated) to 255 seconds and leaves the factory programmed for 30 seconds.

If the timing is programmed, when the alarm center is activated by the keyboard, it will beep every 1 second, and in the last 5 seconds of the timing, the beeps will be faster.

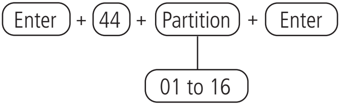
All zones of the partition to be programmed will be affected by the output timing, except for zones programmed as 24 hours, Panic, Medical Emergency or Fire.

The output timing is valid only for activation of the unit via keyboard. When activation is done via remote control the timing will always be zero (instantaneous). On non-partitioned systems, program the output 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 setting, press the *Exit* key and no programming will be changed.

### Disable Beep Out

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

To program this function, type:

Enter + 514 + Enter

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

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

## 6.13. Alarm Center Time Settings

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

**Clock**

To set the clock, type:

Enter + 400 + Hours + Minutes + Seconds + Enter

Hours: hh
Minutes: mm
Seconds: ss

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 setting, press the *Exit* key and no programming will be changed.

**Calendar**

To set the calendar, type:

Enter + 401 + Day + Month + Year + Enter

Day: DD
Month: MM
Year: AA

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 setting, press the *Exit* key and no programming will be changed.

***Note:*** If the clock and calendar are not programmed correctly, the alarm center will operate normally, but the date and time of events stored in the internal buffer will not correspond to the actual date and time, and also the holiday setting and self-activation may not operate correctly.

### Weekday adjustment

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

To program this function, type:

From 1 to 7
1 = Sunday
7 = Saturday

Enter + 402 + Weekday + 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 setting, press the *Exit* key and no programming will be changed.

### Time interval for date and time synchronization

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 (24 hour factory standard synchronization), for third party software they should be consulted. The synchronization will occur in the following situations:

- At the programmed time interval.
- At the moment that the alarm center is connected to the mains.
- If the date and time are changed manually.
- If the connection to the server is down.

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 setting, press the *Exit* key and no programming will be changed.

### Time zone command

Timezone (as of version 2.0.8).

When the control panel 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 + Spindle + Enter

00 - Desabilitado
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 scheduled interval, enter:

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.

## 6.14. Periodic Test

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

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

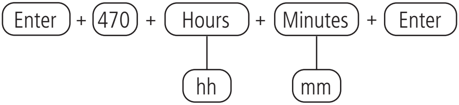
The *Periodic Test* function can operate in two modes:

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

***Note:*** *if you wish to use the Periodic Test by Time in conjunction 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 test by time

To program this function, type:



To cancel the periodic test by time, type:

Enter + 470 + Deactive + Enter

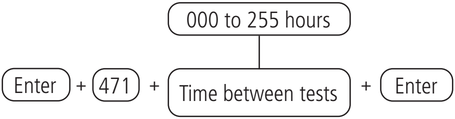
To edit/view the programmed value, type:

Enter + 470 + Enter

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

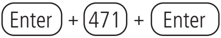
### Periodic test by time interval

To program this function, type:



***Note:*** To deactivate the periodic 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 setting, press the *Exit* key and no programming will be changed.

## 6.15. Autoactivation

With this function enabled, the alarm center will activate if all zones are closed and there is no movement in the environment 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 centers, the *Autoactivation* when executed, will be exercised on all partitions with the partition autoactivation option enabled. If you want to use Partition Autoactivation, refer to *Program the Partitioning of the Alarm Center*.

The following are examples of using autoactivation:

» Example 1

In a place where there is no fixed time to activate the alarm center we can program the *Autoactivation by inactivity* to occur whenever all sensors are closed, for example, for 50 minutes. This time should be chosen according to the site routine. If it is very busy, the time may be shorter. If there is little movement of people, the time should be longer, to prevent the alarm center from being activated in an unwanted hour.

» Example 2

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

Programmed and Inactivity Autoactivation can be used together. For example, if you want the center to be automatically activated by inactivity only after 10:00pm.

For this programming we have 3 examples that explain the alarm center's Autoactivation, displayed below, considering that the Programmed Autoactivation will be at 10:00pm and the inactivity time will be 10 minutes:

1. A sensor (opening and closing) was detected at 9:50pm, so the center will automatically activate at 10:00pm.
2. A sensor (opening and closing) was detected at 9:55pm, so the center will automatically activate at 10:05pm.
3. One sensor (open only) was opened at 9:59pm and this sensor remained open until 10:30pm, then the center will automatically activate at 10:40pm.

### Autoactivation by Inactivity

With this function programmed, the alarm center will be activated as soon as the time set for the zones to remain closed is achieved. The time must be entered with two digits from 00 to 99 minutes. If 00 is entered, the Autoactivation by Inactivity will be cancelled.

To program this function, type:

00 to 99 minutes

Enter + 460 + Inactivity time + Enter

To edit/view the programmed value, type:

Enter + 460 + Enter

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

### Programmed Autoactivation and Autodisactivation

These functions allow you to activate and deactivate the system automatically at pre-programmed times, one for each weekday and one more special for holidays. To use the function, follow the procedure:

1. Select the days of the week on which Autoactivation will occur;
2. Select the days of the week for Autodeactivation;
3. Schedule the desired times;

4. Adjust the system date and time;
5. Adjust the day of the week;

   ***Note:*** *to adjust the day of the week, consult the programming in topic 6.13 Time settings of the control panel.*

6. If you want to enable automatic time and date synchronization with the server (make sure you are using the latest version of Intelbras IP Receiver for the correct effect).

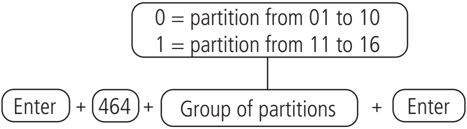
Use the table below for the following required settings:

| Key | Weekday |
|---|---|
| Key 1 | Sunday |
| Key 2 | Monday |
| Key 3 | Tuesday |
| Key 4 | Wednesday |
| Key 5 | Thursday |
| Key 6 | Friday |
| Key 7 | Saturday |
| Key 8 | Holiday |

*Selecting Autoactivation and Autodeactivation by Partitions*

Selects which partitions will have the autoactivation and autodeactivation function programmed. Factory default, all partitions enabled.

To program this function, type:

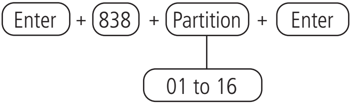


Use the keyboard to enable the function on the partitions, partitions 01 through 10 are in partition group 0 and partitions 11 through 16 are in partition group 1, so that the corresponding numbers for the partitions you want to have the function enabled remain marked on the display and then confirm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

***Note:*** *if all partitions are selected, autoactivation will only occur if all zones of the center are closed.*

### *Days of the week for autoactivation*

Select the days on which Partition Autoactivation will occur.


Enter
+
838
+
Partition
+
Enter
01 to 16

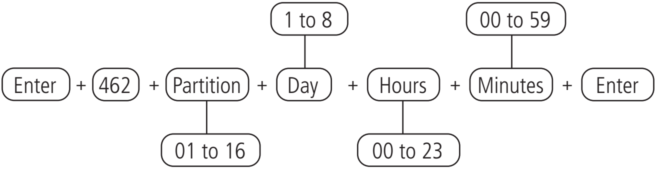
Use the keyboard to set the days for partition autoactivation occurs, so that the numbers you want to have the days enabled remain checked and the days with the disabled function remain unchecked, then confirm with the *Enter* key.

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

### *Autoactivation time*

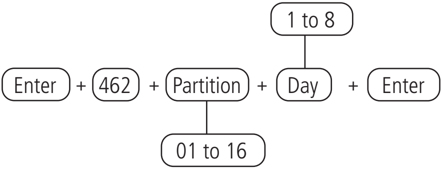
Select the time on which Partition Autoactivation will occur.

To program this function, type:


1 to 8
00 to 59
Enter
+
462
+
Partition
+
Day
+
Hours
+
Minutes
+
Enter
01 to 16
00 to 23

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

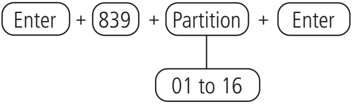
To edit/view the programmed value, type:


1 to 8
Enter
+
462
+
Partition
+
Day
+
Enter
01 to 16

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

### *Weekdays for Autodeactivation*

Select the days on which Partition Autodeactivation will occur.


Enter
+
839
+
Partition
+
Enter
01 to 16

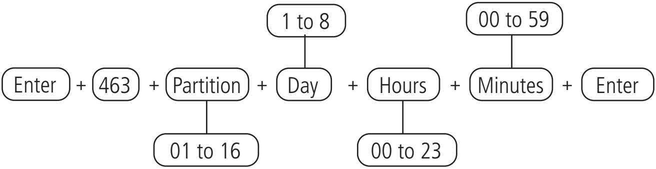
Use the keyboard to set the days for partition autodeactivation occurs, so that the numbers you want to have the days enabled remain checked and the days with the disabled function remain unchecked, then confirm with the *Enter* key.

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

#### *Autodeactivation time*

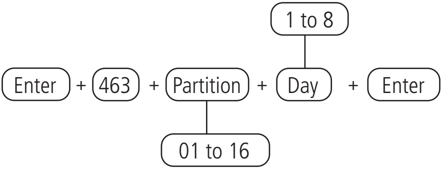
Select the time on which Partition Autodeactivation will occur.

To program this function, type:


1 to 8
00 to 59
Enter
+
463
+
Partition
+
Day
+
Hours
+
Minutes
+
Enter
01 to 16
00 to 23

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

To edit/view the programmed value, type:


1 to 8
Enter
+
463
+
Partition
+
Day
+
Enter
01 to 16

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

### Holidays

Alarm center has 10 memories (0 to 9) to schedule dates that require a special time for Autoactivation and Autodeactivation.

When the system date is the same as one of the programmed dates, the settings of the weekday will be superimposed by the times programmed in the address of the commands described above, referring to the programming of autoactivation of the alarm center.

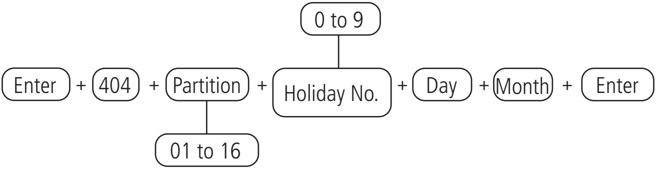
For the correct operation of this function it is necessary to check whether the following programmed autoactivation and autodeactivation schedules are enabled correctly:

- Days for programmed autoactivation.
- Time for programmed autoactivation.
- Days for programmed autodeactivation.
- Time for programmed autodeactivation.
- Weekday adjustment
- Time interval for date and time synchronization.

### *Set holidays for Autodeactivation/Autodeactivation.*

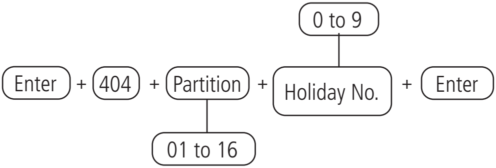
If the center is partitioned, holidays can be defined per partition.

To program this function type:



**Note:** » *in the above command for 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 setting, press the *Exit* key and no programming will be changed.

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

## 6.16. Telephony and Monitoring Settings

AMT 8000 alarm center was specially developed to be monitored remotely, that is, a contractor can monitor several events in real time, for example:

- » System activation and deactivation.
- » Lack of power.
- » Violation of the system (triggering).
- » Fault in the phone line.
- » Violation of the sensors (tamper).
- » Siren failure.

When an event occurs, the alarm center will contact the monitoring company and will transmit via DTMF or IP (Ethernet, Wi-Fi or 2G/3G/4G) the event occurred (internal buffer for 512 events).

***Note:*** *for monitoring via telephone line, the FXO 8000 expander module must be added to the control panel and for monitoring via GPRS, the GPRS module (XAG 8000, XAG 8000 3G or XG 4G) is required.*

### Contact-ID Events

The alarm center leaves the factory with all events enabled and with the standard Contact-ID code corresponding to these events.

In the standard configuration of the programmable Contact-ID protocol the following events will be sent with the most common event codes. This will eliminate the need to register new events in the monitoring software, but the information will not be as full as in the complete Contact-ID protocol. See below for a list of Contact-ID events.

| **Event** | **Standard code** |
|---|---|
| Medical emergency | 100 |
| Fire alarm | 110 |
| Panic | 120 |
| Activation and deactivation under duress | 121 |
| Silent panic | 122 |
| Zone triggering/Zone restoration | 130 |
| 24 hour zone triggering | 133 |
| Silent triggering | 146 |
| AC mains failure/AC mains restoration | 301 |

| | |
|---|---|
| Low System Battery/Restore System Battery | 302 |
| System Reset | 305 |
| Programming change | 306 |
| Absent Battery/Restoration Battery | 311 |
| Phone line Cut/Restore Phone line | 351 |
| Failure to communicate event | 354 |
| Failure of supervision/Restoration supervision | 147 |
| Expander Device Tamper/Restore Expander Device Tamper | 145 |
| Sensor Tamper / Restore Sensor Tamper | 383 |
| Low Battery of Wireless Device/Restoration Device Battery | 384 |
| System Activation/Deactivation | 401 |
| Automatic Activation/Deactivation | 403 |
| Remote Activation/Deactivation | 407 |
| Activation by a key | 408 |
| Remote access | 410 |
| Incorrect password | 461 |
| Registration/deletion of RF | 533 |
| Registration/change/deletion of password | 534 |
| Enable/disable zones | 535 |
| Partial activation of the system | 456 |
| Zone Bypass/Restoration Zone Bypass | 570 |
| Periodic Test | 602 |
| Manual testing | 601 |
| Maintenance request | 616 |
| Event Buffer Reset | 621 |
| Restart date and time | 625 |

***Note:*** some event codes may not be registered in allmonitoring software. If necessary, register the corresponding comment, because these events facilitate the identification and solution of problems.

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

| Device type | Index/address initial | Index/address final |
|---|---|---|
| Sensor/zone | 001 | 064 |
| Remote control activation/ deactivation | 100 | 197 |
| Keyboard activation/deactivation | 200 | 297 |
| Keyboard failures | 201 | 216 |
| Siren failures | 301 | 316 |
| Amplifier failures | 401 | 404 |
| PGM 8000 wireless actuator | 501 | 516 |

The following are examples of sending *Contact-ID* events to the devices:

- **Sensor trip in zone 01:** event *130* (factory standard) and with user/zone being *001*.
- **Sensor trip in zone 25:** event *130* (factory standard) and with user/zone being *025*.
- **Sensor communication failure in zone 12:** event *147* (factory standard) and with user/zone being *012*.
- **Sensor reset in zone 64:** event *130* (factory standard) and with user/zone being *064*.
- **Sensor tamper in zone 05:** event *383* (factory standard) and with user/zone being *005*.
- **Siren tamper registered at address 09:** event *145* (factory standard) and with user/zone being *309*.
- **Keyboard communication failure registered at address 01:** event *381* (factory standard) and with user/zone being *201*.

As can be seen in the following commands, according to the registered Contact-ID code, the event may be blocked if configured as 000 (will not be sent to the IP Receiver). The registration of the Contact-ID code can be done according to the available options of Contact-ID code, or even, when registering FFF will cause the option that is registered with this value to send to the monitoring company the default Contact-ID code.

The following tables show the events and the respective standard Contact-ID codes:

**Events of the opening type**

**Zone triggering**

| Zone no. | Event | Contact-ID Code |
|---|---|---|
| 01 to 64 | Zone triggering | 130 |

The commands relating to the Contact-ID, more specifically the Programmable Contact-ID, the communication protocol must be set to Programmable Contact-ID, otherwise events will be sent with the standard Contact-ID. Refer to the topic *Reporting*mode, in the part explaining the Phone Protocol 1/2.

Use the table above to perform the *Contact-ID* event change command for zone triggering described below:

Enter + 901 + Zone N° + Enter

Zone N°: 01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* key and no programming will be changed.

**Events of the restoration type**

**Zone triggering**

| Zone no. | Event | Contact-ID Code |
|---|---|---|
| 01 to 64 | Restoration of zone triggering | 130 |

Use the table above to perform the *Contact-ID* event change command for zone restoration described below:

Enter + 911 + Zone N° + Enter

01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* key and no programming will be changed.

**Events of the opening type**

**Sensor tamper**

| Zone no. | Event | Contact-ID Code |
|---|---|---|
| 01 to 64 | Sensor tamper | 383 |

Use the table above to carry out the *Contact-ID* event change command for zone sensor tamper triggering, as described below:

To edit/view the programmed value, type:

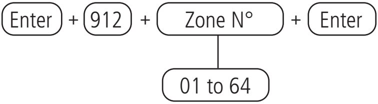
Enter + 902 + Zone N° + Enter

01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* key and no programming will be changed.

| Events of the restoration type | | |
|---|---|---|
| **Sensor tamper** | | |
| Zone no. | Event | Contact-ID Code |
| 01 to 64 | Sensor tamper restoration | 383 |

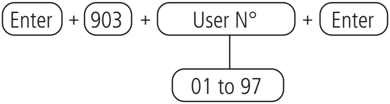
Use the table above to carry out the *Contact-ID* event change command for zone sensor tamper restoration, as described below:



After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* key and no programming will be changed.

| Events of the opening type | | |
|---|---|---|
| **User Deactivation** | | |
| User no. | Event | Contact-ID Code |
| 01 to 97 | User Deactivation | 401 |

Use the table above to perform the *Contact-ID* event change command to deactivate each registered user, as described below:



After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* and no programming will be changed.

**Events of the restoration type**

**User Activation**

| User no. | Event | Contact-ID Code |
|---|---|---|
| 01 to 97 | User Activation | 401 |

Use the table above to perform the *Contact-ID* event change command to activate each registered user, as described below:

To edit/view the programmed value, type:

Enter + 913 + User N° + Enter

01 to 97

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* and no programming will be changed.

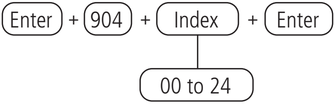
**Events of the opening type**

**System events**

| Index | Internal event | Standard code |
|---|---|---|
| 00 | Battery low of wireless device | 384 |
| 01 | N/A | 344 |
| 02 | Failure of supervision | 147 |
| 03 | Zone bypass | 570 |
| 05 | AC mains failure | 301 |
| 06 | Low system battery | 302 |
| 07 | Absent battery | 311 |
| 08 | Phone line cut | 351 |
| 09 | Remote deactivation | 404 |
| 10 | Automatic deactivation | 403 |
| 11 | N/A | 408 |
| 12 | N/A | 121 |
| 13 | System Reset | 305 |
| 14 | Programming change | 306 |
| 15 | Failure to communicate event | 354 |
| 16 | Incorrect password | 461 |
| 17 | Remote access | 410 |
| 18 | Manual testing | 601 |
| 19 | Periodic Test | 602 |

| | | |
|---|---|---|
| 20 | Event Buffer Reset | 621 |
| 21 | Restart date and time | 625 |
| 22 | Expander Device Tamper/Restore Expander Device Tamper | 145 |
| 23 | Sensor Tamper / Restore Sensor Tamper | 383 |
| 24 | Maintenance request | 616 |
| 25 | AC wireless device failure | 342 |
| 26 | PGM activation | 422 |

Use the table above to perform the change command to open system events , as described below:



After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Exit* key and no programming will be changed.

**Events of the restoration type**

**System events**

| Index | Internal event | Standard code |
|---|---|---|
| 00 | Restoration of low battery wireless device | 384 |
| 01 | N/A | 344 |
| 02 | Restoration of supervision failure | 147 |
| 03 | Zone bypass restoration | 570 |
| 05 | AC mains restoration | 301 |
| 06 | Low system battery restoration | 302 |
| 07 | Battery restoration | 311 |
| 08 | Phone line restoration | 351 |
| 09 | Remote Activation | 404 |
| 10 | Automatic Activation | 403 |
| 11 | Activation by a key | 408 |
| 12 | Activation under duress | 121 |
| 13 | N/A | 305 |
| 14 | N/A | 306 |
| 15 | N/A | 354 |
| 16 | N/A | 461 |
| 17 | N/A | 410 |
| 18 | N/A | 601 |

| | | |
|---|---|---|
| 19 | N/A | 602 |
| 20 | N/A | 621 |
| 21 | N/A | 625 |
| 22 | Tamper of expansion devices | 145 |
| 23 | Tamper sensors | 383 |
| 24 | N/A | 616 |
| 25 | AC wireless device failure | 342 |
| 26 | PGM activation | 422 |

Use the table above to perform the change command to restore system events , as described below:

Enter + 914 + Index + Enter

00 to 24

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the *Enter* key to confirm. If you only want to view the setting, press the *Back/Exit* key that no programming will be changed.

### ***Push* Events**

Notifications that will be sent to the Intelbras Guardian application when the corresponding event occurs with the alarm center, and the alarm center must be connected to the Internet (Ethernet, GPRS or Wi-Fi).

For more information about the application, please refer to the*Utilizando aplicativo Intelbras Guardian (para dispositivos móveis)section.*

| Event Group (EV) | Event | Key | Standard Value |
|---|---|---|---|
| 0 | ARME_DESARME_USUARIO, | Key 1 | Enabled |
| | N/A | Key 2 | Enabled |
| | DISPARO_ZONA, | Key 3 | Enabled |
| | DISPARO_24H, | Key 4 | Enabled |
| | DISPARO_SILENCIOSO, | Key 5 | Enabled |
| | DISPARO_EMERGENCIA_MEDICA, | Key 6 | Enabled |
| | DISPARO_INCENDIO, | Key 7 | Enabled |
| | DISPARO_PANICO_AUDIVEL, | Key 8 | Enabled |
| | DISPARO_PANICO_SILENCIOSO, | Key 9 | Enabled |
| | TAMPER_SENSOR, | Key 0 | Enabled |

|  |  |  |  |
|---|---|---|---|
| 1 | BATEIRA_BAIXA_SENSOR, | Key 1 | Enabled |
|  | N/A | Key 2 | Enabled |
|  | FALHA_SUPERVISAO_RF, | Key 3 | Enabled |
|  | BYPASS_ZONA, | Key 4 | Enabled |
|  | BYPASS_AUTOMATICO, | Key 5 | Enabled |
|  | FALHA_REDE_ELETRICA, | Key 6 | Enabled |
|  | BATERIA_PRINCIPAL_BAIXA, | Key 7 | Enabled |
|  | BATERIA_PRINCIPAL_AUSENTE, | Key 8 | Enabled |
|  | FALHA_LINHA_TELEFONICA, | Key 9 | Enabled |
|  | ARME_DESARME_REMOTO, | Key 0 | Enabled |
| 2 | AUTO_ARME_DESARME, | Key 1 | Enabled |
|  | ARME_RAPIDO, | Key 2 | Enabled |
|  | ARME_DESARME_SOB_COACAO, | Key 3 | Enabled |
|  | RESET_SISTEMA, | Key 4 | Enabled |
|  | PROGRAMACAO_ALTERADA, | Key 5 | Enabled |
|  | FALHA_AO_COMUNICAR_EVENTO, | Key 6 | Enabled |
|  | SENHA_INCORRETA, | Key 7 | Enabled |
|  | ACESSO_DOWNLOAD, | Key 8 | Enabled |
|  | TESTE_MANUAL, | Key 9 | Enabled |
|  | TESTE_PERIODICO, | Key 0 | Enabled |
| 3 | RESET_BUFFER_EVENTOS, | Key 1 | Enabled |
|  | RESET_DATA_HORA, | Key 2 | Enabled |
|  | TAMPER_KEYBOARD, | Key 3 | Enabled |
|  | N/A | Key 4 | Enabled |
|  | SOLICITACAO_MANUTENCAO, | Key 5 | Enabled |
|  | FALHA_REDE_ELETRICA_MOD_EXPANSOR, | Key 6 | Enabled |
|  | Acionamento/desacionament_PGM | Key 7 | Enabled |

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

Enter + 92 + Push Event Group + Enter

From 0 to 3

Use the keyboard to enable the *Push*event options, so that the corresponding numbers you 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 setting, press the *Back/Exit* key that no programming will be changed.

### Panic events generated by the remote control

| Number of users | Partitions | | | | | | | | | | | | | | | | Event |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 to 97 | 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 |

***Note:***

- *User registered in only one partition the panic event will arrive in the registered partition.*
- *User registered for more than one partition, the generated panic event will arrive on partition 00.*
- *User without permission to partition the panic event will arrive on partition 00.*

### Reporting Mode

The alarm centre can be configured to report events to the monitoring company in one of the ways described below:

- **Deactivated:** in this mode the center will operate as an unmonitored alarm centre, not reporting events through any channel, only for applications, if used.
- **Regular Phone:** when an event occurs, the alarm center will send them through the communication channels available in the sequence: Phone 1, Phone 2, IP1, IP2, until the event is sent or the number of attempts (default *9 attempts*) is reached.
- **Double Phone:** the central will report the events that occurred to both Phone 01 and Phone 02 and, in case of failure, up to nine attempts will be made for each Phone (with this option enabled the event will not be reported via IP).
- **Regular IP:** the same operation as Regular Phone, but following the sequence IP1, IP2, Phone 1 and Phone 2.
- **Dual IP:** uses IP1 and IP2. In IP1 fault the event will be reported to Phone 01 and in IP2 fault the event will be reported to Phone 02, this if Phones 01 and 02 are registered.
- **Double Mix:** will use IP1 and phone 1.

To program this function, type:

Enter + 17 + Reporting Mode + Phone 1 Protocol + Phone 2 Protocol + Enter

Reporting Mode:

0 = deactivated
1 = regular phone
2 = not applicable
3 = double phone
4 = regular IP
5 = not applicable
6 = double IP
7 = double mix

Phone 1 Protocol: 0 or 1

Phone 2 Protocol: 0 or 1

- **Phone 1/2 Protocol:** indicates the protocol that will be used when phone 1/2 is dialed:
- **0:** Contact-ID.
- **1:** Programmable Contact-ID.

To edit/view the programmed value, type:

Enter + 17 + Enter

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

### Blocking the sending of 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 control panel is not partitioned or when a zone common to all partitions is triggered (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:

Enter + 515 + Enter

Use the 8 key on the keyboard to enable the send 00 blocking function, so that the number 8 remains marked to enable and deselected 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 phone line

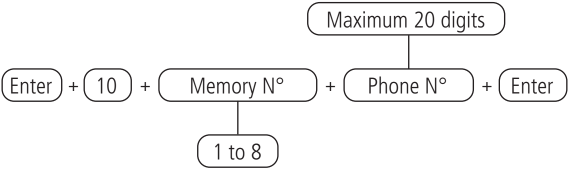
The alarm center has 8 phone memories, divided as follows:

| | |
|---|---|
| Memories 1 and 2 | Monitoring company |
| Memory 3 | Download/upload |
| Memories 4 to 8 | Personal Phones |

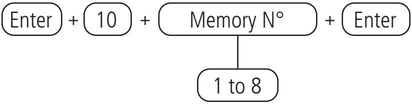
- **Monitoring company:** phones to which the center will call ifit is configured as monitored and some event is generated.
- **Download/upload:** used to configure the center remotely via a microcomputer with modem (necessary to configure only when you want to use the *Call-back* function for remote access. For simple remote access it is not necessary to configure).
- **Personal Phones:** in case of triggering or activation the *Panic*function, the center will call the programmed numbers and emit the sound of a siren for approximately 50 seconds.

*Programming/deleting and testing phone numbers*

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



To edit/view the programmed value, type:



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

To delete a previously programmed phone, type:

Enter + 10 + Memory N° + Deactive + Enter

1 to 8

To test whether the phone number has been programmed correctly, enter:

Enter + 11 + Memory N° + Enter

1 to 8

The alarm center will generate the manual test event and dial the selected phone to report this event (memories 1 and 2), start the download/upload process (memory 3), call the phones (memories 4 to 8).

***Note:*** Memory 3 test is used to start the download/upload process from the alarm centre. For example, an installer does the entire physical installation (sensors, phone, etc.), programs the download/upload phone in memory 3 and then you can execute this command so that the rest of the programming is done remotely, using a microcomputer with a modem and the installed Intelbras *AMT 8000 programmer* software.

To interrupt the phone test, enter:

Enter + 11 + Enter

### *Programming the number of ringtones*

It will set the number of phone ringtones the system should wait before answering a phone call. If set to 00, the download/upload procedure will be disabled.

This setting is only valid for download via phone line. Downloading via Ethernet/GPRS is always enabled and has no relation to this programming.

» To program this function, type:

Enter + 12 + N° of rings + Enter

00 to 20

To edit/view the programmed value, type:

Enter + 12 + Enter

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

### *Monitoring Account*

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

To program this function, type:

Enter + 15 + Partition + Enter

01 to 16

After entering the command, enter the monitoring account code always with 4 digits and being 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 and no programming will be changed.

**Note:** if the AMT 8000 alarm system is not partitioned, use the partition as01.

### *Pending Event Reset*

This command will cancel the sending of all events not transmitted, but the events remain recorded and can be accessed through the download. For example, if the system has been left without a phone line installed for some time, the event buffer can have up to 512 events not transmitted. If the *Reset Lock* is activated, it will not be possible to perform this function (see *Locks section*).

To program this function, type:

Enter + 16 + Enter

### *Forced Service*

Function used to force a call to be answered for download. When executed, the alarm center occupies the phone line even if it is not programmed to answer calls.

To program this function, type:

Enter + 14 + 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 is factory set for 9 attempts, this value can be changed respecting the limit of 1 to 9 attempts.

To program this function, type:

Enter + 13 + N° 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 setting, press the *Exit* key and no programming will be changed.

### *Level of generated DTMF signal*

It allows changing the amplitude of the generated DTMF signal to solve communication problems in places where the line signal is very low. The DTMF level adjustment should be performed at the location where the unit will operate, as the adjustment can vary from place to place and all options should be tested, starting from level 0 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 setting, press the *Exit* key and no programming will be changed.

### Monitoring via Ethernet/Wi-Fi Connection

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

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

- » **Ethernet:** It is necessary to install an RJ45 cable 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 at the alarm center, event reporting and connections will use this route, and for this at the installation site of the center must have a router or device to send the signal with good quality (check the distance between the signal replicator device and the alarm center). The alarm center when connected via Wi-Fi can also be accessed remotely through Intelbras applications.

To connect to a Wi-Fi network, the following commands are required:

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

Enter + 850 + Enter

After entering the command, use the keys on the XAT 8000 keyboard to enter the name of the network you wish 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 setting, press the *Exit* key and no programming will be changed.

***Note:*** check if the network to be connected has special characters, numbers and various symbols in its name, which if not entered can prevent connection to the correct network.

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

Enter + 851 + Enter

After entering the command, use the keys on the XAT 8000 keyboard to enter the network password you wish 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 setting, press the *Exit* key and no programming will be changed.

***Note:*** check if the network to be connected has special characters, numbers and various symbols in its password, which if not entered can prevent 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 entering the command, use the keys on the XAT 8000 keyboard to define the type of network configuration that will connect.

| 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 setting, press the*Enter* key to confirm. If you only want to view the setting, press the *Back/Exit* key that no programming will be changed.

***Note:*** *if the unit 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 will be the Wi-Fi connection. When only the Wi-Fi network is used, this will be the priority.*

In order to establish the connection via Ethernet/Wi-Fi it is necessary to make the following settings:

### *Communication priority*

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

To program this function, type:

Enter + 19 + Priority + Enter

0 - Ethernet
1 - GPRS
2 - Ethernet - GPRS
3 - GPRS - Ethernet

To edit/view the programmed value, type:

Enter + 19 + Enter

After changing the configured value, press the *Enter* key. If you only want to view the setting, 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 by this address(es) and select if the IP address or the domain name (DNS) will be used.

- **Transmission of events to IP1/DNS1:** marker filled (■) = enabled, marker empty (☐) = disabled (address must be programmed).
- **Transmission of events to IP2/DNS2:** marker filled (■) = enabled, marker empty (☐) = disabled (address must be programmed).
- **IP1 or DNS1:** marker empty (☐) = IP address will be used, marker filled (■) = domain name (DNS) will be used.
- **IP2 or DNS2:** marker empty (☐) = IP address will be used, marker filled (■) = domain name (DNS) will be used.

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

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

Enter + 830 + Enter

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

### *Destination IP address*

IP address of the computer that will receive the events from the alarm center (monitoring company). Up to two addresses (IP1 and IP2) can be programmed, regardless if the communication channel used is Ethernet, Wi-Fi or GPRS, reporting will be done to the same addresses. To receive events through 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 alarm center.

To program this function, type:

Enter + 801 + IP Address + Enter

1 - IP1
2 - IP2

After the command enter 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 setting, press the *Back/Exit* key that no programming will be changed.

**Note:** for correct operation no equal destination IP addresses must be added with the same port referring to IP1 and IP2, otherwise it will bring blocks/faults in the event reporting.

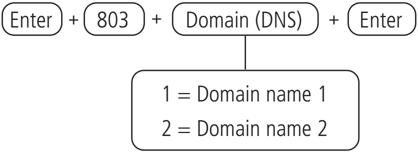
### *Destination Domain Name (DNS)*

It allows programming the address of the target computer in DNS format (Domain Name System – ex.: name.domain.xx).

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

***Note:*** There are free services available on the Internet that allow users to obtain sub-domains, which point to IP addresses, which regularly change (ex.: No-IP®, DynDNS®), but may not guarantee the continuous functioning of the system. These services usually have long update times and may go through periods of instability and even temporary absence.

To program this function, type:



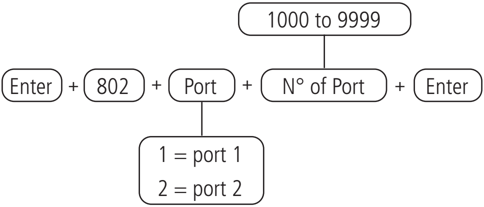
After changing the configured value, press the *Enter* key. If you only want to view the setting, press the *Back/Exit* key that no programming will be changed.

**Note:** for the correct operation no equal destination DNS addresses should be added with the same port referring to domains 1 and 2, otherwise it will bring blocks/faults in the event reporting.

*Port*

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

To edit the communication port to be used, enter:



To edit/view the programmed value, type:

Enter + 802 + Port + Enter

1 = port 1
2 = port 2

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

***Note:*** Additional values can be charged by the service provider for the use of communication ports, so should be consulted its availability and release/configuration costs.

*DNS Servers for Ethernet*

DNS server addresses available on the Internet for the resolution of names and domains (ex.: name.domain.xx).

It is recommended to adopt the servers provided by the Internet provider itself. It is also possible to opt for the use of external and free DNS servers, such as the service offered by site *www.opendns.com*. The following table presents the IP addresses of the servers. In some cases, it is possible to use the addresses of the primary servers as secondary and vice-versa.

| Company | DNS Servers | |
|---|---|---|
| | Primary or preferential (1) | Secondary or alternative (2) |
| Open DNS | 208,067,222,222 | 208,067,220,220 |

***Note:*** this information may be changed without prior notice.

To program this function, type:

Enter + 815 + Server (DNS) + Enter

1 = server 1
2 = server 2

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

### *Local Ethernet Settings*

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

### *Display of alarm center MAC*

To view the unit's MAC, perform the following procedure:

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

### *Switch IP address (cable connection)*

IP address of the local network to which the center is connected. To view/edit the IP address of the center, just perform the following procedure:

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

Enter + 8120 + Enter

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

***Note:*** *the DHCP option shown below must be disabled for manual IP change of center.*

### *DHCP*

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

To program/enable DHCP, enter:

Enter + 831 + Enter

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

***Note:*** Most ADSL modems have DHCP capability and to enable, consult your equipment manual.

#### *Network Mask*

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

Enter + 8130 + Enter

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

***Note:*** the DHCP option must be disabled for change.

#### *Gateway*

To view/edit the gateway, type:

Enter + 8140 + Enter

The current gateway will be displayed, being the factory default *192.168.001.001*, to enter/change the gateway, enter the new programming and press *Enter* to confirm the programming. If you only want to view the setting, press the *Back/Exit* key that no programming will be changed.

### Switch IP address (Wi-Fi connection)

IP address of the local network to which the panel is connected. To view / edit the control panel's IP address, simply perform the following procedure:

1. To program / change the control panel's IP address, type:

   Enter + 8620 + Enter

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

***Note:*** *the DHCP option shown below must be disabled to manually change the control panel's IP.*

### DHCP (Wi-Fi connection)

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

To program / enable DHCP, type:

Enter + 831 + Enter

Use the 1 key on the keypad to enable the DHCP of the panel, so that the number 1 remains marked to enable and unchecked to disable 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.

***Note:*** *ADSL modems, for the most part, have the DHCP feature and to activate, consult the manual of your equipment.*

### Netmask (Wi-Fi connection)

To view / edit the exchange's netmask, type:

Enter + 8630 + Enter

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

***Note:*** *the DHCP option must be disabled to change.*

### Gateway (Wi-Fi connection)

To view / edit the gateway, enter:

Enter + 8640 + Enter

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

### *Heartbeat Ethernet interval (link test)*

To check that the communication between the alarm center and the Intelbras IP Receiver software is working, the alarm center will send a message (known as Heartbeat or Keep alive) according to the programmed time interval. If Intelbras IP Receiver does not receive this message in the programmed time interval, a failure 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 setting, press the *Exit* key and no programming will be changed.

***Note:*** In order to minimize network traffic, it is recommended a time longer than 2 minutes for each test interval, being the factory default in 5 minutes.

### Monitoring via GPRS (General Packet Radio Service) connection

The control panel has a connection for reporting events and being accessed/controlled remotely via a 2G/3G/4G cellular network. This requires the installation of the XAG 8000, XAG 8000 3G, or XG 4G module with the AMT 8000 control panel.

To communicate via 2G/3G/4G, the SIM card must be enabled for a data plan. Voice service is not required. Consult your carrier to purchase the most appropriate plan for the alarm panel's data traffic.

To establish the connection, the following configurations must be completed.

*Login*

Login for connection to the 2G/3G/4G network of the operator used. This field accepts letters and numbers and can contain up to 16 digits.

The following are the standard logins of some operators.

| Operador | Login |
|---|---|
| TIM | tim |
| Claro | claro |
| Vivo | vivo |
| Oi | oi |

***Note:*** this information may be changed without prior notice. For more information, consult the operator used to enter the correct login.

To program this function, type:

Enter + 822 + Operator + Enter

1 = operator 1
2 = operator 2

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

*Password*

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

The following are the standard passwords of some operators.

| **Operador** | **Login** |
|---|---|
| TIM | tim |
| Claro | claro |
| Vivo | vivo |
| Oi | oi |

***Note:*** this information may be changed without prior notice. For more information, consult the operator used in order to enter the correct password.

To program this function, type:

Enter + 823 + Operator + Enter

1 = operator 1
2 = operator 2

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

*APN - Access Point Name*

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 packet. This field accepts letters and numbers and can contain up to 34 digits.

The following are the standard APNs of some operators.

| Operador | APN |
|---|---|
| TIM | tim.br |
| Claro | generica.claro.com.br<br>or claro.com.br |
| Vivo | zap.vivo.com.br |
| Oi | gprs.oi.com.br |

***Note:*** this information may be changed without prior notice. For more information, consult the operator used in order to use the correct APN.

To program this function, type:

Enter + 824 + Operator + Enter

1 = operator 1
2 = operator 2

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

*PIN (Personal Identification Number)*

PIN is an identification of the chip, and if it is incorrect the chip will be blocked. If the PIN of the chip used is enabled, it must be informed through the alarm centre programming mode. Because it is a password type field, the display of its contents on the LCD display is blocked.

It is also possible to set the PIN code and record it permanently on the chip with the help of a mobile phone. In this case, the 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 connections with the Internet in any equipment that uses cellular technology.

To program, type:

0000 to 9999

Enter + 825 + Operator + PIN + Enter

1 = operator 1
2 = operator 2

***Note:*** to unlock a chip if you do not have access to the PIN, it must be placed on a mobile phone and set the PUK code. If you do not have this code (or other codes such as PIN2 and PUK2), consult the operator of the chip used for other information.

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

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

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

To edit the link test interval, type:

Enter + 827 + Interval + Enter

Interval: 001 to 255 minutes

To edit/view the programmed value, type:

Enter + 827 + Enter

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

***Note:*** In order to minimize excessive data consumption, it is recommended a time longer than 2 minutes for each test interval, being the factory default in 5 minutes.

### *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 DNSs provided by the operator.

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

Enter + 828 + Server + Enter

1 = server 1
2 = server 2

After entering the command, enter the DNS server code (according to the server used) and then press the*Enter* key to confirm.

***Note:*** You can use the addresses suggested in the Obs.: valores adicionais podem ser cobrados pela prestadora de serviços para utilização de portas de comunicação, assim deve ser consultada sua disponibilidade e custos de liberação/configuração*section, however it is recommended to use the addresses provided by the operator of the chip used.*

### *Interval between GPRS connections attempts*

When a cellular modem (XAG 8000 / XAG 8000 3G / XG 4G) connection with the Intelbras IP Receiver software fails, the center tries to make a new connection with it. This function will set the time between these attempts and leave the factory at zero (00 minutes).

This feature is mainly applied in installations that use prepaid plans and has the purpose of reducing credit consumption in constant situations of connection failure, unavailability of services by the operator or the Intelbras IP Receiver software (ex.: *offline* software ).

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

To program, type:

Enter + 829 + Interval + Enter

00 to 20 minutes

To edit/view the programmed value, type:

Enter + 829 + Enter

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

### Cloud Connection

The switch is already directed to the 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:

Enter + 512 + Enter

Use the 6 key on the keyboard to enable or disable the switch's Cloud connection, so that the number 6 remains checked to disable and unchecked to enable the Cloud connection 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.

## 6.17. Functions via SMS

**Attention:** as of version 1.7.9, all functions related to SMS (sending and receiving) for the AMT 8000 central were removed.

The alarm center can send information messages via SMS to the mobile phones programmed for activation, status reporting, among others.

The necessary settings and their variables are described below, it is not necessary to configure GPRS (login, APN or password) of the chip to enable the *SMS* function.

### Sending SMS messages

The alarm centre can send information messages via SMS to the programmed mobile phones, as described below:

| Event | Message |
|---|---|
| Alarm center activation | Name of alarm center<br>Activation<br>User name |
| Deactivation of the alarm center | Name of alarm center<br>Deactivation<br>User name |
| Trigger | Name of alarm center<br>Trigger<br>Zone name |
| Audible or silent panic | Name of alarm center<br>Panic<br>Zone + Number of the programmed zone as panic or panic user |

| | |
|---|---|
| Audible or silent panic | Name of alarm center<br>Panic<br>Panic user name or zone name set as panic |
| Activation or deactivation with the duress password | Name of alarm center<br>Activation or Deactivation<br>Danger-duress |

### Sending chip options and operating method

It is necessary to enable the chips installed in the alarm center to be used. It is also necessary to configure the alarm center to send and receive SMS or only one of the functions, according to its use.

- **Chip 1:** enables the use of the chip allocated in slot/position 1 in the module. If no chip is enabled, the center does not continue the connection to the operator's network.
- **Chip 2:** enables the use of the chip allocated in slot/position 2 in the module. If no chip is enabled, the center does not continue the connection to the operator's network.
- **SMS sending:** enables the sending of SMS messages when the selected events occur.
- **SMS reception:** enables the alarm center to receive SMS messages. For more details, see the *Program SMS* section.

Use the following table to disable/enable the alarm center settings for SMS, as described below:

Enter + 832 + Enter

| | |
|---|---|
| Key 1 | Chip 1 |
| Key 2 | Chip 2 |
| Key 3 | Sending SMS |
| Key 4 | Receiving SMS |

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

### Select *SMS* events

Selects which events will be sent via SMS if the *SMS Sending* function is enabled, with the factory default: *all events are enabled.*

| | |
|---|---|
| Key 1 | SMS at activation |
| Key 2 | SMS at deactivation |
| Key 3 | SMS for trips |
| Key 4 | SMS activation/deactivation by duress password |

Use the table above to disable/enable the alarm center settings for SMS, as described below:

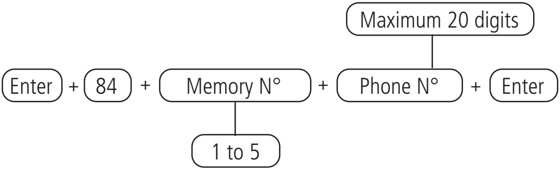
Enter + 833 + Enter

Use the *1*, *2*, *3* and *4* on the keyboard to enable the selection of *SMS*events, so that the corresponding numbers that you wish to have the function active, remain marked on the display and then confirm with the *Enter* key. If you only want to view the setting, press the *Back/Exit* key that no programming will be changed.

### Phone to SMS

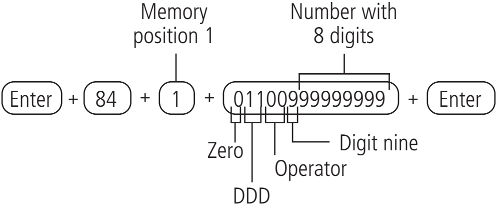
Sets the numbers of the mobile phones that will receive SMS messages from the alarm center if the *SMS sending* function is enabled. The alarm center has 5 (five) memory positions for registering cell phone numbers, and when a new number is programmed in a position already occupied, the previous number occupying this memory is deleted.

To program this function, type:


Maximum 20 digits
Enter
+
84
+
Memory N°
+
Phone N°
+
Enter
1 to 5

***Note:*** enter the number of the phone to be programmed, starting with the DDD, then operator and finally the number always starts with the digit 9 (nine) - if it is cellular - followed by more 8 (eight) numbers.

E.g.:


Memory position 1
Number with 8 digits
Enter
+
84
+
1
+
011009999999999
+
Enter
Zero
DDD
Operator
Digit nine

To edit/view the programmed phones, enter:

Enter + 84 + Memory N° + Enter

1 to 5

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

To delete the programmed phones, enter:

Enter + 84 + Memory N° + Deactive + Enter

1 to 5

### Remote operation by SMS

With the *SMS* function enabled, it is possible to send SMS messages from a mobile phone to the alarm center equipped with the GPRS module, with the chips correctly installed and thus control some functions of the alarm center, as shown in the table below:

| **Function** | **SMS message to be sent** |
|---|---|
| Activates the complete center | !passwordA! |
| Only activate partition 01 | !passwordA01! |
| Only activate partition 02 | !passwordA02! |
| Only activate partition 03 | !passwordA03! |
| Only activate partition 04 | !passwordA04! |
| Only activate partition 05 | !passwordA05! |
| Only activate partition 06 | !passwordA06! |
| Only activate partition 07 | !passwordA07! |
| Only activate partition 08 | !passwordA08! |
| Only activate partition 09 | !passwordA09! |
| Only activate partition 10 | !passwordA10! |
| Only activate partition 11 | !passwordA11! |
| Only activate partition 12 | !passwordA12! |
| Only activate partition 13 | !passwordA13! |
| Only activate partition 14 | !passwordA14! |
| Only activate partition 15 | !passwordA15! |
| Only activate partition 16 | !passwordA16! |

| | |
|---|---|
| Deactivates the complete center | !passwordD! |
| Only deactivate partition 01 | !passwordD01! |
| Only deactivate partition 02 | !passwordD02! |
| Only deactivate partition 03 | !passwordD03! |
| Only deactivate partition 04 | !passwordD04! |
| Only deactivate partition 05 | !passwordD05! |
| Only deactivate partition 06 | !passwordD06! |
| Only deactivate partition 07 | !passwordD07! |
| Only deactivate partition 08 | !passwordD08! |
| Only deactivate partition 09 | !passwordD09! |
| Only deactivate partition 10 | !passwordD10! |
| Only deactivate partition 11 | !passwordD11! |
| Only deactivate partition 12 | !passwordD12! |
| Only deactivate partition 13 | !passwordD13! |
| Only deactivate partition 14 | !passwordD14! |
| Only deactivate partition 15 | !passwordD15! |
| Only deactivate partition 16 | !passwordD16! |
| Request alarm center status | !passwordS! |

To use the table functions, choose the function and send an SMS message with the text of the second column to the chip number installed in the GPRS module of the alarm center, replacing the password with the user password used to activate/deactivate the system. Use 4 or 6 digits password, depending on the alarm center settings.

The status request will send a four-line SMS message in the following format to the programmed phones:

- **Alarm center name:** Display the alarm center's programmed name on the first line.
- **Status:** display of the alarm center Activated or Deactivated on the second line.
- **Siren:** display of the siren On or Off on the third line.
- **Triggers:** if there are triggers, the zone numbers separated by space are displayed, if there are no triggers, nothing is displayed. Example: if there are triggers in zones 1 and 7, display on the fourth line as *01 07.*

### Changing the Display Name of the Alarm Center

Programming to change the display name of the alarm center, being factory default: *AMT 8000.*

To change the name, enter:

Enter + 1 + Active + 00 + Enter

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

## 6.18. Activation/deactivation of Functions

The AMT 8000 alarm center has several functions that can be activated or deactivated according to the needs of each installation. These functions are divided into 6 groups:

- General settings 1
- General settings 2
- Locks
- General settings 3
- Events that generate triggers
- Monitoring

### General settings 1

The parameters configured in this function group are described below:

- **Partitioning:** with this feature, the alarm center can be divided as if it were up to 16 independent systems. For more information, see *Program or partitioning of the central section.*
- **Activation by a key:** If this function is activated, you can activate the system by pressing the Active key for 3 seconds. All partitions will be activated in the case of a partitioned center, if a common keyboard is used, and in the case of a keyboard with permission on a specific partition, only this partition will be activated.

  **Note:** this command does not allow deactivating the alarm center. For more information, see Partição do teclado.
- **Siren beep in the activation/deactivation:** Activates/deactivates the beep emitted by the siren on activation/deactivation of the alarm center. On activation, the siren will emit 1 short beep and on deactivation, the siren will emit 2 short beeps. If a trouble is detected and the *Indication of Troubles by siren* function is enabled, the siren will beep one long time on activation and two long beeps on deactivation.
- **Activation with open zones:** The system can only be activated in the factory setting 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 output timing ends so that a trip does not occur.

- **6-digit password:** increases the number of digits of the password from 4 to 6. Passwords programmed before the function is enabled remain the same and must be entered 00 at the end to complete the 6-digit password before they are changed. While this function is enabled, the system will only accept programming passwords with 6 digits.
- **Remote Control Clears Trigger:** Allows the memorization of the occurred triggers 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 by a key |
| 3 | Siren beep on activation/deactivation |
| 4 | Activation with open areas |
| 5 | Password with 6 digits |
| 6 | N/A |
| 7 | N/A |
| 8 | Remote control clean trigger |

Use the keyboard to set the function status, so that the numbers that you want to have the function active remain checked and the functions that should remain inactive remain unchecked, then confirm with the*Enter*key.

### General settings 2

The parameters configured in this function group are described below:

- **Silent panic by key *0*:** if key *0* is pressed for 3 seconds, the siren will remain off and the *Silent Panic* event 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 *Audible Panic* event will be reported to the monitoring company.
- **Medical Emergency by 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 6 seconds 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 beep intermittently.

- **Maintenance request by key *Enter*:** by enabling this function the user can request equipment maintenance by pressing *Enter* key for 3 seconds, eliminating the need to call the monitoring company/system installer.
- **Indication of troubles by siren:** if the *Indication of troubles by siren in activation/deactivation* and *Beep of siren in activation/deactivation* functions are enabled and if any trouble is detected, a long beep will beep on activation and two long beeps on deactivation.
- **Automatic cancellation by zone opening:** in normal operation, the *Automatic cancellation of zones* function works taking into account the number of siren trips. With this function enabled, cancellation is made by the number of times the zone is opened.

To program this function, type:

Enter + 511 + Enter

| Key | Function |
|---|---|
| 1 | Silent panic by key *0* |
| 2 | Audible panic by key *2* |
| 3 | Medical emergency by key *5* |
| 4 | Fire by key *8* |
| 5 | Maintenance request by key *Enter* |
| 6 | N/A |
| 7 | Indication of troubles by siren |
| 8 | Automatic cancellation by zone opening |

Use the keyboard to set the function status, so that the numbers that you want to have the function active remain checked and the functions that should remain inactive remain unchecked, then confirm with the *Enter* key.

### Locks

The parameters configured in this function group are described below:

- **Reset lock:** With this function active, all forms of reset are locked.
- **Remote control lock:** all remote controls are locked and the system can only be activated/deactivated through 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 event of incorrect password will be sent to the monitoring company. If the function is disabled, the event will be sent, but the keyboard will still work normally.

To program this function, type:

Enter + 512 + Enter

| Key | Function |
|---|---|
| 1 | Reset lock |
| 2 | Remote control lock |
| 3 | Keyboard lock in case of incorrect password |

Use the keyboard to set the function status, so that the numbers that you want to have the function active remain checked and the functions that should remain inactive remain unchecked, then confirm with the*Enter*key.

### General settings 3

The parameters configured in this function group 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 shooting).
- **Telephone line cut:** when activated, the function will check the voltage on the telephone line and, if it is above the limit for 3 consecutive tests, it considers that the line is inoperative. The telephone line cut event is generated and, if programmed, will trigger the siren even if the system is turned off (see the Triggering Issues section).

To program this function, type:

Enter + 513 + Enter

| Key | Function |
|---|---|
| Key 1 | Alarm center Tamper |
| Key 2 | keyboard tamper |
| Key 3 | Phone line cut |

Use the keyboard key 3 to enable the alarm center function, so that the number 3 remains checked to enable and unchecked to disable and then confirm with the *Enter* key. If you only want to view the setting, press the *Back/Exit* key that no programming will be changed.

### Monitoring

The parameters configured in this function group are described below:

- **Call back:** when enabled, the alarm center will answer the call according to the programmed number of rings and when receiving a valid password, will terminate the call and call the phone programmed in memory 03 to start the download/upload.
- **Overlay of answering machine:** this function will prevent the answering machine from answering a download/upload call. When enabled, the center will only answer if two calls occur in a maximum interval of 1 minute. For example, a call is received, and is allowed to ring twice, hangs up and switches on again. If disabled, the alarm center will answer the call after the number of programmed rings.
- **Real-time reporting:** in *Standard* mode, when triggering in a zone occurs, the alarm center will send the triggering event only once to the monitoring company and send the terminated triggering event only when the system is deactivated. If real-time reporting is enabled, the unit will send the trip and stop events whenever the zone is opened or closed while the system is enabled.
- **Periodic Test Only by Phone:** This option will only work with the Regular IP reporting mode. With this option enabled whenever a *Periodic Test* event is generated it will be sent by phone line. The other events will continue to be sent according to the rules of the *Regular IP* mode, i.e., they will only be sent by telephone if there is a failure in the IP communication.
- **Disable beep of output time:** This option will disable the beep that the keyboard emits during the exit (after entering the password).

To program this function, type:

Enter + 514 + Enter

| Key | Function |
|---|---|
| 1 | Call back |
| 2 | Overlay of answering machine |
| 3 | Real-time reporting |
| 4 | N/A |
| 5 | N/A |
| 6 | N/A |
| 7 | Periodic test only by phone |
| 8 | Disable beep of output time |

Use the keyboard to set the function status, so that the numbers that you want to have the function active remain checked and the functions that should remain inactive remain unchecked.

### Troubles that generate triggering

With this function enabled, sirens will be triggered if at least one of the following events is detected: supervision failure, phone line cut, tampering of devices beyond system intrusions. With the function disabled only the corresponding event will be generated, but the siren remains switched off.

- **Supervision failure:** the system has the supervision of communication with all wireless devices to the alarm center, and with the function active, the system will generate the failure if any of the devices lose communication.

  **Note:** the wireless devices of the 8000 line have fixed device supervision time in 35 minutes and cannot be changed this time. During this time, if there is no communication with the alarm center, it will generate the supervision failure if enabled.
- **Phone line cut:** when the phone line disconnection is checked, the alarm center will generate the fault. See the *General settings 3* section to enable the checking of this item (*enabled* factory default ).
- **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 (*disabled*factory default ), even if the system is active, no fault trips will be generated.

To program this function, type:

Enter + 515 + Enter

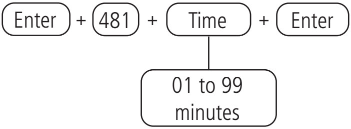
| Key | Function |
|---|---|
| Key 1 | N/A |
| Key 2 | Failure of supervision |
| Key 3 | N/A |
| Key 4 | Phone line cut |
| Key 5 | Tamper of devices |
| Key 6 | Do not generate trips |

Use the keyboard to set the function status, so that the numbers that you want to have the function active remain checked and the functions that should remain inactive remain unchecked, then confirm with the *Enter*key.

## 6.19. Time to send the AC fault

As soon as a mains failure is detected, the alarm center will wait for the programmed time to generate the corresponding event. If during this time the mains is restored, no event will be generated. This time leaves the factory programmed for 1 minute and can be changed to up to 99 minutes.

To program this function, type:



To edit/view the programmed value, type:

Enter + 481 + Enter

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

## 6.20. System Reset

There are two types of reset, one temporary for hardware and the other permanent for software (programming mode). The *Temporary Reset* resets the installer password to *9090* and the master password to *1234* for 1 minute, without deleting any programming done. The *Reset by programming mode* , not only returns the installer and master passwords (see topic *6.8. Passwords*) to the factory default, but also deletes all secondary passwords and all settings made.

If the *Reset Lock* is enabled, it is not possible to perform the *Reset* of system (see *6.18. Activation / deactivation of item functions*).

### Temporary Reset of Master and Installer Passwords

If you have forgotten the master password or the installer password, you will not be able to enter programming mode and gain access to the center's settings/operations. If this occurs, there is a temporary reset for these passwords following the step below:

1. With the alarm center on, press the wireless device registration key for approximately 15 seconds, when the LED flashes again the center will enter the temporary reset mode for 1 minute. During this time the master password will be *1234* and the installer password will be *9090*.

During this time it will be possible to enter programming mode and change the master password and/or the installer password (see topic *6.8. Passwords*). If nothing is done during this period, the passwords will return to the same previously programmed values.

### Reset by programming mode

The *Reset by programming mode*, erases all programming done in your alarm center and cancels the reporting of pending events."

To program this function, type:

Enter + 0000 + Enter

***Note:*** this command does not erase the wireless devices registered in the alarm center or the editable messages.

If you want to perform a single command to erase all the settings of the alarm center, including wireless devices registered and editable messages, type:

Enter + 9999 + Enter

**Attention:** this command will return the alarm center to the factory standard, so even the keyboard used to perform the command will lose its registration, and all programming must be redone.

## 6.21. Quick programming reference

This quick reference considers that the alarm center is in programming mode and assumes the reading of the complete manual and knowledge of the result of each function.

When accessing the programming mode, editing or viewing some programming through 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 or command must be started again.

### Enter programming mode

When you press the *Enter* key on the initial screen, the *Prog. Password* message will be displayed, indicating that the center is waiting for the master password or the installer password to be entered.

*Entering the programming mode with the installer password*

*Enter + Installer Password* (with 4 or 6 digits - factory default being *9090* with 4 digits).

### *Entering the programming mode with the master password*

*Enter + Master Password* (with 4 or 6 digits - factory default with 4 digits).

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

To exit the programming mode, enter the corresponding password without starting with the *Enter* key.

### *Registration by synchronization key*

Press and release the synchronization key of the alarm center and wait for LED *3*, located next to this key to be continuously lit, indicating that the center is ready for the registration of wireless devices. When the registration of all devices is complete, press the synchronization key of the alarm center again and check that LED *3* has left the *Continuous* mode (flashes indicating its normal operation), showing that the center has left the wireless device registration mode.

- » **Wireless keyboards (addresses 01 to 16):** with the function active on the alarm center, press the synchronization key on the keyboard located at the back (remove the bracket for fixing on surfaces) or any other key on the keyboard. The addressing of the keyboard will be according to the sequence performed, respecting the maximum limit of 16 devices of this type. To delete a registered keyboard in the alarm center, keep the synchronization key of the device pressed for 20 seconds, until the *Unregistered keyboard* information is shown on its display.
- » **Remote controls (addresses 00 to 97):** the control register follows the principle similar to keyboards, however any of the control keys performs the register with the alarm center if its function is active. Each registered control will be associated to the user according to the registration sequence. To delete a registered control in the alarm unit, press and hold the keys in positions 2 and 3 (padlock closed and padlock open respectively) of the device for 10 seconds until the LED flashes twice in red.
- » **Wireless sensors (addresses 01 to 64):** follows the same principle as the other devices, however each sensor will be associated to a zone of the alarm center according to the registration sequence, starting with sensor 01 (corresponds to zone 01) up to sensor 64 (corresponds to zone 64). With the function active in the alarm center, press the synchronization key on each sensor that you want to synchronize according to its models. To delete a sensor registered in the alarm center, hold down the synchronization key on the device for 20 seconds until the LED flashes red twice.

- **Wireless sirens (addresses 01 to 16):** follow the same principle as the other devices, with the synchronization function active on the alarm center, press the synchronization key on the back of the siren (remove the base for fixing on surfaces) and check if the LED flashes green, indicating success in the registration, if the LED flashes red then process must be repeated. The addressing of the siren will be according to the sequence performed, respecting the maximum limit of 16 devices of this type. To delete a registered siren at the alarm center, keep the device synchronisation key pressed for 20 seconds until the LED flashes twice in red.

### *Keyboard commands for wireless devices*

- **Keyboard**
  - **Register wireless keyboard**

*Enter + 620 + NT + Enter + Press the keyboard* by pressing the sync key

NT = keyboard number from 01 to 16.

- **Delete wireless keyboards**

*Enter* + 720 + NT + *Enter*

NT = keyboard number from 01 to 16.

- **Wireless Keyboard Partition**

*Enter* + 223 + NT + PP + *Enter*

NT = keyboard address from 01 to 16

PP = partition from 00 to 16 (00 = common keyboard, i.e. the keyboard will be allowed access to all partitions of the alarm center).

- **Change messages**

*Enter + GM + Active + (User, device, partition or zone) + Enter*

GM = message group of 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 |
|---|---|---|
| Name of the alarm center | 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 + Disable + Enter*

  **Note:** Returns all messages from the alarm center to the factory standard.

- ***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.

  - **Delete remote control**

    *Enter + 70 + NU + Enter*

    NU = user number from 00 to 97.

  - **Functions of Remote Control Keys**

    *Enter + 65 + T + NU + FC + Enter*

    T = control key of 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 | Atv/Dtv all partitions |
| 02 | Only activates all partitions |
| 03 | Only deactivates all partitions |
| 04 | Atv/Dtv all partitions in *Partial* mode (stay) |
| 05 | Arm only in*Partial* mode (stay) |
| 06 | Panic with siren |
| 07 | Silent panic |
| 08 | Fire panic |

|  |  |
|---|---|
| 09 | Medical emergency |
| 10 | N/A |
| 11 | Atv/Dtv only Partition 1 |
| 12 | Atv/Dtv only Partition 2 |
| 13 | Atv/Dtv only Partition 3 |
| 14 | Atv/Dtv only Partition 4 |
| 15 | Atv/Dtv only Partition 5 |
| 16 | Atv/Dtv only Partition 6 |
| 17 | Atv/Dtv only Partition 7 |
| 18 | Atv/Dtv only Partition 8 |
| 19 | Atv/Dtv only Partition 9 |
| 20 | Atv/Dtv only Partition 10 |
| 21 | Atv/Dtv only Partition 11 |
| 22 | Atv/Dtv only Partition 12 |
| 23 | Atv/Dtv only Partition 13 |
| 24 | Atv/Dtv only Partition 14 |
| 25 | Atv/Dtv only Partition 15 |
| 26 | Atv/Dtv only Partition 16 |
| 27 | N/A |
| 28 | N/A |
| 29 | N/A |
| 30 | N/A |
| 31 | Atv/Dtv Partial mode (stay) for Partition 1 only |
| 32 | Atv/Dtv Partial mode (stay) for Partition 2 only |
| 33 | Atv/Dtv Partial mode (stay) for Partition 3 only |
| 34 | Atv/Dtv Partial mode (stay) for Partition 4 only |
| 35 | Atv/Dtv Partial mode (stay) for Partition 5 only |
| 36 | Atv/Dtv Partial mode (stay) for Partition 6 only |
| 37 | Atv/Dtv Partial mode (stay) for Partition 7 only |
| 38 | Atv/Dtv Partial mode (stay) for Partition 8 only |
| 39 | Atv/Dtv Partial mode (stay) for Partition 9 only |
| 40 | Atv/Dtv Partial mode (stay) for Partition 10 only |
| 41 | Atv/Dtv Partial mode (stay) for Partition 11 only |
| 42 | Atv/Dtv Partial mode (stay) for Partition 12 only |
| 43 | Atv/Dtv Partial mode (stay) for Partition 13 only |
| 44 | Atv/Dtv Partial mode (stay) for Partition 14 only |
| 45 | Atv/Dtv Partial mode (stay) for Partition 15 only |
| 46 | Atv/Dtv Partial mode (stay) for 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 synchronisation key

ZZ = zone that the sensor will be linked from 01 to 64.

- **Delete wireless sensors**

*Enter + 71 + ZZ + Enter*

ZZ = zone that will be unlinked the sensor from 01 to 64.

- **Adjusting 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 = Sens. Minimum / 1 = Sens. Normal / 2 = Sens. Intermediate / 3 = Sens. Maximum

L = Sensor LED, where 0 = Off / 1 = On

M = Sensor operating mode, where 0 = Economic / 1 = Continuous

***Note:*** for XAS 8000 and TX 8000 the Sensitivity, Sensor LED andOperation Mode settings are allowed by the unit, but only the LED configuration is accepted by XAS 8000 and TX 8000.

- **Wireless sensor testing**

  *Enter + 52 + Enter + Activate sensor*

- **Disable sensor tamper**

  *Enter + 78 + X + Enter*

  X = Group of zones 0 to 6

- **Disable digital tamper of the IVP 8000 EX sensor**

  *Enter + 79 + X + Enter*

  X = Group of zones 0 to 6

- **IVP 8000 EX sensor digital tamper reset**

  *Enter + 543 + ZZ+ Enter*

  ZZ= 2-digit zone number.

- **Viewing the firmware of the sensors**

  *Enter + 641 + ZZ + Enter*

  ZZ = 2-digit zone number

- **Wireless siren**

  - **Register wireless sirens**

    *Enter + 621 + NS + Enter + Activate the siren* by pressing the synchronisation key

    NS = siren number from 01 to 16.

  - **Delete wireless sirens**

    *Enter + 721 + NS + Enter*

    NS = siren number from 01 to 16.

  - **Wireless siren partition**

    *Enter + 222 + NS + PP + Enter*

    NS = siren number from 01 to 16.

    PP = partition from 00 to 16 (00 = common address for all zones and 01 to 16 the individual center partitions).

  - **Enable/disable the siren beep on system activation/deactivation**

    *Enter + 510 + Enter + Key 3 + Enter*

  - **Enable/disable the siren beep per partition**

    *Enter + 224 + GP + Enter*

GP = group of partitions, with partitions 01 to 10 in group 0 and partitions 11 to 16 in group 1.

- » **Changing the siren time**

*Enter + 41 + TS + Enter*

TS = siren time from 01 to 99.

**Note:** factory default 5 minutes, and if placed 00 on the command will be beeped error.

- » **Register range RF amplifier (REP 8000 repeater)**

*Enter + 622 + NA + Enter + Activate the amplifier* by pressing the synchronisation key

NA = amplifier number from 01 to 04.

- » **Delete Range RF Amplifier (REP 8000 Repeater)**

*Enter + 722 + NA + Enter*

NA = number of amplifier from 01 to 04.

- » **Reset wireless devices**
  - » **Delete all registered wireless devices**

*Enter + 7 + Disable + Enter*

**Note:** all wireless devices in the alarm center, including the keyboard itself, will be unregistered.

**Changing RF Channel**

*Enter + 630 + RF + Enter*

RF = channels from 08 to 11

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

**Remote update**

- » **To download/checking a new version**

*Enter + 9922 + Enter*

If there is a version to download, the *Download Wait* information will be displayed and it will start, which will take about 3 to 5 minutes (variable according to the connection used). If the alarm center does not have a version for download will be shown *Alarm center is already updated. If you have any problems on the network or Internet where the alarm center is connected, the* *message will be displayed: Download failure.*

- **Install download version**

  *Enter + 9933 + Enter*

  The new version that was downloaded will be installed and will not be lost records and programming of the alarm center. To check the firmware version of the alarm center, access *Menu* and with the arrow keys click on *Version of the alarm center* to be displayed.

**Attention:** to download the firmware, the control panel must be connected to the Cloud via an Ethernet or Wi-Fi connection. Downloading/updating via a GPRS connection is not possible due to the connection's download rate and excessive consumption of the package used.

### Passwords

- **Password programming 1 (exclusive programming of programmer user)**
  - **Change passwords for users of positions 98 and 99**

    *Enter + 20 + NU + PASSWORD + Enter*

    NU = user number 98 or 99.

    PASSWORD = password to be programmed containing 4 or 6 digits.
  - **Delete user password from position 98**

    *Enter + 20 + 98 + Enter*

    **Note:** the password of position 99 cannot be deleted.
- **Password programming 2 (exclusive programming of the Master user)**
  - **Change/create passwords for users of positions 00 to 97**

    *Enter + 20 + NU + PASSWORD + Enter*

    NU = user number from 00 to 97.

    PASSWORD = password to be programmed containing 4 or 6 digits.
  - **Delete password of users from positions 01 to 97**

    *Enter + 20 + NU + Enter*

    NU = user number from 01 to 97.

    ***Note:*** *the password of position 00 cannot be deleted.*

» **Permission of passwords**

» **Set password partition permission**

*Enter + 21 + NU + GP + Enter*

NU = user number from 01 to 96.

GP = group of partitions, with partitions 01 to 10 in group 0 and partitions 11 to 16 in group 1.

» **Set permission to only Enable or Bypass permission**

*Enter + 2 + P + GS + Enter + Select password + Enter*

P = permission setting, 5 active only and 6 bypass permission.

GS = group of passwords from 0 to 9, with group 0 going from 01 to 10, group 1 from 11 to 20 and so on, closing with group 9 from 91 to 97.

» **Setting permission for *Partial* mode (stay)**

*Enter + 221 + GS + Enter + Select password + Enter*

GS = group of passwords from 0 to 9, with group 0 going 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 + G + Enter*

G = Zones group from 0 to 6.

After inserting the command, use the keyboard to enable/disable the corresponding zones for the group and press the*Enter* key to confirm.

» **Enable *Partial* mode (stay)**

*Enter + 02 + G + Enter*

G = Zones group from 0 to 6.

After inserting the command, use the keyboard , to enable/disable the corresponding zones for the group and press the*Enter* key to confirm. Passwords must also have permission for *Partial* mode (stay).

» **Zone Functions**

*Enter + 3 + F + G + Enter*

F= functions of zones from 1 to 6.

G = Zones group from 0 to 6.

After inserting the command, use the keyboard , to enable/disable the corresponding zones for the group and press the*Enter* key to confirm.

| Zone Functions | |
|---|---|
| 1 | Timed |
| 2 | Follower |
| 3 | 24 Hour |
| 4 | Panic |
| 5 | Medical emergency |
| 6 | Fire |

» **Zone operation mode**

*Enter + 0 + MP + G + Enter*

MP= mode of zones from 7 or 8.

G = Zones group from 0 to 6.

After inserting the command, use the keyboard , to enable/disable the corresponding zones for 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 trips from 0 to 9.

» **Alloy input (from version 1.9.2)**

*Enter + 09 + ZZ + Enter*

ZZ = zones 01 to 64

» **Alloy input partition**

*Enter + 516 + GP + Enter*

GP = group of partitions, with partitions from 01 to 10 in group 0 and partitions from 11 to 16 in group 1.

» **Permission to activate and / or deactivate the alloy input**

*Enter + 518 + Enter*

Key 2 - Activation permission

Key 3 - Disable permission

### Partitioning

- **Enable partitioning**

*Enter + 510 + Enter + Select option 1 + Enter*

- **Partitioning the zone**

*Enter + 01 + ZZ + PP + Enter*

ZZ = zone from 01 to 64.

PP = partition from 01 to 16.

- **Set password partition permission**

*Enter + 21 + NU + GP + Enter*

NU = user number from 01 to 96

GP = group of partitions, with partitions 01 to 10 in group 0 and partitions 11 to 16 in group 1.

**Attention:** besides the above mentioned programming points, user passwords must be created/defined (topic *Passwords*) the registering of wireless controls for access (topic *Remote control*) and the partitioning of keyboards (topic *Keyboard*) and sirens (topic *Wireless siren*).

### Timings

- **Input Timing**

*Enter + 42 + PP + TTS + Enter*

PP = partition from 01 to 16 (non-partitioned alarm center, use PP = 01).

TTS = time from 000 to 255 seconds.

- **Output Timing**

*Enter + 44 + PP + TTS + Enter*

PP = partition from 01 to 16 (non-partitioned alarm center, use PP = 01).

TTS = time from 000 to 255 seconds.

- **Disable Beep Out**

*Enter + 514 + Enter + Key 8 + Enter*

### Alarm Center Time Settings

- **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.

AA = year from 00 to 99.

» **Weekday adjustment**

*Enter* + 402 + D + *Enter*

D = weekday from 1 to 7 (1 = Sunday, 2 = Monday, 3 = Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday).

» **Time interval for date and time synchronization**

*Enter* + 403 + HHH + *Enter*

HHH = interval between synchronizations from 000 to 255 hours.

### 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 test by time**

*Enter + 470 + Disable + Enter*

» **Periodic test by time interval**

*Enter + 471 + HHH + Enter*

HHH = hours from 000 to 255.

### Autoactivation/autodeactivation and Autoactivation/autodeactivation per partition

» **Enable autoactivation per inactivity**

*Enter + 460 + TM + Enter*

TTS = time from 00 to 99 minutes.

» **Selecting Autoactivation and Autodeactivation by Partitions**

*Enter + 464 + GP + Enter*

GP = Partition group 0 or 1 (0 = Partition group 01 to 10 and 1 = Partition group 11 to 16).

- **Define holidays**

  *Enter + 404 + PP + F (0 a 9) +DD + MM + Enter*

  PP = partition (non-partitioned alarm center, use PP = 01)

  F = holiday memory number from 0 to 9.

  DD = day of the month that will be a holiday from 01 to 31.

  MM = holiday month from 01 to 12.

- **Weekday for autoactivation**

  *Enter + 838 + PP + Enter*

  PP = partition from 01 to 16 (non-partitioned alarm center, use PP = 01).

  After the command, using the keyboard, 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.

- **Autoactivation Time**

  *Enter + 462 + PP + D + HH + MM + Enter*

  PP = partition from 01 to (non-partitioned alarm center, use PP = 01).

  D = weekday 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.

- **Weekdays for Autodeactivation**

  *Enter + 839 + PP + Enter*

  PP = partition from 01 to 16 (non-partitioned alarm center, use PP = 01).

  After the command, using the keyboard, 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.

- **Autodeactivation Time**

  *Enter + 463 + PP + D + HH + MM + Enter*

  PP = partition from 01 to 16 (non-partitioned alarm center, use PP = 01).

  D = weekday 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.

- **Set holidays for Autodeactivation/Autodeactivation.**

  *Enter + 404 + PP + F + DD + MM + Enter*

  PP = partition from 01 to 16 (non-partitioned alarm center, use PP = 01).

  F = holiday memory number from 0 to 9.

  DD = day from 01 to 31.

  MM = month from 01 to 12.

### Wi-Fi Connection

- **Insert name of the network to be connected**

*Enter + 850 + Enter + Insert network name + Enter*

- **Insert password of the network to be connected**

*Enter + 851 + Enter + Insert network password + Enter*

- **Enable/disable Wi-Fi**

***Note:*** the alarm center connects only with 2.4GHz 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 |

### Settings for monitoring and SMS

- **Schedule monitoring account**

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

After the command, enter the 4-digit monitoring account number and press the *Enter* key to confirm.

- **Program phone number for monitoring company**

*Enter + 10 + M + phone number of monitoring company + Enter*, where M = memory for phone from 1 to 8

- **Delete Phone**

*Enter + 10 + M + Disable + Enter*

M = memory for phone from 1 to 8

- **Phone Test**

*Enter + 11 + M + Enter*

M = memory for phone from 1 to 8

- **End Phone Test**

*Enter + 11 + Enter*

- **Event reporting mode**

*Enter + 17 + A + B + C + Enter*

A = indicates in which mode the alarm center will operate from 0 to 7, where 0: disabled, 1: regular phone, 2: not applicable, 3: dual phone, 4: regular IP, 5: not applicable, 6: dual IP, 7: dual Mix.

B = indicates the protocol that will be used when phone 01 is dialed, being 0 = Contact-ID and 1 = Programmable Contact-ID.

C = indicates the protocol that will be used when phone 01 is dialed, being 0 = Contact-ID and 1 = Programmable Contact-ID.

**Note**: the programmable Contact-ID protocol can only be edited by the download/upload software (*AMT 8000 programmer*).

- **Blocking the sending of 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.

- **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 default DTMF level stored in the alarm center memory does not work, type the following command and test all the options from 0 to 6 to see which one gives the best result.

*Enter + 18 + N + Enter*

N = number of attempts from 0 to 6.

- **Pending Event Reset**

*Enter + 16 + Enter*

- **Program communication priority**

*Enter + 19 + P + Enter*

P = communication priority from 0 to 3, where 0 = Ethernet, 1 = 2G/3G/4G, 2 = Ethernet/2G/3G/4G, 3 = 2G/3G/4G/Ethernet.

- **Program target IP**

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

After the command, enter 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, being 1 = port 1 and 2 = port 2.

After the command insert the port number with 4 digits.

**Note:** This field defines the port to which the center will connect, factory default : 9009. Intelbras IP Receiver software must be configured for the same port.

**Important:** you must not use the same port from another manufacturer for this communication, because there is the possibility of conflict.

- **Program target domain name (DNS)**

If you don't want to use DNS, go to the next command, otherwise, type:

*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 keys on the keyboard, 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 the 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, perform the next step, otherwise, type the following command and also the next ones.

*Enter + 831 + Enter*

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

- **Switch IP address (cable connection)**

*Enter + 8120 + Enter*

After the command, enter the IP address for the alarm center.

**Note:** You can only edit/enter the address manually if the DHCP function is disabled, otherwise only the IP address of the alarm center will be displayed.

» **Programming the network mask**

*Enter + 8130 + Enter*

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

» **Programming the gateway**

*Enter + 8140 + Enter*

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

» **Programming DNS Servers for Ethernet**

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

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

» **IP address of the exchange (WI-FI connection)**

*Enter + 8620 + Enter*

After the command, enter the IP address for the panel.

***Note:** it will only be possible to edit / enter the address manually if the DHCP function is disabled, otherwise only the IP address of the control panel will be displayed.*

» **Program the netmask (WI-FI connection)**

*Enter + 8630 + Enter*

After the command, enter the Netmask number and press the Enter key to confirm.

» **Program the gateway (WI-FI connection)**

*Enter + 8640 + Enter*

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

» **Program DNS servers for Ethernet**

*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 ranging from 000 to 255 minutes (factory minutes*5 minutes*)

» **Program login**

*Enter + 822 + O + Enter*, where O = 1 or 2 (Operator 1 ou Operator 2)

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

» **Enable chips**

*Enter + 832 + Enter*

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

» **Program password**

*Enter + 823 + O + Enter*, where O = 1 or 2 (Operator 1 ou Operator 2)

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

» **Program APN**

*Enter + 824 + O + Enter*, where O = 1 or 2 (Operator 1 ou Operator 2)

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

» **Programming the PIN (Personal Identification Number)**

If you want to use the PIN, make the command in sequence, otherwise go to the next command.

If the PIN is incorrect the chip will be locked.

*Enter + 825 + O + PIN number with 4 digits + Enter*, where O = 1 or 2 (Operator 1 or Operator 2)

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

*Enter + 827 + TTM + Enter*, onde TTM = Heartbeat interval time 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 entering the command, enter the DNS server code (according to the server used) and then press the*Enter* key to confirm.

» **Interval between GPRS connections attempts**

*Enter + 829 + TG + Enter*, where TG = interval time of reconnection attempts from 00 to 20 (standard *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 SMS*

**Attention:** as of version 1.7.9, all functions related to SMS (sending and receiving) for the AMT 8000 central were removed.

- **Program GPRS channel options to enable chips and SMS sending/receiving**

*Enter + 832 + Enter*

After the command, use the keys on the keyboard to enable *1 (chip 1), 2 (chip 2), 3 (send SMS), 4 (receive SMS)* options and press the *Enter* key to confirm.

- **Select *SMS* events**

*Enter + 833 + Enter*

After the command, use the keys on the keyboard to enable *1, 2, 3, 4* options and press the *Enter* key to confirm.

- **Program phone to SMS**

*Enter + 84 + M + Phone number with up to 20 digits + Enter*, where M = memory number ranging from 1 to 5

The phone number must be a maximum of 20 digits and in format: *0 + operator code + area code + phone number starting with the digit 9.*

- **Change display name of alarm center**

*Enter + 1 + Active + 00 + Enter*

After the command, use the keyboard to change the name of the alarm center to be displayed in the SMS message.

### *Contact-ID Codes*

For the following commands that configure the Contact-ID code, the communication protocol must be set to Programmable Contact-ID (see *Event Reporting Mode*), otherwise events will be sent with the standard Contact-ID.

- **Set up Contact-ID code for zone opening type events**

*Enter* + 901 + ZZ + *Enter*

ZZ = zone from 01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm. Factory default *130.*

» **Set Contact-ID code for zone restore type events**

*Enter + 911 + ZZ + Enter*

ZZ = zone from 01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm. Factory default *130.*

» **Set up Contact-ID code for tamper-open type events**

*Enter + 902 + ZZ + Enter*

ZZ = zone from 01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm. Factory default *145* for expansion devices and *383* for sensors.

» **Setup Contact-ID code for tamper-restore type events**

*Enter + 912 + ZZ + Enter*

ZZ = zone from 01 to 64

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm. Factory default *145* for expansion devices and *383* for sensors.

» **Setup Contact-ID Code for User Deactivation Events**

*Enter + 903 + NU + Enter*

NU = user number from 01 to 97

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm. Factory default *401*.

» **Setup Contact-ID code for user activation events**

*Enter + 913 + NU + Enter*

NU = user number from 01 to 97

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm. Factory default *401.*

» **Setup Contact-ID code for opening type system events**

*Enter + 904 + II + Enter*

II = System event index from 00 to 26

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm.

» **Setup Contact-ID code for system events of restore type, enter:**

*Enter + 914 + II + Enter*

II = System event index from 00 to 26

After entering the command, enter the event value in hexadecimal format from 000 to FFF (accepts numbers from 0 to 9 and the letters B, C, D, E and F) and press the*Enter* key to confirm.

**Use to configure the Contact-ID code of the restore and open type system**

| Index | Internal event | Standard code |
|---|---|---|
| 00 | Low Battery of Wireless Device/Restoration Device Battery | 384 |
| 01 | N/A | 344 |
| 02 | Failure of supervision/Restoration supervision | 147 |
| 03 | Zone Bypass/Restoration Zone Bypass | 570 |
| 05 | AC mains failure/AC mains restoration | 301 |
| 06 | Low System Battery/Restore System Battery | 302 |
| 07 | Absent Battery/Restoration Battery | 311 |
| 08 | Phone line Cut/Restore Phone line | 351 |
| 09 | Remote Activation/Deactivation | 407 |
| 10 | Automatic Activation/Deactivation | 403 |
| 11 | Activation by a key | 408 |
| 12 | Activation and deactivation under duress | 121 |
| 13 | System Reset | 305 |
| 14 | Programming change | 306 |
| 15 | Failure to communicate event | 354 |
| 16 | Incorrect password | 461 |
| 17 | Remote access | 410 |
| 18 | Manual testing | 601 |
| 19 | Periodic Test | 602 |
| 20 | Event Buffer Reset | 621 |
| 21 | Restart date and time | 625 |
| 22 | Tamper of expansion devices | 145 |
| 23 | Tamper sensors | 383 |
| 24 | Maintenance request | 616 |
| 25 | AC wireless device failure | 342 |
| 26 | PGM activation | 422 |

### » Setup Event Code *Push*

*Enter + 92 + EV + Enter + Select event + Enter*

EV = group of events from 0 to 3, group 0 being from 01 to 10 and so on, until group 3 being from 31 to 35.

| Event Group (EV) | Event | Key | Standard Value |
|---|---|---|---|
| 0 | ARME_DESARME_USUARIO, | Key 1 | Enabled |
| | N/A, | Key 2 | Enabled |
| | DISPARO_ZONA, | Key 3 | Enabled |
| | DISPARO_24H, | Key 4 | Enabled |
| | DISPARO_SILENCIOSO, | Key 5 | Enabled |
| | DISPARO_EMERGENCIA_MEDICA, | Key 6 | Enabled |
| | DISPARO_INCENDIO, | Key 7 | Enabled |
| | DISPARO_PANICO_AUDIVEL, | Key 8 | Enabled |
| | DISPARO_PANICO_SILENCIOSO, | Key 9 | Enabled |
| | TAMPER_SENSOR, | Key 10 | Enabled |
| 1 | BATERIA_BAIXA_SENSOR, | Key 1 | Enabled |
| | N/A, | Key 2 | Enabled |
| | FALHA_SUPERVISAO_RF, | Key 3 | Enabled |
| | BYPASS_ZONA, | Key 4 | Enabled |
| | BYPASS_AUTOMATICO, | Key 5 | Enabled |
| | FALHA_REDE_ELETRICA, | Key 6 | Enabled |
| | BATERIA_PRINCIPAL_BAIXA, | Key 7 | Enabled |
| | BATERIA_PRINCIPAL_AUSENTE, | Key 8 | Enabled |
| | FALHA_LINHA_TELEFONICA, | Key 9 | Enabled |
| | ARME_DESARME_REMOTO, | Key 10 | Enabled |
| 2 | AUTO_ARME_DESARME, | Key 1 | Enabled |
| | ARME_RAPIDO, | Key 2 | Enabled |
| | ARME_DESARME_SOB_COACAO, | Key 3 | Enabled |
| | RESET_SISTEMA, | Key 4 | Enabled |
| | PROGRAMACAO_ALTERADA, | Key 5 | Enabled |
| | FALHA_AO_COMUNICAR_EVENTO, | Key 6 | Enabled |
| | SENHA_INCORRETA, | Key 7 | Enabled |
| | ACESSO_DOWNLOAD, | Key 8 | Enabled |
| | TESTE_MANUAL, | Key 9 | Enabled |
| | TESTE_PERIODICO, | Key 10 | Enabled |

| | | | |
|---|---|---|---|
| 3 | RESET_BUFFER_EVENTOS | Key 1 | Enabled |
| | RESET_DATA_HORA | Key 2 | Enabled |
| | N/A | Key 3 | Enabled |
| | N/A | Key 4 | Enabled |
| | SOLICITACAO_MANUTENCAO | Key 5 | Enabled |
| | FALHA_REDE_ELETRICA_MOD_EXPANSOR | Key 6 | Enabled |
| | ACTIVATION/DEACTIVATION_PGM | Key 7 | Enabled |

## » Activation/deactivation of Functions

*Enter + 51 + GF + Enter + FUNCTION + Enter*

GF = function group from 0 to 5.

FUNCTION = key corresponding to the function.

| Key | Function group 0 | Function group 1 | Function group 2 | Function group 3 | Function group 4 | Function group 5 |
|---|---|---|---|---|---|---|
| 1 | Partitioning | Silent panic by key *0* | Locks of reset | Alarm control panel tamper | - | - |
| 2 | Activation by a key | Audible panic by key *2* | Remote control lock | - | - | Failure of supervision |
| 3 | Siren beep on activation/ deactivation | Medical emergency by key *5* | Keyboard lock in case of incorrect password | Phone line cut | Real-time reporting | Phone line cut |
| 4 | Activation with open areas | Fire by key *8* | - | - | - | - |
| 5 | Password with 6 digits | Maintenance request by *Enter* key | - | - | - | Tamper of devices |
| 6 | Remote control clean trigger | - | - | - | - | Do not generate trips |
| 7 | - | Indication of troubles by siren | - | - | Periodic Test only by phone | - |
| 8 | - | Automatic cancellation by opening of zone | - | - | Disable Beep Out | - |

**Fault sending time**

- **AC mains failure**

*Enter + 481 + TM + Enter*

TM = 01 to 99 minutes failure send time.

**System Reset of the entire system except wireless device registration**

*Enter + 0000 + Enter*

- **Reset of the entire system (Programming, Messaging and Wireless Devices)**

*Enter + 9999 + Enter*

## 6.22. Approval

ANATEL 05326-18-00160

This equipment has no right to be protected against harmful interference and may not cause interference to duly authorized systems. This is a product approved by Anatel, the approval number can be found on the product label, for queries use the link *https://www.gov.br/anatel/pt-br.*

# Warranty Term

It is expressly stated that this contractual warranty is given subject to the following conditions:

---

Name of customer:
Signature of the customer:
No. of the invoice:
Date of purchase:
Model: Serial No:
Reseller:

---

1. All parts, pieces and components of the product are warranted against any manufacturing defects, which may present, for a period of 1 (one) year - this being 90 (ninety) days of legal warranty and 9 (nine) months of contractual warranty - as from the date of purchase of the product by the Consumer, as stated in the invoice of product purchase, which is part of this Term throughout the national territory. This contractual warranty includes the free exchange of parts, pieces and components that have a manufacturing defect, including the expenses with the labor used in this repair. In case no manufacturing defect is found, but defect from inappropriate 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 to be installed and configured by a qualified technician, look for a suitable and specialized professional, and the costs of these services are not included in the value of the product.
3. If you notice a defect, you should immediately contact the nearest Authorized Service listed by the manufacturer - only they are authorized to examine and remedy the defect during the warranty period provided herein. If this is not adhered to, this warranty will lose its validity, as it will be characterized by the violation of the product.
4. In the event that the Consumer request home care, it should refer to the nearest Authorized Service for the technical visit fee. If the need for withdrawal of the product is found, the expenses arising, such as transportation and safety to and from the product, are under the responsibility of the Consumer.
5. The warranty will totally lose its validity in the event of any of the following: a) if the defect is not of manufacture, but caused by the Consumer or by third parties alien to the manufacturer; b) if the damage to the product comes from accidents,

casualties, agents of nature (lightning, floods, landslides, etc.. ), humidity, mains voltage (overvoltage caused by accidents or excessive mains fluctuations), installation/use in disagreement with the user manual or due to natural wear of parts, pieces and components; c) if the product has been influenced by chemical, electromagnetic, electrical or animal (insects, etc.); d) if the product's serial number has been disfigured or erased; e) if the device has been tampered.

6. This warranty does not cover loss of data, so it is recommended that the Consumer make a regular backup of the data on the product.
7. Intelbras is not responsible for the installation of this product and also for any attempts of fraud and/or sabotage on its products. Keep software and application updates, if any, up to date, as well as network protections necessary to protect against hackers. The equipment is guaranteed against defects within its normal conditions of use, and it is important to be aware that, since it is an electronic equipment, it is not free from frauds and scams that may interfere with its correct functioning.
8. Battery-powered product. Dispose of at authorized Intelbras sites or at collection points specifically designed for this purpose. It can cause risk to human health and the environment. Questions: www.intelbras.com.br, suporte@intelbras.com.br or (48) 2106-0006 or 0800 7042767.
9. 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 suporte@intelbras.com.br or (48) 2106-0006 or 0800 7042767 for more information.

As these are the conditions of this additional Warranty Term, 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.

Dispose of batteries in appropriate places and do not dispose of electronic materials in common waste.

This product is covered by the Informatics Legislation.

*US Robotics is a registered trademark of USRobotics. Motorola is a registered trademark of Motorola, Inc. Lucent is a registered trademark of Alcatel-Lucent. Agere is a registered trademark of LSI Corporation. Android is a registered trademark of Google, Inc. Windows, Windows XP, Windows Vista, Windows 7, MSN, NetMeeting, Windows, DirectX, Direct Sound 3D and Media Player are registered trademarks or trademarks of Microsoft Corporation in the United States or other countries or regions. DynDNS is a registered trademark of Dynamic Network Services Inc.*

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

01.26
Made in Brazil