Translated from Spanish to English - www.onlinedoctranslator.com

INTERCOM MANUAL

PANPHONE IP CSIP V6

Installation, configuration and start-up manual for the PANPHONE CSIP V6 with firmware 6.0.

Document details

EQUIPMENT	**PANPHONE IP CSIP V6**
ID SHOWN BY THE EQUIPMENT	**CSIP H6 - V 6.0**
FIRMWARE DOCUMENTED	**6.0**
MANUAL	**CSIP V6 - 6.0 - ES**
GUY	**Technical installation and configuration manual**

DOCUMENT

Warning and declaration of conformity

This document refers to the device**PANPHONE IP CSIP V6**.

For questions about installation, configuration or operation, please see the Contact and Support section.

> **Use of the document.**Total or partial reproduction of this manual without authorization is prohibited.

The manufacturer reserves the right to make hardware or software modifications to the device described in this document. Available features may vary depending on the firmware version, activated licenses, installed modules, and device configuration.

Statement.

The manufacturer declares that PANPHONE IP products comply with the essential requirements applicable to radio equipment and telecommunications equipment, in accordance with the relevant regulations.

Documentary support.

For copies, document updates, or specific regulatory information, please consult the official channels of the supplier or the person responsible for the installation.

CONTENT

General index

01 1. Introduction	02 2. Installation, assembly and connection	03 3. Programming and first access	04 4. SIP Accounts
05 5. Connectivity	06 6. Multimedia	07 7. Relays and access	08 8. Keyboard / Pushbutton
09 9. Modules and licenses	10 10. Tools	11 11. Users	12 12. OPTO Board
13 13. Accessories of mounting	14 14. Technical data	15	16

1. Introduction

Welcome to the PANPHONE IP CSIP V6 manual. This device is part of a line of communication and access control systems designed for industrial environments, offices, multi-family buildings, and facilities where secure call and access management is required.

1.1 General description

The PANPHONE CSIP V6 is a smart, hands-free IP intercom that can connect as a SIP extension to an IP PBX, a SIP trunk, or another terminal via direct IP call. It can operate on a local network or in remote environments, depending on the network and communications configuration available at the installation.

The device features relays with voltage-free contacts to operate doors, barriers, or other external devices such as lights, sirens, or auxiliary systems. Activation can be performed during communication, using DTMF codes from an authorized telephone, or via access control systems configured on the board.

Programming is done through an internal web page on the device itself. It can be accessed using a compatible browser from a computer connected to the same Ethernet network or via the path established by the installer.

The web interface organizes the configuration into the sections Home, SIP Accounts, Connectivity, Multimedia, Relays, Keypad/Pushbutton, Modules and Licenses, Tools and Users.

1.2 Main features

SIP Communication

Up to five independent SIP accounts with major audio codecs, communication via IP PBX, SIP trunk or direct point-to-point IP calling.

Audio and call

Full-duplex audio, auto-answer for incoming calls, signaling tones, pre-recorded audio, echo cancellation and noise reduction.

Sound settings

Independent control of speaker volume and microphone sensitivity, with remote audio testing from the web interface.

Video and multimedia

Possibility of video calls with optional camera, image adjustments, recordings, RTSP streaming, LCD screen and selection of voice language.

Connectivity

Ethernet connection and wireless communication via WiFi or optional 4G/LTE, plus network utilities such as Ping, SMTP, SNMP and VPN.

Relay activation

Activation of relays from extensions or telephones that support DTMF, with voltage-free contacts for doors or other external devices.

Access control

Access system using PIN key, RFID cards, QR codes, schedules and assignment of access to specific relays.

Histories and logs

History of actions or events, access control history and VoIP traffic log for review and technical diagnosis.

Web interface

Complete device configuration via internal web server, with separate menus for network, SIP, multimedia, access, tools and users.

Calls from the web

Making test calls to an extension or IP address directly from the configuration interface.

Keyboard and push button

Configurable keys, dialing modes, manual dialing length, access key length, and status LED settings.

Modules and integrations

Compatibility with RS485, API, Modbus, SNMP, OPTO board, third relay, WiFi, 4G/LTE, video, RFID and QR depending on installed hardware, license and configuration.

1.3 Technical characteristics

- Supported audio codecs: G.711 (u-Law, a-Law), G.722, G.726, G.729, GSM and OPUS. VoIP
- protocols: SIP-RTP in accordance with RFC 3261.
- DTMF Detection: RFC 2833.
- Power supply: 12 Vdc +/- 15%, 2 A, recommended power supply depending on installation, or PoE 802.3af.
- Two independent 2 A / 24 Vdc relays with voltage-free contacts; optional third relay via add-on board. Operating
- temperature: -10 to +55 °C. Storage temperature: -10 to +55 °C.
- RFID reader Mifare 13.56 MHz on devices with a built-in reader.
- QR code reader via camera on compatible devices.
- Integrated video in devices with cameras, with video, recording and streaming functions depending on configuration.

1.4 Data required before configuring

Before starting the configuration, the installer must have the network data, authorized access credentials, SIP information, and relay connection diagram. Technical parameters should not be modified without knowing their effect on the installation.

Required information	What is it used for?
IP address or method of accessing the equipment	It allows you to access the web panel to perform the configuration.
Username and password authorized	They allow access to the web interface. They must be kept safe and changed if they are initial credentials.
SIP Data	Extension, user, password, server, port, transport, and registration type so that the card can call or register on the PBX.
Network data	DHCP or static IP, subnet mask, gateway, DNS and VLAN if applicable.
Relays and access points	Identification of each door, barrier, lock or automation connected to each relay.
Installed modules and licenses	Camera, RFID, QR, RS485, OPTO, WiFi, 4G/LTE, SNMP, API or other modules available depending on the equipment supplied.

> **Important.**Access credentials to the equipment must be kept safe by authorized personnel. They must not be included in public documentation or shared with unauthorized users.

1.5 CSBOX Formats

The device is also available in a CSBOX format (plastic or metal enclosure) for installations that do not require the standard front panel. The enclosure dimensions are 125 x 93 x 52 (or 42) mm.



Plastic or Metal CSBOX (125 x 93 x 52 or 42 mm).

Model	Description
CSBOX-P-IP	Full Duplex IP-SIP Enhanced Audio Intercom PCB Card with Gray Plastic Housing. Speaker output power up to 1W.(*)
CSBOX-P-IP-10W	Full Duplex IP-SIP Enhanced Audio Intercom PCB Card with Gray Plastic Housing. 10W Amplifier. Speaker output power up to 10W.(*)
CSBOX-P-IP-OPTO	Full Duplex IP-SIP Enhanced Audio Intercom PCB Card with Gray Plastic Housing + OPTO Card. Speaker output power up to 1W.(*)
CSBOX-P-IP-10W-OPTO	Full Duplex IP-SIP Enhanced Audio Intercom PCB Card with Gray Plastic Enclosure + OPTO Card. 10W Amplifier. Speaker output power up to 10W.(*)
CSBOX-P-IP-10W-BM	IP-SIP Intercom PCB Board with Enhanced Full Duplex Audio, Gray Plastic Housing, and Magnetic Loop. 10W Amplifier. Speaker output power up to 10W. (*)

CSBOX-P-IP-10W-OPTO-4G	IP-SIP Intercom PCB Board with Enhanced Full Duplex Audio and Gray Plastic Housing + Extra 4G Module. 10W Amplifier. Speaker output power up to 10W. (*)
CSBOX-P-IP-10W-CAM	IP-SIP Intercom PCB Board with Enhanced Full Duplex Audio, Gray Plastic Enclosure, and USB Camera. 10W Amplifier. Speaker output power up to 10W. (*)
CSBOX-M-IP	Full Duplex IP-SIP Enhanced Audio Intercom PCB Card with Aluminum Metal Housing. Speaker output power up to 1W.(*)
CSBOX-M-IP-10W	Full Duplex IP-SIP Enhanced Audio Intercom PCB Card with Aluminum Metal Housing. 10W Amplifier. Speaker output power up to 10W.(*)

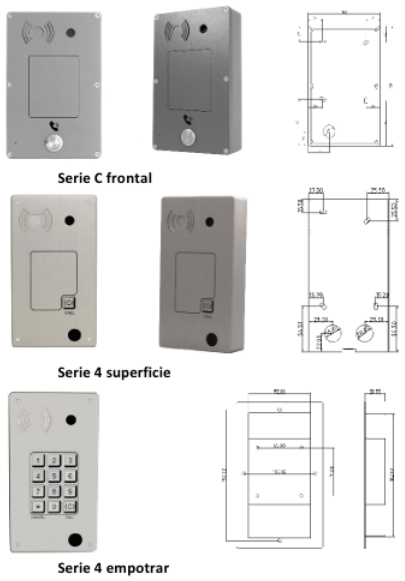
2. Installation, assembly and connection

The PANPHONE IP CSIP V6 must be installed according to the supplied model, mounting hardware, and electrical diagram of the installation. Before mounting or powering the device, check the wiring routing, connector locations, available power supply, and the purpose of each relay.

2.1 Installation models

The equipment can be supplied in different installation formats. The assembly procedure depends on the model purchased and the accessory used.

- **Front C-Series:**Front format for installation according to corresponding support.
- **Series 4 surface:**installation with back cover fixed to wall.
- **Series 4 recessed:**integrated installation in a prepared recess for the equipment.



PANPHONE IP CSIP V6 mounting models and references.

2.2 Required Materials

The following materials are required as a minimum for basic mechanical installation:

- Wall plugs suitable for the type of wall or support. Screws compatible with the
- wall plugs and the base of the equipment. Marking tool, drill, and appropriate
- screwdriver. Network, power, and access wiring prepared according to the
- installation.

2.3 Surface mounting

1. Take the base or back cover and place it in its final position.
2. Mark the fixing points on the wall.

3. Drill the marked points and insert the dowels.
4. Run the necessary wiring before closing the assembly.
5. Secure the base to the wall with the corresponding screws.
6. Install the intercom front panel.
7. Adjust the safety screw located at the bottom of the equipment.

2.4 Flush mounting

In the recessed model, an approximate opening of**182 x 92 mm**with a depth of**30 mm**Before making the hole, confirm the dimensions of the supplied accessory and leave enough space for the cable to pass through.

2.5 Identification of internal connections

The panel photograph provided for this revision shows the silkscreen marking "CSIP V6.1," but its front image does not clearly identify the function and numbering of all pins. Before connecting, use the silkscreen marking and wiring diagram corresponding to the physical revision supplied. "CSIP H6 — V 6.0" is the panel string; it does not, by itself, identify the board revision.

2.6 Relay power supply and connection

The installation can use PoE over Ethernet or an external power source compatible with the supplied board. The relay contacts are wired according to the wiring diagram for that board and the connected automation system. Do not apply power to a terminal or connect a lock based solely on a photograph or the part number of another revision.

> **Before wiring.**Confirm with the technical lead the polarity, voltage, relay capacity, and assignment of each terminal on the physical board. The pinout diagram for revision V6.1 is pending validation for this release.

2.7 NO/NC relay contact configuration

The relay contacts can be configured as**NO**(normally open) or**NC**((normally closed) using the corresponding jumpers on the plate. This configuration must be defined according to the type of lock, door opener, barrier, or automation system connected.

> **Caution.**Do not exceed the maximum capacity allowed by the relay contacts. If in doubt, use an intermediate relay or consult the installation's electrical diagram.

2.8 Equipment configuration bridges

The Home panel indicates the status of three jumpers. This reading does not confirm the function of each position in the supplied physical inspection. Do not install or remove jumpers to change the network or restore the equipment without the approved schematic for that board and the service procedure.

2.9 Access Recovery

If you have forgotten the panel's regular password, use the individual recovery credentials provided for that same board by the authorized administrator. If the current IP address is unknown or the credentials do not allow access, request the specific procedure for physically inspecting the equipment from the technical lead. Do not apply a jumper sequence from another repair without verifying it.

2.10 Checks before powering the equipment

- Verify that the equipment is firmly secured and without mechanical stress on the wiring.
- Verify that the Ethernet cable, power supply, and relay contacts are correctly connected to the connection area. Do not
- power the device until polarity, voltage, and relay connections have been checked.
- If using PoE, confirm that the switch or injector meets the installation requirements. If using an
- external power supply, verify that it delivers 12 Vdc within the supported range.
- Identify each opening wire before connecting it to the relays to avoid operating the wrong door.

> **Security.**The installation, power supply, and connection of locks or automation systems must be performed by qualified personnel. Do not handle the wiring while the equipment is powered on.

3. Programming and first access

The PANPHONE IP CSIP V6 is configured through its internal web interface. To access it, the computer must be connected to the same network as the device or to the address set by the installer. This first part explains how to access the panel, the login screen, the main menu, and the Home screen.

3.1 Access from browser

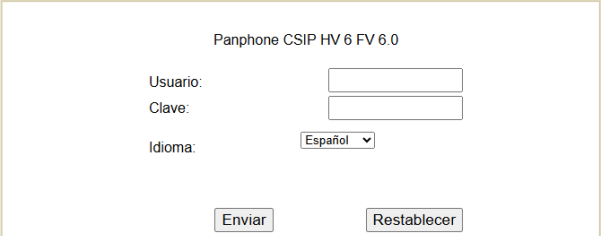
Use a compatible browser, preferably Chrome or Microsoft Edge. In the address bar, enter the computer's IP address followed by the web access port.

- **Factory address:**http://192.168.1.50:8090.
- **If the IP address has been changed:**Use the new address provided by the installer, keeping the configured port. **Network range:**The
- computer from which you are accessing the system must be on the same network range as the computer, unless there is a route or VPN configured.

> **Note.**If you do not know your current IP address or have forgotten your regular password, refer to the secure options in section 2.9.

3.2 Identification Screen

Accessing the device's web address displays the login screen. From this screen, you enter your username, password, and interface language.



Identification screen.

Field	Description
User	Authorized username to access the web panel.
Clue	Password associated with the user. It must be kept safe and changed after setup if a default password is used.
Language	Language in which the web interface will be displayed. The panel language selection does not necessarily replace the language of the audio prompts.
Send	Validate the entered data and open the settings panel.
Reset	Clears the fields on the identification screen.

3.3 Access and recovery credentials

The daily password allows access to this board's panel. The system may require you to change it after the first login. The individual recovery credential provided by the administrator still allows you to regain access to that same board if you forget the new password; it is not a general password for other boards.

> **Custody.**Keep your individual recovery credential in the facility's authorized password manager, linked to your board identifier. Do not publish it in this manual or include it in screenshots or support requests. If you suspect it has been disclosed, contact the administrator for the appropriate replacement or revocation procedure.

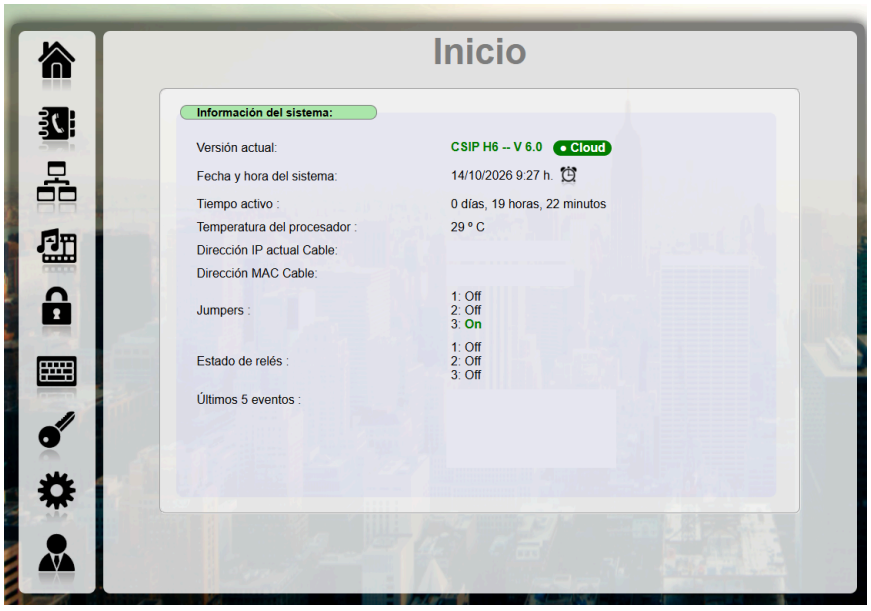
3.4 Main Menu

Once you enter your login details, the panel displays a side menu with the main configuration categories. This menu remains available while you navigate and allows you to jump between sections.

Icon	Section	What is it for?
	Start	Check the overall status of the equipment: version, date and time, network, jumpers, relays, and recent events.

	SIP Accounts	Configure call accounts, PBX registration, whitelist, and SIP options.
	Connectivity	Configure wired network, WiFi or 4G/LTE if applicable, network utilities, SMTP, SNMP and VPN.
	Multimedia	Adjust audio, video, recordings, RTSP streaming, LCD, and voiceovers.
	Relays	Manage openings, PIN, RFID, schedules, QR codes, logs, alarms, and advanced options.
	Keyboard / Button	Defines the dialing mode, code length, LED behavior, and auxiliary inputs.
	Modules and licenses	Activate or deactivate available features depending on installed hardware and license.
	Tools	Includes test call, restart, updates, web server, API and Cloud.
	Users	It allows you to change your password, select the panel language, and log out. The username is displayed as non-editable data in the reviewed screenshot.

3.5 Home Screen



Home screen of a 6.0 motherboard. IP address, MAC address, and device events have been hidden.

The Home screen is the initial check view. It is not used for programming complex parameters; it serves to verify the device's status before proceeding with the configuration.

Data shown	Utility
Current version	The update screen displays the string "CSIP H6 — V 6.0" on the tested device. The 6.0 part identifies the firmware; do not deduce the processor from this string.
System date and time	It must be correct for schedules, events, logs, and temporary access to function properly.
Active time	Indicates how long the equipment has been running since the last startup.
Temperature of processor	It helps detect abnormal operating or ventilation conditions.
IP and MAC address	Identify the device's active network connection.
Jumpers	Displays the status of the configuration jumpers read during startup.
Relay status	Indicates whether each relay appears active or deactivated.

Latest events	Summarizes recent events, such as SIP registrations, calls, accesses, or logins.

> **Initial check.**Before continuing, verify that the version is the expected one, the time is correct, the IP corresponds to the installation, and the relays appear to be at rest unless there is a test or operation in progress.

3.6 Initial Start-up Summary

Use this sequence as a quick guide for basic installation. Each step refers to later sections of the manual when more detailed configuration is required.

Passed	Action	Testing
1	Assemble the equipment and check the connections.	The equipment is fixed, with no mechanical tension on the cables and with the relays identified.
2	Power via PoE or authorized external source.	The board starts up and allows access to the web panel.
3	Access the panel from the browser.	The identification screen is displayed.
4	Log in with authorized credentials and change your password if necessary.	Access is secured before the installation is handed over.
5	Check Start, date/time, network, jumpers, relays and events.	No anomalous states appear before configuring calls or openings.
6	Configure the necessary network and connectivity.	The IP, gateway, DNS, WiFi, 4G/LTE or VPN match the installation.
7	Configure the SIP account or direct call.	The account is registered or the point-to-point call is proven.
8	Configure relays, PIN, RFID, QR codes, or schedules if applicable.	Each access activates only the intended door or exit.
9	Perform test call and opening test.	Audio, call, DTMF and relays are working correctly.
10	Log out and document the delivered configuration.	Only the installed, activated, and tested functions are recorded.

4. SIP Accounts

The SIP Accounts section allows you to configure calls on the PANPHONE IP CSIP V6. From this section, you can manage SIP accounts, PBX registration or direct IP calling, the incoming call whitelist, and general communication parameters.

Switchboard data

SIP extension or user, key, server, port, transport and supported codecs.

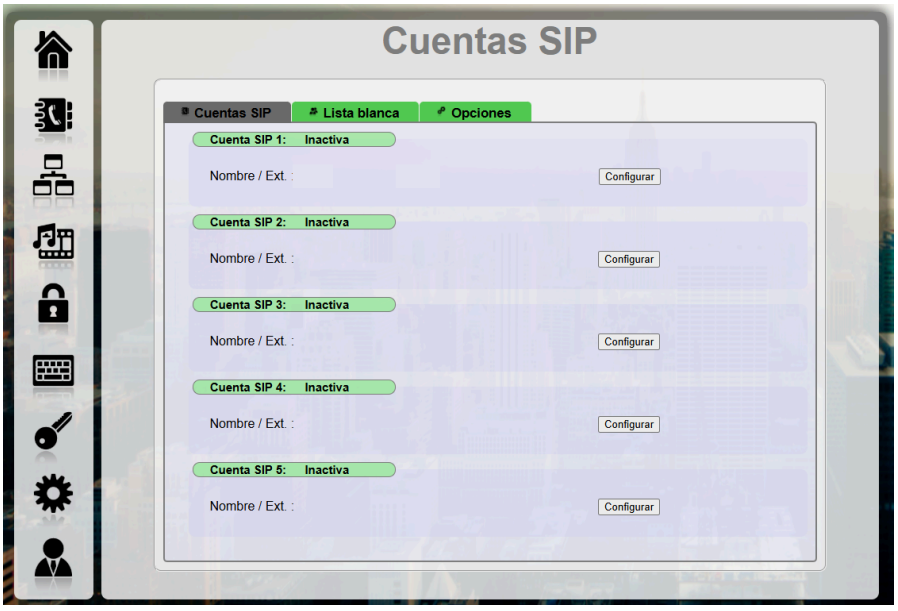
Type of call

PBX if it registers against a central switchboard. IP if it works in direct point-to-point calling.

Network used by SIP

Cable, WiFi, 4G/LTE or VPN depending on the installed hardware and the installation network.

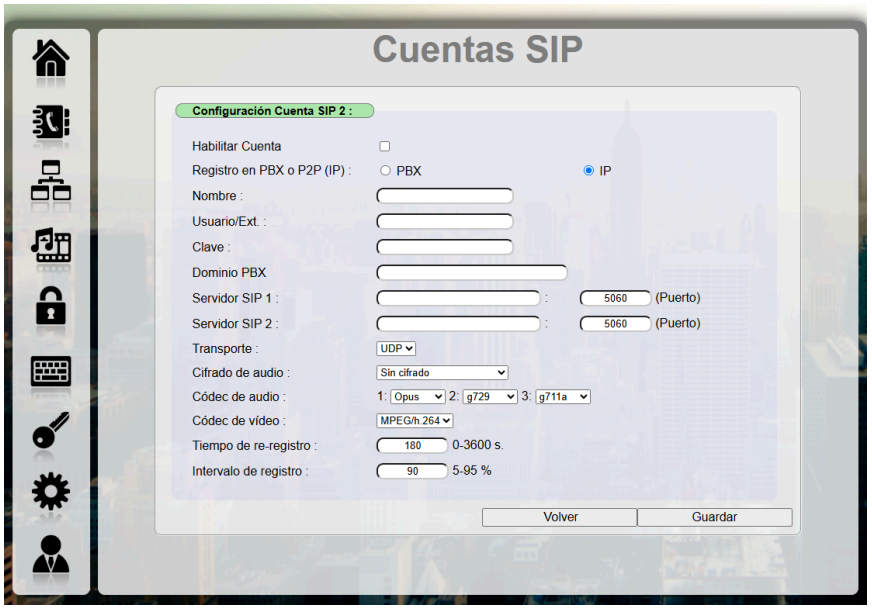
4.1 Account Overview



SIP account view; configured extensions have been hidden.

Element	What to watch or select	Note for configuration
SIP Account 1 to 5	Select the account that will be used for the installation.	Configure only the necessary accounts. Unused accounts should be deactivated.
Registered	The account appears to be correctly connected to the PBX or SIP service.	This is the expected state after saving and applying a PBX account with an available network.
Inactive	The account is disabled or does not have valid settings.	If that account is supposed to work, open it.**Set up**and check username, password, server, and network.
Name / Ext.	You must display the identifier assigned to that account.	It is advisable to use the actual extension or a recognizable name for the installation.
Set up	Tap to edit the corresponding account.	Do not change multiple accounts at once; set up and test one before moving on to the next.

4.2 Setting up a SIP account

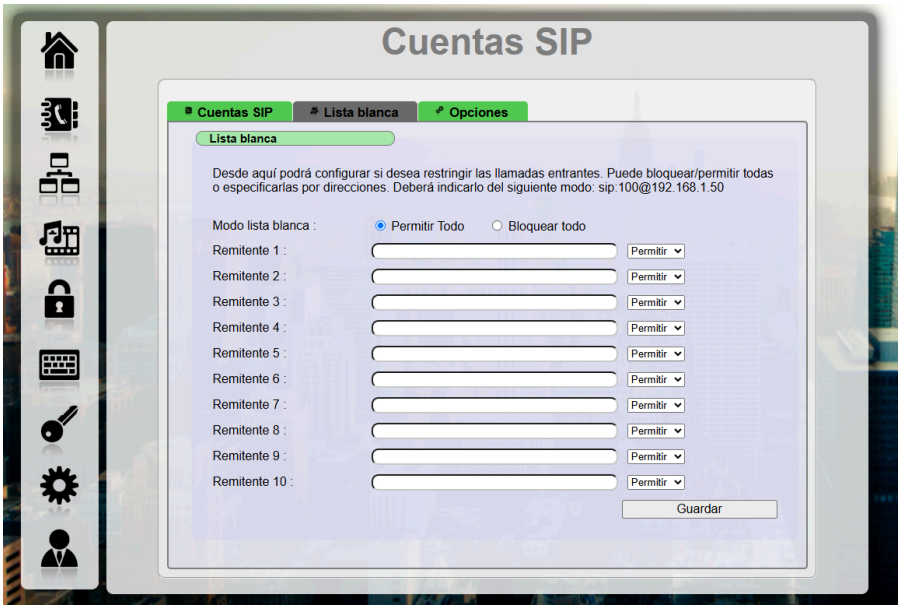


SIP account form with empty identification fields.

Field	What should you put	How to decide
Enable account	Activated if that account is going to be used.	It must be selected to register or call from that account. Deactivate it if you are not using it.
PBX or P2P (IP) Registration	**PBX**if there is a control unit.**IP**if it called directly to an IP address.	PBX is standard in installations with extensions. IP is used in point-to-point scenarios.
Name	Account identifier name.	Use a clear name to identify the sign: main entrance, garage door, reception, etc.
User / Ext.	SIP user or assigned extension.	It must exactly match the data from the control unit.
Clue	SIP account password.	Copy it without spaces. If the registration fails, check capitalization, symbols, and length.
PBX Domain	PBX domain or IP address, if required.	It can be left empty only if the control unit does not request it.
SIP Server 1	IP address or domain of the main SIP server and its port.	The usual port is 5060, unless otherwise configured.
SIP Server 2	Secondary server, if one exists.	Use only if the installation has SIP backup.
Transport	UDP, TCP or available option indicated by the switchboard.	UDP is usually the standard; always respect the PBX configuration.
Audio codec	Preferred codec order for the call.	Select codecs compatible with the control unit. The device allows you to prioritize multiple codecs.
Video codec	Video system compatible codec, if used.	It only affects devices with a camera or video call; on devices without video, it is not a critical setting.
Re-registration time	SIP registration renewal time.	Keep the value indicated by the control unit or the default value if there is no specific requirement.
Recording interval	Percentage of registration time returned by the PBX.	Do not change it unless instructed by a technician.

> **Recommendation.**Configure one account at a time and verify its registration before modifying another. If the account is not registered, check the username, password, server, port, transport, network, and connectivity to the PBX.

4.3 Whitelist



SIP whitelist. The example address is for illustrative purposes.

Field	What should you put	When to use it
Allow everything	Select this option if the board should accept any incoming calls.	Useful in closed and controlled networks, when the central unit already filters the sources.
Block all	Select this option to reject calls by default.	Recommended when only specific extensions or origins should be able to make calls.
Sender 1 to 10	SIP address authorized or blocked.	Use one line for each source you want to control.
Allow / Deny	Action applied to the entered sender.	Allow authorizes that source; Deny blocks it.
Format	sip:user@address,For example sip: 100@192.168.1.50 .	The format must match the identifier sent by the switchboard.

4.4 SIP Options

Field	What should you put	Note / Usual value
Network adapter for SIP	Select wired, WiFi, 4G or VPN depending on the network output the board needs to use.	If an option appears as unavailable, the device does not detect that module or connection.
Maximum time of communication	Maximum allowed duration for each call.	The display allows 0 to 7200 seconds. Use a reasonable limit to avoid calls remaining open indefinitely.
Local SIP port	Local SIP signaling port.	5060 is the usual value. Only change it if the network or PBX requires it.
Autoresponder	Manual, automatic, or automatic after 1, 2, or 3 tones.	Automatic response without intervention. Manual requires physical or user action depending on the installation.
RTP Port start	First port in the range used for audio/video.	It must be permitted on the network and not conflict with other services.
RTP Port end	Last port in the range used for audio/video.	It must be higher than the initial port and within the range allowed by the screen.

Caution. The SIP/RTP ports and network adapter directly affect call functionality. Do not change these settings without knowing the PBX and network configuration.

5. Connectivity

The Connectivity section groups the computer's network configuration and associated tools: wired network, WiFi or 4G/LTE modules when installed, diagnostic utilities, email sending, SNMP and VPN connection.

Network data

IP address, mask, gateway, DNS, VLAN and DHCP/static criteria.

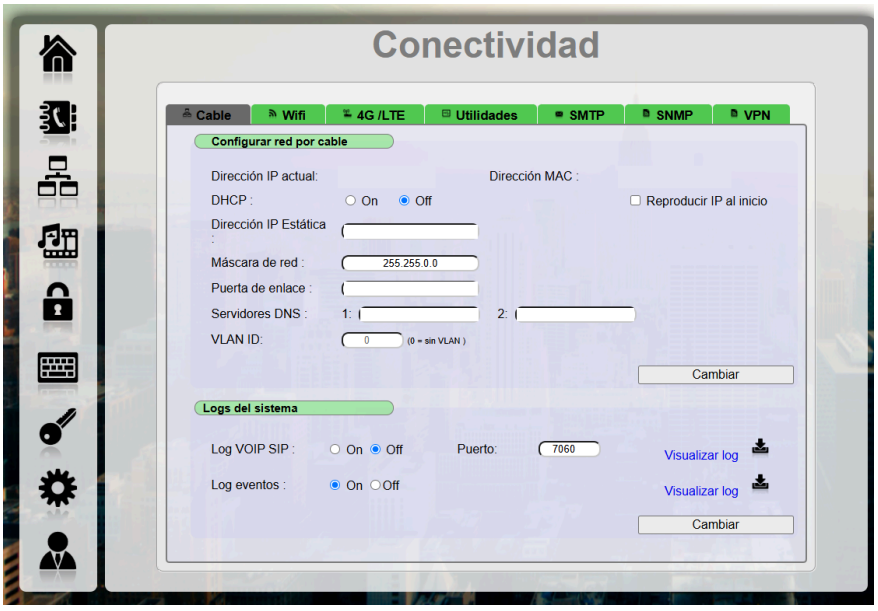
External services

Mail server, recipients, SNMP, trap servers and VPN data if used.

Modules installed

WiFi, 4G/LTE and VPN should only be configured when the equipment and installation support it.

5.1 Wired Network



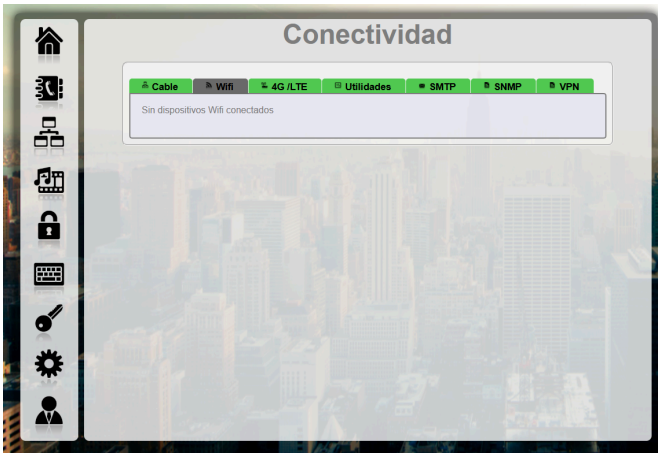
Wired network configuration. IP, MAC, gateway, and DNS have been hidden.

Field	What should you put	How to decide
Current IP address	Value shown by the team.	It is used to confirm which IP address is being accessed at that moment.
MAC Address	Physical identifier of the network interface.	Useful for DHCP reservations, network inventory, or filtering on switches/routers.
DHCP	**On**if the network assigns IPs automatically. **Off**if a static IP address is configured.	For final installations, a static IP address or documented DHCP reservation is usually recommended.
Static IP address	The IP address that the card will have when DHCP is disabled.	It must belong to the customer's network and not be used by another device.
Network mask	Mask corresponding to the local network.	It must match the installation's addressing.
Gateway	IP address of the router or device that provides access to other networks.	Required for communication outside the local network, remote SIP, email, VPN, or external services.
DNS Servers	Primary and secondary DNS.	Required if domains are used instead of IP addresses.
VLAN ID	VLAN identifier if required by the network. A value of 0 indicates no VLAN.	It only needs to be modified if the switch and the client network work with VLANs.

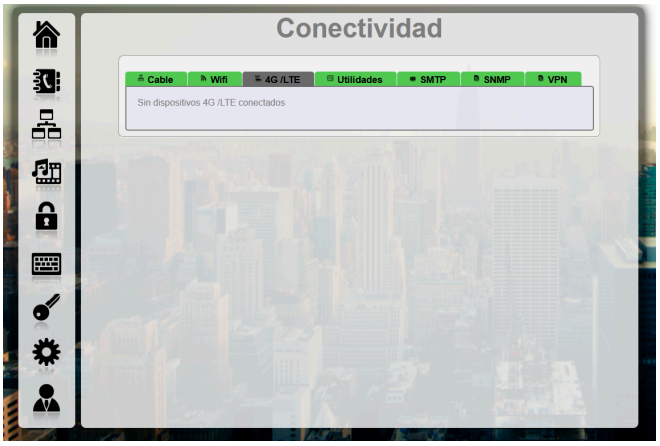
Play IP at startup	Enabled if you want the computer to advertise its IP address when it starts up.	It can help with commissioning or maintenance when the IP address is unknown.
SIP VoIP Log	Activated for SIP diagnostics only.	Use the port indicated on the screen and deactivate it when the test is finished if it is not needed.
Event log	Enabled if equipment event logging is required.	It allows you to review operating information from the viewing or download options.

Important. Before changing your IP address, confirm that the new address, subnet mask, and gateway are correct. Saving an IP address outside the network may result in loss of web access. In such a case, consult the security options in section 2.9 and your technical support team.

5.2 WiFi and 4G/LTE



WiFi tab of the device; no devices are connected in this screenshot.



4G/LTE tab; no devices are connected in this screenshot.

Screen	What to check	Interpretation
WiFi	Registration status, SSID, key, security type, MAC address, DHCP, static IP, mask, gateway, and DNS.	Configure WiFi only if the module is installed and the wireless network has sufficient coverage at the location of the equipment.
State	Indicates whether the device is registered/ connected to the WiFi network.	If "Not Registered" appears, check SSID, password, security, and coverage.
SSID	Name of the WiFi network to which the device will connect.	It must be entered exactly as it appears in the access point. The Search Networks button helps locate available networks.
Key and security	Network password and security mode, for example WPA2.	It must match the actual configuration of the router or access point.
DHCP	■ On ☐ Off	On: Obtains IP automatically. Off: Allows you to enter a static IP address, subnet mask, gateway, and DNS.
Static IP address / Subnet mask / Gateway / DNS	Network parameters used when DHCP is Off.	They must belong to the client's WiFi network and not duplicate another existing IP address.
4G/LTE	Mobile network status, signal level, IMEI, PIN, APN, username and password.	Configure this data only with a valid SIM and the parameters provided by the operator.

Network identification	Indicates whether the mobile module is registered or if it requires PIN verification.	If it asks you to check the PIN, check the SIM PIN before continuing.
Network type / Level	It displays available coverage using signal bars.	If the signal is weak, check the antenna, location, or operator coverage.
IMEI	Unique identifier of the mobile module.	It is used for service support or registration; it should not be modified.
PIN	SIM card PIN, if required by the SIM.	It must be entered exactly. An incorrect PIN may block the SIM.
APN / Username / Password	Mobile network access details of the operator.	Fill them in only with the official data of the operator or the client.
SIP adapter	If a module exists, also check the adapter selected in SIP Options.	The SIP call must go out over the actually available network: cable, WiFi, 4G/LTE or VPN.

5.3 Network Utilities

Field	What should you put	What is it for?
Gateway	Gateway associated with the selected adapter.	Allows you to check or change the network output used by the device.
Network adapter	Cable or other available adapter.	Select the link you want to try.
Address	IP address or destination domain of the test.	Use the IP address of the PBX, the router, or a test domain depending on what you want to verify.
Take the test	Run the PING test.	The result helps to determine if there is connectivity to the indicated destination.
Result area	Result returned by the test.	If there is no response, check IP, mask, gateway, DNS, cabling, or network rules.

5.4 SMTP

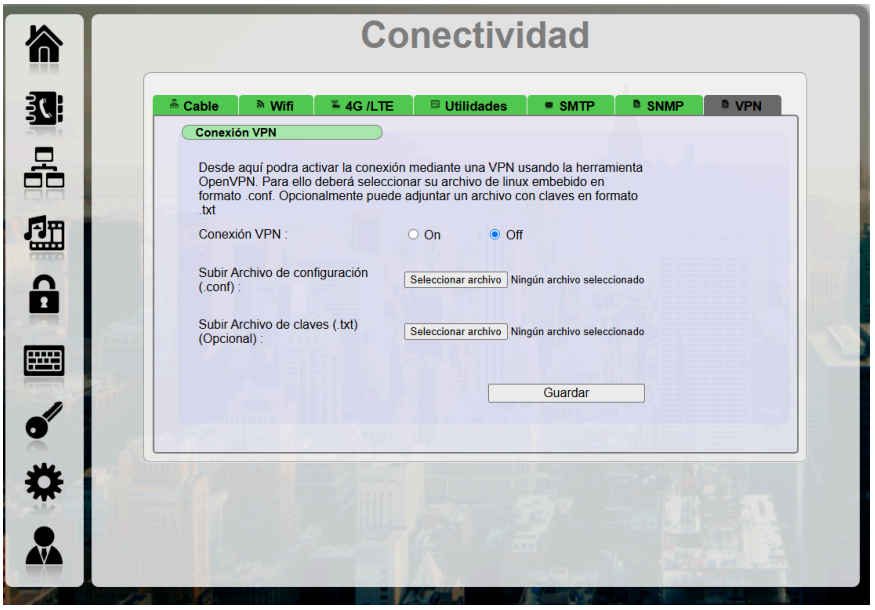
Field	What should you put	How to decide
Addressee	Email address that will receive the notifications or the proof.	It must be a valid address, reviewed by the customer or maintenance.
Sender	Email address from which the messages will be sent.	It must be allowed by the SMTP server used.
Use server	Internal or external, depending on the installation's mail server.	Use external when the client provides their own SMTP server.
Mail server (SMTP)	SMTP server domain or IP address and port.	The port depends on the server. The screen shows port 25 as an example. configuration.
User	SMTP authentication user if required by the server.	It must match the configured email account.
Password	SMTP account key.	Only introduce it in facilities where email sending is approved and documented.
Security	Security mode available in the dropdown menu.	Select the value required by the mail server.
Send test email	Send an email to verify the settings.	It must be tested before handing over the installation if mail notifications are to be used.

5.5 SNMP

Field	What should you put	When to use it

SNMP Status	Current status of the SNMP service.	It must be verified before documenting active monitoring.
Sending traps	On if the team should send traps; Off if they are not used.	Activate traps only if there are servers prepared to receive them.
Server 1 to 3	IP address or name of the monitoring servers.	Use the servers provided by the client or network administrator.
Community	SNMP community string.	It must match the SNMP platform configuration.
Name	Team identification name.	Use a name that allows the location or function of the plate to be recognized.
Description	Device description.	It helps to identify it in the monitoring tool.
Location	Physical or logical location of the equipment.	It must be clear for maintenance: portal, door, building, floor, etc.
Contact	Email or responsible contact.	Use a contact authorized by the customer.

5.6 VPN



Panel 6.0 VPN options. No key file is attached.

Field	What should you put	Caution
VPN connection	Turn On to activate the VPN; Turn Off to keep it deactivated.	Do not activate VPN without confirming that the files and network are correct.
Configuration file (.conf)	OpenVPN configuration file.	It must correspond to the client's installation and VPN server.
Key file (.txt)	Optional file with keys or credentials, if required by the deployment.	It must be protected as sensitive information.
Keep	Apply the selected settings.	Afterwards, verify that the equipment maintains access via the expected route.

> **Good practices.**Always document the final IP address, the adapter used for SIP, and any configured external services. Do not leave logs, SNMP, SMTP, or VPN enabled if they are not part of the delivered installation.

6. Multimedia

The Multimedia section allows you to adjust audio, video, recordings, RTSP streaming, and the LCD screen. Some functions depend on the installed hardware, especially those related to the camera, video calls, recordings, and display.

Call audio

Speaker volume, microphone sensitivity, echo cancellation, buffers, and audio test.

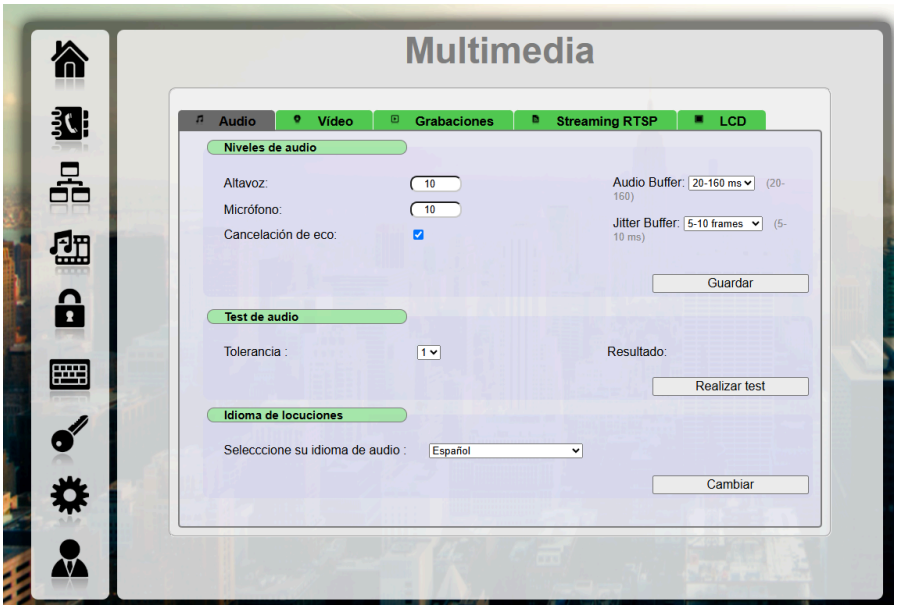
Image and video

Preview, brightness, contrast, saturation, hue, resolution and camera parameters.

Multimedia services

Recordings, RTSP, voiceover language and LCD screen messages where available.

6.1 Audio



Audio controls and sound test panel 6.0.

Field	What should you put	How to decide
Speaker	Speaker output level.	Adjust it during an actual call. Turn it up only as much as necessary for clear sound.
Microphone	Microphone pickup sensitivity.	If the other person hears it quietly, increase the value; if there is saturation or noise, reduce it.
Echo cancellation	Activated or deactivated.	It must remain activated except for specific technical tests.
Audio Buffer	Audio buffer available in the dropdown menu.	This affects stability and latency. Keep the current setting if the call works. correctly.
Jitter Buffer	Buffer against network variations.	It can help on unstable networks, but high values can increase latency.
Tolerance	Level used for the audio test.	Use the test to check remote audio without sending personnel to the panel.
Language of speech	Language or audio mode of the voiceovers.	Select the language for audible messages or turn off voiceovers/sounds if the installation requires it.

6.2 Video

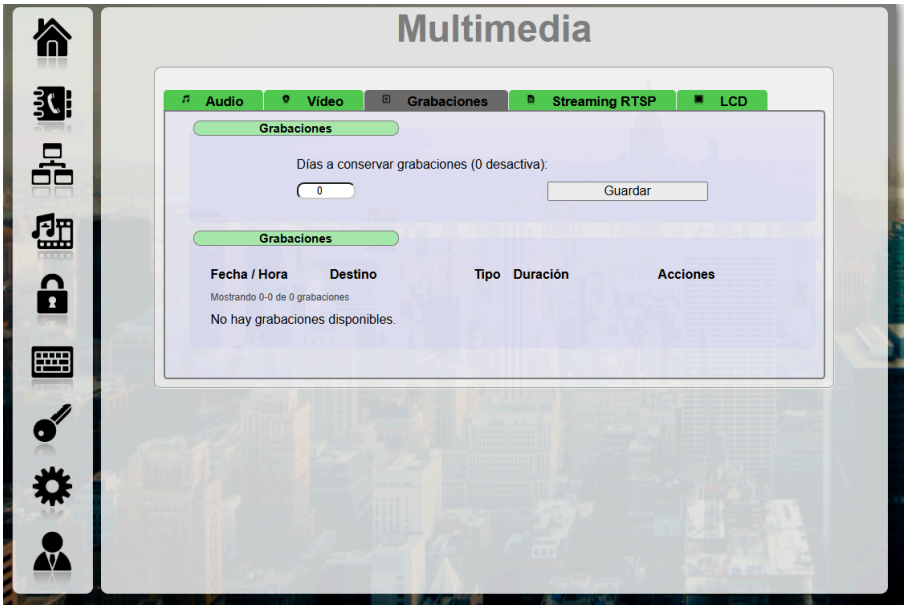


Video image controls; preview is disabled during capture.

Field	What should you put	When to play it
Live preview	It does not fill in; it displays the camera image.	It is used to check framing, visual focus and the effect of adjustments.
Glow	Image brightness level.	Adjust it if the scene looks too dark or overexposed.
Contrast	Difference between light and dark areas.	Adjust it if the image looks flat or lacks detail.
Saturation	Color intensity.	Use moderate values to avoid artificial colors.
Tone	Image color correction.	Do not change it unless the image has a dominant color.
Resolution	320x240, 640x480 or 800x600, depending on the available selection.	Higher resolution offers more detail; lower resolution can reduce network consumption.
White balance automatic	Enabled to allow the camera to adjust color temperature.	This is recommended in most facilities.
White temperature	Manual value if automatic balance is not used.	It should only be adjusted when working in manual mode.
Backlight compensation	Off or On.	Activate if there is a strong light behind the person or object you want to see.
Line frequency	Off, 50 Hz or 60 Hz.	In European electrical installations, 50 Hz is commonly used to reduce flickering.
Restore default values	Returns video parameters to base values.	Use this option if the adjustments leave the image incorrect and you need to start from scratch.

Note. Video settings are saved and automatically applied when you move a control, as indicated on the version 6.0 screen. Make small changes and check the preview before proceeding.

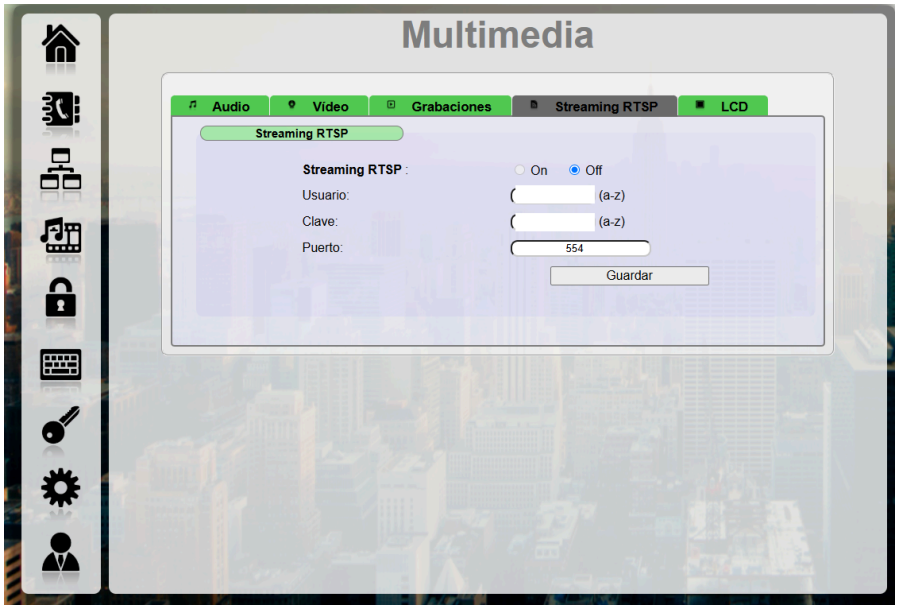
6.3 Recordings



Screen of recordings with no available recordings.

Field	What should you put	Interpretation
Days to keep recordings	Number of days of retention. A value of 0 disables retention.	Define it according to the client's policy and available capacity.
Date / Time	Data shown in existing recordings.	It allows you to locate the time of the recorded event.
Destination	Destination associated with the recording.	It helps to identify calls, access, or related events.
Guy	Type of recording or event.	It is used to filter or understand the origin of the recording.
Duration	Recorded time.	It should be reviewed whether calls or incidents are being investigated.
Actions	Available operations on the recording.	It may vary depending on whether or not recordings are available.

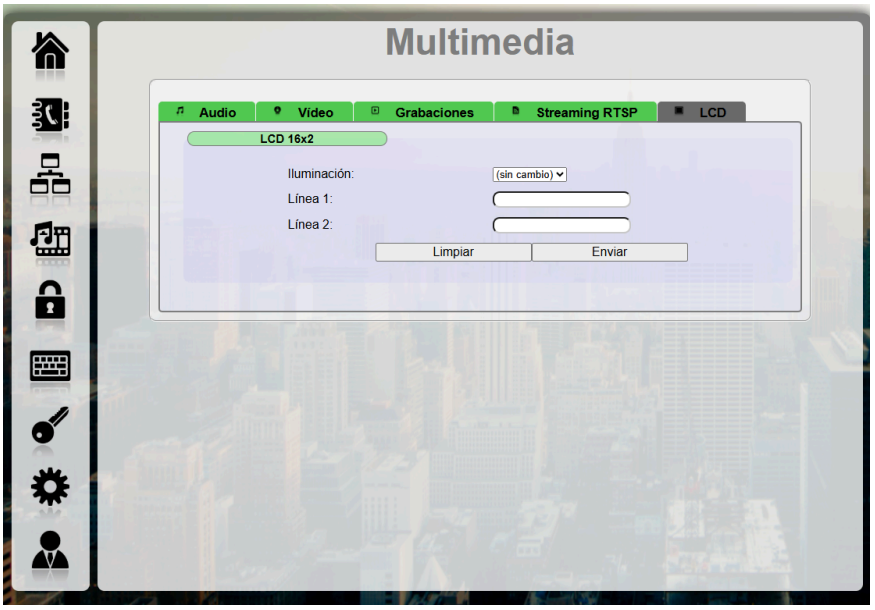
6.4 Streaming RTSP



RTSP configuration. The visible username and password have been hidden.

Field	What should you put	Caution
RTSP Streaming	On to activate; Off to deactivate.	The screen indicates that RTSP is unavailable while the QR reader is active.
User	RTSP access user.	It should only be known by authorized personnel.
Clue	RTSP access key.	Change default values before delivery if the service remains active.
Port	RTSP listening port.	The value displayed on the screen is 554; change it only if the network requires it.

6.5 LCD



LCD controls 16×2.

Field	What should you put	What is it for?
Lightning	Select On, Off or (no change).	Controls the backlighting of the 16x2 LCD screen if the device has one.

Line 1	First text to display.	Use short and clear messages.
Line 2	Second text to display.	It serves to complete the message without cluttering the screen.
Send	Apply the written text.	Check the result on the physical screen of the device.
Clean	Clear the displayed content.	Useful when you want to remove a temporary message.

Final check. After modifying audio, video, RTSP or LCD, make a test call and verify image, sound, messages and external services before handing over the installation.

7. Relays and access

The Relays section allows you to define how opening outputs operate and how access is authorized using PINs, RFID cards, schedules, QR codes, logs, alarms, and advanced options. These settings directly affect doors, locks, automation systems, and auxiliary outputs.

Opening exits

Relays 1, 2, 3 and combined action 1+2+3, with different activation modes.

Access credentials

PIN, RFID and QR allow you to associate name, code, schedule and opening relay.

Control and traceability

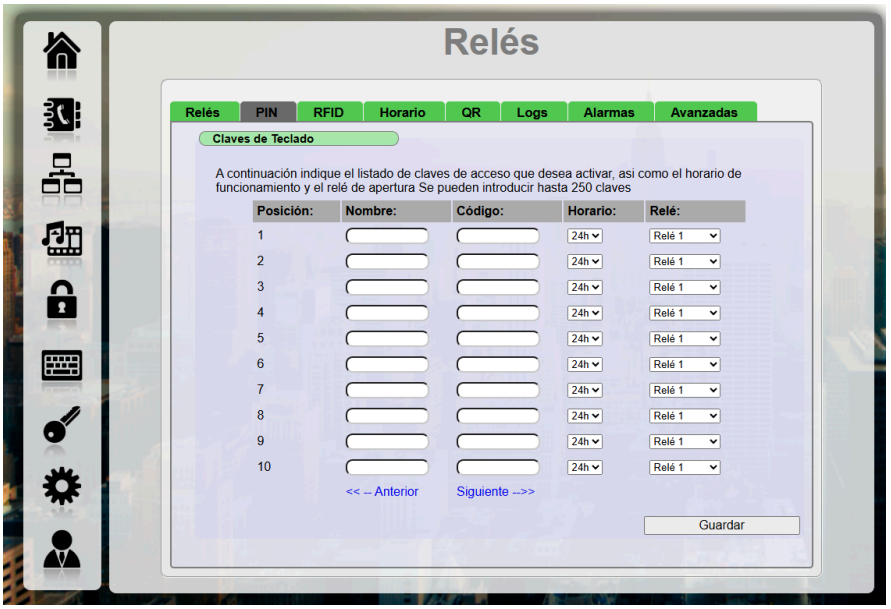
Schedules, logs, alarms, and an external database help to limit and audit usage.

7.1 Relay configuration

Selectable value	What does it mean	When to use it
Relay 1 / Relay 2	Main opening or maneuvering outlets.	Use each relay for a door, lock, barrier, light, or other automation defined in the installation.
Relay 3	Third output available when the equipment/hardware supports it.	It should only be documented if the board has this output or additional module.
Combined relay 1+2+3	Joint operation of several relays.	Useful when an authorization needs to activate multiple outputs at once.
Timed	The relay is activated for a configured time and then returns to rest.	Usual method for opening doors or locks.
Manual	The relay is maintained according to the manual activation/deactivation order.	Use it only when the installation requires maintained manual control.
During communication	The relay remains active as long as communication exists.	Applicable to maneuvers that depend on an active call.
During stamping	The relay is activated during the ringing/ calling period.	Use this option only if the automation needs to follow the incoming or outgoing call state.
Pulsation	The relay acts as a pulse associated with an action.	Useful for systems that require a brief boost.

Caution. Before saving changes, confirm that each relay physically corresponds to the expected door or output. An incorrect assignment may open a different door than intended.

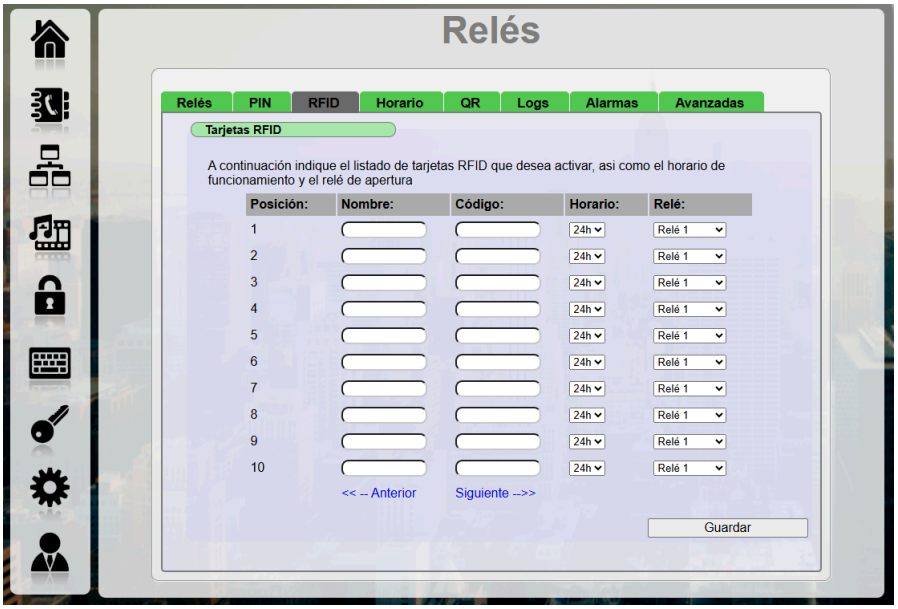
7.2 Access via PIN



PIN key management: name, code, schedule and associated relay.

Field	What should you put	Good practices
Position	Registration number within the list.	It is used to organize and locate credentials.
Name	Person, dwelling, service or use assigned to the PIN.	Use clear names so that access can be audited later.
Code	Numeric key to be entered on the keyboard.	Do not use obvious or repetitive codes. Document who is authorized to use them.
Schedule	Schedule that limits the operation of the PIN.	Select the appropriate time if access should not always be available.
Relay	Output that will be activated upon PIN validation.	Please check that it corresponds to the correct door.
Previous / Next	Navigate between key pages.	Use pagination to review all records before submitting.

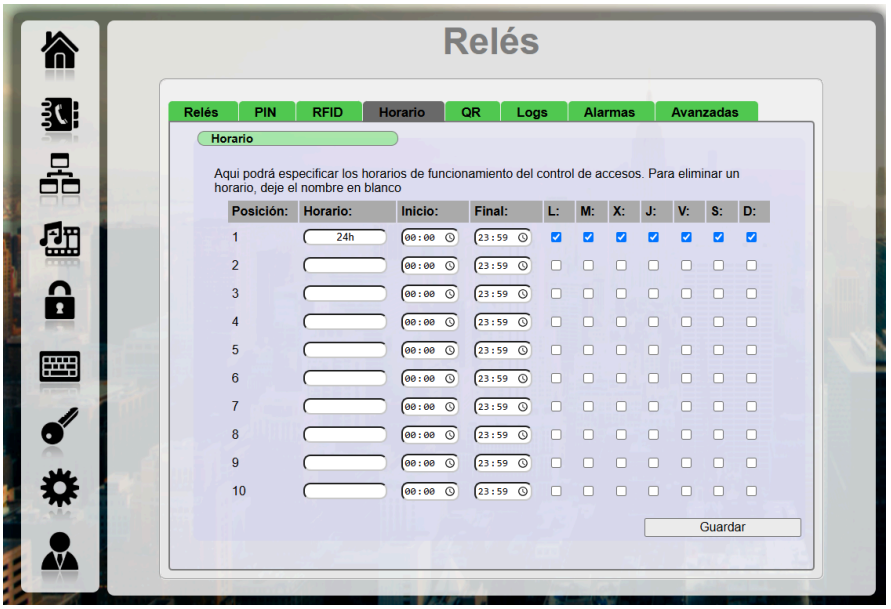
7.3 Access via RFID



RFID credential management: name, code, schedule and associated relay.

Field	What should you put	How to use it
Name	User, dwelling, vehicle or assigned card.	It must allow identification of who the card belongs to.
Code	RFID code of the card or credential.	Enter the exact identifier recognized by the system.
Schedule	Card validity period.	Useful for maintenance access, suppliers, or users with limited bandwidth.
Relay	Exit that will be activated with that card.	Select the appropriate door or maneuver.
Keep	Apply the changes from the current page.	Save after modifying additions, removals, or relay/schedule changes.

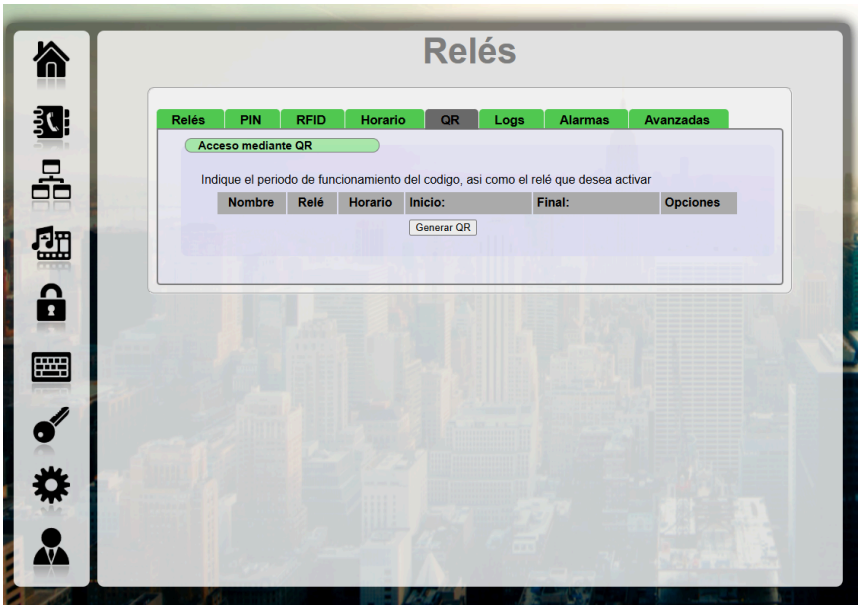
7.4 Access times



Setting up time slots and allowed days.

Field	What should you put	Example of use
Schedule	Time slot name.	For example: Labor, Maintenance, Delivery, 24h.
Start / End	Start and end time of validity.	Use clear time format and check that the system time is correct.
LMXJVSD	Days of the week on which it applies.	Mark only the authorized days.
Blank name	Delete the schedule as indicated on the screen.	Before deleting, check that no active PIN, RFID, or QR codes are in use.

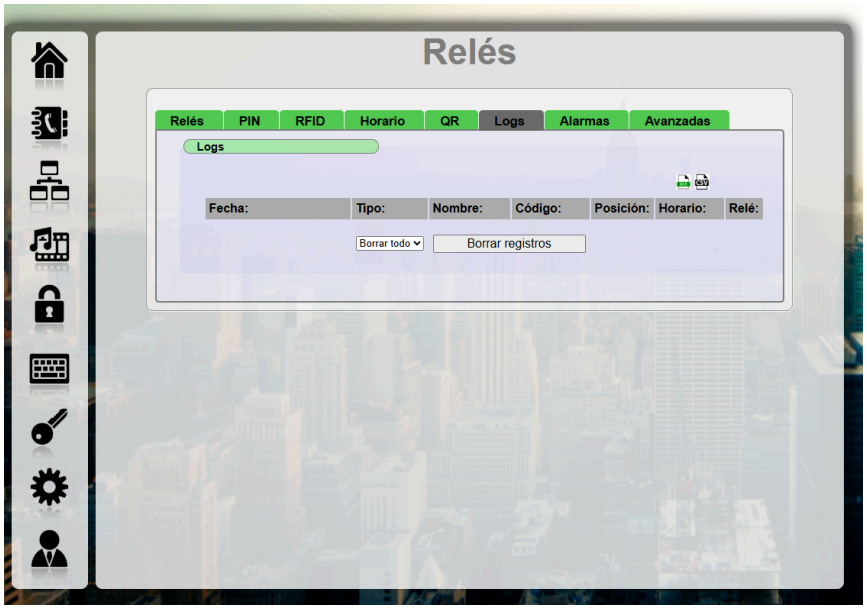
7.5 Access via QR



List of QR access codes and button to generate a new code.

Field	What should you put	Caution
Name	Identification of the generated QR code.	Use a name that indicates user, visit, service, or purpose.
Relay	Exit that will activate the QR code.	Verify that it matches the authorized door.
Schedule	Schedule associated with the QR code, if applicable.	Useful for limiting usage by days and hours.
Start / End	Code validity period.	Define expiration dates/times when access is temporary.
Temporary	Quick QR duration, for example one hour when that value is selected.	Use this option for short, controlled access.
Date range	Start and end date and time.	Use this option when the QR code needs to be valid for a specific period.
Send by mail to	Recipient's email address.	Requires SMTP to be configured and should only be used with authorization from the responsible party.
Generate QR code	Create the code for its use.	Do not distribute QR codes without registering who they are valid for and until when.

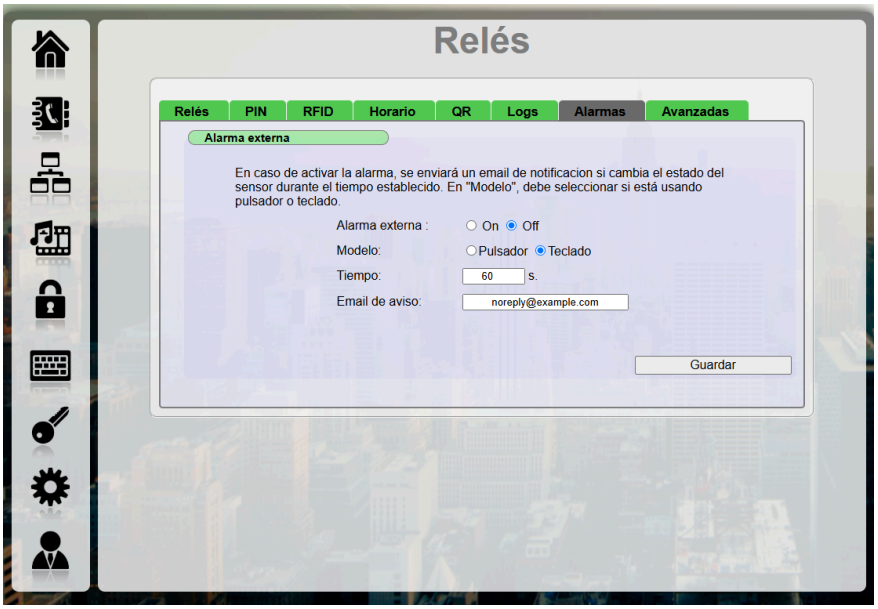
7.6 Access Logs



Query and export access logs. The capture contains no logs.

Field	Which shows	Recommended use
Date	Time of registration.	Necessary for auditing incidents.
Guy	Type of event recorded.	It helps to distinguish PIN, RFID, QR or other access codes.
Name / Code	Identification associated with access.	It allows you to link the event to a credential.
Position / Time / Relay	Configuration data used for access.	Useful for checking why an output was activated.
Export	Download records, according to available icons.	Use export before deleting records if evidence needs to be preserved.
Delete records	Delete records according to the selected option.	Do not delete logs without authorization from the person responsible for the installation.

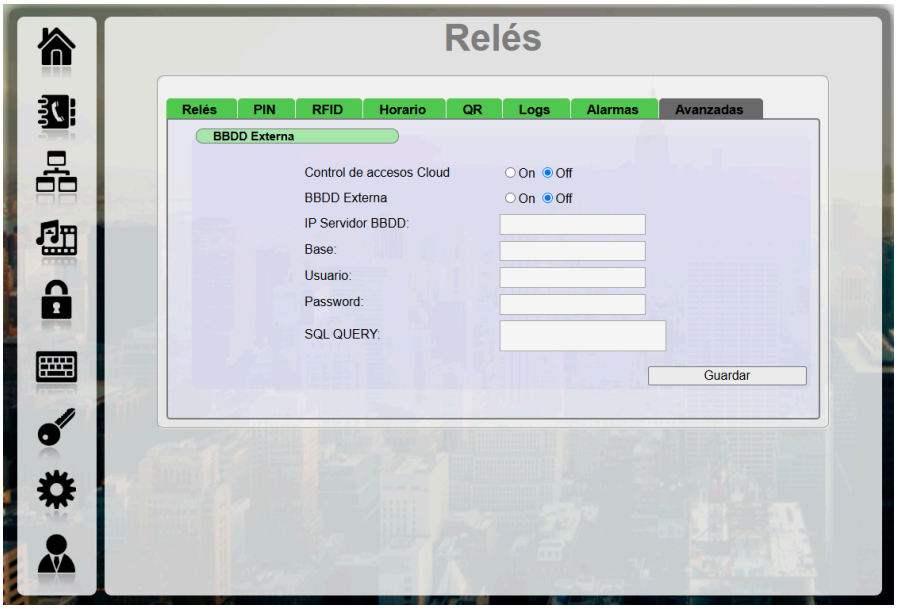
7.7 Alarms



External alarm options. The email address is an example of the interface.

Field	What should you put	Precondition
External alarm	On to activate; Off to deactivate.	Activate only if sensor change notification is required.
Model	Pushbutton or Keyboard.	It must match the installed front panel/equipment.
Time	Monitoring time in seconds.	Define how long the state change is evaluated.
Notification email	Address that will receive the notification.	SMTP must be configured correctly in Connectivity.

7.8 Advanced Options



Cloud configuration and external database. IP address, database, username, password, and SQL query have been hidden.

Field	What should you put	Caution
Use CLOUD	On or Off depending on the integration contracted.	Do not activate Cloud if it is not part of the project.
external database	On if an external database is consulted.	Requires server, credentials, and query validated by the client.
Database server IP	Database server address.	It must be accessible from the team's network.
Base	Database name.	It must exactly match the server configuration.
Username / Password	Database access credentials.	This is sensitive data and must be protected.
SQL QUERY	SQL query to be executed.	It must be provided and validated by authorized technical personnel.

> **Delivery to the customer.**Document which relays each credential opens, what hours they are active, and who is authorized. Do not release PINs, cards, QR codes, database credentials, or cloud configurations without approval from the person responsible for the installation.

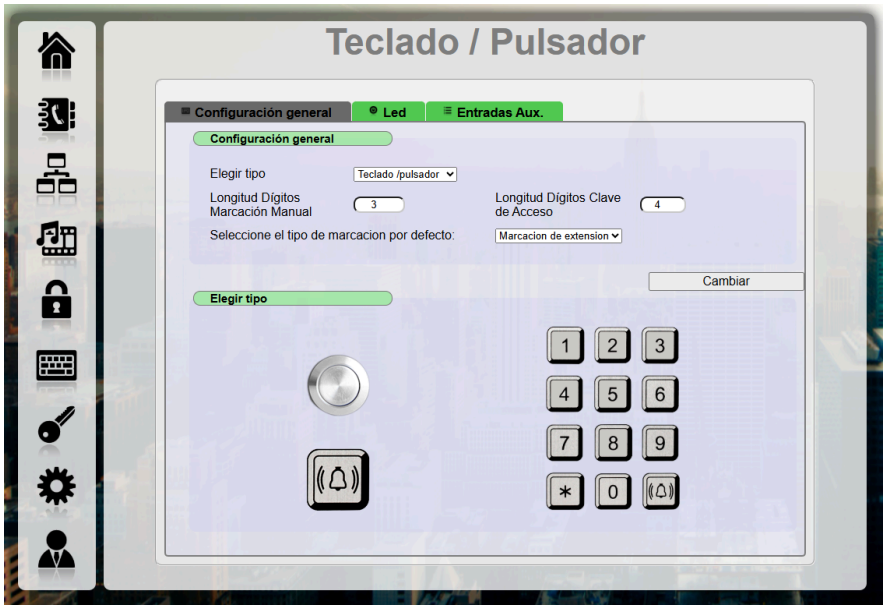
8. Keyboard / Pushbutton

The Keypad/Pushbutton section defines how the keypad, pushbuttons, status LED, and auxiliary inputs behave. These settings determine whether the user dials extensions, enters PINs, calls contacts, activates relays, or

It uses external inputs.

Front panel mode	Marking	Signaling
Keyboard, push button, auxiliary inputs, headphone jack or combinations depending on the installed equipment.	Digit length, default mode, calls by extension, by IP or key actions.	Status LED, auxiliary inputs, and behavior when a button is held down.

8.1 General configuration



General configuration of the front panel Keyboard/Pushbutton.

Field	Options / value	Correct use
Choose type	■ Keyboard / Pushbutton ☐ Auxiliary Inputs ☐ Keyboard + Relay button ☐ Handset ☐ Headset + keyboard	It must match the front panel and installed accessories. Do not select hardware features that the computer does not have.
Keyboard / Pushbutton	Mixed mode for keyboard and push button.	Use when the device has a keypad and call/open button according to the configuration.
Auxiliary Inputs	Give prominence to the auxiliary entrances.	Use if calls or relays will be triggered from external contacts.
Keyboard + Relay button	It combines a keyboard with a push button associated with a relay.	Use if the push button needs to operate a relay output.
Headset / Headset + keyboard	Modes for devices with headphones.	It should only be selected on models that have a headphone jack.
Manual dialing digit length	Number of digits that make up a manually dialed extension.	It must match the length of the installation extensions.
Length of access key digits	Expected number of digits for access PIN.	It must match the length of the codes defined in Relays and access.
Default dialing	☐ Extension dialing ■ PIN dialing ☐ API Markup	Defines what the equipment interprets when the user enters digits.

Extension dialing	The digits are treated as a call extension.	Use in facilities where the visitor directly dials an extension.
PIN dialing	The digits are treated as an access key.	Use when the keyboard is primarily used for opening by code.
API Markup	The digits are sent or interpreted via API integration.	Use only if a defined external integration exists.
Drawing of buttons and numbers	The icons on the push button and each number on the keypad are shortcuts to your settings screen.	Configure each button or key that will be used after selecting the general mode.

8.2 Pushbutton or key configuration

Selectable value	What are you doing	Required fields
Choose type	■ Single Key ☐ End call ☐ Call prefix ☐ Key prefix ☐ Call to extension ☐ Direct IP call ☐ Manual response	Select the action that this key or button should perform.
Single Key	The key remains as a simple system action.	No additional call data is required.
Cancel current call, End call	Cancel the dialing or end a call.	It does not require a destination.
Call prefix	Enter a call prefix.	It should only be used if the installation markings require it.
Key access prefix	Enter a prefix for key/PIN.	It must match the defined access criteria.
Call to Extension	Call a PBX extension.	Fill in User/Ext. and select SIP Account 1 to 5.
Direct IP call	Call directly to an IP address or server.	Fill in IP, User/Ext. and SIP Account 1 to 5.
Manual Response in Incoming call	It allows you to use the key to manually answer incoming calls.	Use when the installation requires a manual response from the equipment.
SIP Account	■ SIP Account 1 ☐ SIP Account 2 ☐ SIP Account 3 ☐ SIP Account 4 ☐ SIP Account 5	Select a configured and operational account in the SIP Accounts section.
SIP Account 1 to 5	Each option indicates which SIP account that key will use to make a call.	If the chosen account is not registered, the key will not be able to complete the call.

8.3 Pushbutton contacts

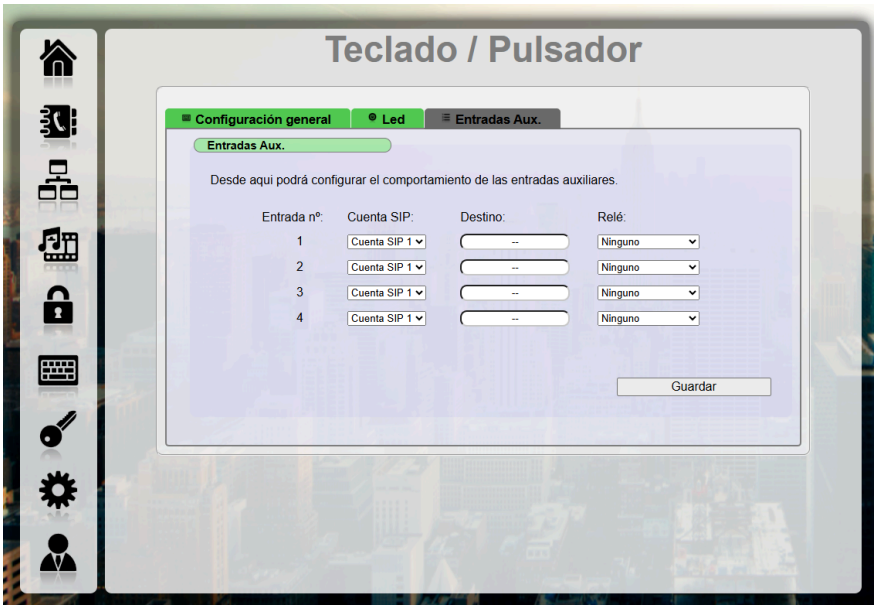
Field	What should you put	How to decide
Waiting time	Seconds before moving on to the next contact. The interface supports a range of 3 to 99 seconds.	Allow enough time for the destination to respond without unduly delaying the progressive call.
Contact 1 to 4	Call order. Contact 1 is attempted first; if there is no answer, it continues with the next configured contact.	Order the destinations by priority: reception, concierge, maintenance, etc.
Name	Descriptive label of the contact.	Use clear names for maintenance and subsequent review.

User / Ext.	Extension or target user.	It must match the configured switchboard or destination.
IP / Server	Destination server or IP address.	Use the corresponding SIP server or IP address.
Port	SIP port of destination.	5060 is common, but the actual installation configuration must be respected.
Allow hanging up by pressing a button	Activated if a single press allows you to end the call.	Use if you want the user to be able to end the call from the button.
Delay in pulse	■ Deactivated ☐ 0.5 s ☐ 1 s ☐ 1.5 s ☐ 2 s ☐ 3 s	Defines how long the button must be held down before the action is performed; higher values prevent accidental presses.

8.4 LED Configuration

LED option	What are you doing	When to use it
configurable states	Rest, Registration OK, Making call, Incoming call and In communication.	Assign a consistent and easily recognizable behavior for the end user.
Available options	☐ Off ■ On ☐ Normal blinking ☐ Rapid blink ☐ Slow blink	The same list can be chosen for each state.
Off	The LED remains without light in that state.	Use if visual indication is not desired.
On	The LED remains fixed.	Useful for indicating rest, correct recording, or stable state.
Normal blinking	Intermediate blink.	Useful for indicating active communication without being too conspicuous.
Rapid blink	More visible blinking.	Useful for outgoing or incoming calls, when you want to attract attention.
Slow blink	Soft blinking.	It can be used for lower priority informational statuses.

8.5 Auxiliary inputs



SIP account assignment, destination and relay output via auxiliary input.

Auxiliary input

Identify which of the four physical inputs is being configured.

Associated call

SIP account and destination define where the call is coming from and who is calling.

Relay output

It allows you to not activate anything or to maneuver a specific exit.

Element	Options / value	Correct use
Entrance	Entrance 1, 2, 3 or 4.	Identify the physical contact being configured. It must match the actual wiring of the installation.
SIP Account	■ SIP Account 1 ☐ SIP Account 2 ☐ SIP Account 3 ☐ SIP Account 4 ☐ SIP Account 5	Select the account from which the call associated with the entry will be made.
Destination	Configured extension, user, or destination.	It must match the destination that should receive the call or action.
Relay	■ None ☐ Relay 1 ☐ Relay 2 ☐ Relay 3 ☐ Combined 1+2+3	Use None if the input should not open or activate an output; select relay only if it must operate an output.
None	The auxiliary input does not activate any relays.	Use when the input should only generate a call or notification.
Relay 1 / 2 / 3	Activate a specific output of the device.	It must match the door, lock, or control wired to that relay.
Combined 1+2+3	Activate all three relays together.	Use only if the installation requires a documented simultaneous operation.

Testing. After changing the type of keypad, LED, auxiliary inputs, or pushbuttons, physically test each key and each input to confirm that it calls the correct destination and does not activate unintended relays.

9. Modules and licenses



View of the available modules and their activation controls.

The Modules and Licenses section allows you to activate or deactivate features available on the computer. These settings should match the installed hardware, available licenses, and actual usage of the installation.

Module	That enables	When should it be active
API	It allows the use of integrations or external calls to team functions.	Activate only if the installation uses documented API integration.
Modbus	Enables communication with Modbus compatible systems.	Use On if the equipment is part of an industrial or control integration that requires it.
Video	Activate camera-related functions, preview, video call, or video services.	It must be active when the equipment has a camera or the installation uses video.
RFID	Enables RFID reader and card functions.	Activate only on devices with an installed RFID reader and configured card access.
RS485	Enables communication via RS485 bus.	Use On when there is an RS485 connection in the installation.
QR	Enables access functions via QR code.	It must be active if QR codes are to be generated and read.
SNMP	Enables SNMP monitoring functions.	Activate only if the client has an SNMP platform and it is configured in Connectivity.

> **Important.**If a function is not used, it should remain deactivated. Before handing over the installation, verify that only the necessary modules remain active and that each active function has been tested.

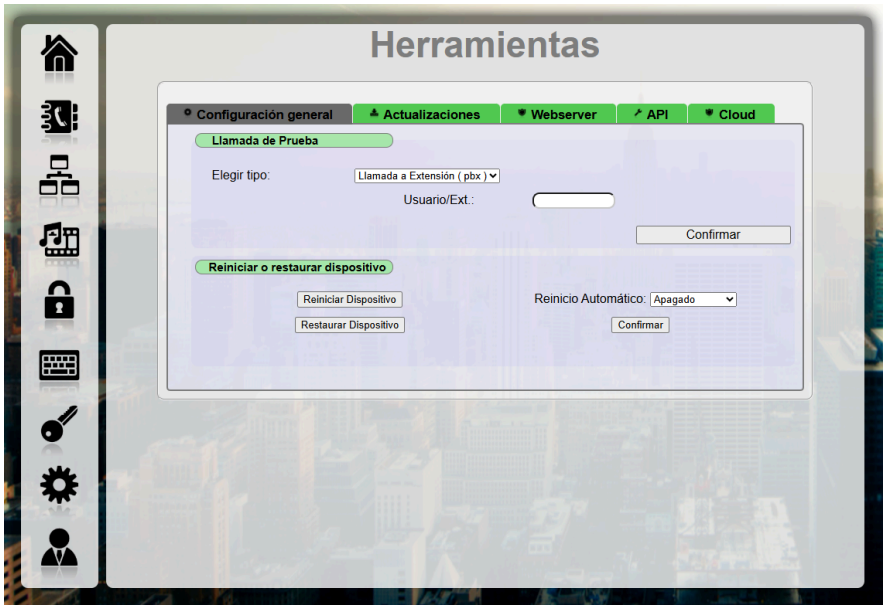
10. Tools

The Tools section of the examined 6.0 device includes test call, reboot, firmware updates, web server, API, and Cloud settings. These are sensitive settings because they can affect remote access, communication, or the overall operation of the device.

Testing and restarting	Maintenance	Access and integration

It allows you to launch test calls, restart the equipment, and schedule automatic restarts.	Check firmware version, update server, and manual update.	Control HTTPS, web port, API and Cloud.

10.1 General configuration



General device tools. Restarting or restoring affects operation and settings.

Field / action	Options / value	Correct use
Test call	It allows you to initiate a call from the device to check communication.	Use this test after configuring SIP, network, or call destinations.
Choose type	■ Call to Extension (PBX) ☐ Direct IP call	PBX calls a PBX extension. Direct to IP also displays the IP field and is used for point-to-point calls.
User / Ext.	Extension, SIP user, or test destination.	It must exist on the PBX or at the specified IP destination.
Restart Device	Restart the computer while keeping the settings.	Useful after changes that require a restart or to recover a blocked service.
Restore Device	Restore factory settings.	Critical action: Deletes settings. Use only with authorization and after backing up necessary data.
Automatic Restart	■ Off ☐ Every 12 hours. ☐ Daily ☐ Weekly ☐ Monthly	Schedule restarts only if the installation requires it. It can remain off during normal use.
Off	It does not schedule automatic restarts.	Recommended option if there is no specific need for preventative maintenance.
Every 12 hours.	Restart your computer twice a day.	Use only in facilities where this policy has been expressly defined.
Daily	It performs an automatic restart every day.	It can be used in facilities with scheduled maintenance.
Weekly / Monthly	Reduce the frequency of automatic restarts.	Select the frequency indicated by the technical manager.

10.2 Updates

Field	Which indicates	Correct use
Current version	Firmware installed on the device. The device examined shows "CSIP H6 — V 6.0"; 6.0 is the firmware version, not the processor version.	It is used to identify the version before support, maintenance, or updates.
State	Indicates whether the firmware is up to date according to the configured server.	Please check this field before manually uploading firmware.
Server URL	Server from which the team checks for updates.	Do not change the URL unless instructed by support or the technical lead.
Manual update	Allows you to select a compatible firmware file.	Use only the correct files for the model and version. Maintain a stable power supply and network connection during the process.

Caution. An interrupted update may render the device inaccessible. Before updating, confirm the model, file version, stable power supply, and maintenance window.

10.3 Web Server

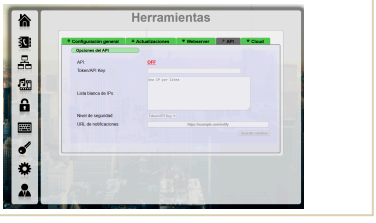
Field	Options / value	Correct use
HTTPS	☐ Activated ■ Deactivated	Enabled forces encrypted access if the installation supports it. Disabled maintains normal HTTP access.
Port	TCP port of the web server. On the examined computer it was listed as 8090.	If it changes, access will use the new address with that port. Example: http://IP:port/.
Save changes	Apply the web settings.	Before saving, confirm that you know the new IP address and port to avoid losing access to the panel.

10.4 API

CONFIGURATION REFERENCE

External integration via API

The examined 6.0 panel displays the API status, token/API key, IP whitelist, security level, and notification URL. The reference team's API was disabled; the behavior of all controls when enabled has not been verified.



Field	Options / value	Correct use
API	Indicates whether the API is active.	It depends on the corresponding module/license. If external integration is not used, it should remain disabled.
Token / API Key	Key that authorizes requests to the API.	Sensitive data. Do not share in screenshots, emails, or public documents.
IP whitelist	One IP address per line.	Limits which addresses can use the API. Recommended when the IP address of the external system is known.
Security level	■ Token/API Key ☐ IP ☐ Token + IP	Token + IP is the most restrictive option when integration allows it.

Token/API Key	The request must include the configured key.	Useful when you cannot limit by IP or when the IP of the external system changes.
IP	Authorization is based on the IP address included in the whitelist.	Use only if the authorized IPs are static and known.
Token + IP	It requires a valid key and a source included in the whitelist.	It is the safest option when the external system has a static IP address.
Notification URL	External address that will receive notices or events.	It must be a valid URL and maintained by the receiving system.

Security. The API should only be active if a documented integration exists. Protect the token, limit IPs where possible, and test the integration before deploying the installation.

10.5 Cloud

CONFIGURATION REFERENCE

Remote access from the Cloud

The Cloud tab displays the service status, a link to cloud.panphone.es, and the "Cloud Services Usage" option. The "Connected" status in the screenshot only applies to that device; please check the status of your own device.



Element	What it shows	Correct use
State	Service connection indicator.	Check the status on the device itself; do not assume the connection is operational simply because the tab is present.
Use of cloud services	Activation box and "Save changes" button.	Enable it only if the facility has the service and authorization for remote access.
cloud.panphone.es	Link displayed by the panel.	Access to the portal may require an account or separate permissions from the computer.

Scope. The panel displays a Cloud option under Tools and another "Use Cloud" option under Relays' advanced settings. It hasn't been verified whether both share a service or internal configuration; review their purpose before enabling them.

Remote access. If the installation has cloud access, the board's control panel can be opened remotely. Access to the panel is granted using your own credentials; the individual recovery credentials for this board must be retained even if the daily password is changed. Accessing the cloud portal and accessing the board's control panel are separate processes.

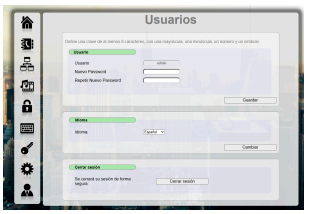
11. Users

The Users section allows you to change your web panel access password, select the interface language, and log out of the administration session. It is the last section of the sidebar settings panel.

CONFIGURATION REFERENCE

User, language and logout

This screen manages access to the web panel. The password must be kept secure and changed during setup if a default password or one known to multiple people is used.



Field / action	What should you put	Correct use

User	Current user of the web panel.	Identify the account used to manage the device.
New Password	New password to access the panel.	Panel 6.0 requires at least 8 characters, including one uppercase letter, one lowercase letter, one number, and one symbol. Store it in the authorized procedure.
Repeat New Password	Repeat the new password.	It must exactly match the previous field to avoid errors when saving.
Keep	Save the password change.	After saving, document the new key in the authorized internal procedure, not in the customer manual.
Language	☐ English ☐ Portuguese ■ Spanish ☐ Basque ☐ Catalan	Change the web interface language. This setting does not necessarily change the audio prompt language, which is configured in Multimedia.
Change	Apply the selected language.	Use the language required by the installer or maintenance manager.
Log out	Securely log out of the admin session.	It should be used at the end of the setup, especially on shared equipment or client networks.

Delivery. Do not include real passwords in screenshots, reports, or submitted documentation. After setup is complete, log out and verify that access is secure.

11.1 System Date and Time

The board includes a dedicated date and time setting screen. This setting is important because it affects access times, event logs, time codes, and maintenance checks.

Field / action	What should you put	Correct use
System date and time	Displays the current date and time on the license plate.	It should be reviewed before activating schedules, records, or temporary access.
Date type	■ Automatic ☐ Manual	Automatic synchronization with NTP server. Manual allows entering date and time from the panel.
Automatic	The license plate gets its time from an NTP server.	Recommended when the computer has a network connection to the configured server.
Manual	The installer sets the date and time directly.	Use this mode if there is no NTP access or during an isolated startup.
NTP Server	Time server, for example es.pool.ntp.org.	It must be accessible from the network configured on the board.
Time zone	Installation time zone.	For mainland Spain, select Europe/ Madrid.
Manual date/time	Date and time entered by the installer.	This only applies when the date type is set to Manual.
Keep	Apply the time setting.	After saving, check that the time is correct in the Start menu and in the logs.

Revision. If events appear with incorrect times or access times do not act when they should, first check time zone, date mode, and NTP server.

12. OPTO Additional Board

The OPTO add-on board is an optional accessory for installations requiring auxiliary inputs and an additional relay output. This section only applies when the OPTO board is physically installed in the equipment.

Tickets 1-4

They allow wiring external contact signals.

Feeding of inputs

It is possible to work with internal or external power supply according to JP1 and JP2.

Relay 3

It provides an additional output with voltage-free contacts.

12.1 Identification of terminals and jumpers

Terminal / element	Indicated function	Correct use
1 to 4	Entrance 1, Entrance 2, Entrance 3 and Entrance 4.	Connect here the external contacts that need to be detected by the board.
5	GND.	Ground reference for the input wiring according to the scheme used.
6	+ V.	Positive reference for input feed.
7 and 8	Relay contacts 3.	Voltage-free output for the additional operation defined in the installation.
JP1 and JP2	Feed selection bridges.	Connected: internal power. Disconnected: external power.
Bridge NO/NC	Relay output selection as normally open or normally closed.	It must be adjusted to the type of lock, barrier or automation connected.

12.2 Input Power Supply

The OPTO board supports two ways to power the inputs. The choice depends on the type of signal available in the installation and must comply with the board's connection diagrams.

Mode	Status of JP1 and JP2	Recommended diet
Internal feeding	JP1 and JP2 connected.	5 V (+V). Confirm this mode with the schematic of the supplied board.
External power supply	JP1 and JP2 disconnected.	5-24 V and GND. Confirm this mode with the schematic of the supplied board.

> **Caution.**Do not mix internal and external power supplies in the same configuration without verifying the electrical schematic. Jumpers and terminals should not be manipulated while the equipment is powered on.

12.3 OPTO wiring check

Before proceeding with the equipment configuration, verify that the OPTO board's physical wiring matches the installation diagram. This step does not replace the auxiliary input configuration in the Keyboard/Pushbutton section; it only confirms that the add-on board is correctly connected.

Testing	What you should check	Expected result
Tickets 1-4	Each external contact must be connected to the designated input terminal.	The physical entrance matches the installation layout.
GND and +V	The power supply reference must correspond to the selected mode.	There is no mixing of internal and external feeding.

JP1 and JP2	Check if they are connected or disconnected according to the scheme used.	JP1/JP2 connected for internal power; disconnected for external power.
Relay 3	Terminals 7 and 8 should only be connected to the intended operation.	Relay 3 is not used if it is not wired and documented.
NO/NC	Check the position of the relay output jumper.	The contact remains normally open or normally closed depending on the lock or automation system.

12.4 OPTO Functional Test

1. Verify that the OPTO board is installed and that the equipment is de-energized before handling it.
2. Check if JP1 and JP2 should be connected or disconnected depending on the chosen power supply mode.
3. Verify that each physical input corresponds to the function intended in the project.
4. Test each entry individually and confirm that it calls the correct destination or activates the intended maneuver.
5. Test relay 3 only if it is wired and part of the installation.

> **Delivery to the customer.**Document which OPTO input has been used, which physical contact activates it, whether it works with internal or external power, and which relay or destination is associated with it.

13. Mounting accessories

This section contains dimensional references for assembly for the indicated series. The dimensions should be used as an installation guide and physically verified before drilling, machining, or preparing the recess for embedding.

C Series

Reference for gray rear cover.

Series 4 surface

Back cover reference for surface mounting.

Series 4 recessed

Frame reference for recessed installation.

13.1 C-Series, gray rear

13.2 Surface Series 4

13.3 Series 4 for recessed mounting

> **Before installing.**Always check the supplied physical model, the type of enclosure, the front panel orientation, and the cable routing. Do not drill or machine anything until you have confirmed that the dimensions match the installed accessory.

14. Technical data

This section contains the technical specifications of the PANPHONE IP CSIP V6. The base corresponds to the technical characteristics of the CSIP V6 board; the software functions were compared with the screens of the examined firmware 6.0.

> **Model and version.**CSIP V6 identifies the device family; "CSIP H6 — V 6.0" is the string displayed on the examined panel. In this manual, 6.0 refers to the firmware. The string alone does not confirm the processor model or the physical board revision.

14.1 Communication and pushbuttons

Feature	Technical data	Observation
Communication protocol	SIP 2.0 in accordance with RFC 3261.	It allows you to register the device on an IP PBX or make direct calls via IP depending on the configuration.

Buttons / keyboard	A call key or 12-key keypad: 0-9, # and *.	It depends on the front panel installed. Configuration is done in the Keypad/Pushbutton section.

14.2 Audio

Feature	Technical data	Observation
Microphone	1 electret.	Sensitivity is adjusted from Multimedia > Audio.
Speaker	2 W, 8 ohms.	The volume is adjusted from Multimedia > Audio.
Audio improvements	Echo cancellation and ambient noise reduction.	It helps improve hands-free conversation in noisy environments.
Audio mode	Full duplex.	It allows you to speak and listen simultaneously during communication.
Sound pressure	77.5 dB at 1 kHz / 1 m.	Speaker reference value.
Audio codecs	G.711a/u, G.722, G.726-32, G.729, GSM and OPUS.	Codec priority is configured in each SIP account.

14.3 Electrical properties, consumption and network

Feature	Technical data	Observation
External power supply	12 Vdc +/- 15%, 2 A.	Recommended power supply for continuous use.
PoE Power Supply	IEEE 802.3af PoE (Class 0, 12.95W max).	It allows you to power the equipment directly through the RJ45 network cable.
Standby power consumption	100 mA (~1.2 W at 12 Vdc).	Equipment on standby, registered and in service.
Call usage	Maximum 350 mA (~4.2 W at 12 Vdc).	During active conversation with standard speakerphone.
Power consumption with amplifier: 10 W	Up to 1 A (~12 W peak at 12 Vdc).	In versions equipped with a 10W amplifier stage at maximum volume.
LAN interface	RJ45, 10/100 Base-TX with Auto MDI-X.	Direct connection to local Ethernet network.
Relay contacts	2 NC/NO relays, max. 24 V / 2 A DC, 120 V / 2 A AC.	Voltage-free. Optional third relay via OPTO board.

14.4 Supported Protocols

Protocol / service	Availability	Use
SIP 2.0	Supported.	SIP registration and calls.
UDP / TCP	Supported.	Communications transport according to configuration.
RTSP	Supported on devices with video.	Camera streaming with username, password, and port.
HTTP / HTTPS	Internal web server; HTTPS configurable in Webserver.	Authorized local or remote access to the configuration panel.
MODBUS	Available as a module/license.	Integration with external systems or SCADA.
RS485	Available as a module/license.	Serial communication in compatible installations.
SNMP	Available as a module/license.	Supervision and sending of traps.
DHCP	Supported.	Automatic IP assignment.
NTP	Supported.	Automatic date and time synchronization.

14.5 Dimensions and mechanical characteristics

Element / Characteristic	Dimensions / Data	Observation
Surface Dimensions Series 4	**185 x 105 x 31 mm**	Wall mount with included back cover.
Dimensions Series 4 for recessed mounting	**216 x 128 x 8 mm**(Front) Recessed opening:**182 x 92 x 30 mm**	Recessed wall installation with recessed box or frame.
Dimensions C Series (Front)	**175 x 100 x 30 mm**approx.	Front format for mounting on columns or specific supports.
CSBOX format dimensions	**125 x 93 x 52 (or 42) mm**	Closed box made of plastic or aluminum.
Plate dimensions CSIP electronics	**100 x 85 mm**	Motherboard dimensions without enclosure.
OPTO auxiliary board dimensions	**42 x 42 mm**	Optional expansion card.
Temperature of operation	-10°C to +55°C.	Suitable for indoor and outdoor installations depending on the enclosure.
Relative humidity	10% to 95%, non-condensing.	Acceptable environmental range.

14.6 Special features

Feature	Availability	Observation
Remote opening by dialing code	Yeah.	It allows you to open from an authorized external extension or phone.
Voice messages	Yeah.	Messages such as "door open" or "making call" can be customized and configured in different languages.
Integrated relays	2 independent relays.	Voltage-free contacts configurable as NC or NO.
Input for push button or external sensor	1.	Available input on the motherboard depending on the model and cabling.
Wiegand Mifare Port	1.	For compatible proximity or biometric sensors.
LED Indicators	1.	Indication of waiting, call and communication according to configuration.
OPTO Expansion Card	Optionally available.	Add 4 auxiliary inputs and an output relay.
DHCP Automatic IP Assignment	Yeah.	Configurable from Connectivity.
Traffic log control	Yeah.	It allows you to review records from the panel.
Local and remote configuration via web	Yeah.	Access via the computer's internal web server.
SIP call I/O event notification	Yeah.	It allows SIP call notifications based on inputs and configuration.
Integration via API	Optionally available.	The examined 6.0 panel displays API status, token, IP whitelist, security level, and notification URL.
MODBUS protocol	Yeah.	Oriented towards integration with SCADA or external systems.

RTSP Streaming	Yes, on devices with video.	Configurable with username, password, and port. The interface indicates that it is unavailable while the QR reader is active.