Manual v1.3 Date 02/03/2026

User Manual

Audio Compact
Audio Pro (1/2/4/Keypad)
Audio Pro Classic (1/2/4/Keypad)
Video Compact
Video Pro (1/2/4/Keypad)
Video Pro Classic (1/2/4/Keypad)
Proline
Touch

PoE Injector
Button Extender

BOUT THIS MANUAL

Thank you for choosing a Robin intercom system.

Robin intercom solutions are designed for environments where performance, reliability, and refined aesthetics are essential. Combining precision-engineered hardware with advanced IP technology, Robin systems deliver exceptional audio clarity, optional high-definition video, and seamless interoperability with modern telephony, SIP, and access control infrastructures. Every product is developed with a focus on durability, security, and long-term operational stability, making it suitable for demanding residential, commercial, healthcare, and industrial environments.

Robin intercoms are built to integrate effortlessly into professional network environments. Whether deployed as a standalone access point or as part of a larger communication and security ecosystem, the system is designed to provide consistent performance and intuitive operation. High-grade materials, robust construction, and carefully optimized firmware ensure that the device performs reliably under continuous use.

This manual provides detailed information for the installation, configuration, integration, and daily operation of your Robin intercom system. It is intended for professional installers, system integrators, IT administrators, and advanced users who require a structured and technically accurate reference to achieve a correct and efficient setup.

The documentation guides you through network configuration, telephony setup, event management, integration with third-party systems, and advanced automation features. Clear explanations and configuration examples are provided to support both standard installations and more complex integration scenarios.

Before installing or operating the device, please read this manual carefully. Following the recommended procedures and configuration guidelines will help ensure safe operation, optimal performance, and long-term reliability. Proper installation and configuration are essential to fully benefit from the system’s advanced capabilities.

For additional technical documentation, firmware updates, integration notes, or support, please consult the official support resources or contact your authorized distributor.

This manual applies to the following product ranges:

- Audio-only: Audio Compact, Audio Pro, Audio Pro Classic
- Video: Video Compact, Video Pro, Video Pro Classic, Proline, Touch
- Smart devices: Doorbell

PRODUCT INFORMATION, TRAINING AND SUPPORT

Robin Telecom Development BV
Flemingstraat 50
1704 SL Heerhugowaard
The Netherlands
info@robintele.com
support@robintele.com
+31 72 534 64 26

AMERICAS

CDVI Americas
828 St-Martin Blvd West
H7M 0A7 Laval, Quebec
Canada
+1 450 490 7945
+1 866 610 0102
support@cdvi.ca

EUROPE

CDVI Benelux
Otegemstraat 241
8550 ZWEVEGEM, Belgium
+32 56 73 93 00
+31 85 00 22 359
support@cdvibenelux.com

CDVI France
31, Avenue du Général Leclerc
93500 PANTIN, France
+33 1 48 91 01 02
technique@cdvi.com

CDVI Germany
Dahlweg 105 / Tor 2
D-48153 Münster, Deutschland
+49 251 798 477 0
technik@cdvi.de

CDVI Iberica
C. Electricitat 12
08755 Castellbisbal, Barcelona, España
+34 935 39 09 66
info@cdviberia.com

CDVI Italy
Via I° Maggio n° 9/11
28040 Borgo Ticino (NO) Italia
+39 0321 90 57 3
technico@cdvi.it

CDVI Nordic AB
Datavägen 12 b,
436 32 Askim (Göteborg), Sverige
+46 31 760 19 30
support@cdvi.se

CDVI Poland
Św. Jacka Odrowąża 15
03-310 Warszawa, Polska
+48 12 659 23 44
info@cdvi.com.pl

CDVI Suisse
Chemin du Croset 7
1024 Ecublens, Suisse
+41 21 882 18 41
info@cdvi.ch

CDVI UK
Unit B1, Knaves Beech Business Centre Davies Way
HP10 9QR Loudwater, Buckinghamshire
United Kingdom
+44 1628 531 300
+353 1 800 939 590
+27 800 014 506
technical@cdvi.co.uk

ASIA-PACIFIC (APAC), MIDDLE EAST & AFRICA (MEA)

CDVI Export
31, Avenue du Général Leclerc
93500 PANTIN, France
+33 1 48 91 01 02
export@cdvi.com

WARRANTY AND RETURNS

CDVI products are covered by a five (5) year limited warranty commencing from the date of manufacture (MFC), as determined by the product label, serial number, or other manufacturer identification, and not from the date of purchase, delivery, or installation. This warranty applies solely to defects in materials and workmanship under normal use and service conditions and is subject to proper installation, operation, and maintenance in accordance with CDVI's published guidelines. The warranty does not extend the coverage period beyond five years from the manufacturing date and may be subject to additional terms, conditions, limitations, and exclusions as defined by CDVI.

In the event of a warranty claim, CDVI shall, at its sole discretion, repair or replace the defective product, or provide an equivalent product, provided the product is returned in accordance with CDVI's Return Material Authorization (RMA) procedures. An RMA number must be obtained from CDVI prior to any return, and products returned without a valid RMA may be refused and returned at the sender's expense. All returned products must be properly packaged, clearly identified with the RMA number, and shipped in accordance with CDVI's instructions. Repaired or replacement products shall not extend or renew the original warranty period, which shall remain calculated from the original date of manufacture.

For service, repair, or warranty support, end users must contact the installer who performed the original installation. Products must not be returned directly by end users to CDVI. The installer is responsible for coordinating the return process and, depending on the applicable distribution model, may be required to return the product to the authorized distributor. Where applicable, the distributor must return the product to the CDVI branch from which the product was originally purchased. If the original installer is no longer active or available, end users may contact the relevant CDVI commercial branch, which will provide guidance and, where possible, direct them to an alternative installer or an authorized distributor capable of handling the repair. All returns are subject to CDVI's Return Material Authorization (RMA) procedures and applicable regional policies.

Robin devices that do not use CDVI product naming may be returned directly if found to be defective, in accordance with the applicable Robin return and service procedures. These products are not subject to the standard CDVI return process described above. In such cases, the products are subject to the warranty period defined by Robin for the specific product concerned. For further information or assistance, users may contact Robin using the contact number stated on the previous page.

TRADEMARKS AND COMPATIBILITY

Robin and related product names are trade names and/or trademarks used by Robin Telecom Development B.V.

CDVI and related product names are trademarks and/or registered trademarks of the CDVI Group (and/or its affiliates), depending on the jurisdiction.

Apple®, Apple TV®, HomePod®, iPhone®, iPad®, Apple Watch®, Siri®, Apple Home™, and Apple HomeKit® are trademarks of Apple Inc., registered in the United States and other countries and regions. This product is certified and approved for use with Apple HomeKit®. References to Apple products, services, or technologies are made solely for informational and compatibility purposes and do not imply any affiliation, sponsorship, or endorsement by Apple Inc., except where such certification is explicitly stated.

Matter® is a registered trademark of the Connectivity Standards Alliance. References to Matter® apply solely to compatible third-party accessories and do not indicate that this product itself is Matter-certified.

WebRelay™ and related product names are trademarks or registered trademarks of ControlByWeb. References to WebRelay-Quad are provided for informational and compatibility purposes only and do not imply any affiliation, sponsorship, or endorsement by ControlByWeb.

CyberGate™ and related product names are trademarks or registered trademarks of CyberTwice. References to CyberGate are provided solely for informational and compatibility purposes and do not imply any affiliation, sponsorship, or endorsement by CyberTwice.

Microsoft®, Microsoft 365®, Office 365®, and Microsoft Teams® are trademarks or registered trademarks of Microsoft Corporation. References to these products are made solely for informational and compatibility purposes.

IQ Messenger and related product names are trademarks and/or trade names of IQ Messenger B.V. (and/or its affiliates). References to IQ Messenger are provided solely for informational and compatibility purposes.

MQTT is a trademark of OASIS Open. References to MQTT are made solely to describe supported communication protocols and do not imply any affiliation, sponsorship, or endorsement by OASIS Open.

All trademarks and registered trademarks are the property of their respective owners. Use of third-party names is solely for the purpose of identifying compatibility and does not imply any affiliation, sponsorship, endorsement, or certification unless explicitly stated.

IMPORTANT SAFETY INFORMATION

The Robin intercom is intended for professional installation in fixed installations. Installation, connection and configuration shall be carried out by qualified personnel with appropriate knowledge of IP networks, Power over Ethernet (PoE) systems and low-voltage control circuits.

The device shall be powered exclusively via Power over Ethernet (PoE) compliant with IEEE 802.3af. Only PoE-compliant network switches or PoE injectors shall be used. The Ethernet interface is classified as a SELV circuit. No external voltages shall be applied to the Ethernet connector. Ethernet and PoE connections are limited to a maximum cable length of 100 metres per cable segment between two active network devices, as defined by the Ethernet standard. Depending on cable quality, installation conditions and power demand, reliable operation may require shorter cable lengths.

The built-in relay output provides a potential-free (dry) contact intended for controlling external equipment. The relay output is intended for SELV circuits only. The maximum permissible relay load is 24 V AC/DC at 0.75 A. Connection to mains voltage or hazardous energy sources is not permitted. External circuits connected to the relay output shall comply with applicable electrical safety standards and local regulations.

The device shall be installed using the supplied or officially approved mounting accessories to ensure mechanical stability, environmental protection and adequate thermal performance. Wall mounting, flush mounting or in-wall installation without approved accessories is considered a non-standard installation. Any damage or malfunction resulting from non-standard installation methods or the use of non-approved accessories is outside the scope of the warranty.

The device is designed for operation within a local area network (LAN). Direct exposure to public networks, including the use of port forwarding, is strongly discouraged. Default credentials shall be changed immediately after installation and strong passwords with a minimum length of 12 characters shall be used. The connected PBX or VoIP system shall be configured to restrict outgoing calls to authorised destinations only. Firmware updates shall be installed to maintain security and compliance.

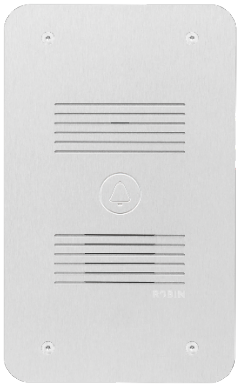
The installer is responsible for ensuring that the complete installation, including connected external equipment, complies with EN 62368-1, applicable national and local regulations, and the intended use described in this documentation.

CONTENTS

INTRODUCTION

ROBIN INTERCOMS

This manual applies to the following models:



Audio Compact

Video Compact

Audio Pro (Classic)

Video Pro (Classic)

Proline / Doorbell

Touch

FEATURES

CORE CAPABILITIES

Robin intercom systems are engineered as professional-grade communication and access control endpoints. Each device combines premium materials, enterprise networking standards, and advanced automation capabilities in a single integrated platform.

Designed for demanding residential, commercial, healthcare and industrial environments, Robin devices offer long-term operational stability and seamless integration into modern IP infrastructures.

DESIGN AND BUILD QUALITY

- Precision-machined aluminium and brass front panels
- Recessed security screws
- Optional ambient illumination
- Flush and surface mounting options
- Weather-resistant construction
- Five-year limited warranty

PROFESSIONAL TELEPHONY ARCHITECTURE

- Full SIP compliance (UDP, TCP, TLS 1.2)
- Secure RTP (SRTP) support
- Up to four simultaneous SIP registrations
- Direct Peer-to-Peer (P2P) capability
- Microsoft Teams integration (via CyberGate)
- Advanced call routing and scheduling

This ensures flexible deployment in small standalone installations as well as large enterprise PBX environments.

ADVANCED ACCESS CONTROL INTEGRATION

- Built-in dry contact relay (24V AC/DC – 0.75A)
- DTMF-controlled door release
- External WEBRelay compatibility
- Request-to-Exit (REX) input
- Event-based relay activation
- Schedule-based access logic

The system integrates easily with existing access control infrastructures and external IP relay modules.

EVENT-DRIVEN AUTOMATION ENGINE

Robin devices include a powerful event management system supporting:

- HTTP triggers
- MQTT publishing
- Audio detection
- Motion detection
- Time-based scheduling
- External system integration

This enables integration with building management systems, VMS platforms, automation systems, and third-party controllers.

ENTERPRISE VIDEO AND SURVEILLANCE SUPPORT

- Full HD video with HDR
- RTSP streaming (H.264)
- MJPEG compatibility
- Video Management System (VMS) integration
- Motion detection zones
- Configurable bitrate and stream control

The device functions as both intercom and IP security camera within a single network endpoint.

SECURE NETWORK INTEGRATION

- IEEE 802.3af PoE (Mode A)
- HTTPS support
- Certificate management
- Static IP or DHCP
- VLAN compatible
- Configurable HTTP/HTTPS ports
- Secure authentication policies

Designed for integration into professional IT environments with high security requirements.

OPEN INTEGRATION AND API SUPPORT

- REST API
- HTTP event sources and actions
- MQTT publishing
- Third-party relay control
- Flexible automation scenarios

This ensures compatibility with modern IP-based automation and monitoring platforms.

OPERATION

DAILY USE

In daily use, a Robin intercom becomes a seamless part of the building environment. It is not experienced as a technical device, but as a natural extension of communication and access control within the property.

When a visitor arrives and presses the call button, the interaction feels immediate and intuitive. The call is routed according to the configured logic, whether to a desk phone, a mobile device, or a Microsoft Teams user. Clear audio and high quality video allow the recipient to assess the situation with confidence before granting access. The process is simple for the end user, yet carefully managed by secure communication protocols in the background.

Throughout the day, the intercom remains continuously available. It does not only react to calls, but can also respond to motion, sound, schedules, or external system triggers. In this way, the device participates actively in the wider building ecosystem. It can support automation flows, monitoring strategies, and access control decisions without requiring constant manual intervention. Because the system is built on open standards and professional network architecture, it integrates smoothly into both compact installations and complex enterprise infrastructures. It operates predictably, respects network policies, and supports secure access through encrypted communication and controlled authentication.

Over time, this results in a consistent and dependable user experience. Visitors experience clear communication. Users retain full control over access. Installers and administrators benefit from stable performance and structured integration.

In practice, the Robin intercom delivers refined communication, controlled security, and long term reliability as part of a professional building environment.

OPERATING THE INTERCOM

To initiate a call, the visitor presses the illuminated button on the intercom. The device immediately confirms the interaction with an acoustic signal and starts the configured call sequence.

Depending on the installation, the call may be routed to a desk phone, mobile client, Microsoft Teams user, or defined call group. The intercom manages this process automatically according to the configured logic and schedules. The illuminated feedback on the device confirms that the call has been registered. From that moment, the system handles the communication session through the defined network infrastructure, ensuring stable and secure transmission of audio and, when applicable, video.

The interaction is intuitive for the visitor and structured for the system.

ANSWERING A CALL

Incoming calls from the intercom are answered in the same way as any standard SIP or Teams call. Once the recipient answers, a live audio connection is established instantly. On video capable devices, the live camera image becomes available as soon as the call is accepted. This allows the recipient to visually verify the visitor before making any access decision.

Audio processing is optimized to provide clear speech reproduction with minimal background interference. This ensures reliable communication, even in environments with varying acoustic conditions.

The user experience remains simple and familiar, while the intercom ensures controlled and secure session management in the background.

CONTROLLING THE INTEGRATED RELAY

During an active call, authorized users can activate the integrated relay using the predefined control sequence configured in the system.

The relay provides a potential free contact suitable for controlling electric strikes, gates, barriers, or external control interfaces. When activated, the relay follows the configured timing parameters and automatically returns to its normal state. Access control decisions are therefore made consciously and remotely. The intercom does not grant access autonomously, but responds only to authorized interaction or configured automation logic.

For more advanced installations, the relay can be combined with schedules, event triggers, or external IP relay modules, allowing the intercom to function as part of a broader access control strategy.

This approach ensures both operational flexibility and controlled security in daily use.

WARNING

The relay is able to switch a maximum of 24V – 0.75A.

SMART HOME AND SMART OFFICE INTEGRATION

In modern environments, an intercom is no longer an isolated device. It forms part of a connected ecosystem that includes telephony platforms, automation systems, access control, and building management solutions.

Robin intercoms are designed to operate within such intelligent environments. Through open standards and configurable event logic, the device can interact with smart home and smart office systems using secure network communication. Whether integrated with Microsoft Teams, SIP based PBX systems, MQTT workflows, HTTP automation triggers, or external relay modules, the intercom becomes a flexible interface between visitor interaction and building intelligence.

This allows installations to evolve over time. The intercom can participate in automated workflows such as activating lighting scenes, notifying security personnel, triggering recording systems, or integrating with broader access control logic.

Rather than being limited to basic door communication, the device supports structured integration within connected residential and commercial environments.

SUSTAINABILITY AND MATERIAL INTEGRITY

Sustainability is no longer a secondary consideration in building technology. It is an essential part of responsible design and long term investment. Robin intercom systems are developed with this principle in mind, combining durable materials, efficient electronics, and extended product lifespan into a coherent whole.

The visible character of a Robin intercom is defined by its materials. Front panels are precision manufactured from high grade aluminium or brass. These metals are chosen not only for their refined appearance, but for their structural strength and resistance to environmental exposure. Aluminium offers excellent corrosion resistance and long term dimensional stability. Brass provides natural durability and develops a distinctive patina over time without compromising integrity. Both materials are fully recyclable at the end of their lifecycle.

By selecting solid metals instead of coated plastics or composite alternatives, the product maintains its mechanical strength and visual quality over many years of daily use. This reduces the likelihood of premature replacement and supports a longer service life within residential, commercial, and institutional environments.

Energy efficiency is integrated at system level. The intercom operates via IEEE 802.3af Power over Ethernet, eliminating the need for separate power adapters and reducing installation complexity. LED technology is used for button illumination, display backlighting, and ambient lighting functions. These light sources are designed for low power consumption and long operational lifespan, contributing to reduced energy demand over time.

The ambient lighting is carefully engineered to enhance visibility and architectural presence without excessive power usage. It provides functional illumination during visitor interaction while maintaining efficient operation throughout daily use.

Firmware architecture also contributes to sustainability. Through structured updates and open protocol compatibility, the system remains adaptable to evolving telephony platforms and network environments. This future oriented design approach helps extend the functional lifetime of the device beyond changing infrastructure standards.

Sustainability in this context is not a marketing label, but the result of deliberate engineering choices. Durable materials, efficient power design, open integration standards, and long term reliability together create a product that aligns with contemporary expectations of environmental responsibility and architectural quality.

For projects where performance, aesthetics, and environmental awareness must coexist, Robin intercom systems offer a balanced and responsible solution.

PRODUCT OVERVIEW

PRODUCT ALIASING

Since Robin Telecom Development became part of the CDVI Group in 2025, your Robin device may be listed under a different name than the one used in this guide. You can find the corresponding device names in the list below:

CDVI Name	*Robin Name*
Audio Compact	Compact Secure SIP 1 button
Video Compact	SmartView SIP HD 1 button
Audio Pro 1 (/2/4/Keypad)	PRO Secure SIP 1 (/2/4/Keypad)
Video Pro 1 (/2/4/Keypad)	PRO SIP SV 1 HD 1080p (or SV 2/4/Keypad)
Video Pro Classic 1 (/2/4/Keypad)	Proline Classic SV SIP 1 piezo (or 2/4/Keypad piezo)
Video Proline	Proline Ambient Light
Doorbell	ProLine HD

POWER-OVER-ETHERNET

All PoE devices manufactured by Robin operate exclusively using PoE Mode A in accordance with the IEEE 802.3af and IEEE 802.3at standards.

In PoE Mode A, power is supplied over pins 1–2 and 3–6 of the RJ45 connector. These are the same wire pairs used for data transmission. When connected to a standards-compliant IEEE 802.3af or IEEE 802.3at PoE switch or injector, power detection and negotiation are performed automatically and no manual configuration is required.

Caution must be taken when using passive PoE switches or injectors. Passive PoE equipment does not perform automatic detection and may supply voltage on different wire pairs (commonly pins 4–5 and 7–8, known as Mode B) or may provide non-standard voltage levels such as 24 V passive PoE. Connecting a Robin device to an incompatible passive PoE source can result in immediate malfunction and may cause permanent damage to the device.

Before connecting a Robin device to any passive PoE source, always verify that:

- Power is supplied on pins 1–2 and 3–6 (Mode A)
- The output voltage complies with IEEE 802.3af or IEEE 802.3at specifications
- The equipment is intended for use with standard IEEE-compliant Powered Devices (PD)

If there is any doubt about compatibility, do not connect the device. Use only a certified IEEE 802.3af or IEEE 802.3at PoE switch or injector. Installation should be carried out by qualified personnel familiar with PoE systems. Damage caused by incorrect power connections is not covered under warranty.

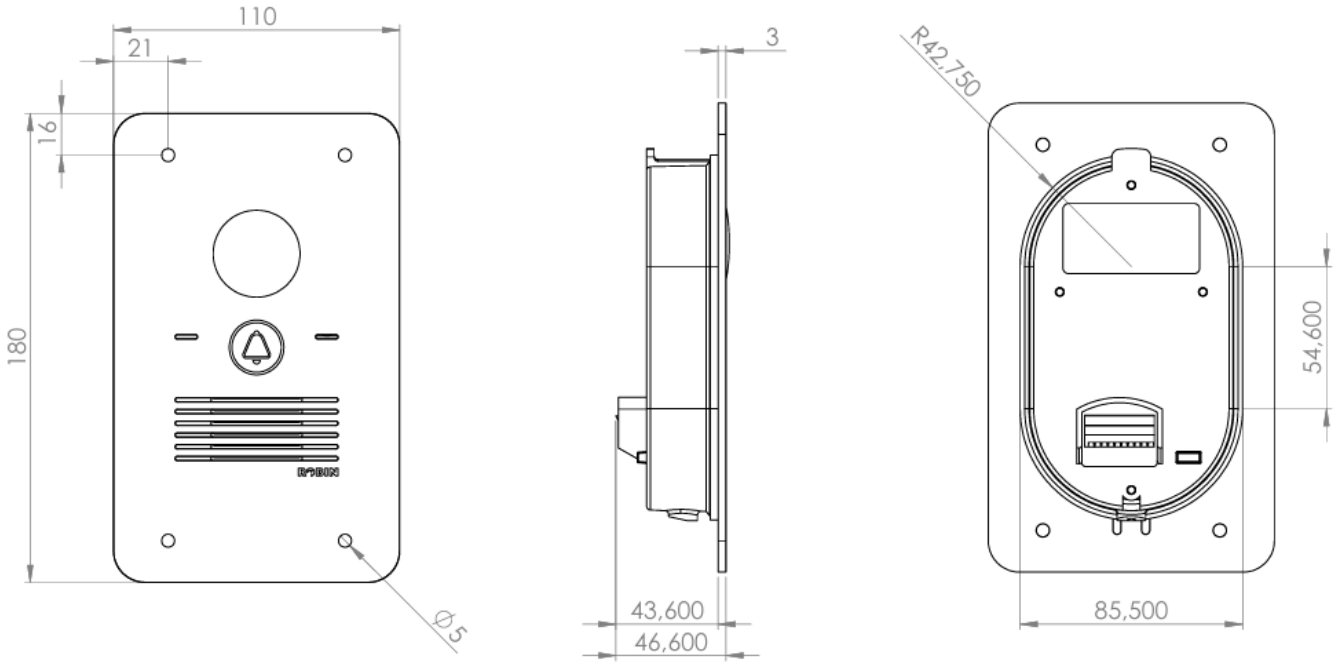
ROBIN COMPACT

PACKAGE CONTENTS

This package contains the following elements:

- Robin Compact
- Drilling template
- Mounting package (screws and plugs)

INSTALLATION DIMENSIONS



ACCESSORIES

Description	*CDVI Reference*	*Robin Reference*
WEBRelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Compact SB	F0408000018	C01100
Compact FB	F0408000019	C01110

PRODUCT REFERENCES

Description	*CDVI Reference*	*Robin Reference*
Robin Audio Compact	F0413000001	C91060
Robin Video Compact	F0414000001	C92050

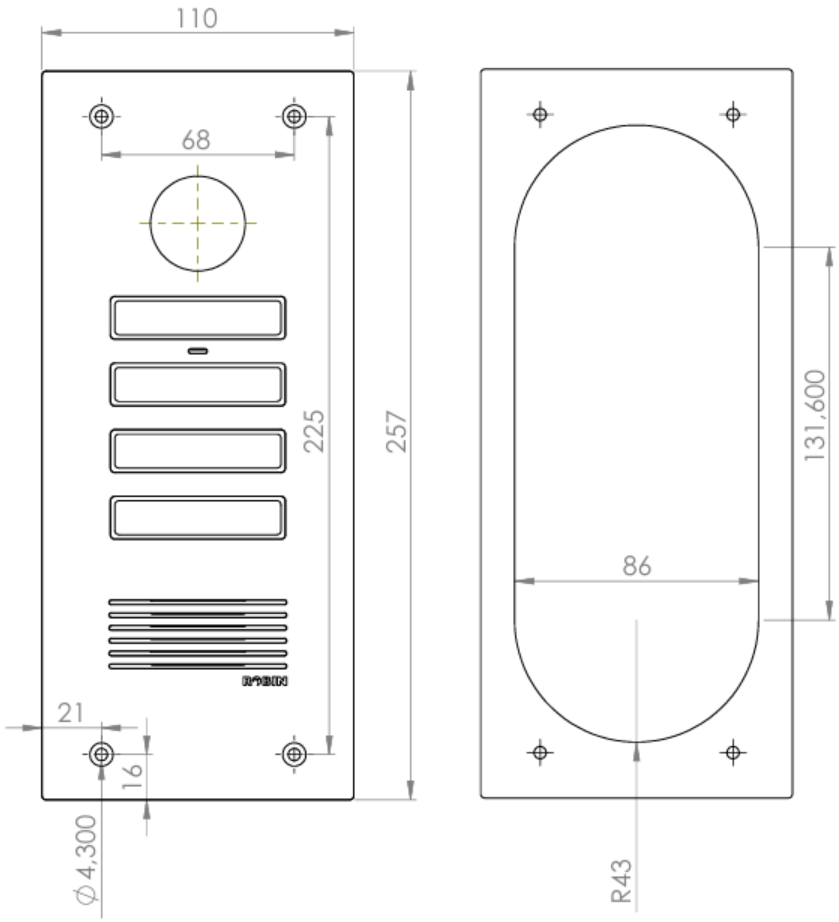
ROBIN PRO (CLASSIC)

PACKAGE CONTENTS

This package contains the following elements:

- Robin Pro or Pro Classic
- Drilling template
- Mounting package (screws and plugs)

INSTALLATION DIMENSIONS



ACCESSORIES

Description	*CDVI Reference*	*Robin Reference*
WEBRelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Pro SB	F0408000020	C03001
Pro FB	F0408000021	C01112

PRODUCT REFERENCES

Description	*CDVI Reference*	*Robin Reference*
Robin Audio Pro 1	F0413000002	C93065
Robin Audio Pro 2	F0413000003	C93066
Robin Audio Pro 4	F0413000004	C93067
Robin Audio Pro Keypad	F0413000005	
Robin Video Pro 1	F0414000005	C93050
Robin Video Pro 2	F0414000006	C93052
Robin Video Pro 4	F0414000007	C93054
Robin Video Pro Keypad	F0414000008	
Robin Video Pro Classic 1	F0414000009	C03071
Robin Video Pro Classic 2	F0414000010	C03072
Robin Video Pro Classic 4	F0414000011	C03074
Robin Video Pro Classic Keypad	F0414000012	

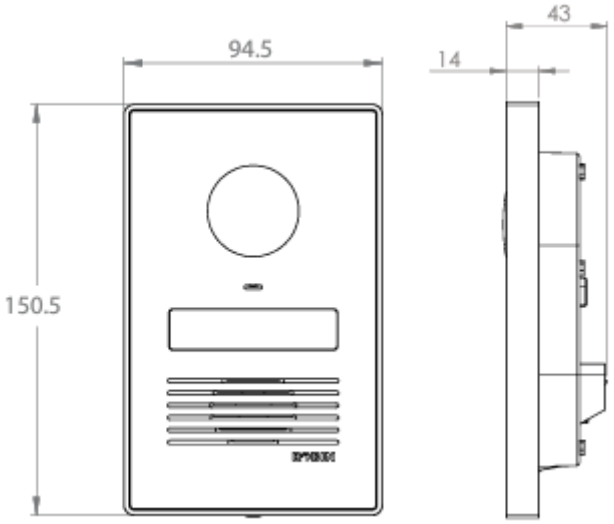
ROBIN PROLINE

PACKAGE CONTENTS

This package contains the following elements:

- Robin Proline
- Robin Proline Ambient frame
- Drilling template
- Mounting package (screws and plugs)

INSTALLATION DIMENSIONS



ACCESSORIES

Description	*CDVI Reference*	*Robin Reference*
WEBRelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Proline SB Black	F0408000024	A91523
Proline SB Gray	F0408000023	
Proline SB Silver	F0408000022	

PRODUCT REFERENCES

Description	*CDVI Reference*	*Robin Reference*
Robin Proline Black	F0414000004	A93027
Robin Proline Gray	F0414000003	A93025

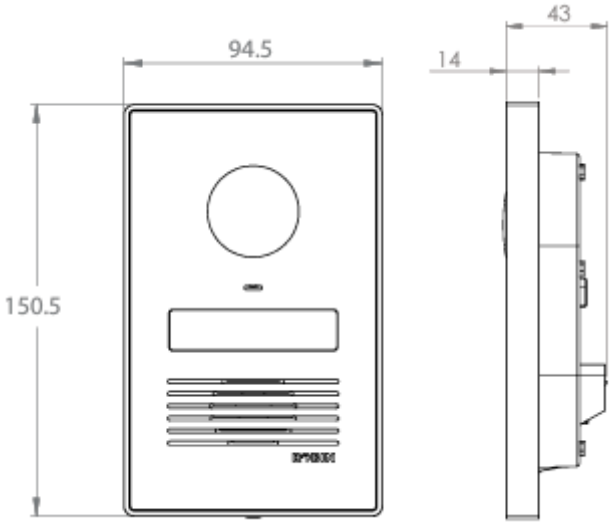
ROBIN DOORBELL

PACKAGE CONTENTS

When acquiring the Robin Doorbell, you will receive a full package having all the goods needed for a proper installation:

- Robin Doorbell
- Flush mount
- Robin PoE-injector
- 15m UTP-cable
- Mounting screws and installation screws

INSTALLATION DIMENSIONS



ACCESSORIES

This product is compatible with a classic external door chime (max. 24V 0.5A), and works with Matter®-compatible accessories or Apple HomeKit®.

PRODUCT REFERENCES

Description	*CDVI Reference*	*Robin Reference*
Robin Doorbell Black	F0415000002	NONE
Robin Doorbell Silver	F0415000001	
Robin Doorbell Bronze	F0415000004	
Robin Doorbell Space Gray	F0415000003	
Robin Doorbell Sunset Gold	F0415000005	

IMPORTANT NOTE

The integrated output is specifically designed for low-power door chime applications (max 24V / 0.5A). It is not intended for controlling electric strikes or access control hardware.

This product is not compatible with the WEBRelay Quad.

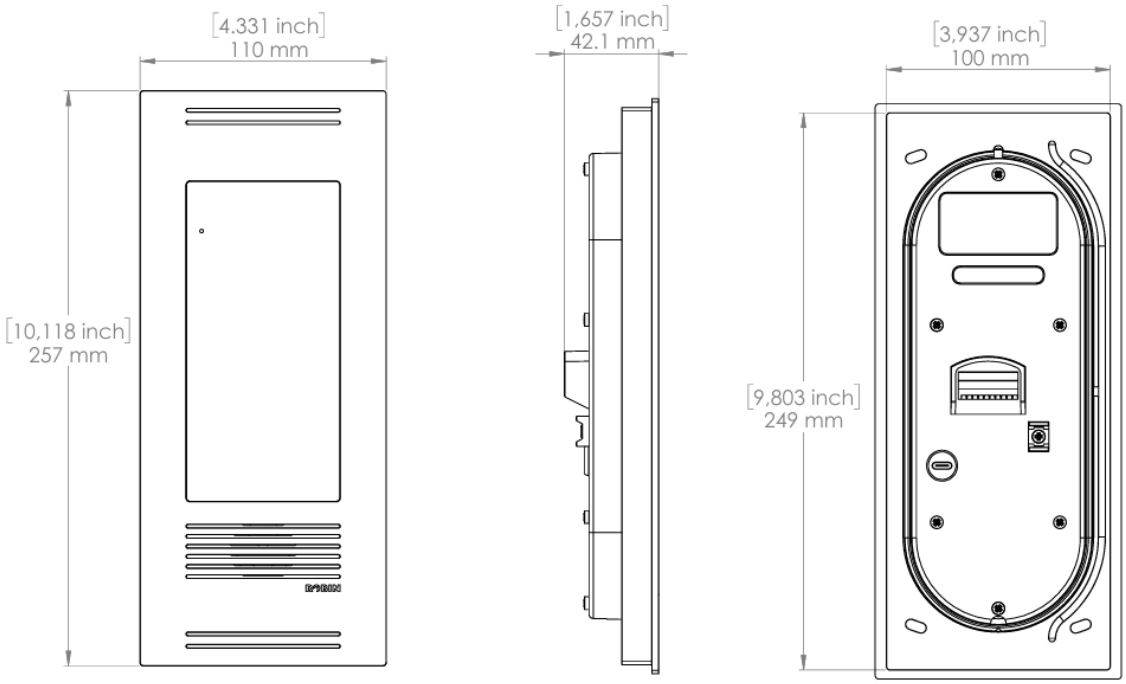
ROBIN TOUCH

PACKAGE CONTENTS

This package contains the following elements:

- Robin Touch
- Robin Touch Ambient frame
- Drilling template
- Mounting package (screws and plugs)

INSTALLATION DIMENSIONS



ACCESSORIES

Description	*CDVI Reference*	*Robin Reference*
WEBRelay	F0410000172	C01037
PoE Adapter	F0406000002	8061996
Touch SB	F0408000025	
Touch FB	F0408000026	

PRODUCT REFERENCES

Description	*CDVI Reference*	*Robin Reference*
Robin Touch Black	F0414000013	NONE

ROBIN POE-INJECTOR

PACKAGE CONTENTS

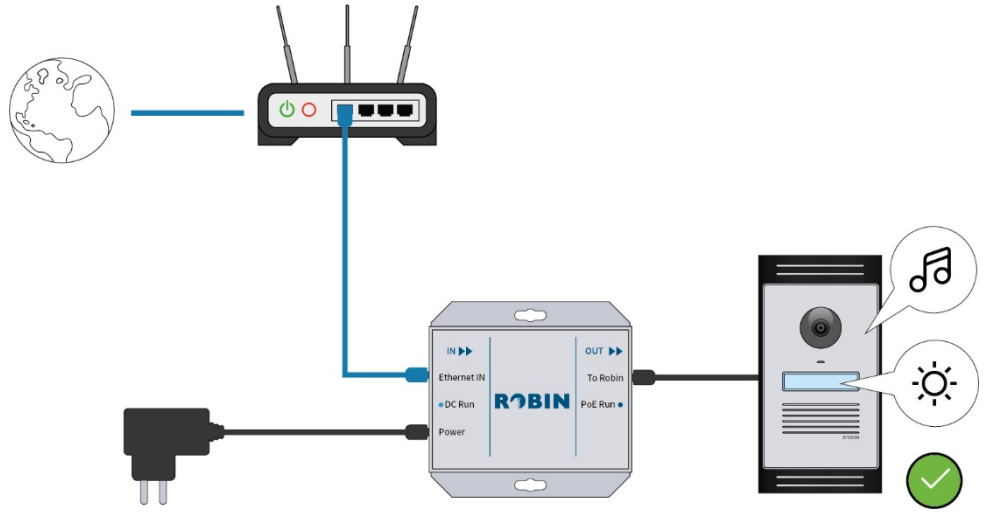
This package contains the following elements:

- The PoE-injector
- A 12VDC 1,5A (18W) power supply
- Socket conversion pack for international use

COMPATIBILITY

This accessory is compatible with all Robin intercoms.

INSTALLATION



To install the PoE-injector, connect the device to your Robin on the "to Robin" side. Connect the Ethernet IN to your switch or router and power supply to an outlet.

ROBIN BUTTON EXTENDER

PACKAGE CONTENTS

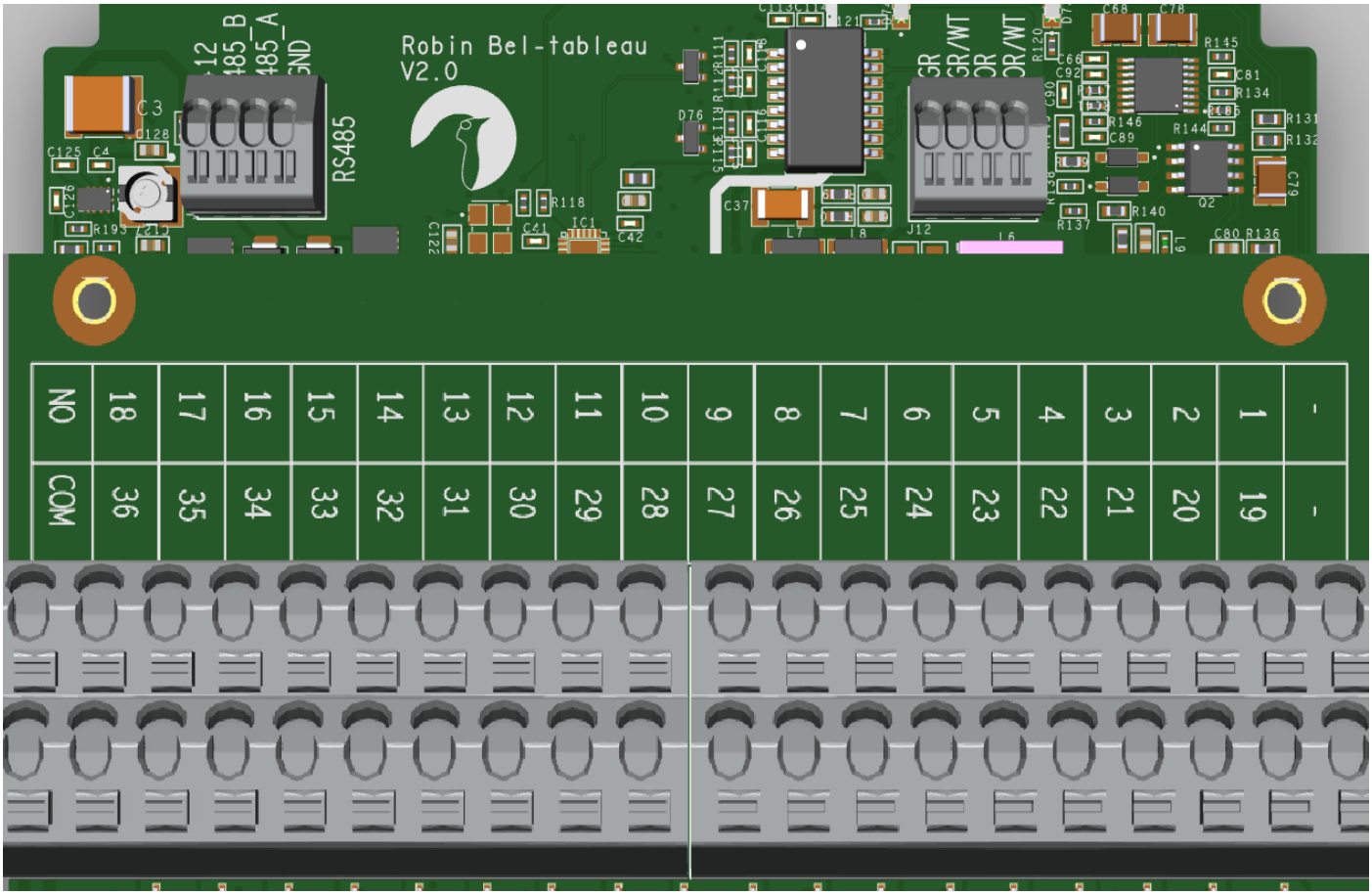
This package contains the following elements:

- Robin Button Extender
- Mounting package (screws and plugs)

COMPATIBILITY

This accessory is compatible with all SIP-supporting Robin intercoms.

INSTALLATION



To install the button extender:

- Connect the wires GR (Green), GR/WT (Green/White), OR (Orange) and OR/WT (Orange/White) from your network cable to the Button Extender, and connect the device in the same network range as your intercom.
- Connect each physical button with one wire to a numbered contact (1-36), and with the other wire to your COM-contact. (The buttons need to be NO)
- When triggering the respective numbered contact for the first time, it will automatically add a button to your web interface in "Telephony" (chapter Telephony → Button Settings)
- The extender is automatically detected within the same IP range. Refer to Telephony → Button Extender for configuration details.

TECHNICAL INSTALLATION

MOUNTING A ROBIN INTERCOM USING THE SURFACE MOUNT BOX

REFERENCES

Description	*Model(s)*	*CDVI Reference*	*Robin Reference*
Compact SB	Compact series	F0408000018	C01110
Pro SB	Pro (Classic) series	F0408000020	C03001
Proline SB Silver	Proline, Doorbell	F0408000022	-
Proline SB Grey	Proline, Doorbell	F0408000023	-
Proline SB Black	Proline, Doorbell	F0408000024	-
Touch SB	Touch		

INSTALLATION

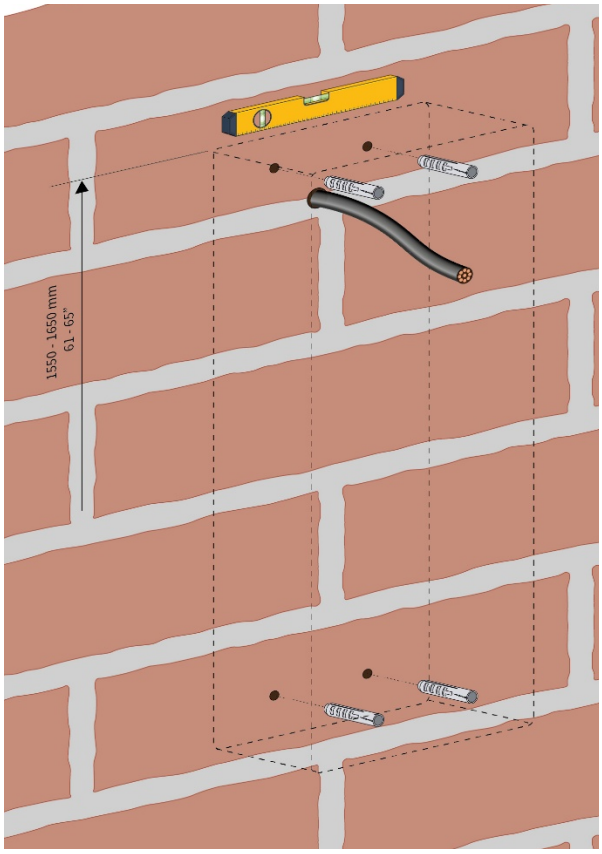
REQUIREMENTS

The following tools are recommended when installing the intercom in flush-mount configuration, including wall cutting and preparation:

- Measuring tape and pencil (for marking dimensions)
- Spirit level (to ensure correct alignment)
- Rotary hammer / drill with masonry drill bits
- Hole saw (if required for cable entry)
- Screwdriver or Allen key (model dependent, for fixing the unit)
- Vacuum cleaner or dust extraction equipment
- Protective equipment: safety glasses, dust mask, gloves, hearing protection

PLACING THE BOX

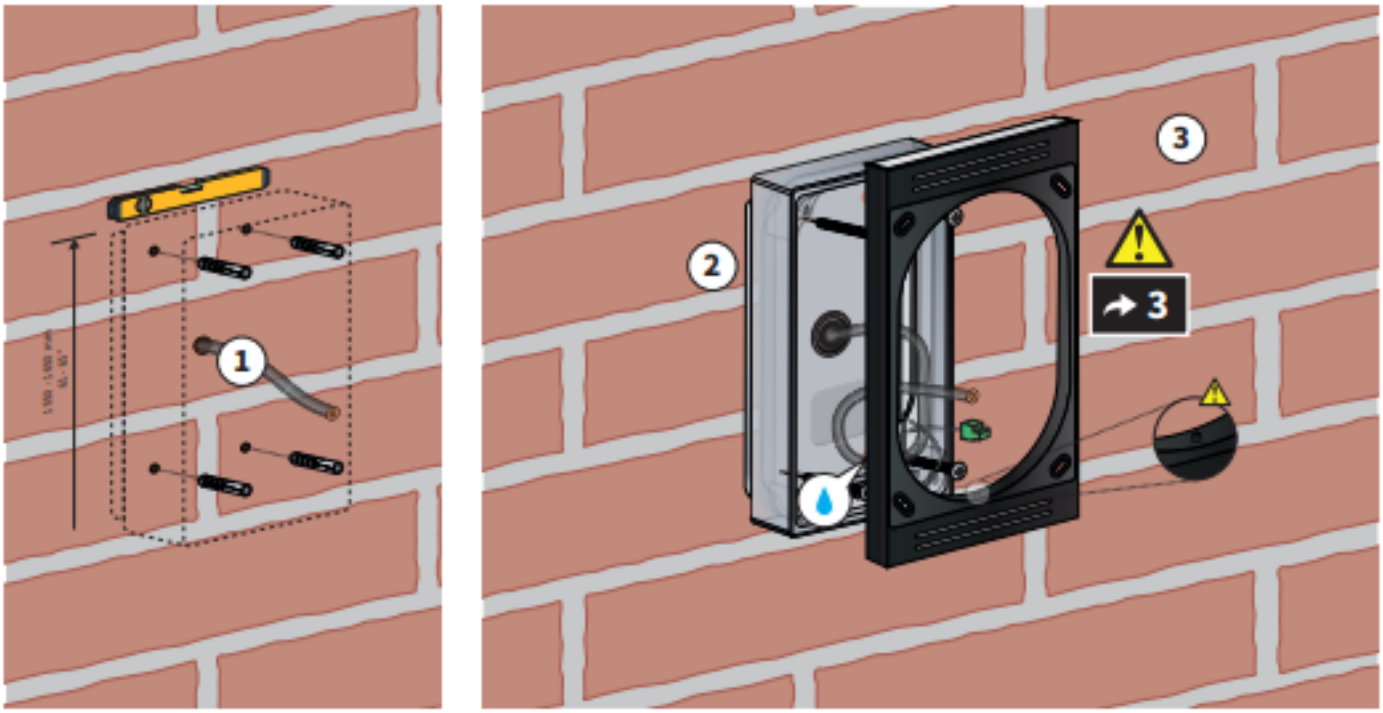
FOR MODELS WITHOUT AMBIENT FRAME



Keep the surface-mounting box in the right place on the wall and make sure it is level. Mark the four mounting holes on the wall with a pencil. Also mark the point where to make the hole for the intercom cables. Drill the holes.

Feed the Ethernet cable and the optional electronic relay and/or request-to-exit cable through the drilled hole. Route the Ethernet cable along the side of your intercom system. Consult the section "Wiring" to make sure your device has been setup properly, and make sure you protect your device from scratching during this process. Screw the surface-mounting box to the wall.

FOR MODELS WITH AMBIENT FRAME



Keep the surface-mounting box in the right place on the wall and make sure it is level. Mark the four mounting holes on the wall with a pencil. Also mark the point where to make the hole for the intercom cables. Drill the holes.

Feed the Ethernet cable (1) and the optional electronic relay and/or request-to-exit cable through the drilled hole. Screw the surface-mounting box to the wall (2) and route the Ethernet cable along the side of your intercom system.

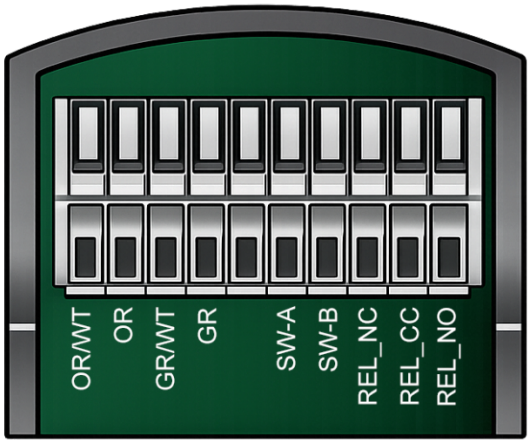
Once this has been completed, install the ambient frame onto the surface-mount box using the supplied screws (3). Ensure that the side featuring the small drainage opening in the ambient light is positioned at the bottom. This prevents water accumulation and protects the frame from moisture-related damage.

The ambient frame is equipped with a small connector (either a Phoenix connector or USB-C, depending on the model). This connector must be connected after the electrical wiring has been completed.

Consult the section “Wiring” to make sure your device has been setup properly, and make sure you protect your device from scratching during this process.

When wiring is complete, connect the ambient frame and proceed to the section “Finishing installation”.

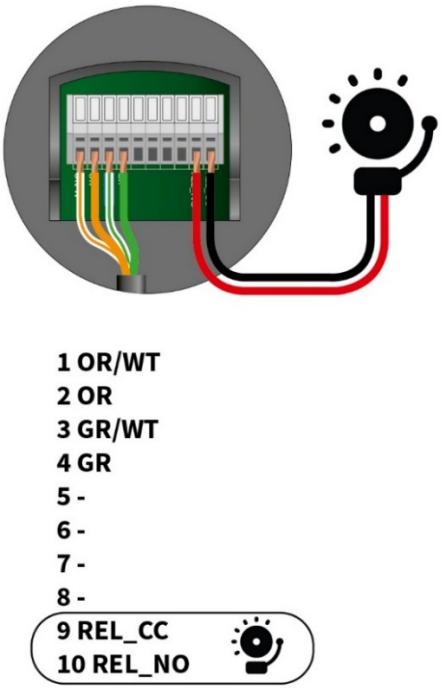
WIRING[1]



1	**OR/WT**	Network Cable (Orange/White)
2	**OR**	Network Cable (Orange)
3	**GR/WT**	Network Cable (Green/White)
4	**GR**	Network Cable (Green)
5		*Not used*
6	**SW-A**	Request-to-Exit button, Wire 1
7	**SW-B**	Request-to-Exit button, Wire 2
8	**REL_NC**	Relay, Normally Closed
9	**REL_CC**	Relay, Common
10	**REL_NO**	Relay, Normally Open

During wiring of the intercom, the plug-in terminal ensures a secure and reliable connection to your cables. However, to prevent cosmetic or mechanical damage during installation, it is recommended to temporarily wrap the device in a soft cloth, leaving the plug-in terminal accessible. Damage to the housing or ambient frame resulting from installation or mounting is not covered by warranty.

The colours for the individual cores must match the colour coding on the PCB. An additional cable (two-wire) is required for the optional electronic door lock (2). Attach the cable(s) to the housing as a tension relief using the supplied tie wrap (3).



[1] Connecting options are dependent on the model of the intercom

MOUNTING A ROBIN INTERCOM USING THE FLUSH MOUNT BOX

REFERENCES

Description	*Model(s)*	*CDVI Reference*	*Robin Reference*
Compact FB	Compact series	F0408000019	C01100
Pro FB	Pro (Classic) series	F0408000021	C01112
Proline FB	Proline, Doorbell	Included w/ product	Included w/ product
Touch FB	Touch		

INSTALLATION

REQUIREMENTS

The following tools are recommended when installing the intercom in flush-mount configuration, including wall cutting and preparation:

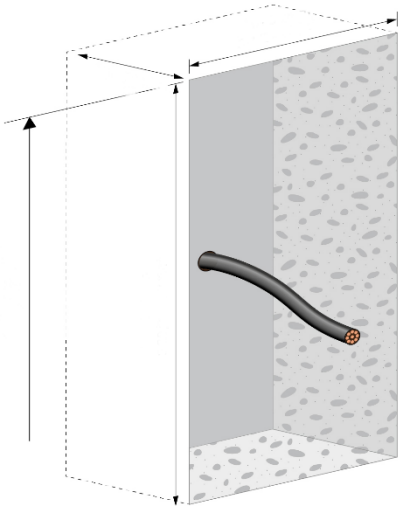
- Measuring tape and pencil (for marking dimensions)
- Spirit level (to ensure correct alignment)
- Wall chaser or angle grinder with diamond disc (for cutting the wall opening)
- Hammer and chisel (for finishing and adjusting the recess)
- Rotary hammer / drill with masonry drill bits
- Hole saw (if required for cable entry)
- Screwdriver or Allen key (model dependent, for fixing the unit)
- Vacuum cleaner or dust extraction equipment
- Protective equipment: safety glasses, dust mask, gloves, hearing protection

WALL OPENING DIMENSIONS

These are the measurements that have to be taken into account when creating a wall opening:

Model(s)	*Height*	*Width*
Audio/Video Compact	150-155 mm	90-95 mm
Audio/Video Pro (Classic) series	240-245 mm	90-95 mm
Proline, Doorbell	150-155 mm	90-95 mm
Touch		90-95 mm

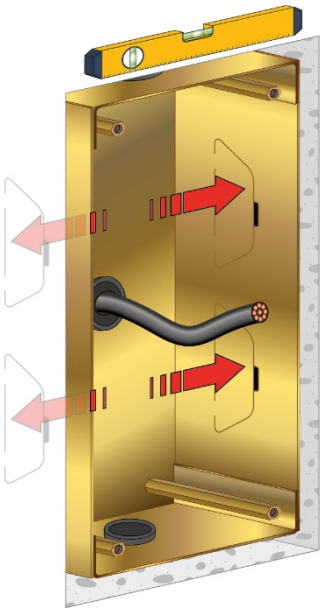
PLACING THE BOX



For mounting in a stone wall, make a recess in the wall. Drill a hole through the wall for the Ethernet cable and optional electronic door lock cable.

The measurements for the recess are dependent on the model of the intercom you have selected. Please consult the measurements of your specific model with the flush mount box before proceeding making a hole in your wall.

In the previous topic you will also find a reference table with the measurements of your specific model.



Place your flush-mounting box in the created hole and pass the cables through one of the four holes in the flush-mounting box. Don't forget to use the rubber sealing in all holes, and make sure the punctured rubber for passthrough is fitting nicely with the used cable.

Make sure the flush-mounting box is level and flush with the wall. Pull out the four tabs so that it is fixed in position (red arrows).

Fill the space between the flush-mounting box and the wall with wall filler and let it dry.

Once this process is complete you can continue with the next step, connecting the cable to your intercom.

→ Refer to section "**Wiring"** for terminal layout in the section "Mounting a Robin intercom using the surface mount box".

MOUNTING THE INTERCOM WITHOUT A FLUSH OR SURFACE BOX

Any damage or malfunction resulting from improper installation or the use of non-approved mounting methods or accessories is not covered by the warranty. For reliable operation and compliance with product specifications, the use of the provided or officially approved accessories is strongly recommended.

TOOLS

The following tools and materials are required when mounting the Robin:

- Core drill, 90 mm in diameter
- Masonry drill, 6 mm in diameter
- Stone chisel
- General set of tools
- Anti-theft Allen key (supplied)
- Anti-theft screws (supplied)
- 6mm wall plugs (supplied)
- Drilling template (supplied)
- Tie wrap (supplied)

MOUNTING

Follow the step-by-step plan described below for problem-free mounting of the Robin. Step-by-step plan:

1. Drill holes of 90 mm in diameter and 60 mm in depth using the core drill. Use the drilling template supplied in the package for this.
2. Remove the cores from the drilling using the stone chisel. Shape the hole so that the plastic housing of the Robin fits with room to spare.
3. Feed the cable into the hole, leave enough excess length for a loop in the hole.
4. Drill the four fixing holes for the front panel using the drilling template and insert the wall plugs supplied with the set into the holes.
5. Connect the Ethernet cable to the clamp connector.
    a. Optional - connect the cable for operating the relay to the clamp connector.
6. Secure the cable to the plastic housing using a tie-wrap.
7. Position the Robin in the hole in such a way that the looped cable fits neatly behind the device.
8. Fix the device securely in place using the anti-theft screws supplied in the package.

→ Refer to section "**Wiring"** for terminal layout in the section "Mounting a Robin intercom using the surface mount box".

FINISHING THE INSTALLATION

FOR MODELS WITHOUT AN AMBIENT FRAME

Secure the intercom to the flush-mount back box using the screws supplied with the unit. Depending on the model and the type of screws provided, use either the appropriate Allen key or a suitable screwdriver. Carefully align the intercom with the mounting frame or back box, ensuring that it sits straight and flush before tightening.

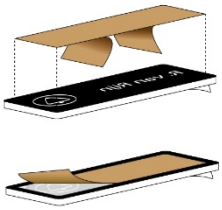
Tighten the screws manually by hand. Do not use power tools, as excessive torque may damage the housing, threads, or mounting components. Gradually tighten the screws evenly to ensure the unit is firmly and securely fixed in place. If required for high-vibration environments, a small amount of suitable thread-locking compound may be applied to the screws. Always ensure the device is securely mounted and stable after installation.

FOR MODELS WITH AMBIENT FRAME

When your model has Ambient illumination, finalising the installation needs to be done in another way. Whilst the models without this function have 4 holes for fitting screws, the ambient models have a small puncture in the bottom light. These models also have a long, slim Allen key that fits into the hole in the bottom ambient light.

After sliding in your device into the ambient frame, use that Allen key to ensure your device is securely fixed in its frame.

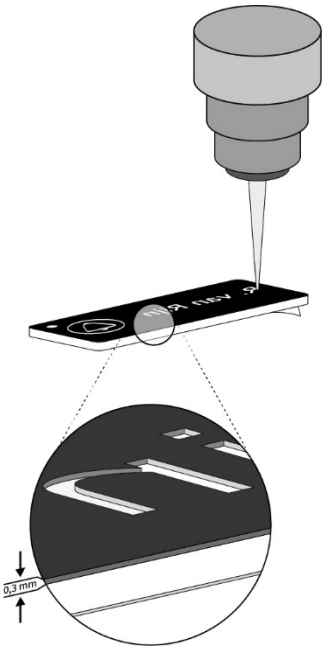
INSTALLING THE NAMETAG[2]



Once the device has been installed, the anthracite tag (personalised or standard) must be applied. First, remove the protective backing from one side of the adhesive and carefully attach it to the center of the tag. Press firmly to ensure proper adhesion.

Afterwards, remove the protective film from the other side of the adhesive. Position the tag neatly in the designated area on the intercom and press it firmly into place. Ensure that the bell symbol is positioned on the right-hand side when facing the intercom.
When you order a personalised tag, a blank tag is always supplied as well. This allows you to easily replace the tag in the future, for example if the device changes ownership.

ENGRAVING THE TAG



To engrave a tag correctly, the transparent adhesive must not yet be applied.

Place the tag in reversed (mirror) orientation before engraving. The top side must remain at the top, but the bell symbol will now appear on the left-hand side when viewed from above. The engraving must then be performed from right to left in mirror image.

Once engraving is complete, turn the tag over lengthwise so that the bell symbol is positioned on the right-hand side again, while keeping the top side at the top. The name will now appear correctly oriented.

You may now apply the adhesive to the rear side of the tag and proceed with installation. After the tag has been mounted, remove the protective front film to eliminate scratch protection and reveal the final finish.

[2] Only for models using the anthracite tag (1/2/4-button models)

PROVIDING A HIGH-END FINISH

After installation, the intercom should be carefully cleaned and visually inspected to ensure a flawless, high-end finish prior to handover. This final step enhances the perceived quality of the product and removes fingerprints, dust, and installation residues.

Use a high-quality microfiber polishing cloth that is clean and lint-free. The cloth must be dry or only very lightly dampened with clean water. Avoid paper towels or abrasive fabrics, as these may cause micro-scratches on aluminium or brass surfaces.

FOR ALUMINIUM FINISHES

Gently wipe the surface using straight, uniform strokes that follow the natural grain of the metal (if brushed). Do not apply excessive pressure. If necessary, a neutral, non-abrasive cleaner specifically intended for delicate metal surfaces may be used. The cleaner must be free from ammonia, solvents, acids, or alkaline components.

FOR BRASS FINISHES

Use a soft microfiber cloth and polish lightly to remove fingerprints and installation marks. Only use a neutral, non-abrasive metal care product suitable for finished or coated brass surfaces. Avoid any polishing compounds designed for restoring heavily oxidised brass, as these may alter the factory finish.

GENERAL RECOMMENDATIONS

Do not use alcohol, acetone, solvent-based cleaners, scouring pads, abrasive sponges, or chemical metal polish. Do not spray liquids directly onto the device. Always apply any approved cleaning product to the cloth first. Avoid excessive moisture around buttons, microphones, speakers, or seals.

FINAL INSPECTION

After cleaning, inspect the unit from multiple angles under natural light. Remove any remaining dust particles, fingerprints, or installation debris. Ensure that the lens, display, and nameplate areas are perfectly clean and free of streaks.

A properly cleaned unit significantly enhances the visual impact of the installation and reflects professional workmanship at the time of delivery.

CLEANING THE DEVICE

Regular cleaning preserves the aesthetic quality of the aluminium and brass finishes and maintains the original factory appearance. Cleaning frequency depends on environmental exposure and usage.

GENERAL INSTRUCTIONS

Use only a soft, lint-free microfiber cloth. For light cleaning, use the cloth dry. For heavier dirt, lightly dampen the cloth with clean water. If necessary, use a neutral pH, non-abrasive cleaner suitable for delicate metal surfaces.

Do not use abrasive pads, scouring sponges, metal polish, ammonia, solvents, acids, or alkaline cleaners. Do not spray liquids directly onto the device. Always apply any cleaning solution to the cloth first. Avoid excessive moisture near openings, buttons, microphones, speakers, or seals.

ALUMINIUM FINISH

For routine cleaning (every 1–3 months), wipe the surface with a dry microfiber cloth. For brushed aluminium, always clean in the direction of the grain. For visible dirt or fingerprints, use a slightly damp cloth and dry the surface immediately to prevent streaks.

BRASS FINISH

Clean regularly with a dry microfiber cloth to remove dust and fingerprints. For moderate dirt, use a lightly damp cloth and dry immediately. Do not use traditional brass polishing compounds unless the product is specified as untreated solid brass. Polishing agents may alter the factory finish or remove protective coatings.

ENVIRONMENTAL EXPOSURE

In coastal or industrial environments, increase cleaning frequency (monthly recommended) to remove salt or pollution deposits. Always dry the unit thoroughly after cleaning.

Regular, gentle maintenance ensures long-term durability and a professional appearance throughout the product’s lifetime.

SYSTEM INSTALLATION

REQUIREMENTS PRIOR TO INSTALLATION

Before configuring your device, please verify that the following requirements are met:

- Network connection with PoE (Power over Ethernet) for use with the Robin device
  - The PoE power supply must be 802.3af compliant.
- PC with web browser
  - The interface is optimized for Firefox, Safari and Google Chrome
- Network with or without DHCP support (DHCP support is recommended)
- Network cable
  - Optional: Two-core cable for relay operation

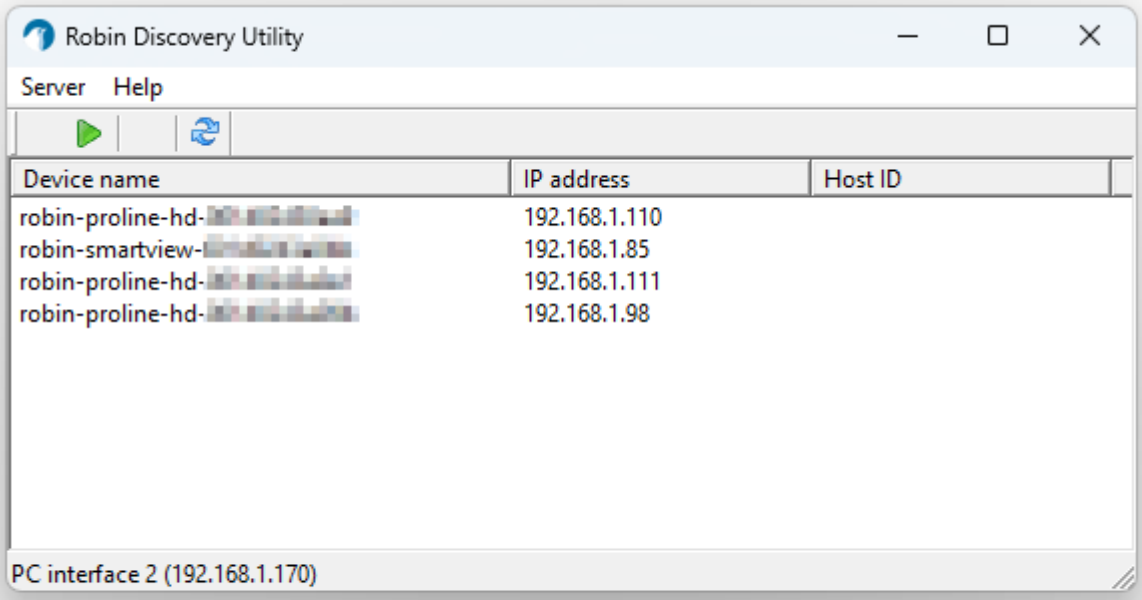
CONNECTING YOUR DEVICE TO THE NETWORK

Connect the Robin to the network via the network connection socket on the rear. The Robin will boot automatically. This can take up to 60 seconds.

Ethernet and PoE connections are limited to a maximum of 100 metres per cable segment, as defined by the Ethernet standard.
This limit applies between two active network devices.
Depending on cable quality, installation conditions, power requirements and the PoE equipment used, reliable operation may require shorter cable lengths.
The use of intermediate active network equipment may allow longer overall distances.

USING ROBIN DISCOVERY UTILITY (ALL ROBIN SIP-MODELS)

Copy the 'Robin Discovery Utility' software to a PC that is connected to the network. Start the 'Robin Discovery Utility' software and click the "Play" button. The software will scan for Robin devices in the network. When a Robin is detected, it is displayed in the list. Double-click on the detected Robin you would like to configure; the web interface for the selected Robin will show.

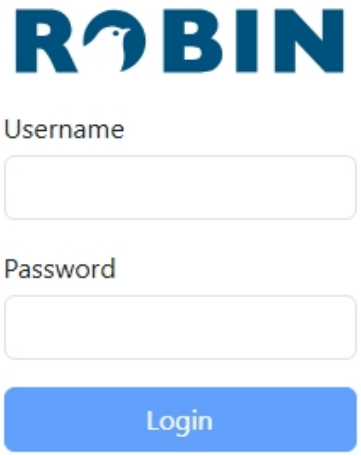


On non-Windows systems, device discovery can be performed using standard network scanning tools such as Nmap or via DHCP lease inspection.

CONFIGURATION

LOGGING IN TO THE WEB INTERFACE

When going to the IP-address of your device (using a fixed IP, an IP-scanner or the Robin Discovery Utility), you will automatically proceed to the login-page of your device:



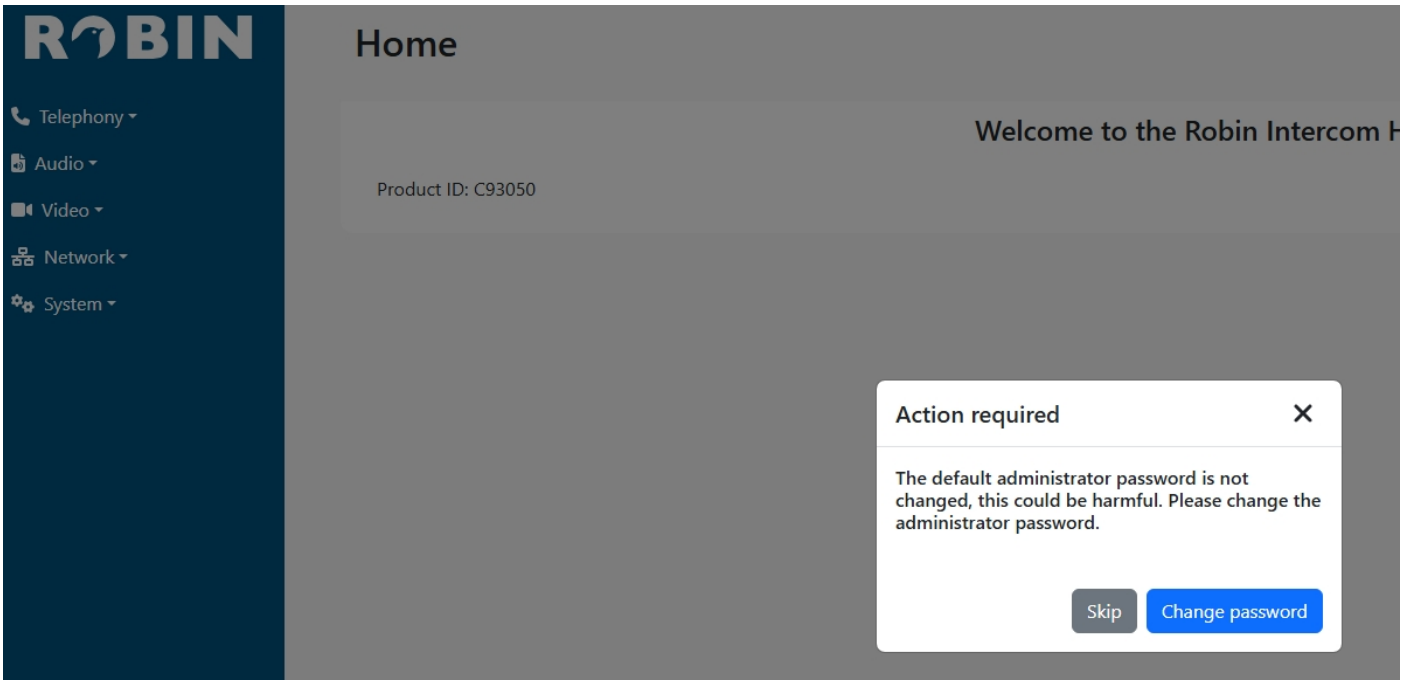
In this screen, you can login with default credentials:

- Username: admin
- Password: 123qwe

Press login to continue.

SETTING UP FOR USE

When you login for the first time, the device will prompt you to set a new password:



Select "Skip" to provide a new password another time, or select "Change password" to immediately change your credentials to make the authentication more secure. Kindly ensure that your credentials are retained and accessible at all times[3].

After choosing to skip or change the password settings, the essential system parameters must be configured before the device can be placed into operation. Refer to the relevant chapters according to the technical requirements of the specific installation.

Under standard installation conditions, the following configuration steps are recommended:

1. IP-configuration: The default setting is DHCP. Under standard installation conditions, it is recommended to assign a fixed IP address to ensure stable access and simplify future configuration changes (chapter Network → IP)
   The system will reboot after changing the IP-address
2. Connection with SIP, Teams or P2P: Follow the configuration provided in the following chapter to make a correct configuration of your device to connect with your phone system provider, or configure your P2P-connection (chapter Telephony → SIP/Peer-To-Peer)
3. Configure your call-buttons (chapter Telephony → Phonebook and Button Settings)
4. Make sure your time and date are correct (chapter System → Time)

By implementing these configurations, the system will be fully initialized and ready for immediate deployment. According to more specific settings, the following chapter will overview all possible settings and integrations that can be configured according to your needs and for your device.

[3] It is strongly recommended to change the default credentials immediately before connecting the device to any operational network.

Some settings will not be visible or shown on your device. This manual provides an overview of all available settings on a device, but some settings will be limited or not provided if your equipment does not have that particular functionality. For example, video options will not show on audio-only devices. Keep in mind that if an option is unavailable, this is because of the limitations within your product. Neither Robin nor CDVI has the possibility to activate functions that are not supported by the device.

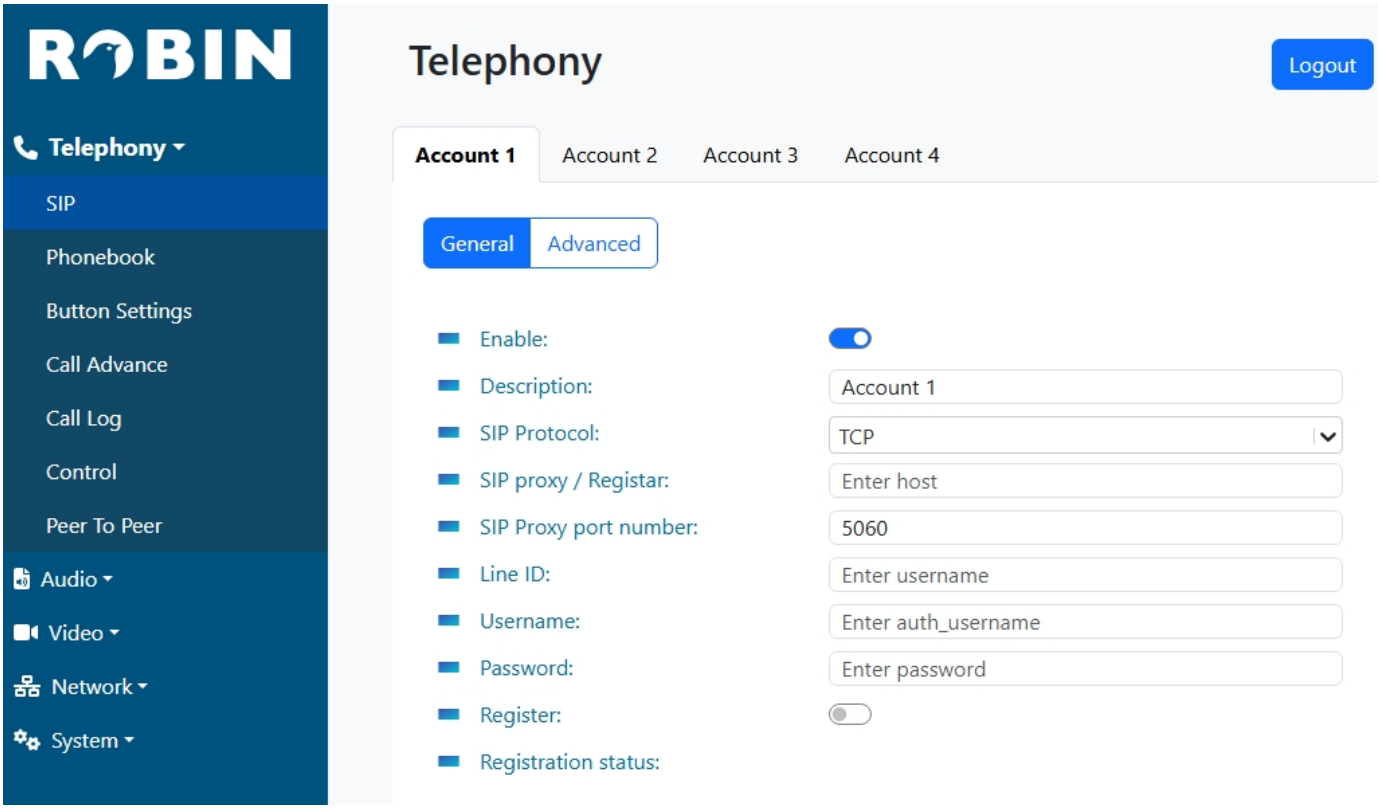
TELEPHONY

The Telephony section describes how the Robin intercom communicates using the Session Initiation Protocol (SIP). Through SIP, the Robin operates as a network-based door intercom that can place and receive calls via an IP-PBX, a VoIP service provider, or a direct peer-to-peer connection.

In this section, you configure the parameters required for call handling and registration, including SIP server settings, call destinations, and basic network-related telephony options. Depending on the device type, both audio and audio-video communication are supported, allowing users to speak with visitors and control door access during a call.

Correct configuration of the telephony settings is essential for reliable communication, good call quality, and stable operation within a professional network environment.

SIP



When opening the first menu item under Telephony, the SIP configuration section is displayed. This section forms the core of the intercom's telephony functionality and allows configuration of up to four SIP accounts. In most installations, the settings available in the "General" tab are sufficient. The required credentials and parameters depend on the configuration of the connected SIP PBX system or VoIP provider.

The following section describes the available parameters and outlines the configuration procedure.

Before proceeding, ensure that the necessary SIP account credentials have been created in the PBX or VoIP platform. These details are typically provided by the IT or telephony administrator.

FIELDS

In this menu, you will find the following fields:

Field	*Description*
Enable	Switches the account on or off
Description	Descriptive name of this account (e.g. Company)
SIP Protocol	Select the SIP-protocol (UDP/TCP or TLS)
SIP proxy / Registrar	Enter the IP address or hostname for the IP-PBX, Teams- or VoIP-provider
SIP Proxy port number	Enter the IP port number for the IP-PBX or VoIP-provider
Line ID	Enter the Line ID. If not available, use the same name as the Authentication-parameter in your PBX, generally the "Username"
Username	Enter the authentication username for registration to the IP-PBX or VoIP provider
Password	Enter the password for registration to the IP-PBX or VoIP-provider
Register	Activate or deactivate registration to the IP-PBX or VoIP provider
Registration status	Shows the current status of your registration

In advanced mode, you will have the following additional options:

Field	*Description*
Outbound proxy	Select this option when a SIP proxy server is used
DNS SRV	Select this option when DNSsrv is used
Audio RTP port start	Enter the lowest IP port that may be used for the RTP audio stream
Audio RTP port end	Enter the highest IP port that may be used for the RTP audio stream
Video RTP port start	Enter the lowest IP port that may be used for the RTP video stream
Video RTP port end	Enter the highest IP port that may be used for the RTP video stream
RTP Maximum MTU size	Enter the largest packet size that an RTP-stream can safely use without being fragmented at the IP layer
RTP port random	Use random RTP ports (within the specified range)
SIP port random	Use random SIP ports (within the specified range)
Keepalive	Enable keepalive packages
Enable REFER	Accept 'REFER' packages (off by default)
Expires	Enter the expiration interval (3600 by default)

CONFIGURING THE PBX

In order to get the details required for your configuration, the phone system (PBX) needs to be configured first. While PBX implementations may vary, the fundamental provisioning workflow remains comparable across platforms:

1. Log in to your PBX system (e.g. Asterisk, 3CX, …)
2. Create a new Line/User in your phone system (e.g. Intercom)
3. Add a phone to this Line/User
4. When adding a phone, a username and password will be provided or you will have the opportunity to define it.
5. The PBX system will also provide you with information to connect to your local SBC or cloud-system

Make sure you keep this data in a safe place. You now have the required information to complete the configuration.

CONFIGURING THE ROBIN

The collected PBX credentials can now be entered into the SIP configuration of the Robin-device. Select the tab "Account 1" (Keep it on General) and fill in the blanks:

- Enable: Active
- Description: Phone System
- SIP Protocol: UDP (depending on your PBX location or when using an SBC)
    - Use TCP/TLS if your system is not locally present
- SIP Proxy: Enter the hostname, e.g. 192.168.1.100 or site.phonepbx.com
- SIP Proxy port number: 5060 is usually the correct port
- Line ID: Fill in the local phoneline for your user "Intercom", e.g. 101
- Username: Fill in the username provided when creating your phone
- Password: Fill in the password provided when creating your phone
- Register: Active
    - If registration repeatedly fails, it is recommended to temporarily disable the account to prevent automatic IP blocking by the PBX security policy.

When all is correct, the "Registration status" will show the message "Registered".

USING MICROSOFT TEAMS

If you are using a phone system by Microsoft Teams, then you can integrate this as well with your Robin intercom. Integration with Microsoft Teams requires a compatible SIP-to-Teams gateway, but this guide focusses on the use of CyberGate. For this an external licence can be used, which is purchasable from the Microsoft Azure Marketplace or Microsoft AppSource.

When your licence has been purchased, go to https://admin.cybergate.cybertwice.com.

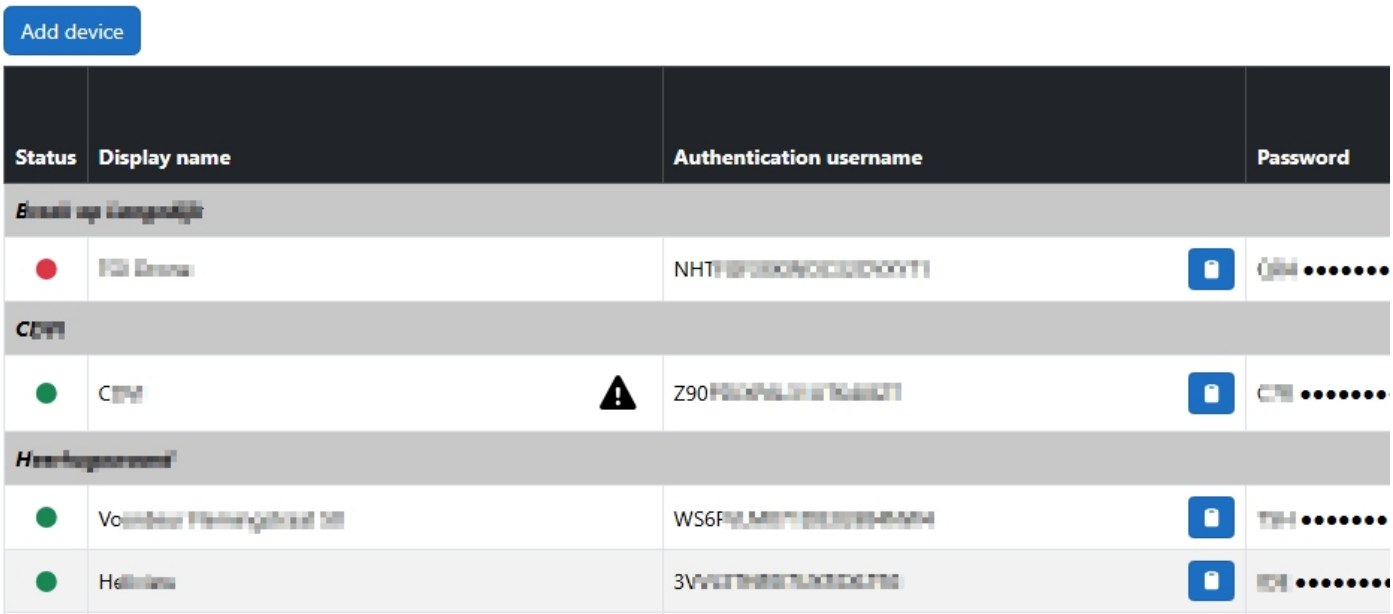
Login with your Microsoft credentials (additional authentication can be required using SMS, call or Authenticator). Once logged in, you will see the Cybergate web interface.

The section describing configuration via CyberGate has been prepared based on the version available at the time of writing. As CyberGate is an external product and not developed, maintained, or controlled by Robin or CDVI, its interface, functionality, or visual layout may change without prior notice and without responsibility on the part of Robin or CDVI. Minor visual or procedural differences may therefore occur compared to the descriptions and screenshots provided in this manual.

CONFIGURING CYBERGATE

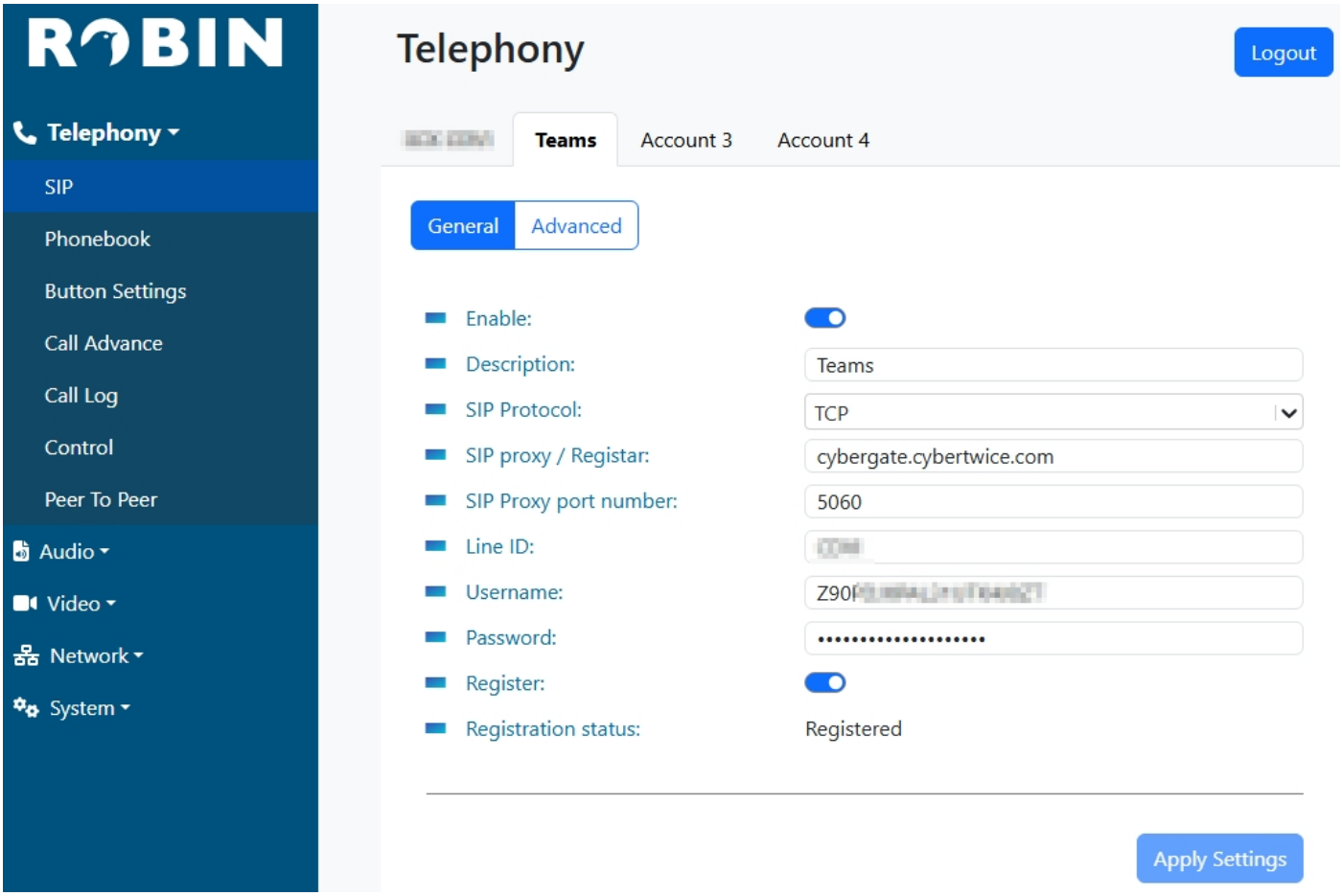
After logging in to the CyberGate portal, you will arrive in a window where you can change your personal settings, add your domain or local WAN to the licence and add intercom devices.

First of all, go to the "Network Settings" and add your local IP or device location domain to the licence. After that step, proceed to "Device":



Add your device. Afterwards, you can use the username and password to program your Robin device in the next step:

CONFIGURING THE ROBIN FOR TEAMS

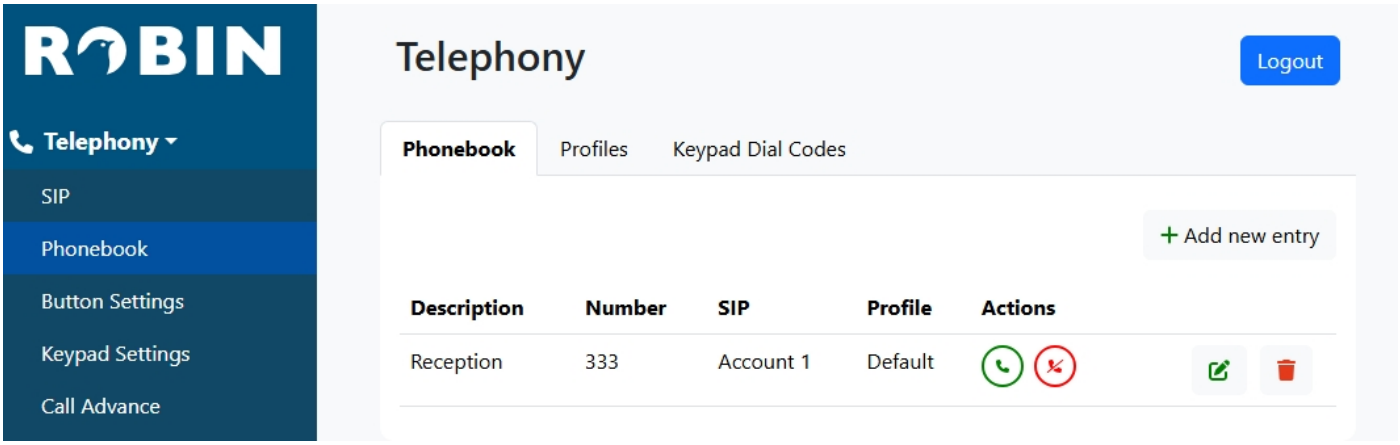


This procedure is identical to SIP-configuration, with the following exemptions:

- Protocol is TCP, Proxy is cybergate.cybertwice.com
- Line ID is the "Display name" in CyberGate and should be identical
- Username and password are specified in the CyberGate profile

PHONEBOOK

PHONEBOOK TAB



In the "Phonebook" tab you will have the possibility to add different numbers for both destinations as for operators who have the possibility to access the intercom.

In this menu you will be able to add for example a reception desk, who will receive the call when the "Call" button on your device is pressed, but also contacts who have the ability to call the intercom device and receive audio and video feedback.

If you wish to call the intercom device with your SIP phone or application, it is highly recommended that you create yourself as a contact (or every individual in your team) inside the Phonebook. By doing this, you have the ability for each person to select which codec the intercom will provide to your device, allowing you to always connect with a compatible audio (and video) stream.

Since adding additional people is optional, it does provide the function of providing codec information about each incoming device. When adding a person who has the ability to call incoming, you are able to configure a codec for each of those people, providing maximum compatibility in the device calling the intercom.

Adding a device can be easily done by pressing "Add new entry". The following parameters can be set:

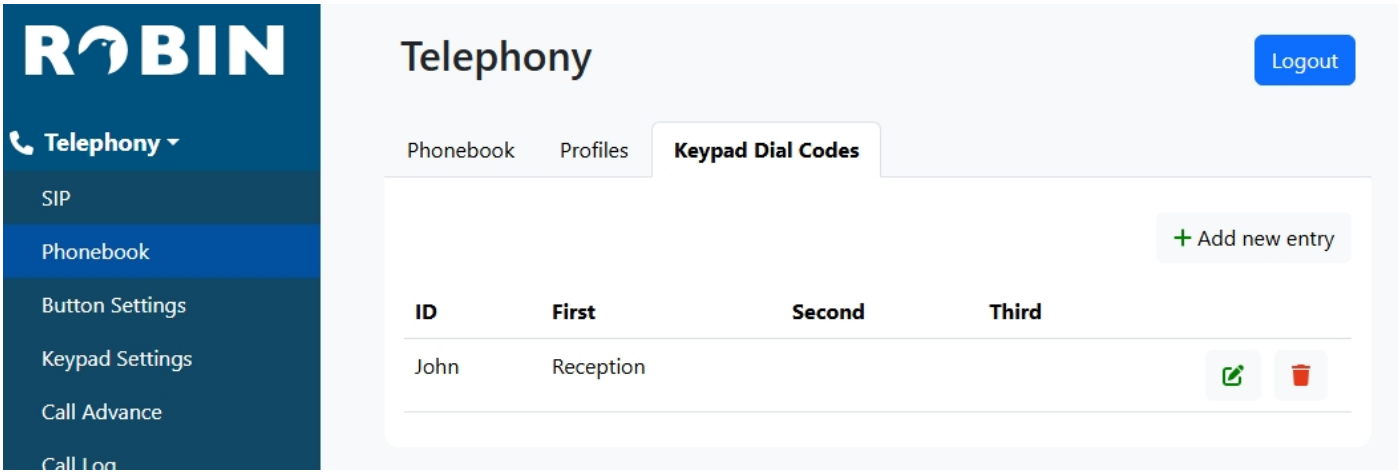
- Description: For example "Reception", or the recipients name
- Number: The internal phone number or Teams-id for that specific person
- SIP account: Here you can specify the account connected to that number
- Profile: This provides the codec that will be assigned to that specific person
- Logo[4]: Add a logo for the specific contact in your Phonebook

PROFILES TAB

In Profiles, two default profiles are displayed, preconfigured for standard usage and Teams. Nevertheless, you have the ability to add unlimited additional profiles for individual devices. When adding a new entry, you have can configure independent codecs and payload types, including bitrate for your PBX or device. Once the profile is made and saved, it can be used in your Phonebook to connect to any contact.

[4] This feature is only available on models with touchscreen.

KEYPAD DIAL CODES TAB[5]



The Keypad Dial Codes tab allows keypad codes to be defined and associated with a specific PIN or destination number.

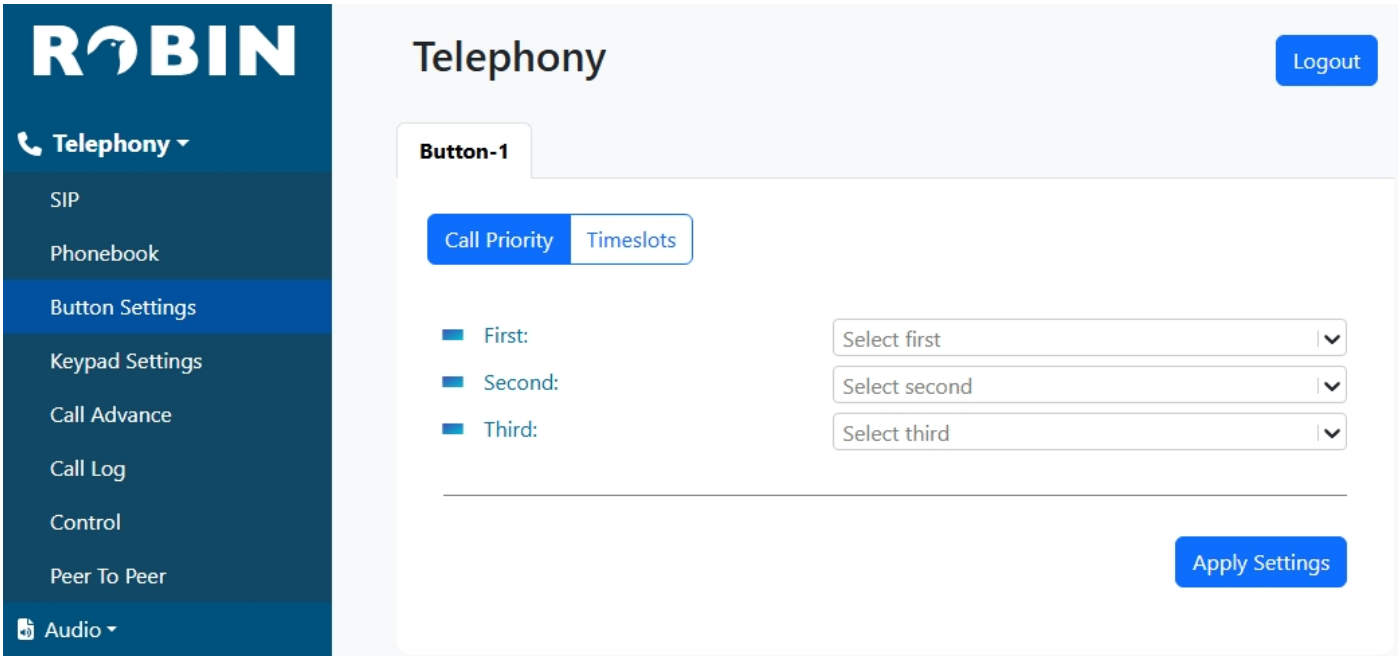
When creating a new entry, the following parameters must be configured:

- ID: Here you can specify the identification, such as apartment number
- First: The first number it should call
- Second: The second number that the device will call
- Third: Same function for a third number
- Pin: A code that can be entered in the keypad to trigger the relay

When using an intercom system that has access control, such as the Robin Touch, a separate menu will be available to add user access to the relay in a more secured way. You can find a detailed explanation in the section Access Control → Pin.

[5] This feature is only available on models with keypad.

BUTTON SETTINGS



The next menu allows configuration of the "Button Settings". On default, the number of tabs (Button-1, In the next menu, the "Button Settings" can be configured. By default, the number of available tabs (Button 1, Button 2, etc.) depends on the number of physical call buttons present on the device.

On models equipped with a keypad or touchscreen, one button is available by default. Additional virtual buttons may become available depending on the number of contacts defined in the "Phonebook"[6].

When multiple buttons are available, a call destination must be configured individually for each button.

Each button configuration is divided into two sections. The first section, "Call Priority", defines the order in which numbers are dialled when multiple SIP accounts are configured. If only one SIP account is used, call priority can alternatively be managed within the PBX. However, at least one contact, ring group, or queue must be defined in the "First" field to ensure proper call routing.Button-2) is dependent on the number of physical buttons available on your device. In models that contain a keypad or touchscreen the default is 1 button, and will add more depending on the amount of contacts in your "Phonebook". When multiple buttons are available, directing your call is required for each of the available buttons.

When your "SIP" has been setup and running, the "Phonebook" is configured and your "Button Settings" are completed, your system is ready for the first call.

[6] Models with touchscreen require that it is set to "Multiple" within the display settings.

BUTTON EXTENDER[7]

The Button Extender is a PoE-powered input module that allows you to expand the number of physical call buttons connected to the intercom. Each extender supports up to 36 individual buttons, making it ideal for residential buildings, office environments, or any installation where multiple direct call buttons are required.

A common example is a mailbox or apartment panel where every resident has their own physical button. Each button can directly call the correct SIP destination, while the intercom itself can remain a central unit, for example calling reception, concierge, or building management.

ADDING THE BUTTON EXTENDER TO YOUR MENU

The Button Extender is automatically detected on the network, provided it is connected within the same IP range as the intercom. Once detected, a new menu item appears under Telephony → Button Extender.

No manual IP configuration is required, as long as standard network connectivity is available and PoE power is supplied.

LINKING THE EXTENDER TO YOUR INTERCOM

After detection, the extender must be linked to the correct intercom.

- Navigate to Telephony → Button Extender
- Click Add extender
- Select one of the detected extenders from the list

Confirm to associate it with the current intercom. Once linked, the extender will appear in the overview list and becomes active for button detection.

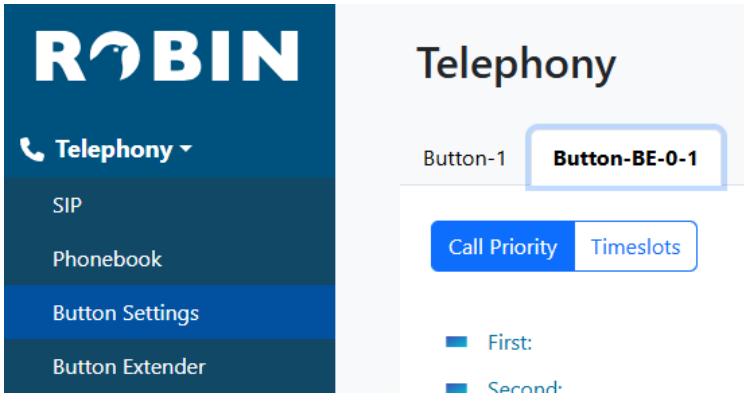
REGISTERING PHYSICAL BUTTONS

After the extender has been linked, the physical buttons must be registered. Press each physical button one by one on the connected button panel.

When a button press is detected:

- The extender automatically registers the button.
- A new button entry is created under Telephony → Button Settings.

From there, each button can be configured individually, including call priority, time schedules, and SIP destination.



This approach ensures that the physical layout of the installation is directly reflected in the configuration interface, allowing precise and scalable call routing.

[7] This function is only available if a Button Extender is installed.

KEYPAD SETTINGS[8]

When using a keypad-only model or a touchscreen-based Robin device, you will have this option where you have the ability to set instructions for the usage of the keypad. In this menu, you have the ability to set the following items:

- Preset to call when I-button is pressed: Here you can set a line/number that will be called when the informational button (the I-button) is pressed on the keypad
- Block leading zeros: When entering a number (e.g. 11) which is pressed as "011", it will block all zeros entered before seeing the first digit which is not a zero
- Max preset length: Here you can instruct the maximum number of digits that can be pressed on the keypad before automatically dialling the selected number

CALL ADVANCE

An intercom is a 2-direction device. Because of this, these parameters will aid you in bidirectional audio and/or video. This menu can set the following parameters:

- Auto answer: When activated, it will automatically pickup a call when you are calling the intercom line number. When this is enabled, it will also show the auto answer delay
    - Auto answer delay: This option will wait for X seconds before picking up automatically
- No answer timeout: This function will automatically cut the call after X seconds whenever a call is made
- Max call duration: This option is to define the maximum of time that a call can contain before automatically cutting the communication. This option is used as a failsafe so any open calls will not remain open
- Early offer[9]: When this is enabled, the intercom will show video to a remote screen as soon as the call button has been pressed. With this active, you have the ability to watch any video feed before answering the visitor.

[8] On models with keypad or touchscreen

[9] On models with video and support for early offer

CALL LOG

The Call Log section in the web interface provides an overview of all incoming and outgoing calls handled by the intercom. It allows installers and administrators to verify call activity, confirm successful connections, and identify missed or failed call attempts. This information supports faster troubleshooting and helps validate correct SIP configuration. By offering clear insight into recent call history, the Call Log improves transparency, maintenance efficiency, and overall system diagnostics. You also have the ability to delete the entire calling log, or partial.

CONTROL

The call control buttons in the web interface allow installers and service technicians to initiate test calls directly from a browser without physically pressing the intercom button. This makes it possible to quickly verify SIP signaling, audio, and video functionality during commissioning or after configuration changes. It also simplifies remote troubleshooting when the device is accessed over the network. As a result, installation time is reduced and maintenance and support procedures become more efficient.

Inside the “Control” menu, you will see the current calling status of your intercom device. Here you can make an immediate call (with the same principle as pressing the “Call” button on your device) to the recipient. It also provides the ability to end the call with the “Hangup” button. Besides this functionality it also shows the status of your SIP-registration and any current call status.

PEER TO PEER (P2P)

Peer-to-Peer (P2P) in this context means that the intercom establishes a direct SIP connection with a single SIP monitor or SIP telephone, without the use of a SIP server, PBX, or cloud service.

When a call button is pressed, the intercom directly sends a SIP INVITE to the IP address of the configured monitor or phone. Audio (RTP) and, if supported, video are streamed directly between both devices. The communication path is therefore device-to-device, without intermediate call routing, registration server, or account-based infrastructure.

In a P2P setup, both devices are typically configured with fixed IP addresses (or known hostnames), and the intercom is programmed to dial the SIP URI of the target device directly. No SIP registration to a central server is required.

In summary, Peer-to-Peer SIP communication offers a simple and direct solution for small installations with one intercom and one monitor or phone on the same network. For larger, more flexible, or remotely accessible systems, a SIP server or PBX-based architecture is recommended.

SETTING UP PEER-TO-PEER IN YOUR DEVICE

Setting up a Peer-to-Peer connection is a two-step process. Both the intercom and the receiving device (monitor or phone) must be configured accordingly.

Before proceeding, ensure that both devices are assigned a fixed IP address. For the Robin intercom, IP configuration can be found under “Network” → “IP”.

Verify with the system administrator that the SIP communication port (default 5060) is open and accessible between both devices.

CONFIGURATION FOR P2P ON THE ROBIN

Access the “Peer-to-Peer” configuration under the “Telephony” menu.

AUDIO

The Audio section describes how sound is processed and handled by the Robin intercom. In this section, you can configure settings that affect speaker output, microphone input, and overall audio behaviour during calls and events.

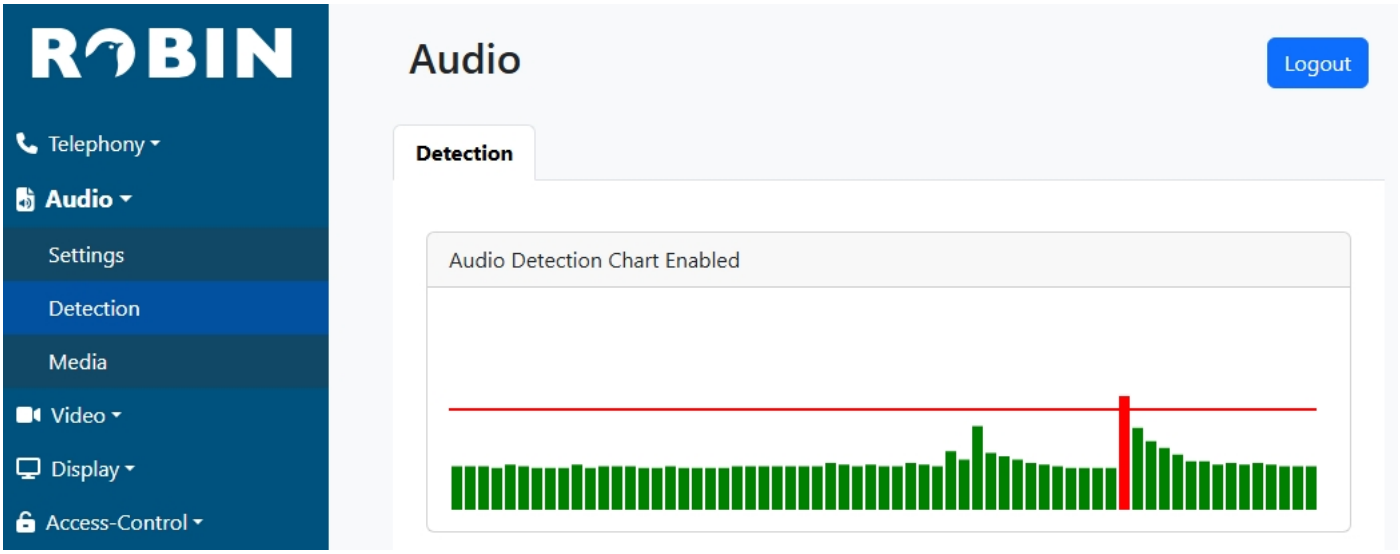
These settings allow the audio performance to be adapted to the installation environment, ensuring clear communication, minimal echo, and reliable detection of sound-related events. Proper adjustment of the audio parameters contributes directly to call quality and user experience.

SETTINGS

The Audio Settings section allows you to configure the audio behaviour of the intercom, including speaker output, microphone sensitivity, system tones, and mute behaviour.

- Speaker volume: Adjusts the output level of the built-in speaker. The value can be set between 0 and 100. Increasing this value raises the playback volume for calls, tones, and other audio signals
- Microphone sensitivity: Adjusts the sensitivity of the built-in microphone, also on a scale from 0 to 100. A higher value increases the microphone gain, making the intercom more sensitive to sound. This may be useful in environments where the speaker is positioned further away. Lower values can help reduce background noise or echo
- Tone volume: Defines the volume level of system tones on a scale from 0 to 10. The default value is 2. This setting controls sounds such as confirmation tones or notification beeps
- Mute: The Mute dropdown menu determines how audio and tones are handled. The available options are:
    - Off: All audio and tones are active
    - Tones incoming: Only incoming tones are muted. Other system sounds and audio remain active
    - Tones all: All system tones are muted, but voice audio during calls remains active
    - All audio: Mutes all audio output. The tone-related mute options are linked to the System → Events configuration, where events can trigger specific tones. These settings allow selective suppression of default sounds or all tones, depending on installation requirements
- Test tone: When enabled, a test sound is played through the speaker. This function is useful during installation to verify correct speaker operation and to adjust the volume level accordingly

DETECTION



The Audio Detection section allows you to configure sound-based event detection using the built-in microphone. This function can be used to trigger actions when a defined sound level is exceeded, such as a loud noise or voice activity.

At the top of the page, a real-time audio detection chart is displayed. The green bars represent the current ambient sound level detected by the microphone. The horizontal red line indicates the configured threshold level. When the audio signal exceeds this threshold for a defined duration, a detection event can be triggered.

- Enabled: Activates or deactivates audio detection. When disabled, no sound-based events will be generated
- Threshold: Defines the sound level that must be exceeded to trigger detection. Increasing the threshold reduces sensitivity and helps prevent false triggers caused by background noise. Lowering the threshold makes the system more sensitive to quieter sounds.
- Duration: Defines how long the sound level must remain above the threshold before a detection event is triggered. This helps filter out short, sudden noises and ensures that only sustained sound levels activate the event.

When the configured threshold and duration conditions are met, an audio detection event can be triggered. The corresponding actions, such as sending a notification or activating a relay, are configured in the System → Events section.

MEDIA

The Media section allows you to manage custom audio files used by the intercom for tones and event sounds. This menu consists of two tabs: Media and Media Mapping.

MEDIA

The Media tab displays a list of available audio files. This includes the default system sounds as well as any custom sounds that have been uploaded.

You can upload additional audio files by selecting Add new entry. When uploading a file, the following fields must be completed:

- Name: Defines the identifier of the custom sound. This name will be used when selecting the file in the Media Mapping tab
- File upload: Allows you to upload the audio file. Supported formats are WAV (8-bit, 16000 Hz, PCM) or MP3 (128 kbps). Files that do not match these specifications may not function correctly

Once uploaded, custom sounds appear in the list and can be played, edited, or removed. Default system sounds are always available but cannot be deleted.

MEDIA MAPPING

The Media Mapping tab allows you to assign custom audio files to specific phone events. For each entry, you select a Phone Event and link it to one of the uploaded custom media files.

Available phone events include:

- Button
- Ring
- Ringback
- Disconnect
- Busy

Only custom uploaded sounds are available for selection in Media Mapping. Default system sounds are not shown in this list. If no custom sound is assigned, the intercom will use the standard default sound for that event.

This configuration allows installers to personalize the acoustic behavior of the intercom according to project requirements.

VIDEO[10]

The Video section describes how the integrated camera of the Robin intercom is configured and used. In this section, you can view live video, adjust image and encoder settings, and define how video is processed and transmitted.

These settings allow the video performance to be optimized for the installation environment and network conditions, ensuring a clear and stable video stream during calls and for monitoring purposes.

LIVE

The Live section displays the real-time video stream of the intercom camera. This page allows you to monitor the current camera view directly from the web interface. No configuration settings can be modified on this page; it is intended for live viewing and verification purposes. The displayed stream reflects the active video configuration of the device. This makes the Live page useful during installation and commissioning to verify camera positioning, focus, lighting conditions, and overall image quality.

If OSD (On-Screen Display) is enabled in the Video → Settings section, the configured OSD elements will be visible in the live video stream. The OSD can be used to display information such as date, time, or custom text overlays. These OSD settings also apply to external video streams, including RTSP streams configured in Network → RTSP. Changes made to the OSD configuration will therefore affect both the Live view in the web interface and any connected RTSP clients.

SETTINGS

The Settings section allows you to configure the image parameters and on-screen display (OSD) of the intercom camera. This menu is divided into three tabs: General, Advanced, and Overlay.

GENERAL

The General tab displays the live video stream and provides direct control over the basic image parameters. The following settings can be adjusted using sliders:

- Brightness: Adjusts the overall light level of the image
- Contrast: Controls the difference between light and dark areas in the image
- Saturation: Adjusts the intensity of the colours
- Sharpen: Enhances edge definition to improve perceived image clarity
- HDR: The HDR (High Dynamic Range) toggle can be enabled to improve image quality in high-contrast scenes, such as entrances with strong backlight. HDR helps balance bright and dark areas within the image

Changes are immediately reflected in the live preview, allowing real-time visual adjustment.

[10] Not included in Audio-only models or non-SIP models

ADVANCED

The Advanced tab provides additional control over image compression and streaming parameters.

- JPEG quality: Defines the compression level of JPEG snapshots. The default value is 70%. Higher values improve image quality but increase file size and bandwidth usage.
- Bitrate: Defines the video stream bitrate. Available options are 512, 1024, 1536, 2048, 2560, and 3072 kbps. A higher bitrate improves video quality but requires more network bandwidth. The optimal setting depends on the network capacity and recording requirements.

OVERLAY

The Overlay tab allows configuration of the On-Screen Display (OSD), which adds information directly onto the video stream.

- Enable: Activates or disables the OSD
- Time stamp: Displays the current date and time on the video stream
- Device name: Displays the configured device name
- Device location: Displays the configured device location
- Extra text: Allows you to enter a custom line of text that will be added to the video overlay

The Device name and Device location are defined in System → Device, under the Identity tab. Any changes made there will be reflected in the OSD when the corresponding options are enabled.

OSD settings apply to both the web-based Live view and external streams such as RTSP.

MOTION

The Motion section allows you to configure motion detection for the intercom camera. The page displays the live video stream, enabling you to visually define detection zones directly on the image.

You can draw one or more rectangular zones on the video. Motion detection will only be evaluated within these defined areas. This allows you to ignore irrelevant background movement, such as public roads or trees, and focus only on specific areas of interest.

- Enabled: The Enabled toggle activates or deactivates motion detection. When disabled, no motion events will be generated
- Sensitivity: The sensitivity slider determines how easily movement is detected. A higher sensitivity increases the likelihood that small changes in the image will trigger detection. Lower sensitivity reduces false triggers caused by minor lighting variations or small movements.
- Object size: The object size slider defines the minimum size of movement that will be considered as a valid trigger. Increasing this value helps filter out small movements, such as shadows, rain, or small animals

When motion is detected within the configured zones and according to the defined sensitivity and object size, a motion event can be triggered. The actual action that follows, such as sending an email, activating a relay, or notifying an external system, is configured in System → Events.

STREAMS

The Streams section provides an overview of all currently active video streams from the intercom. This page is informational only and cannot be used to modify stream settings.

For each active stream, the following information is displayed:

- Start: Indicates the date and time at which the stream session was initiated
- Stream type: Shows the type of stream that is active, for example motion-triggered stream or continuous MJPEG stream
- Remote IP: Displays the IP address and port number of the client device that is receiving the stream. This allows you to identify which system, NVR, or workstation is connected to the intercom
- Width and Height: Indicate the video resolution currently being transmitted to the client
- Codec: Shows the video codec used for the stream, such as MJPEG.
- Quality: Displays the compression quality setting applied to the stream, expressed as a percentage or bitrate

This overview is useful for diagnostics and monitoring purposes, allowing installers or administrators to verify active connections, detect unexpected stream usage, and confirm video parameters in real time.

DISPLAY[11]

The display settings allow you to tailor the visual interface of the intercom to your project's identity and functional requirements. From layout selection and typography to on-screen controls and video presentation, every element can be configured to ensure a consistent, intuitive and refined user experience.

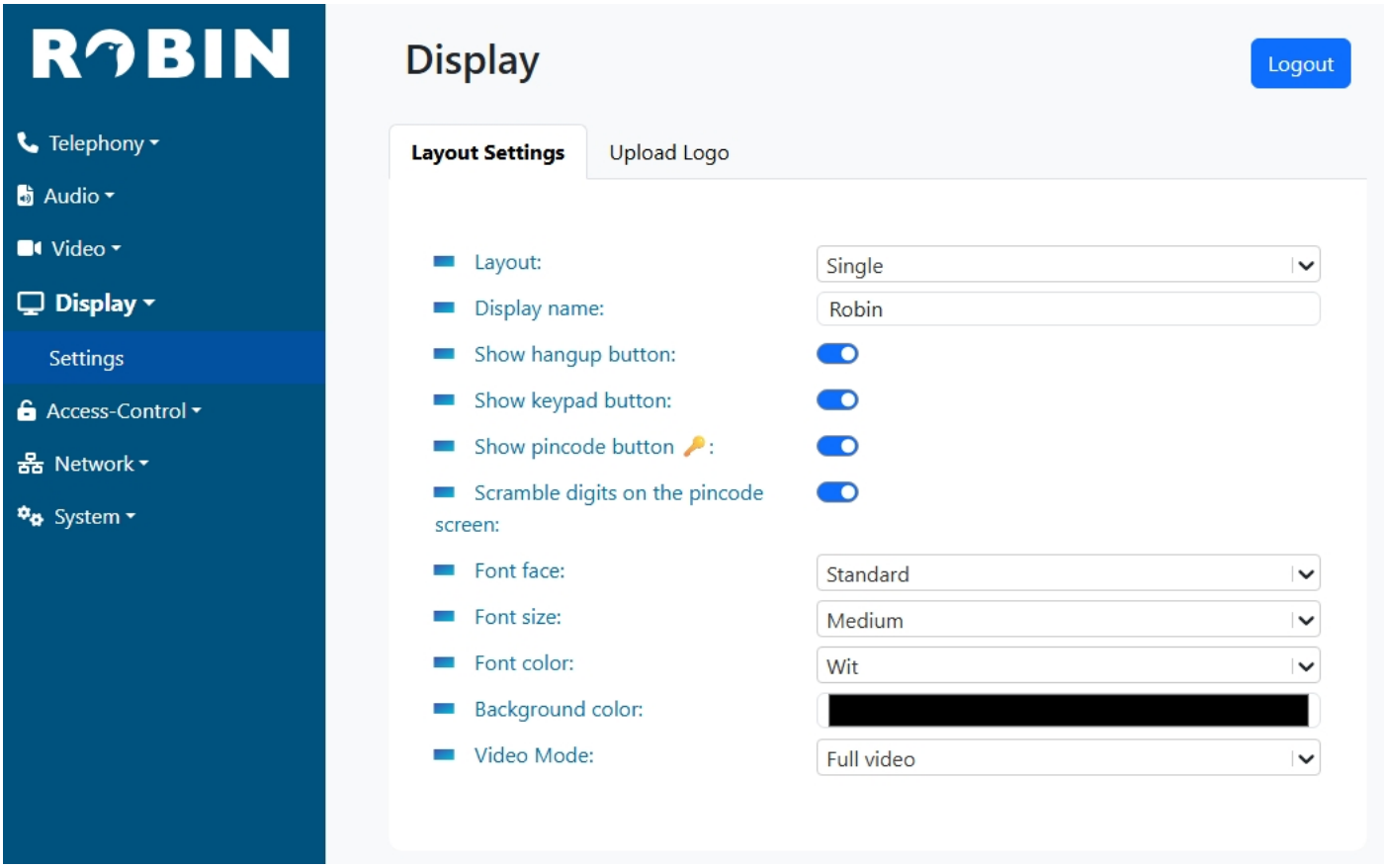
Whether the device is installed in a residential entrance, corporate lobby or high-end architectural environment, the touchscreen interface can be aligned with the aesthetic and operational needs of the location.

OVERVIEW

Images (left, right): Robin Touch: Scrambled pincode screen, Single button mode

[11] This function requires a device with touchscreen

SETTINGS



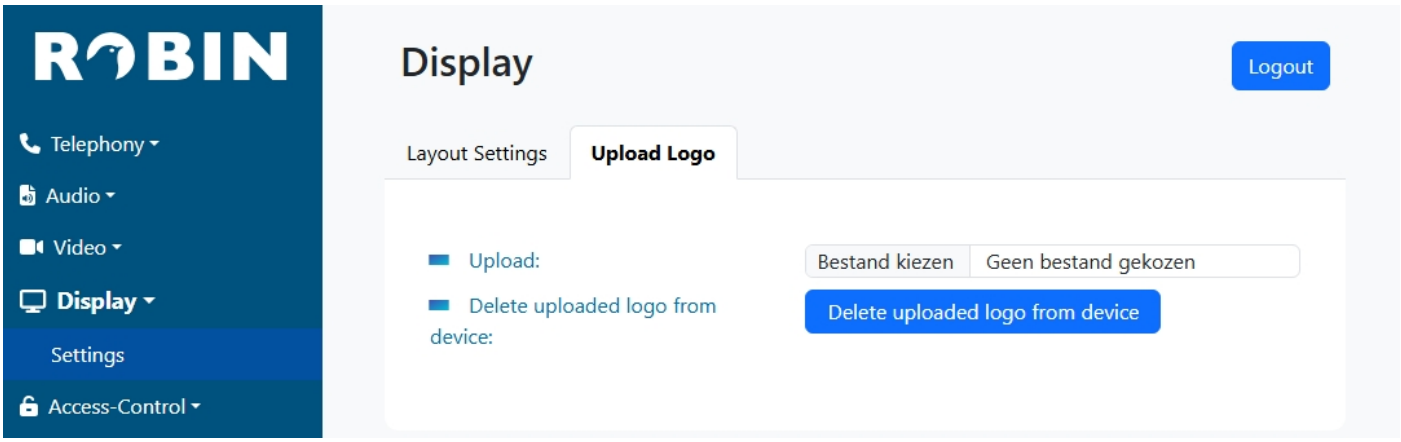
LAYOUT SETTINGS

The Layout Settings define the visual structure and interaction model of the touchscreen interface. These parameters allow the installer to align usability, readability and visual presentation with the specific environment in which the intercom is installed.

- Layout: Select the screen layout structure
  - Single (default): Displays one primary contact or interface element at a time. This configuration offers a clean and focused presentation, ideal for residential or single-tenant environments.
    In "Single Mode" (→ Overview) it will always show a pulsating call-button to allow a user-friendly access.
  - Multiple: Displays multiple contacts or selectable elements simultaneously. This layout is suited for multi-tenant buildings or installations requiring direct selection from a list, with swiping options and ability to upload a logo as button.
- Display name: Defines the name shown on the display. This can be used for branding, building identification or functional labelling
- Show hangup button: Enables or disables the on-screen hang-up control during a call session
- Show keypad button: Activates the keypad shortcut on the main screen, allowing users to manually enter a call number (→ Overview)
- Show pincode button: Displays a dedicated button for PIN code access. This function is typically used in access-controlled environments
- Scramble digits on the pincode screen: Randomizes the numeric keypad layout each time the PIN screen is opened. This enhances security by reducing the risk of code observation (→ Overview)

- Font face: Defines the typography style used across the interface
  - Classic: A traditional typeface offering a formal and neutral appearance
  - Standard (default): A modern and balanced font designed for optimal legibility in most environments
  - Handwritten: A more informal typeface, suitable for hospitality or residential contexts where a softer visual identity is desired
- Font size[12]: Adjusts text size for readability depending on mounting height and viewing distance
  - Extra small, Small, Medium (default), Large, Extra large
- Font color[13]: Defines the color of on-screen text
  - Black
  - White (default)
- Background color: Allows full customization of the interface background using the integrated color picker tool. This enables alignment with architectural finishes or corporate branding guidelines
- Video Mode: Determines how live video is displayed during operation
  - Full video: Displays the complete video feed within the screen boundaries. The entire image remains visible without cropping
  - Zoom to screen: Scales the video until the display is fully filled. The image is centered, and outer edges may be cropped to ensure a seamless full-screen presentation
  - No 2-way video: Disables the two-way video functionality on the device. Video transmission to the remote party remains unaffected if supported by the system configuration

UPLOAD LOGO



This section allows the installer to personalize the interface with a custom logo, reinforcing brand identity or site-specific presentation.

- Upload: Upload a logo file from a local device. Once applied, the logo will only show in Single Mode (For multiple logos, consult the paragraph Telephony → Phonebook)
- Delete uploaded logo from device: Removes the currently stored logo from the device

[12] Larger sizes are recommended for installations where the intercom is mounted higher or where accessibility considerations apply.
[13] The selected color should provide sufficient contrast with the chosen background color for optimal readability.

ACCESS CONTROL

The Access Control section allows you to configure secure entry using PIN codes directly on the intercom touchscreen. This functionality enables controlled access without requiring external readers or additional hardware.

Each entry can be individually defined and linked to the internal relay, allowing flexible configuration for residential, commercial or mixed-use environments. The system is designed to offer straightforward management while maintaining a professional and secure user experience.

For full-scale access control environments requiring advanced credential management, multi-door control, and audit logging, integration with a dedicated CDVI access control platform such as the Krypto system is recommended.

PIN

The Pin section provides an overview of all configured PIN entries. Each entry consists of an identification label and associated access behaviour.

In the overview section, the following items are displayed:

- ID: The unique identifier assigned to the PIN entry. This can represent a person, tenant, function or reference label
- Activate Internal Relay: Indicates whether the internal relay will be triggered when the corresponding PIN code is entered correctly.

From this overview, entries can be edited or removed, and new entries can be created.

ADDING A NEW ENTRY

Select Add new entry to create a new PIN configuration.

The following parameters can be defined:

- ID: Enter a unique name or reference for the PIN entry. This field is used for administrative clarity and does not appear on the public interface unless configured elsewhere
- Pin: Define the numeric access code that must be entered on the touchscreen keypad. It is recommended to use sufficiently complex codes to reduce unauthorized access risks
- Activate Internal Relay: Enable this option to trigger the internal relay when the correct PIN is entered. This typically unlocks the connected door or activates the configured output.

Once configured, select Apply Settings to store the entry.

EDITING AN ENTRY

Existing entries can be modified at any time. This allows:

- Updating the identification label
- Changing the PIN code (codes cannot be viewed)
- Enabling or disabling relay activation

Changes take effect after applying the updated settings.

DELETING AN ENTRY

Entries that are no longer required can be removed from the list. Deleting an entry immediately revokes access for the associated PIN.

OPERATIONAL BEHAVIOR

When the PIN keypad is enabled in the Display settings, users can enter their code directly on the touchscreen.

If the entered PIN matches a configured entry:

- The associated action is executed
- The internal relay is activated if enabled

If the PIN is incorrect, no action is taken.

SECURITY CONSIDERATIONS

For enhanced security, it is recommended to:

- Use unique PIN codes per user
- Avoid simple or repetitive number combinations
- Enable the scramble digits function in the Display settings to reduce observation risks
- Regularly review and remove unused entries

The integrated PIN access functionality is designed for controlled environments and standalone installations.

For projects requiring credential-based access, advanced user management, audit trails or multi-door scalability, the intercom can be seamlessly integrated with a full-scale CDVI access control system such as the Atrium or Centaur platform.

NETWORK

The Network section describes how the Robin intercom is connected to and communicates within an IP network. In this section, you can view and configure network parameters such as IP addressing, name resolution, and communication ports.

Correct network configuration is essential for stable operation, reliable connectivity, and proper interaction with telephony, video, and system services.

STATUS

The Status section provides a real-time overview of the intercom's network connection. This page is informational only; no settings can be changed here. It is intended to help installers verify connectivity and quickly diagnose network-related issues.

The MAC address (Media Access Control address) is a unique hardware identifier assigned to the network interface of the device. It consists of six pairs of hexadecimal characters and is globally unique. Network switches and routers use the MAC address to identify devices on a local network segment. This address cannot be modified.

The IPv4 information displays the device's current IP address, subnet mask, and gateway. The system supports both DHCP (automatic IP assignment by a router or DHCP server) and a fixed (static) IP configuration. When DHCP is enabled, the network automatically assigns the IPv4 settings. When using a fixed IP, the address is manually defined in the network configuration menu (see section "IP").

The Link State indicates the physical network connection status and speed. For example, "100 Mbps Full-Duplex" means the device is connected at 100 megabits per second and can send and receive data simultaneously. If no cable is connected or no link is detected, the link state will indicate this accordingly.

The IPv4 link-local address is an automatically generated address in the range 169.254.x.x. It is used when no DHCP server is available and no fixed IP is configured. This allows basic local communication between devices on the same network segment without requiring a router. Link-local addresses are not routable and cannot be used for communication outside the local network.

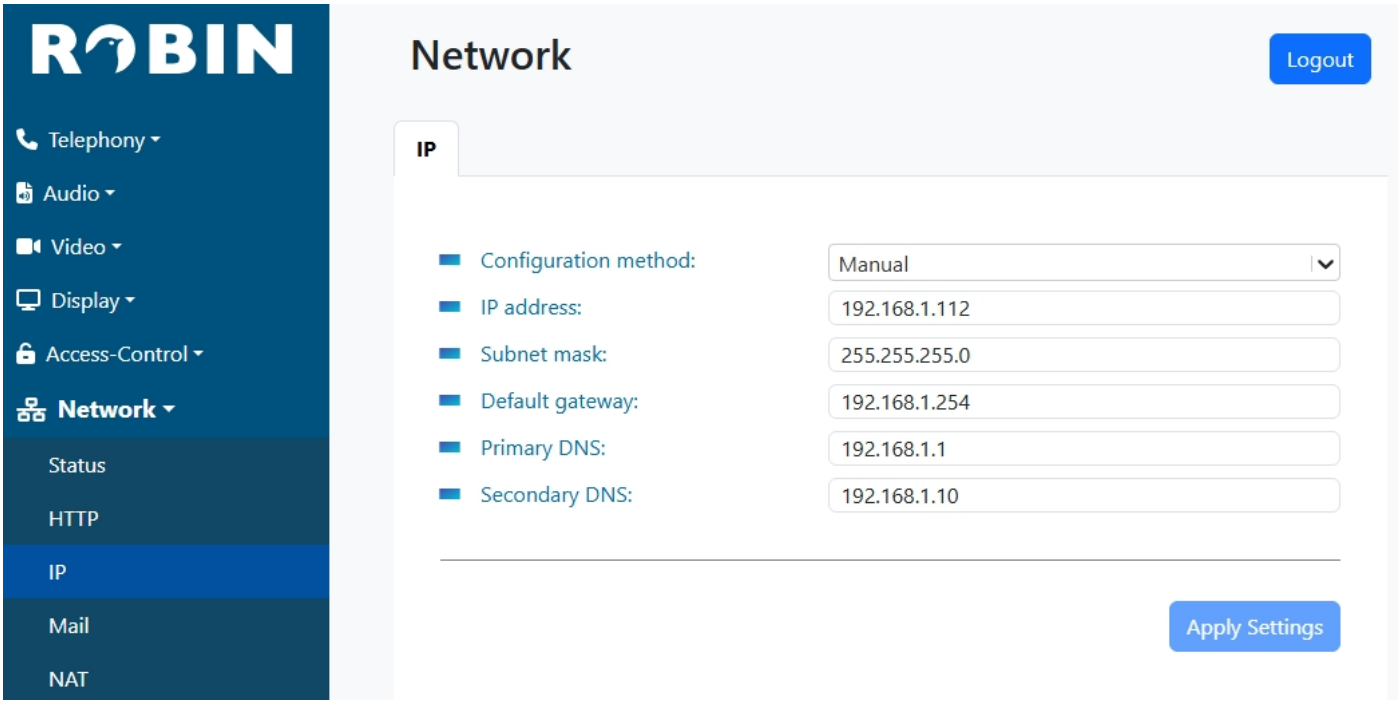
HTTP

The HTTP section allows you to configure how the intercom's web interface is accessed over the network. Here you can define the HTTP port used for standard web access. By default, HTTP typically uses port 80, but this can be adjusted if required by the network environment or security policy.

HTTPS can also be enabled in this section. When HTTPS is activated, you can define a separate HTTPS port (default is typically 443). HTTPS encrypts the communication between the user's browser and the intercom, ensuring that login credentials and configuration data are securely transmitted.

The system includes a self-signed certificate by default, allowing secure access without additional configuration. However, for professional or public-facing installations, it is recommended to use a trusted certificate issued by a recognized Certificate Authority. Certificates can be managed in the menu under System → Certificates. In that section, you can upload, install, and manage certificates that will be available for selection in the HTTPS configuration.

IP



The IP section allows you to configure how the intercom obtains its IPv4 network settings. You can choose between automatic configuration (DHCP) and manual configuration (static IP).

When DHCP is selected, the device automatically receives its IP address, subnet mask, default gateway, and DNS settings from a DHCP server on the network (usually a router or managed switch). This is the recommended setting for most standard installations, as it simplifies deployment and reduces the risk of address conflicts.

When Manual (static IP) is selected, the network parameters must be entered manually. The following fields are available:

- IP address: Defines the unique IPv4 address of the intercom within the local network. This address must be within the correct subnet and must not already be in use by another device.
- Subnet mask: Determines which part of the IP address identifies the local network and which part identifies the device. In most small to medium-sized networks, this is typically 255.255.255.0.
- Default gateway: Specifies the IP address of the router that provides access to other networks or the internet. Without a correct gateway, external communication (e.g. SIP servers, cloud services, email servers) may not function.
- Primary and Secondary DNS: DNS (Domain Name System) servers translate domain names into IP addresses. A primary DNS server is required for resolving hostnames. A secondary DNS server can be configured as a backup.

After making changes, click Apply Settings to activate the new configuration. Depending on the changes made, the device may temporarily become unreachable if the IP address has been modified.

MAIL

The Mail section allows the intercom to send email notifications, for example for events, system alerts, or integration purposes. This menu consists of three tabs: Server, Address Book, and Test.

SERVER

In the Server tab, you configure the outgoing mail server (SMTP). You must enter the server name, for example mail.provider.com. This is the address of the SMTP server that will handle outgoing emails.

You can also select the encryption method. The available options are None or TLS/SSL. For most modern mail servers, TLS/SSL is required to ensure secure communication between the intercom and the mail server. Make sure the selected encryption type matches the requirements of your mail provider.

ADDRESS BOOK

The Address Book tab allows you to create a list of predefined recipients. Each entry consists of a Name and an Address field, for example John and john.doe@domain.com. These entries can later be used when configuring event-based email notifications, reducing the need to manually re-enter email addresses.

Multiple lines can be added, allowing you to build a structured list of recipients for different purposes.

TEST

The Test tab allows you to verify the SMTP configuration. In the To field, you enter the email address to which the test message should be sent. After initiating the test, the system will attempt to send an email using the configured SMTP server.

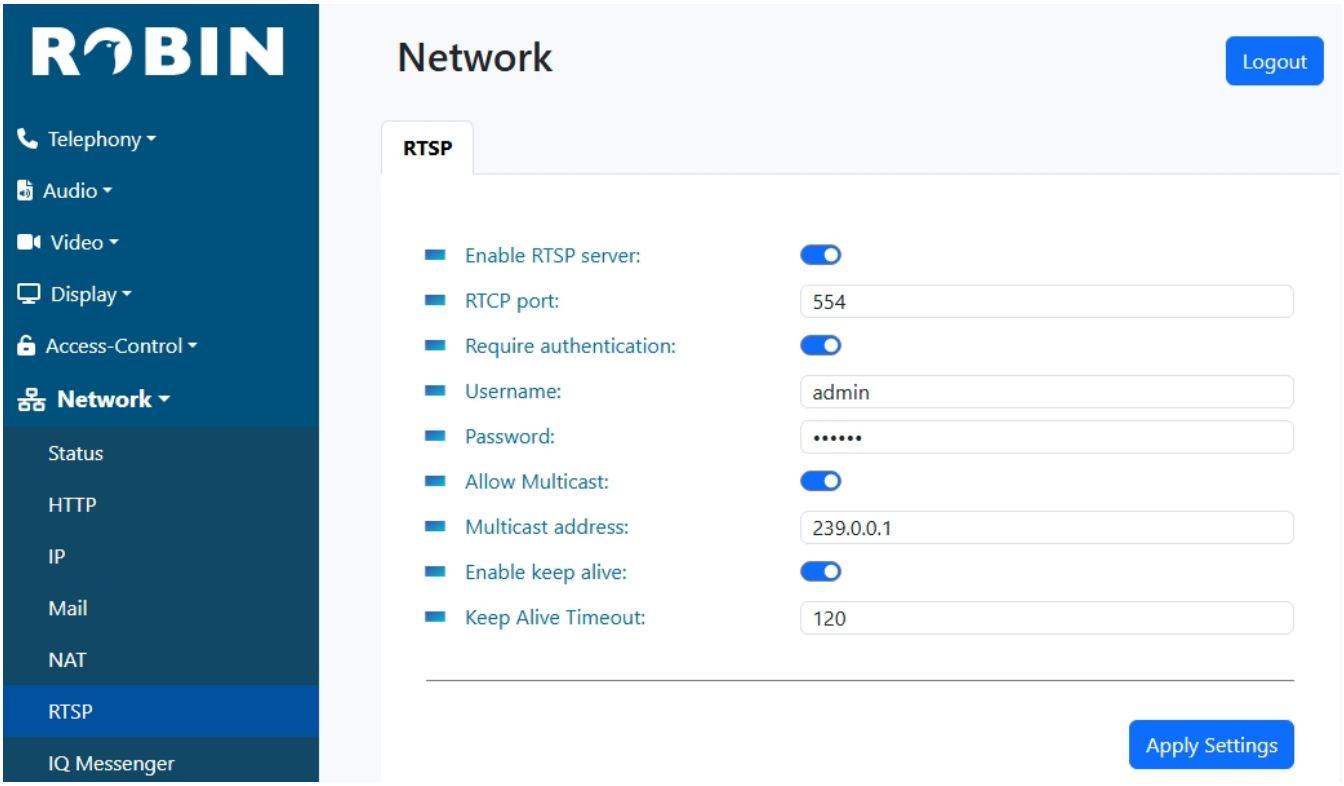
The SMTP test result is displayed on the same page, indicating whether the message was successfully sent or if an error occurred. This function is useful for validating server settings, encryption configuration, and network connectivity.

NAT

The NAT section allows you to enable or disable Network Address Translation (NAT) support for the intercom. NAT is typically used when the device is installed behind a router that translates private internal IP addresses to a public external IP address. In certain network environments, especially when using SIP or remote services, enabling NAT support may be required to ensure proper communication with external servers.

By default, NAT is disabled. In standard local network installations without specific routing or SIP requirements, no changes are usually necessary. After modifying the setting, press Apply Settings to store and activate the configuration.

RTSP



The RTSP section allows you to configure the Real-Time Streaming Protocol (RTSP) server of the intercom. By default, RTSP is disabled. When enabled, the device can provide a direct video stream to compatible video management systems (VMS), NVRs, or third-party applications. Once the RTSP server is enabled, the configuration options become available:

RTSP PORT

Defines the port used for the RTSP stream (default: 554). This is the standard port for RTSP communication. If required by the network policy, this port can be adjusted.

REQUIRE AUTHENTICATION

When enabled, access to the RTSP stream requires a username and password. This is strongly recommended to prevent unauthorized access to the video stream. The username and password fields are used to define the RTSP credentials.

ALLOW MULTICAST

When enabled, the video stream can be distributed using multicast addressing. This allows multiple clients to receive the same stream simultaneously without increasing the bandwidth load on the intercom. A multicast address (for example 239.0.0.1) must be defined. Multicast requires proper network support and configuration.

ENABLE KEEP ALIVE

The keep-alive function maintains the RTSP session by periodically sending control messages. The Keep Alive Timeout defines the interval (in seconds). This helps maintain stable connections, especially in networks where inactive sessions may be closed automatically.

After configuring the desired settings, press Apply Settings to activate the RTSP configuration.

IQ MESSENGER

The IQ Messenger section allows the Robin intercom to integrate with an IQ Messenger system. This integration enables the intercom to send event-based notifications, such as a doorbell press, to the IQ Messenger platform. Within IQ Messenger, these events can be routed, escalated, or distributed according to the configured workflow. Optionally, a callback function can be used to establish a return call from IQ Messenger to the intercom.

This page defines the connection parameters required for communication with the IQ Messenger server. The actual transmission of messages is typically triggered through the Event configuration, where IQ Messenger is selected as an action type.

SERVER URL

Defines the address of the IQ Messenger server. This is the endpoint used by the intercom to communicate with the IQ Messenger system. The URL is provided by the IQ Messenger system administrator.

USERNAME AND PASSWORD

These credentials are used to authenticate the intercom with the IQ Messenger server. The configured account must have the necessary permissions within the IQ Messenger environment.

MESSAGE TYPE

Specifies the type of message that will be sent to IQ Messenger. This value must correspond to a predefined message type within the IQ Messenger configuration. The message type determines how the event is processed and routed within the system.

DEVICE CODE

Identifies the intercom within the IQ Messenger platform. This unique code ensures that incoming messages are associated with the correct device and workflow.

CALLBACK NUMBER

Defines the number that IQ Messenger can use to initiate a return call to the intercom. This is typically a SIP registration number of the device. If the callback functionality is not used, this field may remain empty depending on the system configuration.

MESSAGE ID

Used to define a specific identifier for the message configuration. In most installations, this field can remain empty unless explicitly required by the IQ Messenger setup.

After entering the required parameters, press Apply Settings to store and activate the configuration. Proper setup should always be coordinated with the IQ Messenger administrator to ensure correct integration and workflow behaviour.

SYSTEM

The System section contains settings that affect the general operation and behavior of the Robin intercom. In this section, you can configure device identity, time and scheduling, security options, event handling, and system maintenance functions.

These settings control how the device operates on a daily basis and provide the tools required for monitoring, troubleshooting, and long-term management of the intercom.

DEVICE

The Device section provides general system information, device identification settings, and access to system logs. This menu is divided into three tabs: Info, Identity, and Logs.

INFO

The Info tab displays technical and operational information about the intercom. This page is informational only and cannot be modified.

The following details are shown:

- Product: Indicates the exact product model
- Serial Number: Displays the unique serial number of the device
- Software version: Shows the installed firmware version
- Software revision number: Indicates the internal software build reference
- Uptime: Displays how long the device has been running since the last reboot
- Load average: Shows the current system load
- CPU temperature: Displays the current processor temperature
- CPU speed: Indicates the processor speed
- Current time: Shows the current system date and time
- Runs: Indicates the number of system runs or restarts

This overview is useful for diagnostics, maintenance, and support purposes.

IDENTITY

The Identity tab allows you to define descriptive information for the intercom:

- Device name: Defines the name of the device. This name may be displayed in the web interface and can also be used in the video overlay if enabled in Video → Settings
- Device location: Defines the physical location of the intercom. This can also be shown in the video overlay when configured
- Device contact Allows you to enter contact information related to the installation, such as the installer or service provider

These fields help identify the device within larger installations or management systems.

LOGS

The Logs tab allows you to download the system log files. These logs contain diagnostic and operational information that can assist in troubleshooting.

When reporting issues to Robin support, it is recommended to download and include the system logs to facilitate analysis and problem resolution.

CLOCK

The Clock section allows you to configure the date and time settings of the intercom. Accurate time configuration is essential for event logging, video overlays, scheduling, and system synchronization.

- Time zone: Defines the geographical time zone in which the device is installed. Selecting the correct time zone ensures that the displayed time and scheduled events correspond to the local time, including automatic daylight saving adjustments where applicable
- Current time: Displays the current system date and time of the intercom
- Method: Indicates how the device obtains its time. When NTP (Network Time Protocol) is selected, the intercom automatically synchronizes its internal clock with a time server over the network
- NTP server address: Defines the address of the NTP server used for time synchronization, for example pool.ntp.org. This can be adjusted if a local or company-specific NTP server is required
- NTP status: Shows the current synchronization status, including the server with which the device is synchronized. This confirms whether the clock is correctly aligned with the selected NTP source

After making any changes, press Apply Settings to store and activate the configuration. For reliable operation, it is recommended to use NTP synchronization whenever a network connection is available.

EVENTS

The Events section allows you to create logic-based automation within the intercom. Events link a Source (what happens) to an Action (what the system must do). This flexible structure enables customized behaviour such as placing a call, activating a relay, sending notifications, or triggering other system functions. The menu consists of two tabs: Sources and Actions.

SOURCES

A Source defines the trigger condition, with other words: sources define when something happens, but they do not define what should happen. It represents an event detected by the system. The overview shows:

- Name: The identifier of the source
- Enabled: Indicates whether the source is active
- Triggered: Shows whether the source is currently triggered
- Source Type: Defines the type of trigger (for example Call, Motion, Audio detection, etc.)
- Duration: Defines the minimum time (in seconds) that the source will remain active after it has been triggered

When creating a new source, the following parameters are available:

- Source type: Selects the type of trigger
  - Audio: Triggered when the configured audio threshold and duration are exceeded (Audio → Detection)
  - Button: Triggered when a physical call button is pressed. This is the most commonly used source in standard doorbell configurations
  - Call: Triggered by call state changes. This can include call start, call connected, or call ended conditions depending on the configuration
  - DTMF: Triggers when a DTMF tone is received during an active call. The specific DTMF key is configurable
  - HTTP: Triggers when a specific URL is called. By default, the URL is http://<ip-address>/evmgr/emit. The endpoint "emit" is configurable. (Consult the section "HTTP" for more information)
  - Input1: Triggers when the physical input on the rear of the device is activated
  - Motion: Triggered when motion is detected within configured video detection zones (Video → Motion)
  - None:
  - Ring: Triggers when the intercom starts ringing
  - Timer: Triggers based on a timer interval. The event is activated every configured number of seconds. The interval is configurable
  - Busy: Triggers when an outgoing call receives a busy response
  - Preset[14]: Triggers when a preset is activated. This is only available when using a keypad or Robin Touch device. Configuration is available under Telephony → Phonebook → Keypad Dial Codes
  - Pincode[14]: Triggers when a valid PIN code is entered. This is only available when using a keypad or Robin Touch device. Configuration is available under Access Control
- Name: Defines a descriptive name
- Enable: Activates or deactivates the source
- Minimum duration: Defines how long the condition will remain active

[14] Only models that have a keypad or touchscreen

ACTIONS

An Action defines what the system must do when a Source is triggered.

The overview shows:

- Name: The action identifier
- Enable: Indicates whether the action is active
- Source: Defines which source triggers the action
- Edge: Defines the trigger condition. "Rising" means the action is triggered when the source becomes active
- Action type: Defines the type of action performed (for example Call, Relay control, IQ Messenger, etc.)
- Schedule: Defines whether the action is limited to a specific schedule

When creating a new action, the following parameters are available:

- Action Type: Selects the type of action to perform
  - Beep: Sounds a beep through the intercom speaker
    - Adds the item "Beep frequency" (default: 50)
  - Call: Will virtually trigger the call button on the device
  - Call Phonebook: Establish a call with someone in the Phonebook
    - Adds the item "Phonebook Entry" and "Allow call hangup"
  - HTTP: *Consult the paragraph "HTTP" in this section*
  - None: No action (e.g. testing)
  - Playback: Plays a sound from the library (Audio → Media)
  - Switch1: Triggers the internal relay
  - WebRelay: *Consult the paragraph "WebRelay" in this section*
  - MQTT: *Consult the paragraph "MQTT" in this section*
  - IQ Messenger: *Consult the paragraph "IQ Messenger" in this section*
- Name: Defines a descriptive name
- Enable: Activates or deactivates the action
- Source: Links the action to a previously defined source
- Trigger edge: Defines when the action is triggered (for example Rising)
- Schedule: Optionally links the action to a schedule defined in System → Schedules

By combining Sources and Actions, you can create customized workflows. For example, when the Call source is triggered (button pressed), the system can perform a Call action, activate a relay, send a notification, or trigger external integrations.

HTTP

The HTTP functionality within the Event Manager allows the intercom to communicate with external systems over a network. This enables integration with building management systems, access control platforms, home automation systems, healthcare platforms, or custom software solutions.

Using HTTP, the intercom can either respond to commands received from external systems or send notifications and data to external servers. This makes the device highly flexible and suitable for advanced automation scenarios.

Two different mechanisms are available: An HTTP Source allows an external system to trigger an event inside the intercom by calling a specific URL. An HTTP Action allows the intercom to send an HTTP request to an external server when a defined event occurs.

The following sections explain both mechanisms in detail.

SOURCES

The HTTP Source allows the intercom to be triggered by an external system through a web request. Instead of a physical event such as a button press, the trigger is generated by calling a specific URL on the intercom. When the configured HTTP path is accessed, the Event Manager treats it as a trigger and can execute linked Actions.

HOW IT WORKS

By default, the intercom listens for HTTP requests at:

http://<ip-address>/evmgr/emit

The word “emit” can be changed in the HTTP Path field. For example, if you configure the path as:

dooropen

The trigger URL becomes:

http://<ip-address>/evmgr/dooropen

When this URL is accessed from a browser, script, or external system, the HTTP Source becomes active.

CONFIGURATION FIELDS

- Source type: HTTP (select HTTP as the trigger type)
- Name: Assign a logical name such as “External Trigger” or “API Door”
- Enable: Must be enabled for the trigger to function
- HTTP Path: Defines the last part of the URL. This is the keyword that external systems must call
- HTTP Auth: When enabled, authentication is required before the trigger is accepted. This increases security and prevents unauthorized triggering
- Minimum duration: Defines how long the trigger must remain active. For HTTP triggers this is usually set to 0 or 1 second

PRACTICAL EXAMPLE

You can test this by opening a browser and entering:

http://192.168.1.50/evmgr/test (where 192.168.1.50 is the IP of the intercom)

If "test" is configured as the HTTP Path, the linked Action will execute immediately.

This makes it possible to integrate the intercom with building management systems, access control platforms, or custom automation software.

ACTIONS

The HTTP Action allows the intercom to send a web request to an external server when a Source is triggered. This is commonly used to notify third-party systems, trigger automation platforms, or communicate with external APIs.

In simple terms:

HTTP Source = external system triggers the intercom
HTTP Action = intercom triggers an external system

HOW IT WORKS

When the linked Source becomes active, the intercom sends an HTTP request to the configured URL. The request can be customized in terms of method, content type, and body content.

CONFIGURATION FIELDS

- Action type: HTTP (select HTTP as the action type)
- Name: Assign a logical name such as "Notify Server" or "Webhook Call"
- Enable: Must be enabled to function
- Method: Defines the HTTP method
  - GET is typically used for simple URL calls
  - POST is used when sending structured data (recommended for API integrations)
- Content type: Defines the format of the message body
  Common values:
  - application/json
  - application/x-www-form-urlencoded
  - text/plain
- Start URL: The destination URL that will receive the request.
  Example: https://example.com/api/doorbell
- Start body: Defines the content that will be sent in the request (mainly used with POST)
  Example JSON body:

```
{
        "device": "FrontDoor",
        "event": "button_pressed"
}
```

- Use HTTP auth: If enabled, the intercom will use configured credentials when sending the request
- Source: Select the Source that triggers this HTTP Action
- Trigger edge: Usually set to Rising to prevent duplicate calls
- Schedule: Optionally restrict the action to certain time periods

PRACTICAL EXAMPLE

If you want the intercom to notify a home automation server when the button is pressed:

- Create a Button Source
- Create an HTTP Action
- Set Method to POST
- Set Content type to application/json
- Enter the server URL
- Add a simple JSON message.

Each time the button is pressed, the external server receives a notification.

WEBRELAY

The WebRelay function allows the intercom to control an external relay module over the network. This makes it possible to operate doors, gates, barriers, or other electrical devices without using the built-in relay of the intercom. This is a standalone PoE network device that provides one or more relay outputs which can be controlled via HTTP commands. When properly configured, the intercom can send a command to the WebRelay whenever a defined event occurs.

Before configuring the WebRelay inside the Event Manager of the intercom, the WebRelay device itself must first be correctly installed and configured on the network. This ensures stable communication and secure operation.

The following section explains how to configure the WebRelay device.

WEBRELAY-SIDE

Before configuring the WebRelay inside the intercom Event Manager, the WebRelay device itself must be properly configured. This ensures reliable communication between the intercom and the relay module.

ASSIGN A FIXED IP ADDRESS

The WebRelay must use a fixed (static) IP address. If the IP address changes, the intercom will no longer be able to control the relay. Open the WebRelay interface in a browser and navigate to the Network section (http://<ip>/setup.html, default user: admin / password: webrelay)

Configure:

- IP Address: Set a fixed IP address within the same network range as the intercom
- Netmask: Configure according to your network (typically 255.255.255.0)
- Gateway: Set the correct gateway of the local network
- TCP Port: Default is usually 80. Only change this if required by the network configuration
- Modbus Port: Only required when using Modbus communication. For standard HTTP control this can remain unchanged

After changing network parameters, reboot the WebRelay for the settings to take effect.

It is recommended to reserve this IP address in the DHCP server or configure it outside the DHCP range to prevent conflicts.

CONFIGURE PROTECTED ACCESS

For security reasons, it is strongly recommended to protect the WebRelay with a username and password.

Navigate to the Password section.

Configure:

- Username: Define a login username
- Password: Define a strong password

Save the settings.

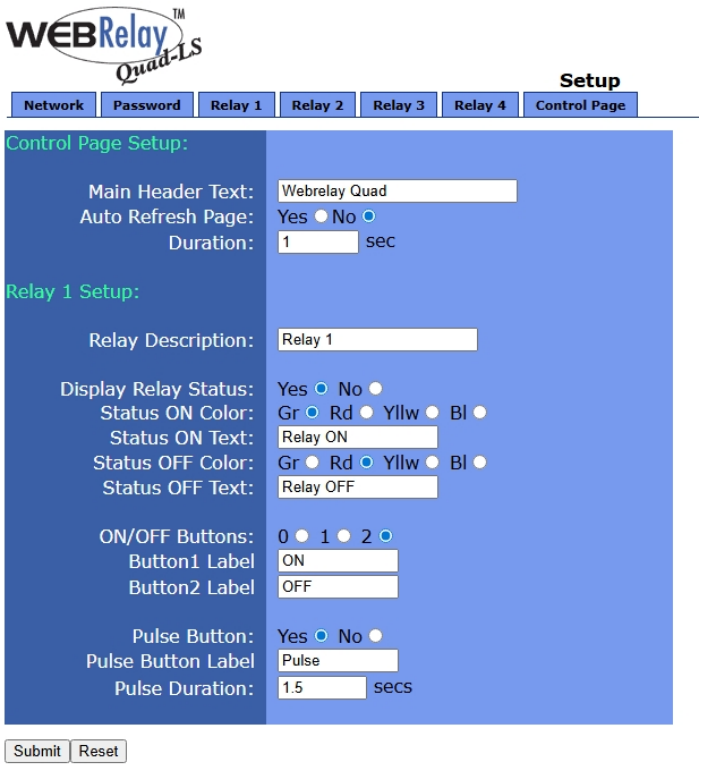
These credentials will later be entered in the WebRelay Action configuration inside the intercom. If authentication is not configured, anyone with network access could potentially operate the relay.

WIRING DEVICE AND CONFIGURE THE RELAY OUTPUT

The WebRelay provides potential-free (dry contact) relay outputs. Each relay typically has three terminals:

- C (Common)
- NO (Normally Open)
- NC (Normally Closed)

The correct wiring depends on the type of lock or device being controlled.



For an electric strike or gate controller that should only activate when triggered (fail-secure / working current), connect the circuit through C and NO. In this configuration, the contact closes only when the relay is activated.

For a fail-safe lock (resting current lock) that must remain energized to stay locked and release when power is interrupted, connect the circuit through C and NC. In this configuration, the contact opens when the relay is activated.

Always verify the lock type before wiring. Using the wrong contact (NO instead of NC or vice versa) may result in inverted behaviour. The relay contact itself does not provide power. It only switches the connected circuit. The external power supply for the lock or gate must be wired through the relay contact according to the installation requirements. Ensure that the electrical ratings of the relay (voltage and current) are not exceeded. Each relay must be configured according to the intended application.

Navigate to the Relay section (Relay 1, Relay 2, etc.).

Configure:

- Relay Description: Assign a logical name, such as “Front Door” or “Gate”
- Display Relay Status: Optional. Can be enabled for easier visual monitoring
- ON/OFF Buttons: Leave enabled unless a specific control mode is required
- Pulse Button: Enable pulse mode if the relay must operate momentarily (recommended for door strikes)
- Pulse Duration: Define the activation time in seconds
    - For electric door strikes, a duration between 1 and 5 seconds is typical
    - For access control applications, pulse mode is generally recommended instead of permanent ON/OFF control

This completes the configuration on the WebRelay side. Proceed with the configuration of the intercom device.

ROBIN INTERCOM-SIDE

After the WebRelay device has been configured with a fixed IP address and secured with a password, it can be linked to the intercom via the Event Manager.

System → Events → Actions

- Create a new Action and select WebRelay as the Action Type.

WEBRELAY ACTION CONFIGURATION

- Action Type: Select WebRelay
- Name: Assign a logical name, such as "Open Front Door" or "Gate Pulse"
- Enable: Enable the action to activate it
- Web relay IP address: Enter the fixed IP address configured in the WebRelay device
  Example: 192.168.1.99
- Relay: Select the relay number you want to control (Relay 1, Relay 2, etc.)
- Action: Choose the relay operation
  - Pulse: Activates the relay for a defined duration. This is recommended for door strikes and access control
  - On: Switches the relay permanently on until another action switches it off
  - Off: Switches the relay off

  For most access control applications, Pulse is recommended.

- Duration: Define the activation time in seconds when using Pulse mode.
  Typical values for electric strikes are between 1 and 5 seconds
- Use authentication: Enable this option if the WebRelay device is protected with a username and password
- Password: Enter the password configured in the WebRelay device
- Source: Select the Source that should trigger the relay
  Example: Button-1
- Trigger edge: Typically set to Rising to ensure the relay is activated only once when the Source becomes active
- Schedule: Optionally restrict the relay activation to specific days or time periods

EXAMPLE CONFIGURATION

If the goal is to open a door when the call button is pressed:

- Create a Button Source
- Create a WebRelay Action
- Enter the WebRelay IP address
- Select Relay 1
- Choose Pulse
- Set Duration to 2 seconds
- Link the Action to the Button Source
- Set Trigger edge to Rising

Each time the button is pressed, the intercom sends a command to the WebRelay, which activates the selected relay.

IMPORTANT NOTES

The intercom does not directly switch power. It sends a network command to the WebRelay. Therefore:

• The WebRelay must be reachable on the network

• The IP address must remain fixed

• Authentication settings must match the WebRelay configuration

If the WebRelay is unreachable, the relay will not activate. Ensure network connectivity before troubleshooting the Event configuration.

MQTT

The MQTT Action allows the intercom to publish a message to an MQTT broker when a defined event occurs. This enables integration with home automation systems, building management systems, IoT platforms, or custom software environments. MQTT is a lightweight messaging protocol commonly used in IoT environments. The intercom acts as an MQTT client and sends (publishes) a message to a specific topic on a configured MQTT broker.

MQTT is only available as an Action. There is no MQTT Source type.

CONFIGURATION IN THE INTERCOM

Navigate to: System → Events → Actions (if not already done so)

Create a new Action and select MQTT as the Action Type.

MQTT ACTION CONFIGURATION

- Action Type: Select MQTT
- Name: Assign a logical name, such as "Notify Automation" or "Doorbell MQTT"
- Enable: Enable the action to activate it
- Host: Enter the IP address or hostname of the MQTT broker
  Example: 192.168.1.100 or mqtt.example.local
- Port: Enter the MQTT broker port
  Default MQTT port is 1883
  If TLS is used (if supported), the default is typically 8883
- Topic: Define the MQTT topic where the message will be published
  Example: building/frontdoor/button
  Topics are case-sensitive and follow a hierarchical structure using forward slashes
- Message: Enter the message payload that will be sent when the Source is triggered
  This can be plain text or JSON
  Example (simple text):
  pressed
  Example (JSON format):

```
{
        "device": "FrontDoor",
        "event": "button_pressed"
}
```

- QoS: Defines the Quality of Service level:
  0 – Message is sent once, without confirmation
  1 – Message is delivered at least once (recommended)
  2 – Message is delivered exactly once
  For most integrations, QoS level 1 is recommended
- Use authentication: Enable this option if the MQTT broker requires username and password authentication
- Source: Select the Source that should trigger the MQTT message
  Example: Button-1, Motion, Call, etc.
- Trigger edge: Typically set to Rising to avoid duplicate messages
- Schedule: Optionally restrict publishing to certain days or time periods

EXAMPLE CONFIGURATION

If you want to notify a home automation platform when the doorbell is pressed:

- Create a Button Source
- Create an MQTT Action
- Enter the MQTT broker IP address
- Set port to 1883
- Define topic: home/frontdoor/doorbell
- Set message: pressed
- Set QoS to 1
- Link the Action to the Button Source
- Set Trigger edge to Rising

Each time the button is pressed, the MQTT broker receives the message, and the automation system can react accordingly.

IMPORTANT NOTES

The intercom does not store MQTT messages if the broker is unreachable. If the MQTT server is offline, the message will not be delivered.

Ensure:

• The MQTT broker is reachable from the intercom network

• The port is open and not blocked by a firewall

• Authentication settings match the broker configuration

MQTT enables seamless integration with modern automation and IoT platforms without requiring complex HTTP scripting.

IQ MESSENGER

IQ Messenger is a platform commonly used in healthcare environments. It is an IoT-based system where all devices are connected to the network and caregivers receive notifications on a wearable device and in the IQM application.

When integrating an intercom with IQM, the device does not operate in the standard calling mode. Instead of directly initiating a SIP call when the button is pressed, the intercom sends an HTTP message to the IQM server. IQM processes this message and distributes the notification within its system.

In the IQM environment, a device must first be created. For example, a device code such as "robin000001" can be defined. This code is used in the HTTP message so IQM can identify which intercom is sending the event. The device must also be linked to a type, typically "Bell1", so that IQM recognizes it as a doorbell event.

The IQM platform usually includes a SIP server, often based on Asterisk. If required, the IQM application can initiate a SIP call back to the intercom using a configured callback extension.

CONFIGURATION IN THE INTERCOM

The integration is configured under System → Events.

First, create a Source. In most cases, this will be the physical call button. The Source should be enabled and configured with a minimum duration, typically one second. The Source only detects the button press; it does not contain the IQ Messenger logic itself.

Next, create an Action of type IQ Messenger. Assign a name of your choice and enable the action. Select the previously created button Source, set the trigger edge to Rising, and leave the schedule open unless a specific time restriction is required. The Rising edge is important to prevent duplicate messages when the button is released.

Within the IQ Messenger action, configure the following parameters: the Type must match the type configured in IQM, typically Bell1; the Device code must exactly match the code created in the IQM environment; the Message defines the text that will appear in the IQM application; the Callback can contain a SIP extension for return calls; the Start URL must contain the full IQM server endpoint; and the Username and Password must correspond to the IQM API credentials.

TECHNICAL OPERATION

When the configured Source is triggered, the intercom sends an HTTP POST request to the IQM server. Authentication is performed using Basic Authentication with the configured username and password. The request contains the device code, event type, message text, and optional callback extension.

If the IQM server is unreachable, the intercom continues to operate normally. The IQ Messenger action does not block the device or interfere with other configured functions.

DIFFERENCE FROM STANDARD OPERATION

In a standard configuration, pressing the button immediately initiates a SIP call from the intercom.

With IQ Messenger integration, pressing the button generates an HTTP event that is sent to IQM. IQM determines how the event is handled and which caregiver receives the notification. If a call is required, it is initiated from the IQM environment rather than directly by the intercom.

SECURITY

The Security section allows you to configure authentication, token-based access, and API access to the intercom. This menu consists of three tabs: Authentication, Tokens, and API.

AUTHENTICATION

The Authentication tab defines how users can access the web interface and manage the device.

- Require authentication: When enabled, users must log in with valid credentials to access the web interface. It is strongly recommended to keep this option enabled to prevent unauthorized access
- Admin username and Admin password: Defines the administrator account credentials. The administrator has full access to all configuration settings. The password can be changed to ensure secure operation
- User enabled: Enables a secondary user account with limited permissions
- User username and User password: Defines the credentials for the user account. This account can be used for restricted access, depending on the configuration
- User account locked: When enabled, the user account is locked and cannot be used for login
- User can control door opener: When enabled, the user account is allowed to activate the door opener. If disabled, door control is restricted to the administrator account
- Allow HTTP access only from LAN: When enabled, access to the web interface is restricted to devices within the local network. This increases security by preventing direct remote HTTP access from external networks

After modifying authentication settings, press Apply Settings to activate the changes.

TOKENS

The Tokens tab allows you to create and manage authentication tokens for secure communication with external systems or applications.

You can add a new token by selecting Add new entry and entering a name or description. Each token can be individually enabled or disabled using the toggle button. Tokens provide an alternative to username/password authentication for API or system integrations.

API

The API tab allows you to enable or disable API access to the intercom.

When API access is enabled, external systems can communicate with the device using the available API interface, subject to authentication and security settings. If not required, it is recommended to keep API access disabled to reduce the attack surface.

CERTIFICATES

The Certificates section allows you to manage SSL/TLS certificates used by the intercom for secure HTTPS communication and other encrypted services. This menu consists of two tabs: Certificates and CSR.

CERTIFICATES

The Certificates tab provides an overview of all installed certificates on the device.

For each certificate, the following information is displayed:

- Name: The identifier of the certificate
- Status: Indicates whether the certificate and private key are correctly installed and valid
- Valid: Shows whether the certificate is currently valid

Additional details can be viewed by opening the certificate information. This includes technical data such as:

- Subject: The entity to which the certificate is issued
- Version: The certificate version
- Serial number: The unique identifier assigned to the certificate
- Signature algorithm: The algorithm used to sign the certificate (for example SHA256 with RSA encryption)
- Public key algorithm: Indicates the type of public key used
- Issuer: The authority that issued the certificate
- Not valid before / Not valid after: Defines the certificate validity period
- SHA1 fingerprint: A unique fingerprint used to verify the certificate

By default, the system includes a self-signed certificate. This allows secure HTTPS access without additional configuration. For production environments, it is recommended to install a certificate issued by a trusted Certificate Authority to avoid browser security warnings.

CSR

The CSR (Certificate Signing Request) tab allows you to generate a certificate signing request. This is used when requesting a trusted certificate from a Certificate Authority.

The following parameters must be defined:

- Name: Internal name for the certificate request
- Key length: Defines the length of the generated key (for example 2048 bits)
- Digest: Specifies the hashing algorithm used for the request (for example sha256)
- Common Name (CN): The fully qualified domain name (FQDN) of the device, for example intercom.company.com
- Department (OU): Organizational unit within the company
- Organization (O): Company or organization name
- Location (L): City or locality
- State/Province (ST): State or province
- Country (C): Two-letter country code
- E-mail Address: Administrative contact email address.

After completing the required fields, select Generate CSR to create the certificate signing request. The generated CSR can then be submitted to a Certificate Authority to obtain a signed certificate, which can subsequently be installed on the device.

SCHEDULES

The Schedules section allows you to define time-based schedules without predefined limits that can be used in combination with events and other system functions. Schedules are typically used to activate or restrict certain actions during specific days and time periods.

The main page provides an overview of all configured schedules. You can create a new schedule by selecting Add new entry.

When creating or editing a schedule entry, the following fields are available:

- Name: Defines a description for the schedule. This helps identify its purpose within the system
- Day: Specifies on which day(s) the schedule applies. The available options are:
    - All: Applies every day of the week
    - Weekdays: Applies from Monday to Friday
    - Weekend: Applies on Saturday and Sunday
    - Monday through Sunday: Allows selection of a specific individual day
- From: Defines the start time of the schedule
- To: Defines the end time of the schedule

The schedule becomes active only within the defined time range on the selected day(s). Outside this time window, the schedule is inactive. After entering the required information, press Apply Settings to store the schedule.

Configured schedules can be referenced in other sections of the system, such as System → Events, to control when certain actions are allowed or executed.

SOFTWARE

The Software section allows you to manage firmware updates, configuration backups, and system maintenance functions. This menu consists of three tabs: Updates, Backup, and Tools.

UPDATES

The Updates tab allows you to check for new software versions.

- Check for new software versions: Initiates a check to determine whether a newer firmware version is available
- Current version: Displays the firmware version currently installed on the device
- Available version: Displays the latest firmware version available for installation, if applicable

Keeping the device updated ensures optimal performance, security improvements, and access to the latest features.

Software updates are checked automatically so the system can detect when a new version is available and inform the administrator. However, installation must be performed manually to ensure that updates are applied in a controlled manner, at a suitable time, and with minimal disruption to operation. This prevents unexpected reboots or temporary service interruptions during critical use.

BACKUP

The Backup tab allows you to manage configuration backups.

You can download the current system configuration as a backup file (backup.txt). This file contains the device settings and can be stored securely for future use. You can also upload a previously saved backup file to restore the configuration. This is useful when replacing a device or restoring settings after a reset.

TOOLS

The Tools tab provides maintenance functions.

- Reboot device: Restarts the intercom. This may be required after certain configuration changes or for troubleshooting purposes
- Restore application defaults: Resets the device configuration to factory default settings. All custom settings will be lost. It is recommended to create a backup before performing a reset.

These tools provide basic system management and recovery options.

RELAY

The Relay section allows you to manually control and configure the relay output of the intercom. This relay is typically used to control an electric strike, magnetic lock, or other access control device. The menu consists of two tabs: Control and DTMF.

CONTROL

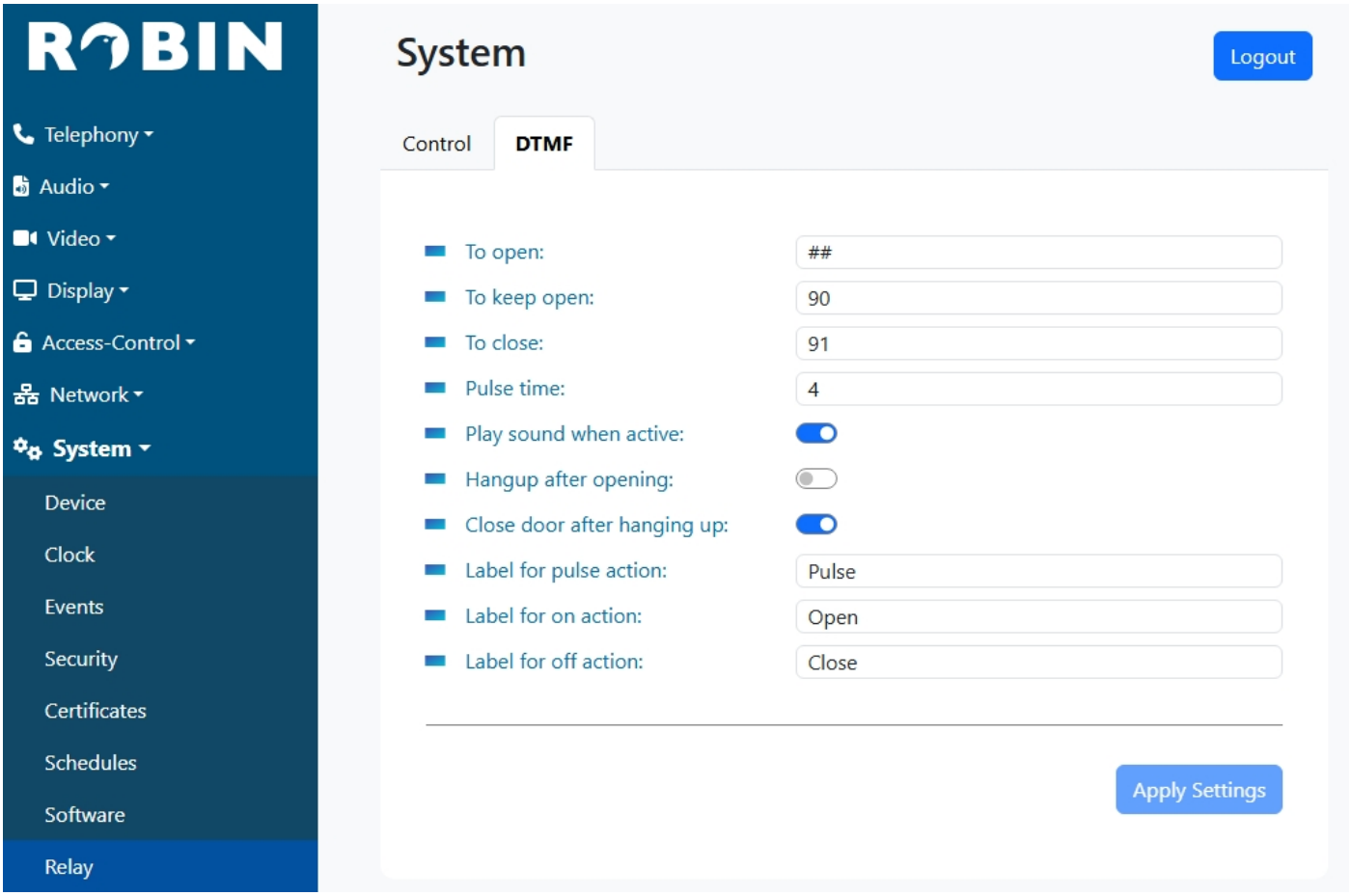
The Control tab provides direct manual control of the relay.

- Status: Displays the current state of the relay (Open or Close)
- Close: Sets the relay to the closed state
- Open: Sets the relay to the open state
- Pulse: Activates the relay for a defined pulse time (set in the DTMF tab) and then automatically returns it to its default state. This is commonly used to momentarily unlock a door

This tab is mainly used for testing and commissioning during installation.

DTMF

The DTMF tab allows configuration of relay control during a SIP call using DTMF (Dual-Tone Multi-Frequency) tones entered on a telephone keypad.



- To open: Defines the DTMF code required to activate the relay
- To keep open: Defines the DTMF code that keeps the relay continuously active
- To close: Defines the DTMF code that deactivates the relay
- Pulse time: Defines the duration (in seconds) of the relay pulse when the open command is used
- Play sound when active: When enabled, an audible confirmation sound is played when the relay is activated
- Hangup after opening: If enabled, the call is automatically terminated after the relay is activated
- Close door after hanging up: When enabled, the relay automatically returns to the closed state after the call ends
- Label for pulse action: Defines the label used in the interface for the pulse action
- Label for on action: Defines the label used for the open action
- Label for off action: Defines the label used for the close action

After modifying the settings, press Apply Settings to store and activate the configuration.

DEBUG

The Debug section provides advanced diagnostic tools intended for troubleshooting and technical support. This menu consists of two tabs: Trace and Go to Robin.

TRACE

The Trace tab allows you to capture network traffic for analysis.

- Status: Displays the current state of the trace function
- Trace duration: Defines the duration (in seconds) for which the network trace will run
- PCAP filter line: Allows you to define a capture filter to limit the recorded traffic to specific protocols, ports, or IP addresses. This helps reduce file size and focus on relevant data
- Start: Begins the trace capture process. The captured data can be used for advanced diagnostics and may be requested by technical support

This function is primarily intended for installers or support engineers familiar with network analysis tools.

GO TO ROBIN

The Go to Robin tab allows the creation of a secure remote connection between the intercom and Robin support.

- Connect: Establishes a secure VPN tunnel to Robin. Once connected, a Robin technician can access the device remotely for diagnostics and support
- Status: Displays the current connection state

The VPN tunnel is initiated outbound from the intercom, meaning no inbound ports need to be opened on the local network. This ensures that the local network remains protected and that remote access is only possible when explicitly initiated.

This function should only be enabled when remote support is required and can be disconnected once troubleshooting is completed.

LIGHTING[15]

The Lighting section allows you to configure the illumination of the device. This includes the backlight of the name tag or display and the ambient lighting positioned above and below the intercom. The menu consists of two tabs: Base and Ambient.

BASE

The Base tab contains the lighting settings for the name tag backlight or the display brightness, depending on the device model. Here you can adjust the brightness level to ensure optimal visibility under different lighting conditions. This allows the installer to balance readability and energy efficiency, while avoiding excessive brightness during low-light conditions.

AMBIENT

The Ambient tab controls the integrated ambient lighting. This is the lighting located above and below the device, designed to illuminate the person standing in front of the intercom or to subtly light the surrounding façade.

- Current lamp mode: Displays the current active lighting mode
- Day: Defines the brightness level of the ambient lighting during daytime conditions
- Night: Defines the brightness level during nighttime conditions
- Call: Defines the brightness level when the call button is pressed. This allows the lighting to intensify during interaction, improving visibility for the camera and enhancing user feedback
- Lamp mode override: Provides a dropdown menu with the options Off, Day, Night, and Call. This function allows manual override of the lighting mode for testing and installation purposes.

The override is typically used during commissioning to verify brightness levels and visual effect without waiting for environmental light changes or triggering a call event.

[15] On models with ambient lighting

SUPPORT

For technical assistance, installation guidance or troubleshooting support, always contact CDVI Support first.

As the official manufacturer and system partner, CDVI provides dedicated assistance for product integration, access control configuration and combined intercom solutions. This ensures a coordinated and efficient resolution process.

USING CDVI SUPPORT PORTAL

The CDVI Support Portal provides structured technical assistance for professional installers and integrators.

Through the portal, you can:

- Submit technical support requests via a ticketing system
- Track the status and progress of your cases
- Access documentation, manuals and how-to guides
- Obtain assistance for system integration and configuration

Support availability may vary by country. Please consult the CDVI website relevant to your region for local contact details and support options.

When submitting a request, include the product type, serial number, system configuration details and, where possible, screenshots or log files. Providing complete information allows for faster and more precise assistance.

CDVI Support should always be your first point of contact for installation, integration and system-related matters.

USING ROBIN SUPPORT PORTAL

For product-specific information related to Robin intercom hardware or software functionality, the Robin Support Portal is available as an additional resource.

The portal provides:

- A knowledge base with technical articles and documentation
- Software and firmware information
- Product-specific support guidance

In cases where advanced manufacturer-level assistance is required, CDVI Support will coordinate directly with Robin to ensure a streamlined resolution. For efficient handling of your request, always initiate support through CDVI before contacting the Robin portal independently.

DEFINITIONS

Term	*Explanation*
AC (voltage)	Alternating Current. In an intercom system, this refers to the type of electrical voltage that a relay can switch or control, where the current periodically changes direction, typically used for door strikes, locks, or other access devices.
API	Application Programming Interface. A defined set of rules and endpoints that allows external systems or applications to interact with the intercom or VoIP device for configuration, control, monitoring, or data exchange.
Authentication token	A secure, time-limited digital credential used by an intercom or VoIP system to verify identity and authorize access to services or APIs without repeatedly transmitting usernames and passwords.
Bitrate	The amount of data transmitted per second in an audio or video stream, typically measured in bits per second; higher bitrate generally results in better quality but requires more network bandwidth.
Certificate (SSL)	A digital certificate used in intercom and VoIP systems to verify the identity of a device or server and enable encrypted communication, ensuring secure connections for services such as HTTPS and TLS.
Codec	A method or algorithm used to encode and decode audio or video data for transmission and playback, typically optimizing bandwidth usage while maintaining acceptable media quality.
CSR	Certificate Signing Request. A file generated by an intercom or VoIP device that contains its identification information and public key, used to request a trusted SSL/TLS certificate from a certificate authority.
DC (voltage)	Direct Current. In an intercom system, this refers to the type of electrical voltage that a relay can switch or supply, where the current flows in a single direction, commonly used for door locks, access control devices, and electronic components.
DHCP	Dynamic Host Configuration Protocol. A network protocol that automatically assigns IP addresses and other network configuration parameters (such as subnet mask, gateway, and DNS servers) to devices on an IP network.
DNS	Domain Name System. A service that translates domain names into IP addresses, allowing the intercom to locate servers such as SIP or update servers.
DNSsvr	Domain Name System server. A server that resolves human-readable domain names into IP addresses and may also provide service records used for locating network services.
Dry contact (potential-free)	A relay contact in an intercom system that does not supply its own voltage, acting only as a simple open/close switch to control external devices, allowing the use of separate AC or DC power sources.
DTMF	Dual-Tone Multi-Frequency. A signaling method that uses keypad tones to represent digits and commands, allowing users to send control input through the intercom system during a call.

DTMF event payload	A media payload transmitted in RTP that represents keypad digits as signaling events rather than audio tones, allowing reliable detection of user input in intercom and VoIP systems.
Extension	A unique internal number or identifier assigned to an intercom or user, used to route calls and communications within the system.
G.711 (A-law, μ-law)	A standard audio codec used in telephony that encodes voice using pulse code modulation; A-law and μ-law are two companding variants used in different regions, providing low latency and compatibility with traditional phone systems.
G.722	A wideband audio codec that provides higher voice quality than standard telephony codecs by using a wider audio frequency range, typically used for high-definition voice communication.
Gateway	A network device, typically a router, that provides a path for the intercom to communicate with devices outside its local network.
H264	A video compression standard used to encode and decode video streams efficiently, providing good image quality at relatively low bitrates.
H264 payload type	An identifier used in RTP streams to indicate that the carried media data is encoded using the H.264 video codec, enabling the receiving device to correctly interpret and decode the video stream.
HDR	High Dynamic Range. A video feature that increases the range between the darkest and brightest parts of an image, improving detail and color accuracy, but typically requiring more processing power and data compared to standard video.
Host	A device or system on a network that has an IP address and can send or receive data.
HTTP	Hypertext Transfer Protocol. A communication protocol used by intercom and VoIP devices to access web-based interfaces and services, such as device configuration, status monitoring, and firmware updates.
HTTPS	Hypertext Transfer Protocol Secure. A secure version of HTTP used by intercom and VoIP devices to access web interfaces and services with encrypted communication, protecting configuration data and credentials from unauthorized access.
Inband STUN	A method where STUN messages are sent within the same media path as the audio or video stream, allowing the intercom or VoIP device to determine NAT and connectivity information without using a separate signaling channel.
Inbound	Refers to network traffic or signaling that is received by a device or system from an external source.
IP-PBX	An Internet Protocol Private Branch Exchange. A telephone system that manages internal and external voice calls using IP networks, providing call routing, extensions, and telephony features without relying on traditional analog phone lines.
IPv4	Internet Protocol version 4. An addressing system that assigns a numerical address to each device on a network, enabling intercom and VoIP devices to communicate. Example: 192.168.1.100

IPv6	Internet Protocol version 6. A newer addressing system designed to replace IPv4, using longer addresses to support a much larger number of networked devices and improved network features. Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
JPEG	A digital image compression format used to store and transmit still images, commonly used in intercom and camera systems for snapshots or individual video frames due to its balance of image quality and file size.
KADEX	A device-specific data exchange or configuration interface used by the intercom system to manage communication, settings, or integration with other systems, typically for control, monitoring, or diagnostics purposes.
Keepalive	A periodic message or signal sent to maintain an active network connection, verify reachability, and prevent timeouts or session termination due to inactivity.
LAN	Local Area Network. A network that connects intercoms, VoIP devices, and other equipment within a limited area such as a building or site, enabling local communication and access to network services.
Link-local address	An automatically assigned IP address used for communication only within the local network segment, typically when no DHCP server is available.
MAC	Media Access Control address. A unique hardware identifier assigned to a network interface, used to identify an intercom device on the local network.
MJPEG	Motion JPEG. A video format in which each video frame is encoded as a separate JPEG image, providing simple and reliable video streaming at the cost of higher bandwidth usage.
Multicast	A network communication method in which audio or video data from an intercom is sent once and delivered simultaneously to multiple receiving devices on the network, reducing bandwidth usage compared to sending separate streams to each receiver.
MQTT	Message Queuing Telemetry Transport. A lightweight messaging protocol used in intercom and VoIP systems to publish and receive events or status updates, enabling efficient integration with automation, monitoring, or building management systems.
NAT	Network Address Translation. A networking method that allows intercom and VoIP devices on a private network to communicate with external networks by translating internal IP addresses to a public address, often used by routers and firewalls.
NTP	Network Time Protocol. A protocol used by intercom and VoIP systems to synchronize their internal clocks with a reference time source, ensuring accurate timestamps, logs, and scheduled operations.
OPUS	An adaptive audio codec designed for real-time communication, capable of delivering high audio quality over a wide range of bitrates and network conditions, commonly used for voice and multimedia streaming.
Outbound	Refers to network traffic or signaling that is sent from a device or system to an external destination.

Payload type	An identifier used in media transport protocols to indicate the format of the carried media data, allowing the receiver to correctly interpret and decode the stream.
PCAP	Packet Capture. A file format used to record network traffic, allowing intercom and VoIP communications to be analyzed for troubleshooting, diagnostics, and performance verification.
Peer-to-Peer (P2P)	A communication model in which devices connect and exchange data directly with each other without relying on a central server for media transmission.
Port	A logical communication endpoint identified by a number, used by transport-layer protocols to direct network traffic to specific services or applications on a host.
Proxy	An intermediary server that receives requests from clients and forwards them to other servers, often providing functions such as routing, security, policy enforcement, or address hiding.
REFER	A SIP method used to request that a recipient initiate a new SIP request, typically to transfer an existing call to another destination.
Registrar	A SIP server responsible for receiving and maintaining registration information that associates user identities with their current network locations.
Resolution	The dimensions of a video image, expressed as width × height in pixels; higher resolution produces more detailed images but increases the amount of data that must be transmitted and processed.
REST API	Representational State Transfer Application Programming Interface. A web-based interface that allows external systems to interact with the intercom using standard HTTP or HTTPS requests to perform functions such as control, configuration, monitoring, and data retrieval.
RTP	Real-time Transport Protocol. A protocol used to deliver real-time audio and video over IP networks, providing sequencing and timestamping for synchronized media playback.
RTSP	Real Time Streaming Protocol. A network control protocol used to establish, control, and terminate audio and video streams from the intercom, and commonly used to access the intercom's video feed as a security camera stream in monitoring or recording systems.
Schedule	A configurable time-based rule set that defines when the intercom operates in specific modes or allows certain actions, such as call handling, access control, or notifications, based on date and time.
Self-signed certificate	A digital certificate generated and signed by the intercom or server itself rather than by a trusted certificate authority, providing encryption but requiring manual trust to avoid security warnings.
SIP	Session Initiation Protocol. A signaling protocol used to establish, modify, and terminate multimedia communication sessions such as voice and video calls over IP networks.
SIP server	A network server that manages SIP signaling in intercom and VoIP systems, handling user registration, call setup, routing, and termination of communication sessions.

Stream (audio)	A continuous flow of digital audio data transmitted in real time, allowing live voice communication through the intercom system.
Stream (video)	A continuous flow of digital video data transmitted in real time, allowing live visual monitoring through the intercom system.
S/FTP	Shielded Foiled Twisted Pair cable. A type of network cable used for intercom and VoIP installations in which each twisted wire pair is individually foil-shielded and the entire cable is additionally shielded, providing strong protection against electromagnetic interference in demanding environments.
SSL/TLS	Encryption protocols used to secure email communication from the intercom system, protecting authentication credentials and message content when sending notifications or alerts via mail servers.
STP	Shielded Twisted Pair. A type of network cable used to connect intercom and VoIP devices, featuring twisted wire pairs with added shielding to reduce electromagnetic interference and improve signal quality in electrically noisy environments.
STUN	Session Traversal Utilities for NAT. A protocol used in intercom and VoIP systems to discover the public IP address and port assigned by a NAT device, helping enable reliable audio and video communication across different networks.
Subnet mask	A network parameter that defines which part of an IP address identifies the local network and which part identifies the individual device, allowing intercom and VoIP devices to determine whether communication is local or must be routed through a gateway.
TCP	Transmission Control Protocol. A connection-oriented transport-layer protocol used in intercom and VoIP systems for signaling and configuration data, providing reliable delivery, error correction, and ordered data transmission.
Threshold	A configurable sensitivity level that defines the minimum audio or video signal required for the intercom system to detect activity and trigger an action; higher threshold values require stronger sound or motion to be detected.
TLS	Transport Layer Security. A security protocol used in intercom and VoIP systems to encrypt signaling and data exchanges, protecting communications from eavesdropping, tampering, and unauthorized access.
Tone	The audible quality or character of a person’s voice during intercom communication, reflecting how the voice sounds while speaking, such as calm, sharp, or strained.
Trace	A diagnostic process that records or displays network signaling and traffic flows, used to monitor, debug, and troubleshoot intercom and VoIP communication issues.
Trigger edge (relay)	A relay activation mode that defines whether the intercom relay is triggered when the control signal changes from off to on (rising edge) or from on to off (falling edge), allowing precise control of connected devices.
UDP	User Datagram Protocol. A connectionless transport-layer protocol commonly used in intercom and VoIP systems to transmit audio and video with low latency, accepting possible packet loss in favor of real-time performance.

UTP	Unshielded Twisted Pair. A type of network cable commonly used to connect intercom and VoIP devices to a LAN, consisting of twisted wire pairs that reduce interference without additional shielding.
VLAN	Virtual Local Area Network. A logical network that segments devices on the same physical LAN into separate broadcast domains, allowing intercom and VoIP traffic to be isolated for improved security, performance, and management.
VoIP	Voice over Internet Protocol. A technology that enables voice communication over IP networks by converting audio into digital data for transmission and reconverting it to audio at the receiving end.