



PART OF THE CDVI GROUP

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

ABOUT THIS MANUAL

Thank you for choosing a Robin intercom system.

Robin intercoms are designed for professional environments where performance, reliability, and design matter. Built with high-quality hardware and advanced IP technology, they deliver clear audio, optional HD video, and seamless integration with telephony, Secure SIP, and access control systems.

WHO THIS MANUAL IS FOR

This manual is intended for:

- IT installers
- System integrators
- IT administrators
- Advanced users

It provides the information needed to install, configure, and integrate your Robin intercom system efficiently.

WHAT THIS MANUAL COVERS

This guide includes:

- Installation and setup
- Network configuration
- Telephony configuration (SIP)
- Event and action management
- Third-party system integration
- Advanced automation features
- Daily operation

Configuration examples are provided for both standard installations and advanced integrations.

BEFORE YOU BEGIN

Before installing or operating the device:

- Read this manual carefully
- Follow recommended installation procedures
- Apply configuration guidelines

Proper installation ensures:

- Safe operation
- Optimal performance
- Long-term reliability

PROFESSIONAL INTEGRATION READY

Robin intercoms are designed for professional network environments and are deployable:

- As a standalone access point
- As part of a larger communication system
- Within an access control ecosystem

High-grade materials, robust construction, and optimised firmware ensure reliable operation under continuous use.

PRODUCT RANGES

TYPE	REFERENCE
Audio	Audio Compact Audio Pro
Video	Video Compact Video Pro Video Pro Classic Proline Robin Touch
Smart Devices	Doorbell

Additional Resources

For additional documentation, firmware updates, or technical support:

- Visit CDVI's official support resources
- Contact CDVI Technical Support
- Contact your authorised distributor

(See [next page](#) for contact details)



PART OF THE CDVI GROUP

Robin Telecom Development BV

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



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 Germany

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

CDVI Italy

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

ASIA-PACIFIC, MIDDLE EAST & AFRICA

CDVI Export

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

CDVI Poland

Św. Jacka Odrowąża 15
03-310 Warszawa
Polska
+48 607 445 682
info@cdvi.com.pl

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

CDVI France

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

CDVI Iberica

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

CDVI Nordic AB

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

CDVI Suisse

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

WARRANTY AND RETURNS

WARRANTY COVERAGE

Robin products are covered by a 5-year warranty:

- The warranty period starts from date of manufacture (MFC), determined by the product label, serial number, or other manufacturer identification. It does not start from date of purchase, delivery, or installation date.
- Applies solely to defects in materials and workmanship.
- Is valid under normal use and service conditions and requires proper installation, operation, and maintenance.



The warranty does not extend beyond 5 years from manufacturing date and is subject to CDVI terms, conditions, and exclusions.

WARRANTY CLAIMS

If a product is found to be defective and is returned in accordance with CDVI's Return Material Authorisation (RMA) procedures, CDVI may at its sole discretion:

- Repair the product
- Replace the product
- Provide an equivalent product

Before returning a product:

- Obtain an RMA number. Returns without RMA may be refused and returned at the sender's expense.
- Clearly mark the RMA number on packaging.
- Package the product securely and follow CDVI return instructions.

Important

- Repaired or replacement products **do not extend** the warranty period.
- The period remains based on original manufacturing date.

CDVI RETURN PROCESS

For service, repair, or warranty support follow the process below:

1. The end user must **contact the original installer**.
2. The installer coordinates the return.
3. The installer returns the product to the distributor (if applicable).
4. The distributor returns to the CDVI branch from which the product was originally purchased.

- End users must not return products directly to CDVI
- All returns must follow CDVI RMA procedures
- Regional policies may apply

If the original installer is unavailable:

- Contact the local CDVI branch for guidance.
- You may be referred to an alternative installer or an authorised distributor.

ROBIN PRODUCT RETURNS

Robin devices without CDVI product naming follow a separate return process. These products may be returned directly if defective and are not subject to the standard CDVI return process.

For these products, the warranty period is defined by Robin. Follow Robin return and service procedures. For assistance, contact Robin using the contact details on the [previous page](#).

TRADEMARKS AND COMPATIBILITY

Robin	Robin and related product names are trade names and/or trademarks of Robin Telecom Development B.V.
CDVI	CDVI and related product names are trademarks and/or registered trademarks of the CDVI Group (and/or its affiliates), depending on jurisdiction.

THIRD-PARTY TRADEMARKS AND COMPATIBILITY

The following names and technologies are referenced for compatibility and integration purposes only.

Apple	Apple®, Apple TV®, HomePod®, iPhone®, iPad®, Apple Watch®, Siri®, Apple Home®, Apple HomeKit® These trademarks are owned by 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 do not imply affiliation or endorsement, unless explicitly stated
Matter	Matter® is a registered trademark of the Connectivity Standards Alliance References to Matter® apply only to compatible third-party accessories. This product may not be Matter-certified unless explicitly stated.
ControlByWeb	WebRelay™ and related product names are trademarks or registered trademarks of ControlByWeb References to WebRelay-Quad are for compatibility purposes only. No affiliation, sponsorship, or endorsement is implied.
CyberTwice	CyberGate™ and related product names are trademarks or registered trademarks of CyberTwice References to CyberGate are for compatibility purposes only. No affiliation, sponsorship, or endorsement is implied
Microsoft	Microsoft®, Microsoft 365®, Office 365®, Microsoft Teams® These are trademarks or registered trademarks of Microsoft Corporation. References are made for informational and compatibility purposes only.
IQ Messenger	IQ Messenger and related product names are trademarks and/or trade names of IQ Messenger B.V. (and/or its affiliates) References are provided for compatibility purposes only
MQTT	MQTT is a trademark of OASIS Open References to MQTT describe supported communication protocols only No affiliation, sponsorship, or endorsement is implied

General Trademark Notice

All trademarks and registered trademarks are the property of their respective owners.

Third-party names are used solely to identify compatibility and integration and do not imply affiliation, sponsorship, endorsement, and certification Unless explicitly stated.



IMPORTANT SAFETY INFORMATION

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

POWER AND CABLE REQUIREMENTS

- Power the device exclusively via Power-over-Ethernet (PoE) complying with IEEE 802.3af.
- Use PoE-compliant switches or PoE injectors only.
- Ethernet interface is classified as a SELV circuit.
- Do not apply external voltage to the Ethernet connector.
- Maximum **cable length: 100 metres** per segment.
This applies between two active network devices. Shorter cable lengths may be required depending on cable quality, installation conditions, or power consumption.

RELAY OUTPUT

The built-in relay provides a potential-free (dry) contact for controlling external equipment.

- SELV circuits only
- Maximum load: 24 V AC/DC at 0.75 A

Do not connect to mains voltage or hazardous energy sources. External equipment must comply with electrical safety standards and local regulations.

MOUNTING AND INSTALLATION

Use supplied or officially approved mounting accessories only to ensure mechanical stability, environmental protection and proper thermal performance.

The following are considered **non-standard installations**:

- Wall mounting without approved accessories
- Flush mounting without approved accessories
- In-wall installation without approved accessories

Damage caused by non-standard installation is **not covered by the warranty** and may affect device performance.

NETWORK SECURITY

The device is designed for use within a **Local Area Network (LAN)**.
For security reasons we recommend:

- Avoid direct exposure to public networks
- Avoid port forwarding where possible
- Change default credentials immediately
- Use strong passwords (minimum 12 characters)
- Restrict outgoing calls on PBX / VoIP systems
- Install firmware updates regularly

COMPLIANCE AND RESPONSIBILITY

The installer is responsible for ensuring that the installation complies with the EN 62368-1 regulation and that the national and local regulations are followed. He must also ensure that the connected equipment meets safety requirements and that the device is used as described in this documentation.

CONTENTS

ABOUT THIS MANUAL	2
Who This Manual Is For	2
Before You Begin	2
Professional Integration Ready	2
Product Ranges	2
What This Manual Covers	2
Product Information, Training and Technical Support	3
Warranty and Returns	4
Warranty Coverage	4
Warranty Claims	4
CDVI Return Process	4
Robin Product Returns	4
Trademarks and Compatibility	5
Third-Party Trademarks and Compatibility	5
Power and Cable Requirements	6
Relay Output	6
Mounting and Installation	6
Network Security	6
Compliance and Responsibility	6
Important Safety Information	6
CONTENTS	7
INTRODUCTION	11
Robin Intercoms	11
Features	12
Design and Build Quality	12
Advanced Access Control Integration	12
Enterprise Video/Surveillance Support	12
Open Integration and API Support	12
Professional Telephony Architecture	12
Event-Driven Automation Engine	12
Secure Network Integration	12
OPERATION	13
Features / Daily Use	13
Initiating a Call	14
Controlling the Integrated Relay	15
Integrations with Internal and External Platforms	16
SUSTAINABILITY AND MATERIAL INTEGRITY	17
Durable	17
Future-Ready Firmware	17
Energy-Efficient	17
Long Lifecycle	17
PRODUCT OVERVIEW	18
Product Aliasing	18
Power-Over-Ethernet	18
Robin Touch	19
Package Contents	19

Installation Dimensions	19
Accessories.....	19
Product References	19
Audio Compact, Video Compact	20
Package Contents	20
Installation Dimensions	20
Accessories.....	20
Product References	20
Audio Pro (Classic), Video Pro (Classic)	21
Package Contents	21
Accessories.....	21
Product References	21
Installation Dimensions	21
Proline.....	22
Package Contents	22
Installation Dimensions	22
Accessories.....	22
Product References	22
Doorbell.....	23
Package Contents	23
Accessories.....	23
Product References	23
Installation Dimensions	23
PoE Injector	24
Package Contents	24
Compatibility	24
Installation	24
Product References	24
Button Extender.....	25
Package Contents	25
Compatibility	25
Installation	25
Product References	25
MOUNTING INSTRUCTIONS	26
Surface Mount	26
References	26
Tool Requirements	26
Standard Surface Housing Installation	27
Surface Ambient Frame Installation.....	28
Flush Mount	29
References	29
Tool Requirements	29
Recessed Wall Cutout Dimensions	29
Installation	30
Mounting Without Housing	31
Tool Requirements	31
Installation	31
Wiring	32
Finalise the Installation	33
Without Ambient Frame.....	33
With Ambient Frame	33

Placing the Nametag	34
Engraving the Nametag	34
High-End Finish	35
Cleaning the Device.....	36
General Instructions.....	36
Aluminium Finish	36
Environmental Exposure	36
Brass Finish	36

SYSTEM INSTALLATION 37

Prerequisites	37
Connect the Device to Your Network	37
Robin Discovery Utility	37

CONFIGURATION 38

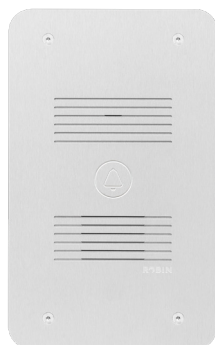
Logging in to the Web Interface	38
Setup.....	38
Telephony	40
SIP.....	40
Phonebook	45
Button Settings	47
Button Extender	49
Keypads Settings.....	50
Call Advance	50
Call Log.....	50
Control.....	50
Peer-to-Peer (P2P).....	51
Audio	54
Settings	54
Detection	54
Media.....	55
Video	56
Live	56
Settings	56
Motion	57
Streams	58
Display	59
Overview.....	59
Settings	60
Access Control	62
PIN.....	62
Network.....	64
Status.....	64
HTTP.....	64
IP.....	65
Mail	66
NAT	66
RTSP.....	67
IQ Messenger.....	68
System.....	69
Device	69
Clock	70
Events	70

Security	81
Certificates	82
Schedules.....	83
Software	84
Relay	85
Debug.....	86
Lighting	87
SMART HOME CONFIGURATION	88
Wiring	88
Adding the Device to Home	88
Resetting the Device.....	89
SUPPORT	90
CDVI Support Portal	90
Robin Support Portal.....	90
Glossary	91

INTRODUCTION

ROBIN INTERCOMS

This manual applies to the following product ranges:



Audio Compact



Video Compact



Audio Pro



Video Pro



Video Pro Classic



Proline



Doorbell



Robin Touch

FEATURES

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

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 systems and external IP relay modules.

ENTERPRISE VIDEO/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.

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.

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.

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.

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.

OPERATION

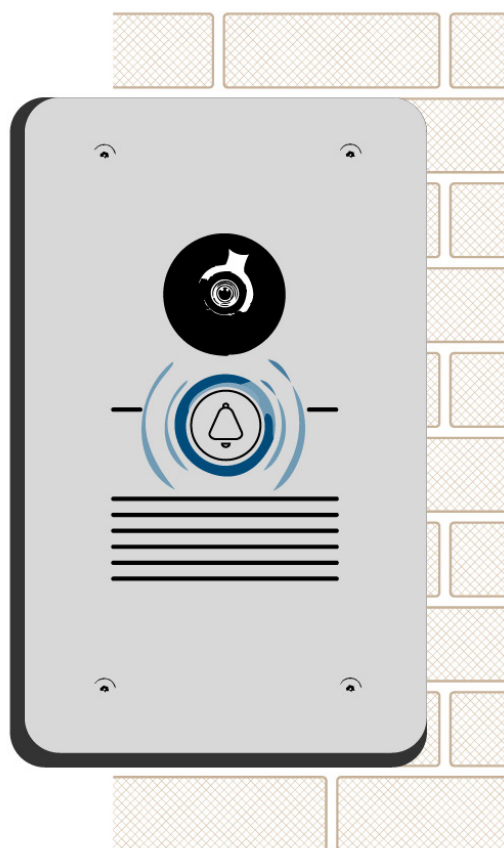
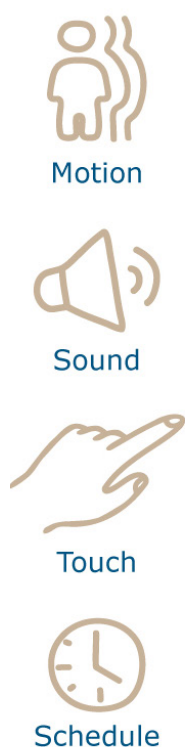
FEATURES / DAILY USE

Robin intercoms are designed to provide fast, intuitive, and reliable visitor communication. With a single button press or automatic detection, the intercom immediately establishes a connection with the configured recipient, ensuring quick response times and a seamless user experience.

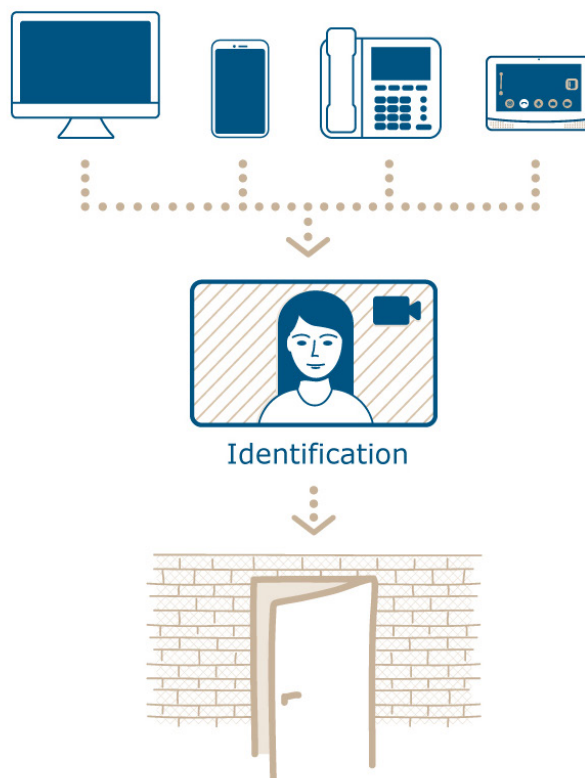
A clear interface enables visitors to interact with confidence, while occupants can answer calls and grant access quickly without navigating complex menus or applications. Optimised hardware and software ensure responsive operation with minimal user interaction.

Built from premium materials for continuous operation, Robin intercoms deliver dependable performance in residential, commercial, healthcare, and industrial environments, providing secure and effortless communication every day.

Detection Triggers



Communication endpoints



Fast connection



Clear image in any lighting condition



Easy access control



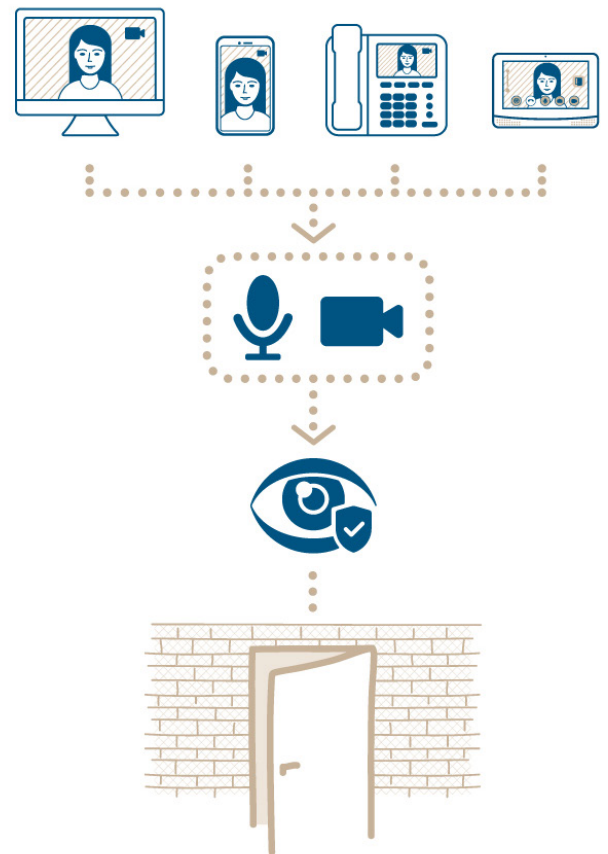
Reliable & Built to last

INITIATING A CALL

Initiating a call with a Robin intercom is straightforward. Depending on the model, visitors can place a call by pressing a call button, selecting a contact from the touchscreen directory, or entering a code on the keypad.

Once activated, the intercom immediately contacts the configured recipient and provides visual and/or audible confirmation. Calls can be routed to a single user, multiple recipients, a reception desk, or a predefined call group.

During the connection process, the intercom displays the current call status, such as ringing, connected, busy, or unavailable. On video models, a live video stream is established when the call is answered, enabling face-to-face communication and a smooth, professional experience for both visitors and occupants.



CONTROLLING THE INTEGRATED RELAY

Robin intercoms provide a convenient and secure way to control access to doors, gates, barriers, and other secured areas. Once a call has been answered, authorised users can communicate with the visitor and grant access remotely, allowing visitors to be verified before entry.

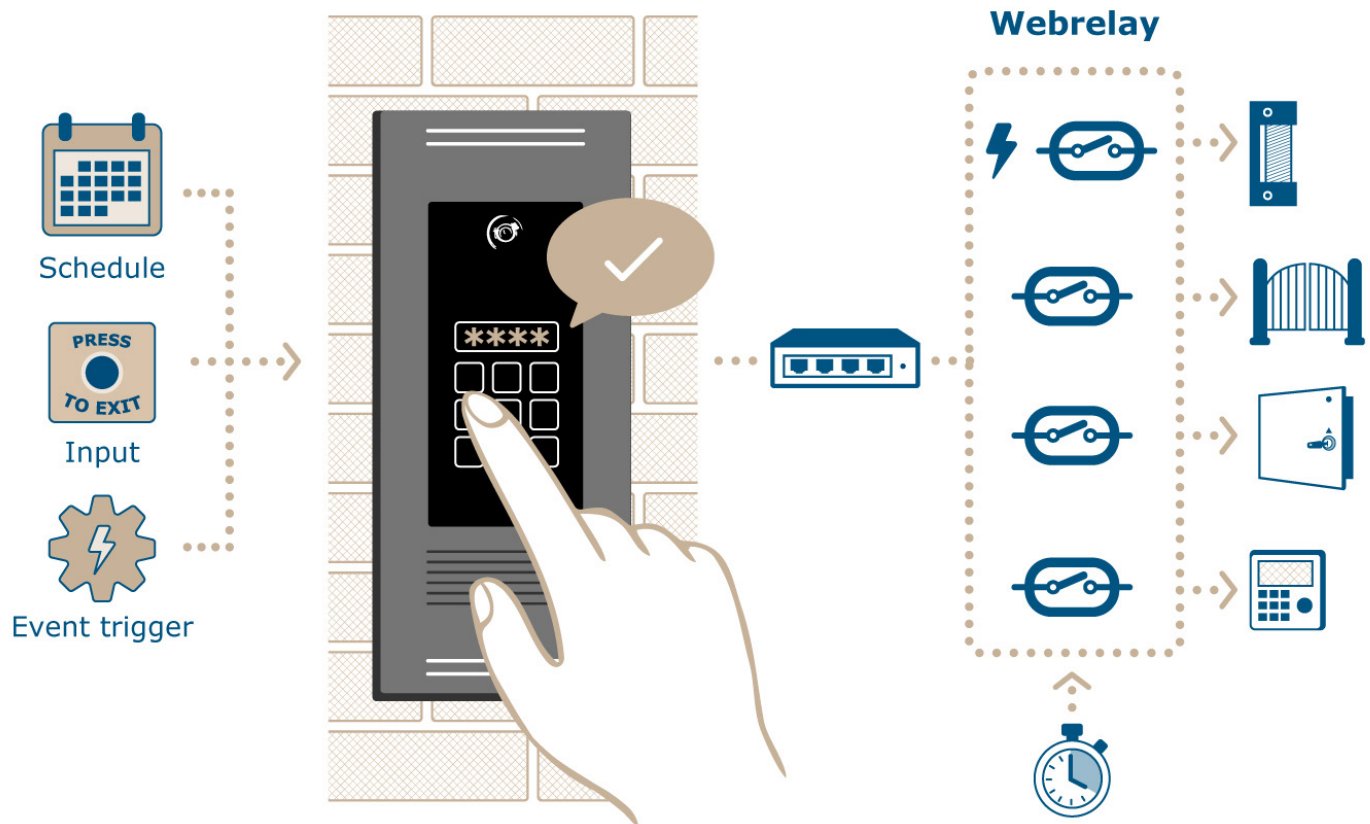
The integrated relay can be used to operate electric strikes, magnetic locks, automatic doors, gate operators, barriers, or traditional doorbells. For higher-security installations, the external Webrelay is recommended. Installed inside the secured area, it protects the locking circuit from tampering while enabling secure remote door control.

In addition to the integrated relay, Robin intercoms support the Webrelay and other compatible third-party relay devices, allowing multiple doors, gates, lighting circuits, alarm inputs, and automation systems to be controlled from a single installation. Relay actions can be triggered manually, automatically through schedules, or in response to intercom events.

Flexible relay configuration allows the system to be tailored to a wide range of residential, commercial, industrial, and high-security applications, providing a scalable solution for modern access control.



Maximum relay switch: 24V – 0.75A.



INTEGRATIONS WITH INTERNAL AND EXTERNAL PLATFORMS

Robin intercoms are designed to operate as part of a modern communication, security, and automation ecosystem. Rather than functioning as a standalone device, they integrate seamlessly with telephony platforms, access control systems, building management software, smart home environments, video management systems, and custom applications.

To support these integrations, Robin devices utilise **open communication standards** including SIP, HTTP, HTTPS, MQTT, RTSP, and dedicated APIs. These protocols enable the intercom to exchange information with external systems, allowing developers and system integrators to create solutions that fit existing workflows and infrastructure.

Using HTTP, HTTPS, APIs, and MQTT, external platforms can retrieve device information, receive event notifications, monitor system status, and trigger actions such as relay control or automated workflows. Real-time events, including button presses, incoming calls, motion detection, keypad activity, and relay activations, allow connected systems to respond immediately, making Robin ideal for smart buildings and IoT environments.

For video-enabled models, RTSP provides direct access to the live video stream for integration with Video Management Systems (VMS), Network Video Recorders (NVR), and other surveillance platforms, enabling video to be viewed and recorded alongside existing security cameras.

Whether integrated with Microsoft Teams, SIP-based PBX systems, building automation, or security platforms, Robin intercoms provide a flexible and scalable solution that supports today's operational requirements while remaining ready for future expansion.



SUSTAINABILITY AND MATERIAL INTEGRITY

Robin intercom systems are designed with **durability, efficiency, and long-term use** in mind. This approach supports sustainable installations and long-term investment in building technology.

DURABLE

Robin intercoms are manufactured using high-quality metals:

- **Aluminium** is corrosion-resistant and dimensionally stable
- **Brass** is naturally durable and develops a protective patina over time

The benefits of using these materials are numerous:

- High structural strength
- Resistance to environmental exposure
- Long-term visual quality
- Fully recyclable materials

Using solid metals instead of coated plastics or composites reduces wear and ageing, maintains appearance over time, extends product lifespan, and minimises premature replacement.

FUTURE-READY FIRMWARE

Sustainability also extends to software and system design:

- Structured firmware updates
- Open protocol compatibility
- Support for evolving platforms

This helps extend functional lifetime, reduce hardware replacement, and maintain compatibility with new systems.

ENERGY-EFFICIENT

Robin intercoms are designed for **low power consumption**:

- Powered via IEEE 802.3af Power-over-Ethernet (PoE)
- No separate power supply is required
- Reduced installation complexity

Energy-efficient components include:

- LED button illumination
- Display backlighting
- Ambient lighting for functional illumination during visitor interaction while maintaining efficient daily use operation

These features provide low power consumption, long operational lifespan, and reduced energy usage over time.

LONG LIFECYCLE

Robin intercom systems combine durable materials, efficient electronics, open integration standards, and long-term reliability.

This results in reduced environmental impact, long product lifespan, and reliable performance. Robin intercoms are designed for projects where performance, aesthetics, and sustainability must work together in a **balanced and responsible solution**.



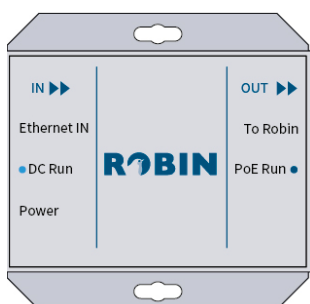
PRODUCT OVERVIEW

PRODUCT ALIASING

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

CDVI REFERENCE	ROBIN REFERENCE
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)
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.

- Power is supplied via pins 1–2 and 3–6 of the RJ45 connector.
- These wire pairs are used for data transmission.
- When connected to a standards-compliant PoE injector, power detection and negotiation is automatic. No manual configuration is required.



Passive PoE Warning

Use caution when connecting passive PoE switches or injectors, especially when using passive **Mode B** PoE equipment:

- It does not perform automatic detection
- It may supply power on different wire pairs: Mode B uses pins 4–5 and pins 7–8
- It may use non-standard voltages (e.g. 24 V passive PoE)

Connecting a Robin device to incompatible passive PoE may cause immediate malfunction and permanent device damage.

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)
- Output voltage complies with IEEE 802.3af / 802.3at
- Equipment supports standard IEEE Powered Devices (PD)

If compatibility is uncertain, do not connect the device. Use certified IEEE 802.3af or 802.3at PoE equipment only. Installation should be performed by qualified personnel only.

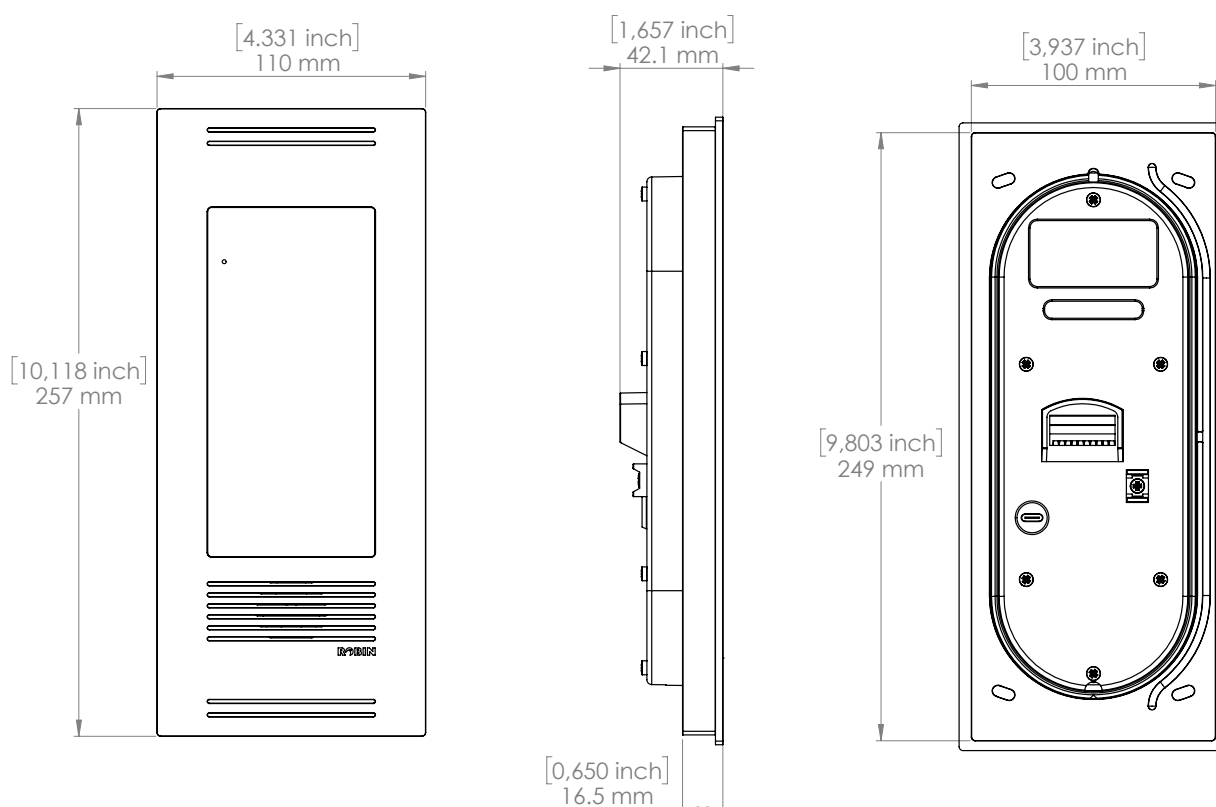
Warranty notice: Damage caused by incorrect power connections, non-compliant PoE equipment, or improper installation is not covered under warranty.

ROBIN TOUCH

PACKAGE CONTENTS



INSTALLATION DIMENSIONS



ACCESSORIES

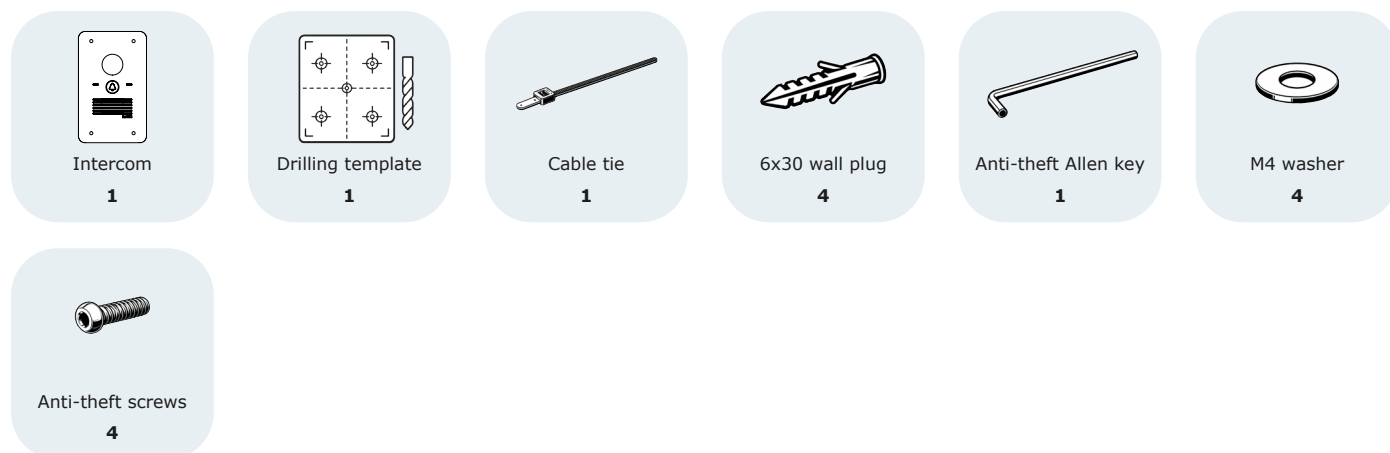
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Webrelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Touch SB	F0408000025	C01770
Touch FB	F0408000026	C01117

PRODUCT REFERENCES

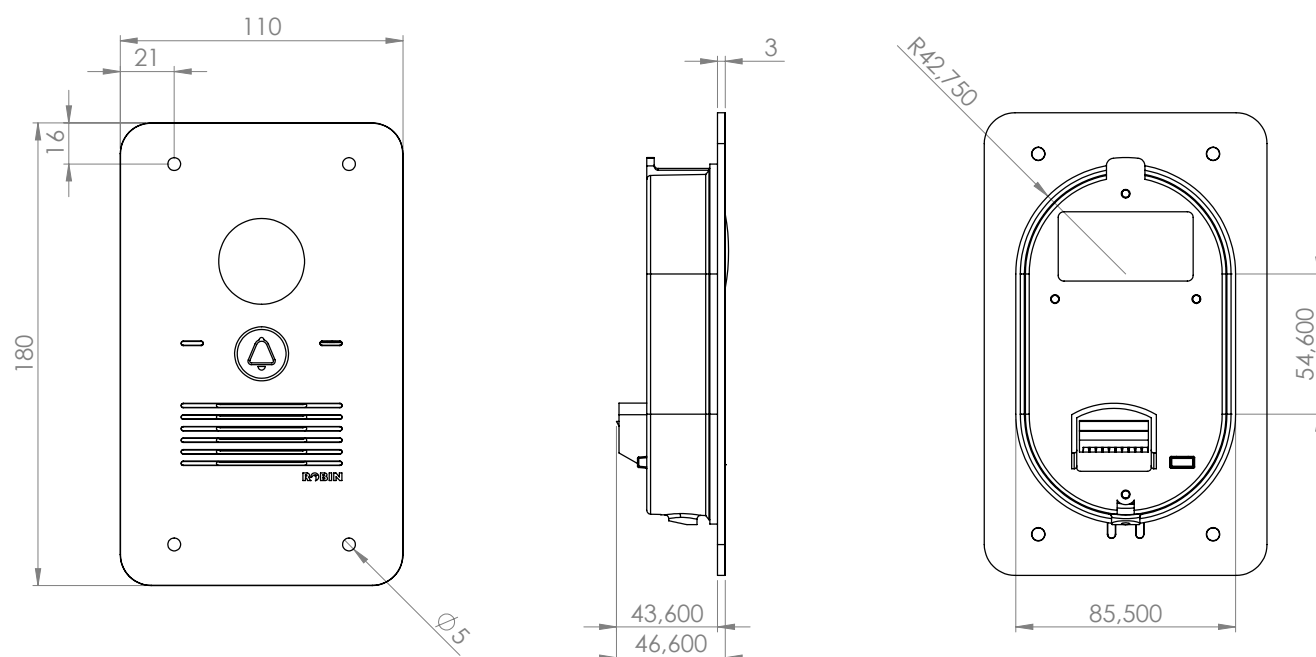
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Robin Touch	F0414000013	C93070

AUDIO COMPACT, VIDEO COMPACT

PACKAGE CONTENTS



INSTALLATION DIMENSIONS



ACCESSORIES

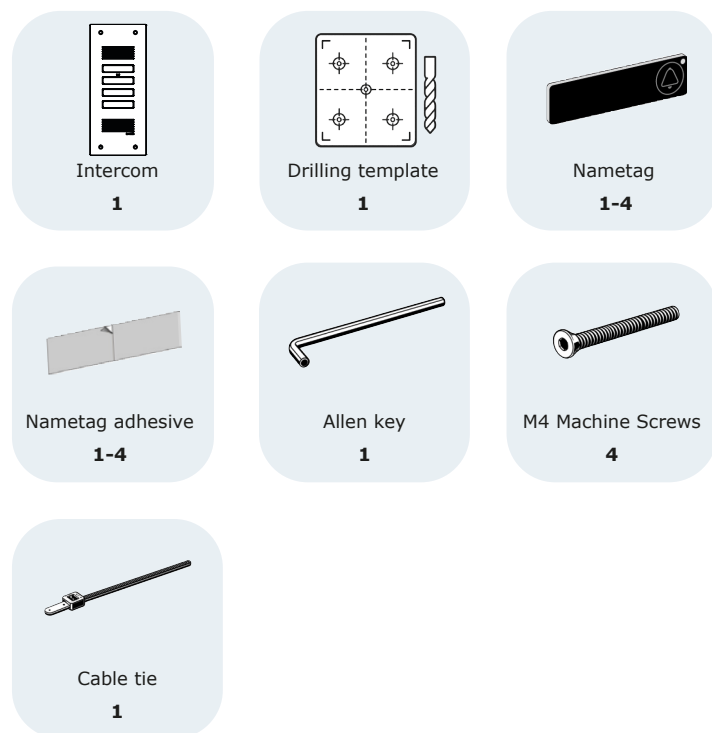
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Webrelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Compact SB	F0408000018	C01100
Compact FB	F0408000019	C01110

PRODUCT REFERENCES

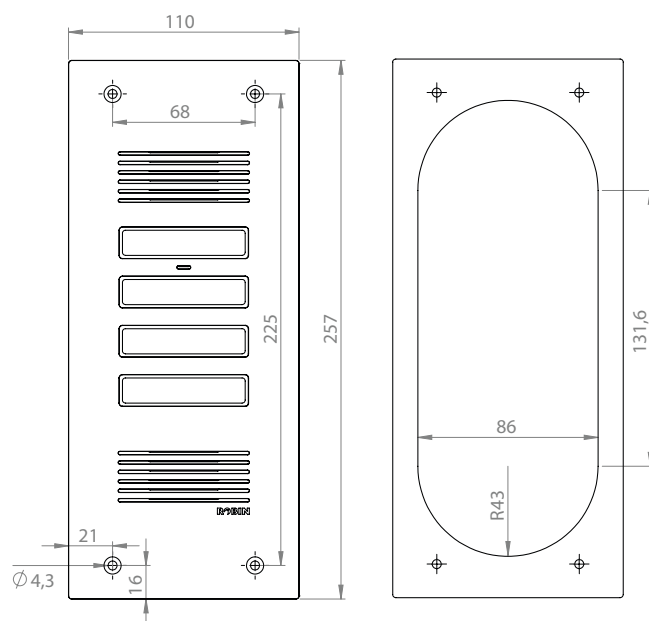
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Audio Compact	F0413000001	C91060
Video Compact	F0414000001	C92050

AUDIO PRO (CLASSIC), VIDEO PRO (CLASSIC)

PACKAGE CONTENTS



INSTALLATION DIMENSIONS



ACCESSORIES

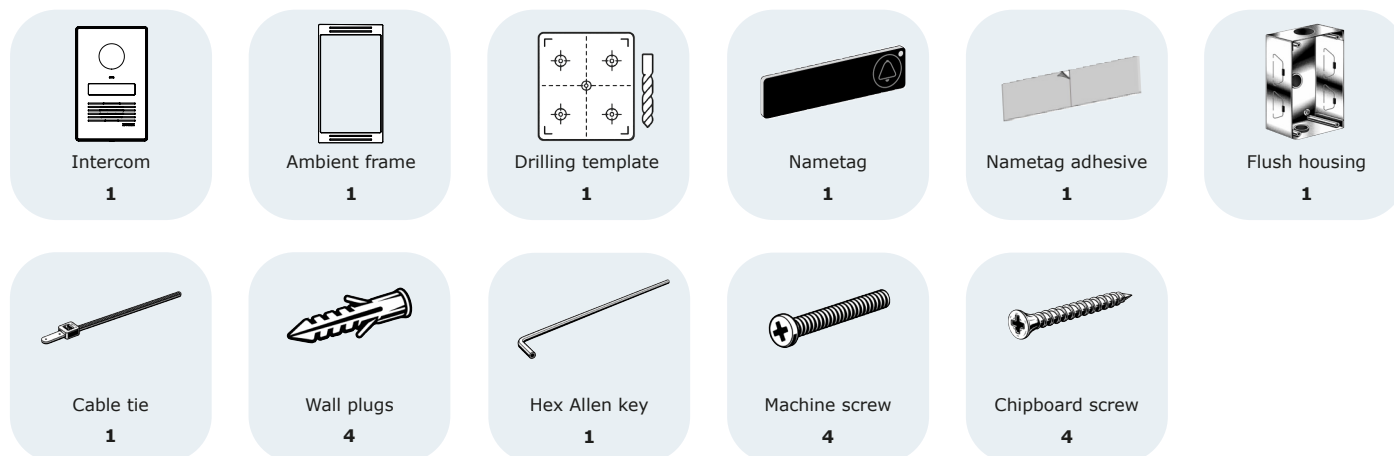
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Webrelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Pro SB	F0408000020	C03001
Pro FB	F0408000021	C01112

PRODUCT REFERENCES

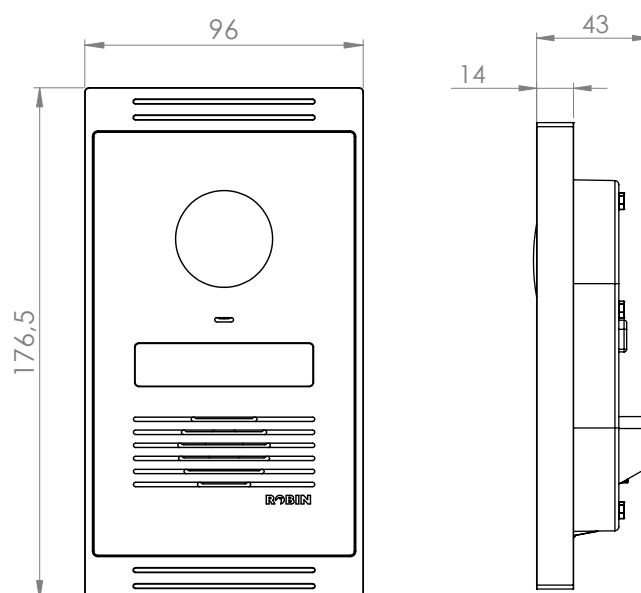
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Robin Audio Pro 1	F0413000002	C93065
Robin Audio Pro 2	F0413000003	C93066
Robin Audio Pro 4	F0413000004	C93067
Robin Audio Pro Keypad	F0413000005	C93068
Robin Video Pro 1	F0414000005	C93050
Robin Video Pro 2	F0414000006	C93052
Robin Video Pro 4	F0414000007	C93054
Robin Video Pro Keypad	F0414000008	C93058
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	C93075

PROLINE

PACKAGE CONTENTS



INSTALLATION DIMENSIONS



ACCESSORIES

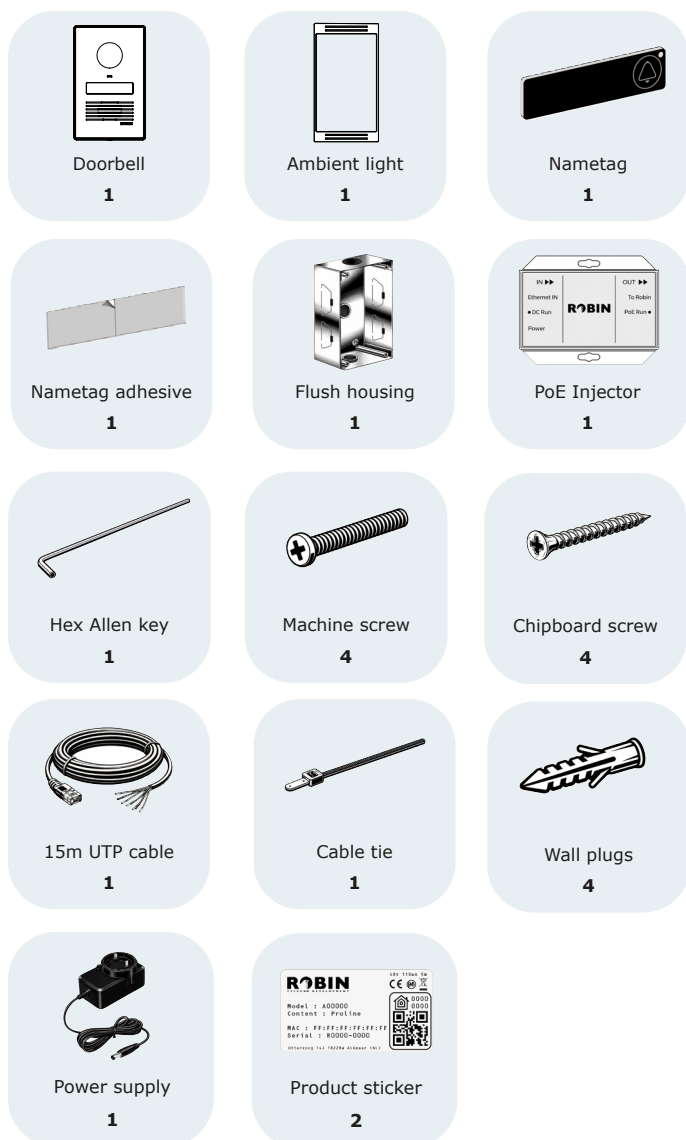
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Webrelay	F0410000172	C01037
PoE Injector	F0406000002	8061996
Proline SB Black	F0408000024	A91523
Proline SB Gray	F0408000023	C93026
Proline SB Silver	F0408000022	A91521

PRODUCT REFERENCES

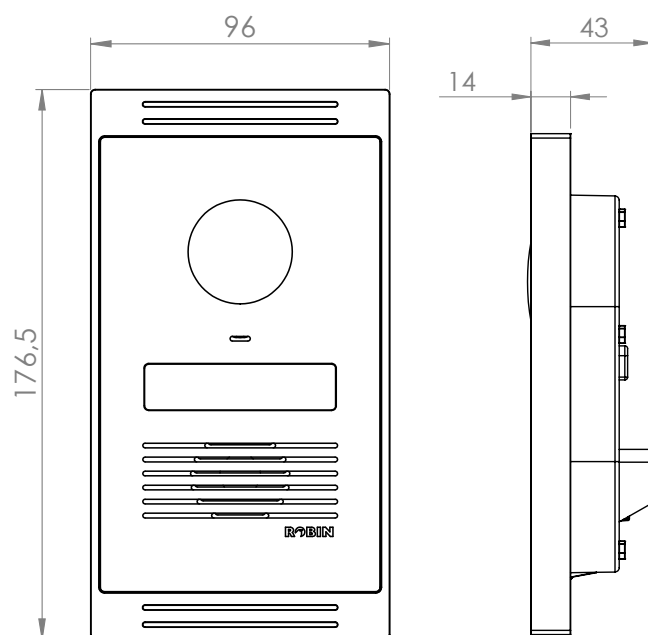
CDVI REFERENCE	CDVI CODE	ROBIN CODE
Proline Black	F0414000004	A93027
Proline Silver	F0414000002	A93025

DOORBELL

PACKAGE CONTENTS



INSTALLATION DIMENSIONS



ACCESSORIES

This product is compatible with a classic external door chime and works with Matter®-compatible accessories or Apple HomeKit®.



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.

PRODUCT REFERENCES

CDVI REFERENCE	CDVI CODE	ROBIN CODE
Doorbell Midnight Black	F0415000002	A91514
Doorbell Arctic Silver	F0415000001	A91512
Doorbell Evening Bronze	F0415000004	A91515

POE INJECTOR

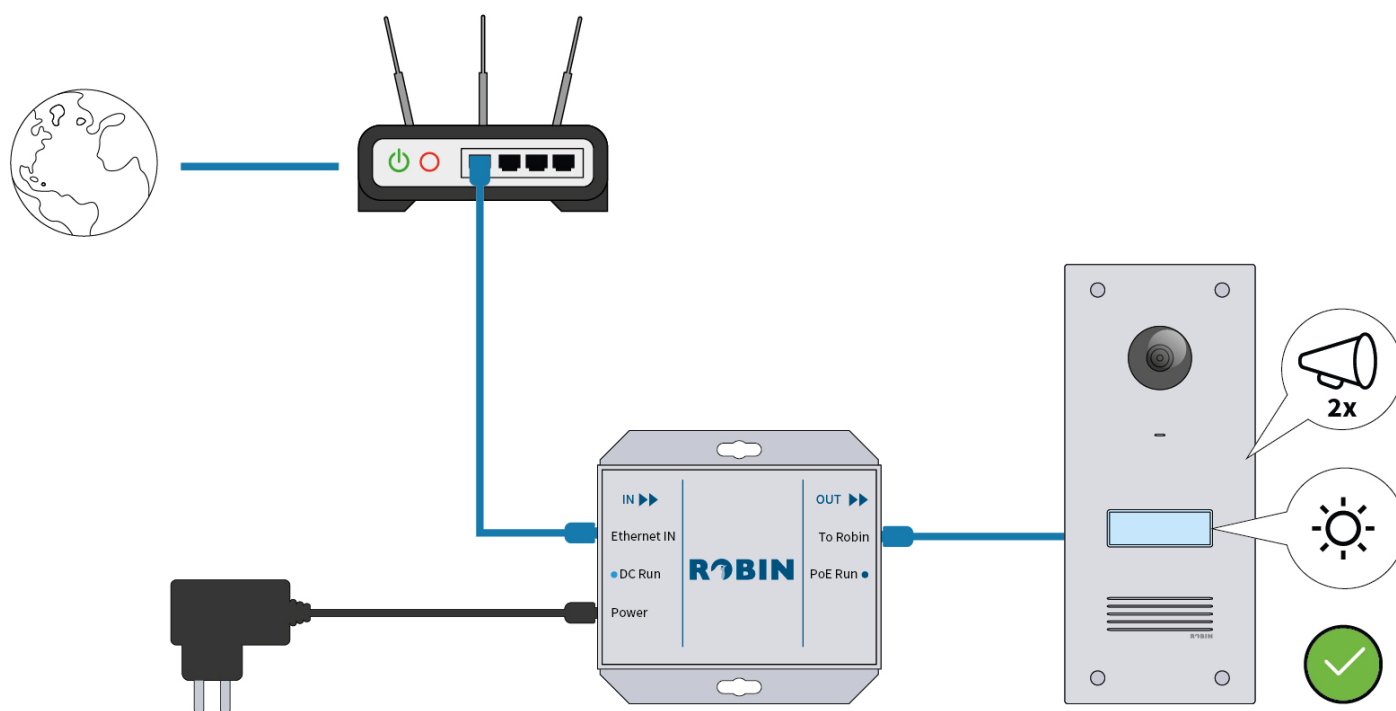
PACKAGE CONTENTS



COMPATIBILITY

This accessory is compatible with all Robin intercoms.

INSTALLATION

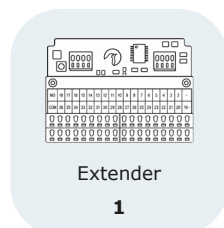


PRODUCT REFERENCES

CDVI REFERENCE	CDVI CODE	ROBIN CODE
PoE Injector	F0414000013	8061996

BUTTON EXTENDER

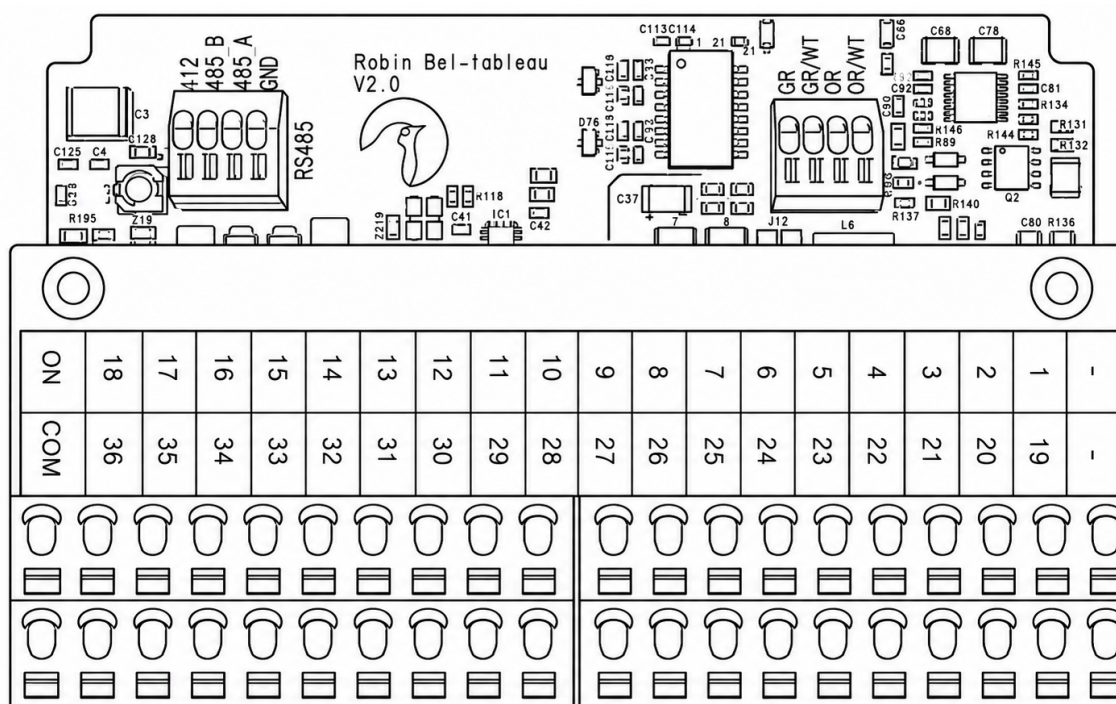
PACKAGE CONTENTS



COMPATIBILITY

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

INSTALLATION



1. Connect the GR (Green), GR/WT (Green/White), OR (Orange) and OR/WT (Orange/White) wires from your network cable to the Button Extender.
2. Connect the device to the same network range as your intercom.
3. Connect each physical button with one wire to a numbered contact (1-36). Connect the other wire to your COM-contact. (The buttons need to be NO)
4. When triggering the respective numbered contact for the first time, it automatically adds a button to your web interface in "Telephony". (see [page 49](#) Telephony > Button Extender)
5. The extender is automatically detected within the same IP range. (see [page 49](#) Telephony > Button Extender)

PRODUCT REFERENCES

CDVI REFERENCE	CDVI CODE	ROBIN CODE
Button Extender	TBD	C91771

MOUNTING INSTRUCTIONS

SURFACE MOUNT

REFERENCES

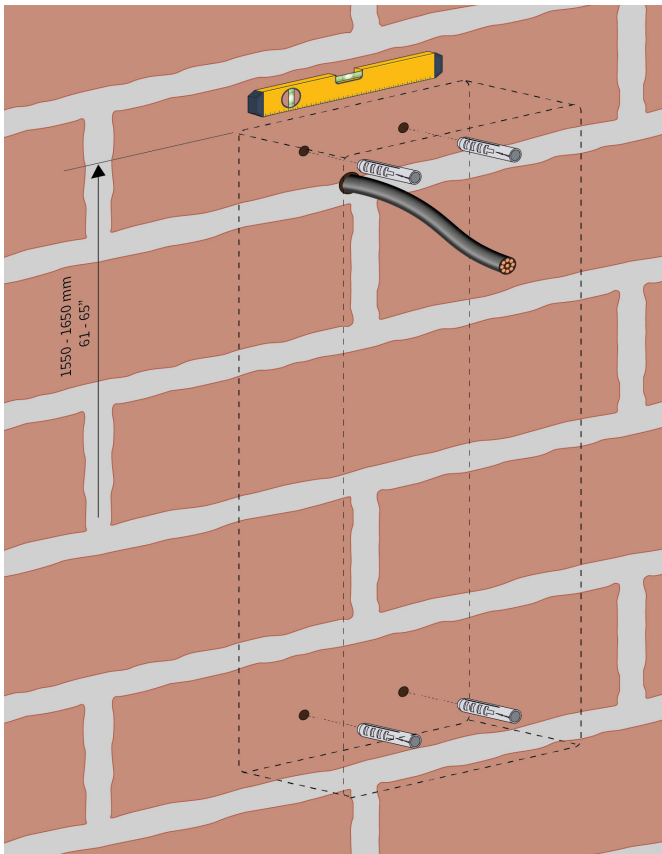
SURFACE HOUSING	MODELS	CDVI CODE	ROBIN CODE
Compact SB	Audio Compact Video Compact	F0408000018	C01110
Pro SB	Audio Pro 1/2/4/Keypad Video Pro 1/2/4/Keypad Video Pro Classic 1/2/4/Keypad	F0408000020	C03001
Proline SB Silver	Proline Silver Doorbell Arctic Silver	F0408000022	A91521
Proline SB Black	Proline Black Doorbell Midnight Black	F0408000024	A91523
Touch SB	Robin Touch	F0414000013	C01770

TOOL REQUIREMENTS

The following tools are recommended when installing the intercom in a surface mount configuration:

TOOL	USAGE
Measuring tape and pencil	To mark 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

STANDARD SURFACE HOUSING INSTALLATION



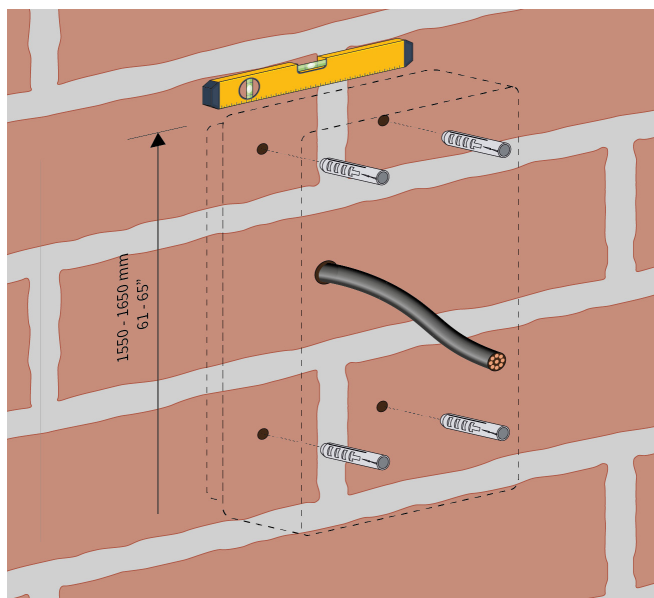
1. Position the surface mount housing in the right place on the wall and make sure it is level.
2. Mark the four mounting holes on the wall with a pencil. Also mark the point to make the hole for the intercom cables.
3. Drill the holes.
4. Feed the Ethernet cable and the optional electronic relay and/or request-to-exit cable through the drilled hole.



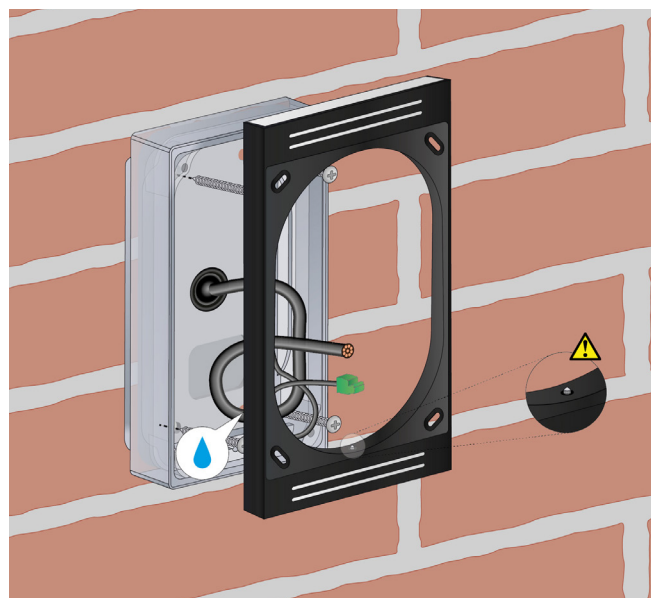
5. Route the Ethernet cable along the side of your intercom system.
6. Consult the "Wiring" section (see [page 32](#)) to make sure your device has been set up properly, and make sure you protect your device from scratching during this process.
7. Screw the surface mount housing to the wall.

Once the installation is complete, proceed to "Finalise the Installation". (see [page 33](#))

SURFACE AMBIENT FRAME INSTALLATION



1. Position the surface mount housing in the right place on the wall and make sure it is level.
2. Mark the four mounting holes on the wall with a pencil. Also mark the point to make the hole for the intercom cables.
3. Drill the holes.
4. Feed the Ethernet cable and the optional electronic relay and/or request-to-exit cable through the drilled hole.



5. Screw the surface mount housing to the wall and route the Ethernet cable along the side of your intercom system.
6. Then install the ambient frame onto the surface mount housing using the supplied screws.

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.

7. Consult the "Wiring" section (see [page 32](#)) to ensure your device has been set up properly. Ensure you protect your device from scratching during this process.
8. The ambient frame is equipped with a small connector (Phoenix connector or USB-C depending on the model). It must be connected once the electrical wiring is completed.

Once installation and wiring are complete, connect the ambient frame and proceed to the section "Finalise the Installation" (see [page 33](#)).

FLUSH MOUNT

REFERENCES

SURFACE HOUSING	MODELS	CDVI CODE	ROBIN CODE
Compact FB	Audio Compact Video Compact	F0408000019	C01100
Pro FB	Audio Pro Video Pro Video Pro Classic	F0408000021	C01112
Proline FB	Proline Doorbell	Included with product	Included with product
Touch FB	Robin Touch	F0408000026	C01117

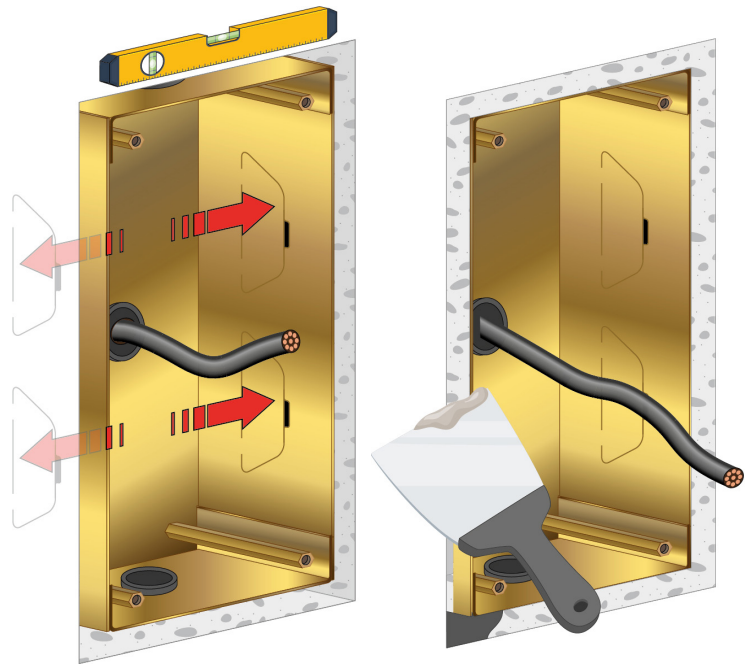
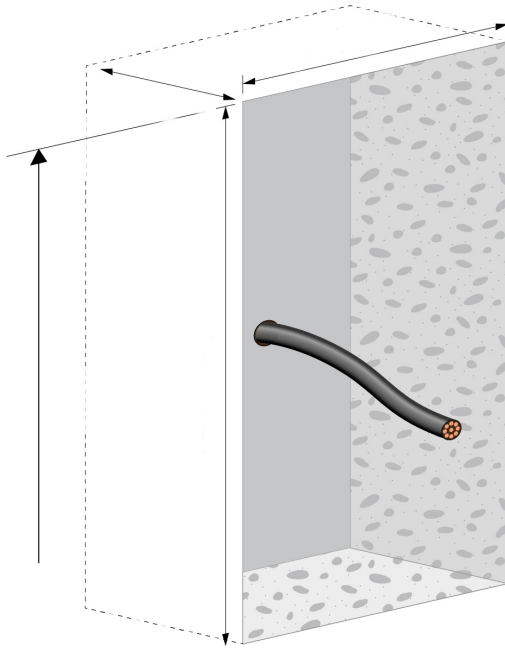
TOOL REQUIREMENTS

The following tools are recommended when installing the intercom in a flush mount configuration:

TOOL	USAGE
Measuring tape and pencil	To mark 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

RECESSED WALL CUTOUT DIMENSIONS

MODELS	HEIGHT	WIDTH
Audio Compact Video Compact	150-155 mm	90-95 mm
Audio Pro Video Pro Video Pro Classic	240-245 mm	90-95 mm
Proline Doorbell	150-155 mm	90-95 mm
Robin Touch	240-245 mm	90-95 mm



1. Consult the measurements of your specific model for the flush mount housing before proceeding to making a hole in the wall.
2. Then make a recess into the wall.
3. Drill a hole through the wall for the Ethernet cable and optional locking cable.

See [previous page](#) for cut out measurements.

4. Place the flush mount housing in the created hole and pass the cables through one of the four holes in the housing.

Remember to use the rubber sealing in all holes, and make sure the punctured rubber for passthrough fits the width of the used cable.

5. Make sure the flush mount housing is level and flush with the wall.
6. Pull out the four tabs so that it is fixed in position (red arrows).
7. 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. (see [Wiring page 30](#))

MOUNTING WITHOUT HOUSING



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.

TOOL REQUIREMENTS

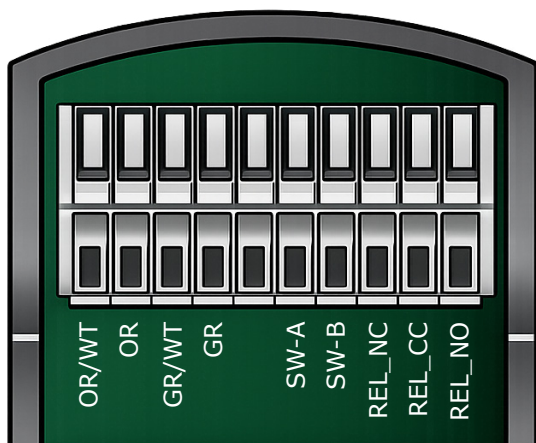
The following tools and materials are required when mounting the intercom with no housing:

- Core drill, $\varnothing$ 90 mm
- Masonry drill, $\varnothing$ 6 mm
- Stone chisel
- General set of tools
- Anti-theft Allen key (supplied)
- Anti-theft screws (supplied)
- 6 mm wall plugs (supplied)
- Drilling template (supplied)
- Cable tie (supplied)

INSTALLATION

1. Use the drilling template supplied in the package to drill holes ($\varnothing$: 90 mm, depth: 600 mm).
2. Remove the drilled cores using the stone chisel.
3. Shape the hole so that the device's plastic housing fits with room to spare.
4. Feed the cable into the hole. Leave enough excess length for a loop in the hole.
5. Drill the four fixing holes for the front panel using the drilling template and insert the wall plugs supplied into the holes.
6. Connect the Ethernet cable to the clamp connector. (Optional: Connect the cable for operating the relay to the clamp connector).
7. Secure the cable to the plastic housing using a tie-wrap.
8. Position the Robin in the hole so that the looped cable fits neatly behind the device.
9. Fix the device securely in place using the supplied anti-theft screws.
10. Once completed, proceed to the wiring of the device. (see *Wiring* [page 30](#))

WIRING¹

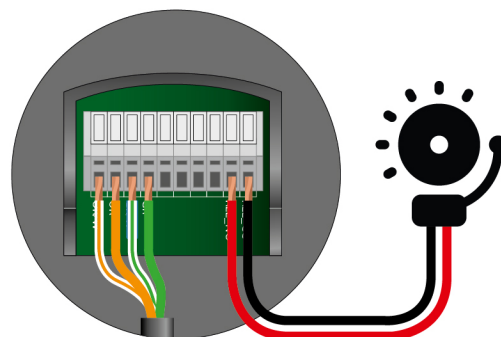
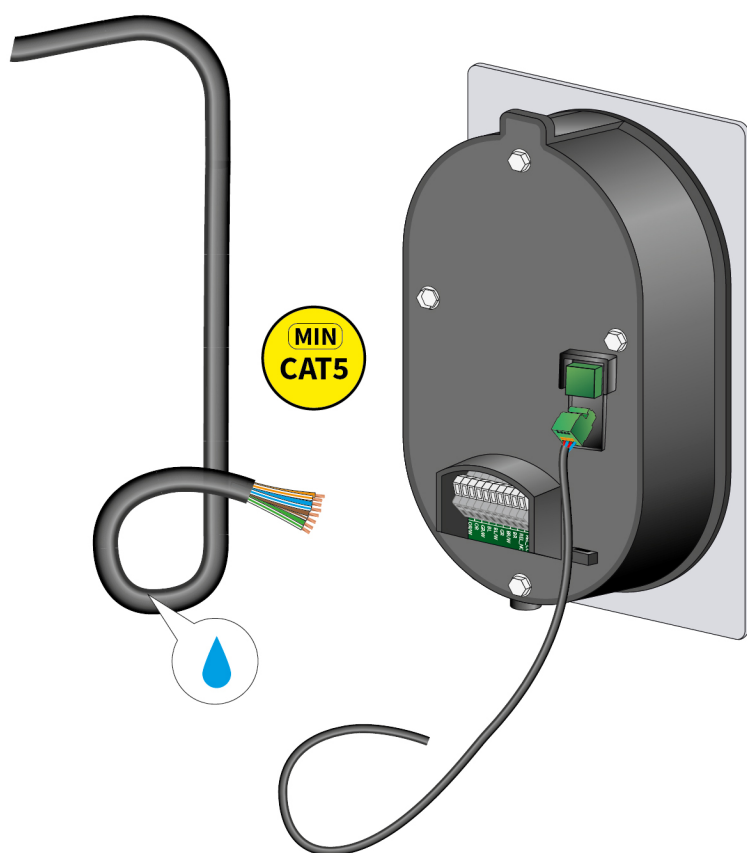


PORT	DESCRIPTION
OR/WT	Network Cable (Orange/White)
OR	Network Cable (Orange)
GR/WT	Network Cable (Green/White)
GR	Network Cable (Green)
	Not used
SW-A	Request-to-Exit button, Wire 1
SW-B	Request-to-Exit button, Wire 2
REL_NC	Relay, Normally Closed
REL_CC	Relay, Common
REL_NO	Relay, Normally Open



To prevent cosmetic or mechanical damage during wiring, it is recommended to temporarily wrap the device in a soft cloth, to have 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.
Attach the cable(s) to the housing as a tension relief using the supplied Cable tie.



- 1 OR/WT
- 2 OR
- 3 GR/WT
- 4 GR
- 5 -
- 6 SW-A
- 7 SW-B
- 8 REL_NC
- 9 REL_CC
- 10 REL_NO



¹ Connecting options are dependent on the intercom model.

FINALISE THE INSTALLATION

WITHOUT AMBIENT FRAME



1. Secure the intercom to the flush mount housing using the supplied screws. Depending on the model and the type of screws provided, use either the appropriate Allen key or a suitable screwdriver.
2. Carefully align the intercom with the surface or flush housing, ensuring that it sits straight and flush before tightening.
3. Tighten the screws manually by hand.

Do not use power tools, as excessive torque may damage the housing, threads, or mounting components.

4. 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.
5. Ensure the device is securely mounted and stable after installation.

WITH AMBIENT FRAME

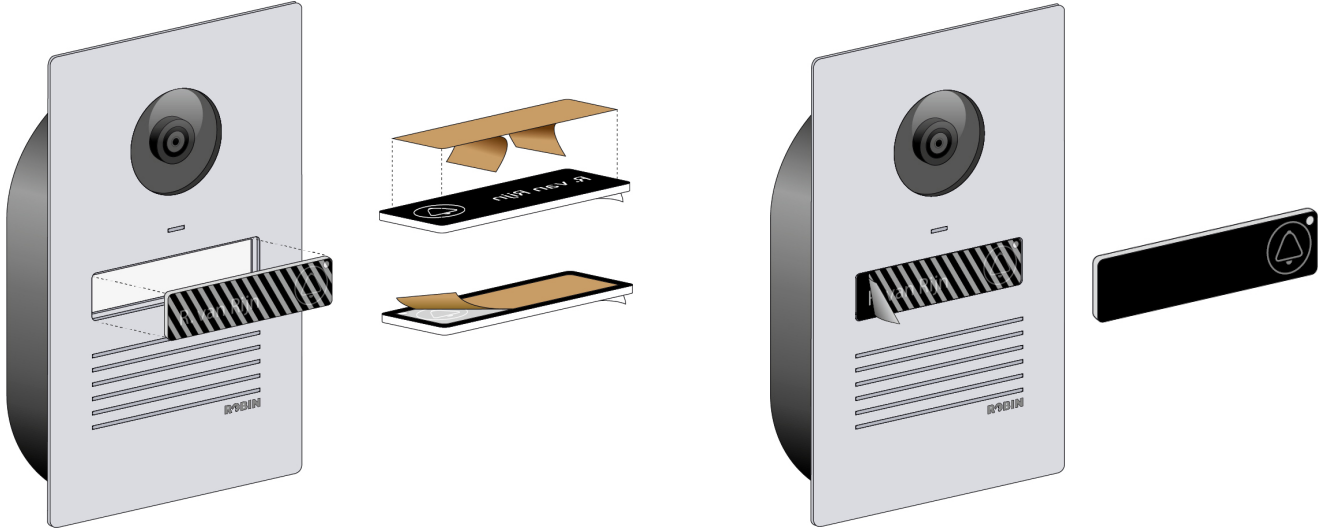


1. Locate the puncture and hole at the bottom of the ambient light frame.
2. Slide your device into the ambient frame.
3. Fasten the bottom screw using the supplied Allen key to secure the device in its frame.

PLACING THE NAMETAG

Once the device is installed, the anthracite tag (personalised or standard) must be applied.

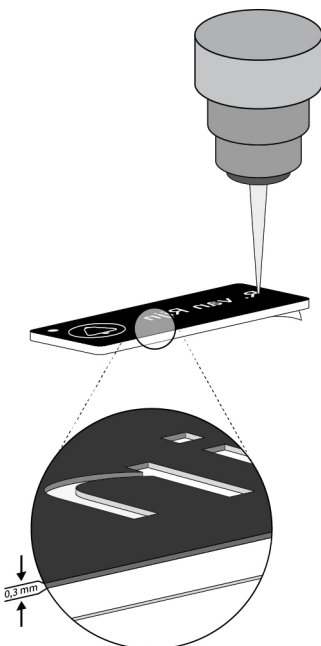
When ordering a personalised tag, a spare tag is always supplied.



1. First, remove the protective backing from one side of the adhesive and carefully attach it to the center of the tag.
2. Press firmly to ensure proper adhesion.
3. Remove the protective film from the other side of the adhesive.
4. Ensure that the bell symbol is positioned on the right-hand side when facing the intercom.
5. Position the tag neatly in the designated area on the intercom and press it firmly into place.
6. Remove the protective front film to reveal the final finish.

ENGRAVING THE NAMETAG

To engrave a nametag, do not apply the transparent adhesive yet.



1. Place the tag in reverse (mirror) orientation before engraving. The top side must remain at the top, but the bell symbol now appears on the left-hand side when viewed from above.
2. Perform the engraving from right to left in mirror image.
3. Once engraving is complete, turn the tag over lengthways so that the bell symbol is positioned on the right-hand side again, while keeping the top side at the top. The name now appears correctly oriented.
4. Apply the adhesive to the rear side of the tag and proceed with installation.
5. Once the tag is applied, remove the protective front film to reveal the final finish.

HIGH-END FINISH

After installation, carefully clean the intercom and visually inspect it to ensure a flawless, high-end finish before handover. This final step enhances the perceived quality of the product and removes fingerprints, dust, and installation residue.

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

ALUMINIUM FINISH

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.

BRASS FINISH

Use a soft microfibre 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 nametag 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 a soft, lint-free microfibre 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 microfibre 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 microfibre 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

PREREQUISITES

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

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

CONNECT THE DEVICE TO YOUR NETWORK

1. Connect the Robin device to the network via the network connection plug on the back.
2. The device boots automatically. This can take up to 60 seconds.

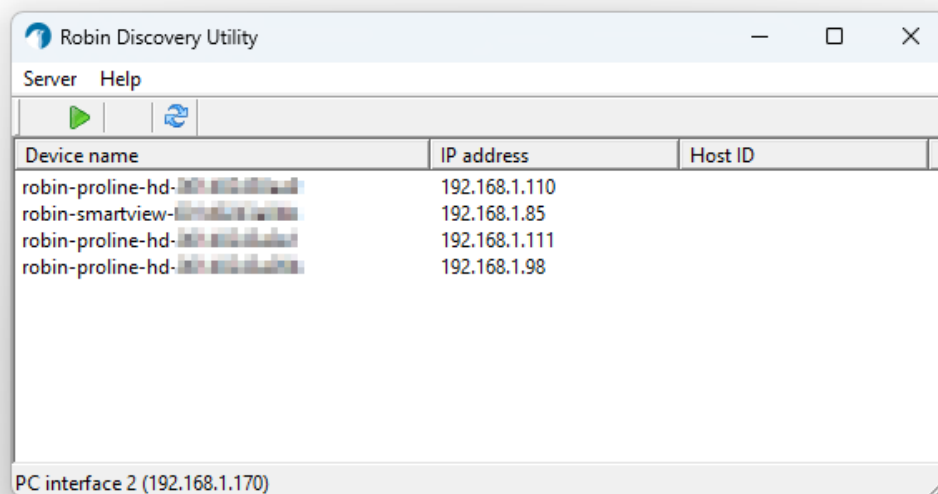


Ethernet and PoE connections are limited to 100 metres per cable segment (max), as defined by the Ethernet standard. This limit applies between two active network devices. Depending on cable quality, installation conditions, power requirements and the PoE equipment used, reliable operation may require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

ROBIN DISCOVERY UTILITY

Robin Discovery Utility applies to all Robin SIP models.

1. Copy the 'Robin Discovery Utility' software to a PC that is connected to the network.
2. Start the 'Robin Discovery Utility' software and click the "Play" button.
3. The software scans for Robin devices in the network. When a Robin intercom is detected, it is displayed in the list.
4. Double-click on the detected intercom you would like to configure.
5. The web interface of the selected Robin device appears.



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

CONFIGURATION

LOGGING IN TO THE WEB INTERFACE

1. Go to the IP address of your device (using a fixed IP, an IP scanner, or the Robin Discovery Utility).
2. You will automatically be directed to the login page of your device:



Username

Password

Login



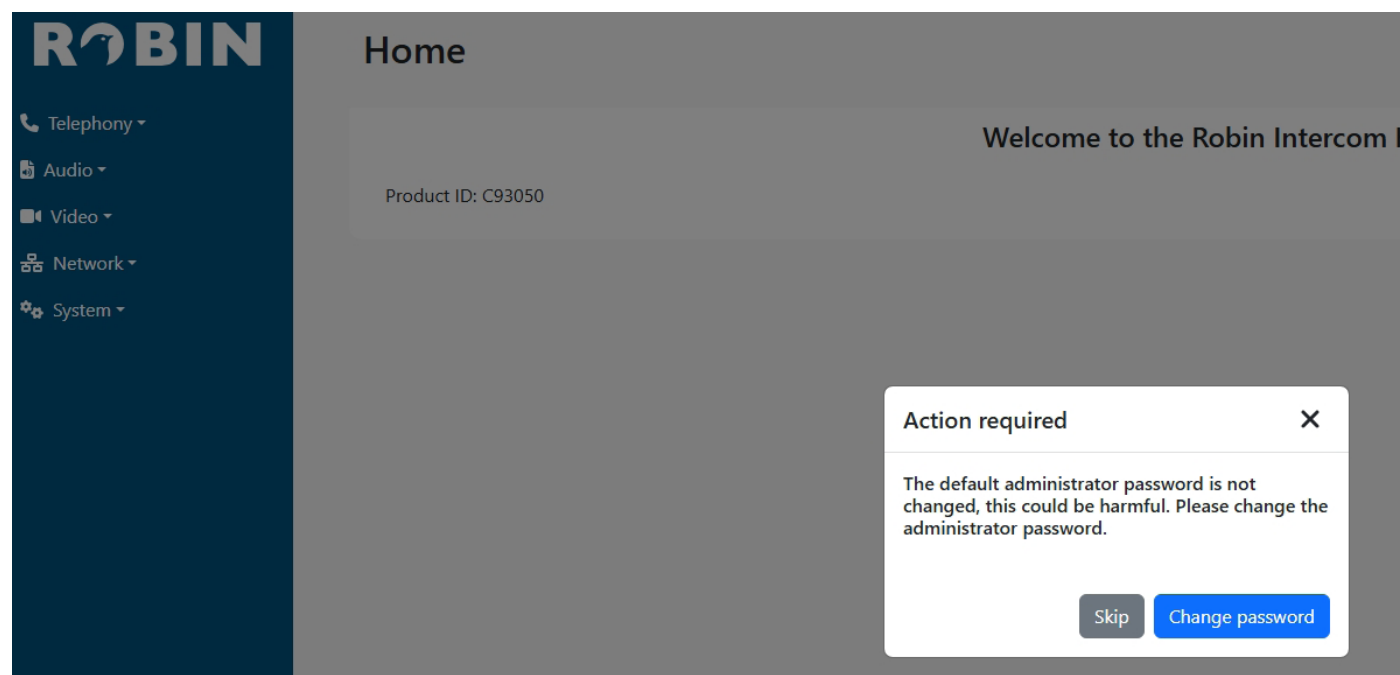
3. Log in with the following default credentials:

Username:	admin
Password:	123qwe

4. Click "Login" to continue.

SETUP

1. When you log in for the first time, the device prompts you to set a new password.



2. Select "Skip" to change your password later, or select "Change password" to immediately change your credentials to improve the security of the system.

Ensure that your credentials are retained and accessible at all times.

3. The essential system parameters must be configured to prepare the device for operation. Refer to the relevant chapters according to the technical requirements needed for your installation.

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

- IP configuration: The default setting is DHCP. It is recommended to assign a fixed IP address to ensure stable access and simplify future configuration changes. The system reboots after changing the IP address. (see [page 65](#) Network > IP)
- Connection with SIP, Teams or P2P: Follow the configuration provided in the following Telephony chapter to connect your device with your phone system provider, or configure your P2P connection. (see [page 51](#) Telephony > Peer-To-Peer)
- Configure your call buttons. (see [page 45](#) Telephony > Phonebook and Button Settings)
- Make sure your time and date settings are correct. (see [page 70](#) System > Clock)

By implementing these configurations, the system will be fully initialised and ready for immediate deployment.

For specific settings, the following chapters overview all possible settings and integrations that can be configured according to your needs and device type.



Some settings may not appear on your device. This manual covers all available options, but certain settings will only be shown if your device supports them. For example, video settings are not available on audio-only devices. If an option is missing, it is due to your device's capabilities. Unsupported features cannot be enabled by Robin or CDVI.

TELEPHONY

The Telephony section describes how the Robin intercom communicates using Session Initiation Protocol (SIP). Through SIP, the Robin device 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

The screenshot displays the Robin web interface for configuring SIP settings. On the left is a dark blue sidebar with the 'ROBIN' logo and a menu under 'Telephony' (SIP, Phonebook, Button Settings, Call Advance, Call Log, Control, Peer To Peer) and other system categories (Audio, Video, Network, System). The main area is titled 'Telephony' and has a 'Logout' button in the top right. Below the title are tabs for 'Account 1', 'Account 2', 'Account 3', and 'Account 4'. Under 'Account 1', there are 'General' and 'Advanced' tabs. The 'General' tab is active, showing a list of settings: 'Enable' (toggle on), 'Description' (text field 'Account 1'), 'SIP Protocol' (dropdown 'TCP'), 'SIP proxy / Registrar' (text field 'Enter host'), 'SIP Proxy port number' (text field '5060'), 'Line ID' (text field 'Enter username'), 'Username' (text field 'Enter auth_username'), 'Password' (text field 'Enter password'), 'Register' (toggle off), and 'Registration status' (text field). An 'Apply Settings' button is at the bottom right.

The first menu item under Telephony is the SIP configuration section. 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.

FIELD MENUS

Enable	Switches the account on or off
Description	Descriptive name for 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:

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. A username and a password will be provided or you will have the opportunity to define it. 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 ROBIN

The collected PBX credentials can now be entered into the Robin device's SIP configuration.

1. Select the tab "Account 1" (Keep it on General).
2. Fill in the blanks.

Telephony ▾

SIP

Phonebook

Button Settings

Call Advance

Call Log

Control

Peer To Peer

Audio ▾

Video ▾

Network ▾

System ▾

Telephony

Logout

Account 1

Account 2

Account 3

Account 4

General

Advanced

Enable:

☒

Description:

Account 1

SIP Protocol:

TCP ▾

SIP proxy / Registrar:

Enter host

SIP Proxy port number:

5060

Line ID:

Enter username

Username:

Enter auth_username

Password:

Enter password

Register:

☐

Registration status:

Apply Settings

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.

If the information is correct, the registration status displays "Registered".

MICROSOFT TEAMS

Integration of your phone system with Microsoft Teams requires a compatible SIP-to-Teams gateway. This guide focuses on the use of CyberGate only, for which an external licence is required.

1. Purchase your licence from the Microsoft [Azure Marketplace](#) or [Microsoft AppSource](#).
2. Go to <https://admin.cybergate.cybertwice.com>.
3. Login with your Microsoft credentials (additional authentication may be required using SMS, call or Authenticator).
4. Once logged in, you will see the Cybergate web interface.

CONFIGURING CYBERGATE



This 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.

After logging into 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.

1. Go to "Network Settings" and add your local IP or device location domain to the licence.
2. After that step, proceed to "Device".
3. Click "Add device" to add your device.
4. Use the username and password to program your Robin device in the next step: "Configuring Robin for Teams."

Add device

Status	Display name	Authentication username	Password
Built up configuration			
●	IP2 Server	NHTPXXXXXXXXXXXXXX1	QW1
CPE			
●	CPE ⚠	Z90XXXXXXXXXXXXXX1	CPE
Hearingsystem			
●	Voicemail Hearingsystem 30	WS6PXXXXXXXXXXXXXX1	TH1
●	Hearingsystem	3VVVXXXXXXXXXXXXXX1	TH1

CONFIGURING ROBIN FOR TEAMS

Telephony ▾

SIP

Phonebook

Button Settings

Call Advance

Call Log

Control

Peer To Peer

Audio ▾

Video ▾

Network ▾

System ▾

Telephony

Logout

Account 3

Account 4

General

Advanced

Enable:

Description:

SIP Protocol:

SIP proxy / Registrar:

SIP Proxy port number:

Line ID:

Username:

Password:

Register:

Registration status:

☒

Teams

TCP

cybergate.cybertwice.com

5060

COM1

Z90XXXXXXXXXXXXXX1

.....

☒

Registered

Apply Settings

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

SIP Protocol	TCP
SIP Proxy	cybergate.cybertwice.com
Line ID	"Display name" in CyberGate and should be identical
Username	Specified in the CyberGate profile
Password	Specified in the CyberGate profile

PHONEBOOK

PHONEBOOK TAB

In the "Phonebook" tab, you can add destinations and operators who can access the intercom. For example, you can assign a reception desk to receive calls when the "Call" button is pressed, as well as contacts who can call the intercom and receive audio and video.

If you plan to call the intercom using a SIP phone or app, it is recommended to add yourself (or each team member) as a contact. This allows you to define which codec the intercom uses, ensuring compatibility with your device.

Adding users is optional, but it enables you to assign specific codecs to incoming callers, improving compatibility for each device connecting to the intercom.

To add a new device, click "+ Add new entry" and set the following parameters:

Description	For example "Reception", or the recipient's 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 ¹	Add a logo for the specific contact in your Phonebook

¹ This feature is only available on models with a touchscreen.

PROFILES TAB

In Profiles, two default profiles are available for standard use and Teams. You can also create unlimited additional profiles for specific devices. Each profile allows you to configure codecs, payload types, and bitrate for your PBX or device. Once saved, profiles can be assigned to contacts in the Phonebook.

KEYPAD DIAL CODES TAB

The screenshot shows the Robin Telephony interface. On the left is a sidebar with the Robin logo and a 'Telephony' dropdown menu containing options: SIP, Phonebook (selected), Button Settings, Keypad Settings, and Call Advance. The main content area is titled 'Telephony' and has a 'Logout' button in the top right. Below the title are three tabs: 'Phonebook', 'Profiles', and 'Keypad Dial Codes' (which is active). In the 'Keypad Dial Codes' tab, there is a '+ Add new entry' button and a table with the following structure:

ID	First	Second	Third
John	Reception		

At the end of the row for 'John', there are two icons: a green checkmark and a red trash can.

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	Specify the identification, such as apartment number
First	The first number it should call
Second	The second number that the device should call
Third	Same function for a third number
Pin	A code that can be entered on 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 Access Control > PIN chapter. (see [page 62](#))

BUTTON SETTINGS

Telephony ▾

SIP

Phonebook

Button Settings

Call Advance

Call Log

Control

Peer To Peer

Audio ▾

Button-1

Call Priority

Timeslots

First:

Showroom X ▾

Second:

Select second ▾

Third:

Select third ▾

Apply Settings

This menu allows configuration of the “Button Settings”. By default, the number of available tabs (Button 1, Button 2, etc.) depends on the number of physical call buttons present on the device.

For intercom 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”¹.

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

Each button configuration is divided into two sections:

Call Priority	Defines the order in which numbers are dialed 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.
Timeslots	Whenever a visitor presses the button, the Robin intercom automatically evaluates the assigned schedule. If the current date and time fall within the configured schedule, the scheduled destination is called. If no schedule is active, the intercom automatically uses the default destination instead.

When your “SIP” is set up and running, the “Phonebook” configured and your “Button Settings” are completed, your system is ready for the first call.

¹ Models with touchscreen must have “Multiple” in the display settings.

TIMESLOTS

Robin intercoms support time-based call routing, allowing each call button to automatically route calls to different destinations based on the day and time. For example, calls can be directed to a reception desk during office hours and forwarded to a security desk, mobile phone, or on-call engineer outside business hours. The same approach can be used for weekends, holidays, or temporary opening hours without requiring manual reconfiguration.

The screenshot shows the Robin Telephony interface. On the left is a sidebar with the Robin logo and a menu: Telephony (selected), SIP, Phonebook, Button Settings, Keypad Settings, Call Advance, Call Log, Control, Peer To Peer, and Audio. The main area is titled 'Telephony' and has a 'Logout' button. Below the title is a tab for 'Button-1'. Inside this tab, there are two sub-tabs: 'Call Priority' and 'Timeslots' (which is active). A '+ Add new entry' button is in the top right of the Timeslots section. Below this is a table with two columns: 'Schedule' and 'Extension'.

Schedule	Extension
Office hours	
Night Desk	
Weekend	

Edit Entry



Edit Timeslot Item

☒ Schedule:

☒ Extension:

Apply Settings

Before a schedule can be assigned to a button, it must first be created under **System > Schedules** (see [page 83](#)). Once configured, navigate to **Telephony > Button Settings** to assign the schedule, define the destination used during the scheduled period, and configure the default destination for all other times.

Whenever a visitor presses a button, the intercom automatically evaluates the assigned schedule and routes the call to the appropriate destination. Schedules are managed centrally, allowing a single schedule to be assigned to multiple buttons. Any changes made under System > Schedules are immediately applied to all linked buttons, ensuring consistent call routing across the installation without requiring a reboot.

BUTTON EXTENDER

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.

Example

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 in 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:

1. Navigate to Telephony > Button Extender.
2. Click "Add extender".
3. Select one of the detected extenders from the list.
4. Confirm to associate it with the current intercom.

Once linked, the extender appears in the overview list and becomes active for button detection.

REGISTERING PHYSICAL BUTTONS

Once the extender is linked, the physical buttons must be registered.

1. Press each physical button one by one on the connected button panel. When a button press is detected the extender automatically registers the button and a new button entry is created in Telephony > Button Settings.
2. Configure each button 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.

KEYPADS SETTINGS ¹

When using a keypad-only or a touchscreen model, you can set instructions for the usage of the keypad. In this menu, you are able to set the following items:

Preset to call when I-button is pressed	Set a line/number that is called when the information 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 blocks all zeros entered before seeing the first digit which is not a zero.
Max preset length	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 communication device. The following parameters help you in bi-directional audio and/or video settings:

Auto answer	When activated, it automatically picks up a call when calling the intercom line number. When enabled, it also shows the auto answer delay: This option waits for X seconds before picking up automatically.
No answer timeout	This function automatically cuts the call after X seconds whenever a call is made.
Max call duration	This option defines the maximum time that a call can contain before automatically ending the call. This option is used as a fail safe so that any open calls don't remain open.
Early offer ²	When enabled, the intercom shows the video to a remote screen as soon as the call button is pressed. With this active, you are able to watch any video feed before answering the call.

CALL LOG

The Call Log menu provides an overview of all incoming and outgoing calls from the intercom.

It allows installers and administrators to verify call activity, confirm successful connections, and identify missed or failed call attempts. You also have the possibility to delete the call log entirely or partially.

Clear insight into call history supports faster troubleshooting, helps validate correct SIP configuration, improves maintenance efficiency, and overall system diagnostics.

CONTROL

The Control menu allows 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 signalling, 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.

The menu shows 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 "Hang up" button. The menu also shows the status of your SIP registration and any current call status.

¹ On models with keypad or touchscreen only.

² On models with video and support for early offer.

PEER-TO-PEER (P2P)

Peer-to-Peer (P2P) allows the intercom to establish a direct SIP connection with a SIP monitor or SIP telephone, without the need for a SIP server, PBX, or cloud service.

When a call button is pressed, the intercom sends a SIP INVITE directly to the configured device. Audio (RTP) and, where supported, video are streamed directly between both devices. In a P2P installation, the intercom is configured to call the SIP URL of the target device, which is typically assigned a fixed IP address or hostname. No SIP registration is required.

P2P can be used with the four available SIP accounts, allowing calls to be routed either directly to a P2P destination or via a SIP server. As call handling is performed by the intercom itself, the number of supported P2P destinations depends on the available system resources. P2P is therefore best suited to smaller installations, while larger or more complex systems should use a SIP PBX architecture.

WHEN TO USE P2P

Typical applications include private residences, small office buildings, workshops, warehouses, retail stores, and start-up companies where only a limited number of users need to receive intercom calls.

It is also suited for apartment buildings where each intercom button calls a dedicated indoor station or SIP endpoint directly, without requiring a central telephone system.

Example

Smaller companies may initially route calls directly to employees' SIP phones or softphones using P2P. As the organisation expands and requires features such as call groups, reception services, voicemail, or Microsoft Teams integration, the installation allows for migration to a SIP PBX without replacing the Robin intercom itself.

SET UP AND CONFIGURE P2P ON YOUR DEVICE

To set up P2P on your device, follow the steps below:

1. Both the intercom and the receiving device (monitor or phone) must be configured accordingly. Ensure that both devices are assigned a fixed IP address. For the Robin intercom, IP configuration is found under Network > IP. (see [page 65](#))
2. Verify with the system administrator that the SIP communication port (default 5060) is open and accessible between both devices.
3. Go to "Peer-to-Peer" under the "Telephony" menu:

The screenshot shows the Robin web interface. On the left is a dark blue sidebar with the 'ROBIN' logo at the top. Below the logo is a 'Telephony' menu with a dropdown arrow. The menu items are: SIP, Phonebook, Button Settings, Keypad Settings, Call Advance, Call Log, Control, and Peer To Peer (which is highlighted in a lighter blue). The main content area is white and titled 'Telephony' in a large, bold font. In the top right corner of this area is a blue 'Logout' button. Below the title are three tabs: 'Settings' (active), 'Phonebook', and 'Profiles'. The 'Settings' tab contains a toggle switch for 'Peer to peer', which is currently turned on (blue). Below the toggle is a horizontal line, and at the bottom right of the settings area is a blue 'Apply Settings' button.

The **Actions** column provides two quick testing functions. Clicking the green telephone icon immediately initiates a call to the selected destination, allowing the configuration to be verified without pressing a physical call button. The red telephone icon terminates an active call.

Click the **Edit** button to edit existing entries at any time. Permanently remove an existing entry clicking the **Delete** button. Any changes are applied immediately and become available throughout the system.

Once an entry is created, it can be selected in button configurations, schedules, or other telephony features, ensuring consistent and centralised management of all call destinations.

PROFILES

Profiles define the media parameters that are used when establishing P2P SIP calls. Instead of configuring codecs and video settings for every individual destination, these settings are grouped into reusable profiles that can be assigned to one or more phonebook entries. This allows different devices or telephony platforms to use their own optimised media configuration while keeping the overall configuration simple and consistent.

Description	Codec	Video Resolution	Actions
Default	uLaw, aLaw, opus, g722, h264	1280x720	
Teams	uLaw, aLaw, opus, g722, h264	1920x1080	
CDVI	uLaw, aLaw, opus, g722, h264	1280x720	
	uLaw, aLaw, opus, h264	1280x720	

Each profile contains a pre-defined list of supported audio and video codecs and the preferred video resolution. During call setup, the Robin intercom negotiates the available codecs with the remote SIP end-point and automatically selects the best compatible combination. If video is supported by both devices, the configured video resolution is used whenever possible.

To create a new profile, click “Add new entry” and specify the desired codec order and video resolution. In most installations, the default profile provides the recommended codec configuration and requires no further modification.

Additional profiles should only be created when specific SIP platforms or network conditions require different codec priorities or video resolutions. For example: One profile may be optimised for a specific SIP-monitor, another for a SIP phone, while a third can be configured for low-bandwidth network connections.

Any changes to a profile automatically affect every phonebook entry that uses that profile, making it easy to update media settings throughout the entire installation from a single location.



Peer-to-Peer shares the same Profile database as the (SIP) Phonebook configuration. As a result, Microsoft Teams profiles may also appear within the Peer-to-Peer configuration. However, P2P is not supported with Microsoft Teams applications or compatible devices: Microsoft Teams desktop and mobile apps, Teams-certified phones - unless differently specified by the device.

AUDIO

The Audio section enables you to 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 allow you to configure the intercom's following audio behaviour:

Speaker volume	Adjusts the output level of the built-in speaker on a scale from 0 to 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 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 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: - 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

- Telephony ▾
- Audio ▾**
- Settings
- Detection
- Media
- Video ▾
- Display ▾
- Access-Control ▾

Audio

Logout

Detection

Audio Detection Chart Enabled

The Audio Detection section configures sound-based event detection using the built-in microphone. This function is useful for triggering 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 is triggered. The corresponding actions, such as sending a notification or activating a relay, are configured in the System > Events section. (see [page 70](#))

MEDIA

The Media section manages 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.

Click "Add new entry" to upload additional audio files and fill in the following fields:

Name	Define the name of the custom sound, which will be listed in the Media Mapping tab.
File upload	Select the audio file to upload. Supported formats are WAV (8-bit, 16000 Hz, PCM) or MP3 (128 kbps).

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 assigns custom audio files to specific phone events. For each entry, select a Phone Event and link it to one of the uploaded custom media files. This allows installers to personalise the acoustic behavior of the intercom according to project requirements.

Phone Events	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 uses the standard default sound for that event.

VIDEO

The Video section describes how the Robin intercom's integrated camera is configured and used: View live video, adjust image and encoder settings, and define how video is processed and transmitted.

These settings allow the video performance to be optimised 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 from the intercom camera directly from the web interface. This page is view-only (no settings can be changed). The image shown reflects the device's active video configuration.

It is mainly used during installation and commissioning to verify camera positioning, focus, lighting conditions, and overall image quality.

If On-Screen Display (OSD) is enabled in Video > Settings, elements such as date, time, or custom text overlays appear in the video. These settings apply to all video streams, including RTSP (see *Network > RTSP* [page 62](#)), so any changes affect both the Live view and connected RTSP clients.

SETTINGS

The Settings section configures 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	HDR = High Dynamic Range. When toggled it improves image quality in high-contrast scenes (e.g. backlit entrances) by balancing bright and dark areas.

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

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 On-Screen Display (OSD) configuration, 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 to be added to the video overlay

The Device name and Device location are defined in System > Device, under the Identity tab (see [page 69](#)). Any changes made there are 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 configures the intercom camera's motion detection and shows a live video feed for setup. Define detection zones by drawing one or more rectangles directly on the image. Motion is only detected within these areas, allowing you to ignore irrelevant background movement such as public roads or trees and focus on specific zones of interest.

Enabled	Toggle to activate or deactivate motion detection. When disabled, no motion events are generated.
Sensitivity	Slide to determine how easily movement is detected. Higher sensitivity increases the likelihood that small changes in the image triggers detection. Lower sensitivity reduces false triggers caused by minor lighting variations or small movements.
Object size	Slide to define the minimum size of movement to be considered 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 is triggerable. The actual action that follows, such as sending an email, activating a relay, or notifying an external system, is configured in System > Events. (see [page 70](#))

STREAMS

The Streams section provides an overview of all currently active video streams. 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	Indicates 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

The Display settings let you customise the intercom interface to match your project's identity and requirements. This includes layout, typography, on-screen controls, and video presentation.

By aligning the touchscreen interface with the aesthetic and operational needs of the location, you ensure a consistent, refined and intuitive user experience, whether the device is installed in a residential entrance, corporate lobby, or architectural environment.

OVERVIEW



Scrambled keypad mode



Single button mode

SETTINGS

LAYOUT SETTINGS

- Telephony ▾
- Audio ▾
- Video ▾
- Display ▾
 - Settings
- Access-Control ▾
- Network ▾
- System ▾

Display

Logout

Layout Settings

Upload Logo

Layout:

Single ▾

Display name:

Robin

Show hangup button:

☒

Show keypad button:

☒

Show pincode button

☒

Scramble digits on the pincode screen:

☒

Font face:

Standard ▾

Font size:

Medium ▾

Font color:

Wit ▾

Background color:

Video Mode:

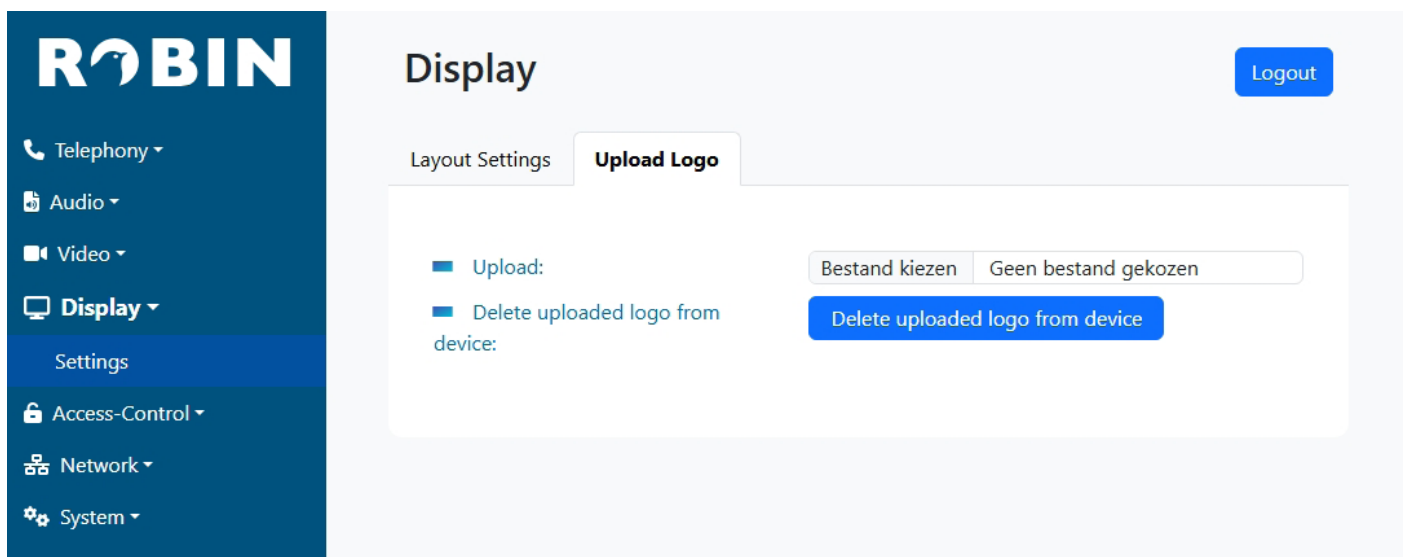
Full video ▾

The Layout Settings define the visual structure 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. It offers a clean and focused presentation with a pulsating call-button for user-friendly access, ideal for residential or single-tenant environments. ● Multiple: Displays multiple contacts or selectable elements simultaneously. Suited for multi-tenant buildings or installations requiring direct selection from a list, with scrolling options and the ability to upload a logo as a button.
Display name	Defines the name shown on the screen. Used for branding, building identification, or functional labelling.
Show keypad button	Activates the keypad shortcut on the main screen, allowing users to manually enter a call number.
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	Randomises the numeric keypad layout each time the PIN screen is opened. This enhances security by reducing the risk of code observation.

Font face	Defines the typography style used across the interface: • Classic: A traditional typeface (formal and neutral appearance). • Standard (default): A modern and balanced typeface (optimal legibility). • Handwritten: A more informal typeface (suitable for hospitality or residential contexts for a softer visual identity).
Font size ¹	Select the text size for readability. Depends on mounting height and viewing distance • Extra small, Small, Medium (default), Large, Extra large
Font color ²	Defines the colour of the on-screen text • Black, White (default)
Background color	Customise the interface background colour using the RGB colour picker tool. Ensure alignment with architectural finishes or corporate brand 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



Personalise the interface with a custom logo to reinforce brand identity or site-specific presentation if required.

Upload	Upload a logo file from a local device. Once applied, the logo only shows in "Single" mode. For multiple logos, consult Telephony > Phonebook. (see page 45)
Delete uploaded logo from device	Removes the currently stored logo from the device

¹ Larger sizes are recommended for installations where the intercom is mounted higher or where accessibility considerations apply.

² The selected color should provide sufficient contrast with the chosen background color for optimal readability.

ACCESS CONTROL

ID	Activate Internal Relay
John Doe	false
Mike Smith	true

The Access Control section enables secure entry using PIN codes directly on the intercom’s touchscreen, without the need for external readers or additional hardware.

Each entry is configured individually and linked to the internal relay, allowing flexible use in residential, commercial, or mixed-use installations while maintaining a simple and secure user experience.

For larger or more advanced access control setups, such as multi-door control, credential management, and audit logging, integration with a dedicated CDVI system like ATRIUM KRYPTO is recommended.

PIN

The PIN section gives 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, you can create, edit, or remove entries.

ADDING A NEW ENTRY

Select “Add new entry” to create a new PIN configuration.

Edit Entry
X

New Preset

ID:

John

Pin:

....

Activate Internal Relay:

☐

Apply Settings

Define the following parameters:

ID	Enter a unique name or reference for the PIN entry. This field is used for admin 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. Use sufficiently complex codes to reduce the risk of unauthorised access.
Activate Internal Relay	Enable this option to trigger the internal relay when the correct PIN is entered. This typically unlocks the door or activates the configured output.

EDITING AN ENTRY

Modify existing entries at any time to:

- Update the identification label.
- Change the PIN code (codes cannot be viewed).
- Enable or disable relay activation.

Changes take effect once the updated settings are applied.

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 BEHAVIOUR

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 ATRIUM or CENTAUR.

NETWORK

The Network section describes how the Robin intercom is connected to and communicates within an IP network. 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

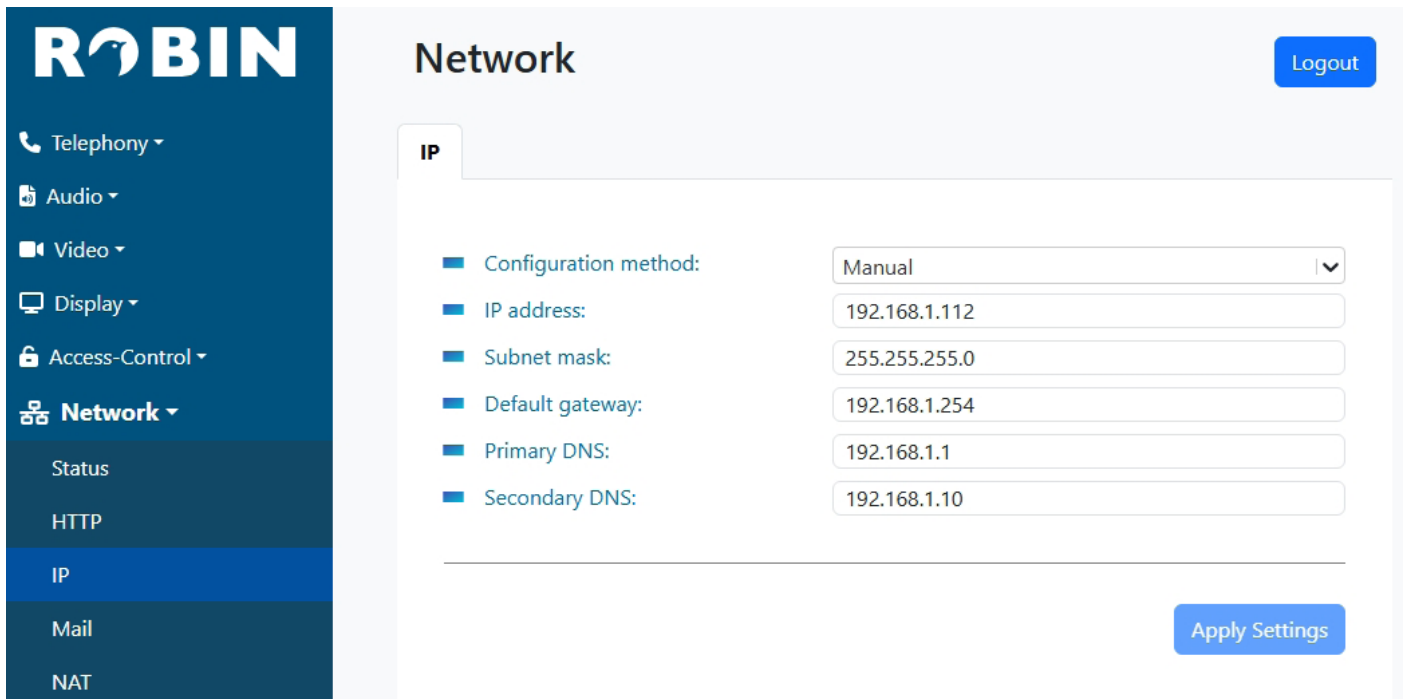
The Status section gives a real-time overview of the intercom's network connection. This page is informational only. It is intended to help installers verify connectivity and quickly diagnose network-related issues.

MAC address (Media Access Control address)	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.
IPv4	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 IP page 60)
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 indicates this accordingly.
IPv4 link-local address	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 configures how the intercom's web interface is accessed over the network.

HTTP Port	Defines the HTTP port used for standard web access. By default, HTTP typically uses port 80. Adjust the port if required by the network environment or security policy.
HTTPS	When HTTPS is enabled, 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.
Self-signed certificate	The system includes a self-signed certificate by default, allowing secure access without additional configuration. For professional or public-facing installations, it is recommended to use a trusted certificate issued by a recognised Certificate Authority. Manage certificates in System > Certificates (see page 82). Upload, install, and manage certificates. They will be available for selection in the HTTPS configuration.



The screenshot shows the ROBIN web interface. On the left is a dark blue sidebar with the ROBIN logo and a menu with options: Telephony, Audio, Video, Display, Access-Control, Network (selected), Status, HTTP, IP (highlighted), Mail, and NAT. The main content area is titled 'Network' and has a 'Logout' button in the top right. Below the 'Network' title is a tab labeled 'IP'. The IP configuration section contains several fields: 'Configuration method' (set to 'Manual'), 'IP address' (192.168.1.112), 'Subnet mask' (255.255.255.0), 'Default gateway' (192.168.1.254), 'Primary DNS' (192.168.1.1), and 'Secondary DNS' (192.168.1.10). An 'Apply Settings' button is located at the bottom right of the configuration area.

The IP section configures how the intercom obtains its IPv4 network settings.

Choose between **automatic** (DHCP) or **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 the internet or other networks. 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 (especially if the IP address was modified).

MAIL

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

SERVER

Configure the outgoing mail server (SMTP) in the Server tab.

Server name	You must enter the server name (e.g. mail.provider.com). This is the address of the SMTP server that handles outgoing emails.
Encryption	Select the encryption method: 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 creates a list of predefined recipients.

Each entry consists of a Name and an Address field (e.g. John and john.doe@domain.com). These entries can be used later when configuring event-based email notifications, reducing the need to manually re-enter email addresses. Add multiple entries to build a structured list of recipients for different purposes.

TEST

The Test tab verifies the SMTP configuration.

To	Enter the email address to which the test message should be sent
----	--

After initiating the test, the system attempts to send an email using the configured SMTP server.

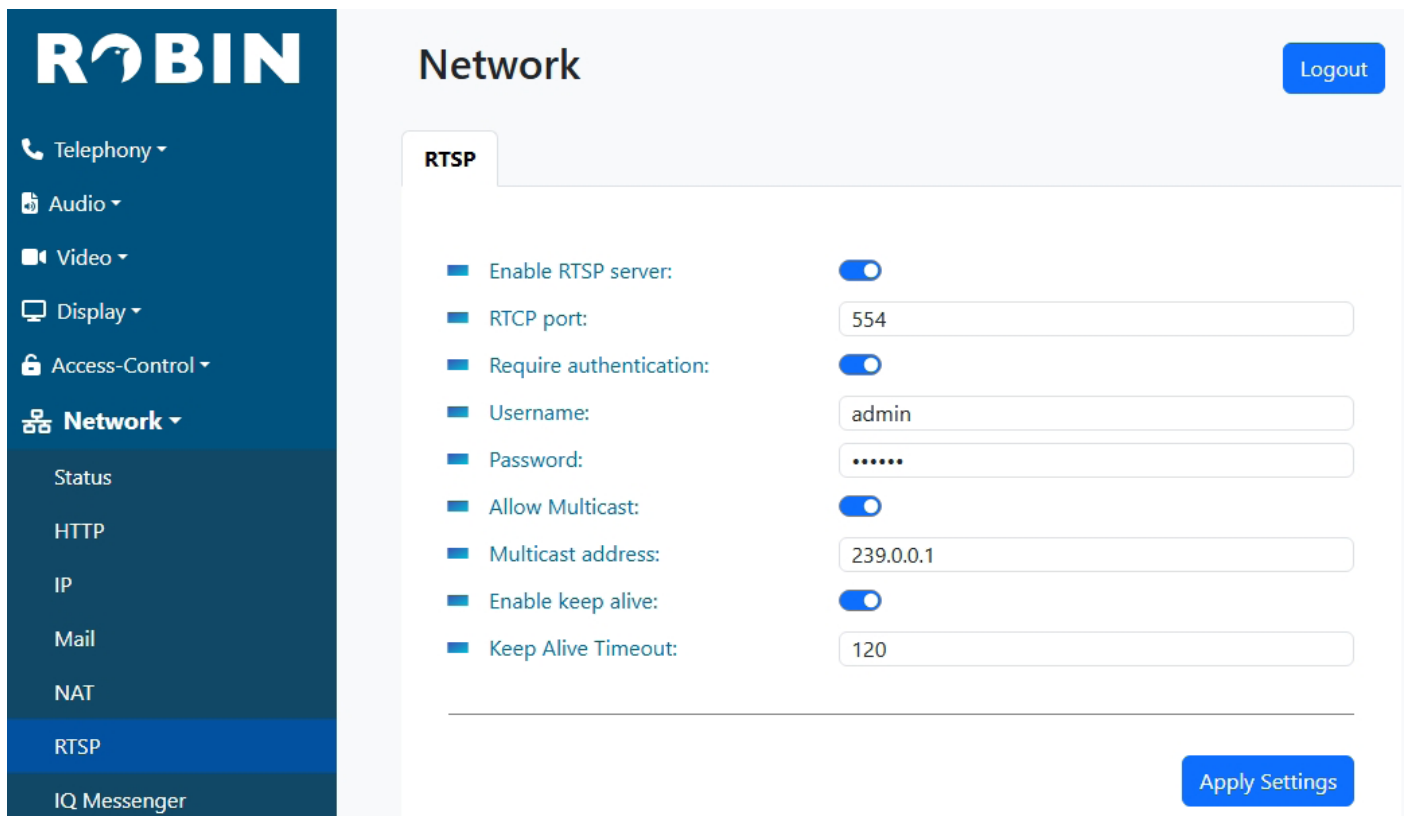
The SMTP test result is displayed on the same page, indicating whether the message was successfully sent or if an error occurred. This function is useful for validating server settings, encryption configuration, and network connectivity.

NAT

The NAT section enables or disables 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, usually no changes are necessary.

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



The screenshot shows the Robin web interface. On the left is a dark blue sidebar with the 'ROBIN' logo at the top and a list of menu items: Telephony, Audio, Video, Display, Access-Control, Network (highlighted), Status, HTTP, IP, Mail, NAT, RTSP, and IQ Messenger. The main content area is titled 'Network' and has a 'Logout' button in the top right. Below the 'Network' title is a tab labeled 'RTSP'. The RTSP configuration section contains the following settings:

- Enable RTSP server:** A toggle switch that is currently turned on.
- RTCP port:** A text input field containing the value '554'.
- Require authentication:** A toggle switch that is currently turned on.
- Username:** A text input field containing the value 'admin'.
- Password:** A text input field with masked characters (dots).
- Allow Multicast:** A toggle switch that is currently turned on.
- Multicast address:** A text input field containing the value '239.0.0.1'.
- Enable keep alive:** A toggle switch that is currently turned on.
- Keep Alive Timeout:** A text input field containing the value '120'.

An 'Apply Settings' button is located at the bottom right of the configuration area.

The RTSP section configures the Real-Time Streaming Protocol (RTSP) server of the intercom.

By default, RTSP is disabled. When enabled, the device provides a direct video stream to compatible video management systems (VMS), NVRs, or third-party applications. Once the RTSP server is enabled, the following 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 is adjustable.
Require authentication	When enabled, access to the RTSP stream requires a username and password. This is strongly recommended to prevent unauthorised 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	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 explains how to integrate the Robin intercom with an IQ Messenger system. This integration enables the intercom to send event-based notifications (i.e. a doorbell button 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.

Proper setup should always be coordinated with the IQ Messenger administrator to ensure correct integration and workflow behaviour.

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 message type sent to IQ Messenger. This value must correspond to a predefined 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.

Press "Apply Settings" to store and activate the configuration.

SYSTEM

The System section contains settings that control the general operation and behaviour of the Robin intercom. Here, you can configure device identity, scheduling, security options, event handling, and maintenance functions for monitoring, troubleshooting, and long-term system management.

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 for information purposes only. It is useful for diagnostics, maintenance, and support.

The following items 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

IDENTITY

The Identity tab contains descriptive information about the intercom to help identify the device within larger installations or management systems.

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. (see page 56)
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.

LOGS

The Logs tab allows downloading of 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 configures the date and time settings of the intercom. Accurate time configuration is essential for event logging, video overlays, scheduling, and system synchronisation.

Time zone	Defines the geographical time zone in which the device is installed. This 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 synchronises its internal clock with a time server over the network.
NTP server address	Defines the address of the NTP server used for time synchronisation (e.g. pool.ntp.org). Adjustable if a local or company-specific NTP server is required.
NTP status	Shows the current synchronisation status, including the server with which the device is synchronised. This confirms whether the clock is correctly aligned with the selected NTP source.

It is recommended to use NTP synchronisation whenever a network connection is available.

Press "Apply Settings" to store and activate the configuration.

EVENTS

The Events section enables logic-based automation within the intercom. Events link a Source (what happens) to an Action (what the system must do). This flexible structure enables customised 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 (not what should happen once the event is triggered). It represents an event detected by the system.

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	Minimum time (in seconds) that the source remains active once triggered

When creating a new source, define the following parameters:

	Selects the type of trigger: • Audio: Triggered when the configured audio threshold and duration are exceeded. (see page 54 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 change. This can include call start, call connected, or a call ended conditions depending on the configuration. • DTMF: Triggered when a DTMF tone is received during an active call. The specific DTMF key is configurable. • HTTP: Triggered when a specific URL is called. By default, the URL is <a href="http://<ip-address>/evmgr/emit">http://<ip-address>/evmgr/emit. The endpoint "emit" is configurable. (see page 64 Network > HTTP)
Source type	• Input1: Triggered when the physical input on the rear of the device is activated. • Motion: Triggered when motion is detected within configured video detection zones. (see page 57 Video > Motion) • None: No source. • Ring: Triggered when the intercom starts ringing. • Timer: Triggered based on a timer interval. The event is activated every configured number of seconds. The interval is configurable. • Busy: Triggered when an outgoing call receives a busy response. • Preset¹: Triggered when a preset is activated. Configuration is available under Telephony > Phonebook > Keypad Dial Codes. (see page 50) • Pincode¹: Triggered when a valid PIN code is entered. Configuration is available under "Access Control". (see page 62)
Name	Descriptive name for the source
Enable	Activates or deactivates the source
Minimum duration	Defines how long the condition remains active

¹ Only for 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 (e.g. Call, Relay control, IQ Messenger, etc.)
Schedule	Defines whether the action is limited to a specific schedule

When creating a new action, configure the following parameters:

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: Virtually triggers the call button on the device • Call Phonebook: Establishes a call with someone in the Phonebook. Adds the item "Phonebook Entry" and "Allow call hangup" • HTTP: Consult the "HTTP" in this section (<i>see next page</i>) • None: No action (e.g. testing) • Playback: Plays a sound from the library (<i>see page 55 Audio > Media</i>) • Switch1: Triggers the internal relay • Webrelay: Consult "Webrelay" in this section (<i>see page 75</i>) • MQTT: Consult "MQTT" in this section (<i>see page 78</i>) • IQ Messenger: Consult "IQ Messenger" in this section (<i>see page 80</i>)
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 (e.g. Rising)
Schedule	Optionally links the action to a schedule defined in System > Schedules (<i>see page 83</i>)

Create customised workflows by combining Sources and Actions. For example, when the call source is triggered (button pressed), the system performs a call action, activates a relay, sends a notification, or triggers 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 either responds to commands received from external systems or sends notifications and data to external servers. This makes the device highly flexible and suitable for advanced automation scenarios.

Two different mechanisms are available:

HTTP Source	Allows an external system to trigger an event inside the intercom by calling a specific URL
HTTP Action	Allows the intercom to send an HTTP request to an external server when a defined event occurs

HTTP SOURCE

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 executes linked Actions.

1. 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.

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.

2. CONFIGURATION FIELDS

Source type	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 unauthorised triggering
Minimum duration	Defines how long the trigger must remain active. For HTTP triggers this is usually set to 0 or 1 second

Example

Test the above. Open a browser and enter: <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 executes immediately.

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

HTTP ACTION

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.

1. HOW IT WORKS

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

2. CONFIGURATION FIELDS

Action type	Select HTTP as the action type
Name	Assign a name that makes sense 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. <i>Example: https://example.com/api/doorbell</i>
Start body	Defines the content that is sent in the request (mainly used with POST) <i>Example JSON body:</i> <pre>{ "device": "FrontDoor", "event": "button_pressed" }</pre>
Use HTTP auth	If enabled, the intercom uses 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

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.

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

WEBRELAY

The Webrelay function allows the intercom to control an external relay module to operate doors, gates, barriers, or other electrical devices without using the intercom's built-in relay. It is a standalone PoE network device with one or more relay outputs which are controlled via HTTP commands. When properly configured, the intercom sends a command to the Webrelay whenever a defined event occurs.

Before configuring the Webrelay in the Events 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.

1. Navigate to the Password section
2. Define a username and password (use a strong password)
3. Save the settings

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

WIRING AND CONFIGURING 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 that is being controlled.

Fail Secure (working current)	Fail Safe (resting current)
Only activates when triggered	Remains energised to stay locked and releases when power is interrupted
Connect circuit through C and NO	Connect circuit through C and NC
Contact only closes when the relay is activated	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 required relay contacts.
- Ensure that the electrical ratings of the relay (voltage and current) are not exceeded.
- Each relay must be configured according to the intended application.

WEBRelay™ Quad-LS

Setup

Network Password Relay 1 Relay 2 Relay 3 Relay 4 Control Page

Control Page Setup:

Main Header Text: Webrelay Quad

Auto Refresh Page: Yes ☐ No ☒

Duration: 1 sec

Relay 1 Setup:

Relay Description: Relay 1

Display Relay Status: Yes ☐ No ☒

Status ON Color: Gr ☐ Rd ☐ Yllw ☐ Bl ☐

Status ON Text: Relay ON

Status OFF Color: Gr ☐ Rd ☐ Yllw ☐ Bl ☐

Status OFF Text: Relay OFF

ON/OFF Buttons: 0 ☐ 1 ☐ 2 ☒

Button1 Label: ON

Button2 Label: OFF

Pulse Button: Yes ☐ No ☒

Pulse Button Label: Pulse

Pulse Duration: 1.5 secs

Submit Reset

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

Relay Description	Assign a logical name, such as "Front Door" or "Gate"
Display Relay Status	Optional. Enable 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 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 on the intercom side.

CONFIGURE WEBRELAY IN ROBIN

Once the Webrelay device is configured with a fixed IP address and secured with a password, it is ready to be linked to the intercom via the Event Manager menu:

1. Navigate to System > Events > Actions.
2. Create a new Action and select Webrelay as the Action Type.
3. Action configuration:

Action Type	Select "WebRelay"
Name	Assign a name that makes sense, such as "Open Front Door" or "Gate Pulse"
Enable	Enable to activate the action
Web relay IP address	Enter the fixed IP address configured in the Webrelay device
User account locked	When enabled, the user account is locked and cannot be used for login <i>Example: 192.168.1.99</i>
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 strikes and access control applications - On: Switches the relay permanently on until another action switches it off - Off: Switches the relay off
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 <i>Example: Button-1</i>

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

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 does 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.

MQTT ACTION CONFIGURATION

1. Navigate to System > Events > Actions menu.
2. Create a new action and select MQTT as the Action Type.
3. Configure the action:

Action type	Select MQTT
Name	Assign a name that makes sense, such as "Notify Automation" or "Doorbell MQTT"
Enable	Enable to activate the action

Host	Enter the IP address or hostname of the MQTT broker <i>Example: 192.168.1.100 or mqtt.example.local</i>
Port	Enter the MQTT broker port Default MQTT port is 1883
Topic	Define the MQTT topic where the message will be published. Topics are case-sensitive and follow a hierarchical structure using forward slashes. <i>Example: building/frontdoor/button</i>
Message	Enter the message payload that will be sent when the Source is triggered This can be plain text or JSON <i>Example (simple text):</i> <i>pressed</i> <i>Example JSON format:</i> <pre>{ "device": "FrontDoor", "event": "button_pressed" }</pre>
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
Use authentication	Enable this option if the MQTT broker requires username and password authentication
Source	Select the Source that should trigger the MQTT message <i>Example: Button-1, Motion, Call, etc.</i>
Trigger edge	Typically set to Rising to avoid duplicate messages
Schedule	Optionally restrict publishing to certain days or time periods

Example

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.

DIFFERENCE FROM STANDARD OPERATION

When integrating an intercom with IQM, the device does not operate in the standard SIP calling mode. Instead of initiating a direct SIP call when the button is pressed, the intercom sends an HTTP message to the IQM server. IQM processes the event, distributes the notification within the system, and can optionally initiate a SIP callback to the intercom when required.

In the IQM environment, a device must first be defined (e.g. Device code: "robin000001"). 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 recognises 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.

INTERCOM CONFIGURATION

The integration is configured under System > Events. (see [page 70](#))

- 1. Create a Source:** In most cases, this is a physical call button. The source only detects the button press. It does not contain the IQ Messenger logic itself.
 - Enable the Source.
 - Configure its minimum duration (typically one second).
- 2. Create an IQ Messenger Action:**
 - 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.
- 3. Configure IQ Messenger Parameters:**
 - The Type must match the type configured in IQM (typically Bell1).
 - The Device code must match the code created in the IQM environment.
 - The Message defines the text that will appear in the IQM application.
 - The Callback contains a SIP extension for return calls.
 - The Start URL must contain the full IQM server endpoint.
 - 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.

SECURITY

The Security section configures 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 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 unauthorised 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.

TOKENS

The Tokens tab creates and manages authentication tokens for secure communication with external systems or applications. Tokens provide an alternative to username/password authentication for API or system integrations.

1. Click "Add new entry" to add a new token.
2. Enter a name or description.
3. Toggle the button to enable or disable each token.

API

The API tab enables or disables API access to the intercom.

When API access is enabled, external systems 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 manages 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 gives an overview of all certificates installed on the device.

For each certificate, the following information is displayed:

Name	The certificate's identifier
Status	Indicates whether the certificate and private key are correctly installed and valid
Valid	Shows the certificate's validity

Open the certificate's information to view additional details. 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 (example: SHA256 with RSA encryption)
Public key algorithm	Indicates the public key type 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

CSR

The CSR (Certificate Signing Request) tab generates a certificate signing request. This is used when requesting a trusted certificate from a Certification Authority.

The following fields must be completed:

Name	Internal name for the certificate request
Key length	Defines the length of the generated key (example: 2048 bits)
Digest	Specifies the hashing algorithm used for the request (example: sha256)
Common Name (CN)	The fully qualified domain name (FQDN) of the device (example: intercom.company.com)
Department (OU)	Organisational unit within the company
Organization (O)	Company or organisation 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

Click 'Generate CSR' to create the certificate signing request. Then submit the generated CSR to a Certification Authority to obtain a signed certificate and then subsequently install it on the device.

SCHEDULES

The Schedules section defines time-based schedules without pre-defined limits. Schedules are typically used to activate or restrict certain actions during specific days or time periods.

The main page provides an overview of all configured schedules. Click "Add new entry" to create a new schedule.

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

Name	Describes 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 to every day of the week - Weekdays: Applies from Monday to Friday - Weekend: Applies on Saturday and Sunday - Monday through Sunday: Allows selection of individual days
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, click "Apply Settings" to store the schedule.

Configured schedules can be referenced in other sections of the system to control when certain actions are allowed or executed. (see *System > Events* [page 65](#))

SOFTWARE

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

UPDATES

The Updates tab checks 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. The system detects when a new version is available and informs the administrator. However, installation must be performed manually to ensure minimal disruption and prevent unexpected reboots or temporary service interruptions during critical use.

BACKUP

The Backup tab enables downloading of the current system configuration as a backup file (backup.txt).

This file contains the device settings and is 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 enables 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 gives direct manual control of the relay. It is mainly used for testing and commissioning during installation.

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.

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.

- Telephony ▾
- Audio ▾
- Video ▾
- Display ▾
- Access-Control ▾
- Network ▾
- System ▾**
 - Device
 - Clock
 - Events
 - Security
 - Certificates
 - Schedules
 - Software
 - Relay

System

Logout

Control

DTMF

To open:

##

To keep open:

90

To close:

91

Pulse time:

4

Play sound when active:

☒

Hangup after opening:

☐

Close door after hanging up:

☒

Label for pulse action:

Pulse

Label for on action:

Open

Label for off action:

Close

Apply Settings

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	Enable to play an audible confirmation sound when the relay is activated
Hangup after opening	Enable to automatically terminate the call after the relay is activated
Close door after hanging up	Enable to automatically return the relay 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

Click "Apply Settings" to store the changes 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 captures network traffic for analysis. This function is primarily intended for installers or support engineers familiar with network analysis tools.

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	Defines 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 is used for advanced diagnostics and may be requested by technical support

GO TO ROBIN

The Go to Robin tab creates a secure remote connection between the intercom and Robin support. This function should only be enabled when remote support is required.



Contact your **local CDVI Technical Support** team before initiating a remote connection with Robin. CDVI will guide you and advise the need for direct remote connection. (see [page 3](#) for contact details)

Connect	Establishes a secure VPN tunnel to Robin. Once connected, a Robin technician is able to 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.

LIGHTING¹

The Lighting section configures the illumination of the device. This includes the name tag backlight, 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 setting adjustments for the name tag backlight or the screen brightness, depending on the device model. This ensures visibility, readability, and energy efficiency in different lighting 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	Brightness level of the ambient lighting during daytime conditions
Night	Brightness level during nighttime conditions
Call	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	Allows manual override of the lighting mode for testing and installation purposes. Select an option from the drop-down menu: Off, Day, Night, and Call. Typically used during commissioning to verify brightness levels and visual effect without waiting for environmental light changes or a call event.

¹ On models with ambient lighting: Proline, Doorbell & Robin Touch.

SMART HOME CONFIGURATION

For smart home devices (Robin Doorbell), configuration options are more limited to match the ease of integration in your home ecosystem.

WIRING

Wire your device using a PoE switch or use the supplied PoE Injector to connect your device to the network switch or modem.

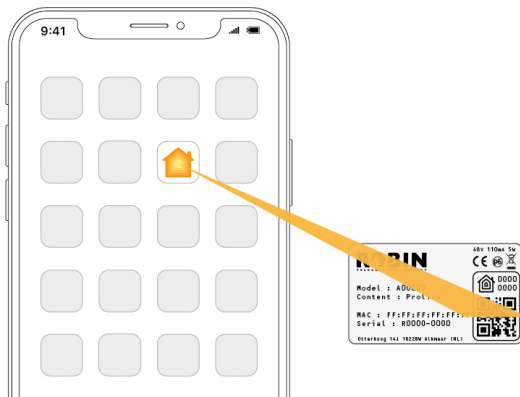
This device is wired the same way as the Robin SIP models (*see Wiring [page 30](#)*), with the only difference that the internal relay is exclusively used for a wired door chime.

Boot up the device after wiring. It will automatically receive an IP address using DHCP.

ADDING THE DEVICE TO HOME



A hub (**Apple TV** or **HomePod (mini)**) is required to use this device.



Follow the steps below once your device is connected and has received an IP address:

1. Open the Home app on your iPhone or iPad.
2. In the app, click on the + symbol to add an accessory. This automatically opens your camera.
3. Scan the QR code included with your device to easily add it to your residence.
4. Once added, the app asks you to add the device to a room. Fill in the additional parameters: Recording options, integrations with one or multiple HomePods and/or TV.

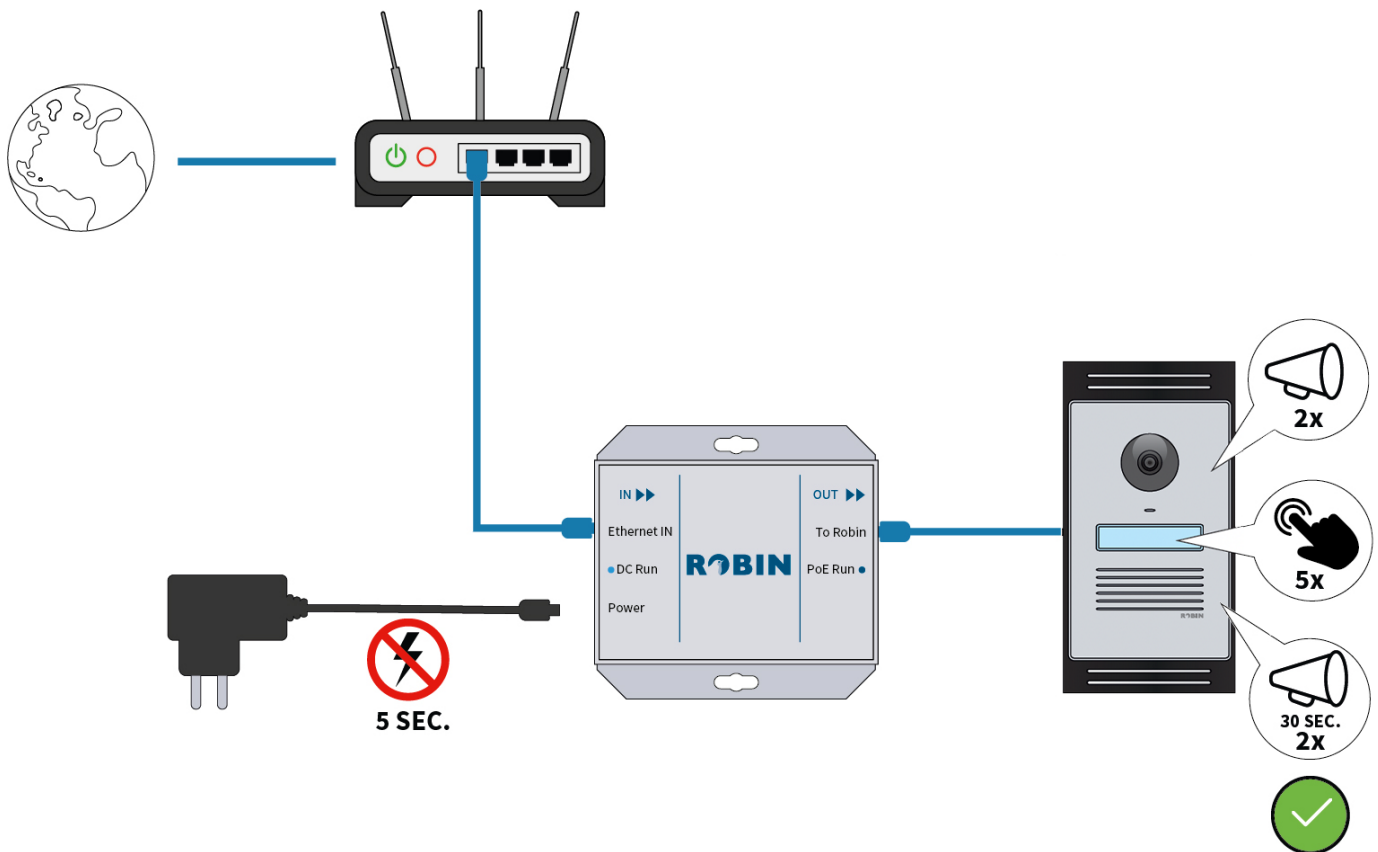
If your home has multiple family members, additional rights are automatically provided depending on the family members' settings in iCloud. Every individual is able to adjust their own settings to their personal preferences.

RESETTING THE DEVICE

When problems arise or you wish to recycle the device or use it for other purposes, a reset may be required.

Follow the steps below to execute the reset:

1. Turn the power from the PoE injector or switch off and wait 5 seconds.
2. Re-attach the power to the device.
3. After booting, you will hear a sound. This indicates that the device has received an IP address.
4. When this sound is heard, immediately press the "call" button 5 times within 10 seconds.
5. The device is now rebooting. You will hear the boot sound again within 30 seconds.
6. The device is now reset and available for use.



SUPPORT

For technical assistance, installation guidance, or troubleshooting support, always contact your local CDVI Technical Support first (see [page 3](#) for contact details).

As the official manufacturer and system partner, CDVI provides dedicated assistance for product integration, access control configuration, and combined intercom solutions.

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

Note: CDVI Support Portal 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.

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 (<https://support.robin.nl>).

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 Technical 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.

GLOSSARY

Term	Description
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 authorise 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 optimising 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 signalling 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 signalling 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 H264 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 colour 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 unauthorised 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 signalling channel.
Inbound	Refers to network traffic or signalling 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 analogue 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. <i>Example: 192.168.1.100</i>
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. <i>Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334</i>
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 synchronise 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 signalling 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 analysed 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 initiates 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 synchronised 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 signalling 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 signalling 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 electro-magnetic 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 electro-magnetic 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 signalling 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 signalling and data exchanges, protecting communications from eavesdropping, tampering, and unauthorised 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 signalling 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 reconvertng it to audio at the receiving end.



Welcome with
confidence

CDVI FRANCE + EXPORT

+33 (0) 1 48 91 01 02
www.cdvi.fr

CDVI AMERICAS

+1 866 610 0102
www.cdvi.ca

CDVI BENELUX

+32 (0) 56 73 93 00
www.cdviBenelux.com

CDVI GERMANY

+49 (0) 251 798477 0
www.cdvi.de

CDVI SWITZERLAND

+41 (0) 21 882 18 41
www.cdvi.ch

CDVI IBERIA

+34 935 39 09 66
www.cdviiberica.com

CDVI ITALY

+39 (0) 321 90 573
www.cdvi.it

CDVI NORDIC

+46 (0) 31 760 19 30
www.cdvi.se

CDVI UK

+44 (0) 1628 531300
www.cdvi.co.uk

CDVI POLAND

+48 607 445 682
www.cdvi.com.pl

Robin Telecom

+31 72 534 64 26
www.robintele.com



Disclaimer: Every effort is made to ensure all information in this document is correct at the time of publication, but it is offered without any guarantee and/or liability for completeness or correctness. Any information or images could be perceptibly different and we reserve the right to adjust, remove, or replace information or images without prior notice.

Published: 19/08/26