2N LiftIP 2.0

User Manual

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Table of Contents

Product Description

In this section, we introduce the **2N LiftIP 2.0** product, outline its application options and highlight the advantages following from its use.

Product Versions

Main Units in Universal Design

These units are installed behind the elevator panel, which is prepared for installation in advance.

Part No. 921640E

2N LiftIP 2.0 COP unit, EN

Part No. 921640XE

2N LiftIP 2.0 COP unit, EN, Cable version

Includes 2 LEDs (green, yellow), microphone and speaker connected via cables.

Part No. 921618BE

2N LiftIP 2.0 COP unit – Flush mounting, EN, With button

Equipped with a stainless steel cover, this unit is designed for lift panel mounting.

Part No. 921618E

2N LiftIP 2.0 COP unit – Flush mounting, EN, Without button

Equipped with a stainless steel cover, this unit is designed for lift panel mounting.

Main Units in TOC Design

- **Part No. 921630E**

  2N LiftIP 2.0 TOC unit, EN

  The units in the metal cover are designed for installation on the elevator cabin.

  Main Units in TOC Design

Part No. 921630E

2N LiftIP 2.0 TOC unit long, EN

Basic design set with switch for interconnection of 2N Voice Alarm Station audio units in metal cover.

Includes 2 LEDs (green, yellow), microphone and speaker connected via cables.

The units in the metal cover are designed for installation on the elevator cabin.

Basic Features

2N LiftIP 2.0 is an emergency elevator lift communicator providing full-duplex audio transmission via the VoIP technology directly from the elevator cabin. A microphone and a speaker are built-in behind the elevator panel for bidirectional communication. **2N LiftIP 2.0** is designed for sites where a LAN is available and connected via an RJ-45 connector. 2N LiftIP 2.0 can be fed either from a 10–30 V DC / 0.5 A external supply or directly from the LAN if equipped with PoE 802.3af supporting elements. From **2N LiftIP 2.0** you can only make calls to pre-programmed numbers. Thanks to IP connectivity, **2N LiftIP 2.0** can be constantly monitored, remotely configured and state detected. The advantage is the connection option for an almost unlimited count of communication units.

Advantages of Use

- Basic announcement set playing
- Recording of up to 8-minute long announcements (10 user messages)
- Optimum acoustic properties
- Adjustable speaker volume via audio unit buttons (during a call)
- Configuration via device web interface
- Checking call function once in 3 days (programmable)
- Function indication – two LEDs meeting the applicable elevator regulations
- Automatic redialing of up to four numbers
- Protection against unintentional/useless startup (CANCEL)
- Call control from control center
- No additional power supply requirement if PoE is used
- Easy installation into any elevator button panel
- Powerful indication options – illuminated pictograms (including bulbs)
- DTMF via RFC-2833, in-band or SIP INFO.

Product Versions

Main Units in Universal Design

These units are installed behind the elevator panel, which is prepared for installation in advance.

Part No. 921640E

2N LiftIP 2.0 COP unit, EN

Part No. 921640XE

2N LiftIP 2.0 COP unit, EN, Cable version

Includes 2 LEDs (green, yellow), microphone and speaker connected via cables.

Part No. 921618BE

2N LiftIP 2.0 COP unit – Flush mounting, EN, With button

Equipped with a stainless steel cover, this unit is designed for lift panel mounting.

Part No. 921618E

2N LiftIP 2.0 COP unit – Flush mounting, EN, Without button

Equipped with a stainless steel cover, this unit is designed for lift panel mounting.

Main Units in TOC Design

- **Part No. 921630E**

  2N LiftIP 2.0 TOC unit, EN

  The units in the metal cover are designed for installation on the elevator cabin.

  Main Units in TOC Design

- **Part No. 921630E**

  2N LiftIP 2.0 TOC unit long, EN

  Basic design set with switch for interconnection of 2N Voice Alarm Station audio units in metal cover.

  Includes 2 LEDs (green, yellow), microphone and speaker connected via cables.

  The units in the metal cover are designed for installation on the elevator cabin.

Accessories

Part No. 921661E

2N Voice Alarm Station – Switch

2N LiftIP 2.0 audio unit interconnection switch

Part No. 921001SET

2N Voice Alarm Station Set

Includes 2 2N Voice Alarm Station units and 1 2N Voice Alarm Station – Switch.

Part No. 921623E

2N LiftIP 2.0 Relay extender

1 output providing extender

Description and Installation

In this section, we describe the **2N LiftIP 2.0**product and its installation.

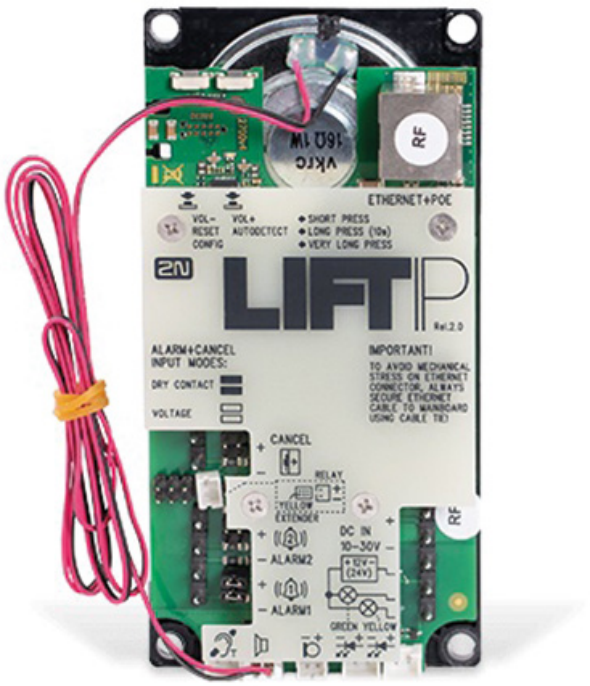
2N LiftIP 2.0 is an emergency elevator lift communicator providing full-duplex audio transmission via the VoIP technology directly from the elevator cabin. A microphone and a speaker are built-in behind the elevator panel for bidirectional communication. It includes external power supply terminals, an ALARM button, illuminated pictograms (device states as standardized) and a CANCEL input (optional cabin door opening signal).

Device Operation

Press the ALARM button. The **Wait** pictogram goes on immediately; the **Connection established** pictogram goes on after communication is established.

Universal Design

The electronics board is located between the mounting panel and the instruction printed cover (see the Fig.). The overall dimensions are 65 (W) x 130 (H) x 24 (D) mm The speaker, microphone and 2 LEDs (green, yellow) are connected on the motherboard (according to the Part No.). Jumpers (included in the product accessories) are mounted to the left. The small bottom connectors are intended for an induction loop connection (for hearing-impaired people). Typically, illuminated pictograms (also bulbs) are connected to this product. The pictograms and the ALARM button are not part of the delivery (they are design elevator elements).



COP Design

The electronics board is located under the stainless steel panel with pictograms (see the Fig.). The overall dimensions are 100 (W) x 220 (H) x 26 (D) mm. The speaker, microphone and LED are included in the delivery. Jumpers (included in the product accessories) are mounted to the left. The small bottom connector is intended for an induction loop connection (for hearing-impaired people).

TOC Design

The electronics board is mounted in a metal cover (see the Fig.). The overall dimensions are 82 (W) x 186 (H) x 33 (D0) mm for the basic version and 82 (W) x 257 (H) x 33 (D) mm for the long version with 2N Voice Alarm Station. The speaker and microphone are attached to the panel. The speaker, microphone and 2 LEDs (green, yellow) are connected on the motherboard (according to the Part No.). Slide-on terminals (included in the product accessories) are mounted to the left. The small bottom connectors are intended for an induction loop connection (for hearing-impaired people). Typically, illuminated pictograms (also bulbs) are connected to this product. The pictograms and the ALARM button are not part of the delivery (they are design elevator elements).

Before You Start

Check the product package for completeness before starting the installation.

Package Contents

- **2N LiftIP 2.0**
- 4 multi-connection terminals
- 6 jumpers
- 1 speaker and 1 microphone
- 2 LED equipped cables
- 3 stickers
- 5 cable ties
- 1 Certificate of Ownership
- 1 Brief Manual

NOTE
The count and types of accessories may differ in different Part Nos.

2N LiftIP 2.0 Installation Conditions

- **2N LiftIP 2.0** is not designed for outdoor applications.

- The product is connected to the LAN.
- The covering against mechanical damage, water, dust and other influences must be provided by the installing company if necessary.
- The communicator mounting surface must be perfectly flat, for details see Section Mechanical Installation (p. 12).

CAUTION
Installation and setting of this device, including any handling thereof, should only be carried out by duly trained persons.

NOTE
Having been connected to the LAN, **2N LiftIP 2.0** gets the IP address from the DHCP server.

Universal Design

Check whether the lift panel is ready for **2N LiftIP 2.0** mounting.

Mechanical Installation

CAUTION
Make sure that the position, appearance and marking of the communicator controls (ALARM button, e.g.) are in accordance with the applicable lift standards.

Installation Conditions

- Make sure that the lift panel is ready for installation, including speaker perforation.
- The panel must include the following prescribed elements:
  - ALARM button;
  - **Request accepted** illuminated pictogram;
  - **Connection established** illuminated pictogram.
- Make sure that the positions of these pictograms are in accordance with the applicable regulations.
- Leave free space behind the panel of 65 (W) x 130 (H) x 25 (D) mm.

2N LiftIP 2.0 Position

Mount **2N LiftIP 2.0** into any position as needed. The optimum position of **2N LiftIP 2.0** is approximately at the adult's mouth height. **2N LiftIP 2.0** is designed for places where any touch of the operating personnel is excluded (refer to Security Precautions).

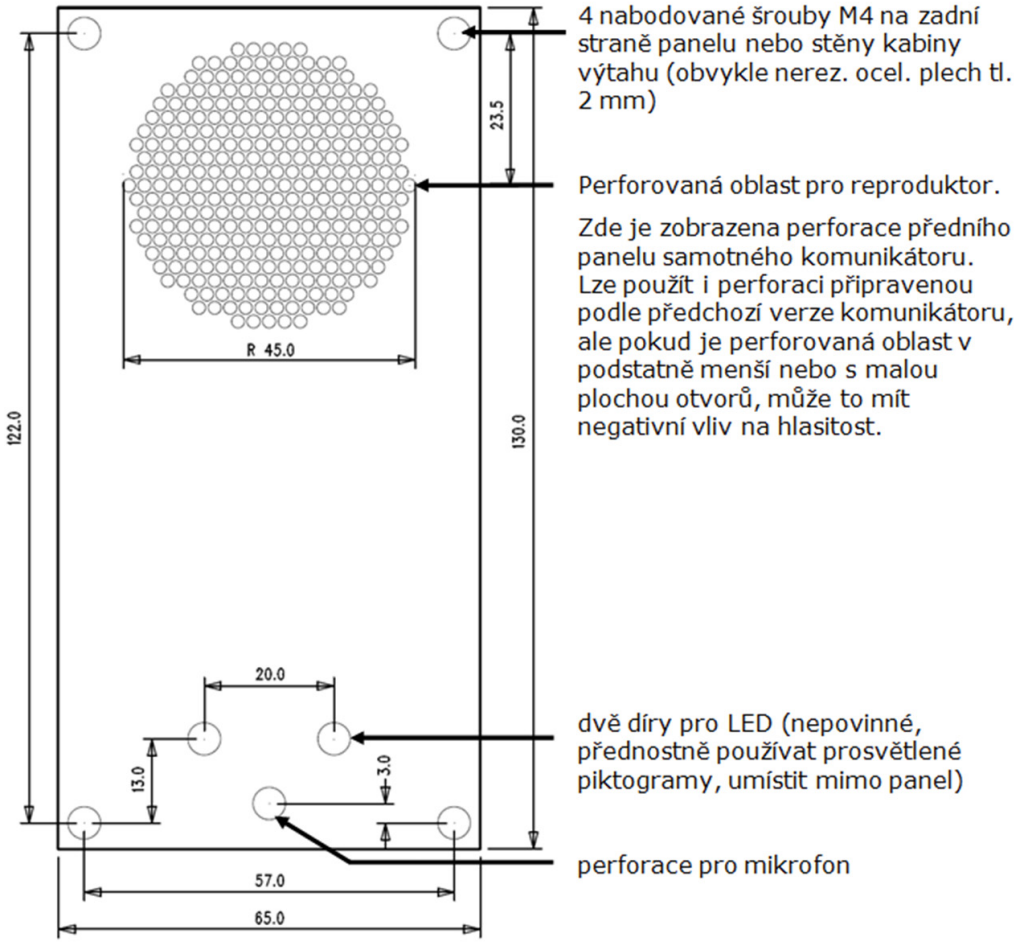
CAUTION
We recommend that the electronics is not mounted without the mounting panel, otherwise the manufacturer cannot guarantee safety. The panel provides electrical insulation.

2N LiftIP 2.0 Electronics Panel Mounting

What you need to mount the electronics panel onto the lift button panel:

- 4 spot-welded M4 screws from the inside with a pitch of 57 (W) x 122 (H) mm
- sufficiently perforated speaker area (may be larger than as shown in the figure but **may never exceed the panel size** to avoid acoustic fault)
- microphone hole
- holes for 2 LEDs if necessary

Mounting Drawing for 50 mm Speaker Installation



If you do not use the prescribed screws, make sure that the minimum isolation distance between the electronics and non-standard fixing elements is 2 mm. Mount the panel in such a manner that it does not resonate during the product function. Make sure that there is no gap between the button panel and **2N LiftIP 2.0** panel or seal the gap if any properly to avoid the speaker acoustic fault and speaker – microphone acoustic feedback (see later).

CAUTION
Make sure that microphone hole is sealed properly to record only sounds from the cabin instead of the noise from the shaft or space behind the panel.

2N LiftIP 2.0 TOC Design Installation

The TOC version is designed for elevator cabin wall mounting. Fit the metal cover onto screws that are smaller than the hole of the diameter 0.8 mm if possible. Use screws with flat surfaces alone or cone-head

screws combined with the appropriate washer. Place the device on the selected installation site, mark the screw holes.

CAUTION

- If you use screws larger than recommended, the device may not be easily removed without unscrewing the screws.
- Or, if you use smaller screws than recommended, the device may not be fitted properly.

Off-Panel Microphone Mounting

By default, the microphone is located directly on the **2N LiftIP 2.0** PCB (refer to the drawing for location). In cable versions, the external microphone is attached to a holder with a diameter of 25 mm and self-adhesive foil, the microphone is typically connected to the appropriate motherboard connector via a cable. The sticker helps you mount the microphone behind any button panel hole (the minimum hole diameter is 3 mm or the hole is composed of smaller holes of the same area). Refer to this file for external microphone size details. **The minimum center-to-center distance between the speaker and the microphone is 90 mm**. A shorter distance may lead to acoustic feedback. A longer distance does not matter.

The external microphone connection state does not change during operation. The valid external microphone state is only detected when the device is started/restarted.

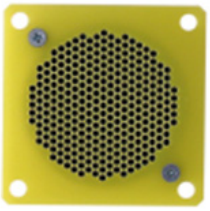
Off-Panel Speaker Mounting

Typically, the speaker is connected to the appropriate motherboard connector via a cable. Refer to this file for external speaker size details. The cable length enables the device to be placed within 1 m from the **2N LiftIP 2.0** motherboard. **In this case, mind the electrical safety, see below!**

CAUTION

Installing the speaker separately, make sure that the grid does not surpass the speaker dimensions in any case to eliminate the acoustic fault between the speaker front and back sides!

DANGER
Make sure that the 50mm speaker is mounted on an insulating (non-metal) surface. Otherwise, request an external panel, see the figure below (not included in the delivery).



CAUTION
We do not recommend you to install the microphone and speaker on completely different cabin sites (ceiling and wall, e.g.) as the users should find the speaker (grid/perforation) easily and then speak into the microphone near it.

CAUTION
Should there be an acoustic feedback between the microphone and the speaker (echo), turn down the speaker volume.

How to Achieve Ideal Acoustic Properties

To ensure the minimum acoustic pressure according to the EN 81-28:2015 standard requirements, the holes in the communicator speaker covering panel should occupy 20 % of the speaker area at least and be placed above the speaker.

Make sure that the speaker and the microphone fit tightly to the covering panel. If this is impossible due to an uneven panel surface, we recommend that a speaker seal is used to avoid sound leaking into the

space behind the panel. A good microphone sealing is crucial for high-quality sound transmission and good intelligibility.

Try to minimize the microphone - speaker acoustic feedback while mounting.

CAUTION
If you test the cabin control panel outside the elevator (on a desk, e.g.), the sound may seem too silent. This is due to the lack of a sound enclosure and acoustic properties of the elevator panel. The final volume does not match until the device is installed properly.

Installing Indicators

There are three types of **2N LiftIP 2.0** state indicators:

1. Illuminated pictograms that are part of the cabin control panel.
2. LEDs located directly on the **2N LiftIP 2.0** electronics.
3. Two LEDs (yellow, green) connected to the **2N LiftIP 2.0** electronics in the cable version.

NOTE
Make sure the selected type of indication meets the applicable legislation. However, no indication elements are necessary for the main function of **2N LiftIP 2.0** (communication).

Connection

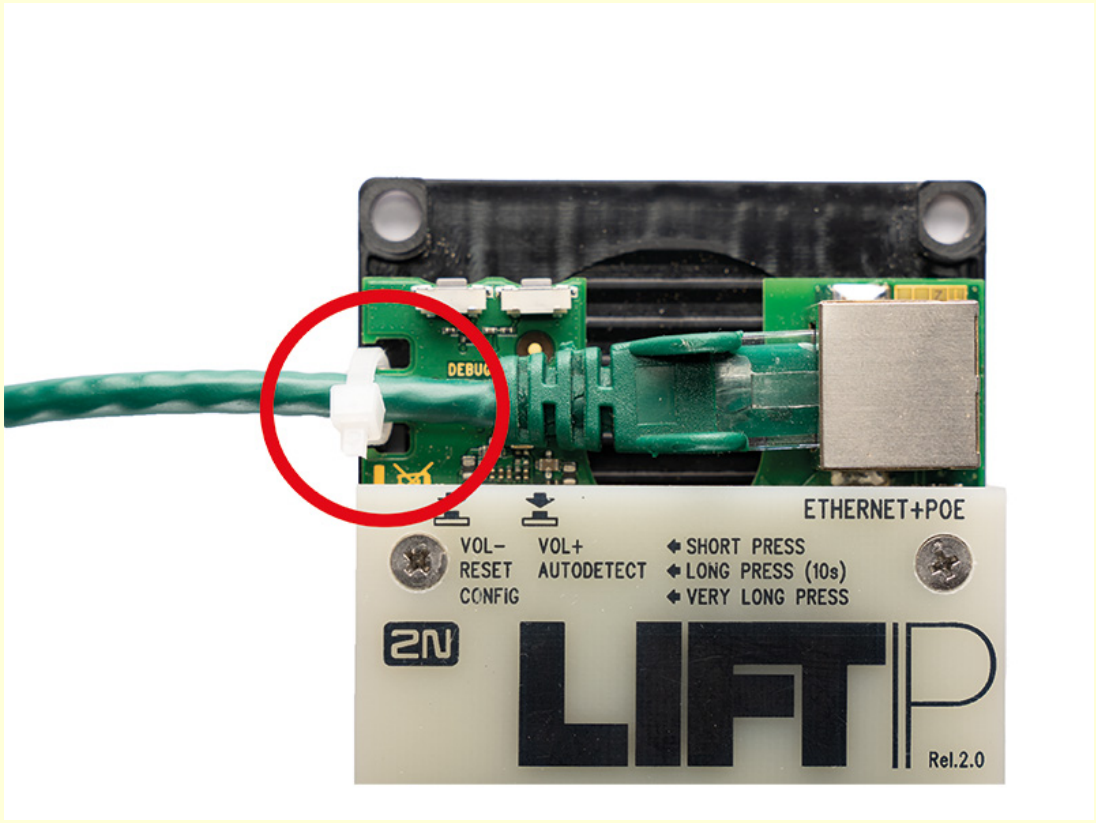
2N LiftIP 2.0 Connection to Network

2N LiftIP 2.0 is connected to the LAN via a Cat-5e or higher UTP cable terminated with RJ-45 (LAN connector). **2N LiftIP 2.0** can be fed via PoE or from an external power supply (10–30 V DC, 0.5 A). Once connected to the LAN, **2N LiftIP 2.0** gets the IP address from the DHCP server.

Or, retrieve the IP address using 2N Network Scanner, which includes the network scanner. Refer to Subs.IP Address Retrieval Using 2N Network Scanner for details.

By default, **2N LiftIP 2.0** receives DTMF via RFC-2833 or in-band / SIP INFO detection.

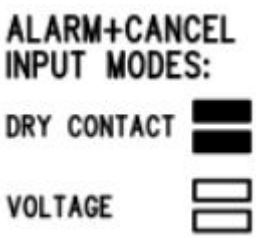
CAUTION
Fit the Ethernet cable to the motherboard using a cable tie to prevent mechanical stress of the connector.



ALARM 1/2 Connection – Contact Control

DANGER
Remember that the button must be safe – the button contacts may never be connected to any other circuits. If such conditions cannot be met, use voltage control.

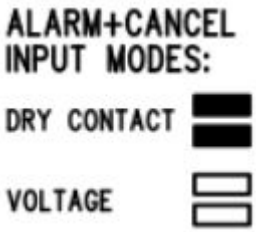
1. Connect the button contacts to the ALARM terminal. The alarm is set as N/O (both jumpers mounted) from the factory.
2. The button can have an N/O or N/C contact. If the case is a N/C contact, invert the button function in the device web configuration, refer to Digital Inputs (p. 61).



ALARM 1/2 Connection – Voltage Control

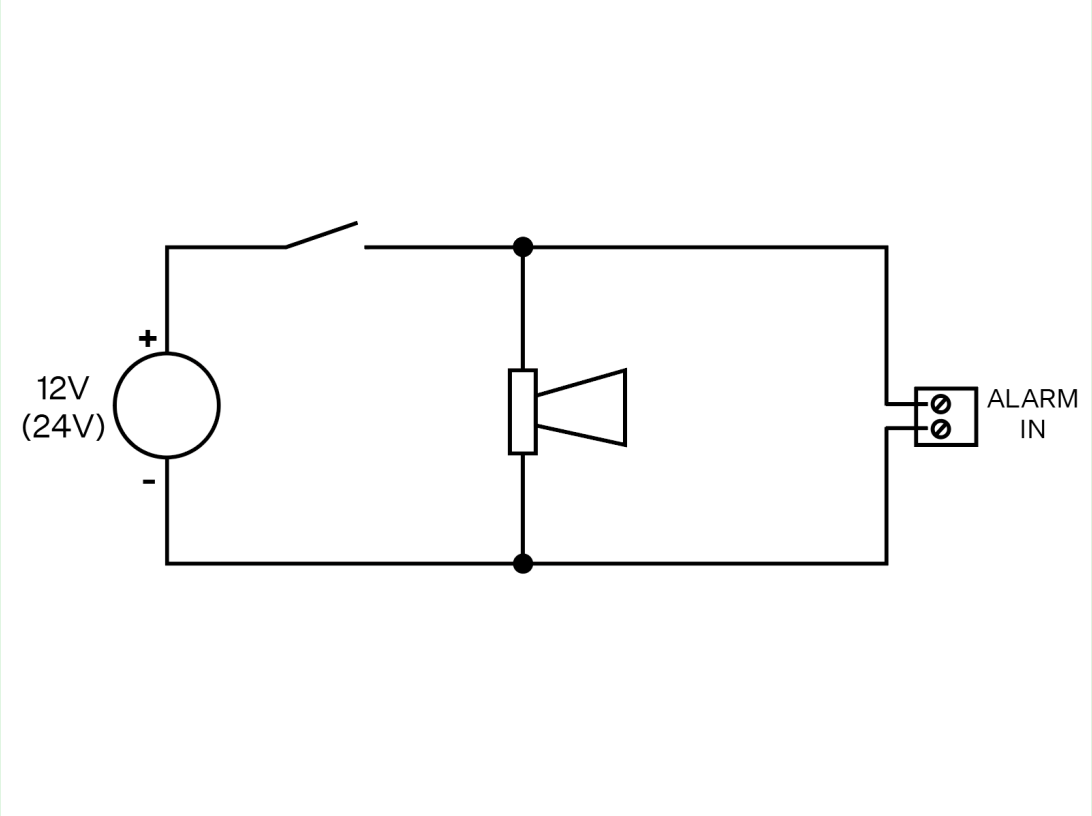
TIP
DC voltage of 5–48 V can be used. Such source, however, must be backed up against power outage.

1. Voltage connection / disconnection is used for activation. The alarm is set to contact control from the factory.
2. Slide all the jumpers off the configuration jumper link to control ALARM by voltage connection.



WARNING
Keep polarity (see the cover print).

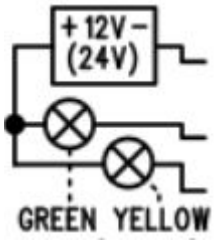
TIP
Here is an example of wiring of an alarm button with a siren:



Indicator Connection

Basic connection

Any indicators can be used in this connection mode (illuminated pictograms, e.g.). The indicator brightness intensity is ensured by the use of an external power supply. **2N LiftIP 2.0** includes just switches; connect a circuit to limit the current if necessary if LEDs are used.



Requirements

- 12–24 V supply (backed up if the indicators should work at power outage).

WARNING
Keep the power supply polarity!

- 200 mA permanent current (even with bulbs).

- Make sure that both the indicators are connected!

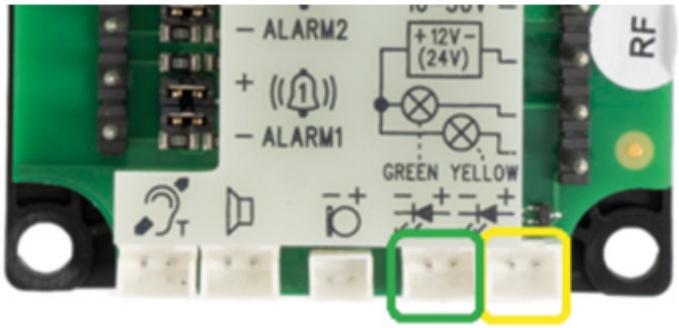
Use of LEDs mounted on 2N LiftIP 2.0 electronics

In this case, the LEDs are mounted on the electronics board and no additional connection is needed.

Cable connected LEDs

NOTE
If the LED indicators are connected via a cable, the installation company is responsible for the correct positioning of the signaling element and the design of the pictograms used.

Used where no illuminated pictograms are available. Such LEDs are part of the device cable version accessories. They are LEDs with the diameter of 5 mm and very high luminosity.



Requirements

- Keep the LED polarity (see the cover print).
- Keep the colors: request confirmation – yellow, connection confirmation – green.

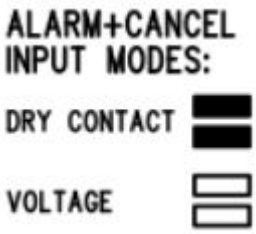
NOTE
The printed circuit LED is off in this type of connection.

CANCEL Connection (Door Contact, Optional)

CAUTION
Make sure that the door switch or door opening signal indicates that the door is open only if both the internal and external elevator doors are open and the people can leave the cabin.

Switch control

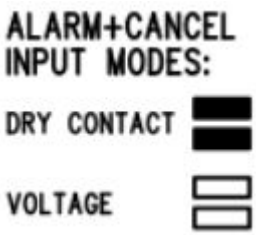
1. Connect the switch to the CANCEL terminal.
2. The **2N LiftIP 2.0** is set to contact control from the factory. Both the jumpers are mounted on the configuration jumper.
3. CANCEL can be set to N/C contact too. If the case is a N/C contact, invert the CANCEL input function in the device web configuration, refer to Digital Inputs (p. 61).



Voltage Control

DC voltage ranging from 5 to 48 V can be used.

1. Slide both the jumpers off the configuration jumper link for voltage control.
2. To use voltage disconnection control, invert the CANCEL input function in the device web configuration, refer to Digital Inputs (p. 61).



CAUTION
If voltage presence signals a **closed** door, make sure that the power supply is backed up against power outage.

WARNING
Keep polarity (see the cover print).

Induction Loop Connection

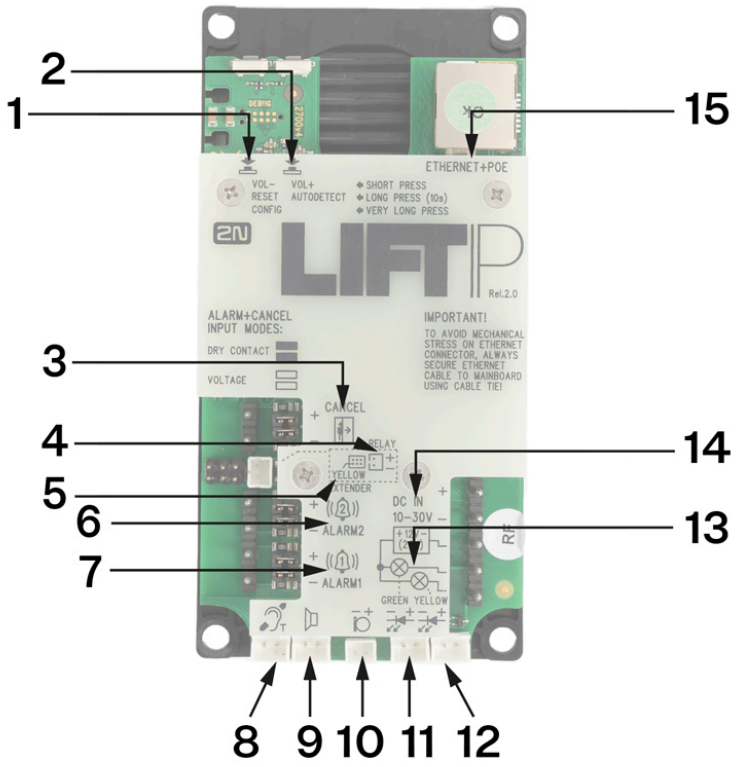
Follow the applicable regulations while mounting the communicator as they might require that the induction loop for deaf people should be a mandatory part of a lift cabin communicator installation. Connect the loop to the **2N LiftIP 2.0** backside connector. Polarity is arbitrary. If agreed so, the induction loop can be part of the delivery including a 4m cable.

Requirements

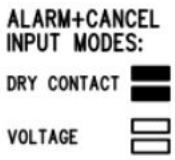
- We recommend you to install the induction loop behind a non-metallic, non-magnetic cover to avoid deterioration of the induction loop field radiation.
- Make sure that the induction loop is marked with an appropriate symbol (ear) and its position complies with the applicable standards.

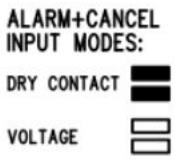
Description of Terminals, Jumpers, Connectors and LEDs

Description of terminals and connectors



1	Button **VOL−** **RESET**, **CONFIG**	Short press (**VOL−**) − turn down the speaker volume Long press (**RESET**) – restart the device in approx. 10 s Very long press (**CONFIG**) − retrieve the device IP address, switch the static / dynamic IP address mode and reset the factory default values
2	Button **VOL+**, **AUTODETECT**	Short press (**VOL+**) − turn up the speaker volume Long press (**AUTODETECT**) – set the default ALARM 1/2 input polarity in approx. 10 s

Description of terminals and connectors					
3	**CANCEL terminal**	Contact control	N/O contact (default)	Use the configuration jumpers for setting. **N/O contact**: both the jumpers are mounted.	
			N/C contact	**N/C contact**: both the jumpers are mounted and input polarity is inverted in the software configuration in Subs. Digital Inputs (p. 61).	
		Voltage control	5-48 V DC connection	**Voltage connection** control: no jumper is mounted and input polarity is inverted in the software configuration in S. Digital Inputs (p. 61).	
			Disconnect DC voltage of 5–48 V	**Voltage disconnection** control: no jumper is mounted.	
4	**RELAY** connector		**2N LiftIP 2.0** Relay extender connector		
5	**YELLOW EXTENDER** (6-pin connector)		Used for 2N Voice Alarm Station connection.		

Description of terminals and connectors					
6/7	**ALARM 1/2** terminal	Contact control	N/O contact (default)	Use the configuration jumpers for setting. **N/O contact**: both the jumpers are mounted.	
			N/C contact	**N/C contact**: both the jumpers are mounted and input polarity is inverted in the software configuration in S. Digital Inputs (p. 61).	
		Voltage control	5-48 V DC connection	**Voltage connection** control: no jumper is mounted and input polarity is inverted in the software configuration in S. Digital Inputs (p. 61).	
			Disconnect DC voltage of 5–48 V	**Voltage disconnection** control: no jumper is mounted.	

Description of terminals and connectors			
8	**Induction loop** connector	The induction loop is not a standard part of the delivery. It must be installed behind an non-conductive and non-magnetic cover. Polarity does not matter. *Notes:* • *If mounted behind a non-conductive and non-magnetic cover, the speaker can work as an induction loop to a limited extent.* • *The output is short-circuit proof. The output power is limited by the resistor only.*	
9	**Speaker** connector	The speaker is connected in the standard delivery.	
10	External **microphone** connector	The external microphone connection state does not change during operation. The valid external microphone state is only detected when the device is started/restarted.	
11	"**Establishing connection**" GREEN connector	Green LED	The LEDs are not a standard part of the delivery (available only in cable versions).
12	"**Connection established**" YELLOW connector	Yellow LED	Once an external LED is connected, the on-board LED remains inactive.
13	Indicator connecting terminals **+ 12 V (24 V)**	DC 12–24 V / 2× 200 mA externally supplied indicators; keep the wiring diagram.	
14	**DC IN 10–30 V** terminal	External power supply (unless PoE is available)	DC 10–30 V
15	**ETHERNET + POE**	RJ-45 LAN connector (PoE 802.3af)	

WARNING
Keep polarity for voltage-controlled ALARM and CANCEL buttons (see the instructions on the cover).

LED (front side – during call)

Color	State	Features	Description
Yellow	Pause once every 3 seconds	Establishing connection	Signals alarm call connecting process and rescue mode in progress if enabled.
Green	Pause once every 3 seconds	Connection established	Signals alarm call connection with the option to talk to the counterparty. The alarm call is confirmed, the incoming call is answered.
Yellow + green	Alternately flashing	Checking call failure	Signals a checking call failure. Checking call failure signaling Another call is signaled when it starts, see the cases above. Once the call ends, flashing is restored. An error state is terminated by alarm call confirmation (ALARM1 only) or a subsequent successful checking call.
No light signaling		At relax	Signals the device relax state.

Button Functions

The buttons located in the left-hand upper part of the main unit board are used for setting basic parameters and controlling the device without access to the device web interface.

Volume Control

Press the VOL−/VOL+ button shortly to turn down/up the speaker volume by one level. The master volume low/high limit is confirmed by an acoustic signal.

ALARM 1/2 Default Setting

Press the AUTODETECT button for approx. 10 s to detect the ALARM 1/2 input control type. The detected values are automatically written into the software configuration. The input control type is considered as the relax state at the moment of auto detection. Resetting of the input default values is indicated by an acoustic signal.

Device Restart

Press the RESET button for approx. 10 s to restart the device without any configuration change.

NOTE
The time interval between the RESET long press and device reconnection to the network after restart is a few tens of seconds.

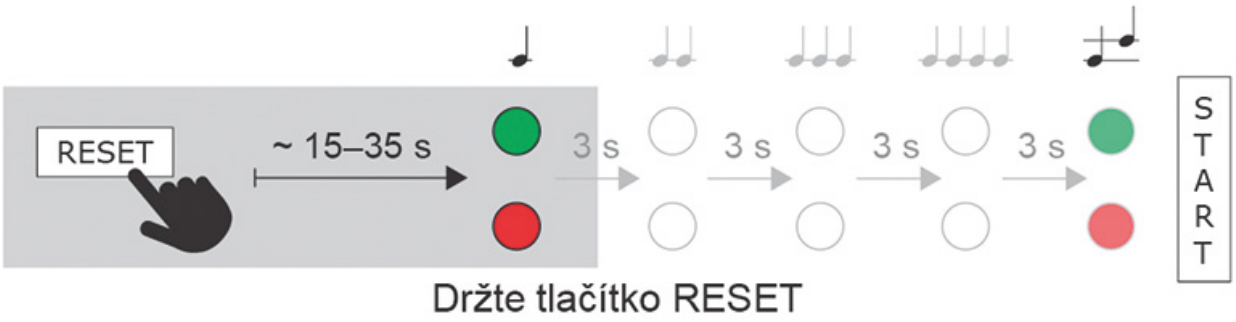
IP Address, IP Address Change and Factory Reset

The VOL−/RESET/CONFIG button located in the left-hand upper part of the main unit helps you retrieve the device IP address, switch the IP address static/dynamic states and reset the device factory defaults.

IP Address Retrieval

Follow the instructions below to **retrieve the current IP address**:

1. Press the button RESET and keep it pressed.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal ♩ can be heard (approx. 30 s).
3. Release the RESET button.
4. The device announces the current IP address via the speaker automatically.



NOTE
The time interval between the RESET press and the first light and acoustic signals is approx. 30 s.

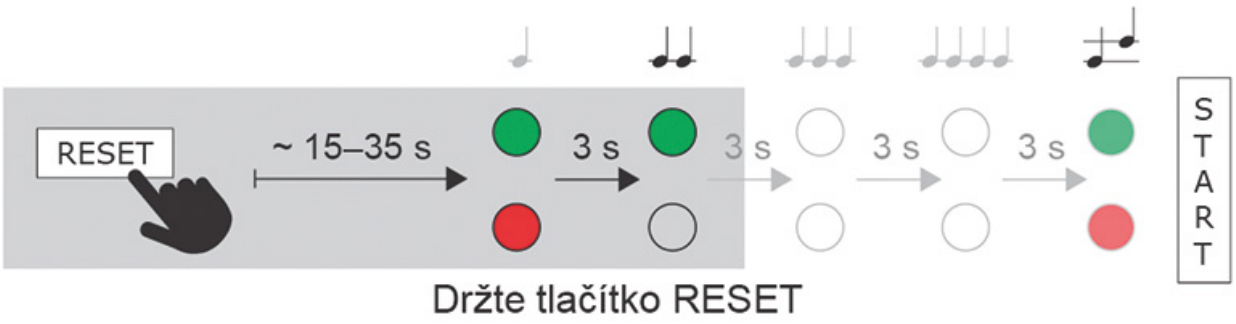
Static IP Address Setting

Follow the instructions below to switch on the **Static IP address** mode (DHCP OFF):

1. Press the button RESET and keep it pressed.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard (approx. 30 s).
3. Wait until the red LED goes off and the acoustic signal can be heard (approx. for another 3 s).
4. Release the RESET button.

The following network parameters will be set after restart:

- IP address: 192.168.1.100
- Network mask: 255.255.255.0
- Default gateway: 192.168.1.1



Držte tlačítko RESET

Follow the instructions below to switch on the **dynamic IP address** mode (DCHP ON):

Dynamic IP Address Setting

1. Press and hold the RESET button.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard (approx. 30 s).
3. Wait until the red LED goes off and the acoustic signal can be heard (approx. for another 3 s).
4. Wait until the green LED goes off and the red LED goes on again and the acoustic signal can be heard (approx. for another 3 s).

5. Release the RESET button.

Factory Reset

Follow the instructions below to **reset the factory default values**:

1. Press and hold the RESET button.
2. Wait until the red and green LEDs go on simultaneously and the acoustic signal can be heard ♩ (approx. 30 s).
3. Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
4. Wait until the green LED goes off and the red LED goes on again and acoustic signal can be heard ♩♩♩ (approx. for another 3 s).
5. Wait until the red LED goes off and the acoustic signal can be heard (approx. for another 3 s).
6. Release the RESET button.

Držte tlačítko RESET

2N Lift Voice Alarm Station

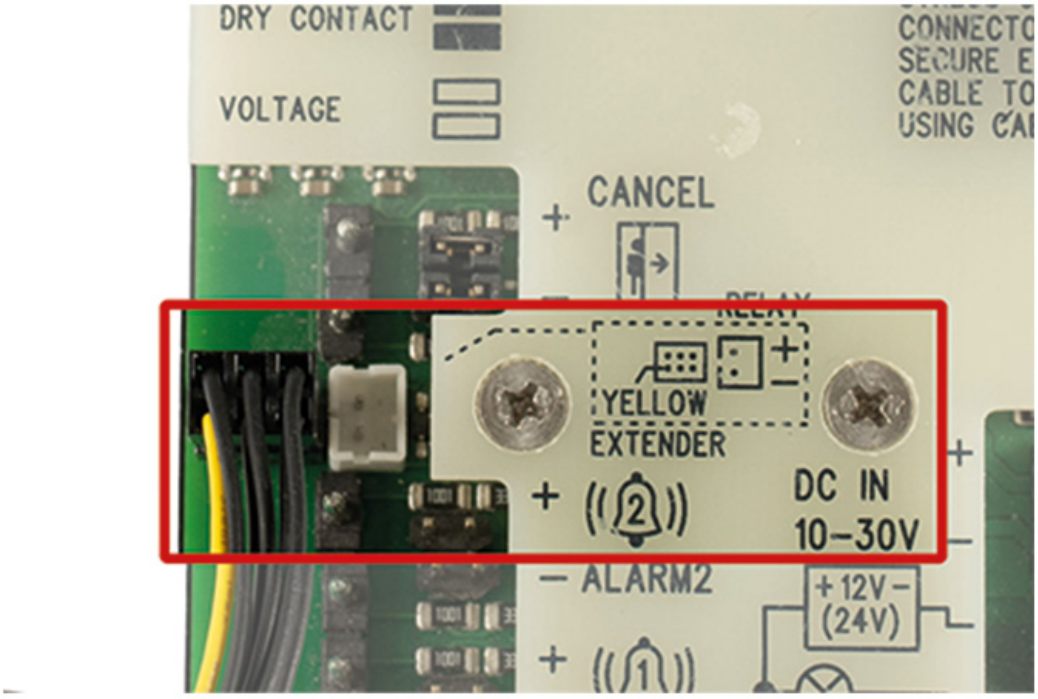
2N Voice Alarm Station extends **2N LiftIP 2.0** to include an audio unit on the cabin roof and under the cabin. It is fitted with its own microphone, speaker and emergency button. A switch is used for interconnecting **2N LiftIP 2.0** and one or two audio units.

2N Voice Alarm Station **Installation**

1. To install 2N Voice Alarm Station, disconnect **2N LiftIP 2.0** from the power supply..

2. Put the 6-pin switch interconnecting cable plug on the 6-pin EXTENDER connector on 2N LiftIP 2.0. Keep the proper orientation of the yellow wire.

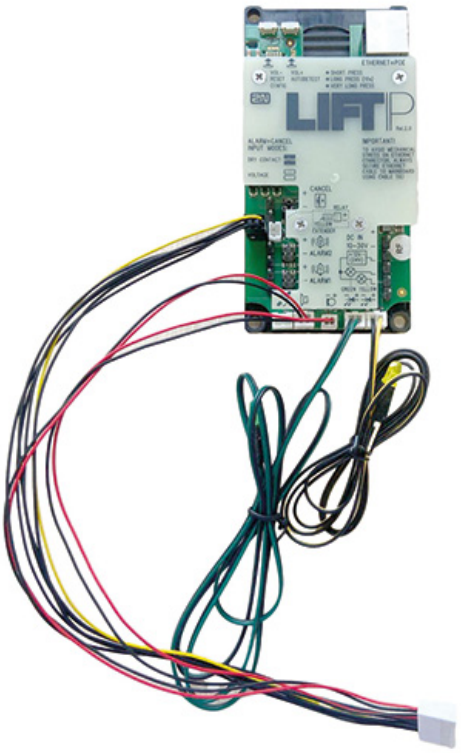
WARNING
An incorrect connection can damage the module.



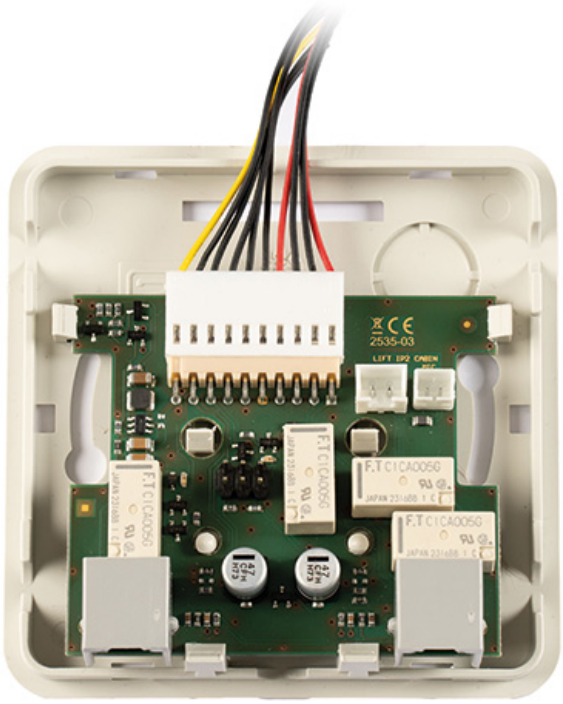
3. Disconnect the speaker and microphone from the connectors (external microphone if available) on **2N LiftIP 2.0**.

CAUTION
The external microphone connection/disconnection state does not change during operation. The valid external microphone state is only detected when the device is started/restarted.

4. Connect the switch interconnecting cable connectors into the **2N LiftIP 2.0** microphone and speaker connectors (the microphone and speaker connectors have different sizes and are mounted according to the pictograms on the **2N LiftIP 2.0** cover, so they cannot be confused).

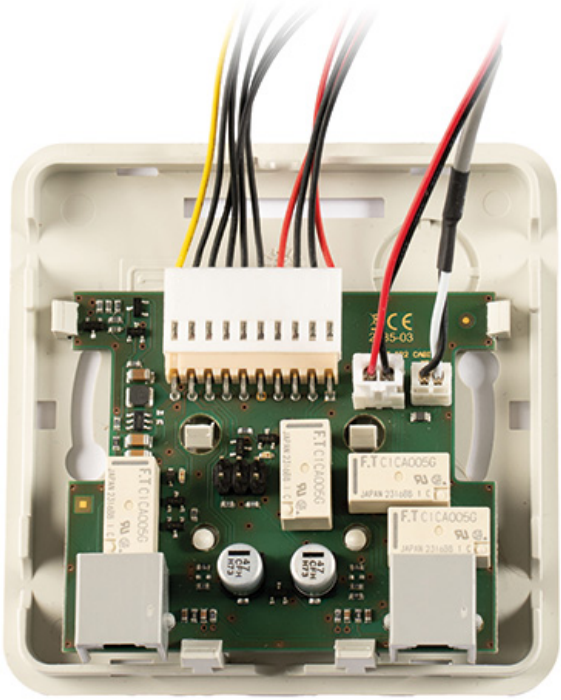


5. Remove the switch cover. Slide the interconnecting cable plug onto the 10-pin switch connector to interconnect the switch and **2N LiftIP 2.0**.



6. Connect the microphone and speaker, previously disconnected from **2N LiftIP 2.0**, into the switch connectors. The connectors are marked SPK for the speaker and MIVC for the microphone.

> **WARNING**
> If you use the **2N LiftIP 2.0** cable version, then connect the microphone on the cable into the MIC connector on the switch, otherwise this connector remains unmounted.



7. Break out a cable installation hole in the switch cover upper edge. Depending on the installation method, you can alternatively lead the cables through a hole broken out in the right-hand upper corner of the switch cover back side. Having installed the cables in either way, replace the switch top cover. There is one RJ-12 connector on each side of the switch bottom part for audio unit connection. Use the cable included in the audio unit package to interconnect the audio unit and the switch. Find the appropriate connector under a hinged cover on the right-hand side of the audio unit. Secure the hinged cover with the included screw after connecting the cable.
8. Once the mounting is completed, reconnect **2N LiftIP 2.0** to the power supply.

> **NOTE**
> The 6-pin connector on the switch board is only used for advanced diagnostic hardware operations for servicing purposes and does not provide any function to a common user.

Configuration

Set call routing from the 2N Voice Alarm Station via the web configuration interface of the **2N LiftIP 2.0** device to which the 2N Voice Alarm Station is connected. Settings are made in **Calls > Alarm Call > Alarm Call 2**.

The Alarm call 2 events are written into the **State > Events** configuration menu.

WARNING
If the Alarm call 2 destination is empty, no call can be set up. One and the same user can be set both for ALARM1 and ALARM2.

Operation

Press Press to call shortly on the 2N Voice Alarm Station audio unit for activation. A call is set up to the alarm call destination defined in ALARM2 from **2N LiftIP 2.0**.

NOTE
The 2N Voice Alarm Station audio unit does not include a LED for connection establishing indication. A LED is on on the **2N LiftIP 2.0** audio unit to indicate call setup and connection confirmation.

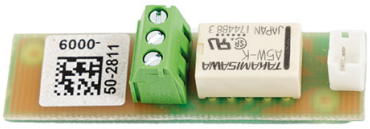
2N Voice Alarm Station **Dimensions**

Audio unit – 2N Voice Alarm Station 225 x 87 x 67 mm

Switch: 81 x 81 x 30 mm

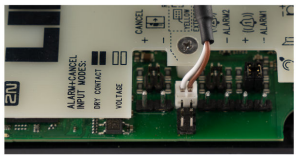
2N LiftIP 2.0 Relay extender

The 2N LiftIP 2.0 Relay extender extends **2N LiftIP 2.0** to include one additional output. The relay output type makes it possible to switch both voltage polarities. According to the activation type, the blocking output opens/closes if it is impossible to set up an alarm call from **2N LiftIP 2.0** (if there is no number in the Alarm button configuration or no SIP server registration except when Direct call (P2P call) is set for the Alarm button).



2N LiftIP 2.0 Relay Extender **Connection**

The 2N® LiftIP 2.0 Relay extender is connected to the RELAY connector (refer to the Description of Terminals, Jumpers, Connectors and LEDs (p. 23)).



1. Disconnect **2N LiftIP 2.0** from the power supply (10–30 V DC or PoE) while connecting 2NLiftIP 2.0 Relay extender.
2. To protect the circuits against short circuit with other conductive objects, put2NLiftIP 2.0 Relay extender **into an insulation tube and secure it with cable ties before installation!**

3. Interconnect **2N LiftIP 2.0** and 2N LiftIP 2.0 Relay extender using a cable.
4.

CAUTION
Keep the proper connection (yellow wire). An incorrect connection can damage the module.

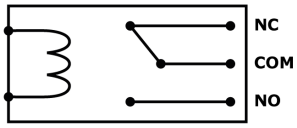
NOTE
The relay output error state is signaled in the same way as if the device was disconnected from the power supply. The relay output is without voltage.

2N LiftIP 2.0 Relay Extender **Technical Parameters**

Output	
Maximum switching power	15 W

Output	
Maximum switching voltage	30 V
Maximum switching current	2 A
Output Type	galvanically isolated, enables both voltage polarities to be switched

Diagram

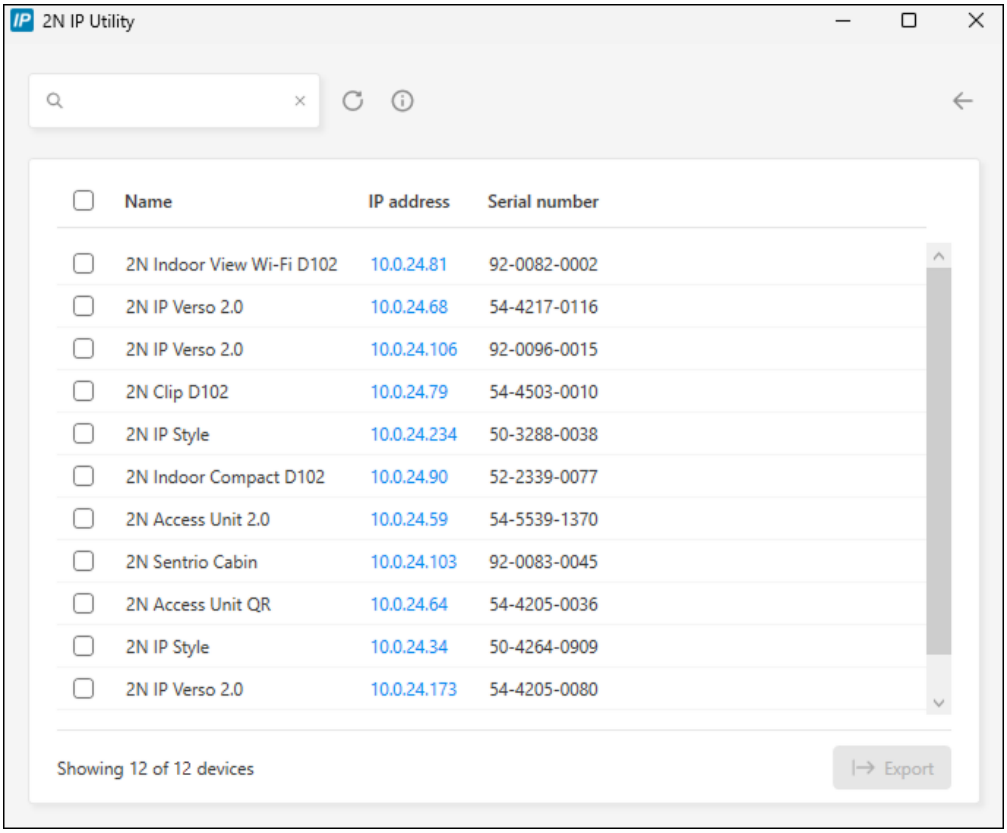


Example: Use the COM and NO contacts to make the relay connect the circuit after voltage is carried to the coil.

IP Address Retrieval Using 2N IP Utility

The 2N IP Utility application helps find the 2N device IP address in the LAN. Download 2N IP Utility from the 2N.com website. Make sure that Microsoft .NET Framework 4.7.2 is installed for successful app installation.

1. Run the 2N IP Utility installer.
2. The Installation Wizard will help you with the installation.
3. Having installed 2N IP Utility, start the application using the Microsoft Windows Start menu.
   Once started, the application begins to automatically search the LAN for all the 2N and AXIS devices which have been DHCP/statically assigned IP addresses. These devices are then shown in a table.



4. Select the device to be configured and left-click it. This opens the right-hand part of the web configuration interface window.

TIP

- Access to the web configuration interface is also possible via the **Open in external browser** button, which opens the interface in a separate browser window.
- Click a device in the list to display detailed information. Click the **IP settings** button to change the IP address by entering the required static IP address or activating DHCP.
- The application also allows you to export selected devices into a CSV file. First select a device by ticking the boxes in the list, then use the **Export** button that appears at the bottom of the window. The exported file shall include the names, IP addresses and serial numbers of the selected devices.

The default login data are:
Username: **Admin**
Password: **2n**
It is necessary to change the password immediately upon the first login.

TIP

It is recommended that a password is used that is difficult to break. It is not recommended that names, places or things, especially those closely related to the user, are used in the password.

For increased password security, it is recommended that:

- the random password generator is used,
- the password length is 12 characters at least,
- various characters from different character sets are combined (small/capital letters, digits, special characters, etc.).

Web configuration interface

Basic Orientation

The displayed homepage is illustrative. The display of tiles depends on the available features of the specific device.

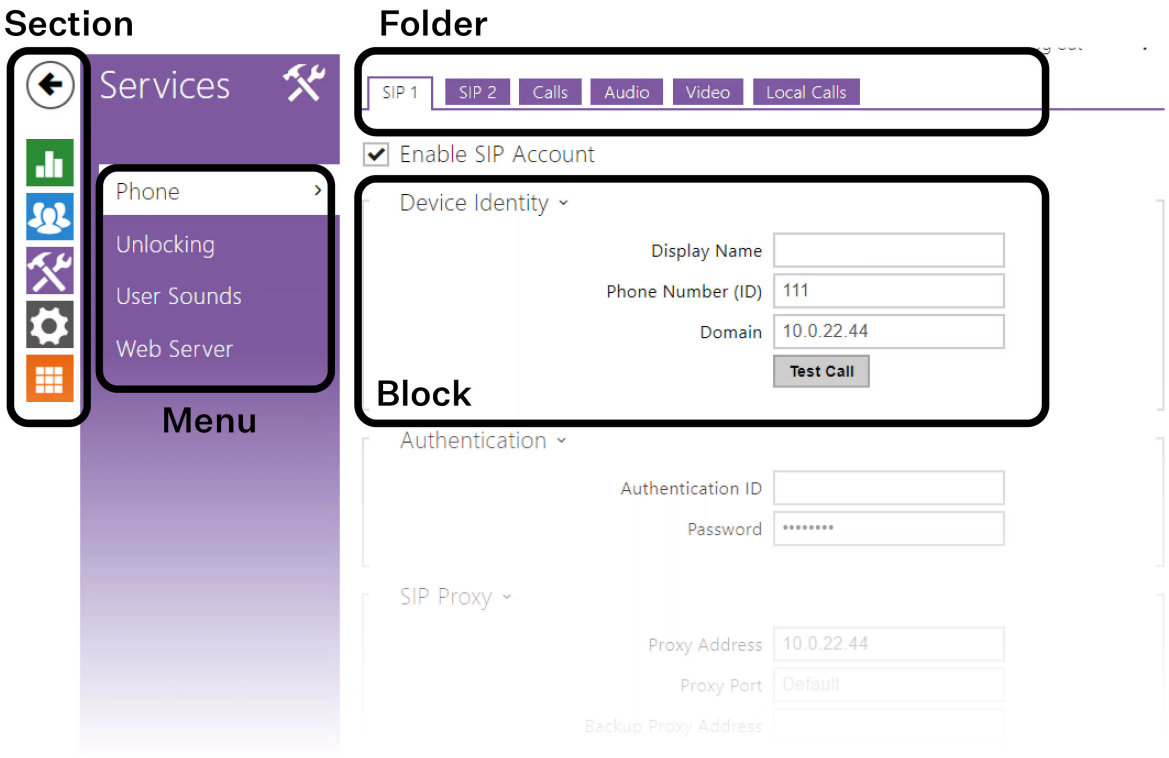
The start screen is displayed whenever you log into the **2N LiftIP 2.0** web configuration interface. Use the button in the left-hand upper corner on each of the other web configuration interface pages to return to this screen anytime. The page header shows the device name (refer to Device Name in **Services > Web Server**.

Menus

Use the menu in the right-hand upper corner of the web interface to select language. Click Log out in the right-hand upper corner of the screen to log out from the device, press the question mark icon to display Help or use the bubble to provide feedback.

Legend

The start screen is also the first menu level and quick navigation (click on a tile) to selected **2N LiftIP 2.0** configuration sections.



Device Configuration Interface Access

2N LiftIP 2.0 is configured via a web configuration interface. You have to know the device IP address.

Web Configuration Interface Login

1. The login screen is now displayed.
   Should the login screen fail to appear, make sure that you have typed the correct IP address, port or domain name. The login screen also does not appear when the administration web server is off. If you do not have a certificate generated for the IP address / domain name, an invalid security certificate warning may be displayed. In this case, you have to confirm that you want to go to the web configuration interface.
2. Enter the login data.
   The default login data are:
   Username: **Admin**
   Password: **2n**
   It is necessary to change the password immediately upon the first login.
   After login using the default password, the access to the web configuration interface functions is limited.

TIP
It is recommended that a password is used that is difficult to break. It is not recommended that names, places or things, especially those closely related to the user, are used in the password.

For increased password security, it is recommended that:

- the random password generator is used,
- the password length is 12 characters at least,
- various characters from different character sets are combined (small/capital letters, digits, special characters, etc.).

Recommended browsers

The web configuration interface is optimized for the Chromium-based web browsers (Google Chrome, Microsoft Edge or Opera, e.g.). With other browsers, there may be slight differences in the interface function and appearance.

State

The State menu provides clear status and other essential information on the device.

Lift

The Lift menu shows information on the model and its properties and error states.

Lift State

Lift ID – set the lift / lift intercom ID to be sent or read in calls. The identification number has to consist of 16 digits at most.

Last Successful Checking Call - display the time of the last successful checking call.

Next Checking Call – indicates the time of the next periodic checking call.

Rescue Mode – indicates whether the rescue mode is currently active.

Blocking Relay Active - display the relay output status where the parameter will be active in the case of a SIP registration / configuration error. If one of the errors occurs, the elevator will be blocked.

External Microphone - display the connection of an external microphone to the device.

CAUTION
The external microphone connection state does not change during operation. The valid external microphone state is only detected when the device is started/restarted.

Error States

SIP Registration Error – indicates that there is a current problem with the SIP account registration.

Configuration Error – indicates whether the device has a valid configuration for alarm calls (ALARM1).

Audio Error – indicates whether the last audio test was successful and no audio error has been detected.

ALARM1 Button Error – indicates whether the ALARM1 button is currently in defect.

Checking Call Error – indicates whether the last checking call has failed.

Device

The Device tab displays information on the model, its features, firmware and bootloader versions, etc.

Device Info

Factory Certificate Installed – specify the user certificate and private key to validate the intercom right to communicate with the ACS.

Locate Device – optical or acoustic signaling of the device.

Services

The Services tab displays the statuses of the network interface and selected services.

Call Logs

The call log provides a list of all accomplished calls. Each call carries the following information:

- contact type,
- name,
- call date and time,
- call duration and status (incoming, outgoing, missed, picked up elsewhere, doorbell button).

The search box is used for fulltext search in the call name. The check box is used for selecting all records for bulk deletion. The selected call record can also be deleted individually using the button. The list includes the last 20 records that are arranged from the latest call to the oldest one.

Events

The Events tab displays the last 500 events captured by the device. Every event includes the capturing time and date, event type and detailed description. Use the pop-up menu above the event record to filter the events by the type.

Events	Meaning
CallSessionStateChanged	Event describing the call direction/state, address, session number and call sequence number.
CallStateChanged	Indicates the call direction (incoming, outgoing) and opponent / SIP account identification at a call state change (ringing, connected, terminated).
CapabilitiesChanged	Event that informs of a change in the list of available functions of the device.
ConfigurationChanged	Device Configuration Change
DeviceState	Device state indication, startup of the device, for example.
DirectoryChanged	Change in the directory.

Events	Meaning
DirectorySaved	Change saved in the directory.
DtmfEntered	DTMF code received in call or off call locally.
ErrorStateChanged	Device error state.
KeyPressed	Generated whenever a button is pressed (numeric keypad digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
KeyReleased	Generated whenever a button is released (the digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
LogAutomationEvent	
LoginBlocked	Whenever 3 wrong logins to the web configuration interface have been entered. Includes data on the IP address of these accesses, time, time zone and device uptime (time after the last restart in seconds).
OutputChanged	Signals a change of the logic output state.
RegistrationStateChanged	Change of the SIP Proxy registration state.
RescueStateChanged	Change in the rescue mode state.

Directory

Directory is one of the crucial parts of the device configuration. It is used for creating and managing contacts .

Users

CAUTION
Make sure that at least one user with a phone number and a selected **Confirmation Mode** has been added to the phone book for emergency communication in the elevator.

The Search function in the Devices menu works as a fulltext search in names and phone numbers. It searches for all matches in the whole list. Find Device helps find registered devices and add them to the list if necessary.

Click Add user to create a new user and use the  icon to show the user setting details. Click  to remove a user and delete its details. Set the list arrangement according to the name, phone number or confirmation mode. 1 list page can display 15, 25 or 50 devices.

User Basic Information

Every record in the Users list includes the following parameters:

Name – user name for the selected Phone Book position. This parameter facilitates orientation among users.

Device Type – set the device type manually or automatically by searching the registered devices in the device list folder.

E-Mail – the device sends information on missed call, e.g., to these e-mails. You can set more e-mail addresses separated with a comma or semicolon.

User Phone Numbers

Each user in the phone book can be assigned up to 6 phone numbers. An outgoing call is routed to all the numbers simultaneously. Once the call is connected on one phone number (i.e. confirmed), the calls to the other phone numbers are terminated. This rule is valid regardless of the confirmation mode setting.

Phone Number – enter the phone number of the station to which the call shall be routed. Enter ""sip:\[user_id@\]domain\[:port\]"", e.g.: ""sip:200@192.168.22.15"" or ""sip:name@yourcompany"" for the so-called direct SIP calling. Enter “device:device_ID” for local calls and for calls to the 2N My2N application. If you enter /1 or /2 behind the phone number SIP 1 or SIP 2 respectively shall be used for outgoing calls. Enter /S to force an encrypted call, or /N for an unencrypted call. The account and encryption selections can be combined into the suffix /1S, for example.

Press  to set the phone number details.

Setting the phone number

- **Call Type** – set the scheme in the called destination URI. If you choose Without scheme ([unspecified]), the URI is completed with the data from the SIP account settings. Other options include direct SIP call (sip:), 2N local calls (device:), calls to Crestron devices (rava:), connection with MS Teams (msteams:), or calls with VMS, e.g., AXIS Camera Station (vms:).
- **Destination** – set the other parts of the called destination URI. As a rule, it contains the number, IP address, domain, port or device identifier. Enter an asterisk “*” for calls to the VMS.
- **Preferred SIP Account** – SIP account 1 or 2 is primarily used for calling.
- **Call Encryption** – set mandatory call encryption or no encryption.

Confirmation Mode – define how the alarm call shall be received for the given number.

Calling

Calling is the basic function of **2N LiftIP 2.0** – helps you establish connections with other IP network terminal devices. The device supports the extended SIP.

Calls

General Settings

Call Time Limit – set the call time limit after which the call is automatically terminated. The device beeps 10 s before the call ends to signal that the call end is approaching. If the call time limit is set to 0 and SRTP is not used, the call is not time limited.

Confirmation Timeout – set the timeout during which it is possible to confirm a call after call setup. When the timeout expires, the device will call the next number. If Confirmation by pickup is selected, this parameter is irrelevant.

Outgoing Calls

Connecting Time Limit – set the maximum outgoing call connection timeout after which the calls are automatically terminated. If the calls are routed to the GSM network via GSM gateways, you are advised to set a value higher than 20 s.

Ring Time Limit – set the maximum call setup and ringing time in which all outgoing calls are automatically terminated. If the calls are routed to the GSM network via GSM gateways, you are advised to set a value longer than 20 s. Minimum value: 1 s, maximum value: 600 s. Set 0 to disable the time parameter.

Advanced Settings

Starting RTP Port – set the initial local RTP port in the range of 64 ports used for audio and video transmission. The default value is 4900 (i.e. the range is 4900–4963). The parameter applies to both the SIP accounts.

RTP Timeout – set the audio stream RTP packet receiving timeout during a call. If this limit is exceeded (RTP packets are not delivered), the call will be terminated by the device. Enter 0 to disable this parameter. The parameter applies to both the SIP accounts.

Extended SIP Logging – allow SIP telephony details to be recorded in syslog (for troubleshooting purposes only).).

Local Calls

Configuration

Enable Local Calls – enable calls between 2N devices in the LAN. With this function off, the other LAN devices cannot locate this device, i.e. cannot call the device in the device:device_ID format.

Network Identification

Device ID – set the device ID to be displayed in the LAN device list in all the 2N devices in one and the same LAN. You can direct a call to this device by setting the user phone number as “device:device_ID” in these devices.

Test Call – display a dialog box enabling you to make a test call to a selected phone number, see below.

Connection to Lobby Units

Access key 1 and 2 – set the access key between the cabin unit (2N communicator) and the lobby unit (**2N Sentrio Cabin**). If the access key is empty or does not match the key of the paired device, the devices cannot communicate with each other.

LAN Devices

LAN Device count – display the number of local devices in the network.

Show LAN device list – display a detailed list of local devices in the network.

Video

Video Preview Parameters

Enable Video Preview – enable video preview multicast transmission.

Multicast Group – set the multicast address to which the video stream from **2N LiftIP 2.0** shall be sent. Select 1 of the the 8 preset addresses or set the mode in which the intercom selects the address automatically.

Low Bandwidth Mode – reduce the quality of the video preview to conserve bandwidth.

Audio

DTMF Sending

RTP (RFC-2833) – enable DTMF sending via the RTP according to RFC-2833.

SIP INFO (RFC-2976) – enable DTMF sending via SIP INFO messages according to RFC-2976.

DTMF Receiving

RTP (RFC-2833) – enable DTMF receiving via RTP according to RFC-2833.

SIP INFO (RFC-2976) – enable DTMF receiving via SIP INFO messages according to RFC-2976.

Transmission Quality Settings

Jitter Compensation – set the buffer length for compensation of interval unevenness in audio packet arrivals. Set a higher value to increase the receiving immunity at the cost of a higher sound delay.

SIP

2N LiftIP 2.0 allows two independent SIP accounts to be configured. Thus, the intercom can be registered under two phone numbers at the same time, with two different SIP exchanges, for example. Both the SIP accounts process incoming calls equivalently. Outgoing calls are primarily processed using account SIP1. Or, if SIP1 is not registered (due to SIP exchange error, e.g.), SIP2 is automatically used for outgoing calls. Select the account number for the phone numbers included in the phone directory to specify the account to be used for outgoing calls (example: 2568/1 - calls to number 2568 go via account 1, sip:1234@192.168.1.1/2 calls to sip uri via account 2).

Configuration

SIP Account Enabled – allow the SIP account use for calling. If disallowed, the account cannot be used for making outgoing calls and receiving incoming calls.

Device Identity

Display Name – set the name to be displayed as CLIP on the called party's phone.

Phone Number (ID) – set your device phone number (or another unique ID composed of characters and digits). Together with the domain, this number uniquely identifies the device in calls and registration.

Domain – set the domain name of the service with which the device is registered. Typically, it is equivalent to the SIP Proxy or Registrar address.

Test Call – display a dialog box enabling you to make a test call to a selected phone number, see below.

Authentication

Authentication ID – set the alternative user ID for device authentication.

Password – set the device authentication password. If your PBX requires no authentication, the parameter will not be applied.

SIP Proxy

Proxy Address – set the SIP Proxy IP address or domain name.

Proxy Port – set the SIP Proxy port (typically 5060).

First Backup Proxy Address – backup SIP Proxy IP address or domain name. The address is used where the main proxy fails to respond to requests. If the domain name is set and the backup SIP Proxy port number is not filled in here, the resultant backup SIP Proxy IP address will be set according to the NAPTR and SRV record data obtained from the DNS for the given name. If the DNS fails to provide such data or the backup SIP Proxy port number is set, the address from record A is used for the given name.

First Backup Proxy Port – set the backup SIP Proxy port. In case the parameter is empty or set to 0, the device tries to set the port number according to the NAPTR and SRV record data obtained from the DNS. If the DNS fails to provide these records, the default port number is set based on the transport layer (5060 for UDP and TCP, 5061 for TLS).

Second Backup Proxy Address – backup SIP Proxy IP address or domain name. The address is used where the main proxy fails to respond to requests. If the domain name is set and the backup SIP Proxy port

number is not filled in here, the resultant backup SIP Proxy IP address will be set according to the NAPTR and SRV record data obtained from the DNS for the given name. If the DNS fails to provide such data or the backup SIP Proxy port number is set, the address from record A is used for the given name.

Second Backup Proxy Port – set the backup SIP Proxy port. In case the parameter is empty or set to 0, the device tries to set the port number according to the NAPTR and SRV record data obtained from the DNS. If the DNS fails to provide these records, the default port number is set based on the transport layer (5060 for UDP and TCP, 5061 for TLS).

SIP Registrar

Registration Enabled – enable device registration with the set SIP Registrar.

Registrar address – set the SIP Registrar IP address or domain name.

Registrar Port – set the SIP Registrar port (typically 5060).

Backup Registrar Address – set the backup SIP Registrar IP address or domain name. The address is used where the main Registrar fails to respond to requests.

Backup Registrar Port – set the backup SIP registrar port (typically 5060).

Registration Expiry – set the registration expiry, which affects the network and SIP Registrar load by periodically sent registration requests. The SIP Registrar can alter the value without letting you know.

Registration State – display the current registration state (Not Registered, Registering..., Registered, Unregistering...).

Failure Reason – display the reason for the last registration attempt failure: the registrar's last error reply, e.g. 404 Not Found.

Advanced Settings

SIP Transport Protocol – set the SIP communication protocol: UDP (default), TCP or TLS.

Lowest Allowed TLS Version – set the lowest TLS version to be accepted for device connection.

Enforce SIPS URI Scheme – SPS URI Scheme is enforced when the parameter is activated (**sips** is used in outgoing messages and incoming messages must contain **sips**).

Verify Server Certificate – verify the SIP server public certificate against the CA certificates uploaded in the device.

Client Certificate – specify the client certificate and private key used for verifying the intercom's authority to communicate with the SIP server.

Local SIP Port – set the local port for the device for SIP signaling. A change of this parameter will not be applied until the device is restarted. When the parameter is empty, the default value is used:

Default Local Port Values for SIP

SIP	UDP and TCP	TLS
SIP 1	5060	5061
SIP 2	5062	5063

SIP	UDP and TCP	TLS
SIP 3	5064	5065
SIP 4	5066	5067

PRACK Enabled – enable the PRACK method for reliable confirmation of SIP messages with codes 101–199.

REFER Enabled – enable call forwarding via the REFER method.

Send KeepAlive Packets – set that the device shall send STUN/CRLF packets to the registrar on a regular basis and also SIP OPTIONS during calls to keep the setup connection active.

IP Address Filter Enabled – enable the blocking of SIP packet receiving from addresses other than SIP Proxy and SIP Registrar. The primary purpose of the function is to enhance communication security and eliminate unauthorized phone calls.

Receive Encrypted Calls Only (SRTP) – set that SRTP encrypted calls shall only be received on this account. Unencrypted calls will be rejected. At the same time, TLS is recommended as the SIP transport protocol for higher security.

Encrypted Outgoing Calls (SRTP) – set that outgoing calls shall be SRTP encrypted on this account. At the same time, TLS is recommended as the SIP transport protocol for higher security.

Use MKI in SRTP Packets – enable the use of MKI (Master Key Identifier) if required by the counterparty for master key identification when multiple keys rotate in the SRTP packets.

Do Not Play Incoming Early Media – disable playing of the incoming audio stream before the call sent by some PBXs or other devices is picked up (early media). A standard local ringtone will be played instead.

QoS DSCP Value – set the SIP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header. Enter the value as a decimal number. A change of this parameter will not be applied until the device is restarted.

STUN Enabled – enable STUN functionality for the SIP account. Address and ports acquired from the configured STUN server will be used in SIP headers and SDP media negotiation.

STUN server address – set the IP address of the STUN server that will be used for this SIP account.

STUN server port – set the port of the STUN server that will be used for this SIP account.

External IP Address – set the public IP address or router name to which the device is connected. If the device IP address is public, leave this parameter empty.

Compatibility With Broadsoft Devices – set the Broadsoft PBX compatibility mode. Having received re-invite from a PBX in this mode, the intercom replies by repeating the last sent SDP with currently used codecs instead of sending a complete offer.

Rotate SRV Records – allow SRV record rotation for SIP Proxy and Registrar. This is an alternative method of transition to backup servers in the event of main server failure or unavailability.

Video

Video Codecs

Enable/disable the use of video codecs for call setups and set their priorities.

Transmission Quality Settings

QoS DSCP value – set the video RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.

Maximum packet size – set the size limit for the video RTP packets to be sent.

Extended Codec Settings

Enabled – enable the packetization mode and set the payload type for each codec. The payload type can be selected automatically in case it cannot be set manually.

SDP Payload Type – set the payload type for video codec H.264 (packetization mode 1). Set a value from the range of 96 through 127, or 0 to disable this codec type.

Audio

Audio Codecs

Enable/disable the use of audio codecs for call setups and set their priorities in this block.

DTMF Sending

This block helps you define how DTMF characters shall be sent from the device. Check the opponent's DTMF receiving options and settings to make the function work properly.

Sending mode – define whether it will be possible to send DTMF during a call by pressing 0 through 9, * and # on the device numeric keypad. Set the sending mode for incoming/outgoing/all calls.

In-Band (Audio) – enable the classic method of sending DTMF in the audio band using standardized dual tones.

RTP (RFC-2833) – enable DTMF sending via the RTP according to RFC-2833.

SIP INFO (RFC-2976) – enable DTMF sending via SIP INFO messages according to RFC-2976.

DTMF Receiving

This block helps you define how DTMF characters shall be received from the intercom. Check the opponent's DTMF sending options and settings to make the function work properly.

In-Band (Audio) – enable classic DTMF dual tone receiving in the audio band.

RTP (RFC-2833) – enable DTMF receiving via RTP according to RFC-2833.

SIP INFO (RFC-2976) – enable DTMF receiving via SIP INFO messages according to RFC-2976.

Transmission Quality Settings

QoS DSCP Value – set the audio RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.

Jitter Compensation – set the buffer length for compensation of interval unevenness in audio packet arrivals. Set a higher value to increase the receiving immunity at the cost of a higher sound delay.

Alarm Call

Alarm Call

Basic Settings

Press Time for Activation – set the minimum press time in milliseconds for the ALARM1 button to initiate an alarm call. In accordance with the applicable EU standards, the maximum value must not exceed 3000 ms. The recommended range is 2000–3000 ms.

Delayed Call – set that the alarm call shall be delayed (the same sound message is played in the cabin during the delay as it is during call setup).

Call Delay – set the alarm call delay in seconds (the same audio message is played in the cabin during the delay as it is during call setup). Do not set this parameter to a value lower than in the **Press Time for Activation** parameter in the **Test Alarm** block. The function must be set to more than 0 s according to the applicable EU standards.

Test Alarm

NOTE
This function must be enabled according to the applicable EU standards.

Enable – make it possible to initiate a test alarm call by a mere long press of the ALARM1 button.

Press Time for Activation – set the press time in seconds for the ALARM1 button to initiate a test alarm call. The value may not be higher than as set in the **Delayed Call** parameter. The value must be set to 30 seconds in accordance with the applicable EU standards.

Destinations

The Destinations block helps you select a user to which the connection will be directed during the alarm call.

Repetition Count – set the count of call cycles in case the call is not confirmed/picked up. The default cycle count is 3, the maximum value is 9. When the set call cycle count has been accomplished and the call has not been picked up, the call is ended automatically.

Test ALARM Call – use this parameter to initialize the test alarm call.

Alarm Call 2

Destinations

The Destinations block helps you select a user to which the connection will be directed during the alarm call.

Repetition Count – set the count of call cycles in case the call is not confirmed/picked up. The default cycle count is 3, the maximum value is 9. When the set call cycle count has been accomplished and the call has not been picked up, the call is ended automatically.

Test ALARM2 Call – use this parameter to initialize the test alarm call 2.

Checking Call

Checking Call is used for automatic setup of a checking call, whose purpose is to check the proper function of **2N LiftIP 2.0**. This feature simulates an outgoing call.

NOTE
This function must be enabled according to the applicable EU standards.

Checking Call Enabled – enable test calls.

Basic Settings

NOTE
The checking call function must be performed at least once every three days according to the applicable EU standards.

Period – the checking call is always repeated once in the set number of days. The first checking call is made at a randomly selected time during the first 24 hours after the device startup.

Next Call – indicates the time of the next periodic checking call.

Destination

The Destination block helps you select a user to which the connection will be directed during the checking call.

Repetition Count – set the count of call cycles in case the call is not confirmed/picked up. The default cycle count is 3, the maximum value is 9. When the set call cycle count has been accomplished and the call has not been picked up, the call is ended automatically.

Test Checking Call – initialize the start of the test checking call.

Operational Call

Destination

The Destination block helps you select a user to which the connection will be directed during the operational call.

The operational call is used for automatic operational call setup if one of the preset events occurs. This section sets the destination to which the operational call will be routed. The call setup itself is set using Automation, refer to Automation (p. 56). The operational call is activated by the StartLiftCall action with the parameter CallType = operational. The action is triggered whenever the event to which the action is bound occurs:

- **RescueTerminated** to set up an operational call when the release mode is terminated.
- **ErrorStateChanged** to set up an operational call in the case of button failure/repair or audio failure/repair. The type of error state change is determined by the parameters of this event.

1–2 – select a user to which the connection will be directed.

Repetition Count – set the count of call cycles in case the call is not confirmed/picked up. The default cycle count is 3, the maximum value is 9. When the set call cycle count has been accomplished and the call has not been picked up, the call is ended automatically.

Services

Lift

Basic Settings

Lift ID – set the lift / lift intercom ID to be sent or read in calls. The identification number has to consist of 16 digits at most.

Rescue Mode

The release mode occurs when an alarm (emergency) call is connected. When enabling the mode, it is necessary to set the way of its subsequent termination.

NOTE

For EU version: Enable the Rescue mode in **Services > Lift > Rescue mode**. **This step is necessary so that the EU legislation can be met.** The device allows the Rescue mode to be active after activation, during which multiple alarm calls can be made. This facilitates displaying multiple alarm calls in Elevator Center within one rescue mode and returning to chats.

For US version: Make sure that the Rescue mode is disabled in **Services > Lift > Rescue mode**. **This step is necessary so that the US legislation can be met.** Every alarm call will be logged as a new entry in Elevator Center.

Enable Rescue Mode – enable the Rescue mode (the enabled rescue mode requires one type of Rescue mode end at least).

End by ALARM2 Button – make it possible to end the Rescue mode using the ALARM2 button.

End by Password – set that the Rescue mode end shall be confirmed with a password (sent to the device as DTMF into the call). Entering the password for exiting the Rescue mode is ineffective if an alarm call is in progress.

Password – set the Rescue mode end password. The password is sent to the device as DTMF into the call and may contain digits only (up to 16). The password is entered into DTMF in the following format: “*password*”. For example, if the password is 12345, you need to enter “*12345*”.

Cabin Monitoring

Monitoring Mode – set the device monitoring mode. This changes the microphone behavior (mute) and monitoring mode indication by the device (the device signals that the cabin audio and video are unavailable due to privacy protection). Monitoring can be:

Allow After Alarm Call For – set the time during which the microphone shall remain off and the device shall signal that monitoring is not allowed (the cabin audio and video are unavailable for privacy protection) after an alarm call. This applies only if **Monitoring Mode** is set to “Enabled after Alarm Call”.

E-Mail

SMTP

SMTP Service Enabled – enable/disable sending e-mails from the device.

SMTP Server Settings

Server Address – set the SMTP server address to which e-mails shall be sent.

Server Port – set the SMTP server port. The default value is 25, a modification is suitable only if the SMTP server configuration is non-standard.

Security Type – choose the security type for the SMTP server communication.

SMTP Server Login

Username – enter a valid username for login if the SMTP server requires authentication. Otherwise, the field can be left empty.

Password – enter a valid password for login if the SMTP server requires authentication. Otherwise, the field can be left empty.

Client Certificate – specify the client certificate and private key used for encrypting the device - SMTP server communication.

Common E-Mail Settings

From Address – set the default address for all the e-mails to be sent.

Advanced Settings

Deliver In – set the time limit for delivering an e-mail to an inaccessible SMTP server.

Automation

2N devices provide very flexible setting options according to various user requirements. There are situations when the usual range of settings (eg setting the behavior of switches or calls) is not enough, and for these cases 2N devices provide a special programmable Automation interface. A typical use of Automation is in applications that require more complex integration with third-party systems.

The Automation interface is entered by clicking on  for the function you want to create or change.

TIP
A detailed description of the Automation function and configuration is available in Automation manual.

NOTE
The automation feature is only available with the Gold license.

HTTP API

HTTP API is an application interface designed for the control of selected device functions via HTTP. It enables the 2N devices to be integrated easily with third party products, such as home automation, security and monitoring systems, etc.

Services

HTTP API Services

HTTP API provides the following services:

- **System API** – device configuration changes, status info and upgrade.
- **I/O API** – device logic input/output control and monitoring.
- **Audio API** – audio playback control and microphone monitoring.
- **E-Mail API** – sending user e-mails from the device.
- **Phone/Call API** – incoming/outgoing call control and monitoring.
- **Logging API** – reading out event records from the device.
- **Automation API** – setting Secure/Insecure communication and authorization requirements.
- **Elevator API** – **Sentrio Lobby** connection to the emergency elevator communicator.

Set the connection type (HTTP=TCP or HTTPS=TLS) and way of authentication (None, Basic or Digest) for each function. Create up to five user accounts (with own username and password) in the HTTP API configuration for detailed access control of services and functions.

Set the authentication methods for the requests to be sent to the device for each service. If the required authentication is not executed, the request will be rejected. Requests are authenticated via a standard authentication protocol described in RFC-2617. The following three authentication methods are available:

- **None** – no authentication is required. In this case, this service is completely insecure in the LAN.
- **Basic** – Basic authentication is required according to RFC-2617. In this case, the service is protected with a password transmitted in an open format. Thus, we recommend that this option is combined with HTTPS where possible.
- **Digest** – Digest authentication is required according to RFC-2617. This is the default and most secure option of the three above listed methods.

Account 1–5

The 2N device allows you to manage up to five user accounts dedicated to access to the HTTP API services. A user account includes the user name and password and a table of the user access rights to each of the HTTP API services.

Account Enabled – enable the user account.

User Settings

Username – enter the HTTP API authentication username.

Password – enter the HTTP API authentication password.

User Privileges

The table of access rights helps you manage the user account privileges to the services.

Integration

MS Teams Tab

Microsoft Teams integration provides calls between a 2N device and the Microsoft Teams account. You have to configure the Microsoft Teams SIP gateway to interconnect the device with Microsoft Teams. Refer to the FAQ or the MS Teams documentation for details. Once you enter the configuration server address into the 2N device configuration, the integration (onboarding) is accomplished. Upon onboarding, you can log in to the Microsoft Teams account in the web configuration interface.

Microsoft Teams Enabled – enable integration with MS Teams

Service

State – display the current status of the onboarding and login processes.

- “Disabled” – function disabled.
- “Onboarding” – the device is getting/has got the shared configuration for onboarding or individual configuration for onboarding (before login).
- “Onboarding failed” – the device was unable to get the shared/individual onboarding configuration or to register with the onboarding SIP server.
- “Offline” – no sever response.
- “Online” – successful device registration with the end SIP server.
- “Registration Failed” – the device failed to register with the end SIP server.
- “License Required” – the device is not equipped with the license required for this function.

Phone Number – display the phone number (ID) that the device obtained from the MS Teams server.

Test Call – display a dialog box enabling you to make a test call to a selected phone number.

Provisioning Server Settings

Address Retrieval Mode – select whether the MS Teams onboarding server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 or 150 shall be used.

Server Address – enter the MS Teams onboarding server manually.

DHCP (Option 66/150) address – check the server address retrieved via the DHCP Option 66 or 150.

Configuration Update Schedule

At Boot Time – enable check and, if possible, update upon every device start.

Update period – set the update period. hourly, daily, weekly and monthly.

Update At – set the update time in the HH:MM format for periodical updating The parameter is not applied if the update interval is shorter than 1 day. Time is set in UTC. Check the Next Update Time value to see the actual update time scheduled.

Discovery Service Tab

Settings

Integration Server Address – set the URL of the Discovery Service. The device sends HTTP requests with basic data at startup, whenever the IP address changes and periodically (if configured). If the field is empty, no requests are sent.

NOTE
The JSON request sent contains the following information about the device: MacAddress, Dhcp, IpAddress, NetMask, Gateway, SwVersion, SerialNumber, Variant, VariantId, Description, ProductName, CameraResolution (max.), HttpPort, HttpsPort.

Verify Server Certificate – enable validation of the integration server certificates to ensure that the Discovery requests are sent to a trusted server.

Client Certificate – select which of the uploaded certificates will be used for encrypted communication with the integration server.

Send Discovery Requests Periodically – enable sending the Discovery HTTP requests.

Discovery Period – set the period of sending the HTTP request to the configured URL in seconds.

Integration Status – display the integration status based on the response from the server.

Details – display the details contained in the response from the server.

User Sounds

2N LiftIP 2.0 signals variable operational statuses with a sequence of tones. If the standard signaling tones do not meet your requirements, you can modify them.

Sound Mapping

Language 1–3 – select a language for the device sound messages. If there is a translation available for a mapped sound, the message is played in the selected language. If no translation is available, the message is played in English or as a language-neutral sound.

Sound Mapping

- “Establishing Connection” – set a sound message to be played in the cabin while the alarm call is being established.
- “Alarm Call” – set a sound message to be played in the call when the alarm call has been established.

- “Checking Call” – set a sound message to be played in the call when the checking call has been established.
- “Call Extension” – set a sound message to be played in the call when the call is approaching its end.
- “Disconnection” – set a sound message to be played in the call and the cabin (if relevant for the given call type) in case the active call has to be interrupted.
- “Call End” – set a sound message to be played in the cabin when the call has ended.
- “Rescue End” – set a sound message to be played in the call and the cabin when the rescue mode has ended (relevant only if the rescue mode is enabled).

Sound Upload

Up to 10 sound files with a maximum length of 60 seconds can be added to the device. You can assign a unique name to each added sound for better orientation.

Sound Adding Procedure

1. Press to upload a sound file to the device.
2. Select a file from your PC in the dialog box and click Upload.
3. Press to record a sound file via your PC microphone.
4. Press to remove a file. Click to play a successfully uploaded sound file (locally on your PC).

Web Server

2N LiftIP 2.0 can be configured using a common browser that approaches the web server integrated in the device. The HTTPS protocol is used for the browser - device communication.

Basic Settings

Device Name – set the device name to be displayed in the right-hand upper corner of the web interface, in the login window and in other applications if necessary (2N Network Scanner, etc.).

Web Interface Language – set the default language after the administration web server login. Use the upper toolbar buttons to change the language temporarily.

Password – set the device login password. Click the pencil icon to change the password. Make sure that the password contains 8 characters at least, including one small alphabet letter, one capital alphabet letter and one digit.

Advanced Settings

HTTP Port – set the web server port for HTTP communication. The port change will not be applied until the device is restarted.

HTTPS Port – set the web server port for HTTPS communication. The port change will not be applied until the device is restarted.

Lowest Allowed TLS Version – set the lowest TLS version to be accepted for device connection.

HTTPS Server Certificate – set the server certificate and private key used for encrypting the communication between the device HTTPS server and user web browser.

Remote Access Enabled – enable remote access to the device web server from off-LAN IP addresses.

User Localization

Original Language – download an original XML file from the device including all user interface texts in English.

Custom Language – upload , download and/or remove user files including translations of the user interface texts.

Audio Test

Audio Test Enabled – enable the automatic execution of the audio test.

Test Settings

Test Period – set the test executing period. The test can be started automatically once a day or once a week.

Test Start Time – set the test time period. Set the time in the HH:MM format. We recommend that the time value is set at which a low device traffic is expected.

Test Result

Test Status – display the current test status.

Last Test Time – display the start time of the last-performed test.

Last Test Result – display the result of the last-performed test.

SNMP

The 2N access units integrate a functionality that allows the network devices to be monitored remotely using the SNMP.

Service Enabled – turn on this feature.

SNMP Settings

Lowest Allowed Version – select the lowest SNMP version accepted by the device. SNMPv3 enforces encryption.

Community String – text string representing the access key to the MIB table objects.

Trap IP Address – IP address to which the SNMP traps are to be sent.

Download MIB File – download the current MIB table definition from a device.

SNMP Identification

Contact – enter the device manager contact (name, e-mail, etc.).

Name – enter the device name.

Location – enter the device location (1st floor, e.g.).

Authorized IP Addresses

IP Address 1 – enter the valid IP addresses for access to the SNMP agent. The access from other addresses will be blocked. If the field is empty, the device may be accessed from any IP address.

SNMPv3 Settings

Username – set the algorithm to be used for the SNMPv3 trap authentication.

Authentication – set the algorithm to be used for the SNMPv3 trap decryption.

Authentication Password – set the SNMPv3 authentication password.

Privacy / Encryption – set the algorithm to be used for the SNMPv3 trap decryption.

Decryption Password – set the SNMPv3 trap decryption password.

Hardware

Audio

This part of the configuration is used to set the call volume and the signaling volume for various device states.

The master volume of the device affects both the call volume and the volume of signaling tones. Set this parameter according to the noise level of the environment in which the device is used.

TIP
The master volume of the device can also be controlled using the VOL+ and VOL− buttons.

Phone Call Volume

Call Progress Tone Volume – set the dial tone, ringtone and busy tone volume levels. This setting is not applied when the dial tones are generated externally. The value is relative against the master volume value.

Signaling Volume

Warning Tone Volume – set the volume of warning and signaling tones described in the Signaling of Operational Statuses section. The value is relative to the master volume.

Suppress Warning Tones – suppress signaling of the following operational states: Internal application started, IP address received and IP address lost.

User Sounds Volume – set the volume of user sounds played by automation. The value is relative to the master volume.

Network Start and State Signaling – select the sound signaling mode for application launch and IP address gain/loss.

- **Enabled** – The device plays audio signals each time the application starts and whenever the IP address changes.
- **Disabled** – No audio signals are played.
- **Only Once** – The device plays the application startup and IP address acquired signals only once after boot. This is useful when the IP address changes frequently or intermittent connectivity issues occur, as repeated signaling might cause user discomfort.

Audio Inputs Settings

Microphone Input Gain – set the microphone input gain.

Digital Inputs

The Digital Inputs menu describes the digital input options for the device.

Input Inversion

Inverted ALARM1 button – an inverted input is active when the contact is open or voltage is applied.

Inverted ALARM2 button – an inverted input is active when the contact is open or voltage is applied.

Inverted CANCEL Input – an inverted input is active when the contact is open or voltage is applied.

Buttons

Button Error Evaluation Time – set the time during which the ALARM1 button has to be activated until the button error is detected.

External Camera

External IP Camera

Camera enabled – enable RTSP stream download from an external IP camera. Complete the valid RTSP stream address or the username and password to make the function work properly.

RTPS Stream Address – set the RTSP stream address in the format “rtsp://camera_ip_address/parameters”. The parameters are specific for the selected IP camera model.

Username – enter the username for the external IP camera authentication. The parameter is mandatory only if the external IP camera requires authentication.

Password – enter the external IP camera authentication password. The parameter is mandatory only if the external IP camera requires authentication.

Local RTP Port – the local RTP port can be changed if the network configuration requires so.

External IP Camera Log

The External IP Camera Log displays the RTSP communication with the selected external IP camera including failures and error states if any.

System

Network

2N LiftIP 2.0 is connected to the LAN and has to be assigned a valid IP address or obtain the IP address from the LAN DCHP server. The Network section helps you configure the IP address and DHCP.

TIP
To retrieve the IP address, use 2N Network Scanner, which can be downloaded freely from 2N.com. Refer to Subs. IP Address Retrieval Using 2N Network Scanner for details.

Basic

Use DHCP Server – enable automatic obtaining of the IP address from the LAN DHCP server. If no DHCP server is existing or available in the network, set the network manually.

Static IP Address Setting

Static IP Address – static IP address of the device. The address is used together with the below mentioned parameters if the Use DHCP Server parameter is disabled.

Network Mask – network mask setting.

Default Gateway – default gateway address for off-LAN communication.

DNS Setting

Always Use Manual Setting – enable manual setting of the DNS server addresses.

Primary DNS – primary DNS address for domain name-to-IP address translation.

Secondary DNS – secondary DNS address where the primary DNS is unavailable.

Network Interface Settings

Required Port Mode – set the LAN port mode to be preferred: Automatic or Half Duplex – 10 Mbps. The bit rate is reduced to 10 Mbps in case the available LAN cabling is unreliable for a 100 Mbps traffic.

Current Port State – current LAN port state: Half or Full Duplex – 10 Mbps or 100 Mbps.

Network Identification

Hostname – set the device LAN identification.

Vendor Class Identifier – set the manufacturer identifier as a character string for DHCP Option 60.

VLAN Settings

VLAN Enabled – enable the virtual network support (VLAN according to 802.1q). Remember to set the VLAN ID too.

VLAN ID – choose a VLAN ID from the range of 1–4094. The device shall only receive packets with the set ID. An incorrect setting may result in a connection loss and subsequent factory reset.

Firewall Tab

Enable Firewall – enable a firewall that protects the device from adverse requests. It is strongly recommended that the firewall is activated at all times.

Firewall

Enabled – enable a firewall that protects the device from adverse requests.

Status – display the state of the firewall. The firewall status can be Off, On, or Possible Attack Detected (when a problem is detected and some requests are ignored).

Date and Time

Select Use Time from Internet to synchronize the device time with the Internet time or click Synchronize with Browser to synchronize time with your current PC time.

CAUTION
It is recommended that the Use time from Internet function is enabled for a maximum accuracy and reliability. The device time error can be up to ±2 minutes per month under normal operation conditions.

NOTE
The device does not need the current date and time values for its basic function. .

Current Time

Use Time From the Internet – Enable the NTP server use for device time synchronization.

Synchronize With Browser – click the button to synchronize the device time with your current PC time value.

Time Zone

Automatic Detection – define whether the time zone shall be detected automatically from My2N. In case automatic detection is disabled, the Manual selection parameter is Used (manually selected time zone or Own rule).

Detected Time Zone – the automatically found time zone. In case the function is unavailable or disabled, N/A is displayed.

Manual Selection – set the time zone for your installation site. to define time shifts and summer/winter time transitions.

Custom Rule – if the device is installed on a site that it not included in the Time Zone parameter, set the time zone rule manually. The rule is applied only if the Time Zone parameter is set to Manual.

NTP Server

NTP Server Address – set the IP address/domain name of the NTP server used for the device internal time synchronization. The server IP address and domain name cannot be set if Use Time from Internet is disabled.

NTP Time Status – display the state of the last local time synchronization attempt via NTP: Unsynchronized. Synchronized, Error.

Features

The menu provides a list of published beta functions designed for user testing.

The list includes:

- function name,
- function status (started/stopped),
- action that starts/stops the function.

The function will not be started/stopped until the device is restarted. The status change request can be cancelled using the **Interrupt** action before the device is restarted.

NOTE
The test functions are not warranted and 2N TELEKOMUNIKACE a.s. shall not be held liable for any functionality limitations and damage incurred as a result of functionality limitations of the beta functions. The beta functions are provided for testing purposes exclusively.

Certificates

Some **2N LiftIP 2.0** LAN services use the secure TLS protocol for communication with the other LAN devices. This protocol prevents third parties from eavesdropping on or modifying call contents. TLS is based on one/two-sided authentication, which requires certificates and private keys.

The following device services use the TLS protocol:

1. Web server (HTTPS)
2. 802.1x (EAP-TLS)
3. SIPs

The device allows you to upload up to 3 sets of certificates from certification authorities, which help you authenticate the communicating device, and also 3 user certificates and private keys for encryption purposes.

Each certificate requiring service can be assigned one certificate set, refer to Web Server (p. 59). The certificates can be shared by the services.

The device supports the DER (ASN1) and PEM certificate formats.

Upon the first power up, the intercom automatically generates the Self Signed certificate and private key for the Web server and services without forcing you to load a certificate and private key of your own.

NOTE
If you use the Self Signed certificate for encryption of the device web server – browser communication, the communication is secure, but the browser will warn you that it is unable to verify the device certificate validity.

The current list of uploaded CA and user certificates is available in the following two folders: CA Certificates and User Certificates.

Certificate Upload

1. Click to upload a certificate saved in the storage.
2. Select the certificate (or private key) file in a dialog window.
3. Press the **Upload** button.
4. Press to remove a certificate from the device.

NOTE

- A certificate with a private RSA key longer than 2048 bits can be rejected. and the following message will be displayed:
  “The private key file/password was not accepted by the device!”
- For certificates based on elliptic curves use the secp256r1 (aka prime256v1 aka NIST P-256) and secp384r1 (aka NIST P-384) curves only.

CSR

You can create a custom Certificate Signing Request (CSR) in the web configuration interface to be submitted to a certification authority (CA) for signing. This process ensures that the certificate is correctly paired with the private key that was generated when the CSR was created and remains securely stored only on your device.

1. Click to create a new certificate request.

2. A dialog box will appear for you to fill in the following information:
   - **Common Name (CN)** – this entry must contain the IP address/domain name under which the 2N IP intercom web interface can be accessed.
   - **SAN: mDNS** – enable the inclusion of **mDNS (Multicast DNS)** as an alternative subject name (SAN) in the certificate. It is used for access through a domain name in the local network.
   - **SAN: IP** – enable the inclusion of the **IP address** as an alternative subject name (SAN) in the certificate. It is used for access via IP address.
   - **Public Key Algorithm** – specify the type of the algorithm to be used for generating the public key in the certificate.
   - **CSR ID** – unique identifier of the Certificate Signing Request (CSR).
   - **Country (C)** – two-letter code of the country in which the organization is registered (according to ISO 3166-1 alpha-2).
   - **State/Country/Region (S)** – state/region in which the organization is registered (not abbreviated).
   - **City/Locality (L)** – name of the city/locality in which the organization is registered (not abbreviated).
   - **Organization (O)** – legal name of the organization including such suffixes as Inc., Corp., Ltd.
   - **Organizational Unit (OU)** – name of a department/unit within an organization.
   - **E-Mail** – e-mail address of the contact person or certificate manager.
3. Click Generate to create a certificate signing request. Download the created CSR file and save it in a safe place.
4. Submit the CSR file to the certification authority (CA), which issues a digital certificate based on it.
5. Upload the issued digital certificate back to the CSR file in the web interface. Click + in the row of the certification request for upload.

Press 🗑 to delete the CSR. Press ⓘ to view the CSR parameters.

Auto Provisioning

My2N

The My2N cloud platform is used for remote administration and configuration of the 2N IP devices and helps you remotely connect to the device web interface.

My2N Enabled – enable connection to My2N.

My2N Security Code

Serial Number – display the serial number of the device to which the valid My2N code applies.

My2N Security Code – device code for adding to My2N.

Generate New – the active My2N Security Code will be invalidated and a new one will be generated.

Connection State

It displays information on the state of the device connection to My2N.

My2N ID – unique identifier of the company created via the My2N portal.

TR069

Use this tab to enable and configure remote device management via the TR-069 protocol. TR-069 helps you reliably configure the device parameters, update and back up configuration and/or upgrade device firmware.

The TR-069 protocol is utilized by the My2N cloud service. Make sure that TR-069 is enabled and Active profile set to My2N to make the device work with My2N properly. Only then the device will be able to log in to My2N periodically for configuration.

This function helps you connect the device to your ACS (Auto Configuration Server). In this case, the connection to My2N will be disabled in the device.

My2N / TR069 Enabled – enable connection to My2N or another ACS server.

General Settings

Active Profile – select one of the pre-defined profiles (ACS), or choose a setting of your own and configure the ACS connection manually.

Next Synchronization In – display the time period in which the device shall contact a remote ACS.

Connection State – display the current ACS connection state or error state description if necessary.

Communication Status Detail – server communication error code or HTTP status code.

Connection Test – test the TR069 connection according to the set profile, see the Active profile. The test result is displayed in the Connection status.

Diagnostics

Diagnostics

The interface allows you to capture diagnostic logs to be downloaded and sent to the Technical support subsequently. The diagnostic logs help identify and solve reported troubles. The logs include information on the device and its configuration, LAN operations, crash log and memory statistics.

Diagnostic Package

Packet Capture Status – display whether or not packet capture is started in the Packet capture folder.

Size of Captured Packets – display the amount of the packets captured.

Syslog Capture State – display whether or not Syslog message capture is started in the Syslog folder.

Duration of Captured Syslogs – display how long Syslog messages are captured in the Syslog folder.

Size of Captured Syslogs – display the amount of the Syslog messages captured.

Stop Syslog Capture – set the data capture time.

Start capturing using the recording button  . By repressing the recording button  the capture will be restarted and run again. Download the packet capture file using  . The packet capture file includes a file with the stored device configuration.

Encrypt the file with a password for additional security. This password will be needed when restoring the configuration to decrypt the file and access its contents. Make sure you do not lose your password and store it in a safe place.

Exporting a hash for a secure output adds a hash form to the values in the configuration file in which they are written to the syslog. The hash form is added as an attribute **DiscreteHash** to the values.

CAUTION

- The start of diagnostic data capture restarts the packet capture if running.
- Encrypt the file with a password for additional security. This password will be needed when restoring the configuration to decrypt the file and access its contents. Make sure you do not lose your password and store it in a safe place.

Tools

Verify network address accessibility – verify the network address accessibility via the Ping command in standard operating systems. Press Ping to display a dialog box for you to enter the IP address/domain

name and press Ping to send the test data to the set address. If the IP address/domain name is invalid, a warning is displayed and the Ping button remains inactive until the IP address becomes valid. The dialog box also displays the procedure state and result. Failed means that either the IP address was unavailable within 10 s or it was impossible to translate the domain name into an address. If a valid response is received, the response sending IP address and response waiting time in milliseconds are displayed. Press Ping again to send another query to the same address.

Packet Capture

In the Trace tab, you can launch capturing of incoming and outgoing packets on the network interface. The captured packets can be stored locally in a 4 MB buffer or remotely in the user PC. The file with captured packets can be downloaded for Wireshark processing, e.g. (www.wireshark.org).

Local Packet Capture

We recommend that you lower the video stream transmission rate below 512 kbps while capturing packets locally. When the local capture buffer is full, the oldest packets are rewritten automatically.

1. Click  to start packet capturing.
2. Click the icon  to stop packet capturing.
3. Click  to save the packet capture file on a disk.

Remote Packet Capture

1. Click  .
2. A box will open for you to set the incoming/outgoing packet capturing time (in seconds).
3. Click OK to start capture.
4. Select a location on the disk for the packet capture file to be saved.
5. Click  to stop capturing.

Syslog

2N LiftIP 2.0 allows you to send system messages to the Syslog server including relevant information on the device states and processes for recording and subsequent analysis and audit. It is unnecessary to configure this service for common operations.

Such sensitive data as access codes, card identifiers, login credentials, etc. are stored in the syslog in an encrypted (hash) form. The assignment of hash values to real values can be done according to the configuration file.

Syslog Server Settings

Send Syslog Messages – enable sending of syslog messages to the Syslog server. Make sure that the server address is valid.

Server Address – set the “IP[:port]” or MAC address of the server on which the Syslog message capture application is running.

Severity Level – set the severity level of the messages to be sent (Error, Warning, Notice, Info, Debug 1–3). Debug 1–3 level setting is only recommended to facilitate troubleshooting for the Technical Support department.

Local Syslog Messages

This block provides a general overview of local Syslog messages. Local Syslog messages can be uploaded  and downloaded  .

Maintenance

This menu helps you maintain the device configuration and firmware. You can back up and restore all the parameters, upgrade firmware and/or factory reset the device.

Configuration

Restore Configuration – restore configuration from a previous backup. Press the button to display a dialog box to select a configuration file and upload it to the device. Before uploading choose whether or not the LAN settings and SIP PBX connection settings are to be applied.

When restoring a configuration from an encrypted file, you need to enter a password to decrypt it.

CAUTION

The login password is saved in the configuration file. If the password is not encoded in the file or 2n is the default password, the valid configuration part will only be uploaded. This means that the configuration is uploaded, but the password remains the same, not assuming the value given in the file.

Back Up Configuration – back up the complete current device configuration. Press the button to download the complete configuration into a storage.

CAUTION

- As the device configuration may include delicate information, such as user phone numbers and access passwords, handle the file cautiously.
- Encrypt the file with a password for additional security. This password will be needed when restoring the configuration to decrypt the file and access its contents. Make sure you do not lose your password and store it in a safe place.

Reset Configuration – used for restoring all the device parameters to the default state. Restoring the network parameters and certificate settings requires additional confirmation in the confirmation box.

System

Upgrade Firmware – upload a new firmware version to the device. Press the button to display a dialog box and select the proper firmware file. Once the firmware is uploaded successfully, the device is restarted automatically. After restart, the device becomes fully operational with a new firmware version. The whole upgrading process takes less than one minute. Download the current firmware version for your device from 2N.com. The FW upgrade does not affect configuration. The device checks the firmware file and prevents you from uploading an incorrect or corrupt file.

Firmware Status – display whether a new firmware version is available. If not, Check is displayed for you to verify online if a new firmware version is available. If so, press Update to download the firmware and upgrade the device automatically.

Notify of Beta Versions – enable monitoring and downloading of the latest firmware beta version.

NOTE
There is no automatic firmware update on this device to ensure stable operation and prevent potential compatibility issues with third-party systems integrated into your environment. To maintain system integrity and avoid unintended disruptions, all updates must be manually confirmed or initiated by the user. Before applying any update, please review the release notes and verify compatibility with your existing infrastructure.

Restart Device – restart the device. The process takes about 30 s. Once restart is completed and the device is assigned its IP address, the login window will be displayed automatically.

CAUTION
The device configuration change writing takes 3–15 s depending on the device configuration size. Do not restart the device during this process.

Third Party Library License – click Show to open a dialog box including a list of used licenses and third party libraries. It also includes a EULA link.

Usage Statistics

Send Anonymous Statistics Data – enable sending of anonymous statistic data on device usage to the manufacturer. No such delicate information as passwords, access codes or phone numbers are included. This information helps 2N TELEKOMUNIKACE a.s. improve the software quality, reliability and performance. You can participate in this voluntarily and cancel your statistic data deliveries any time.

Used Ports

Service	Port	Protocol	Direction	Configurable	Settings
RTP	9 000			✓	**Calling > General Settings**
DHCP	68	UDP	In/Out	×	–
DNS	53	TCP/UDP	In/Out	×	–

Function and Use

This section describes the basic and advanced functions of the **2N LiftIP 2.0** product.

Function description

The purpose of this section is to provide aid in troubleshooting. If the system fails to work correctly, a qualified technician is commissioned to follow its operation according to the descriptions included herein. Having found a discrepancy between a description and reality, the technician describes this discrepancy, which significantly accelerates finding of the trouble cause. This procedure often reveals that the system works properly but the user had a different idea of its function.

Outgoing Call

The process is initiated by pressing the ALARM button on the audio unit (CANCEL may delay or block the execution). When the ALARM button is pressed, **2N LiftIP 2.0** establishes connection with the control center (refer to Automatic Dialing for details). **2N LiftIP 2.0** plays the “Wait please, connection is being established” message to the person in the lift and “Press 1 for confirmation” to the control center (if DTMF 1 confirmation is used). It is necessary to confirm the call manually or automatically. The call is time limited (Attention, the call end is near. Press 4 to extend the call.”), but can be extended. Refer to the Control Center Instructions Subs. for control during a call (DTMF dialing).

TIP
Set the alarm call destinations and checking and operational call destinations.

Checking Call

Checking call is an automatically made outgoing call (typically once in 3 days) whose purpose is to check the 2N LiftIP 2.0 function. The operation is the same as with an outgoing call. The difference is that a different announcement is played, e.g. “This is a checking call”, and a different set of phone numbers is used (refer to 4.3.6 Checking Call). The checking call enables automatic processing. A checking call voice message is played for manual pickup (confirmation 1 or pickup setting) and no message is played for automatic processing.

TIP
A checking call can be initiated manually too. The regular checking call schedule is not affected.

WARNING
If the **checking call** memory set is completely empty, no checking call is made, even to the alarm call memory set.

Operational Call

Operational call is a call made automatically whenever a defined event happens (stuck button, rescue end, audio error, ...). Refer to Subs. Operational Call (p. 54) s for settings and details.

Incoming Call

The control center can also call the **2N LiftIP 2.0** number, which automatically receives every incoming call. The incoming call is time limited and controlled like the outgoing call (extension, identification).

The incoming call can, for example, inform a trapped person about the rescue squad arrival, etc. Also, it helps check **2N LiftIP 2.0** remotely for a proper function and connection.

Useless Startup Protection

As the only purpose of **2N LiftIP 2.0** is to call for help when a person gets trapped in a lift, no call is necessary if the cabin door is open. If the elevator is equipped with a door contact, connect the contact to the **2N LiftIP 2.0** CANCEL input and define a timeout for **2N LiftIP 2.0** to wait after the ALARM button is pressed until it establishes connection Thus, if the ALARM button is pressed by mistake, the elevator arrives in a floor, the door opens and the call is canceled. Also, the minimum button pressing time can be set to eliminate erroneous pressing of the button.

Call End (Outgoing/Incoming)

The call end (line hang-up) occurs whenever any of the below listed situations happens:

- the counterparty (control center) hangs up;
- The maximum call duration expires – 10 s before the expiry, **2N LiftIP 2.0** plays the “Attention, the call end is near. Press 4 to extend the call.” to allow you to extend the call.

Control Centre Instructions

DTMF Control during Call (DTMF)

You can use tone dialing (if Automatic dialing with confirmation is enabled) during a call to control **2N LiftIP 2.0** as shown below. Commands 1 through 4 are arranged conveniently for typical use.

DTMF character	Function description
1	Successful call confirmation for 2N LiftIP 2.0. 2N LiftIP 2.0 mutes the currently played announcement and sends its confirmation signal, the call goes on until the call time limit is exhausted and any of the following commands can be used.
3	Play the communicator information.
4	Call Extension – extend the call by 120 s, can be used repeatedly.

List of 2N LiftIP 2.0 Announcements

Announcement	Meaning
“Wait please, connection is being made”	The announcement is played to the elevator user when the call is being set up (before confirmation).
“This is an alarm call”	The announcement is played to the control center before call confirmation.
“This is a checking call.”	The announcement is sent to the control center only (if DTMF 1 confirmation is enabled).
“Attention, the call end is near. “Press 4 to extend the call.”	The announcement signals during an outgoing/incoming call that the maximum call duration shall expire in 10 seconds.
“Sorry, your call has to be interrupted.”	The announcement is played to the elevator user during an active call.
“Call end”	The announcement is sent before hang-up.
“Rescue process has been ended”	Confirmation that the alarm situation signaling has been terminated.

2N LiftIP 2.0 Identification

When the alarm call is confirmed, the control center can press DTMF 3 to get the communicator serial number. The communicator information can be obtained during an incoming call too.

Call Confirmation Types

These settings apply to the alarm, checking and error reporting calls.

Confirmation by pressing 1

Up to 4 phone numbers and a repetition count can be stored for calls to the control center.

2N LiftIP 2.0 then tries to call the set numbers one by one. **2N LiftIP 2.0** uses tone dialing (DTMF) as the most reliable confirmation method. The control center has to press the 1 button on its phone (in the tone dialing mode) during manual call answering. If the called number is busy or unanswered within a timeout or unconfirmed, **2N LiftIP 2.0** dials the next number in the sequence until it exhausts the preset count of attempts for all the numbers stored. Checking calls or failure reports are made equally, yet a separate set of 2 numbers can be used.

Evaluation of Dialing with Confirmation Situations

Situation	2N LiftIP 2.0
Call termination by the counter-party (Busy, Number not found, etc.)	Dials the next number immediately.
Call	Waits for a timeout.
Ringing	Waits for a timeout.
DTMF character 1	Confirms the connection (“Connection confirmed"), mutes the announcement played and the call takes the maximum preset time (Maximum call time).
1 3 4	These digits are interpreted as control characters.

Confirmation by Off-Hook

VOIP

CAUTION
The call is confirmed after the voice message is played.

The called user does not have to press any button. Both the modes share a set of numbers and cycle counts and respond identically to situations during dialing.

WARNING
Make sure before using this mode that no VoiceMail box, fax machine or any other device that could answer the call before the preset ring count is installed on any of the numbers to be called. This would lead to automatic dialing termination.

CPC (Antenna and KONE)

Used wherever the counterparty is equipped with the required SW. When the line is answered, a DTMF string is sent. The elevator identifies itself. The call is either switched to voice communication (alarm call) or confirmed automatically and terminated (checking call).

P100

Used wherever the counterparty is equipped with the required SW. When the line is answered, a DTMF character is sent. The elevator identifies itself. The call is either switched to voice communication (alarm call) or confirmed automatically and terminated (checking call).

DTMF Protocol Auto Detection (CPC/P100)

When the DTMF string is sent, the lift identifies the protocol and responds accordingly.

WARNING

- If, for example, the call is routed via GSM,**2N LiftIP 2.0** may not detect the DTMF characters and identify the protocol.
- If this happens, we recommend you to change the CPC or P100 settings (3 or 5).

CPC (Antenna), P100 2N ext (for alarm calls only)

The protocols work as described in items 3 and 4 for CPC and item 5 for P100. The only difference is that the audio unit type is transmitted too. Used for alarm calls to the communicator only.

Audio Unit Audio Test

The audio unit audio test enables the automatic audio test. It sets a daily / weekly period at a selected time. If the audio unit is OK, the next checking call will be made. If an error is detected during the audio test, the next checking call will not be made.

Event after Audio Error

This event informs of an audio test failure. Set the event via the device web configuration, see Operational Call (p. 54). When the audio test is evaluated as unsuccessful, the event is executed (an operational call is set up).

- Operational call – the call is set up to the number set for the operational call.

Rescue Process Activation / End

Rescue Process Activation

If an alarm call is set up, the yellow LED keeps shining on the audio unit after the call end. This indicates the rescue process activation.

Rescue Process End

2N LiftIP 2.0 and enter the rescue end confirming password (***password***) during the call to end the rescue process Or, press ALARM2 in the elevator cabin.

The audio unit announces "Rescue process has been ended" when the rescue process has been completed.

Set the operation via the web interface, refer to Rescue Mode.

Event after Rescue End

An event can be made when the rescue process has been ended. **2N LiftIP 2.0** supports operational calls only.

- Operational call – the call is set up to the number set for the operational call.

Set the operation via the web interface, see Operational Call (p. 54).

CPC and P100 Protocols

CPC

The CPC protocol supports 3 options: **KONE**, **Antenna** and **Antenna 2N Ext**.

The data message consists of:

Command – Call type – DATA – ID

CPC

Call Type	Command	Call Type	Data	ID
Alarm	04	10	0000000000000	Lift ID
Alarm 2	04	10	0000000000000	Lift ID
Checking Call	04	21	0000000000000	Lift ID
Rescue process ended	04	84	0000000000000	Lift ID
Button Error	04	90	0000000000000	Lift ID
Button Repair	04	90	0000000000001	Lift ID
Audio Error	04	91	0000000000000	Lift ID
Audio Repair	04	91	0000000000001	Lift ID

NOTICE
This is only a part of the data message. It does not contain the beginning, checksum and end.

04900000000000000187654321 – Button fixed, identification number 87654321.

The data message consists of:

Command – Call type – ID

CPC Antenna

Call Type	Command	Call Type	Data	ID
Alarm	04	27	-	Lift ID
Alarm 2	04	27	-	Lift ID
Checking Call	04	26	-	Lift ID
Rescue process ended	04	84	-	Lift ID
Button Error	04	90	-	Lift ID
Button Repair	04	90	-	Lift ID
Audio Error	04	91	-	Lift ID
Audio Repair	04	91	-	Lift ID

NOTICE
This is only a part of the data message. It does not contain the beginning, checksum and end.

0492687654321 – Checking call, identification number 87654321.

The data message consists of:

Command – Call type – DATA – ID

CPC Antenna 2N Ext

Call Type	Command	Call Type	Data	ID
Alarm	04	27	00000	Lift ID
Alarm 2	04	27	00000	Lift ID

Call Type	Command	Call Type	Data	ID
Checking Call	04	26	00000	Lift ID
Rescue process ended	04	84	00000	Lift ID
Button Error	04	90	00000	Lift ID
Button Repair	04	90	00001	Lift ID
Audio Error	04	91	00000	Lift ID
Audio Repair	04	91	00001	Lift ID

NOTICE
This is only a part of the data message. It does not contain the beginning, checksum and end.

04910000087654321 – Audio error, identification number 87654321.

CAUTION

- The Button fixed/Audio fixed information is only transmitted via the 2N Ext protocol.
- If the 2N Ext mode is not set, the operational call cannot be established.
- The CPC protocol uses up to 16 digits for elevator identification, P100 uses only 8 digits.

P100

The data message consists of:

Call type – ID – DATA

P100

Call Type	Call Type	ID	DATA
Alarm	1	Lift ID	

Call Type	Call Type	ID	DATA
Alarm 2	1	Lift ID	
Checking Call	3	Lift ID	
Rescue process ended	2	Lift ID	500
Button Error	2	Lift ID	800
Button Repair	2	Lift ID	801
Audio Error	2	Lift ID	200
Audio Repair	2	Lift ID	201

NOTICE
This is only a part of the data message. It does not contain the beginning, checksum and end.

287654321500 – Rescue process ended, identification number 87654321.

Functionality Tests in Accordance with EN 81-28

This subsection describes the procedures for verifying the functionality of the ALARM emergency signaling system in an elevator with **2N LiftIP 2.0** according to the EN 81-28 standard requirements. The tests must be carried out before the elevator is put in operation and periodically as a maintenance task.

Preparation

1. Open the web configuration interface of **2N LiftIP 2.0** .
2. Go to **Calling > Alarm Calls** and verify the following settings:
   - **Delayed Call** is enabled.
   - **Test Alarm** is enabled and the button press time for the test alarm activation is set to 30 seconds.
3. Go to **Services > Elevator** and verify the following settings:
   - **Rescue Mode** is enabled.
   - If **Terminate by Entering Password** is enabled, make a note of the password.

6.2.2 ALARM Emergency Signaling Information (4.1.2)

1. Press and hold the ALARM button with the bell symbol for the time required to trigger the test alarm (min. 30 seconds).

2. Check that the yellow LED lights up and the sound signal is heard.
3. When the call is connected to the rescue service, make sure the green LED starts flashing.
4. Verify the two-way communication with the rescue service.

6.2.3 ALARM Emergency Signaling End (4.1.3)

1. Follow the test steps for 6.2.2 ALARM Emergency Signaling Information (4.1.2) (p. 79).
2. Ask the rescue service to end the call.
3. Check that the green LED stops lighting when the call is ended. The yellow LED remains on.
4. Exit the rescue mode.

Exit with button 2

a. Press button 2 for 3 seconds.
   Button 2 is an external button plugged into the audio unit connector marked as ALARM 2; the location being determined by the installing company.

Exit by entering password

a. Call **2N LiftIP 2.0** – dial **2N LiftIP 2.0**.
b. Enter the rescue password and press an asterisk for confirmation.

5. Check that the yellow LED has gone off.

6.2.4 Emergency Power Supply (4.1.4)

The **2N LiftIP 2.0** audio units do not have an emergency power supplies of their own. Their operation during emergency power supply must be verified at the gateway/element providing emergency power to the emergency communication system.

6.2.5 Visual and Acoustic Signals in Elevator Cage (4.1.5)

For some audio units, the external LEDs are led out into the elevator cabin. The installing company is responsible for their placement. Check that the external LEDs are led into the elevator cabin.

Audio Unit	Connecting call	Active call	Active rescue mode	Rescue mode end
921618B, 2N LiftIP 2.0 COP unit – flush mounting, EN, with button	Yellow LED + sound signal	Yellow LED + green LED flashing	Yellow LED	No LED is on
921618 2N LiftIP 2.0 COP unit – flush mounting, without button	Yellow LED + sound signal	Yellow LED + green LED flashing	Yellow LED	No LED is on

6.2.6 Communication (4.1.8), ALARM Emergency Signaling Verification (4.1.6), Identification (4.1.7)

Communication Response

1. Make sure that the elevator door is not fully open.
2. Press the ALARM button with the bell symbol for the ALARM button press time (parameter 962).
3. Check that the yellow LED lights up and the sound signal is heard.
4. When the call is connected to the rescue service, make sure the green LED starts flashing.

5. Verify the two-way communication with the rescue service.

ALARM Verification and Restart

1. Make sure that the elevator door is not fully open.
2. Press the ALARM button with the bell symbol for the ALARM button press time (parameter 962).
3. Check that the yellow LED lights up and the sound signal is heard.
4. When the call is connected to the rescue service, make sure the green LED starts flashing.
5. Verify the two-way communication with the rescue service.
6. Ask the rescue service to end the call.
7. Check that the green LED stops lighting when the call is ended. The yellow LED remains on.
8. Press the ALARM button shortly.
9. Make sure that an audio signal sounds to indicate that the call is being connected. The system must establish connection immediately after the short press.
10. When the call is connected to the rescue service, make sure the green LED starts flashing.

It is necessary to verify on the receiving side that the device is correctly identified on the receiving device. The receiving device is not in the **2N LiftIP 2.0** portfolio.

Accessibility and Reliability (4.2.1)

The communication in the event of unavailability of the main receiving device and automatic test records (operational calls) need to be verified at the receiving device. The receiving device is not in the **2N LiftIP 2.0** portfolio.

Technical Parameters

Electric Parameters	
Supply voltage:	10–30 V DC (keep polarity) or 48 V PoE 802.3af
Consumption:	max. 2 W with integrated speaker, max. 3.5 W with 4 Ω impedance speaker

ALARM and CANCEL voltage range	
Inputs:	5–48 V DC (keep polarity)

Audio Parameters	
Speaker:	integrated 16 Ω / 1 W (0.45 W output power) Option to increase the output power to 0.75 W by connecting a speaker with 4 Ω impedance
Microphone:	integrated, option to connect an external electret microphone
Voice switching:	Full duplex audio processor
Induction loop output:	3.35 V RMS, 100 Ω output impedance
Codec:	PCMU, PCMA, G.711 (approx. 90 kbps), L16, G.722 and G.729

Connection of External Indicators	
Voltage:	10–30 V DC, external supply
Maximum current:	200 mA (100 mA if a bulb is used)

Other Parameters	
Dimensions:	65 (W) x 130 (H) x 23 (D) mm.
Range of operating temperatures:	−20 °C to 50 °C
Relative humidity:	10 to 90 % non-condensing
Recommended altitude:	0 – 2000 m

2N LiftIP 2.0 – User Manual

2N.com