2N LiftIP 2.0 User Manual

2N

1. 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.

Here is what you can find in this section:

> ⚠ **Caution**
>
> - This product, its installation and configuration are not intended for persons with physical, sensory or mental disabilities or persons with limited experience and skills unless expert supervision or relevant instructions are provided to them by a person responsible for their safety.

1.1 Product Description

Basic Features

2N® LiftIP 2.0 is an alarm lift communicator providing full-duplex audio transmission via the VoIP technology directly from the lift cabin. A microphone and a speaker are built-in behind the lift 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.
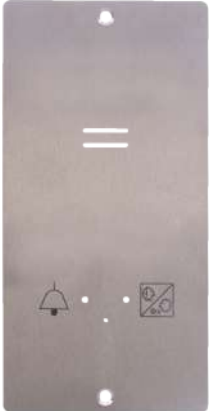
Advantages of Use:

- Basic announcement set playing
- Optimum acoustic properties
- Configuration via device web interface
- Adjustable speaker volume via audio unit buttons (during a call)
- Recording of up to 8-minute long announcements (10 user messages)
- Check call function once in 3 days (programmable)
- Function indication – two LEDs meeting the applicable lift 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 lift button panel
- Powerful indication options – illuminated pictograms (including bulbs)
- DTMF via RFC-2833, in-band or SIP INFO

1.2 Main Units and Accessories

Main Units in Universal Design		
These units are installed behind the lift panel, which is prepared for installation in advance.		
Part No.921640E		**2N® LiftIP 2.0 COP unit, EN** • Basic design
Part No. 921640XE		**2N® LiftIP 2.0 COP unit, EN, Cable version** • Basic design with cables • Includes 2 LEDs (green, yellow), microphone and speaker connected via cables.
Equipped with a separate stainless steel cover, this unit is designed for lift panel mounting.		
Part No. 921618BE		**2N® LiftIP 2.0 COP unit – Flush mounting, EN, With button** • Basic design with stainless steel cover • With button

Part No. 921618E		**2N® LiftIP 2.0 COP unit – Flush mounting, EN, Without button**
		• Basic design with stainless steel cover • Without button

Main Units in TOC Design
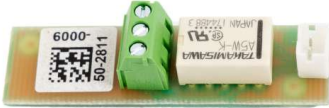
These units are designed for lift cabin mounting.

Part No. 921630E		**2N® LiftIP 2.0 TOC unit, EN**
		• Basic design with metal cover.

Part No. 921631E		**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.
Accessories		
Part No. 921661E		**2N® Voice Alarm Station** – Switch • **2N® LiftIP 2.0** audio unit interconnection switch

Accessories		8 /
Part No. 921661SET		**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

Associated 2N Products

Part No. 5024101E		**2N® LiftGate Main Unit, supports 2 CS, Aku+, EU plug** • Main Unit • Support of 2 Cabin switch units
Part No. 5024201E		**2N® LiftGate Main Unit, supports 4 CS, Accu+, EU plug** • Main Unit • Support of 4 Cabin switch units
Part No. 5024101US		**2N® LiftGate Main Unit, supports 2 CS, Accu+, US plug** • Main Unit • Support of 2 Cabin switch units
Part No. 5024201US		**2N® LiftGate Main Unit, supports 4 CS, Aku+, US plug** • Main Unit • Support of 4 Cabin switch units
Part No. 5024101AU		**2N® LiftGate Main Unit, supports 2 CS, Aku+, AU plug** • Main Unit • Support of 2 Cabin switch units
Part No. 5024201AU		**2N® LiftGate Main Unit, supports 4 CS, Aku+, AU plug** • Main Unit • Support of 4 Cabin switch units
Part No. 502460E		**2N® LiftGate Cabin Switch, 4x ETH, 12 V DC** • Cabin unit for connection of up to 4 IP devices in the lift cabin

Associated 2N Products

Part No. **22041572**		**GSM/UMTS/LTE 2N antenna** • SMA connector, 3 cable • 2.5 dB, for higher signal quality
Part No. **22041579**		**GSM/UMTS/LTE antenna** • SMA connector, 10m cable • 9 dB, for higher signal quality
Part No. **9137991**		**2N® Elevator Center device fee** • Cloud service license for bulk lift device administration

2. Description and Installation

This section describes the **2N**® **LiftIP 2.0** product and its installation.

Here is what you can find in this section:

2.1 Product Description

2N® **LiftIP 2.0** is an alarm lift communicator providing full-duplex audio transmission via the VoIP technology directly from the lift cabin. A microphone and a speaker are built-in behind the lift 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 pictogram goes on instantaneously. **Wait**, the pictogram goes on after communication is established: **Connection 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 lift 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 lift elements).

2.2 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

> ⚠ **Caution**
>
> - 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 adverse effects must be provided by the installing company if necessary.
- The communicator mounting surface must be perfectly flat, for details see Section 2.3 Montáž.

> ⚠ **Caution**
>
> - Installation and adjustment of this equipment, including any handling of this equipment, should only be carried out by persons qualified to do so.

> ✅ **Tip**
>
> - 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.

2.3 Mounting

Safety Precautions

> ⚠ **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.

Before You Start

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 location of the elements meets the standard requirements.

- 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

4 spotted M4 screws on panel/lift wall backside (typically, 2 mm stainless steel sheet)

Perforated speaker area

Here the perforation of the communicator front panel is shown. You can use perforation from the previous communicator installation but if the perforated area is substantially smaller or the count of holes is lower, the volume level can be affected negatively.

Two optional LED holes (Illuminated pictograms located off the panel are preferred to LEDs.)

Perforated microphone area

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 lift 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 the device operation. The current external microphone state is detected at the device start/restart only.

> ⚠ **Warning**
>
> - Make sure that the microphone hole is sealed against the noise that might get into the microphone through the gap between the cabin wall and the mounting panel. The microphone is supposed to receive sounds from the cabin only and not from the shaft or the **2N LiftIP 2.0** installation cavity!

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!

> ⚠ **Accident Risk**
>
> - 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).
>
>
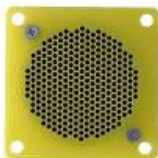
> ⚠ **Caution**
>
> - We do not recommend that the microphone and speaker are installed on completely different cabin sites (ceiling and wall, e.g.) as the users should find the speaker (grid/perforation) easily and then speak into the microphone near it.

> ⚠ **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 in front of 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.

Indicator Mounting

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

1. Illuminated pictograms 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).
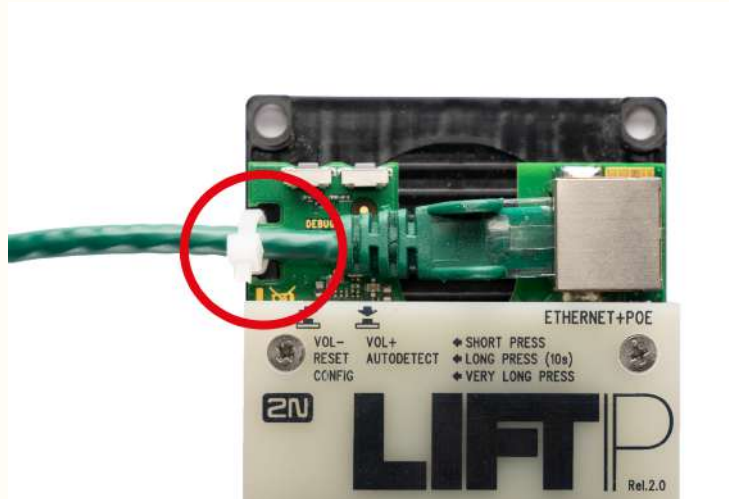
2.4 Connection

2N® LiftIP 2.0 Connection

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 2N® LiftIP 2.0 LAN Location via 2N® Network Scanner for more 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

> ⊘ **Accident Risk**
>
> - 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.

- Connect the button contacts to the ALARM terminal. The alarm is set as N/O (both jumpers mounted) from the factory.
- 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 4.5.2 Digital Inputs.
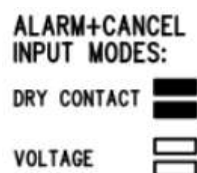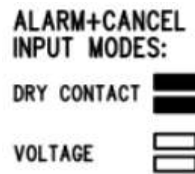

ALARM 1/2 Connection – Voltage Control

> ✓ **Tip**
>
> - DC voltage of 5–48 V can be used. Such source, however, must be backed up against power outage.

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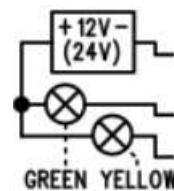

> ⊘ **Warning**
>
> - Keep polarity (see the cover print).

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 are supposed to work at power outage).
- 200 mA permanent current (even with bulbs).
- Make sure that both the indicators are connected!

> ⊘ **Warning**
>
> - Keep the power supply polarity!

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

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.
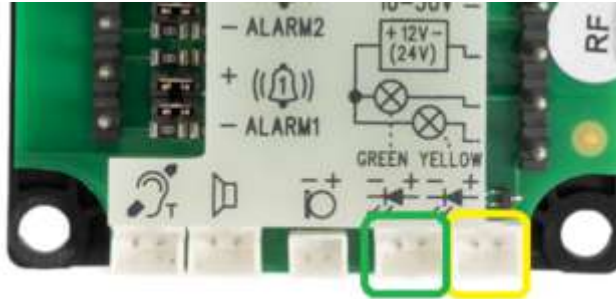
Requirements

- 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 lift doors are open and the people can leave the cabin.

Switch control

- Connect the switch to the CANCEL terminal.
- The **2N® LiftIP 2.0** is set to contact control from the factory. Both the jumpers are mounted on the configuration jumper.
- 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 4.5.2 Digital Inputs.
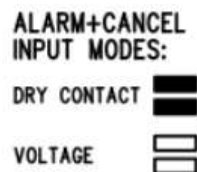
Voltage control

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

- Slide both the jumpers off the configuration jumper link for voltage control.
- To use voltage disconnection control, invert the CANCEL input function in the device web configuration, refer to 4.5.2 Digital Inputs.
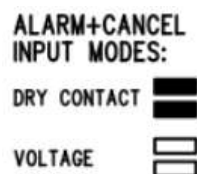
> ⚠ **Caution**
>
> - If voltage presence signals a **closed** door, make sure that the power supply is backed up against power outage.

> ◆ **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 that the induction loop is located behind a non-magnetic cover to avoid the induction loop field radiation worsening.
- Make sure that the induction loop is marked with an appropriate pictogram (ear) and its position meets the standard requirements.

2.5 Description of Terminals, Jumpers, Connectors and LEDs

Description of terminals and connectors	
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
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		
ETHERNET + POE	RJ-45 (PoE according to802.3af) LAN connector	
DC IN 10–30 V terminal	External power supply (unless PoE is available)	10–30 V DC
Indicator connecting terminals **+ 12 V (24 V)**	12–24 V DC / 2× 200 mA externally supplied indicators; keep the wiring diagram.	
"Connection establishing" LED connector	Yellow	The LEDs are not a standard part of the delivery (available only in cable versions). Once an external LED is connected, the on-board LED remains inactive.
"Connection established" LED connector	Green	
External **microphone** connector	The external microphone connection state does not change during the device operation. The current external microphone state is detected at the device start/restart only.	
Speaker connector	The speaker is connected in the standard delivery.	
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.*	

Description of terminals and connectors				
ALARM 1/2 terminal	Contact control	N/O contact (default)	Use the configuration jumpers for setting. **N/O contact**: both the jumpers are mounted.	ALARM+CANCEL INPUT MODES: DRY CONTACT VOLTAGE
		N/C contact	**N/C contact**: both the jumpers are mounted and input polarity is inverted in the software configuration in S. 4.4.2 Input Inversion.	
	Voltage control	Connect DC voltage of 5–48 V.	**Voltage connection** control: no jumper is mounted and input polarity is inverted in the software configuration in S. 4.4.2 Input Inversion.	
		Disconnect DC voltage of 5–48 V.	**Voltage disconnection** control: no jumper is mounted.	
RELAY connector		2N® LiftIP 2.0 Relay extender connector		
YELLOW EXTENDER (6-pin connector)		Used for 2N® Voice Alarm Station connection.		

Description of terminals and connectors				
CANCEL terminal	Contact control	N/O contact (default)	Use the configuration jumpers for setting. **N/O contact**: both the jumpers are mounted.	ALARM+CANCEL INPUT MODES: DRY CONTACT VOLTAGE
		N/C contact	**N/C contact**: both the jumpers are mounted and input polarity is inverted in the software configuration in Subs. 4.4.2 Input Inversion.	
	Voltage control	Connect DC voltage of 5–48 V.	**Voltage connection** control: no jumper is mounted and input polarity is inverted in the software configuration in S. 4.4.2 Input Inversion.	
		Disconnect DC voltage of 5–48 V.	**Voltage disconnection** control: no jumper is mounted.	

> ⬢ **Warning**
>
> - Keep polarity for voltage-controlled ALARM and CANCEL buttons (see the instructions on the cover).

> ⚠ **Caution**
>
> - Should there be an acoustic feedback between the microphone and the speaker (echo), turn down the speaker volume.

LED (front side – during call)

Color	Status	Function	Description
Yellow	Light on	Establishing call	Signals alarm call connecting process and rescue mode in progress if enabled.
Green	Light on	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	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		Relax	Signals the device relax state.

> ⓘ **Note**
>
> - The LEDs are located on the **2N® LiftIP 2.0** audio unit front side.
> - External LEDs can be connected too (Establishing connection, Connection established).

2.6 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.

Current IP address retrieval

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

- Press and hold the RESET button.
- Wait until the red and green LEDs go on simultaneously on the device and the acoustic

  signal ♩ can be heard (approx. 30 s).
- Release the RESET button.
- The device announces the current IP address via the speaker automatically.
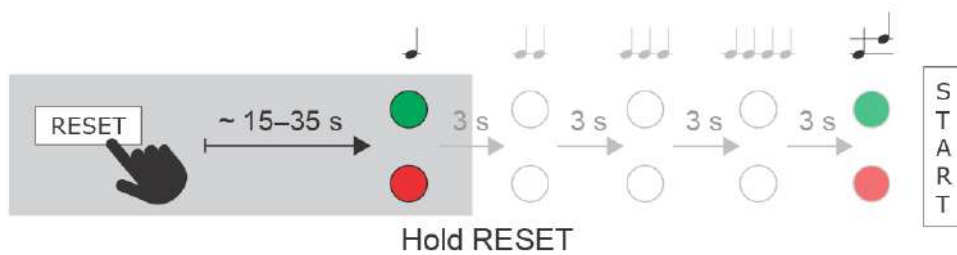
Hold RESET

> ⓘ **Note**
>
> - The time interval between the RESET press and the first light and acoustic signals is approx. 30 s.
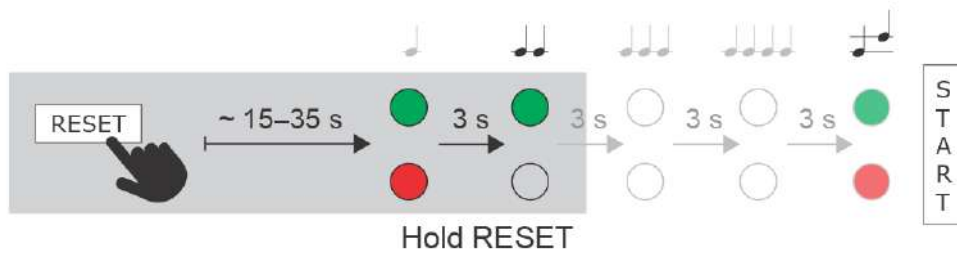
Static IP address setting

To switch on the **static IP address mode** (DHCP OFF), follow the instructions below:

- Press and hold the RESET button.
- Wait until the red and green LEDs go on simultaneously on the device and the acoustic

  signal ♩ can be heard (approx. 30 s).

- Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
- 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

Dynamic IP address setting

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

- Press and hold the RESET button.
- Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard (approx. 30 s).

- Wait until the red LED goes off and the acoustic signal can be heard (approx. for another 3 s).
- 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).
- Release the RESET button.
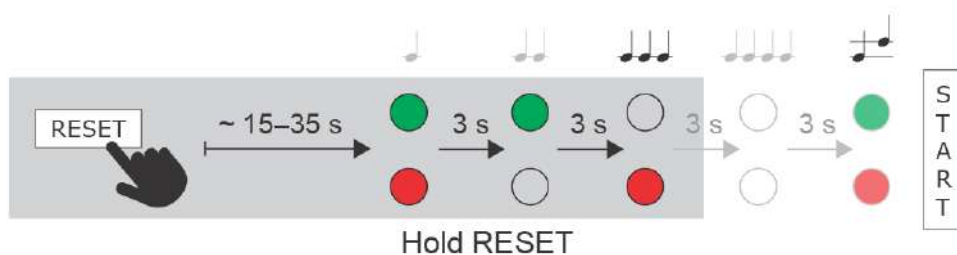
Factory reset

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

- Press and hold the RESET button.
- Wait until the red and green LEDs go on simultaneously and the acoustic signal can be heard (approx. 30 s).

- Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
- 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).
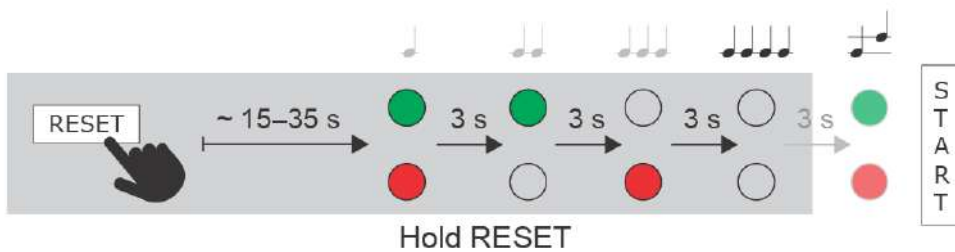- Wait until the red LED goes off and the acoustic signal can be heard ♩♩♩♩ (approx. for another 3 s).
- Release the RESET button.

Hold RESET

2.7 2N® Voice Alarm Station

Description

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.
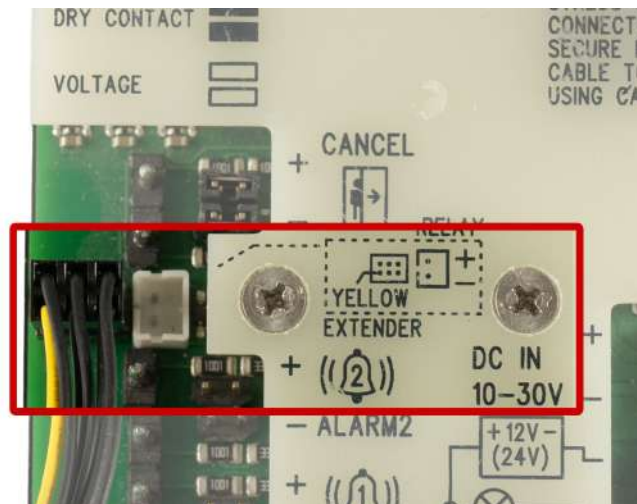
Dimensions

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

Switch: 81 x 81 x 30 mm

Mounting

To install 2N Voice Alarm Station, disconnect **2N LiftIP 2.0** from the power supply (DC 10–30 V or PoE). 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**
>
> - To install 2N Voice Alarm Station, disconnect **2N LiftIP 2.0** from the power supply (DC 10–30 V or PoE).
> - Make sure that all the connector pins are mounted properly.
> - Keep the correct EXTENDER connector wiring (yellow wire).
> - An incorrect connection can damage the module.

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.

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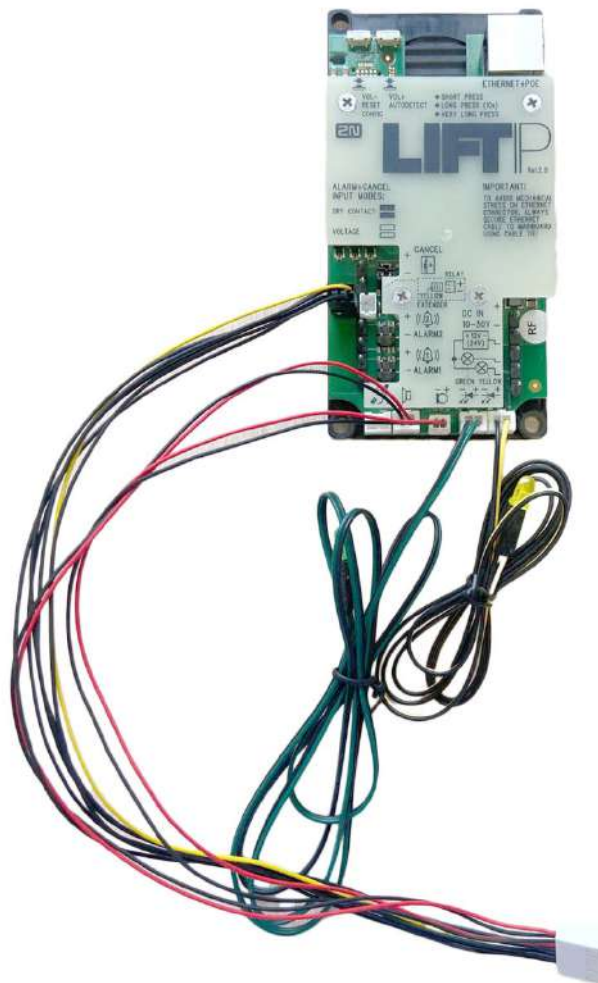
Remove the switch cover. Slide the interconnecting cable plug onto the 10-pin switch connector to interconnect the switch and **2N LiftIP 2.0**.

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 MIC for the microphone.

> ⚠ **Caution**
>
> 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.

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.

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

Enter the 2N LiftIP 2.0 IP address into your Internet browser and complete the username **Admin** and password **2N**, if these default login data have not been changed, to log into the web configuration interface. You can also retrieve the IP address using the 2N Network Scanner, which helps you locate all the 2N IP devices in the LAN and can be downloaded freely at 2n.com.

Upon login, complete the destination and user phone number for Alarm call 2 (Calls > Alarm calls > Alarm call 2) for proper routing. Also, set the count of call cycles in case the call is not confirmed.

> ❗ **Warning**
>
> If the Alarm call 2 destination is empty, no call can be set up.

> ✅ **Tip**
>
> - Procedure for logging into the 2N LiftIP 2.0 web configuration interface
> - The Alarm call 2 events are written into the State > Events configuration menu.

> ⓘ **Note**
>
> It is possible to have the same user set as for the ALARM1 button.

Operation

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

> ⚠️ **Caution**
>
> 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.

2.8 2N® LiftIP 2.0 Relay Extender

Description

The 2N® LiftIP 2.0 Relay extender extends **2N® LiftIP 2.0** to include one additional output. The relay output type makes it posible 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 is set for the Alarm button).
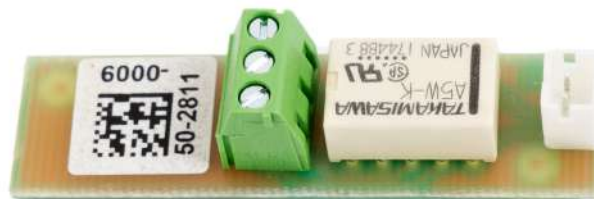
Wiring Diagram

The 2N® LiftIP 2.0 Relay extender is connected into the RELAY connector (see 2.5 Description of LEDs, Terminals, Jumpers and Connectors).

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

> ⚠️ **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.
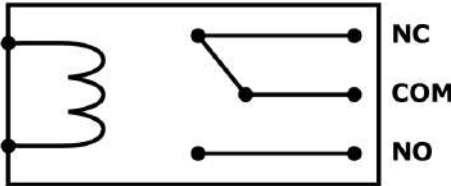
> ❗ **Warning**
>
> - Disconnect **2N® LiftIP 2.0** from the power supply (10–30 V DC or PoE) while connecting 2N® LiftIP 2.0 Relay extender.
> - To protect the circuits against short circuit with other conductive objects, **put** 2N® LiftIP 2.0 Relay extender **into an insulation tube and secure it with cable ties before installation!**
>
>
>
> - Keep the proper connection (yellow wire).
> - A wrong connection may damage the module.

Technical Parameters

Output	
Maximum switching power	15 W
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.

3. 2N LiftIP 2.0 LAN Location via 2N Network Scanner

Configure **2N LiftIP 2.0** via the administration web server. Connect **2N LiftIP 2.0** to the LAN using a UTP cable and make sure that the device is being fed.

2NNetwork Scanner Description

The application is used for retrieving the IP addresses of all the 2N IP devices in the LAN. The application is freely downloadable from the 2N web (www.2n.com). Make sure that Microsoft .NET Framework 2.0 is installed for successful app installation.
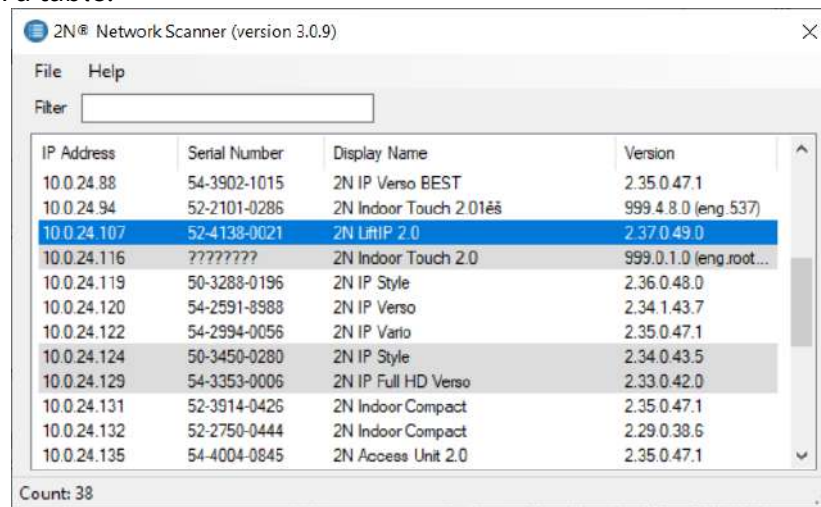
1. Run the**2N Network Scanner** installer.
2. The Installation Wizard will help you with the installation.
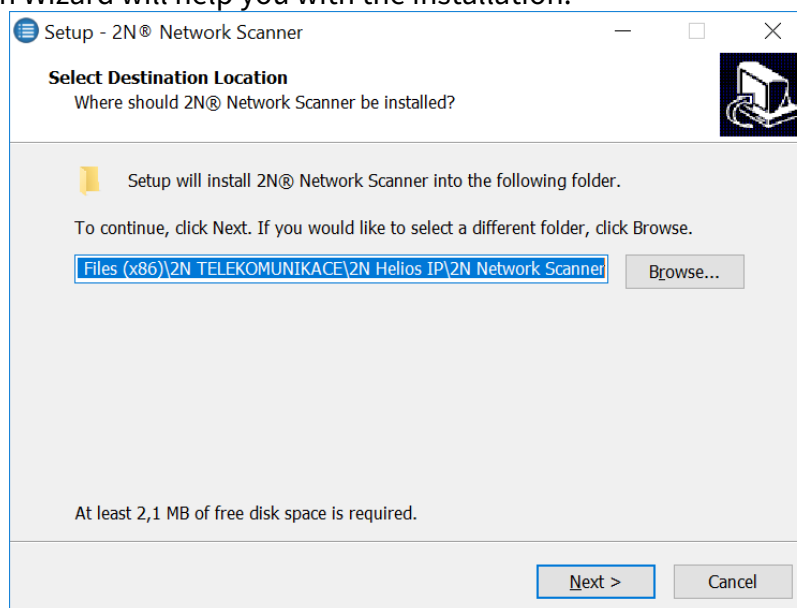
2NNetwork Scanner Installation Wizard

3. Having installed **2N Network Scanner**, start the application using the Microsoft Windows Start menu.

4. Upon launch, the application starts search the LAN for all the 2N devices and their smart extensions whose IP addresses are assigned by DHCP or statically set. These devices are then shown in a table.
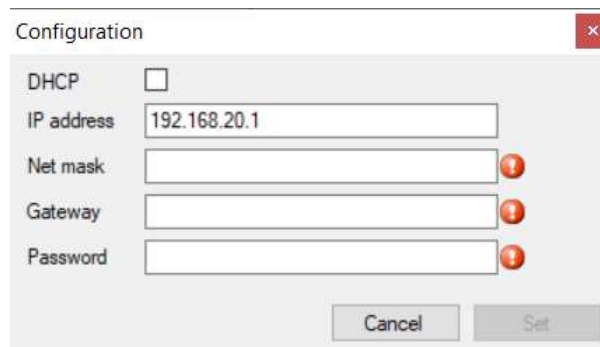

2N Network Scanner Window

5. Choose the **2N LiftIP 2.0** device to be configured from the list and click it with the right-hand mouse button. Select *Browse...* to open the **2N LiftIP 2.0** web administration interface login window for configuration. To change the device IP address, select *Config* and enter the required static IP address or activate DHCP. Enter a password to confirm the setting change. If the default password has been changed (upon the web interface login), use the current password. If not, the default password is **2n**. If the found device is grey highlighted, its IP address cannot be configured using this application. In that case, click Refresh to find the device again and check whether multicast is enabled in your network.

Change of Device IP Address in **2N Network Scanner**

4. Configuration

Typically, configuration takes place via a web interface of the device. Alternatively, configuration can take place via My2N.

2N® **LiftIP 2.0** is configured using a PC equipped with any Internet browser:

- Launch your Internet browser (Chrome, Firefox, Internet Explorer, etc.).
- Enter the IP address of your intercom (http://192.168.1.100/, e.g.).
- Log in using the username **Admin** and password **2n**.

You need to know the device IP address and domain name to get access. Make sure that the device is connected to the local IP network and properly powered. Upon purchase, **2N**® **LiftIP 2.0** is set to the dynamic IP address mode – it retrieves the IP address automatically if there is a properly configured DHCP server in the LAN. If the DHCP server is unavailable, **2N**® **Lift IP 2.0** can be operated in the static IP address mode.

Domain Name

Enter the domain name as *hostname.local* (e.g. 2NILiftIP20-00000001.local) to connect to the device. The new device Hostname consists of the device name and serial number. See below for the device name formats in Hostname. The serial number is entered without hyphens. You can change Hostname in System > Network later.

2N Device	Device Name in Hostname
2N LiftIP 2.0	2NILiftIP2

Login based on a domain name is advantageous if the dynamic IP address is used. While the dynamic IP address changes, the domain name remains the same. It is possible to generate certificates signed by a trusted certification authority for the domain name.

Start Screen

The start screen is an introductory overview screen displayed upon login to the device web interface. Use the button ⬅ in the left-hand upper corner on each of the following web interface pages to return to this screen anytime. The screen header includes the device name (refer to the Display Name parameter in the **Services / Phone / SIP menu**). Use the menu in the right-hand upper corner of the web interface for selecting the 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.

The Start Screen is the first menu level and provides quick navigation (click any tile) into selected parts of the device configuration. Some tiles also display the state of selected services.

Configuration Menu

The **2N® LiftIP 2.0** configuration is divided into 5 main menus – **State**, **Directory**, **Calling**, **Services**, **Hardware** and **System** – and their submenus, refer to the list below.

State

- **Lift** – display basic information on the lift / lift communicator and its error states.
- **Device** – display basic information on **2N® LiftIP 2.0**.
- **Services** – display the states of the network interface and selected services.
- **Events** – display the last 500 events recorded by the device.

Directory

- **Users** – set the directory destination phone numbers.

Calling

- **General Settings** – incoming and outgoing call settings
- **SIP 1** – SIP terminal settings
- **SIP 2** – SIP terminal settings
- **Alarm Call** – set the alarm call.
- **Checking Call** – set the checking call.
- **Notifications** – set the event notifications.

Services

- **Lift** – set the lift identification.
- **Phone** – set the phone and SIP connection.
- **User Sounds** – set and record user sounds.
- **Rescue Mode** – set the rescue mode.
- **Alarm Call** – set the alarm call.
- **Checking Call** – set the checking call.
- **Notifications** – set the event notifications.
- **Web Server** – set the web server and access password.
- **Audio Test** – set the automatic audio test.

Hardware

- **Audio** – set the audio, signaling, etc. volume control, microphone parameters
- **Input Polarity** – set the button and input polarities.
- **External Camera** – set the external IP camera.

System

- **Network** – set the LAN connection, 802.1x, packet capturing
- **Date and Time** – set the real time and time zone.
- **License** – set the licenses, activate the trial license.
- **Certificates** – set the certificates and private keys.
- **Update** – set the automatic firmware and configuration updates.
- **Syslog** – set syslog message sending.

- **Maintenance** – set the backup and configuration reset, firmware update.

4.1 State

Here is what you can find in this section:

4.1.1 Lift

The **Lift folder** provides lift / lift communicator identification, shows the checking call / rescue mode state and displays possible error states.

Lift State ⌄

Lift ID 123456
Last Successful Checking Call N/A
Next Checking Call 03/28/2023 20:30
Rescue Mode No
Blocking Relay Active Yes
External Microphone No
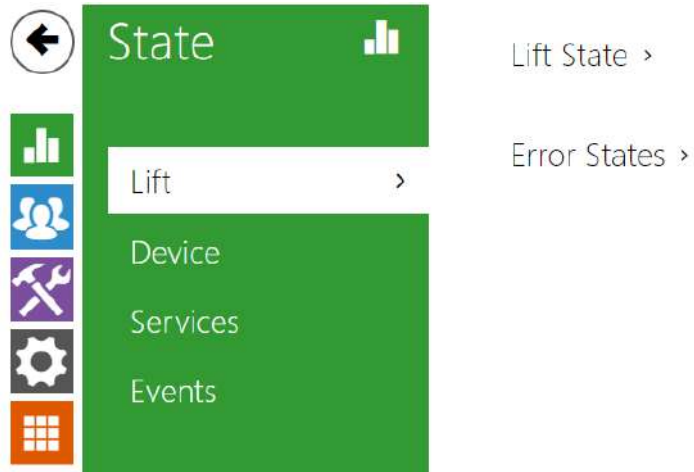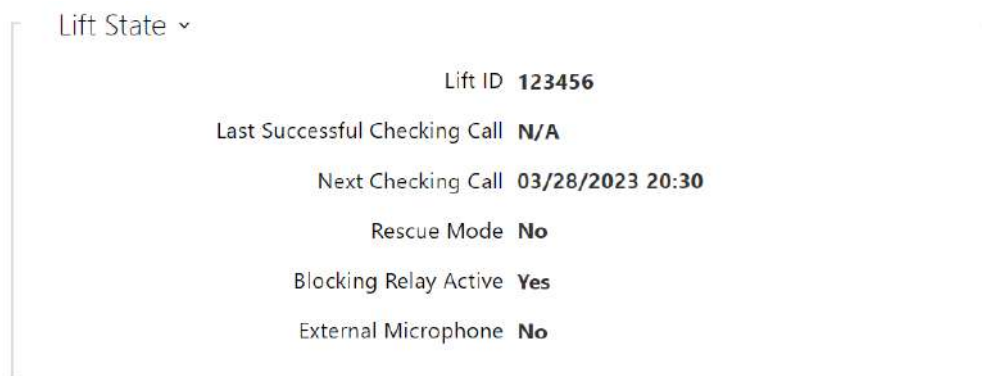
- **Lift ID** – display the lift / lift communicator ID to be sent or read in calls. The identification number has to consist of 16 digits at most.
- **Last Successful Checking Call** – display the last successful checking call time.
- **Next Checking Call** – display the next periodical checking call date and time.
- **Rescue Mode** – display whether the rescue mode is active.
- **Blocking Relay Active** – display the relay output state when the parameter is active in the case of SIP registration / configuration error. When any of the error occurs, the lift will be blocked.
- **External Microphone** – display the external microphone connection to the device.

> ⚠ **Caution**
>
> - The external microphone connection state does not change during the device operation. The current external microphone state is detected at the device start/ restart only.

Error States ⌄

SIP Registration Error No
Configuration Error No
Audio Error No
ALARM1 Button Error No
Checking Call Error No
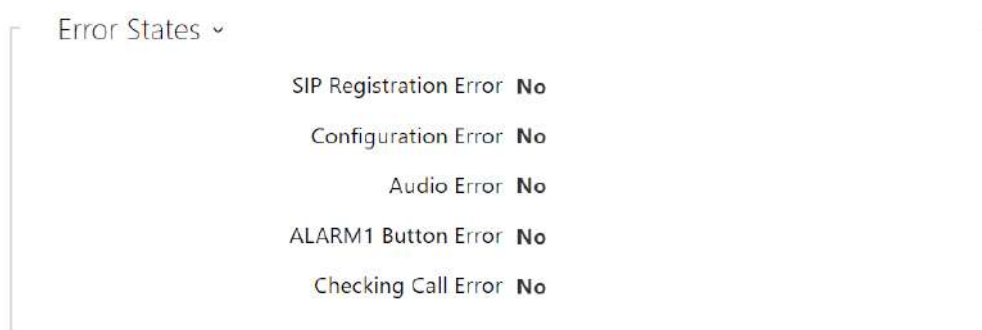
- **SIP Registration Error** – display whether or not there is a current SIP account registration problem.
- **Configuration Error** – find whether or not the device has a valid alarm call configuration (ALARM1).
- **Audio Error** – display whether or not the last audio test reported an audio error.
- **ALARM1 Error** – display the current ALARM1 button state.
- **Checking Call Error** – display whether or not the last checking call failed.

4.1.2 Device

The **Device folder** provides information on the model and its properties, firmware and bootloader versions, certificateetc.
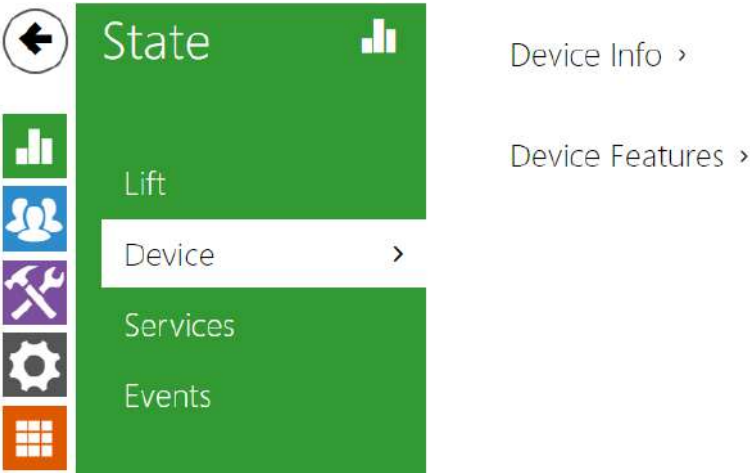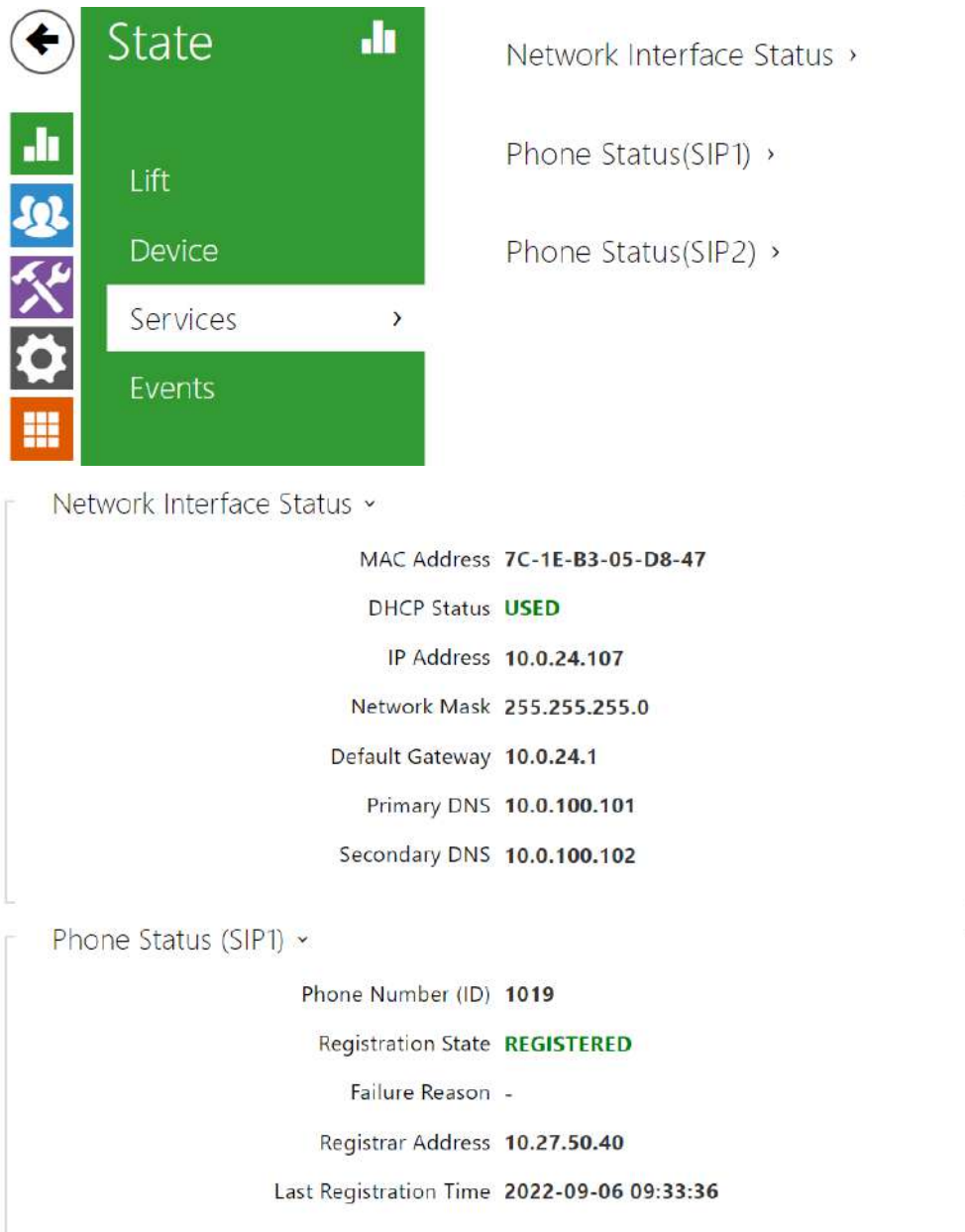

- **Factory Certificate Installed** – specification of the user certificate and private key used for verification of the device authorization to communicate with the third party server.

- **Locate Device** – optical and acoustical device signaling. Optical signaling includes pictogram indicators, acoustic signaling is based on a connected speaker.
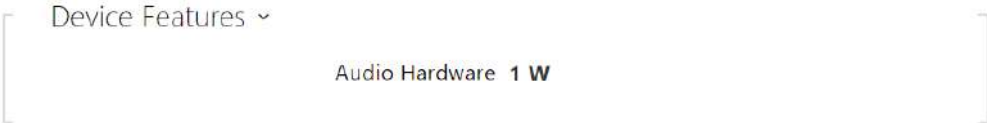
- **Audio Hardware** – display the connected speaker power output.

4.1.3 Services

The Services folder provides information on the network interface state and selected services.

4.1.4 Call Log

The Call Log folder shows a list of all accomplished calls. Every call includes information on its time and date, duration and status (incoming, outgoing and missed).
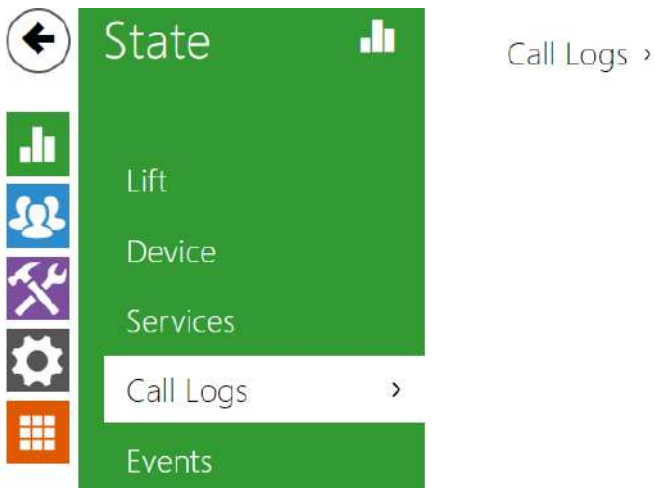
The search field provides fulltext search in call names. The checkbox helps you select all the records to be bulk deleted. Click the 🗑 button to delete a selected call record individually. The list includes the last 20 records.

4.1.5 Events

The Events folder displays the last 500 events recorded by the device. Every event includes the capturing time and date, event type and a detailed description. Use the pop-up menu above the event record to filter the events by the type.
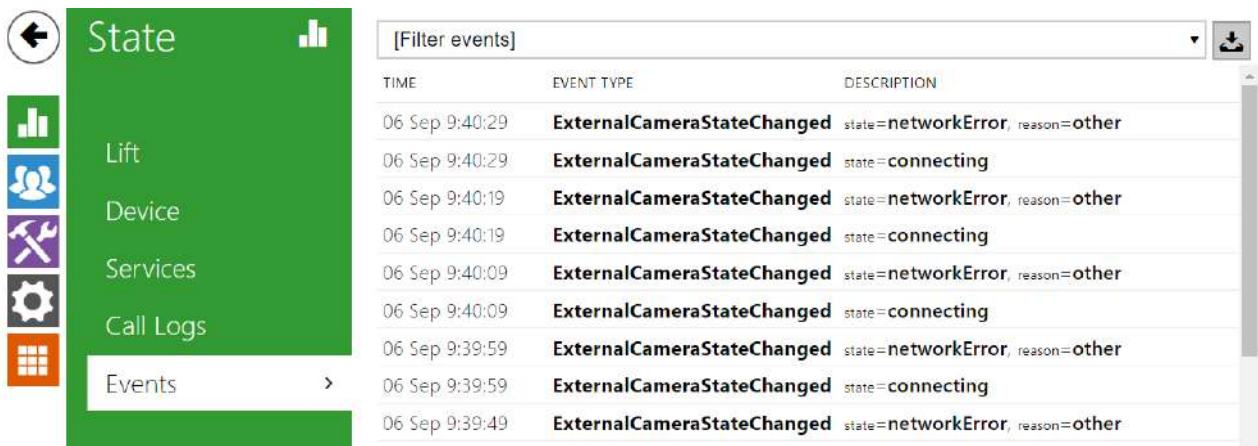
- ⬇ – the button helps you export all the logged events into a CSV file.

Event	Meaning
AudioLoopTest	Audio test result.
CallSessionStateChanged	Provides information on the current call phase (creation, connecting, ringing, connected, terminated).
CallStateChanged	Indicates a call state change (ringing, connected, terminated) including call direction (incoming, outgoing) and counterparty identification.
CapabilitiesChanged	Change of the list of available functions.
ConfigurationChanged	Device configuration change.
DeviceState	Device state indication, e.g. device booting.
DirectoryChanged	Change in the directory.
DirectorySaved	Change saved in the directory.
DtmfEntered	DTMF code received during a call.
ErrorStateChanged	Device error state.
ExternalCameraStateChanged	External IP camera state.
HardwareChanged	Change of extending module connection.
CheckingCall	Checking call state.

Event	Meaning
InputChanged	Logic input change.
KeyPressed	Key pressing event.
KeyReleased	Key releasing event.
LoginBlocked	Entering of 3 wrong logins to the device web. Contains information on the login IP address.
OutputChanged	Logic output change.
RegistrationStateChanged	Change of the SIP Proxy registration state.
RescueStateChange	Rescue mode state change.

4.2 Directory

Directory is one of the most essential parts of the **2N LiftIP 2.0** configuration.
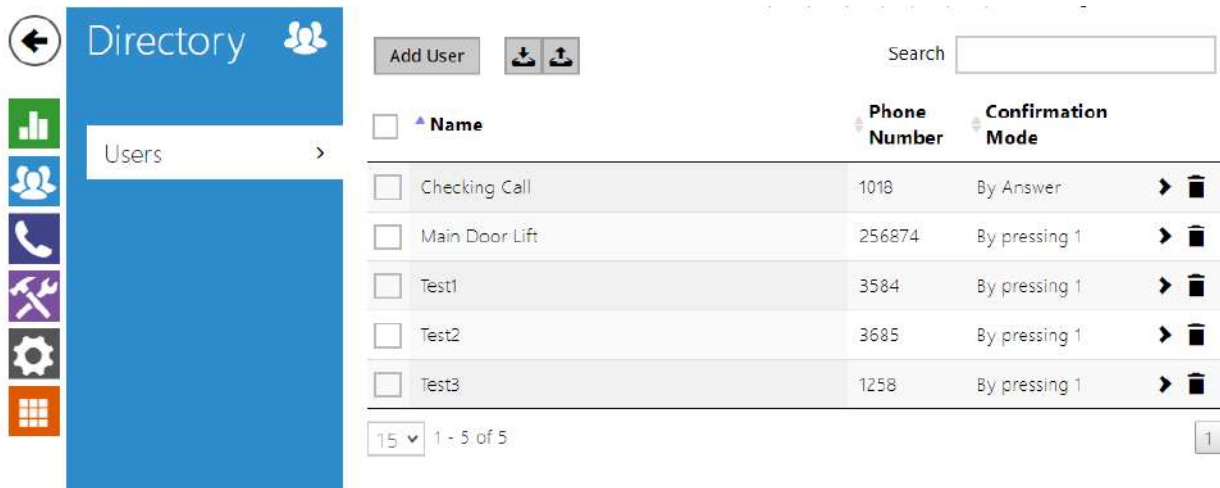
The Search function works as a fulltext search in names and phone numbers. It searches the directory for all matches. Press the button above the table to add a User. Click ![arrow] to show the user details. Press ![trash] to remove a user and delete its details. The user positions in the directory are alphabetically arranged.

Using the ![export]/![import] icon, it is possible to export/import from/into the device a CSV file including a user list. If the directory is empty, a file is exported with the header only (in English) to be used as a user importing template. If an empty file with the header only is imported and **Replace directory** is selected, the whole directory is deleted. Up to 10,000 users can be imported depending on the device type.

> ⚠ **Caution**
>
> - Special users such as those created by **My2N** or **2N Access Commander** are not part of the directory export.
> - While editing the CSV file using Microsoft Excel, remember to save the file in the CSV UTF-8 format (with separators).

Every record in the Users list includes the following parameters:

- **Name**– mandatory parameter for easier user search, for example.

Each user on the list can be assigned up to three phone numbers. An outgoing call is routed to all the numbers simultaneously. Once a 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] for the so-called direct SIP calling, e.g.: sip:200@192.168.22.15 or sip:name@yourcompany. Enter device:device ID for local calls to 2N IP devices and answering units. Set the device name for the relevant devices. Enter RAVA:device_name to make Crestron calls. If you enter **/1** or **/2** after the phone number, SIP account 1 or 2, respectively, will be used for outgoing calls explicitly. Enter /**S** or /**N** to force an encrypted or unencrypted call respectively. Combine account selection, encryption and Callback door opening as e.g. /1S, etc. The parameter may include up to 255 characters.

Click to edit the phone number details.

- **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. Further settings include direct SIP calls (sip:), 2N local calls (device:), Crestron calls (rava:) 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.
- **Door Opening** – via callbacks.

- **Confirmation Mode** – select the confirmation mode to set up a call.
    - By pressing 1
    - By Answer
    - Protocol Autodetection
    - CPC Antenna
    - CPC Antenna Ext
    - CPC KONE
    - P100

4.3 Calling

Calling is the basic function of **2N® LiftIP 2.0** allowing you to establish connections with other IP network terminals. The device supports the extended SIP and is compatible with major SIP PBX and terminal equipment manufacturers.

2N® LiftIP 2.0 uses the following protocols for audio stream encoding (or compression): **G.711**, **L16**, **G.722** and **G.729**.

Explanation of IP Telephony Terms

- **SIP (Session Initiation Protocol)** – a phone call signaling transmission protocol used in IP telephony. It is primarily used for setting up, terminating and forwarding calls between two SIP devices (the device and another IP phone in this case). SIP devices can establish connections directly with each other (Direct SIP Call) or, typically, via one or more servers: SIP Proxy and SIP Registrar.
- **SIP Proxy** – an IP network server responsible for call routing (call transfer to another entity closer to the destination). There can be one or more SIP Proxy units between the users.
- **SIP Registrar** – an IP network server responsible for user registration in a certain network section. As a rule, SIP device registration is necessary for a user to be accessible to the others on a certain phone number. SIP Registrar and SIP Proxy are often installed on one and the same server.
- **RTP (Real-Time Transport Protocol)** – a protocol defining the standard packet format for audio/video transmission via IP networks. The device uses this protocol for audio and video stream transmissions during a call. The stream parameters (port numbers, protocols and codecs) are defined and negotiated via the SDP (Session Description Protocol).

2N® LiftIP 2.0 supports three SIP signaling types:

- Using the **UDP**, which is the most common unsecured way of signaling,
- Using the **TCP**, which is a less widely used, yet recommended way of unsecured signaling;
- Using the **TLS** protocol, where SIP messages are secured against eavesdropping and modifications by third parties.

Here is what you can find in this section:

4.3.1 General Settings

General Settings ˅

Call Time Limit	120 [s]
Confirmation timeout	60 [s]

- **Call Time Limit** – set a timeout after which the call is automatically terminated. The device beeps into the call 10 s before the call end to signal the imminent call termination. Send any DTMF character into the call (e.g. press # on your IP phone) to extend the call. 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 you can confirm the call after setup. When the timeout expires, the device will call the next number. If Confirmation by pickup is selected, this parameter is irrelevant.

Incoming Calls ˅

Microphone Mode	Always enabled
Allow after alarm call to	1 [h]

- **Microphone Mode** – set that the device microphone shall be muted at incoming calls due to privacy.
- **Allow After Alarm Call to** – set how long the microphone shall stay unmuted after an alarm call (in case the Allowed after alarm call microphone mode is selected).

Outgoing Calls ˅

Connection Time Limit	32 [s]
Ring Time Limit	0 [s]

- **Connection 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 after 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.

4.3.2 SIP 1 / SIP 2

2N® LiftIP 2.0 enables you to configure two independent SIP accounts (SIP1 and SIP2 folders). Thus, the device can be registered under two phone numbers, with two different SIP exchanges and so on. Both the SIP accounts process incoming calls equivalently. Outgoing calls are primarily processed by account SIP 1, or, if account SIP 1 is not registered (due to SIP exchange error, e.g.), by account SIP 2. Select the account number for the phone numbers

2N LiftIP 2.0 User Manual

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 SIP 1, sip:1234@192.168.1.1 calls to sip uri via account SIP 2).

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

- **Display Name** – set the name to be displayed as CLIP on the called party's phone.
- **Phone Number (ID)** – set a device name (or another unique ID composed of characters and digits). Together with the domain, this number identifies the device uniquely in calls and registration.
- **Domain** – set the domain name of the service with which the device is registered. Typically, it matches the SIP Proxy / Registrar address.
- **Test Call** – display a dialog box to make a test call to a selected phone number, see below.

- **Authentication ID** – set an alternative user ID for device authentication.
- **Password** – set a password for device authentication. If your PBX requires no authentication, the parameter will not be applied.

- **Proxy Address** – set the SIP Proxy IP address or domain name.
- **Proxy Port** – set the SIP Proxy port. The device uses the default port according to the transport layer (5060 or 5061) or the port obtained from the DNS in case the parameter is empty or set to 0.
- **Backup Proxy Address** – set the backup SIP Proxy IP address or domain name. The address is used where the main Proxy fails to respond to requests.
- **Backup Proxy Port** – set the backup SIP Proxy port. The device uses the default port according to the transport layer (5060 or 5061) or the port obtained from the DNS in case the parameter is empty or set to 0.

- **Registration Enable** – enable registration with the set SIP Registrar.
- **Registrar Address** – set the SIP Registrar IP address or domain name.

- **Registrar Port** – set the SIP Registrar port. The device uses the default port according to the transport layer (5060 or 5061) or the port obtained from the DNS in case the parameter is empty or set to 0.
- **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. The device uses the default port according to the transport layer (5060 or 5061) or the port obtained from the DNS in case the parameter is empty or set to 0.
- **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 (Unregistered, 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	UDP
Lowest Allowed TLS Version	TLS 1.0
Verify Server Certificate	☐
Client Certificate	[Signed by device]
Local SIP Port	5060
PRACK Enabled	☐
REFER Enabled	☐
Send KeepAlive Packets	☐
IP Address Filter Enabled	☐
Receive Encrypted Calls Only (SRTP)	☐
Encrypted Outgoing Calls (SRTP)	☐
Use MKI in the SRTP Packets	☐
Do Not Play Incoming Early Media	☐
QoS DSCP Value	0
External IP Address	
Starting RTP Port	4900
RTP Timeout	60
Compatibility with Broadsoft Devices	☐
Rotate SRV Records	☐

- **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.
- **Verify Server Certificate** – verify the SIP server certificate against the CA certificates uploaded to the device.
- **Client Certificate** – specification of the client certificate and private key used for verification of the device authorization to communicate with the SIP server.
- **Local SIP Port** – set the local port to be used for SIP signaling. A change of this parameter will not be applied until the device is restarted. The default value is 5060.
- **PRACK Enabled** – enable the PRACK method (reliable confirmation of SIP messages with codes 101–199).
- **REFER Enabled** – enable call forwarding via the REFER method.
- **Send KeepAlive Packets** – set whether or not the device shall periodically request the state of the called station via SIP OPTIONS (to detect any station failure during a call) during calls.
- **IP Address Filter Enabled** – enable blocking of SIP packets 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.
- **Do Not Play Incoming Early Media** – disable playing of the incoming audio stream before the call is answered (early media), which is sent by some PBXs or other devices. A standard local ringtone will be played instead.
- **Use MKI in the 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.
- **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 Enable** – 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.
- **Starting RTP Port** – set the starting local RTP port in the range of 64 ports to be used for audio and video transmissions. The default value is 4900 (i.e. the used range is 4900–4963). The parameter is only set for account 1 but applies to both the SIP accounts.
- **RTP Timeout** – set the timeout for receiving audio stream RTP packet 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 is only set for account 1 but applies to both the SIP accounts.

- **Compatibility with Broadsoft Devices** – set compatibility with the Broadsoft PBXs. If, in this mode, the device receives re-invite from a PBX, it responds by repeating the last sent SDP with the currently used codecs instead of sending a complete offer.
- **Rotate SRV Records** – enable rotation of the SRV records 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

The chart helps you enable/disable the video codec H.264 offered for call setups and set its priority.

- **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.

There can be different extended codec settings for different device types.

- **H.264 Baseline Profile, Packetization Mode 1**
- **H.264 Baseline Profile, Packetization Mode 0**

- **H.264 Main Profile, Packetization Mode 1**
- **H.264 Main Profile, Packetization Mode 0**
- **H.264 Constrained Baseline Profile, Packetization Mode 1**
- **H.264 Constrained Baseline Profile, Packetization Mode 0**
    - **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 option.

Advanced SDP Settings ⌄

H.264 Payload Type (1)	123
H.264 Payload Type (2)	124
Use sendrecv Attribute for Video	☐

- **H.264 Payload Type (1)** – set the payload type for video codec H.264 (packetization mode 1). Set a value between 96 and 127 or 0 to disable this codec type.
- **H.264 Payload Type (2)** – set the payload type for video codec H.264 (packetization mode 2). Set a value between 96 and 127 or 0 to disable this codec type.
- **Use sendrecv Attribute for Video** – the setting used to be called Compatibility with Polycom phones. It helps ensure compatibility with some third party devices (Polycom/Cisco and others). With this mode enabled, the device sends sendrecv instead of sendonly in its SDP message in the video codec offer.

Audio

Audio Codecs ⌄

CODEC	ENABLED	PRIORITY
PCMU	✔	2
PCMA	✔	3
L16 / 16 kHz	☐	4
G.729	☐	5 (lowest)
G.722	✔	1 (highest)

This chart helps you enable/disable the audio codecs offered for call setups and set their priorities.

Sending DTMF helps you set the method of sending DTMF characters from the device. Check the opponent's DTMF receiving options and settings to make the function work properly.

- **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.

Receiving DTMF helps you set the method od receiving DTMF characters from the device. 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.

- **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. Enter the value as a decimal number. A change of this parameter will not be applied until the device is restarted.
- **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.

4.3.3 Alarm Call

You can store up to 4 phone numbers for alarm calls and the repetition period. **2N LiftIP 2.0** makes successive calls to the stored numbers, the repetition period is terminated automatically after a call is confirmed.

Once the alarm (emergency) call is connected, the device switches into the rescue mode.

Alarm Call

Basic Settings ˅

Press Time to Activate	100 [ms]
Delayed Call	✔
Call Delay	30 [s]

- **Press Time to Activate** – set the minimum pressing time for the ALARM1 button to initiate an alarm call.
- **Delayed Call** – set that the alarm call shall be delayed (the call establishing sound message is played in the cabin during the delay).
- **Call Delay** – set the alarm call delay (the call establishing sound message is played in the cabin during the delay). Do not set this parameter to a value lower than the Test Alarm's parameter Press Time to Activate.

Test Alarm ˅

Enable	✔
Press Time to Activate	30 [s]

- **Enable**– make it possible to initiate a test alarm call by a mere long press of the ALARM1 button.
- **Press Time to Activate** – set the pressing time for the ALARM1 button to initiate a test alarm call. Do not set this parameter to higher value than the parameter Call Delay.

- **1–4** – select the user to which the connection will be directed.
- **Repetition Count** – set the count of calling cycles if a call is not confirmed.

> ⚠ **Caution**
>
> - If the call is rejected by the called user, the user will be skipped in the next calling cycle.

- **Test ALARM Call** – display a dialog box to carry out an alarm call test to the destinations as defined. The whole cycle repeats as set until a call is confirmed.

Alarm Call 2

- **1** – select the user to which the connection will be directed.
- **Repetition Count** – set the count of calling cycles if a call is not confirmed.

- **Test ALARM2 Call** – display a dialog box to carry out an alarm call test to the destinations as defined. The whole cycle repeats as set until a call is confirmed.

> 🔴 **Warning**
>
> - Make sure that the ALARM2 call destination is completed in the web configuration (Services > Alarm Call > Alarm Call 2) to make a successful call. The same user can be set as in ALARM1.

4.3.4 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**. 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 the phone numbers of the users specified as checking call recipients are used. The default value of the checking call repetition period is 3 days.

- **Checking Call Allowed** – enable the checking calls.

- **Period** – the checking calls are repeated once in the defined count of days. The first checking call is made at a randomly selected time during the first 24 hours after the device startup.
- **Next Call** – display the next periodical checking call date and time.

> ⓘ **Note**
>
> - The periodical checking call cycle is initiated at a randomly selected time after the device startup, then the set intervals are kept.

- **1–2** – select the user to which the connection will be directed.
- **Repetition Count** – set the count of calling cycles if a call is not confirmed.

- **Test Checking Call** – display a dialog box to make a test call to the destinations as defined. The whole cycle repeats as set until a call is confirmed. The test does not affect the checking call period and repetition settings.

> ⚠ **Caution**
>
> - If there is an audio or button error, the checking call is not made despite an active date and time value of the checking call period. This means that no alarm call can be made and the control center cannot be contacted, and so an intervention of a lift service technician is required.
> - If the call routing destination is not completed, the checking call cannot be made even though the function is enabled.

4.3.5 Operational Call

> ⓘ **Note**
>
> - The Notifications block was cancelled in version 2.44.

Operational Call is used for automatic setup of an operational call if one of the preset events occurs. In this section, the destination is set to which the operational call will be routed. The call is set up via Automation, refer to 4.4.3. Automation. The operational call activates the **StartLiftCall** action with the CallType parameter = operational. The action is triggered whenever the event to which the action is linked occurs:

- **RescueTerminated** for operational call setup at rescue mode termination.
- **ErrorStateChanged** for operational call setup at button error/fixed or audio error/fixed. The errror state type is defined by the event parameters.

- **1–2** – select the user to which the connection will be directed.
- **Repetition Count** – set the count of calling cycles if a call is not confirmed.

4.4 Services

Here is what you can find in this section:

- 4.4.1 Lift
- 4.4.2 E-mail
- 4.4.3 Automation
- 4.4.4 HTTP API
- 4.4.5 User Sounds
- 4.4.6 Rescue Mode
- 4.4.7 Web Server
- 4.4.8 Audio Test

4.4.1 Lift

General Setting

The Lift folder displays the lift / lift communicator ID to be sent or read in calls. The identification number has to consist of 16 digits at most.

⚠ **Caution**

- The CPC protocol uses up to 16 digits for lift identification, P100 uses only 8 digits.

Cabin Monitoring

- **Monitoring Mode** – set the device monitoring mode. This changes the microphone behavior (mute) and indication of the monitoring mode by the device (the device signals that audio and video are unavailable from the cabin due to privacy protection). Monitoring can be Enabled permanently, Disabled permanently, Enabled during rescue or Enabled during and after an alarm call.
- **Allow After Alarm Call for** – set how long the microphone shall be off and the device shall signal that monitoring is disabled (cabin audio and video are unavailable due to privacy) after an alarm call. This is valid only if the monitoring mode is set to Enabled after alarm call.

4.4.5 User Sounds

User Sounds helps you set the audio messages in variable languages to be played during alarm calls.
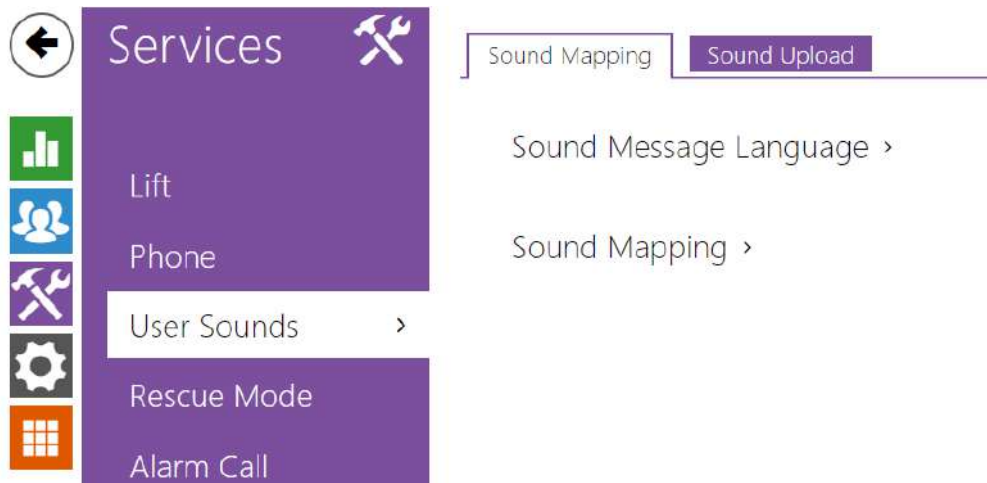
Sound Assignment

- **Language 1, 2, 3** – select a language for the device sound messages. If a file is mapped for the given event for which a translation is available, 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. You can select a combination of up to three sound messages in selected languages to be played consecutively.

> ✅ **Tip**
>
> - If the menu fails to offer a required language, you can create messages of your own in the Sound recording folder and assign them to the selected sound messages.

- **Establishing Connection** – connection establishing announcement.
- **Alarm Call** – alarm call announcement.
- **Checking Call** – checking call announcement.
- **Call Extension** – call termination and possible extension announcement.
- **Disconnection** – call termination announcement.
- **Call End** – call end announcement.
- **Rescue End** – rescue process end announcement.

> ⚠ **Caution**
>
> - If the assigned sound cannot be played, it is because the sound is set to Silence.

Sound Recording

You can upload up to 10 user sound files to the device. You can name each of them for better orientation.

Press to upload a sound file to the device. ⬆ Select a file from your PC in the dialog box and click **Upload**. Press ⊠ to remove a file. Press to play a recorded sound file (locally on your PC) ▶ . Press 🎤 to record a sound file directly via your PC microphone.

You can record a sound file using your PC microphone. Press the button ● to start the record. Press the button to stop ■ . Press the button to play the record ▶ . Press **Upload** to upload the sound into the device.
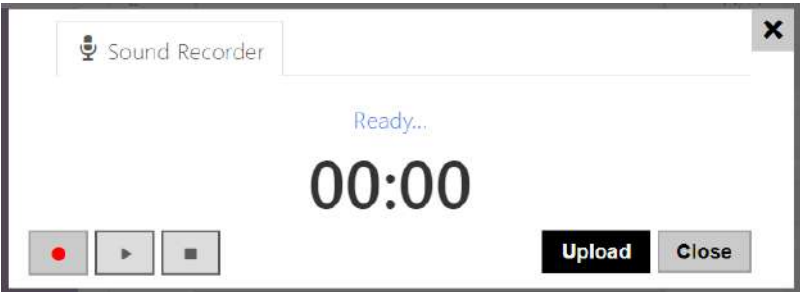
> ✅ **Tip**
>
> - Refer to https://wiki.2n.cz/hip/inte/latest/en/10-media-applications/audacity for how to create user sounds.

> ⓘ **Note**
>
> - The sound recording function is not available on browsers that fail to support the WebRTC standard.

4.4.6 Rescue Mode

The rescue mode is activated after the alarm call is connected. Set the rescue ending method too while enabling the rescue mode.
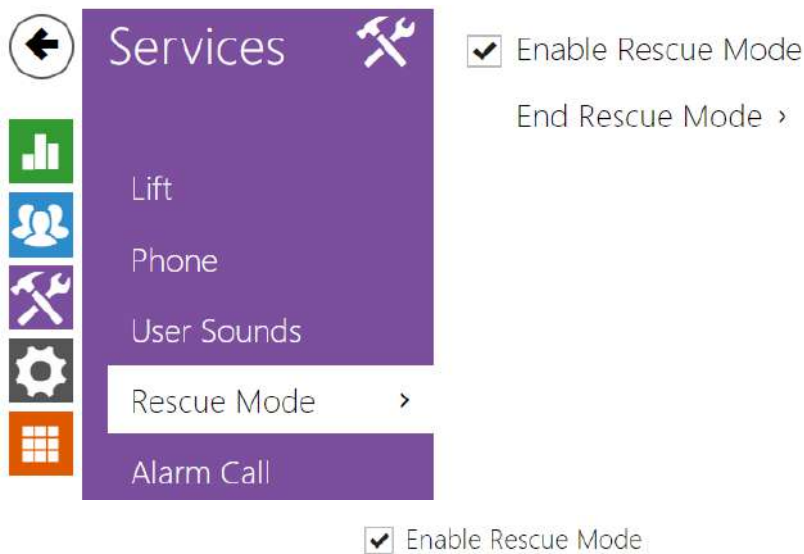
- **Enable Rescue Mode** – enable the rescue mode (if enabled, the rescue mode requires one of the rescue ending methods to be set).

- **By ALARM2 Button**– set that the rescue mode can be ended by pressing the ALARM2 button.
- **By Password** – set that the rescue mode can be ended using a password (sent to the device as DTMF in a call).
- **Password** – set the rescue ending password. The password is sent to the device as DTMF into a call and may contain digits only (up to 16).

4.4.7 Web Server

2N® **LiftIP 2.0** can be configured using a standard browser, which accesses the web server integrated in the PC. The HTTPS protocol is used for the browser - device communication. Enter the login user name and password first. The default login user name and password are **Admin** and **2n**. We recommend that you change the default password as soon as possible.
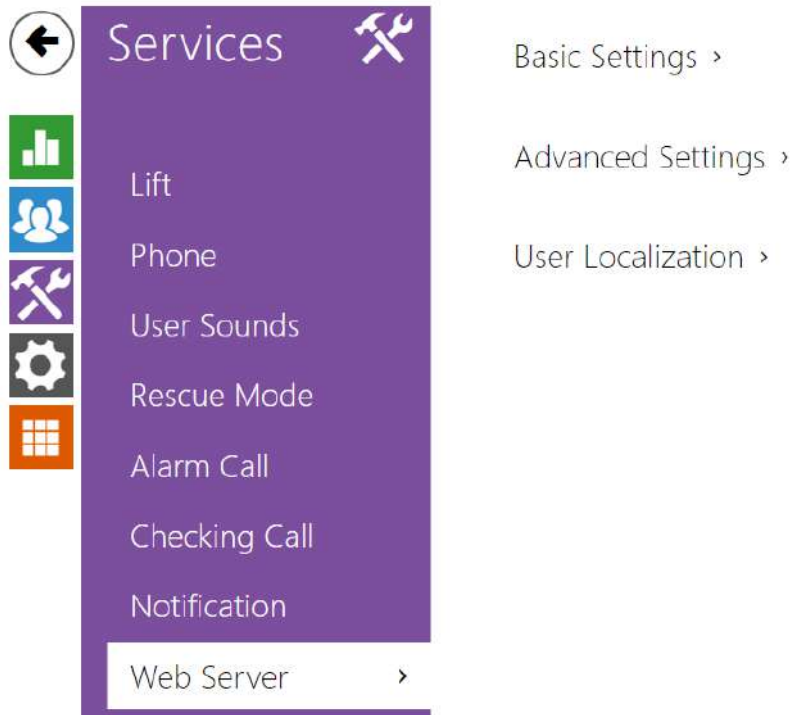
- **Device Name** – set the device name to be displayed in the right-hand upper corner of the web interface, in the login window and in other applications if necessary (Network Scanner, etc.)
- **Web Interface Language** – set the default language after the administration web server login. Use the upper toolbar buttons to change the web interface language temporarily any time.
- **Password** – set the device login password. Press ✎ 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.

- **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** – define the lowest TLS version to be connected to the devices.
- **HTTPS Server Certificate** – set the user certificate and private key to be used for communication encryption between the device HTTP server and the user web browser. Choose one of the three sets of user certificates and private keys (refer to the Certificates subs.) or keep the **Self Signed** setting, in which the certificate automatically generated upon the first device power up is used.
- **Remote Access Enabled** – enable remote access to the device web server from off-LAN IP addresses.

- **Original Language** – download the original file from the device including all user interface texts in English. The file format is XML; see below.
- **Custom Language** – upload, download and remove, if necessary, a user file containing your own user interface text translations.

```
<?xml version="1.0" encoding="UTF-8"?> <strings language="English" languageshort="EN">
 <!-- Global enums--> <s id="enum/error/1">Invalid value!</s> <s id="enum/bool_yesno/
0">NO</s> <s id="enum/bool_yesno/1">YES</s> <s id="enum/bool_user_state/0">ACTIVE</s>
<s id="enum/bool_user_state/1">INACTIVE</s> <s id="enum/bool_profile_state/
0">ACTIVE</s> <s id="enum/bool_profile_state/1">INACTIVE</s> .. .. .. </strings>
```

While translating, modify the value of **<s>** elements only. Do not modify the **id** values. The language name specified by the **language** attribute of the **<strings>** element will be available in the selections of the Web interface language parameter. The abbreviation of the language name specified by the **languageshort** attribute of the **<strings>** element will be included in the language list in the right-hand upper corner of the window and will be used for a quick language switching.

4.4.8 Audio Test

2N® LiftIP 2.0 allows you to perform a periodical check of the integrated speaker and microphone. For the test purpose, the integrated speaker generates one or more short beeps. The integrated microphone receives the generated tone and the test is successful if the tone is detected correctly. The test takes approximately 4 seconds. If the test fails (which may be due to an extreme surrounding noise level, e.g.), a new test is carried out in 10 minutes. Display the test result via the device confirmation interface.
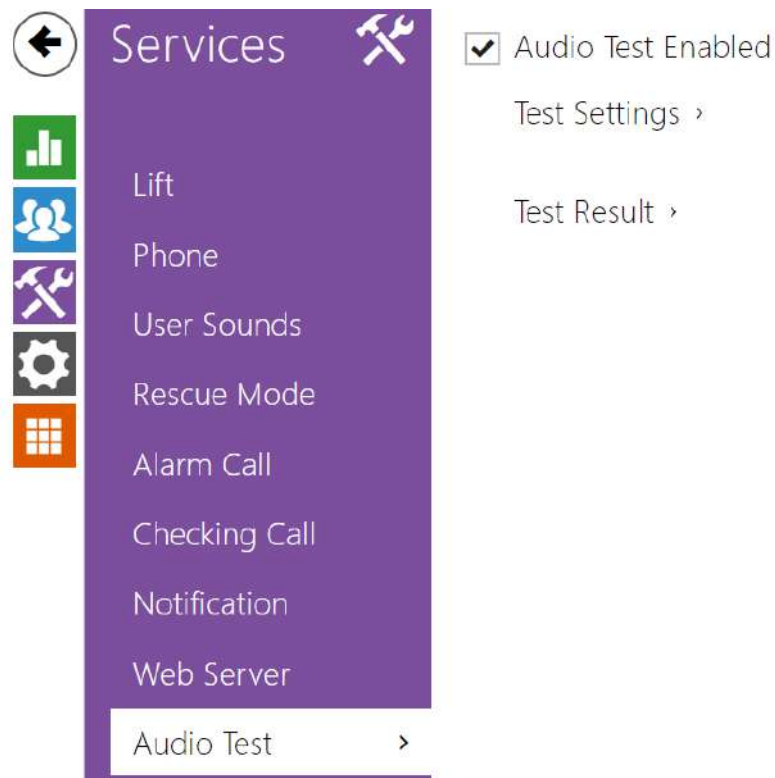
> **ⓘ Note**
>
> - *If a call is active during the audio test start, the audio test is postponed until the call is completed. The audio test will be performed the moment the call is completed.*

☑ Audio Test Enabled

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

Test Settings ⌄

| Test Period | Daily |
| Test Start Time | 14:07 |

Save and run test

- **Test Period** – set the test period. The test can be started automatically once a day or once a week.
- **Test Start Time** – set the test starting time. Use the HH:MM format. We recommend that test should start when a minimum device load is expected.
- **Save and run test**– push the button to start and save the test immediately regardless of the current settings.

Test Result ⌄

Test Status ---

Last Test Time 06/09/2022 14:07:05

Last Test Result **Passed**

- **Test Status** – display the current test status.
- **Last Test Time** – display the time of the last-performed test.
- **Last Test Result** – display the result of the last-performed test.

4.4.2 E-mail

This configuration interface menu helps you set e-mail transmissions via SMTP. The device allows you to execute e-mail sending via Automation, refer to 4.4.3. Automation.

☑ SMTP Service Enabled

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

SMTP Server Settings ⌄

Server Address
Server Port | 25
Security Type | SSL/TLS

- **Server Address** – set the SMTP server address to which e-mails shall be sent.
- **Server Port** – specify the SMTP server port. Modify the value only if the SMTP server setting is substandard. The typical SMTP port value is 25.
- **Security Type** – choose the security type for SMTP server communication. Refer to the documentation of the server for the type of security required by the server.

SMTP Server Login ⌄

Username
Password
Client Certificate | [Signed by device]

- **Username** – enter a valid username for login if the SMTP server requires authentication, or leave the field empty if not.
- **Password** – enter the SMTP server login password.
- **Client Certificate** – specify the client certificate and private key for the device – SMTP server communication encryption. Choose one of the three sets of user certificates and private keys (refer to the 3.5.3 Certifikáty) or keep the **SelfSigned** setting, in which the certificate automatically generated upon the first device power up is used.

Common Email Settings ⌄

From Address [   ]

- **From Address** – set the sender address for all outgoing e-mails from the device.

Advanced Settings ⌄

Deliver In [20 minutes   ▾]

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

E-Mail Sending Diagnostics ⌄

Test E-Mail Address [   ]   **Apply & Test**

Click **Apply & Test** to send a testing e-mail to the defined address with the aim to test the functionality of the current e-mail sending setting. Enter the destination e-mail address into the Test e-mail address field and press the button. The current e-mail sending state is continuously displayed in the window for you to detect an e-mail setting problem if any on the device or another network element.

4.4.3 Automation

> ✅ **Tip**
>
> Refer to the **Automation** Configuration Manual for the Automation function and configuration details.

The **2N LiftIP 2.0** provides highly flexible setting options to satisfy variable user needs. There are situations in which the standard configuration settings (switch or call modes, e.g.) are insufficient and so the device offers **Automation**, a special programmable interface for applications that require complex interconnections with third party systems.

Click the ✎ icon at the function to be created or changed to access the Automation interface.

4.4.4 HTTP API

HTTP API is an application interface designed for control of selected functions via the **HTTP**. It enables **2N LiftIP 2.0** to be integrated easily with third party products, such as home automation, security and monitoring systems, etc.
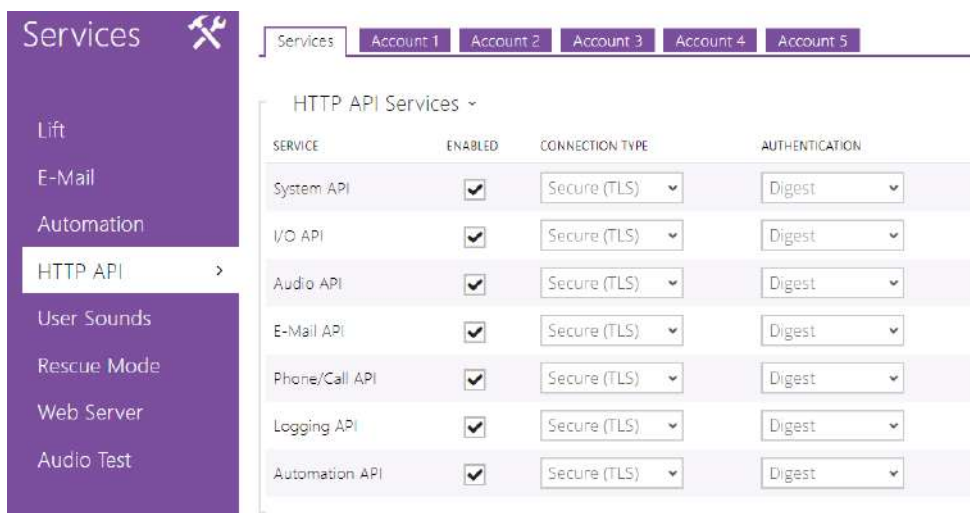
Services

HTTP API provides the following services:

- **System API** – provides device configuration changes, status info and upgrade.
- **I/O API** – provides device logic input/output control and monitoring.
- **Audio API** - provides audio playback control and microphone monitoring.
- **E-mail API** – provides sending of user e-mails.
- **Phone/Call API** – provides incoming/outgoing call control and monitoring.
- **Logging API** – provides reading of event records.
- **Automation API** – provides Secure/Unsecure communication settings and authorization requirements.

Set the transport protocol (**HTTP** or **HTTPS**) 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 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 unsecure 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 you to combine this option 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.

Refer to the HTTP API Configuration Manual for the HTTP API function and configuration details.

Account 1–5

The device allows you to manage up to five user accounts for access to the **HTTP API** services. The user account includes the user name and password and a list of user privileges to **HTTP API**.

☑ Account Enabled

- **Account Enabled** – enable this user account.

User Settings ˅

| Username | vms |
| Password | •••••••• |

- **Username** – enter the username fot the HTTP authentication.
- **Password** – enter the HTTP API authentication password.

User Privileges ˅

DESCRIPTION	MONITORING	CONTROL
System	☐	☐
Phone/Calls	☐	☐
Inputs and Outputs	☐	
Audio		☐
E-Mail		☐
Access to Automation		☐

You can manage the user account priviliges to the services via the table above.

4.5 Hardware

Here is what you can find in this section:

- 4.5.1 Audio
- 4.5.2 Digital Inputs
- 4.5.3 External Camera

4.5.1 Audio

You can set the call and signaling volumes for various device states in this part of configuration. The **Master Volume** parameter controls the overall volume of the device including calls,

signaling tones, etc. Consider the noise level of the ambient environment while setting this parameter.
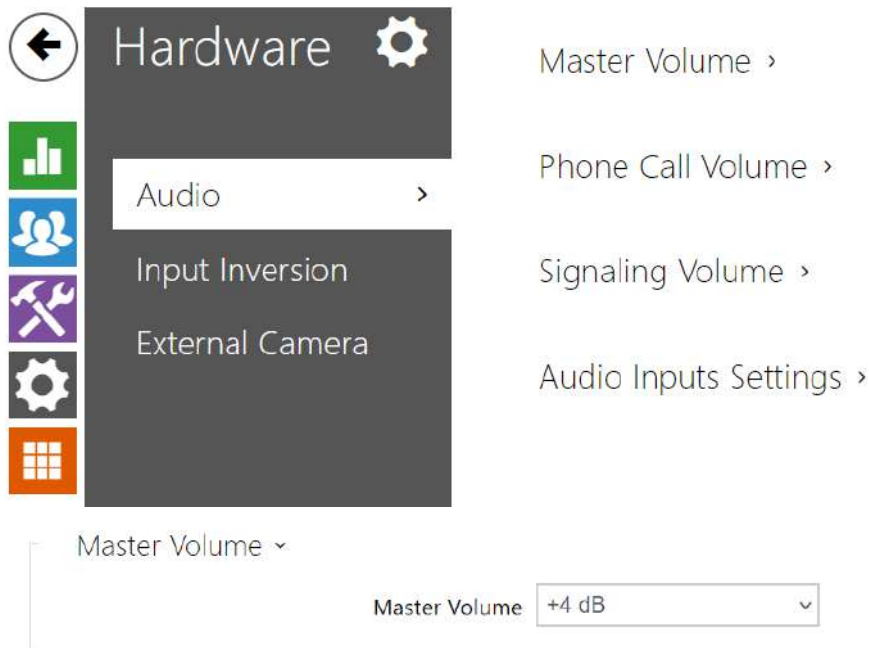
- **Master volume** – set the master volume based on the desired call volume, then adjust other sound volumes as needed. This setting affects the volume of all sounds.

> ✅ **Tip**
>
> - The master volume can be adjusted using the device buttons marked as VOL+/– too. Press the respective button once to turn up/down the volume.
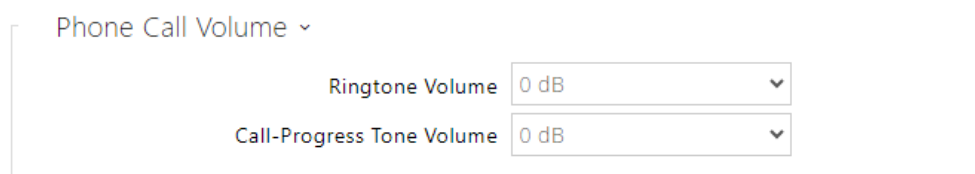
- **Ringtone volume** – set the volume of the incoming call ringtone. The value is relative to the master volume.
- **Call-progress tone volume** – set the volume for dial, ringing, and busy tones. This setting will not be applied if ringback tones are generated externally. The value is relative to the master 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** – the following operational statuses will not be signaled: Internal application started, IP address received and IP address lost.
- **User Sound Volume** – set the volume of user sounds played by automation. The value is relative to the master volume.

- **Microphone Input Gain** – set the microphone input gain.

4.5.2 Digital Inputs

Input Inversion enables you to set the input response to the pulse rising / falling edge (press / release the button).
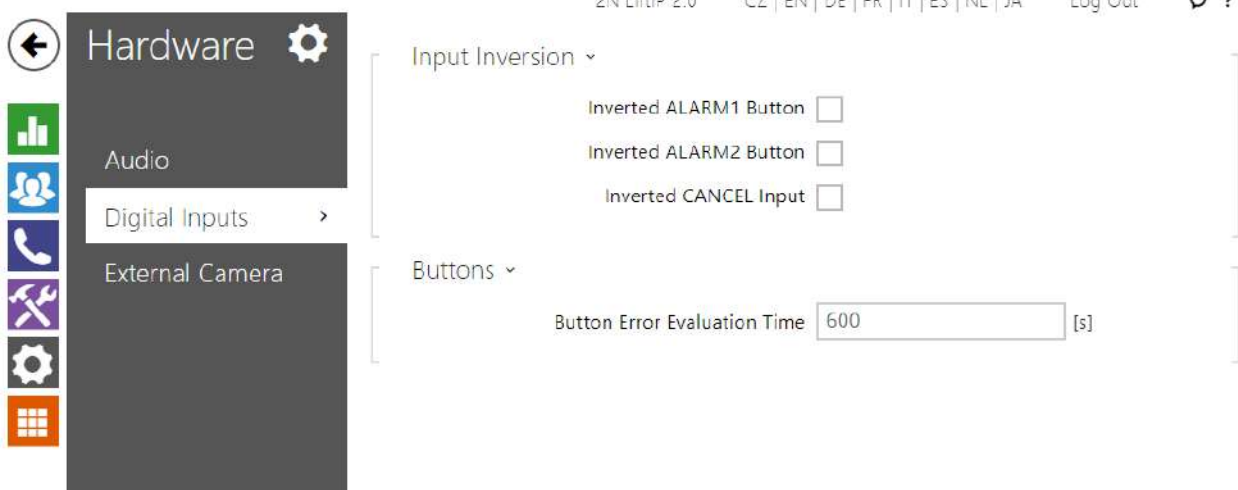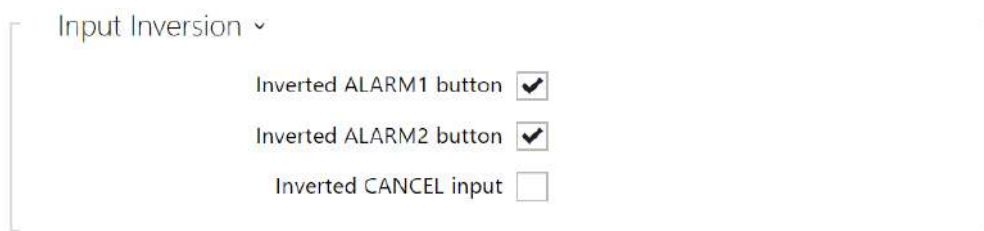
- **Inverted ALARM1 Button** – the inverted input is active when the contact is open or voltage is connected.
- **Inverted ALARM2 Button** – the inverted input is active when the contact is open or voltage is connected.
- **Inverted CANCEL Input** – the inverted input is active when the contact is open or voltage is connected.
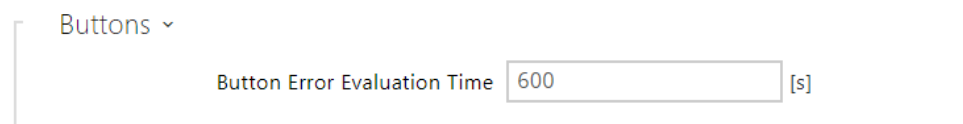
- **Button Error Evaluation Time** – set the timeout during which the ALARM1 button has to be activated before a button error is detected.

4.5.3 External Camera

2N® LiftIP 2.0 enables video to be transmitted during an alarm call from an external camera located in the lift cabin.
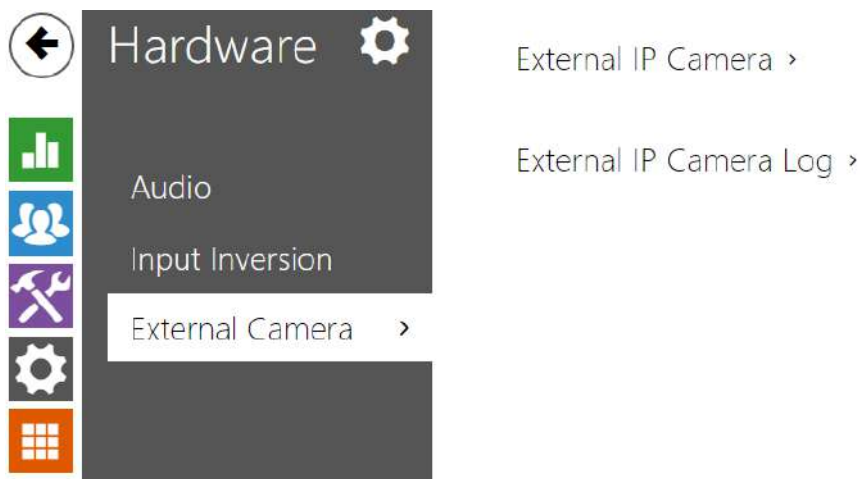
List of Parameters

- **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.
- **RTSP Stream Address** – enter the IP camera RTSP stream address:rtsp:// camera_ip_address/parameters . The parameters are specific for the selected IP camera model. If you use another 2N IP device as an external camera, use the following address: rtsp://ip_address/mjpeg_stream.
- **Username** – enter the username for the external IP camera connection authentication. The parameter is mandatory only if the external IP camera requires authentication.
- **Password** – enter the external IP camera connection authentication password. The parameter is mandatory only if the external IP camera requires authentication.
- **Local RTP Port** – local RTP port. Change the value according to your network configuration if necessary.

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

> ⚠ **Caution**
>
> - Make sure that the camera provides such video stream parameters that are expected from the device to which a call is made from 2N® Lift IP 2.0. If there are different video stream parameters, the video call may not work properly.

4.6 System

Here is what you can find in this section:

- 4.6.1 Network
- 4.6.2 Date and Time
- 4.6.3 Features
- 4.6.4 Certificates
- 4.6.5 Auto Provisioning
- 4.6.6 Diagnostics
- 4.6.7 Maintenance

4.6.1 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 to work properly. Configure the IP address and DHCP in the Network folder.
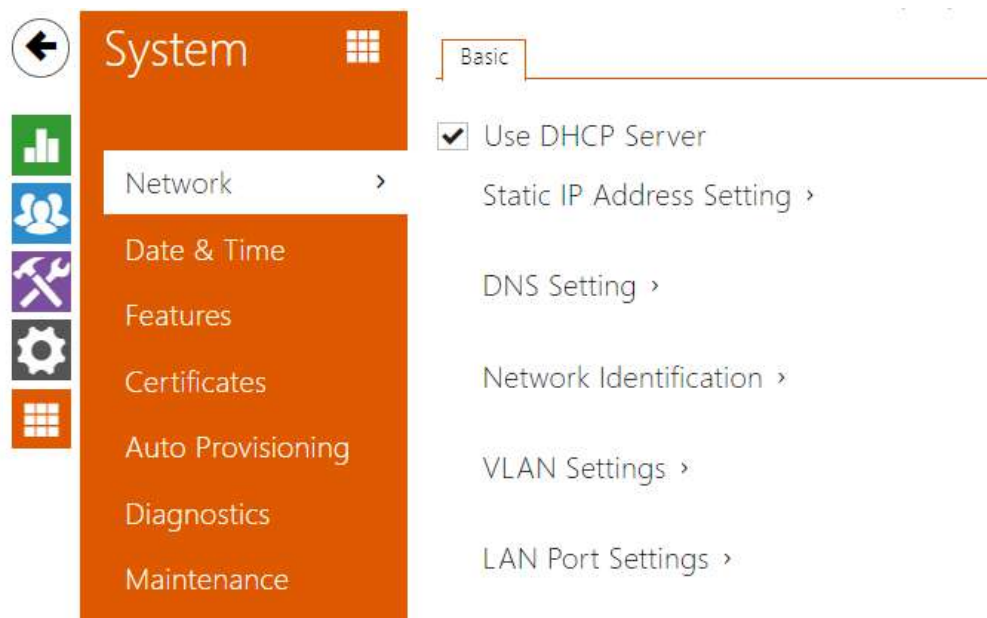
Basic

- **Use DHCP Server** – enable automatic IP address retrieval from the LAN DHCP server. If there is no DHCP server or the DHCP cannot be used in your network, use the manual network setting.

Static IP Address Setting ⌄

Static IP Address	10.0.24.107
Network Mask	255.255.255.0
Default Gateway	10.0.24.1

- **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	✔
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4

- **Primary DNS** – primary DNS address for domain name-to-IP address translation. After the factory default reset, the primary DNS server will be set to 8.8.8.8.
- **Secondary DNS** – secondary DNS address where the primary DNS is unavailable. After the factory default reset, the secondary DNS server will be set to 8.8.4.4.

Network Identification ⌄

Hostname	2NLiftIP20-5241380021
Vendor Class Identifier	

- **Hostname** – set the device identification in the LAN.
- **Vendor Class Identifier** – set the manufacturer identifier as a character string for DHCP Option 60.

VLAN Settings ⌄

VLAN Enabled	☐
VLAN ID	1

- **VLAN Enabled** – enable the virtual network (VLAN) support (according to recommendation 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. A wrong setting may result in a connection loss and need to reset the device to factory values.

LAN Port Settings ˅

Required Port Mode | Automatic

Current Port State | **Full Duplex – 10 Mbps**
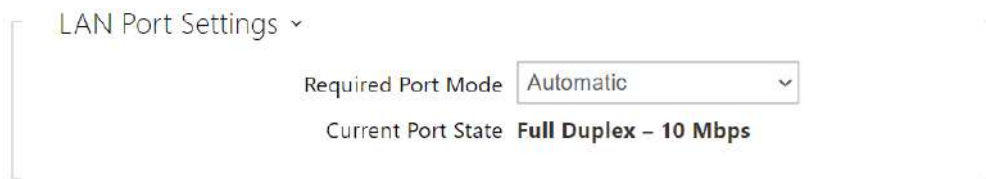
- **Required Port Mode** – set the preferred network interface port mode: Autonegotiation or Half Duplex – 10 Mbps. The lower bit rate of 10 Mbps may be necessary if the used network infrastructure (cabling) is not reliable for the 100 Mbps traffic.
- **Current Port State** – current network interface port state (Half or Full Duplex – 10 Mbps or 100 Mbps).

4.6.2 Date and Time

2N® LiftIP 2.0 is equipped with a real time clock to back up the device for even a few days in the case of power outage. Press the **Synchronize with browser** button to synchronize the device time with your current PC time value.
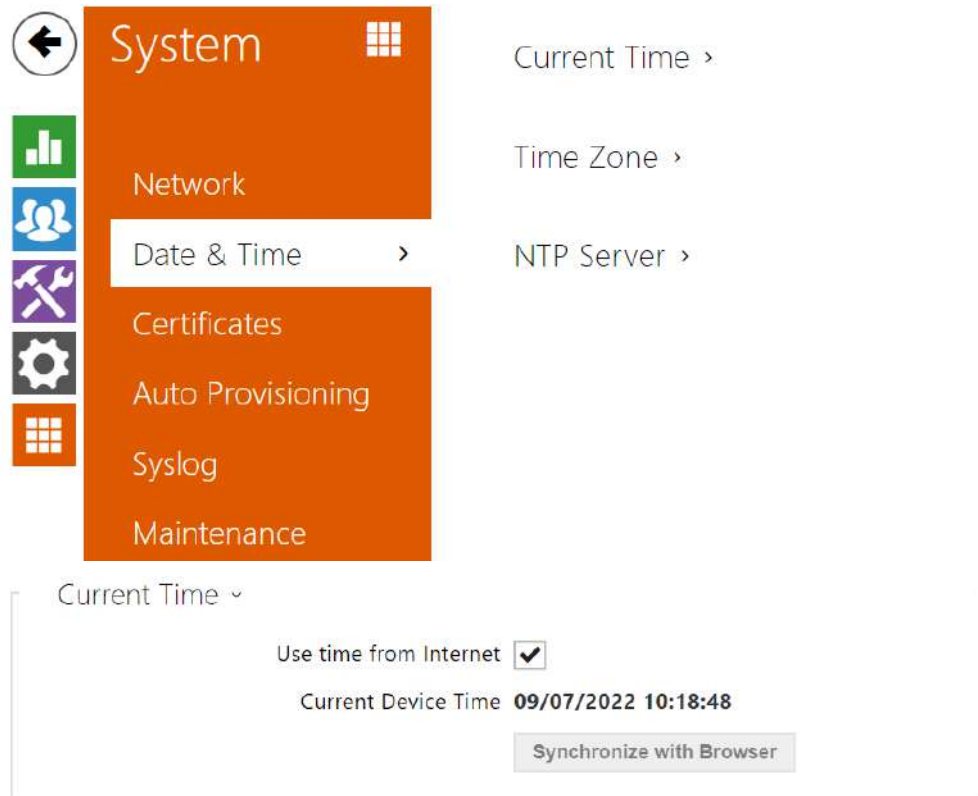
- **Use time drom internet** – enable the use of the NTP sever for internal time synchronization.
- **Current Device Time** – display the internal current time of the device.
- **Synchronize with Browser** – click the button to synchronize the device time with your current PC time value.
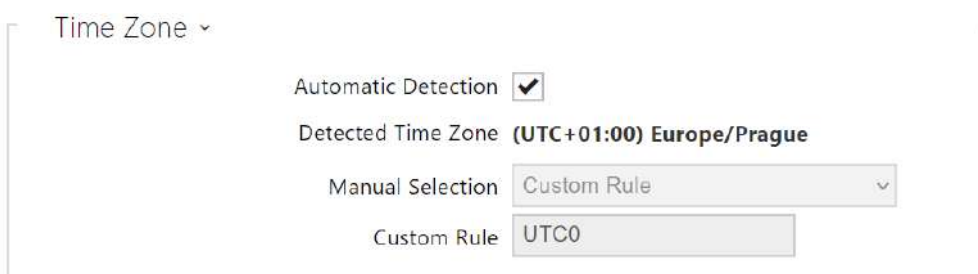
- **Automatic Detection** – define whether the time zone shall be detected automatically from My2N. In case automatic detection is disabled, the Manual selection parameter is used (manually selected time zone or Custom rule).

- **Detected Time Zone** – display 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. The setting defines the time shifts and summer/winter time transitions.
- **Custom Rule** – set the time zone rule manually if your device is installed on a site that is not included in the Time Zone list.
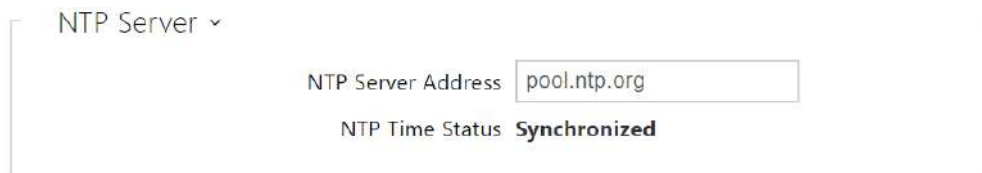
- **NTP Server Address** – set the IP address/domain name of the NTP server used for your intercom time synchronization.
- **NTP Time Status** – display the state of the last local time synchronization attempt via NTP: Unsynchronized, Synchronized, Error.

4.6.3 Features
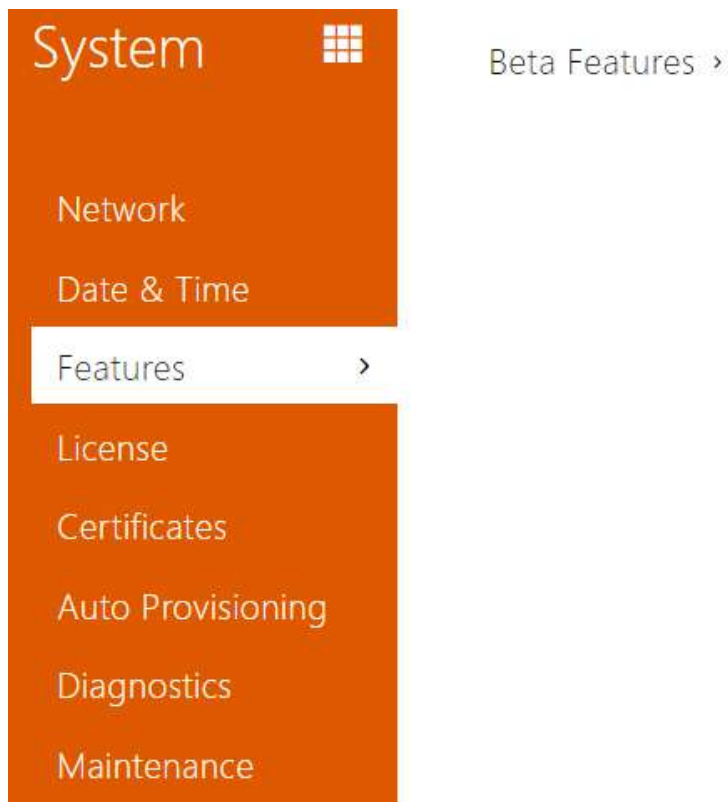
A list of public beta functions designed for user testing is shown here.
The list includes:

- function name,
- function status: started or stopped,
- event allowing to start/stop the function.

The function does not start/stop until the device is restarted. Hence, the status change request can be canceled by **Interrupt** until the restart.

> ⓘ **Note**
>
> - There is no warranty on the testing functions and 2N TELEKOMUNIKACE a.s. shall not be held liable for any functional limitations and damage incurred as a result of functional limitations of the beta functions. The beta functions are provided for testing purposes exclusively.

4.6.4 Certificates

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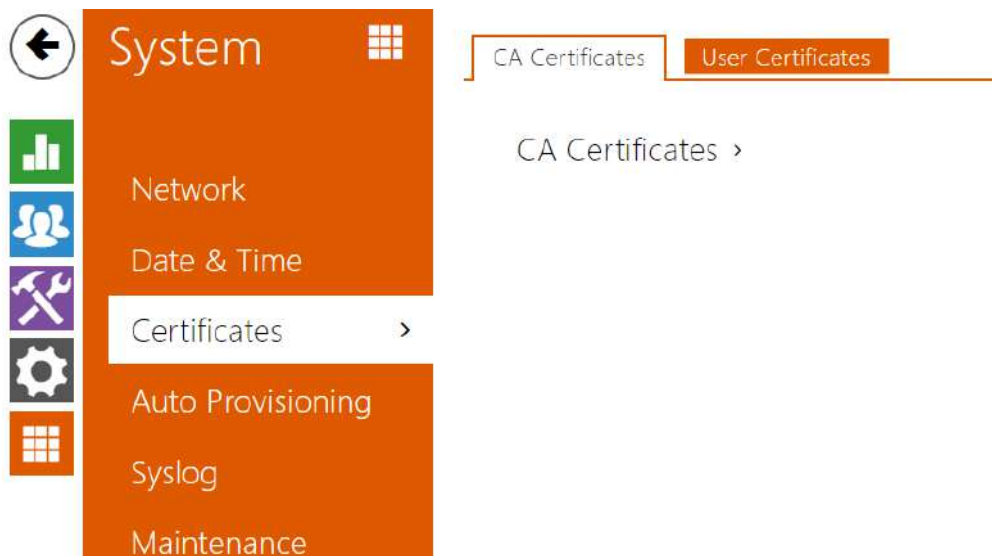
Device services that use the TLS protocol:

    a. Web server (HTTPS)
    b. SIPs

2N® LiftIP 2.0 allows you to upload sets of CA certificates, which are used for identity verification of the communicating device, and upload user certificates and private keys used for communication encryption.

Each certificate requiring service can be assigned one certificate set, refer to the **Web Server** subsection. The certificates can be shared by the services.

- **2N® LiftIP 2.0** accepts certificates in the DER (ASN1) and PEM formats.
- **2N® LiftIP 2.0** supports the AES, DES and 3DES encryption standards.
- **2N® LiftIP 2.0** supports the following algorithms:
  - RSA up to 2048bit key size for user uploaded certificates; internally up to 4096bit keys (while connection – intermediate and equivalent certificates)
  - Elliptic Curves

> ⚠ **Caution**
>
> - The CA certificates must use the X.509 v3 format.

Upon the first power supply connection, the so-called **Self Signed certificate** and **private key** are generated to be used for the **Web server** and **E-mail** services without the need to upload a certificate and private key of your own.

> ⓘ **Note**
>
> - *In case you use the Self Signed certificate for communication encryption between the device web server and the browser, your communication is secure, but you will be warned by the browser that the intercom certificate's trustworthiness cannot be verified.*

The current list of uploaded CA certificates and user certificates is displayed in two folders:

Click to upload a certificate saved on your PC into the device. Select the certificate (or private key) file in the dialog box and click **Upload**. Press to remove the certificate. Press to show certificate information.

> ⚠ **Caution**
>
> - Note that a certificate with a private RSA key longer than 2048 bits may be rejected. In that case, 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.

4.6.5 Auto Provisioning

2N LiftIP 2.0 helps you update firmware and configuration manually or automatically from a storage on a TFTP/HTTP server selected by you according to predefined rules.

The TFTP and HTTP server addresses can be configured manually. **2N LiftIP 2.0** supports automatic IP address retrieval from the local DHCP server (Option 66/150).

> ⚠ **Caution**
>
> - The login password is saved in the configuration file. If the password is 2n (default), the valid configuration part is only uploaded. This means that the configuration is uploaded, but the password remains the same, not assuming the value included in the file.
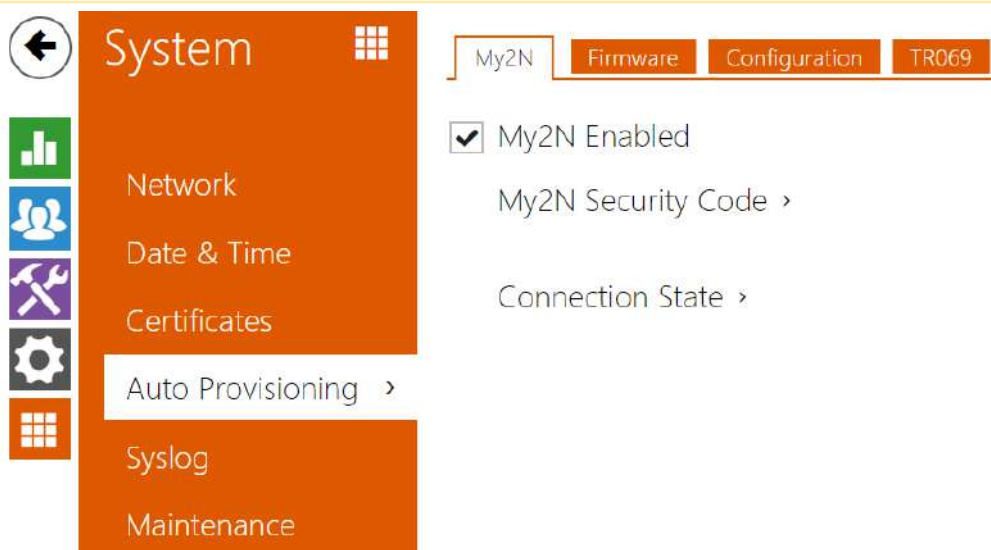
My2N

- **My2N Enabled** – enable connection to My2N or another ACS.

- **Serial Number** – display the serial number of the device for which the My2N code is valid.
- **My2N Security Code** – display the full application activating code.

- **Generate New** – the active My2N Security Code will be invalidated and a new one will be generated.
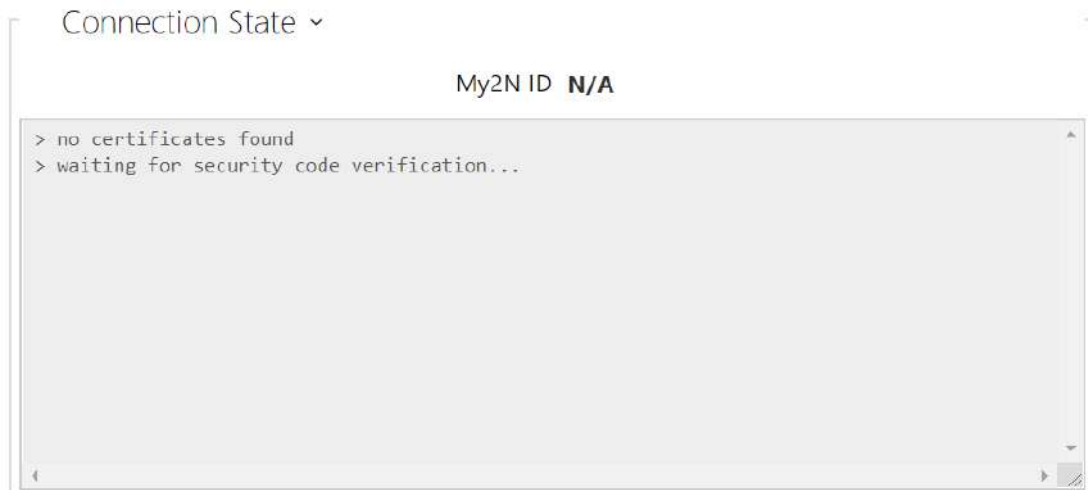
The folder provides information on the device connection to My2N.

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

Firmware

The Firmware folder helps you set automatic firmware download from a server defined by you. The device compares the server file with its current firmware file periodically and, if the server file is later, automatically updates firmware and gets restarted (approx. 30 s). Therefore, we recommend that you update when the device traffic is very low (at night, e.g.).

2N LiftIP 2.0expects the following files on the servers:

a. **MODEL**-firmware.bin – device firmware
b. **MODEL**-common.xml – common configuration for all devices of one model
c. **MODEL**-**MACADDR**.xml – specific configuration for one device

Lip in the file name gives the technical specification of the device.

MACADDR is the MAC address of the device in the 00-00-00-00-00-00 format. Find the MAC address on the production label or directly in the **State / Services** folder on the web interface.

Example:

2N Lift IP 2.0 with MAC address 00-87-12-AA-00-11 downloads the following files from the TFTP server:

- lip-firmware.bin
- lip-common.xml

- lip-00-87-12-aa-00-11.xml

☑ Firmware Update Enabled

- **Firmware Update Enabled** – enable automatic firmware download from the TFTP/HTTP server.

Server Settings ˅

Address Retrieval Mode	DHCP (Option 66/150) ˅
Server Address	
DHCP (Option 66/150) Address	
File Path	/
Use Authentication	✔
Username	
Password	
Verify Server Certificate	☐
Client Certificate	ⓘ ˅

- **Address Retrieval Mode** – select whether the TFTP/HTTP 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 TFTP (tftp://ip_address), HTTP (http://ip_address) or HTTPS (https://ip_address) server address manually.
- **DHCP (Option 66/150) Address** – check the server address retrieved via the DHCP Option 66 or 150.
- **File Path** – set the path to firmware files folder. Enter / to search for model-firmware.bin (specific model) in the server's root folder. Refer to the sidebar (?) for details about models, etc.
- **Use Authentication** – enable authentication for HTTP server access.
- **Username** – enter the user name for server authentication.
- **Password** – enter the password for server authentication.
- **Verify Server Certificate** – specification of a set of CA certificates for verification of the ACS public certificate validity.
- **Client Certificate** – – specification of the client certificate and private key used for verification of the device authorization to communicate with the ACS.

> ⓘ **Info**
>
> - The device contains Factory Cert, a signed certificate used for British Telecom integration, for example.

Update Schedule ⌄

At Boot Time	Check for Update
Update Period	Daily
Update At	01:00
Next Update At	09/07/2022 23:00:00

Apply & Update

- **At Boot Time** – enable check and, if possible, update execution upon every device start.
- **Update Period** – set the update period. Set an automatic update to take place hourly/daily/weekly/monthly, or set the period manually.
- **Update At** – set the update time in the HH:MM format for periodical updating. Thus, you can set that the update shall take place at a low-traffic time. The parameter is not applied if the update period is set to a value shorter than 1 day.
- **Next Update At** – set the next update time.

Update Status ⌄

Last Update At	09/07/2022 11:36:06
Update Result	DHCP option 66 failed
Communication Result Detail	N/A

- **Last Update At** – display the last update time.
- **Update Result** – display the last update result. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail** – server communication error code or TFTP/HTTP status code.

Result	Description
Invalid server address	The server address is invalid.
Unsupported protocol	The protocol is not supported. HTTP(s) and TFTP are supported only.

Result	Description
Invalid file path	The provisioning file location is invalid.
DHCP option 66 failed	The server address loading via DHCP Option 66 or 150 has failed.
Invalid domain name	The server domain name is invalid due to wrong configuration or unavailability of the DNS server.
Server not found	The requested HTTP/TFTP server fails to reply.
Authentication failed	The HTTP credentials are invalid.
File not found	The file has not been found on the server.
Request queuing...	The provisioning request is queuing...
Running...	Update is in progress.
Invalid file	The file to be downloaded is corrupted or of a wrong type.
Up-to-date firmware	The firmware update attempt reveals that the latest firmware version has been uploaded.
Successful update	The configuration/firmware update has been successful. With firmware update, the device will be restarted in a few seconds.
Internal error	An unspecified error occurred during file download.

Configuration

Use the Configuration folder to set automatic configuration download from the server defined by you. The device periodically downloads a file from the server. The device gets reconfigured without getting restarted.

☑ Automatic Configuration Update

- **Automatic Configuration Update** – enable automatic configuration download from the TFTP/HTTP server.

Server Settings ˅

Address Retrieval Mode | DHCP (Option 66/150) ˅

Server Address

DHCP (Option 66/150) Address **N/A**

File Path | /

Use Authentication ✔

Username

Password

Verify Server Certificate ☐

Client Certificate ⓘ ˅

- **Address Retrieval Mode** – select whether the TFTP/HTTP server address shall be entered manually or a value shall be retrieved automatically from the DHCP server using Option 66.
- **Server Address** – enter the TFTP (tftp://ip_address), HTTP (http://ip_address) or HTTPS (https://ip_address) server address manually.
- **DHCP (Option 66/150) Address** – check the server address retrieved via the DHCP Option 66 or 150.
- **File Path** – set the firmware/configuration filename directory or prefix on the server. The device expects the XhipY_firmware.bin, XhipY-common.xml and XhipY-MACADDR.xml files, where X is the prefix specified herein and Y specifies the device model.
- **Use Authentication** – enable authentication for HTTP server access.
- **Username** – enter the user name for server authentication.
- **Password** – enter the password for server authentication.
- **Verify Server Certificate** – specification of a set of CA certificates for verification of the ACS public certificate validity.
- **Client Certificate** – – specification of the client certificate and private key used for verification of the device authorization to communicate with the ACS.

> ⓘ **Info**
>
> - The device contains Factory Cert, a signed certificate used for British Telecom integration, for example.

- **At Boot Time** – enable check and, if possible, update execution upon every device start.
- **Update Period** – set the update period. Set an automatic update to take place hourly/daily/weekly/monthly, or set the period manually.
- **Update At** – set the update time in the HH:MM format for periodical updating. Thus, you can set that the update shall take place at a low-traffic time. The parameter is not applied if the update period is set to a value shorter than 1 day.
- **Next Update At** – display the next update time.

- **Last Update At** – display the last update time.
- **Update Result (Common Config)** – display the last common update result. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail (Common configuration)** – server communication error code or TFTP/HTTP status code.
- **Update Result (Private Config)** – private configuration follows the common configuration update. A device with private configuration is identified by the MAC address. The result of the last private update is displayed. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail (Private configuration)** – server communication error code or TFTP/HTTP status code.

TR069

Use this folder to enable and configure remote device administration 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 enables the device to be connected to an ACS (Auto Configuration Server) of its own. In this case, the connection to My2N will be disabled in the device.

- **My2N / TR069** – enable the My2N / TR-069 service.
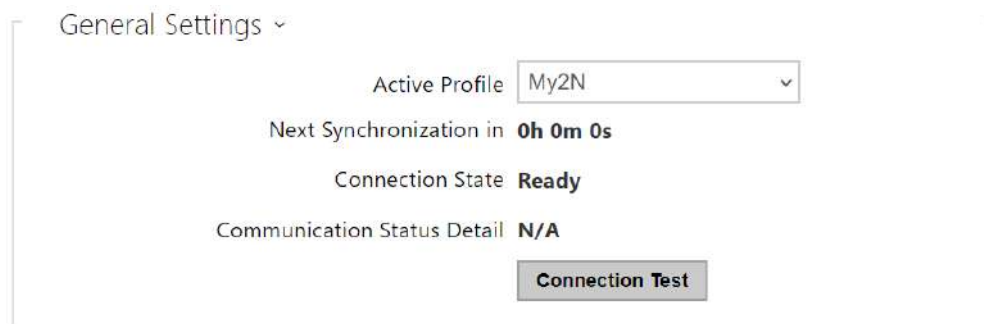
- **Active Profile** – select one of the pre-defined profiles (ACS), or choose a setting of your own and configure the ACS connection manually.
- **Next Synchronization in** – display the time period in which the device shall contact a remote ACS.
- **Connection State** – display the current ACS connection state or error state description if necessary.
- **Communication Status Detail** – server communication error code or TFTP/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.

4.6.6 Diagnostics
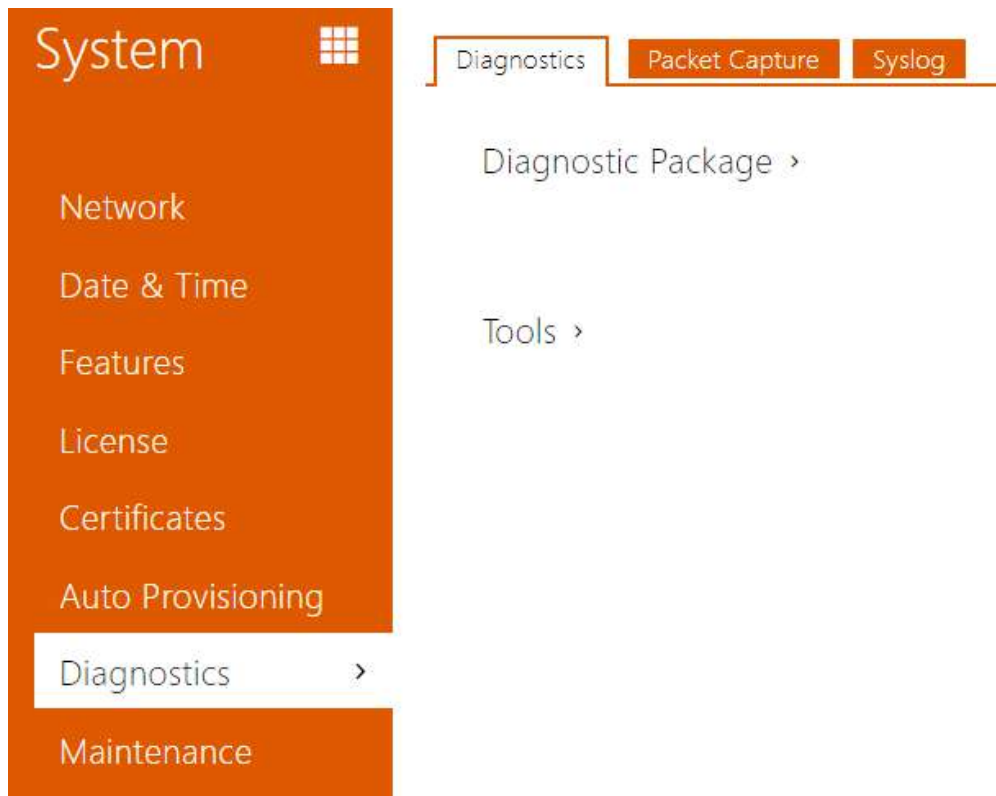
Diagnostics

The interface helps you start capturing diagnostic logs for subsequent download and sending to the Technical Support. The captured diagnostic logs help identify and solve reported problems. The logs contain information on the device, its configuration, network traffic, crash log and memory statistics.

- **Packet Capture State** – shows whether packet capture has been started/stopped in the Packet capture folder.
- **Size of Captured Packets** – shows the size of packets captured.
- **Syslog Capture State** – shows whether syslog capture has been started/stopped in the Syslog folder.
- **Duration of Captured Syslogs** – shows the syslog capture duration in the Syslog folder.
- **Size of Captured Syslog** – shows the size of syslogs captured.
- **Stop Syslog Capture After** – set the data capture timeout.

Press ⏺ to start capturing. Repress the button to restart and rerun capturing. Press ⬇ to download the packet capture file.

> ⚠ **Caution**
>
> - Starting diagnostic data capture restarts packet capture if running.

Tools ˅

Verify the network address accessibility   **Ping**
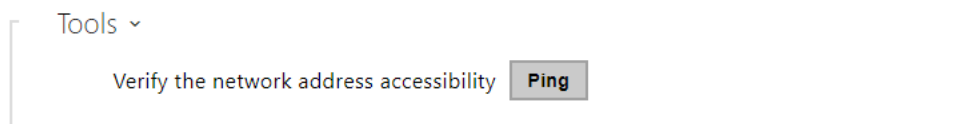
- **Verify the network address accessibility** – verify the network address accessibility via the Ping command in standard operating systems. Press Ping to display a dialogue, enter the IP address/domain name and click Ping to send test data to this address. If the selected IP address/domain name is invalid, a warning is displayed and Ping remains inactive until the given IP address becomes valid.
  The function progress and result are also displayed in the dialogue. Failed means either inaccessibility of the given IP address within 10 seconds or inability to translate the domain name into an address. If a valid response is received, the IP address from which the response came and the response waiting time in milliseconds are displayed.
  Repress Ping to send another query to the same address.

Packet Capture

In the tab, you can launch capturing of incoming and outgoing packets on the intercom network interface. The captured packets can be stored locally in the IP intercom 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 ˅

Current State	**RUNNING**
Buffer Size	**4 MB**
Buffer Utilization	**4 MB**
Number of Captured Packets	**19452**
Packet Capture Control	🔴 ⏹ ⬇
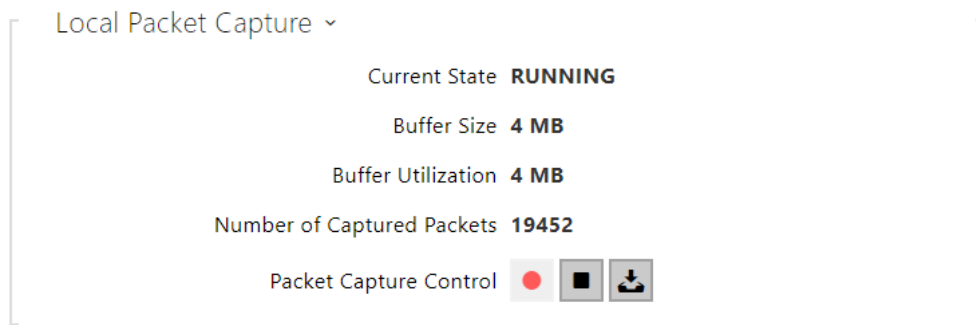
When the local capture buffer is full, the oldest packets are rewritten automatically. We recommend that you lower the video stream transmission rate below 512 kbps while capturing packets locally. Press 🔴 to start, ⏹ to stop and ⬇ to download the packet capture file.

Remote Packet Capture ˅

Current State	**STOPPED**
Count of Sent Packets	**0**
Count of Sent Bytes	**N/A**
Remaining Time	**N/A**
Packet Capture Control	🔴 ⏹
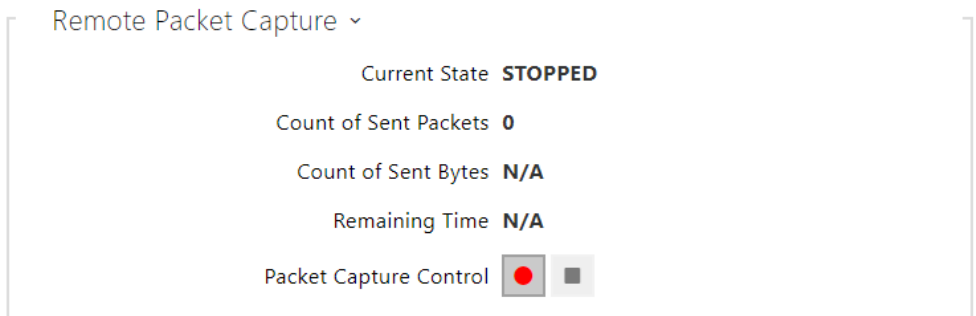
Press 🔴 to start remote capturing. Specify the capturing time interval (s) for the incoming and outgoing packets. When the set time value passes, the packet capture file will be downloaded automatically to the user PC. Press ⏹ to stop capturing.

Syslog

The **2N IP intercoms** allow you to send system messages to the Syslog server including relevant information on the device states and processes for recording, analysis and audit. It is unncecessary to configure this service for common intercom operation.

Syslog Server Settings ˅

Send Syslog Messages	✔
Server Address	
Severity Level	Info ▼

- **Send Syslog Messages** – enable sending of system messages to the Syslog server. Make sure that the server address is set correctly.

- **Server Address** – set the IP[:port] or MAC address of the server running the application to capture syslog messages.
- **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 ˅

Saving Syslog Messages	**RUNNING**
Syslog Messages Saving Passed Time	**0h 4m 26s**
Syslog Messages Saving Remaining Time	**0h 55m 34s**
Saved Syslog Messages Size	**78,335 B**
Available Syslog Messages Saving Time	**0h 4m 26s**
Available Syslog Messages Size	**78,335 B**
Required Saving Time	1 hour ▼
Syslog Messages Saving Control	● ■ ⬇ 🗑

General overview of local syslog messages.

4.6.7 Maintenance

This menu helps you maintain the **2N® LiftIP 2.0** configuration and firmware. You can back up and restore all the parameters, upgrade firmware and/or factory reset the device.
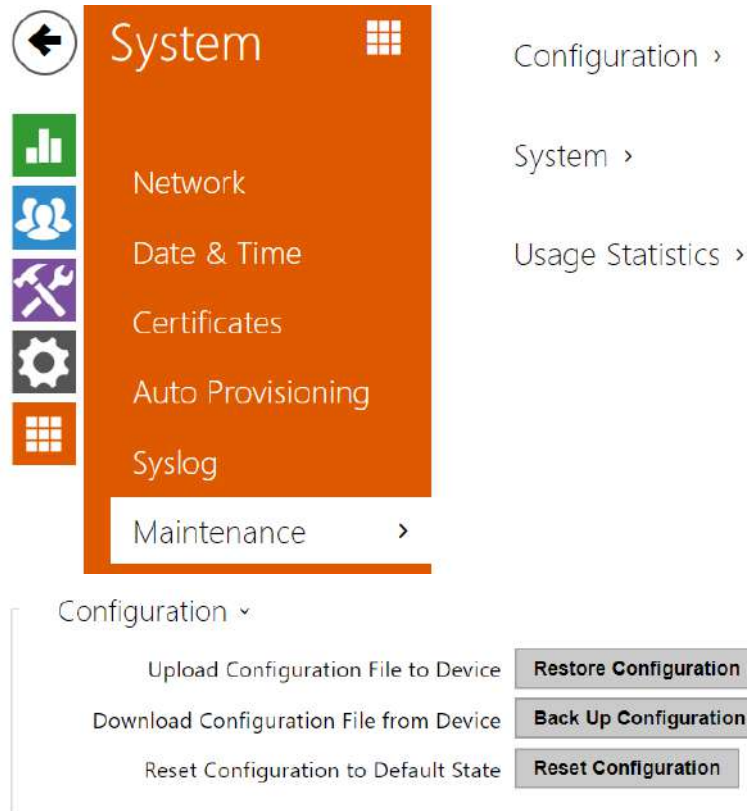
- **Restore Configuration** – restore configuration from a previous backup. Press the button to display a dialog box to select and upload the configuration file to the device. Before uploading, choose whether or not the general settings are to be applied, the directory / network settings / certificates imported and the SIP PBX connection settings used from the configuration file.

> ⚠ **Caution**
>
> - The login password is saved in the configuration file. If the password is not encoded or default (*2n* encoded), the valid configuration part is only uploaded. This means that the configuration is uploaded, but the password remains the same, not assuming the value included in the file.

- **Back Up Configuration** – back up the complete current device configuration. Press the button to download the configuration file to your PC.

> ⚠️ **Caution**
>
> • *As the configuration may include delicate information, such as user phone numbers and access passwords, handle the file cautiously.*

- **Reset Configuration** – reset all the device parameters except for the LAN parameters. Press the Reset button on the device to reset the device completely.

System ⌄

Firmware Version	**2.37.0.49.0**
Minimum Firmware Version	**2.35.0.45.0**
Bootloader Version	**1.0.0.0.4**
Software Build Type	**alpha+740571cc**
Software Build Date and Time	**9/5/2022 18:07:30**
Upgrade Device Firmware	**Upgrade Firmware**
Firmware Status	**Server error**
	Check Now
Notify of Beta Versions	☐
Restart Device	**Restart Device**
Third party library license	**Show**

- **Upgrade Firmware** – upload a new firmware version to the device. Press the button to display a dialog box to select the proper firmware file. Once the firmware is uploaded, the device is restarted automatically. After the restart, it 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 www.2n.com. FW upgrade does not affect configuration. The device checks the firmware file and prevents you from uploading an incorrect or corrupt file.
- **Check Now** – check online if a later firmware version is available. If so, the downloading option is offered followed by automatic upgrade.
- **Restart Device** – restart the device. The process takes about 30 s. Once the restart is completed and the device is assigned its IP address, the login window will be displayed automatically.

> ⚠ **Caution**
>
> - The device configuration change takes 3–15 s depending on the configuration file size. Do not restart the device during this process.

- **Show** – click the Display button to open a dialog box including a list of used licenses and third party software. It also includes a EULA link.

Usage Statistics ⌄

Send Anonymous Statistics Data ✔

- **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.

4.7 Used Ports

Service	Port	Protocol	Direction	Configurable	Settings
RTP	9 000			YES	
DHCP	68	UDP	In/Out	NO	
DNS	53	TCP/UDP	In/Out	NO	

5. Function and Use

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

Here is what you can find in this section:

5.1 Function Description

Purpose

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.

> ⚠️ **Caution**
>
> - 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. 4.3.7 Notifications 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 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 lift 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 lift 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.

5.2 Control Centre Instructions

DTMF Control during Call

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 established"	The announcement is played to the lift 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.

Announcement	Meaning
"Sorry, your call has to be interrupted."	The announcement is played to the lift 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.

5.3 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 counterparty (Busy, Number not found, etc.)	Dials the next number immediately.
Call	Waits for a timeout.
Ringing	Waits for a timeout.

Situation	2N® LiftIP 2.0
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

⚠️   • 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 lift 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 lift 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, a call is routed via GSM, **2N® LiftIP 2.0** may not detect the DTMF characters and identify the protocol.
> - If this happens, we recommend that you 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.

5.4 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 4.3.5 Notifications. 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.

5.5 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

Call **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 lift 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, refer to 4.3.5 Notifications.

5.6 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 KONE				
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 Fixed	04	90	0000000000001	Lift ID
Audio Error	04	91	0000000000000	Lift ID
Audio Fixed	04	91	0000000000001	Lift ID

> ⓘ **Example**
>
> **This is only a part of the data message. It does not contain the beginning, checksum and end.**
> - 049000000000000187654321 – 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 Fixed	04	90	-	Lift ID
Audio Error	04	91	-	Lift ID
Audio Fixed	04	91	-	Lift ID

> ⓘ **Example**
>
> **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
Checking Call	04	26	00000	Lift ID
Rescue process ended	04	84	00000	Lift ID
Button Error	04	90	00000	Lift ID
Button Fixed	04	90	00001	Lift ID
Audio Error	04	91	00000	Lift ID

CPC Antenna 2N Ext				
Call type	**Command**	**Call type**	**Data**	**ID**
Audio Fixed	04	91	00001	Lift ID

> ⓘ **Example**
>
> **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 lift 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	
Alarm 2	1	Lift ID	
Checking Call	3	Lift ID	
Rescue process ended	2	Lift ID	500
Button Error	2	Lift ID	800
Button Fixed	2	Lift ID	801
Audio Error	2	Lift ID	200
Audio Fixed	2	Lift ID	201

> ⓘ **Example**
>
> **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.

6. Technical Parameters

Electric Parameters

- **Supply voltage:** 10–30 V DC (keep polarity) or 48 V PoE 802.3af
- **Power 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
- **Codecs: 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:** (W) 65 x (H) 130 x (D) 23 mm
- **Working temperature range:** - 20 to +50 ˚C
- **Relative humidity:** 10 to 90 % non-condensing
- **Recommended altitude:** 0–2000 m

7. Supplementary Information

7.1 General Instructions and Cautions

Please read this User Manual carefully before using the product. Follow all instructions and recommendations included herein.

Any use of the product that is in contradiction with the instructions provided herein may result in malfunction, damage or destruction of the product.

The manufacturer shall not be liable and responsible for any damage incurred as a result of a use of the product other than that included herein, namely undue application and disobedience of the recommendations and warnings in contradiction herewith.

Any use or connection of the product other than those included herein shall be considered undue and the manufacturer shall not be liable for any consequences arisen as a result of such misconduct.

Moreover, the manufacturer shall not be liable for any damage or destruction of the product incurred as a result of misplacement, incompetent installation and/or undue operation and use of the product in contradiction herewith.

The manufacturer assumes no responsibility for any malfunction, damage or destruction of the product caused by incompetent replacement of parts or due to the use of reproduction parts or components.

The manufacturer shall not be liable and responsible for any loss or damage incurred as a result of a natural disaster or any other unfavourable natural condition.

The manufacturer shall not be held liable for any damage of the product arising during the shipping thereof.

The manufacturer shall not make any warrant with regard to data loss or damage.

The manufacturer shall not be liable and responsible for any direct or indirect damage incurred as a result of a use of the product in contradiction herewith or a failure of the product due to a use in contradiction herewith.

All applicable legal regulations concerning the product installation and use as well as provisions of technical standards on electric installations have to be obeyed. The manufacturer shall not be liable and responsible for damage or destruction of the product or damage incurred by the consumer in case the product is used and handled contrary to the said regulations and provisions.

The consumer shall, at its own expense, obtain software protection of the product. The manufacturer shall not be held liable and responsible for any damage incurred as a result of the use of deficient or substandard security software.

The consumer shall, without delay, change the access password for the product after installation. The manufacturer shall not be held liable or responsible for any damage incurred by the consumer in connection with the use of the original password.

The manufacturer also assumes no responsibility for additional costs incurred by the consumer as a result of making calls using a line with an increased tariff.

Electric Waste and Used Battery Pack Handling

Do not place used electric devices and battery packs into municipal waste containers. An undue disposal thereof might impair the environment!

Deliver your expired electric appliances and battery packs removed from them to dedicated dumpsites or containers or give them back to the dealer or manufacturer for environmental-friendly disposal. The dealer or manufacturer shall take the product back free of charge and without requiring another purchase. Make sure that the devices to be disposed of are complete.

Do not throw battery packs into fire. Battery packs may not be taken into parts or short-circuited either.

7.2 Directives, Laws and Regulations

2N$^®$ LiftIP 2.0 conforms to the following directives and regulations:

- 2014/35/EU for electrical equipment designed for use within certain voltage limits
- 2014/30/EU for electromagnetic compatibility
- 2014/33/EU for lifts and safety components for lifts
- 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment
- 2012/19/EU on waste electrical and electronic equipment

Industry Canada

This Class A digital apparatus complies with Canadian ICES-003/NMB-003.

FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.

NOTE: These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency

energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

7.3 Terms and Symbols

The following symbols and pictograms are used in the manual:

> ◆ **Safety**
>
> - **Always abide** by this information to prevent persons from injury.

> ◆ **Warning**
>
> - **Always abide** by this information to prevent damage to the device.

> ⚠ **Caution**
>
> - **Important information** for system functionality.

> ✅ **Tip**
>
> - **Useful information** for quick and efficient functionality.

> ⓘ **Note**
>
> - Routines or advice for efficient use of the device.