2N Sentrio

Installation Manual

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

2N.com

Table of Contents

Symbols and Terms Used

The following symbols and pictograms are used in the manual:

DANGER
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.

Product Description

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

Basic Features

2N Sentrio is a comprehensive solution enabling VoIP and text communication between the elevator, remote control room and the technician in the building. This solution provides elevator communication even to persons with hearing impairments. The solution includes:

- **2N Sentrio Cabin** – an emergency elevator communicator located in the elevator cabin, which provides VoIP transmission, communication via text messages and video transmission from an IP camera in the elevator cabin.
- **2N Sentrio Switch** – a switch providing connection of external inputs and outputs to **2N Sentrio Cabin** (not necessary, but a recommended part of the solution).
- **2N Sentrio Lobby** – an internal IP/SIP unit designed for connection with emergency communicators in the elevator cabin. The connection is ensured by VoIP transmission and text message transmission. The device also provides displaying video streams from the elevator cabin. The unit is located directly in the building where the elevators are installed, ensuring fast and efficient communication without any delay caused by remote control communication.

2N Sentrio Cabin is the only unit that the elevator user comes into direct contact with. **2N Sentrio Lobby** should only be operated by a responsible and well-trained person coordinating the evacuation.

For **configuration of 2N Sentrio** you need a PC equipped with any Internet browser.

The **2N Elevator Center** cloud solution helps the operators audio/video/chat communicate with the device during the alarm call. Also, it enables users to configure the device remotely – to set the text messages, including language mutations, to be displayed on the device during alarm calls with the control room, for example.

Basic Features and Advantages of 2N Sentrio

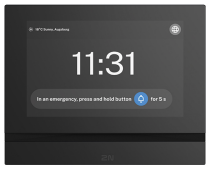
- Full duplex audio transmission using VoIP technology
- Video transmission via an external camera from the elevator cabin (full duplex transmission option)
- Sending messages using text communication

- video codecs H.264 (Main or Baseline profile), MJPEG
- audio codecs G.711a/u, G.722, G.729, L16/16 kHz
- HTTPS server for configuration,
- SNTP client for server time synchronization,
- RTSP server for video streaming,

The following products can be added to the 2N Sentrio solution:

- External IP camera (not included in the 2N portfolio) – video transmission starts at the alarm call. During normal use, video is unavailable from the elevator cabin, which guarantees privacy to the elevator users.
- 2N LiftGate – in combination with 2N Cabin Switch, the IoT gateway provides elevator data connectivity including power backup in case of a main supply failure according to the applicable legislation. Also, it provides communication with the 2N Elevator Center cloud solution.
  One 2N LiftGate ensures 4-hour operation for two elevators with battery backup power, i.e. for two **2N Sentro Cabin** devices, two 2N Cabin Switch units and two external cameras (if an Axis – P9106-V external camera is used).

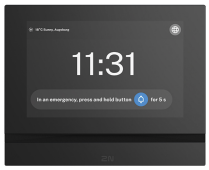
System components



Part No. 91378901US

2N Sentrio Cabin Main Unit – US version

There must be just one main cabin unit in one installation. The main unit installation requires a frame.



Part No. 91378901E

2N Sentrio Cabin Main Unit – EU version

There must be just one main cabin unit in one installation. The main unit installation requires a frame.

Part No. 91378903

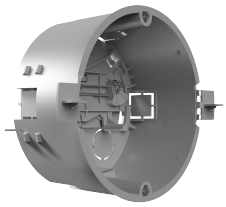
2N Setrio Lobby main unit

The elevator communication unit is designed to communicate with the IP elevator communicators in buildings higher than 18 meters (60 feet) directly from the site.

Accessories

Accessories for Installation

Choose the proper accessories for your particular installation needs.



Axis Part No. 01700-001

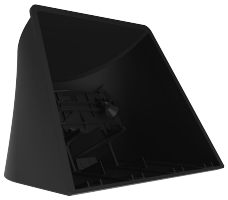
Mounting box

Wall/plasterboard flush mounting box for 2N indoor answering units.

Axis Part No. 02320-001

Wall mounting box

Wall surface mounting box for 2N indoor answering units.



Axis Part No. 02039-001

Stand

Stand for 2N indoor answering units.

2N Sentrio Frame – US version, 3 buttons

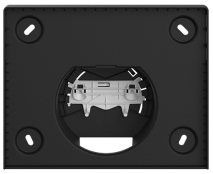
2N Sentrio Cabin frame (Part No. 91378901US) with 3 buttons.

To be ordered together with the switch for this frame version, Part No. 91378904.

2N Sentrio Frame – EU version, 3 buttons

2N Sentrio Cabin frame (Part No. 91378901E) with 3 buttons.

To be ordered together with the switch for this frame version, Part No. 91378904.



2N Sentrio Frame – EZ/US/AU version, buttonless

2N Sentrio Cabin frame without buttons.

2N Sentrio Switch – US/EU version, for frame with 3 buttons

2N Sentrio Cabin - frame interconnection switch with pre-prepared cabling and 3 buttons.

2N Sentrio Switch – US/EU version, for external buttons

2N Sentrio Cabin - frame interconnection switch without buttons, with pre-prepared cabling for external buttons.

Other accessories

Associated Products

Axis Part No. 02660-001

2N IP Phone D7A

Axis Part No. 02659-001

2N IP Phone D7A – USB camera

2N LiftGate

IoT gateway providing elevator data connectivity and battery backup.

2N LiftGate Cabin Switch

Switch for the 2N LiftGate main unit.

2N Voice Alarm Station Audio Unit

The audio alarm designed for installation onto and/or under the elevator cabin.

Package Completeness Check

Please check the product delivery before installation. Contents:

1x	**2N Sentrio**
1x	2.5 mm hexagon key wrench
1x	Quick Start manual
1x	Display cleaning cloth
2x	Terminals for connecting external power supply and ALARM2 button (**2N Sentrio Cabin**) / device lock (**2N Sentrio Lobby**)

Frame Package Completeness Check

The package of frames for **2N Sentrio** includes:

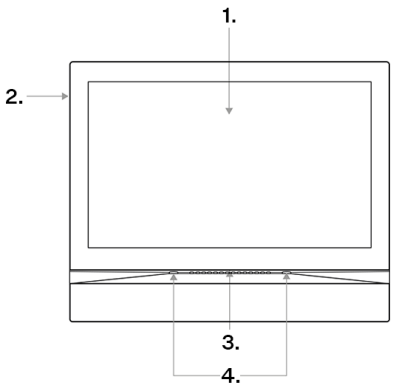
4x	M3 flat-head open steel rivet nut for 0.5–2 mm plates, with the maximum head height of 0.8 mm
4x	stainless steel lens-head 3 x 12 mm screw for 0.5–2 mm plates (with TufLok surface or using a lock washer with the maximum head height of 2.4 mm).

4x	stainless steel flat nut for M3 screw, 12 mm outer diameter, 0.8 mm thickness
1x	Installation Manual

CAUTION
If spare accessories other than the specified types are used, the device warranty might become null and void.

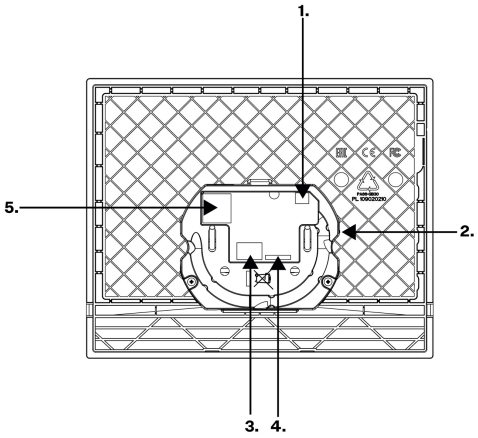
Component Layout

Front



1. Display
2. Microphone
3. Speaker
4. Anchoring holes

Rear



1. External induction loop output
2. RESET button, status LEDs
3. Connectors:
   Left – 10–15 V DC power supply input
   Right – ALARM input (**2N Sentrio Cabin)** / microswitch input (**2N Sentrio Lobby** lock)
4. 2N Sentrio Switch input connector
5. Ethernet

Mechanical Installation

This subsection provides the **2N Sentrio** installation and connection instructions.

Installation Conditions

Make sure that the following 2N Sentrio installation conditions are met.

- There must be enough space for the device installation.
- Make sure that the depths of the dowel holes are accurate!
- Before starting the mechanical installation on a selected place, make sure carefully that the preparations associated with it (drilling, wall cutting) cannot damage the electrical, gas, water and other existing wires and pipes.
- The device is not designed for environments with increased vibrations such as means of transport, machine rooms and so on.
- The device may not be exposed to aggressive gas, acid vapors, solvents, etc.
- The device is not intended for direct connection into the Internet/WAN. The device must be connected to the Internet/WAN via a separating active network element (switch/router).
- Avoid strong electromagnetic radiation on the installation site.

CAUTION

- Exceeding the allowed operating temperature may not affect the device immediately but leads to premature ageing and lower reliability. For the acceptable range of operating temperatures and relative humidity values refer to S.Technical Parameters (p. 95).
- Any intentional mechanical damage to the device (drilling, main unit tampering, etc.) results in a loss of warranty.
- The device installation and setting should only be performed by professionally qualified persons.

Installation Conditions

Make sure that the following 2N Sentrio installation conditions are met.

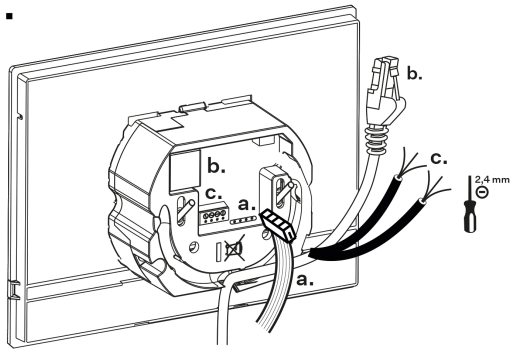
- There must be enough space for the device installation.
- Make sure that the depths of the dowel holes are accurate!
- Before starting the mechanical installation on a selected place, make sure carefully that the preparations associated with it (drilling, wall cutting) cannot damage the electrical, gas, water and other existing wires and pipes.
- The device is not designed for environments with increased vibrations such as means of transport, machine rooms and so on.
- The device may not be exposed to aggressive gas, acid vapors, solvents, etc.
- The device is not intended for direct connection into the Internet/WAN. The device must be connected to the Internet/WAN via a separating active network element (switch/router).
- Avoid strong electromagnetic radiation on the installation site.

CAUTION

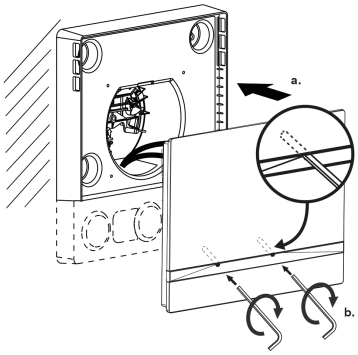
- Exceeding the allowed operating temperature may not affect the device immediately but leads to premature ageing and lower reliability. For the acceptable range of operating temperatures and relative humidity values refer to S.Technical Parameters (p. 95).
- Any intentional mechanical damage to the device (drilling, main unit tampering, etc.) results in a loss of warranty.
- The device installation and setting should only be performed by professionally qualified persons.

Installation 2N Sentrio Cabin

1.



2.



1. First, connect the main unit - switch connecting cable (a) to the main unit. Then connect the Ethernet cable to the device (b). If the PoE cable is not used for power, connect the external power supply cable (c) too.
2. Slide the device into the frame so that it fits on the centering pins and use a hex key to fix it.

Now the device is ready for basic operation. It is necessary to perform software configuration (p. 58) to achieve a full functionality of the device.

Switch and Frame Installation

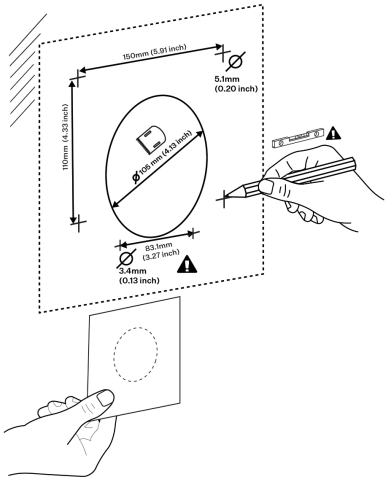
TIP

- 2N Sentrio Frame: Download the drilling template from 2N.com.
- 2N Sentrio Switch: Download the drilling template from 2N.com.

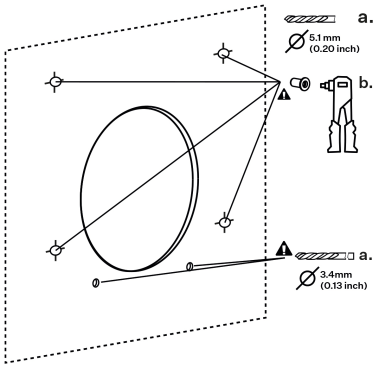
CAUTION

Install the device at such a height that the location of the ALARM control buttons / meets the accessibility requirements of the applicable local standards. Before starting the installation, we recommend that you check the specific values and limits set by the relevant regulations for your location.

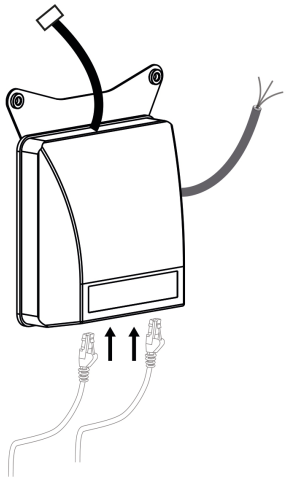
1.


150mm (5.91 inch)
5.1mm
(0.20 inch)
110mm (4.33 inch)
Ø 105 mm (4.13 inch)
83.1mm
(3.27 inch)
3.4mm
(0.13 inch)

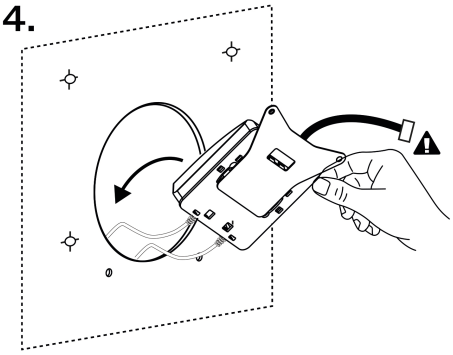
2.


a.
5.1 mm
(0.20 inch)
b.
a.
3.4mm
(0.13 inch)

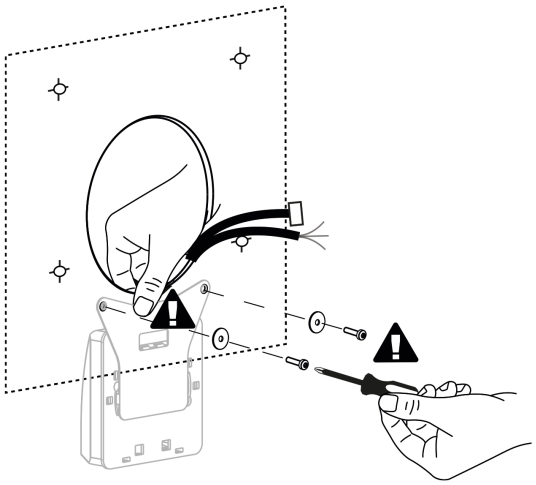
3.



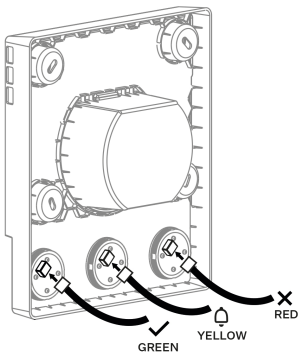
4.



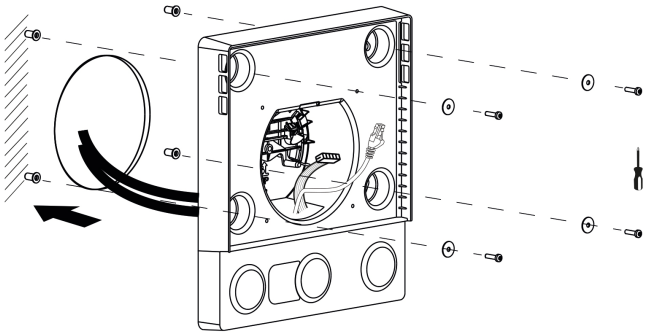
5.



6.


RED
GREEN
YELLOW

7.



1. Make the frame fitting holes and cut a central circular hole for the frame (2N Sentrio Frame) using the drilling template. The recommended diameter of the central hole is 106 mm and that of the rivet holes is 5.1 mm. Now make the switch (2N Sentrio Switch) fitting holes using the drilling template. The drilling template uses the 2 bottom frame fitting holes as reference points.
2. Put the rivet nuts in the frame fitting holes and fix them using riveting pliers.
3. Connect the required cables into the switch that are not connected by factory default.
4. **a.** Pull the switch through the central circular hole holding it from the other side.
   b. Pull the switch cables intended for the main unit and frame interconnection back through the hole.
5. Fit the switch with the screws.
6. **a.** Connect the cables to the frame buttons. The cables are color-coded (green – YES button, red – NO button, yellow – ALARM 1 button).
   b. Pull the **2N Sentrio Cabin** main unit connecting cables through the frame hole.
   c. Insert the frame in the pre-prepared circular hole and fix it with screws.

TIP
Remove the button covering foil.

Installation 2N Sentrio Lobby

The device can be installed on any of the following ways:

- into a wall using a mounting box (not included in the package),
- onto a wall using a mounting box (not included in the package),
- into a stand (not included in the package).

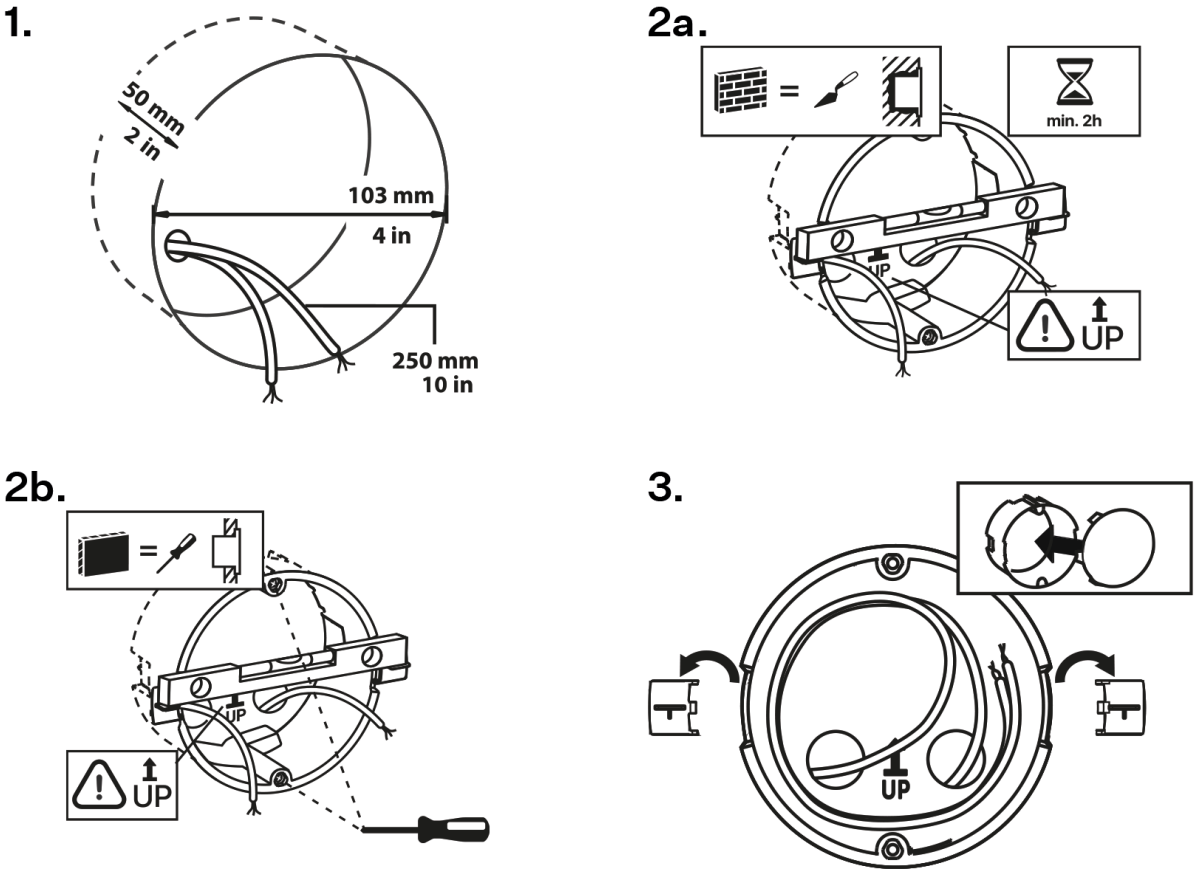
Flush Mounting

1. Flush Mounting Box Installation (p. 16)
2. Flush Mounting Box Device Installation (p. 17)

Flush Mounting Box Installation

CAUTION
Before starting the mechanical installation on a selected place, make sure carefully that the preparations associated with it (drilling, wall cutting) cannot damage the electrical, gas, water and other existing wires and pipes.

TIP
Download the Drilling template from 2N.com .



1. Cut a circular hole in the wall of the diameter of 103 mm and depth of 50 mm before installation. It is assumed that all necessary cables of the maximum length of 25 cm will lead to the hole.
2. Put the flush mounting box in the hole to make sure that the hole is deep enough.
3. If the hole complies with the box size, wall in the box and level the box using a water level on the holding clips.
4. When the mortar hardens, break off the clips and cap the box with the cover provided. Use anchoring elements to fix the device into plasterboard.

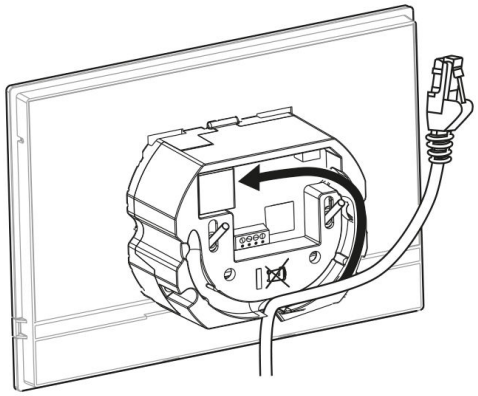
To install **2N Sentrio** into a flush mounting box, get a 2.5 mm hexagon key wrench, which is included in the package.

NOTE
When installing **2N Sentrio** into a wall, take the local standards related to installation of electrical devices on flammable material into consideration.

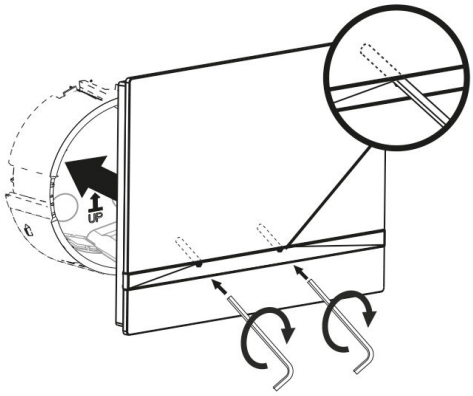
Flush Mounting Box Device Installation

TIP
Refer to Subs. Component Layout (p. 11) for connector layout.

1.



2.



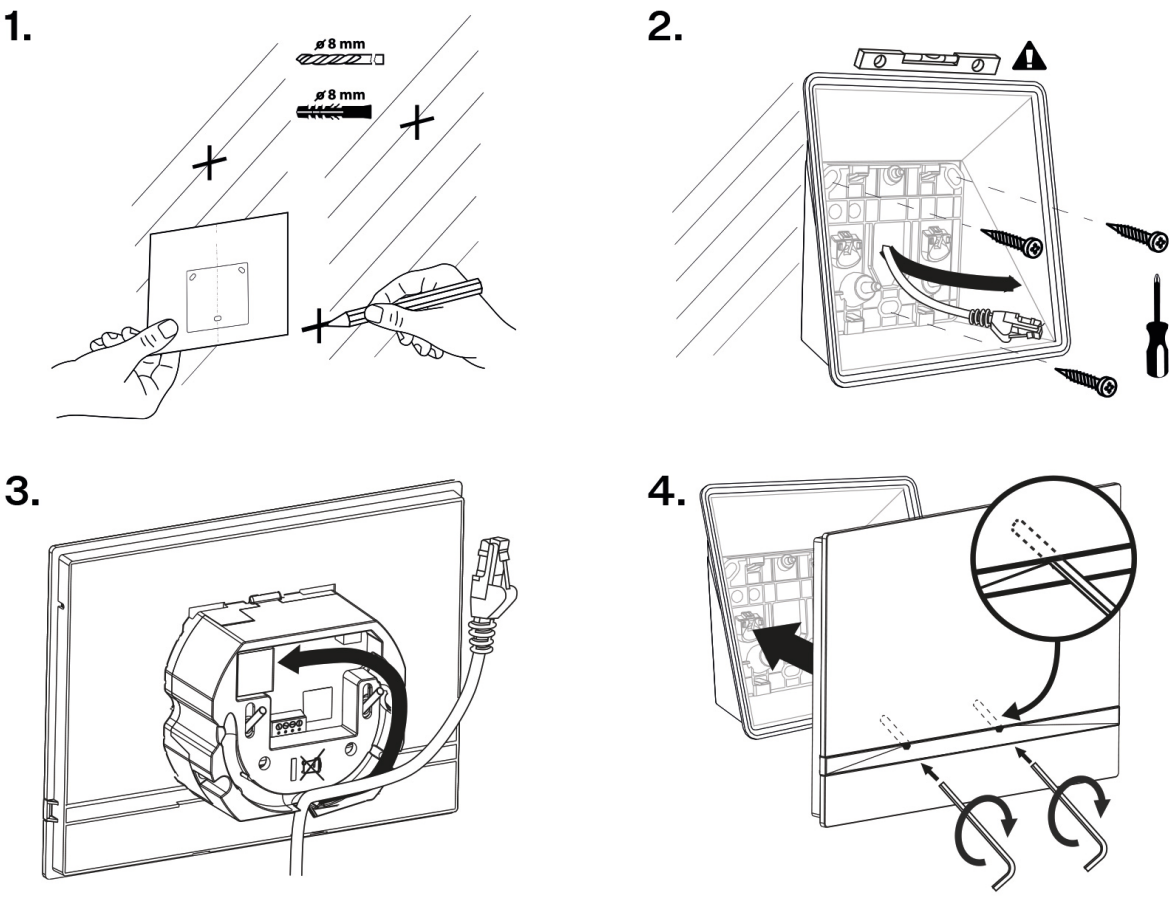
1. Remove the cover from the wall-mounted installation box. Take out the pre-prepared cabling, the UTP cable the bell wire (two-wire), power supply.
2. Shorten the cables to 150 mm or less as required. Connect the doorbell twin cable or power supply cable to the connector provided.
3. Crimp the RJ-45 connector onto the UTP cable.
4. Take the device and lean its bottom edge against the wall below the flush mounting box.
5. First connect the green power supply/doorbell connector to the device.
   Connect the LAN connector.
6. Put the cables carefully in the pre-drilled back slot of the device to prevent them from blocking any horizontal levelling movement during the final installation stage.
7. Insert the device in the flush mounting box making sure that it clicks onto the centering pins. The pins allow for a 5–6 ° inclination on either side for accurate horizontal levelling of the device.
   Now the device is ready for basic operation. It is necessary to perform software configuration (p. 58) to achieve a full functionality of the device.

Wall Mounting Box Installation for Device Wall Mounting

2N Sentrio Lobby can be installed using a wall mounting box. The device display slope is 12% in this type of installation. Use the mounting box (Part No. 91378803), which is not included in the package.

TIP

- Download the drilling template from 2N.com.
- Refer to Subs. Component Layout (p. 11) for connector layout.

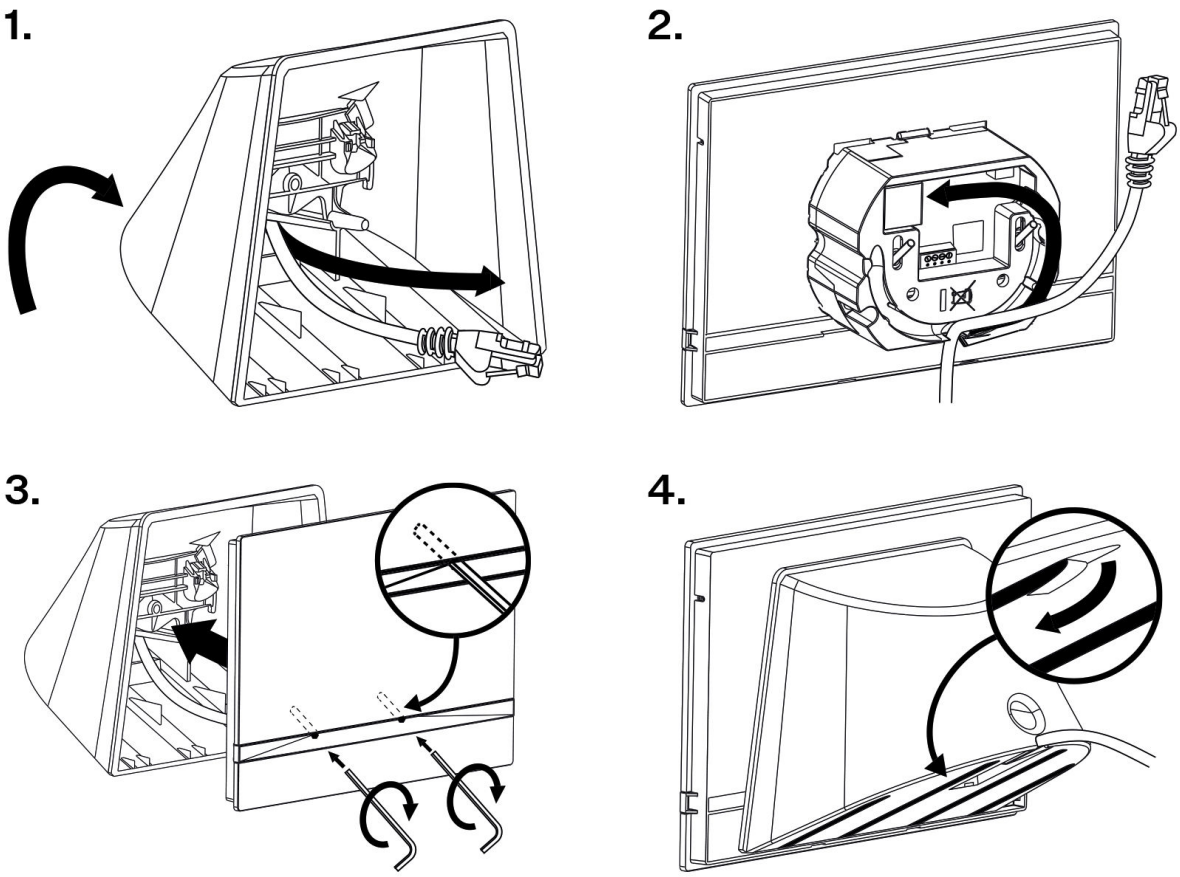


1. Drill holes of the diameter of 8 mm for the dowels and screws (included in the package). It is assumed that all the necessary cables of the maximum length of 25 cm will lead to the place.
2. Fit the wall mounting box into the predrilled holes. Pull the available cables through the box opening. Use a water level for a more precise levelling.
3. First connect the green power supply/doorbell connector to the device.
   Connect the LAN connector.
4. Put the cables carefully in the pre-drilled back slot of the device to prevent them from blocking any horizontal levelling movement during the final installation stage.
5. Fit the device screws into the nuts in the box with the hexagon key wrench provided.
   Now the device is ready for basic operation. It is necessary to perform software configuration (p. 58) to achieve a full functionality of the device.

Stand Installation

Within installation preparations, take out the pre-prepared cabling, UTP cable, doorbell (twin) cable and power supply. Shorten the cables as required. Crimp the RJ-45 connector onto the UTP cable. Connect the doorbell twin cable or power supply into the connector.

TIP
Refer to Subs. Component Layout (p. 11) for connector layout.



1. Pull the cables through the hole in the stand bottom.
2. First connect the green power supply/doorbell connector to the device.
   Connect the LAN connector.
3. Put the cables carefully in the pre-drilled back slot of the device to prevent them from blocking any horizontal levelling movement during the final installation stage.
4. Put the device on the stand making sure that it fits onto the centering pins. The alignment of the stand bottom edge and the device bottom strip means that the device is installed properly. Fit the device to the stand by tightening the screws through the front side. Use a hexagon key wrench for tightening. Tighten the screws gently.
5. Remove the protective foil from the antislip belts on the stand bottom and install the device on a selected place.
   Now the device is ready for basic operation. It is necessary to perform software configuration (p. 58) to achieve a full functionality of the device.

Electric Installation

Power Supply

2N Sentrio can be powered using PoE 802.3af (PoE injector can be used) or an external adapter (10–15 V DC).

The recommended power supply method is connection to the 2N LiftGate Cabin Switch using PoE 802.3af, which ensures data connectivity over 2N LiftGate.

One 2N LiftGate ensures 4-hour operation for two elevators with battery backup power, i.e. for two **2N Sentro Cabin** devices, two 2N Cabin Switch units and two external cameras (if an Axis – P9106-V external camera is used).

Consumption Table

Supply type	Consumption	Polarity reversal protection
PoE, IEEE 802.3af (recommended)	4 W	✓
10–15 V DC adapter	At relax: 4 W Call: 4.3 W	✓

WARNING

- Connection of a defective or improper power supply may lead to a temporary or permanent device failure.
- Higher voltage values or misconnections may result in an irreplaceable device damage.

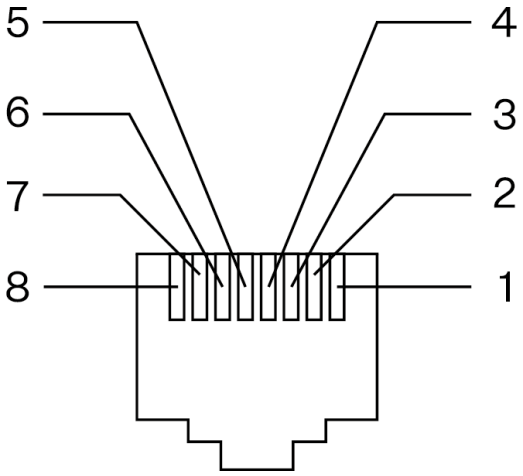
PoE Supply Connection

Use a standard straight RJ-45 terminated cable to connect **2N Sentrio** to the Ethernet. The device supports the 10BaseT and 100BaseT protocols.

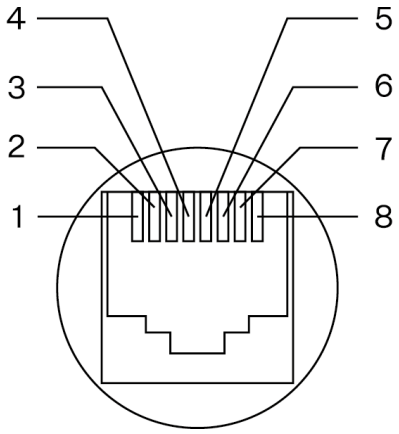
CAUTION

- Factory reset results in a change of the Ethernet interface configuration.
- A defective Ethernet cable may lead to a high packet loss in the Ethernet and subsequent instability and poor call quality.

Ethernet cable connector



Ethernet socket



1. Tx+
2. Tx−
3. Rx+
4. unused
5. unused
6. Rx−
7. unused
8. unused

WARNING
This device cannot be connected directly to telecom lines (or public wireless networks) of any telecom service providers (i.e. mobile providers, landline providers or Internet providers). It is recommended that 2N LiftGate and 2N LiftGate Cabin Switch or a router, if necessary, are used for the product connection to the Internet.

External Power Supply

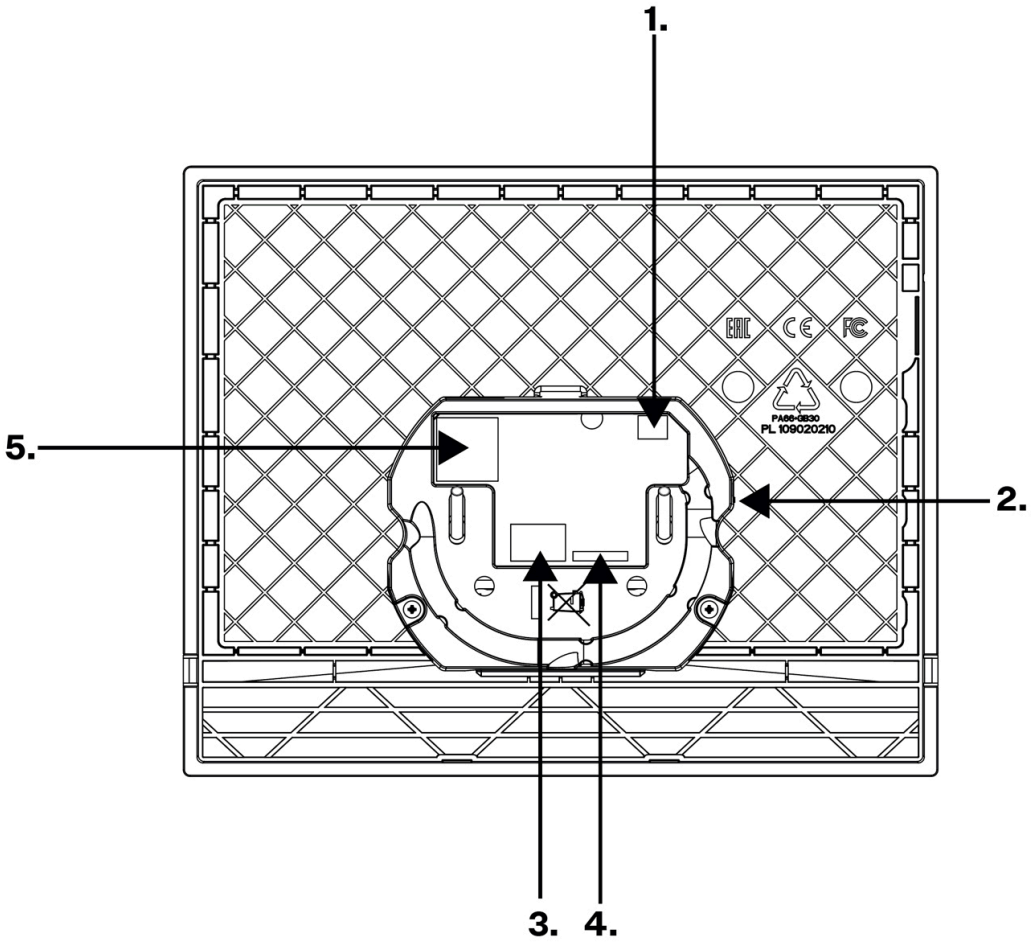
CAUTION

- Make sure that the external power supply meets the power supply class 2 (PS2/LPS) .
- Make sure that the wires are firmly attached to the terminal to avoid any free contact.

Adapter Connection (1341481, 02520-001)

The white wire at the end of the adapter carries the positive charge (+), the black wire carries the negative charge (−).

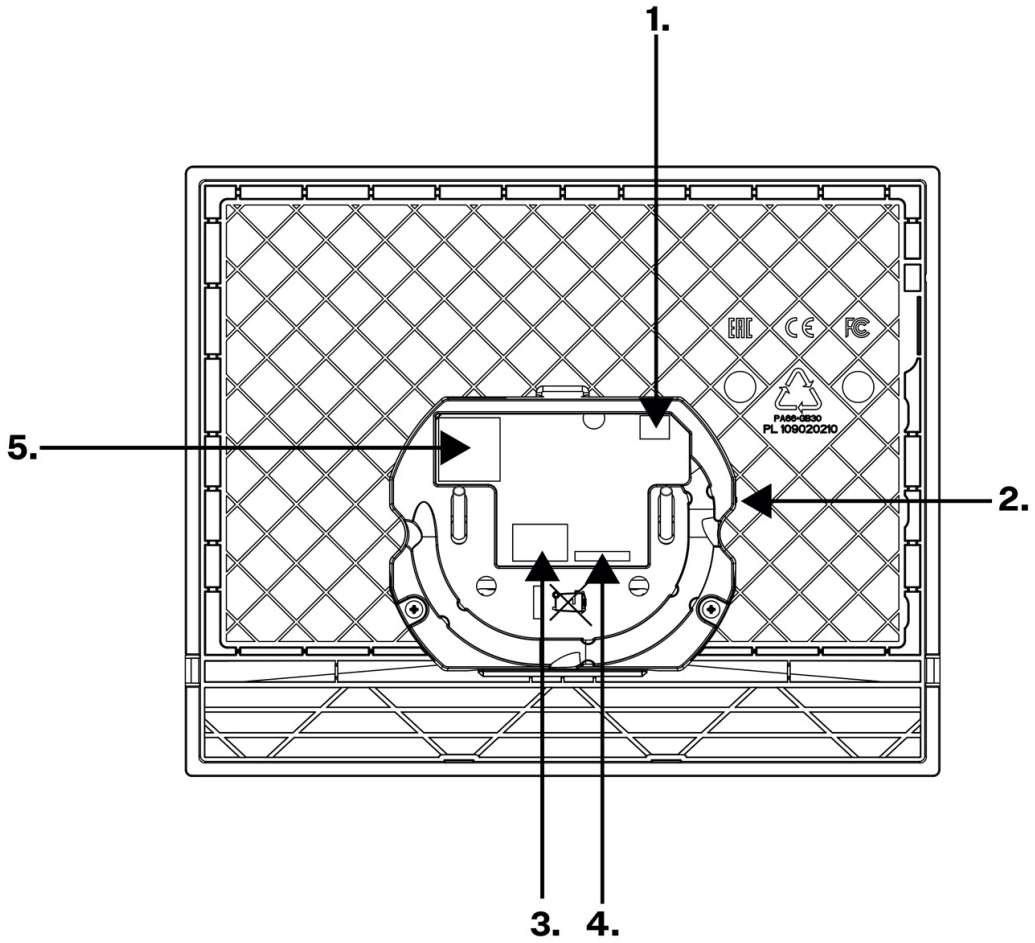
Connectors 2N Sentrio Cabin



Con-nec-tor	Connector name	Description
1	Induction loop	External induction loop output.
2	RESET Button	The RESET button helps you restore the factory default values and restart the device.

Con-nec-tor	Connector name	Description
3	Left-hand connector pair – external power supply input	External adapter (10–15 V DC) input connector. The left contact has a negative polarity (–), the right contact has a positive polarity (+).
	Right-hand connector pair – ALARM2 button	The doorbell button input is used as ALARM2 if the switch is used – accessible only to the operators for alarm call cancellation. **CAUTION** If the switch is not connected to **2N Sentrio**, this connector works as ALARM1 and has to be connected to the elevator cabin external button. Press the button for the predefined period of time to start emergency communication – the alarm call.
4	2N Sentrio Switch	2N Sentrio Switch – main unit interconnection input For the full functionality, the main unit – switch interconnection must be made before the main unit is connected to the power supply from an external source or an Ethernet cable if PoE supply is selected. The switch is interconnected with the **2N Sentrio Cabin** main unit with a 20 cm long eight-wire cable. The main unit feeds the switch using this cable. The main unit does not support more inputs, switch connectors 5–8 helps connect the inputs.
5	LAN Ethernet/PoE	

Connectors 2N Sentrio Lobby



Connector	Connector name	Description
1	Induction loop	External induction loop output.
2	RESET Button	The RESET button helps you restore the factory default values and restart the device.
3	Left-hand connector pair – external power supply input	External adapter (10–15 V DC) input connector. The left contact has a negative polarity (–), the right contact has a positive polarity (+).
	Right pair of connectors – microswitch	Microswitch input. Used for device lock connection. The left contact has a negative polarity (–), the right contact has a positive polarity (+).

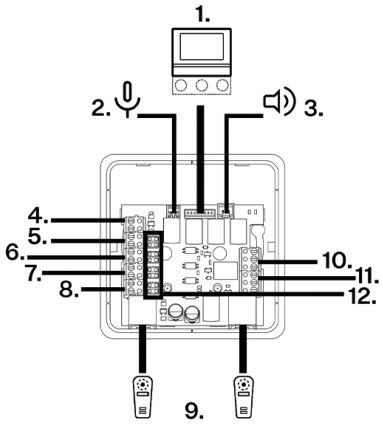
Connector	Connector name	Description
4	Not used	
5	LAN Ethernet/PoE	

Connectors 2N Sentrio Switch

2N Sentrio Switch (Part No. 91378904), for 2N Sentrio Frame 3-button version, has connectors 1, 4–8 and 10–12 connected by factory default.

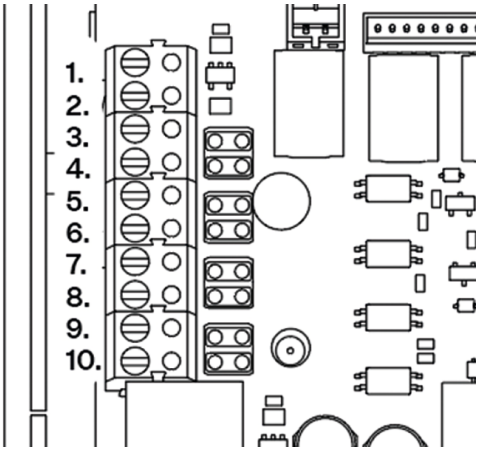
2N Sentrio Switch (Part No. 913789041), for 2N Sentrio Frame external button version, has connectors 1, 5–8 and 10–12 connected by factory default.

Connector Overview



1. **2N Sentrio** Main Unit
2. External Microphone
3. External Speaker
4. LED Button Backlight Power Output
5. Input – ALARM1 button
6. Input – CANCEL
7. Input – YES button
8. Input – NO button
9. Two 2N Voice Alarm Station Intercoms
10. Status Output – RELAY1
11. Status Output – RELAY2
12. Configuration jumpers

Terminal Overview for connectors 4–8



1. Connector 4: +12 V (orange wires, mounted by factory default)
2. Connector 4: GDN (blue wires, mounted by factory default)
3. Connector 5: In1+ (yellow wires, mounted by factory default)
4. Connector 5: In1– (yellow wires, mounted by factory default)
5. Connector 6: In2+
6. Connector 6: In2–
7. Connector 7: In3+ (green wires, mounted by factory default)
8. Connector 7: In3– (green wires, mounted by factory default)
9. Connector 8: In4+ (red wires, mounted by factory default)
10. Connector 8: In4– (red wires, mounted by factory default)

1 2N Sentrio Main Unit

The switch is interconnected with the **2N Sentrio Cabin** main unit with a 20 cm long eight-wire cable. The main unit feeds the switch using this cable. The main unit does not support more inputs, switch connectors 5–8 helps connect the inputs.

2 External Microphone

The external electret microphone connector is especially useful where the 2N Sentrio Cabin unit with an internal microphone is embedded in the elevator wall or the cabin operating panel (COP). If an external microphone is connected, the internal microphone is inoperable.

It is recommended that an external microphone is connected while the device is off. If the microphone is connected during operation, you must restart **2N Sentrio Cabin** to activate it.

3 External Speaker

An external speaker connector (min. 16 Ω / 0.25 W) is suitable whenever the built-in speaker is not sufficiently accessible.

4 LED Button Backlight Power Output

Connector 4 is used for backlighting the LED buttons of connectors 5–8. 12 V / 80 mA DC, see Figure 3: “Connector Overview”.

5–8 External Button and CANCEL Inputs

Up to three external buttons (YES, NO, ALARM1) and one input (CANCEL) can be connected to the switch, see Figure 3: “Connector Overview” . The 2N Sentrio Frame YES, NO and ALARM1 buttons are switchable and backlit.

Inputs 5–8 can be contact or voltage controlled. Use the configuration jumpers for setting. The jumpers are mounted from the factory.

The button is contact controlled.	N/O contact (button/NO relay)	• Both jumpers mounted
	N/C contact	• Both jumpers mounted • The input polarity is reversed in the software configuration – set the reversed button in Hardware > Digital inputs > Input reversal in the web configuration interface.
Voltage control – 10–30 V external voltage (polarity must be observed, galvanically isolated input)	By connecting DC voltage	• Both jumpers unmounted • The input polarity is reversed in the software configuration – set the reversed button in Hardware > Digital inputs > Input reversal in the web configuration interface.
	By disconnecting DC voltage	• Both jumpers unmounted

5 Input – ALARM1 button

ALARM1 input connector.

Press the button for the predefined period of time to start emergency communication – the alarm call.

6 Input – CANCEL

If the ALARM1 delay is set, the CANCEL input can be used for canceling the alarm if activated during the ALARM1 delay interval. The door contact is usually used for activating alarm canceling. When the door is opened, alarm calls are usually no more requested.

7 Input – YES button

Used for connection of the button from 2N Sentrio Frame. It is an optional input, the **2N Sentrio Cabin** touchscreen can be used for sending a response. Alternatively, the elevator cabin panel buttons can be used (door opening/closing button).

8 Input – NO button

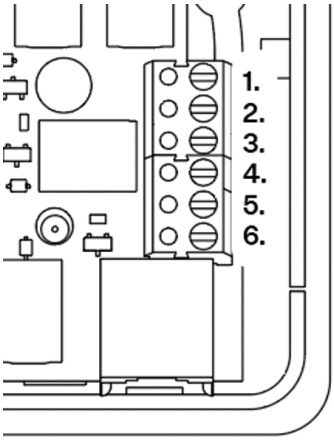
Used for connection of the button from 2N Sentrio Frame. It is an optional input, the **2N Sentrio Cabin** touchscreen can be used for sending a response. Alternatively, the elevator cabin panel buttons can be used (door opening/closing button).

9 Two 2N Voice Alarm Station **Intercoms**

Pre-prepared inputs for connection of 2 2N Voice Alarm Station audio units installed above and below the cabin to the main unit.

10 Status Output – Relay1

Diagram of Status Output 10 and 11 Terminals



A blocking, remotely switchable SPDT-type (single pole, double throw) relay, which signals various error states (typically by sound) and reports device failure states.

The relay is switched on whenever the SIP exchange registration gets lost (registration is necessary for making calls). The error occurs one minute after the last successful re-registration expires (if the SIP registration expiration is set to 120 seconds on the PBX, the error occurs 180 seconds after the last successful registration).

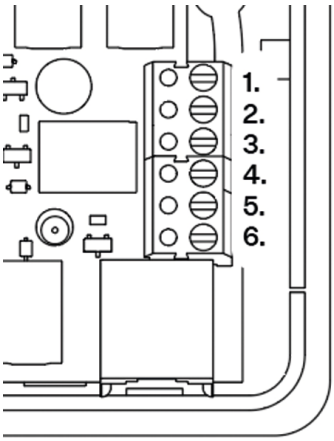
Variable error states can signaled by the relay (such as configuration errors, network disconnection, SIP registration errors or non-functional device).

2 relays whose contacts are brought to separate connectors:

- Terminal 1–2 / 4–5: open at relax (NO)
- Terminal 2–3 / 5–6: closed at relax (NC)

11 Status Output – Relay2

Diagram of Status Output 10 and 11 Terminals



The relay allows for the audible and visual signaling of a telephone line.

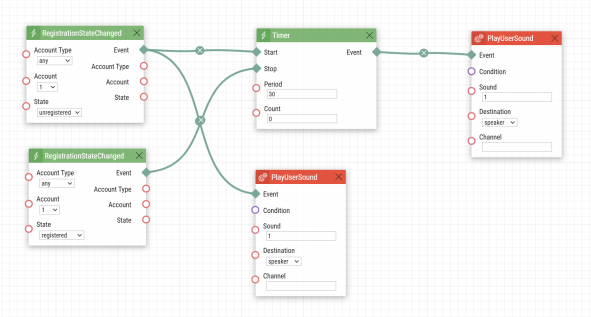
We recommend power from an external source. Alternatively, it can be powered using the 2N LiftGate Cabin Switch.

A user-controlled, remotely switchable SPDT-type (single pole, double throw) relay can be used for Automation in particular, but also for API.

2 relays whose contacts are brought to separate connectors:

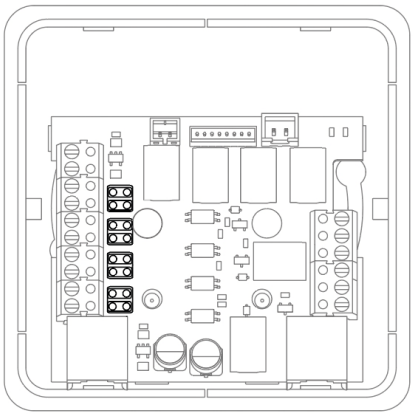
- Terminal 1–2 / 4–5: open at relax (NO)
- Terminal 2–3 / 5–6: closed at relax (NC)

Below is a configuration example using Automation, see Automation (p. 73).



12 Configuration Jumper Location

Jumper Location



Jumper location defines the way of controlling inputs 5–8. The inputs can be contact or voltage controlled, refer to the Table of Inputs 5–8 (p. 26). The jumpers must be mounted for contact control. Use the configuration jumpers for setting, see Figure 7: “Jumper Location”. The jumpers are mounted from the factory.

If a voltage input is required, remove the jumpers.

It is necessary to mount the jumpers horizontally, see the Overview.

Brief Guidelines

Device Configuration Interface Access

2N Sentrio is configured via a web configuration interface. You have to know the device IP address or the device domain name. Make sure that the device is connected to the local IP network and powered.

Domain Name

Enter the device domain name as “hostname.local” to connect to the device. The hostname of a new device consists of the device name and serial number. Enter the serial number into the domain name without dashes. Change the hostname anytime in **System > Network**.

Default domain name 2N Sentrio: 2NSentrioCabin/2NSentrioLobby-{serial number without dashes}.local (e.g.: “2NSentrioCabin/2NSentrioLobby-0000000001.local”)

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.

Web Configuration Interface Login

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

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

For increased password security, it is recommended that:

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

Recommended browsers

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

IP Address Retrieval

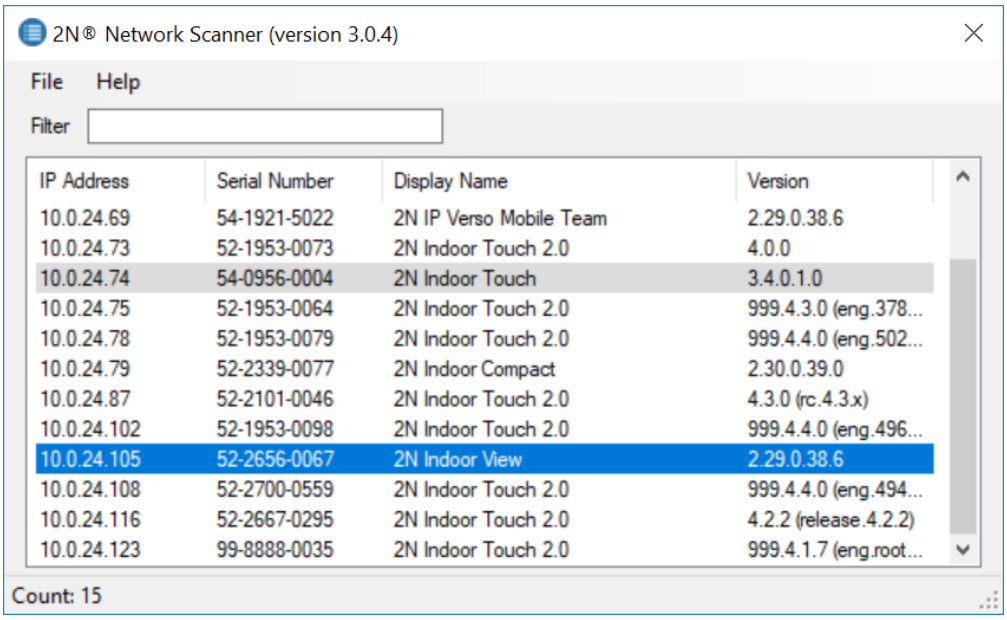
To retrieve the device IP address, take the following steps:

- Use the freely accessible 2N IP Utility.
- Display information on the device display.

IP Address Retrieval Using 2N Network Scanner

The application helps you find the IP addresses of all the 2N devices in the LAN. Download 2N Network Scanner from the 2N.com website. 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.
3. Having installed 2N Network Scanner, start the application using the Microsoft Windows Start menu.
   Once started, the application begins to automatically search the LAN for all the 2N devices which have been DHCP/statically assigned IP addresses. These devices are then shown in a table.



4. Select the device to be configured and right-click it. Select*Browse...* to open the device administration web interface login box for configuration.

CAUTION
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.

TIP
- Double click the selected row in the 2N Network Scanner list to access the device web interface easily.
- To change the device IP address, select *Config* and enter the required static IP address or activate DHCP.

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

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

For increased password security, it is recommended that:

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

IP Address Retrieval using Device Display

2N Sentrio Cabin

To display the IP address on the device display, you must start the Hidden Menu:

1. Wait until the end of the introductory animation on the display after starting/restarting the device.
2. The moment the home screen appears (after approx. 20 s), place your finger in the left-hand upper corner of the display for approx. 5 s.

The IP address of the device will be shown in the Hidden menu. The menu contains the network mask, default gateway address and DHCP switch among others.

If the address is 0.0.0.0, then the device did not get the IP address from the DHCP server and the static IP address (DHCP OFF) has to be used. If DHCP OFF is set, the device static address is 192.168.1.100.

The DHCP mode switch resets all the **System > Network** parameters in the web configuration interface to defaults.

2N Sentrio Lobby

1. From the Dashboard, go to settings .
2. Find the IP address information in the About device section.

Static/Dynamic IP Address Switching on Display

The DHCP mode switch resets all the **System > Network** parameters in the web configuration interface to defaults.

If the address is 0.0.0.0, then the device did not get the IP address from the DHCP server and the static IP address (DHCP OFF) has to be used. If DHCP OFF is set, the device static address is 192.168.1.100.

2N Sentrio Cabin:

To switch the DHCP on the device display, you must start the Hidden Menu:

1. Wait until the end of the introductory animation on the display after starting/restarting the device.
2. The moment the home screen appears (after approx. 20 s), place your finger in the left-hand upper corner of the display for approx. 5 s.

The IP address of the device will be shown in the Hidden menu. The menu contains the network mask, default gateway address and DHCP switch among others.

2N Sentrio Lobby:

1. From the Dashboard, go to settings .

2. Go to **Advanced Settings > Network Settings**.
   Enter a code to access the Advanced settings. Set the Advanced settings access code in the web configuration interface (Hardware > Display > Advanced settings code > Advanced settings code).
3. Activate/deactivate the option **Use a DHCP server**.

Firmware Update

We recommend that the firmware is also updated during the **2N Sentrio** installation. Refer to 2N.com for the latest FW version.

Once the firmware is uploaded successfully, the device is restarted automatically.

TIP
You can make bulk updates for multiple devices via 2N Elevator Center.

Device Restart

To restart the device choose one of the following options:

- using the RESET button,
- via the web configuration interface.

NOTE
The device restart does not result in any change in the configuration settings.

Restart Using RESET Button

Find the RESET button on the device backside (p. 11).

Press the button shortly (< 1 s) to restart the system without changing configuration.

Restart Using Web Configuration Interface

You can restart the device via the web configuration interface. Refer to Web Configuration Interface Login (p. 29) for login details. Restart the device in System > Maintenance (p. 89) > System using Restart device.

The Home screen is displayed after restart. Restarting may take a rather long time after the button press.

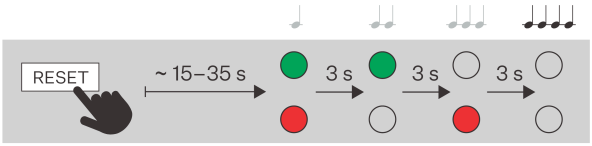
Factory Default Reset with RESET Button

Reset the device factory default values via software in System > Maintenance (p. 89)> Default reset.

Follow the instructions below **2N Sentrio** to reset the factory default values via hardware:

Factory Default Reset with RESET Button

1. Press the button RESET and keep it pressed.
   a. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard (approx. 15–35 s).
   b. Wait until the red LED goes off and an acoustic signal can be heard (approx. for another 3 s).
   c. Wait until the green LED goes off and the red LED goes on again and an acoustic signal can be heard (approx. for another 3 s).
   d. Wait until the red LED goes off and the acoustic signal can be heard (approx. for another 3 s).
2. Release the RESET button.



2N Sentrio Cabin Basic Settings

For the basic setting of **2N Sentrio Cabin**, it is necessary to set the following parameters in the web configuration interface. Having changed or set the parameters, always press Save in the right-hand lower corner for confirmation.

TIP
Make sure in **System > Maintenance** that you are using the latest FW version.

1. Press Add user in the **Directory** section to add a user representing the phone contact to the Call Center to which **2N Sentrio Cabin** is to be connected. For direct SIP calling enter the destination phone number in the format “sip:[user_id@]domain[:port]”.
   Confirmation Mode – define how to confirm a call setup (Press 1, Pick up, Protocol autodetection, CPC Antenna, CPC Antenna Ext, CPC KONE, P100).
2. Select the user in the Directory in **Calls > Alarm call > Alarm call > Destination** with whom the device shall connect during alarm calls.
   Repetition Count – set the count of call cycles in case the call is not confirmed/picked up. The default cycle count is 3, the maximum value is 9. When the set call cycle count has been accomplished and the call has not been picked up, the call is ended automatically.
3. The default maximum alarm call time is 600 s. To define another value, set the call limit after which the call shall be automatically ended in **Calls > General settings > General settings > Maximum call time**. The device beeps 10 s before the call ends to signal that the call end is approaching. Enter any DTMF character into the call (# on your IP phone, e.g.) to extend the call time. The maximum call duration is 3600 s.
   Ending a call does not automatically end the alarm call status.
4. Enable the SIP account in **Calls > SIP 1 > Configuration**. Then set 2000 kbps for the maximum video transmission quality in **Calls > SIP 1 > Video > Bitrate**.

5. The default minimum ALARM1 press time for an alarm call to be started is 3 s. To define another value, set the minimum time for which it is necessary to press the ALARM1 button to start an alarm call in the **Press Time for Activation** parameter in **Calls > Alarm call > Alarm call > Basic settings**.
   If the CANCEL button is active, enable **Delayed Call** and set the time for the alarm call delay after the ALARM1 button is activated. If the CANCEL button is activated or the relay is activated due to door opening within this timeout, the alarm call start will be automatically cancelled. The typical value is the elevator travel time from the lowest to the highest floor. Do not set this parameter to a value lower than the **Press Time for Activation** parameter.
6. Add the **Lift ID** in **Services > Lift > General settings** – the lift/lift intercom ID to be sent or read in calls. The identification number has to consist of 16 digits at most. Select the device location in the **Product Location** parameter.
7. Select **Monitoring Mode** in **Services > Lift > Cabin monitoring**. The selected mode defines when it is possible to view the elevator cabin via an external camera and when the elevator cabin audio can be recorded.
8. Enable the RTSP server in **Services > Streaming > RTSP**. Make sure that **Audio Streaming Enable** and **Video Streaming Enable** are selected in **Services > Streaming > RTSP > Streaming settings** to make the device work properly. Now enter the **Local Stream URL**. To generate the URL, click the  icon and set **Bitrate** to 2000 kbps (or the value set in step 4). The other parameters need not be edited. Now press Use URL to confirm the URL.
9. Remember to set a name and password in **Services > Streaming > RTSP > User accounts** for the external cameras using the 2N OS web configuration interface. Subsequently, complete the same name and password in **Hardware > External camera > External IP camera** in the **2N Sentrio Cabin** web configuration interface.
10. Enable the external camera in **Hardware > External camera**. Now enter the **TRTSP Stream Address** manually – “rtsp://camera_ip_address/parameters”, e.g. “rtsp://10.0.24.11/h264_stream”. The IP address can contain the port number behind the colon, parameter means the camera codec for this purpose.
11. **For EU version:** Enable the Rescue mode in **Services > Lift > Rescue mode**. **This step is necessary so that the EU legislation can be met.** The device allows the Rescue mode to be active after activation, during which multiple alarm calls can be made. This facilitates displaying multiple alarm calls in Elevator Center within one rescue mode and returning to chats.
    For US version: Make sure that the Rescue mode is disabled in **Services > Lift > Rescue mode**. **This step is necessary so that the US legislation can be met.** Every alarm call will be logged as a new entry in Elevator Center.
    The Rescue Mode Enable is set to Off by default.
12. Set the required languages for the device in **Hardware > Display**. **Language** defines the basic language of the device. **Language Selection** displays languages for the users to choose. The field must contain a list of the comma-separated ISO 639-1 language codes in a sequence offered for selection. The first 9 languages are offered to the user at most.

2N Sentrio Lobby – Elevator Cabin Connection

The following subsection describes how to set up a connection with the **2N Sentrio Cabin** unit located in the elevator cabin. The same procedure applies to connecting all of the 2N IP emergency communicators. However, the text messaging feature is only available between **2N Sentrio Lobby** and **2N Sentrio Cabin**.

To ensure connection, you need to set the service on both devices through which communication will take place - either local calls for connection in the local network or a SIP account. Next, you need to add the emergency communicator to the **2N Sentrio Lobby** directory.

Local Area Network Communication Settings

Do the following in the web configuration interface of both the devices:

1. Go to **Calls > Local calls**.
2. Allow **Local calls**.
3. Set the same value for the **Access Key** on both the devices.
   With this setting, the devices will be visible to each other in the LAN and can be added to the directory address book directly from the **2N Sentrio Lobby** display.

SIP Communication Settings

SIP Account Enable

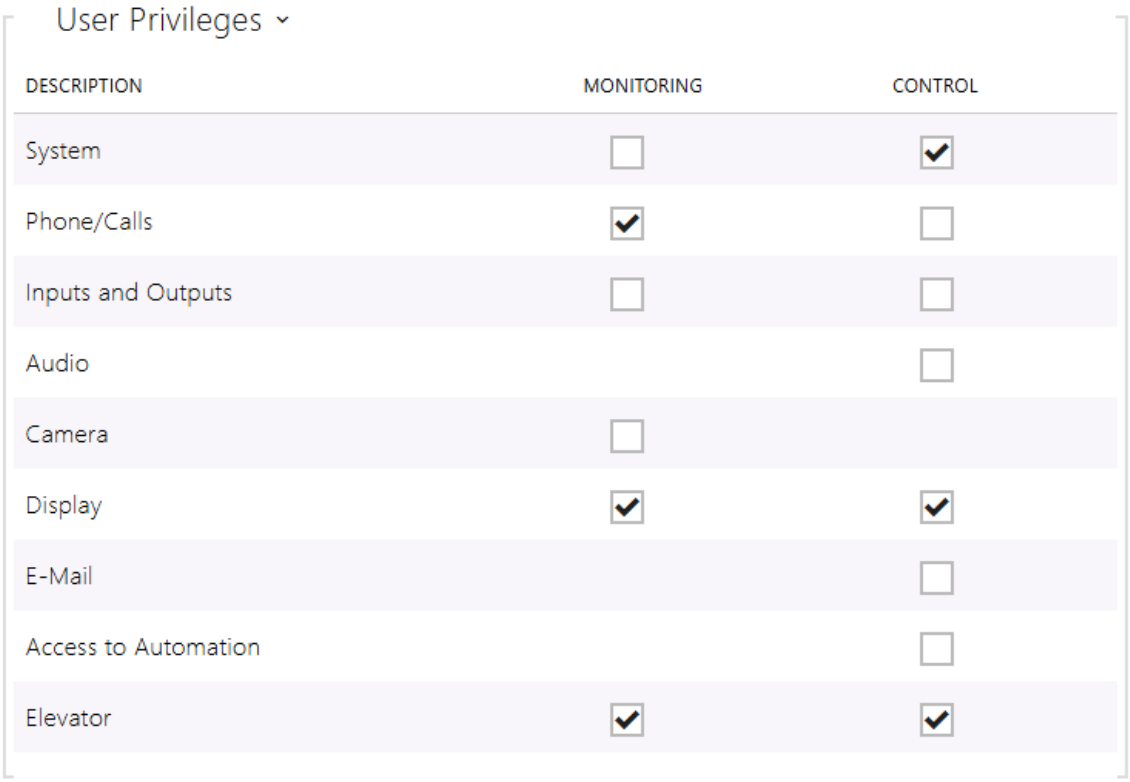
Do the following in the web configuration interface of both the devices:

1. Go to **Calling > SIP** (select one of the SIP accounts for the communication).
2. Enable the SIP account.

HTTP API Account Setup for 2N Sentrio Cabin

Enable data transfer in the **2N Sentrio Cabin** web configuration interface:

1. Go to **Services > HTTP API**.
2. Make sure the following services are enabled: System API, Logging API, Display API (if available), Elevator API.
3. Set **User name** and **Password** in one of the **Account** tabs to be entered into **2N Sentrio Lobby**.
4. Enable the following in your Account **User rights**, see the figure below:
   - Monitoring – Phone/Calls, Display (if available), Elevator
   - Control – System, Display (if available), Lift



Adding Communicator to 2N Sentrio Lobby Directory:

In web configuration interface:

Do the following in the **2N Sentrio Lobby** web configuration interface:

1. Go to **Directory > Users**.

2. **a.** For connection via Local calls:
   Click Find device above the table. Check the listed device that you want to establish connection to. Once the device is added, editing becomes available.
   b. For connection via SIP:
   i. Click Add user. The contact editing box will open.
   ii. Click the pencil icon next to the Phone number to open phone number editing.
   Enter the elevator communicator destination IP address / SIP URI into the Destination field.
   iii. Fill in the HTTP API account username and password for **2N Sentrio Cabin**.
3. Name the new contact to improve identification.

Using 2N Sentrio Lobby display:

NOTE
Only those elevator communicators that are in the same LAN as **2N Sentrio Cabin** can be added from the device display.

1. Open **Settings> Advanced settings** on the **2N Sentrio Lobby** display.
2. Enter the advanced settings code.
   Enter a code to access the Advanced settings. Set the Advanced settings access code in the web configuration interface (Hardware > Display > Advanced settings code > Advanced settings code).
3. Open the **Elevator Management** section.
   A list of elevator communicators visible on the local network will be displayed.
4. Use to add the selected device.
5. After adding the device, you can open its editing and set the device name (for example, specify the elevator in which it is located).

2N Elevator Center **Basic Configuration**

The 2N Elevator Center cloud solution helps users audio/video/chat communicate with **2N Sentrio** during the alarm call. It also enables users to configure the device remotely – set the communication messages to be displayed on the device during alarm calls with the call center, e.g., including language mutations. Refer to the on-line **2N Sentrio** Configuration Manual for more 2N Elevator Center configuration details.

The cloud solution can be used in the modes according to the type of users that will use the solution:

- Lift company – standard display of the 2N Elevator Center cloud environment
- Call Center company – simplified cloud environment focused on the operation of alarm calls

Lift Company **Configuration Options**

The Lift company can add devices, allow access of the Call Center company to selected devices in 2N Elevator Center.

It is necessary to apply for access to the 2N Elevator Center cloud solution via the 2N business contact. Subsequently, the Company Admin account will be created for the company, which can create and manage accounts for the company.

With the account created, add the device to the system.

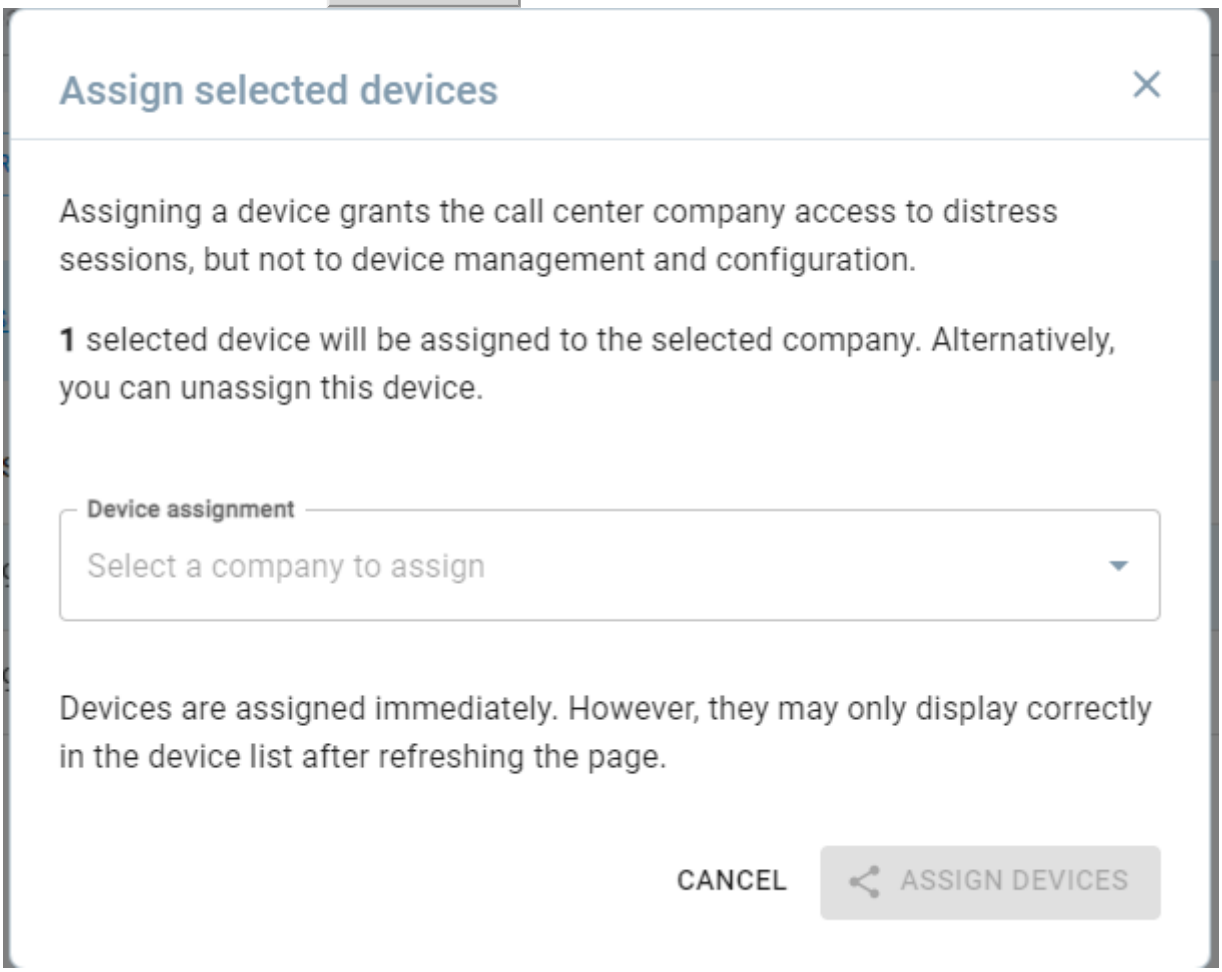
Adding the device to 2N Elevator Center**:**

1. Click Add device.

2. Complete the device name, location in the node if necessary, production number and My2N Security Key (available on the product or product package).
3. Press Add device for confirmation.

Allowing access to the device for the Call Center company**:**

1. Tick off the device for which access shall be allowed.
2. Once the device is selected, the Simple bulk edit button is displayed for you to choose Assign devices.
3. A box will be displayed for you to choose one Call Center company (you can choose multiple devices, but just 1 company). Press Assign devices for confirmation.



Remove the added devices for the Call center company on the device card.

2N Sentrio Cabin Device Control

2N Sentrio can be controlled as follows:

- using frame buttons – for the 2N Sentrio Frame 3-button version
- using external buttons – the elevator cabin buttons can be connected to any elevator panel buttons via 2N Sentrio Switch for external buttons (the door opening/closing buttons and the alarm button are recommended)
- using display – the display touch function is active by default

2N Sentrio is equipped with a touch display for intuitive control.

Device Buttons

It is recommended that **2N Sentrio Cabin** is combined with the 2N Sentrio Frame 3-button version used for:

- / – EU/US alarm button
  Press the button for the predefined period of time to start emergency communication – the alarm call.
- – YES button
  Primarily, the button is used for sending positive responses to the text communication with the Call Center. Another function of the button is the confirmation of the selected menu item.
- – NO button
  Primarily, the button is used for sending negative responses to the text communication with the Call Center. Another function of the button is the navigation through the menu items.

Alternatively, the elevator cabin panel buttons can be used (door opening/closing button). These inputs are optional, the touch screen buttons can be used.

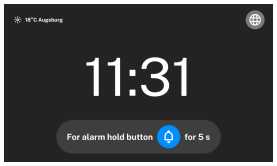
Home Screen

The Home screen helps you start alarm calls and change the device language.

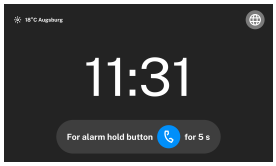
Also, the Home screen shows the current time (set the format in the web configuration interface), temperature and location (if available).

The Home screen allows you to display the background picture (as set in **Hardware > Display > Basic settings** in the web configuration interface). With this display, the time info is moved to the upper bar of the display.

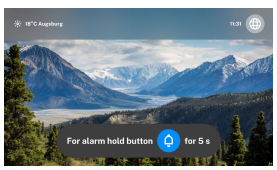
EU version



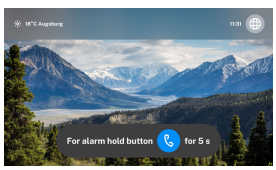
US version



EU version



US version



CAUTION
Common image format types (jpeg, gif, png, bmp, webp) are supported. If the image is in png format, the image format is preserved to preserve any transparent background. If the image is in another format, it is transparently converted to the jpeg format, i.e. it will not have a transparent background (if the uploaded image is in bmp format, the resulting image may have blurred edges, etc.).

To be uploaded, the background image must meet the following requirements:

- The image must have a resolution of at least 1024 x 600 (neither side can be smaller).
  - If the image is larger, it will shrink to exactly that resolution. If it is larger and has a different shape, it is trimmed and made smaller, see the description below.
- The maximum file size is 2 MB.

Make sure that the background picture resolution is 1024 x 600 pixels at least. Images with higher resolutions will be reduced in size.

Automatic cropping and image resizing is governed by the following:

- The image is cropped so that it does not distort.
- The image is cropped to fully fill 1024 x 600 px.
- The image is cropped and resized to keep as much of the original image as possible.

Possible actions	Performance	Action result
Alarm Call Initialization	**EU version** Long press of **US version** Long press of **TIP** Set the required button press time in **Calls > Alarm Call > Basic settings > Press Time for Activation** in the web configuration interface.	The press time countdown after activation appears. The device signals call setup with the Call Center after the alarm call is initialized. Refer to Alarm Call (p. 42) for details.
Language Selection Menu Opening		The device displays all the available languages.

Language Selection

Touch the device to open the language selection menu.

The menu is also opened whenever an alarm call is initialized.

Set the required languages for the device in **Hardware > Display**. **Language** defines the basic language of the device. **Language Selection** displays languages for the users to choose. The field must contain a list of the comma-separated ISO 639-1 language codes in a sequence offered for selection. The first 9 languages are offered to the user at most.

NOTE
The device returns to the basic language after going into the Idle mode.

TIP
The following languages supported by the device can be selected:

- English
- Czech
- German
- Italian
- French
- Spanish
- Russian
- Suomi
- Finnish
- Polish
- Dutch
- Portuguese
- Turkish
- Norwegian
- Swedish
- Hungarian
- Custom

Possible actions	Performance	Action result
Language Selection Menu Opening	🌐	The device displays all the available languages.
Language Confirmation	Press the selected language on the display or ✓ (or the external button substituting ✓).	The device switches the displayed language into the selected one.

Possible actions	Performance	Action result
Return to Home screen	⊗ or when 60 s pass	The selection is cancelled and the menu actions are terminated without saving.

Alarm Call

The alarm call is an emergency call from the elevator cabin. Whenever an alarm call is initialized, the connected Call Center is contacted and its operators can receive the alarm call.

During the alarm call, a voice call between **2N Sentrio Cabin** and the Call Center, external IP camera transmission (camera transmission from the Call Center to **2N Sentrio Cabin** is also possible) and text communication intended primarily for the deaf people are initialized.

It is impossible for the Call Center to contact the elevator cabin without alarm call initialization from **2N Sentrio Cabin**.

Possible actions	Performance		Action result
Alarm Call Initialization	**EU version** Long press of 🔔	**US version** Long press of 📞	The press time countdown after activation appears. The device signals call setup with the Call Center after the alarm call is initialized. Refer to Alarm Call (p. 42) for details.

> **TIP**
> Set the required button press time in **Calls > Alarm Call > Basic settings > Press Time for Activation** in the web configuration interface.

The alarm call has the following stages:

- Alarm call initialization
- Alarm call in progress
- Text communication during alarm call
- Home screen after alarm call end

Alarm call stages	EU version	US version
Alarm call initialization	• – signaling of alarm call initialization and rescue mode start	• – signaling of alarm call setup
Alarm call in progress	• – signaling of rescue mode in progress • – signaling of alarm call in progress The icons start flashing to signal that the alarm call has failed.	• flashing – signaling of alarm call initialization

Text communication during alarm call	• – signaling of rescue mode in progress
	• – signaling of alarm call in progress
	The Call Center operator can use a text for the communication with the elevator users during an alarm call. This type of communication facilitates communication with the hearing impaired persons.
	The operator can communicate as follows:
	• using declarative sentences
	• using Yes/No questions The elevator user can answer as follows:
	  • using the buttons of 2N Sentrio Frame /
	  • using the external buttons of the elevator panel, which substitute the frame buttons
	  • using the device display buttons
		• flashing – signaling of alarm call initialization

Alarm call stages	EU version	US version
Home screen after alarm call end	After the alarm call is ended, the Rescue mode is still in progress (unless terminated). It is possible to make more alarm calls within one Rescue mode. • – signaling of rescue mode in progress The symbol disappears after the Rescue mode is ended (p. 45).	Signaling disappears. Another alarm call can be made. **TIP** The time during which an alternative wording of the status message mentioning another alarm call can be set in the web configuration interface and disappears after the defined timeout. Subsequently, the device displays the Home screen.

CAUTION
Exceptionally, the device cannot establish connection. The device shows this information while attempting to initialize an alarm call.

Device User Settings

To facilitate user orientation, it is recommended that the button shapes on the device display correspond to the elevator panel buttons as much as possible. It is possible to select the following in **Hardware > Display > Buttons** in the web configuration interface:

- button shape – circle or square.
- right button icon – check mark, close door or door open
- left button icon – cross, close door or door open

The default solution setting for the buttons is:

- button shape – circle
- right button icon – check mark
- left button icon – cross

How To End Rescue Mode

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

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

Set the way of ending the Rescue mode in **Services > Lift > Rescue mode** in the web configuration interface. The Rescue mode can be ended as follows:

- **using ALARM2 button** – if the switch is used, the ALARM2 button is located on the main unit, see Connectors 2N Sentrio Cabin (p. 22)
- **by entering the password on the display**
  1. Hold your finger for approximately 5 seconds in the middle of the **2N Sentrio Cabin** main unit screen upper edge to open the Secret menu.
  2. Enter and confirm the password.
- **by entering the password via DTMF** – the password is sent to the device as DTMF into the device and may contain digits only (up to 16). The password is entered into DTMF in the format “*password*”. For example, if the password is 12345, enter “*12345*” in the call.

2N Sentrio Lobby Control

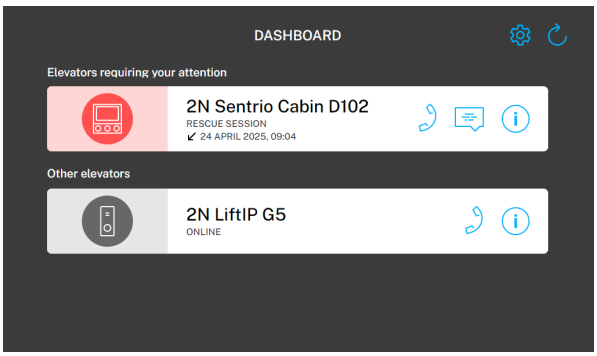
2N Sentrio is equipped with a touch display for intuitive control.

The device is designed to remain locked until needed.

Dashboard

The dashboard is the default device home page, which appears immediately after unlocking (waking up) of the device. It is used as the main navigation point of the user interface.

The dashboard displays a list of all emergency communicators connected. The communicators that require attention are automatically moved to the top of the list. The list also shows the time of the last call made on the communicator.



Highlighting Communicators Requiring Attention

Red color – the elevator is in emergency or rescue mode

Orange color – the communicator reports an error

Possible actions	Performance	Action result
Settings Menu Display		Settings (p. 50) is displayed on the device.
Call Start	 An orange circle indicates that a call is currently in progress on the device.	The communicator automatically answers and connects the call. If another call is in progress on the communicator, you will be asked if you want to end the current call before connecting.

Possible actions	Performance	Action result
Text Message Sending		A selection of preset messages is displayed. You can also type a message of your own. The text of the message itself is not translated. The  icons indicate whether it is an information message or a question.
Viewing Device Status Details	Row clicks	All the attention requiring reasons are displayed: • Emergency state • Rescue mode • Configuration error detected • Audio error detected • Button malfunction detected
Viewing Communicator Information		The detail shows additional information on the device: connection status, firmware version, MAC address, serial number In the detail, the device can be located using  . When a device is located, a sound or visual signal is triggered to help identify the hardware.
Device List Update		The device list and device statuses are updated continuously. This action will perform a manual update.

Call

2N Sentrio Lobby activates the highest priority call.

Possible actions	Performance	Action result
Call Start	 An orange circle indicates that a call is currently in progress on the device.	The communicator automatically answers and connects the call. If another call is in progress on the communicator, you will be asked if you want to end the current call before connecting.

Possible actions	Performance	Action result
Text Message Sending		A selection of preset messages is displayed. You can also type a message of your own. The text of the message itself is not translated. The ⓘ/? icons indicate whether it is an information message or a question. → Sending Text Messages from 2N Sentrio Lobby (p. 48)
End of Call		The call is ended. The text message sent to **2N Sentrio Cabin** will continue to appear on the display.
Extending Active Call		The communicator has a defined call duration. This action extends the current call, thus delaying its automatic termination. The call cannot be extended beyond the maximum call time set for **2N Sentrio Lobby** (**Calling > General settings**).

Sending Text Messages from 2N Sentrio Lobby

In addition to voice transmission, the **2N Sentrio** solution provides text message transmission. Messages in different language versions are preset in **2N Sentrio Lobby**. Having been sent, the message will automatically appear on the target **2N Sentrio Cabin** device in the language set on this device. Thanks to this function, the persons at **2N Sentrio Cabin** in the elevator cabin can communicate in their preferred language even if **2N Sentrio Lobby** uses another language.

In addition to using preset messages, **2N Sentrio Lobby** allows you to write and send messages of your own. Custom messages appear on the **2N Sentrio Cabin** display as they were written. They are not automatically translated. It is possible to create informational messages or Yes/No questions.

Text Messaging

Messages can only be sent between the **2N Sentrio** devices that are connected either through local calls or through an HTTP API sending account. If you have set up the connection according to Subs. **2N Sentrio Lobby** – Elevator Cabin Connection (p. 35), text messaging is ready.

1. If text messaging is available, the  icon will be displayed at the device.
2. Click  to display the preset message list. Click the message to be sent.
   You can also type a message of your own. The text of the message itself is not translated.
   The ⓘ/? icons indicate whether it is an information message or a question.
3. Confirm the message sending in the dialog box.
4. The answer to the submitted question will appear in the same dialog box.

After the dialog box is closed, you can delete the sent message by clicking in the right-hand upper corner of the text message menu.

Changing Preset Messages

Edit the text of the preset messages and their language versions **2N Sentrio Lobby** web configuration interface.

1. Go to **Services > Text messages**.
2. Download **Original text**.
3. Make the desired changes in the downloaded file. The language abbreviations are in the standardized ISO 639-1 format.
4. Upload the saved file back as **User text**.

Technician Arrival Information Message (TechnicianArrival)

If any elevators are in the emergency / rescue mode after unlocking the device, the option to send a technician arrival message (TechnicianArrival) will appear. You need to confirm sending the message. The message is then sent to the devices of all the elevators that are in the emergency / rescue mode.

Edit the relevant lines in the preset message file, see above, to change the wording of the TechnicianArrival message.

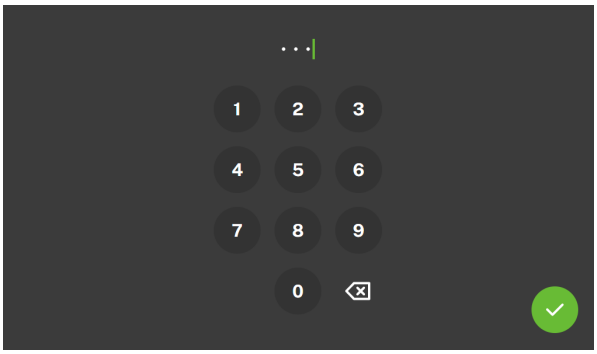
Device Lock

The device is intended for use in emergency situations only. To prevent accidental or unauthorized use, it is recommended that the device is locked.

Possible ways to unlock your device:

- **Entering the unlock code**
  The code is set in the web configuration interface: **Hardware > Display > Unlock device with code**.
- **Using external input**
  The device can be locked via an external switch interconnected with the **2N Sentrio Lobby** hardware. It can be a button, a switch, an electric key knob, etc.

Device Unlocking with Code



NOTE
If any elevators are in the emergency / rescue mode after unlocking the device, the option to send a technician arrival message (TechnicianArrival) will appear. You need to confirm sending the message. The message is then sent to the devices of all the elevators that are in the emergency / rescue mode.

Possible actions	Performance	Action result
Unlocking device with a code	Wake up the display, enter the code and confirm.	The device is unlocked and you can go to other operational statuses and perform other actions. After three incorrect code entering attempts, you must wait 60 seconds before trying again.
Device Unlocking with Input	Activate external input	The device is unlocked and you can go to other operational statuses and perform other actions.

Device unlock settings

Set the device unlocking activation and method in the **2N Sentrio Lobby** web configuration interface.

Unlocking with input

1. Connect the external input to the connector on the **2N Sentrio Lobby** backside, see Component Layout (p. 11).
2. Go to **Hardware > Display**.
3. Enable **Unlock device with input**.
   By default, the device is locked, the device unlocks when the input is switched on. If you want to choose the opposite logic, enable **Inverted unlock input** in **Hardware > Digital inputs**.

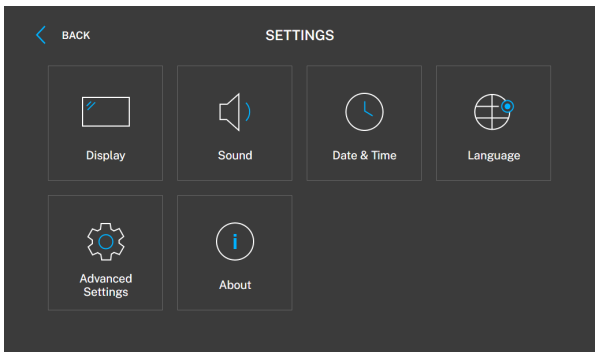
Setting Access Code

1. Go to **Hardware > Display**.
2. Enable **Unlock device with code**.
3. Set the numeric code in **Unlock code** to be entered on the **2N Sentrio Lobby** display.

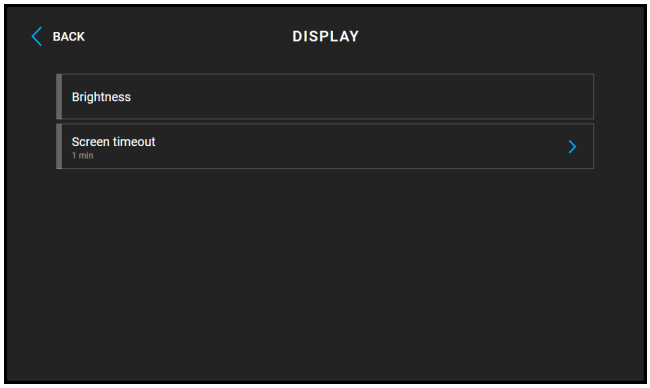
NOTE
If both the unlocking methods are active, you can use any of them to unlock your device.

Settings

Press the ⚙ button on the home screen to display the Device Settings section. The Settings menu helps you set the device locally.



Display



Brightness – sets the value of display backlighting.

Screen timeout – timeout after which the device automatically goes into Sleep Mode if there is no activity.

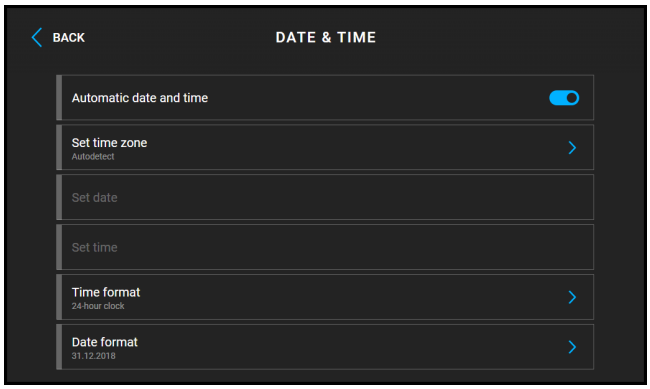
Sound

Ringtone Volume – set the incoming call ringtone volume.

Call Volume – set the phone call volume.

Ringtone – sets the ringtone for incoming calls on the device.

Date and Time



Automatic date and time – activates a mode in which the date and time will be taken from the network.

Set Time Zone – set the time zone for your installation site to define time shifts and summer/winter time transitions.

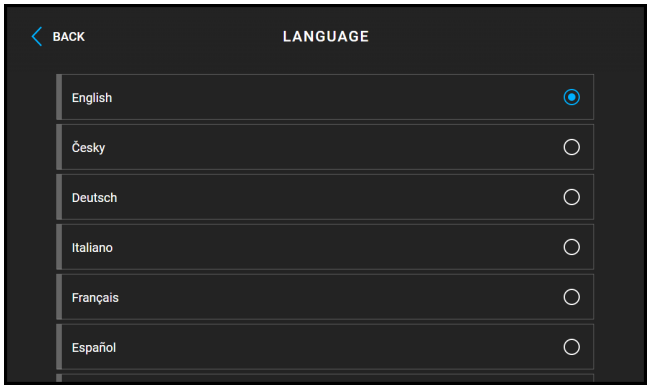
Set date – used to set the date manually.

Set time – used to set time manually.

Time Format – set the time format to be displayed.

Date Format – set the date format to be displayed.

Language



Language – set the language for the texts to be displayed. Choose one of the eight pre-defined languages.

Custom Language – set the language for the texts to be displayed from an uploaded language file of the user localization.

Advanced Settings

Set the code for accessing advanced settings in the web configuration interface (Hardware > Display > Advanced Settings Code > Advanced Settings Code).

Network Settings

NOTE
You can also make network settings in the web configuration interface in **System > Network**.

General

- **Use DHCP Server** – enable automatic obtaining of the IP address from the LAN DHCP server. If the DHCP server is unavailable or otherwise inaccessible in your LAN, use the manual network settings.
- **Static IP Address setting** – set the static IP address, network mask and default gateway. The parameters are used if the Use DHCP Server parameter is disabled.
- **Required Port Mode** – set the LAN port mode to be preferred (Automatic or Half Duplex – 10 Mbps). The bit rate is reduced to 10 Mbps in case the available LAN cabling is unreliable for a 100 Mbps traffic.

Elevator Management

This section displays a list of all the 2N elevator communicators visible in the local network. The devices that have already been added appear at the top of the list.

- – add device from the list
- – display device information and setting options for selected device parameters, see below
- – reload the list
- – add device by entering network parameters

- **Device Parameters**
  -  – locate device
  -  – remove device from the directory
  - **Device Name** – device identification in the directory
  - **SIP URL** – address of the called destination
  - **User Name** (unavailable in the LAN) – login to the HTTP API account, which is required for proper communication with a device outside the LAN
  - **Password** (unavailable in the LAN) – password for the HTTP API account, which is required for proper communication with a device outside the LAN (unavailable in the LAN)
  - The detail shows additional information on the device: connection status, firmware version, MAC address, serial number

Restart Device

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

About

This section provides basic information on the device (serial number, MAC address, FVW version, IP address etc.).

2N Elevator Center – Lift company

The Lift company can add devices, allow access of the Call Center company to selected devices in 2N Elevator Center.

Refer to the 2N Elevator Center Basic Configuration (p. 37) subsection for the basic configuration.

Beyond the scope of the basic configuration, Lift company can use the following sections of 2N Elevator Center:

- – Devices – display the devices added for the Lift company. This device cannot be edited, but can be renamed by the Call Center company. Click the device card or go from the card directly to the web configuration interface to display more details.
  The devices can be searched, filtered or backed up. The section also allows you to choose the columns or device info to be displayed.
- – Rescue sessions – display the list of currently active alarm calls.
  You can search the alarm call list according to the device location, name or ID. The section also allows you to choose the columns or alarm call info to be displayed.

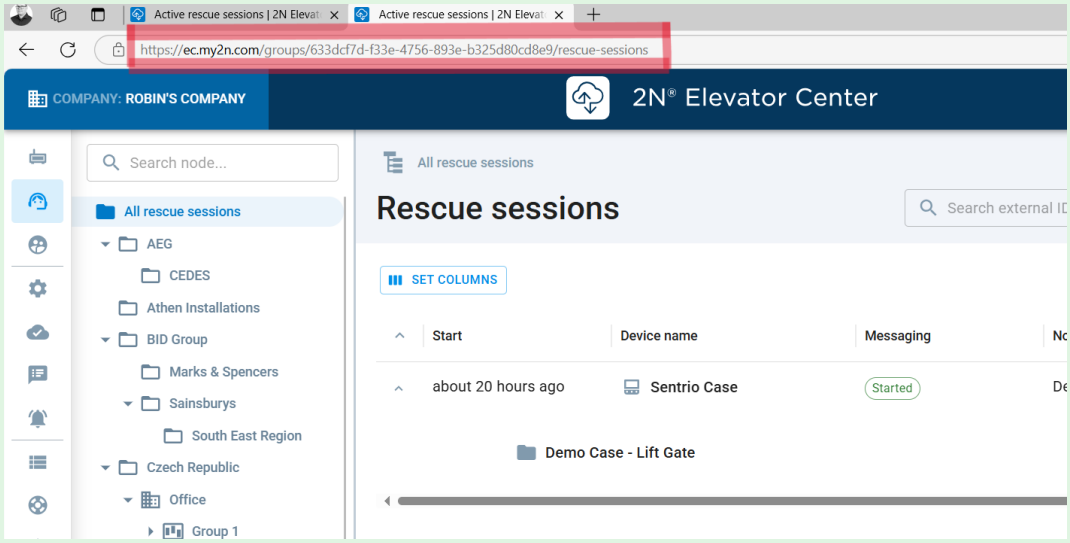
TIP

You can use the URL for searching a device quickly. It is recommended that the URL is saved.

Each folder has its Group ID, which can be used for searching using the URL.

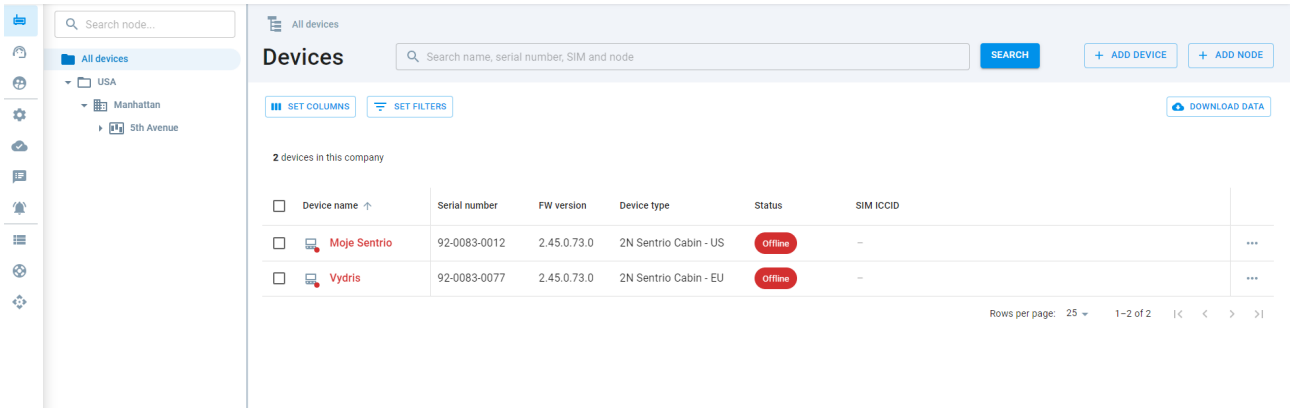
When a selected folder is clicked, the URL may look like, e.g.: “https://ec.my2n.com/groups/b4ec4200-2118-4271-bb74-deb537ba4b8b/rescue-sessions?search=12345”, where:

- “b4ec4200-2118-4271-bb74-deb537ba4b8b” – folder Group ID
  It is recommended that the top folder Group ID is used for searching all the folders.
- “12345” – elevator number to be sought



- – Users – display the Call Center company users and their roles. The Company admin can add users by clicking Create New User and assign them their roles. Once created, the new user gets an automatic e-mail with a temporary password and is prompted to log in and create a new user password.
  User Roles
  - Company admin – the user with this role can create and manage more user accounts for the company. The Company admin is the only one to add, remove and edit messages in Chat messages.
  - Specialist – the user with this role has limited rights compared to the Company admin:
    - cannot create and manage user accounts, can only manage its own account
    - has no access to the Partner API security keys section
  - Operator – the user with this role is supposed to receive alarm calls. For a better orientation in the system, this user can use Rescue sessions, Chat messages (without the message editing option), Users (with the option to manage its own user account) and History of rescue sessions.
- – Configuration Templates – new devices are configured automatically according to the template uploaded. The new device template can be used either for individual devices or in bulk.
- – Device Type Firmware Settings – set a specific firmware version for the selected device type. Enable/disable automatic firmware upgrade. A new device added to 2N Elevator Center will be upgraded to the specific firmware version if selected.
- – Chat messages – display the preset messages saved. It is also possible to edit or create messages here. Refer to How To Set Preset Messages and Their Language Mutations (p. 57) for details.
- - Notification Center – E-mail notification sending option for defined events and selected devices (node/folder).
- – Bulk Actions – option of bulk actions for selected devices, e.g. firmware update, configuration modification, device restart, etc.
- – History of rescue sessions – display the accomplished alarm calls. **Messaging** displays whether or not text communication was used during the alarm call.
  You can search the alarm call list according to the device location, name or ID. The section also allows you to choose the columns or alarm call info to be displayed.
- – Partner API security keys

2N Elevator Center **for Call Center –** Call Center company



1. It displays the list of all the companies that have assigned a device to the Call Center company. The devices are assigned to nodes. The devices are displayed in Devices according to the selected node.
2. Display of a selection section, e.g. Devices.
3. 2N Elevator Center
   - – Devices – display the device with allowed access for this Call Center company. This device cannot be edited, but can be renamed by the Call Center company. Click the device card or go from the card directly to the web configuration interface to display more details.
     The devices can be searched, filtered or backed up. The section also allows you to choose the columns or device info to be displayed.
   - – Rescue sessions – display the list of currently active alarm calls.
     You can search the alarm call list according to the device location, name or ID. The section also allows you to choose the columns or alarm call info to be displayed.
   - – Users – display the Call Center company users and their roles. The Company admin can add users by clicking Create New User and assign them their roles. Once created, the new user gets an automatic e-mail with a temporary password and is prompted to log in and create a new user password.
     User Roles
     - Company admin – the user with this role can create and manage more user accounts for the company. The Company admin is the only one to add, remove and edit messages in Chat messages.
     - Specialist – the user with this role has limited rights compared to the Company admin:
       - cannot create and manage user accounts, can only manage its own account
     - Operator – the user with this role is supposed to receive alarm calls. For a better orientation in the system, this user can use Rescue sessions, Chat messages (without the message editing option), Users (with the option to manage its own user account) and History of rescue sessions.
   - – Chat messages – display the preset messages saved. It is also possible to edit or create messages here. Refer to How To Set Preset Messages and Their Language Mutations (p. 57) for details.
   - – History of rescue sessions – display the accomplished alarm calls. **Messaging** displays whether or not text communication was used during the alarm call.
     You can search the alarm call list according to the device location, name or ID. The section also allows you to choose the columns or alarm call info to be displayed.
4. It displays the logged in profile and provides account logout.

How To Display and Manage Alarm Calls

When an alarm call is active, the given device is listed in Rescue sessions and you have to open it. Subsequently, the basic alarm call management screen is displayed.

1. Video Stream – display the current video transmission from the elevator cabin.
2. Detail Info – display basic information on the device and its node assignment.
3. Text Communicator
   a. Message Display – display the messages that have seen sent.
   b. Direct Message Entering – enable communication using direct writing of text messages.
4. Preset Text Messages
   a. See the elevator cabin device language to the left and the operator language to the right.
   b. Selection of Preset Text Messages
      - providing Information –
      - Question (answer yes/no) –

How to Text Communicate

The operator has the following 2 options to text communicate with **2N Sentrio** into the elevator cabin:

- direct entering of the text – click “Write custom message in...” and choose the message type: declarative sentence or Yes / No question.
- using preset messages – info messages or Yes / No questions. The advantage of the preset messages is the possibility to use pre-translated language mutations. This enables the operator to communicate with the elevator users who speak different languages. The message can be sent using , which appears if you move the mouse to the given row.

How To Set Preset Messages and Their Language Mutations

Chat messages – display the preset messages saved. Messages can be edited or created here by the Company admin user.

How To Create Message

1. The messages are arranged in preset categories for you to choose: **Introductory communication**, **Investigation**, Rescue actions and info**, Repair process** and **System info**. Each category includes preset messages.
   Press Create Message to create a new message. Click the message to be edited and follow the same instructions.
2. Press Create Message to create a new message.
3. Enter the message name for display.
4. Select the message type:
   - providing Information –
   - Question (answer yes/no) –
5. Choose the message language mutations in Languages to edit to the right.
6. Complete the message text in the selected language mutations. The message length limit is 80 characters. If you exceed the limit, the whole message will not be displayed on **2N Sentrio** (see the red-marked letters in the black frame preview).
7. Click Create to save the message.

You can move the messages within the list and between the sections using and remove them using .

You can also back up the messages in the .csv format by clicking Download all messages.

Web configuration interface

Basic Orientation

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

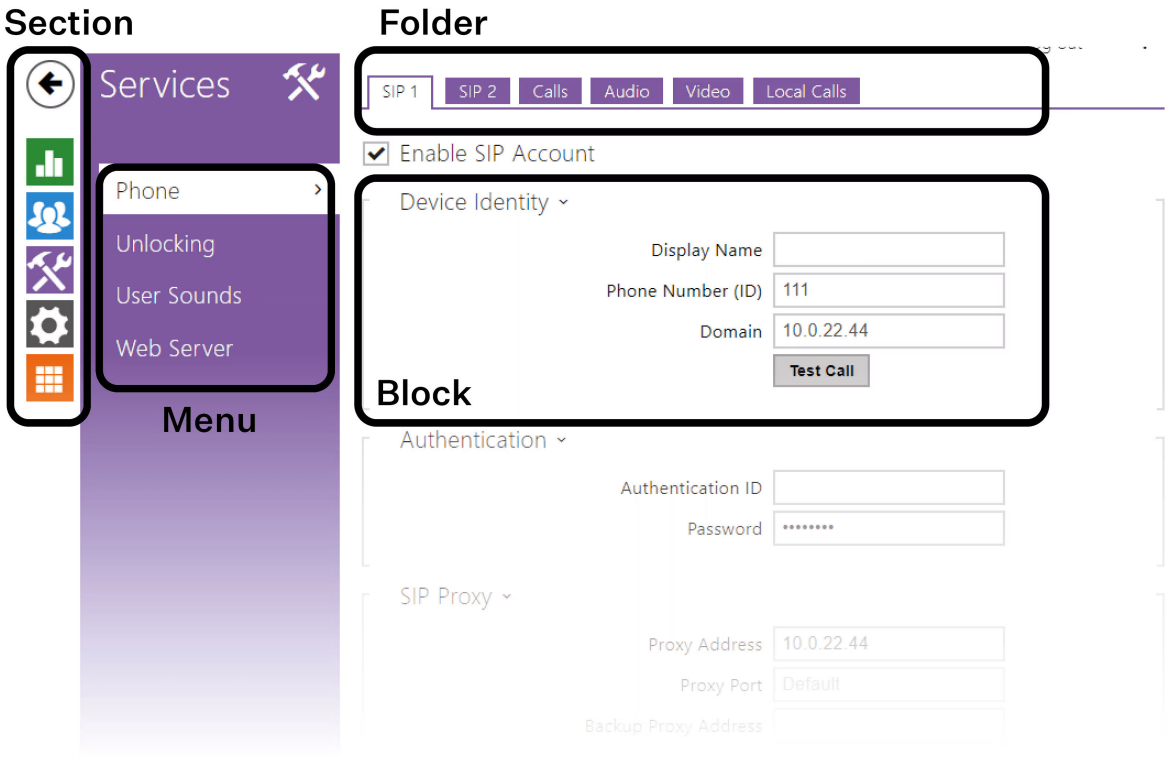
The start screen is displayed whenever you log into the **2N Sentrio** web configuration interface. Use the button in the left-hand upper corner on each of the other web configuration interface pages to return to this screen anytime. The page header shows the device name (refer to Device Name in **Services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

Menus

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

Legend

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



Device Configuration Interface Access

2N Sentrio is configured via a web configuration interface. You have to know the device IP address or the device domain name. Make sure that the device is connected to the local IP network and powered.

Domain Name

Enter the device domain name as “hostname.local” to connect to the device. The hostname of a new device consists of the device name and serial number. Enter the serial number into the domain name without dashes. Change the hostname anytime in **System > Network**.

Default domain name 2N Sentrio: 2NSentrioCabin/2NSentrioLobby-{serial number without dashes}.local (e.g.: “2NSentrioCabin/2NSentrioLobby-0000000001.local”)

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.

Web Configuration Interface Login

1. The login screen is now displayed.
   Should the login screen fail to appear, make sure that you have typed the correct IP address, port or domain name. The login screen also does not appear when the administration web server is off. If you do not have a certificate generated for the IP address / domain name, an invalid security certificate warning may be displayed. In this case, you have to confirm that you want to go to the web configuration interface.

2. Enter the login data.
   The default login data are:
   Username: **Admin**
   Password: **2n**
   It is necessary to change the password immediately upon the first login.
   After login using the default password, the access to the web configuration interface functions is limited.

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

For increased password security, it is recommended that:

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

Recommended browsers

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

State

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

Lift

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

Lift State

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

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

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

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

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

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

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

Error States

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

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

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

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

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

Device

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

Device Info

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

Locate Device – optical or acoustic signaling of the device.

Services

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

Call Logs

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

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

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

Events

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

Events	Meaning
AudioLoopTest	Performing an automatic audio loop test.
CallSessionStateChanged	Event describing the call direction/state, address, session number and call sequence number.
CallStateChanged	Indicates the call direction (incoming, outgoing) and opponent / SIP account identification at a call state change (ringing, connected, terminated).

Events	Meaning
CapabilitiesChanged	Event that informs of a change in the list of available functions of the device.
CheckingCall	Checking call state.
ConfigurationChanged	Device Configuration Change
DeviceState	Device state indication, startup of the device, for example.
DtmfEntered	DTMF code received in call or off call locally.
ErrorStateChanged	Device error state.
ExternalCameraState-Changed	Signals a status change of the connected external camera.
InputChanged	Signals a state change of the logic input.
KeyPressed	Generated whenever a button is pressed (numeric keypad digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
KeyReleased	Generated whenever a button is released (the digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
LogAutomationEvent	
LoginBlocked	Whenever 3 wrong logins to the web configuration interface have been entered. Includes data on the IP address of these accesses, time, time zone and device uptime (time after the last restart in seconds).
OutputChanged	Signals a change of the logic output state.
RegistrationStateChanged	Change of the SIP Proxy registration state.
RescueStateChanged	Change in the rescue mode state.

Directory

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

Users

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

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

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

User Basic Information

Every record in the Users list includes the following parameters:

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

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

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

User Phone Numbers

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

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

Press  to set the phone number details.

Setting the phone number

- **Call Type** – set the scheme in the called destination URI. If you choose Without scheme ([unspecified]), the URI is completed with the data from the SIP account settings. Other options include direct SIP call (sip:), 2N local calls (device:), calls to Crestron devices (rava:), connection with MS Teams (msteams:), or calls with VMS, e.g., AXIS Camera Station (vms:).
- **Destination** – set the other parts of the called destination URI. As a rule, it contains the number, IP address, domain, port or device identifier. Enter an asterisk "*" for calls to the VMS.

- **Preferred SIP Account** – SIP account 1 or 2 is primarily used for calling.
- **Call Encryption** – set mandatory call encryption or no encryption.

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

Calling

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

Calls

General Settings

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

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

Outgoing Calls

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

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

Advanced Settings

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

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

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

Local Calls

Configuration

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

Network Identification

Local Call Compatibility Mode – allow this device to communicate with older devices in the network (e.g. 2N Indoor Touch). This mode is exclusive and does not allow for calls to devices in another mode.

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

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

Connection to Lobby Units

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

LAN Devices

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

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

Video

Video Call Parameters

Video Resolution – set the video resolution for phone calls (for video codec H.264).

Video Framerate – set the video frame rate for phone calls (for video codec H.264).

Video Bitrate – set the video stream bit rate for phone calls (for video codec H.264).

Video Preview Parameters

Enable Video Preview – enable video preview multicast transmission.

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

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

Audio

DTMF Sending

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

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

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

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

DTMF Receiving

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

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

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

Transmission Quality Settings

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

SIP

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

Configuration

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

Device Identity

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

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

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

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

Authentication

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

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

SIP Proxy

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

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

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

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

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

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

SIP Registrar

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

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

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

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

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

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

Registration State – display the current registration state (Not Registered, Registering..., Registered, Un-registering...).

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

Advanced Settings

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

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

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

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

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

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

Default Local Port Values for SIP

SIP	UDP and TCP	TLS
SIP 1	5060	5061
SIP 2	5062	5063
SIP 3	5064	5065
SIP 4	5066	5067

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

REFER Enabled – enable call forwarding via the REFER method.

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

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

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

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

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

Adaptive Control of Video Quality – Enable the use of extended RTP profile for feedback via the RTCP (RTP/AVPF). Enable the use of interactive video quality control according to RFC-4585 allowing for adaption of the video data flow to the currently available network connection quality.

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

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

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

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

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

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

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

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

Audio

Audio Codecs

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

DTMF Sending

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

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

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

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

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

DTMF Receiving

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

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

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

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

Transmission Quality Settings

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

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

Alarm Call

Alarm Call

Basic Settings

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

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

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

Test Alarm

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

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

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

Destinations

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

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

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

Alarm Call 2

Destinations

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

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

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

Checking Call

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

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

Checking Call Enabled – enable test calls.

Basic Settings

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

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

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

Destination

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

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

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

Operational Call

Destination

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

The operational call is used for automatic operational call setup if one of the preset events occurs. This section sets the destination to which the operational call will be routed. The call setup itself is set using Automation, refer to Automation (p. 73). The operational call is activated by the StartLiftCall action with the parameter CallType = operational. The action is triggered whenever the event to which the action is bound occurs:

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

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

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

Services

Lift

Basic Settings

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

Product Localization – select the legislation to be met. The setting affects the display of icons and indicators according to the selected legislation.

Rescue Mode

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

NOTE

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

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

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

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

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

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

Cabin Monitoring

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

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

Streaming

ONVIF / RTSP

RTSP Server Enabled – enable the RTSP server function in the device.

Stream Settings

Audio Stream Enabled – enable offering audio streaming while the connection with the RTSP server is being established.

Video Stream Enabled – enable offering video streaming while the connection with the RTSP server is being established.

Local Stream URL – generate the stream local URL using .

Generate Local RTSP Stream URL

- **Video Codec** – select the stream video codec.
- **Video Resolution** – set the stream video resolution.
- **Video Framerate** – enter a value between 1 and 30 fps (video codec MJPEG is limited to 15 fps).
- **Bitrate** – set the stream bitrate.
- **Audio** – enable audio transmission in streaming.
- RESET – reset the default parameter values.
- Copy URL to Clipboard – copy the stream URL for insertion in another place.
- Apply URL – confirm the creation of the RTSP stream URL and saving of changes if any.
- Close – close the dialog box without changes.

Authorized IP Addresses

Set up to 4 authorized IP addresses from which you can log in to the RTSP server. If no address is completed, you can connect from any IP address.

Transmission Quality Settings

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

UDP Unicast Enabled – enable audio or video stream sending via the RTP/UDP. If this mode is off, the audio/video stream data are sent via the RTP/RTSP only.

Maximum Video Packet Size – set the maximum size of the video packets to be sent via the RTP/UDP.

Starting RTP Port – set the initial local RTP port in the range of 64 ports used for audio and video transmission. The value must be an even number not higher than 65472. The default value is 4800 (i.e. the used port range is 4800–4863).

Fixed Streaming Profiles

Default Video Codec – set the default video codec for RSTP streaming. To get URL with the currently selected initial codec, you can use URL “rtsp://IP_ADDRESS:554”.

Local Stream URL – modify the local URL of the stream according to the selected video codec.

H.264 Video Parameters

Video Resolution – set the default image resolution for video codec H.264 streaming.

Video Framerate – set the default video frame rate for streaming using video codec H.264.

Video Bitrate – set the default bitrate for streaming using video codec H.264.

MJPEG Video Parameters

Video Resolution – set the default image resolution for streaming using video codec MJPEG.

Framerate – set the default video frame rate for streaming using video codec MJPEG.

Video Quality – set the video compression level for video codec MJPEG in the range of 50–95 (50 – low quality/lowest bitrate, 95 – top quality/ highest bitrate).

JPEG

JPEG Snapshots Download

JPEG Compression Level – set the JPEG compression level to 1–99. The recommended value is 85. The parameter affects the image size and quality.

SNOM Phones Support

JPEG Video Activated by Call – enable camera snapshot downloading by the SNOM 820, 821, 760, D765, 870 phones during a call.

JPEG Video Frame Rate – set the frame rate or camera snapshot downloading period by the SNOM 820, 821, 760, D765, 870 phones.

E-Mail

SMTP

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

SMTP Server Settings

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

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

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

SMTP Server Login

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

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

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

Common E-Mail Settings

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

Advanced Settings

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

Automation

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

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

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

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

HTTP API

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

Services

HTTP API Services

HTTP API provides the following services:

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

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

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

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

Account 1–5

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

Account Enabled – enable the user account.

User Settings

Username – enter the HTTP API authentication username.

Password – enter the HTTP API authentication password.

User Privileges

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

Integration

Discovery Service Tab

Settings

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

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

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

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

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

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

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

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

User Sounds

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

Sound Mapping

Sound Message Language – select a language for spoken messages. If there is a translation available for a mapped sound, the message will be played in specified language. If no translation is available, the message is played in English or as a language-neutral sound.

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

Sound Mapping

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

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

Sound Upload

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

Sound Adding Procedure

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

Web Server

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

Basic Settings

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

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

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

Advanced Settings

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

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

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

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

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

User Localization

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

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

Audio Test

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

Test Settings

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

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

Test Result

Test Status – display the current test status.

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

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

SNMP

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

Service Enabled – turn on this feature.

SNMP Settings

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

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

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

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

SNMP Identification

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

Name – enter the device name.

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

Authorized IP Addresses

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

SNMPv3 Settings

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

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

Authentication Password – set the SNMPv3 authentication password.

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

Decryption Password – set the SNMPv3 trap decryption password.

Weather
The Weather service displays the current weather information for the selected location on the **2N Sentrio** home screen.

Settings
Show Weather – allow the device to display the current weather information.

Location – set the device Location for weather forecast. If Show Weather is enabled and the Location parameter is empty, Prague will be displayed by default. Otherwise, the weather and location values will be hidden.

Location Shown – complete the location name to be shown on the device display. If not completed, the weather forecast location is displayed.

Temperature Units – select the temperature units to be displayed.

Results
Last Update – precise date of the last server data update.

Location Found – weather forecast location found by the weather service.

Country – country of the automatically defined or completed location.

Hardware

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

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

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

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

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

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

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

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

Audio Inputs Settings

Microphone Input Gain – set the microphone input gain.

Display

The Display menu helps you set the display appearance and functionality parameters.

Basic Settings

Set the basic display parameters in this block.

Language – set the language for the texts to be displayed. Choose one of the pre-defined languages.

Language Selection – display languages for the users to choose. The field must contain a list of the comma-separated ISO 639-1 language codes in a sequence offered for selection.

Time Format – set the time format to be displayed.

Background Image – upload a background image. The file must be an image with the minimum resolution of 1024 x 600 pixels. Images with higher resolutions will be reduced in size. PNG images with transparency are supported. The image can be uploaded using  .

Backlight

Intensity in Active Mode – set the backlight brightness level. Set the value as a percentage of the maximum possible LED brightness.

Intensity Reduction in Idle Mode To – set the level of reduction of the backlight intensity if the device goes into Idle mode.

Go to Idle Mode In – set the inactivity timeout after which the device switches to the Idle mode.

Buttons

Button Shape – set the display of the button icons that matches the shape of the cabin buttons.

Right Button Icon – set the right-hand button icon display to match the cabin button icon.

Left Button Icon – set the left-hand button icon display to match the cabin button icon.

User Localization

Built-In Languages – download a  localization file template for a translation of your own or for editing texts. It is an XML file with all the texts to be displayed.

Custom language – remove  , download  and upload  a localization file of your own.

Custom Language Upload

1. Download the original language file (English).
2. Modify the file using a text editor (replace the English texts with your own ones).
3. Upload the modified localization file back to the intercom.
4. Set **Language** to Custom (p. 79) in “Basic Settings”.
5. Check and correct if necessary the texts on the intercom display.

Digital Inputs

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

Input Inversion

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

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

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

Buttons

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

External Camera

External IP Camera

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

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

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

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

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

Camera Preview

The Camera Preview window displays the current image received from an external camera. In case the camera is disconnected or misconfigured, N/A is displayed on a black background.

External IP Camera Log

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

System

Network

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

TIP
To retrieve the IP address, use 2N Network Scanner, which can be downloaded freely from 2N.com. Refer to Subs. IP Address Retrieval Using 2N Network Scanner (p. 30) for details.

Basic

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

Static IP Address Setting

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

Network Mask – network mask setting.

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

DNS Setting

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

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

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

Network Interface Settings

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

Advertised Modes – select the modes to be advertised in autonegotiation.

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

Network Identification

Hostname – set the device LAN identification.

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

VLAN Settings

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

VLAN ID – choose a VLAN ID from the range of 1–4094. The device shall only receive packets with the set ID. An incorrect setting may result in a connection loss and subsequent factory reset (p. 33).

Firewall Tab

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

Firewall

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

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

Date and Time

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

CAUTION

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

NOTE

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

Current Time

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

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

Time Zone

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

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

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

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

NTP Server

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

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

Features

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

The list includes:

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

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

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

Certificates

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

The following device services use the TLS protocol:

1. Web server (HTTPS)

2. 802.1x (EAP-TLS)
3. SIPs

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

Each certificate requiring service can be assigned one certificate set, refer to Web Server (p. 76). The certificates can be shared by the services.

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

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

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

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

Certificate Upload

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

NOTE

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

CSR

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

1. Click to create a new certificate request.

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

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

Auto Provisioning

My2N

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

My2N Enabled – enable connection to My2N.

My2N Security Code

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

My2N Security Code – device code for adding to My2N.

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

Connection State

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

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

Firmware

Firmware Update Enabled – enable automatic firmware/configuration downloading from the TFTP/HTTP server.

Server Settings

Address Retrieval Mode – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using **DHCP (Option 66/150) Address** shall be used.

Server Address – enter the TFTP (“tftp://ip_address[:port]”), HTTP (“http://ip_address[:port]”) or HTTPS (“https://ip_address[:port]”) 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 the folder with the firmware file. Enter “/” to search the server root directory. The 2N devices search for the firmware file named “model-firmware.bin” (specific model), where:

- model – represents the identifier dependent on the device:
  - 2N Access Unit – au
  - 2N Access Unit 2.0 – aug2
  - 2N Access Unit M – aum
  - 2N Access Unit QR – auqr
  - 2N IP Audio Kit – hipak
  - 2N IP Base – hipba
  - 2N IP Force – hipf
  - 2N IP Safety – hipsf
  - 2N IP Solo – hipso
  - 2N IP Style – style
  - 2N IP Vario – hipv
  - 2N IP Verso – hipve
  - 2N IP Verso 2.0 – verso2
  - 2N IP Video Kit – hipvk
  - 2N Sentrio Cabin – sentrica
  -
  - 2N SIP Audio Converter – sac
  - 2N SIP Speaker – ss
  - 2N SIP Speaker Horn – sassh

Use Authentication – enable authentication for the HTTP/HTTPS server.

Username – set the HTTP/HTTPS server access authentication username.

Password – set the HTTP/HTTPS server access authentication password.

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

Client Certificate – specify the client certificate and private key used for verifying the device’s authority to communicate with the ACS server.

Configuration

Automatic Configuration Update – enable automatic firmware/configuration downloading from the TFTP/HTTP server.

Server Settings

Address Retrieval Mode – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using **DHCP (Option 66/150) Address** shall be used.

Server Address – enter the TFTP (“tftp://ip_address[:port]”), HTTP (“http://ip_address[:port]”) or HTTPS (“https://ip_address[:port]”) 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 the folder with the firmware files. Enter “/” to search the server root directory. The 2N devices search for the configuration files named “model-common.xml” or “model-macaddr.xml”, where:

- macaddr – represents the MAC address of a specific device

- model – represents the identifier dependent on the device:
  - 2N Access Unit – au
  - 2N Access Unit 2.0 – aug2
  - 2N Access Unit M – aum
  - 2N Access Unit QR – auqr
  - 2N IP Audio Kit – hipak
  - 2N IP Base – hipba
  - 2N IP Force – hipf
  - 2N IP Safety – hipsf
  - 2N IP Solo – hipso
  - 2N IP Style – style
  - 2N IP Vario – hipv
  - 2N IP Verso – hipve
  - 2N IP Verso 2.0 – verso2
  - 2N IP Video Kit – hipvk
  - 2N Sentrio Cabin – sentrica
  -
  - 2N SIP Audio Converter – sac
  - 2N SIP Speaker – ss
  - 2N SIP Speaker Horn – sassh

Use Authentication – enable authentication for the HTTP/HTTPS server.

Username – set the HTTP/HTTPS server access authentication username.

Password – set the HTTP/HTTPS server access authentication password.

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

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

Configuration Protection

Configuration Password – set the password for the decryption of password-protected configuration.

Update Schedule

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

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

Update At – set the update time in the HH:MM format for periodical updating. The parameter is not applied if the update interval is shorter than 1 day.

TR069

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

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

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

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

General Settings

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

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

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

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

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

Diagnostics

Diagnostics

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

Diagnostic Package

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

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

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

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

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

Stop Syslog Capture – set the data capture time.

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

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

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

CAUTION

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

Tools

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

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

Packet Capture

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

Local Packet Capture

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

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

Remote Packet Capture

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

Syslog

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

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

Syslog Server Settings

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

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

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

Local Syslog Messages

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

Maintenance

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

Configuration

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

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

CAUTION

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

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

CAUTION

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

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

System

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

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

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

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

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

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

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

Usage Statistics

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

Used Ports

Maintenance - Cleaning

2N Sentrio contains no environmentally harmful components. Dispose of the device in accordance with the applicable legal regulations.

If used frequently, the device surface gets dirty. Use a piece of soft cloth moistened with clean water to clean the device. Use appropriate cleaning agents suitable for glasses, optical devices, screens, etc. We recommend that IT cleaning wipes are used.

CAUTION
Use the product for the purposes it was designed and manufactured for, in compliance herewith. The manufacturer reserves the right to modify the product in order to improve its qualities.

If used frequently, the device surface gets dirty. Use a piece of soft cloth moistened with clean water to clean the device. Use appropriate cleaning agents suitable for glasses, optical devices, screens, etc. We recommend that IT cleaning wipes are used.

- Alcohol-based cleaners may not be applied.
- Do not use aggressive detergents (such as abrasives or strong disinfectants).
- Clean the device in dry weather in order to make waste water evaporate quickly.

Functionality Tests in Accordance with EN 81-28

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

Preparation

1. Open the web configuration interface of **2N Sentrio Cabin**.
2. Go to **Calling > Alarm Calls** and verify the following settings:
   - **Activation Press Time** is set to less than 3000 ms.
   - **Delayed Call** is enabled.
   - **Test Alarm** is enabled and the button press time for the test alarm activation is set to 30 seconds.
3. Go to **Services > Elevator** and verify the following settings:
   - **Rescue Mode** is enabled.
   - If **Terminate by Entering Password** is enabled, make a note of the password.

6.2.2 ALARM Emergency Signaling Information (4.1.2)

1. Press and hold the ALARM hardware button with the bell symbol for the time required for triggering the test alarm (min. 30 seconds).
2. Check that the yellow bell icon appears in the left-hand upper corner of the device display.
3. When the call is connected to the rescue service, make sure the green call icon appears in the left-hand upper corner.
4. Verify the two-way communication with the rescue service.

6.2.3 ALARM Emergency Signaling End (4.1.3)

1. Follow the test steps for 6.2.2 ALARM Emergency Signaling Information (4.1.2).
2. Ask the rescue service to end the call.
3. Check that the green call icon on the display has gone off when the call ends. The yellow bell icon remains on.
4. Exit the rescue mode.

Exit with button 2

   a. Press button 2 for 3 seconds.
   Button 2 (ALARM2) is an external button plugged into the connector on the back of the main unit (see Connectors 2N Sentrio Cabin (p. 22)); the location being determined by the installing company.

Exit by entering password

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

5. Check that the yellow bell icon on the display has gone out.

6.2.4 Emergency Power Supply (4.1.4)

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

6.2.5 Visual and Acoustic Signals in Elevator Cage (4.1.5)

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

The emergency signaling states are indicated by the icon in the left-hand upper corner of the display lighting up.

Connecting call	Active call	Active rescue mode	Rescue mode end
				No icon in the left-hand upper corner of the display

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

Communication Response

1. Make sure that the elevator door is not fully open.
2. Press the ALARM hardware button with the bell symbol for the time required for the alarm call activation.
3. Check that the yellow bell icon appears in the left-hand upper corner of the device display.
4. When the call is connected to the rescue service, make sure the green call icon appears in the left-hand upper corner.
5. Verify the two-way communication with the rescue service.

ALARM Verification and Restart

1. Make sure that the elevator door is not fully open.
2. Press the ALARM hardware button with the bell symbol for the time required for the alarm call activation.
3. Check that the yellow bell icon appears in the left-hand upper corner of the device display.
4. When the call is connected to the rescue service, make sure the green call icon appears in the left-hand upper corner.
5. Verify the two-way communication with the rescue service.
6. Ask the rescue service to end the call.
7. Check that the green call icon on the display has gone off when the call ends. The yellow bell icon remains on.
8. Press the ALARM button shortly.
9. Make sure that an audio signal sounds to indicate that the call is being connected. The system must establish connection immediately after the short press.
10. Check that the yellow bell icon on the display has gone out.

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

Accessibility and Reliability (4.2.1)

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

Troubleshooting

Refer to https://www.2n.com/faqs for the most frequently solved problems.

Technical Parameters

2N Sentrio

Supply type	Consumption	Polarity reversal protection	Power Consumption in idle
PoE, IEEE 802.3af (recommended)	12 W 4 W	✓	2.9 W
10–15 V DC adapter	At relax: 4 W Call: 4.3 W	✓	

User interface	
Controls	capacitive touch panel
Display	7" with 1024 × 600 pixel resolution

Signaling protocol	
SIP	UDP, TCP, TLS

Audio	
Microphone	integrated, or external
Speaker	2 W integrated, or external

Audio	
Induction loop output	600 mV RMS

Audio stream	
Protocols	RTP, RTSP
Codecs	G.711a/u, G.729, G.722, L16/16kHz

Video stream	
Protocols	MJPEG, RTP, RTSP, HTTP
Codecs	H.264
Video Resolution	1280 x 720 px
Frame rate	up to 30 frames per s

Interface 2N Sentrio	
LAN	10/100BaseT, RJ-45; Cat5e or higher
2 wires 10 Mbit	2N 2 wire-IP 10 Mbit, recommended single core 24AWG, cat3 cable
Input contacts	ALARM2 (ALARM1 without **2N Sentrio**
Output	Induction loop

2N Sentrio Switch interface	
Input contacts	4x contact (YES, NO, ALARM2, CANCEL)
Output contacts	2x NO/NC (1x blocking – RELAY1, 1x user-configurable – RELAY2)
Voice Alarm Station	2x (audio unit in the upper and lower part of the shaft)
External Microphone	1x
External Speaker	1x

Mechanical Parameters		
Device dimensions (W x H x D)		193 × 157 × 50 mm
Dimensions for 2N Sentrio Cabin flush mounted installation (above surface)		200.6 x 162.8 x 30 mm
Weight	Main unit	555 g
	2N Sentrio Cabin with frame and buttons	950 g
	2N Sentrio Cabin with frame without buttons	830 g
	2N Sentrio Switch	160 g
Operating temperature		–20 to 50 °C
Relative humidity		10 to 90 % non-condensing
Storing temperature		−20 °C to 70 °C
Recommended altitude		up to 2000 m

General Instructions and Cautions

Please read this User Manual carefully before using the product and follow the instructions and recommendations included therein.

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.

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 unfavorable 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, procure software protection of the product. The manufacturer shall not be held liable for any damage incurred as a result of the use of deficient 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 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 to increased tariff lines.

Directives, Laws and Regulations

2N LiftGate meets the cybernetic security requirements of the IEC 62443-4-1 and IEC 62443-4-2 standard. In combination with 2N LiftGate (see the wiring diagram), **2N Sentrio** represents a safe solution complying with the said legislation.

2N Sentrio conforms to the following directives and regulations:

EU

2N Sentrio meets the EN81-28 and EN81-70 (integrated button version) requirements.

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

Industry Canada

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

2N Sentrio meets the requirements of the CSA B44:22 technical standard.

US

2N Sentrio meets the requirements of the ASME A17.1-2022 technical standard.

FCC

This equipment has been tested and found to comply with the limits for a Class B 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 other than 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.

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 household 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.

2N Sentrio – Installation Manual

2N.com