# 2N IP Force

## 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 IP Force** product, outline its application options and highlight the advantages following from its use.

## Basic Features

**2N IP Force** is a highly durable and reliable IP intercom equipped with a number of useful features that are not common in devices in this category. Thanks to the SIP standard support and compatibility with renowned IP PBX and phone manufacturers, it can use all the VoIP network services.

**2N IP Force** can work as a standard or emergency door access intercom for buildings, entrances to premises or garages, manufacturing halls, highways and so on.

### The main advantages of this device are:

**Two highly sensitive microphones and one speakerphone (up to 10 W)** – thanks to an integrated acoustic echo cancelling (AEC) system, the product provides mutual audibility even if the calling persons are talking at the same time under normal conditions.

**Color Wide Angle Camera** – the device can be equipped with a color wide angle camera, which allows the calling persons to be displayed on the called user's phone or PC monitor.

**Keypad** – the device can be equipped with a numeric keypad module, which allows the user to use the device as a code lock for lock switch activation and/or dialing a defined phone number or user number.

**Card Reader** – the device can be equipped with a card reader module, which provides access control functionality based on RFID cards or chips. With additional software features, functions other than the door lock can be RFID card controlled too.

**Speed Dial Buttons** – can be provided with pre-programmed buttons. You can set up to three telephone numbers and time profiles for each of the buttons to increase the accessibility of the called party.

**Electric Lock Switch** – this switch can be can be controlled via a numeric keypad, PC application or any phone during a call.If necessary, the device can be supplemented with an additional switch module.

**Device Installation** – is very easy, all you have to do is connect the system into your LAN via a network cable. The device can be supplied either from a 12 V DC power source or using PoE if supported by your LAN.

**Device Configuration** – use a PC equipped with any Internet browser for configuration. Extensive installations can be easily managed in bulk using 2N Access Commander.

### Other advantages of the device

## Product Versions

**2N IP Force** is designed for outdoor applications and requires no additional roof The W-including models are intended for WAP pressure cleaning and extremely noisy environments (such as highways, etc.).

A frame is included in the main unit package.

**CAUTION**
If combined with RFID readers, **2N IP Force** fails to meet the conditions of a supplementary regulation to the EU Radio Equipment Directive – effective from August 1, 2025. **2N IP Force 2.0** meets the conditions.

Refer to Impacts of the EU Radio Equipment Directive for more details.

## One-button main units


**Part No. 9151101W**

Axis Part No. 01336-001

2N IP Force main unit – 1 button, 10 W loudspeaker

- IP69K
- 1 button
- 10 W loudspeaker
- Extra robust version
- Control of two electric locks
- Additional switch connection option

A frame is included in the main unit package.


**Part No. 9151101CHW**

Axis Part No. 01337-001

2N IP Force main unit – 1 button, HD camera, 10 W loudspeaker

- IP69K
- 1 button
- HD camera
- 10 W loudspeaker
- Control of two electric locks
- Additional switch connection option
- Night vision


**Part No. 9151101RPW**

Axis Part No. 01335-001

2N IP Force main unit – 1 button, pictograms, 10 W loudspeaker, reader ready

- IP69K
- 1 button
- Pictograms
- 10 W loudspeaker
- Control of two electric locks
- Card reader connection option
- Additional switch connection option


**Part No. 9151101CHRPW**

Axis Part No. 01334-001

Main Unit 2N IP Force – 1 button, HD camera, pictograms, 10 W speaker, reader ready

- IP69K
- 1 button
- HD camera
- Pictograms
- 10 W loudspeaker
- Control of two electric locks
- Card reader connection option
- Additional switch connection option
- Night vision


**Part No. 9151101KW**

Axis Part No. 01338-001

2N IP Force main unit – 1 button, keypad, 10 W loudspeaker

- IP69K
- 1 button
- Keypad
- 10 W loudspeaker
- Control of two electric locks
- Additional switch connection option


**Part No. 9151101CHKW**

Axis Part No. 01339-001

2N IP Force main unit – 1 button, HD camera, keypad, 10 W loudspeaker

- IP69K
- 1 button
- HD camera
- Keypad
- 10 W loudspeaker
- Control of two electric locks
- Additional switch connection option
- Night vision

## Two-button main units


**Part No. 9151102RW**

Axis Part No. 01341-001

2N IP Force main unit – 2 buttons, 10 W loudspeaker, reader ready

- IP69K
- 2 buttons
- 10 W loudspeaker
- Card reader connection option
- Control of two electric locks
- Additional switch connection option


**Part No. 9151102CHRW**

Axis Part No. 01340-001

2N IP Force main unit – 2 buttons, HD camera, 10 W loudspeaker, reader ready

- IP69K
- 2 buttons
- HD camera
- 10 W loudspeaker
- Card reader connection option
- Control of two electric locks
- Additional switch connection option
- Night vision


**Part No. 9151102-X1**

2N IP Force set main unit

- IP69K
- 2 buttons with INFO and SOS labels
- 10 W loudspeaker
- Anti-vandal buttons made of stainless steel

Customization available per request.

## Four-button main units


**Part No. 9151104W**

Axis Part No. 01342-001

2N IP Force main unit – 4 buttons, 10 W loudspeaker

- IP69K
- 4 buttons
- 10 W loudspeaker
- Control of two electric locks
- Additional switch connection option


**Part No. 9151104CHW**

Axis Part No. 01343-001

2N IP Force main unit – 4 buttons, HD camera, 10 W loudspeaker

- IP69K
- 4 buttons
- 10 W loudspeaker
- Control of two electric locks
- Additional switch connection option
- Night vision

# Accessories

## Accessories for Installation

**2N IP Force** is designed for both outdoor and indoor applications and requires no additional roof.

Choose the proper frame and, if necessary, other accessories for your particular installation needs.

All **2N IP Force** units can be used without additional accessories for flush and surface installation, however, the appropriate mounting kit must be used for plasterboard or hollow brick masonry installations.

**Part No. 9151001**

Axis Part No. 01348-001

Flush mounting box for walls

The box material is stainless steel.

**Part No. 9151002**

Axis Part No. 01349-001

Flush mounting box for plasterboard

**Part No. 9151005**

Axis Part No. 01351-001

Stand installation spacer

The spacer allows for installation to a height of 120 cm to the top device edge.

**Part No. 9151007**

Axis Part No. 01550-001

Double mounting spacer

The double spacer allows for double installation at heights of 115 cm and 203 cm to the top device edge.

**Part No. 9151006**

Axis Part No. 01352-001

Installation adapter (US)

**Part No. 9151018**

Axis Part No. 01345-001

Security screws

This is a safer alternative to regular screws.

The screw head type is torx with pin (supplied with matching handle).

## Extenders

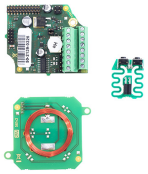
**Part No. 9151010**

Axis Part No. 01350-001

Additional Switch

Allows you to control another appliance (active output of 12 V DC / max. 600 mA) or such non-critical equipment as lights (passive relay output of 30 V / 1 A for an indefinite time).

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.



**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151011**

Axis Part No. 01344-001

Internal 125 kHz RFID card reader

Supported RFID cards 125 kHz:

- EM4x02
- NXP HiTag2

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.

Two more switches, two more logical inputs and a Wiegand interface are available.

It is compatible with the **2N IP Force** models with two buttons and with models with pictograms.

**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151031**

Axis Part No. 02522-001

Internal 13.56 MHz RFID card reader, NFC

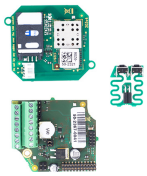
Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

NFC/HCE preparation.

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.

Two more switches, two more logical inputs and a Wiegand interface are available.



**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151031S**

Axis Part No. 01730-001

Internal secured 13.56 MHz RFID card reader, NFC

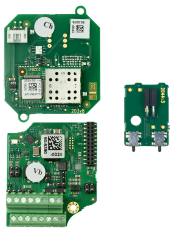
Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **HID PAC** (HID SEOS, HID iClass SE, iClass SR, HID MIFARE DESFire with SIO, HID MIFARE Classic with SIO)
- **My2N**
- **2N PICard**

NFC/HCE preparation.

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.

Two more switches, two more logical inputs and a Wiegand interface are available.



**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151022**

Axis Part No. 03228-001

Internal 125 kHz RFID card reader, OSDP

Supported RFID cards 125 kHz:

- EM4x02
- NXP HiTag2

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.

Two more switches, two more logical inputs and an OSDP interface are available.

It is compatible with the **2N IP Force** models with two buttons and with models with pictograms.

**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151023**

Axis Part No. 03229-001

Internal 13.56 MHz RFID card reader, NFC, OSDP

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

NFC/HCE preparation.

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.

Two more switches, two more logical inputs and an OSDP interface are available.

It is compatible with the **2N IP Force** models with two buttons and with models with pictograms.

**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151023S**

Axis Part No. 03230-001

Internal secured 13.56 MHz RFID card reader, NFC, OSDP

Supported RFID cards 13.56 MHz:

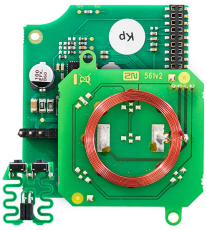
- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **HID PAC** (HID SEOS, HID iClass SE, iClass SR, HID MIFARE DESFire with SIO, HID MIFARE Classic with SIO)
- **My2N**
- **2N PICard**

NFC/HCE preparation.

It also comes with a tamper switch indicating that the **2N IP Force** front panel is open.

Two more switches, two more logical inputs and an OSDP interface are available.

It is compatible with the **2N IP Force** models with two buttons and with models with pictograms.



**CAUTION**

In combination with the **2N IP Force** intercom, this RFID reader does not meet the conditions of the supplementary regulation to the EU Radio Equipment Directive - effective from 1 August 2025. In combination with the **2N IP Verso 2.0** intercom, it meets the requirements.

Refer to Impacts of the EU Radio Equipment Directive for more details.

**Part No. 9151021**

Axis Part No. 02338-001

Internal Induction Loop

The internal induction loop transmits sound wirelessly from **2N IP Force** to the hearing aids of the people with hearing disabilities enabling them to hear and perceive sounds better.


**Part No. 9159050**

Axis Part No. 01391-001

External Induction Loop

The external induction loop transmits sound wirelessly from **2N IP Force** to the hearing aids of the people with hearing disabilities and enables them to hear and perceive sounds better.

**Part No. 9159010**

Axis Part No. 01386-001

Security Relay

A handy add-on that significantly enhances security. It prevents lock tampering.

To be installed between the protected device from which it is also powered and the lock controlled by it.

**Part No. 9159011**

Axis Part No. 01387-001

Wiegand Isolator

The Wiegand isolator is designed for galvanic isolation of two separately supplied devices interconnected via a Wiegand bus.

The Wiegand isolator protects the interconnected devices against communication errors and/or damage.

**Part No. 9155198SET**

Axis Part No. 01975-001

Security Package for 2N Devices

The security package provides increased door security.

The safety package includes a safety relay, a protection switch and an I/O module.

## Power Supply

**Part No. 91378100E (with EU cable)**

**Part No. 91378100US (with US cable)**

Axis Part No. 01403-001

One-port PoE injector

For intercom supply via Ethernet cable where the PoE switch is absent.

**Part No. 91341481E (with EU cable)**

**Part No. 91341481US (with US cable)**

Axis Part No. 02520-001

Stabilized 12 V / 2 A power supply

The supply must be used where PoE is not used.

**Part No. 932928**

Axis Part No. 02529-001

12 V transformer

For 230 V mains voltage.

Designed for external supply of electric locks.

**Part No. 9159052**

Axis Part No. 01393-001

12 V / 1 A power supply for 2N Induction Loop

The external induction loop power supply has 230 V AC input voltage and 12 V DC output voltage.

## Licenses

**Part No. 9137909**

Axis Part No. 01380-001

Gold License

Includes the Enhanced Video, Enhanced Integration and Lift Control licenses.

**Part No. 9137910**

Axis Part No. 01381-001

InformaCast License

**Part No. 9137921**

Axis Part No. 03160-001

MS Teams license

**TIP**

- Refer to the Configuration Manual for 2N IP Intercoms, Subs. Function Licensing for details.
- Please refer to the local 2N distributor for more accessories and recommendations.

## Other accessories


**Part No. 9159013**

Axis Part No. 02523-001

Departure button

The departure button is connected to the device logic input for opening the door from inside the building.

**Part No. 9159012**

Axis Part No. 01388-001

Magnetic door contact

Set for installation on a door, enabling the status of door opening to be ascertained. Used where the device is used for door protection, open door detection or forced opening.



**Part No. 9134173**

Axis Part No. 01384-001

MIFARE RFID chip card, 13.56 Hz

RFID chip card, MIFARE Classic 1k, 13.56 MHz.

**Part No. 9134174**

Axis Part No. 01385-001

MIFARE RFID chip fob, 13.56 MHz

RFID chip fob, MIFARE Classic 1k, 13.56 MHz.

**Part No. 9134165E**

Axis Part No. 01395-001

EM RFID chip card, 125 Hz

RFID chip card, type EM4100, 125 kHz.

**Part No. 9134166E**

Axis Part No. 01396-001

EM RFID chip fob, 125 kHz

RFID chip fob, type EM4100, 125 kHz.

**Part No. 11202601**




Axis Part No. 02787-001

MIFARE DESFire RFID chip card, 13.56 MHz

RFID chip fob, type MIFARE DESFire EV3 4 K, 13.56 MHz (ISO/IEC14443A).

Suitable for data encryption in PICard Commander.

The package includes 10 pieces.

**Part No. 11202602**

Axis Part No. 02788-001

MIFARE DESFire RFID fob, 13.56 MHz

RFID fob, type MIFARE DESFire EV3 4 K, 13.56 MHz (ISO/IEC14443A).

Suitable for data encryption in PICard Commander.

The package includes 10 pieces.

**Part No. 9137420E**


Axis Part No. 01399-001

External RFID reader, 125 kHz

External RFID card reader connectable to a PC via a USB interface.

Suitable for system administration and adding of EM41xx cards (125 kHz) using the device web configuration or PICard Commander.

**Part No. 9137421E**

Axis Part No. 01399-001

External RFID reader, 13.56 MHz + 125 kHz, NFC/HCE

External RFID card reader connectable to a PC via a USB interface.

Suitable for system administration and adding of 13.56 MHz/125 kHz cards and Android devices with NFC/HCE support using the device web configuration or theAccess Commander.

Suitable for uploading of MIFARE DESFire cards into the PICard Commander encryption application.

The following RFID cards can be read:

Supported RFID cards 125 kHz:

- EM4x02
- NXP HiTag2

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

The device can also read the 13.56 MHz 2N PICard RFID cards.

**Part No. 9137424E**

Axis Part No. 01527-001

External secured RFID reader, 13.56 MHz + 125 kHz, NFC/HCE

External secured RFID card reader connectable to a PC via a USB interface.

Suitable for system administration and adding of 13.56 MHz/125 kHz cards and Android devices with NFC/HCE support using the device web configuration or theAccess Commander.

Suitable for uploading of MIFARE DESFire cards into the PICard Commander encryption application.

The following RFID cards can be read:

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **HID PAC** (HID SEOS, HID iClass SE, iClass SR, HID MIFARE DES-Fire with SIO, HID MIFARE Classic with SIO)
- **My2N**
- **2N PICard**


**Part No. 9137410E**

Axis Part No. 01397-001

External IP relay, 1 output

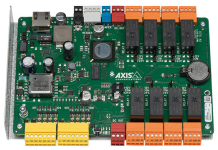
Stand-alone IP relay, which can be controlled from an intercom via HTTP commands and helps control devices from an unlimited distance.

**Part No. 9159014EU/US/UK**

Axis Part No. 01404-001

2N 2Wire (set of 2 adaptors and power source for EU/US/UK)

The 2N 2Wire converter allows you to use the existing 2-wire cabling from your original doorbell or door intercom for connecting any IP device. You do not have to configure anything, all you need is one 2N 2Wire unit at each end of the cable and a power supply connected to at least one of these units. The 2N 2Wire unit then provides PoE power not only to the second converter, but to all of the connected IP end devices.



**Part No. 9160501**

Axis Part No. 0820-001

AXIS A9188 Network I/O Relay Module

The relay is part of the lift access solution. One relay can control up to 8 floors. Intercom or access unit can be interconnected with up to 8 AXIS A9188 lift relays. The solution is thus suitable for up to 64 floors.

## Package Completeness Check

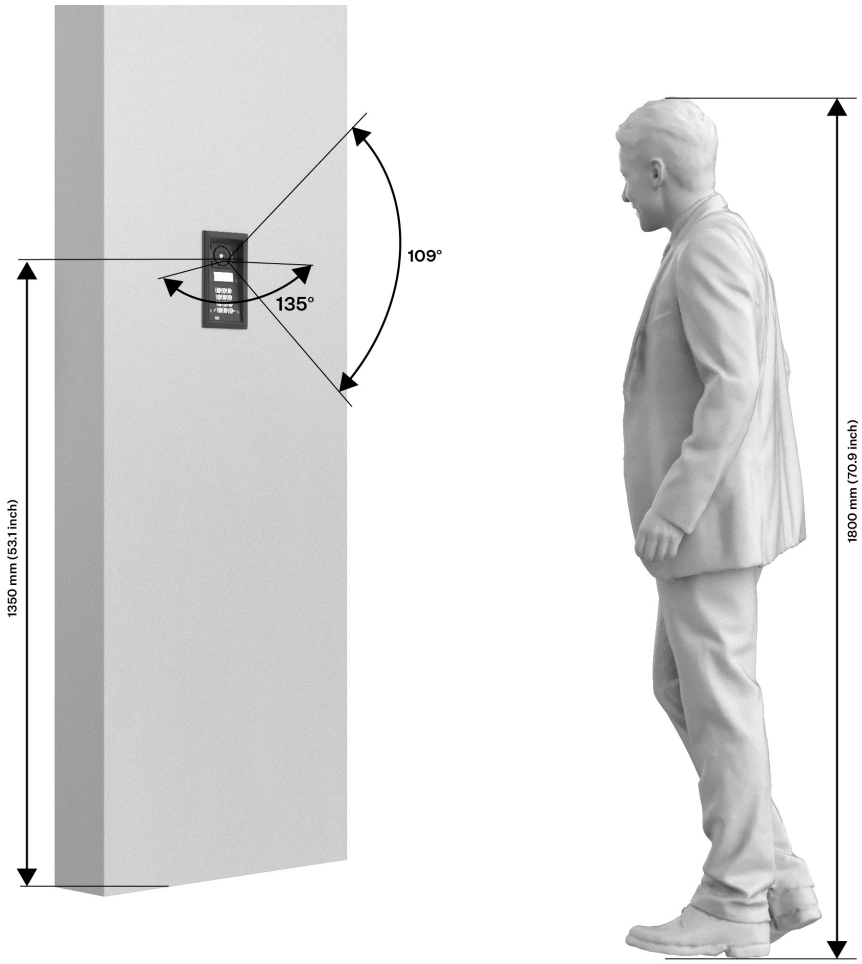
Please check the product delivery before installation. Contents:

| | |
|---|---|
| 1x | **2N IP Force** |
| 1x | Certificate of ownership |
| 1x | Brief Manual |
| 1x | installation drilling template |
| 1x | Torx 10 / Torx 20 double-ended wrench |
| 1x | Frame (in matching color) |

| | |
|---|---|
| 1x | Bushings (enclosed):<br>• 1x big two-hole sealed bushing with nut<br>• 1x spare sealing for big bushing for a thick cable, one hole<br>• 1 big blank with nut<br>• 1x small bushing with nut<br>• 1x bushing plug, big size<br>• 2x bushing plugs, small size |
| 1x | Transparent name plate foil |
| 2x | Frame fitting |
| 1x | spare name tag |
| 1x | Grounding terminal with a screw |
| 4x | 5 x 90 mm screw |
| 4x | "Intelligent" dowel (8 x 50 mm) |
| 2x | tactile sticker |

# Installation

For optimum functionality, it is recommended that the device is placed at a height according to the following scheme:




## Mechanical Installation

### Installation Conditions

### Make sure that the following 2N IP Force installation conditions are met.

- There must be enough space for the device installation.
- Make sure that the dowel holes have the required diameter. If the diameters are too large, the dowels may get loose! Use the mounting glue to secure the dowels if necessary.
- Do not use low-quality dowels to avoid their falling out of the wall!
- Make sure that the depths of the dowel holes are accurate! The plugs are 50 mm long and the screws are 90 mm long.
- Stainless steel screws are used for the **2N IP Force** assembly. Other screws than stainless steel ones corrode soon and may aesthetically deteriorate the surrounding environment!
- 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).
- Having removed the front panel, make sure that no dirt gets inside the product, especially onto the sealing surface and microphone wave guides.

**NOTE**
The microphone sound guides are normally loose after the front panel is removed! The screw is only used as a fall-out protection during installation.

- Avoid strong electromagnetic radiation on the installation site.
- Make sure that the VoIP connection is configured properly according to the SIP and other VoIP recommendations.

**WARNING**
Be sure to keep strictly the hole dimensions while mounting the device into classic bricks without the flush mounting box as shown in the picture with dimensions.

**CAUTION**

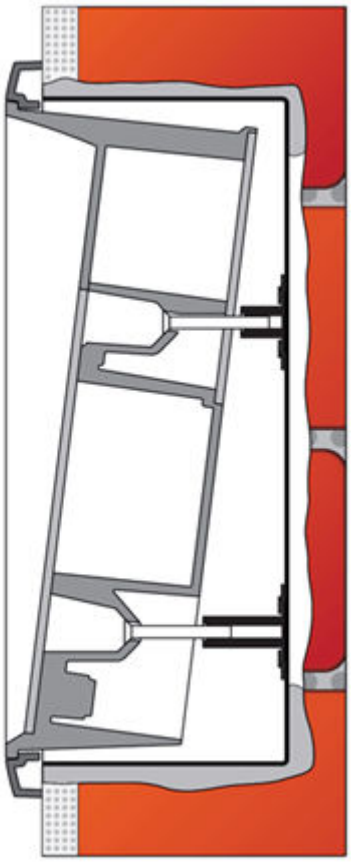
- When the proper installation instructions are not met, water might get in and destroy the electronics. As the device circuits are constantly under voltage water leakage causes electrochemical reaction. The manufacturer‘s warranty shall be void for products damaged in this way!
- The warranty does not apply to the product defects and failures arisen as a result of improper installation (in contradiction herewith). The manufacturer is neither liable for damage caused by theft within an area that is accessible after the attached electric lock is switched on. The product is not designed as a burglar protection device except when used in combination with a standard lock, which has the security function.
- 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. 99).
- 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 Tips

- The recommended height is 135 cm for standard installations (100–120 cm for disabled persons) from the floor to the device camera level. The installation heights may vary depending on the device use.
- The mounting box can be purchased in advance. Thus, a building company can be commissioned to do the rough work. The mounting box also helps you put your device exactly in the vertical position (with a max deviation of 2 ° while walling in).

## Flush Mounting

## Flush mounting – into classic masonry



What you need for mounting:

- **2N IP Force**
- a properly cut hole as instructed in the box package (131 x 222 x 82 mm)
- flush mounting box for walls (9151001, 01348-001)

If you use the brick flush mounting box, follow the instructions below:

1. Make a hole using the template. Suppose that all the required cables have been carried into the hole.
2. Put the flush mounting box inside for testing purposes to make sure that the hole is deep enough and the uneven hole edge is perfectly covered with the frame.
3. If the hole is perfect, wall in the flush mounting box.
4. Remove the front panel from the device.
5. Select the holes for cable supply. Insert the included blanks into the other holes. Apply the cable bushings or a suitable sealant to prevent penetration of insects or water. You can also insert the small bushing in the device bottom hole.
6. Attach the frame to the device.
7. Place the device into the flush mounting box while introducing the cables. Leave some of the cables inside the device as a reserve and keep the rest under the device bottom.

8. Insert the supplied screws in the side mounting holes making sure that they penetrate into the flush mounting box nuts. Tighten all the screws properly.

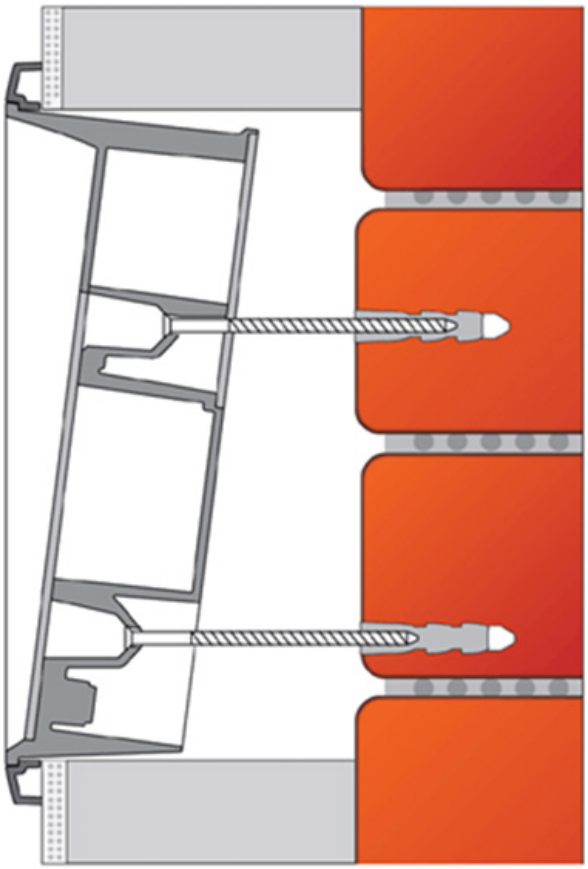
> **WARNING**
> Keep the maximum tightening torque of 1.5 Nm. Be careful, the screw tightening sequence may affect the device position.

9. It is recommended that the frame – wall gap is sealed with silicone or another sealant. This prevents water leakage behind the device.

Do not complete mounting until you have finished electrical installation.

> **TIP**
>
> - While flush mounting, pull the cables through the device back hole. A reserve cable length can be left behind the device.
> - If the cables cannot be cut in the wall deep enough, you can use a smaller hole on the device bottom.

## Flush mounting – into insulated facade



What you need for mounting:

- **2N IP Force**
- a properly cut hole as instructed in the box package (135 x 243,5 x 85 mm)
- longer screws (depending on the thermal insulation thickness)

1. Cut out the thermal insulation layer using the template (the same as for classic brick wall). Suppose that all the required cables have been carried into the hole.
2. Put the device inside for testing purposes to make sure that the hole is deep enough and the uneven hole edge is perfectly covered with the frame.
3. Remove the front panel from the device.
4. Select the holes for cable supply. Insert the included blanks into the other holes. Apply the cable bushings or a suitable sealant to prevent penetration of insects or water. You can also insert the small bushing in the device bottom hole.
5. Attach the frame to the device.
6. Place the device into the flush mounting box while introducing the cables. Leave some of the cables inside the device as a reserve and keep the rest under the device bottom.
7. Insert the supplied screws in the side mounting holes making sure that they penetrate into the flush mounting box nuts. Tighten all the screws properly.

   **WARNING**
   Keep the maximum tightening torque of 1.5 Nm. Be careful, the screw tightening sequence may affect the device position.

8. It is recommended that the frame – wall gap is sealed with silicone or another sealant. This prevents water leakage behind the device.

Do not complete mounting until you have finished electrical installation.

**CAUTION**

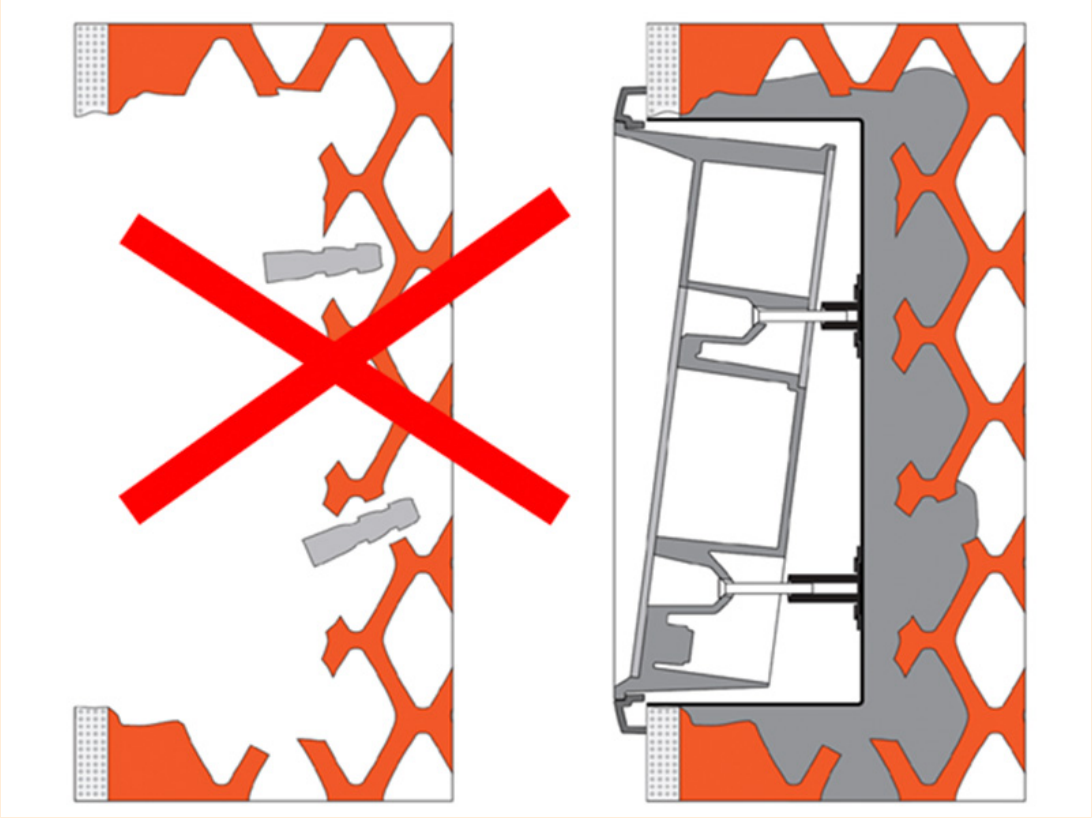
- The hole depth depends on the insulation layer thickness. If the insulation layer is rather thick, you may need longer screws! If there are hollow bricks under the insulation, make sure that your screws pass through the whole dowel (50 mm)! Otherwise, the dowel does not hold in a hollow brick.
- Make sure that the dowel holes have the required diameter. If the diameter is too large, the dowels may get loose! Use the mounting glue to secure the dowels if necessary.
- Make sure that the depths of the dowel holes are accurate! The dowel length is 50 mm and the screw length is 90 mm.

## Flush installation – in a hollow brick

What you need for mounting:

- **2N IP Force**
- a properly cut hole as instructed in the box package (131 x 222 x 82 mm)
- flush mounting box for walls (9151001, 01348-001)

**WARNING**
Note that the external side of the bricks gets damaged by cutting and the dowels cannot practically be fixed into the thin internal part of the bricks. Therefore, use the wall flush mounting box and follow the instructions for this box.



If you use the brick flush mounting box, follow the instructions below:

1. Make a hole using the template. Suppose that all the required cables have been carried into the hole.
2. Put the flush mounting box inside for testing purposes to make sure that the hole is deep enough and the uneven hole edge is perfectly covered with the frame.
3. If the hole is perfect, wall in the flush mounting box.
4. Remove the front panel from the device.
5. Select the holes for cable supply. Insert the included blanks into the other holes. Apply the cable bushings or a suitable sealant to prevent penetration of insects or water. You can also insert the small bushing in the device bottom hole.
6. Attach the frame to the device.
7. Place the device into the flush mounting box while introducing the cables. Leave some of the cables inside the device as a reserve and keep the rest under the device bottom.
8. Insert the supplied screws in the side mounting holes making sure that they penetrate into the flush mounting box nuts. Tighten all the screws properly.

**WARNING**
Keep the maximum tightening torque of 1.5 Nm. Be careful, the screw tightening sequence may affect the device position.

9. It is recommended that the frame – wall gap is sealed with silicone or another sealant. This prevents water leakage behind the device.

Do not complete mounting until you have finished electrical installation.

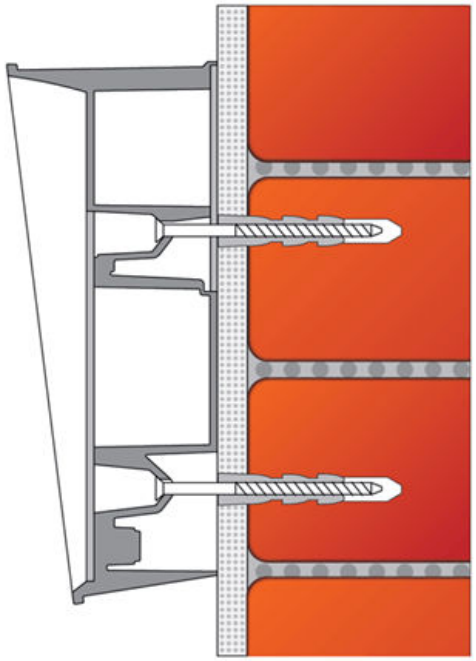
## Flush mounting – into plasterboard

What you need for mounting:

- **2N IP Force**
- a properly cut hole as instructed in the box package (116 x 233 x 78 mm)
- flush mounting box for plasterboards (9151002, 01349-001)

Use the flush mounting box for plasterboards and follow the instructions for this box.

## Surface Installation



What you need for mounting:

- **2N IP Force** (the frame is not used)

**WARNING**
Eliminate the risk of personal injury! Surface installation is not recommended for narrow passages or places where people's attention is distracted by something else. The manufacturer shall not be liable for injuries in such cases!

**CAUTION**

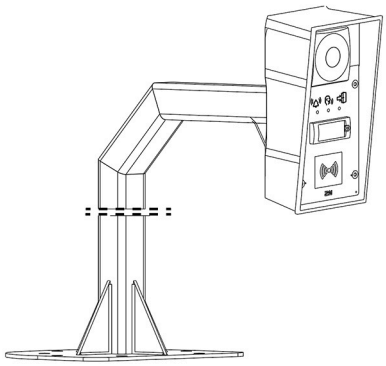
- If the device is installed in locations with an increased risk of damage (e.g., in public garages or in areas prone to vandalism), replace the supplied dowels and screws with steel anchoring elements.
- Be sure to insert plugs into unused bushing holes to avoid water leakage during facade cleaning, for example. Never leave the holes open for even a short time (one day delay between mounting and cable connection, e.g.).

**TIP**

Download the drilling template from 2N.com.

1. Select position with respect to the supply cables. Where the cables are installed inside a structure or wall, use the hole at the device bottom.
2. Drill holes of the depth of 70 mm for dowels in the wall as shown in the figure. Push or hammer the enclosed dowels into the drilled holes. Use some suitable building adhesive if the dowels are too loose. Use fixing elements of your own for steel structure surface mounting (metric screws + nuts, e.g.).
3. Remove the front panel from the device.
4. Select the holes for cable supply. Select and mount the bushings depending on the cables: 2-hole bushing or 1-hole bushing or both. Insert the included blanks into the other holes.
5. Put the device on the wall/structure while introducing cables inside. Leave some of the cables inside as a reserve. Insert the plugs in the unused bushings and tighten the bushing nuts carefully.
6. Do not complete mounting until you have finished electrical installation – refer to Mounting Completion. Where cables lead along the surface, use the bushings included in the delivery.

## Stand Installation



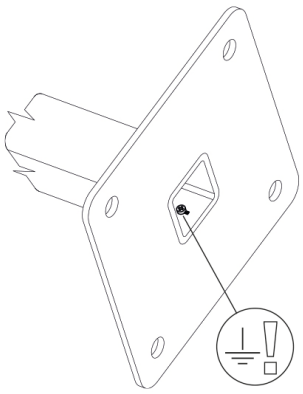
What you need for mounting:

- **2N IP Force**
- stand installation spacer (9151005, 01351-001)

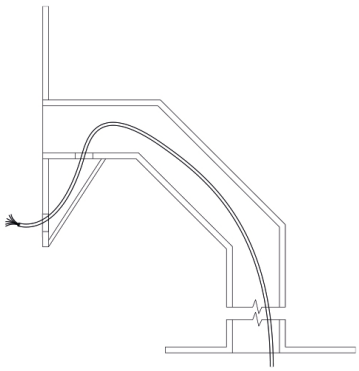
**CAUTION**

Remember to fit the stand to the base thoroughly especially if there is a risk of vandalism (public garages, etc.). Steel fitting elements are recommended.

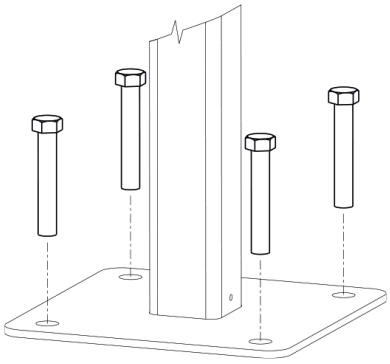
1.



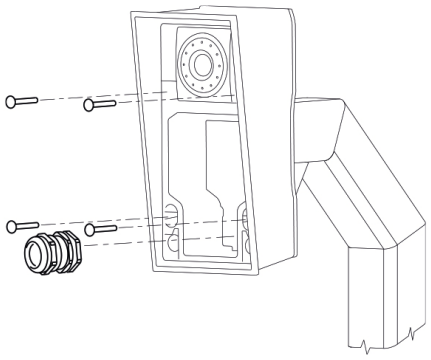
2.



3.



4.



1. Connect grounding.

> **TIP**
> You can use an M4×6 stainless steel hex key (A4).

2. Pull the cable through the stand.
3. Fit the stand to the base Refer to the base drilling template for the dimensions of the fitting elements. The screws are not included in the package. Use screws of your own according to the type of surface.

> **TIP**
> The screw hole in the stand has a diameter of 15 mm. You can use an M14×100 stainless steel bolt with a hexagonal head or a threaded rod fixed with a chemical anchor in the concrete.

4. Use a cable bushing for the **2N IP Force** cable feed-out!

> **TIP**
> You can use four M4x30 stainless steel countersunk screws (PZ2).

## Use of Cable Bushings

The cable bushings are designed for the following cables:

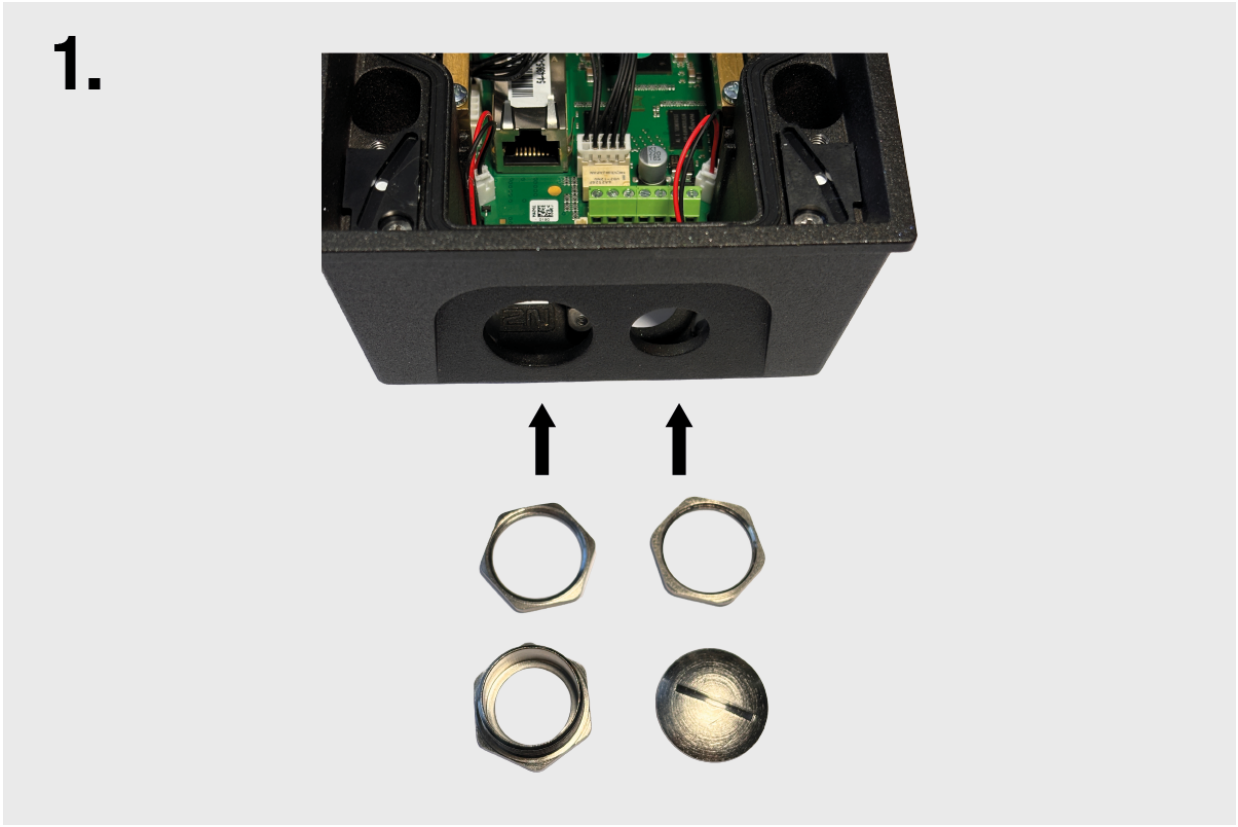
- big bushing: for two cables of the diameter of 5–6 mm (UTP cable), or, upon insert replacement, for one thick cable/tube of the diameter of up to 14 mm

- small bushing: for one cable of the diameter of 5–8 mm

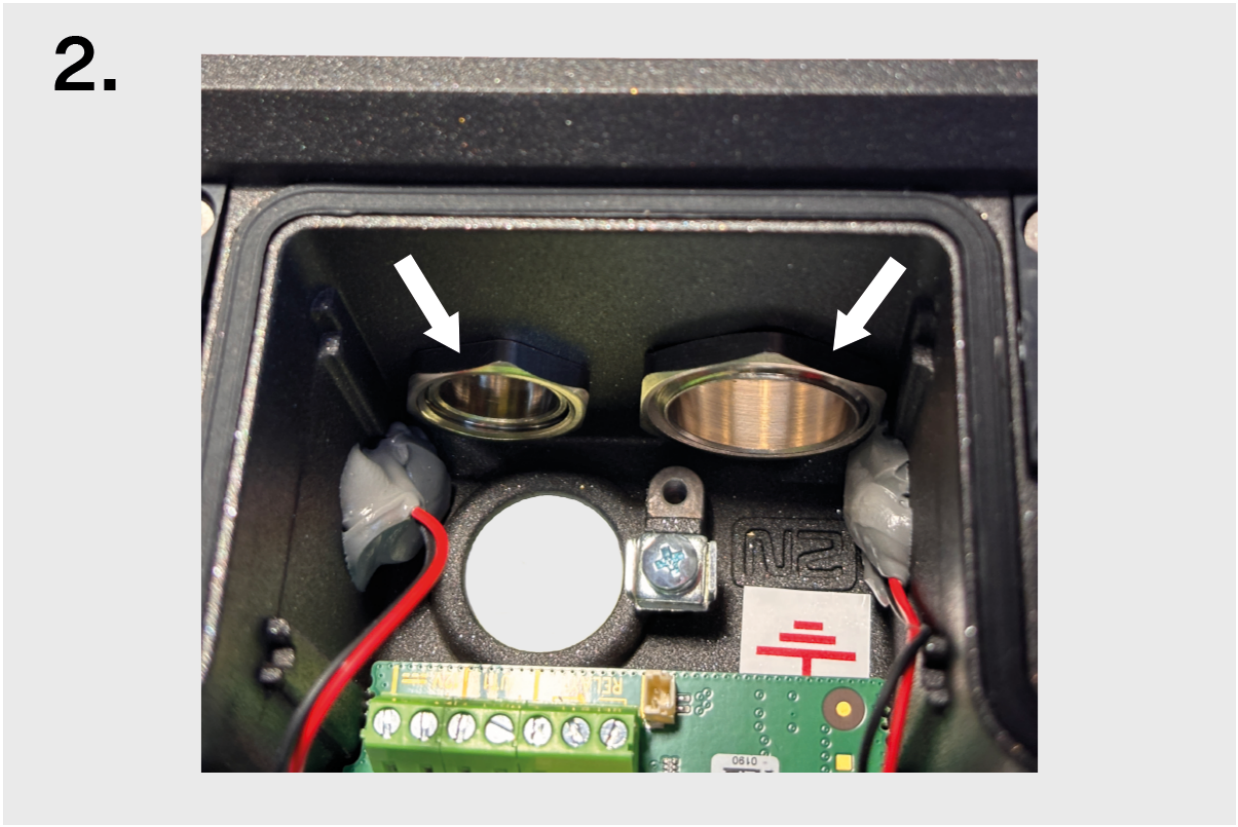
**TIP**
Even a LAN cable including the RJ-45 connector can go through the big bushing. See below for instructions.

## How to Pull a RJ-45 Terminated Cable through a Bushing

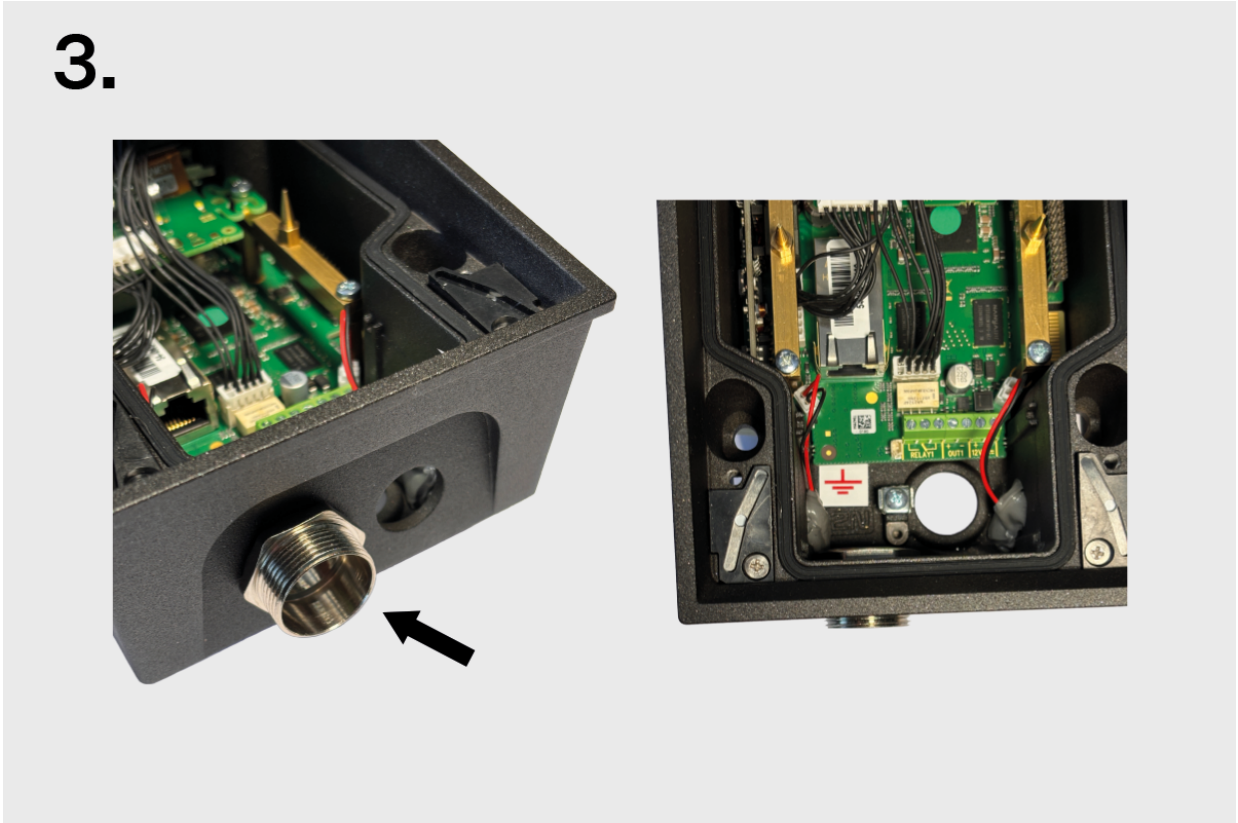
1. The cable wiring holes are located on the bottom of the device.



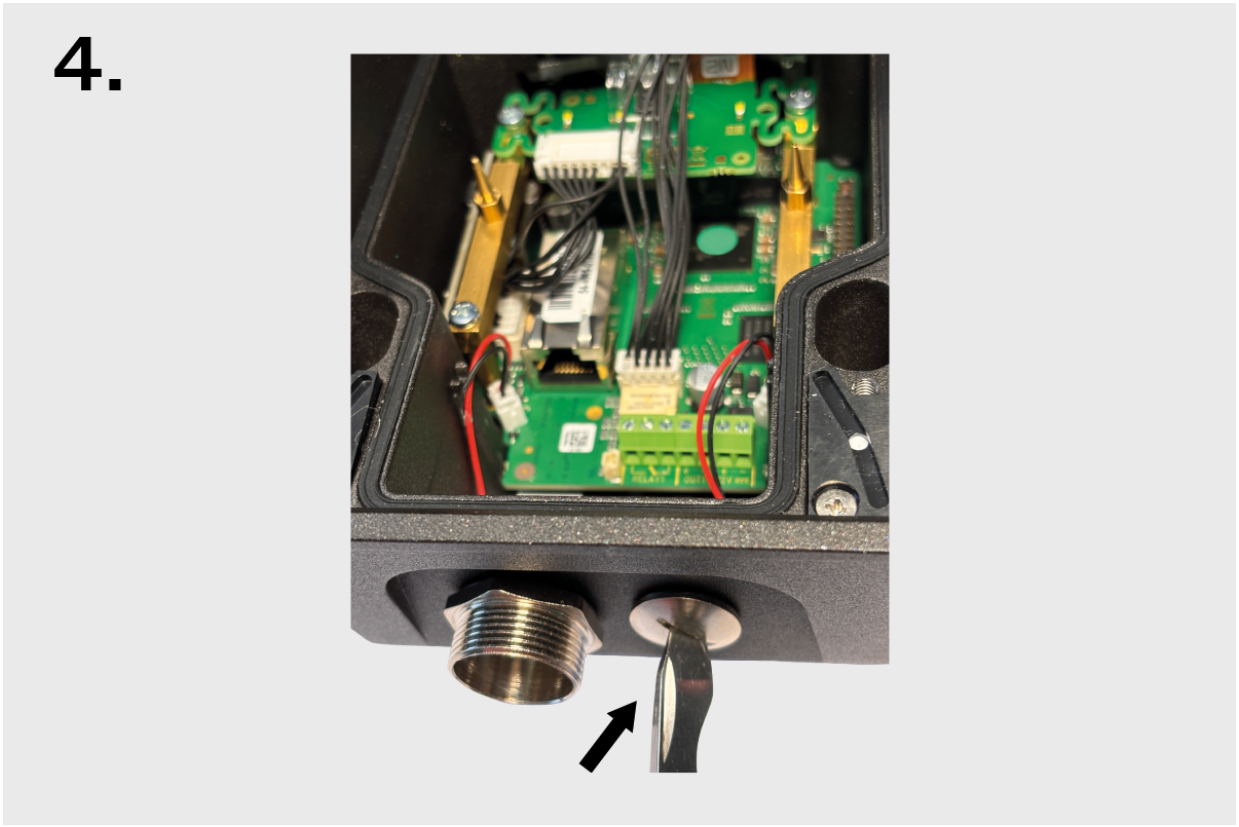
2. Place the nuts on the inside of the holes.



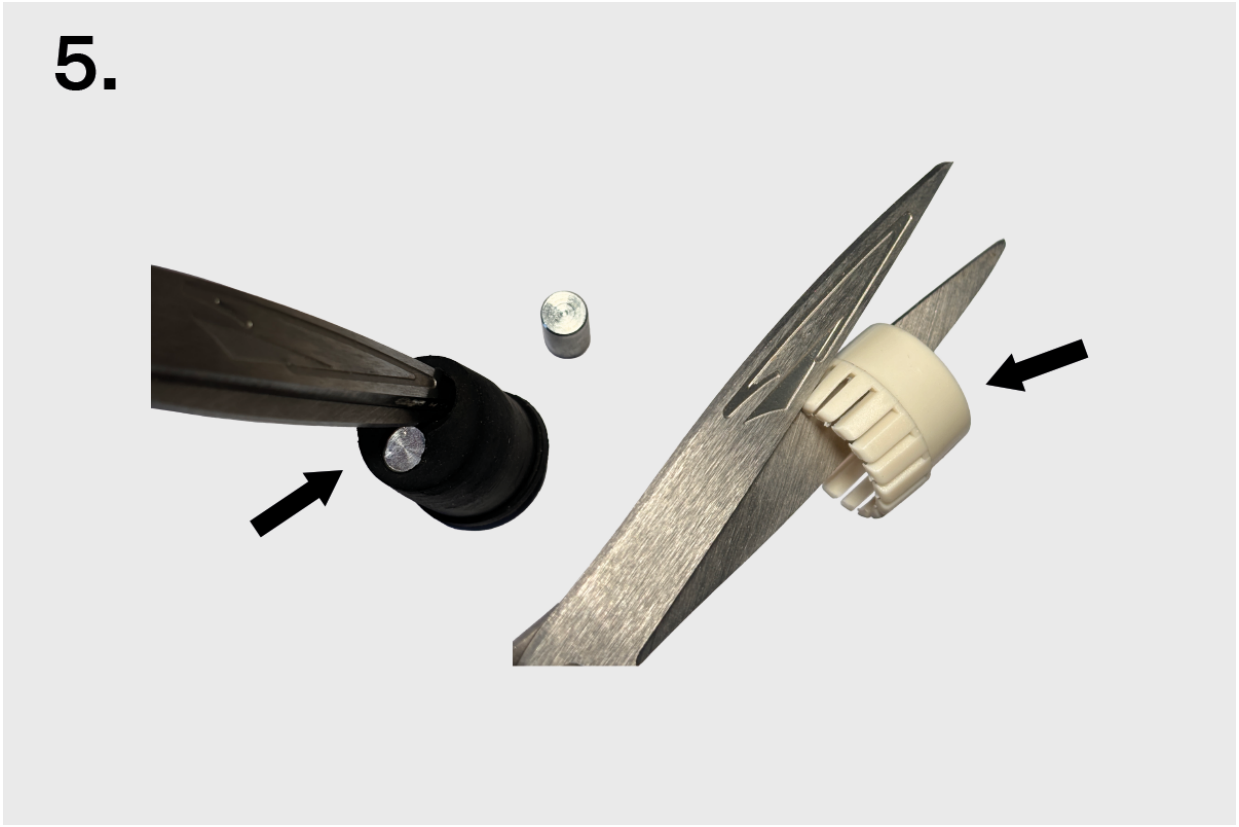

3. Screw on and tighten the bushing.



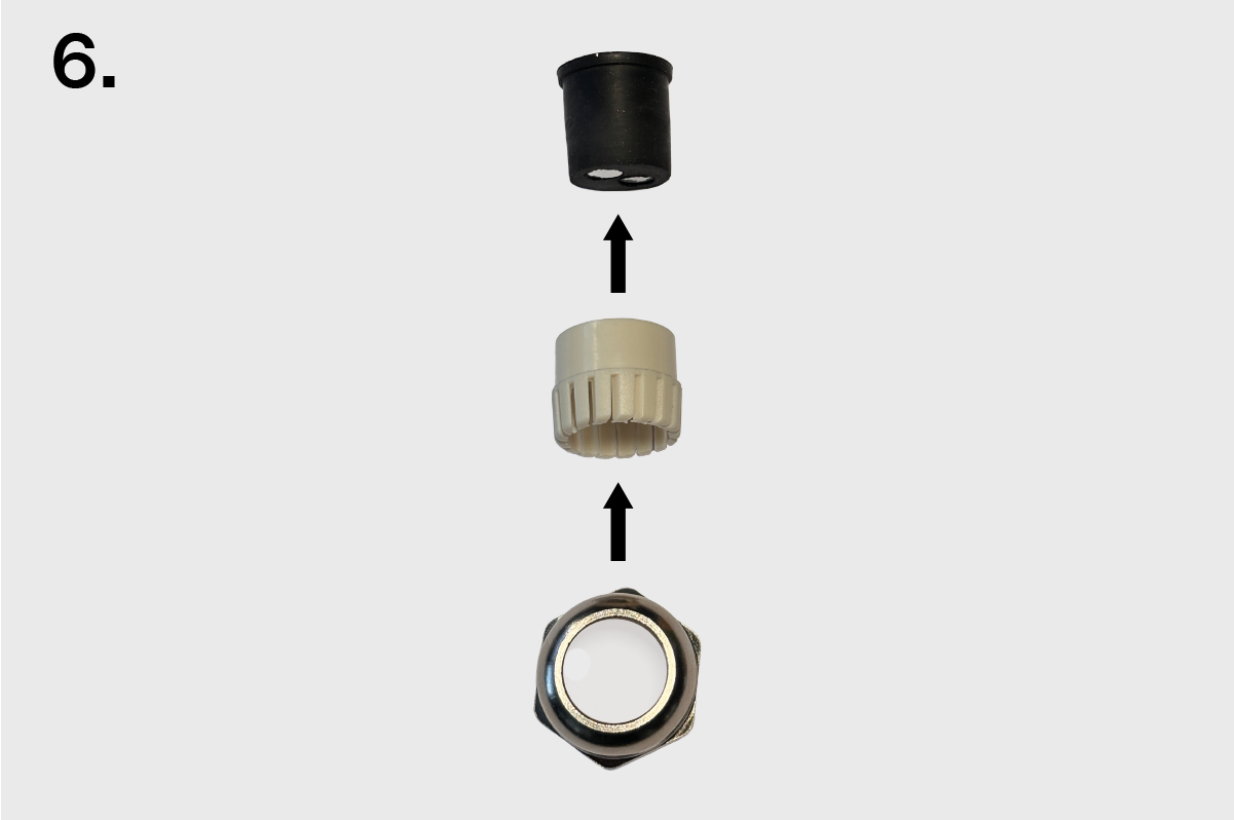
4. Screw on and tighten the blank.



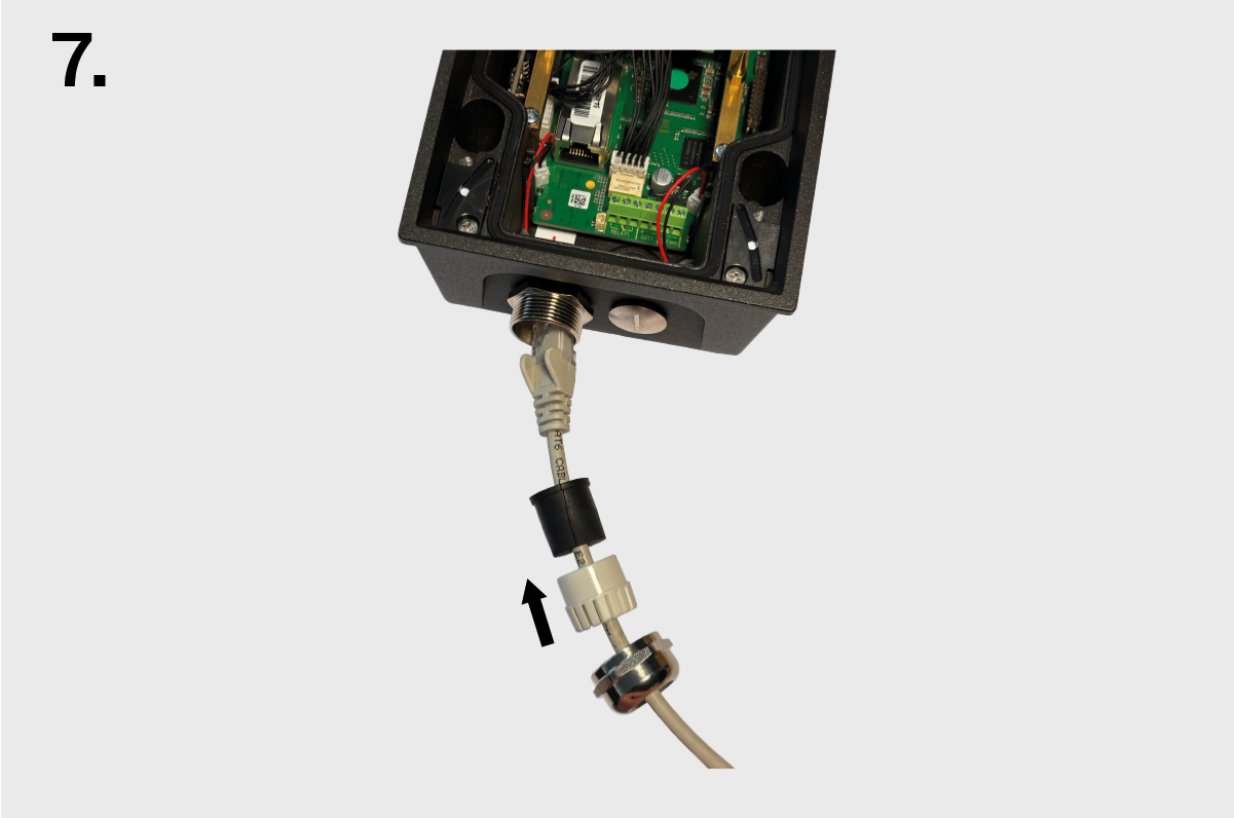

5. Remove the necessary number of cable glands from the seal.Place the nuts on the inside of the holes. Cut the case as shown.



6. To ensure tightness, follow the correct order and orientation of the case, seal and nut.

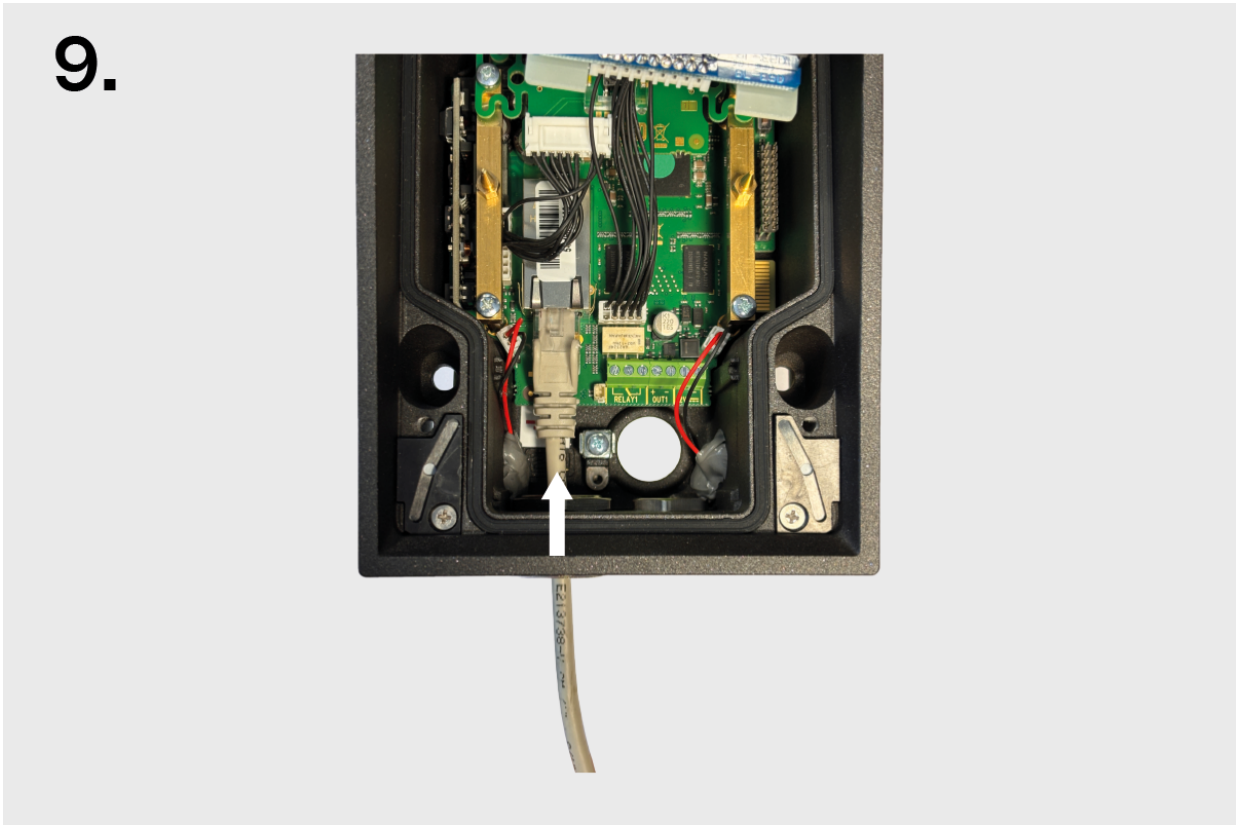



7. Attach the bushing nut, case and seal to the cable.

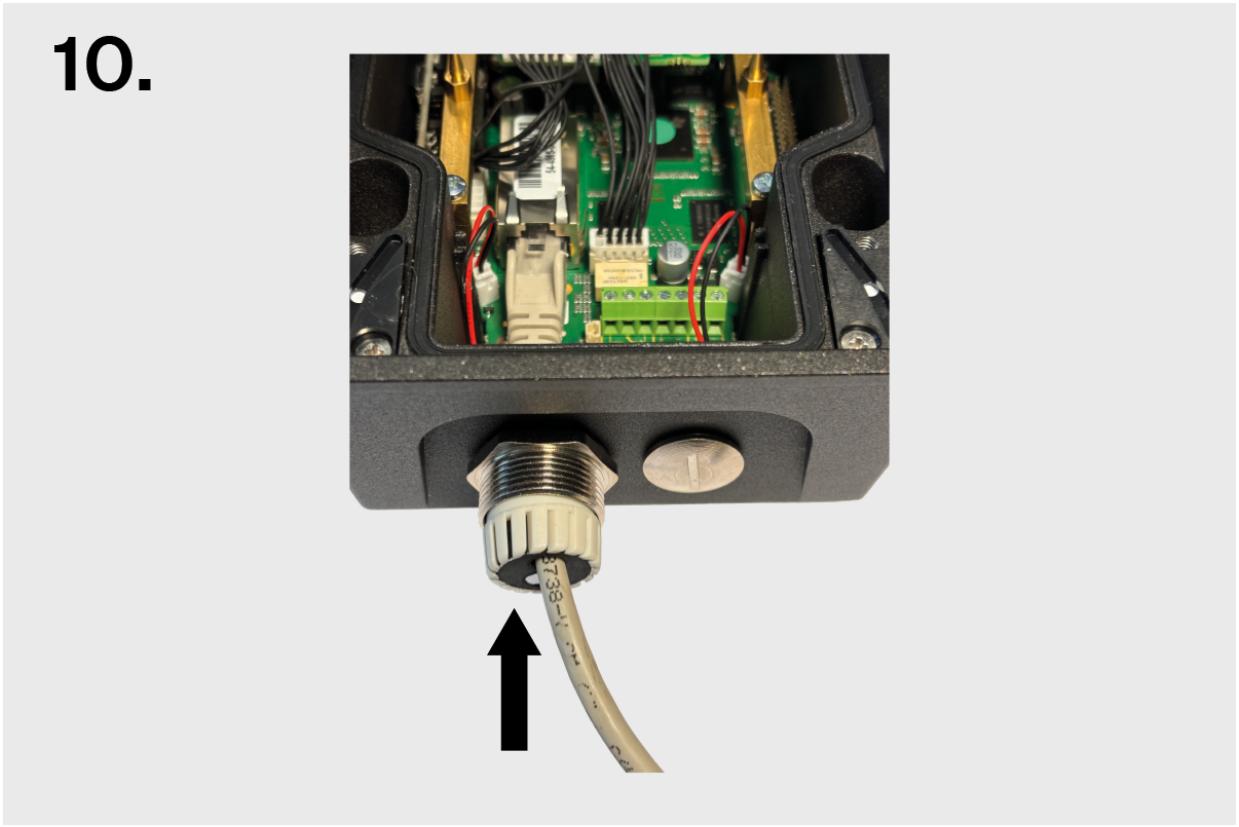


8. Pull the cable end through the bushing body into the intercom.

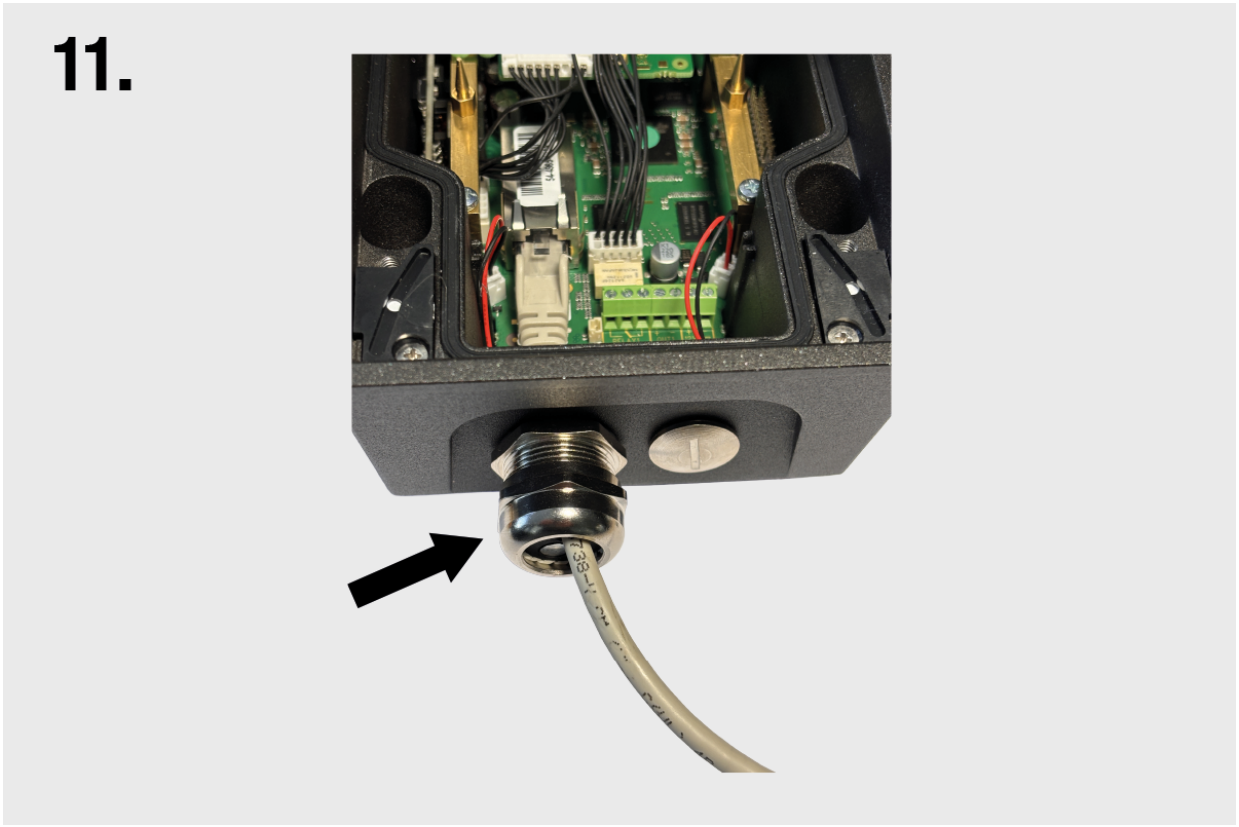

9. Snap the cable end into the motherboard connector.



**10.** Move the sealing including the case along the cable as far as the bushing body.




**11.** Screw on and tighten the nut.



# Electric Installation

## Power Supply

**2N IP Force** can be fed either directly from the LAN if equipped with PoE 802.3af (Class 0, max. 12,95 W) supporting network elements or from an external 12 V ±15 % / 2 A DC power supply.

**CAUTION**

- The device must be part of the electrical system of the building.
- The external power supply should comply with PS2/LPS.

## PoE Supply

**2N IP Force** is compatible with the PoE 802.3af (Class 0, max. 12,95 W) technology (Class 0, max. 12.95 W) and can be supplied directly from the LAN via compatible network elements. If your LAN does not support this technology, insert a PoE injector, between **2N IP Force** and the nearest network element.

## External Power Supply

Use a SELV supply 12 V ±15 % dimensioned to the current consumption feeding of at least 4A to make your device work reliably.

**CAUTION**

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 (−).

## Combined Power Supply

## LAN Connection

**2N IP Force** is connected to the LAN by inserting a SSTP cable ( Cat-5e or higher) terminated with an RJ-45 plug into the marked LAN connector on the device (connector X11). As the device is equipped with the Auto-MDIX function, you can use either the straight or crossed cable version.

This device must be deployed within a network infrastructure that provides adequate protection against Denial-of-Service (DoS) attacks and similar network-based threats. The device does not include built-in protection against high-volume or malicious traffic and relies on the surrounding network environment—such as firewalls, intrusion prevention systems, or rate limiting—for defense. Failure to implement appropriate network security measures may lead to service degradation or unavailability. The equipment's user documentation shall contain a description of all exposed network interfaces and all services exposed via network interfaces, which are delivered as part of the factory default state.

**WARNING**
On the first launch, the device must only be connected to a secure and trusted network that is fully under control of the user or administrator.

If the device is first configured on an insecure or public network, there is a risk of an unauthorized person taking control of the device.

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). A router has to be used for the device Internet connection.

Recommendation: Use a secure network or private Wi-Fi protected with a strong password.

**CAUTION**

- We recommend the use of a LAN surge protection (p. 53).
- We recommend the use of a shielded SSTP Ethernet cable.

## Board Versions

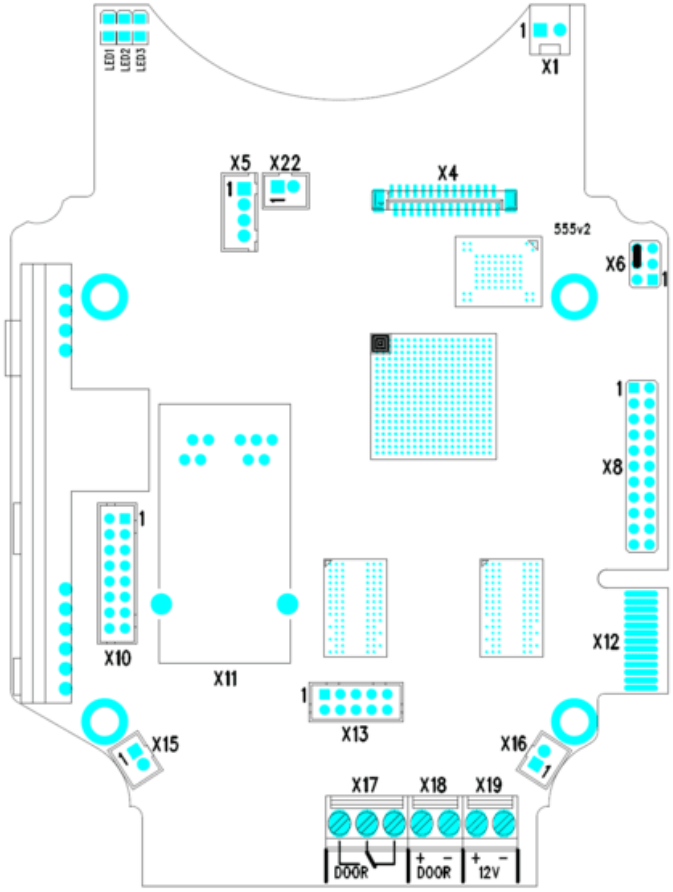
This subsection includes diagrams showing the main PCB connectors for different board versions.

The figures below show the layout of connectors on the printed circuit board (PCB). Cables, accessories and other system components are connected to connectors X1 through X22 shown in the figures.

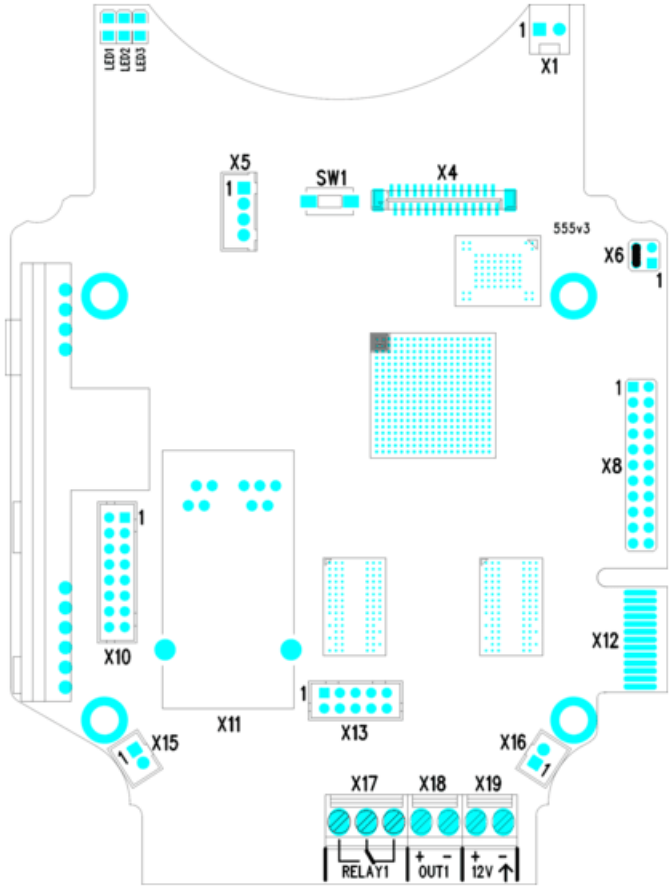
| Connector | Description |
|---|---|
| X1 | Speaker |
| X2 | Button 2 |
| X3 | Button 3 |
| X4 | Camera module |
| X5 | Button 1 |
| SW1 | Reset button (PCB version 555v3 and higher) |
| X6 | Configuration jumpers |
| X7 | Induction loop output Connector type JST SHR-02V-S |

| Connector | Description |
|---|---|
| X8 | Extending module (RFID card reader or additional switch) |
| X10 | Buttons 1 through 4 |
| X11 | LAN connection |
| X12 | Servicing connector |
| X13 | Keypad module |
| X15 | Left-hand microphone |
| X16 | Right-hand microphone |
| X17 | Relay NO and NC contacts max. 30 V / 1 A AC/DC. Used for connection of non-critical devices only (lights, e.g.). |
| X18 | Switched output 8 to 12 V DC depending on the power supply (PoE: 10 V; adapter: supply voltage minus 2 V), max. 600 mA. |
| X19 | 12 V ±15 % / 2 A DC power input |
| LED1/2 | System status indicators are displayed |
| LED3 | LAN connection activity |

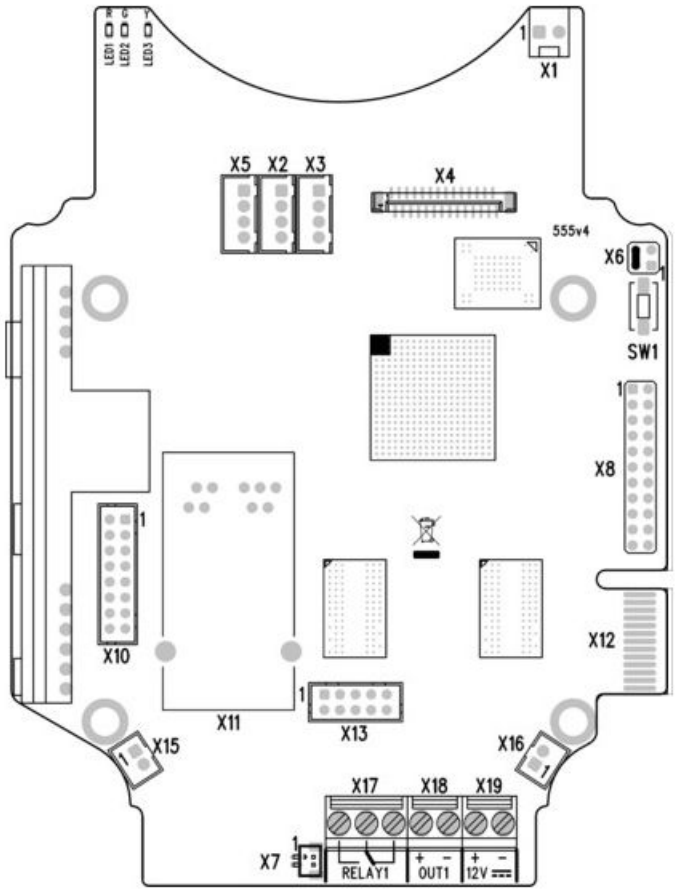
## 2N IP Force – version 555v2



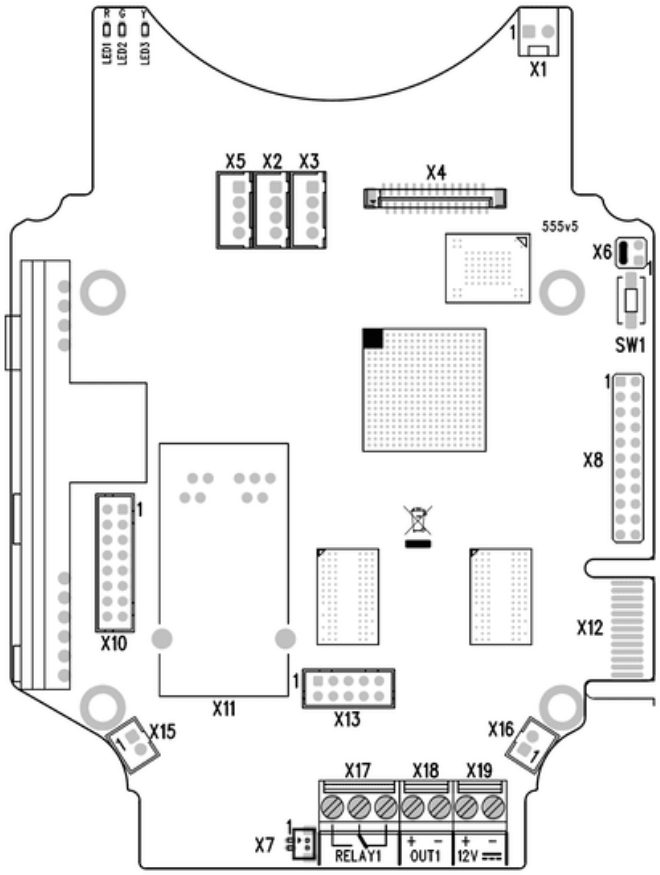
## 2N IP Force – version 555v3



## 2N IP Force – version 555v4



## 2N IP Force – version 555v5

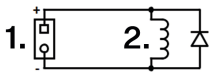



## Available switches

| Location | Name | Description |
|---|---|---|
| Main unit | RELAY1 | **Passive switch:**<br>• NO contact<br>• max. 30 V / 1 A AC/DC<br>• only used to connect non-critical devices (e.g. lights) |
| | OUTPUT1 | **Active switch output:**<br>• 8 – 12 V DC depending on the power supply, max. 600 mA<br>  • PoE: 11.6 V<br>  • adapter: source voltage -0.4 V |

| Location | Name | Description |
|---|---|---|
| Additional switch<br><br>(9151010, 01350-001) | RELAY2 | **Passive switch:**<br><br>• make and break contact<br>• max. 30 V / 1 A AC/DC<br>• only used to connect non-critical devices (e.g. lights) |
| | OUTPUT2 | Active switch output:<br><br>• 8 – 12 V DC depending on the power supply, max. 600 mA<br>  • PoE: 11.6 V<br>  • adapter: source voltage -0.4 V |
| Internal RFID card readers | RELAY 2 | Passive switch:<br><br>• NO contact<br>• max. 30 V / 1 A AC/DC |
| | OUTPUT 2 | Active switch output:<br><br>• 9.8 – 13.8 V DC depending on the power supply, max. 400 mA<br>  • PoE: 11.6 V<br>  • adapter: source voltage -0.4 V |

**DANGER**
If a coil containing device is connected, e.g. relays/electromagnetic locks, it is necessary to protect the device output against voltage peak while switching off the induction load. For this way of protection we recommend a 1 A / 1000 V diode (e.g., 1N4007, 1N5407, 1N5408) connected antiparallel to the device.




1. Terminals
2. Coil. e.g. relay or electromagnetic lock

**WARNING**
The 12V output is used for lock connection. If the device is installed in a location where there is a danger of unauthorized access (building front, e.g.), we strongly recommend the use of the 2N Security Relay (9159010, 01386-001) to ensure the maximum installation security.

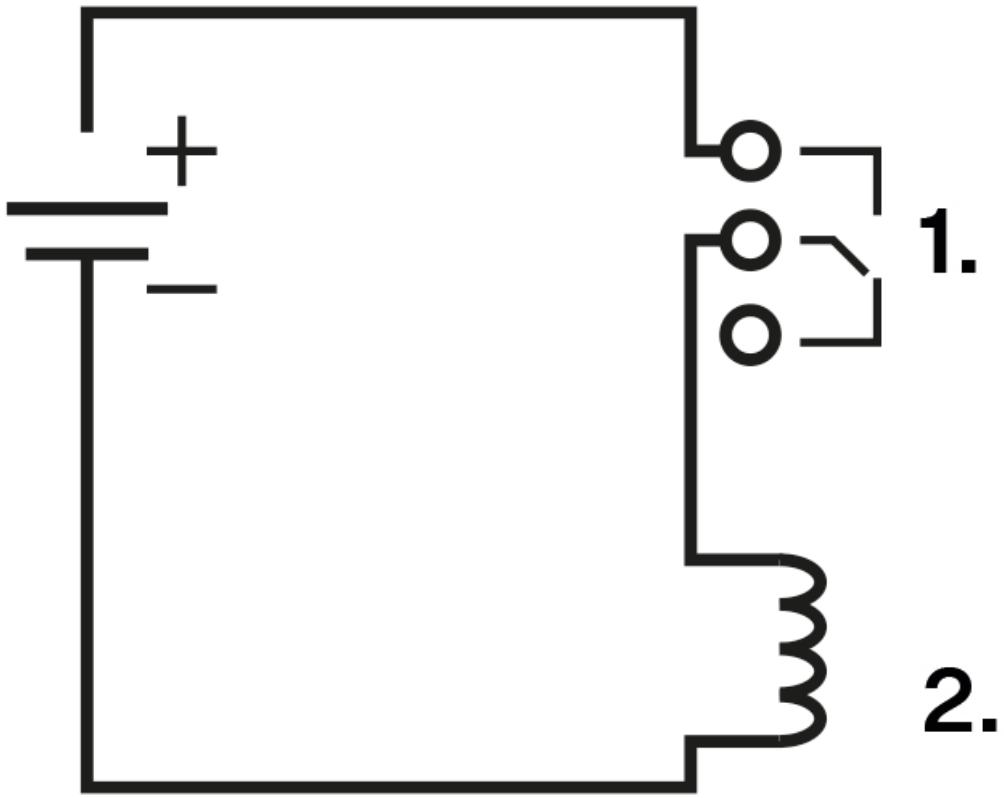
## Relay Terminal Wiring Diagrams

It is possible to connect a device to the **2N IP Force** relay terminals to be controlled by this relay, e.g. an electric/electromechanical door lock.

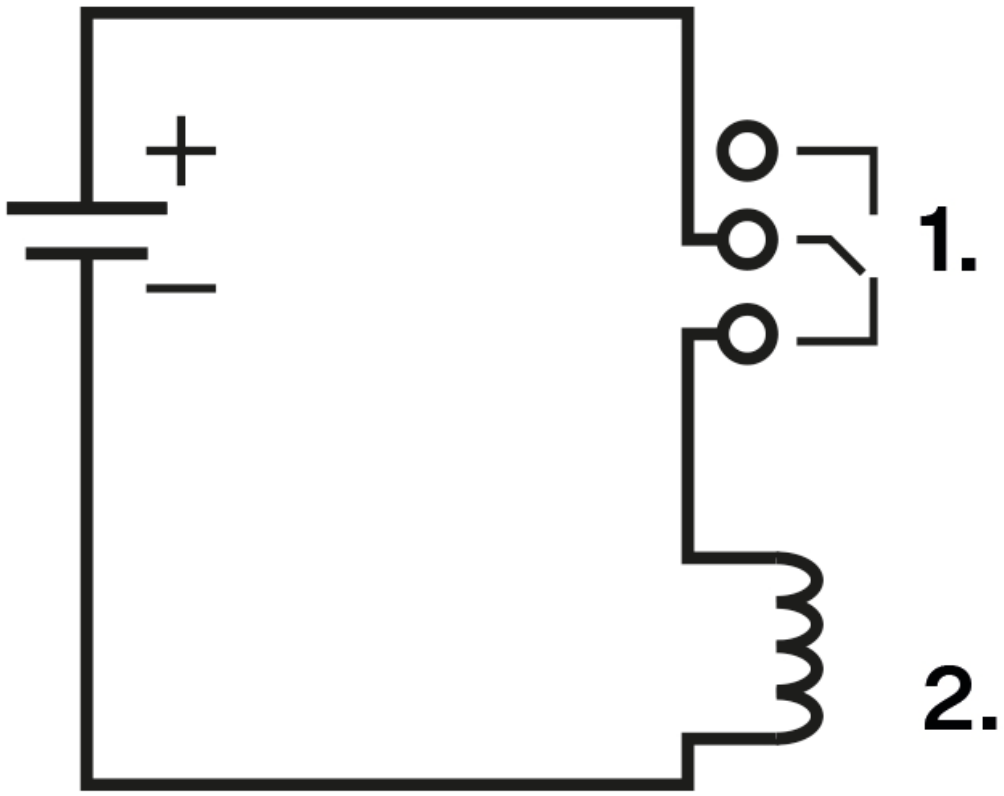
The elements are designated as follows in the diagrams below:

1. Device relay
2. Controlled device

### Wiring diagram for closing the electric circuit of the controlled device



### Wiring diagram for opening the electric circuit of the controlled device

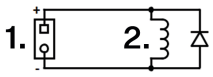



## Electric Lock Connection

**2N IP Force** is equipped with a galvanically isolated relay switch with a connected normally open and normally closed contact (terminals X17, max. 30 V / 1 A AC/DC) and a switched output of 9 to 13 V DC depending on the power supply (PoE: 9 V; adapter: source voltage minus 1 V), max. 600 mA (terminals X18), to which a conventional electric lock or another suitable appliance can be connected.

**DANGER**

If a coil containing device is connected, e.g. relays/electromagnetic locks, it is necessary to protect the device output against voltage peak while switching off the induction load. For this way of protection we recommend a 1 A / 1000 V diode (e.g., 1N4007, 1N5407, 1N5408) connected antiparallel to the device.

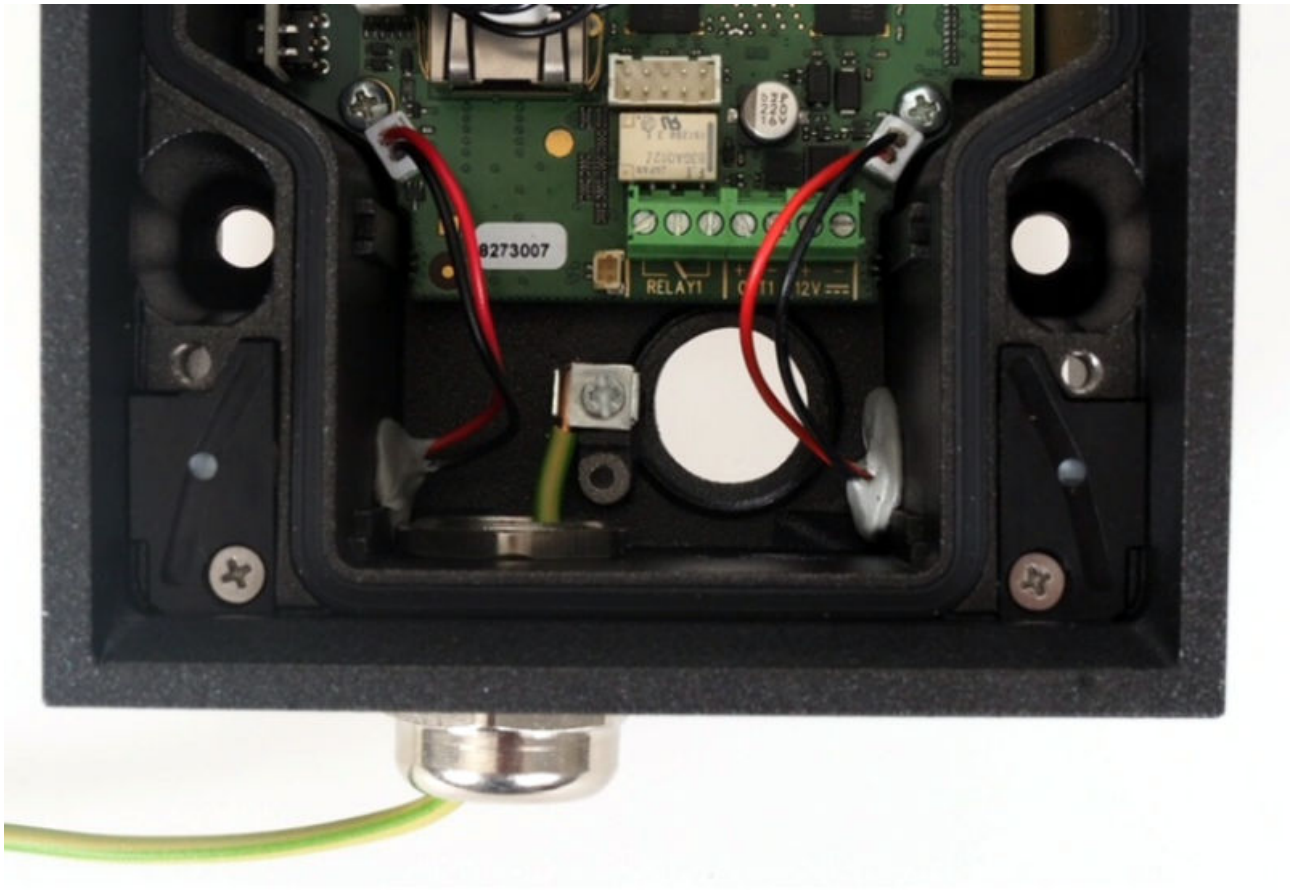



1. Terminals
2. Coil. e.g. relay or electromagnetic lock

**NOTE**
Devices with PCB version 555v3 and higher provides independent control of 12 V switched output (terminal block X18) and relay switch (terminal block X17). Devices with PCB version 555v2 have both outputs switched simultaneously.

## Grounding

To increase the static electricity resistance, you need a cable of the minimum cross-section of 4 $mm^2$. Connect the cable to the terminal in the bottom part of the device as shown in the figure below. The terminal is included in the delivery.




## Overvoltage Protection

The 2N device cables have to be protected against atmospheric overvoltage caused by external causes (lightning, e.g.). A surge can damage a device installed outside/inside the building if the wires are unprotected.

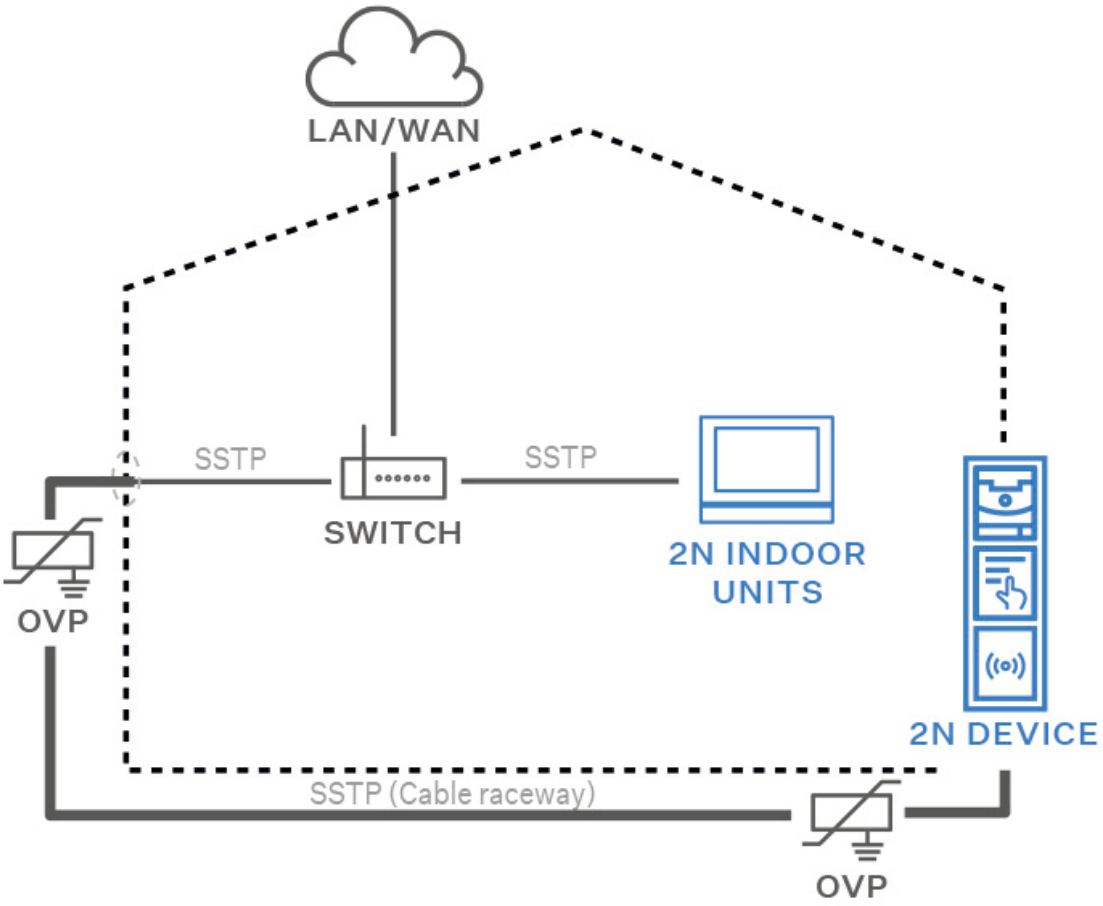
Therefore, we recommend that additional overvoltage protectors (OVP) be installed on the outer walls or roof for all the wires leading outside the building. Keep the following instructions while installing overvoltage protectors:

- Make sure that the overvoltage protector is installed as close as possible to the device installed outside the building.
- Make sure that the overvoltage protector is installed as close as possible to the device installed on an external part of the building.

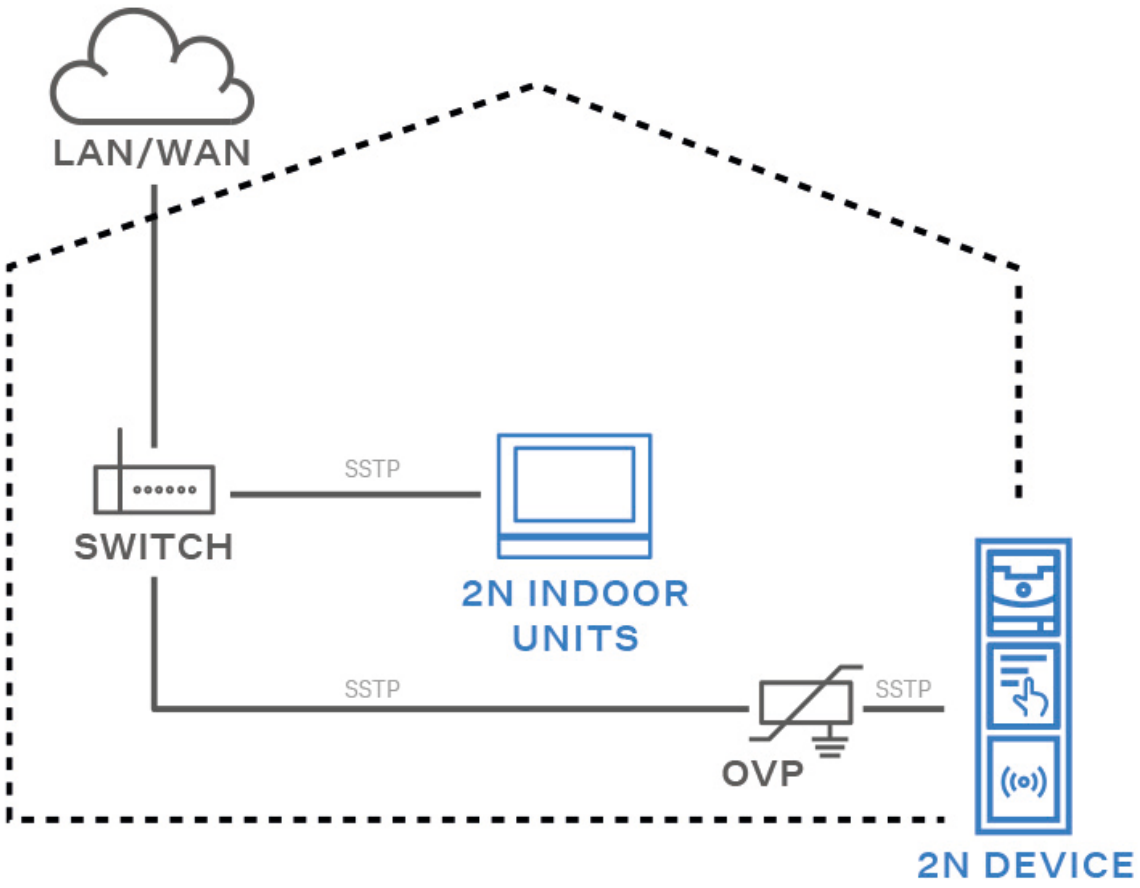
- Make sure that the overvoltage protector is installed as close as possible to the point where the cabling leaves the building.

## Examples of Overvoltage Protection Installation

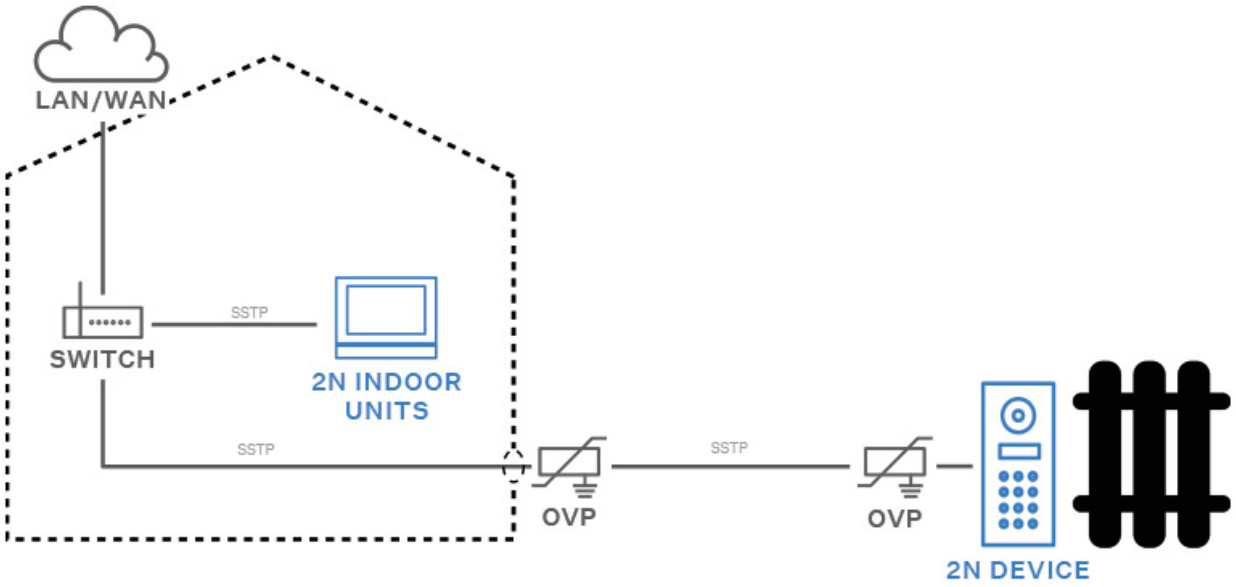
### Overvoltage protection installation diagram for a device installed on the building facade and cables outside the building



**Overvoltage protection installation diagram for a device installed on the building facade and cables inside the building**



### Overvoltage protection installation diagram for a device and cables installed outside the building




## Main and Extending Modules

**CAUTION**
In case the firmware versions of the module to be connected and the main unit are incompatible, the module will not be detected. Therefore, update the device firmware after connecting the modules. Update firmware via the web configuration interface in System > Maintenance.

**2N IP Force** can be interconnected with the following modules:

- Internal 125 kHz RFID card reader (p. 58)
- Internal RFID Card Reader 13.56 MHz (p. 61)
- Internal secured RFID Card Reader 13.56 MHz (p. 63)
- Internal RFID Card Reader 125 kHz, OSDP (p. 65)
- Internal RFID Card Reader 13.56 MHz, NFC, OSDP (p. 68)
- Internal secured RFID Card Reader 13.56 MHz, NFC, OSDP (p. 70)
- Additional Switch
- Wiegand Isolator

- Induction Loop external (p. 74)
- Induction Loop internal (p. 73)
- Security Relay (p. 79)

## Internal RFID card readers

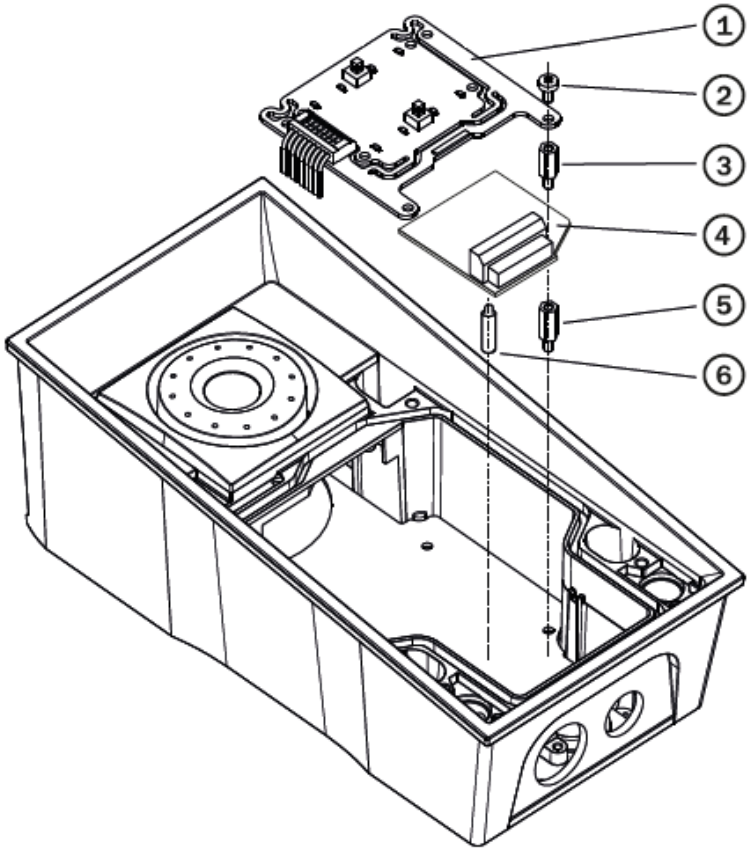
Internal RFID card readers are designed for mounting into the **2N IP Force**main unit and is compatible with the main unit Part Nos. 9151101RPW, 9151101CHRPW, 9151102RW and 9151102CHRW. These models have a window, which is necessary for antenna operation. If the Internal RFID Card Reader is installed, it is not possible to install an Additional Switch.

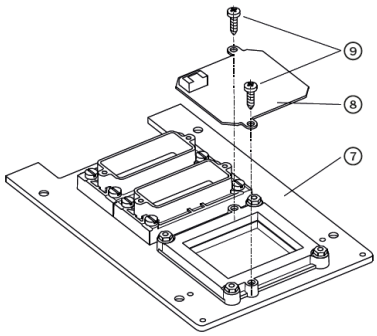
The **2N IP Force** Internal RFID Card Reader adds two logical inputs, two switches and a tamper switch to the main unit.

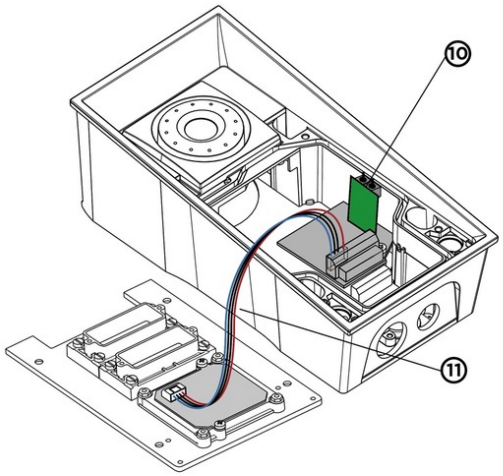
The purpose of the tamper switch is to signal any unauthorized opening of the device (to prevent a theft, e.g.). It is recommended to use the tamper switch.

**TIP**
FAQ: Tamper Switch - How to Connect It to 2N IP Intercom

## Installation



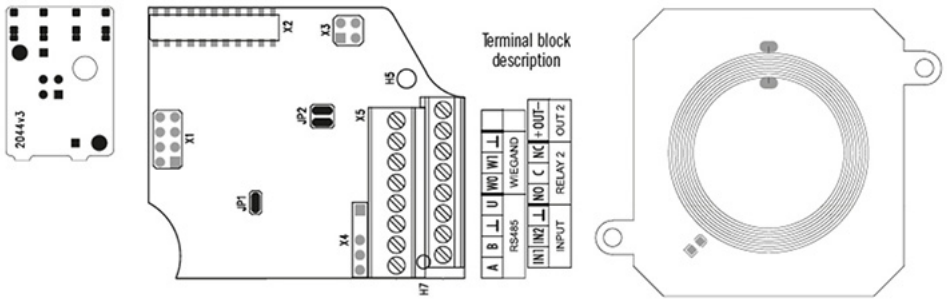



1. Turn off the device.
2. Remove the front panel (7) from the device.
3. Mount the antenna board (8). Use the two enclosed screws (9).
4. Plug the enclosed cable (11) to the antenna board connector.
5. Demount the button PCB (1). Do not disconnect its cable!
6. Dismount the right-hand bottom spacer (there are four spacers altogether).
7. There are two short plastic spacers enclosed to the induction loop. Take the shorter, 6,5 mm long spacer. Screw it into the free hole on the motherboard.
8. Plug the enclosed plastic support (6) into the reader board from the bottom side.
9. Put the reader board (4) in the motherboard connector. Make sure that the screw hole is directly above the spacer.
10. Screw in the remaining metal spacer (3), which is 10.5 mm long.
11. Fit the button PCB (1) back to its position using the original screws.
12. If you want to use the tamper switch (to detect unauthorized case opening for theft protection), insert the tamper board (10) in the connector located in the right-hand bottom part of the switch board (4). As the tamper switch shares the Relay2 NO and NC terminals, you cannot use the RELAY2 output and the tamper switch at the same time.
13. Plug the antenna cable (11) to its connector at the reader board (4).
14. Replace the front panel and tighten all the four screws.

## Internal 125 kHz RFID card reader, Wiegand

The Internal RFID Card Reader 125 kHz (Part No. 9151011, 01344-001) is used for reading RFID card Ids in the 125 kHz band.

## Specification




### Card Reader

Supported RFID cards 125 kHz:

- EM4x02
- NXP HiTag2

- Operating frequency: 125 kHz
- Minimum reading distance: 10 mm above the **2N IP Force** surface

### Passive output

- Max. 30 V / 2A AC / DC

### Switched output

- 9 to 12 V DC according to power supply (PoE: 9 V; adapter: source voltage minus 1 V), up to 600 mA

### Logical inputs

Active mode – requires external voltage (JP2 jumper OFF)

- $U_{IN}$-ON = min. +2.5 V
- $U_{IN}$-OFF = max. +1.5 V
- $U_{IN}$ max. = +48 V
- $I_{IN}$ ($U_{IN}$ +48 V) = max. 1 mA

Passive mode – requires external contact only (JP2 jumper ON)

- $U_{OUT}$ = approx. 8.3 V
- $I_{LOOP}$ = approx. 0.5 mA

### Signaling output

- Internal red LED under the intercom front panel

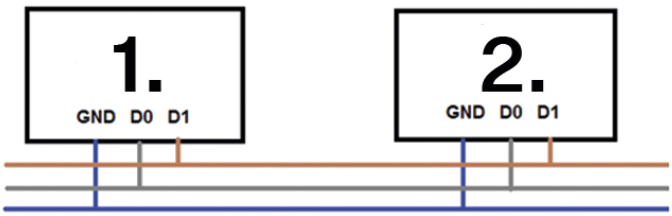
### WIEGAND interface

- Off/Input/Output (as programmed)

| Wiegand Input Technical Parameters | |
|---|---|
| Current | 5 mA |
| Input resistance | 680 Ω |
| Pulse length | 50 µs |
| Inter-pulse interval | approx. 2 ms |

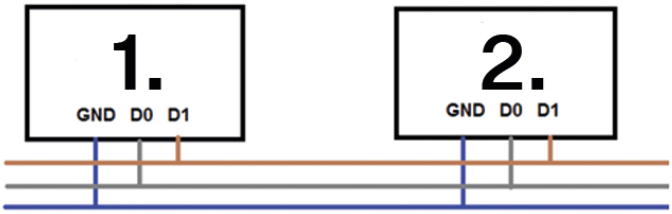
**Recommended Wiegand bus wiring diagram, 2N device as a receiver.**

1. **2N IP Force**
2. External RFID Card Reader



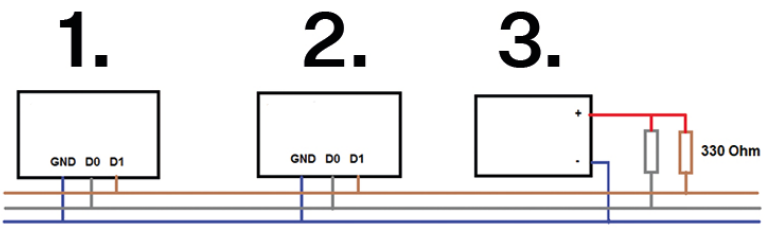
### Recommended Wiegand bus wiring diagram, 2N device as a transmitter.

1. External RFID Card Reader
2. **2N IP Force**




### Recommended reader & OC output wiring diagram

1. **2N IP Force**
2. External RFID Card Reader
3. 5 V power supply



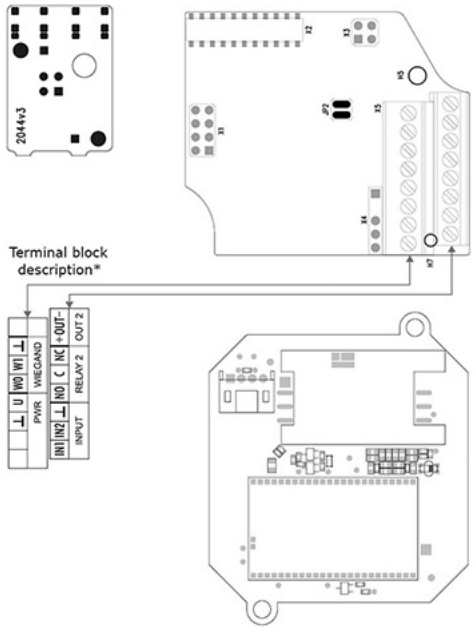

### Module Settings

Refer to the Configuration Manual for details of Wiegand, output and reader settings. Refer to the Automation manual for input, red LED and tamper switch settings and use.

## 13.56 MHz Internal RFID Card Reader, Wiegand

The Internal RFID Card Reader 13.56 MHz (Part No. 9151031, 02522-001) is used for reading RFID card Ids in the 13.56 MHz band, NFC supported.

## Specification




### Card Reader

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

- Operating frequency: 13.56 MHz
- Minimum reading distance: 30 mm above the **2N IP Force** surface

### Relay (SSR A, SSR B)

- NO contact max. 30 V / 1 A AC/DC

### Switched output

- 9.8 to 13.8 V DC according to power supply (PoE: 11.6 V; adapter: supply voltage minus 0,4 V), up to 400 mA

### Logical inputs

Active mode – requires external voltage (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN}$-ON = min. +2.5 V
- $U_{IN}$-OFF = max. +1.5 V
- $U_{IN}$ max. = +48 V

- $I_{IN}$ ($U_{IN}$ +48 V) = max. 1 mA

Passive mode – requires external contact only (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN1}$ = approx. 8.3 V
- $U_{IN2}$ = approx. 8.3 V
- $I_{LOOP}$ = approx. 0.5 mA

### Signaling output

- Internal red LED under the intercom front panel

### Power Supply

- For external RFID card reader
- 12 V DC ± 15% / 350 mA

### WIEGAND interface

- Off/Input/Output (as programmed)

| Wiegand Input Technical Parameters | |
|---|---|
| Current | 5 mA |
| Input resistance | 680 Ω |
| Pulse length | 50 µs |
| Inter-pulse interval | approx. 2 ms |

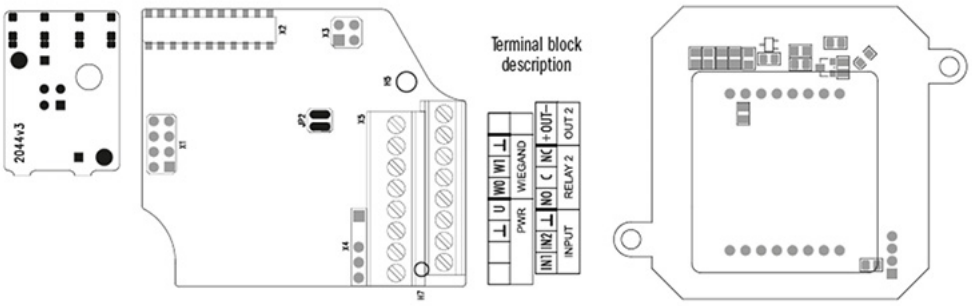
### Module Settings

Refer to the Configuration Manual for details of Wiegand, output and reader settings. Refer to the Automation manual for input, red LED and tamper switch settings and use.

## Internal secured RFID Card Reader 13.56 MHz, Wiegand

The 13.56 MHz Internal secured RFID Card Reader (Part No. 9151031S/01730-001) is used for reading RFID card IDs in the 13.56 MHz band, NFC supported.

## Specification




### Card Reader

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **HID PAC** (HID SEOS, HID iClass SE, iClass SR, HID MIFARE DESFire with SIO, HID MIFARE Classic with SIO)
- **My2N**
- **2N PICard**

- Operating frequency: 13.56 MHz
- Minimum reading distance: 30 mm above the **2N IP Force** surface

### Passive output

- Max. 30 V / 2A AC / DC

### Switched output

- 9 to 12 V DC according to power supply (PoE: 9 V; adapter: source voltage minus 1 V), up to 600 mA

### Logical inputs

Active mode – requires external voltage (JP2 jumper OFF)

- $U_{IN}$-ON = min. +2.5 V
- $U_{IN}$-OFF = max. +1.5 V
- $U_{IN}$ max. = +48 V

- $I_{IN}$ ($U_{IN}$ +48 V) = max. 1 mA

Passive mode – requires external contact only (JP2 jumper ON)

- $U_{IN1}$ = approx. 8.3 V
- $U_{IN2}$ = approx. 8.3 V
- $I_{LOOP}$ = approx. 0.5 mA

### Signaling output

- Internal red LED under the intercom front panel

### Power Supply

- For external RFID card reader
- 9 to 12 V / 350 mA depending on power supply

### WIEGAND interface

- Off/Input/Output (as programmed)

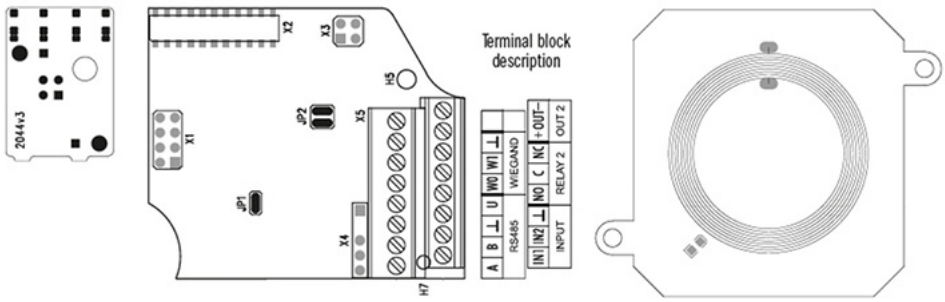
### Module Settings

Refer to the Configuration Manual for details of Wiegand, output and reader settings. Refer to the Automation manual for input, red LED and tamper switch settings and use.

## Internal RFID Card Reader 125 kHz, OSDP

The 13.56 MHz Internal Secured RFID Card Reader (Part No. 9151022, 03228-001) is used for reading RFID card IDs in the 125 kHz band. Provides communication between a connected OSDP device (control panel, door controller) and 2N device via the OSDP.

### Specification




### Card Reader

Supported RFID cards 125 kHz:

- EM4x02
- NXP HiTag2

- Operating frequency: 125 kHz
- Minimum reading distance: 30 mm above the **2N IP Force** surface

### Relay (SSR A, SSR B)

- NO contact max. 30 V / 1 A AC/DC

### Switched output

- 9.8 to 13.8 V DC according to power supply (PoE: 11.6 V; adapter: supply voltage minus 0,4 V), up to 400 mA

### Logical inputs

Active mode – requires external voltage (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN}$-ON = min. +2.5 V
- $U_{IN}$-OFF = max. +1.5 V
- $U_{IN}$ max. = +48 V
- $I_{IN}$ ($U_{IN}$ +48 V) = max. 1 mA

Passive mode – requires external contact only (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN1}$ = approx. 8.3 V
- $U_{IN2}$ = approx. 8.3 V
- $I_{LOOP}$ = approx. 0.5 mA

### Signaling output

- Internal red LED under the intercom front panel

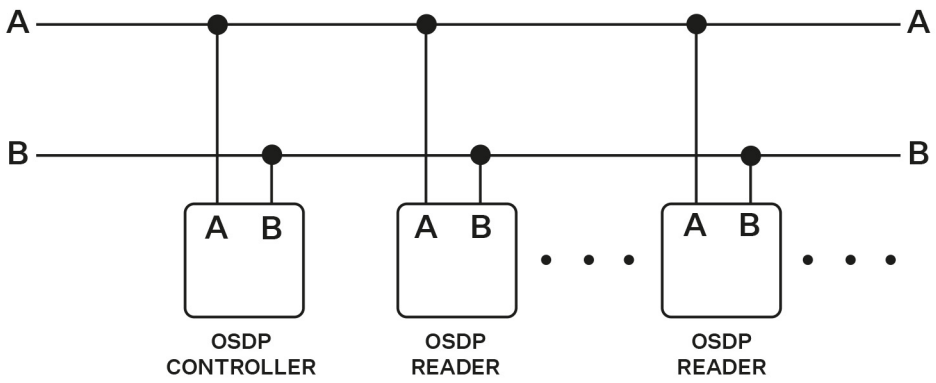
### Power Supply

- For external RFID card reader
- 12 V DC ± 15% / 350 mA

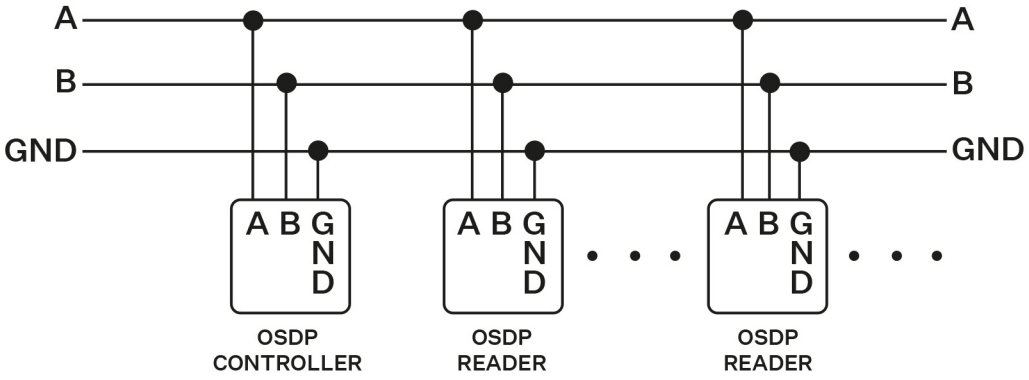
### OSDP Interface

- OSDP reader (software configurable)

## Wiring diagram for two-wire connection




## Wiring diagram for three-wire connection




### Module Settings

Refer to the Configuration Manual for OSDP, output and reader settings. Refer to the Automation manual for input, red LED and tamper switch settings and use.

## Internal RFID Card Reader 13.56 MHz, NFC, OSDP

The 13.56 MHz Internal RFID Card Reader, NFC, OSDP (Part No. 9151023, 03229-001) is used for reading RFID card IDs in the 13.56 MHz band, NFC supported. Provides communication between a connected OSDP device (control panel, door controller) and 2N device via the OSDP.

### Specification

### Card Reader

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

- Operating frequency: 13.56 MHz
- Minimum reading distance: 30 mm above the **2N IP Force** surface

### Relay (SSR A, SSR B)

- NO contact max. 30 V / 1 A AC/DC

### Switched output

- 9.8 to 13.8 V DC according to power supply (PoE: 11.6 V; adapter: supply voltage minus 0,4 V), up to 400 mA

### Logical inputs

Active mode – requires external voltage (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN}$-ON = min. +2.5 V
- $U_{IN}$-OFF = max. +1.5 V
- $U_{IN}$ max. = +48 V
- $I_{IN}$ ($U_{IN}$ +48 V) = max. 1 mA

Passive mode – requires external contact only (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN1}$ = approx. 8.3 V
- $U_{IN2}$ = approx. 8.3 V
- $I_{LOOP}$ = approx. 0.5 mA

### Signaling output

- Internal red LED under the intercom front panel

### Power Supply

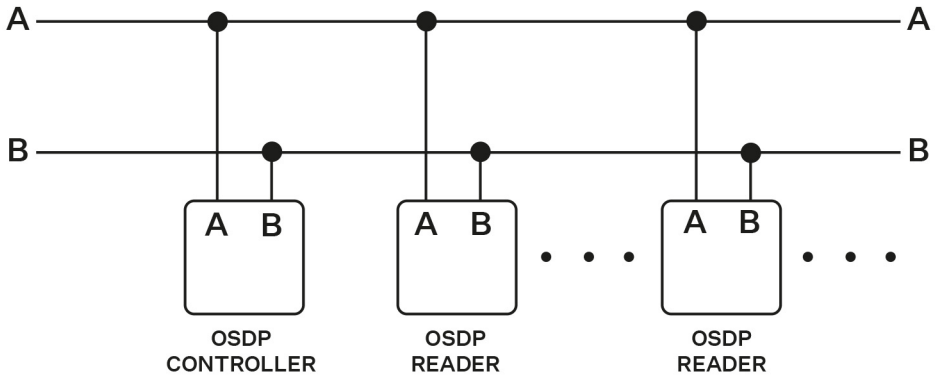
- For external RFID card reader
- 12 V DC ± 15% / 350 mA

### OSDP Interface

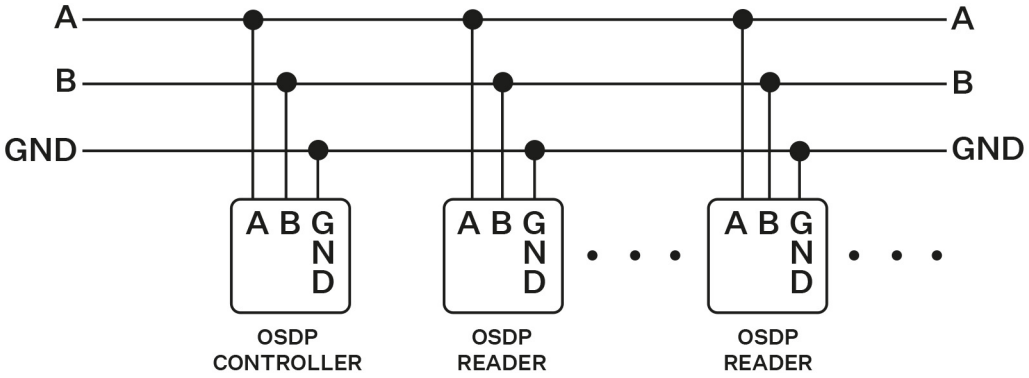
- OSDP reader (software configurable)

### Recommended wiring

### Wiring diagram for two-wire connection




### Wiring diagram for three-wire connection



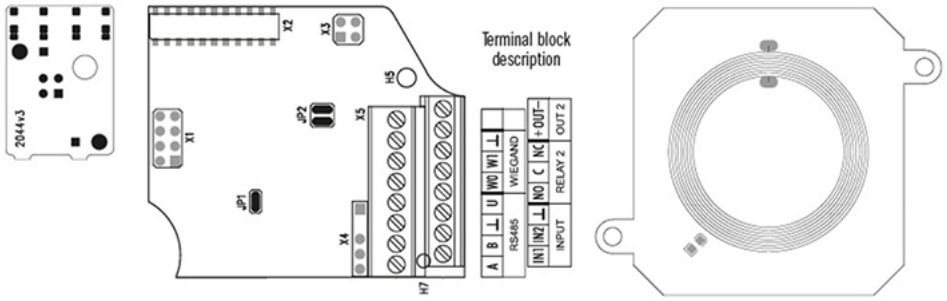

### Module Settings

Refer to the Configuration Manual for OSDP, output and reader settings. Refer to the Automation manual for input, red LED and tamper switch settings and use.

## Internal RFID Card Reader 13.56 MHz, NFC, OSDP

The 13.56 MHz Internal secured RFID Card Reader, NFC, OSDP (Part No. 9151023S, 03230-001) is used for reading RFID card IDs in the 13.56 MHz band, NFC supported. Provides communication between a connected OSDP device (control panel, door controller) and 2N device via the OSDP.

### Specification




### Card Reader

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **HID PAC** (HID SEOS, HID iClass SE, iClass SR, HID MIFARE DESFire with SIO, HID MIFARE Classic with SIO)
- **My2N**
- **2N PICard**

- Operating frequency: 13.56 MHz
- Minimum reading distance: 30 mm above the **2N IP Force** surface

### Relay (SSR A, SSR B)

- NO contact max. 30 V / 1 A AC/DC

### Switched output

- 9.8 to 13.8 V DC according to power supply (PoE: 11.6 V; adapter: supply voltage minus 0,4 V), up to 400 mA

## Logical inputs

Active mode – requires external voltage (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN}$-ON = min. +2.5 V
- $U_{IN}$-OFF = max. +1.5 V
- $U_{IN}$ max. = +48 V
- $I_{IN}$ ($U_{IN}$ +48 V) = max. 1 mA

Passive mode – requires external contact only (jumper JP1 for IN1, pins 3–4 are open, jumper JP1 for IN2, pins 1–2 are open)

- $U_{IN1}$ = approx. 8.3 V
- $U_{IN2}$ = approx. 8.3 V
- $I_{LOOP}$ = approx. 0.5 mA

## Signaling output

- Internal red LED under the intercom front panel

## Power Supply

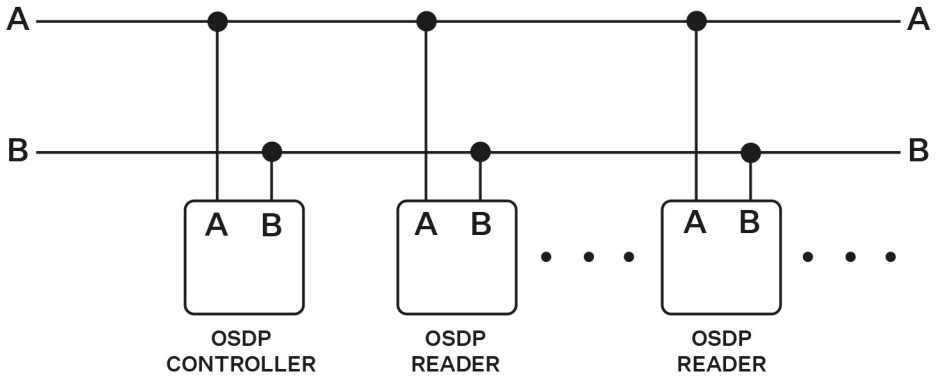
- For external RFID card reader
- 12 V DC ± 15% / 350 mA

## OSDP Interface

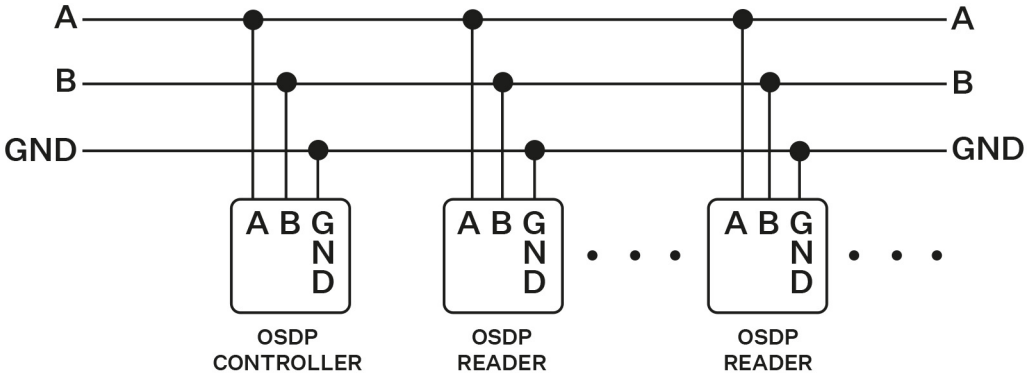
- OSDP reader (software configurable)

### Recommended wiring

### Wiring diagram for two-wire connection




### Wiring diagram for three-wire connection




### Module Settings

Refer to the Configuration Manual for OSDP, output and reader settings. Refer to the Automation manual for input, red LED and tamper switch settings and use.

## Internal Induction Loop

The internal induction loop (Part No. 9151021, 02338-001) is one of the **2N IP Force** extending modules, which is used for people with disabled hearing equipped with a special hearing aid that receives reproduced sound via a magnetic field sensor.

## Compatibility

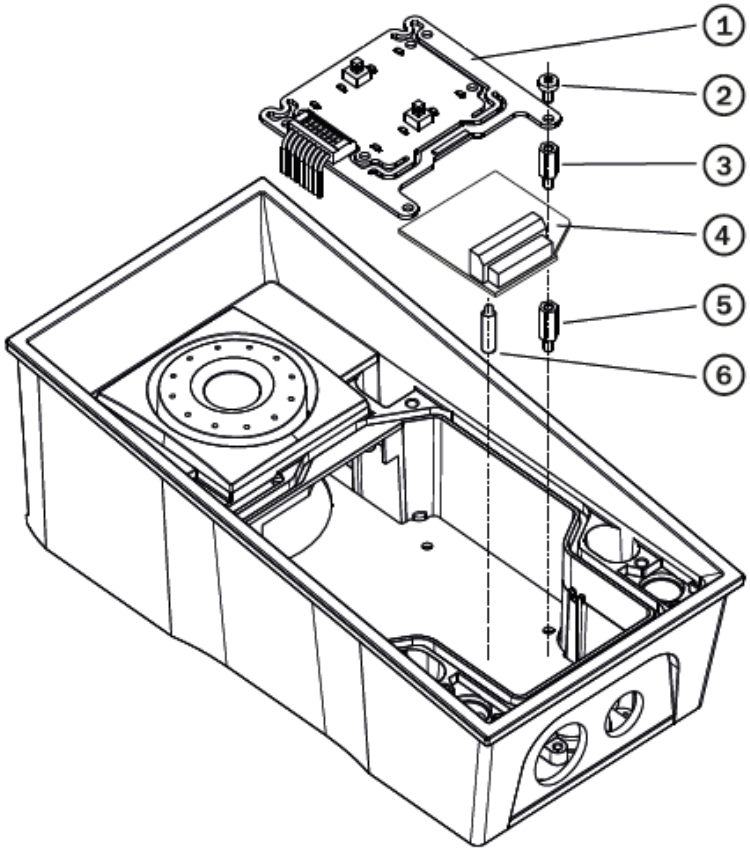
**CAUTION**

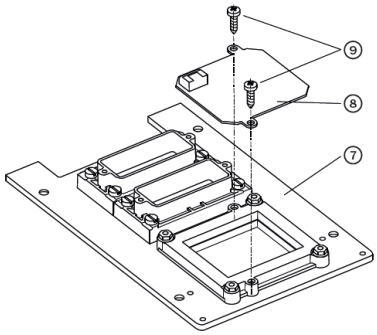
- Where an internal induction loop is used, an RFID card reader cannot be inserted in the device.
- If the additional and tamper switches are installed at the same time, no internal induction loop or RFID card reader can be installed in addition to them.

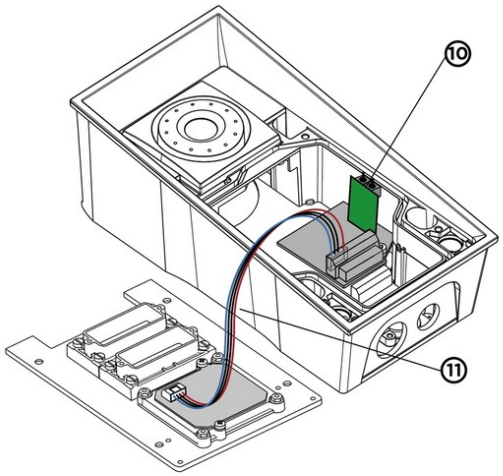
The module is compatible with the basic units with Part No.:

- 9151101RPW
- 9151101CHRPW
- 9151102CHRW
- 9151102RW

## Installation






1. Turn off the device.
2. Remove the front panel (7) from the device.
3. Mount the antenna board (8). Use the two enclosed screws (9).
4. Plug the enclosed cable (11) to the antenna board connector.
5. Demount the button PCB (1). Do not disconnect its cable!
6. Dismount the right-hand bottom spacer (there are four spacers altogether).
7. There are two short plastic spacers enclosed to the induction loop. Take the shorter, 6,5 mm long spacer. Screw it into the free hole on the motherboard.
8. Plug the enclosed plastic support (6) into the reader board from the bottom side.
9. Put the reader board (4) in the motherboard connector. Make sure that the screw hole is directly above the spacer.
10. Screw in the remaining metal spacer (3), which is 10.5 mm long.
11. Fit the button PCB (1) back to its position using the original screws.
12. If you want to use the tamper switch (to detect unauthorized case opening for theft protection), insert the tamper board (10) in the connector located in the right-hand bottom part of the switch board (4). As the tamper switch shares the Relay2 NO and NC terminals, you cannot use the RELAY2 output and the tamper switch at the same time.
13. Plug the antenna cable (11) to its connector at the reader board (4).
14. Replace the front panel and tighten all the four screws.

## Induction Loop external

External inductive loop (Inductive loop amplifier – Part No. 9159050, 01391-001, Inductive loop amplifier without accessories – Part No. 9159054, 12 V DC power adapter – Part No. 9159052, 01393-001) is used for reading RFID card IDs in the 13.56 MHz band, with NFC support. Provides communication between a connected OSDP device (control panel, door controller) and 2N device via the OSDP.

## Specification

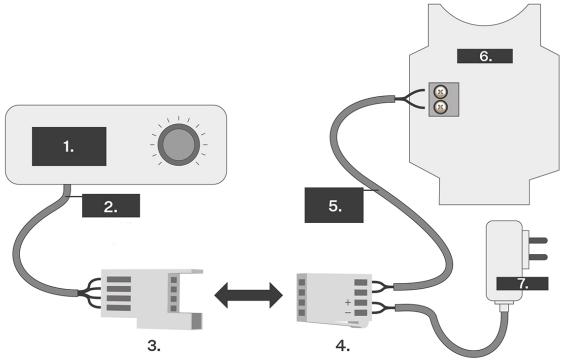
- Supply voltage: : 8–18 V DC
- Supply current at 12 V supply:
  - 1 Ω load, full power output; 1.4 A, sine wave signal; 1 A, pink noise signal
  - 8 Ω load, half power output; 550 mA, sine wave signal; 1.4 A, sine wave signal; 400 mA, pink noise signal
  - no signal; 100 mA
  - standby; max. 10 mA
- Switch to standby without signal: 10 s

- Basic input level: 100 mV – 6 Vef
- Increased input level: 1 V – 35 Vef
- Input impedance: 2 kΩ parallel with 0.3 H
- Output current, 1 Ω load: 2.2 Aef (sine)
- Full power: 1.6 Aef (pink noise)
- Output current, 8 Ω load: 730 mAef sine wave signal
- Half power: 520 mAef pink noise signal
- Output short-circuit resistance: unlimited time
- Frequency characteristics: 100 Hz – 5 KHz ±3 dB
- Temperature range: −20 to +50 °C
- Covering: IP65 (with round cable of 5–10 mm diameter)
- Dimensions: 144 x 100 x 31 mm
- Weight: 0.3 kg

## Installation

The induction loop amplifier can be wall mounted with the use of an internal induction loop where a signal covering is requested. Outdoor use is possible thanks to the IP65 covering. A four-wire cable of the length of one meter is mounted to the supplied product for easier connection to the intercom. In the cable there are two wires for 12 V DC supply and two wires for signal input, the wires are connected into interconnection connector. If you shorten the cable, follow the color marking.

1. Before wall mounting the amplifier, run the cable through the hole that you have prepared. Indicate the position of the holes for installation, the two holes on the front.
2. Remove the amplifier and drill the mounting holes.
3. Use the plugs and screws included in the delivery. Use a drill of the diameter of 6 mm.
4. After fastening, cover the screws with the blanks supplied.
5. Use the supplied connectors to connect the amplifier to the intercom and power supply.
6. The A connector is connected to the amplifier four-wire cable.
7. Insert a special intercom-connecting cable supplied with the amplifier and 12 V power supply outlets to the B connector. Connect the special cable to the intercom and connect the power supply to the mains.
8. You can place the mated A and B connectors into the 2N device cover. The connectors help you connect stripped cables. Open the connector by pushing a thin screwdriver onto the white spots at its front and close the connector by sliding the movable part through a side gap.
9. Finally, test the amplifier function using a suitable receiver for hearing impaired persons or magnetic field communication tester. No other settings are required.




1. Amplifier with pre-installed cable
2. Four-wire cable
   - IN1 – brown
   - IN2 – white
   - +12 V – yellow
   - 0 V – green
3. Connector A
4. Connector B
5. Connecting cable
6. 2N intercom
7. Power supply

## Additional Switch

The Additional Switch (Part No. 9151010, 01350-001) is used for extending the count of inputs/outputs.

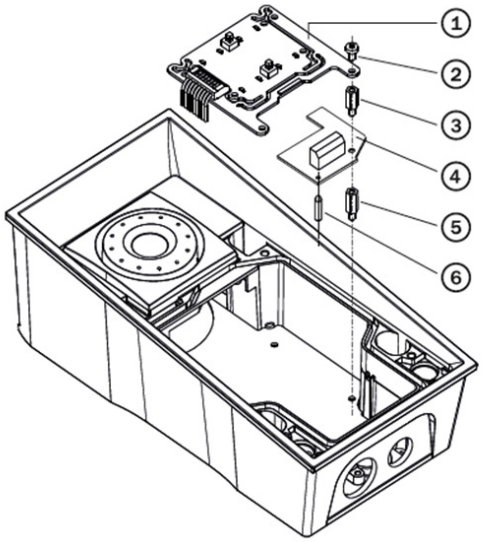
**CAUTION**
If the Additional Switch is installed, it is not possible to install the Internal RFID Card Reader.

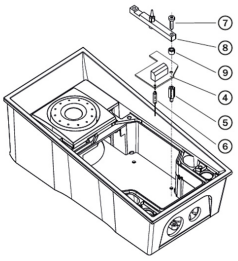
## Features

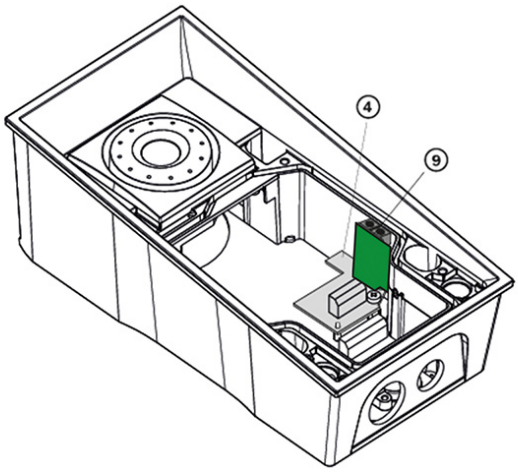
- The **2N IP Force** Additional Switch adds two additional switches, one logical input and a tamper switch to the main unit.
- The purpose of the tamper switch is to signal any unauthorized opening of the device (to prevent a theft, e.g.). It is recommended to use the tamper switch.

**TIP**
FAQ: Tamper Switch - How to Connect It to 2N IP Intercom

## Installation





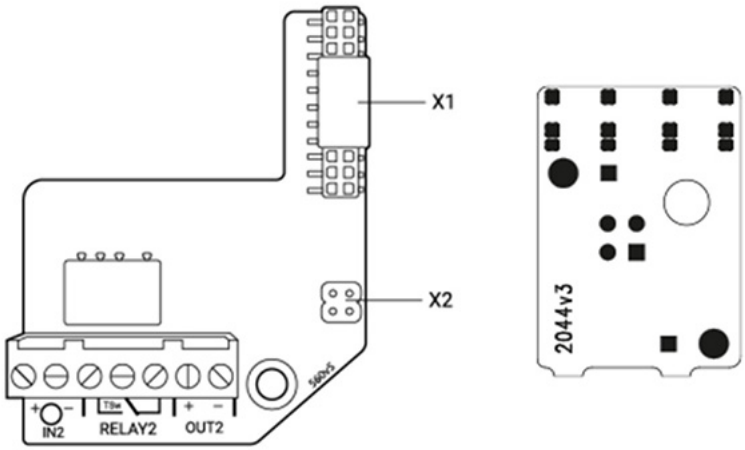

1. Turn off the device.
2. Remove the front panel from the device.
3. According to your model:
   a. If you are mounting the switch into a two-nameplate model, demount the button PCB (1) and remove the right-hand bottom spacer (there are four PCB fitting spacers altogether).
   b. If you are mounting the switch into a keypad model, take the keypad out of the holder. Demount the right-hand keypad holder - beam with a pin (8) – remembering its position. Demount the right-hand bottom spacer. Do not disconnect the button cable!
   c. If you are mounting the switch into a model other than the two ones mentioned in items 3a and 3b above, remove the right-hand bottom screw from the motherboard.
4. Screw the enclosed 12 mm spacer (5) into the vacated motherboard slot.
5. Mount the enclosed plastic support (6) onto the switch board bottom side.
6. Put the switch board (4) in the motherboard connector. Make sure that the screw hole is directly above the spacer.
7. According to your model:
   a. If you are mounting the switch into a two-nameplate model, fit the switch board with the enclosed 10.5 mm spacer (3) and reinstall the button PCB (1).
   b. If you are mounting the switch into a keypad model, reinstall the beam (8) of the keypad holder (the pin is on the top). Insert the enclosed 4.5 mm washer (9) between the beam and the switch board, fitting the assembly with the 15 mm screw enclosed (7).
   c. If you are mounting the switch into a model other than the two ones mentioned in items 7a and 7b, fit the switch board with the original 6 mm screw (2).
8. If you want to use the tamper switch, insert the tamper board (9) in the connector located in the right-hand bottom part of the switch board (4). As the tamper switch shares the RELAY2 NO and NC terminals, you cannot use the RELAY2 output and the tamper switch together.
9. Replace the front panel and tighten all the four screws.

## Module Settings

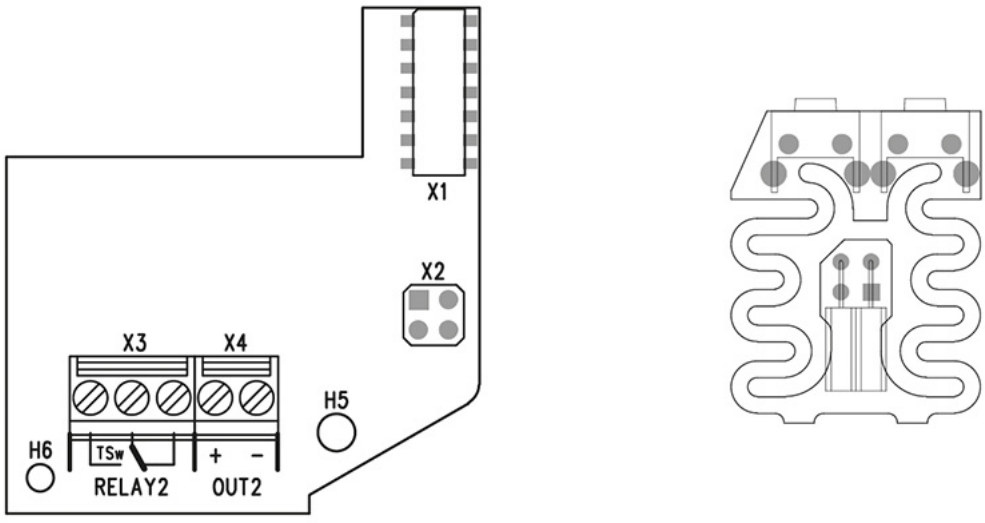
Refer to the Configuration Manual for details.

## Connection

### Version 5




### Version 4 and lower



## Security Relay

The Security Relay (9159010, 01386-001) is used for enhancing security between **2N IP Force** and the connected electric lock. The Security Relay significantly enhances security of the connected electric lock by preventing unlocking due to device tampering.

**TIP**
FAQ: 2N Security Relay – description of the device and use with the 2N intercoms

## Specification

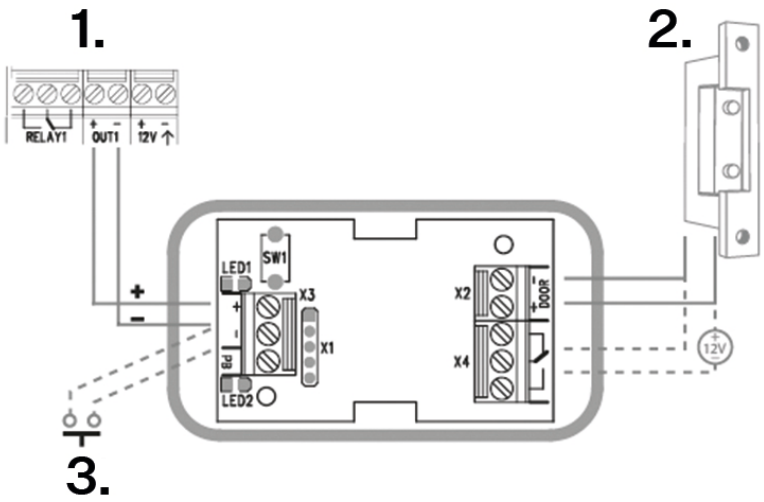
| | |
|---|---|
| Passive switch | NO/NC contact, up to 30 V / 1 A AC/DC |
| Switched output | • Where the Security Relay is fed from the device, 8 to 12 V DC is available on the output depending on the power supply, 400 mA DC.<br>  • PoE: 10 V<br>  • adapter: source voltage of minus 2 V<br>• Where the Security Relay is fed from an external power supply, 12 V / 700 mA DC is available on the output. |
| Dimensions | 66.5 × 32.5 × 20.5 mm |
| Weight | 24 g |

## Connectors and Installation

The Security Relay is installed between the device (outside the secured area) and the electric lock (inside the secured area). The Security Relay includes a relay that can only be activated if a valid access card/code is detected on the unit.

The Security Relay is installed on a two-wire cable between the device and the electric lock inside the area to be secured (typically behind the door). The Security Relay is powered and controlled via this two-wire cable and can thus be added to an existing installation. Thanks to its compact dimensions, the device can be installed into a standard mounting box.

The Security Relay is designed with holes for surface anchoring. It is recommended that a screw of the diameter of 3 mm with a lens head of the diameter of 6 mm is used. Using a countersunk head may cause irreversible damage to the plastic cover!




1. **2N IP Force**
2. Door lock
3. Departure button

Connect the Security Relay to the access unit as follows:

- To the Active output

Connect the electric lock to the Security Relay as follows:

- to the switched output
- to the passive output in series with the external power supply

The Security Relay also supports the Departure button connected to the ‘PB’ and ‘– 2N IP intercom’ terminals. Once the Departure button is pressed, the output is activated for 5 seconds.

https://www.youtube.com/embed/ardukvQzw5A

## Status Signaling

| Green LED | Red LED | State |
|---|---|---|
| flashing | off | Operational mode |
| on | off | Activated output |
| flashing | flashing | Programming mode – waiting for initialization |
| on | flashing | Error – wrong code |

## Configuration

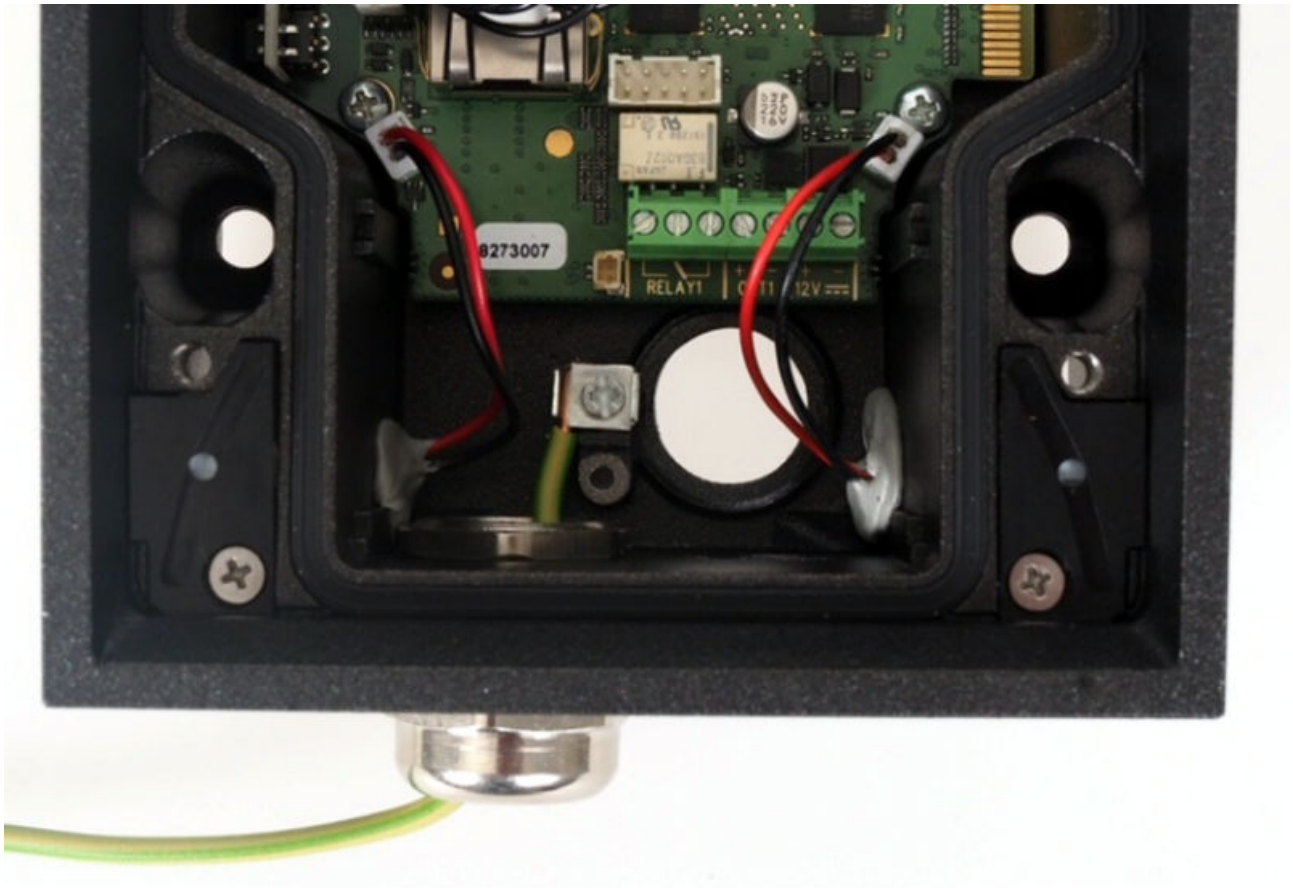
1. Connect the Security Relay to the properly set Security output of the device. Refer to the Configuration Manual for details. Make sure that one LED at least is on or flashing.

2. Press and hold the Relay RESET button for 5 seconds to switch the device in the programming mode (red and green LEDs flashing).
3. Activate the output switch using the keypad, telephone, etc. The first code sent from the device will be stored in the memory and considered valid. After code initialization, the Security Relay will pass into the operational mode (green LED flashing).

**CAUTION**
Having reset the factory defaults on a device with firmware 2.18 or higher, remember to reprogram Security Relay using the instructions above.

## Grounding

To increase the static electricity resistance, you need a cable of the minimum cross-section of 4 $mm^2$. Connect the cable to the terminal in the bottom part of the device as shown in the figure below. The terminal is included in the delivery.




## Installation Completion

1. Having connected all the wires, make sure that the bushings, if used, are tightened properly and the RJ-45 connector is inserted in the PCB connector.

2. Replace the front cover carefully. Make sure that the connector is inserted correctly and the wires inside the device leave enough space for the board if you are installing a four-button board. Tighten the four screws thoroughly to push the panel by about 1 mm to fit tightly to the metal chassis. You can use the wrench included in package for tightening (Torx 20). Keep the maximum tightening torque of 1.5 Nm.

**WARNING**

- Properly installed device is waterproof. An incorrectly made installation may compromise the device waterproofness. Water infiltration may damage the electronic part.
- Stainless steel screws are used for the **2N IP Force** assembly. Other screws than stainless steel ones corrode soon and may aesthetically deteriorate the surrounding environment!

# Name Tags

## Name Tag Printing

1. A sheet of translucent foil is en closed to every device. Print it using a laser printer.
2. Cut the printed foil and insert the nametags in the buttons. Every name plate includes a piece of foil, which can be written over manually, using a waterproof permanent marker, if necessary.

**TIP**

Refer to the Support > Download Center section at 2N.com for the name tag printing template.

•

## Name Tag Insertion/Replacement

The advantage of **2N IP Force** is its intuitive, simple access to name tags. There is no need to remove the front panel for replacement and so there is no risk of losing parts.

1. Loosen the name plate screw using the wrench enclosed, for example. You can open the name plate window like a door without losing the tightened screw.
2. Remove the used or blank name tag and insert a new tag.
3. Close the name plate window and tighten the screw appropriately.
4. Check the click effect of the button: if the button fails to click properly when pressed (when moved by approx. 0.5 mm), the tag is too thick or thin. Make sure that the button clicks when you press it on both ends.

# Nametag Insertion/Replacement

The advantage of **2N IP Force** is its intuitive, simple access to name tags. There is no need to remove the front panel for replacement and so there is no risk of losing parts.

1. Loosen the name plate screw using the wrench enclosed, for example. You can open the name plate window like a door without losing the tightened screw.
2. Remove the used or blank name tag and insert a new tag.
3. Close the name plate window and tighten the screw appropriately.
4. Check the click effect of the button: if the button fails to click properly when pressed (when moved by approx. 0.5 mm), the tag is too thick or thin. Make sure that the button clicks when you press it on both ends.

## Tactile stickers

Special tactile stickers with raised surfaces are included in the package. These stickers help people with visual impairments to recognize the basic controls of the device.

We recommend placing the sticker on the primary quick dial button. Place the sticker on the button edge and adjust the text on the label as needed to make it legible and not obscured by the sticker.

**NOTE**
Clean the device surface from dust and dirt before applying the sticker.

# Brief Guidelines

## Device Configuration Interface Access

**2N IP Force** 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.

Refer to the Configuration Manual for 2N IP Intercoms for the device configuration details.

### 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 IP Force:** 2NIPForce-{serial number without dashes}.local (e.g.: “2NIP-Force-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.

### IP address

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

- Use the freely accessible 2N IP Utility.
- Use hardware (RESET button).
- Use the Speed Dial button.

### Web Configuration Interface Login

1. Fill in the **2N IP Force** address or domain name into the internet browser.
   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.

## Configuration via Hardware

The RESET button helps you reset the factory default values, restart the device, retrieve the device IP address and switch the IP address static/dynamic mode.

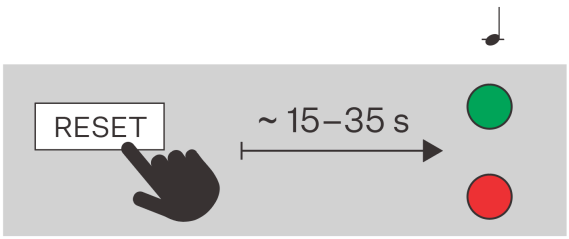
### Device Restart

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

### IP Address Retrieval Using Hardware

Follow the instructions below to retrieve the current IP address:

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).
2. Release the RESET button.
3. The device announces the current IP address via the speaker automatically.

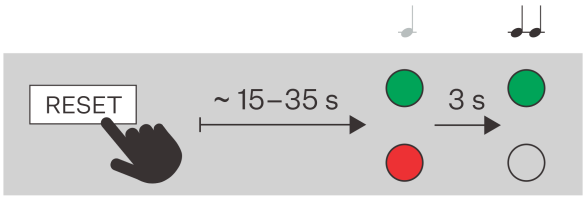



**NOTE**
The delay after pressing RESET till the first light and sound signaling is set to 15–35 s depending on the device model used.

## Static IP Address Setting with RESET Button

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

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).
2. Release the RESET button.



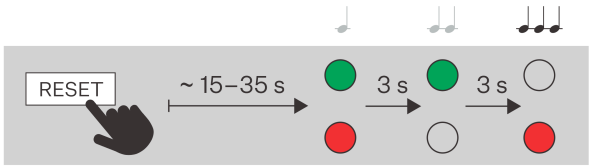

**NOTE**
The following network parameters will be set after restart:

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

## Dynamic IP Address Setting via RESET

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

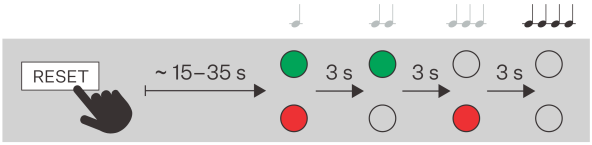
1. Press the button RESET and keep it pressed.
   a. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard (approx. 15–35 s).
   b. Wait until the red LED goes off and an acoustic signal can be heard (approx. for another 3 s).
   c. Wait until the green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



**NOTE**
The default network parameters will be set after restart.

### 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.




## IP Address Retrieval

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

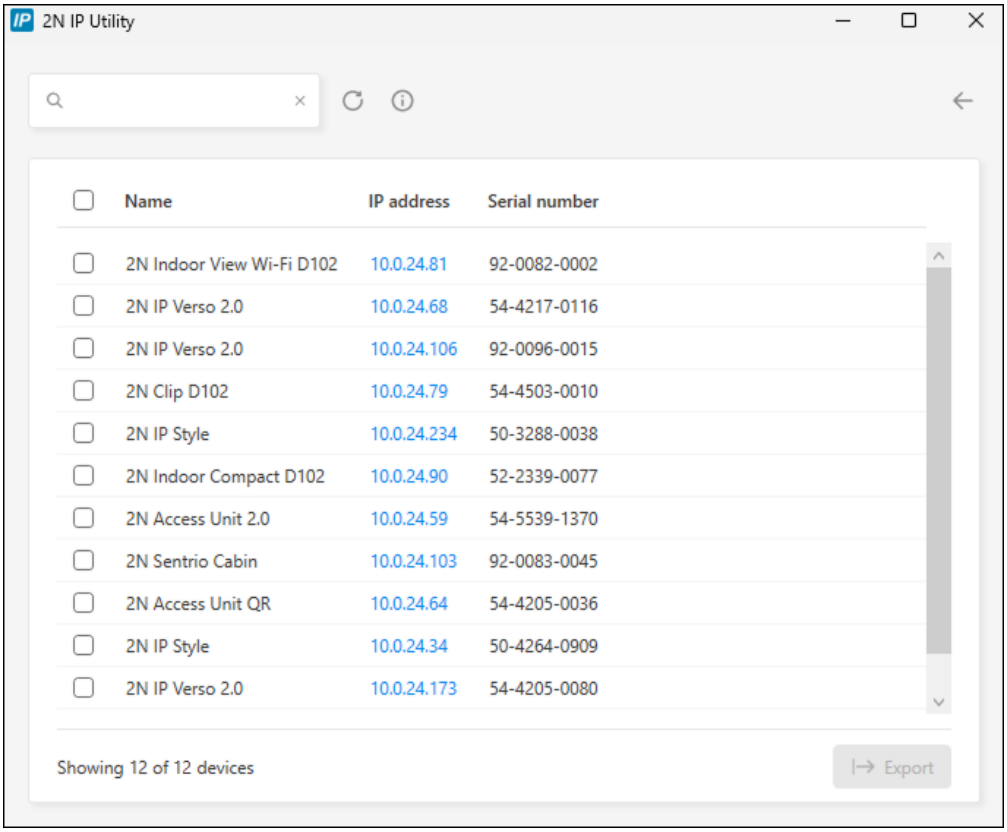
- Use the freely accessible 2N IP Utility.
- Use hardware (RESET button).
- Use the Speed Dial button.

### IP Address Retrieval Using 2N IP Utility

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

1. Run the 2N IP Utility installer.
2. The Installation Wizard will help you with the installation.

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




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

**TIP**

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

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

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

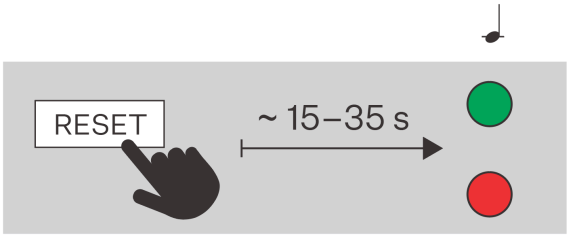
For increased password security, it is recommended that:

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

## IP Address Retrieval Using Hardware

Follow the instructions below to retrieve the current IP address:

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).
2. Release the RESET button.
3. The device announces the current IP address via the speaker automatically.




**NOTE**
The delay after pressing RESET till the first light and sound signaling is set to 15–35 s depending on the device model used.

## IP Address Retrieval Using Speed Dial Button

Take the following steps to retrieve the **2N IP Force** IP address:

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Press the Quick dial button 5 times on the main unit.
3. The device reads its IP address.

**NOTE**

- If the address is 0.0.0.0, it means that the device has not obtained the IP address from the DHCP server.
- Press the button sequence within 30 seconds after the sound signal for security reasons. Up to 2 s intervals are allowed between the presses.

# Device Static/Dynamic IP Address Switching with Speed Dial Button

Take the following steps to reset the network settings and switch the static IP address (DHCP OFF) / dynamic IP address (DHCP OFF) mode in the device network configuration:

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the first sound signal.
3. Press the first Speed dial button 15 times on the main unit.

**NOTE**
After the static address mode is switched on, the basic network parameters are reset to the following default values:

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

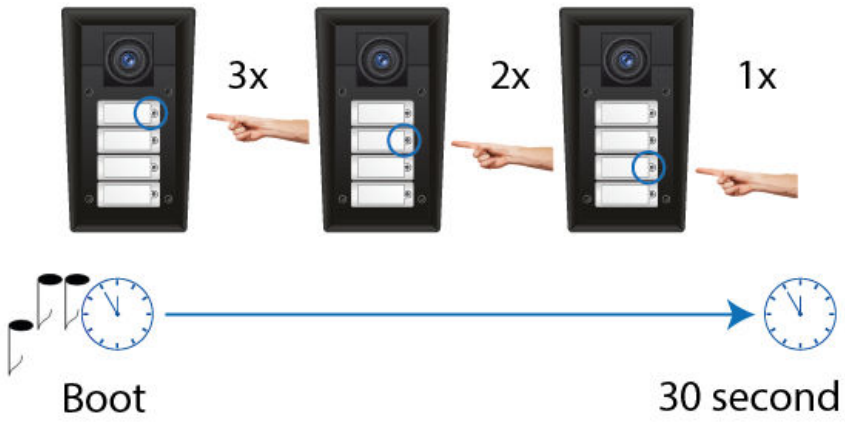
## 4-Button Models

### Static IP Address Setting with RESET Button

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

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the first sound signal .

3. Press buttons 1, 1, 1, 2, 2, 3 sequentially.




**CAUTION**
Be sure to press the button sequence within thirty seconds after the sound signal for security reasons. Up to 2 s intervals are allowed between the presses.

4. The acoustic signal indicates mode switching.
5. Wait until the device is restarted automatically.

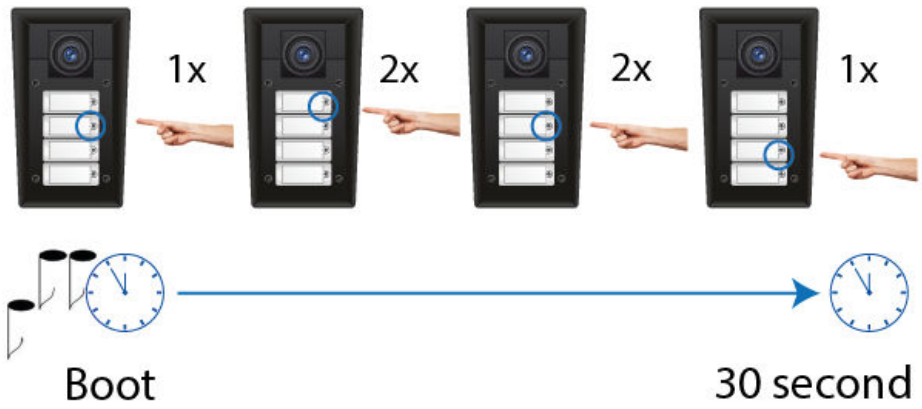
**NOTE**
After the static address mode is switched on, the basic network parameters are reset to the following default values:

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

## Dynamic IP Address Setting via RESET

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the first sound signal .

3. Press buttons 2, 1, 1, 2, 2, 3 sequentially.




**CAUTION**
Be sure to press the button sequence within thirty seconds after the sound signal for security reasons. Up to 2 s intervals are allowed between the presses.

4. The acoustic signal indicates mode switching.
5. Wait until the device is restarted automatically.

## 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

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. 84) for login details. Restart the device in System > Maintenance > System using Restart device.

## Firmware Update

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

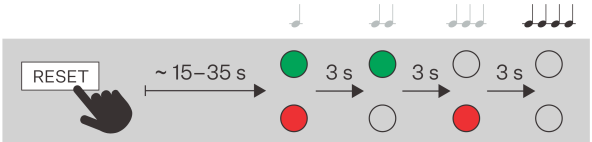
Update firmware via the web configuration interface in System > Maintenance, refer to the device Configuration Manual.

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

**TIP**
You can make bulk updates for multiple devices via 2N Access Commander.

## 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.




## Factory Default Reset (version 555v3)

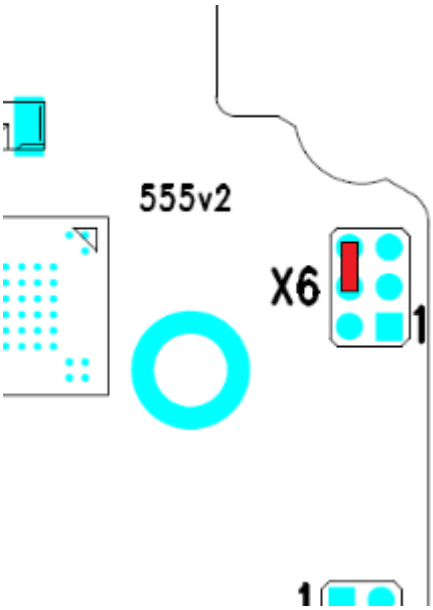
For resetting device to default settings press and hold SW1 button. Wait for the first sound signalization and then release the button. If you press the button for short time device will reboot only.

**WARNING**
Having reset the factory defaults on a device with firmware 2.18 or higher, remember to reprogram Security Relay using the instructions above.

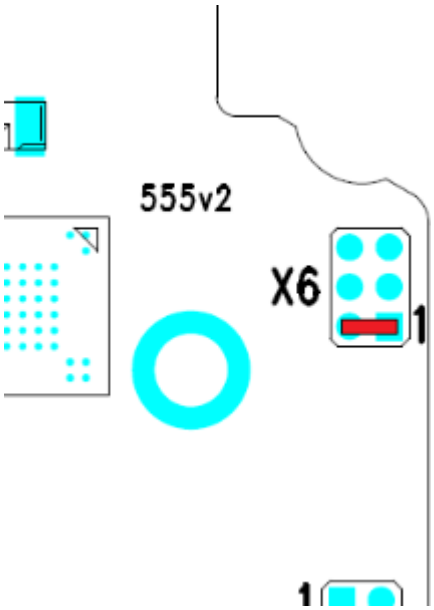
# Factory Default Reset (version 555v2)

1. Disconnect the device from the power supply.
2. Move the short-circuit jumper on connector X6 into the Default setup position. Configuration jumpers (X6) are located in the right-hand upper corner of the PCB.
3. Reconnect the power supply and wait for a start signalling sound.
4. Disconnect the device from the power supply.
5. Move the short-circuit jumper on connector X6 into the Normal operation position.
6. Reconnect the power supply. The device will be reset to factory default.

**Configuration jumpers X6, PCB version 555v2 – Normal Operation**




**Configuration jumpers X6, PCB version 555v2 – Factory Reset**




**WARNING**
Having reset the factory defaults on a device with firmware 2.18 or higher, remember to reprogram Security Relay using the instructions above.

# Call Connection

To make calls with other terminal devices in IP networks, it is necessary to assign the device to a contact in the Directory.

## Connection with 2N Devices in LAN

1. Make sure that Local calls is enabled on both the 2N devices.
2. 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.
3. Edit the following:
   - a virtual number to start a call by entering the number via your numerical keypad
   - basic information and access options for the device user

4. To dial calls using a device button, assign the selected user to the speed dial button in **Calls > Dialing**, refer to Speed dial buttons.
5. Make sure that Local calls is enabled on the called 2N device to make a successful call.

## Connection with Other Devices

1. Click Add user or open the existing contact detail to create a new contact.
2. Click the pencil icon next to the Phone number to open phone number editing.
3. Enter the calling destination address into the destination field to which the call is to be routed. Complete the target IP address or SIP URI in the format " user_name@host" (e.g.: "johana@2.255.4.255" or "johana@calls.2N.com"). For local calls, fill in the called 2N device ID as specified in the Local calls tab in the called device web configuration interface.
4. Edit the following:
   - a virtual number to start a call by entering the number via your numerical keypad
   - basic information and access options for the device user
5. To dial calls using a device button, assign the selected user to the speed dial button in **Calls > Dialing**, refer to Speed dial buttons.
6. Make sure that the call transmitting service is enabled on the called 2N device to make a successful call.

**TIP**

- Each user can be assigned up to 3 phone numbers. In case the first user fails to answer, the call is forwarded to the next number. Alternatively, you can set calling to multiple phone numbers simultaneously. Check Call in group between the selected numbers to set such multiple phone number calling for one user.
- In case all the user phone numbers are unavailable, you can set call forwarding to **Deputy**.
- Users can be gathered in calling groups. The calling group name is shown in the phone book on the device display. You can assign a calling group to a quick dial button. To terminate an outgoing group call after the first rejection from any of the called users, set this function in Calls > General Settings.

# Device Control

**2N IP Force** is an intercom allowing you to:

- call other devices
  - use quick dial buttons
  - dial phone number
- receive and reject incoming calls
- activate switch (e.g. door opening, lift control, etc.)
  The device works as an authorization intermediary, which authenticates the user access rights and, if the user access is valid, activates the switch. The door lock, lifts etc. can be controlled by the switch.

  The device control depends on the product version:

  - using RFID cards and chips – by tapping a card/chip on the device,
  - using NFC,
  - by entering a numeric access code via a keypad application

## Speed Dial Buttons

By pressing the speed dial button on the main unit, you can make a quick call to the assigned position in the phone book, see the Intercom Configuration > Calling > Dialing chapter in the Configuration Manual.

Call setup is signaled by a long intermittent tone or otherwise as configured in the PBX connected.

Pressing the same button repeatedly during or while making a call can be assigned the function of hanging up or hanging up simultaneously with a call to the next phone number of the called party. Alternatively, pressing the same button repeatedly may have no function, see **Intercom Configuration > Calling > General Settings** in the Configuration Manual.

For keypad equipped models, you can also hang up the call at any time by pressing # if enabled so by the Button function during an outgoing call parameter, see **Intercom Configuration > Calling > General Settings** in the Configuration Manual.

## Calling to Phone Book Position

The Phonebook **2N IP Force** can contain up to 1 999 pre-programmed positions. Depending on the number of speed dial buttons actually installed, you can call a given number of positions in the phone book. The remaining positions can be retrieved via the numeric keypad if the **Speed dial using digits** is enabled in configuration.

1. Enter the position number using your numeric keypad (05, 15, 200 e.g. – two digits at least and four digits at most) and press * for confirmation.
2. For keypad equipped models, you can also hang up the call at any time by pressing # if enabled so by the Button function during an outgoing call parameter, see **Intercom Configuration > Calling > General Settings** in the Configuration Manual.

## Calling to User-Defined Phone Number

If the **Phone Function Enable** parameter is set, you can use the numeric keypad to call a user-entered phone number.

1. Press the * button.

2. You will hear a continuous tone from the speaker.
3. Enter the telephone number using the numerical keypad and repress * for confirmation.
4. For keypad equipped models, you can also hang up the call at any time by pressing # if enabled so by the Button function during an outgoing call parameter, see **Intercom Configuration > Calling > General Settings** in the Configuration Manual.

## Incoming Call Answering/Rejecting

If the automatic incoming call answering function is turned off, an incoming call is signaled by a loud ringing tone. Push the * button to answer the call and the # button to reject the call.

## Door Opening (Switch Activation) by Code

**2N IP Force** is equipped with a door unlocking switch. Enter the valid code (refer to Subs. Switchesof the Configuration Manual for IP Intercoms) using the numeric keypad to activate this switch.

1. Enter the switch activating numeric code using the numeric keypad and press the * button for confirmation.
2. A valid code is notified by a continuous switch activation tone or a predefined unlocking user sound. An invalid code or interruption longer than as defined in **Timeout for Entering Numbers** is signaled acoustically ♩♩♩ or using a user sound.

# Troubleshooting

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

# Technical Parameters

| Power supply types | |
|---|---|
| PoE | IEEE PoE 802.3af (Class 0, max. 12,95 W) (Class 0, max. 12.95 W) |
| External supply | 12 V ±15 % / 2 A DC |

| Signaling protocol | |
|---|---|
| SIP | UDP, TCP, TLS |

| Buttons | |
|---|---|
| Button design | Transparent, white backlit buttons with easily replaceable nametags |
| Button count | 1, 2 or 4 |
| Numeric Keypad | Optional |

| Audio | |
|---|---|
| Microphone | 2 integrated |
| Amplifier | 10 W (class D) |
| Speaker | 10 W |
| Sound pressure level (SPL max) | 78.5 dB (1 W model, for 1 kHz at 1 m); 94 dB ± 3 % (10 W model, for 1 kHz at 1 m) |

| Audio | |
|---|---|
| Volume Control | Adjustable with automatic adaptive mode |
| Full duplex | Yes (AEC) |

| Audio stream | |
|---|---|
| Protocols | • RTP<br>• RTSP |
| Codecs and Used Bandwidth | • G.711 (PCMA, PCMU) – 64 kbps (with 85.6 kbps headers)<br>• G.729 – 16 kbps (with 29.6 kbps headers)<br>• G.722 – 64 (with 85.6 kbps headers)<br>• L16/16kHz – 256 kbps (with 277.6 kbps headers) |

| Camera | |
|---|---|
| Sensor | 1/3" color CMOS |
| JPEG resolution | Up to 1280 x 960 |
| Video resolution | 640 x 480 |
| Frame rate | 30 fps |
| Sensor sensitivity | 5.6 V/lux-sec (550 nm) |
| Viewing angle | 135° (H), 109° (V) |
| Infrared illumination | Yes |
| Focal length | 2.3 mm |

| Video stream | |
|---|---|
| Protocols | • RTP<br>• RTSP<br>• HTTP |
| ONVIF/RTSP streaming codecs | • H.264<br>• MPEG-4<br>• MJPEG |
| IP Camera Function | Yes – compatible profiles:<br>• ONVIF v2.4 profile S |

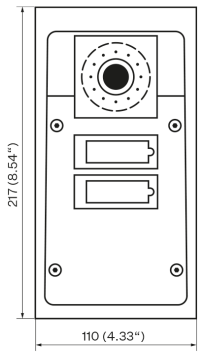
| Interface | |
|---|---|
| LAN | 10/100BASE-TX with Auto-MDIX, RJ-45 |
| Recommended cabling | Cat-5e or higher |
| Supported protocols | SIP2.0, DHCP opt. 66, SMTP, 802.1x, RTSP, RTP, TFTP, HTTP, HTTPS, Syslog, ONVIF |
| Passive switch (relay) | NO/NC contact, up to 30 V / 1 A AC/DC |
| Active switch output | 8 to 12 V DC according to power supply, up to 600 mA<br>• PoE: 10 V<br>• adapter: source voltage –2 V |

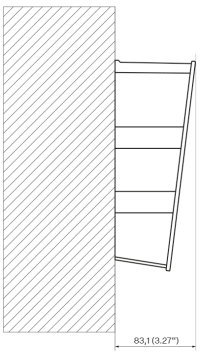
| Mechanical Parameters | |
|---|---|
| Cover | Robust aluminum cast product<br>Color:<br>• metallic black, semi-matt (not RAL) |
| Front Panel | Aluminum cast<br>• Fiberglass FR4 |

| Mechanical Parameters | | |
|---|---|---|
| Body material | | |
| Dimensions with frame | | 242 x 136 x 83 mm |
| Weight (depending on configuration) | Max. net | 2 kg |
| | Max. gross | 2.5 kg |
| Operating temperature | | −40 °C to 55 °C |
| Relative humidity | | 10 to 95 % (non-condensing) |
| Storing temperature | | −40 °C to 70 °C |
| Recommended altitude | | up to 2000 m |
| Protection class | | IP65, IP69K (91511xxxW), NEMA X4 |
| Resistance level | | IK10 |

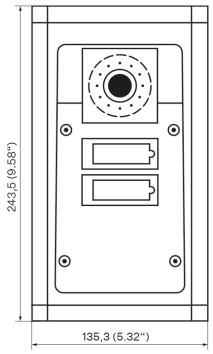
# General Drawings

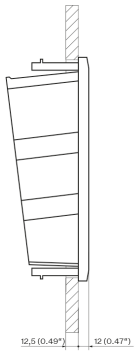
## Surface Installation

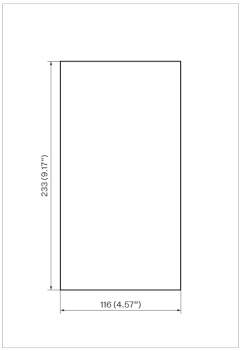


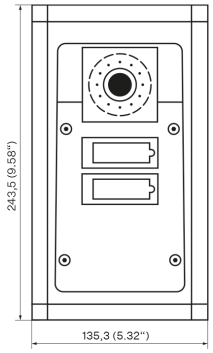
## Flush mounting – into plasterboard

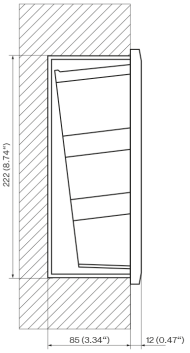


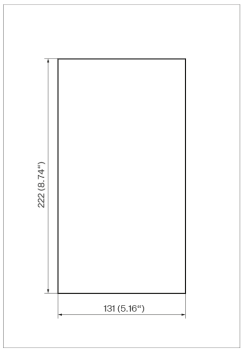



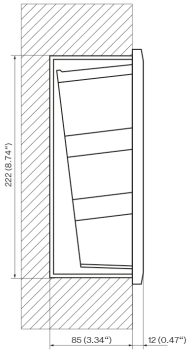




## Flush mounting – into classic masonry




222 (8.74")
131 (5.16")


222 (8.74")
85 (3.34")
12 (0.47")

# 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 IP Force** conforms to the following directives and regulations:

### EU

- 2012/19/EU on waste electrical and electronic equipment

- 2014/53/EU for radio equipment
- 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.

## Compliance with DDA:

The 2N Telekomunikace devices comply with the Disability Discrimination Act (DDA) of 2005 stipulating the following conditions:

1. The devices are mounted in such a manner that their bottom edges are 100 to 120 centimeters above the ground.
2. The devices use keypads with a mechanical protrusion on digit 5.
3. The devices use an electromagnetic loop as the hearing aid.

## Legislation of Thailand

เครื่องโทรคมนาคมและอุปกรณ์นี้มีความสอดคล้องตามมาตรฐานหรือข้อกำหนดทางเทคนิคของ กสทช.

กสทช.

เครื่องวิทยุคมนาคมนี้ ได้รับยกเว้น ไม่ต้องได้รับใบอนุญาตให้มี ใช้ซึ่งเครื่องวิทยุคมนาคมหรือตั้งสถานีวิทยุคมนาคมตามประกาศ กสทช. เรื่อง เครื่องวิทยุคมนาคม และสถานีวิทยุคมนาคมที่ได้รับยกเว้นไม่ต้องได้รับใบอนุญาตวิทยุคมนาคมตามพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498

กสทช. | โทรคมนาคม
กำกับดูแลเพื่อประชาชน
Call Center 1200 (โทรฟรี)

## Legislation of Japan

本製品は、特定無線設備の技術基準適合証明 を受けています。

本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

本製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ等）の通信回線（公衆無線 LAN を含む）に直接接続することができません。本製品をインターネットに接続する場合は、必ずルータ等を経由し接続してください。

# 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 IP Force – Installation Manual



**2N.com**