# 2N IP Force 2.0

## Installation Manual




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

2N.com

# Table of Contents


**Symbols and Terms Used** ..... **4**

**Product Description** ..... **5**

Basic Features ..... 5

Product Versions ..... 6

Accessories ..... 9

Accessories for Installation ..... 9

Extenders ..... 11

Licenses ..... 22

Other accessories ..... 23

Package Completeness Check ..... 23

**Installation** ..... **25**

Mechanical Installation ..... 25

Flush Mounting ..... 26

Surface Installation ..... 28

Stand Installation ..... 29

Use of Cable Bushings ..... 30

Electric Installation ..... 37

Power Supply ..... 37

LAN Connection ..... 37

Device Connectors ..... 38

Available switches ..... 40

Relay Terminal Wiring Diagrams ..... 42

Electric Lock Connection ..... 43

Grounding ..... 44

Overvoltage Protection ..... 45

Main and Extending Modules ..... 47

Internal RFID card readers ..... 47

Internal Induction Loop ..... 56

Additional Switch ..... 58

Security Relay ..... 62

Installation Completion ..... 63

Name Tags ..... 64

Tactile stickers ..... 64

**Brief Guidelines** ..... **65**

IP Address Retrieval ..... 65

IP Address Retrieval Using 2N IP Utility ..... 65

IP Address Retrieval with CONTROL Button ..... 66

IP Address Retrieval Using Speed Dial Button ..... 67

Access to web device configuration ..... 67

Password Change ..... 67

Recommended browsers ..... 68

Firmware Update ..... 68

Update from Server ..... 68

Automatic Updates (Auto-Provisioning) ..... 69

Manual Firmware Check and Installation ..... 70

Device Restart ..... 70

Restart Using Web Configuration Interface ..... 70

Factory Default Reset ..... 70

Factory Default Reset with CONTROL Button ..... 71

Configuration via Hardware ..... 72

IP Address Retrieval with CONTROL Button ..... 72

Static IP Address Setting with CONTROL Button ..... 73

Dynamic IP Address Setting via CONTROL Button ..... 73

Factory Default Reset with CONTROL Button ..... 74
Device Static/Dynamic IP Address Switching with Speed Dial Button ..... 74
**Device Control ..... 76**
**Troubleshooting ..... 77**
**Technical Parameters ..... 78**
**General Instructions and Cautions ..... 82**
Directives, Laws and Regulations ..... 82
EU ..... 82
Industry Canada ..... 83
US ..... 83
Compliance with DDA: ..... 83
Legislation of Thailand ..... 84
Electric Waste and Used Battery Pack Handling ..... 84

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

## Basic Features

**2N IP Force 2.0** is a highly durable and reliable IP intercom equipped with a number of useful features that are not common in devices in this category. It is built on the powerful ARTPEC-8 processor.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 2.0** 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:

**Speakerphone (1 W)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 up to 54 1 or 2 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 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

- industrial design and variable mounting options,
- wide supply power range and PoE supply,
- integrated 10 W power amplifier,
- external amplifier connection,
- external microphone/audio signal source connection,
- galvanically isolated RELAY output,
- two controlled active 12 V outputs,
- two galvanically isolated logic inputs,

- up to 3 signaling LED outputs,
- up to 16 external buttons/matrix keypad connection,
- integrated one-porttwo-port LAN switch,
- uncompromising Antivandal design,
- variable mounting options (brick/plasterboard flush mounting, surface mounting),
- sensitive microphone and loud speaker
- bidirectional communication – acoustic echo cancellation,
- integrated color FullHD camera with a wide-angle lens,
- selectable number of speed dial buttons with nametags and backlight,
- optional numeric keypad with backlight,
- integrated electronic lock switches with wide setting options,
- optional RFID reader module with OSDP / Wiegand support
- VBUS connector for connecting an extending module from the 2N IP Verso product line (e.g. Bluetooth module with Wavekey support)
- LAN (PoE+) or external 12 V / 4 A power supply
- configuration via  web interface,
- QR code reading support, face zooming
- SIP 2.0 support
- up to 54 buttons for calling preset phone numbers,
- up to 10,000 users to be added,
- up to 20 user time profiles,
- video codecs H.264 (Main or Baseline profile), MJPEG
- audio codecs G.711a/u, G.722, G.729, L16/16 kHz
- HTTPS server for configuration,
- SNTP client for server time synchronization,
- SMTP client for e-mail sending,
- RTSP server for video streaming,
- TFTP/HTTP client for automated configuration update.

# Product Versions



**Part No. 9151301**

Axis Part No. 03359-001

2N IP Force 2.0 main unit — 1 Button, 10 W Speaker

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



**Part No. 9151301C**

Axis Part No. 03361-001

Main Unit 2N IP Force 2.0 – 1 button, HD camera, 10 W loudspeaker

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



**Part No. 9151301RP**

Axis Part No. 03366-001

2N IP Force 2.0 main unit — 1 button, pictograms, 10 W speaker, reader-ready

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



**Part No. 9151301CRP**

Axis Part No. 03364-001

Main Unit 2N IP Force 2.0 – 1 button, HD camera, pictograms, 10 W speaker, reader re

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



**Part No. 9151301K**

Axis Part No. 03365-001

2N IP Force 2.0 main unit — 1 button, keypad, 10 W speaker

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



**Part No. 9151301CK**

Axis Part No. 03362-001

Main Unit 2N IP Force 2.0 – 1 button, HD camera, keypad, 10 W loudspeaker

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



**Part No. 9151302R**

Axis Part No. 03368-001

2N IP Force 2.0 main unit — 2 buttons, 10 W speaker, reader-ready

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



**Part No. 9151302CR**

Axis Part No. 03367-001

Main Unit 2N IP Force 2.0 – 2 buttons, HD camera, 10 W loudspeaker, reader ready

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



**Part No. 9151304**

Axis Part No. 03360-001

2N IP Force 2.0 main unit — 4 Buttons, 10 W Speaker

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



**Part No. 9151304C**

Axis Part No. 03369-001

Main Unit 2N IP Force 2.0 – 4 buttons, HD camera, 10 W loudspeaker

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



**Part No. 9151301CM**

Axis Part No. 03363-001

2N IP Force 2.0 main unit - emergency button, HD camera, 10 W speaker

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

**NOTE**
Each main unit includes a frame for flush mounting.

# Accessories

## Accessories for Installation

**2N IP Force 2.0** is designed for both outdoor and indoor applications.

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

All **2N IP Force 2.0** 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**

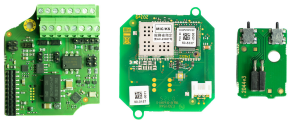
Axis Part No. 01345-001

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. 9151324**

Axis Part No. 03355-001

Internal 125 kHz, 13.56 MHz RFID card reader, NFC ready & Wiegand

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

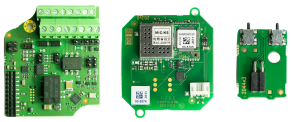
Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **ISO14443B** (Calypso)
- **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 2.0** front panel is open.

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



**Part No. 9151324-S**

Axis Part No. 03356-001

Internal 125 kHz RFID card reader, Seos® Compatible 13.56 MHz, NFC ready & Wiega

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

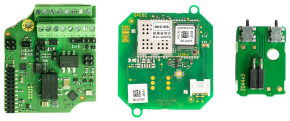
Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **ISO14443B** (Calypso)
- **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**

NFC/HCE preparation.

It also comes with a tamper switch indicating that the **2N IP Force 2.0** front panel is open.

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



**Part No. 9151325**

Axis Part No. 03357-001

Internal 125 kHz, 13.56 MHz RFID card reader, NFC ready & OSDP

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

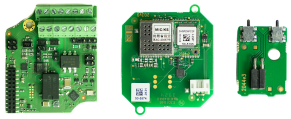
Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **ISO14443B** (Calypso)
- **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 2.0** front panel is open.

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



**Part No. 9151325-S**

Axis Part No. 03358-001

Internal 125 kHz RFID card reader, Seos® Compatible 13.56 MHz, NFC ready & OSDP

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)
- **ISO14443B** (Calypso)
- **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**

NFC/HCE preparation.

It also comes with a tamper switch indicating that the **2N IP Force 2.0** front panel is open.

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



**Part No. 9155030**

Axis Part No. 01252-001

2N IP Verso – Infopanel

The Infopanel module helps you place such information into the device installation as house number, opening hours and similar data.

The Infopanel backlight is software controlled.




**Part No. 9155031**

Axis Part No. 01253-001

2N IP Verso – Keypad

The numeric keypad module helps you dial users via their phonebook positions or phone numbers. Also, it helps you control the lock and other functions via a numeric code.

The digits and symbols are backlit.




**Part No. 9155031B**

Axis Part No. 01254-001

2N IP Verso – Keypad – black

The numeric keypad module helps you dial users via their phonebook positions or phone numbers. Also, it helps you control the lock and other functions via a numeric code.

The digits and symbols are backlit.



**Part No. 9155035**

Axis Part No. 01258-001

2N IP Verso – 5-button

A module with 5 mechanical speed dial buttons.

The buttons are backlit and can include nametags.



**Part No. 9155041**

Axis Part No. 01263-001

2N IP Verso – Induction Loop

The induction loop is used for transmitting audio signals directly into hearing aids via a magnetic field.



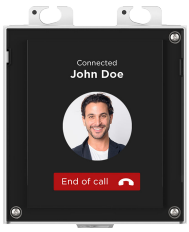

**Part No. 9155047**

Axis Part No. 01277-001

2N IP Verso – Touch Keypad

The numeric touch keypad module helps you dial users via their phone-book positions or phone numbers, Also, it helps you control the lock and other functions via a numeric code.

The digits and symbols are backlit.




**Part No. 9155036**

Axis Part No. 01275-001

2N IP Verso – Touch Display

The touch display module allows visitors to dial users in a smartphone-like way.

In addition the display also features a keypad.



**Part No. 91550941**

2N IP Verso 125 kHz

It provides access control via contactless cards or key fobs.

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox



**Part No. 91550941US**

Axis Part No. 02140-001

2N IP Verso 125 kHz

It provides access control via contactless cards or key fobs.

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox



**Part No. 91550942**

Axis Part No. 02139-001

2N IP Verso 13.56 MHz, NFC ready

It provides access control via contactless cards or key fobs. The module supports the following 13.56 MHz cards or other carriers:

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **ISO14443B** (Calypso)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**



**Part No. 91550942-S**

Axis Part No. 02141-001

2N IP Verso 13.56 MHz, secured NFC ready

It provides access control via contactless cards or key fobs. The module supports the following 13.56 MHz cards or other carriers:

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **ISO14443B** (Calypso)
- **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**



**Part No. 91550451**

Axis Part No. 03507-001

2N IP Verso – Biometric Fingerprint Reader

Used for verification of human fingerprints for access control and intercom/third party equipment control.



**Part No. 9155086**

Axis Part No. 01712-001

2N IP Verso RFID – secured 13.56 MHz, NFC

It provides access control via contactless cards or key fobs. The module supports the following 13.56 MHz cards or other carriers:

Compatible with firmware version 2.13 and higher.

Supported RFID cards 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **ISO14443B** (Calypso)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**



**Part No. 91550945**

Axis Part No. 02778-001

2N IP Verso Bluetooth & RFID – 125 kHz, 13.56 MHz, NFC

A combined Bluetooth & card reader module helps you control access using a numeric code, contactless cards or key fobs. The module supports the 125 kHz and 13.56 MHz cards and/or other carriers.

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)
- **ISO14443B** (Calypso)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**



**Part No. 91550945-S**

Axis Part No. 02444-001

2N IP Verso Bluetooth & RFID – 125 kHz, secured 13.56 MHz, NFC

A combined Bluetooth – card reader module helps you control access using an access code, My2N in your smartphone or an access card. The module supports the 125 kHz and 13.56 MHz cards and/or other carriers.

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)
- **ISO14443B** (Calypso)
- **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**




**Part No. 91550946**

Axis Part No. 02779-001

2N IP Verso Touch keypad & RFID – 125 kHz, 13.56 MHz, NFC

A combined touch keypad – card reader module helps you control access using a numeric code, contactless cards or key fobs. The module supports the 125 kHz and 13.56 MHz cards and/or other carriers.

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)
- **ISO14443B** (Calypso)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**




**Part No. 91550946-S**

Axis Part No. 02443-001

2N IP Verso Touch keypad & RFID – 125 kHz, secured 13.56 MHz, NFC

A combined touch keypad – card reader module helps you control access using a numeric code, contactless cards or key fobs. The module supports the 125 kHz and 13.56 MHz cards and/or other carriers.

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)
- **ISO14443B** (Calypso)
- **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**




**Part No. 91550947**

Axis Part No. 02781-001

2N IP Verso Touch keypad & Bluetooth & RFID – 125 kHz, 13.56 MHz, NFC

A combined touch keypad – Bluetooth – card reader module helps you control access using an access code, My2N in your smartphone or an access card. The module supports the 125 kHz and 13.56 MHz cards and/or other carriers.

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)
- **ISO14443B** (Calypso)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**




**Part No. 91550947-S**

Axis Part No. 02782-001

2N IP Verso Touch keypad & Bluetooth & RFID - 125 kHz, secured 13.56 MHz, NFC

A combined touch keypad – Bluetooth – card reader module helps you control access using an access code, My2N in your smartphone or an access card. The module supports the 125 kHz and 13.56 MHz cards and/or other carriers.

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)
- **ISO14443B** (Calypso)
- **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**



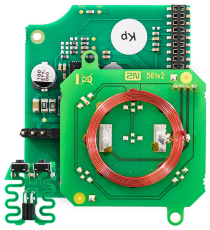
**Part No. 9151010**

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 2.0** front panel is open.



**Part No. 9151321**

Axis Part No. 03399-001

Internal Induction Loop

The internal induction loop transmits sound wirelessly from **2N IP Force 2.0** 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 2.0** 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.

## 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. 9154004**

Axis Part No. 01479-001

Water-proof metal button

Suitable for internal RFID card reader.

## Package Completeness Check

Please check the product delivery before installation. Contents:

| | |
|---|---|
| 1x | **2N IP Force 2.0** |
| 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

## Mechanical Installation

### Installation Conditions

### Make sure that the following 2N IP Force 2.0 installation conditions are met.

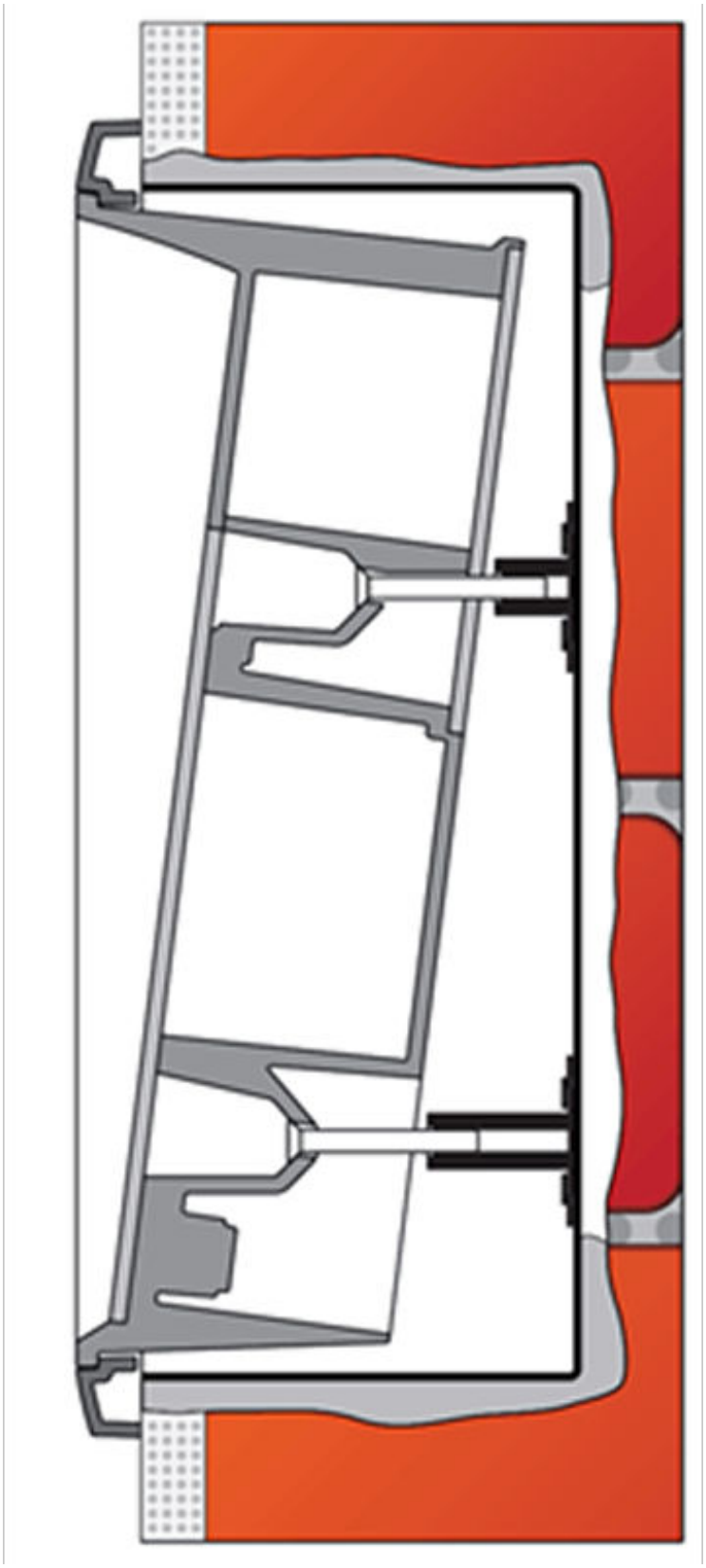
- There must be enough space for the device installation.
- Make sure that the dowel holes have the required diameter. If the diameters are too large, the dowels may get loose! Use the mounting glue to secure the dowels if necessary.
- Do not use low-quality dowels to avoid their falling out of the wall!
- Make sure that the depths of the dowel holes are accurate!
- Before starting the mechanical installation on a selected place, make sure carefully that the preparations associated with it (drilling, wall cutting) cannot damage the electrical, gas, water and other existing wires and pipes.
- The device is not designed for environments with increased vibrations such as means of transport, machine rooms and so on.
- The device may not be exposed to aggressive gas, acid vapors, solvents, etc.
- The device is not intended for direct connection into the Internet/WAN. The device must be connected to the Internet/WAN via a separating active network element (switch/router).
- Avoid strong electromagnetic radiation on the installation site.

**CAUTION**

- 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!
- 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..
- Any intentional mechanical damage to the device (drilling, main unit tampering, etc.) results in a loss of warranty.
- The installation and adjustment of this device, including any handling thereof, should only be carried out by persons qualified to do so.

## Flush Mounting

### Flush mounting – into classic masonry



What you need for mounting:

- **2N IP Force 2.0**
- 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.

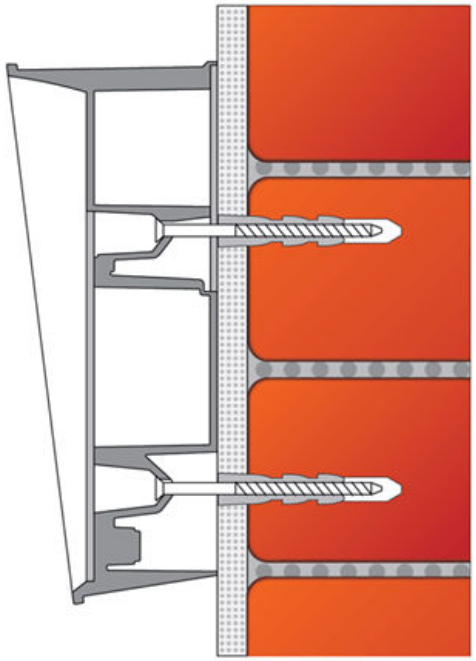
## Flush mounting – into plasterboard

What you need for mounting:

- **2N IP Force 2.0**
- 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 2.0**

**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!

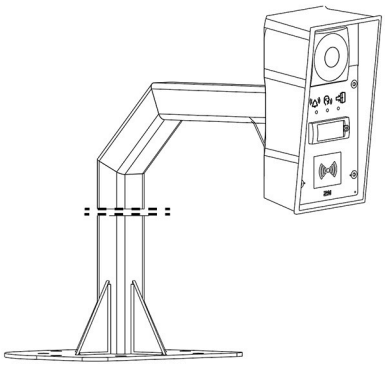
**CAUTION**

- 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

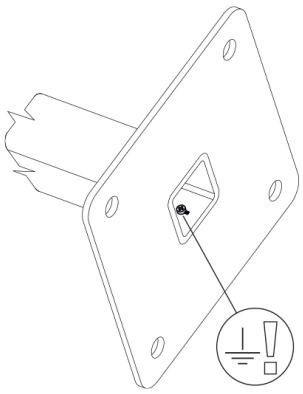


What you need for mounting:

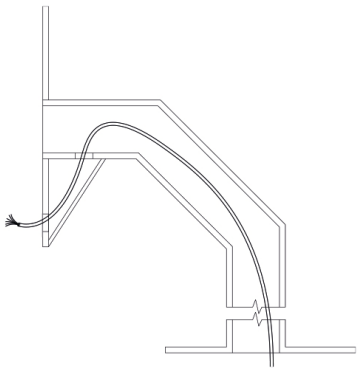
- **2N IP Force 2.0**
- stand installation spacer (9151005, 01351-001)

**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.

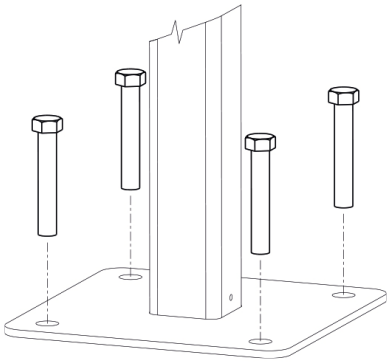
1.



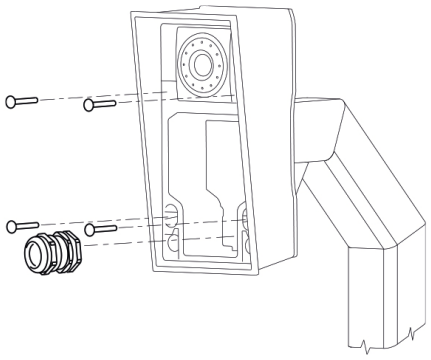
2.



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 2.0** 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:

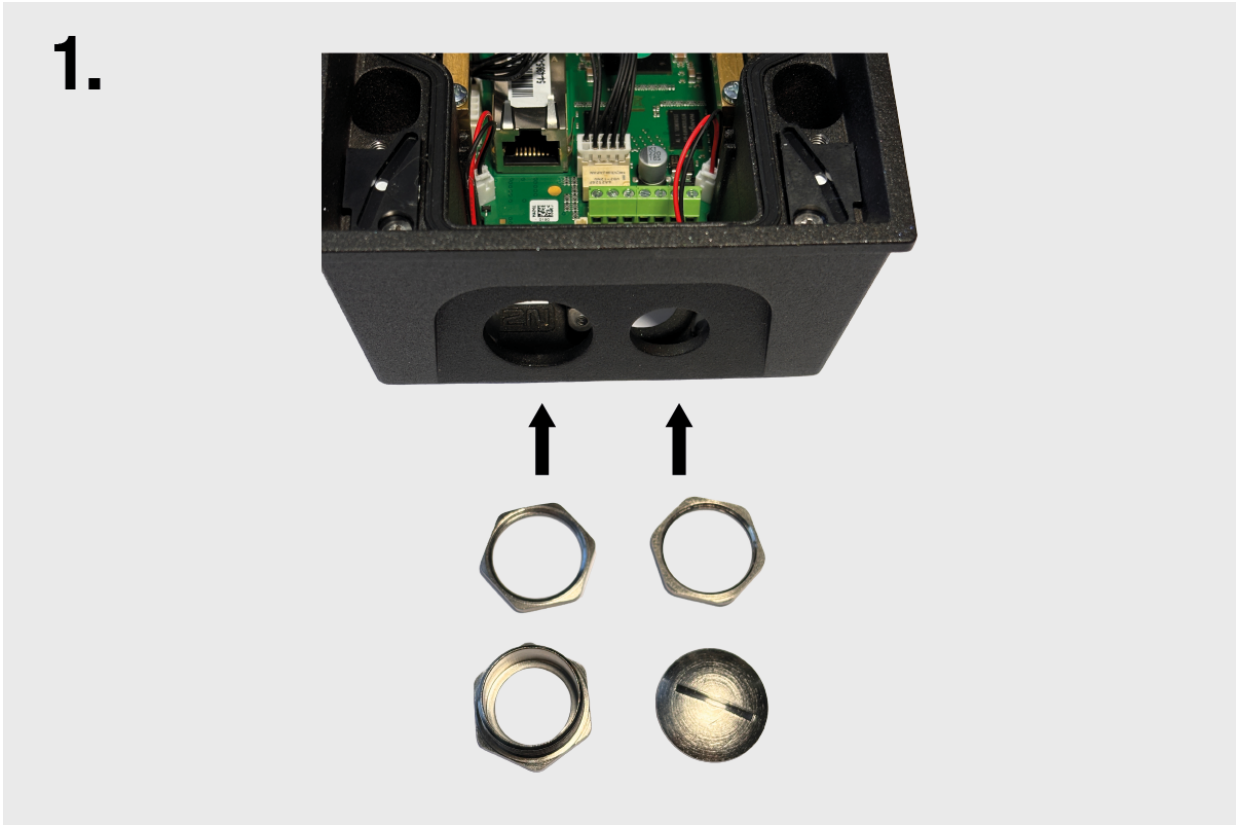
- big bushing: for two cables of the diameter of 5–6 mm (UTP cable), or, upon insert replacement, for one thick cable/tube of the diameter of up to 14 mm

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

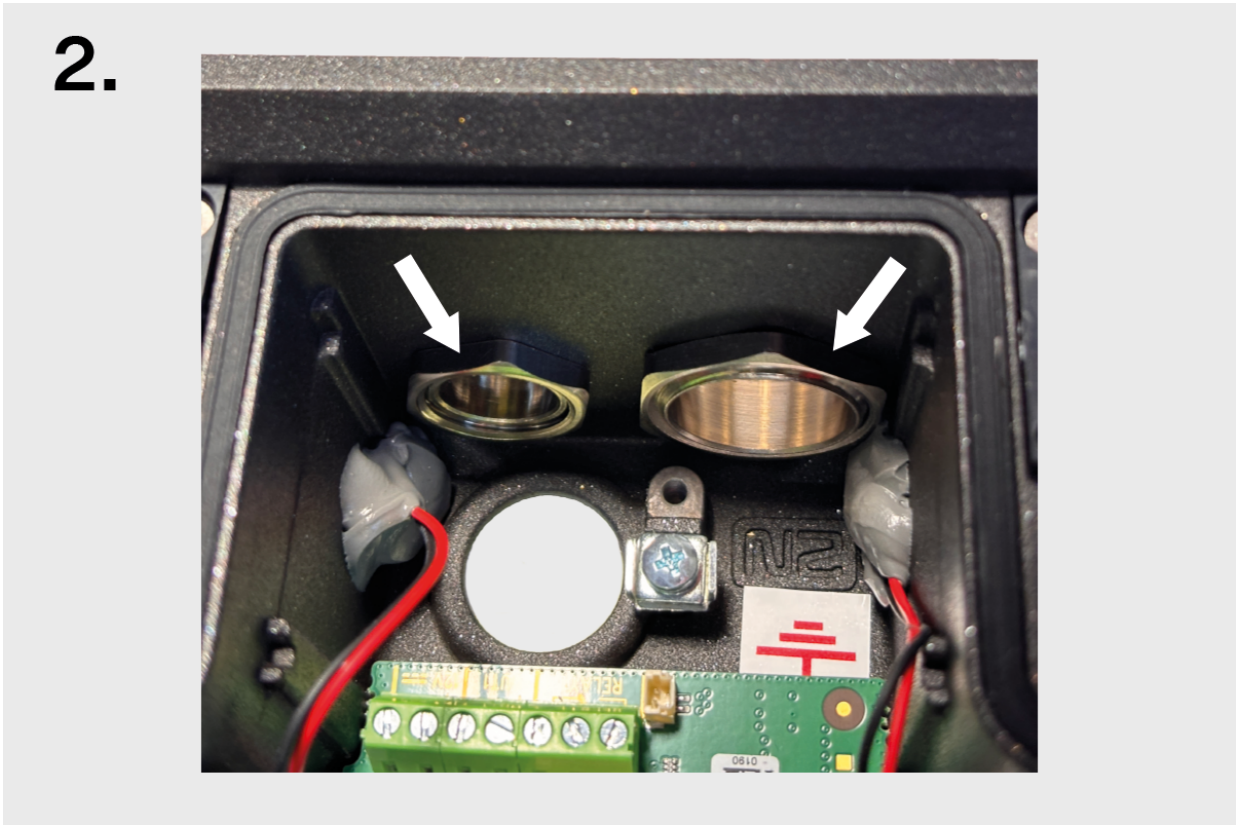
**TIP**
Even a LAN cable including the RJ-45 connector can go through the big bushing. See below for instructions.

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

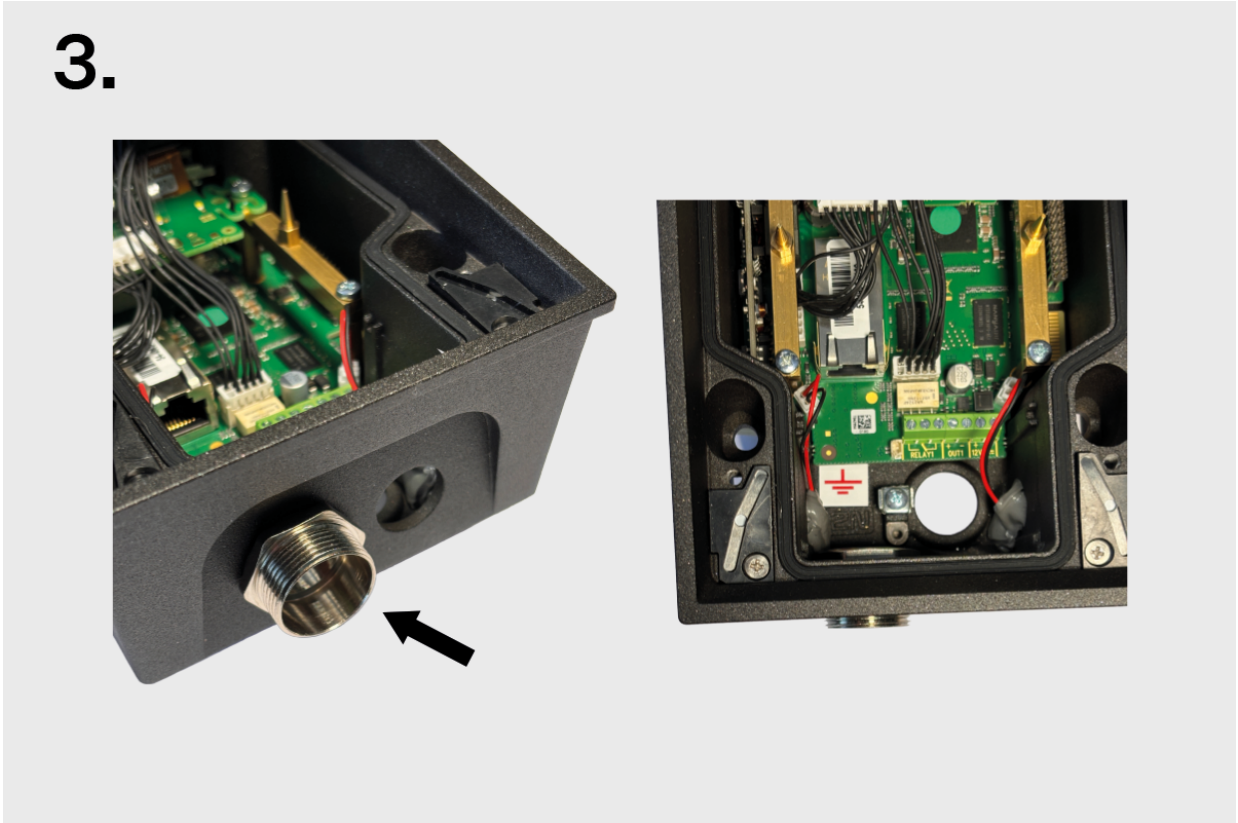
1. The cable wiring holes are located on the bottom of the device.



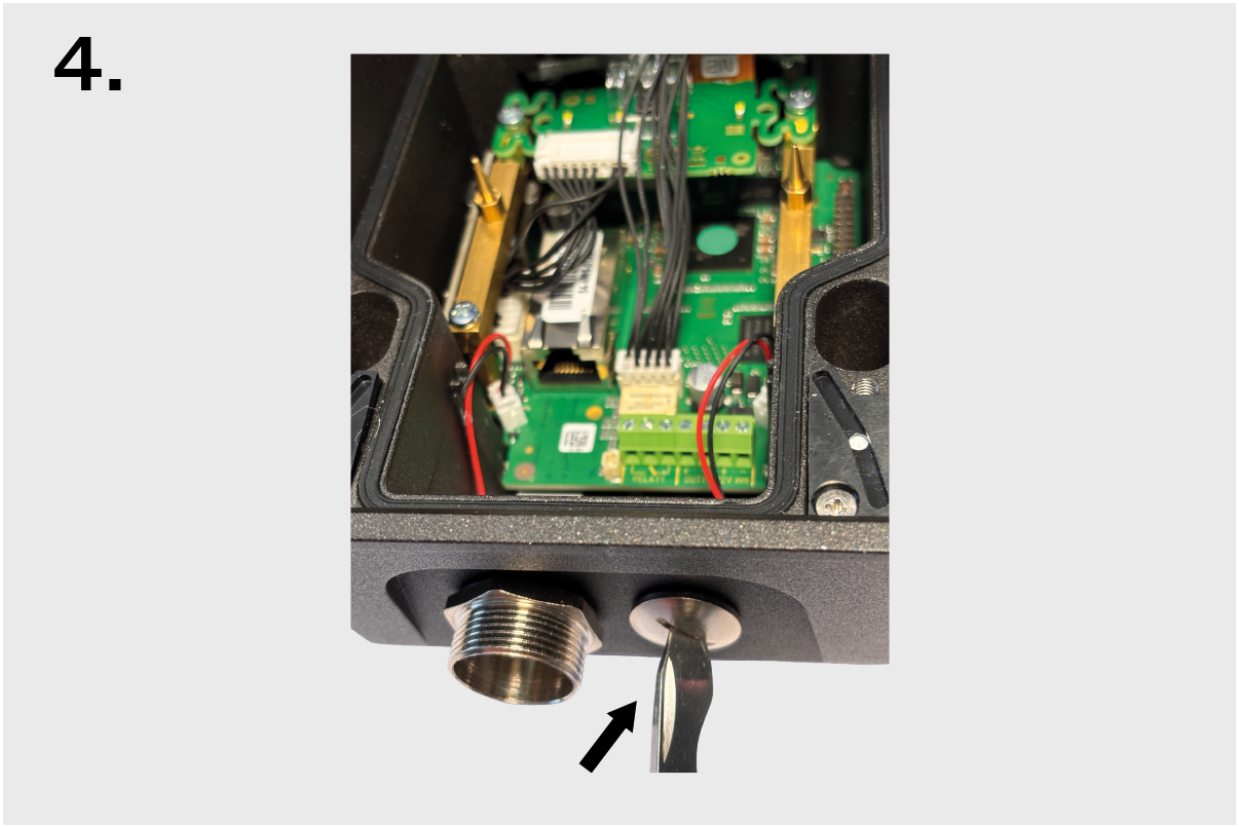
2. Place the nuts on the inside of the holes.



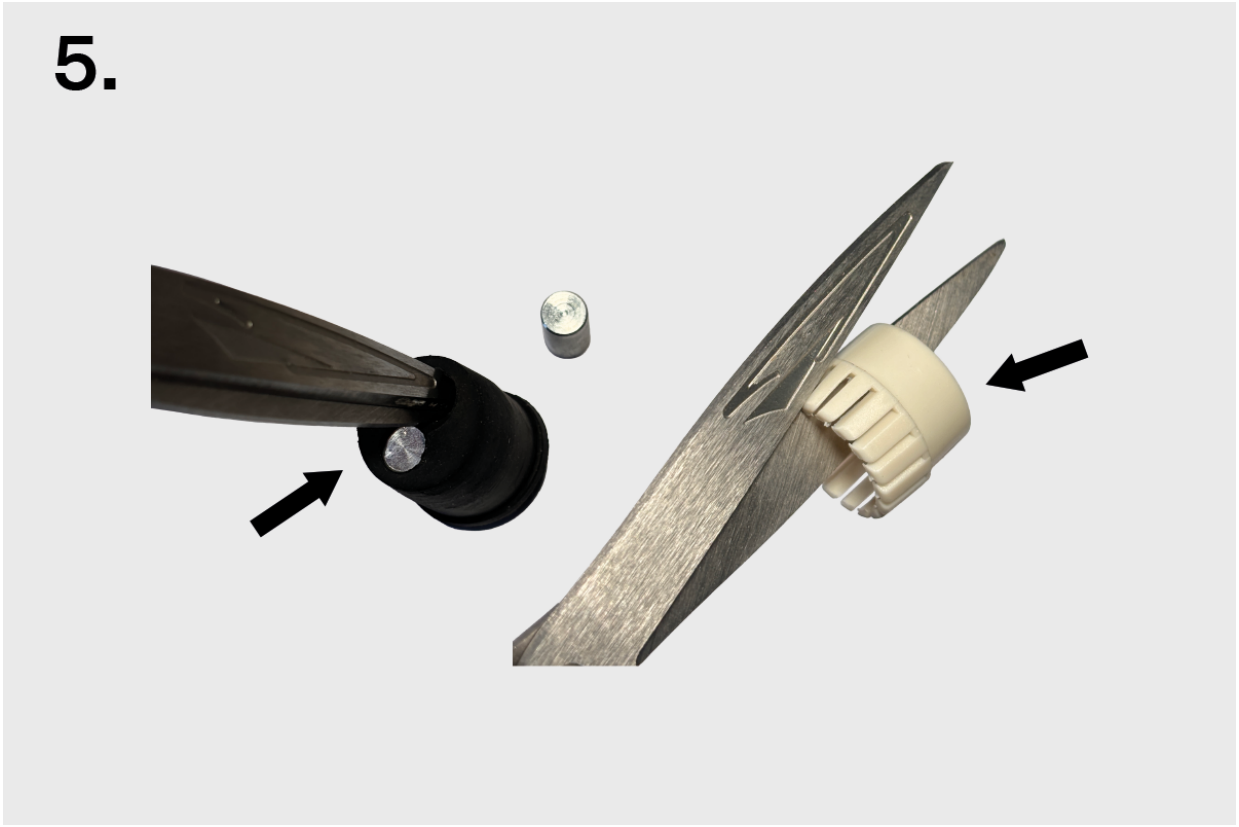

3. Screw on and tighten the bushing.



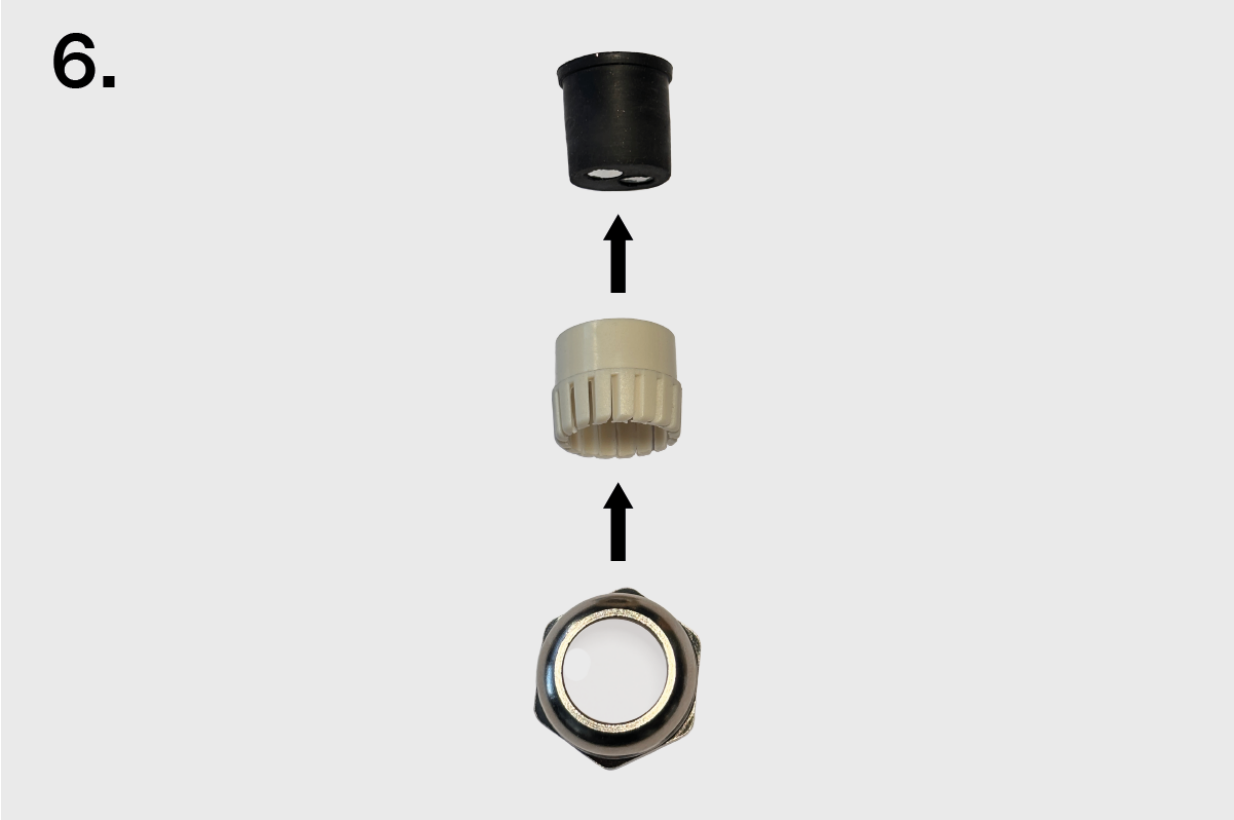
4. Screw on and tighten the blank.



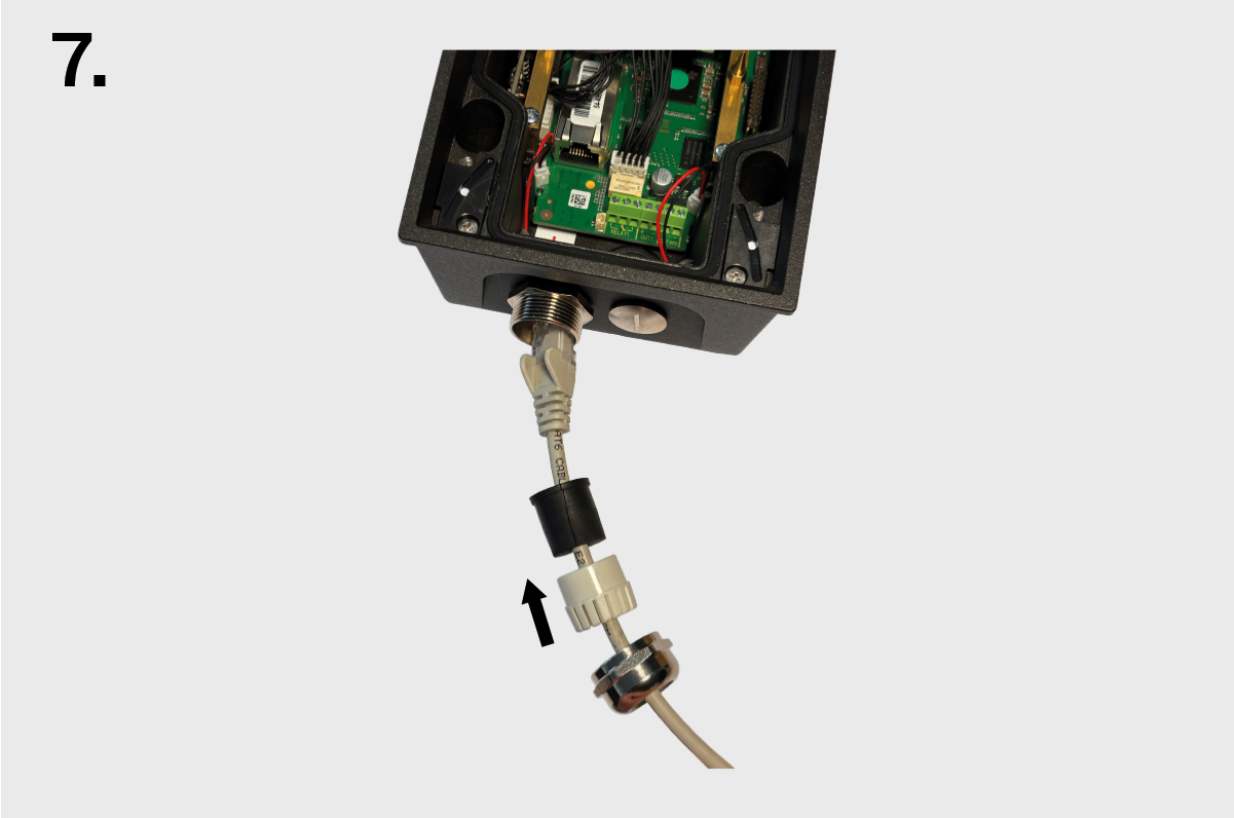

5. Remove the necessary number of cable glands from the seal.Place the nuts on the inside of the holes. Cut the case as shown.



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



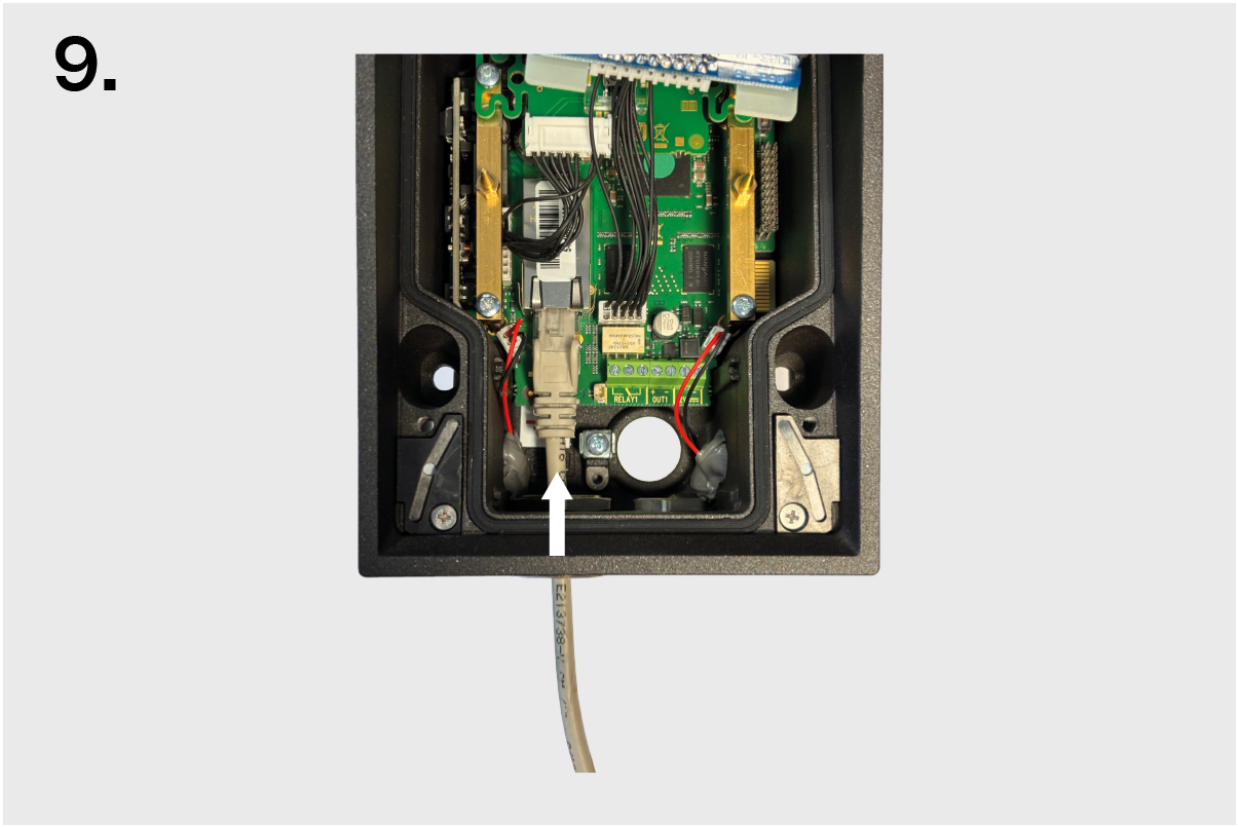

7. Attach the bushing nut, case and seal to the cable.



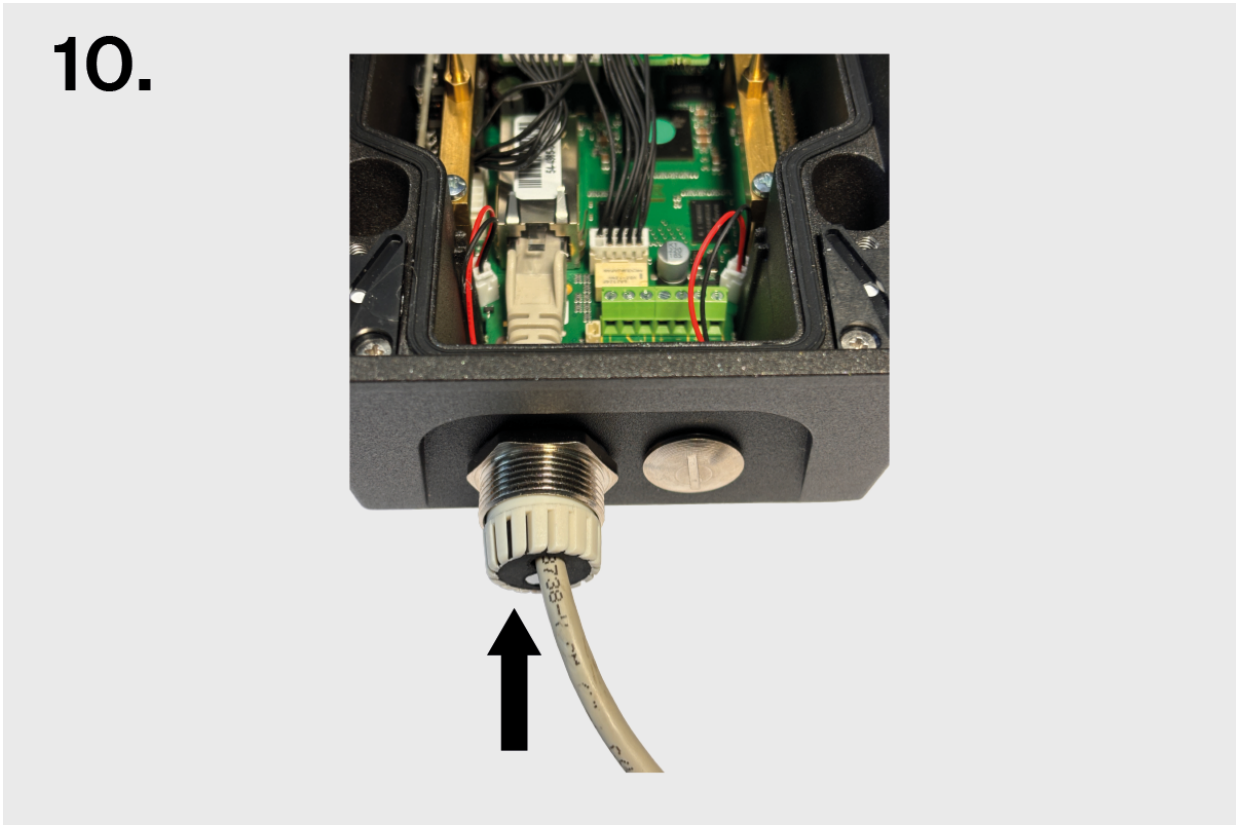
8. Pull the cable end through the bushing body into the intercom.



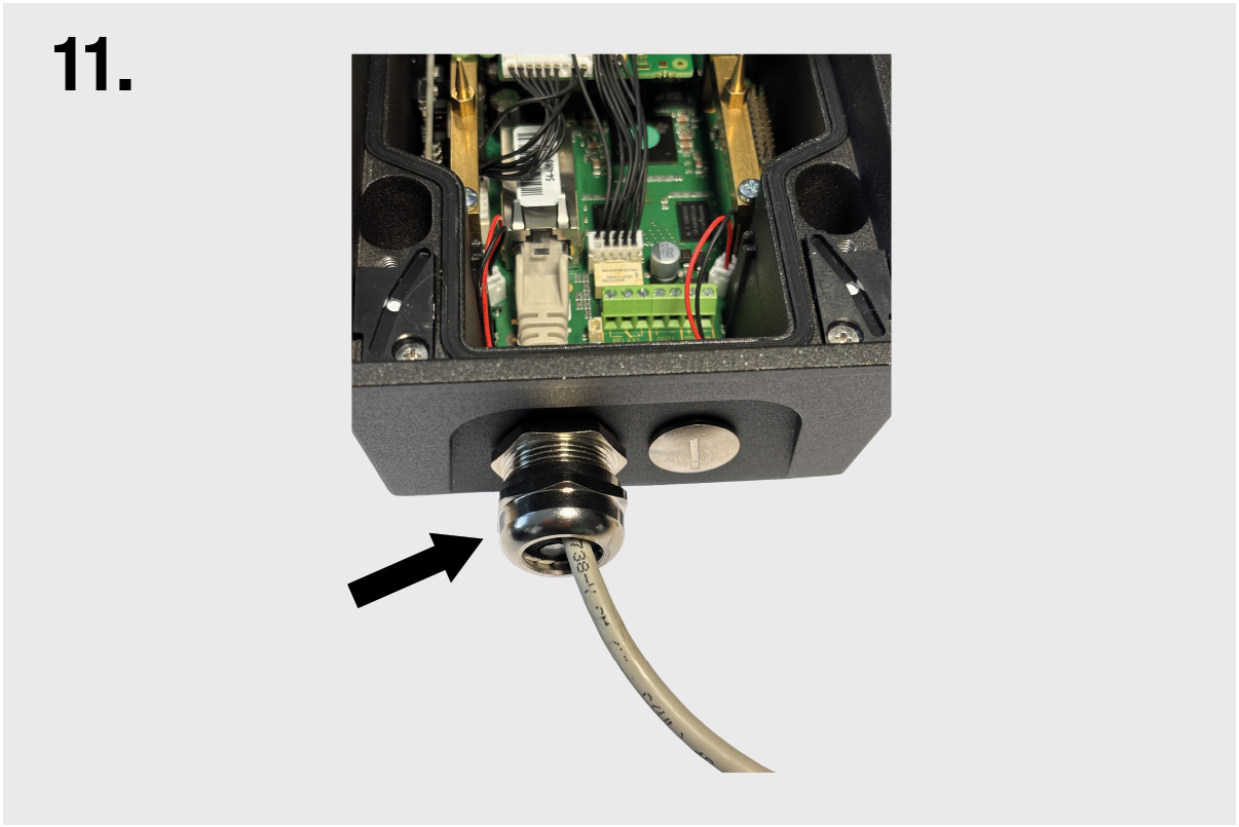

9. Snap the cable end into the motherboard connector.



**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 2.0** can be fed either an external 12 V / 4 A DC power supply.

**CAUTION**

- The external power supply should comply with PS2/LPS.

## PoE Supply

**2N IP Force 2.0** is compatible with the PoE+ 802.3at (Class 4–25,5 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 2.0** and the nearest network element.

## External Power Supply

Use a SELV supply 12 V dimensioned to the current consumption 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 2.0** is connected to the LAN by inserting a SSTP cable (, Cat-6 or higher) terminated with an RJ-45 plug into the marked LAN connector on the device (connector X14). 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**

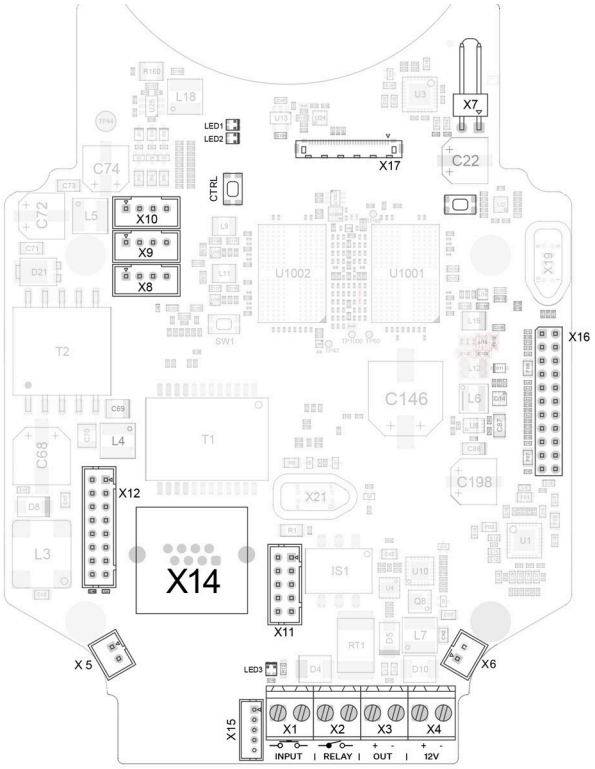
- We recommend the use of a LAN surge protection (p. 45).
- We recommend the use of a shielded SSTP Ethernet cable.

## Device Connectors

The diagram below shows the connector layout on the printed circuit board (PCB). The diagram includes the connectors to which cables, accessories and other device components are connected.

| Connector | Description |
|---|---|
| X1 | Logical Input 1 |
| X2 | Switching contact SSR relay<br>Used for connection of non-critical devices only (lights, e.g.). |
| X3 | Active output |
| X4 | Power input 12 V ±15 % / 4 A DC |
| X5 | Left-hand microphone |
| X6 | Right-hand microphone |
| X7 | Speaker |
| X8 | Button 1 |

| Connector | Description |
|---|---|
| X9 | Button 2 |
| X10 | Button 3 |
| X11 | Keypad module |
| X12 | Buttons 1 through 4 |
| X14 | LAN connection |
| X15 | External VBUS line connector |
| X16 | Extending modules (RFID card reader, additional switch, etc.) |
| X17 | Camera module |
| LED1 | PWR Status LEDs |
| LED2 | STAT Status LEDs |
| LED3 | LAN connection activity |
| SW3 | CTRL button (factory reset button) |

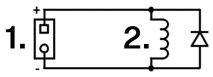



## Available switches

| 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.

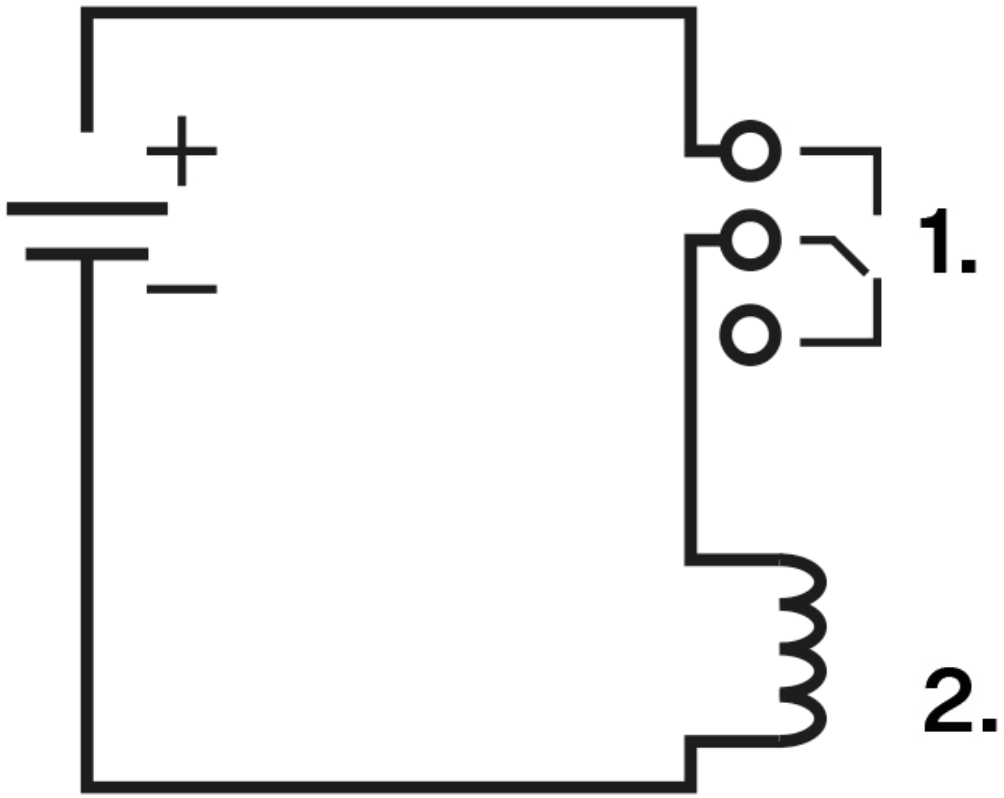
## Relay Terminal Wiring Diagrams

It is possible to connect a device to the **2N IP Force 2.0** relay terminals to be controlled by this relay, e.g. an electric/electromechanical door lock.

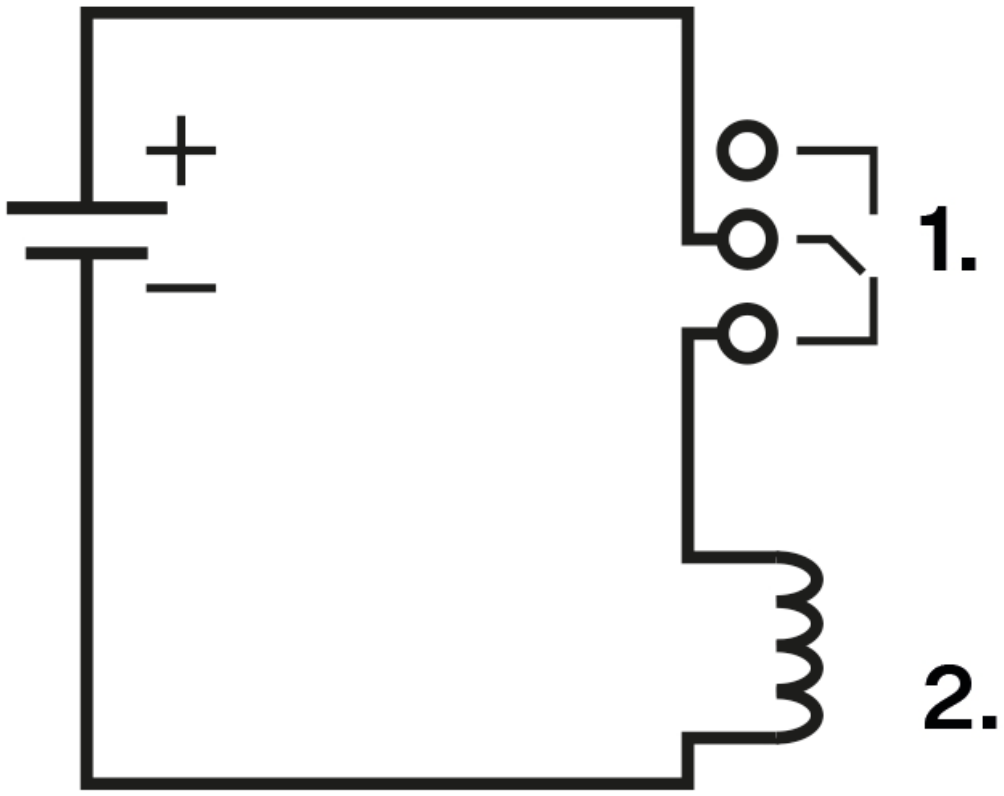
The elements are designated as follows in the diagrams below:

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

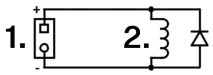



## Electric Lock Connection

**2N IP Force 2.0** 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. The location of the terminals on the board is shown in Device connectors (p. 38) for Force 2.0 and Board versions for Force.

**2N IP Force 2.0** is equipped with a galvanically isolated NO contact (terminals X2) and an active output with the nominal voltage of 12 V DC (terminals X3), to which a conventional electric lock or another suitable appliance can be connected. The location of the terminals on the board is shown in Device Connectors (p. 38).

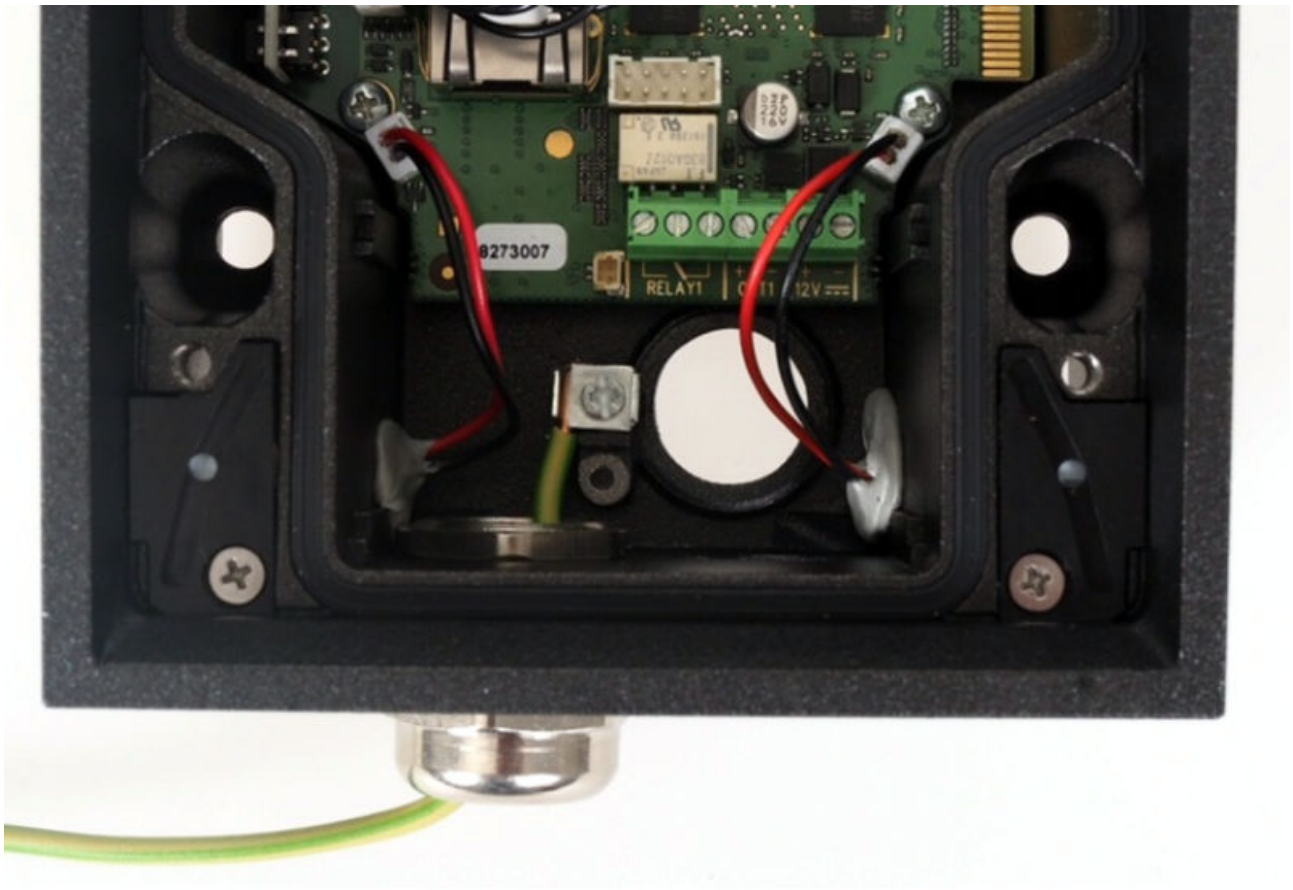
**DANGER**
If a coil containing device is connected, e.g. relays/electromagnetic locks, it is necessary to protect the device output against voltage peak while switching off the induction load. For this way of protection we recommend a 1 A / 1000 V diode (e.g., 1N4007, 1N5407, 1N5408) connected antiparallel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




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

## 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

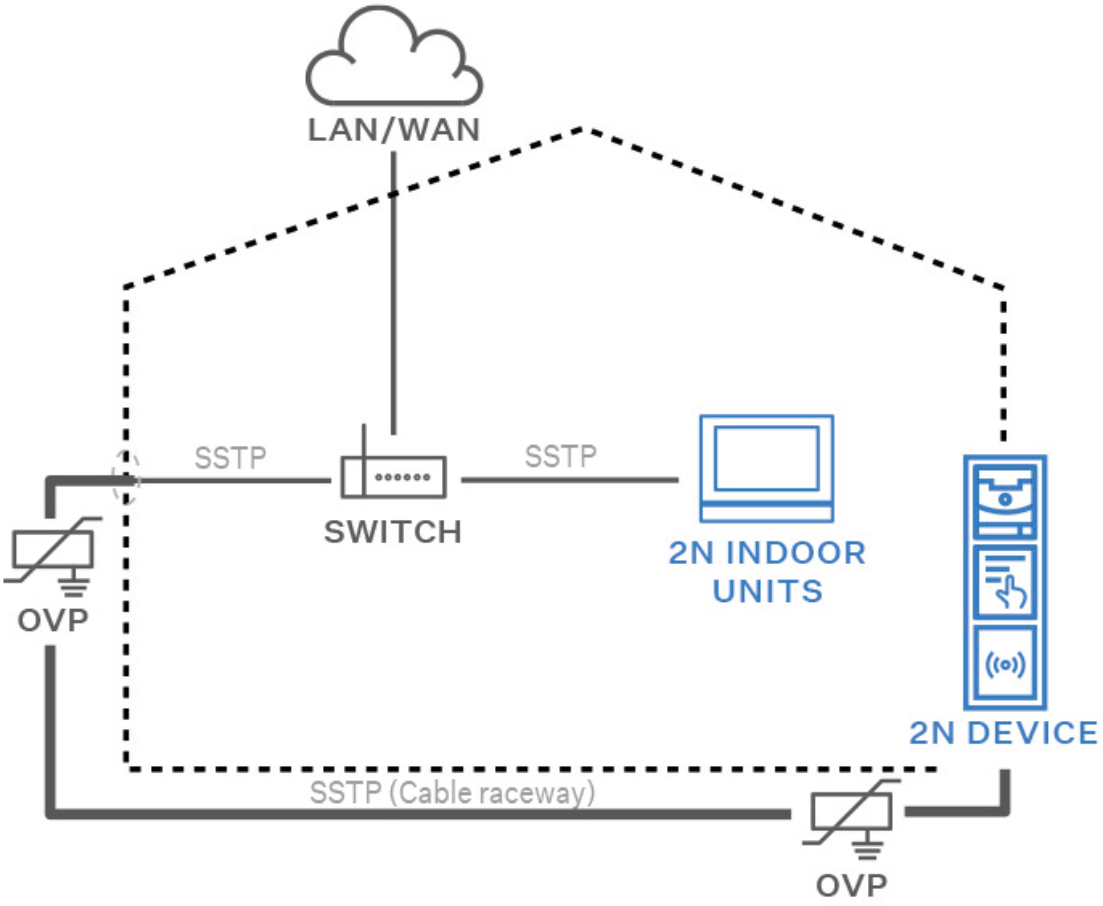
The 2N device cables have to be protected against atmospheric overvoltage caused by external causes (lightning, e.g.). A surge can damage a device installed outside/inside the building if the wires are unprotected.

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:

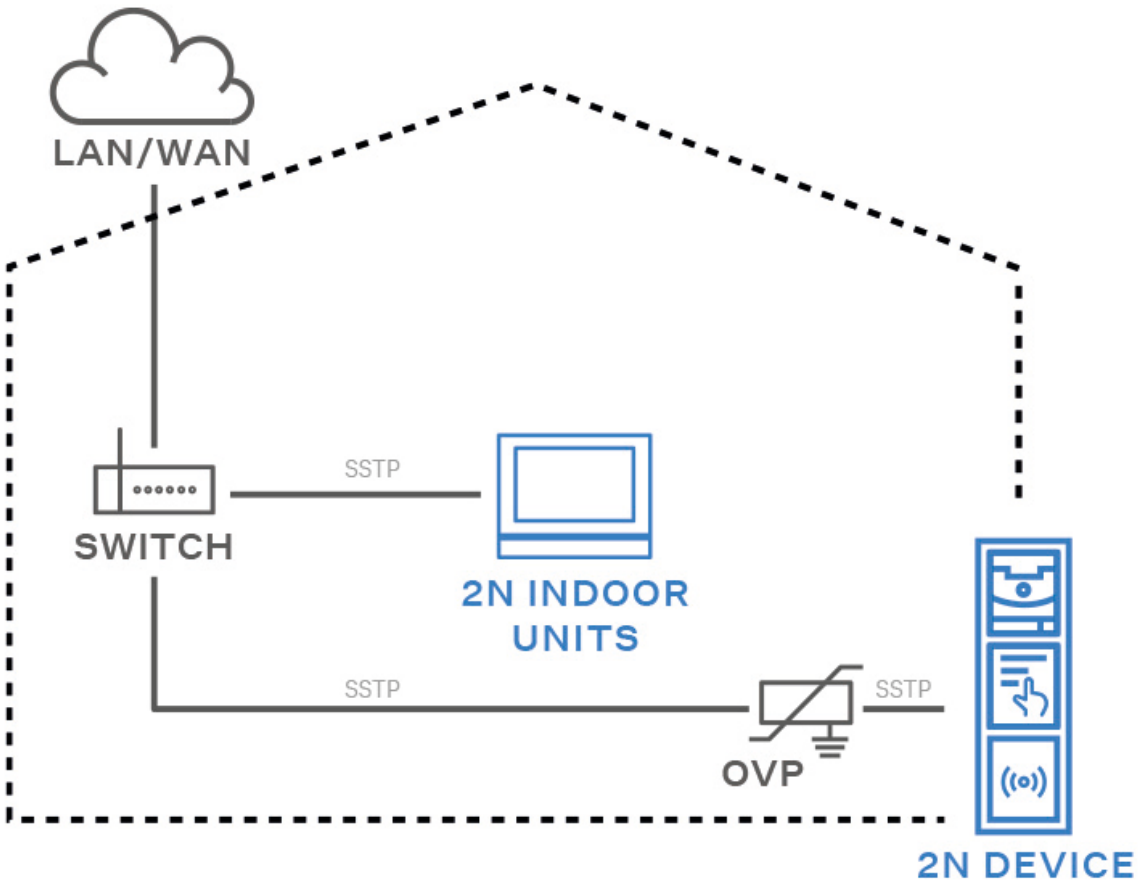
- Make sure that the overvoltage protector is installed as close as possible to the device installed outside the building.
- Make sure that the overvoltage protector is installed as close as possible to the device installed on an external part of the building.
- Make sure that the overvoltage protector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

## Examples of Overvoltage Protection Installation

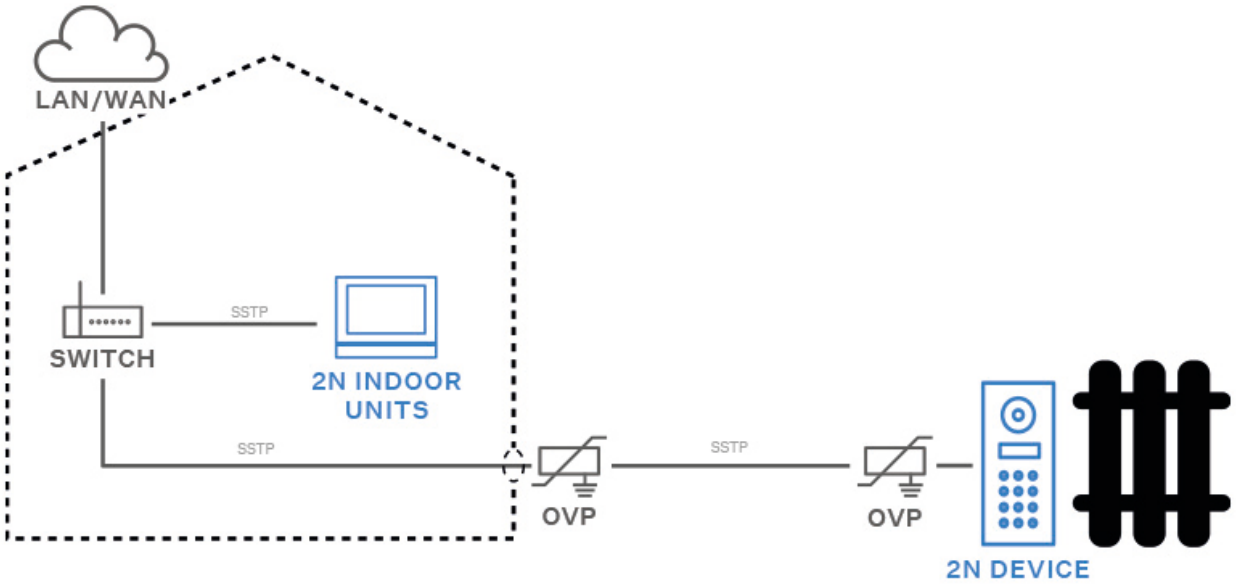
### Overvoltage protection installation diagram for a device installed on the building facade and cables outside the building



**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.

### Internal RFID card readers

Internal RFID card readers are designed for mounting in the **2N IP Force 2.0** main unit, see Compatibility below.

The Internal RFID Card Reader is used for reading RFID card Ids in the 125kHz and 13.56 MHz band, NFC supported. Provides communication between a connected Wiegand/OSDP device (control panel, door controller) and 2N device via the Wiegand/OSDP.

The **2N IP Force 2.0** Internal RFID Card Reader adds two logical inputs, an active output, an SSR Relay and a tamper switch to the main unit **2N IP Force 2.0**.

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.

## Compatibility

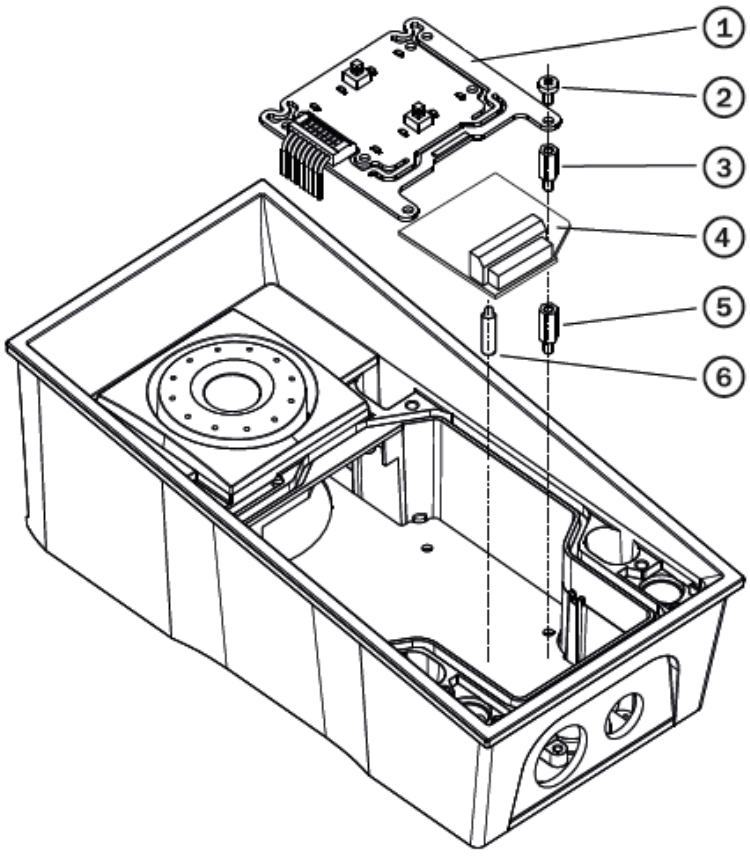
**CAUTION**

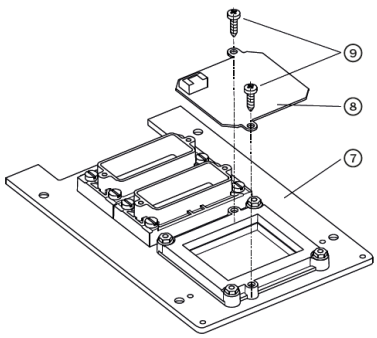
- Where an internal induction loop is used, an RFID card reader cannot be inserted in the device.
- If the additional and tamper switches are installed at the same time, no internal induction loop or RFID card reader can be installed in addition to them.
- Alternatively, an extending 2N IP Verso induction loop module can be connected via the VBUS connector.

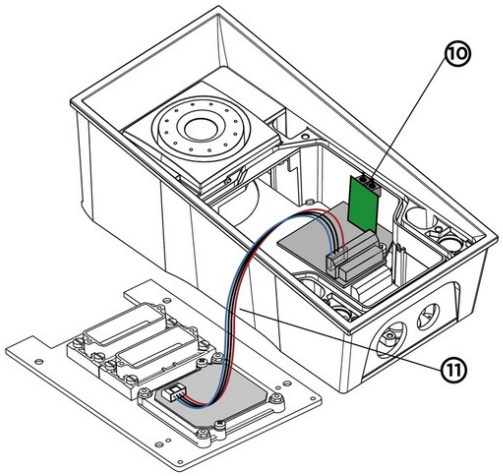
The module is compatible with the basic units with Part No.:

- 9151301CRP
- 9151302CR
- 9151302RP
- 9151302

## 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 longer, 12 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.

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

## Module Settings

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

# Technical Specifications

## Supported cards

| Part No. 9151324 and 9151325 | Part Nos. 9151324-S and 9151325-S |
|---|---|
| Supported RFID cards 125 kHz:<br>• EM4x02<br>• HID Prox<br>Supported RFID cards 13.56 MHz:<br>• **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)<br>• **ISO14443B** (Calypso)<br>• **PicoPass** (HID iClass CSN, Picopass)<br>• **FeliCa** (Standard, Lite)<br>• **ST SR** (SR, SRI, SRIX)<br>• **My2N**<br>• **2N PICard** | Supported RFID cards 125 kHz:<br>• EM4x02<br>• HID Prox<br>Supported RFID cards 13.56 MHz:<br>• **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)<br>• **ISO14443B** (Calypso)<br>• **PicoPass** (HID iClass CSN, Picopass)<br>• **FeliCa** (Standard, Lite)<br>• **ST SR** (SR, SRI, SRIX)<br>• **HID PAC** (HID SEOS, HID iClass SE, iClass SR, HID MIFARE DESFire with SIO, HID MIFARE Classic with SIO)<br>• **My2N**<br>• **2N PICard** |

### Relay (SSR A, SSR B)

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

### Active output (OUT)

- 9.8 to 13.8 V DC according to power supply (PoE: 11.6 V; adapter: power supply voltage minus 0.4 V), up to 400 mA

### Logical inputs (IN1, IN2)

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 closed, jumper JP1 for IN2, pins 1–2 are closed)

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

### Signaling output

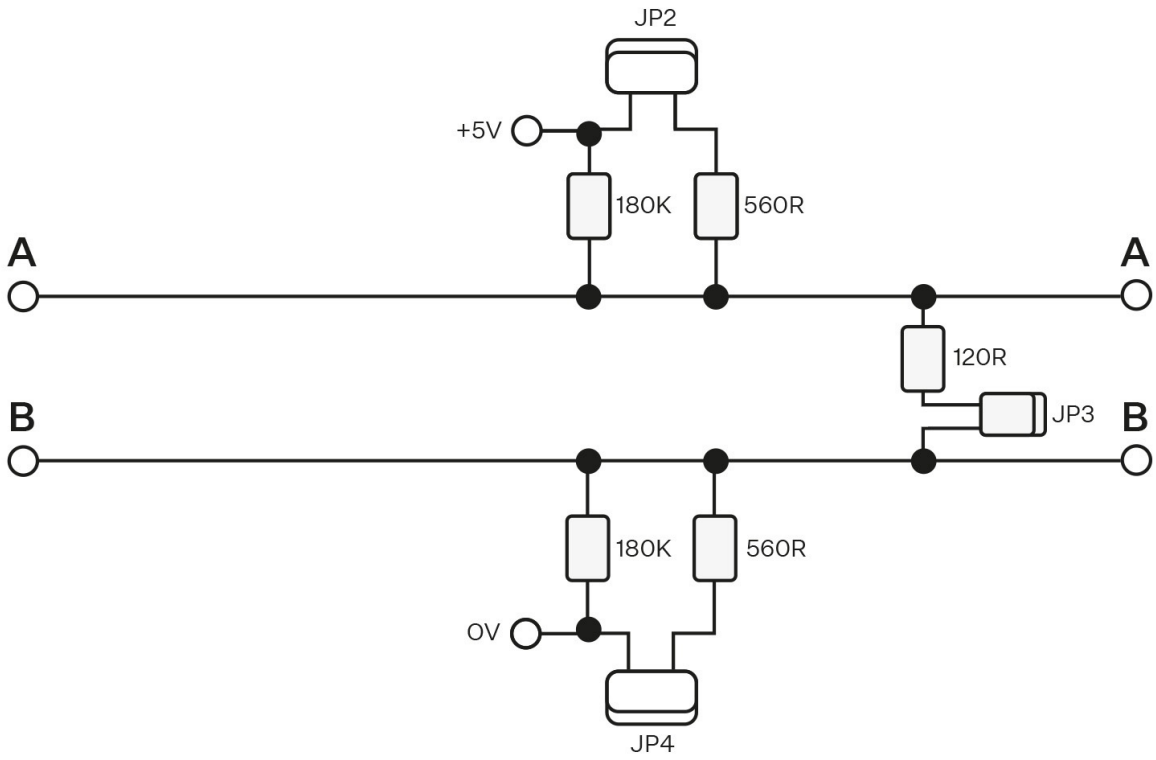
- Internal red LED under the intercom front panel

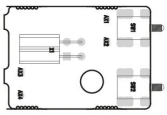
### Power Supply

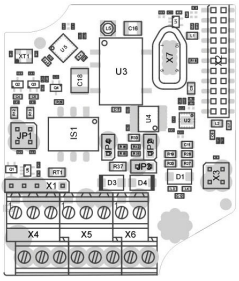
- For external RFID card reader
- 12 V DC ± 15% / 350 mA

## OSDP Interface

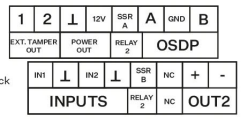
- OSDP reader (software configurable)

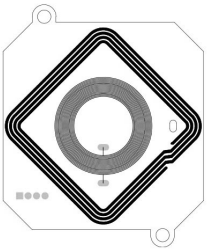







Terminal block description



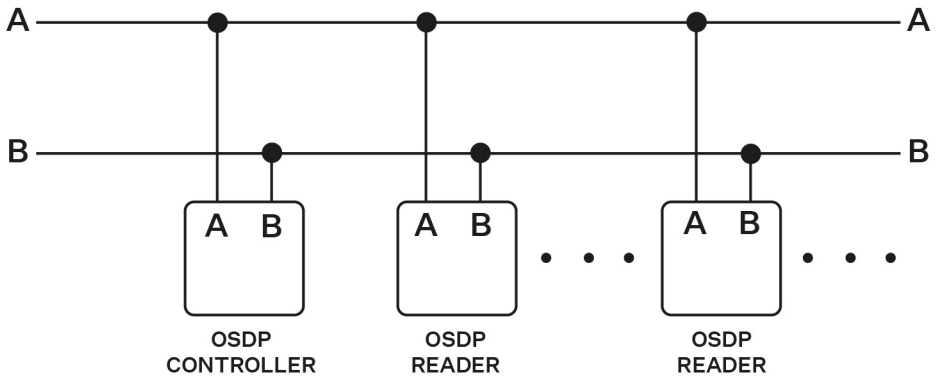



**CAUTION**

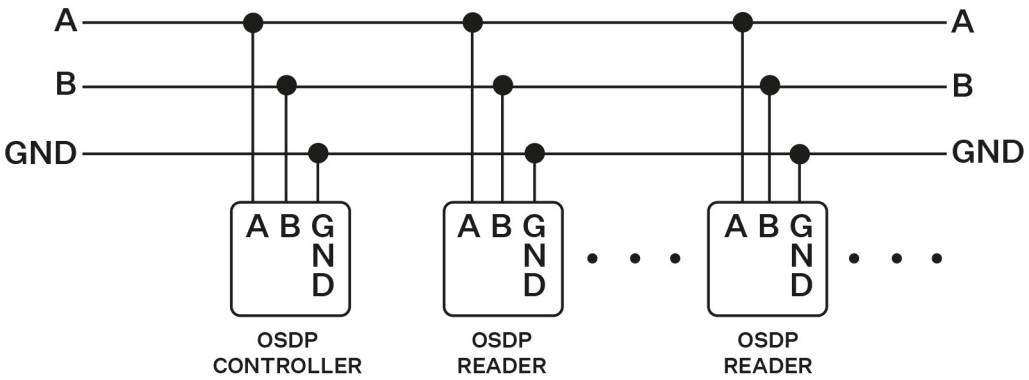
- Mounting jumpers JP2 and JP4 results in a connection of strong pull-up/pull-down resistors (560 ohms) to the RS-485 bus. These jumpers must be mounted/unmounted together, i.e. one jumper cannot be mounted alone. Strong pull-up and pull-down resistors can be connected only and exclusively to one arbitrary device on the OSDP bus.
- Mounting JP3 results in a connection of the terminating 120 ohm resistor between wires A and B of the OSDP bus. The terminating resistors may be connected exclusively on the first and last modules on the OSDP bus. We recommend the connection of these resistors on the first and last modules.

## Connection Recommendations

### Wiring diagram for two-wire connection

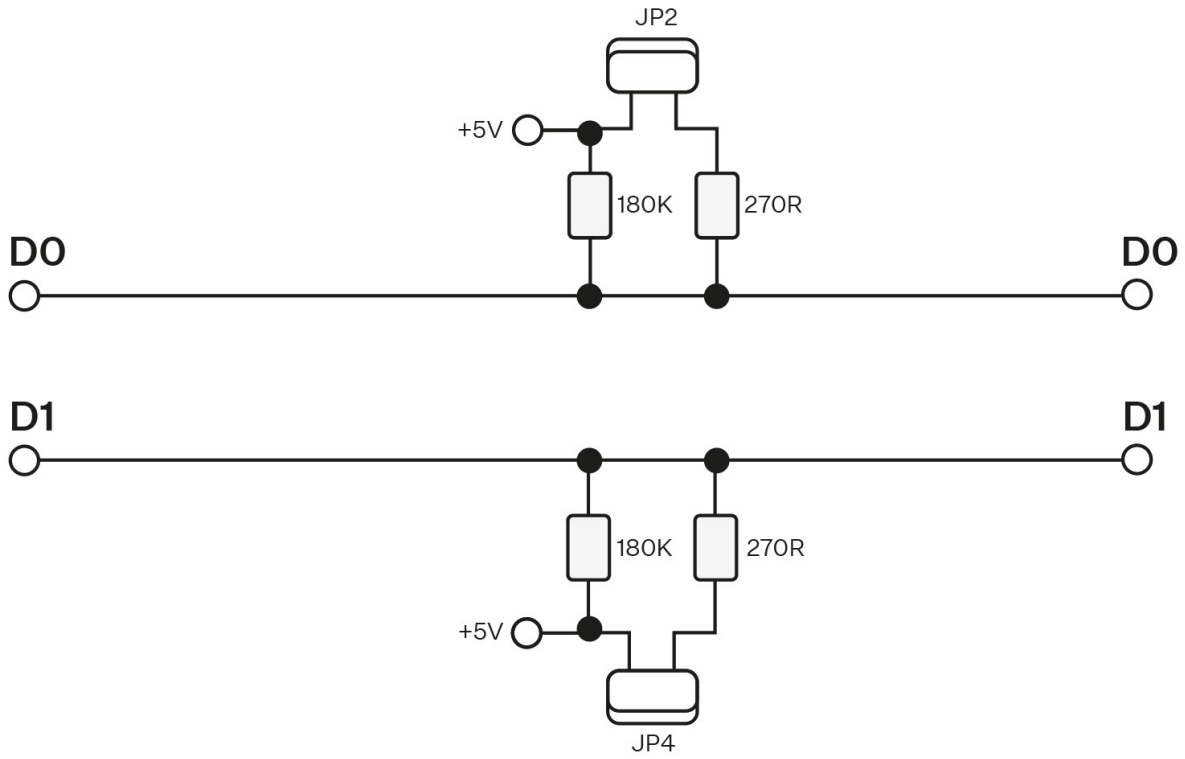


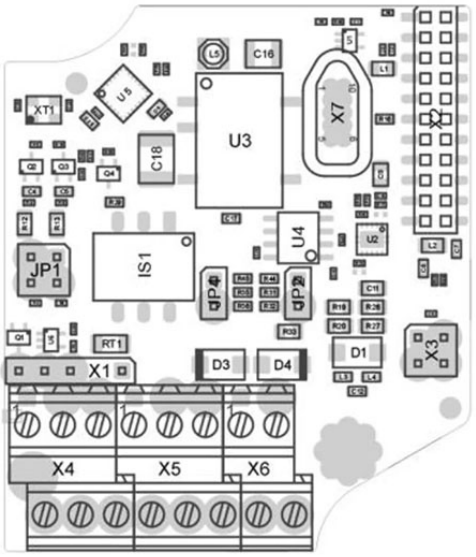

### Wiring diagram for three-wire connection

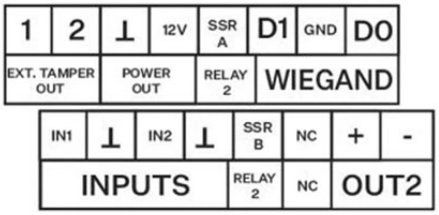


## Wiegand Interface

- Off/Input/Output (as programmed)






Terminal block description

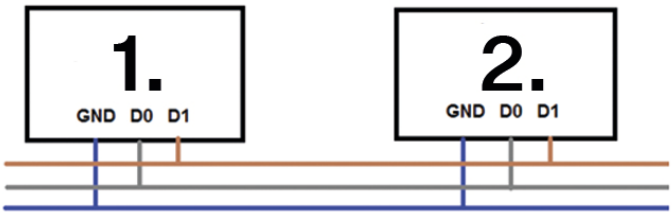
**CAUTION**

Mounting jumpers JP2 and JP4 results in a connection of strong pull-up resistors (270 Ω) to the Wiegand bus. These jumpers must be mounted/unmounted together, i.e. one jumper cannot be mounted alone. We recommend installing jumpers on the units operating in the transmitter mode and leaving jumpers uninstalled on the units operating in the receiver mode.

## Connection Recommendations

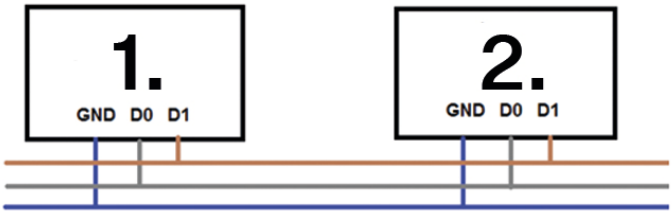
### Recommended Wiegand bus wiring diagram, 2N device as a receiver.

1. **2N IP Force 2.0**
2. External RFID Card Reader




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

1. External RFID Card Reader
2. **2N IP Force 2.0**




## Internal Induction Loop

The internal induction loop (Part No. 9151321) is one of the **2N IP Force 2.0** 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

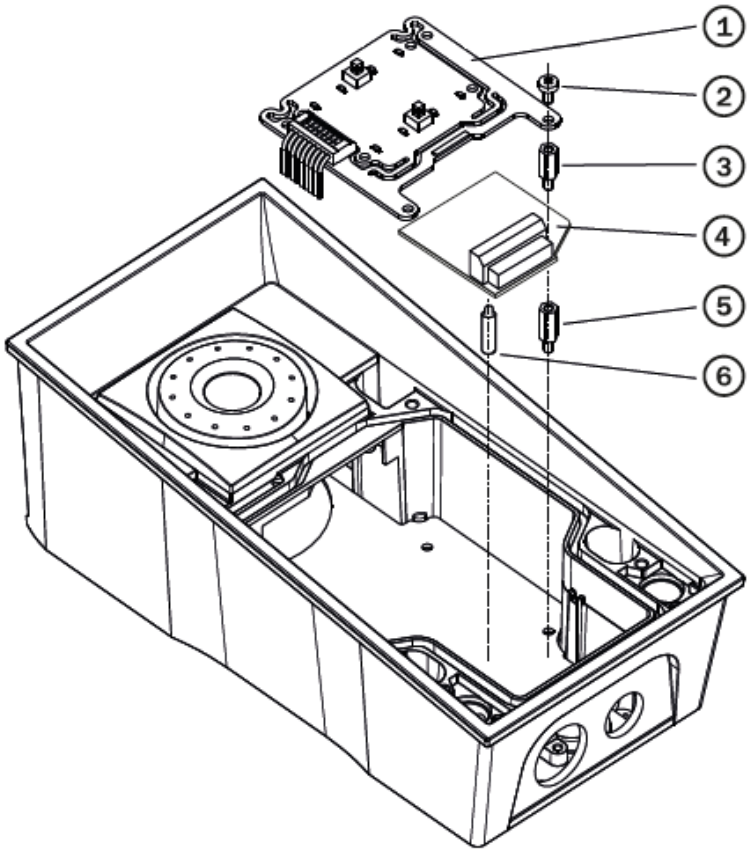
**CAUTION**

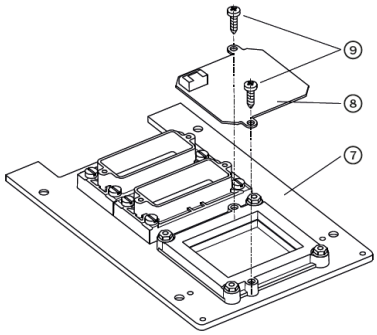
- Where an internal induction loop is used, an RFID card reader cannot be inserted in the device.
- If the additional and tamper switches are installed at the same time, no internal induction loop or RFID card reader can be installed in addition to them.
- Alternatively, an extending 2N IP Verso induction loop module can be connected via the VBUS connector.

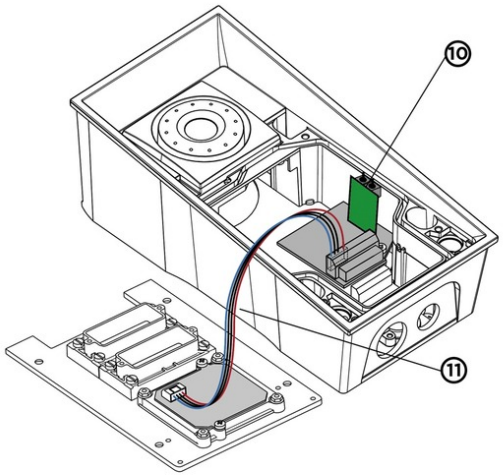
The module is compatible with the basic units with Part No.:

- 9151301CRP
- 9151302CR
- 9151302RP
- 9151302

## 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 longer, 12 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.

## 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.

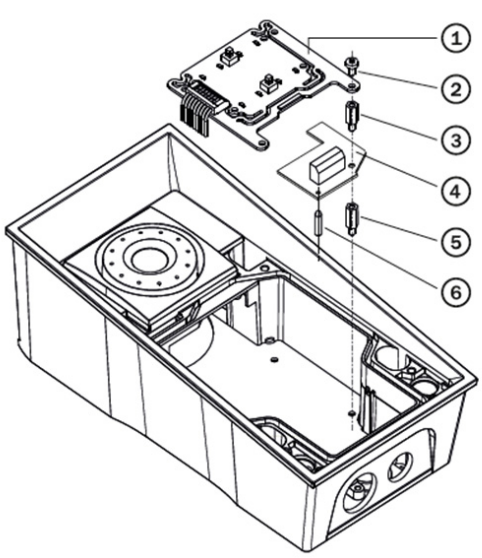
## Features

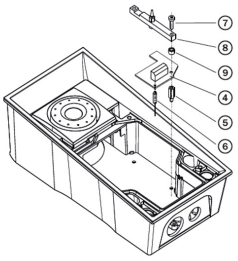
- The **2N IP Force 2.0** Additional Switch adds two additional switches, one logical input and a tamper switch to the main unit.

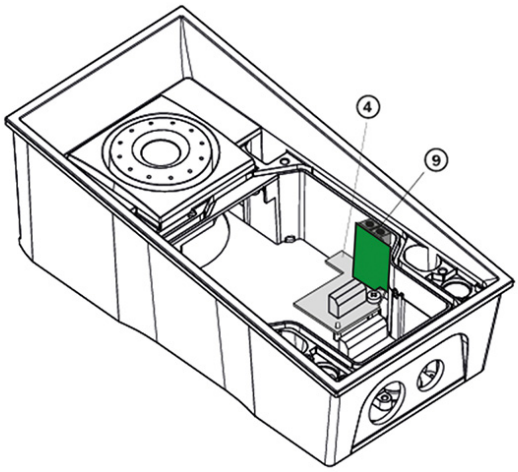
- The purpose of the tamper switch is to signal any unauthorized opening of the device (to prevent a theft, e.g.). It is recommended to use the tamper switch.

**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.

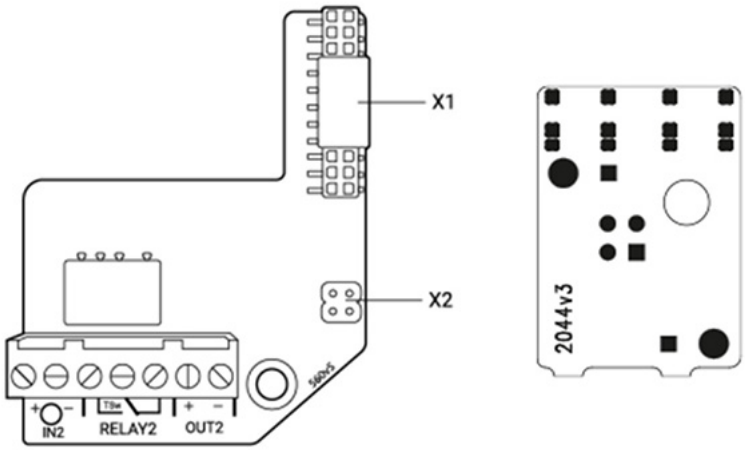
3. According to your model:
   a. If you are mounting the switch into a two-nameplate model, demount the button PCB (1) and remove the right-hand bottom spacer (there are four PCB fitting spacers altogether).
   b. If you are mounting the switch into a keypad model, take the keypad out of the holder. 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

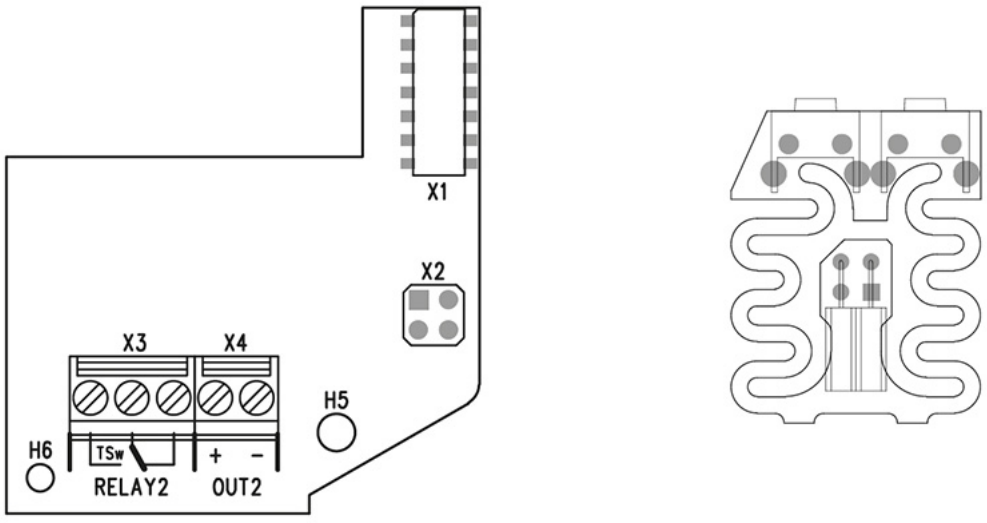
Refer to the Configuration Manual for details.

## Connection

### Version 5




### Version 4 and lower



## Security Relay

The Security Relay (9159010, 01386-001) is used for enhancing security between **2N IP Force 2.0** 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>  • 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!

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.

## 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 2.0** assembly. Other screws than stainless steel ones corrode soon and may aesthetically deteriorate the surrounding environment!

# Name Tags

**What you need:**

- **TORX 10:** You need a TORX wrench to loosen the frame screws.
- **New name tags:** Printed and cut according to the template.

## Download name tag template

1. Use official 2N templates for printing new name tags.
   - 2N IP Force, Force 2.0, Uni
2. A sheet of translucent foil is en closed to every device. Print it using a laser printer.
3. 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**

## Name tag opening

1. Unscrew the screw located on the right side of the name tag cover.

## Name tag closing

1. Look for the TORX screws on the frame, usually on the sides or bottom edge.
2. Insert the TORX 10 key and turn counterclockwise to loosen the screws. It is unnecessary to remove them completely.

## Name tag closing

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.

# 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

## IP Address Retrieval

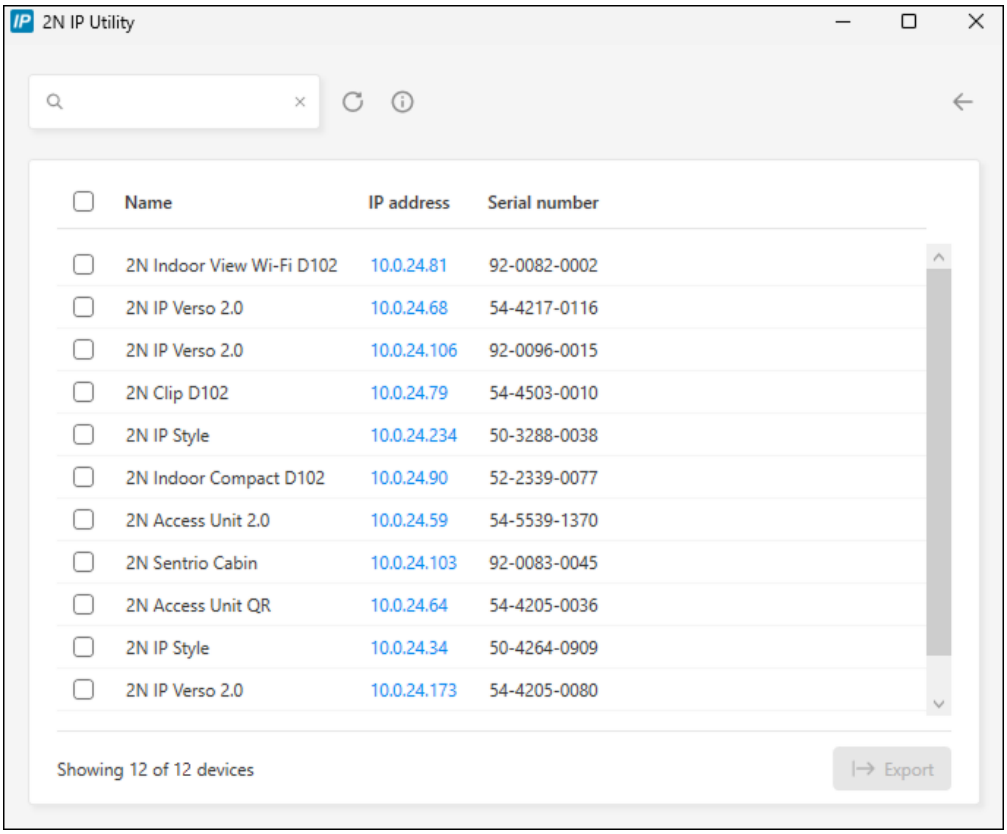
To retrieve the device IP address, take the following steps:

- Use the freely accessible 2N IP Utility.
- Use hardware (CONTROL 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 with CONTROL Button

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the device to start up completely.
   Backlight turning on indicates a complete start-up.
3. Press and hold the CONTROL button.
   Gradually wait for the following signals:
   a. one beep
4. Release the CONTROL button.
5. The device announces the current IP address via the speaker automatically.

**NOTE**
Remember to press the CONTROL button within 30 seconds after the device starts up.

Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

### IP Address Retrieval Using Speed Dial Button

Take the following steps to retrieve the **2N IP Force 2.0** IP address:

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Press the first Speed 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.

## Access to web device configuration

Configure **2N IP Force 2.0** via a web configuration interface, which is accessible from a web browser.

You need to know the IP address or domain name of the device for access to the interface. Make sure that the device is connected to the local IP network and powered.

The web configuration interface can also be accessed from the connected My2N portal or the 2N Access Commander configuration tool.

### Web Configuration Interface Login

1. Start your Internet browser.
2. Enter the device IP address or domain name (refer to Subs.Finding devices in the network).
3. If no certificate has been generated for the IP address, a security certificate invalidity notification may appear. In that case, confirm that you want to go to the web configuration interface.
4. The login screen is now displayed.
5. Enter the login data.
   The default login data are:
   - Username: **Admin**
   - Password: **2n**
6. After the first login, change the password.

### Access from 2N Access Commander

1. Log in to the Access Commander interface.
2. Go to the Devices page.
3. For the selected device, press .

### Password Change

You must change the default password to get full access to the web configuration interface features. You cannot configure the device without changing the default password.

**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.

## Firmware Update

**CAUTION**
The functionality, reliability and security of the device depend on the installed firmware. Regular firmware updates to the latest version are part of the terms of use of the product. The errors that may be caused by using an outdated firmware version cannot be subject to warranty claims. Always use the latest version, which contains bug fixes and security updates.

#### Update Modes

The device supports the following methods for obtaining a new firmware version:

- automatic update from the official 2N public update server
- automatic update from the provisioning server (auto-provisioning)
- management via a third-party service (Access Commander / My2N)
- manually uploading firmware from a local storage

Refer to **System > Firmware > Firmware Update Status** for information about the current firmware version.

### Update from Server

The device checks the official 2N update server, where the latest firmware versions are published.

### Update Settings from Update Server

1. Go to **System > Firmware** .
2. Choose **Server Update** on the **Firmware Update Configuration** card.
3. Select the firmware branch:
   - **Active Track** – latest stable version (recommended)
   - **Long Term Support (LTS)** – stable version with long-term support
   - **Beta Program** – test version

4. Set the update check interval.

> **TIP**
> Schedule updates for off-peak hours (night hours, e.g.) to avoid limitations of the device availability.

5. Save the changes.

## Automatic Updates (Auto-Provisioning)

The device regularly checks the defined provisioning server. The device will download the new version if available.

### Firmware source setting

1. Go to **System > Firmware** .
2. Choose **Automatic Updates** on the **Firmware Update Configuration** card.
3. In the open dialog box, complete the following:
   - provisioning server IP address parameters
   - relative path to the firmware file
4. If the server is secured, fill in the access details.
5. To increase security, set up the server certificate authentication and select the Client Certificate under which it will be authenticated.
6. In the next step, set the server check interval.

> **TIP**
> Schedule updates for off-peak hours (night hours, e.g.) to avoid limitations of the device availability.

7. Save the changes.

## Required File Structure

The device expects files with names in the format: `MODEL-firmware.bin`

**Name parameters**

- MODEL – device identifier

| device | MODEL |
|---|---|
| 2N IP Verso 2.0 | verso2 |
| 2N IP Style | style |
| 2N IP One | ipone |

### Manual Firmware Check and Installation

#### Manual Check for Update Availability

1. Go to **System > Firmware** .
2. Click the Check for Updates button on the **State** card.

**NOTE**
You can find information about the last and scheduled checks in the Firmware Update Log panel.

### Manual Firmware Installation

#### Uploading New Firmware from Storage

1. Go to **System > Firmware** .
2. Click the **Upload Firmware button on the Firmware Update Status card.**
3. In the open dialog box, select a file from your own storage.
4. Click Upload to confirm the file upload.
   The device checks the firmware file and prevents you from uploading an incorrect or corrupt file.
5. Once the firmware is uploaded successfully, the device is restarted automatically. After the restart, the device becomes fully operational with a new firmware version. The FW upgrade does not affect configuration.

**CAUTION**
Do not disconnect the device from power during the update process.

## Device Restart

To restart the device choose one of the following options:

- using power disconnection and reconnection
- via the web configuration interface.

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

### Restart Using Web Configuration Interface

1. Open the web configuration interface.
2. Go to **System > Maintenance**.
3. Press Restart Device in the page header.

## Factory Default Reset

Factory settings can be restored using the CONTROL button on the device hardware.

**CAUTION**
In case the factory default values are reset on the device with a firmware version 2.18 or higher, it is necessary to reprogram the 2N Security Relay using the instructions given in Security Relay (p. 62).

**NOTE**
It is possible to restore the default configuration values in the web configuration interface. Restoring the default configuration is not the same as factory reset – it preserves, for example, the network configuration and some door switch states.

The detailed procedure is provided in the Configuration Manual.

## Factory Default Reset with CONTROL Button

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the device to start up completely.
   Backlight turning on indicates a complete start-up.
3. Press and hold the CONTROL button.
   Gradually wait for the following signals:
   a. one beep
   b. two beeps after 3 seconds
   c. three beeps after 3 seconds
   d. four beeps after 3 seconds
4. Release the CONTROL button.
5. The device reboots and starts up with the factory settings.

**NOTE**
Remember to press the CONTROL button within 30 seconds after the device starts up.

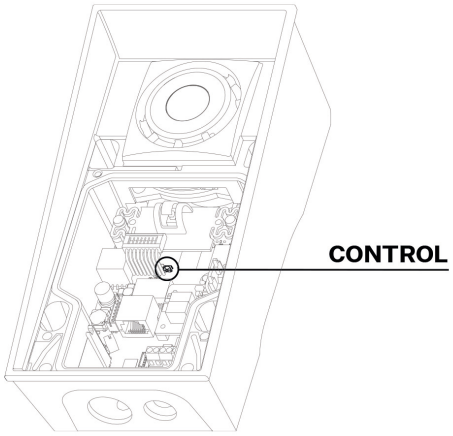
Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

# Configuration via Hardware

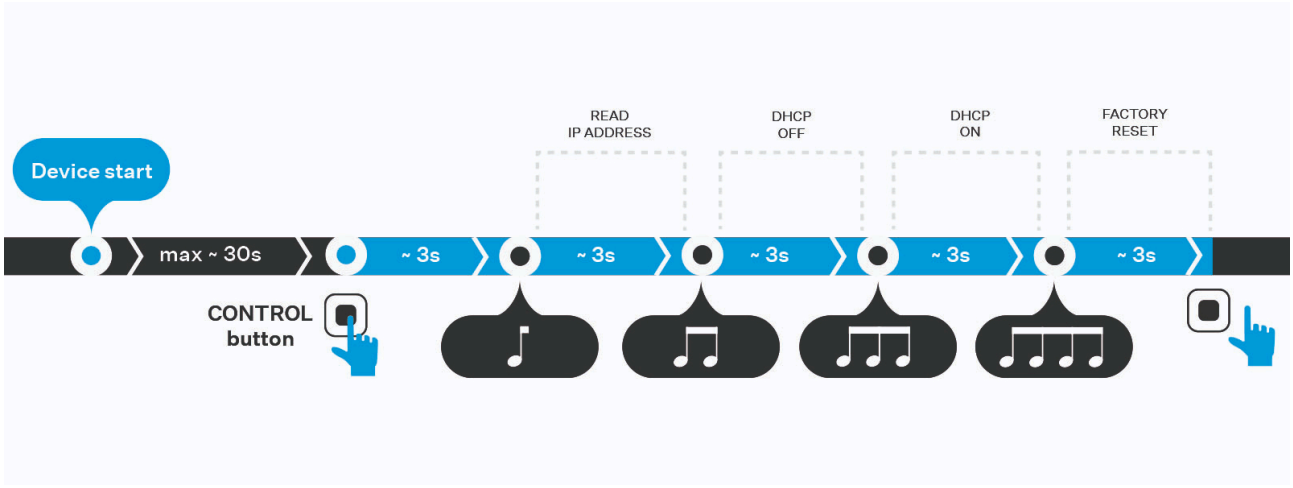
Where software configuration is unavailable, make the basic settings using the hardware CONTROL button.

The CONTROL button allows you to retrieve the device IP address, switch the IP address retrieval mode or restore the factory settings.

## CONTROL Button Position




## Hardware Configuration Intervals




Once the device is started, you have 30 seconds to press and hold the button to trigger a sequence of sound signals (beeps). Each function is assigned to a certain number of beeps. Releasing the button within a given interval will perform the corresponding action. If you continue to hold the button after the fourth beep, the device will not execute any action and the process will be aborted.

## IP Address Retrieval with CONTROL Button

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the device to start up completely.
   Backlight turning on indicates a complete start-up.
3. Press and hold the CONTROL button.
   Gradually wait for the following signals:
   a. one beep ♩
4. Release the CONTROL button.
5. The device announces the current IP address via the speaker automatically.

**NOTE**
Remember to press the CONTROL button within 30 seconds after the device starts up.

Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

## Static IP Address Setting with CONTROL Button

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the device to start up completely.
   Backlight turning on indicates a complete start-up.
3. Press and hold the CONTROL button.
   Gradually wait for the following signals:
   a. one beep
   b. two beeps after 3 seconds
4. Release the CONTROL button.
5. The following static network parameters are now set for the device:
   - IP address: 192.168.1.100
   - Network mask: 255.255.255.0
   - Default gateway: 192.168.1.1

**NOTE**
Remember to press the CONTROL button within 30 seconds after the device starts up.

Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

## Dynamic IP Address Setting via CONTROL Button

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the device to start up completely.
   Backlight turning on indicates a complete start-up.
3. Press and hold the CONTROL button.
   Gradually wait for the following signals:
   a. one beep
   b. two beeps after 3 seconds
   c. three beeps after 3 seconds
4. Release the CONTROL button.
5. The device is now set to obtain an IP address from a DHCP server.

**NOTE**
Remember to press the CONTROL button within 30 seconds after the device starts up.

Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

### Factory Default Reset with CONTROL Button

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Wait for the device to start up completely.
   Backlight turning on indicates a complete start-up.
3. Press and hold the CONTROL button.
   Gradually wait for the following signals:
   a. one beep
   b. two beeps after 3 seconds
   c. three beeps after 3 seconds
   d. four beeps after 3 seconds
4. Release the CONTROL button.
5. The device reboots and starts up with the factory settings.

**NOTE**
Remember to press the CONTROL button within 30 seconds after the device starts up.

Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

## 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. 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

# Device Control

**2N IP Force 2.0** is an intercom allowing you to:

- call other devices
  - use speed 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,
  - using a QR code
  - by entering a numeric access code via a keypad application



**NOTE**
Refer the for call setup and assigning contacts to speed dial buttons.

# Troubleshooting

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

# Technical Parameters

| Power supply types | |
|---|---|
| PoE | IEEE PoE+ 802.3at (Class 4–25,5 W) |
| External supply | 12 V / 4 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 | 10W / 4 Ω (class D) |
| Speaker | 10 W |
| Sound pressure level (SPL max) | 94 dB (for 1 kHz, distance 1 m) |

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

| Audio stream | |
|---|---|
| Protocols | • RTP |
| 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 2592 × 1944 |
| Video resolution | 2560 × 1920 |
| Frame rate | 30 fps (H.264), 15 fps (MJPEG) |
| Sensor sensitivity | 14000 $e^{-}$/Lux-sec |
| Viewing angle | 133° (H), 112° (V) |
| Infrared illumination | Yes |
| Sensor sensitivity without IR light | 0.1 Lux ± 20 % |
| Focal length | 1.935 mm |

| Video stream | |
|---|---|
| Protocols | • RTP<br>• RTSP<br>• SRTP<br>• HTTP |
| ONVIF/RTSP streaming codecs | • H.264<br>• H.265<br>• MJPEG |
| IP Camera Function | Yes – compatible profiles:<br>• ONVIF v2.4 profile S<br>• ONVIF Profile T |

| Interface | |
|---|---|
| LAN | 10/100BASE-TX with Auto-MDIX, RJ-45 |
| Recommended cabling | Cat6 (MPTL) |
| Supported protocols | SIP2.0, SIPS, DHCP opt. 66, SMTP, SNMP, TR069, 802.1x, RTSP, RTP, SRTP, TFTP, HTTP, HTTPS, Syslog, ONVIF |
| Passive switch (relay) | SSR NO, max. 30 V / 1A 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) |

| Mechanical Parameters | |
|---|---|
| Front Panel | Aluminum cast<br>• Fiberglass FR4 |
| Body material | |
| Body material | ADC12 ALUMINIUM |
| Device dimensions | 217 × 109 × 83 mm |
| Weight | 2 kg |
| Operating temperature | −30 °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 | IP69 |
| Resistance level | • Frame: IK10<br>• Camera: IK08<br>• Front panel: IK08 |

# 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 2.0** conforms to the following directives and regulations:

### EU

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

- 2014/35/EU for electrical equipment designed for use within certain voltage limits
- 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.

Contains an RFID IC module: 22140-NFC2F.

## US

Contains an RFID module FCC ID: 2AQPZNFC2F.

## FCC

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

NOTE: These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

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

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

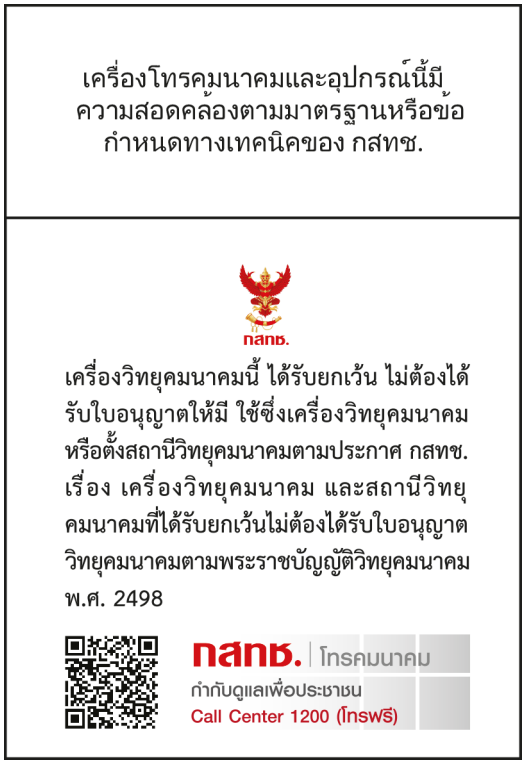
Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

## 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




## Legislation of Japan

この装置は、クラス B 機器です。この装置は、住宅環境で使用この装置は、クラス B 機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。 取扱説明書に従って正しい取り扱いをして下さい。
VCCI – B

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 2.0 – Installation Manual

© 2N Telekomunikace a. s., 2026

**2N.com**