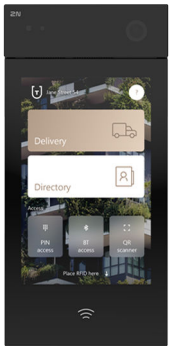
2N IP Style

Installation Manual



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

2N.com

Table of Contents

Symbols and Terms Used

The following symbols and pictograms are used in the manual:

DANGER
Always abide by this information to prevent persons from injury.

WARNING
Always abide by this information to prevent damage to the device.

CAUTION
Important information for system functionality.

TIP
Useful information for quick and efficient functionality.

NOTE
Routines or advice for efficient use of the device.

Product Description

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

Basic Features

2N IP Style is an elegant and reliable intercom equipped with lots of useful functions. Thanks to SIP support and compatibility with major brands of PBX manufacturers, it can benefit from using VoIP networks.

2N IP Style can be used as a door or special purpose intercom for office buildings, residential areas and/or other applications.

The main advantages of this device are:

ARTPEC-7 – Axis' high-performance processor.

Wide Angle Camera with HD Resolution – the calling persons can be displayed to the called user on the 2N answering units, the user phone or PC. The camera is elegantly hidden behind darkened glass, so it is not visible. The device is also equipped with a night vision system, which automatically selects the night/day mode according to the ambient light.

10" touch display – displays the list of destinations (groups/individuals) for outgoing call setups. You can set up to three phone numbers and call time profiles to each of the buttons to make the called subscriber accessible any time.

Keypad – touch numeric keypad allowing you to use the intercom as a code lock for lock switch activation or for making calls to a selected user phone/virtual number.

Card reader – integrated card reader providing access control management using 125 kHz and 13.56 MHz (optionally secured) RFID cards. With additional software features, functions other than the door lock can be RFID card controlled too.

Electric lock switch – this switch can be controlled using an RFID card reader, a numeric keypad, the 2N My2N application in your smartphone, a PC application or during a call from any phone. If necessary, more modules with required outputs can be added.

Robustness – the device is designed as a robust, mechanically resistant intercom, which withstands weather conditions without needing extra accessories.

Audio Quality– thanks to the integrated acoustic echo cancellation (AEC) system, full duplex communication provides bilateral audibility even when the calling users are speaking at the same time.

Device Installation – the option is to use surface installation using a chassis or flush mounting using a wall mounting box.

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,
- high-end design,
- 10" touch display,
- weather resistance,
- surface/flush mounting,
- sensitive microphone and speakerphone,
- bidirectional communication – acoustic echo cancellation,
- integrated color HD camera with a wide-angle lens and night vision,
- numeric touch keypad,
- integrated electronic lock switches with wide setting options,
- integrated 125 kHz and 13.56 MHz (optionally secured) RFID card reader,
- LAN (PoE+) or external 12 V / 4 A power supply
- configuration via web interface,
- QR code reading support, face zooming
- SIP 2.0 and SIPS support
- up to 54 buttons for calling preset phone numbers,
- up to 10 000 phone book positions,
- up to 20 user time profiles,
- video codecs (H.264, MJPEG),
- audio codecs (G.711, 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. 9157101

Axis Part No. 02521-001

Main unit 2N IP Style

Includes an internal 125 kHz and 13.56 MHz card reader.

Part No. 9157101-S

Axis Part No. 02407-001

Main unit 2N IP Style

Includes an internal 125 kHz card reader and 13.56 MHz secure card reader.

Accessories

Accessories for Installation

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

Choose the proper accessories for your particular installation needs.

Extenders

NOTE
2N IP Style also supports the **2N IP Verso** extending modules.

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. 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. 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)
- **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)
- **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)
- **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)
- **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)
- **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)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **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)
- **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)
- **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. 9155034

Axis Part No. 01257-001

I/O Module

The module provides logical inputs and outputs for integration of sensors or other devices.

The module is installed under another module, i.e. needs no separate position.

Part No. 9155037

Axis Part No. 01259-001

Wiegand Module

The Wiegand module helps you interconnect your system with other systems via the Wiegand interface.

The module is installed under another module, i.e. needs no separate position.

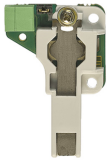
Part No. 91550371

Axis Part No. 02577-001

OSDP Module

The OSDP module provides OSDP communication with a connected OSDP device (control panel, door controller) and **2N IP Style** (placed outside).

The module is installed under another module, i.e. needs no separate position.



Part No. 9155038

Axis Part No. 01260-001

Tamper Switch

Tamper Switch is a module which detects that the device has been opened or the top cover removed.

The module is installed under another module, i.e. needs no separate position.

Remember to purchase the I/O module (9155034, 01257-001), along with the Tamper Switch.

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. 9155198SET

Axis Part No. 01975-001

Security Package for 2N Devices

The security package provides increased door security.

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

Power Supply

Part No. 9159052

Axis Part No. 01393-001

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

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

Licenses

Part No. 9137909

Axis Part No. 01380-001

Gold License

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

Part No. 9137910

Axis Part No. 01381-001

InformaCast License

Part No. 9137921

Axis Part No. 03160-001

MS Teams license

TIP

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

Other accessories

Part No. 9159013

Axis Part No. 02523-001

Departure button

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

Part No. 9159012

Axis Part No. 01388-001

Magnetic door contact

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

Part No. 9134173

Axis Part No. 01384-001

MIFARE RFID chip card, 13.56 Hz

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

Part No. 9134174

Axis Part No. 01385-001

MIFARE RFID chip fob, 13.56 MHz

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

Part No. 9134165E

Axis Part No. 01395-001

EM RFID chip card, 125 Hz

RFID chip card, type EM4100, 125 kHz.

Part No. 9134166E

Axis Part No. 01396-001

EM RFID chip fob, 125 kHz

RFID chip fob, type EM4100, 125 kHz.

Part No. 11202601

Axis Part No. 02787-001

MIFARE DESFire RFID chip card, 13.56 MHz

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

Suitable for data encryption in PICard Commander.

The package includes 10 pieces.

Part No. 11202602

Axis Part No. 02788-001

MIFARE DESFire RFID fob, 13.56 MHz

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

Suitable for data encryption in PICard Commander.

The package includes 10 pieces.

Part No. 9137420E

Axis Part No. 01399-001

External RFID reader, 125 kHz

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

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

Part No. 9137421E

Axis Part No. 01399-001

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

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

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

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

The following RFID cards can be read:

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

Supported RFID cards 13.56 MHz:

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

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

Part No. 9137424E

Axis Part No. 01527-001

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

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

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

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

The following RFID cards can be read:

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

Supported RFID cards 13.56 MHz:

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

Part No. 9137410E

Axis Part No. 01397-001

External IP relay, 1 output

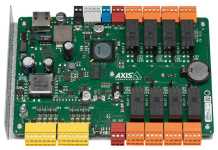
Stand-alone IP relay, which can be controlled from an intercom via HTTP commands and helps control devices from an unlimited distance.

Part No. 9159014EU/US/UK

Axis Part No. 01404-001

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

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



Part No. 9160501

Axis Part No. 0820-001

AXIS A9188 Network I/O Relay Module

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

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 Style**
1x	Certificate of ownership
1x	Brief Manual
2x	Frame fitting

Module / Frame Package Completeness Check

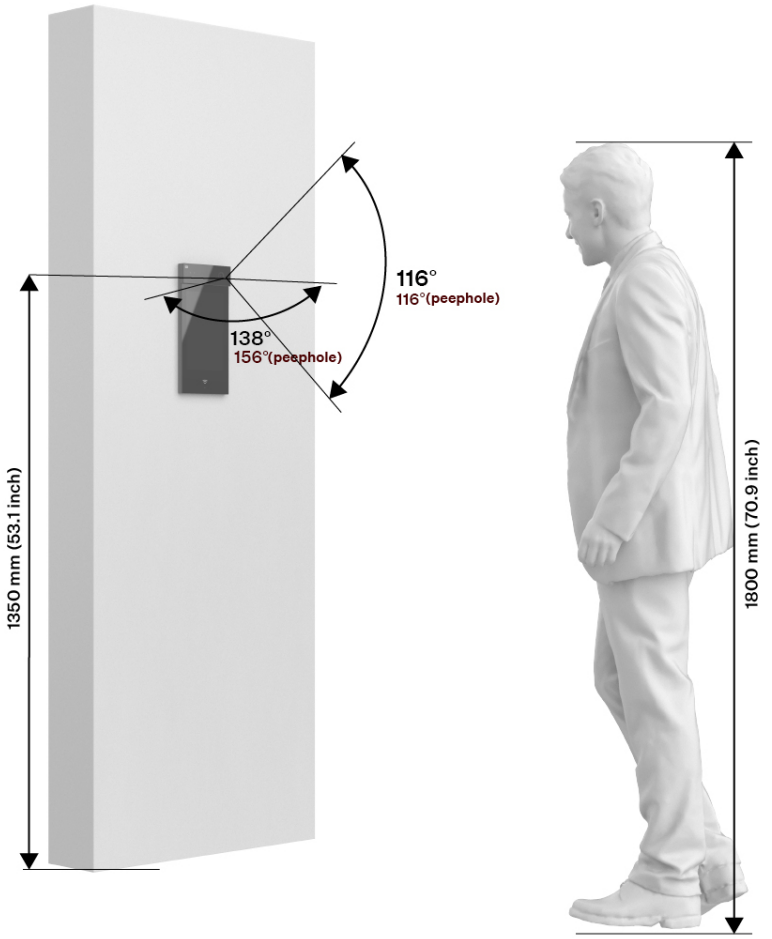
The package of modules for **2N IP Style** includes:

3x	3 x 8 mm stainless steel thread-forming lens head screw for plastic

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

Installation

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



Mechanical Installation

Installation Conditions

Make sure that the following 2N IP Style 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 designed for vertical wall mounting (perpendicular to the floor) in the height of up to 1350 mm above the floor. If necessary, operate the device in a position other than as aforementioned for a short time only, for quick testing purposes in a servicing center, for example.

- Make sure that the plasterboard interior does not show a pressure value significantly different from that of the room, e.g. that it is not connected with overpressure ventilation. If the difference is too great, separate the device in terms of pressure (using, e.g., a mounting box) and seal the cable passage.
- 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.
- Make sure that the VoIP connection is configured properly according to the SIP and other VoIP recommendations.

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.Technical Parameters (p. 77).
- Any intentional mechanical damage to the device (drilling, main unit tampering, etc.) results in a loss of warranty.
- The device installation and setting should only be performed by professionally qualified persons.
- The installation and adjustment of this device, including any handling thereof, should only be carried out by persons qualified to do so.

Installation Tips

- The recommended height is 135 cm for standard installations (100–120 cm for disabled persons) from the floor to the device camera level. The installation heights may vary depending on the device use.

Viewing angle	138° (H), 114° (V)

Flush Mounting

The flush mounting box allows you to place cables in the wall below **2N IP Style** and mount the device.

What you need for mounting:

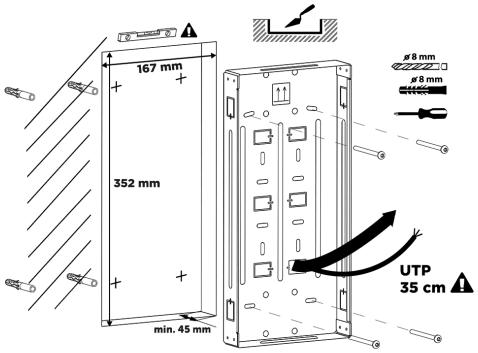
- **2N IP Style**
- Flush mounting box (9157001, 02405-001)

TIP

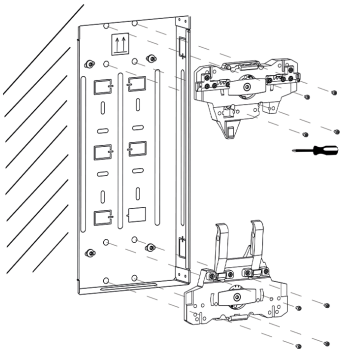
The drilling template and the surface drilling template is available for download at 2N.com.

Box Installation

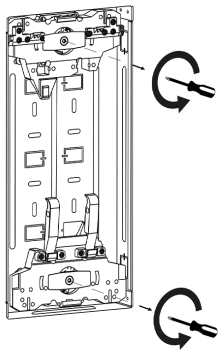
1.



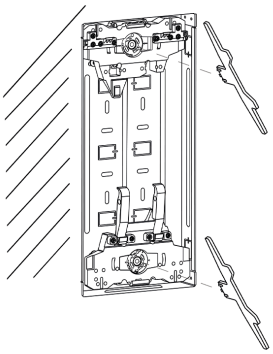
2.



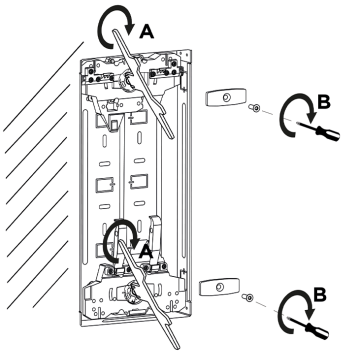
3.



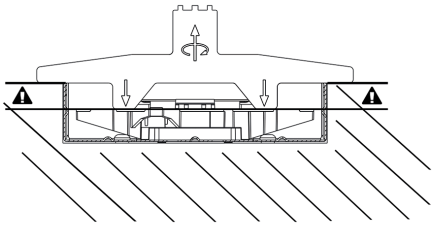
4.



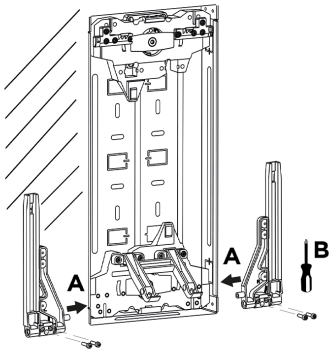
5.



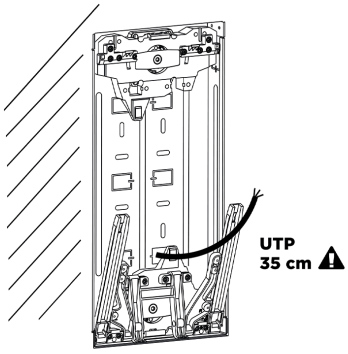
6.



7.



8.



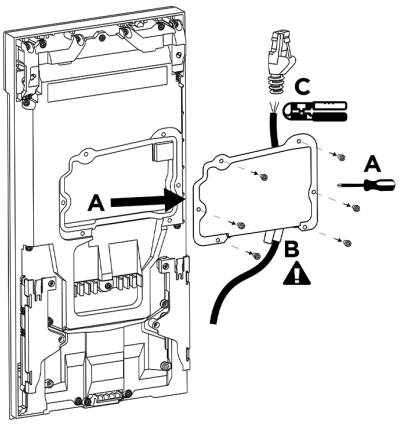
1. Make a hole of the size of 352 (h) x 167 (w) x 45 (d) mm for the mounting box installation. Remove the selected blank for cabling. Thread the cables through the selected box hole and put the mounting box in the pre-prepared hole. Make sure that the box hole is deep enough and that the box edges are aligned with the wall surface. If the hole is convenient, anchor the box using screws and dowels.

2. Insert the enclosed detents in the riveting nuts. Make sure that the tops of the detents direct towards the box center against each other. The detent with 2 handles is intended exclusively for the box bottom installation. Fit the detents with screws.
3. If the detent seat seems too deep, remove the detent fixture by unscrewing the screw.
4. Insert the levelling wrench into the grooves of the levelling mechanism in a twisting motion to bring it to the desired height. The levelling mechanism allows for a shift of up to 8 mm in height.
5. After levelling re-anchor the fixture with a screw.
6. Use a levelling key to check the proper height of detent embedding to make sure that the key is aligned with the mounting box edge and also touches the detent surface.
7. Put the brackets to the left and right sides of the bottom detent handle (7A) and fit their positions using screws (7B).
8. Now the mounting box installation is complete.

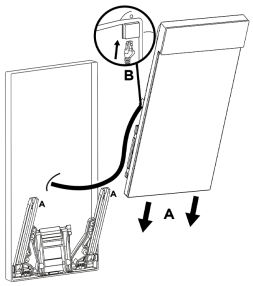
Main Unit Installation

All necessary cables must be routed to deploy the main unit. The recommended length of the accessible cables is 35 cm.

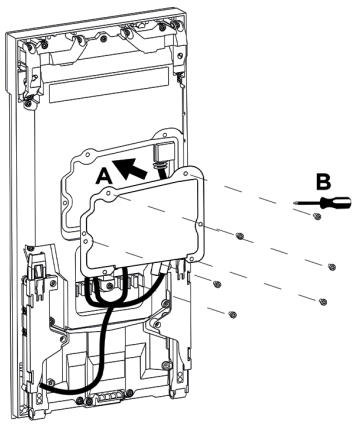
1.



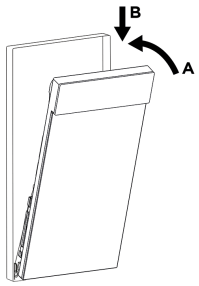
2.



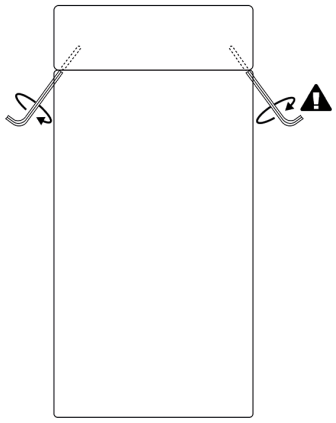
3.



4.

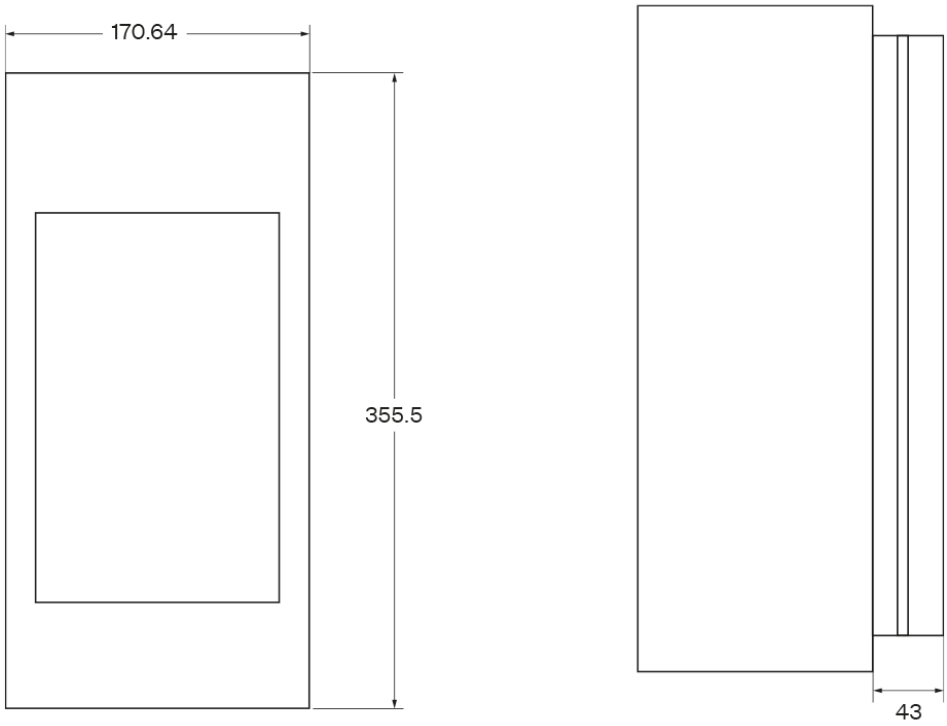


5.



1. Unscrew the connector cover on the back of the device. Thread all of the cables with no connectors (terminals or end pieces, etc.) through the bushing on the inside of the connector cover. After threading the cables through the bushing, fit the required end pieces.
2. Fold out the mounting bracket located at the bottom of the chassis or flush mounting box. Fit the profiles on the device back onto the mounting bracket and slide them down to the lowest possible position, anchoring the device by snapping it into place (2A). Connect all the cables to the device (2B). The mounting bracket provides sufficient support for cable installation and so it is unnecessary to support the device in any way.
3. After connecting and fixing the excess lengths of cables in the handles (3A), screw the connector cover back (3B).
4. Push the device towards the chassis or flush mounting box (4A) and then push downwards (4B). The installation is sealed.
5. Lock the position by tightening the two screws inside the device using an Allen key.

Surface Installation



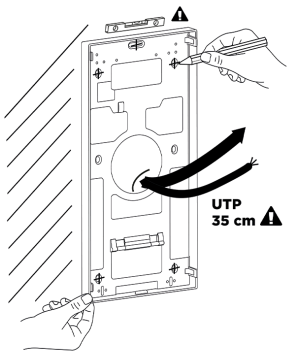
What you need for mounting:

- **2N IP Style**
- surface mounting chassis (9157002, 02406-001)

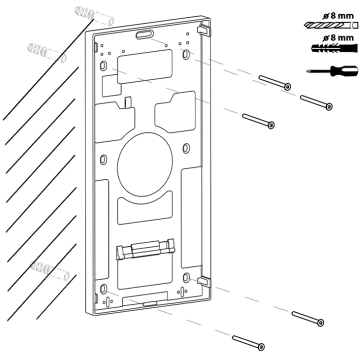
TIP
Download the drilling template from 2N.com.

Chassis Installation

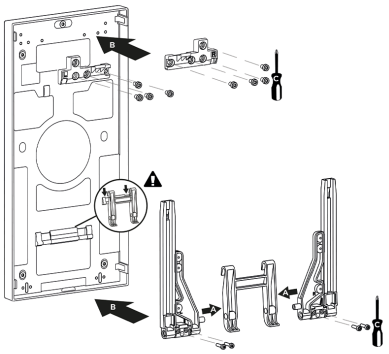
1.



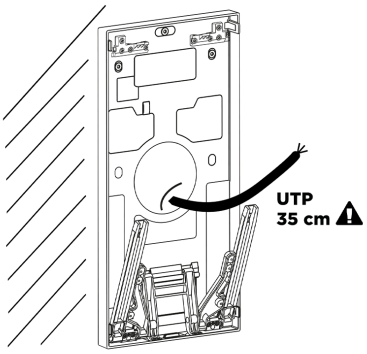
2.



3.



4.

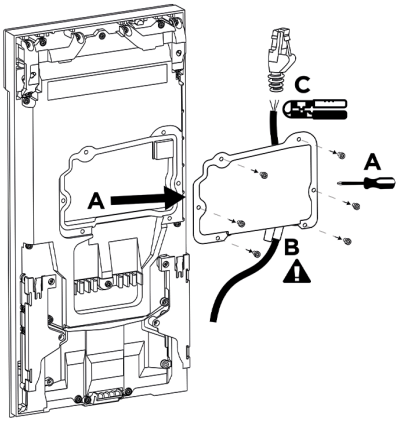


1. Drill chassis anchoring holes on a proper place. Use the chassis itself as a template to maintain the horizontal level and carry the cabling at the bottom edge of the cable hole. The recommended length of the accessible cables is 35 cm.
2. Insert the dowels in the holes drilled and use the screws to anchor the chassis.
3. Put the brackets to the left and right sides of the support handle and fit their positions using screws (3A). Fit the lock counterparts to the upper chassis part, hang the handle with the brackets to the bottom part (3B) and fit all the components using screws (3C).
4. Now the chassis installation is complete.

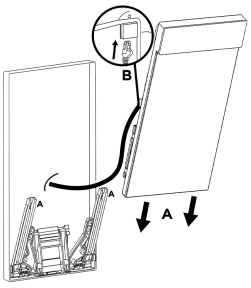
Main Unit Installation

All necessary cables must be routed to deploy the main unit. The recommended length of the accessible cables is 35 cm.

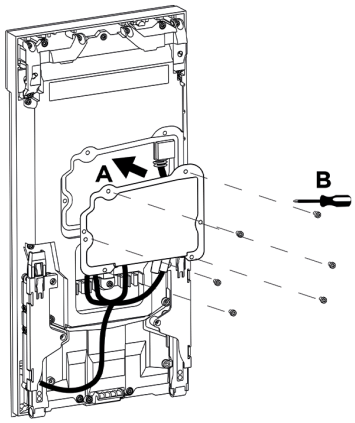
1.



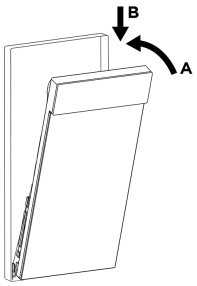
2.



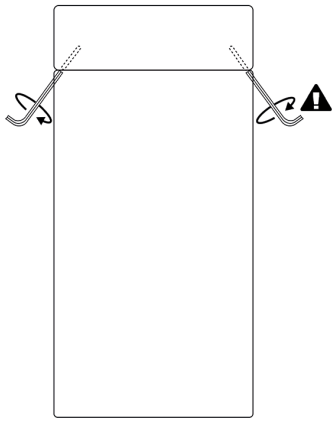
3.



4.



5.



1. Unscrew the connector cover on the back of the device. Thread all of the cables with no connectors (terminals or end pieces, etc.) through the bushing on the inside of the connector cover. After threading the cables through the bushing, fit the required end pieces.
2. Fold out the mounting bracket located at the bottom of the chassis or flush mounting box. Fit the profiles on the device back onto the mounting bracket and slide them down to the lowest possible position, anchoring the device by snapping it into place (2A). Connect all the cables to the device (2B). The mounting bracket provides sufficient support for cable installation and so it is unnecessary to support the device in any way.
3. After connecting and fixing the excess lengths of cables in the handles (3A), screw the connector cover back (3B).
4. Push the device towards the chassis or flush mounting box (4A) and then push downwards (4B). The installation is sealed.
5. Lock the position by tightening the two screws inside the device using an Allen key.

Electric Installation

Power Supply

2N IP Style can be fed either directly from the LAN if equipped with PoE+ 802.3at supporting network elements or from an external 12 V ±15 % / 4 A DC power supply.

CAUTION

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

PoE Supply

2N IP Style is compatible with the PoE+ 802.3at 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 Style** and the nearest network element. This power supply provides **2N IP Style** with 21.6 W for its own feeding .

CAUTION

- The PoE power supply cannot provide **2N IP Style** with a full functionality as it only offers a limited mode (Low Power Mode) for basic configuration. This way of feeding is not recommended. Connect the device to a PoE+ supply or a convenient DC supply and restart the device.
- The PoE power supply detection is performed during the device restart.
- If PoE supply is used where the device works in the Low Power Mode:
  - The power supply trouble is displayed in all the settings
  - The display backlight is limited (the backlight can be just 25% of the available brightness value)
  - The status LED on the front side is nonfunctional
  - Any module connected to the device via the vbus cable is nonfunctional

External Power Supply

Use a SELV supply 12 V ±15 % dimensioned to the current consumptionaccording to the required power output for the to make your device work reliably.

CAUTION

Make sure that the wires are firmly attached to the terminal to avoid any free contact.

Current consumption [A]	Available power output [W]
3	36
4	48

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

2N IP Stylecan be fed from an external power supply and PoE at the same time. In this configuration, the maximum power for the is available.

WARNING

- In case the external power supply is disconnected / fails during the combined external / PoE feeding, the device will get restarted. The device will run in the Low Power Mode and a feeding problem warning will be displayed in all of the configuration sections.
- Reconnect the device to an external power supply or Poe+ and force restart to recover the full functionality.

Combined Power Supply

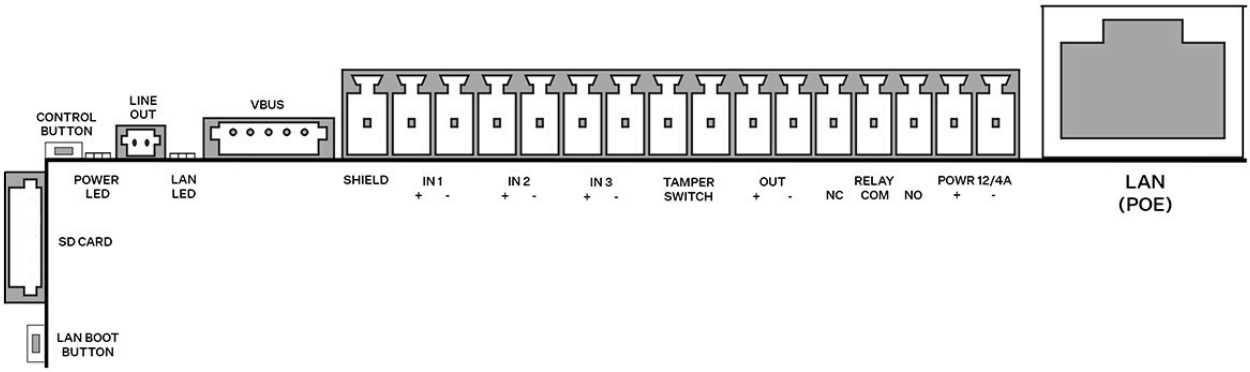
Main Unit Max Power Overview

Main unit	Max consumption mA (from 12V supply)	Max consumption W (from 12V supply)	Max consumption W (z PoE+)
At relax	505	6.06	7.13
Restart	700	8.4	9.88
Infrared light (100%)	655	1.8	2.12
Display backlight intensity (100%)	950	4.8	5.65
Audio (100 %)	1420	10.98	12.92
Video motion detection	20	0.24	0.28
OUTPUT	600	7.2	8.47
RFID ON	550	0.54	0.64
Pictogram backlight (100 %)	570	0.24	0.28
Video streaming (ON)	530	0.3	0.35
CPU (100 %)	50	0.6	0.71
Memory (100 %)	25	0.3	0.35
GPU (100 %)	50	0.6	0.71
3 x Stream H.264 (1920 x 1080) MJPEG (1280 x 720)	50	0.6	0.71

Main unit	Max consumption mA (from 12V supply)	Max consump-tion W (from 12V supply)	Max consumption W (z PoE+)
Maximum Power	**5 925**	**33,66**	**39,61**

Device Connectors

Main unit connector wiring



Name	Description
LAN BOOT BUT-TON	LAN Connection Restart Button
SD CARD	SD card slot

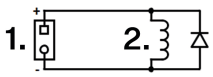
Name	Description
CONTROL BUTTON	Factory reset button
POWER LED	Device status LED
LAN LED	LAN connection status LED
VBUS	Bus connector
SHIELD	Grounding terminal **CAUTION** We recommend that a grounding cable of the cross-section of 1.5 mm^2 is used.
IN 1/2/3	Input terminals for passive/active mode (-30 V to +30 V DC) • OFF = open contact or U_{IN} > 1.5 V • ON = closed contact or U_{IN} < 1.5 V
TAMPER SWITCH	Security system connecting terminals (on the back side above the connectors)
OUT	Active switch output: 12 V DC, max. 600 mA
RELAY	RELAY terminals with accessible 30 V / 1 A AC/DC NO/NC contact. Used for connection of non-critical devices only (lights, e.g.).
POWER 12 V / 4 A	External power supply terminals /
LAN (POE)	LAN connector (PoE+ 802.3at)
Tamper Switch	Switch detecting unauthorized device opening

Available switches

Location	Name	Description
Main unit	RELAY	**Passive switch:** • switching and expandable contact • max. 30 V / 1 A AC/DC • only used to connect non-critical devices (e.g. lights)
	OUT	**Active switch output:** • 10 to 12 V DC, max. 600 mA

Multiple modules marked with an asterisk (*) can be used.

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

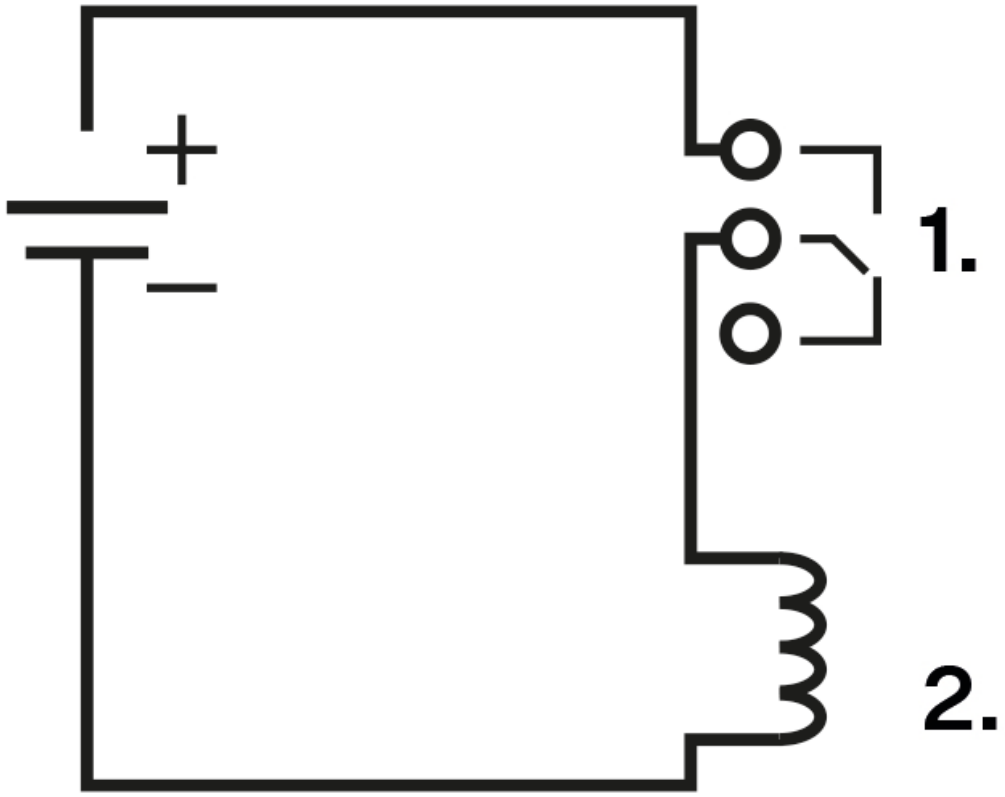
It is possible to connect a device to the **2N IP Style** relay terminals to be controlled by this relay, e.g. an electric/electromechanical door lock.

The elements are designated as follows in the diagrams below:

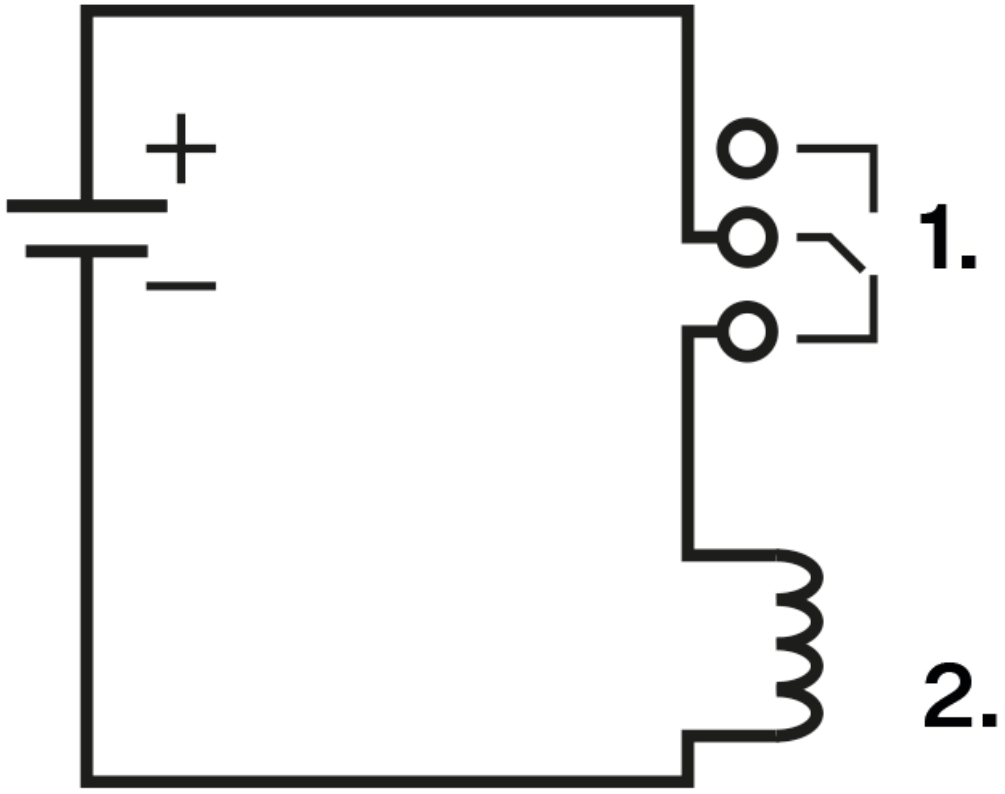
1. Device relay

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

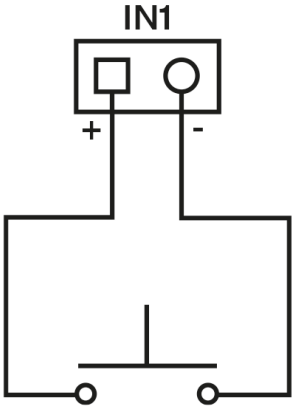


Connection of IN1 inputs (or IN2)

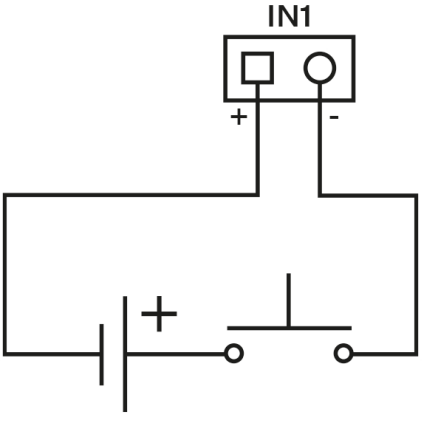
It is possible to connect an external button, e.g. a departure button or door open sensor, to the IN1 or IN2 terminals of device**2N IP Style**.

The following wiring diagrams apply both to IN1 and IN2.

Wiring diagram of IN1 terminals in active mode



Wiring diagram of IN1 terminals in passive mode



LAN Connection

2N IP Style is connected to the LAN by inserting a SSTP cable (Cat-5e or higher) terminated with an RJ-45 plug into the marked LAN connector on the device . 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. 36).
- We recommend the use of a shielded SSTP Ethernet cable.

TIP

Remove the protective connector cover to facilitate the threading of the SSTP cable RJ terminal into the device box.

Overvoltage Protection

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

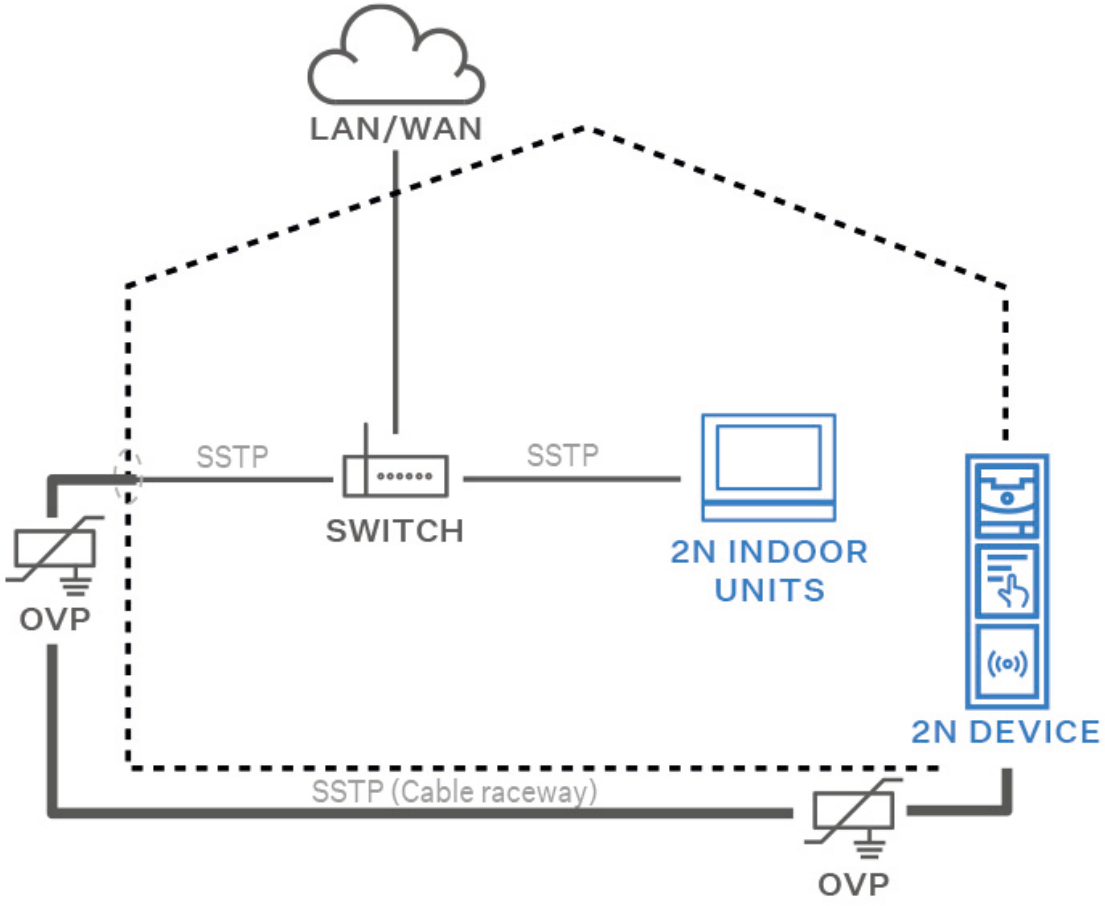
Therefore, we recommend that additional overvoltage protectors (OVP) be installed on the outer walls or roof for all the wires leading outside the building. Keep the following instructions while installing overvoltage protectors:

- Make sure that the overvoltage protector is installed as close as possible to the device installed outside the building.

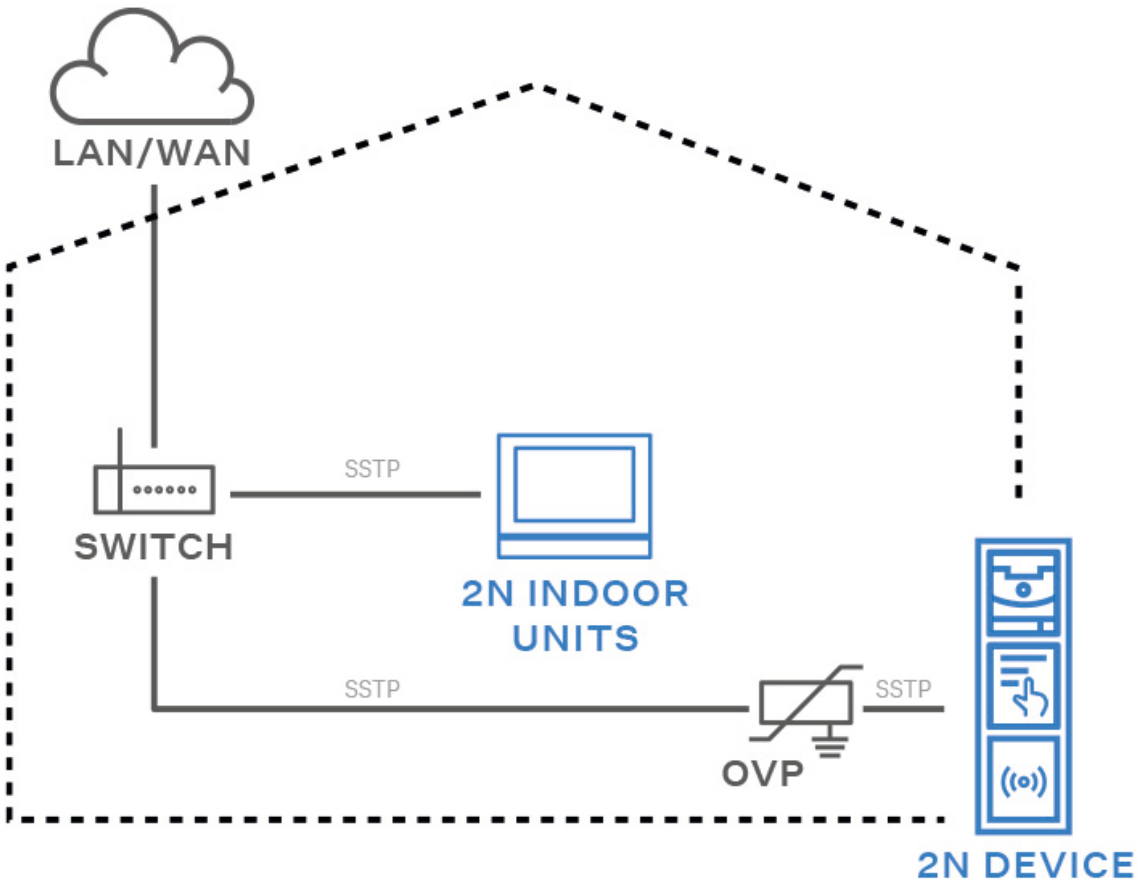
- Make sure that the overvoltage protector is installed as close as possible to the device installed on an external part of the building.
- Make sure that the overvoltage protector is installed as close as possible to the point where the cabling leaves the building.

Examples of Overvoltage Protection Installation

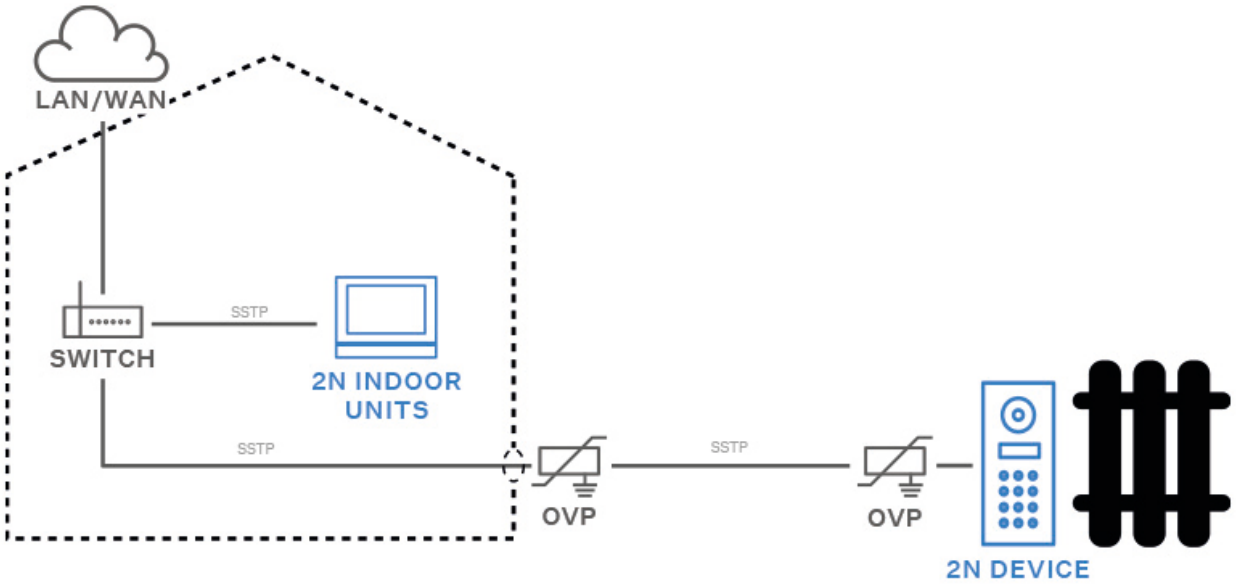
Overvoltage protection installation diagram for a device installed on the building facade and cables outside the building



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



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



Main and Extending Modules

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

2N IP Style can be interconnected with the following modules:

- 125 kHz RFID card reader (p. 41)
- 13.56 MHz NFC RFID card reader (p. 41)
- Secured 13.56 MHz, NFC RFID card reader (p. 42)
- Biometric fingerprint reader (p. 42)
- 5-button (p. 43)
- I/O module (p. 43)
- Wiegand module (p. 45)
- Security Relay (p. 49)
- Tamper Switch module (p. 51)
- OSDP module (p. 53)
- Induction Loop module (p. 57)

Module Interconnection

All the modules that can be connected to the device are interconnected via a bus. The bus starts on the main unit and goes over all the modules. The order of the modules on the bus is irrelevant. And it is also irrelevant which bus connector is used as the input and which is used as the output on the module.

The modules include a 220 mm long bus interconnecting cable.

The Wiegand, OSDP and I/O modules include an 80 mm long bus cable.

It is possible to order separate bus cables of the length of 1 m, 3 m or 5 m (9155050/9155054/9155055, 01267-001/01268-001/01269-001 respectively), which are intended for remote module installations. Typically, they help install an RFID card reader on the opposite side of the wall on which the device communicator is installed. This cable may only be used once on the bus. The total length of all the bus cables used in these extended installations may not exceed 7 m.

CAUTION
Purchase a frame / mounting box for the extending modules to be connected according to the type of installation. This does not apply to the I/O, Wiegand and tamper switch extending modules.

Module Power Supply

All the modules connected to the device, except for the Tamper Switch, are powered from the bus. The available bus power output depends on the power supply type.

Power Supply	Specification	Available power output
External supply	12 V ±15 % / 4 A DC	up to 48
PoE	PoE+ 802.3at	up to 21.6 W
Combined	External supply + PoE+	up to 69.6 W

Module Specifications

125 kHz RFID Card Reader Module

The 125 kHz RFID card reader module (91550941, 02140-001) is used for reading RFID card IDs in the 125 kHz bandwidth.

To accelerate access card reading, we recommend that the used card types are only selected in the module settings.

CAUTION
We recommend that the M-Bus and LAN cable are not crossed but carried separately through separate bushings to increase the reading distance of this reader & touch display installation.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 220 mm long interconnecting cable.

Supported RFID cards 125 kHz:

- EM4x02
- HID Prox

13.56 MHz, NFC RFID Card Reader Module

The 13.56 MHz RFID card reader (91550942, 02139-001) is used for reading RFID card IDs in the 13.56 kHz bandwidth.

To accelerate access card reading, we recommend that the used card types are only selected in the module settings.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 220 mm long interconnecting cable.

Supported RFID cards 13.56 MHz:

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

Secured 13.56 MHz NFC RFID Card Reader Module

The 13.56 MHz RFID card reader (91550942-S/9155086, 02141-001/01712-001) is used for reading secured RFID card IDs in the 13.56 MHz bandwidth.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 220 mm long interconnecting cable.

Supported RFID cards 13.56 MHz:

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

Biometric Fingerprint Reader Module

The Biometric fingerprint reader module (9155045, 01276-001) is used for verification of human fingers for access control and 2N/third party equipment control.

WARNING
The fingerprint reader may not be installed on places exposed to direct sunlight. If exposed to direct sunlight, the device may report errors.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 220 mm long interconnecting cable.

Important module properties:

- FBI PIV and Mobile ID certification – FAP20
- durable glass touch surface
- rejection of spoof fingerprints
- operating temperature range: −20 to 55 °C
- 0–90 % relative humidity, noncondensing

CAUTION

- A higher moisture may deteriorate the finger papillary line scanning. You are advised to dry your finger and the reader scanning surface for successful authentication.
- Fingerprint scanning may be more difficult for seniors whose finger papillary lines are not so distinctive (skin elasticity drops with age and a higher scanning pressure may lead to fingerprint blurring).

5-Button Module

The 5-Button module (9155035, 01258-001) is used for selected Automation functions. Refer to 2N.com for the printing template.

The buttons are backlit and can include nametags.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 220 mm long interconnecting cable.

Specification

Nametag dimensions (W x H)	• 1 button: 52.0 (W) x 15.2 (H) mm (dimensional tolerance: +0; −0.5 mm) • 5-button: 57.5 (W) x 89.0 (H) mm (dimensional tolerance: +0; −0.5 mm)

I/O Module

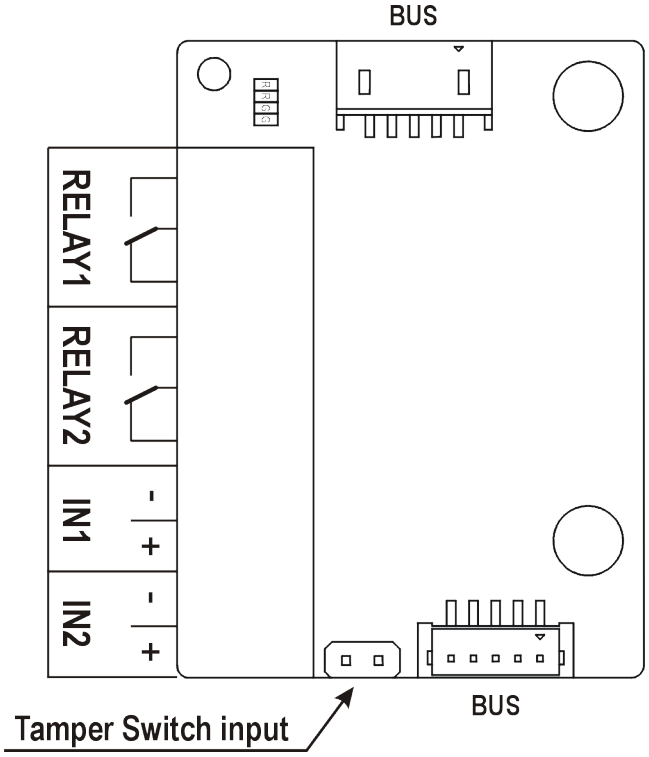
The I/O module (9155034, 01257-001) is used for extending the inputs and outputs.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.

- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 80 mm long interconnecting cable.
- The inputs / outputs are addressed as follows: <module_name>.<input/output_name>, e.g. “module5.relay1”. Configure the module name in the Module Name parameter in **Hardware > Extending modules**.

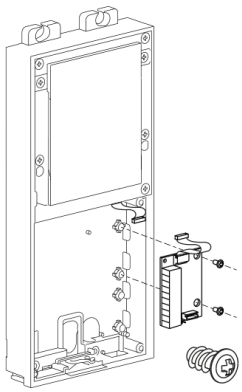
Connectors and Installation



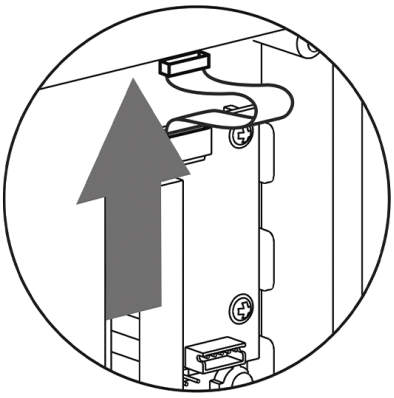
RELAY1/2	RELAY1/2 terminals with accessible 30 V / 1 A AC/DC NO/NC contact
IN1/2	IN1/2 terminals for input in passive / active mode (−30 V to +30 V DC) • OFF = open or U_{IN} > 1.5 V • ON = short-circuited or U_{IN} < 1.5 V
TAMPER	Tamper Switch (9155038, 01260-001) input

The module is installed under another module, i.e. needs no separate position.

1.



2.



Wiegand Module

The Wiegand module (9155037, 01259-001) is used for connecting an external Wiegand device (RFID card reader, fingerprint/biometric data scanner) and/or connecting **2N IP Style** to an external security exchange.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 80 mm long interconnecting cable.
- Configure the module name in the Module Name parameter in **Hardware > Extending modules**.
  - LED IN is addressed as follows: <module_name>.<input1>, e.g. “module2.input1”.
  - The Tamper input is addressed as follows: <module_name>.<tamper>, e.g. “module2.tamper”.
  - LED OUT (negated) is addressed as follows: <module_name>.<output1>, e.g. “module2.output1”.

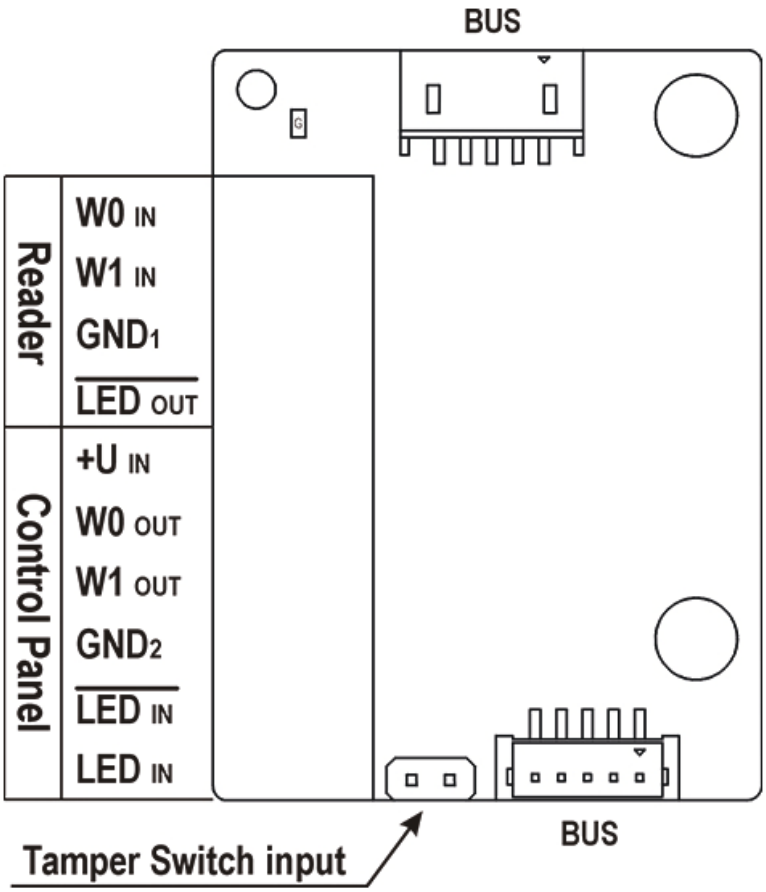
Specification

Technical Parameters of Wiegand Input

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

Connectors and Installation

All the inputs and outputs are galvanically isolated from the device with the insulation strength of 500 V DC. It is necessary to feed $+U_{IN}$ on Wiegand $W0_{OUT}$ from the Control Panel.



Reader helps connect an external Wiegand-supporting reader. The reader sends the device card ID.

The Control Panel is used for connection to the security PBX / access system to which the device sends the card ID information.

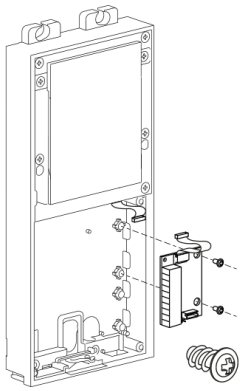
The module contains two BUS connectors for device bus connection. These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.

Reader	$W0_{IN}$, $W1_{IN}$, GND_1	Isolated 2-wire WIEGAND IN
	LED_{OUT}	Isolated open LED OUT switched against GND_1 (up to 24 V / 50 mA)

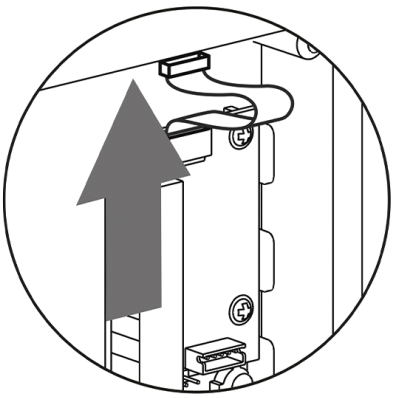
Control Panel	$+U_{IN}$	$+U_{IN}$ (5 to 15 V DC) for WIEGAND OUT power supply
	$W0_{OUT}$, $W1_{OUT}$, GND_2	Isolated 2-wire WIEGAND OUT
	LED_{IN} (negated)	Isolated input for open LED IN, input activated by GND_2 connection
	LED_{IN}	Isolated input for open LED IN, input activated after +U connection
	G	$+U_{IN}$ WIEGAND OUT active supply LED indicator
	TAMPER	Tamper Switch (9155038, 01260-001) input

The module is installed under another module, i.e. needs no separate position.

1.

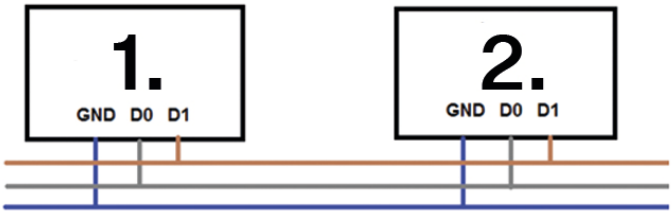


2.



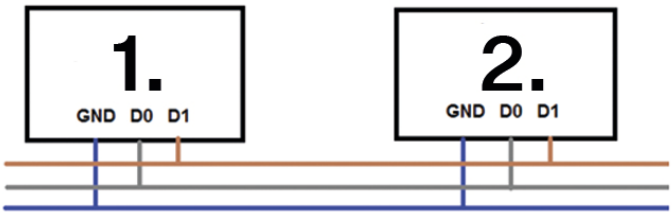
Recommended Wiegand bus wiring diagram, 2N device as a receiver.

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



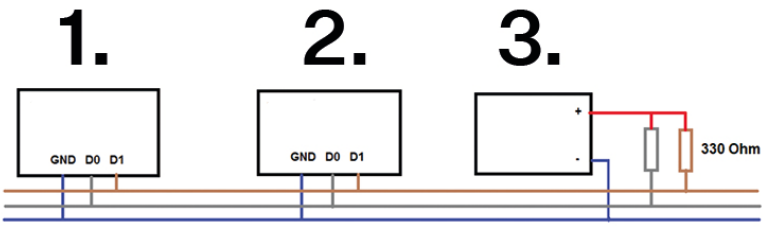
Recommended Wiegand bus wiring diagram, 2N device as a transmitter.

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



Recommended reader & OC output wiring diagram

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



Security Relay

The Security Relay (9159010, 01386-001) is used for enhancing security between **2N IP Style** 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.
	  • PoE: 10 V
	  • adapter: source voltage of minus 2 V
	• Where the Security Relay is fed from an external power supply, 12 V / 700 mA DC is available on the output.

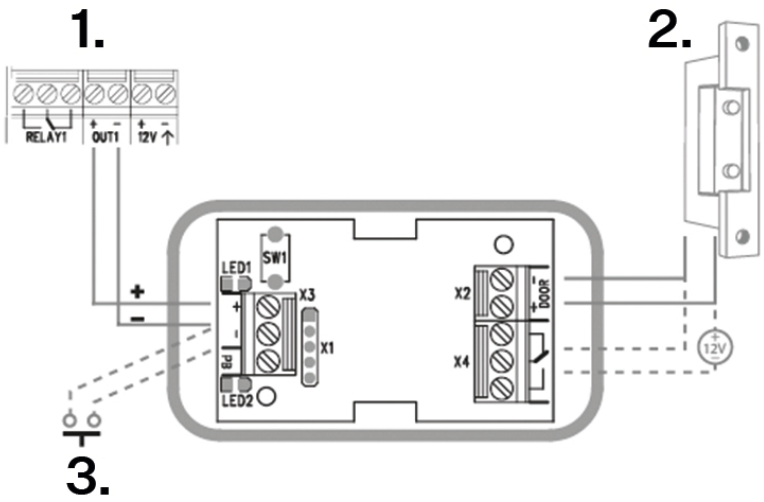
Dimensions	66.5 × 32.5 × 20.5 mm
Weight	24 g

Connectors and Installation

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

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

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



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

Connect the Security Relay to the access unit as follows:

- To the Active output

Connect the electric lock to the Security Relay as follows:

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

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

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

Status Signaling

Green LED	Red LED	State
flashing	off	Operational mode

Green LED	Red LED	State
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.

Tamper Switch Module

The Tamper Switch module (9155038, 01260-001) of **2N IP Style** is used for securing the system against unauthorized tampering.

The tamper switch module is designed to protect an external module connected via VBUS. The **2N IP Style** main unit has a tamper switch of its own.

CAUTION
Remember to purchase I/O Module (p. 43), OSDP Module (p. 53) or Wiegand Module (p. 45) along with the Tamper Switch.

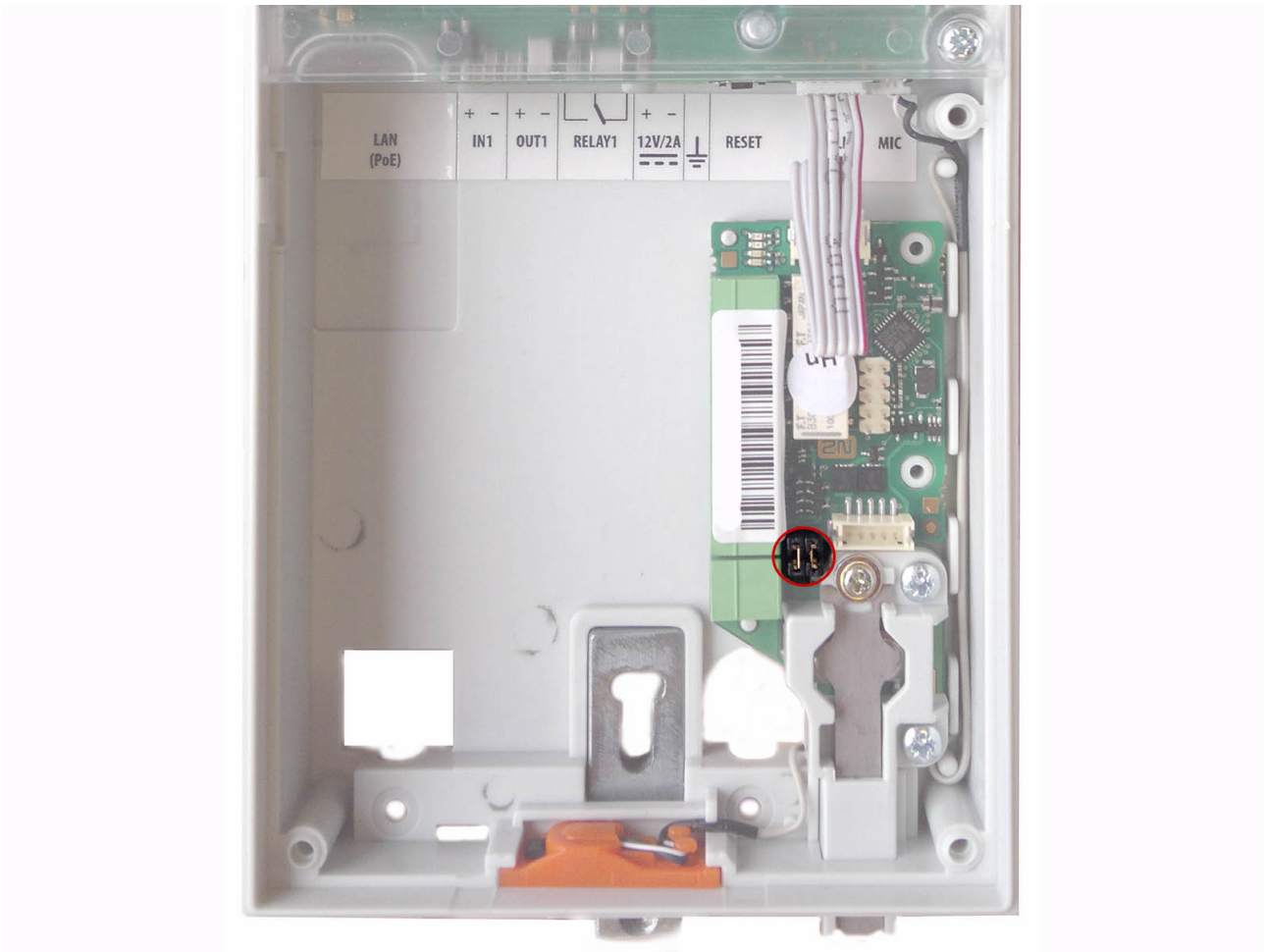
Features

The module contains two switches that open whenever the front frame is removed:

- One switch leads directly to the terminal board and is designed for connection to an external security exchange (32 V DC / 50 mA max).
- The other switch, in combination with the I/O module (p. 43), OSDP module (p. 53) or Wiegand module (p. 45), can be used for alarm triggering via the Automation interface in the **2N IP Style** configuration.

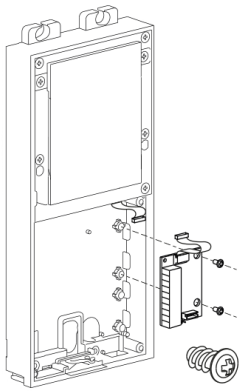
Connectors and Installation

This module is not connected to the bus.

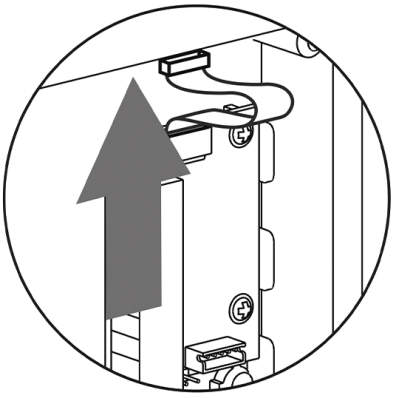


Jumpers are used for interconnecting the Tamper Switch pins with the I/O / OSDP / Wiegand module.

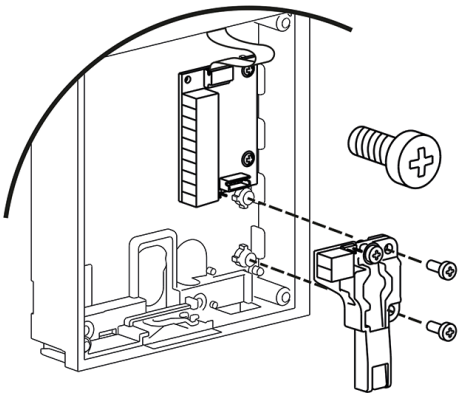
1.



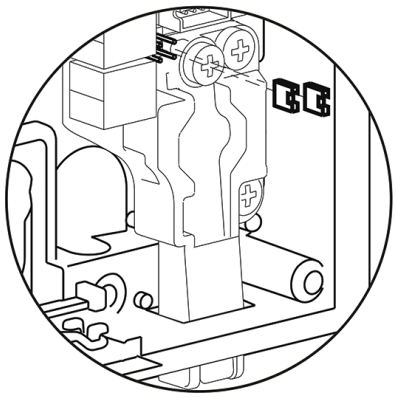
2.



3.



4.



OSDP Module

The OSDP module (91550371, 02577-001) of **2N IP Style** provides OSDP communication between a connected OSDP device (control panel, door controller) and the device. The OSDP module provides secure sending of such access data as the access card ID or PIN code.

Features

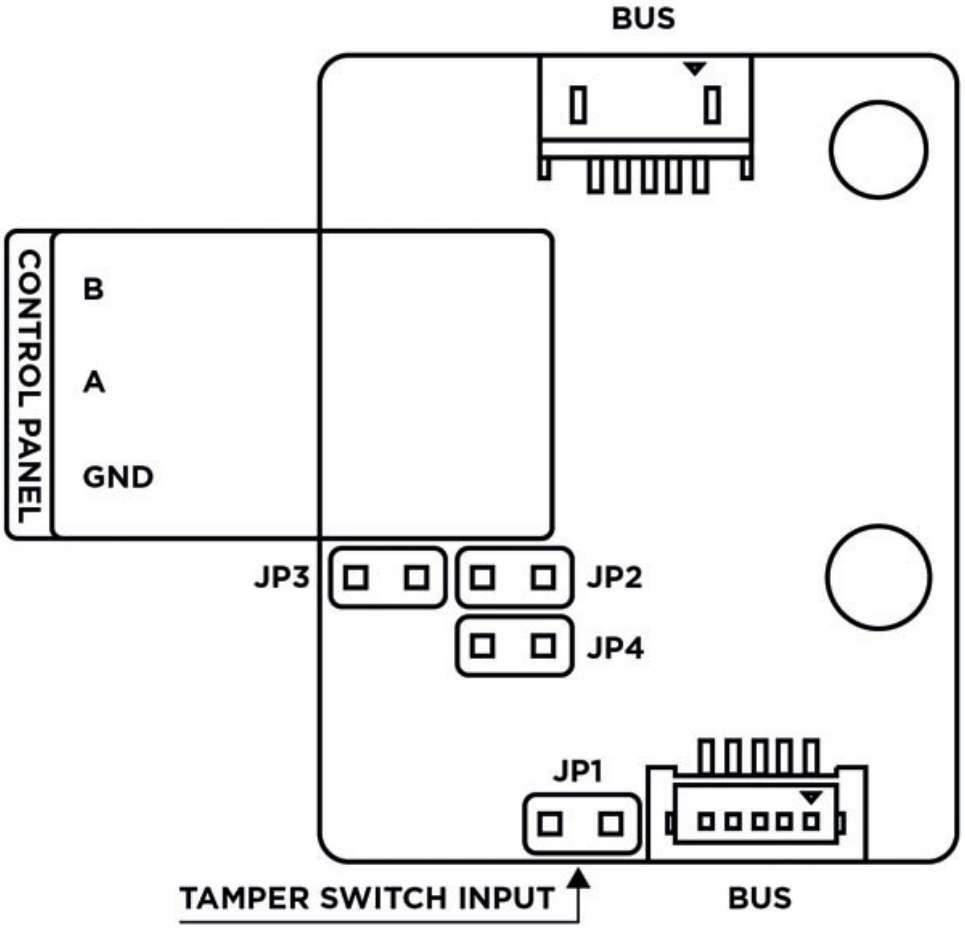
- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 80 mm long interconnecting cable.

The module also includes:

- Isolated OSDP bus
- Power and pairing mode signaling LED
- Tamper Switch (9155038, 01260-001) input

Connectors and Installation

All the inputs and outputs are galvanically isolated from **2N IP Style** with the insulation strength of 1500 V DC.



BUS	VBUS connectors for the bus connection
Control Panel: A, B GND	
JP1/2/3/4	Jumpers 1/2/3/4
TAMPER	Tamper Switch (9155038, 01260-001) input

The module is installed under another module, i.e. needs no separate position.

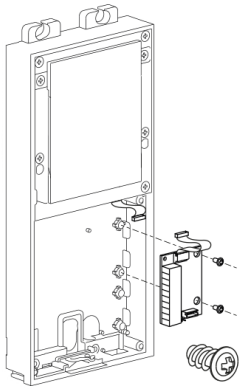
1. Having connected the OSDP module to **2N IP Style** via the VBUS, connect the OSDP device to the module. The OSDP module uses the RS-485 bus for the interface.

2. Connect the OSDP device as instructed (A to B or B to A) keeping the correct order to avoid malfunction.

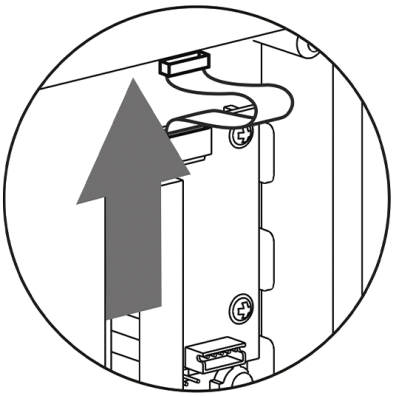
CAUTION

- Mounting jumpers JP2 and JP3 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 JP4 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.

1.

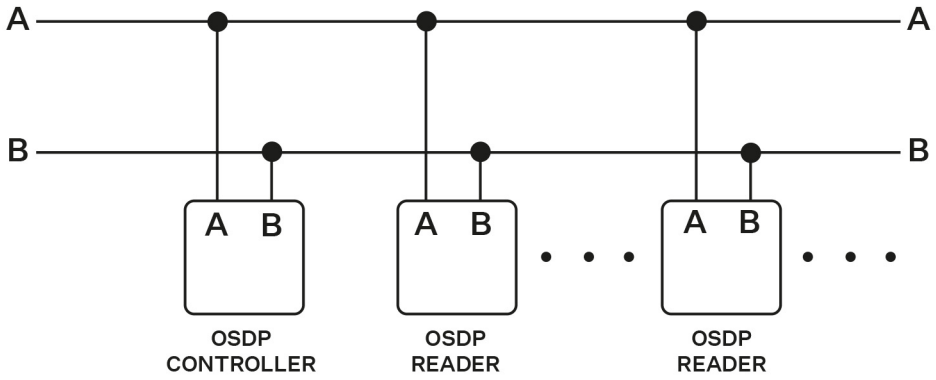


2.

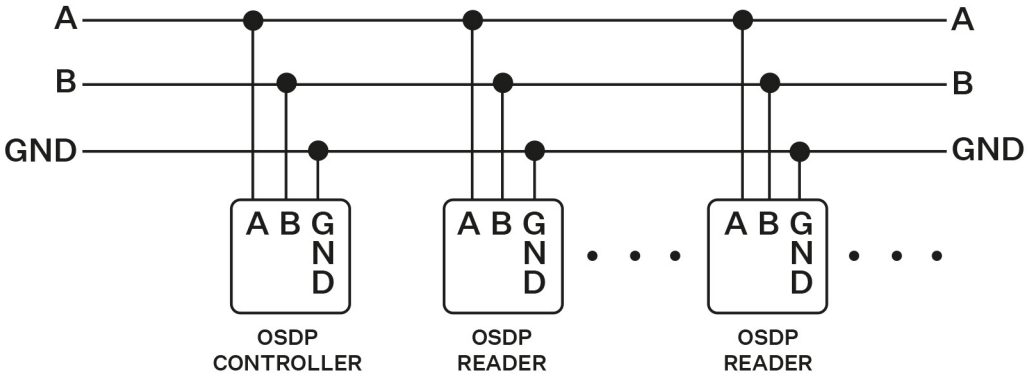


Connection Recommendations

Wiring diagram for two-wire connection



Wiring diagram for three-wire connection



Configuration

Having logged in to the device web interface, use the **Hardware > Extending modules** menu to set the following:

1. Name the module for user identification (optional).
2. Choose a group for access data resending, making sure that the settings are identical with those of the access readers from which the data are to be resent (card ID, PIN).
3. The setting of the codes to be transmitted is optional.
4. Enter the OSDP address between 0 and 126 to set the OSDP module address on the OSDP line.
5. Set the communication rate in accordance with the requirements of the device to be connected.
6. Enter your own encryption key into **2N IP Style** and the opponent's device to ensure encrypted communication.
7. Enable forced encryption just for encrypted communication.

Any unencrypted communication from the OSDP device will be rejected if forced encryption is enabled.

If the OSDP device enables remote encryption key setting on a peripheral, you can use the installation mode. Once the encryption key is received, the common mode is automatically switched on. The installation mode is signaled by a LED fast flashing on the OSDP module.

Induction Loop Module

The Induction Loop module (9155041, 01263-001) on **2N IP Style** is used for transmitting audio signals via the magnetic field directly into the hearing aids.

Features

- The module contains two bus connectors for the **2N IP Style** bus.
- These two connectors are fully interchangeable and can be used either as inputs from the main unit or outputs to other modules.
- If this module is the last one on the bus, one of the connectors remains unconnected.
- The module package includes a 220 mm long interconnecting cable.

Specification

Used mode	T
Maximum power	2 W
Frequency range	100 Hz – 5 kHz / ± 3 dB
Antenna output short circuit resistance	without restriction

Brief Guidelines

IP Address Retrieval

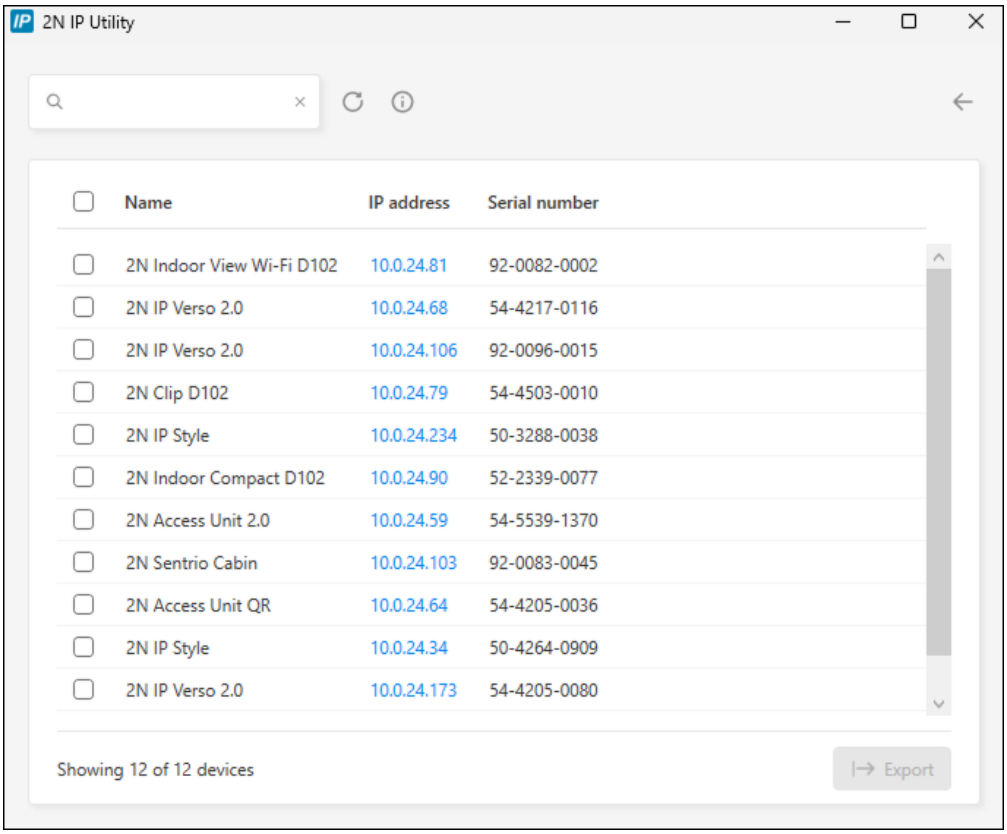
To retrieve the device IP address, take the following steps:

- Use the freely accessible 2N IP Utility.
- Display information on the device display.
- Use hardware (CONTROL 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.).

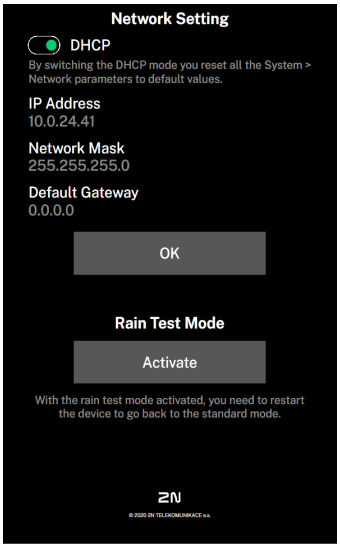
IP Address Retrieval with CONTROL Button

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 Device Display



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

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

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

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

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

Access to web device configuration

Configure **2N IP Style** 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

New firmware versions are available on the update server. If the web configuration interface does not provide access to the public Internet, it is possible to upload the firmware file manually to the device.

NOTE
Firmware updates are not automatic. To ensure system integrity and eliminate unintentional failures, all updates must be manually confirmed or initiated by the user. Please check the release notes of the new version and verify compatibility with your existing infrastructure before performing any updates.

Getting Firmware from Update Server

CAUTION
In version 3.0.0, firmware updates from the update server are only available from the older version of the web interface.

a. Click Go to the old interface in the web configuration interface header.

1. Go to **System > Maintenance > Firmware**.
2. Click Check for Updates.
3. If an update is available, its release notes are loaded. To start the upgrade, click Upgrade in the window header.
4. 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.

Uploading New Firmware from Storage

1. Go to **System > Maintenance > Firmware**.
2. Click Upload Firmware.
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.

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.

CAUTION
Do not touch the display during reboot, it is being calibrated.

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

The factory settings can be restored

- via the web configuration interface.
- Use hardware (CONTROL button).

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. 49).

Factory Default Reset via Web Configuration Interface

Soft reset the device factory default values in **System > Maintenance** using Default Reset.

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.

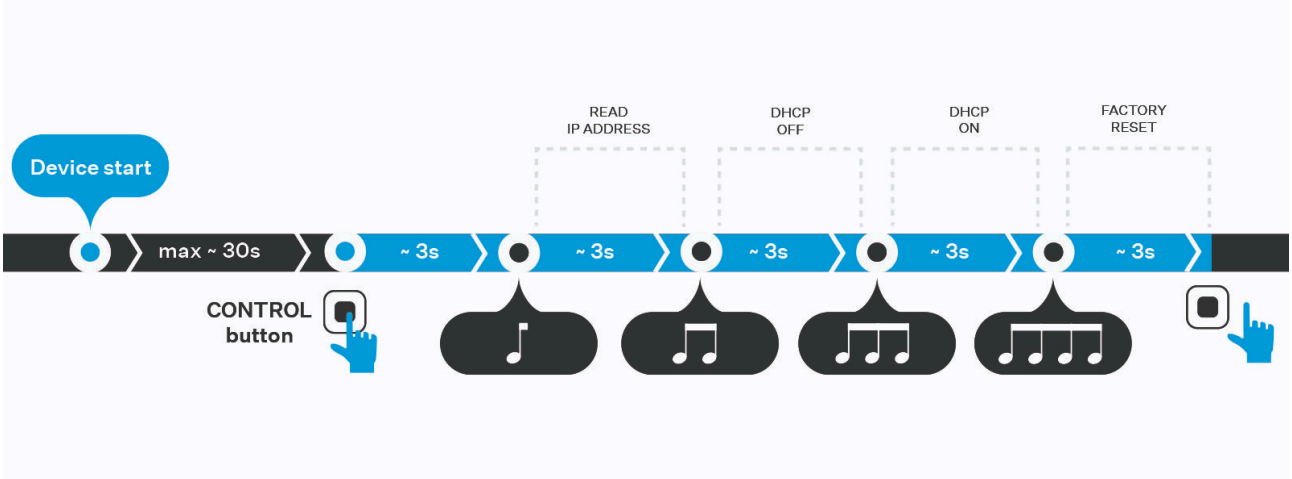
Release the button within 3 seconds after the appropriate tones are heard. If you release the button outside this time interval, the process will be interrupted and have to be repeated from the beginning.

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.

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 Control

2N IP Style is an intercom allowing you to:

- call other devices
  - use speed dial buttons
  - dial phone book position
  - 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 the **2N My2N** application – by pressing the device touchscreen in the vicinity of a mobile device with **2N My2N** logged in,
  - using NFC,
  - using a QR code
  - using biometric data (fingerprint)
  - by entering a numeric access code via a keypad , touch keypad or in the 2N My2N application
- control the device using a touch display
- activate/deactivate users or profiles using the **2N My2N** mobile application

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

Door Opening (Switch Activation) by RFID Card

2N IP Style is equipped with a door unlocking switch. To activate this switch, tap a valid card or chip on the integrated card reader. Remember to complete the user access card ID to get an RFID card / chip access.

1. Tap a valid RFID card / chip on the integrated card reader located in the bottom part of the device, whose symbol is backlit.
2. A valid RFID card / chip use is notified visually and by a continuous switch activation tone or a predefined unlocking user sound. An invalid RFID card / chip use is signaled acoustically or using a user sound.

Door Opening (Switch Activation) by Code

2N IP Style is equipped with a door unlocking switch. Enter the valid code using the touch numeric keypad to activate this switch.

1. Enter the switch activating numeric code using the touch numeric keypad and press the button for confirmation.

2. A valid code is notified visually and by a continuous switch activation tone or a predefined unlocking user sound. An invalid code entry or interruption of the entry for a period longer than as set in the device web configuration interface, is announced by an audible or a user-defined sound.

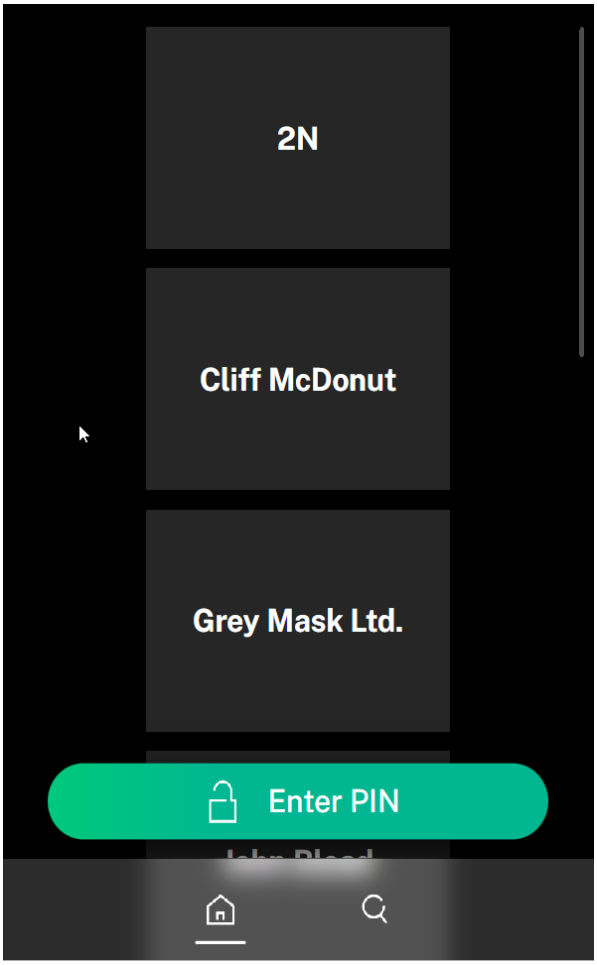
Door Opening (Switch Activation) by 2N My2N

2N IP Style is equipped with a door unlocking switch. Activate this switch using the 2N My2N authentication in your smartphone. The application is available for devices with iOS 12 and higher (iPhones 4s and higher) or Android 6.0 Marshmallow and higher (Bluetooth 4.0 Smart supporting phones).

1. The first step is different for different authorization modes:
   - **Touch mode** – press or drag from left to right on the display (depending on the Bluetooth authentication setting) to activate the switch.
   - **Tap in app mode** – unlock your smartphone, open the app and press the virtual button to activate the switch.
   - **Motion mode** – motion has to be detected by the device camera to activate the switch. Arrival in the proximity or waving of the hand will do.
   - **Card mode** – move your smartphone close to the integrated RFID card reader to activate the switch.
2. Switch activation is notified visually and by a continuous tone or a predefined user sound – unlocking. An invalid authentication is signaled acoustically or using a user sound.

Home Screen

The Home page displays the group / user name list to be called.



Use the icon to display a full-text array to retrieve contacts in the device directory. Also, the possibility to enter the access code via the touch numeric keypad is offered.

If configured so, the home page can provide the possibility to call user virtual numbers or get access via the 2N My2N mobile application under the icon .

The icon helps you return to the home page.

Blind Assistance Mode

The Blind Assistance Mode makes the **2N IP Style** intercom control accessible to users with visual impairments. With this feature, the users who have a problem with visual orientation on the display can locate the intercom and place their hand on the display to initiate a call to a preset contact.

Blind Assistance Mode Settings

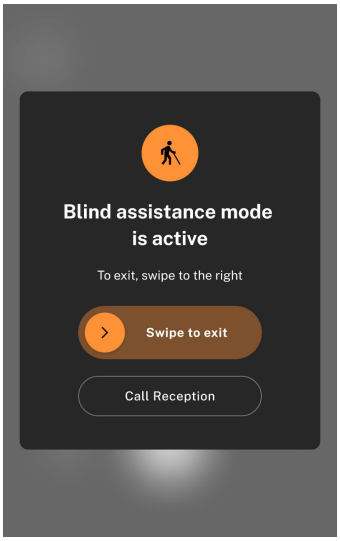
1. Open the **2N IP Style** web configuration interface.
2.
   CAUTION
   This setting is still done in the older version of the web configuration interface.

   Click Go to the old interface in the web configuration interface header.
3. Go to **Calling > Dialing > Blind Assistance Mode**.
4. Enable **Blind Assistance Mode**.

5. In the **Call button settings** block, select the user to whom the call will be set up in the Blind Assistance Mode. For example, the main contact should be the reception or another central service. You can also enter multiple users. The intercom will call them simultaneously.
   The intercom display will show the destination you set in **Contact Name on the display**. If you leave this parameter blank, the name of one of the selected contacts will be displayed.

Intercom Function in Blind Assistance Mode

The Blind Assistance Mode is activated whenever the intercom camera detects a person approaching the intercom head-on. The intercom camera must detect the person approaching the device for 15 seconds. This time can be changed in the web configuration interface.



In the Blind Assistance Mode, the intercom guides the user to the display by sound. The user is also audibly instructed to touch the display with the palm of their hand to set up a call to a preset contact. The message is played in the language set for the intercom display.

TIP
The message with instructions can be changed. To record a custom soundtrack, go to **Customization > User Sounds**.

The activated Blind Assistance Mode is visually indicated on the intercom display. Drag the option on the display to exit the mode.

Idle Mode

2N IP Style switches to the Sleep mode after an idle timeout (default value is 60 s). In the Idle mode, you can go to the Showcase mode to display a presentation or the company logo/address.

Touch any part of the display to cancel the Idle mode and display the Home page.

CAUTION
After a 2-minute idle timeout, the screensaver is activated, which alternately decreases and increases the display brightness in 20-second intervals. The screensaver is deactivated by a display touch, access attempt, incoming call, notification display or motion detection even in case the motion detection function is disabled. If the screensaver is running on the Showcase mode background, any display touch deactivates the screensaver and switches to the Home page.

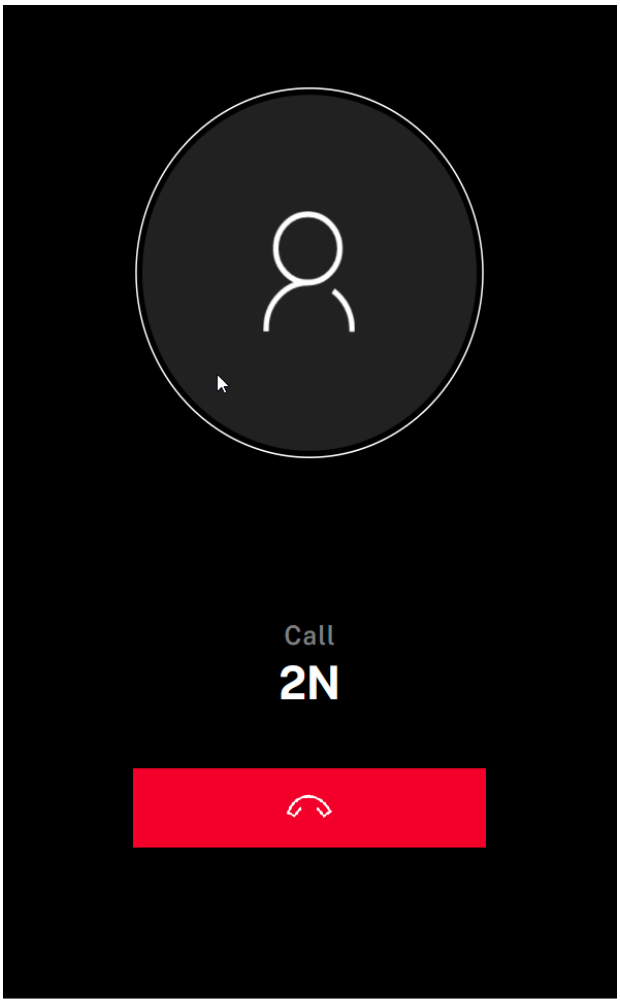
Calls

In this state, connection or connection attempt is in progress with another device. The **2N IP Style** functions are limited, it is impossible to switch to the home page and go to menus. Possible actions are included in the table below.

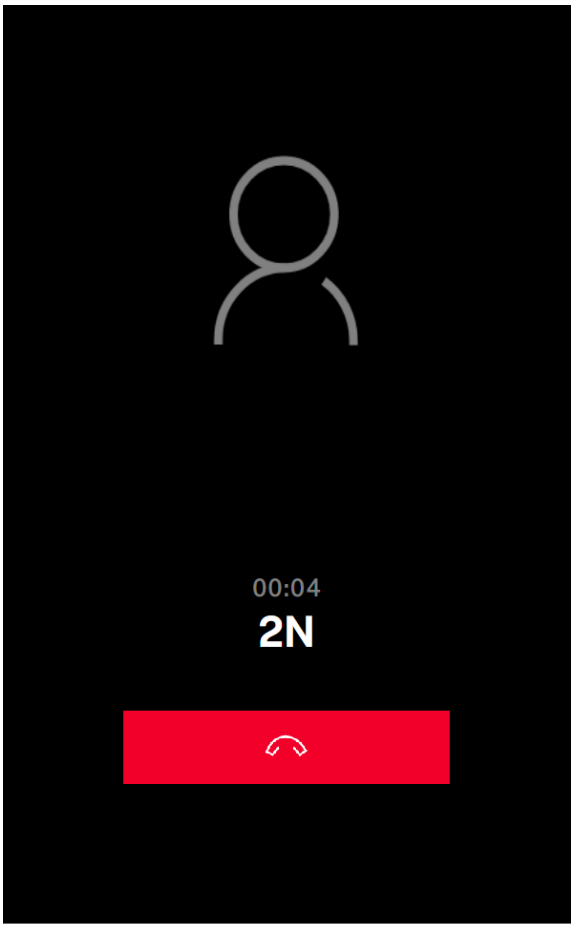
In this state, one of the following call types can be active in the device:

- **Outgoing call** initiated by the device
- **Incoming call** trying to establish connection with the **2N IP Style** device.
- **Active call**, if connection between the devices is established, sound is transmitted and camera preview if available is displayed.

Outgoing Call



Active Call



Possible actions	Performance	Action result
Incoming call receiving		Connection with the other device has been established, a call is in progress. The call can be ended without answering.
End of Call		The outgoing call is cancelled./The incoming call is rejected./The active call is interrupted. Home screen is displayed.
Outgoing Call Start	Press the selected user position in the phonebook or the user card.	The active call is interrupted.

Virtual Number Call

If the Calling Virtual Numbers parameter is set (refer to Calls > General Settings of the Configuration Manual for IP Intercoms), you can dial a user-defined phone number using the device numeric keypad.

1. Press the button.
2. Enter the phone number using the numeric keypad and repress the green button for confirmation.
3. Press the red button any time to end the call.

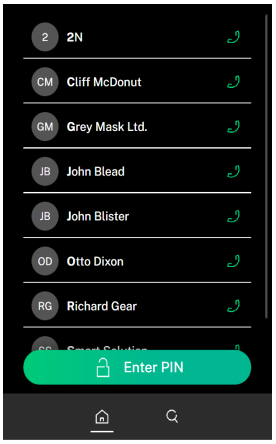
Directory Menu

A group / user name list is displayed in the Directory.

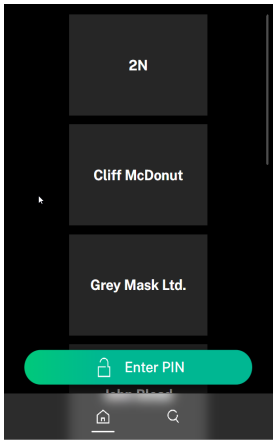
The Directory can contain up to 10 000 pre-programmed positions. The user groups are superior to the users, the list is arranged in the alphabetical order.

To set the display and order of contacts on the device display, go to **Calling > Dialing > Phonebook Display**.

Directory – List



Directory – Cards



Possible actions	Performance	Action result
Outgoing call setup	Press the selected user position on the list or the user card	An outgoing call is set up to the destination of the selected contact.
Movement in Group / User List	Touch the screen and move upwards / downwards	Thus, you move up / down in the group / user list on the screen.
Directory User Search	 Press and enter a few letters of the user name to be searched	A fulltext field looks up the user based on the user name letters. All options are displayed from the list that contain the searched string.

LED pictograms

Signaling LED pictograms may appear on the notification bar at the display upper edge. See the table below for the meanings of the pictograms:

Pictogram	Description
	Means that the area where the device is located is secure. To activate the area security, for example, assign it to a physical input, use HTTP API and so on.
	Means that the door unlocking switch is activated. Refer to Device Control (p. 66) for door opening options.

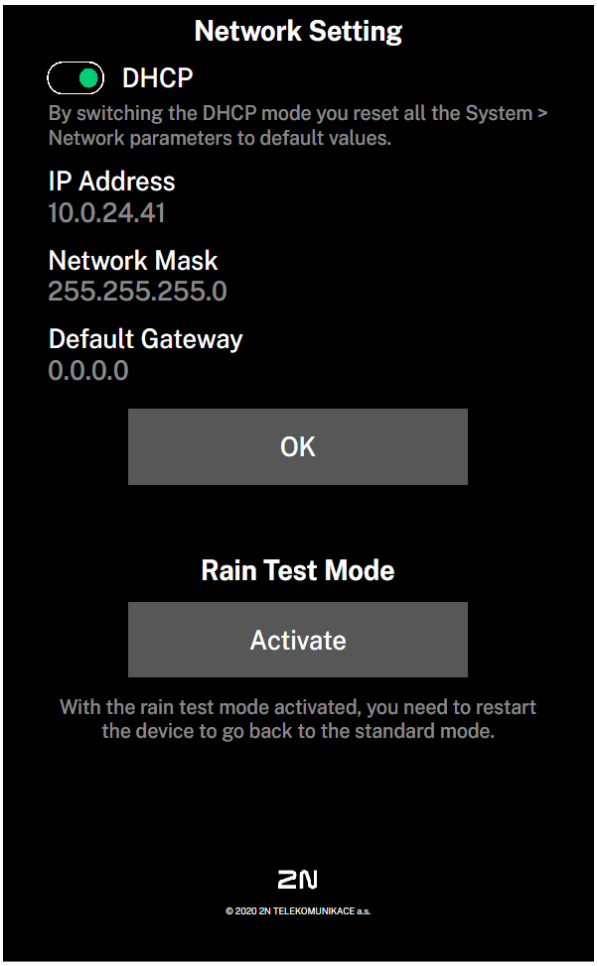
Rain Test Mode

The Rain test mode shows where water has been detected on the display. When the mode is activated, a black screen is displayed showing the water impact spots. Triple touch quickly any part of the display to delete the impact records.

The device does not support the intercom functions during the test (no calls, no card reading, etc.). It is necessary to restart the device to go from the Rain test mode back to the standard mode.

It is also necessary to start the Hidden menu to activate the rain test:

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



Colour Signalling

Devices with a display or LED pictograms display different statuses in color.

Status Signaling

Color	State	Description
Red	Active Access Blocking	Occurs if access is not allowed (it is not possible to activate the door switch) or occurs again after a specified period of time after the door switch is deactivated.
	Switch Locking	Applies to a switch that is configured as a door switch.
	Secured Status	Display of this status is only allowed on the device main unit if signaling is available.
Blue	Entering Access Code	Occurs when the user is entering the code and signals the possibility to confirm the code.
Green	Access Enable	Occurs when the access lock is deactivated and signals door opening or switch activation.

Maintenance - Cleaning

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

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

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

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

- Do not use aggressive and alcohol/peroxide based detergents.

TIP
To disinfect the surface of the device against bacteria and viruses (Anti-Covid) and maintain the hygienic conditions of critical surfaces and touch points, we recommend that you use the Zoono – Microbe Shield Surface Sanitiser spray.

Troubleshooting

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

Technical Parameters

Power supply types	
PoE	IEEE PoE+ 802.3at
External supply	12 V ±15 % / 4 A DC

Signaling protocol	
SIP	UDP, TCP, TLS

Audio	
Microphone	2 integrated
Amplifier	2 x 4 W (class D)
Speaker	2 x 4 W / 4 Ω
Sound pressure level (SPL max)	85 dB (for 1 kHz at 1 m)
LINE OUT	1 VRMS / 600 Ω
Volume Control	Adjustable with automatic adaptive mode
Full duplex	Yes (AEC)

Audio stream	
Protocols	• RTP • RTSP • SRTP

Audio stream	
Codecs and Used Bandwidth	• G.711 (PCMA, PCMU) – 64 kbps (with 85.6 kbps headers) • G.729 – 16 kbps (with 29.6 kbps headers) • G.722 – 64 (with 85.6 kbps headers) • L16/16kHz – 256 kbps (with 277.6 kbps headers)

Camera	
Sensor	1/2.7" color CMOS
JPEG resolution	Up to 2560 (H) x 1920 (V), (4:3); max. QHD (16:9)
Video resolution	2560 (H) x 1920 (V), (4:3); max. QHD (16:9)
Frame rate	30 fps
Sensor sensitivity	14000 V/lux-sec
Viewing angle	138° (H), 114° (V)
Infrared illumination	Yes
Sensor sensitivity without IR light	0.1 Lux ± 20 %
Focal length	1.7 mm

Video stream	
Protocols	• RTP • RTSP • SRTP • HTTP
ONVIF/RTSP streaming codecs	• H.264 • H.265 • MJPEG

Video stream	
IP Camera Function	Yes – compatible profiles: • ONVIF v2.4 profile S

Interface	
LAN	10/100BASE-TX with Auto-MDIX, RJ-45
Recommended cabling	Cat-5e or higher
Supported protocols	SIP2.0, SIPS, DHCP opt. 66, SMTP, SNMP, TR069, 802.1x, RTSP, RTP, SRTP, TFTP, HTTP, HTTPS, Syslog, ONVIF
Passive switch (relay)	NO/NC contact, up to 30 V / 1 A AC/DC
Active switch output	10 to 12 V / 600 mA DC
Passive / active input	−30 V to +30 V DC

Bluetooth	
Bluetooth	in compliance with BLE (Bluetooth Low Energy)
Range	Adjustable: • short ~ 2 m • long ~ up to 10 m
Support of mobile applications	Android 10.0 and higher, iOS 17.0 and higher

Touch Display	
Resolution	85 dB (for 1 kHz at 1 m)

Touch Display	
Contrast ratio	800 : 1
Brightness	85 dB (for 1 kHz at 1 m)
Viewing angle	85° from all directions
Numeric Keypad	numeric touch keypad,
Touch buttons	press the display
Directory	residential / business (for 10 000 users)

I/O module, Wiegand module	
Dimensions	43 x 31.5 x 1.5 mm

Mechanical Parameters	
Cover	Hardened glass
Body material	• Material - EN-AW6060 • Surface finish: body - RAL 7021 (dark grey variant), chassis - RAL 7043
Device dimensions	170.6 x 355.5 x 41.8 mm
Flush installation dimensions – overlapping part of the device	170 x 355 x 22 mm
Weight	1 950 g
Operating temperature	–30 °C to 60 °C
Relative humidity	10 to 95 % (non-condensing)

Mechanical Parameters	
Storing temperature	–30 °C to 70 °C
Protection class	IP65
Resistance level	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 Style conforms to the following directives and regulations:

EU

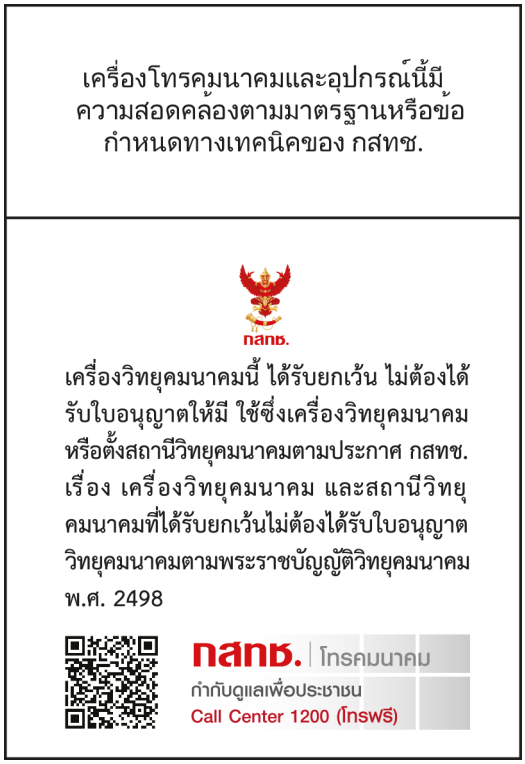
- 2012/19/EU on waste electrical and electronic equipment

- 2014/30/EU for electromagnetic compatibility
- 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.

Legislation of Thailand



Legislation of Japan

本製品は、特定無線設備の技術基準適合証明 を受けています。

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 Style – Installation Manual

2N.com