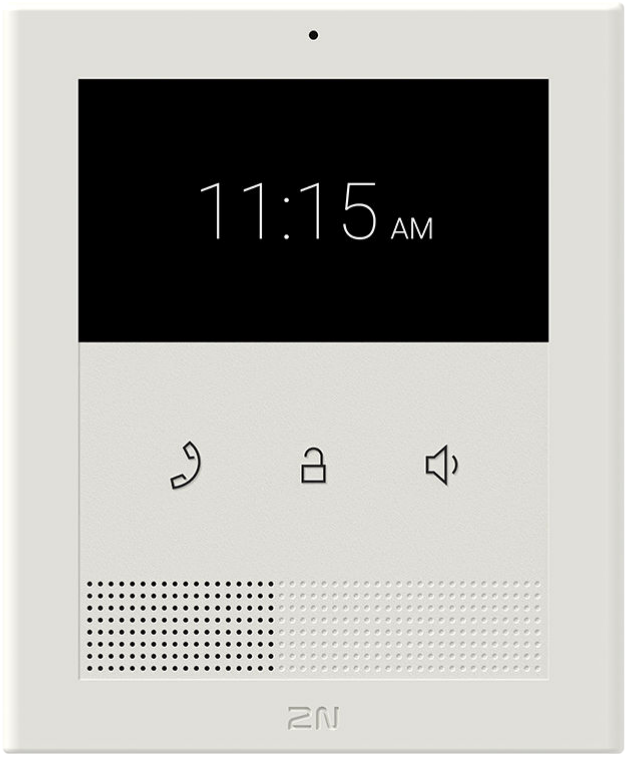
2N Clip 2wire-IP

User 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 Clip 2wire-IP** product, outline its application options and highlight the advantages following from its use.

Basic Features

2N Clip 2wire-IP is an internal IP/SIP unit providing communication with the 2N IP intercoms.

includes a control panel with three buttons, a loudspeaker, a high-quality microphone for excellent audibility and clarity, a 2-wire interface for connecting to the LAN, a power connector and a doorbell connector.

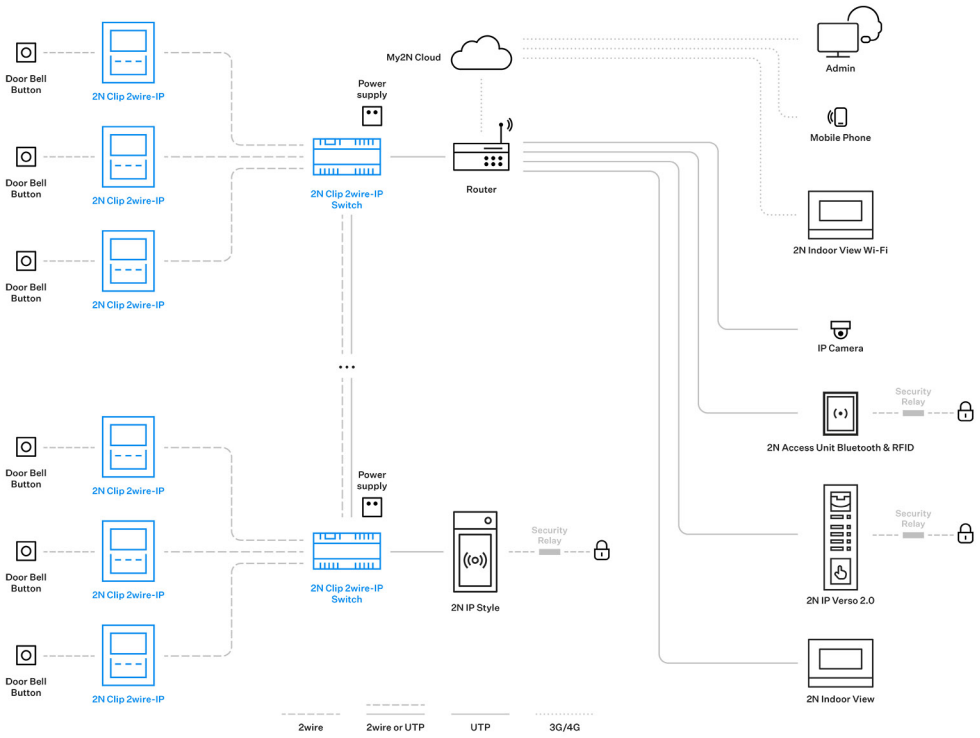
The device includes a control panel with three buttons, a loudspeaker, a high-quality microphone for excellent audibility and clarity, for connecting to the LAN, and connectors for connecting an external power supply and a doorbell connector.

2N Clip 2wire-IP is equipped with a specific user interface for an increased user comfort and safety.

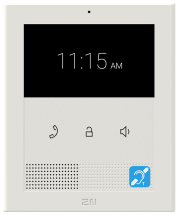
Basic Features **2N Clip 2wire-IP**:

- 2 mm thick plexiglass display
- LAN connection and power supply via a twisted pair cable
- remote administration and configuration via **2N Remote Configuration**
- device lock
- remote door lock control
- time display
- integrated administrator web interface
- integrated induction loop version option,
- external doorbell button input.

Complex solution connection diagram



Product Versions

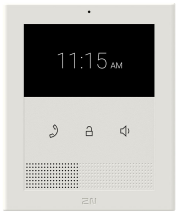


Part No.: 9138522

Axis Part No. 03449-001

2N Clip 2wire-IP

Version with induction loop



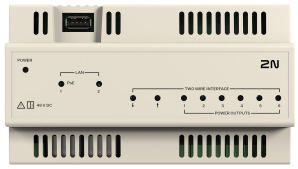
Part No.: 9138521

Axis Part No. 03448-001

2N Clip 2wire-IP

Version without induction loop

Switches



Order number: 9138001

Axis Part No. 03450-001

2N Clip 2wire-IP Switch

Switch with 2-wire interface for connecting up to 6 2N Clip 2Wire-IP units.

Power Supply

Part No. 1120302

Axis Part No. 03479-001

Power Supply for 2N Clip 2wire-IP Switch

Accessories for Installation

Choose the proper accessories for your particular installation needs.

Part No. 9138003

Axis Part No. 02906-001

Mounting holder

Single-Gang Box installation plate for **2N Clip 2wire-IP**.

US mounting metal holder for **2N Clip 2wire-IP**.

Part No. 9138002

Axis Part No. 02905-001

Desk Stand

Stand for **2N Clip 2wire-IP**.

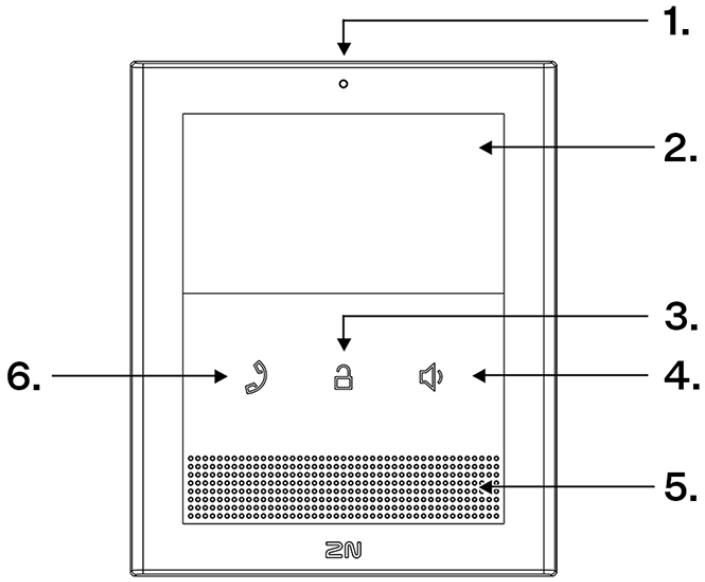
Package Completeness Check

Please check the product delivery before installation. Contents:

1x	**2N Clip 2wire-IP**
1x	Certificate of ownership
1x	Quick Start manual
1x	Metal holder
2x	3 x 12 mm self-tapping lens head screw for holder fitting
1x	Doorbell connection terminal (removable)
1x	Power supply and data transmission terminal (removable)
2x	Tactile sticker

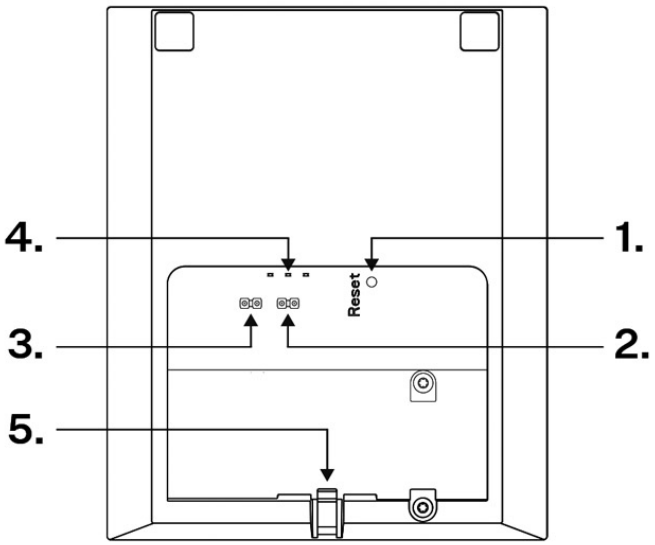
Component Layout

Front



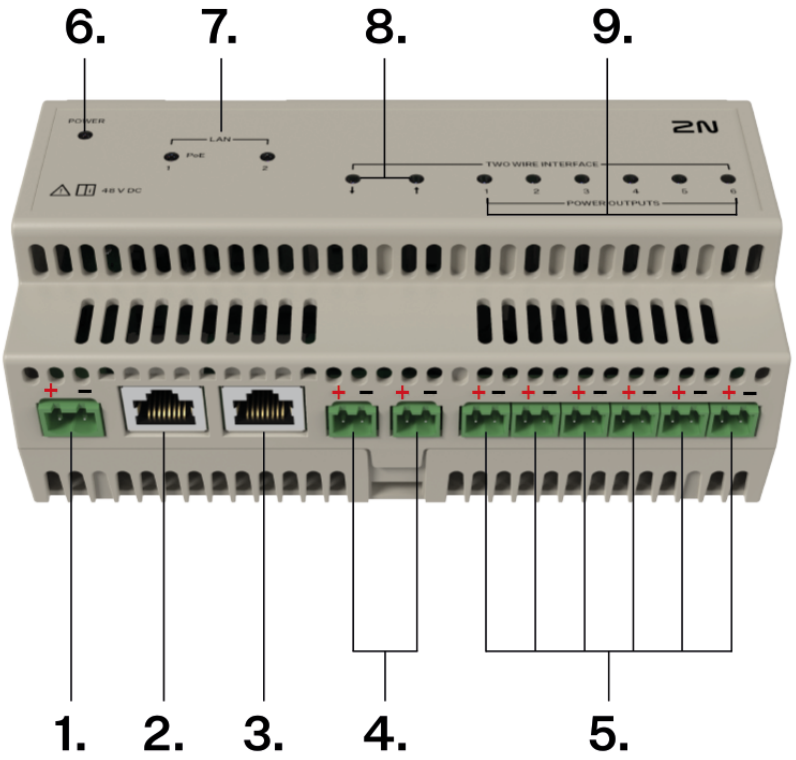
1. Microphone
2. Display
3. Lock button
4. Speaker button
5. Speaker
6. Earphone button

Rear



1. RESET Button
2. Doorbell Button Input
3. Power supply and data transmission input
4. Status LEDs
5. Locking Latch

Switch controls and LED



1.	Power connector		48 V DC / 1.92 A
2.	LAN connector with PoE function (IEEE 802.3af)	Function:	IP device connection floor interconnection via LAN
3.	LAN connector	Function:	IP device connection floor interconnection via LAN
4.	↓ 100 Mbps input/output Leader X ↑ 100 Mbps input/output Follower	Function:	Interconnection between floors with another 2N Clip 2wire-IP switch
5.	10Mbps output (POWER + DATA)	Function:	2N Clip 2wire-IP answering unit connection

6.	POWER	indicates the switch status	illuminated	function of the switch OK
			flashes once in 2 s	USB operations (update, read configuration, write statuses)
			flashes once in 200 ms	initialization or switch function error
7.	LAN	indicates network activity	illuminated	connected
			flashing	activity
			no light signaling	disconnected
8.	TWO WIRE INTERFACE	indicates floor interconnection	illuminated	connected
			flashing	activity
			no light signaling	disconnected
9.	POWER OUTPUTS	indicates IP device connection	illuminated	connected
			flashing	activity
			no light signaling	disconnected

NOTE
The USB connector is for service purposes only.

Mechanical Installation

This subsection provides the **2N Clip 2wire-IP** installation and connection instructions.

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

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

Installation Conditions

CAUTION
The device mounting and setting should only be performed by professionally qualified persons.

- 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. 70).
- Keep some free space above and below the device to allow air to flow and conduct heat away.
- No strong electromagnetic radiance is allowed on the installation site.
- The device is designed for vertical wall mounting (perpendicular to the floor) in the approximate height of 125 cm 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.

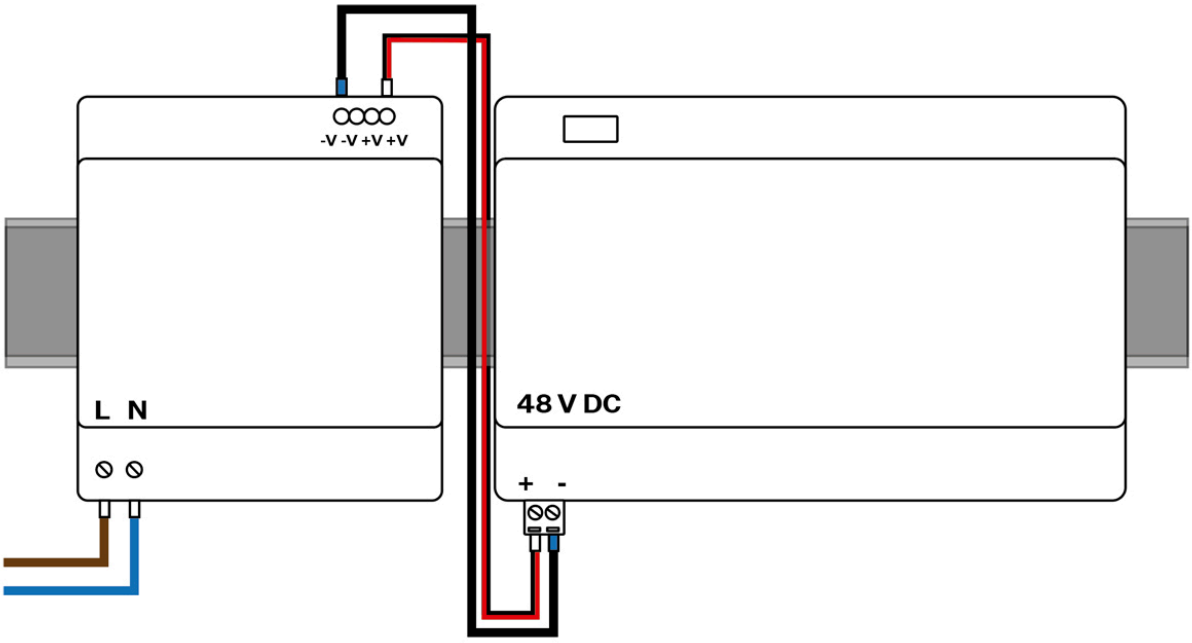
WARNING
This device must be deployed within a network infrastructure that provides adequate protection against Denial-of-Service (DoS) attacks and similar network-based threats. The device does not include built-in protection against high-volume or malicious traffic and relies on the surrounding network 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.

Switch Installation

The 2N Clip 2wire-IP switch enables an effective transition from an analog infrastructure to the IP technology using the existing twisted-pair cabling. It provides reliable network connectivity and high-speed data transfer. It supports connection of up to 6 2N Clip 2wire-IP units via a two-wire line. It is suitable for residential buildings, office buildings and commercial buildings where it is important to minimize the reconstruction cost and at the same time ensure modern functionality of the communication system.

The installation must be carried out by a qualified person or firm with electrical expertise to ensure safe operation.

1. Attach the 48 V DC / 1.92 A LPS (Limited Power Source) power supply and the 2N Clip 2wire-IP switch to the DIN rail of the switchboard.
2. Interconnect the switch with the power supply using the low voltage cable included in the switch package. Position the cables so that the correct polarity is maintained. To connect the cable to the switch, use the terminal fitted in the power connector, the cable to the power supply is connected directly.
3. Check the existing twisted pair wiring for a good condition to ensure a proper answering unit connection and operation.
4. Shorten the twisted pair cable to the desired length (the cable length from the switch to the unit should not exceed 100 meters).
5. Mount the terminal placed at the switch connector to the end of the twisted pair for connecting the 2N Clip 2wire-IP answering unit.
6. Connect the attached twisted pair cable to the switch.



Up to 6 2N Clip 2wire-IP units can be connected to the switch. The correct unit connection is indicated by a permanently lit LED located at the connector position.

CAUTION

- The power supply is intended exclusively for powering one switch. We do not recommend feeding other devices with the same power supply.
- Connection of a defective or improper power supply may lead to a temporary or permanent device failure.
- The length of the wire between the power supply and the switch must not exceed 3 m.
- Observe the polarity as marked on the switch and answering unit connectors.

LAN Connection

To provide a network connection from the main network (LAN), connect a UTP cable to any switch to the LAN connector.

In the case of floor interconnection via UTP cables, see below, it is preferable to use the first or last switch in the row to connect the main network. We recommend a connector without PoE (Power over Ethernet).

2N IP Intercom Connection

To connect an 2N IP intercom, we recommend using a LAN connector with PoE, which is primarily used for IP device connection and provides not only data connection but also power supply.

NOTE
In case more than one IP device need to be connected, an adapter can be used (Part No. 1120114). The adapter helps convert the UTP signal to a two-wire connection, allowing you to connect additional devices to the twisted-pair connector. It also provides power from the two-wire interface to the UTP side using the PoE standard.

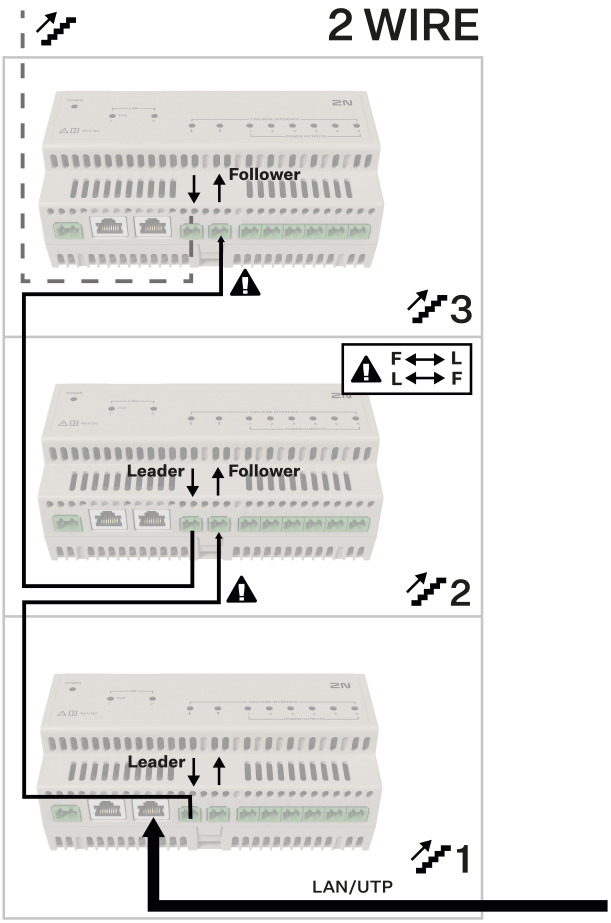
Floor Interconnection

To interconnect the floors, it is necessary to interconnect the switches with a twisted pair cable or UTP cable. Always observe the correct wiring.

CAUTION
The cable length between the switches should not exceed 10 meters.

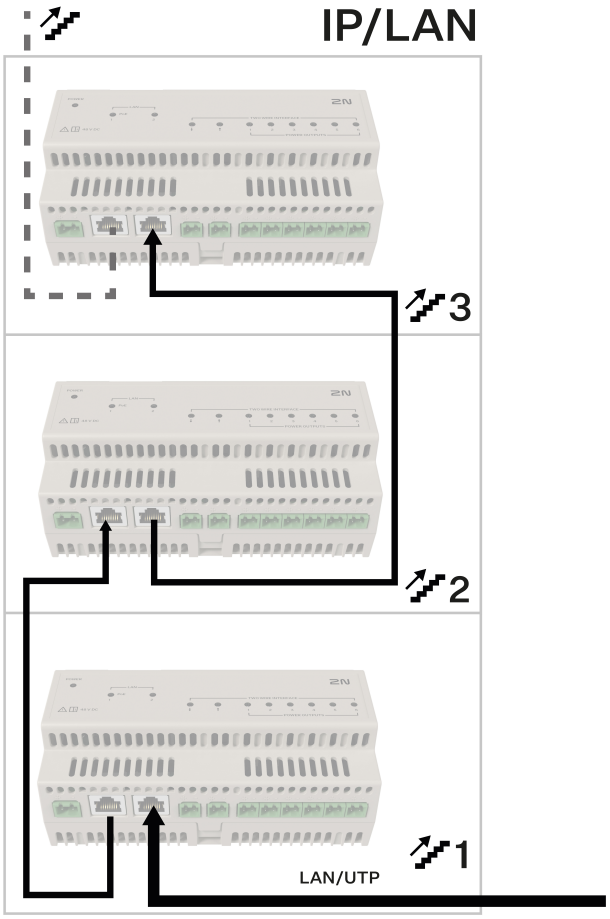
Via twisted pair cabling

Plug the cable into the ↓ Leader connector on the first switch in the row. Plug the other end into the ↑ Follower connector on the next switch. Repeat this procedure for all the switches in the row.



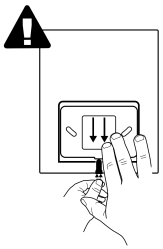
Via UTP cable

Plug the UTP cable into the LAN connector on the first switch in the row. Plug the other end into any LAN connector on the next switch. Repeat this procedure for all the switches in the row.



Wall Installation

WARNING
Having unpacked **2N Clip 2wire-IP**, remove the metal holder located on the device back side for installation. Use both your hands at the same time to remove the metal holder safely. A careless removal and insufficient push of the locking latch might lead to a locking latch damage. Follow the below mentioned removal instructions closely!



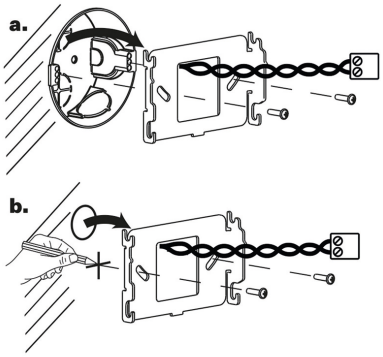
1. Push the locking latch in the center of the device bottom edge with your left hand in such a manner that it bends sufficiently for the metal holder removal. Do not push the locking latch from the top. You might get injured while removing the metal holder.
2. Grasp the metal holder with your right hand and slide it downwards for removal.

2N Clip 2wire-IP is installed directly on the wall using a metal holder or onto a pre-prepared mounting box. The metal holder on the device backside is compatible with the electrical mounting boxes with a fitting hole pitch of 60 mm. A US metal holder is available for installations compatible with single-gang boxes.

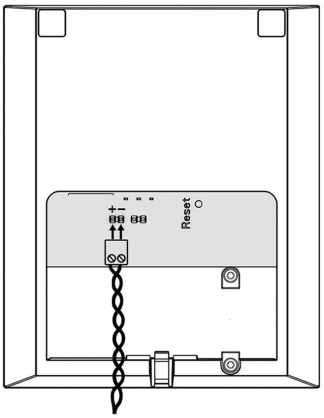
The recommended installation height is 135 cm from the ground. The installation heights may vary depending on the device use.

TIP
Download the Drilling template from 2N.com.

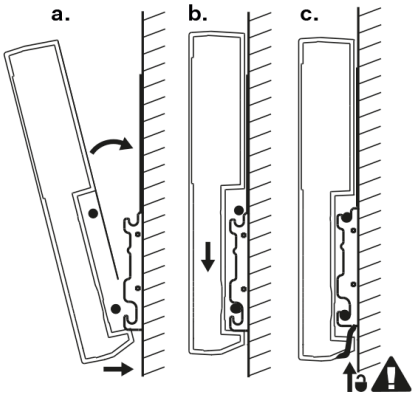
1.



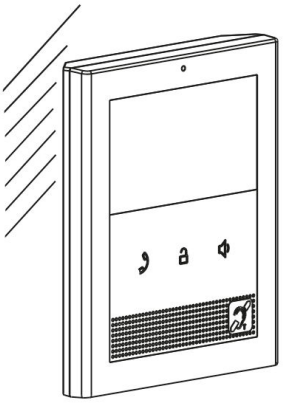
2.



3.



4.



1. Pull the twisted twin cable terminal leading from the wall through the metal holder. Make sure that it is correctly oriented for connection to the device after installation.

   TIP
   Make sure that the proper orientation is maintained during the holder wall installation. To do this, mark the bulge profile on the holder bottom side.

   Remove the cover from the wall-mounted installation box. Take out the pre-prepared cabling, the twisted pair cables, the bell wire.
2. Connect the twisted pair cable to the device.

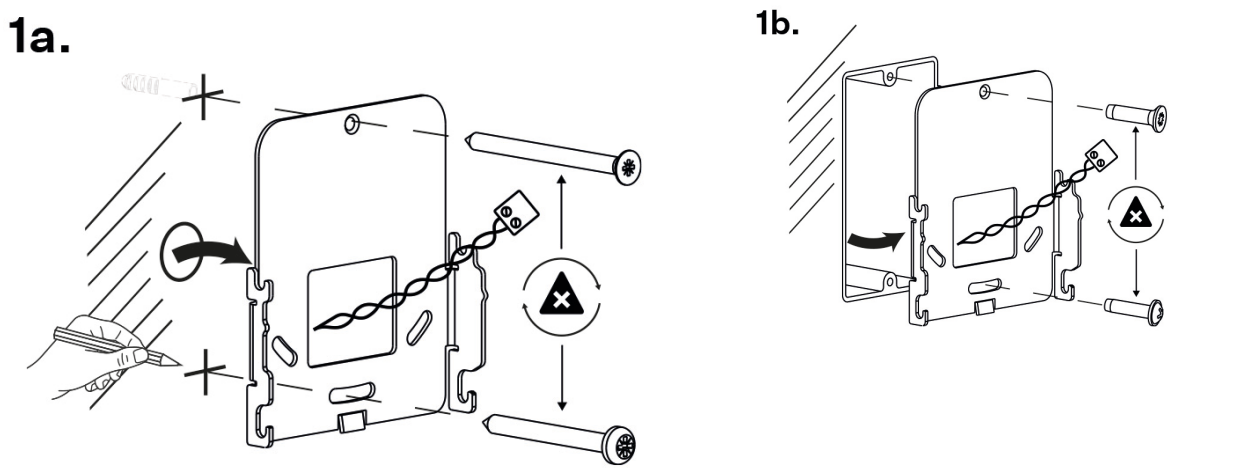
3. **a.** Put the device under the holder with its bottom edge first. Then put the device vertically on the wall keeping the device bottom edge under the holder.
   b. Slide the device gently downwards along the wall.
   c. Once the locking latch clicks, the device is properly mounted.
4. Now the device is ready for basic operation. It is necessary to perform software configuration (p. 31) to achieve a full functionality of the device.

Single-Gang Box Mounting

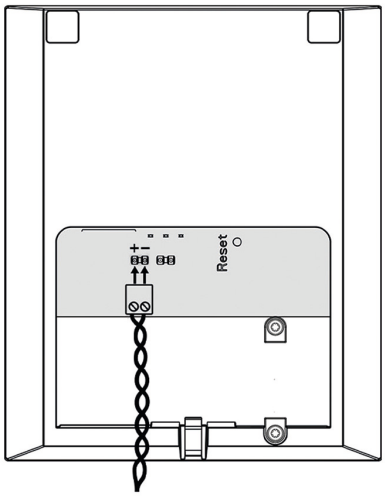
You are advised to use a metal holder (not included in the package) for **2N Clip 2wire-IP** installation in the USA. With the aid of this holder, the device can be installed into universal US single-gang mounting boxes. The device can also be installed directly on a wall without a mounting box.

The recommended installation height is 135 cm from the ground. The installation heights may vary depending on the device use.

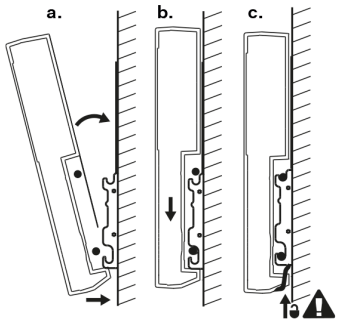
TIP
Download the Drilling template from 2N.com.



2.



3.



1. Draw the the twisted pair cable fitted with a terminal leading from the wall through the metal holder. Make sure that it is properly oriented for connection to the device after installation. If necessary, align the holder using a level and drill it into the mounting box or on the wall. The wall mounting screws are not part of the delivery, the included screws are only for the device installation into a mounting box.

   CAUTION
   During holder installation, it is **necessary** to pay attention to the location of the screws fitting the metal holder to the wall/mounting box. Use a flat head screw for the holder top round hole and a raised head screw for the bottom longitudinal opening. A confusion of the screws might lead to the device damage.

2. Connect the the twisted pair terminal to the device.
3. **a.** Put the device under the holder with its bottom edge first. Then put the device vertically on the wall keeping the device bottom edge under the holder.
   b. Slide the device gently downwards along the wall.
   c. Once the locking latch clicks, the device is properly mounted.
4. Now the device is attached properly. There is a slight distance between the device and the wall due to a rather big size of the metal holder, which is fully compliant with the installation conditions.
   Now the device is ready for basic operation. It is necessary to perform software configuration (p. 31) to achieve a full functionality of the device.

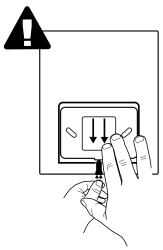
Stand Installation

Alternatively, the device can be installed into a stand placed on a desk, for example. The stand is not included in the package.

As part of the installation preparation, take out the pre-prepared cabling, the twisted pair cable, the bell wire. Shorten the cables to the required length. Connect the bell wire to the connector together with the the twisted pair cable for power and data transmission.

WARNING

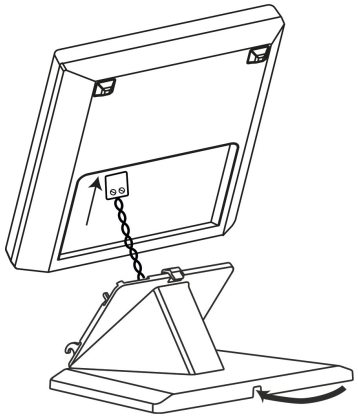
Having unpacked **2N Clip 2wire-IP**, remove the metal holder located on the device back side for installation. Use both your hands at the same time to remove the metal holder safely. A careless removal and insufficient push of the locking latch might lead to a locking latch damage. Follow the below mentioned removal instructions closely!



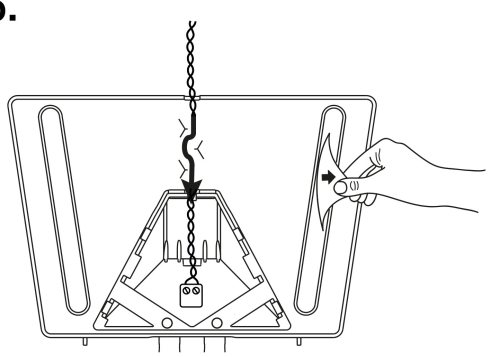
a. Push the locking latch in the center of the device bottom edge with your left hand in such a manner that it bends sufficiently for the metal holder removal. Do not push the locking latch from the top. You might get injured while removing the metal holder.

b. Grasp the metal holder with your right hand and slide it downwards for removal.

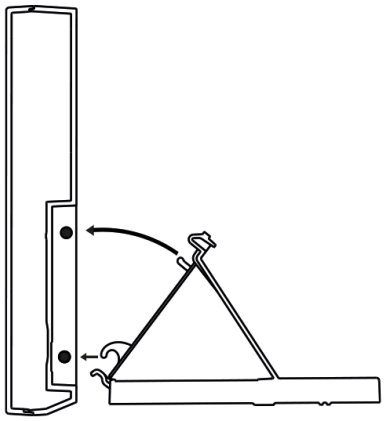
1a.



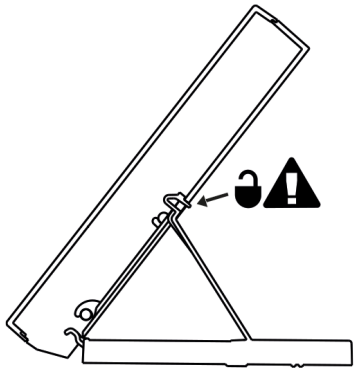
1b.



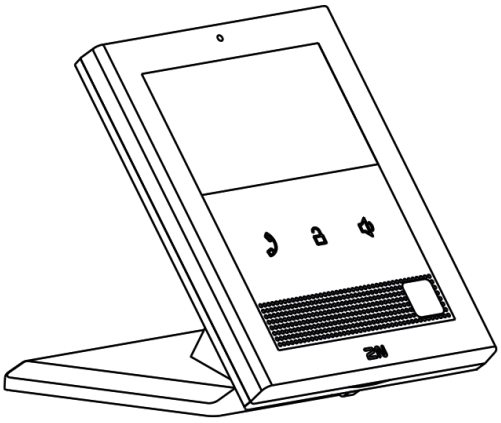
2a.



2b.



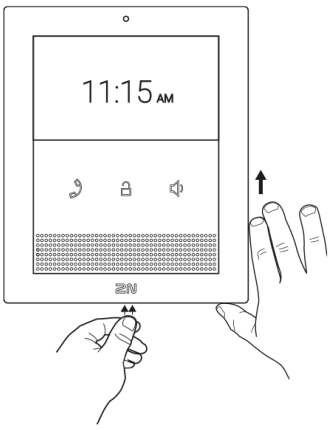
3.



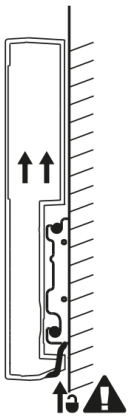
1. Pull the prepared the twisted pair cable fitted with a terminal through the bottom of the stand and connect it on the DATA&SUPPLY input. Place the cable in the groove in the middle of the stand base. Remove the protective film from the non-slip surfaces of the stand.
2. Put the stand including the properly drawn and connected cable on the device. First snap in the stand hooks, then tilt the stand towards the device and lock the latches on the stand top edge into the device body.
3. Now the device is ready for basic operation. It is necessary to perform software configuration (p. 31) to achieve a full functionality of the device.

Device Removal

1.



2.



1. Press the locking latch located in the center of the device back bottom edge. Pull the device gently upwards to release it from the metal holder/stand.
2. Remove the device from the hooks and take it away safely.

Power Supply

2N Clip 2wire-IP is powered from the switch via a two-wire bus (2wire-IP). Each switch is fed by an external power supply.

Supply type
2N 2wire-IP bus, 48 V DC nominal

Technical Parameters

WARNING

- We recommend securing each power supply in the installation with its own circuit breaker. If multiple power supplies are connected to a single circuit breaker, we recommend purchasing a Mean Well ICL-16R inrush current limiting module in the free market.
- 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.

Tactile stickers

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

We recommend placing the sticker next to the incoming call receiving button.

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

Brief Guidelines

Device Configuration Interface Access

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

Domain Name

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

Default domain name 2N Clip 2wire-IP: Clip 2wire-IP-{serial number without dashes}.local (e.g.: “Clip 2wire-IP-0000000001.local”)

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

IP address

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

- Use the freely accessible **2N Network Scanner**.
- Display information on the device display.
- Use hardware (RESET button).

Web Configuration Interface Login

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

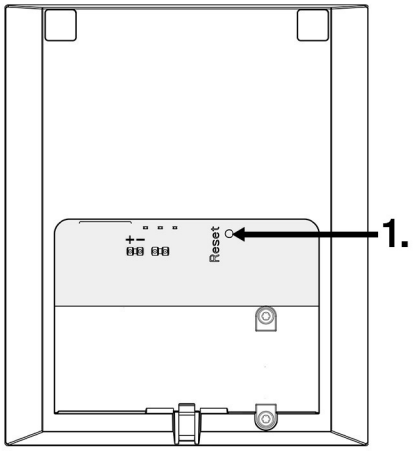
TIP
It is recommended that a password is used that is difficult to break. It is not recommended that names, places or things, especially those closely related to the user, are used in the password.

For increased password security, it is recommended that:

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

Configuration via Hardware

Where software configuration is unavailable, make basic settings using the RESET button (refer to 1.).



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

Device Restart

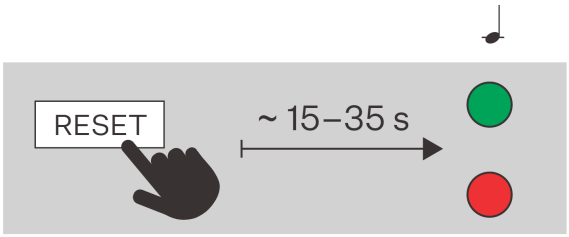
Press the button shortly (< 1 s) to restart the system without changing configuration.

IP Address Retrieval Using Hardware

Follow the instructions below to retrieve the current IP address:

1. Press the button RESET and keep it pressed.
   a. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
2. Release the RESET button.

3. The device announces the current IP address via the speaker automatically.

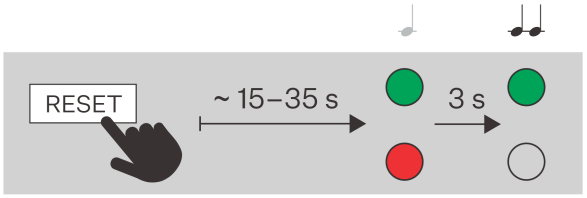


NOTE
The delay after pressing RESET till the first light and sound signaling is set to 15–35 s depending on the device model used.

Dynamic/Static IP Address Switching

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

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



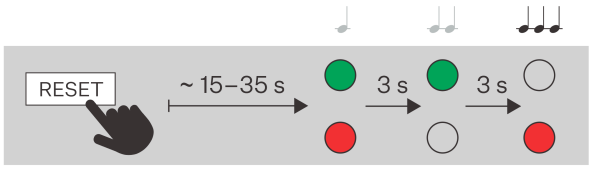
NOTE
The following network parameters will be set after restart:

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

Dynamic IP Address Setting

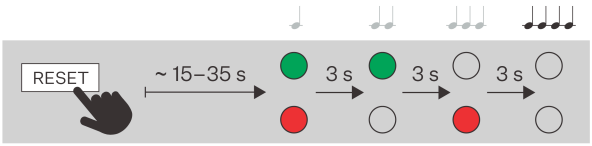
Follow the instructions below to switch on the Static IP address mode (DCHP ON):

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



Factory Default Reset

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



IP Address Retrieval

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

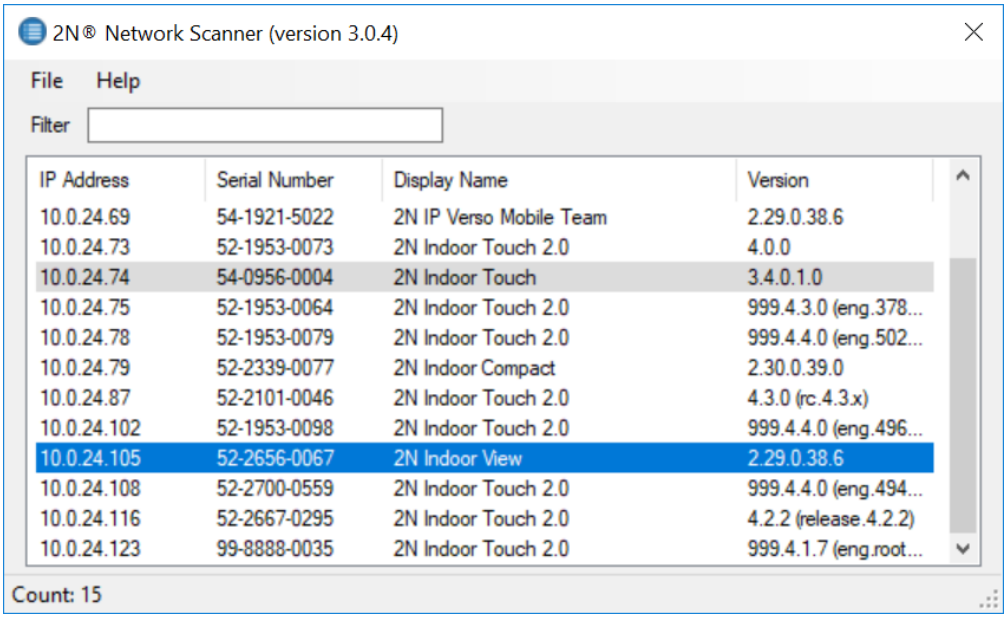
- Use the freely accessible **2N Network Scanner**.
- Display information on the device display.
- Use hardware (RESET button).

IP Address Retrieval Using 2N Network Scanner

The application helps you find the IP addresses of all the 2N devices in the LAN. Download **2N Network Scanner** from the 2N.com website. Make sure that Microsoft .NET Framework 2.0 is installed for successful app installation.

1. Run the **2N Network Scanner** installer.
2. The Installation Wizard will help you with the installation.

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



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

CAUTION
If the found device is grey highlighted, its IP address cannot be configured using this application. In that case, click Refresh to find the device again and check whether multicast is enabled in your network.

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

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

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

For increased password security, it is recommended that:

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

IP Address Retrieval using Device Display

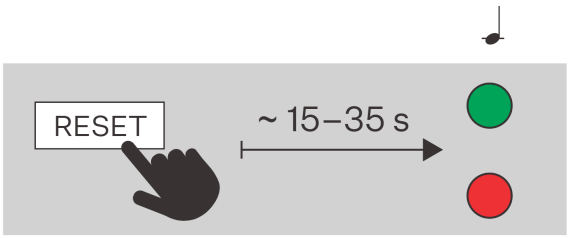
Follow the instructions provided in Subs. IP Address Retrieval Using **2N Network Scanner** (p. 26) to retrieve the **2N Clip 2wire-IP** IP address using **2N Network Scanner**.

To find the device IP address on the device, click any button to quit the Idle mode. The Settings menu (p. 61) is displayed on the Home screen after a long press of the earpiece and speaker buttons. Find the IP address information in About device.

IP Address Retrieval Using Hardware

Follow the instructions below to retrieve the current IP address:

1. Press the button RESET and keep it pressed.
   a. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard (approx. 15–35 s).
2. Release the RESET button.
3. The device announces the current IP address via the speaker automatically.



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

Firmware Update

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

Refer to Subs. Maintenance (p. 53) for firmware upgrade details.

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

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

Device Restart

To restart the device choose one of the following options:

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

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

Restart Using Device Buttons

Press the and buttons on the device simultaneously for a long time to display the Settings menu. Click to select Device administration > Device restart (press for confirmation). Press again to complete the restart. The device is then restarted.

The Home screen (p. 58) is displayed after restart. Restarting may take a rather long time after the button press.

Restart Using RESET Button

Find the RESET button on the device backside (p. 7).

The Home screen (p. 58) is displayed after restart. Restarting may take a rather long time after the button press.

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

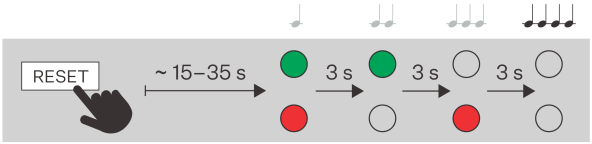
Restart Using Web Configuration Interface,

You can restart the device via the web configuration interface. Refer to Web Configuration Interface Login (p. 23) for login details. Restart the device in System > > System using Restart.

The Home screen (p. 58) is displayed after restart. Restarting may take a rather long time after the button press.

Factory Default Reset

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



Call Connection

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

Connection with 2N Devices in LAN

1. Make sure that Local Calls (p. 38) is enabled on both the 2N devices.
2. Click Find device above the table. Check the listed device that you want to establish connection to. Once the device is added, editing becomes available.
3. Edit the following:
   - starting a call with the contact by a long/short press of the call button
   - a virtual number to start a call by entering the number via your numerical keypad
   - basic information
4. Make sure that Local Calls (p. 38) is enabled on the called 2N device to make a successful call.

Connection with Other Devices

1. Click or open the existing contact detail to create a new contact.
2. Click the pencil icon next to the Phone number to open phone number editing.
3. Enter the calling destination address into the destination field to which the call is to be routed. Complete the target IP address or SIP URI in the format “ user_name@host” (e.g.: “johana@2.255.4.255” or “johana@calls.2N.com”). For local calls, fill in the called 2N device ID as specified in the Local Calls (p. 38) tab in the called device web configuration interface.
4. Edit the following:
   - starting a call with the contact by a long/short press of the call button
   - a virtual number to start a call by entering the number via your numerical keypad
   - basic information
5. Make sure that the call transmitting service is enabled on the called 2N device to make a successful call.

Web configuration interface

Basic Orientation

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

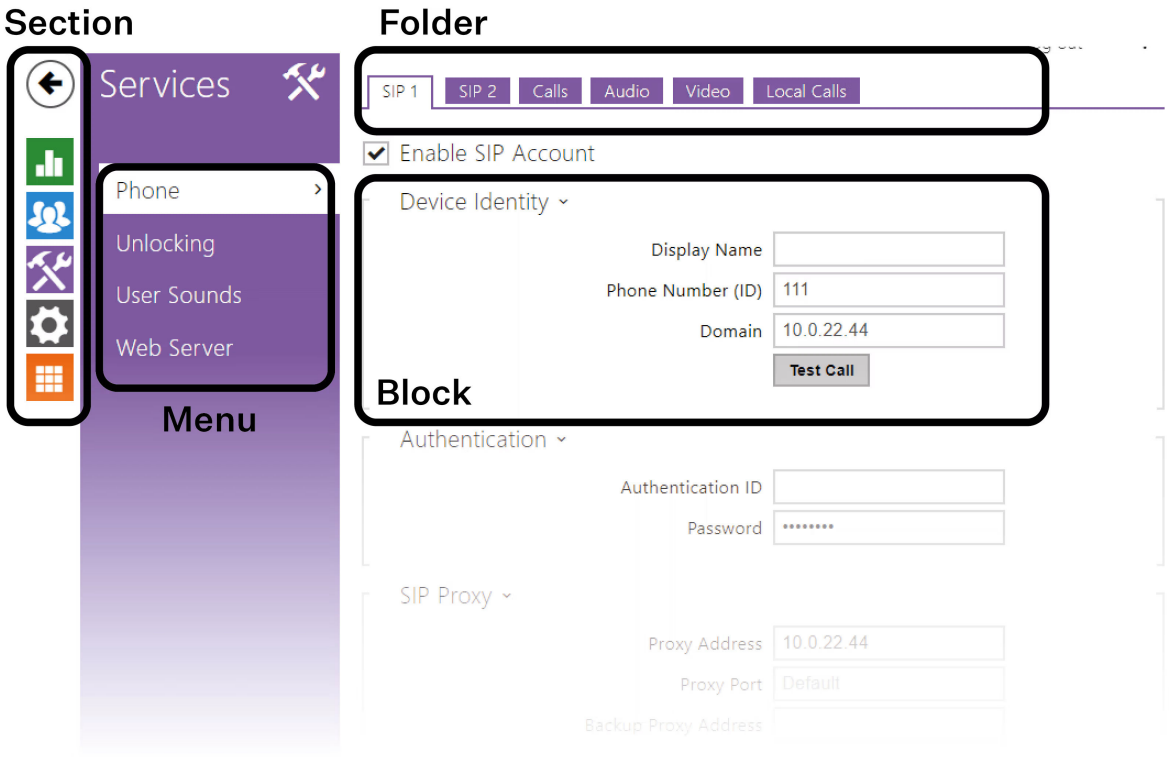
The start screen is displayed whenever you log into the **2N Clip 2wire-IP** web configuration interface. Use the  button in the left-hand upper corner on each of the other web configuration interface pages to return to this screen anytime. The page header shows the device name (refer to Device Name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

Menus

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

Legend

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



Device Configuration Interface Access

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

Domain Name

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

Default domain name 2N Clip 2wire-IP: Clip 2wire-IP-{serial number without dashes}.local (e.g.: “Clip 2wire-IP-0000000001.local”)

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

IP address

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

- Use the freely accessible **2N Network Scanner**.
- Display information on the device display.
- Use hardware (RESET button).

Web Configuration Interface Login

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

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

For increased password security, it is recommended that:

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

State

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

Device

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

Device Info

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

Locate Device – optical or acoustic signaling of the device.

Optical signaling is only available if the device is equipped with backlight. If a speaker is not integrated in the device, make sure than an external speaker is connected to the sound signaling connection.

Services

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

Call Logs

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

- contact type,
- name,

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

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

Events

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

Events	Meaning
ApiAccessRequested	Generated whenever the request is sent to /api/accesspoint/grantaccess with the "success" : true result.
CallSessionStateChanged	Event describing the call direction/state, address, session number and call sequence number.
CallStateChanged	Indicates the call direction (incoming, outgoing) and opponent / SIP account identification at a call state change (ringing, connected, terminated).
DeviceState	Device state indication, startup of the device, for example.
DtmfEntered	DTMF code received in call or off call locally.
DtmfSent	DTMF code sent in call or off call locally.
ErrorStateChanged	Device error state.
InputChanged	Signals a state change of the logic input.
KeyPressed	Generated whenever a button is pressed (numeric keypad digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
KeyReleased	Generated whenever a button is released (the digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
LogAutomationEvent	

Events	Meaning
LoginBlocked	Whenever 3 wrong logins to the web configuration interface have been entered. Includes data on the IP address of these accesses, time, time zone and device uptime (time after the last restart in seconds).
OutputChanged	Signals a change of the logic output state.
RegistrationStateChanged	Change of the SIP Proxy registration state.

Directory

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

Up to 200 devices can be added to the Directory.

Device

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

Add Device helps create a new device. The  icon displays the user settings details. The  icon helps remove a device from the list including all of its data. You can arrange the list according to the name or phone number ( feature icon of the device that is allowed to be displayed,  feature icon of the device that is allowed to receive incoming calls,  feature icon of the device to which an alarm call will be set up after the doorbell button is pressed,  / icons for initiating a phone call after a short/long press). One list page can display 15, 25 or 50 devices.

Basic Settings

Each device list item includes the following data in the Basic settings block:

Device Name – enter the device name for the selected Phone Book position. This parameter is optional and helps you find items in the Phone Book more easily.

Displayed Icon – display the reception desk symbol or a standard symbol.

Device Type – set this parameter manually or automatically using search for registered devices in the Device list.

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

Press  to set the phone number details.

Setting the phone number

- **Call Type** – set the scheme in the called destination URI. If you choose Without scheme ([unspecified]), the URI is completed with the data from the SIP account settings. Other options include direct SIP call (sip:), 2N local calls (device:), calls to Crestron devices (rava:), connection with MS Teams (msteams:), or calls with VMS, e.g., AXIS Camera Station (vms:).
- **Destination** – set the other parts of the called destination URI. As a rule, it contains the number, IP address, domain, port or device identifier. Enter an asterisk "*" for calls to the VMS.
- **Preferred SIP Account** – SIP account 1 or 2 is primarily used for calling.
- **Call Encryption** – set mandatory call encryption or no encryption.
- **Door Opening** – via callbacks.

Individual Ringtone – set an individual ringtone for specific contacts for better distinction.

Call Button Function

Start Call on Short Press – a phone call to the selected device will be set up after a short press of the call button.

Start Call with Long Press – a phone call to the selected device will be set up after a long press of the call button.

Alarm Call

Start Call with Doorbell Button Press – a phone call to this device will be set up after the alarm call button is pressed. Set the doorbell alarm call function in **Hardware >** **Digital inputs (p. 46)** **> Doorbell button**.

Unlock Button Function

Short Press Code – the code assigned to a short press of the unlocking button is sent. It used for remote unlocking of the entrance door, for example. Make sure that the code includes at least two door unlocking characters via the intercom keypad and at least one door unlocking DTMF character via a phone. Four characters at least are recommended. You need to make sure that the device is configured to accept this code.

Long Press Code – the code assigned to a long press of the unlock button is sent. It is used for remote unlocking of the entrance door, for example. Make sure that the code includes at least two door unlocking characters via the intercom keypad and at least one door unlocking DTMF character via a phone. Four characters at least are recommended. You need to make sure that the device is configured to accept this code.

CAUTION

At Relax (p. 66):

- If only 1 device is added to the directory, the code after a long press will be sent whenever the unlock button is pressed .
- If 2 devices are added to the directory, the code after a short press will be sent whenever the unlock button is pressed .

During Call:

- The unlock button sends the code after a long press if set.

Calling

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

Calls

General Settings

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

Incoming Calls

Local Call Answering Mode – set the way of receiving incoming local calls. The following three options are available:

- “Always busy” – the device rejects incoming calls.
- “Manual Pickup” – the device rings to signal incoming calls and the user can press a button to pick up.
- “Automatic” – the device picks up incoming calls automatically.

Call Receiving Mode (SIP 1/2/3/4) – set the way of receiving incoming calls. You can set the call receiving mode for each SIP account separately. The following three options are available:

- “Always busy” – the device rejects incoming calls.
- “Manual Pickup” – the device rings to signal incoming calls and the user can press a button to pick up.
- “Automatic” – the device picks up incoming calls automatically.

MS Teams Call Answering Mode - set how the intercom shall answer incoming calls from your Microsoft Teams account. The following three options are available:

- “Always busy” – the device rejects incoming calls.
- “Manual Pickup” – the device rings to signal incoming calls and the user can press a button to pick up.
- “Automatic” – the device picks up incoming calls automatically.

Pick Up In – this parameter is only active when the Automatic pickup mode is enabled. The call is picked up automatically after the preset timeout.

Outgoing Calls

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

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

Advanced Settings

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

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

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

Local Calls

Configuration

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

Network Identification

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

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

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

Connection to Intercoms

Access Key 1, 2 – set the access key shared by the 2N answering units and intercoms. If the keys in the 2N answering units and the intercoms fail to match, the devices cannot communicate, i.e. the intercom cannot call the 2N answering unit and vice versa.

Connection to Answering Units

Access Key - set the access key to be shared between the 2N devices in the local network. This ensures that only those 2N devices that have the same access code can communicate with each other, e.g. an intercom can call an answering unit, an answering unit can watch video from an intercom. Up to three access keys can be assigned to each device, making it part of up to three independent groups of intercoms and answering units. The access key can be up to 63 characters long.

Multicast Address – set the network multicast address to which the answering unit message shall be sent.

Connection to Lobby Units

LAN Devices

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

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

Audio

DTMF Sending

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

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

DTMF Receiving

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

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

Transmission Quality Settings

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

SIP

2N Clip 2wire-IP allows two independent SIP accounts to be configured. Thus, the intercom can be registered under two phone numbers at the same time, with two different SIP exchanges, for example. Both the SIP accounts process incoming calls equivalently. Outgoing calls are primarily processed using account SIP1. Or, if SIP1 is not registered (due to SIP exchange error, e.g.), SIP2 is automatically used

for outgoing calls. Select the account number for the phone numbers included in the phone directory to specify the account to be used for outgoing calls (example: 2568/1 - calls to number 2568 go via account 1, sip:1234@192.168.1.1/2 calls to sip uri via account 2).

Configuration

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

Device Identity

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

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

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

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

Authentication

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

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

SIP Proxy

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

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

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

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

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

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

SIP Registrar

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

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

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

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

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

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

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

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

Advanced Settings

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

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

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

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

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

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

Default Local Port Values for SIP

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

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

REFER Enabled – enable call forwarding via the REFER method.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Video

Video Codecs

Enable/disable the use of video codecs for call setups and set their priorities.

Extended Codec Settings

Enabled – enable the packetization mode and set the payload type for each codec. The payload type can be selected automatically in case it cannot be set manually.

SDP Payload Type – set the payload type for video codec H.264 (packetization mode 1). Set a value from the range of 96 through 127, or 0 to disable this codec type.

Audio

Audio Codecs

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

DTMF Sending

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

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

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

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

DTMF Receiving

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

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

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

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

Transmission Quality Settings

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

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

Services

Unlocking

Unlocking is another function of **2N Clip 2wire-IP**, which sets the remote door unlocking parameters.

Unlock Settings

Default Unlock Code – use this code when a call has been set up with a device/phone number that is not in the unit phone book.

Hang Up After Door Unlocking – end the call when the door unlocking request has been sent successfully.

Hang Up Delay – end the call when the door unlocking request sending timeout has elapsed.

Integration

MS Teams Tab

Microsoft Teams integration provides calls between a 2N device and the Microsoft Teams account. You have to configure the Microsoft Teams SIP gateway to interconnect the device with Microsoft Teams. Refer to the FAQ or the MS Teams documentation for details. Once you enter the configuration server address into the 2N device configuration, the integration (onboarding) is accomplished. Upon onboarding, you can log in to the Microsoft Teams account in the web configuration interface.

Microsoft Teams Enabled – enable integration with MS Teams

Service

State – display the current status of the onboarding and login processes.

- "Disabled" – function disabled.
- "Onboarding" – the device is getting/has got the shared configuration for onboarding or individual configuration for onboarding (before login).
- "Onboarding failed" – the device was unable to get the shared/individual onboarding configuration or to register with the onboarding SIP server.
- "Offline" – no sever response.
- "Online" – successful device registration with the end SIP server.

- “Registration Failed” – the device failed to register with the end SIP server.
- “License Required” – the device is not equipped with the license required for this function.

Phone Number – display the phone number (ID) that the device obtained from the MS Teams server.

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

Provisioning Server Settings

Address Retrieval Mode – select whether the MS Teams onboarding server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 or 150 shall be used.

Server Address – enter the MS Teams onboarding server manually.

DHCP (Option 66/150) address – check the server address retrieved via the DHCP Option 66 or 150.

Configuration Update Schedule

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

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

Update At – set the update time in the HH:MM format for periodical updating The parameter is not applied if the update interval is shorter than 1 day. Time is set in UTC. Check the Next Update Time value to see the actual update time scheduled.

Discovery Service Tab

Settings

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

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

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

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

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

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

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

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

User Sounds

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

Sound Mapping

Sound Mapping

- “Busy Tone” – set the busy tone to be played when the called user is busy.
- “Call End Extension” – set the sound to be played upon the call end.
- “Ringtone” – set the sound to be played when the called user is ringing.
- “Ringing before Call Answering” – set the sound to be played before answering an incoming call (device ringtone).
- “Doorbell” – set the sound to be played when the door button is pressed.

Web Server

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

Basic Settings

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

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

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

Advanced Settings

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

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

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

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

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

User Localization

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

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

Hardware

Audio

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

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

TIP

The master volume of the device can also be controlled using the

Phone Call Volume

Call Volume – set the phone call volume.

Ringtone Volume – set the volume of the incoming call ringtone. The value is relative to the master volume.

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

Signaling Volume

Button Press Volume – set the Button Press Volume. The volume values are relative against the set master volume.

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

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

Display

The Display menu helps you set the display appearance and functionality parameters as well as the parameters of the menu shown on the display.

Basic Settings

Set the basic display parameters in this block.

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

Date Format – set the date format to be displayed.

Time Format – set the time format to be displayed.

Enable Screen Lock – enable the screen lock in the Idle device mode. Enter the screen lock PIN to unlock the user interface.

Display Setting Menu – display the Setting menu. Or, configure the device via the web and remote access.

When the Doorbell Button Function is set to Doorbell (refer to Digital Inputs (p. 46)), a bell activation notification is displayed whenever the doorbell is pressed. If the Idle time transition timeout is ≤ 120 s, the notification will be displayed for 120 seconds. If the Idle time transition timeout is > 120 s, the home screen will be displayed after the 120-second timeout until the device goes into the Idle mode.

Backlight

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

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

User Localization

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

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

Custom Language Upload

1. Download the original language file (English).
2. Modify the file using a text editor (replace the English texts with your own ones).
3. Upload the modified localization file back to the intercom.
4. Set **Language** to Custom (p. 45) in “Basic Settings”.
5. Check and correct if necessary the texts on the intercom display.

Digital Inputs

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

Doorbell Button

Doorbell Button Function – select a doorbell function (doorbell, alarm call). The button is used either as a classical doorbell or an alarm call activating button.

System

Network

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

TIP
To retrieve the IP address, use **2N Network Scanner**, which can be downloaded freely from 2N.com. Refer to Subs. IP Address Retrieval Using **2N Network Scanner** (p. 26) for details.

If the network uses the RADIUS server and 802.1x-based verification of connected equipment, you can make the device use the EAP-MD5 or EAP-TLS authentication. Set this function in 802.1x (p. 47).

Basic

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

Static IP Address Setting

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

Network Mask – network mask setting.

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

DNS Setting

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

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

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

Network Interface Settings

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

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

Network Identification

Hostname – set the device LAN identification.

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

VLAN Settings

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

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

802.1x

Device Identity

Device Identity – User name (identity) for authentication via EAP-MD5 and EAP-TLS.

MD5 Authentication

Authentication Allowed – enable network device authentication via the 802.1x EAP-MD5 protocol. If the network does not support 802.1x, the intercom will become unavailable.

Password – enter the access password for EAP-MD5 authentication.

TLS Authentication

Authentication Allowed – enable network device authentication via the 802.1x EAP-MD5 protocol. If the network does not support 802.1x, the intercom will become unavailable.

Trusted Certificate – specify the set of trusted certificates for verification of the RADIUS server public certificate validity. Choose one of three certificate sets, see Certificates (p. 49). If no trusted certificate is included, the RADIUS public certificate is not verified.

Client Certificate – specify the user certificate and private key for verification of the intercom authorization to communicate via the 802.1x-secured network element port in the LAN. There are three sets of user certificates and private keys, refer to the Certificates subsection, see Certificates (p. 49).

PEAP MSCHAPv2 Authentication

Authentication Allowed – enable authentication of network devices via the 802.1x PEAP MSCHAPv2 protocol. If the network does not support 802.1x, the intercom will become unavailable.

Trusted Certificate – specify the set of trusted certificates for verification of the RADIUS server public certificate validity. Choose one of three certificate sets, see Certificates (p. 49). If no trusted certificate is included, the RADIUS public certificate is not verified.

Password – enter the access password for PEAP-MSCHAPv2 authentication.

Firewall Tab

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

Firewall

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

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

Date and Time

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

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

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

Current Time

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

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

Time Zone

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

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

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

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

NTP Server

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

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

Features

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

The list includes:

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

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

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

Certificates

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

The following device services use the TLS protocol:

1. Web server (HTTPS)
2. 802.1x (EAP-TLS)
3. SIPs

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

Each certificate requiring service can be assigned one certificate set, refer to Web Server (p. 44). The certificates can be shared by the services.

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

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

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

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

Certificate Upload

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

NOTE

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

CSR

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

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

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

Auto Provisioning

My2N

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

My2N Enabled – enable connection to My2N.

My2N Security Code

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

My2N Security Code – device code for adding to My2N.

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

Connection State

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

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

TR069

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

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

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

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

General Settings

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

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

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

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

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

Diagnostics

Diagnostics

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

Diagnostic Package

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

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

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

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

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

Stop Syslog Capture – set the data capture time.

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

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

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

CAUTION

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

Tools

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

Packet Capture

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

Local Packet Capture

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

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

Remote Packet Capture

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

Syslog

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

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

Syslog Server Settings

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

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

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

Local Syslog Messages

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

Maintenance

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

Configuration

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

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

CAUTION

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

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

CAUTION

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

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

System

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

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

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

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

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

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

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

Usage Statistics

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

Used Ports

Service	Port	Protocol	Direction	On by default	Configurable	Settings
802.1x	–	–	In/Out	×	×	–

Service	Port	Proto-col	Direc-tion	On by default	Config-urable	Settings
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device dis-covery)*	8002	UDP	In/Out	✓	×	–
2N IP Eye	8003	UDP	Out	×	×	–
HTTP	80	TCP	In/Out	✓	✓	Web Server (p. 44)
HTTPS	443	TCP	In/Out	✓	✓	Web Server (p. 44)
NTP client	123	UDP	In/Out	✓	×	–
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	×	✓	Calling (p. 37)
RTSP client	554	UDP	In/Out	×	✓	Calling (p. 37)
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	Calling (p. 37)
SIPS	5061	TCP	In/Out	×	✓	Calling (p. 37)
Syslog	514	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–

Service	Port	Proto-col	Direc-tion	On by default	Config-urable	Settings
My2N Tribble Tun-nel	443	TCP	Out	✓	×	–
Sitechannel (ICU protocol)	8004	UDP	In/Out	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

Device Control

There are 3 buttons on the device front side for basic control of the device:

- – the earphone button is primarily used for starting an outgoing and receiving/rejecting an incoming call,
- – the lock button is primarily used for unlocking the set device,
- – the speaker button is primarily used for the device volume control.

Button Functions

There are three types of a device button press:

- short press,
- long press,
- simultaneous long press of two buttons.

The device control options in the basic home screen display are as follows:

Button	Press type	Generated action
	Short press	Outgoing call to device A (see the note below for setting details).
	Long press	Outgoing call to device B (see the note below for setting details).
	Short press	Unlocking of device A lock (see the note below for setting details).
	Long press	Unlocking of device B lock (see the note below for setting details).
	Short press	Volume increase by one level (after the upper limit is reached, volume goes to the lowest value – value rotation) Upon a volume level change, the device plays the new volume level sound. The sound signaling is shown as a percentage on the display. The volume level is the same for all states and sounds. When the lowest volume level is selected (mute), the Mute signaling is displayed in all the states except for the Idle mode .
	Long press	Ringtone Setting Menu (p. 62) is displayed.

Button	Press type	Generated action
a	Simultaneous long press of both buttons	Device Lock (p. 67) is activated. Enable the Device lock option in the Settings menu or in the web configuration interface.
and	Simultaneous long press of both buttons	Settings Menu (p. 61) is displayed.

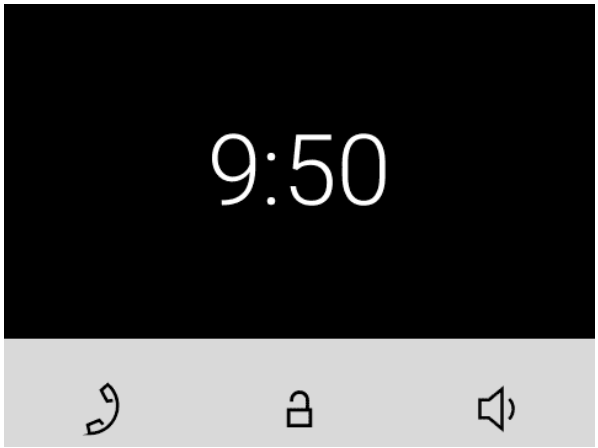
TIP
Select **Start Call with Short Press** to set device A and select **Start Call with Long Press** to set device B in the web configurationDevice (p. 35).

The button control may be different in different operational states or menus of the device. Refer to the descriptions of the states and menus below for more information on the button actions:

- Settings Menu (p. 61),
- Ringtone Setting Menu (p. 62),
- Calls (p. 64),
- Idle Mode (p. 66),
- Device Lock (p. 67).

Home Screen

The Home screen is set as the start screen of the device, which is displayed whenever the device is activated by a or button press in the Idle mode. Its appearance depends on the device configuration, see below.



It is possible to activate the device lock from this state.

The device displays:

- Time – display the time format as set in the web configuration menu Display (p. 45) – 12h or 24h.

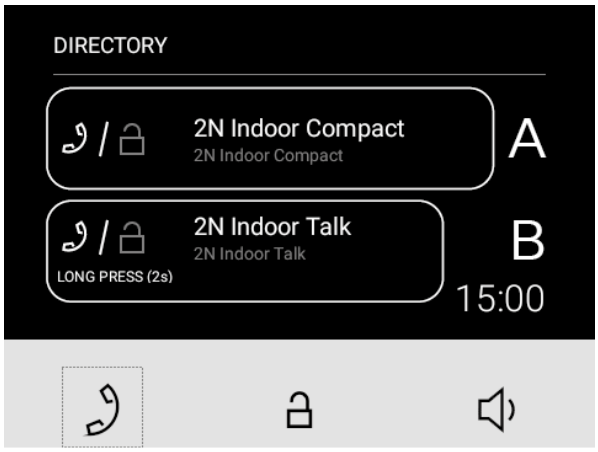
The home screen provides access to:

- Ringtone Setting Menu
- Directory
- Settings

Possible actions	Performance	Action result
Display of Ringtone Setting Menu	Long Button Press	Ringtone Setting Menu (p. 62) is displayed.
Settings Menu Display	Simultaneous long press of and	Settings Menu (p. 61) is displayed on the device.

Directory Menu

If 2 or more devices are added to **2N Clip 2wire-IP**, the Directory menu is displayed as introduction instead of the home screen. The Directory menu helps you display 2 devices – device A and device B. The displayed devices can be selected, see the note below. If there are more than 2 devices in the Directory or more than 2 are selected for display, they are arranged in the order and then alphabetically. If a group of devices is to be displayed, the name and icon of the first device on the list is used for display.



TIP
Select **Start Call with Short Press** to set device A and select **Start Call with Long Press** to set device B in the web configuration Device (p. 35).

The Directory menu includes a list of added devices and available actions. If a call is missed from a displayed device, the missed call icon appears at the respective device. The icon disappears when any action is performed from the home screen.

The Directory menu shows all the actions included in Subs. Home Screen (p. 58).

NOTE
If just 1 device is added, the Directory menu does not replace the introductory screen of the device. If a call is missed from a displayed device, the missed call icon appears next to the time value. The icon disappears whenever an action is performed from the home screen.

Possible actions	Performance	Action result
Outgoing call to device A	Short press of	Call to device A is started.
Outgoing call to device B	Long press	Call to device B is started.
Device 1 Unlocking	Short press of	The code of the unlock button short press is sent to open the device lock for which this code has been defined.
Device 2 Unlocking	Long press	The code of the unlock button long press is sent to open the device lock for which this code has been defined.
Settings Menu Display		Settings Menu (p. 61) is displayed on the device.
Device lock activation	Simultaneous long press of and	Device Lock (p. 67) is activated.
Display of Ringtone Setting Menu	Long Button Press	Ringtone Setting Menu (p. 62) is displayed.

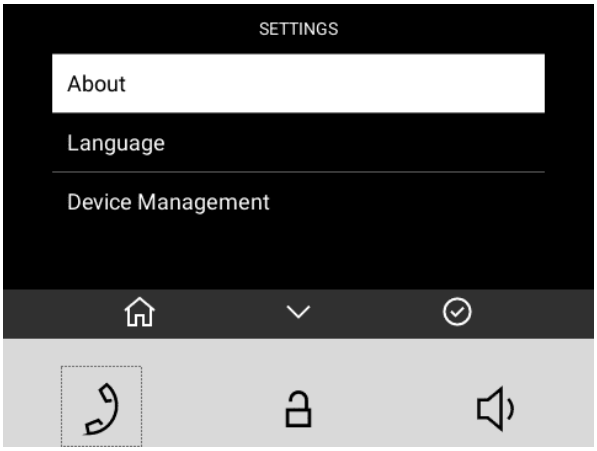
Settings Menu

After a long press of buttons and , the home screen displays the Settings menu.

The Settings menu helps you set the device locally and contains a context menu in the bottom part, which is controlled using the device buttons.

The Settings menu makes it possible to:

- display information on the device (firmware version, IP address (p. 28), etc.),
- change the device language,
- restart the device (p. 29),
- set the device display brightness,
- set the display inactivity timeout, i.e. the transition timeout for the device to switch into the Idle mode (p. 66),
- activate the Device lock (p. 67).



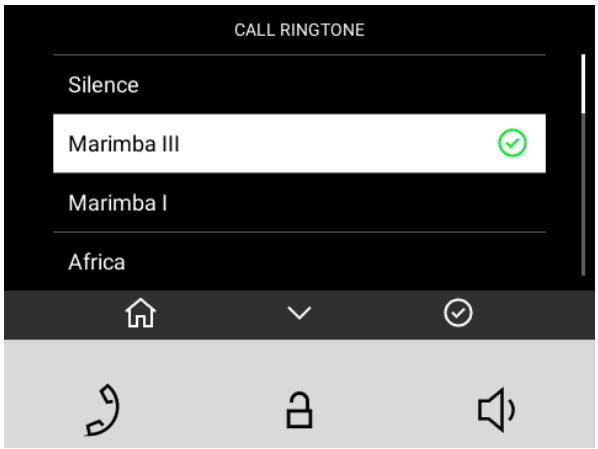
NOTE
Use the Display (p. 45) menu in the web configuration to block the access to the menu. At that moment, the device can be only be configured by software or remote access.

Possible actions	Performance	Action result
Return to home screen	by a short press of , or in 10 seconds without any button being pressed, or after a call if any.	The selection is cancelled and the menu actions are terminated without saving.
Back (return to preceding action)	Short press of	Navigation to the preceding menu section.
Selection confirmation	Short press of	Confirmation of the selected setting option or transition to the selected menu section.

Possible actions	Performance	Action result
Move to next position	Short press of	Movement by one position down in the setting. The movement is signaled with a white box highlighting the current position. When the list end is reached, the first position is moved onto.
Device restart confirmation	Short press of	Device is restarted. The Home screen (p. 58) is displayed after restart. **NOTE** Restarting may take a rather long time after the button press.
Quit device restart dialog	Short press of	Navigation to the preceding menu section.

Ringtone Setting Menu

A long button press displays the ringtone list.



Possible actions	Performance	Action result
Cancel the selection and return to the home screen.	Short press of	The selection is cancelled and the menu actions are terminated without saving. Home screen (p. 58) is displayed.

Possible actions	Performance	Action result
Move to next ringtone	Short press of 	Movement by one position down in the setting. The movement is signaled with a white box highlighting the current position. When the list end is reached, the first position is moved onto. The selected ringtone position is white highlighted in the list. When the list end is reached, the first position is moved onto. Ringtone examples are played during the movement in the settings.
Selection confirmation	Short press of 	the selection is confirmed. The device sets the selected ringtone. Home screen (p. 58) is displayed.

Operational Statuses

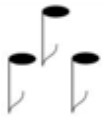
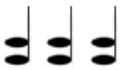
This section includes a basic description of user scenarios and states that can occur during the use of **2N Clip 2wire-IP**, a list of user options in variable states and expected results of these actions.

- Signaling of Operational Statuses (p. 63)
- Calls (p. 64)
- Idle Mode (p. 66)
- Device Lock (p. 67)

Signaling of Operational Statuses

The device generates sounds to signal changes of and switching between operational statuses. Each status change is assigned a different type of tone. See the table below for the list of signals.

Sound signaling	State
	**Internal application started** The internal application is launched after the power supply is turned on or the device is restarted.
	**Connected to the LAN, IP address received** Once the internal application is started, the device logs in to the LAN.

Sound signaling	State
	**Disconnected from the LAN, IP address lost.** Disconnected from the LAN, IP address lost
	**Invalid phone number or invalid switch activation code** The device allows you to enter the door opening code. This tone signals that invalid values have been entered.
	**Reset of network parameters** Upon power up, the network parameters can be changed by hardware, refer to Configuration via Hardware (p. 24).
	Approaching call end signaling The device allows you to set a call end timeout, refer to General Settings (p. 37).
	**Call extension confirmation signaling** A call can be extended by pressing a key on the VoIP phone.
	**Connected call from a VoIP phone to the device** A short tone is played to signal that the VoIP call has been connected to the device.

Calls

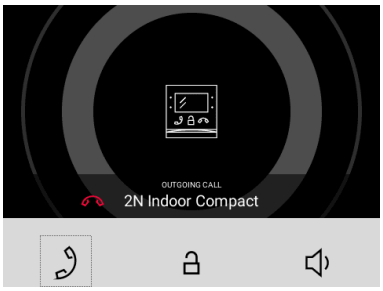
In this state, connection or connection attempt is in progress with another device. The **2N Clip 2wire-IP** functions are limited, it is impossible to switch to the home page and go to menus. Possible actions are included in the table below.

A preview of the camera if available is shown on the display.

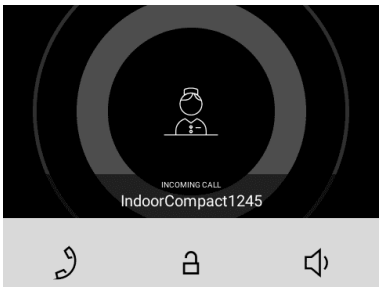
In this state, one of the following call types can be active in the device:

- **Outgoing call** initiated by the **2N Clip 2wire-IP** answering unit.
- **Incoming** trying to establish connection with the **2N Clip 2wire-IP** answering unit.
- **Active call** – if connection between the devices is established, sound is transmitted.

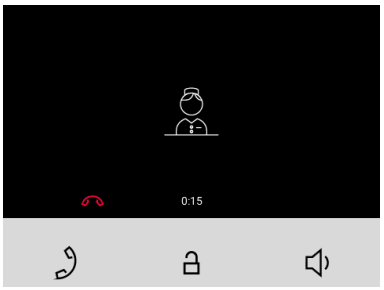
Outgoing Call



Incoming Call



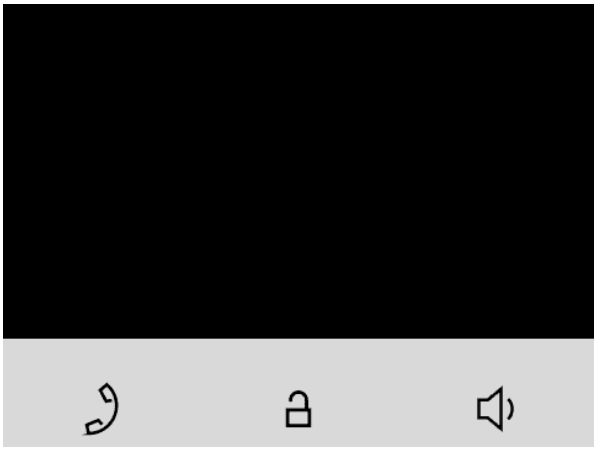
Active Call



Possible actions	Performance	Action result
Incoming call receiving		Connection with the other device has been established, a call is in progress. The call cannot be ended until answered.
End of call		The active call is interrupted. The call cannot be ended until answered.
Target device lock opening		A specifically configured unlock code is sent to the target device and, if the code is compatible with the device, the target device lock opens. If no unlock code is set, the default unlock code is sent to the target device. During a call, the unlock button sends a code after a long press, if set. Door unlocking is signaled by a tone and green flash of the lock button. After unlocking, automatic call ending can be set in the web configuration interface Unlocking (p. 42).
Call volume control		Volume increase by one level (after the upper limit is reached, volume goes to the lowest value – value rotation)
Ringtone Disable		The ringtone stops playing when a call comes in. The incoming call is not ended. The repress of the button does not cancel mute.

Idle Mode

2N Clip 2wire-IP transits into the Idle mode after a set inactivity period. Set the inactivity timeout in the Display (p. 45) web configuration menu. The operation power consumption is reduced in the Idle mode.



The device shows no information on the display in the Idle mode.

At Relax (p. 66):

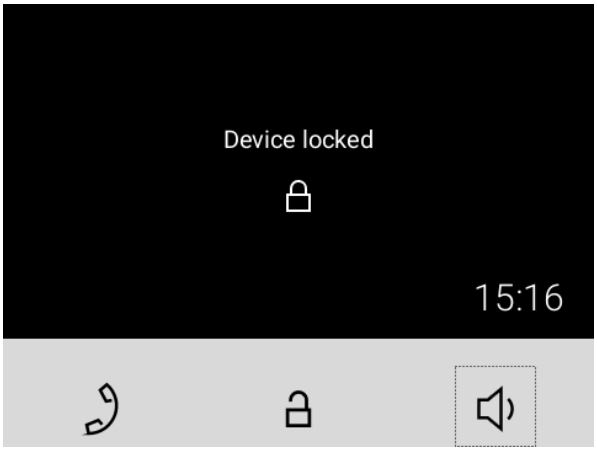
- If only 1 device is added to the directory, the code after a long press will be sent whenever the unlock button is pressed .
- If 2 devices are added to the directory, the code after a short press will be sent whenever the unlock button is pressed .

Possible actions	Performance	Action result
Idle mode end	Press any key	The device quits the Idle mode. The Directory MenuHome Screen (p. 58) or Device Lock (p. 67) is displayed.

Device Lock

Enable the Device lock option in the Settings menu or in the web configuration interface.

When the lock is activated, the device rings to signal an incoming call and displays the caller identification including the camera preview if available. The call cannot be received until the device lock is deactivated.



NOTE
Set the device lock activation in the Idle mode in the Display (p. 45) menu in the web configuration interface.

Possible actions	Performance	Action result
Device lock activation	Simultaneous press of and for 3 seconds	The lock is activated.
Device lock deactivation	Simultaneous press of and for 3 seconds	The device is unlocked and you can go to other operational statuses and perform other actions.

Maintenance - Cleaning

2N Clip 2wire-IP 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.

Troubleshooting

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

Technical Parameters

2N Clip 2wire-IP

Power Consumption	
Stand-by mode with display off	1,2 W
Stand-by mode with display on	2.0 W
Calls without audio	2.4 W
Calls with audio	4.4 W
Calls with induction loop	6.4 W

User interface	
Controls	3 capacitive buttons
Display	4" with 480 x 272 pixel resolution

Signaling protocol	
SIP	UDP, TCP, TLS

Audio	
Microphone	integrated
Speaker	3 W integrated

Audio	
Induction loop output	NO (induction loop integration depends on the model version)

Audio stream	
Protocols	RTP
Codecs	PCMU, PCMA, G.729, G.722, L16/16kHz

Video stream	
Protocols	RTP, RTSP, HTTP
Codecs	H.264
Video Resolution	480 x 272 px
Frame rate	up to 15 frames per s

Interface	
2 wires 10 Mbit	2N 2 wire-IP 10 Mbit, recommended single core 24AWG, cat3 cable

Doorbell input	
Input type	Switching contact (button/relay)
Contact type	Normally open (NO)

Doorbell input	
Contact parameters	Min. 12 V / 20 mA, DC

Mechanical Parameters		
Device dimensions (W x H x D)		124 x 150 x 26 mm
Weight	Main unit	295 g
Operating temperature		0 to 50 °C
Relative humidity		10 to 90 % non-condensing
Storing temperature		−20 °C to 70 °C
Recommended altitude		up to 2000 m

2N Clip 2wire-IP Switch

Power supply	
Power supply	48 V DC, the cable length between the switch and the power supply must not exceed 3 m (installation)
Limited Power Source (LPS)	1.92 A LPS

Interface	
LAN	for connecting two IP devices, the first position provides PoE (IEEE 802.3af) functionality
	100Base-TX, RJ45, LAN1 PoE
	recommended cable type: min. Cat 5e shielded 24AWG
2N 2Wire-IP interface (TWO WIRE INTERFACE)	↓ 100 Mbps input/output Leader ↑ 100 Mbps input/output Follower designed for connection to another 2wire switch
	1-6 10 Mbps output (POWER OUTPUTS) designed for connecting an answering unit (typically 48 V DC / max guaranteed continuous output current of 200 mA (short-circuit protection) / it is recommended that a device with continuous power consumption of max 10 W is connected)
	recommended cable type: min. Cat 3 single pair, 24AWG
USB	service connector intended exclusively for the manufacturer's service purposes

Mechanical Parameters	
Device dimensions (W x H x D)	157 x 58.5 x 102 mm (with terminals mounted)
Operating temperature	−10 °C to +55 °C
Recommended altitude	0 to 2000 m
Mounting	DIN rail for electrical switchboard with protective cover

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 Clip 2wire-IP 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
- 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.

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 Clip 2wire-IP – User Manual

2N.com