2N

2N Clip
User Manual

11:15 AM

Abstract

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** product, outline its application options and highlight the advantages following from its use. The section also includes safety precautions.

Basic Features

2N Clip is an indoor IP/SIP unit allowing for audio and video communication with the 2N IP intercoms.

The device includes a three-button control panel, Speakerphone, high-quality microphone with excellent audibility and intelligibility properties, Ethernet LAN interface and external power supply and doorbell connectors. **2N Clip** is a top-quality, cost efficient, easy to install and configure indoor answering unit. One installation can combine variable answering units manufactured by 2N Telekomunikace a.s.

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

Basic Features **2N Clip**:

• 2 mm thick Plexiglass display,
• ,
• 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.

Product and Accessory Versions

Product Versions 2N Clip
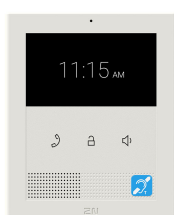
Part No.: 9138512

Axis Part No. 02893-001

2N Clip

Version with induction loop
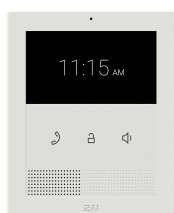
Part No.: 9138511

Axis Part No. 02892-001

2N Clip

Version without induction loop

Accessories for Installation

Choose the proper a mounting box depending on your particular installation needs.
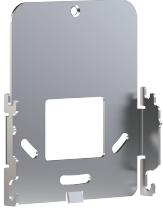
Part No. 9138003

Axis Part No. 02906-001

Mounting holder

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

Not included in the package of **2N Clip**.

Part No. 9138002

Axis Part No. 02905-001

Stand

Stand for **2N Clip**.

Not included in the package of **2N Clip**.

Device Description

This subsection provides the product package content and description of the device elements.

Package Completeness Check

Please check the product delivery before installation. Contents:

1x	**2N Clip**
1x	Certificate of ownership
1x	Quick Start manual
1x	Metal holder
2x	Holder fitting screws (3 x 12 mm self-tapping lens head screw)
1x	Doorbell connection terminal (removable)

Component Layout

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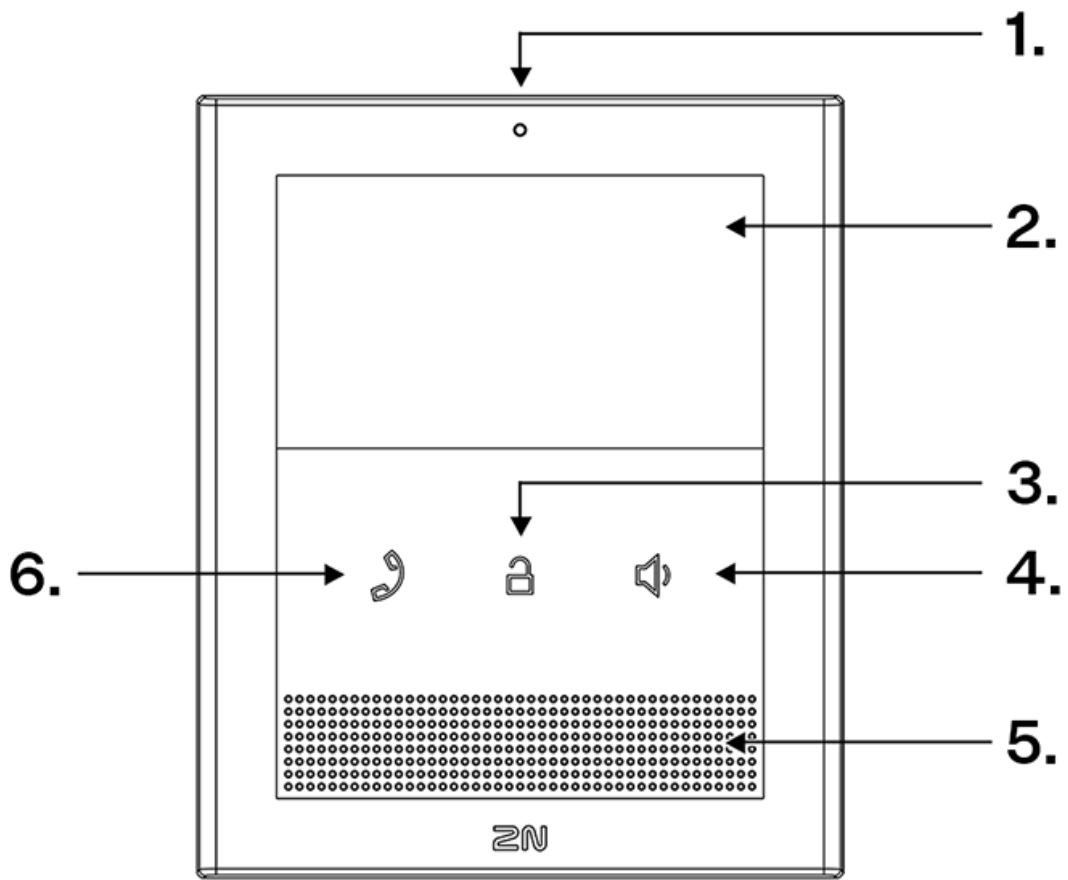
1. Microphone
2. Display
3. Lock button
4. Speaker button
5. Speaker
6. Earphone button

Rear

1. RESET Button
2. Doorbell Button Input
3. LAN Ethernet/PoE
4. Status LEDs
5. Locking Latch

Mechanical Installation

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

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

• onto a wall using a KU68 mounting box (not included in the package),
• onto a wall using a metal holder,
• into a stand (not included in the package).

> **⚠ WARNING**
> Having unpacked **2N Clip**, remove the metal holder located on the device back side for installation. Use both your hands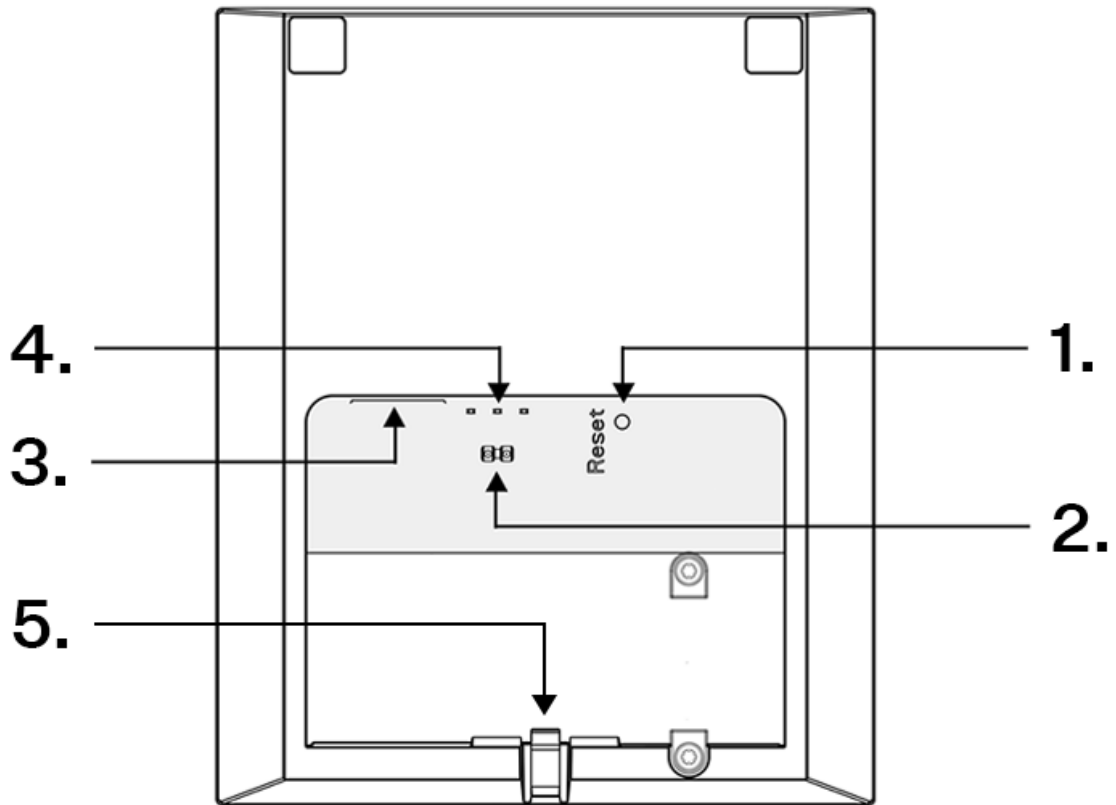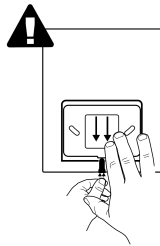 at the same time to remove the metal holder safely. A careless removal and insufficient push of the locking latch might lead to a locking latch damage. Follow the below mentioned removal instructions closely!
>
>
>
> 1. Push the locking latch in the center of the device bottom edge with your left hand 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.

Installation Conditions

Make sure that the following **2N Clip** installation conditions are met:

• There must be enough space for the device installation.
• The device is designed for vertical wall mounting (perpendicular to the floor) in the approximate height of 135 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.
• 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. 66).
• The device is not designed for environments with increased vibrations such as means of transport, machine rooms and so on.
• The device is not intended for dusty environments and places with unstable humidity and abrupt temperature changes.
• The device may not be exposed to aggressive gas, acid vapors, solvents, etc.
• The device is not intended for direct connection into the Internet/WAN. The device must be connected to the Internet/WAN via a separating active network element (switch/router).
• The device is designed for indoor use. It may not be exposed to rain, flowing water, condensing moisture, fog, etc.
• The device cannot be operated on places exposed to direct sunshine and near heat sources.

- 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.
- Make sure that the VoIP connection is configured properly according to the SIP and other VoIP recommendations.

Wall Installation

- Flush Mounting Box Installation
- Flush Mounting Box Device Installation

2N Clip can be installed into a KU 68 mounting box using an EU metal holder (included in the package), the recommended height of a standard installation being 135 cm above the ground level. The installation heights may vary depending on the device use. The device can also be installed directly on a wall without a mounting box.

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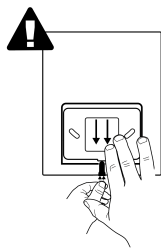
1. Push the locking latch in the center of the device bottom edge with your left hand in such a manner that it bends sufficiently for the metal holder removal. Do not push the locking latch from the top. You might get injured while removing the metal holder.
2. Grasp the metal holder with your right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

💡 **TIP**
Download the drilling template from 2N.com.

1.

2.

3.

4.

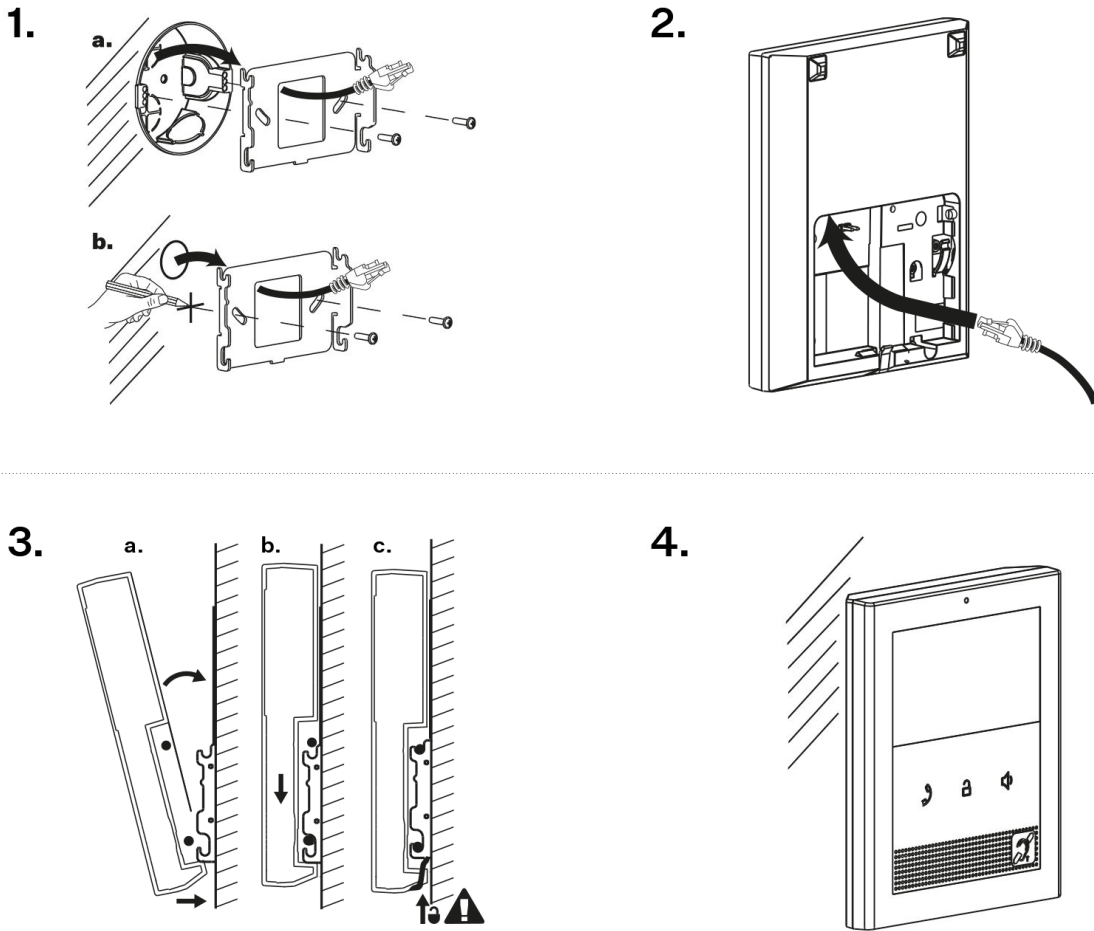1. Draw the LAN connector leading from the wall through the metal holder. Make sure that it is properly oriented in terms of device connection after installation.

> 🔆 **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 walled-in mounting box. Remove the pre-prepared cabling, UTP cable, doorbell twin cable and power supply cable.

2. Connect the LAN connector.

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. 29) to achieve a full functionality of the device.

You are advised to use a metal holder (not included in the package) for **2N Clip** 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.

> **TIP**
> Download the drilling template from 2N.com.

1a.

1b.

2.

3.

1. Draw the LAN connector leading from the wall through the metal holder. Make sure that it is properly oriented in terms of device connection 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.
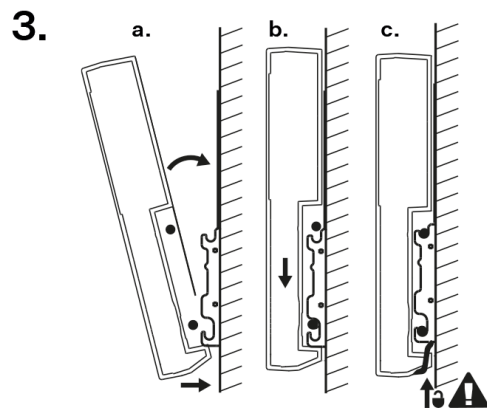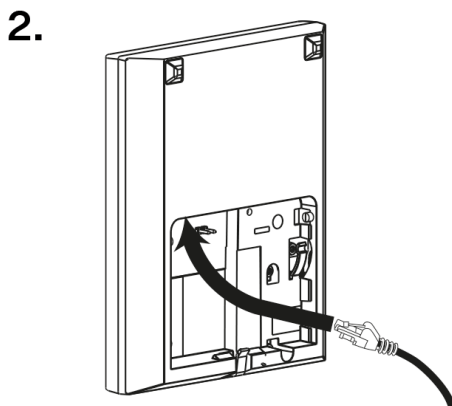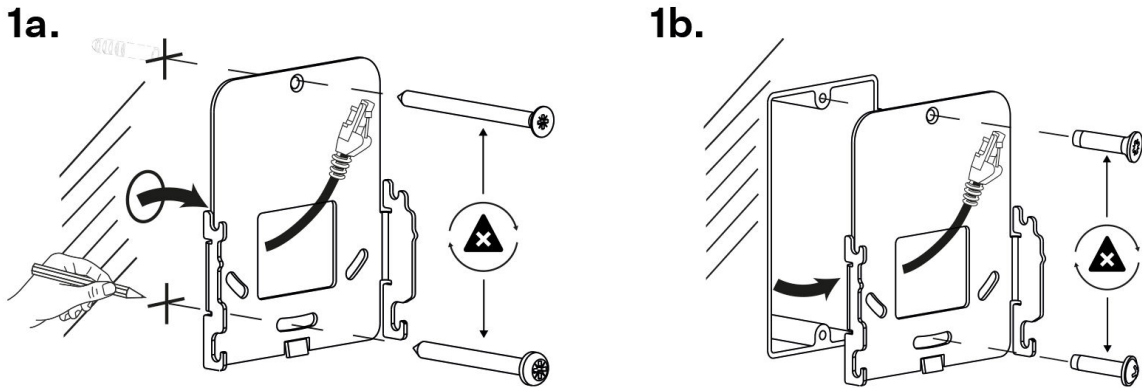
2. Connect the LAN connector to the device.

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.

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 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.

Within installation preparations, take out the pre-prepared cabling, UTP cable, doorbell (twin) cable and power supply. Shorten the cables to the required length. Crimp the RJ-45 connector onto the UTP cable. Connect the doorbell twin cable to the connector together with the LAN connector.

WARNING

Having unpacked **2N Clip**, 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!
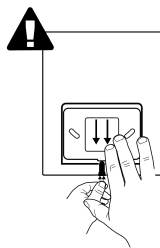
a. Push the locking latch in the center of the device bottom edge with your left hand in such a manner that it bends sufficiently for the metal holder removal. Do not push the locking latch from the top. You might get injured while removing the metal holder.

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

1a.
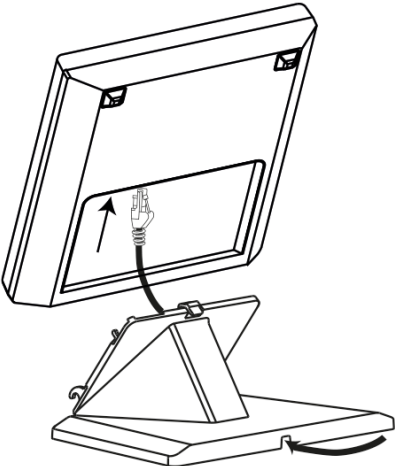
1b.

2a.

2b.

3.

1. Draw the LAN connector through the stand bottom and connect it to the LAN connector socket. Put the cable in the pre-prepared groove in the stand base. Unstick the protective foil from the stand anti-slip surfaces.
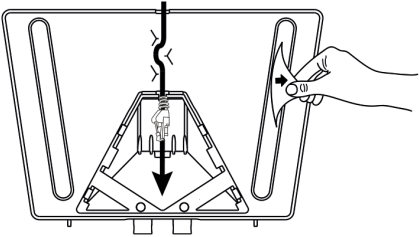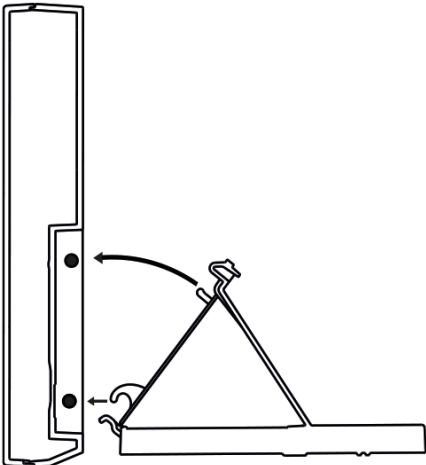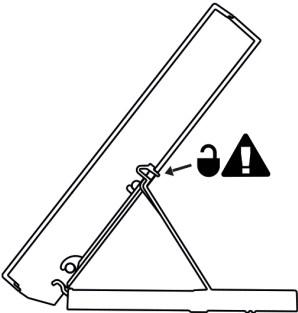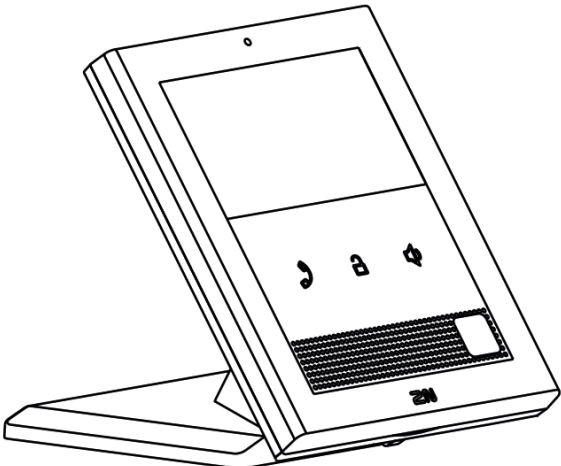
> ⚠ **CAUTION**
> We recommend that you use a CAT5e UTP cable to fit the stand bottom groove size.

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.

    Now the device is ready for basic operation. It is necessary to perform software configuration (p. 29) to achieve a full functionality of the device.

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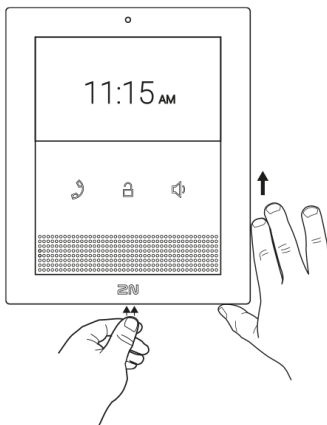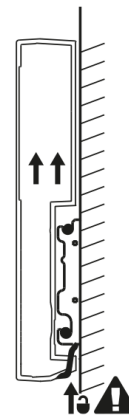
1. Press the locking latch located in the center of the device back bottom edge. Pull the device gently upwards to release it from the metal holder/stand.
2. Remove the device from the hooks and take it away safely.

Power Supply

2N Clip is fed via an Ethernet cable connected to a PoE power supply or PoE supporting Ethernet switch/router.

Supply type

PoE, IEEE 802.3af, Class 0 (0,44–12,95 W)

> ⚠ **WARNING**
>
> • Do not connect any external power supply if PoE is used and vice versa.
> • Connection of a defective or improper power supply may lead to a temporary or permanent device failure.

> **CAUTION**
> Make sure that the external power supply meets the power supply class PS2/LPS.

PoE Supply Connection

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

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

Figure 1. Ethernet cable connector   **Figure 2. Ethernet socket**
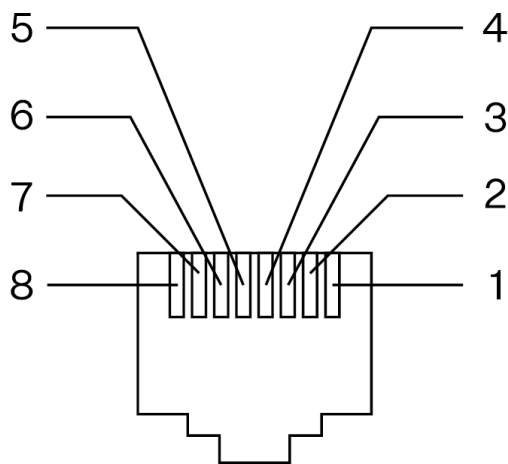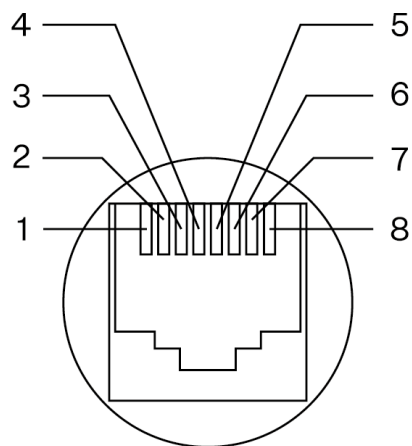
1. Tx
2. Tx
3. Rx
4. unused
5. unused
6. Rx
7. unused
8. unused

⚠️ **WARNING**

This device cannot be connected directly to telecom lines (or public wireless networks) of any telecom service providers (i.e. mobile providers, landline providers or Internet providers). A router has to be used for the device Internet connection.

Brief Guidelines

Device Configuration Interface Access

2N Clip is configured via the administration web interface. Connect the device to the LAN IP and make sure it is properly powered. You have to know the IP address for access.

Domain Name

Enter the domain name as "hostname.local". The new device Hostname consists of the device name and serial number. See below for the device name formats in Hostname. The serial number is entered without hyphens. You can change Hostname in System > Network later.

Ddefault domain name 2N Clip: 2NClip-{serial number without dashes}.local (e.g.: "2NClip-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 IP Address Retrieval (p. 20):

- 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** address or domain name into the internet browser.
   The login screen is now displayed.
   Should the login screen fail to appear, you must have typed a wrong IP address, port, domain name or the administration web server has been switched off. If you do not have a certificate generated for the IP address or domain name, an invalid security certificate warning may be displayed. In this case, you need 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**
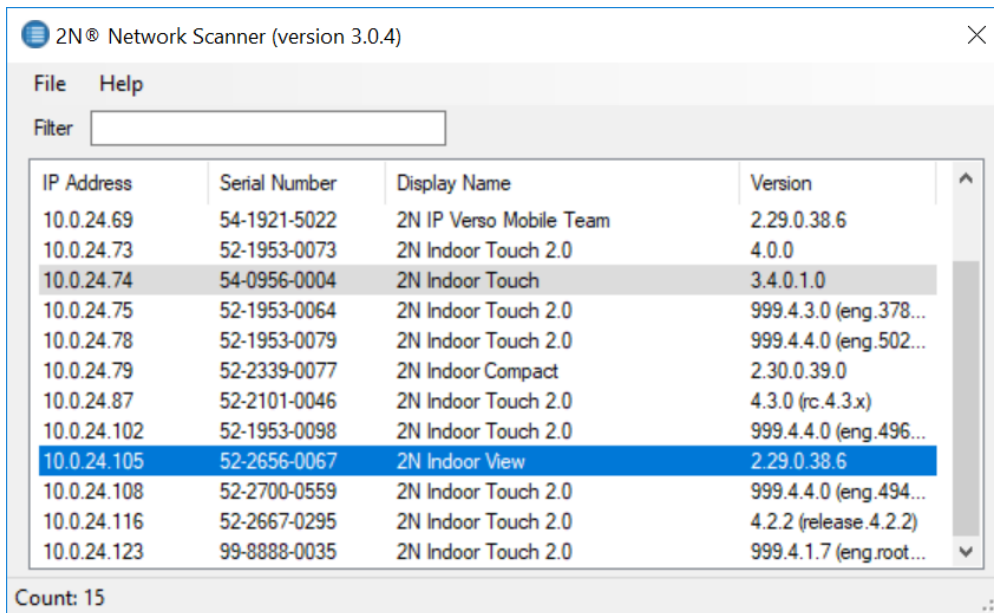
IP Address Retrieval

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.

> **TIP**
> - Double click the selected row in the 2N Network Scannerlist 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**

> **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.

IP Address Retrieval using Device Display

Follow the instructions provided in Subs. IP Address Retrieval Using 2N Network Scanner (p. 21) to retrieve the **2N Clip** IP address using 2N Network Scanner.

To find the device IP address using the display, press any button to quit the Idle mode. The Settings menu (p. 56) is displayed on the home screen after a long press of the earpiece ♪ and speaker ◁ buttons. Find the IP address information in the About device menu.
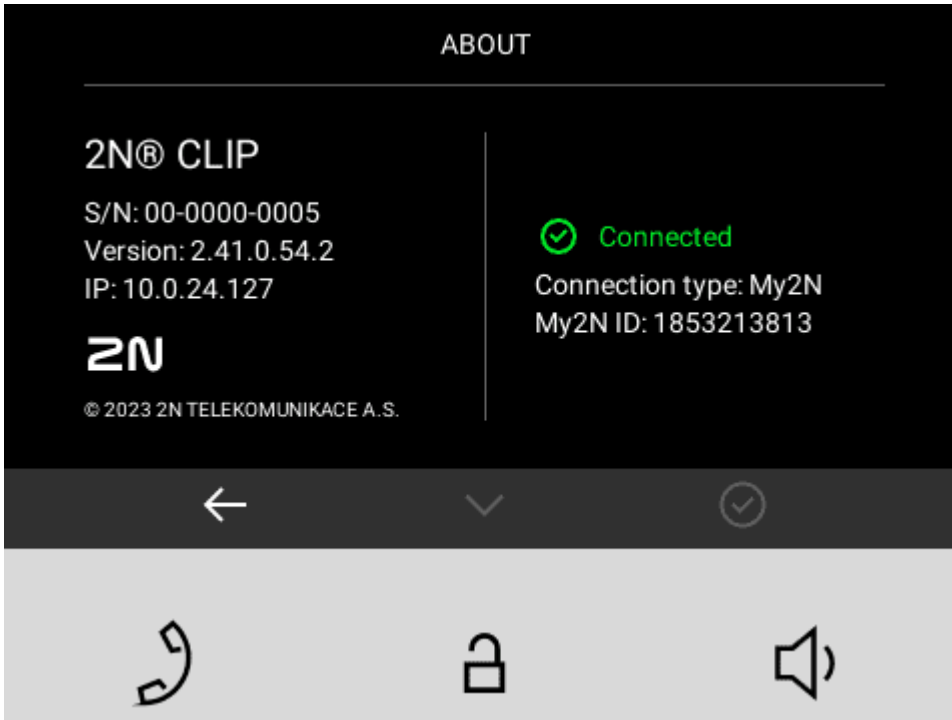
IP Address Retrieval Using Hardware

Follow the instructions below to retrieve the current IP address:

1. Press and hold the RESET button.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
3. Release the RESET button.
4. The device announces the current IP address via the speaker automatically.
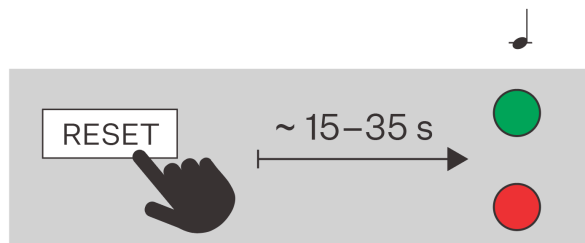
> **NOTE**
> The delay after pressing RESET till the first light and sound signaling is set to 15–35 s depending on the device model used.

Firmware Update

We recommend that the firmware is also updated during the **2N Clip** installation. Refer to 2N.com for the latest FW version. Refer to Maintenance (p. 47) for the firmware upgrade procedure.

> **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. 53) 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. 9).

The Home screen (p. 53) is displayed after restart. Restarting may take a rather long time after the button press.

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. 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. 20) for login details. Restart the device in System > Maintenance (p. 47) > System using Restart .

The Home screen (p. 53) is displayed after restart. Restarting may take a rather long time after the button press.

Factory Default Reset

Follow the instructions below **2N Clip** to reset the factory default values:

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

3. Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
4. 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).

5. Wait until the red LED goes off and the acoustic signal can be heard ♩♩♩♩ (approx. for another 3 s).
6. Release the RESET button.
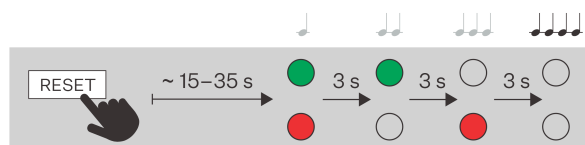
Call Connection

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 Add device 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. Select the type of call:
   - "SIP" for calls via SIP
   - "rava" for calls with Creston
   - "vms" for calls with Axis Camera Station
   - "device" for calls with a local 2N device

4. 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 interface.

5. 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

6. Make sure that the call transmitting service is enabled on the called 2N device to make a successful call.

Configuration

2N Clip can be configured by software via the configuration web interface or by hardware using the RESET button. Hardware configuration is used for basic settings only.

Basic Configuration via Hardware

Where software configuration is unavailable, make basic settings using the RESET button (refer to 1).
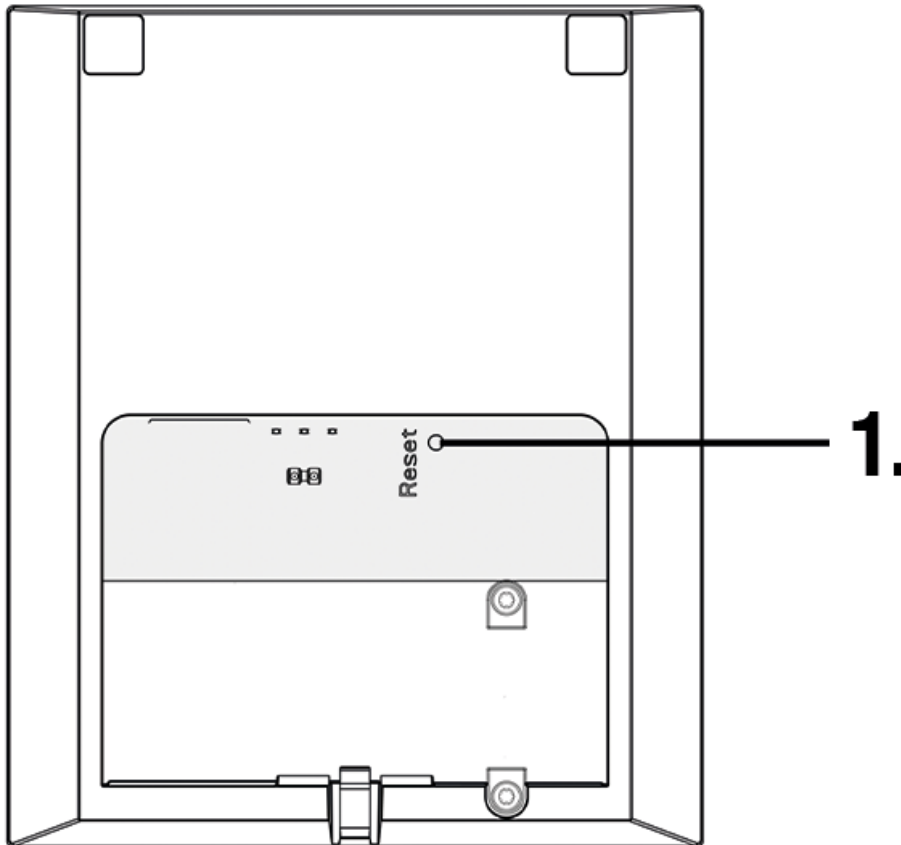
The RESET button helps you reset the factory default values, restart the device, retrieve the device IP address and switch the IP address static/dynamic mode.

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 and hold the RESET button.

2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
3. Release the RESET button.
4. The device announces the current IP address via the speaker automatically.
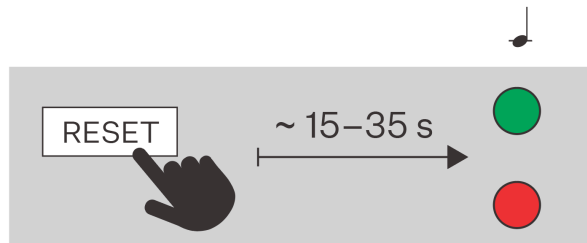
NOTE
The delay after pressing RESET till the first light and sound signaling is set to 15–35 s depending on the device model used.

Static IP Address Setting

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

1. Press and hold the RESET button.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
3. Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
4. Release the RESET button.
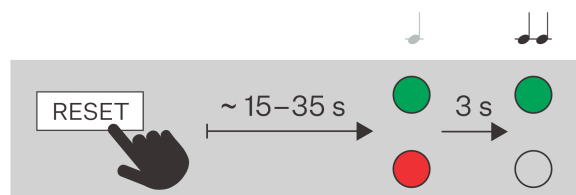
> **NOTE**
>
> The following network parameters will be set after restart:
>
> - IP address: 192.168.1.100
> - Network mask: 255.255.255.0
> - Default gateway: 192.168.1.1

Dynamic IP Address Setting

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

1. Press and hold the RESET button.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
3. Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
4. 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).
5. Release the RESET button.

Factory Default Reset

Follow the instructions below **2N Clip** to reset the factory default values:

1. Press and hold the RESET button.
2. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
3. Wait until the red LED goes off and the acoustic signal can be heard ♩♩ (approx. for another 3 s).
4. 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).
5. Wait until the red LED goes off and the acoustic signal can be heard ♩♩♩♩ (approx. for another 3 s).
6. Release the RESET button.

Software Configuration

The start screen is displayed upon login to the web interface **2N Clip**. Press ⬅ in the left-hand upper corner on each of the following web interface pages to return to this screen anytime. The screen header includes the device name (refer to the Display Name parameter in Services > Phone > SIP) (p. 35).

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** configuration sections.

Section   **Folder**

Menu

Block

Device Configuration Interface Access

2N Clip is configured via the administration web interface. Connect the device to the LAN IP and make sure it is properly powered. You have to know the IP address for access.

Domain Name

Enter the domain name as "hostname.local". The new device Hostname consists of the device name and serial number. See below for the device name formats in Hostname. The serial number is entered without hyphens. You can change Hostname in System > Network later.

Ddefault domain name 2N Clip: 2NClip-{serial number without dashes}.local (e.g.: "2NClip-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** address or domain name into the internet browser.
   The login screen is now displayed.
   Should the login screen fail to appear, you must have typed a wrong IP address, port, domain name or the administration web server has been switched off. If you do not have a certificate generated for the IP address or domain name, an invalid security certificate warning may be displayed. In this case, you need 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**

State

The Status menu provides clear status and other essential information on the device. The section includes the following menus:

- Device (p. 31)
- Services (p. 31)
- Call Log (p. 31)
- Events (p. 31)

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 – 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 Log

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

- contact type,
- called/calling user ID,
- 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.
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 ...).
LoginBlocked	Event generated after 3 wrong logins to the web interface. Contains information about IP address.
RegistrationStateChanged	Change of the SIP Proxy registration state.

Directory

Directory is one of the crucial parts of the device configuration. It helps you add new devices (2N IP intercoms, answering units, etc.). 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, ![icon] feature icon of the device to which an alarm call will be set up after the doorbell button is pressed). One list page can display 15, 25 or 50 devices.

Using the ![icon] icon, it is possible to export/import from/into the device a CSV file including a user list. If the directory is empty, a file is exported with the header only (in English) to be used as a user importing template. If an empty file with the header only is imported and Replace directory is selected, the whole directory is deleted. Up to 10,000 users can be imported depending on the device type.

> **CAUTION**
>
> - Special users such as those created by My2N or 2N Access Commander are not part of the directory export.
> - While editing the CSV file using Microsoft Excel, remember to save the file in the CSV UTF-8 format (with separators).

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_name" for calls to the 2N IP Mobile application. Set the device name in the mobile application. Enter /1 or /2 behind the phone number to specify which SIP account shall be used for outgoing calls (account 1 or 2). Enter /S or /N to force an encrypted or unencrypted call respectively. The account and encryption selections can be combined into the suffix /1S, for example.

Press ![icon] 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, the URI is completed with the data from the SIP account settings. Further settings include direct SIP calls (sip:), 2N local calls (device:), Crestron calls (rava:) or calls with video management systems, 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.

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 HW > Digital inputs (p. 41) > Doorbell button.

Unlock Button Function

Unlock Code – 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. The supported characters also include * or #. Four characters at least are recommended.

Calling

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

The Call section consists of the following menus:

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

Call Receiving Mode (SIP 1/2, SIP 2) – 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 Answering** – 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.

Local Call Receiving Mode – set the way of receiving incoming local calls.

- **Always busy** – the device rejects incoming calls.
- **Manual Answering** – 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 is only set for SIP 1 but 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 is only set for account 1 but applies to both the SIP accounts.

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

SIP 1 / SIP 2

2N Clip 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 Enable – 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).

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

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

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 Expires – 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 (Unregistered, Registering..., Registered, Unregistering...).

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.

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. The default value is 5060.

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 Keep Alive Packets – set that the device shall inquire periodically about the state of the called station via SIP OPTIONS requests during the call (used for station failure detection during the call).

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.

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 is 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.

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 is only set for SIP 1 but 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 is only set for account 1 but applies to both the SIP accounts.

Broadsoft Compatibility Mode – 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.

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
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 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.

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

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

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.

Services
The Services section includes the following menus:

- Unlocking (p. 38)
- User Sounds (p. 38)
- Web Server (p. 39)

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

Unlocking 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 Timeout – end the call when the door unlocking request sending timeout has elapsed.

User Sounds
2N Clip 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 Signaling** – 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 (intercom ringtone).
- **Doorbell** – set the sound to be played when the door button is pressed.

Web Server

2N Clip 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 ![pencil] 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 User 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.

User Language – upload ![upload], download ![download] and/or remove ![remove] user files including translations of the user interface texts.

Hardware

The Hardware section provides the device hardware settings and includes the following menus:

- Audio (p. 40)
- Display (p. 40)
- Digital Inputs (p. 41)

Audio

2N Clip is equipped with a speaker. Set the phone call and state signaling volume control in this configuration section.

Master Volume (adjusted using) controls the general device volume affecting both the call volume and the signaling tone volume. Consider the noise level of the ambient environment while setting this parameter.

Phone Call Volume

Call Volume – set the phone call volume.

Ringtone Volume – set the incoming call ringtone volume.

Call Progress Tone Volume – set the dialtone, ringtone and busy tone volume levels. In case the call progress tones are automatically generated by the PBX, this setting will not be applied.

Signaling Volume

Key Beep Volume – set the key beep volume. The volume values are relative against the set master volume.

Warning Tone Volume – set the volume of warning and signaling tones. The volume values are relative against the set 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.

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. 41)), 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

Display Backlight Intensity – 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

Original language – download a localization file template for a translation of your own. It is an XML file with all the texts to be displayed in English.

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 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 for alarm call activation.

System

The System section includes the following menus:

Network

2N Clip 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. for details.

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

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 Identification

Hostname – set the device LAN identification.

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

VLAN Settings

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

VLAN ID – choose a VLAN ID from the range of 1–4094. The device shall only receive packets with the set ID. An incorrect setting may result in a connection loss and subsequent factory reset (p. 28).

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.

802.1x

Device Identity

Device identity – username (identity) for authentication via EAP-MD5 and EAP-TLS.

MD5 Authentication

Authentication enabled – 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 enabled – 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. 44). 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. 44).

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. 44). If no trusted certificate is included, the RADIUS public certificate is not verified.

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

Date and Time

2N Clip is equipped with a real time clock without power outage backup. Select Use Time from Internet (p. 0   ) to synchronize the device time with the Internet time or click Synchronize with Browser to synchronize time with your current PC time.

> **(i) NOTE**
>
> The device does not need the current date and time values for its basic function. .

> **(!) CAUTION**
>
> It is recommended that the Use time from Internet (p. 0   ) 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.

Current Time

Use time from 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 Display – 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 (p. 0   ) is disabled.

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

Functions

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

The list includes:

• function name,
• function status (started/stopped),
• event 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.

> **ℹ 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** 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.
3. 802.1x (EAP-TLS)
4. 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 . 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.

> **ℹ 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.

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 Status – 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.

Syslog Capture Time – display how long Syslog messages are captured in the Syslog folder.

Size of Captured Packets – 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 .

> ⚠ **CAUTION**
> The start of diagnostic data capture restarts the packet capture if running.

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 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.

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.

Backup 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.

Reset Configuration – reset all the device parameters except for the LAN parameters. To reset the device completely, use the appropriate jumper or press Reset.

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 State – 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.

Restart – 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.

Third Party Library Licenses – 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	Proto-col	Direc-tion	On by default	Config-urable	Settings
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device discov-ery)*	8002	UDP	In/Out	✓	×	–
HTTP	80	TCP	In/Out	✓	✓	Web Server (p. 39)
HTTPS	443	TCP	In/Out	✓	✓	Web Server (p. 39)
Multicast audio for ICU protocol	8006	UDP	In	✓	×	–
Multicast video for ICU protocol	8008	UDP	In	✓	×	–
Multicast video (wide) for ICU protocol	8016	UDP	In	✓	×	–
NTP client	123	UDP	In/Out	✓	×	—
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	×	✓	Calling (p. 34)
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	Calling (p. 34)

Service	Port	Proto-col	Direc-tion	On by default	Config-urable	Settings
SIPS	5061	TCP	In/Out	×	✓	Calling (p. 34)
Syslog	514	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	10080	TCP	Out	✓	×	–
Unitchannel	8011	UDP	In/Out	✓	×	–
Sitechannel (ICU pro-tocol)	8004	UDP	In/Out	✓	×	–
CWMP Stun	3478	UDP	Out	×	✓	Auto Provi-sioning (p. 45)

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. 58) is displayed.
🔓 a 🔊	Simultaneous long press of both buttons	Device Lock (p. 62) is activated.
) and 🔓	Simultaneous long press of both buttons	Settings Menu (p. 56) 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. 32).

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. 56),
- Ringtone Setting Menu (p. 58),
- Calls (p. 60),

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. 40) – 12h or 24h.
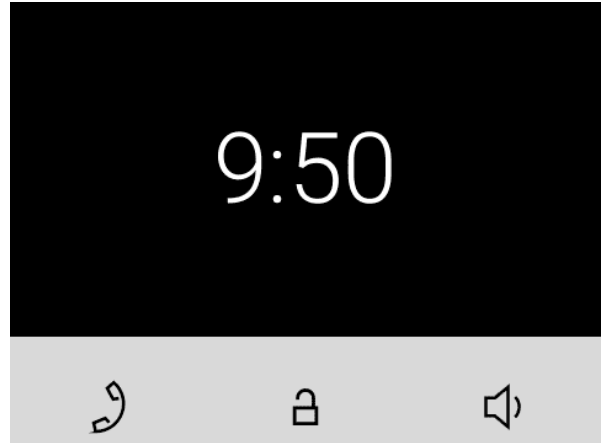
The home screen provides access to:

- Ringtone Setting Menu,
- Directory,
- Settings.

Possible actions	Performance	Action result
Display of Ringtone Setting Menu	Long Button Press	Ringtone Setting Menu (p. 58) is displayed.
Settings Menu Display	Simultaneous long press of and	Settings Menu (p. 56) is displayed on the device.

Directory Menu

If 2 or more devices are added to **2N Clip**, 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. 32).
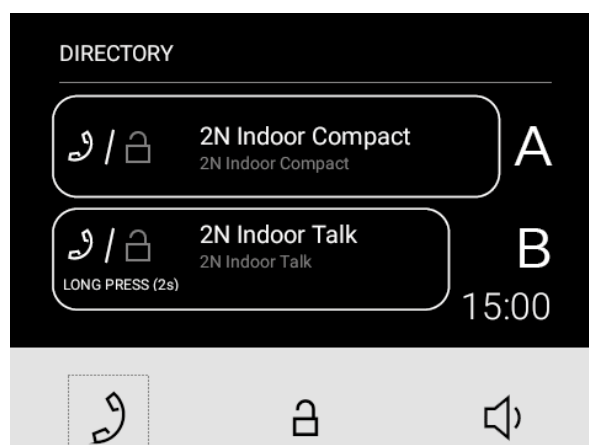
The Directory menu includes a list of added devices and available actions. If a call is missed from a displayed device, the missed call icon ↲ appears at the respective device. The icon disappears when any action is performed from the home screen.

The Directory menu shows all the actions included in Subs. Home Screen (p. 53).

> ⓘ **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 A unlocking	Short press of 🔓	Device A lock is unlocked.
Device B unlocking	Long press 🔓	Device B lock is unlocked.
Settings Menu Display	Simultaneous long press of ☎ and 🔊	Settings Menu (p. 56) is displayed on the device.
Device lock activation	Simultaneous long press of 🔓 and 🔊	Device Lock (p. 62) is activated.
Display of Ringtone Setting Menu	Long press of ☎	Ringtone Setting Menu (p. 58) 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. 21), etc.),
- change the device language,
- restart the device (p. 23),
- 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. 62),
- activate the Device lock (p. 62).

ⓘ **NOTE**
Use the Display (p. 40) 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.
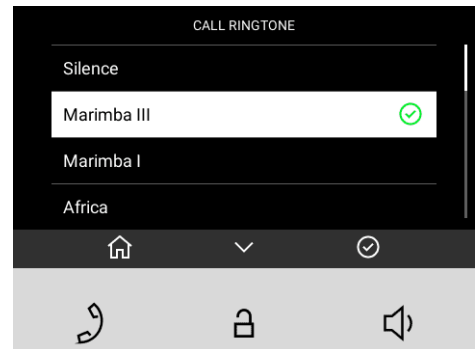
Possible actions	Performance	Action result
Return to home screen	by a short press of ☏ , or in 10 seconds without any button being pressed, or after a call if any.	The selection is cancelled and the menu actions are terminated without saving.
Back (return to preceding action)	Short press of ☏	Navigation to the preceding menu section.
Selection confirmation	Short press of ◁	Confirmation of the selected setting option or transition to the selected menu section.
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. 53) 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.

A simultaneous press of the 🔊 and 🔊 buttons for 3 seconds puts the device in the Ringtone Setting menu.

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. 53) is displayed.
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. 53) is displayed.

Operational Statuses

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

-

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.
	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 Basic Configuration via Hardware (p. 26).
	Approaching call end signaling The device allows you to set a call end timeout, refer to General Settings (p. 34).
	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** 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 in the LANis 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** answering unit.
- **Incoming** trying to establish connection with the **2N Clip** answering unit.
- **Active call** – if connection between the devices is established, sound is transmitted.
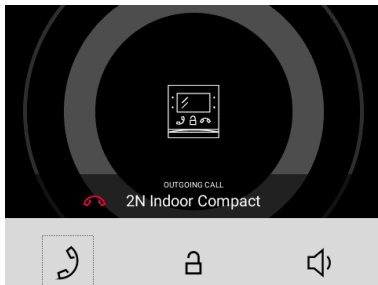
Outgoing Call
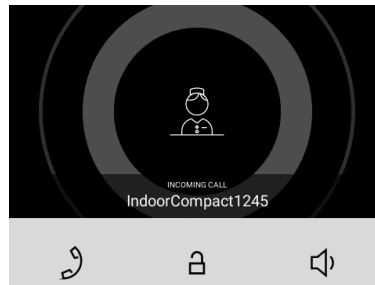
Incoming Call

Active Call

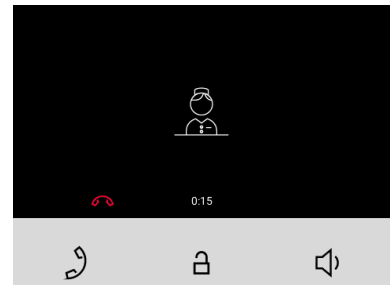| Possible ac-tions	Perform-ance	Action result
Incoming call receiving	☏	Connection with the other device has been established, a call is in progress. The call cannot be ended until answered.
End of call	☏	The active call is interrupted. The call cannot be ended until answered.
Target device lock opening	🔓	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. Door unlocking is signaled by a tone and green flash of the lock but-ton. After unlocking, automatic call ending can be set in the Unlocking (p. 38) web configuration .
Call volume control	🔊	Volume increase by one level (after the upper limit is reached, volume goes to the lowest value – value rotation)
Ringtone Dis-able	🔊	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 transits into the Idle mode after a set inactivity period. Set the inactivity timeout in Display (p. 40) > Backlight of the web configuration or through the device control settings in Settings Menu (p. 56). The operation power consumption is reduced in the Idle mode.

The device shows no information on the display in the Idle mode.
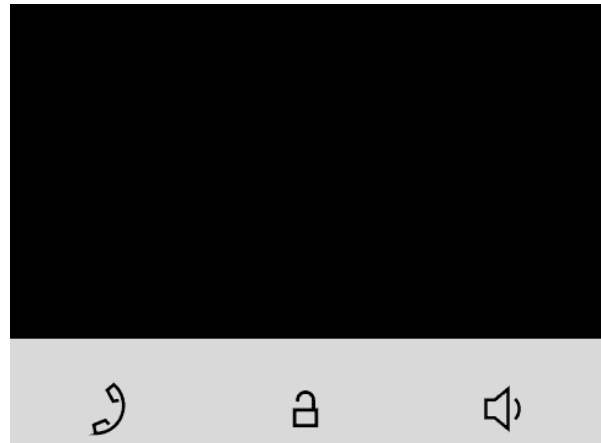
Possible actions	Performance	Action result
Idle mode end		
	Press any key	The device quits the Idle mode. The Directory Menu (p. 54), Home Screen (p. 53) or Device Lock (p. 62)is displayed.

Device Lock

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. 40) web configuration menu.

Device locked

15:16
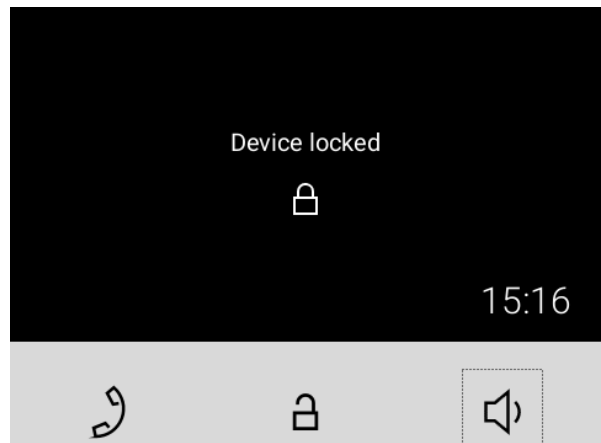
Enable the Device lock option in the Settings menu or in the web configuration interface.

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

64

If used frequently, the device surface gets dirty. Use a piece of soft cloth moistened with clean water to clean the device.

It is recommended that the principles below are followed while cleaning:

- Use appropriate cleaning agents suitable for glasses, optical devices, screens, etc.
- Alcohol-based cleaners may not be applied.
- We recommend that IT cleaning wipes are used.

> ⚠ **CAUTION**
> Do not use aggressive detergents (such as abrasives or strong disinfectants).

Troubleshooting

65

Refer to faq.2n.cz for the most frequently solved problems.

Technical Parameters

Supply type
PoE, IEEE 802.3af, Class 0 (0,44–12,95 W)

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 kapacitní tlačítka
Display	4" with 480 x 272 pixel resolution

Signaling protocol	
SIP	UDP, TCP, TLS

Technical Parameters

Audio	
Microphone	Integrated
Speaker	3 Wintegrated
Induction loop output	NO (induction loop integration depends on the product version)

Audio stream	
Prootocols	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	
LAN	10/100BaseT, RJ-45; Cat5e or higher

Doorbell input	
Input type	Switching contact (button/relay)
Contact type	Normally open (NO)
Contact parameters	Min. 120 V / 20 mA, DC

Mechanical Parameters	
Dimensions (w x h x d)	124 x 150 x 26 mm
Weight	295 g
Operating temperature	0 to 50 °C
Relative humidity	10 to 90 % non-condensing
Storing temperature	−20 °C to 70 °C
Recommended altitude	0 to 2000 m

Directives, Laws and Regulations - General Instructions and Cautions

2N Clip conforms to the following directives and regulations:

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

Industry Canada

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

FCC

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

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

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

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

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

⚠ **WARNING**

In order to ensure the full functionality and guaranteed performance, we strongly recommend that the topicality of the product / device version in use be verified as early as in the installation process. The customer hereby acknowledges that the product / device can achieve the guaranteed performance and full functionality pursuant to the manufacturer's instructions only if the latest product / device version is used after having been tested for full interoperability and not having been determined by the manufacturer as incompatible with certain versions of other products, and only in conformity with the manufacturer's instructions, guidelines or recommendations and in conjunction with suitable products and devices of other suppliers. The latest versions are available at https://www.2n.com/cs_CZ/ or can be updated via the configuration interface if the devices are adequately technically equipped. Should the customer use a product / device version other than the latest one or a version determined by the manufacturer as incompatible with certain versions of other products, or should the customer use the product / device in contradiction to the manufacturer's instructions, guidelines or recommendations or in conjunction with unsuitable products / devices of other suppliers, the customer is aware of and agrees with all functionality limitations of such a product / device if any as well as with all consequences incurred as a result thereof. Using a product / device version other than the latest one or a version determined by the manufacturer as incompatible with certain versions of other products, or using the product / device in contradiction to the manufacturer's instructions, guidelines or recommendations or in conjunction with unsuitable products / devices of other suppliers, the customer agrees that the 2N TELEKOMUNIKACE a.s. company shall not be held liable for any functionality limitation of such a product or any damage, loss or injury related to this potential functionality limitation.

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.

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

wiki.2n.com

2N Clip – User Manual

© 2N Telekomunikace a. s., 2024

2N.com