2N

2N Indoor View Wi-Fi

User Manual

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 Indoor View Wi-Fi** product, outline its application options and highlight the advantages following from its use.

Basic Features

2N Indoor View Wi-Fi is an internal IP/SIP unit providing audio and video communication with the 2N IP intercoms.

The device includes a panel with a 3 mm thick hardened glass touchscreen, Speakerphone, high-quality microphone with excellent audibility and intelligibility properties, Ethernet and Wi-Fi interface for LAN connection and induction loop, external power supply and doorbell connectors. **2N Indoor View Wi-Fi** is a top-quality and easy to install and configure indoor answering unit. One installation can combine variable answering units manufactured by 2N Telekomunikace a.s.

2N Indoor View Wi-Fi is equipped with a specific user interface for an increased user comfort and safety.

Basic Features **2N Indoor View Wi-Fi**:

- 7" color LCD video display,
- full duplex handsfree HD audio communication
- LAN interface with PoE supply option ,
- Wi-Fi interface for wireless LAN connection
- easy flush mounting
- remote administration and configuration via **2N Remote Configuration**,
- call setup option via **2N Mobile Video** on a smartphone,
- Do Not Disturb Mode
- device lock,
- remote door lock control
- time display,
- current weather display,
- integrated administrator web interface,
- external power supply input
- Induction loop output,
- external doorbell button input.

Product Versions

Part No.: 91378611WH

Axis Part No. 03135-001

2N Indoor View Wi-Fi

White version

Part No.: 91378611

Axis Part No. 03134-001

2N Indoor View Wi-Fi

Black version

Accessories for Installation

Choose the proper a mounting box depending on your particular installation needs.
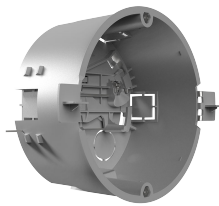
Axis Part No. 01700-001

Mounting box

Wall/plasterboard flush mounting box for 2N indoor answering units.

Not included in the package of **2N Indoor View Wi-Fi**.

Axis Part No. 02320-001

Wall mounting box

Wall surface mounting box for 2N indoor answering units.

Not included in the package of **2N Indoor View Wi-Fi**.
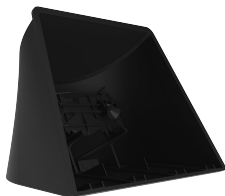
Axis Part No. 02039-001

Stand

Stand for 2N indoor answering units.

Not included in the package of **2N Indoor View Wi-Fi**.

Package Completeness Check

Please check the product delivery before installation. Contents:

1x	**2N Indoor View Wi-Fi**
2x	External power and doorbell button terminals
1x	Certificate of ownership
1x	2.5 mm hexagon key wrench
1x	Quick Start manual
1x	Display cleaning cloth

Component Layout

Front
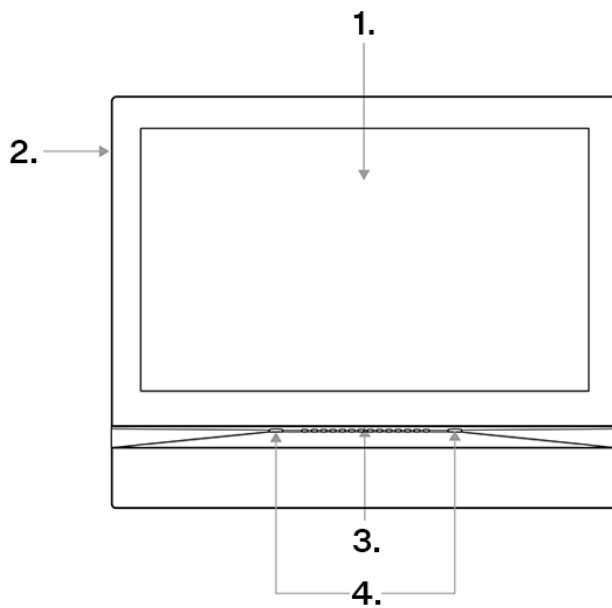
1. Display
2. Microphone
3. Speaker
4. Anchoring holes

Rear
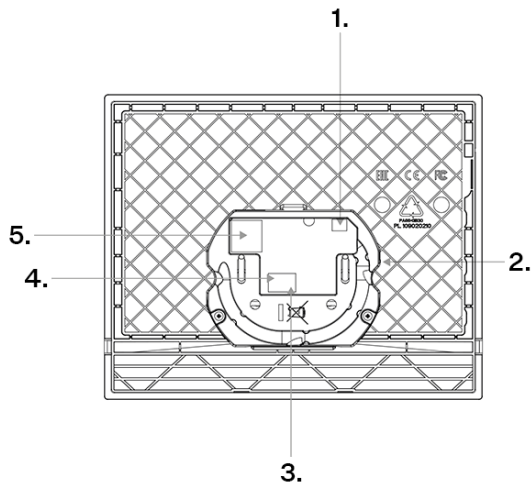
1. External induction loop output
2. RESET Button
3. Doorbell button input
4. 12 V / 1 A DC power supply input
5. Ethernet

Mechanical Installation

This subsection provides the **2N Indoor View Wi-Fi** installation and connection instructions.

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

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

Installation Conditions

- 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. 82).
- 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.
- It is recommended that the power adapter be connected to the mains via a UPS and reliable overvoltage protection.

> ⚠ **CAUTION**
>
> This device and its installation and configuration techniques are not intended for persons with diminished physical, sensory or mental capacities or persons with limited experience and knowledge unless expertly supervised or duly advised as to the use of this device by a person responsible for their safety.

Wall Installation

2N Indoor View Wi-Fi is designed for flush mounting (brick, plasterboard, wood). Use the flush mounting box (Part No. 91378800), which is not included in the package. Alternatively, the product can be surface installed in a wall box (Part No. 91378803) or mounted into a desk stand (Part No. 91378802).

-
  Flush mounting using a walled-in mounting box
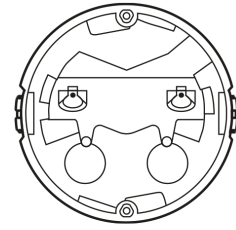
-
  On-wall mounting using a wall surface mounting box

Flush Mounting

Flush Mounting Box Installation

> ⚠️ **CAUTION**
> Before starting the mechanical installation on a selected place, make sure carefully that the preparations associated with it (drilling, wall cutting) cannot damage the electrical, gas, water and other existing wires and pipes.

1.

2a.

2b.

3.
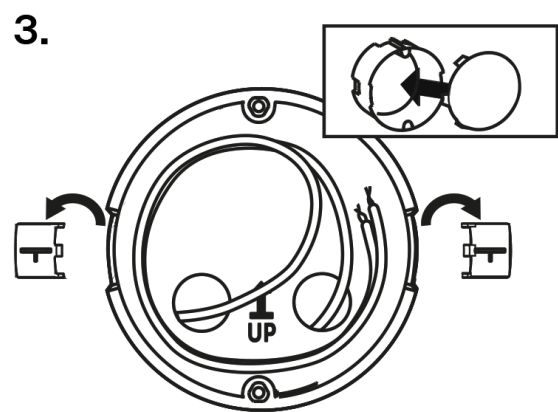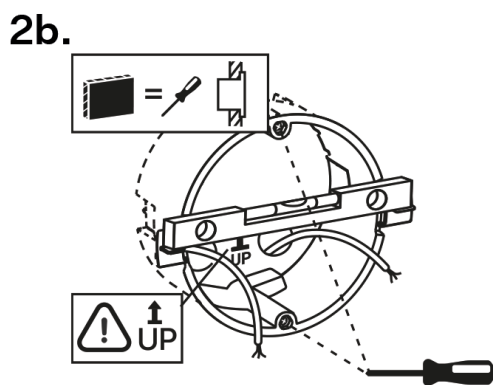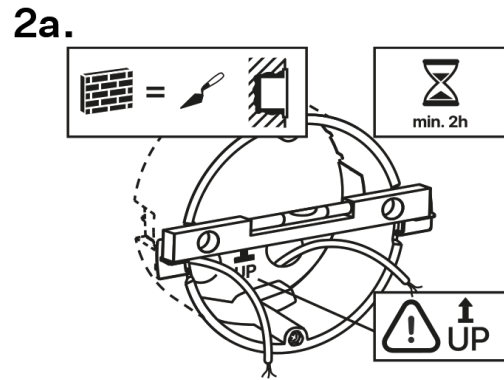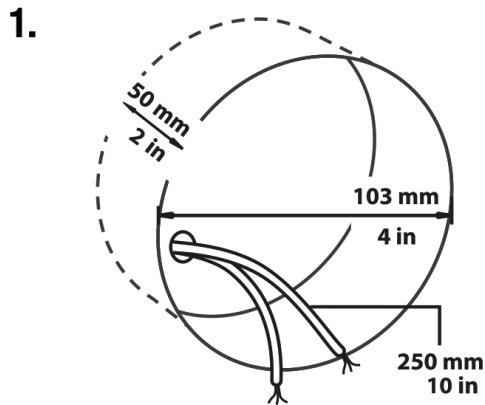
1. Cut a circular hole in the wall of the diameter of 103 mm and depth of 50 mm before installation. It is assumed that all necessary cables of the maximum length of 25 cm will lead to the hole.

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

2. Put the flush mounting box in the hole to make sure that the hole is deep enough.
3. If the hole complies with the box size, wall in the box and level the box using a water level on the holding clips.
4. When the mortar hardens, break off the clips and cap the box with the cover provided. Use anchoring elements to fix the device into plasterboard.

To install **2N Indoor View Wi-Fi** into a flush mounting box, get a 2.5 mm hexagon key wrench, which is included in the package.

> **NOTE**
> When installing **2N Indoor View Wi-Fi** into a wall, take the local standards related to installation of electrical devices on flammable material into consideration.

Flush Mounting Box Device Installation

> **TIP**
> Refer to Subs. Component Layout (p. 7) for connector layout.

1.

2.
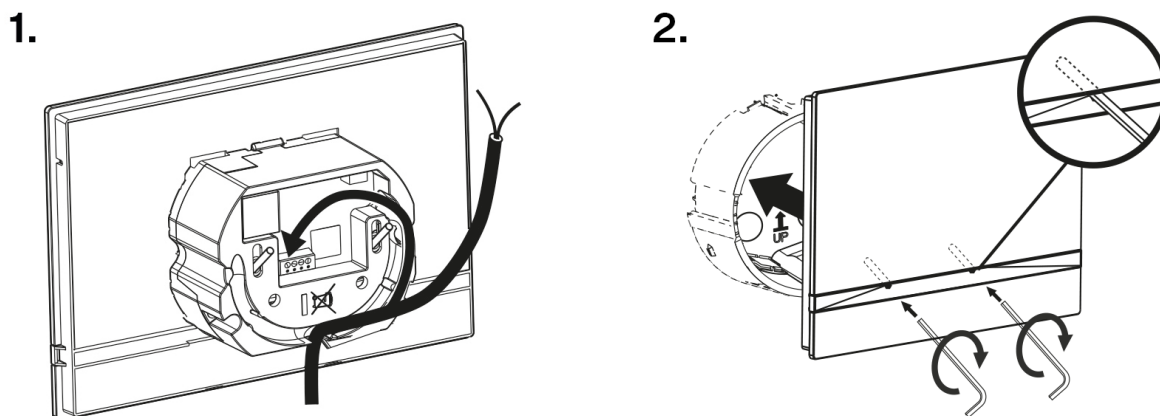
1. Remove the cover from the walled-in mounting box. Remove the pre-prepared cabling, UTP cable, doorbell twin cable and power supply cable.
2. Shorten the cables to 150 mm or less as required. Connect the doorbell twin cable or power supply cable to the connector provided.
3. For connection via Ethernet.
   Crimp the RJ-45 connector onto the UTP cable.
4. Take **2N Indoor View Wi-Fi** and lean its bottom edge against the wall below the flush mounting box.
5. First connect the green power supply/doorbell connector to the device.
   For connection via Ethernet.
   Connect the LAN connector.
6. Put the cables carefully in the pre-drilled back slot of the device to prevent them from blocking any horizontal levelling movement during the final installation stage.
7. Insert the device in the flush mounting box making sure that it clicks onto the centering pins. The pins allow for a 5–6 ° inclination on either side for accurate horizontal levelling of the device.
   Now the device is ready for basic operation. It is necessary to perform software configuration (p. 27) to achieve a full functionality of the device.

Wall Mounting Box Installation for Device Wall Mounting

2N Indoor View Wi-Fi can be installed using a wall mounting box. The device display slope is 12% in this type of installation. Use the mounting box (Part No. 91378803), which is not included in the package.

> **TIP**
> - Download the Drilling template from 2N.com.
> - Refer to Subs. Component Layout (p. 7) for connector layout.

1.

2.

3.

4.
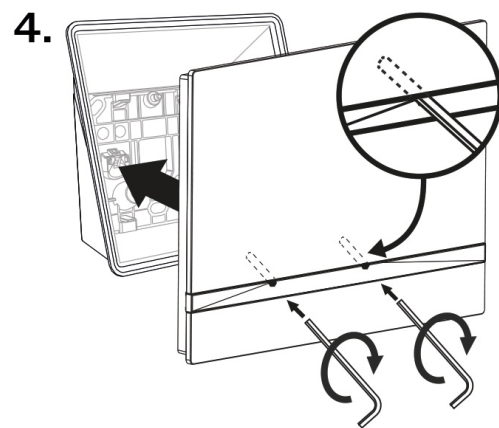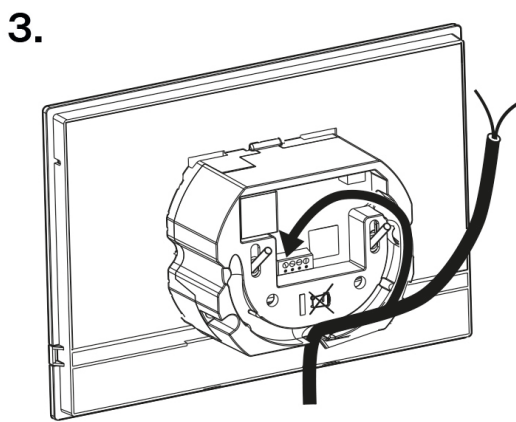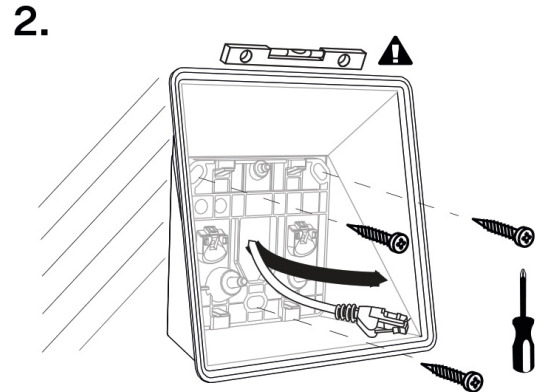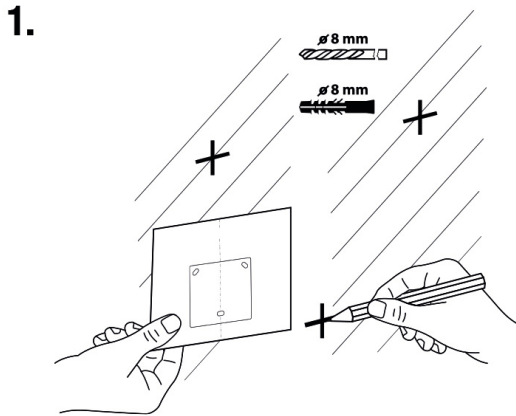
1. Drill holes of the diameter of 8 mm for the dowels and screws (included in the package). It is assumed that all the necessary cables of the maximum length of 25 cm will lead to the place.
2. Fit the wall mounting box into the predrilled holes. Pull the available cables through the box opening. Use a water level for a more precise levelling.
3. First connect the green power supply/doorbell connector to the device.
   For connection via Ethernet.
   Connect the LAN connector.
4. Put the cables carefully in the pre-drilled back slot of the device to prevent them from blocking any horizontal levelling movement during the final installation stage.
5. Fit the device screws into the nuts in the box with the hexagon key wrench provided.
   Now the device is ready for basic operation. It is necessary to perform software configuration (p. 27) to achieve a full functionality of the device.

Stand Installation

Within installation preparations, take out the pre-prepared cabling, UTP cable, doorbell (twin) cable and power supply. Shorten the cables as required. Crimp the RJ-45 connector onto the UTP cable. Connect the doorbell twin cable or power supply into the connector.

> **TIP**
> Refer to Subs. Component Layout (p. 7) for connector layout.

1.

2.

3.

4.
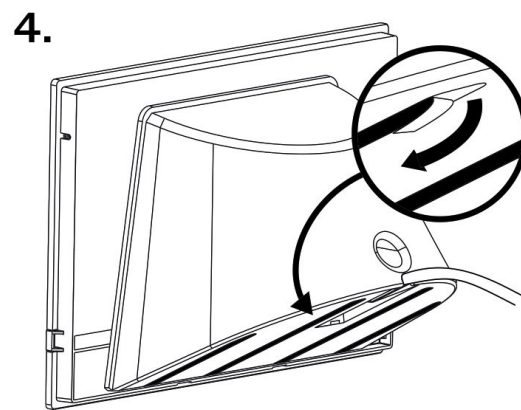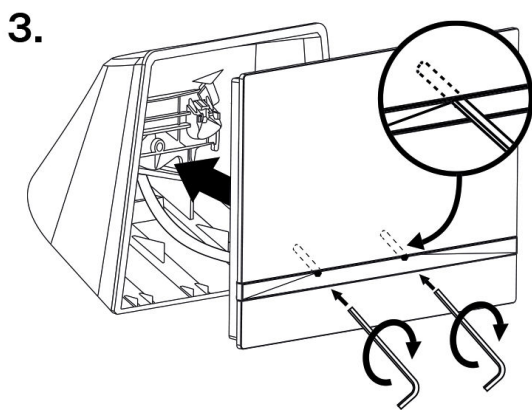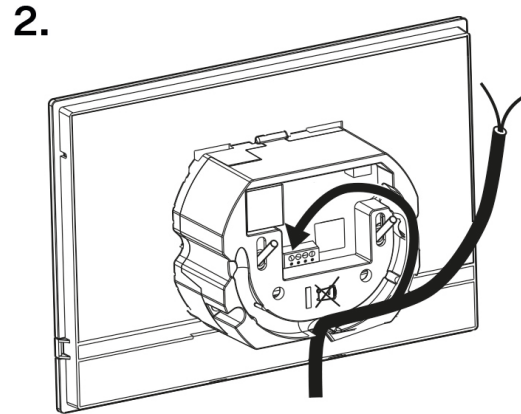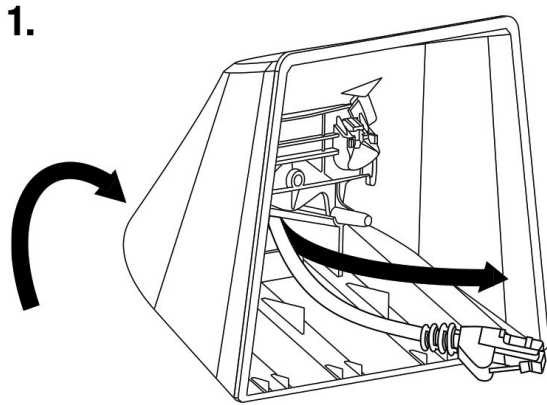
1. Pull the cables through the hole in the stand bottom.
2. First connect the green power supply/doorbell connector to the device.
    For connection via Ethernet.
    Connect the LAN connector.
3. Put the cables carefully in the pre-drilled back slot of the device to prevent them from blocking any horizontal levelling movement during the final installation stage.
4. Put the device on the stand making sure that it fits onto the centering pins. The alignment of the stand bottom edge and the device bottom strip means that the device is installed properly. Fit the device to the stand by tightening the screws through the front side. Use a hexagon key wrench for tightening. Tighten the screws gently.
5. Remove the protective foil from the antislip belts on the stand bottom and install the device on a selected place.
    Now the device is ready for basic operation. It is necessary to perform software configuration (p. 27) to achieve a full functionality of the device.

Power Supply

Power supply must comply with PS1 class output.

You can feed **2N Indoor View Wi-Fi** as follows:

1. Using a 12 V / 1 A DC power adapter connected to the backside terminal board.
2. Use an Ethernet cable connected to a PoE supply or PoE supporting Ethernet switch/router.

It is recommended that the power adapter be connected to the mains via a UPS and reliable overvoltage protection.

2N Indoor View Wi-Fi Consumption Table:

Supply type	Consumption	Polarity reversal protection
PoE, IEEE 802.3af	12 W	✓
12 V DC ±10 % adapter; 1 A (recommended)	12 W	✓

⚠ **WARNING**

- Connection of a defective or improper power supply may lead to a temporary or permanent device failure.
- If you use a power adapter other than the recommended one, do not exceed the 12 V rated supply voltage. Also check the supply voltage polarity. Higher voltage values or misconnections may result in an irreplaceable device damage.

ⓘ **CAUTION**
Make sure that the external power supply meets the power supply class 2 (PS2/LPS) .

PoE Supply Connection

Use a standard straight RJ-45 terminated cable to connect **2N Indoor View Wi-Fi** 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.

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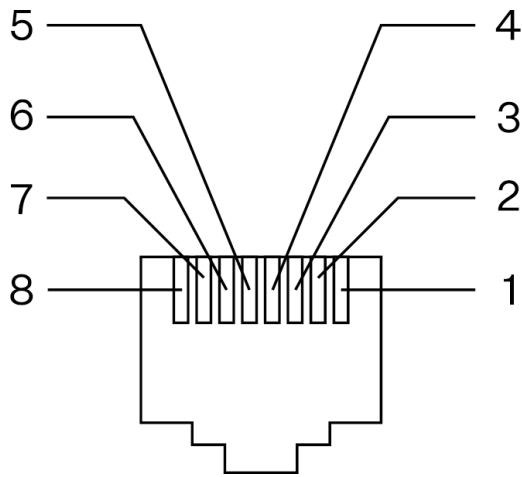
Ethernet socket
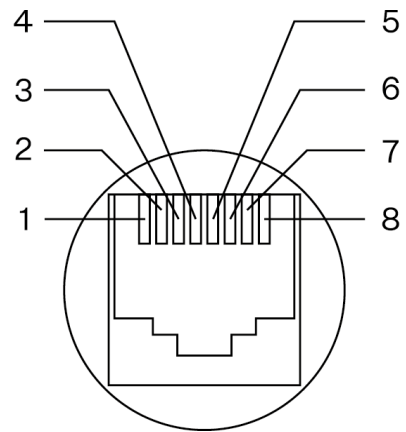
1. Tx+
2. Tx-
3. Rx+
4. unused
5. unused
6. Rx-
7. unused
8. unused

⚠️ **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 Indoor View Wi-Fi is configured via the web configuration interface. You have to know the device IP address portal or the device domain name. Make sure that the device is connected to the local IP network and powered.

Domain Name

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

Default domain name 2N Indoor View Wi-Fi: 2NIndoorViewWiFi-{serial number without dashes}.local (e.g.: "2NIndoorViewWiFi-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 Indoor View Wi-Fi** address or domain name into the internet browser.
    The login screen is now displayed.
    If the login screen is not displayed, check the IP address, port or domain name for validity. The login screen is not displayed if the web interface server is off. If no certificate has been generated for the IP address or domain name, a security certificate invalidity notification may appear. In that case, confirm that you want to go to the web configuration interface.
2. Enter the login data.
    The default login data are:
    Username: **Admin**
    Password: **2n**
    It is necessary to change the password immediately upon the first login.
    After login using the default password, the access to the web configuration interface functions is limited.

> **TIP**
>
> It is recommended that a password is used that is difficult to break. It is not recommended that names, places or things, especially those closely related to the user, are used in the password.
>
> For increased password security, it is recommended that:
>
> - the random password generator is used,
> - the password length is 12 characters at least,
> - various characters from different character sets are combined (small/capital letters, digits, special characters, etc.).

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 Scanner list to access the device web interface easily.
> - To change the device IP address, select *Config* and enter the required static IP address or activate DHCP.

The default login data are:

Username: **Admin**

Password: **2n**

It is necessary to change the password immediately upon the first login.

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

> **TIP**
> It is recommended that a password is used that is difficult to break. It is not recommended that names, places or things, especially those closely related to the user, are used in the password.
>
> For increased password security, it is recommended that:
>
> - the random password generator is used,
> - the password length is 12 characters at least,
> - various characters from different character sets are combined (small/capital letters, digits, special characters, etc.).

IP Address Retrieval using Device Display

To find the device IP address using the display, press any to quit the Idle mode. The Settings menu is displayed on the home screen the setting icon ⚙ in the right-hand bottom corner buttons. Find the IP address information in the About device menu.
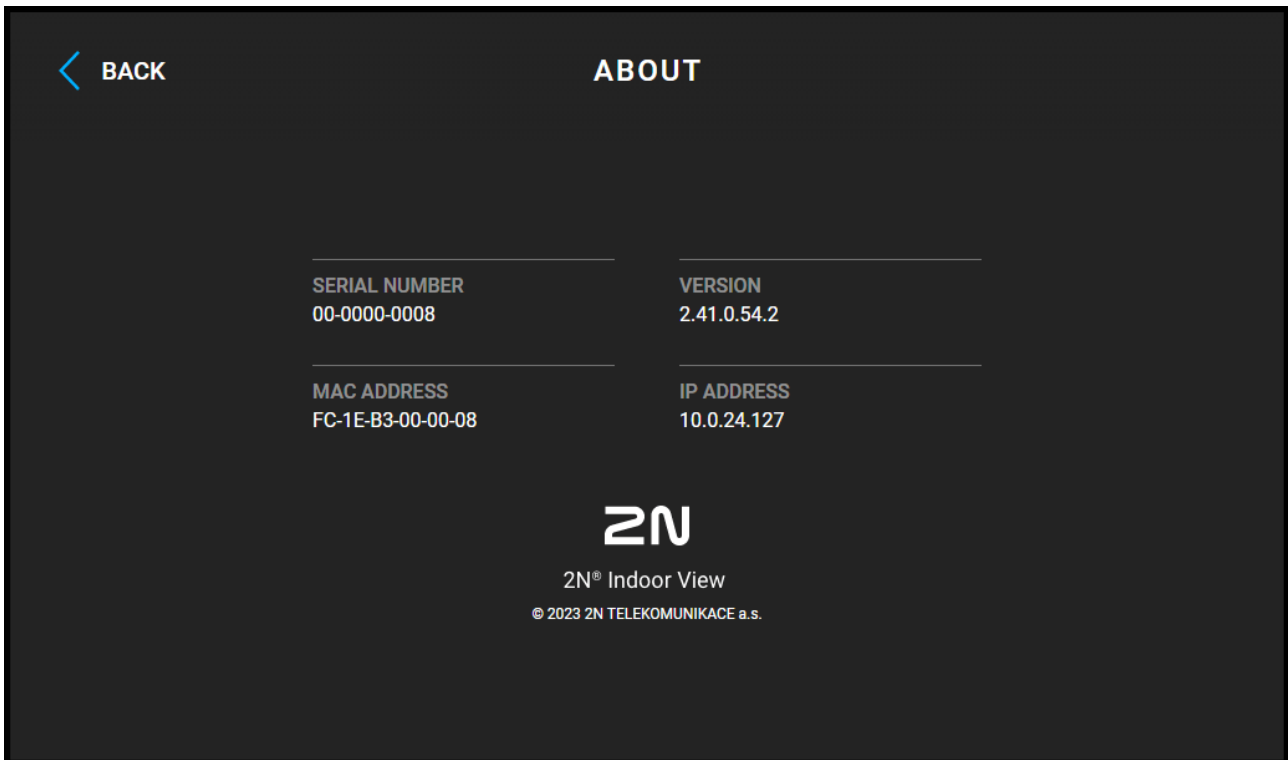
IP Address Retrieval Using Hardware

Follow the instructions below to retrieve the current IP address:

1. Press and hold the RESET (p. 7) 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.
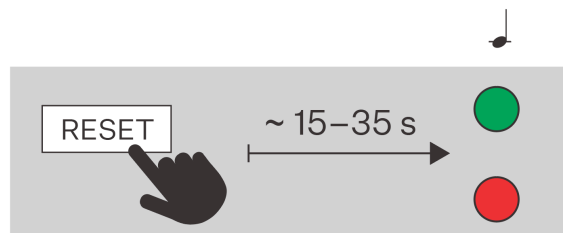
ℹ️ **NOTE**
The delay after pressing RESET till the first light and sound signaling is set to 15–35 s depending on the device model used.

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 (p. 7) 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 (p. 7) 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 (p. 7) 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

1. Press and hold the RESET (p. 7) 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.

Wi-Fi Connection

2N Indoor View Wi-Fi supports two network connection methods: wireless Wi-Fi or Ethernet cable. These methods cannot active at the same time. Upon the first start (factory default), set the Wi/Fi connection directly on the device using the display.

Wi-Fi Connection via Display

1. From the Home screen go to Settings > Advanced settings.

> **NOTE**
> The Advanced settings are available without a code in the factory default configuration. Having changed the default web configuration interface login password, you have to enter an access code. Set the Advanced settings access code in the web configuration interface (Hardware > Display > Advanced settings code > Advanced settings code).

2. Go to Network settings > Connection type.
3. Select Wi-Fi and then click Find wireless network.
4. The list of available wireless networks will be loaded. Select the network to connect to.
5. If the network is password secured, you will be prompted to enter the password.
6. Restart the device. Go back to the Advanced settings main menu and select **Restart Device**.

> ⚠️ **CAUTION**
> A change of the network interface will not be applied until the device is restarted.

> ℹ️ **NOTE**
> You can also make network settings in the web configuration interface in System > Network.

Firmware Update

We recommend that the firmware is also updated during the **2N Indoor View Wi-Fi** installation. Refer to 2N.com for the latest FW version.

Refer to Subs. Maintenance (p. 51) for firmware upgrade details.

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

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

Device Restart

To restart the device choose one of the following options:

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

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

Restart Using Device Buttons

Restart the device in Settings > Advanced settings.

Enter a code to access the Advanced settings. Set the Advanced settings access code in the web configuration interface (Hardware > Display > Advanced settings code > Advanced settings code).

Restart Using RESET Button

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

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. 17) for login details. Restart the device in System > Maintenance (p. 51) > System using Restart .

The Home screen (p. 62) is displayed after restart. Restarting may take a rather long time after the button press.

Factory Default Reset

Reset the device factory default values via software in System > Maintenance (p. 51) Default reset.

Follow the instructions below **2N Indoor View Wi-Fi** to reset the factory default values via hardware:
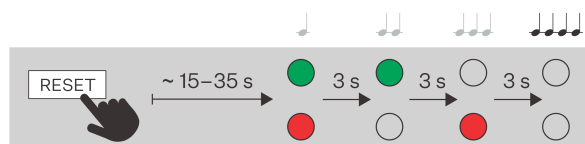
Factory Default Reset

1. Press and hold the RESET (p. 7) 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.
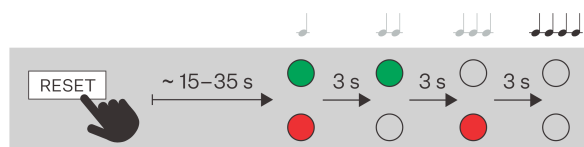
Call Connection

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

> **NOTE**
> When using a Wi-Fi connection, make calls to the local device as you would to any other device (via SIP), see below.

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:
   • allowing the contact to be shown on the display by checking the selected box
   • a virtual number to start a call by entering the number via your numerical keypad
   • basic information.
   Once saved, the contact will be shown in the phone book on the device display.
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. Enter the calling destination address into the destination field to which the call is to be routed. Complete the target IP address or SIP URI in the format " user_name@host" (e.g.: "johana@2.255.4.255" or "johana@calls.2N.com"). For local calls, fill in the called 2N device ID as specified in the Local Calls (p. 38) tab in the called device web configuration interface.
4. Edit the following:
   • allowing the contact to be shown on the display by checking the selected box
   • a virtual number to start a call by entering the number via your numerical keypad
   • basic information.
   Once saved, the contact will be shown in the phone book on the device display.
5. Make sure that the call transmitting service is enabled on the called 2N device to make a successful call.

Web configuration interface

Basic Orientation

The home page is displayed after logging into the **2N Indoor View Wi-Fi** web interface. You can return to it at any time using the ⬅ button located in the top left corner of the other pages of the web interface. The header of the page displays the device name (see the Device name parameter in the Services section > Web Server.

Menus

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

Legend

The start screen is also the first menu level and quick navigation (click on a tile) to selected **2N Indoor View Wi-Fi** configuration sections.

Section **Folder**

Menu **Block**

Device Configuration Interface Access

2N Indoor View Wi-Fi is configured via the web configuration interface. You have to know the device IP address portal or the device domain name. Make sure that the device is connected to the local IP network and powered.

Domain Name

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

Default domain name 2N Indoor View Wi-Fi: 2NIndoorViewWiFi-{serial number without dashes}.local (e.g.: "2NIndoorViewWiFi-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 Indoor View Wi-Fi** address or domain name into the internet browser.

   The login screen is now displayed.

   If the login screen is not displayed, check the IP address, port or domain name for validity. The login screen is not displayed if the web interface server is off. If no certificate has been generated for the IP address or domain name, a security certificate invalidity notification may appear. In that case, confirm that you want to go to the web configuration interface.

2. Enter the login data.

   The default login data are:

   Username: **Admin**

   Password: **2n**

   It is necessary to change the password immediately upon the first login.

   After login using the default password, the access to the web configuration interface functions is limited.

> **TIP**
>
> It is recommended that a password is used that is difficult to break. It is not recommended that names, places or things, especially those closely related to the user, are used in the password.
>
> For increased password security, it is recommended that:
>
> • the random password generator is used,
> • the password length is 12 characters at least,
> • various characters from different character sets are combined (small/capital letters, digits, special characters, etc.).

State

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

Device

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

Device Info

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

Locate Device – optical and 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).
CapabilitiesChanged	Event that informs of a change in the list of available functions of the device.
ConfigurationChanged	Device Configuration Change
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.
ExternalCameraState-Changed	Signals a status change of the connected external camera.
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 (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, 🔔 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, 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.

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 ✏ to set the phone number details.

Setting the phone number

- Call Type – set the scheme in the called destination URI. If you choose Without scheme ([unspecified]), the URI is completed with the data from the SIP account settings.
- Destination – set the other parts of the called destination URI. As a rule, it contains the number, IP address, domain, port or device identifier. Enter an asterisk "*" for calls to the VMS.

- Preferred SIP Account – SIP account 1 or 2 is primarily used for calling.
- Call Encryption – set mandatory call encryption or no encryption.
- Door Opening – via callbacks.

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

Alarm Call

Start Call with Doorbell Button Press – a phone call to this device will be set up after the alarm call button is pressed. Set the doorbell alarm call function in Hardware > Digital inputs (p. 44) > Doorbell button.

Unlock Button Function

Time Profiles

Assign a Time profile to the DND mode to define when the selected function is available and when it is not.

Each time profile defines the function availability based on a week calendar. Just set From-To and/or specify the weekdays for availability. 2N devices helps you create up to 20 time profiles (depending on the model) The selected function can be assigned any time profile created in Calls > General settings (p. 34) > Incoming calls.

Basic Settings

Profile name – enter a profile name. This parameter is optional and helps you find items in the profile list more easily.

Profile Time Sheet

This block helps you set an active time profile within a week. A profile is active when the current time falls into the set intervals.

If a day is marked as holiday (refer to Holidays (p. 33)), the last table row (Holiday) is applied regardless of the day in a week.

> **ℹ NOTE**
>
> - You can set any count of time intervals per day: 8:00–12:00, 13:00–17:00, 18:00–20:00, for example.
> - To make a profile active the whole day, add an interval covering one whole day, i.e. 00:00–24:00

Holidays

Here select the bank holidays (including Sundays). You can assign them different time intervals than to working days in their time profiles (refer to Time Profiles (p. 33)).

You can set holidays for the coming 10 years (click the year number at the top of the screen to select a year). The screen displays a calendar for the whole year. A calendar is displayed for you to select/unselect a holiday. Fixed (annual) holidays are marked green. Variable holidays (valid for the particular year only) are blue. Click a date once to select a fixed holiday, click twice to select a variable holiday and click for the third time to remove the holiday from the holiday list.

Calling

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

Calls

General Settings

Call Time Limit – set the call time limit after which the call is automatically terminated. The device beeps 10 s before the call ends to signal that the call end is approaching. Enter any DTMF character into the call (# on your IP phone, e.g.) to extend the call time. 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. 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.

Voicemail Mode – a pre-defined voice message (as set in User Sounds (p. 39)) is played into the call after a timeout defined in the Pick Up in parameter in the automatic/manual call answering mode if the "Only Out of Office Message is" set. A beep is also played in the Voicemail mode and an up to 20-second long call recording starts (audio and video if available) for the calling user to leave a message. If no user message is recorded, a default voice message in one of the seven available languages (as set in the Voice Message Language parameter inUser Sounds (p. 39)) can be used.

> **TIP**
> You can also set Voicemail from the device, Settings > Sound.

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.

Reject Calls in DND Mode – if this function is activated, the device reject calls in the Do not Disturb mode. The function can be used for immediate call redirection at absence to a mobile phone call, for example.

DND Mode for Doorbell Button – if this function is activated, the device shall not ring when the doorbell button is pressed.

Do Not Disturb Mode with Time Profile – choose one or more time profiles to be applied to the DND mode. Set the time profiles in Directory > Time profiles (p. 33).

Click the ⊙ icon to set the selection from predefined profiles or manual setting of a time profile for the given element.

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.

Call Log

Save Image during Call – if enabled, one or more snapshots are automatically taken from each video call and saved into the call log (depending on the device type and setting). More images can be taken manually during a call on some devices.

> **⚠ CAUTION**
> If the Save Image during Call function is disabled, all the snapshots will be deleted but the call logs will be preserved.

Automatic Image Count – set the count of snapshots that shall be automatically taken during a call and saved into the call log.

Advanced Settings

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

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

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

SIP 1 / SIP 2

2N Indoor View Wi-Fi 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 KeepAlive Packets – set that the device shall send STUN/CRLF packets to the registrar on a regular basis and also SIP OPTIONS during calls to keep the setup connection active.

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

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

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

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

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

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

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

DTMF Sending
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

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

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

Services

Unlocking

Unlocking is another function of **2N Indoor View Wi-Fi**, 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.

Show Door Open Sensor – enable displaying of the intercom door open sensor states.

HTTP Command

The HTTP Command on **2N Indoor View Wi-Fi** helps you send up to 3 selected HTTP commands by a button press. These buttons can be shown on the Home screen display, on the display during calls and on the display in the camera preview. Up to 3 HTTP commands can be set up for each of these button displays.

URL – set the HTTP command to be sent to an external device by pressing a button. The command is sent via the HTTP (GET request). The command format is http://ip_address/path. E.g. "http://192.168.1.50/relay1=on". If the parameter is empty, the command is not sent.

Icon – choose the HTTP command button icon. The button is displayed on the device home page and can be used for sending the set HTTP command.

Name – set the HTTP command name.

Username – set the user name for the HTTP commands sent during the switch activation /deactivation. It is only required if authentication is required.

Password – set the password for the HTTP commands sent during the switch activation /deactivation.

User Sounds

2N Indoor View Wi-Fi 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 Message Language – select a language of spoken messages. If there is a translation available for a mapped sound, the message will be played in specified language. If no translation is available, the message is played in English or as a language-neutral sound.

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 (device ringtone).
- Doorbell – set the sound to be played when the door button is pressed.
- Away Message – set the message on absence to be played when the call is not answered (before recording if the answering machine is allowed).

Sound Upload

Up to 10 sound files can be added to the device. You can assign a unique name to each added sound for better orientation.

Sound Adding Procedure

1. Press ⬆ to upload a sound file to the device.
2. Select a file from your PC and click Upload .
3. Press 🎤 to record a sound file via your PC microphone.
4. Press ✕ to remove a file. Click ▶ to play a successfully uploaded sound file (locally on your PC).

Web Server

2N Indoor View Wi-Fi can be configured using a common browser that approaches the web server integrated in the device. The HTTPS protocol is used for the browser - device communication.

Basic Settings

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

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

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

Advanced Settings

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

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

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

HTTPS 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 [icon], download [icon] and/or remove [icon] user files including translations of the user interface texts.

Weather

The Weather service displays the current weather information for the selected location on the **2N Indoor View Wi-Fi** home screen.

Settings

Show Weather – allow the device to display the current weather information.

Location – set the device location for weather forecast. If Show Weather is enabled and the Location parameter is empty, Prague will be displayed by default. Otherwise, the weather and Location values will be hidden.

Location Shown – complete the location name to be shown on the device display. If not completed, the weather forecast location is displayed.

Temperature units – select the temperature units to be displayed.

Results

Last Update – precise date of the last server data update.

Location Found – weather forecast location found by the weather service.

Country – country of the automatically defined or completed location.

Hardware

Audio

2N Indoor View Wi-Fi is equipped with a speaker. Set the phone call and state signaling volume control in this configuration section.

Phone Call Volume

Call Volume – set the phone call volume.

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

Call Progress Tone Volume – set the 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

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

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

User Sound Volume – set the volume of user sounds played by automation. The value is relative to the master volume.

Camera

2N Indoor View Wi-Fi helps you configure up to 16 external cameras for video call streaming.

> **(i) NOTE**
>
> The 2N answering units receive standard external IP cameras supporting the RTSP streams meeting the following limits:
>
> - codec H.264 or MJPEG
> - 1280x720 px resolution
> - maximum framerate of 30 FPS for H.264 or 15 FPS for MJPEG. Higher frame rates may result in undesired effects (less smooth playing).
> - High profile with 5000 kbps bitrate if codec H.264 is used

Camera enabled – enable RTSP stream download from an external IP camera. Complete the valid RTSP stream address or the username and password to make the function work properly.

Camera Assignment

Click [+] to open the device list and select the devices to which a camera is to be assigned. In the call with the device to which the camera is assigned, it is possible to show the selected camera preview on the answering unit and switch it to previews of other assigned and allowed cameras.

Click [×] to cancel all assignments of the selected camera.

> **TIP**
>
> Cameras can also be assigned to devices in respective device settings in the Directory > section Device (p. 29). Once saved, the change will automatically be written in both the sections.

Settings

Display Name – set the name to be displayed at the camera preview in the directory on the device. If the parameter is empty, the default name set for the selected language is displayed.

RTSP Stream Address – enter the IP camera RTSP stream IP address: "rtsp://camera_ip_address/parameter1=value&parameter2=value", refer to the parameter table below. The parameters are specific for the selected IP camera model. If you choose another 2N IP intercom for the external camera, enter " http://ip_address/mjpeg_stream" or "http://ip_address/h264_stream".

> **TIP**
>
> To connect stream from a camera of another 2N device, copy the Local URL of the stream of the given device from Services > ONVIF/RSTP.

Parameter	Description	Example / Values
audio	audio	• audio=0 (disabled) • audio=1 (enabled)
fps	frame rate	fps=15 (1 to 30 fps, maximum MJPEG video codec value is 15 fps).
vbr	video bitrate	vbr=768 for 768 kbps
vcodec	video codec	vcodec=h264 for codec H.264 vcodec=mjpeg for codec MJPEG
vres	video resolution	vres=1920x1080 for FullHD
zipstream	zipstream	• zipstream=off (disabled) • zipstream=low • zipstream=medium • zipstream=high • zipstream=higher

Username – enter the username for the external IP camera authentication. The parameter is mandatory only if the external IP camera requires authentication.

Password – enter the external IP camera authentication password. The parameter is mandatory only if the external IP camera requires authentication.

Local RTP port – set the local UTP port for RTP stream receiving.

Camera Preview

The Camera Preview window displays the current image received from an external camera. In case the camera is disconnected or misconfigured, N/A is displayed on a black background.

External IP Camera Log

The External IP Camera Log displays the RTSP communication with the selected external IP camera including failures and error states if any.

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 – Language – set the language of the texts displayed on the screen. You can choose from predefined languages or a user-defined language.

Date Format – set the date format to be displayed.

Time Format – set the time format to be displayed.

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

Screen Lock PIN – set the screen lock activation/deactivation code.

Advanced Settings Code – set the access code for the Advanced settings on the device display. If the parameter is left empty, the Advanced settings cannot be opened from the display.

Device Mode – select the normal or hotel mode. In the Hotel mode, the device has a simplified user interface and altered functions compared with the normal mode.

• "Hotel Mode"
  • In the Hotel mode, the device can dial calls to one preset contact and receive incoming calls. The device displays time and weather. The other functions are limited. The Do Not Disturb mode cannot be set from the device. The device does not allow access to the Directory, Call Log and Settings menus. The device does not provide quick access to the weather settings. The device does not display notifications (missed calls, door contact states, etc.).
  • It is possible to set a call to one contact by a short press. Start the short press call by touching the blue phone earpiece button. Set this function in the device properties in Directory > Device.

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

Display Time in Idle Mode – allow the device to display time in the Idle mode.

When the Doorbell Button Function is set to Doorbell (refer to Digital Inputs (p. 44)), 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.

Intensity Reduction in Idle Mode to – set the level of reduction of the backlight intensity if the device goes into Idle mode.

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 Custom (p. 43) 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.

Camera Assigned to Doorbell Button – select the external camera to be displayed when the doorbell is ringing. The camera preview does not interrupt the active call or ringing. Tap on the green bar in the display upper part to return to the call/ringing. If the doorbell is not confirmed, a warning will be displayed on the device and a record will be created in the Call log.

System

Network

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

> **TIP**
> To retrieve the IP address, use 2N Network Scanner, which can be downloaded freely from 2N.com. Refer to Subs. IP Address Retrieval Using 2N Network Scanner (p. 18) 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 802.1x (p. 46).

> **NOTE**
> You can also make basic network settings in Settings > Advanced settings on the device.

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. 25).

Network Interface Settings

Active Network Interface – defines the device network interface.

- "Ethernet" – connection via a physical cable
- "Wi-Fi" – wireless connection

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.

Offered Modes – select the modes to be advertised in autonegotiation.

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

Network SSID – enter the name of the wireless network to which the device shall be connected. This name is

displayed whenever the device connects to Wi-Fi. Click to open a dialog box including a list of available wireless networks. Click the network name to select the network.

Secured Wi-Fi – define the security level of the given wireless network manually. Once you select a network from the list, this parameter is completed automatically based on whether or not the selected network requires password.

Password – enter the password for the wireless network to which the device shall be connected. The password can be entered if the Secured Wi-Fi parameter is confirmed.

Wi-Fi Status – indicates the wireless network connection status.

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. 48). 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. 48).

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. 48). 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 Indoor View Wi-Fi is equipped with a real time clock without power outage backup. Select Use Time from Internet to synchronize the device time with the Internet time or click Synchronize with Browser to synchronize time with your current PC time.

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

> **i NOTE**
> The device does not need the current date and time values for its basic function. The current date and time values are necessary for a proper function of the time profiles and correct event times in some lists (Syslog, entered cards, log downloaded via HTTP API, etc.).

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 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.

> **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 Indoor View Wi-Fi** LAN services use the secure TLS protocol for communication with the other LAN devices. This protocol prevents third parties from eavesdropping on or modifying call contents. TLS is based on one/two-sided authentication, which requires certificates and private keys.

The following device services use the TLS protocol:

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

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

Each certificate requiring service can be assigned one certificate set, refer to Web Server (p. 40). The certificates can be shared by the services.

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

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

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

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

Certificate Upload

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

ⓘ **NOTE**

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

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 Indoor View Wi-Fi 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.

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

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 discovery)*	8002	UDP	In/Out	✓	×	–
HTTP	80	TCP	In/Out	✓	✓	Web Server (p. 40)
HTTPS	443	TCP	In/Out	✓	✓	Web Server (p. 40)
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. 33)
RTP+RTCP ports (external camera)	4800+ (range of 64 ports)	UDP	In/Out	×	×	–

Service	Port	Proto-col	Direc-tion	On by default	Config-urable	Settings
RTSP client	554	UDP	In/Out	×	✓	Calling (p. 33)
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	Calling (p. 33)
SIPS	5061	TCP	In/Out	×	✓	Calling (p. 33)
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. 49)

Device Control

2N Indoor View Wi-Fi is equipped with a touch display for intuitive control.

Idle Mode

The device will automatically go into the Idle mode if there is no activity (after selection of the 15s –10min timeout). The device configuration allows date and time, the current weather information and door contact state to be displayed in the Idle mode if configured so.

Home Screen
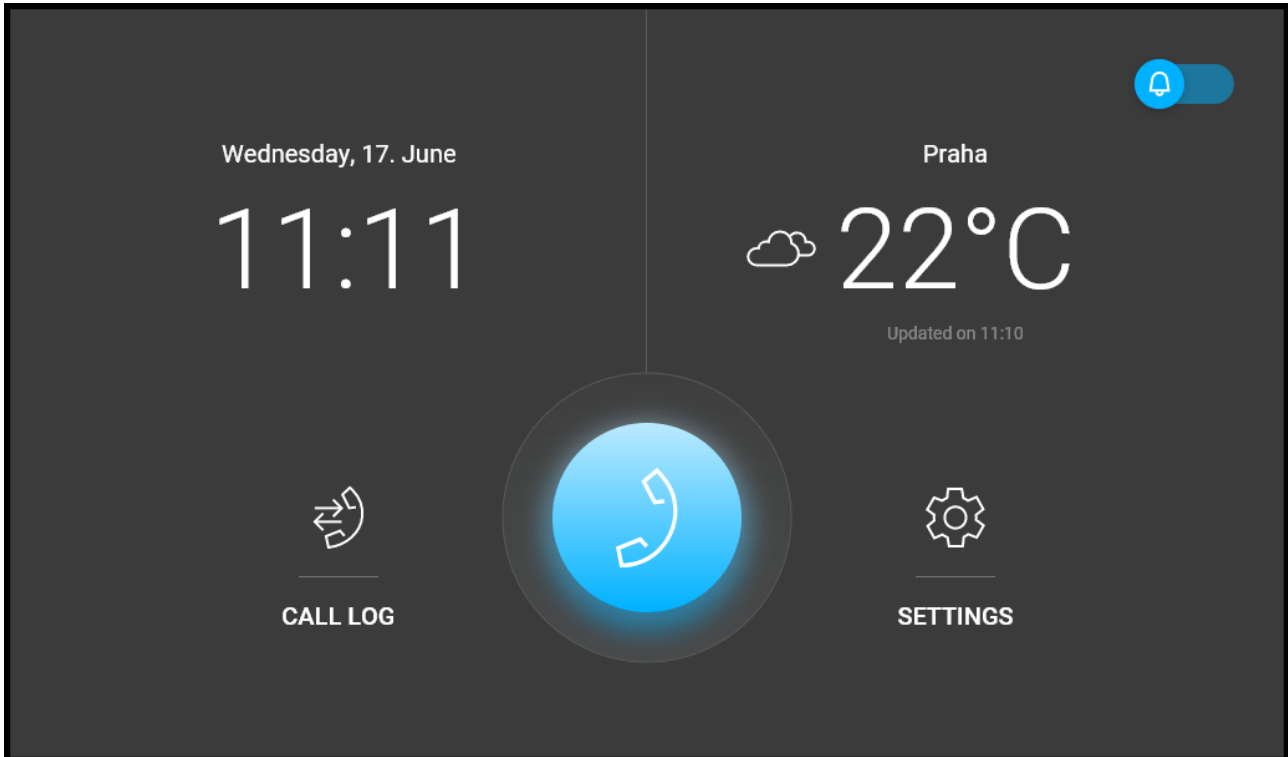
The Home screen is set as the start screen, which is displayed when the device is switched from the Idle mode by a finger touch. It shows the current date, time, temperature and location and provides access to the Logs, Directory and Settings as well as direct activation of the Do Not Disturb mode. The device configuration allows you to display the door contact state notifications and buttons with the selected icons of the configured HTTP commands on the Home screen.

> **TIP**
> A long press on the Home page location / current weather area automatically displays the Settings > Weather section.

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 (p. 7) 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 (p. 7) 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 (p. 7) 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

1. Press and hold the RESET (p. 7) 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.

Icons used on the display

Icon	Description
☌	Receiving incoming call / Starting outgoing call
☍	Rejection of incoming call / Termination of outgoing/active call
🗑	Remove
🔕	DND mode
⚙	Device configuration
⤺☍	Call Log
🔊	Incoming call ringtone volume up
🔉	Incoming call ringtone volume down
🔇	Incoming call ringtone volume mute
+	Value up
−	Value down
🎙	Microphone mute in call
🔓	Unlocked, screen lock activated/deactivated

Icon	Description
〉	Call info
👁	Camera Preview
📹1	Camera 1
📹2	Camera 2
N/A	Camera unavailable
←	Back
⤢	Camera Video Preview Zoom In

Icon	Description

Home Screen

The home screen is set as the start screen of the device, which is displayed whenever the device is activated by a display touch in the Idle mode.

The device displays:

- weather conditions in the given location,
- missed call icon (if the call was from a device/number included in the Directory),
- Do Not Disturb icon,
- HTTP command activation icon (as set in the device configuration),
- date,
- time.

The home screen provides access to:

- Directory,
- Call Log,
- Settings.

The dominant of the Home screen is a phone earpiece icon on a blue background, which allows you to make calls to the destinations listed in the Directory. If the earpiece icon is highlighted in red, **2N Indoor View Wi-Fi** cannot establish phone connections. This happens when the device has an unroutable address (0.0.0.0) or cannot log in to My2N or SIP Proxy.
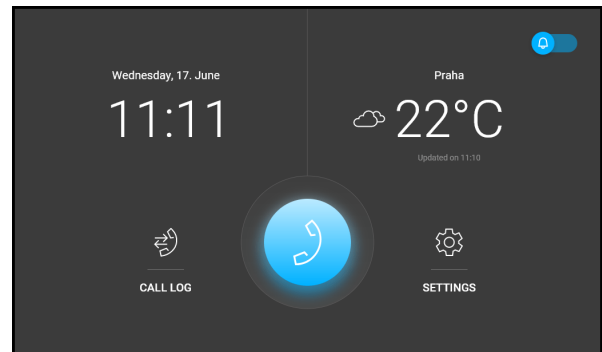
> **TIP**
> A long press on the Home page location / current weather area automatically displays the Settings > Weather section.
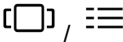
Possible actions	Performance	Action result
Display of Directory Menu	⌣	??? is displayed with alladded devices and an external camera.
Call Log Menu Display	⇄	Call Log (p. 65) is displayed including a list of accomplished calls.
Do Not Disturb Activation	🔕	Do Not Disturb Mode (p. 79) is activated and the activation message is displayed.
Settings Menu Display	⚙	Settings (p. 66) is displayed on the device.
Send the set HTTP command (p. 39)	Press the set HTTP command icon.	The HTTP command is sent to an external device.

Directory Menu

The Directory menu provides a list of contacts and connected external cameras.

Set the Directory contacts in Directory > Device (p. 32) in the web interface.

Possible actions	Performance	Action result
Outgoing call setup	☎	An outgoing call is set up to the destination of the selected contact.
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. **NOTE** If no unlocking code is set in the device and no default unlock code is set, the lock button is not displayed.
Device detail display	👁	The preview of the device camera is displayed if available.
HTTP command (p. 39) sending in call.	Press the set HTTP command icon.	The HTTP command is sent to an external device.
Directory display switch	⟮▢⟯ / ☰	The Directory items can be displayed as: • a list in a column – scroll up/down to select an item, • tiles in a row – browse from right to left to select an item.

Call Log

Press ⟳ to display the call log.

The device displays a list of all accomplished

calls including date, time, status (outgoing ↗ ,

incoming ↙ or missed ⌄) and information on
from/to which destination the call was made.

The maximum call log capacity is 20 calls. The
log list and details provide door contact status in-
formation as configured (door open too long, door
open by force).
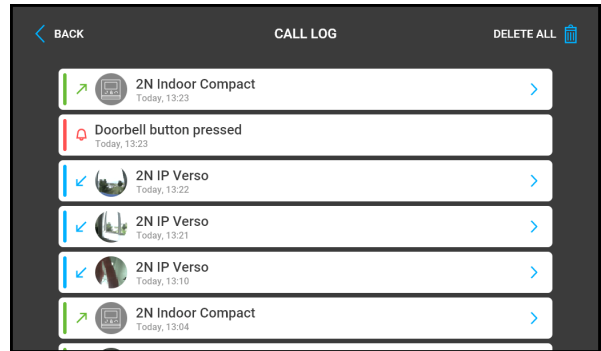
⚠	**CAUTION**
	The device restart results in a deletion of the call list.

65

| Possible actions	Performance	Action result
Show call detail	❯ or touch the selected call row	Call information and device camera preview if available are displayed. If available, screenshots are displayed in the call detail and can be switched between. The screenshot time is shown in the right-hand upper corner.
Outgoing call setup	☎ in call detail	An outgoing call is set up to the selected record destination.
Selected Device Unlocking	🔓 in call detail	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.

> ℹ️ **NOTE**
> If no unlocking code is set in the device and no default unlock code is set, the lock button is not displayed.
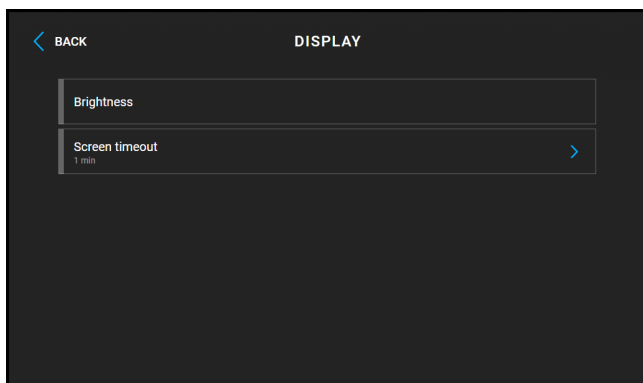
Settings

Press the ⚙ button on the home screen to display the Device Settings section. The Settings menu helps you set the device locally.
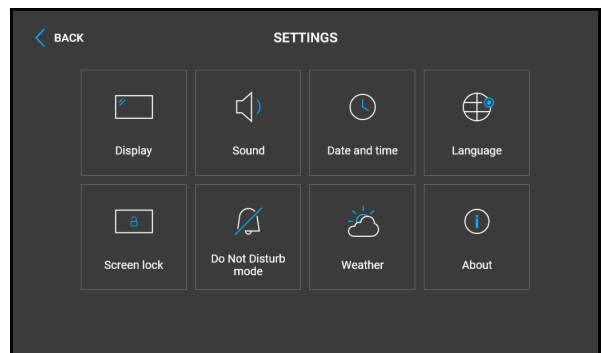
It includes the following 8 sections:

Display

Brightness – sets the value of display backlighting.

Screen timeout – timeout after which the device automatically goes into Sleep Mode if there is no activity.

Screen lock – switches the screen lock or also the so-called parental lock on/off.

With the device lock on, enter the PIN code to enable the screen lock. Enter the same PIN code to disable the screen lock.

Language
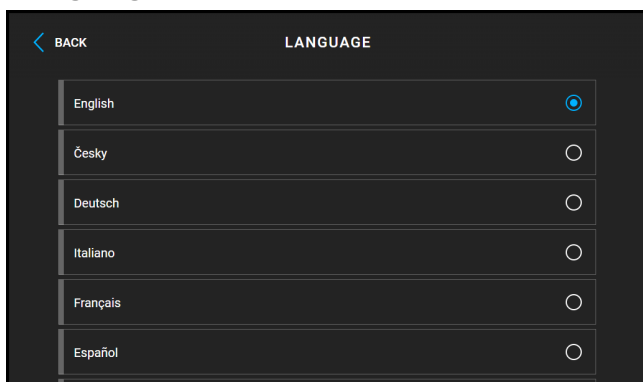
Language – set the language for the texts to be displayed. Choose one of the eight pre-defined languages (CZ, EN, DE, NL, FR, ES, IT, RU).

Custom Language – set the language for the texts to be displayed from an uploaded language file of the user localization.

Do Not Disturb Mode

Do Not Disturb mode – switches Do Not Disturb mode on/off. This allows you to switch off the ringtone for the incoming call for the period of time when this mode is active. By default, the DND mode does not apply to doorbell notification, i.e. the incoming ringtone is off and the doorbell ringtone is on. Change this setting via the web interface in the Hardware > Audio menu.

Reject Calls in DND Mode – with this function activated, the device rejects calls in the Do Not Disturb mode. The function can be used for immediate call forwarding at absence to a mobile phone call, for example.

Mute Doorbell in DND Mode – with this function activated, the device does not ring when the doorbell button is pressed in the DND mode.

Date and Time
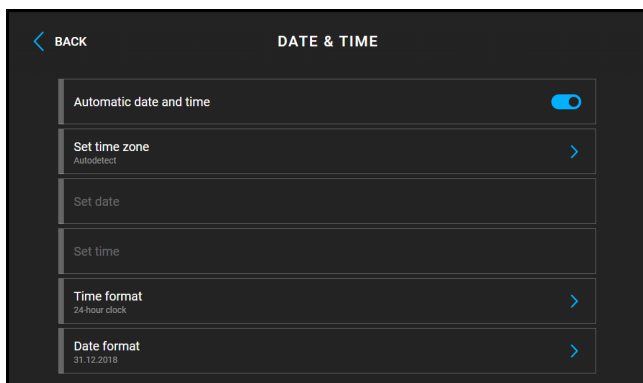
Automatic date and time – activates a mode in which the date and time will be taken from the network.

Set Time Zone – set the time zone for your installation site to define time shifts and summer/winter time transitions.
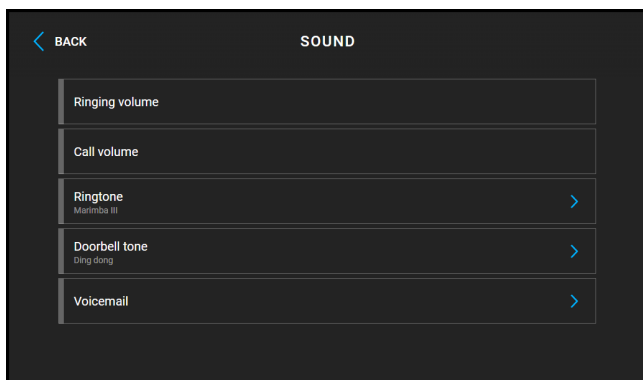
Set date – used to set the date manually.

Set time – used to set time manually.

Time Format – set the time format to be displayed.

**Date Format** – set the date format to be displayed.

Sound

Ringtone Volume – set the incoming call ringtone volume.

Call Volume – set the phone call volume.

Ringtone – sets the ringtone for incoming calls on the device.

Doorbell Tone – set the tone to be played when the doorbell is used.

Voicemail – set the Voicemail modes directly on the device. This function helps leave a message to be played to the caller if the device fails to answer their incoming call. The caller can record a message to be stored in the device Voicemail and played back on the device later. This settings is particularly useful in working or personal environments where it is important to keep communication even if the user is absent.
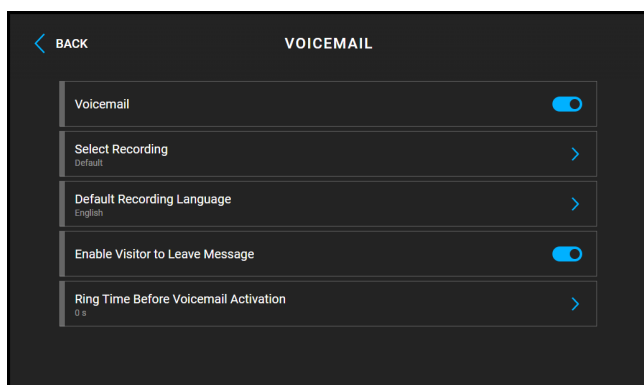
Voicemail – enable the function that helps leave an out-of-office message to be played to the caller if the device fails to answer their incoming call for a period of time longer than as defined in **Voicemail Activation Timeout**. Once this function is enabled, the **Enable Leaving Message** parameter is activated automatically.

Select Recording – set the Away message to be played to the calling user. You can record a new message through a microphone in this setting.

Default Recording Language – set the language for the default recording.

Enable Leaving Message – allow the caller to leave a message to be stored in the device. When the Away message has been played, a tone is generated and recording starts for up to 20 s. The message includes both audio and video depending on the capacities of the calling device. End the call to terminate the recording earlier. If this function is disabled, the out-of-office message is only played and the call is ended afterwards.

Voicemail Activation Timeout – set the incoming call ringing timeout after which the Away message is played.

Weather
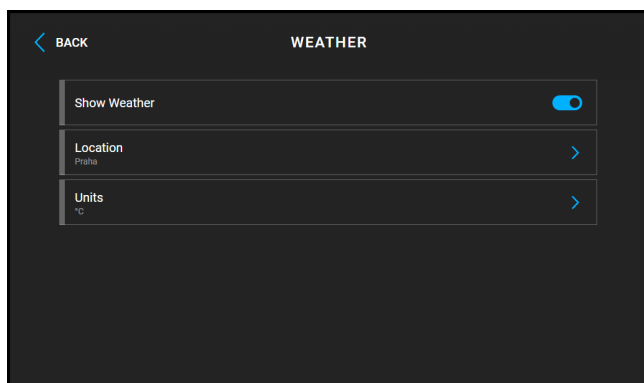
Display weather – displays or hides information about the current weather on the home screen.

Location – set the device location for weather forecast. Press the Home page weather area shortly to set the location in the Weather / Settings section, which will be displayed automatically. Use the keypad to enter the location name with diacritic marks. Prague is the default location value.

Units – allows you to set display in metric (°C) or imperial (°F) units.

Advanced Settings

The Advanced settings are available without a code in the factory default configuration. Having changed the default web configuration interface login password, you have to enter an access code. Set the Advanced settings access code in the web configuration interface (Hardware > Display > Advanced settings code > Advanced settings code).
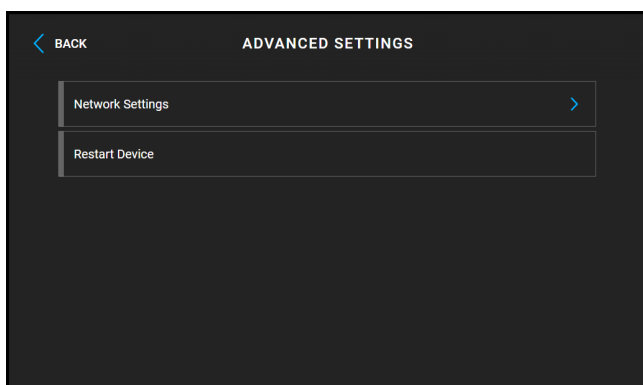
Network Settings

> **NOTE**
> You can also make network settings in the web configuration interface in System > Network.

General

- **Use DHCP Server** – enable automatic obtaining of the IP address from the LAN DHCP server. If the DHCP server is unavailable or otherwise inaccessible in your LAN, use the manual network settings.
- **Set Static IP Address** – set the static IP address, network mask and default gateway. The parameters are used if the Use DHCP Server parameter is disabled.
- **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.
- **Offered Modes** – select the modes to be advertised in auto-negotiation.

Connection Type

A change of the network interface will not be applied until the device is restarted.

- **Ethernet** – switch the network interface to the Ethernet cable connection.
- **Wi-Fi** – switch the network interface to the Wi-Fi connection.
- **Find Wireless Network** – select any of the available Wi-Fi networks if the Wi-Fi network interface is activated. If a secured Wi-Fi network is selected, the password entering request will appear.

Restart Device

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

About
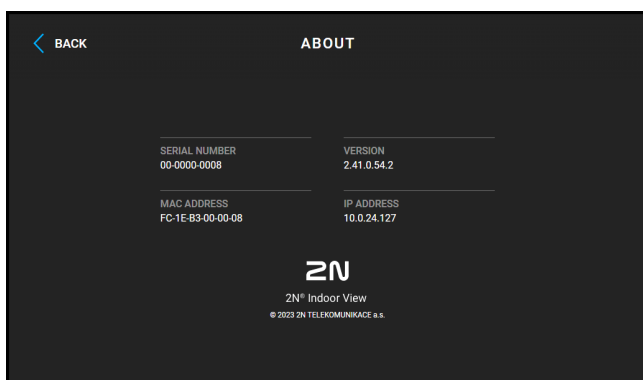
This section provides basic information on the device (serial number, MAC address, FW version, IP address, My2N ID).

Use a long touch of the IP address to set the network interface port mode to be offered for auto-negotiation. The mode can be selected only if the required port mode is defined automatically, see Network (p. 45).

Hotel Mode

In the Hotel mode, the device can dial calls to one preset contact and receive incoming calls. The device displays time and weather. The other functions are limited. The Do Not Disturb mode cannot be set from the device. The device does not allow access to the Directory, Call Log and Settings menus. The device does not provide quick access to the weather settings. The device does not display notifications (missed calls, door contact states, etc.).

The Hotel mode switches into the Idle mode after the preset timeout passes.
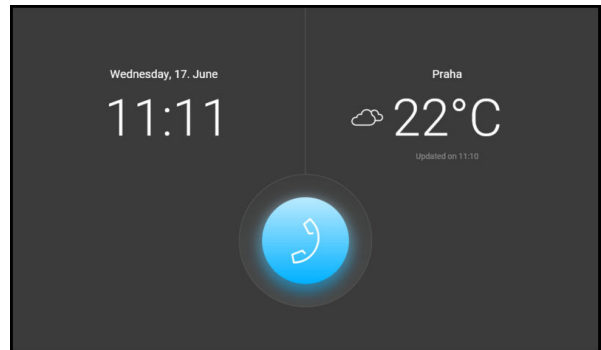
> **NOTE**
> Activate the Hotel mode in Hardware > Display (p. 43) > Device mode.

Possible actions	Perform-ance	Action result
Send the set HTTP command (p. 39)	Press the set HTTP command icon.	The HTTP command is sent to an external device.
Outgoing call setup	✎	A call to the preset contact is started. Select the contact by enabling the **Start Call with Short Press** parameter at the given contact in Directory > Device in the web configuration interface.
Incoming call receiving	✎ or touch of the display beyond the other icons	Connection with the other device has been established, a call is in progress.
Ringtone Disable	🔊	The ringtone stops playing when a call comes in. The incoming call is not ended.
End of Call	☎	The outgoing call is cancelled./The incoming call is rejected./The active call is interrupted.
Target device lock opening (in an active call)	🔓	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 button. After unlocking, automatic call ending can be set in the web configuration interface Unlocking (p. 39).
		ⓘ NOTE If no unlocking code is set in the device and no default unlock code is set, the lock button is not displayed.
Mute call (in an active call)	🎤	**2N Indoor View Wi-Fi** does not transmit audio to the called device. The microphone icons turns red.

Possible actions	Perform-ance	Action result
		"Noone can hear you" is displayed in the active call.
Call volume control		The call volume is increased/decreased by one level by each press of +/− or a scale shift.
Called Device Camera Preview Switch	(Cannot be displayed until is selected.)	The camera preview is switched to another camera assigned to the device. The icon number indicates the camera placement in the sequence.
Camera Preview Focus on Face	(Cannot be displayed until is selected.)	The camera preview focuses on the face of the person standing at the device.
Screenshots		The screenshot is saved in the call log detail. Up to 5 screenshots can be added to one record.

Operational Statuses

This section includes a basic description of user scenarios and states that can occur during the use of **2N Indoor View Wi-Fi**, 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 Configuration via Hardware (p. 20).
	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 Indoor View Wi-Fi** functions are limited, it is impossible to switch to the home page and go to menus. Possible actions are included in the table below.

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

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

- **Outgoing call** initiated by the **2N Indoor View Wi-Fi** answering unit.
- **Incoming** trying to establish connection with the **2N Indoor View Wi-Fi** answering unit.
- **Active call** – if connection between the devices is established, sound is transmitted and camera preview if available is displayed.

Outgoing Call

Incoming Call

Active Call

Possible actions	Performance	Action result
Incoming call receiving	⤷ or touch of the display beyond the other icons	Connection with the other device has been established, a call is in progress.
End of Call	⤸	The outgoing call is cancelled./The incoming call is rejected./The active call is interrupted. Home screen (p. 62) is displayed.
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 button. After unlocking, automatic call ending can be set in the web configuration interface Unlocking (p. 39). ℹ **NOTE** If no unlocking code is set in the device and no default unlock code is set, the lock button is not displayed.
Mute call	🎤̷	**2N Indoor View Wi-Fi** does not transmit audio to the called device. The microphone icons turns red. "Noone can hear you" is displayed in the active call. The microphone buttons is flashing yellow. The action reperformance cancels muting.
Call volume control	🔊	The call volume is increased/decreased by one level by each press of +/− or a scale shift.

Possible actions	Performance	Action result
Ringtone Disable	🔇	The ringtone stops playing. The incoming call is not ended.
Called Device Camera Preview Switch	(Cannot be displayed until ⬚ is selected.)	The camera preview is switched to another camera assigned to the device. The icon number indicates the camera placement in the sequence.
Camera Preview Focus on Face	(Cannot be displayed until ⬚ is selected.)	The camera preview focuses on the face of the person standing at the device.
Screenshots	📷	The screenshot is saved in the call log detail. Up to 5 screenshots can be added to one record.
HTTP command (p. 39) sending in call.	Press the set HTTP command icon.	The HTTP command is sent to an external device.

Idle Mode

2N Indoor View Wi-Fi transits into the Idle mode after a set inactivity period. Set the inactivity timeout in the Display (p. 43) > ??? web configuration menu. The operation power consumption is reduced in the Idle mode.

The device can show the following in the Idle mode as configured:

• door contact state,
• current weather information,
• date,
• time.

11:51
Wed, 17. June

☁ 22°C

Possible actions	Performance	Action result
Idle mode end	Touch any spot on the display.	The device quits the Idle mode. The , Home Screen (p. 62) or Device Lock (Screen Lock) (p. 78)is displayed.

Device Lock (Screen Lock)

When the **2N Indoor View Wi-Fi** lock is activated, enter the PIN code for device locking. The same PIN code is required for device unlocking.

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.
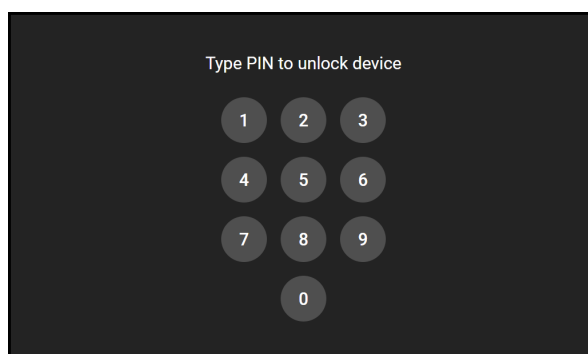
> **NOTE**
> Set the device lock activation in the Idle mode in the Display (p. 43) menu in the web configuration interface.

Possible actions	Performance	Action result
Device lock activation	Activation of the function and setting of a 4-digit PIN code with subsequent confirmation	The lock is activated.
Device lock deactivation	Correct PIN entering	The device is unlocked and you can go to other operational statuses and perform other actions.
		When an incorrect PIN code is entered, a remedy instruction is displayed. The count of incorrect PIN code entering attempts is unlimited.

Do Not Disturb Mode

The incoming call ringtone is switched off in the DND mode. A call can be received, rejected or ended, see Calls (p. 74).

The display shows the camera preview if available , CLIP and the *Incoming call* message.
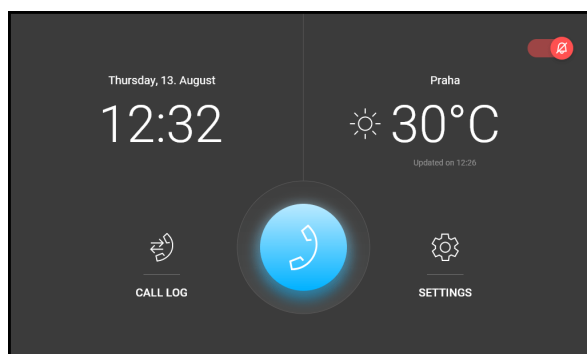
> ⚠️ **CAUTION**
> The doorbell tone is switched on. Set the doorbell tone in the DND mode in the web interface (Calls > Calls (p. 34) > Incoming calls > Do Not Disturb mode for doorbell).

In the DND mode, you can also set automatic call rejection for the device (directly on the device or in Calls > General settings > Incoming calls > Reject calls in DND mode) and automatic DND activation/deactivation according to the set time profiles (Calls > Calls (p. 34) > Incoming calls > Do Not Disturb mode with time profile).

With the hotel mode on, it is not possible to switch the device into the DND mode and the DND icon is hidden on the home screen.

Possible actions	Performance	Action result
Do Not Disturb Activation	on the home screen or in the Settings menu.	Activation of the Do Not Disturb mode. The DND mode can be disabled by a repeated short press of .
Do Not Disturb Deactivation	on the home screen or in the Settings menu.	DND is deactivated and the doorbell icon turns white.

Maintenance - Cleaning

2N Indoor View Wi-Fi contains no environmentally harmful components. Dispose of the device in accordance with the applicable legal regulations.

2N Indoor View Wi-Fi contains no environmentally harmful components. Dispose of the device in accordance with the applicable legal regulations.

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

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

• Alcohol-based cleaners may not be applied.
• Clean the device in dry weather in order to make waste water evaporate quickly.
• Do not use aggressive detergents (such as abrasives or strong disinfectants).

Troubleshooting

81

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

Technical Parameters

Supply type	Consumption	Polarity reversal protection	Power Consumption in idle
PoE, IEEE 802.3af	12 W	✓	2.9 W
12 V DC ±10 % adapter; 1 A (recommended)	12 W	✓	2.9 W

User interface	
Controls	capacitive touch panel
Display	7" with 1024 × 600 pixel resolution

Signaling protocol	
SIP	UDP, TCP, TLS

Audio	
Microphone	Integrated
Speaker	2 Wintegrated
Induction loop output	
	600 mV RHS

Technical Parameters

Audio stream	
Protocols	RTP, RTSP
Codecs	G.711, G.729, G.722, L16/16kHz

Video stream	
Protocols	RTP, RTSP, HTTP
Codecs	H.264
Video Resolution	1280 x 720 px

Interface	
LAN	10/100BaseT, RJ-45; Cat5e or higher
Wi-Fi	2.4/5GHz 802.11a/b/g/n/ac

Doorbell input	
Input type	Switching contact (button/relay)
Contact type	Normally open (NO)
Contact parameters	Max. 50 V / 5 mA, DC

Mechanical Parameters	
Dimensions (w x h x d)	193 × 157 × 50 mm
Weight	555 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 Indoor View Wi-Fi conforms to the following directives and regulations:

- 2014/30/EU for electromagnetic compatibility
- 2014/35/EU for electrical equipment designed for use within certain voltage limits
- 2014/53/EU for radio equipment
- 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment
- 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.

Legislation of Japan

本製品は、特定無線設備の技術基準適合証明 を受けています。

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

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

2N

wiki.2n.com

2N Indoor View Wi-Fi – User Manual

© 2N Telekomunikace a. s., 2024

2N.com