IP intercoms

Configuration manual

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

2N.com

Table of Contents

Used Ports **4**

First Login **7**
- Finding devices in the network 7
  - Domain Name 7
  - Device IP Address 7
  - DHCP Switching 9
- Access to web device configuration 10
  - Password Change 11
  - Recommended browsers 11

Basic Device Settings **12**
- Firmware Update 12
  - Update from Server 12
  - Automatic Updates (Auto-Provisioning) 12
  - Manual Firmware Check and Installation 13
- Directory 14
- Calling 14
  - Creating Calling Contacts 15
  - Adding 2N Local Device 16
  - Dialing Calls 16
  - Calling via SIP 18
  - Local Calls between 2N Devices 19
  - MS Teams Calls 20
- Accesses 21
  - Door Switch Control Methods 21
  - Automatic Door Switch Status Changes 23
  - User Access Settings 23
  - Door Switch Settings 28
  - Access Rules 28
  - Modules 31
  - Elevator Control 32
- Display Settings 34
  - Custom Display Language Upload 34
  - Slideshow 34
  - Showcase Mode (**2N IP Style**) 34
  - Information Messages (**2N IP Style**) 35

Advanced Settings **37**
- Camera and Video Settings 37
  - Internal Camera Settings 37
  - External Camera Settings 38
  - Privacy Policy 38
  - Motion Detection 39
  - Creating Video Stream 40
- Sound Settings 41
  - Device Volume Setting 41
  - Audio Transmission in Calls 41
  - User Sounds 42
  - Other Device Audio Features 42
- Time Profiles 43
  - Holidays 43
- Advanced SIP Account Settings 43
  - SIP Functions 44
  - Media 44
  - Advanced Settings 44

Facial Zoom in Video Call 44
Tamper Switch Settings 44
Blocking other switches when the cover is opened 45
Tamper Switch Events 45
HTTP API 45
Troubleshooting 47
System 48
Date and Time Settings 48
NTP Synchronization 48
Time Update at Outage 48
Network Configuration 48
Firewall 49
Licenses 49
License Key Update 49
Trial License 50
Overview of Licensed Features 50
Event Log 51
Default Reset 54
Signaling of Operational Statuses 55
Used Ports 56
Automation 60

Used Ports

Service	Port	Protocol	Direction	On by default	Configurable	Settings
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device discovery)*	8002	UDP	In/Out	✓	×	–
FTP	21	TCP	Out	×	×	–
2N IP Eye	8003	UDP	Out	×	×	–
HTTP	80	TCP	In/Out	✓	✓	**System > Network connection > WEB SERVER tab**
HTTPS	443	TCP	In/Out	✓	✓	**System > Network connection > WEB SERVER tab**
Multicast audio	22222	UDP	Out	×	✓	**Integration > Audio**
Multicast audio for ICU protocol	8006	UDP	Out	×	×	–

Service	Port	Protocol	Direction	On by default	Configurable	Settings
Multicast video for ICU protocol	8008	UDP	Out	×	×	–
Multicast video (wide) for ICU protocol	8016	UDP	In/Out	×	×	–
NTP client	123	UDP	In/Out	✓	×	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	×	×	–
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	×	✓	**Calling > General Settings**
RTP+RTCP ports (external camera)	4800+ (range of 64 ports)	UDP	In/Out	×	✓	**Integration > ONVIF / RTSP**
RTSP client	554	UDP	In/Out	×	✓	
RTSP server	554	UDP	In/Out	×	×	–
SingleWire Commands	80	TCP	In/Out	×	×	–
SingleWire Communication	8081	TCP	Out	×	×	–
SingleWire Media	20000+	UDP	In	×	×	–
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	**Calling > SIP**
SIPS	5061	TCP	In/Out	×	✓	**Calling >SIP**

Service	Port	Protocol	Direction	On by default	Configurable	Settings
SMTP	25	TCP	Out	×	✓	**Integration > Email notification**
Syslog	514	UDP	Out	×	×	–
TFTP	69	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
SSDP	1900	UDP	In/Out	✓	×	–
SDDP	1902	UDP	In/Out	✓	×	–
Multicast receiver (Automation)	4433	UDP	In	×	×	–
WS-Discovery	3702	UDP	In/Out	✓	×	–
CIP Client (Crestron)	41794	UDP	In/Out	×	×	–
Sitechannel (ICU protocol)	8004	UDP	In/Out	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

First Login

Finding devices in the network

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

Domain Name

To access the web configuration interface, you can enter the domain name into the browser in the format “hostname.local” instead of the IP address. The hostname of a new device consists of the product name and serial number of the device. While entering a hostname, use only letters and digits; do not use spaces, periods, dashes, or other special characters.

Default domain name : 2NIPIntercom20-{serial number without dashes}.local (e.g.: “2NIPIntercom20-0000000001.local”)

The format of the device name is specified in the Installation Manual for the specific product in the Domain Name subsection.

TIP
You can change the hostname later in the web configuration interface at **System > Network Connection > Advanced Configuration > Hostname**.

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.

Device IP Address

By factory default, uses a dynamic IP address assigned by the DHCP server.

The 2N IP Utility application helps find the 2N device IP address in the LAN. Download 2N IP Utility from the 2N.com website. Make sure that Microsoft .NET Framework 4.7.2 is installed for successful app installation.

Depending on the capabilities of the device, you can also retrieve the IP address in one of the following ways:

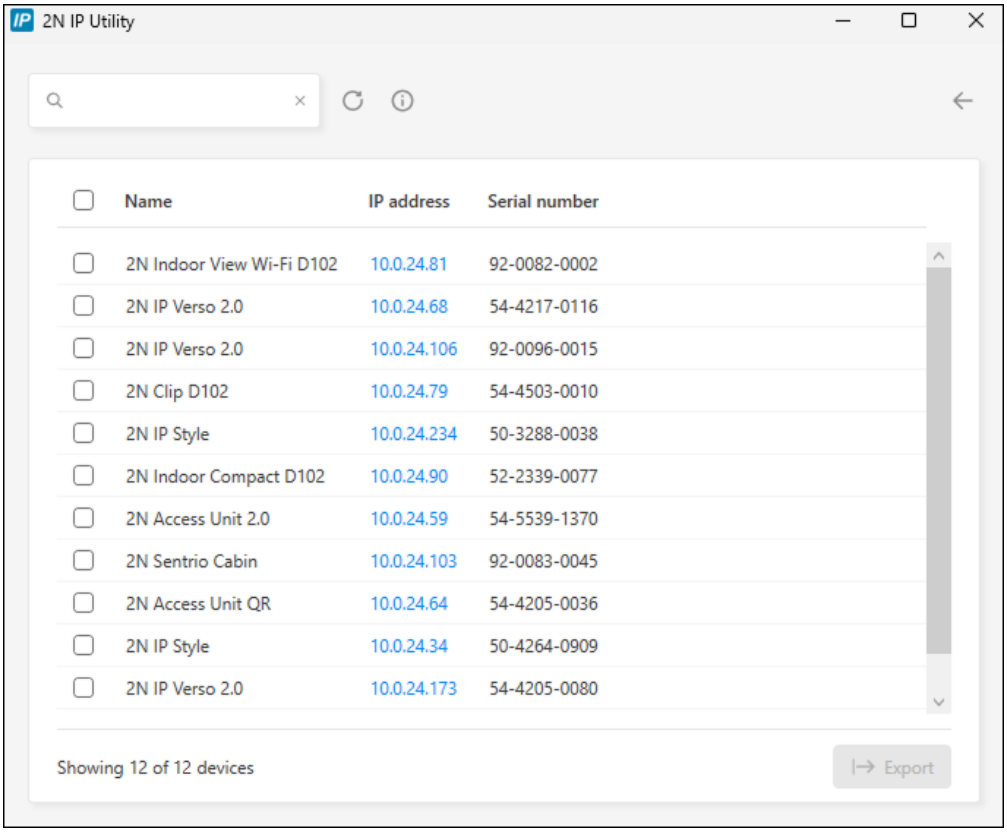
- with the Speed Dial button
- on the device display (see the product Installation Manual for the procedure)

IP Address Retrieval Using 2N IP Utility

The 2N IP Utility application helps find the 2N device IP address in the LAN. Download 2N IP Utility from the 2N.com website. Make sure that Microsoft .NET Framework 4.7.2 is installed for successful app installation.

1. Run the 2N IP Utility installer.
2. The Installation Wizard will help you with the installation.

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



4. Select the device to be configured and left-click it. This opens the right-hand part of the web configuration interface window.

TIP

- Access to the web configuration interface is also possible via the **Open in external browser** button, which opens the interface in a separate browser window.
- Click a device in the list to display detailed information. Click the **IP settings** button to change the IP address by entering the required static IP address or activating DHCP.
- The application also allows you to export selected devices into a CSV file. First select a device by ticking the boxes in the list, then use the **Export** button that appears at the bottom of the window. The exported file shall include the names, IP addresses and serial numbers of the selected devices.

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

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

For increased password security, it is recommended that:

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

IP Address Retrieval Using Speed Dial Button

Take the following steps to retrieve the IP address:

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Press the first Speed dial button 5 times on the main unit.
3. The device reads its IP address.

NOTE

- If the address is 0.0.0.0, it means that the device has not obtained the IP address from the DHCP server.
- Press the button sequence within 30 seconds after the sound signal for security reasons. Up to 2 s intervals are allowed between the presses.

DHCP Switching

By factory default, uses a dynamic IP address assigned by the DHCP server.

Dynamic IP Address

DHCP (Dynamic Host Configuration Protocol) is a network protocol that maintains a list of available IP addresses and automatically assigns them to devices in the LAN. The assigned IP address is dynamic, so the device can be assigned a new IP address after a period of time (lease time).

Static IP Address

If the IP address of the device is to remain unchanged, you must disable IP address allocation by the DHCP server on the device. You can disable the DHCP server in the web configuration interface or using the device hardware.

NOTE
The specific values for the static IP address can only be set in the web configuration interface of the device.

Setting Network Parameters in Web Configuration Interface

1. Go to the web configuration interface.
2. Go to **System > Network Connection > Basic Settings > IP Address Settings**.
3. Set the desired network parameters.
4. Save your changes.

Switching DHCP on Device Hardware

Depending on the capabilities of the device, the IP address can be switched as follows:

- with the Speed Dial button
- on the device display (see the product Installation Manual for the procedure)

TIP
Please refer to the product Installation Manual for the location of the RESET button.

IP Address Retrieval Using Speed Dial Button

Take the following steps to retrieve the IP address:

1. Connect the device to the power supply (if connected, disconnect and reconnect it).
2. Press the first Speed dial button 5 times on the main unit.
3. The device reads its IP address.

NOTE

- If the address is 0.0.0.0, it means that the device has not obtained the IP address from the DHCP server.
- Press the button sequence within 30 seconds after the sound signal for security reasons. Up to 2 s intervals are allowed between the presses.

Access to web device configuration

Configure via a web configuration interface, which is accessible from a web browser.

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

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

Web Configuration Interface Login

1. Start your Internet browser.
2. Enter the device IP address or domain name (refer to Subs.Finding devices in the network (p. 7)).
3. If no certificate has been generated for the IP address, a security certificate invalidity notification may appear. In that case, confirm that you want to go to the web configuration interface.
4. The login screen is now displayed.

5. Enter the login data.
   The default login data are:
   - Username: **Admin**
   - Password: **2n**
6. After the first login, change the password.

Access from 2N Access Commander

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

Password Change

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

TIP

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

For increased password security, it is recommended that:

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

Recommended browsers

The web configuration interface is optimized for the Chromium-based web browsers (Google Chrome, Microsoft Edge or Opera, e.g.). With other browsers, there may be slight differences in the interface function and appearance.

Basic Device Settings

Firmware Update

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

Update Modes

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

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

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

Update from Server

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

Update Settings from Update Server

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

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

Automatic Updates (Auto-Provisioning)

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

Firmware source setting

1. Go to **System > Firmware** .
2. Choose **Automatic Updates** on the **Firmware Update Configuration** card.
3. In the open dialog box, complete the following:

   - provisioning server IP address parameters
   - relative path to the firmware file
4. If the server is secured, fill in the access details.
5. To increase security, set up the server certificate authentication and select the Client Certificate under which it will be authenticated.
6. In the next step, set the server check interval.

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

Required File Structure

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

Name parameters

- MODEL – device identifier

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

Manual Firmware Check and Installation

Manual Check for Update Availability

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

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

Manual Firmware Installation

Uploading New Firmware from Storage

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

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

Directory

The Directory section is a key part of the device configuration. You can create users in the directory and manage their access rights or phone connection parameters. Each user can act as an access right holder, a calling contact or both at the same time.

Adding User Manually to Directory

1. Click Add User on the Directory page.
2. The user detail will open. Name the user on the Personal Information tab.
3. Set the device phone number of the contact according to Creating Calling Contacts (p. 15).
4. Set the access options according to Accesses (p. 21).

> **NOTE**
> The address book has a capacity of N/A records.

Bulk User Management in Access Commander or My2N

If the device is managed through the Access Commander or My2N bulk configuration tools, any changes made in the web configuration interface are overwritten by the settings in the bulk configuration tool. A user created directly in the web interface will be deleted.

The **Holder** column in the Directory table specifies the bulk configuration tool that created the user. The **Holder** column is hidden by default.

Calling

The 2N device provides several ways of connecting calls. Before creating contacts and setting the dialing method, you must first activate and set the call mediating services:

- Calling via SIP (p. 18)
- Local Calls between 2N Devices (p. 19)
- other special integrations

Creating Calling Contacts

Creating a calling contact consists of adding a phone number to the corresponding user in the device directory.

> **TIP**
> You can use the Local calls function to connect to another 2N device in your LAN, refer to Adding 2N Local Device (p. 16).

1. Go to **Directory**.
2. Open the user detail by clicking on the row or select Add User to create a new user.
3. On the **Phone Numbers** tab, click to open the phone number editing.
4. Select **Call Type** for the contact (SIP, local network, MS Teams, VMS, ...).
   - Calling via SIP (p. 18) – for VoIP services and accounts
   - Local Calls between 2N Devices (p. 19) – for calls to 2N devices
   - MS Teams, VMS,... – for special integrations
5. Enter the destination number or address for the device to call.
   Enter the extension number, SIP URI (e.g. “sip:101@192.168.1.50”), domain name (e.g. “2NIPVerso20-22222222” or another number as set in the Call Type) as necessary.
6. Set additional call features that affect the call behavior in **Options**.
   These options allow the administrator to configure the security, functionality and dialing logic to suit the exact needs of the facility, for example, to use encrypted transmission, speed up the connection or enable door reverse opening.
7. Specify the time limit when the number can be called in the **Availability** section. For example, you can set availability only for the user's working hours.
8. Click Confirm to save the change.
9. If you want to use the speed dial button to call the contact, assign a button to the contact on the **Buttons** tab.

Setting 2N IP Eye

The 2N IP Eye application allows you to view video from the IP intercom on your computer screen. After you fill in the **2N IP Eye address**, the video is displayed on the computer whenever a contact makes an incoming call.

Enter the address as follows: `domain[:port1][:port2]`

- `eye_computer.company.cz`
- `192.168.22.111:8009:8080`

The `port1` and `port2` parameters are optional. Enter the values if Network Address Translation (NAT) is in progress between the 2N IP device and 2N IP Eye PC. Set the ports as configured by the router or another NAT-executing device.

- `port1` – default value: 8003, destination port for receiving UDP messages from 2N IP Eye.
- `port2` – default value: 80, destination port for HTTP communication between 2N IP Eye and 2N IP device.

Adding 2N Local Device

CAUTION
Local Calls must be enabled on both this and the device to be searched with the identical **Access Key**, refer to Local Calls between 2N Devices (p. 19).

1. Click Add Local Device on the **Directory** page.
2. In the open dialog box, check the device to get connected to.
3. Select Add to Directory.
4. A new user appears in the directory with one phone number set.
5. Click the user row to edit it further.

TIP
To set the access rights of the holder of this device, follow Accesses (p. 21).

Dialing Calls

Quick Dial Button Assigning

To assign contacts to speed dial buttons, go to **Calling > Dialing > Speed Dial Buttons**.

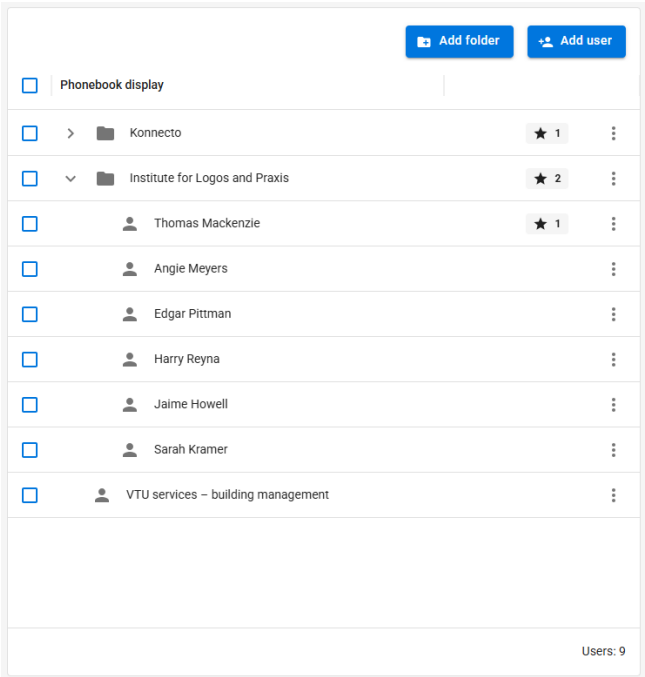
The buttons for quick selection of modules connected to the main unit via VBUS are also set here.

NOTE
Up to 16 users can be assigned to one speed dial button.

The maximum total count of numbers to be dialed at the same time is 16, which can occur when group calling or multiple numbers assigned to a speed dial button are used simultaneously.

Displaying Directory Contacts

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



All contacts with an assigned phone number are stored in the root folder by default. Contacts can be further sorted into folders, for example by the department or building floor.

Moving Contacts to Folder

1. In the phone book table header, create and name a new folder.

> **TIP**
> You can add an image to a folder under which it will appear on the display in the phone book view in the extended menu ⋮ at the folder.

2. To move your contacts to another folder, first select them and then click .
3. Select a new location within the phone book.
4. Click Move to save your changes.

The contacts are usually sorted alphabetically in each folder. This order can be changed by setting the priority (in the extended menu ⋮ for the given contact).

A newly created user with a phone number will automatically appear in the root folder.

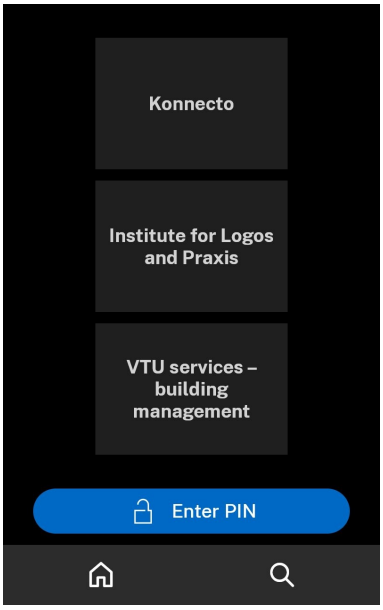
Call Groups

Call groups allow multiple contacts to be called in bulk at the same time (for example, calling the reception and the warehouse at the same time).

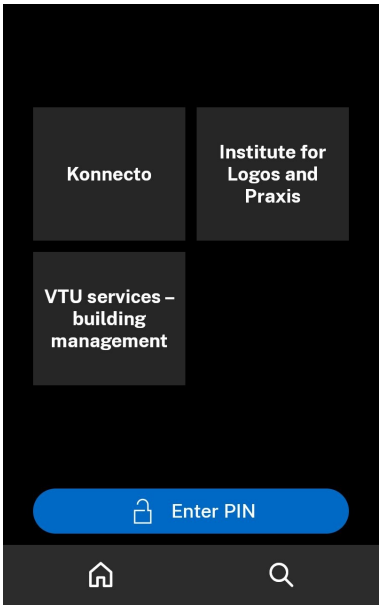
1. In the **Phonebook View** table, select all the contacts that you want to be part of the group.
2. Click above the table.
3. Fill in the calling group name and location within the phone book.
4. Select whether you want to keep the contacts visible as individual contacts or only show them under a call group in the phone book.
5. Click Move to save your changes.

2N IP Style Display Settings

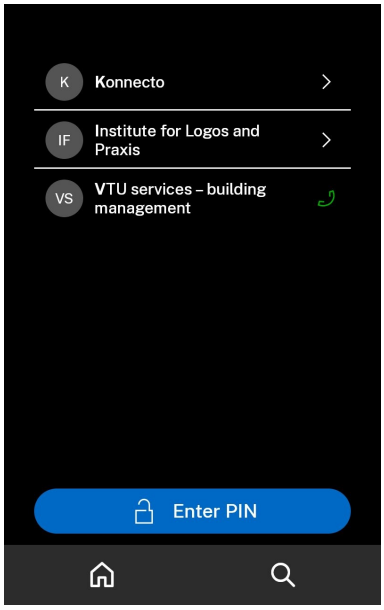
In **Display Settings** on the left tab, you can select one of the following display ways for the showing of the directory on the **2N IP Style** display.



Cards (1 column)



Cards (2 columns)



Phonebook

Calling via SIP

Device Registration to SIP Server

Registration to the SIP server is crucial for full functionality of the device in a SIP environment.

1. Go to **Calling > SIP** of the account to be set up.
2. Enable the SIP account at the top.
3. On the **Device Identity** tab, fill in:
   - **Display Name** – this text will be displayed to the other party as caller ID.
   - **Phone Number (ID)** – 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 SIP Registrar address.

   These three values combined identify the device in the SIP environment.
4. In **Authentication**, fill in the login credentials assigned by the SIP server administrator to authenticate the device to the SIP Proxy server. This authentication prevents unauthorized access, fraudulent calls or identity fraud.

   If **Authentication ID** is not filled in, the device will authenticate with **Phone Number**.
5. Under **Transport Protocol Options**, select the protocol to be used by the SIP server.
6. Enable the **SIP Registrar** feature.

7. Fill in the details of the SIP registrar with which you want to register the 2N device.
   If you leave the **Port** parameter empty or the parameter value is 0, the default port is applied according to the selected transport protocol.

Default Port Values according to Transport Protocol

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

8. The tab header shows the registration status and the registration error messages.

NOTE
Further SIP account settings are described in Subs. Advanced SIP Account Settings (p. 43).

Setting Public Device IP Address

This setting is used when the device is located behind a router (NAT) and communicates with the PBX outside the LAN (in the cloud or over the Internet, e.g.). In SIP communication, the device must specify the public IP address under which it is accessible from the Internet. If it sent its internal IP address, the PBX would not be able to route the call or RTP data stream correctly.

If the device and the PBX are on one and the same LAN, it is unnecessary to set the public IP address.

1. Go to **Calling > SIP** of the account to be set up.
2. On the **Public IP Address** tab select one of the following options:
   - STUN (Automatic)
     Fill in the details of your STUN server.
   - Enter Manually
     Enter your own external IP address for the device.

Local Calls between 2N Devices

It is possible to set up the so-called local calls between the 2N IP devices, which allow for direct communication between 2N devices within one LAN without the need to connect to a SIP server or external infrastructure.

Activating Local Calls

1. Go to **Calls > Local Calls**.
2. Enable the feature in the page header.

3. Set the access keys to ensure secure communication with other devices on the network.
   The access keys ensure that only devices with identical keys can communicate with each other. This contributes to security and the ability to define independent groups of devices.

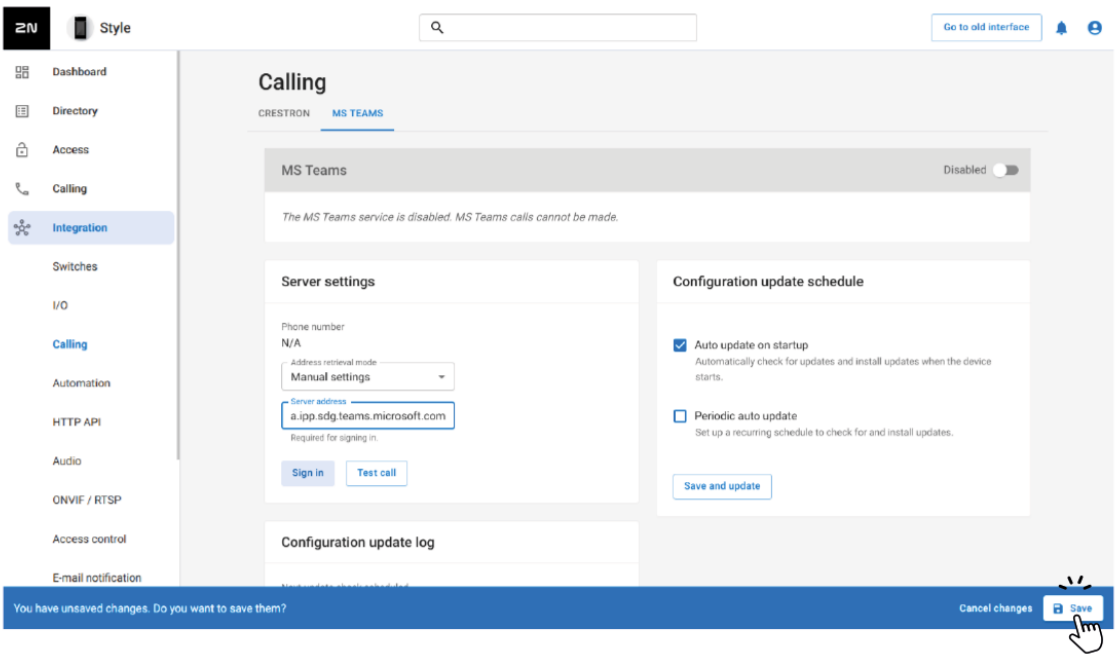
MS Teams Calls

Requirements

- Active MS Teams license
  The MS Teams feature is not part of the GOLD license and requires a separate MS Teams license.
- MS Teams account
- Provisioning server URL for the given region
  Find this address in the Microsoft documentation in the SIP Gateway section. The region determines where the 2N device connects from; this may differ from the MS Teams user's location.

Preparing 2N devices for integration with MS Teams

1. Go to **Integration > Calling** in the web configuration interface.
2. Go to the **MS Teams** tab.
3. Move the switch to **Enabled** in the card header.
4. Fill in the provisioning URL of the given region into the **Server Address** parameter on the **Server Settings** card.
5. Save your changes.



6. Follow the configuration progress on the **Configuration Update Log** card.
7. The device is ready to be linked with an MS Teams account once both the shared and private configurations have been successfully completed.

TIP
If the private configuration fails, click Update on the **Configuration Update Schedule** card.

Device connection to MS Teams account

1. Complete:Preparing 2N devices for integration with MS Teams (p. 20) .
2. Click the Log button on the **Server Settings** card.
3. A dialog box will appear offering instructions and a pairing code. Follow the instructions to complete your sign-in.
4. After the 2N device is connected successfully to the MS Teams account, the **ONLINE** status will be displayed in the page header.

> **TIP**
> If the device is not online, click Update on the **Configuration Update Schedule** card.

Creating MS Teams call contacts

After connecting your device to MS Teams, you can call directly the MS Teams users who are using the application on their PCs or mobile devices.

1. Go to **Directory**.
2. Open the user detail by clicking on the row or select Add User to create a new user.
3. On the **Phone Numbers** tab, click to open the phone number editing.
4. Select “MS Teams” in the **Call Type** field.
5. Enter your MS Teams user ID into the **Destination** field.

Accesses

Managing access and unlocking the electric door lock is one of the basic functions of the device. The device manages access based on the evaluation of access requests according to the predefined access rules. Having considered a request legitimate, the device activates the door switch that controls the electric door lock. This will unlock the door.

> **CAUTION**
> Remember to set the proper function of the switch. Proceed according to Subs. Door Switch Settings (p. 28).

Door Switch Control Methods

In addition to conventional user authentication methods (RFID card, biometrics, Bluetooth, etc.), the switch can also be activated using external signals and interfaces, which provides flexible integration and automation options. Different ways of door switch activation are described below:

User Authentication

The user uses its authentication method and if its user rights are in accordance with the access rules, the user is granted access. The allowed access will activate the door switch.

The setup is described in Subs. User Access Settings (p. 23).

Switch Control in Web Configuration Interface

1. Go to **Integration > Switches**.
2. Find the switch card that controls the door.
3. Click Hold in **Manual Switch Control** .

4. The switch will remain on until you cancel the hold in the manual control again.

Switch activation based on time profile

In the web configuration interface, you can set the switch to hold the door unlocked for a predetermined period of time, for example over lunchtime.

1. Go to **Integration > Switches**.
2. Find the switch card that controls the door.

> **NOTE**
> The door switch function in the device is performed by **Switch 1**.

3. Click the → arrow of the selected switch to go to its detail.
4. Enable the **Time Controlled Switch Hold** on the **Status** tab.
5. Select the time profiles in which the switch should be held or enter a custom time period.

Switch activation from call (DTMF)

DTMF Code Settings

1. Go to **Integration > Switches**.
2. Find the switch card that controls the door.

> **NOTE**
> The door switch function in the device is performed by **Switch 1**.

3. Click the → arrow of the selected switch to go to its detail.
4. You can set the codes to be entered via DTMF during a call with the device on the **Activation Codes** tab.
   The validity of each code can be time limited.

> **NOTE**
> You can set the first activation code to be processed as an older form of the code. In this form, you will not need to confirm the code with an asterisk when entering it on the phone keypad.

Using DTMF Code

1. When connected to the device, enter the activation code on your phone keypad and confirm with an asterisk.

> **NOTE**
> Receiving DTMF signals is enabled by default on the device. You can check the permission on the Call Service page (SIP/Local Calls) on the **Audio** folder on the **Receive DTMF** tab.

Switch activation using HTTP API

Refer to the HTTP API Manual for 2N Devices for complete usage details, including a description of the necessary HTTP API authorization. The door switch is controlled by the `api switch ctrl` endpoint.

For switch 1, the command looks as follows: `https://ip_addres/api/switch/ctrl?switch=1&action=on`.

Switch activation by Automation

Refer to the Automation Manual for Automation setup details. The switch is triggered by the **ActivateSwitch** action.

Automatic Door Switch Status Changes

The table below shows the changes in the states controlling the door switch depending on the system operation.

Switch Status	Device Restart	Setting Default Values	Factory Reset
Switch Locking	No change	No change	Restoring Default Values
Switch Hold (permanently on)	No change	Restoring Default Values	Restoring Default Values
Access Blocking	Restoring Default Values	No change	Restoring Default Values
Blocking when the tamper switch is activated	No change	Restoring Default Values	Restoring Default Values

User Access Settings

To successfully authenticate to the access control unit and unlock the door, the user must meet two conditions: be assigned the access rights to the device and have at least one authentication method established. The available authentication methods depend on the specific device and can include RFID cards, numeric PIN codes, QR codes for scanning by the camera, etc.

Authentication Settings:

1. Go to **Directory**.
2. Open the user detail by clicking on the row or select Add User to create a new user.
3. Set all the methods by which the user will authenticate on the **Authentication** tab, see Authentication Methods (p. 24).
4. Fill in when the user should be granted access to enter and exit on the **Access Settings** tab.
   - Anytime
   - Time profile – choose the set **Time Profiles**.
   - Custom – press the Edit button to set unique time intervals for this user.

   Set an expiration date to limit the user access for a specific calendar period.

   Granting **Exceptions**, you will grant the user permanent access, which will not be restricted even by a temporary locking of the device indicated by the access rules (see Access Rules (p. 28)).

Authentication Methods

CAUTION
The available authentication methods depend on the specific device and modules connected.

RFID Card

One user can be assigned up to 2 RFID cards.

The identifier can be entered manually using the keypad or read by tapping the card onto a USB reader connected to the PC.

RFID Card Requirements

- The identifier must be a hexadecimal number.
- The minimum length of the identifier is 6 characters.
- Only cards supported by the device can be used – the card type must be enabled in the module settings (see **Access > Modules**).

TIP
You can read the identifier of an existing card from the log at **System > Event Log**. Load the new/unassigned card on the device and then copy its identifier (UUID) from the log. After adding the identifier to the RFID cards, the user can start using the card for authentication.

My2N

My2N – used for interconnection with the My2N app, which provides authentication via Bluetooth.

PIN Code / QR Code

The PIN code serves as a personal numeric access code, which the user enters on the device keypad or can be read by the device camera in the form of a QR code.

CAUTION
QR codes can only be read on the device internal camera.

PIN requirements

- The minimum length is 2 digits.
- The code can only contain digits (0-9).
- QR codes can only be used for PINs between 4 and 15 digits long.
- If you use the **Silent Alarm** feature, we recommend creating even-numbered PINs.

NOTE
When a hexadecimal QR code is used, the value must be converted to the decimal format before entering.

Accepted hexadecimal range: 1000 to FFFFFFFF.

Fingerprint

Each user can enroll up to 2 fingerprints.Use an external fingerprint reader for enrollment. Make sure you have installed the 2N USB Driver. The driver can be downloaded here.

The enrolled user fingerprint can be used for the following actions:

- Open the door;
- Trigger silent alarm – can only be set if the Open door function is active;
- F1 and F2 automation – generates the FingerEntered event in Automation. F1 and F2 help distinguish the scanned finger in Automation.

NOTE
A maximum of 2000 fingerprints can be uploaded to the address book of one device.

License Plate

Some devices support vehicle license plate recognition using external AXIS cameras equipped with the **VaxALPR** add-on application. The recognized license plates are sent in an HTTP request to the `api/lpr/licenseplate` endpoint (refer to the HTTP API Manual for IP Intercoms for more details).

TIP
The external camera adding procedure is described in ???.

License Plate – set the vehicle license plate to be scanned by the device and used for user authentication.

License plate requirements:

- The maximum length of one number plate is 10 characters.
- Up to 20 license plates can be assigned to one user.
- Each license plate should be assigned to only one user – if multiple assignments are made, the first record found is used.
- The license plates are used in the recognition function from the external camera image (refer to the Interoperability Manual).

Virtual Card

The virtual card helps identify a user in the devices connected via the Wiegand interface. After successful user authentication via My2N or a biometric reader, the virtual card ID is sent to the Wiegand interface (if sending identifiers is enabled in the configuration, see **Access > Access Rules > Entry/Exit > Advanced**).

Virtual card requirements:

- The ID must be a hexadecimal number (characters 0-9, A-F).
- The length of the ID is 6 to 32 characters.
- One user can be assigned just one virtual card.

Switch Code

Switch Code – set up to 4 switch activation codes (e.g. for the door lock). The switch code is used for door unlocking via the device keypad even as a DTMF code.

Bluetooth Access Settings

Make sure that the My2N app is installed in your mobile phone to make successful authentication via Bluetooth.

GET IT ON Google Play Download on the App Store

CAUTION
The pairing code setting must currently be done in the old configuration interface.

Pairing Code Creation Using Device

1. Go to **Directory** and open the detail of the user for whom you want to create the pairing code.
2. Click Go to the old interface in the web configuration interface header.
   The user detail will open in the old configuration interface format.
3. Click in the **WaveKey** block.
   A pairing code will be generated in the open dialog box to be entered into the My2N application on your device.
4. Open the My2N app and enter the pairing PIN.

   NOTE
   If you already have an app connected to another device, you can enter the pairing PIN via the add icon at the top of the screen.

5. Follow the instructions on your mobile phone – bring the phone close to the device in the pairing mode and click Start pairing.

WARNING
Use the Mobile Key application for pairing of mobile phones with older OSs (Android 9 / iOS 17 and lower).

Mobile Key **Pairing**

1. Download the Mobile Key application to your mobile phone. The app is available at App Store and Google Play.
2. Open the application and enable Bluetooth access for Mobile Key.
3. According to the mobile key type, draw your mobile phone near the USB reader or the pairing device.
4. Click the device offered for pairing in Mobile Key.
5. The application prompts you to enter the PIN code. Enter the pairing code and confirm.

Bluetooth Authentication Methods

Different Bluetooth authentication methods can be set in the web configuration interface.

- **Directly in Mobile App** – the user selects the door to be unlocked directly in the My2N mobile app. If within the range of a 2N device, the user mobile device is will connect with the device and, if the access rules are met, the door will unlock.
- **Bringing Mobile Phone Close to Device and Touching Device** – a user with a mobile device and Bluetooth enabled approaches the 2N device and touches the Bluetooth authentication location on the 2N device, which is usually marked with a Bluetooth icon . Once the connection is established and access rights are verified, the door is unlocked.
- **Motion Detection** – the camera-equipped 2N devices detect movement in the surroundings, automatically activating Bluetooth. If a 2N device detects a user mobile device with valid access within its range, the door will unlock.

Accepted Bluetooth Authentication Method Settings

1. Go to **Access > Modules**.
2. Select the possible methods in **Start Authentication** on the **Bluetooth modules** tab.
3. If you selected “Motion Detection”, select the profile by which motion is to be detected.

NOTE
The motion detection profiles are set in **Customization > Camera > Internal Camera**.

License Plate Authentication Settings

Some devices support vehicle license plate recognition using external AXIS cameras equipped with the **VaxALPR** add-on application. The recognized license plates are sent in an HTTP request to the `api/lpr/licenseplate` endpoint (refer to the HTTP API Manual for IP Intercoms for more details).

TIP
The external camera adding procedure is described in ???.

HTTP API Service Enable

The license plate authentication is evaluated based on an HTTP request. Therefore, you must enable the appropriate HTTP API services on the device. This setting is still done in the older version of the web configuration interface. Refer to FAQ for more details.

Door Switch Settings

The door switch is a logical function of the device that controls the electric door lock. The switch can be activated in various ways (e.g. by HTTP command, RFID card or DTMF signal).

The door switch function in the device is performed by **Switch 1**.

You can assign control of another switch to a specific access module on the **Access > Modules** page.

Door Switch Settings

1. Connect the electric door lock contacts (e.g. magnetic contact) to the dedicated hardware output on the device.
2. Go to **Integration > Switches**.
3. Select the output to which the electric door lock is connected on the **Door Lock** card.
4. Go to **Integration > Switches**.
5. Open the configuration of the set switch by clicking the arrow in the tab header.
6. On the **Switch Configuration** tab, set the parameters of the hardware output that is to control the door switch.
   - **Controlled Output** – specify the output that switches the electric door lock.
   - **Mode** – Monostable / Bistable.
   - **Switch-on Duration** – set the switch-on time for a monostable switch. This value is not applied in the bistable mode.
   - **Output Type** – in the “Security” mode, the output operates in the inverted mode, which means that it is permanently switched on and controls the Security Relay using a specific pulse sequence. If you use a reverse door lock (i.e. the lock is locked when power is applied), set the output type to “Inverse”.

     TIP
     If you use a Security Relay, set the output type to “Security”.

     If multiple switches with differently set output types are connected to one output, the following priority is obeyed:

     1. Security
     2. Inverted
     3. Normal
7. You can set additional switch activation ways on the **Activation** and **Activation Codes** tabs. If you do not set any other methods, the switch will only be activated by allowing user access.
8. Save the changes.

Access Rules

The **Access > Access Rules** page sets the parameters and unlocking logic for the door managed by the device door switch. This configuration determines how access requests (authentication) are evaluated, the conditions necessary for successful user authorization and the rules for managing individual accesses.

While individual rights are set in the user settings, the access rules determine when, under what conditions and how these permissions can be used. For example, you can set whether door passage is allowed in one direction only, whether authentication can trigger a silent alarm, or whether the user may authenticate only once per defined time interval.

Door and Lock Status

The **Status** tab shows whether the door switch is active and whether the door is open.

Door

- “Open” – access has been granted, the door switch is closed and the door can be opened.
- “Closed” – the door is locked and cannot be opened.

Lock

- “Unlocked” – the switch is active and can be operated.
- “Locked” – the switch is disabled and cannot be controlled by the access rules.

TIP
The button with the lock symbol on this tab is used for locking/unlocking the switch from the web interface.

Door Open Sensor Settings

The device allows you to detect undesirable door states and generates an event whenever they occur. This event is recorded in the device log and can also be used as a trigger for automated actions (e.g. notification or alarm).

1. In the web configuration interface, go to **Access > Doors**.
2. Select the input to which the hardware sensor is connected and set the mode according to the contact type on the **Door Open Sensor** card.
3. Select which events should be evaluated by the sensor.
   When **Door Open Too Long Detection** is enabled, set the timeout after which the device will trigger the event.

Arrival and Departure

One device can be used for managing passages in two directions. You can attach some modules to the device on the opposite side of the door and then set these two sides separately. Thus, you can restrict at what time of the day passage will be allowed in the **Arrival** direction and at what time of the day passage will be allowed in the **Departure** direction, or what authentication methods will be accepted in a given direction, etc.

Module Assignment for Arrival or Departure

1. Go to **Access > Access Rules**.
2. Click Management on the **Modules** card on **the Arrival** or **Departure** tab.
3. A dialog box opens with a list of available access managing modules.
4. Drag and drop the modules into groups according to the direction they are supposed to provide.

TIP
Click to locate a specific module. The module triggers a visual or acoustic signal depending on its capabilities.

Access Rules

The access rules determine what authentication methods will be accepted for granting access. Multiple access rules can be set for different time profiles. The access rules can also help determine when any access should be denied.

You can use access rules for restricting the accepted authentication methods and thus forcing users to use an RFID card from 8:00 to 9:00, for example.

TIP
The authentication restriction is useful for the device that manages keys to **2N IP Fortis**. Users will thus be forced to regularly update the keys to **2N IP Fortis** on their RFID cards.

While setting the rules, you can choose to use a zone code for opening a door. The **Zone Code** is applied when the device is assigned to a bulk device management zone (in Access Commander, e.g.). The **Zone Code** can also be manually set in the **Advanced** section. It works similarly to **Switch Activation Code**; when entered on the module keypad, it will activate the door switch.

Silent Alarm

The silent alarm is a special unlocking mode, which allows you to trigger a security action unobtrusively. The silent alarm is used especially on premises and in buildings that are prone to robberies – casinos, financial centers, banks, etc. Once the PIN code is entered, the door opens, but at the same time an alarm is activated without the attacker noticing.

The silent alarm activation will trigger the **SilentAlarm** event. This event can be followed by Automation, for example:

- Sending an HTTP request to the security system.
- Taking images from the device camera.
- Setting up a call to a preset destination.

Silent alarm activation

1. The user enters a code one higher than the normal PIN.
   Example: The user has set a PIN code “1926”. The user enters the code “1927” to open the door. The door opens and the SilentAlarm event is triggered at the same time.

CAUTION
In order to be able to open the door with a PIN code (even if the Silent Alarm is triggered at the same time), you have to enable the **In/Out** tab below.

Blocking Access after Failed Attempts

Access will be blocked for 30 seconds after five consecutive unsuccessful access attempts. Access will not be allowed during this period even if the user authentication is valid.

This feature only blocks access by user authorization. The door switch can also be switched by other methods such as DTMF, HTTP command, etc.

QR Code Reading

The user access PIN code or the switch activation code can be read by the camera in the form of a QR code.

You need to set the **QR Code Reading Mode** for proper loading. The codes are always stored in the decimal format in the device. If read in the decimal mode, the QR codes read must exactly match the PIN codes (4 to 15 digits in length) stored in the device. In the hexadecimal mode, the QR codes are converted to the decimal number format after reading and only then compared to the stored decimal codes. Leading zeros are ignored during hexadecimal reading.

NOTE
Accepted hexadecimal range: 1000 to FFFFFFFF.

For QR code reading, you can also set that the codes only trigger the **CodeEntered** event instead of controlling the door switch. This event can then be followed by further actions via Automation.

The scanned QR code can be forwarded to an external access control system that communicates via a Wiegand interface (see ???).

Anti-Passback

Anti-passback is an extension of the access control system that prevents re-entry during a set time interval. The device in this mode only allows the user to enter once in a given time. After a user successfully enters, the system records this event and the user can only access the system again after a specified time has elapsed. This time is set when Anti-passback is enabled.

Anti-passback modes:

- “Hard” – The user cannot pass through the device in any direction for the set period of time. The user is denied access until the interval expires or access is restored by the device administrator.
- “Soft” – Rule violations are only logged and may alert the administrator, but the user is allowed access.

Wiegand Data Transfer

CAUTION
To forward Wiegand data, a Wiegand extension module must be properly connected to the device. The Wiegand extender is usually not included in the product package.

The Wiegand forwarding function allows the device to forward the authenticated user's identification data to an external access control system that communicates via the Wiegand interface. This ensures integration of the 2N devices with traditional access control systems. The setting allows you to select the appropriate group for data routing.

Data forwarding for Wiegand is set up in **Access > Access Rules > Entry/Exit > Advanced**. Sending authorizations of the users who have read their QR codes is set in **Entry/Exit** at the QR code reading enable.

Modules

The **Access > Modules** page provides central management of all access hardware technologies on the device. Each module has its own tab on the page for separate management. Both modules directly integrated in the device main unit and those connected via VBUS are managed here.

NOTE
The connected module is not detected automatically. Restart the device to display the connected module in the extending module list.

Each module can be named and assigned a specific switch to control. Other parameters depend on the module type.

In factory settings, all the modules control the door switch.

CAUTION
In case the firmware versions of the module to be connected and the main unit are incompatible, the module will not be detected. In this case, upgrade the device firmware (Firmware Update (p. 12)) upon module connection.

Door Open Sensor Settings

The device allows you to detect undesirable door states and generates an event whenever they occur. This event is recorded in the device log and can also be used as a trigger for automated actions (e.g. notification or alarm).

1. In the web configuration interface, go to **Access > Doors**.
2. Select the input to which the hardware sensor is connected and set the mode according to the contact type on the **Door Open Sensor** card.
3. Select which events should be evaluated by the sensor.
   When **Door Open Too Long Detection** is enabled, set the timeout after which the device will trigger the event.

Elevator Control

The device allows you to manage access to individual elevator floors in a building. After successful user authentication, the device activates the corresponding relay, which makes the selected floors accessible. The other floors can be publicly accessible without the need for authentication. You can time restrict access to the floors.

The elevator control is implemented using external Axis relay modules connected to the IP network. You can connect up to 8 relay modules to one 2N device, with each module containing 8 relays for floor control. The device thus controls access to up to 64 floors.

Requirements

- 2N device with an active license for IP intercoms or access units.
- Supported relay modules:
  - AXIS A9188
  - AXIS A9210
  - AXIS A9910
  - AXIS A9920

Elevator Configuration

Relay Module Connection

> **NOTE**
> The procedure is described in the documentation for the specific AXIS relay module, which is available at www.axis.com.

1. Connect the elevator controller inputs to the relay module.
2. Connect the relay module to the IP network and note its IP address.

Floor Configuration

1. Open the web configuration interface of the 2N device that is to manage the elevator accesses.
2. Go to **Integration > Access Control > Elevator**.
3. Click the pencil icon on the module row on the **Relay Modules** card.
4. Fill in the relay module IP address in the open field. Name the module for easy identification.
5. Repeat steps 4 and 5 for all the modules used in the specific elevator installation.
6. Enable the floors to which access is to be managed on the **Elevator Floors** card.
   a. Click the pencil icon for each floor.
   b. Name the floor for easy identification (e.g. Parking −2, Lobby, Level 22). The numerical designation in the access control configuration may not correspond to the floor numbering in the building.
   c. Select the available relay module to which the floor switch is connected in the **Module** parameter.
   d. Select the specific relay controlling the given floor in the **Relay** parameter.
   e. Save the changes.
7. If the module requires authentication to operate, enter the username and password on the **General** card.

   > **CAUTION**
   > Make sure that all the modules used in the installation have the same username and password.

8. Save the changes.

Access Settings

Setting User Access to Floors

1. Go to **Directory**.
2. Open the user detail by clicking on the row or select Add User to create a new user.
3. On **Elevator Access Settings**, select the floors that should be accessible to the user after the user authorization on the device.
   You can time restrict the access.
4. Save the changes.

Setting Public Access to Floors

1. Select the floors that should be accessible to the public (without authorization) on the **Elevator Floors** card.

2. Click the pencil icon at the selected floor.
3. Enable **Public Access** in the open settings.
4. Optionally, select a time profile or set a custom access time to limit the public access time.

Display Settings

Custom Display Language Upload

The web configuration interface allows you to customize the language texts displayed on the device. Thus, you can adapt the device to a different language environment or display custom messages.

1. In the web configuration interface, go to **Customization > Display**.
2. Download the translation file template on the **Language** tab. The template contains default English texts.
3. Open the downloaded file in a text editor.
4. Replace the English expressions in the file with your own texts.

> **CAUTION**
> Do not change the structure and format of the key phrases. If the syntax is modified or some items are missing, the translation file may not load correctly.

5. Save the modified file in the format `.ini`.
6. Return to the **Language** tab in the web interface and select “Custom” from the language drop-down menu.
7. The file upload option will appear – select and upload your modified `.ini` file.
8. Save the changes after successful upload.

Slideshow

> **NOTE**
> More demonstration modes can be set in addition to Slideshow (see Showcase Mode (**2N IP Style**) (p. 34)) on the **2N IP Style** display.

Slideshow is a demonstration mode that displays a sequence of images and videos on the screen. You can set the display time for each item (image or video).

1. Go to **Customization > Display**.
2. Enable the feature in the header of the **Slideshow** tab.
3. Set how long you want the home screen to go into the Showcase mode.
4. You can specify for each item whether the item should be displayed only in a specific time window or outside of it. Click Edit Slideshow to set view by time windows. Expand the advanced menu by clicking for a specific item to set when the item should be displayed in the Slideshow.
5. Save the changes.

Showcase Mode (2N IP Style)

The Showcase mode on **2N IP Style** is a display state into which the device goes after a certain period of inactivity on the home screen. The device display can show, for example, a series of pictures or videos, an address of a building or date and time.

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

Showcase Mode Settings

1. Go to **Customization > Display**.
2. Enable the function in **Showcase Mode** in the header of the tab.
3. Set how long you want the home screen to go into the Showcase mode.
4. Select a Showcase mode type.
5. You can enable the display of information pictograms about the antibacterial surface or the touch icon in the **Icon Display** section.
6. Save the changes.

Slideshow

Slideshow is a demonstration mode that displays a sequence of images and videos on the screen. You can set the display time for each item (image or video).

You can specify for each item whether the item should be displayed only in a specific time window or outside of it. Click Edit Slideshow to set view by time windows. Expand the advanced menu by clicking ⋮ for a specific item to set when the item should be displayed in the Slideshow.

Logo

The **Logo** mode is used for displaying a static company logo on the screen.

You can upload a background image for the display (behind the logo) on the **Background Image** tab.

Text

The **Text** mode displays a static text on the screen, such as the facility address, a welcome note or some other information for the people moving around the facility, for example.

Date and Time

The **Date and Time** mode displays the date, current time and location of the device.

Information Messages (2N IP Style)

The **2N IP Style** device can show pre-set information messages on its display. Having been granted access, the users or visitors can then be shown a message that guides them around the building, informs them of current events, etc.

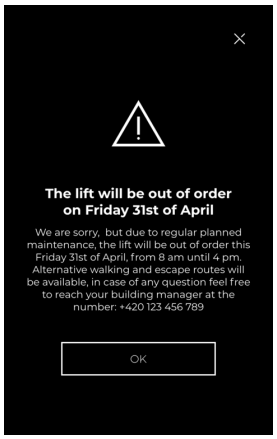
On each tab, you can set specific information messages for each of the following events:

- **Authorized User** – this message is displayed whenever a user stored in the device directory authenticates on the device.
- **Visitor** – this message is displayed whenever a visitor is allowed access during a call. A visitor is a person who initiated a call from a device to a user in the directory. The message appears when this user grants access to the visitor during the call.

- **Access Denied** – this message is displayed when the device denies access.

Information Message Settings

1. Go to **Access > Information Messages**.
2. From the page tabs, select the information message type you want to set up.
3. Enable the information message in the tab header.
4. On the **Scheduling and Time Settings** tab, set the time for the time message to be displayed and also specify how long the information message should stay on the display.
   You can also specify the calendar period for which the message should be displayed.
5. Create a message on the **Message Content** tab. You can either create a text message or insert an image.
6. Save the changes.



Example of a picture and text information message

Advanced Settings

Camera and Video Settings

The 2N intercom internal camera transmits an image to the other party during a video call, detects movement in the surroundings and reads QR codes,

It is possible to connect external cameras to the device, from which it will be possible to display the image. In addition to the video from the called device, you will be able to see the view from another camera during a call.

It is possible to connect external cameras to the device, from which it will be possible to read the image.

Internal Camera Settings

1. Go to **Customization > Camera**.
2. Click → on the **Internal Camera** tab.
3. The **Settings** tab allows you to edit the basic camera image parameters.
4. Once saved, the changes will be reflected in the camera preview.

Mode

The camera mode allows you to set the optimal combination of exposure mode and power frequency to achieve stable and high-quality images. This mode is helps reduce unwanted flickering, which may occur when artificial lighting is used or when the mains frequency varies. When the cameras are installed indoors, a suitable method of suppressing flicker caused by light sources can be selected, while when placed outdoors, a direct sunlight suppression mode can be activated to ensure the optimal image adaptation to the current lighting conditions.

IR LED

The IR LED illumination helps ensure a high-quality image even at low ambient light levels. This mode is triggered whenever the light conditions drop below the set level. The limit level of the light conditions is not set until the IR LED illumination is enabled.

NOTE
If the allowed power consumption might be exceeded – for example, when multiple PoE-powered extending modules are operating simultaneously – the IR power level is automatically optimized to maintain the stability of the device function.

Advanced Settings

Day/Night Mode – switch between color and black and white images depending on the lighting conditions. Set **Always Day** if you want the camera to use an IR suppression filter and the IR illumination to be off. The "Always Night" setting, on the other hand, turns off the filter and turns on the IR illumination, which switches the image into the black and white mode suitable for night vision. The Auto mode switches between these two camera states according to the ambient light level.

Local Contrast – enhances details and textures by increasing the brightness differences between adjacent areas of the image (edges).

Tone Mapping – increases the brightness and visibility of the image, but may cause slight color distortion.

Maximum Exposure Time – specify the maximum time of the image exposure. Where more light is available, the shutter does not have to be open for the whole time and the camera sets a shorter shutter speed automatically.

External Camera Settings

The external camera is added to the 2N device as a video stream (RTSP). An external camera allows you to switch between views from different cameras during a call. The external camera's function is therefore purely display.

CAUTION
QR codes can only be read on the device internal camera.

Adding External Camera:

1. Go to **Customization > Camera**.
2. Select Add Camera on the **External Camera** tab.
3. In the dialog box that opens, enable the camera.
4. Enter the stream source address of the external IP camera in the format `rtsp://ip_address_camera/parameters`.
5. If the external camera stream is subject to authentication, fill in **login details for the stream**.
6. Click Add Camera to save your changes.
7. If the external camera is to be the main camera of the device, then after saving it on the **External Camera** tab, click Set as Default Source.
   When you talk to the device, the image from the camera set as the default source is displayed first.

Privacy Policy

The Privacy feature masks a part of the video image of the **internal camera** so that this part is not visible in the video or otherwise recorded (e.g. for motion detection purposes). This option is ideal for situations where you want to protect sensitive areas of the image. For example, if the device is located at the reception and the camera also records the corridor where strangers pass, you can hide the corridor area.

CAUTION
Privacy protection may restrict the activity of reading QR codes or motion detection. We do not recommend using privacy protection with these features at the same time.

Privacy Area Settings

1. Go to **Customization > Camera**.
2. Click → on the **Internal Camera** tab.
3. Click the pencil icon ✎ next to the **Privacy** parameter on the **Camera Preview** tab.

4. In the camera preview, adjust the square to cover the area to be masked.

> **CAUTION**
> The image area is relative to the current image cutout. If you change the camera image crop, the existing areas will remain the same, but will effectively cover a different part of the space. It is therefore always recommended that these areas are checked and edited after editing a cutout.

5. Select a cloaking mode:
   - **Color** – the selected area will be overlaid with a color of your choice
   - **Mosaic** – the selected area will be pixelated. Set the size of the mosaic according to the level of data anonymization needed.
6. Do not forget to enable privacy protection in the parameter settings header!
7. To save your changes, click the **Save** or **Save and Close** button at the top of the page.

Motion Detection

Motion detection on the 2N devices is a feature that automatically detects motion in the field of view of the **internal camera** and can trigger various actions, such as activating Bluetooth or sending a notification.

For optimal performance, detection can be calibrated to the environment and conditions, for example by changing the sensitivity parameters and the area to be monitored by the camera.

Privacy Area Settings

1. Go to **Customization > Camera**.
2. Click → on the **Internal Camera** tab.
3. Click the pencil icon ✎ next to the **Motion Detection** parameter on the **Camera Preview** tab.
4. A window opens with the motion detection profile settings.
5. Expand the tab of the profile to be set up.
6. By adjusting the square in the camera preview of a specific area in which the camera should record motion.

> **CAUTION**
> The image area is relative to the current image cutout. If you change the camera image crop, the existing areas will remain the same, but will effectively cover a different part of the space. It is therefore always recommended that these areas are checked and edited after editing a cutout.

7. Select the motion capture mode for the profile, see Profile Modes (p. 39).
8. Set other parameters, if necessary, according to the mode.
9. Always remember to enable the profile!
10. To save your changes, click the **Save** or **Save and Close** button at the top of the page.

Profile Modes

Event Trigger

In this mode, the camera captures instantaneous, one-time movements. An example of use is taking a picture when someone enters a room or when a vehicle passes near the device.

The activation of the triggered event can be delayed by setting a delay.

Use the filter to define the types of movements for the camera to ignore – for example, small objects (small birds) or repetitive movements (trees in the wind).

Uploading

This profile will trigger an event of 30 seconds whenever motion is detected. If another movement occurs during this time, the profile will combine everything into one event. This mode is suitable for continuous monitoring and prevents the creation of a large number of short records.

Use the filter to define the types of movements for the camera to ignore – for example, small objects (small birds) or repetitive movements (trees in the wind).

Face Detection

The profile detects motion when a face appears in the monitored area. An event can also occur when a static image of a face (e.g. a photograph) appears in the frame.

Incoming Person Detection

The profile only recognizes moving people and ignores static images of faces.

Creating Video Stream from Device Camera

The video streaming function helps transmit live video from the device**internal camera** over the network to a receiving device, such as a mobile app, surveillance software or a video player on a computer. This process ensures that the users can watch real-time video from different devices.

Creating Video Stream

1. Go to **Integration > ONVIF / RTSP**.
2. Enable the **RTSP Server** service.
3. Set the stream parameters, see Video Stream Parameters (p. 40).
4. You can fill in the IP addresses from which the stream will be available on the **Connection Restrictions** tab. If no IP addresses are filled in, it is possible to connect from any IP address.
5. On the **Preconfigured Streams** tab, specify whether the stream should be accessible:
   - anonymously
   - with authentication – set the authentication details in **Authentication**.
6. On the **Preconfigured Streams** tab, you can find the IP addresses of the configured streams according to the selected video codec.

Video Stream Parameters

General Stream Settings

Jitter Compensation – set the buffer length for compensation of interval unevenness in audio packet arrivals. A longer memory means higher outage resistance, but longer audio delay.

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

UDP unicast enabled – enable audio/video stream sending via the RTP/UDP. If this mode is off, the audio/video stream data are sent via the RTP/RTSP only.

Starting RTP Port – set the initial local RTP port in the range of 60 ports used for audio and video transmission. The default value is 4800 (i.e. the range is 4800–4859).

Zipstream – select the default Zipstream compression level (for H.264). AXIS Zipstream retains all the required important forensic details while decreasing the data transmission and storage requirements by 50% on the average.

Custom Format Stream Settings

1. Click Generate Stream URL on the **Custom Format Streams** tab. A dialog box opens.

2. Set the following in the dialog box:
   - **Codec** – select an item from available codecs.
   - **Enable audio** – specify whether to transmit video only or video with audio.
   - **Resolution** – set the image resolution.
   - **Framerate** – set the frame rate of the recorded video.
   - **Bitrate** – set the bitrate.
   - **Zipstream** – select the default Zipstream compression level (for H.264). AXIS Zipstream retains all the required important forensic details while decreasing the data transmission and storage requirements by 50% on the average.
3. The stream address with parameters is automatically loaded at the bottom of the dialog box.
4. Copy the stream address and save your changes.

Sound Settings

Device Volume Setting

To adjust the volume of your device, go to **Customization > Audio**.

The master volume determines the basic volume level of all the other sounds in the device. Set this parameter considering the noise level of the environment in which the device is installed. So the setting of the other sounds is always relative to this **Master Volume**.

Adaptive Volume

You can enable automatic volume adjustment based on the ambient noise on the **Adaptive Volume** tab. This feature is particularly suitable for installations in environments where the ambient noise is variable.

On the tab, set **Sensitivity Threshold**, after which the device volume will start to increase. The device can be amplified up to an adjustable value of **Maximum Sound Amplification**.

Audio Transmission in Calls

The call audio parameters are set directly on the tab of the service that provides the call (Calling via SIP (p. 18) or Local Calls between 2N Devices (p. 19)), in the **Video** folder.

1. Open the **Calling** section.
2. Go to the page of the service providing the call (specific SIP account, Local calls).
3. Open the **Audio** tab.
4. Here set the necessary sound parameters.

DTMF Signal Transmission Enable

It is possible to switch on the door lock and thus open the door using the DTMF commands sent to this device.

1. Open the **Calling** section.
2. Go to the page of the service providing the call (specific SIP account, Local calls).
3. Open the **Audio** tab.
4. On the **Sending DTMF** tab, select **Sending Mode** to determine during which calls the DTMF signals can be sent.
5. Select the required DTMF sending methods.

   TIP
   Check that you have enabled the methods that are accepted by the device to be called.

6. Then set the DTMF methods that the device will receive on the **Receive DTMF** tab.
7. Save the changes.

User Sounds

The device performs several actions that are accompanied by sound (ringing, switching, etc.). You can change the sounds to be played in **Customization > User Sounds**.

You can upload up to 10 custom sounds to the device library for individual actions.

TIP
You can record user sounds directly using a microphone connected to your computer via the web configuration interface. Choose **Audio Recording in the advanced menu in User Sound Library.**

Other Device Audio Features

Multicast

The device is able to transmit audio from the microphone using RTP packets sent to a multicast address and at the same time receive an audio stream in the same format, which will subsequently be played back by the device through a built-in speaker (or another configured audio output).

Noise Detection

The device can monitor the sound received by the microphone, and when the microphone signal level exceeds the set threshold, the device can generate the `Event.NoiseDetected` event. This event can be followed by other actions in Automation (see Automation (p. 60)).

Noise Detection Activation

1. Go to **Integration > Audio**.
2. Enable the function in the header of the **Noise Detection** tab.
3. In the **Noise Threshold Level** parameter, specify the value [dB] that triggers the **Event.NoiseDetected** event when exceeded.
4. In the **Alarm Start Delay** parameter, you can set the period of time for which the noise must be above the threshold level for the event to be triggered.
5. In the **Alarm End Delay** parameter, on the other hand, you can specify the period of time for which the signal must be below the threshold for the event to end.

Audio Test

Refer to **Integration > Audio > General > Audio Test** for the result of the last test.

The 2N devices can perform a periodical check of the integrated speaker and microphone. For the test purpose, the integrated speaker generates one or more short beeps. The integrated microphone receives the generated tone and the test is successful if the tone is detected correctly. The test takes approximately 4 seconds. If the test fails (which may be due to an extreme surrounding noise level, e.g.), a new test is carried out in 10 minutes. The result of the last test can be displayed in the web configuration interface of the device or processed using Automation.

NOTE
If a call is active when the audio test starts, the audio test will be put off until the call is terminated. The audio test will be performed the moment the call is terminated.

Informacast

If your device supports the InformaCast protocol for streaming audio, you can find its settings in **Integration > Audio > Informacast**. InformaCast helps you set up an audio stream (unicast/multicast RTP/UDP encoded with G.711 U-law) between a 2N device and an InformaCast server (or any other InformaCast client).

Once the service is enabled in **Integration > Audio > InformaCast**, the InformaCast servers are automatically found in the local network using the SLP protocol and the 2N device is automatically registered with them.

Time Profiles

Some of the functions performed by the device are time dependent. The **Time Profiles** section allows you to preset time intervals and select them for these functions. This means you do not have to manually enter time whenever you set a time profile. You can name the time profile for better clarity.

Time Profile Creation:

1. Go to **Customization > Time Profiles**.
2. Click on empty to create a new profile.
3. Enter a profile name.
4. Click Save. The profile detail will open.
5. Set the intervals at which the time profile should be active.
   1. Click on the required interval.
   2. You can specify the profile start and end in an open menu.

   NOTE
   The **Holidays** line helps you set different time intervals during selected days, see Holidays (p. 43).
6. Save the changes.

Holidays

In the device configuration, you can define several days that will be marked as holidays. Special intervals are then set in the time profiles for these days. Typically, these are such days as public holidays, company holidays and other special days.

For each holiday, you specify whether it applies only to a particular year or whether it repeats on the same day each year. Holidays can be planned several years in advance.

Holiday Settings:

1. Go to **Customization > Time Profiles > Holidays**.
2. Select the year for which you want to set the holiday.
3. Click a day in the calendar:
   - The first click marks the holiday that will be repeated on the given day and month every year.
   - The second click changes the holiday to a one-time holiday for the selected year.
4. Save the changes.

Advanced SIP Account Settings

This section describes the optional features and SIP account parameters that are set in the **Calling > SIP** section.

The advanced SIP account settings allow you to increase security, optimize call quality and ensure compatibility with different PBXs. We recommend that only experienced administrators change the settings.

1. Go to **Calling > SIP** of the account to be set up.

SIP Functions

The REFER method allows for dynamic forwarding of active calls between various SIP identities, which provides a more flexible control of communication flows.

The PRACK method provides reliable acknowledgement of continuous call states between devices, which improves the communication quality and stability in SIP systems.

Media

Receive Only Encrypted Calls (SRTP) – allows you to receive SRTP-encrypted calls only. Unencrypted calls will be automatically 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.

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.

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.

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

Do Not Play Incoming Early Media – disable playing of the incoming audio stream before call pick-up, which is sent by some PBXs or other devices. A standard ringtone will be played instead.

Advanced Settings

Sending 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.

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

IP Address Filter – 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.

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.

Facial Zoom in Video Call

The **internal camera** can detect a face during a video call and adjust the video crop and focus to focus on the face of the person standing in front of the device. This makes it easier for the other party of the call to identify the person in front of the device.

The following **Zoom Modes** are available:

- “PTZ” – manual mode controlled using DTMF from the other side of the video call.
- “Face Zooming” – the camera automatically detects the face and zooms in on it.
- “Tilt Zooming” – the camera adjusts the view to a predefined area where a face is expected to appear.

Tamper Switch Settings

The tamper switch detects the opening of the device cover, which is evaluated by the software as a logical switch closure. In this way, the switch indicates any potential physical tampering with the device.

When you activate a tamper switch, you can disable all the other switches or set up Automation to trigger a follow-up action, such as sending an email, creating an HTTP request or activating a silent alarm.

NOTE
Depending on the device type, the tamper switch can either be integrated in the main unit or additionally installed as an extending module. Refer to the Installation Manual of your device for installation instructions.

Blocking other switches when the cover is opened

The device allows you to ensure that the other switches are blocked when the cover is opened (i.e. when the tamper switch is activated). This also prevents the door switch from being activated and thus prevents entry through the door that controls the device.

Switch Blocking Setting

1. Go to **Integration > I/O**.
2. Assign a tamper switch to the input on the **Tamper Switch** tab.
3. Enable **Automatic switch blocking**.

Tamper Switch Events

The tamper switch activation generates events. These events can be followed by Automation (p. 60).

- Opening the cover generates the `TamperSwitchActivated (state: in)` event.
  If the switch is assigned as an input in the **I/O section**, the `InputChange (port: tamper, state: false)` event is generated too.
- Closing the cover generates the `TamperSwitchActivated (state: out)` event.
  If the switch is assigned as an input in the **I/O section**, the `InputChange (port: tamper, state: true)` event is generated too.

HTTP API

HTTP API is an application interface designed for the control and monitoring of selected 2N device functions via HTTP/HTTPs. HTTP API allows you to remotely perform actions (door opening, etc.), obtain device state information or receive event notifications. This interface enables the 2N devices to be integrated easily with third party products, such as home automation, security and monitoring systems in buildings, etc.

NOTE
Refer to the HTTP API Manual for the list of available API methods, parameters and replies. This subsection describes the HTTP API configuration on the device only.

Activation of API Services

1. Go to **Integration > HTTP API** in the web configuration interface.

2. Go to the **HTTP API Configuration** tab on the **Services** page. Find the required services on the card:

Service	Description
System Settings	Access to general system information and device settings (name, network configuration, restart, firmware, etc.).
Access Control	Remote management of access rules, users and access profiles.
Switches	Device switch (relay) control – remote door unlocking, e.g.
Inputs and Outputs	Digital input state reading and device output control.
Display	Intercom display content control (text, message, etc. display).
E-Mail	Send e-mail notifications or configure e-mail parameters via API.
Calling	Call management.
Logs	Access to system logs and device event logs.
Automation	Integration with automation rules and scenarios defined in the device.

3. For the services to be activated, switch to the active position in the **Enabled** column.

CAUTION
By shutting down the service you immediately disable calls to all of the API accounts. Make sure that the service is not used actively by any of the connected systems before turning off. Use of the services can be easily checked on the **Account Authorization Overview** tab below.

4. **Communication Method Settings**
Select whether the communication will be encrypted in the **Connection Type** column:
   - **Unsecure (TCP)** – for isolated network testing only. Data transmitted without encryption can be captured.
   - **Secured (TLS)** – for regular and production operation. The data is encoded via the TLS (HTTPS) protocol.

5. **Authentication Settings**
   Select the method to be used by the API client in the **Authentication** column:

Method	Description
None	Unverified. Anyone with network access can make API calls.
Basic	The username and password are sent in Base64 encoding. If used without TLS, login data can be easily captured.
Digest (RFC 2617)	The password is not transmitted directly – the client responds with a hash value to the server request.
Digest (RFC 7616)	Improved Digest version with SHA-256 support.

6. Save the changes.

API Account Settings

1. Go to **Integration > HTTP API** in the web configuration interface.
2. Go to the account tab (e.g.: **Account 1**).
3. Move the switch to **Enabled** in the card header.
4. Set **User Name** and **Password**.
5. Scroll through the list of service access rights and select only those that the API account should have access to in the given mode:
   - Control (write) – the account can control the function actively
   - Monitoring (read only) – the account can only read the state

> **NOTE**
> Assign the account the minimum rights necessary. The door unlocking account needs no access to the system settings or e-mail.

6. Save your changes.

Troubleshooting

Unable to connect to API

- Make sure that HTTP API is enabled.
- Check the network availability of the device.
- Make sure that the correct protocol has been selected (HTTP / HTTPS).

Authentication failing

- Check the user name and password for the account.
- Make sure that the selected authentication method matches the client configuration.

API call not working

- Make sure that the account has been assigned permission for the service.
- Check whether or not the service has been deactivated.

System

Date and Time Settings

CAUTION
If the device is managed by a bulk management tool (2N Access Commander / 2N My2N), the device time can be managed by this tool. Manual changes in the device web interface do not affect the time setting.

NTP Synchronization

If the device is connected to the Internet, the time and date values can be synchronized using NTP.

1. Go to **System > Date and Time**.
2. Activate the **Automatic Time from NTP or Internet** option on the **Time Synchronization Settings** tab.
3. Enter the address of the NTP server of your choice.

Time Update at Outage

1. Go to **System > Date and Time**.
2. Click Sync with Browser on the **Time Sync Settings** tab.
   This synchronizes the device time with your PC time.

NOTE
The 2N devices are equipped with a real-time clock to back up the device for even a few days in case of power outage.

Network Configuration

By factory default, uses a dynamic IP address assigned by the DHCP server.

A proper IP address configuration is crucial for a stable and reliable connection of the device to your network.

1. Go to **System > Network Connection** to set the device network parameters.

2. You can enable/disable the DHCP server in Basic Settings > IP Address Settings.

   Static IP Address Setting:

   a. Disable the **DHCP Server** option.
   b. Enter the desired IP address, subnet mask, default gateway and DNS servers.
   c. Save your changes. The device will be restarted.

   DHCP Settings

   a. Enable the **DHCP Server** option.
   b. Enter the desired IP address, netmask, default gateway and DNS servers.
   c. Save your changes. The device will be restarted.

> **NOTE**
> If you use the RADIUS server and 802.1x-based verification of connected equipment, you can make the devices use the EAP-MD5 or EAP-TLS authentication. Set this function on the 802.1x tab.

Firewall

> **CAUTION**
> To ensure maximum protection of your device from unauthorized access, we strongly recommend activating and properly configuring a network firewall.

1. Go to **System > Network Connection > Firewall**.
2. Enable the **Firewall** service in the tab header.
3. Save the changes.

Licenses

Some features are only available under the appropriate license. Refer to **System > Licenses > General Information** for an overview of licenses and their active statuses. Find an overview of the available features that are subject to a license on the **Licensed Features** tab.

> **NOTE**
> Having selected the appropriate license, contact your 2N dealer. If you are a 2N partner, you can contact our customer service department at customercare@2n.com. Please indicate the serial number of the device in your request.

License Key Update

The current license key is available on the update server. If the web configuration interface does not provide access to the public Internet, you can manually upload the key file to the device.

Whenever the device reboots, the last available license key is reloaded.

Trial License

The trial license allows you to temporarily use all the features of the Gold license and Microsoft Teams license for a maximum of 800 hours after activation. An activated trial license cannot be suspended.

Go to **System > Licenses > Trial License** to activate a trial license.

CAUTION
One hour of the trial license is removed each time the device is rebooted.

Overview of Licensed Features

Features	Licenses
Sound • User Sounds • Automatic Sound Test • Noise Detection	Free
Security • HTTP API • 802.1x support • SIPS (TLS) support. • SRTP support • Silent Alarm • Limit unsuccessful access attempts • Switch Blocking • Encoded Keypad • Anti-Passback	Free
HTTP API support	Free
NFC support	Free
Video • Audio/Video Streaming (RTSP Server) • External IP camera support • ONVIF support • PTZ function support • Motion detection support	Gold

Features	Licenses
Integrations • Extended switch setting options • Automation functions • E-mail sending (SMTP Client) • Automatic Update (TFTP/HTTP Client) • FTP Client • SNMP client • TR-069 • Genetec Synergis	Gold
Elevator Control	Gold
Paging and emergency communication via the Cisco platform	InformaCast
C-CURE 9000 Server Communication	CCUR Plug-In
Communication with OnGuard server (LenelS2)	OnGuar Plug-In
Communication with the Symmetry server	Symmetry Plug-In
Communication with MS Teams	Licence Microsoft Teams

Event Log

The following overview describes the events that may be generated by the device during operation and briefly describes their conditions. Event availability may vary depending on the device type and configuration.

Event	Description
AccessBlocked	Occurs when access is blocked.
AccessLimited	Occurs after five unsuccessful authentication attempts. Access will then be blocked for 30 seconds.
AccessTaken	Occurs when a card is tapped in the Anti-passback area.
ApiAccessRequested	Occurs when HTTP API `/api/accesspoint/grantaccess` is called successfully.

Event	Description
AudioLoopTest	Occurs when the device microphone and speaker test is completed.
CallSessionState-Changed	Occurs when the call state changes (create, connecting, ringing, connected, terminated). One call can include multiple calls. For example, calling a phone number in a group with a contact deputy creates two simultaneous calls to two different destinations. The event description includes information on the change type, call identifier, current call address and call sequence.
CallStateChanged	Occurs when the call state changes (ringing, connected, terminated). The event description includes information on the change type, call direction (incoming, outgoing) and counterparty/SIP account identification.
CapabilitiesChanged	Occurs when the available device functions change.
CardEntered	Occurs when a card is tapped on the reader.
CardHeld	Occurs when the card is held at the reader for more than 4 seconds.
CodeEntered	Occurs when the code is entered via the numeric keypad and terminated with *.
ConfigurationChanged	Occurs when the device configuration changes.
DeviceState	Occurs when the device state changes (startup, e.g.).
DisplayTouched	Occurs when the display is touched (on the main unit or an extending module connected via VBus).
DoorOpenTooLong	Occurs when Door opening too long is detected.
DoorStateChanged	Occurs when the door state changes (opens/closes).
DtmfEntered	Occurs when a DTMF code is received in or locally off the call.
ExternalCameraState-Changed	Occurs when the external camera state changes.

Event	Description
FingerEntered	Occurs during fingerprint authentication.
InputChanged	Occurs when the logic input changes (including tamper switch).
KeyPressed	Occurs when a button is pressed. The digits are marked 0, 1, 2..., 9. The quick dial button sequence is %1, %2,... The numeric keypads are marked `0-9`. The quick dial button sequence is `%1, %2`, etc.
KeyReleased	Occurs when the button is released. The numeric keypads are marked `0-9`. The quick dial button sequence is `%1, %2`, etc.
LicensePlateRecog-nized	Occurs when the registration plate of a vehicle with valid access rights is recognized, see License Plate Authentication Settings (p. 27).
LiftConfigChanged	Occurs when a Elevator Control (p. 32) setting is changed.
LiftFloorsEnabled	Occurs when elevator floor access is allowed.
LiftStatusChanged	Occurs when the elevator control module is connected or disconnected.
LoginBlocked	Occurs after 3 unsuccessful login attempts. The event description contains information on the IP address of these attempts.
MobKeyEntered	Occurs during Bluetooth authentication.
MotionDetected	Occurs when motion is detected in the camera record, refer to Motion Detection (p. 39).
NoiseDetected	Occurs when an increased noise level is detected, see Other Device Audio Features (p. 42).
OutputChanged	The command occurs when the logic output state changes.
PairingStateChanged	

Event	Description
RegistrationState-Changed	Occurs when the SIP Proxy registration changes.
RexActivated	Occurs when an input configured as the REX button is activated.
SilentAlarm	Occurs when silent alarm is triggered, see Silent Alarm (p. 30).
SwitchesBlocked	Occurs when an invalid access attempt is made while the switch is blocked.
SwitchOperation-Changed	Occurs when the switch function changes. The event signals a switch lockdown/hold state, switch permanent hold or timer change (start, restart, quit).
SwitchStateChanged	Occurs when the switch state changes.
TamperSwitchActivated	Occurs when the state of the tamper switch that reacts to the device cover opening/removing changes.
UnauthorizedDoorOpen	Occurs when an unauthorized door opening is detected.
UserActionActivated	Signals a user action initiated by the user action trigger assigned to it.
UserAuthenticated	Occurs when the user authentication and authorization have been successful.
UserRejected	Occurs when a user authorization is invalid.
WaveKeyActivated	Occurs when Bluetooth authentication is activated.

Default Reset

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

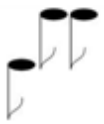
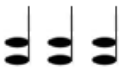
CAUTION
Restoring the default settings deletes the uploaded license key. Save your license key before restoring the default settings.

1. In the web configuration interface, go to **System > Maintenance**.
2. Press the Restore Default Settings button.

NOTE
A complete factory reset is performed on the device hardware, see the Installation Manual for the device.

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.

Sound signaling	State
	Reset of network parameters Upon power up, the network parameters can be changed by hardware, refer to Brief Guidelines.
	Approaching call end signaling The device allows you to set a call end timeout, **Calling > General settings > Call time limit**.
	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.

Used Ports

Service	Port	Protocol	Direction	On by default	Configurable	Settings
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device discovery)*	8002	UDP	In/Out	✓	×	–
FTP	21	TCP	Out	×	×	–
2N IP Eye	8003	UDP	Out	×	×	–

Service	Port	Proto-col	Direc-tion	On by default	Config-urable	Settings
HTTP	80	TCP	In/Out	✓	✓	**System > Network connection > WEB SERVER tab**
HTTPS	443	TCP	In/Out	✓	✓	**System > Network connection > WEB SERVER tab**
Multicast audio	22222	UDP	Out	×	✓	**Integration > Audio**
Multicast audio for ICU protocol	8006	UDP	Out	×	×	–
Multicast video for ICU protocol	8008	UDP	Out	×	×	–
Multicast video (wide) for ICU proto-col	8016	UDP	In/Out	×	×	–
NTP client	123	UDP	In/Out	✓	×	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	×	×	–
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	×	✓	**Calling > General Settings**
RTP+RTCP ports (external camera)	4800+ (range of 64 ports)	UDP	In/Out	×	✓	**Integration > ONVIF / RTSP**
RTSP client	554	UDP	In/Out	×	✓	

Service	Port	Protocol	Direction	On by default	Configurable	Settings
RTSP server	554	UDP	In/Out	×	×	–
SingleWire Commands	80	TCP	In/Out	×	×	–
SingleWire Communication	8081	TCP	Out	×	×	–
SingleWire Media	20000+	UDP	In	×	×	–
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	**Calling > SIP**
SIPS	5061	TCP	In/Out	×	✓	**Calling >SIP**
SMTP	25	TCP	Out	×	✓	**Integration > Email notification**
Syslog	514	UDP	Out	×	×	–
TFTP	69	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
SSDP	1900	UDP	In/Out	✓	×	–
SDDP	1902	UDP	In/Out	✓	×	–

Service	Port	Proto-col	Direc-tion	On by default	Config-urable	Settings
Multicast receiver (Automation)	4433	UDP	In	×	×	–
WS-Discovery	3702	UDP	In/Out	✓	×	–
CIP Client (Crestron)	41794	UDP	In/Out	×	×	–
Sitechannel (ICU protocol)	8004	UDP	In/Out	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

Automation

NOTE
This feature is only available with the Gold license.

The standard 2N device configuration covers the most common scenarios. The Automation function can be used for such advanced cases as the need to customize the device to specific requirements or integrate it with third-party systems. Automation allows you to define the custom logic for the device behavior, which responds to variable events, signals or combinations of conditions. For example, you can trigger specific actions by pressing a speed dial button, activating the Silent Alarm, detecting an open door, closing an entry or detecting movement near the device.

Automation Settings:

1. Go to **Integration > Automation** in the device web interface.
2. Enable the number of functions as required in the function overview.
3. Click to open the Automation configuration interface.
4. Type the name of the function under which the function will be saved in the Automation interface header.
5. Create an Automation flow.
   A detailed description of the Automation function and configuration is available in Automation manual.
6. Once the function is complete, click SAVE and exit the Automation interface.

2N.com/manuals

IP intercoms – Configuration manual

© 2N Telekomunikace a. s., 2026

2N.com