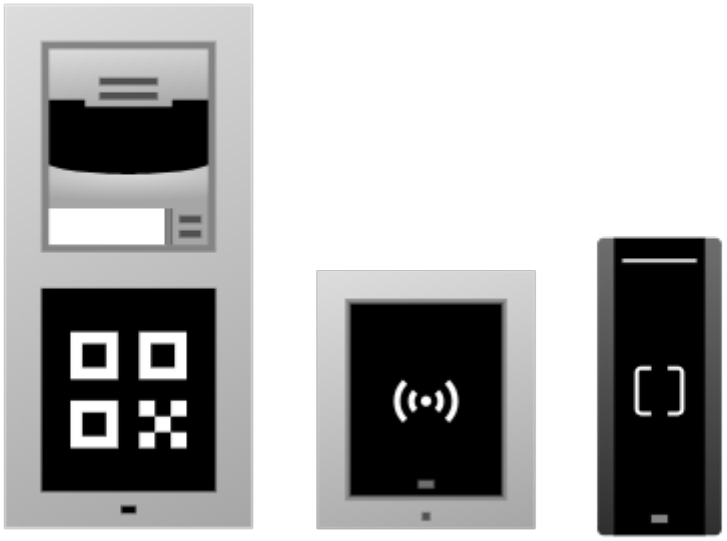
Access Control Units

Configuration manual



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

2N.com

Table of Contents

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 : 2NAccessUnit-{serial number without dashes}.local (e.g.: “2NAccessUnit-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:

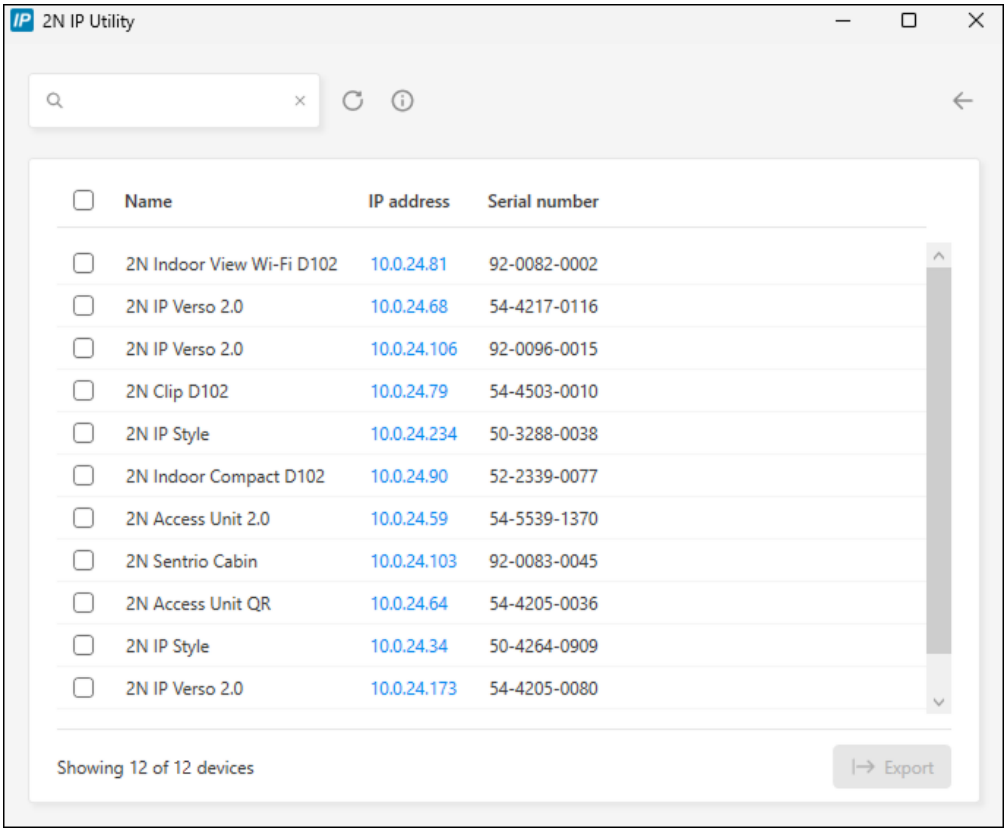
- with the RESET button

IP Address Retrieval Using 2N IP Utility

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

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

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



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

TIP

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

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

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

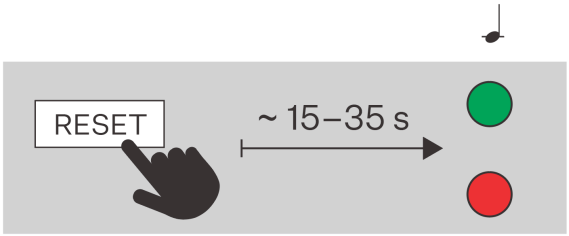
For increased password security, it is recommended that:

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

IP Address Retrieval Using the RESET button

Follow the instructions below to retrieve the current IP address:

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



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

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:

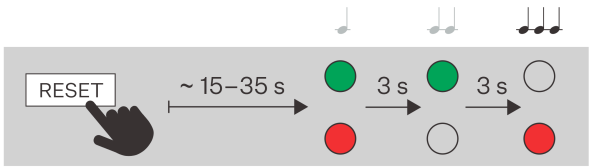
- with the RESET button

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

Dynamic IP Address Setting via RESET

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

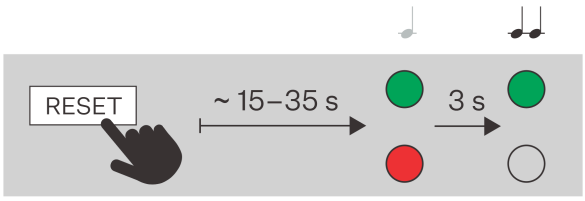
1. Press the button RESET and keep it pressed.
   a. Wait until the red and green LEDs go on simultaneously on the device and the acoustic signal can be heard ♩ (approx. 15–35 s).
   b. Wait until the red LED goes off and an acoustic signal can be heard ♩♩ (approx. for another 3 s).
   c. Wait until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



Static IP Address Setting with RESET Button

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

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



NOTE
The following network parameters will be set after restart:

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

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. 3)).
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

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

NOTE

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

Getting Firmware from Update Server

1. Go to **System > Maintenance > Firmware**.
2. Click Check for Updates.
3. If an update is available, its release notes are loaded. To start the upgrade, click Upgrade in the window header.
4. Once the firmware is uploaded successfully, the device is restarted automatically. After the restart, the device becomes fully operational with a new firmware version. The FW upgrade does not affect configuration.

Uploading New Firmware from Storage

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

NOTE

The functions, reliability and security of the device depend on the firmware installed. Regular firmware upgrades to the latest version are included in the product terms of use. Errors that may be caused by the use of an outdated firmware version cannot be the subject of a claim. The current firmware implements customer experience and requirements in the field of personal data security.

Directory

The Directory section is a key part of the device configuration. You can create users in the directory and manage their access rights.

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 access options according to Accesses (p. 10).

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.

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.

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. 11).

Switch Control in Web Configuration Interface

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 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.

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. 12).
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. 14)).

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.

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.

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 Detection

On the **Doors** tab, you can enable that an unauthorized or excessively long door opening will trigger an event. This event can then be followed by actions via Automation. The events are also written into the device log.

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.

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 designated input on the intercom.
2. Go to **Integration > Switches** in the web configuration interface.
3. Click the arrow in the tab header to open the Switch 1 settings.
4. 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
5. 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.
6. Save the changes.

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.

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.

NOTE
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. 9)) upon module connection.

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**.

Elevator Control

By connecting the AXIS A9188 relay module to a 2N intercom or to a 2N access unit, access to the elevator floors in the building can be controlled. Up to 8 of these relay modules can be connected to one 2N intercom or 2N access unit, each of which being able to control 8 floors, which makes a total of 64 floors. To use this function, you must have an active license: for IP intercoms (Part No. 9137916) or for access units (Part No. 9160401).

Elevator Connection

1. Connect the inputs of the elevator controllers to the AXIS A9188 relay and connect the relay to the IP network. Make a note of the relay IP address.
   Follow the documentation for the AXIS A9188 I/O Relay Module, available at http://www.axis.com.
2. Open the web configuration interface of the 2N device that is to manage the elevator accesses.
3. Go to **Integration > Access Control > Elevator**.
4. Enable one of the modules on the **Relay Modules (AXIS A9188)** tab.
5. Click the pencil icon and enter the IP address of the relay module into the box that opens.
6. If the relay access is subject to authentication, enter the username and password on the **General** tab.
7. Once the relay module is enabled, the floors managed by this module will appear on the **Elevator Floors** tab. You can name each floor.

Setting Public Access to Floors:

1. Select the floors to be accessible to the public (access is not subject to authorization) on the **Elevator Floors** tab.
2. Click the pencil icon next to 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.

Advanced Settings

Camera and Video Settings

The **2N Access Unit QR** camera detects movement around the device and reads QR codes.

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.

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.

Motion Detection 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. 22).
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.

Privacy Policy

The privacy feature masks a part of the image so that it is not visible or recorded in the video. This option is ideal for situations where you want to protect sensitive areas of the image, for example. If, for example, the device is placed at the reception desk and the camera also captures the hallway where strangers are moving, you can hide the hallway 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.

Motion Detection 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.

External Camera

The external camera is added to the 2N device as a video stream (RTSP). Connecting an external camera allows you to switch between views during a call. The function of the external camera is therefore purely displaying.

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.

Creating Video Stream from Device Camera

The IP intercom video streaming function is used for live video transmission from the intercom camera over the network to a receiving device such as a mobile app, tracking software or a video player in your PC. This process ensures that the users can watch real-time video from a variety of devices.

Creating Video Stream

1. Go to **Integration > Video**.
2. Enable the **RTSP Server** service.
3. Set the stream parameters, see Video Stream Parameters (p. 24).
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**.

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**.

Up to 10 custom user sounds can also be uploaded to the device.

Other Device Audio Features

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. 32)).

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.

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. 26).

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.

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. 32).

- 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.

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.

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.

Used Ports

Service	Port	Protocol	Direction	On by default	Configu-rable	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**
NTP client	123	UDP	In/Out	✓	×	–
SLP	427	UDP	In/Out	✓	×	–
SMTP	25	TCP	Out	×	✓	**Integration > Email notification**
Syslog	514	UDP	Out	×	×	–
TFTP	69	UDP	Out	×	×	–

Service	Port	Protocol	Direction	On by default	Configu-rable	Settings
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
Multicast receiv-er (Automation)	4433	UDP	In	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

Automation

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, specific actions can be triggered by pressing a specific speed dial button, activating the Silent Alarm, detecting an open door, activating an entry or detecting motion 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.

Access Control Units – Configuration manual

2N.com