2N Access Unit Configuration Manual

v.2.42

www.2n.com

Content:

1. Product Overview

Door access system **2N Access Unit** can (with addon software and/or with **2N IP intercoms**) offers you a whole setup for access controle over any whole object.

Your **2N Access Unit** can be equipped with a numeric keypad, so you can use it as code lock.

Your **2N Access Unit** can also be equipped with another RFID card reader, so it can be used as a part of your security system or attendance system in your company.

2N Access Unit can be equipped with a relay to control eletric lock or any other device connected to this access system. There are a lot of possibilities to set up, when and how to activate these switches - with code, automaticaly, by pressing a button etc.

The following symbols and pictograms are used in the manual:

Safety

- **Always abide** by this information to prevent persons from injury.

Warning

- **Always abide** by this information to prevent damage to the device.

Caution

- **Important information** for system functionality.

Tip

- **Useful information** for quick and efficient functionality.

Note

- Routines or advice for efficient use of the device.

2. Express Wizard for Basic Settings

LAN Connection Setting

You have to know the IP address to connect to the **2N Access Unit** configuration interface successfully. Automatic IP address retrieval from the DHCP server is set by default in the **2N Access Unit**. Thus, if connected to a network in which a DHCP server configured to assign IP addresses to all new devices is available, the **device** will obtain an IP address from the DHCP server. The **2N Access Unit** IP address can be found in the DHCP server status (according to the MAC address given on the production plate), or will be communicated to you by the **2N Access Unit** voice function; refer to the Installation Manual.

If there is no DHCP server in your LAN, use the **2N Access Unit** RESET button to set the static IP address mode; refer to the respective Installation Manual. Your unit address will then be **192.168.1.100**. Use it for the first login and then change it if necessary.

Now enter the IP address into your favourite browser. We recommend you to use the latest Chrome, Firefox or Internet Explorer (Edge) versions as **2N Access Unit** is not fully compatible with earlier browser versions.

Use the name "admin" and password "2n" (i.e. default reset password) for your first login to the configuration interface. We recommend you to change the default password upon your first login; refer to the Password parameter in the **Services / Web Server** menu. Remember the password well or put it down. It is because if you forget the password, you will have to reset the intercom to default values (refer to the respective Installation Manual) thus losing all your current configuration changes.

Tip

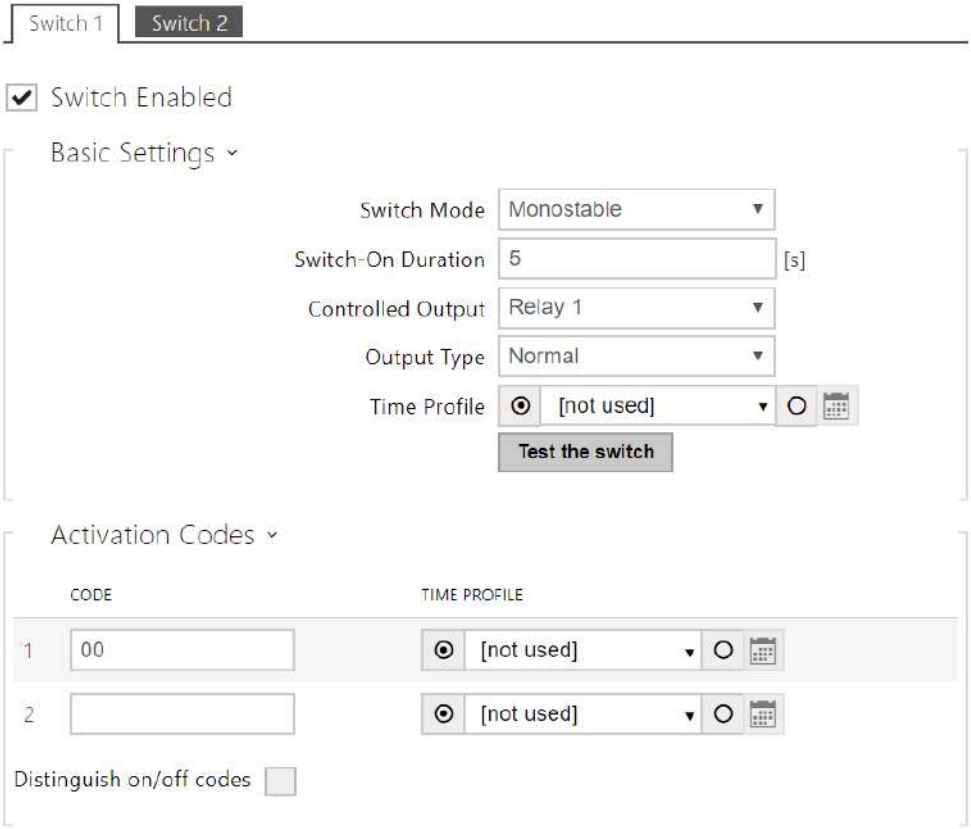
- Installation manual: 2.3 Electric Installation

Firmware Update

We also recommend you to update your firmware upon the first login to the **device**. Refer to www.2n.cz for the latest firmware version. Press the **Update Firmware** button in the **System/ Maintenance** menu to upload firmware. The device will get restarted upon upload and only then the updating process will be complete. The process takes about 1 minute.

Electric Lock Switching Settings

An electric door lock can be attached to the **2N Access Unit** and controlled by a code from the numeric keypad. Connect the electric lock as instructed in the respective Installation Manual.



Enable the switch in the Switch Enabled parameter on the **Hardware / Switches / Switch 1** tab, set the Controlled Output to the intercom output to which the electric door lock is connected. Now set one or more activation codes for the electric door lock switching.

3. Function Licensing

2N Access Unit supports standard licenses integrated in the device such as Enhanced Integration, Enhanced Security and NFC license. The NFC license can only be used in the **2N Access Unit** version that is equipped with a 13MHz card reader.

Refer to the table below for the list of licenses and their features.

License	Features	2N Access Unit 1.0	2N Access Unit 2.0	2N Access Unit M
Enhanced Integration (Standard license part of the device)	Advanced switch setting options	✓	✓	✓
	HTTP API	✓	✓	✓
	Automation function	✓	✓	✓
	E-mail sending (SMTP client)	✓	✓	✓
	Automatic update (TFTP/HTTP client)	✓	✓	✓
	FTP client	✓	✓	✓
	SNMP client	✓	✓	✓
	TR-069	✓	✓	✓
	Synergis	✓	✓	✓
Enhanced Security (Standard license part of the device)	802.1x support	✓	✓	✓
	SIPS (TLS) support	✓	✓	✓
	Switch Blocking by Tamper	✓	✓	✓
	SRTP support	✗	✗	✗
	Silent alarm	✓	✓	✓
	Limit unsuccessful access attempts	✓	✓	✓
	Anti-Passback	✓	✓	✓
	Scrambled keypad	✗	✗	✗
NFC (Standard license part of the device)	NFC support	✓	✓	✓
Lift Control Support	Lift Control	✓	✓	✓

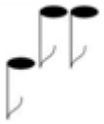
✓ – included in device
★ – licensed function to be purchased additionally
✗ – unavailable

4. Signalling of Operational Statuses

2N Access Unit generates sounds to signal changes and switching of operational statuses. Each status change is assigned a different type of tone. See the table below for the list of signals:

Note

- *Signalling of some of the above mentioned statuses can be modified; refer to the User Sounds subsection.*

Tones	Meaning
	**Internal application launched** The internal application of the **2N Access Unit** is launched upon the **2N Access Unit** power up or restart. A successful launch is signaled by this tone combination.
	**Connected to LAN, IP address received** **2N® Access Unit** logs in upon the internal application launch. A successful LAN login is signalled by this tone combination.
	**Disconnected from LAN, IP address lost** This tone combination signals UTP cable disconnection from the **2N Access Unit**.
	**Default reset of network parameters** Upon power up, a 30 s timeout is set for the default reset code entering. Refer to the Device Configuration subsection in the **2N Access Unit** Installation Manual for details.

5. Web Interface Configuration

Start Screen

The start screen is an introductory overview screen displayed upon login to the **2N Access Unit** web interface. Use the button in the left-hand upper corner of the following web interface pages to return to this screen anytime.

The screen header includes the **2N Access Unit** name (refer to the Display Name parameter in the **Services / Web Server/ Basic Settings**). Use the menu in the right-hand upper corner of the web interface for selecting the language. Click Log out in the right-hand upper corner of the screen to log out from the device, press the question mark icon to display Help or use the bubble to provide feedback.

The start screen is also the first menu level and quick navigation (click on a tile) to selected intercom configuration sections. Some tiles also display the state of selected services.

Configuration Menu

The **2N Access Unit** configuration includes 5 main menus: **Status**, **Directory**, **Hardware**, **Services** and **System** including submenus; refer to the survey below.

Status

- **Device** – essentials on the **2N Access Unit**
- **Services** – information on active services and their states
- **Licence** – current states of licences and available **2N Access Unit** functions
- **Access Log** – list of last ten access cards
- **Events** – list of events

Directory

- **Users** – settings for user phone numbers, quick dial buttons, access cards and switch control user codes
- **Time Profiles** – time profile settings
- **Holidays** – holiday settings

Hardware

- **Switches** – electric lock, lighting, etc. settings
- **Audio** – audio, signalling tone, etc. volume settings
- **Keyboard** – keyboard and code input settings
- **Backlight** – intensity of backlight
- **Card Reader** – card reader, Wiegand interface settings
- **Digital Inputs** – management of digital inputs
- **Extenders** – **2N Access Unit** extender settings
- **Lift Control** – floor lift access settings

Services

- **E-mail** – sending e-mails when e.g. denied events
- **Mobile Key** – Bluetooth settings and management of paired devices
- **Automation** – flexible intercom settings according to user requirements
- **HTTP API** – application programming interface for controlling selected functions of intercom
- **Web server** – web server and access password settings
- **SNMP** – functionality enabling remote monitoring of intercoms in the network using SNMP protokol

System

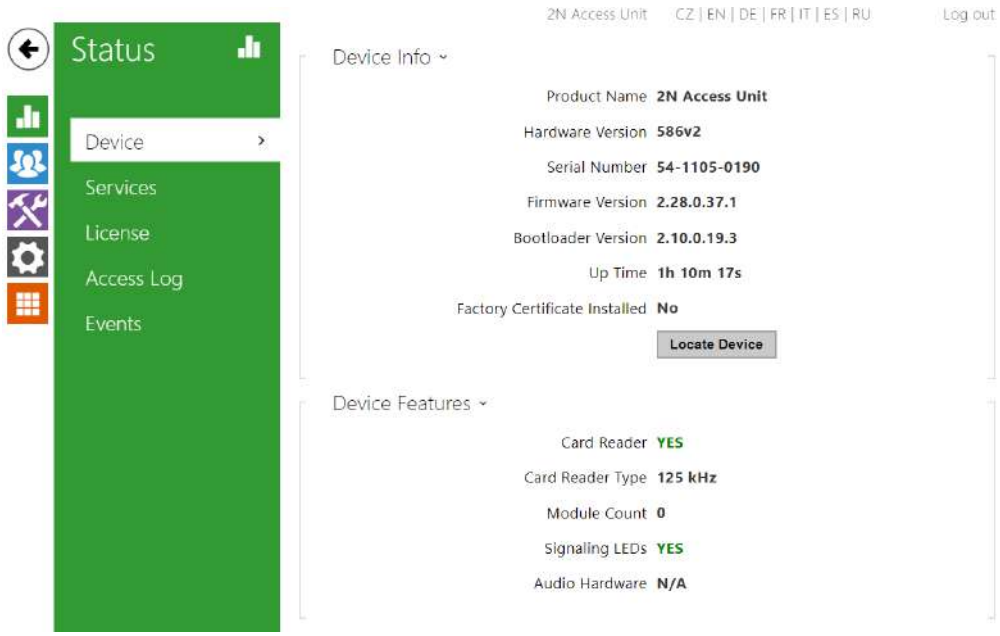
- **Network** – LAN connection settings, 802.1x, packet capturing
- **Date and time** – real time and time zone settings
- **Features** – test function settings
- **Licence** – licence settings, trial licence activation
- **Certificates** – certificate and private key settings
- **Auto Provisioning** – automatic firmware and configuration update settings
- **Syslog** – syslog message sending settings
- **Maintenance** – backup and configuration reset, firmware update

- 5.1 Status
- 5.2 Directory
- 5.3 Hardware
- 5.4 Services
- 5.5 System

Caution

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

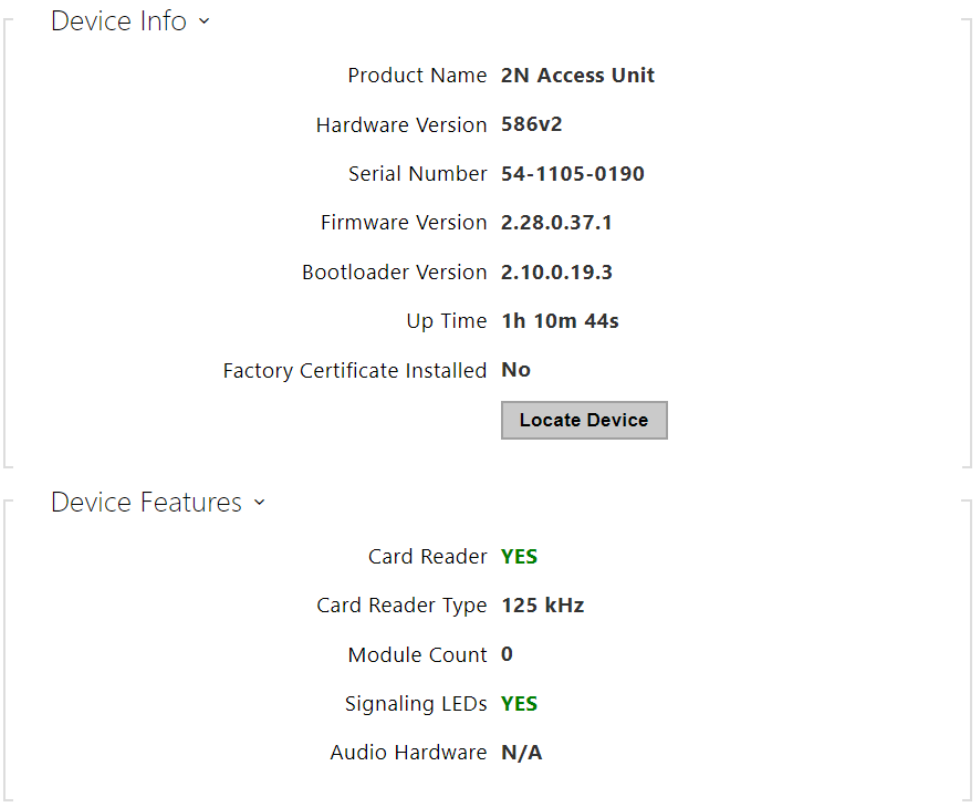
5.1 Status



The **Status** menu provides clear status and other essential information on the **2N Access Unit**. The menu is divided into the following tabs:

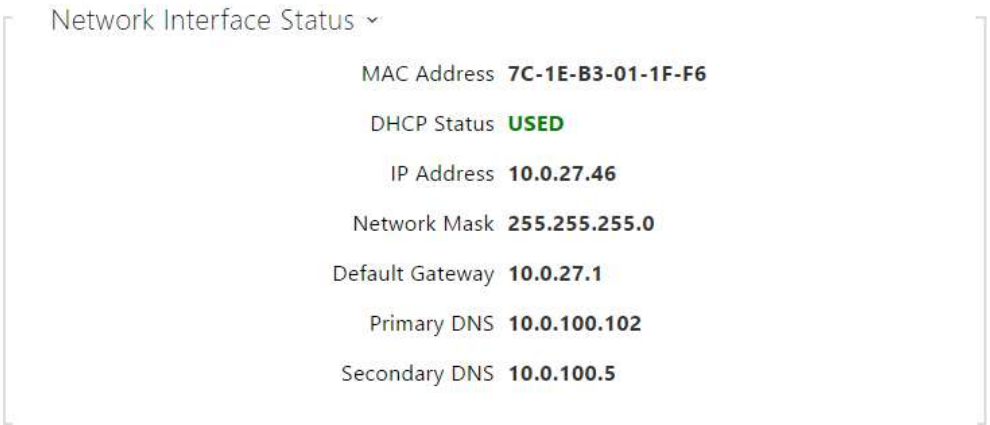
Device

This tab displays basic information on the device model, its features, firmware and bootloader versions and so on.



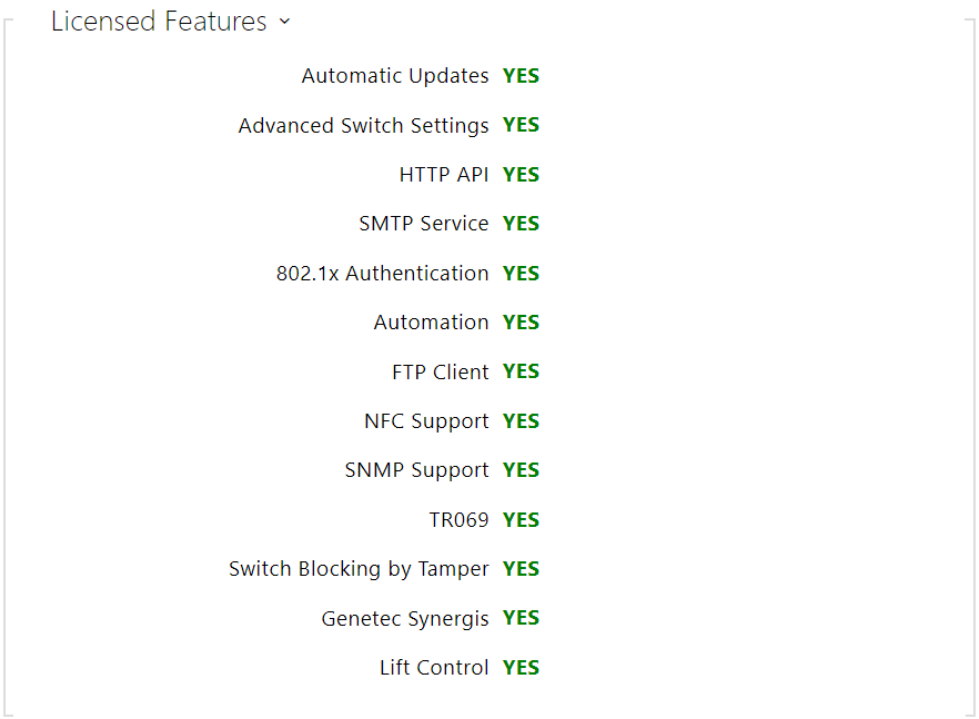
Services

This tab displays the statuses of the network interface and selected services.



Licence

This tab displays the list of licensed functions of the **2N Access Unit** including their current availability (on the basis of a valid licence key entered in the **System / Licences** menu).



Access Log

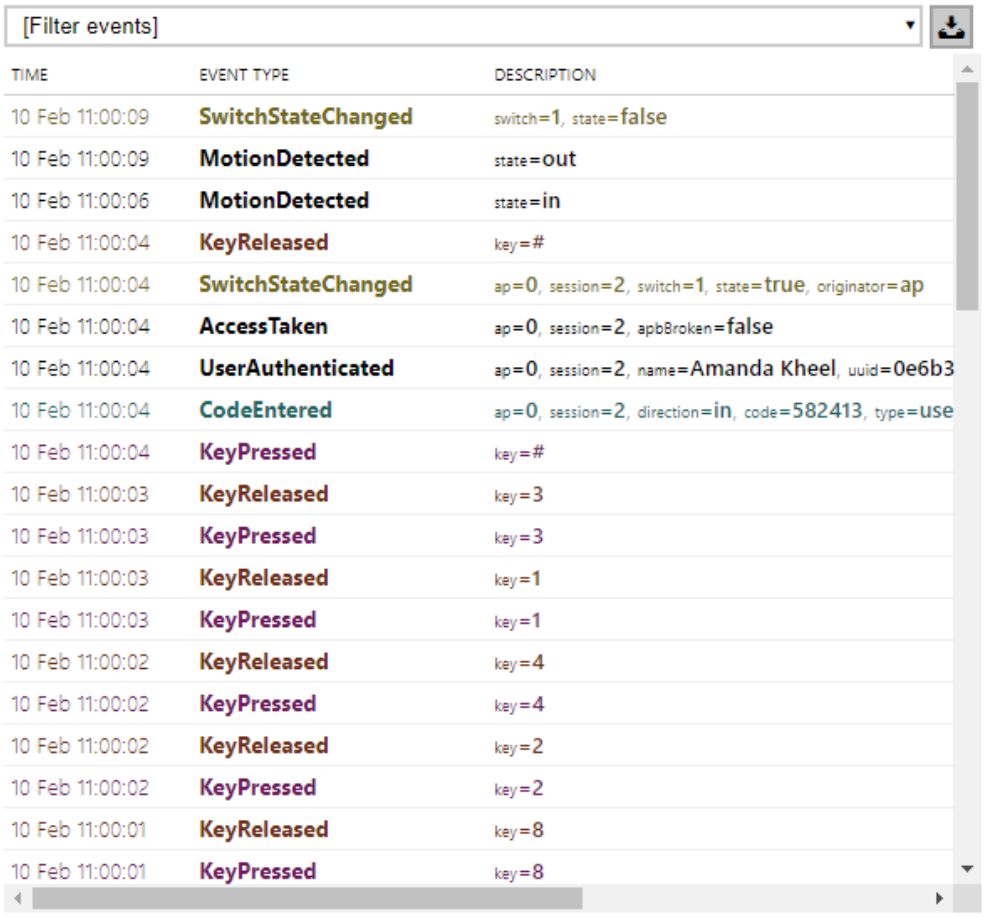
The **Access Log tab** displays the last 10 records on the cards applied. Each record includes the card tapping time, card ID and type and description details (validity, card owner, etc.).

Access Log

	TIME	CARD ID	CARD TYPE	DESCRIPTION
1	01/01/1970 01:26:12	E012FFF8010BE07F	HID iClass	Access denied
2	01/01/1970 01:26:02	4BCFDC13	MIFARE Classic 1k	Access denied
3	01/01/1970 01:25:59	2B2AB69E	MIFARE Classic 4k	Access denied
4	01/01/1970 01:25:56	802C3202239704	MIFARE Ultralight C	Access denied
5	01/01/1970 01:25:51	802AE19A2E9204	MIFARE DESFire	Access denied
6				
7				
8				
9				
10				

Events

The **Events** tab displays the last 500 logged events. Every event contains time and date, event type and description specifying the event. The events can be filtered by type in a dropdown menu, above the event log.



-  – press the button to export all recorded events to a CSV file.

AccessLimited	Event generated after 5 unsuccessful user authentication atttempts (card, code, fingerprint). The access module gets blocked for 30 seconds even if the subsequent authetication is correct.
ApiAccessRequested	
AccessTaken	Card tapping in Anti-passback area.

CardHeld	Indicates that an RFID card has been held for more than 4s.
CardEntered	Indicates that an RFID card has been tapped.
CodeEntered	Generated whenever a code ending with * is entered via the numeric keyboard.
DeviceState	Device state indication, startup of the device, for example.
DoorOpenTooLong	Detection of a too-long opened door, settings in Hardware / Door / Door.
DoorStateChanged	Door open/closed state detection. Settings can be made in Hardware / Door / Door.
FingerEntered	Fingerprint authorisation.
InputChanged	Signals a state change of the logic input.
KeyPressed	Generated whenever a button is pressed (numeric keypad digits are 0,1,2...,9 and quickdial buttons are %1,%2 ...).
KeyReleased	Generated whenever a button is released (numeric keypad digits are 0,1,2...,9 and quickdial buttons are %1,%2 ...).
LiftFloorsEnabled	Floor access via lift enabled.
LiftStatusChanged	Detection of Lift Control module connection/disconnection.
LoginBlocked	Event generated after 3 wrong logins to the web interface. Contains information about IP address.
MobKeyEntered	Bluetooth authorisation.
OutputChanged	Signals a state change of the logic output.
RegistrationStateChanged	Change of the SIP Proxy registration state.

RexActivated	Event at input activation set for the REX button.
SilentAlarm	Silent alarm event generated whenever a code higher by one than the correct one is entered. With access code 123, the silent alarm code is 124. Or, whenever a finger is placed on the fingerprint reader module designated for silent alarm activation.
SwitchesBlocked	Switches blocked by an invalid access attempt.
SwitchOperationChanged	Switch operation changed (signals switch lock/hold, timer start/restart/termination – transition to permanent hold).
SwitchStateChanged	Change of the switch state, settings in Hardware / Switches.
TamperSwitchActivated	Signals tamper switch activation - device cover opening. Make sure that the tamper switch function is configured in the Digital Inputs | Tamper Switch menu.
UnauthorizedDoorOpen	Unauthorized door opening indication, settings in Hardware / Door / Door.
UserAuthenticated	Signals user authentication and subsequent door opening.
UserRejected	User rejection.

5.2 Directory

Here is what you can find in this section:

5.2.1 Users

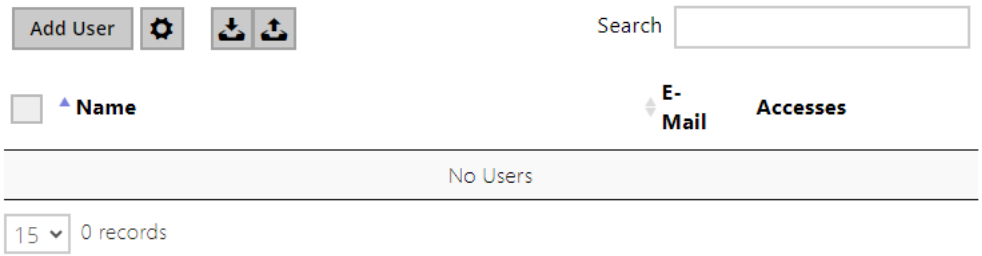
The Users list is one of the crucial parts of the intercom configuration. It contains user information relevant for such intercom functions as quick dialling, RFID card/code door unlocking, missed call e-mails and so on.

The User list contains up to 10 000 users – typically, each user is assigned just one position. The User list provides information on the users that are granted access to the building via the RFID cards.

If your external card reader is connected to the intercom via the Wiegand interface, the card ID is shortened to 6 or 8 characters for transmission (depending on the transmission parameters). If you apply a card to the reader, you will receive a complete ID, which is typically longer (8 chars or more). The last 6 or 8 characters, however, are identical. This is useful for comparing card IDs with the intercom database: if the IDs to be compared have different lengths, they are compared from the end and match has to be found in 6 characters at least. If they have identical lengths, all the characters are compared. This ensures mutual compatibility of the internal and external readers.

All cards applied via the reader or the Wiegand interface are recorded. Refer to the **Status / Access Log** menu for the last 10 cards including the card ID/type, card tapping time and other information if necessary. With small systems, you can make a trick to enter card IDs: tap the card on the intercom reader and find it in the **Access Log**. Double-click to select the card ID and push CTRL+C. Now that you have the card ID in your box, you can insert it with CTRL+V in any intercom setting field.

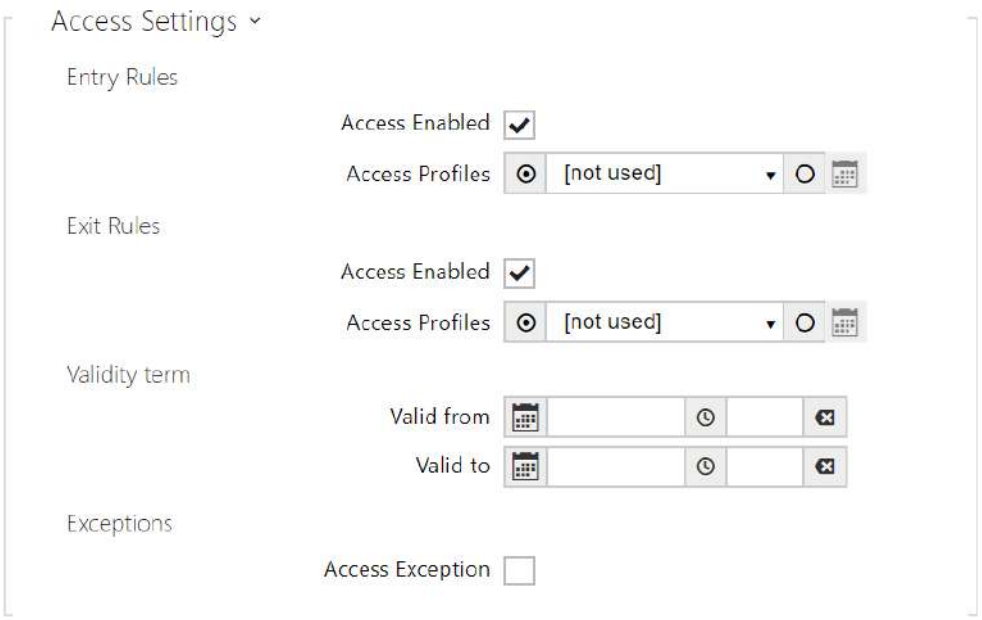
Having been read, the card ID is compared with the intercom card database. If the card ID matches any of the cards in the database, the appropriate action will be executed: switch activation (door unlocking, etc.). To change the switch number to be activated, use the **Associated Switch** parameter in the **Hardware / Card Reader** menu or the **Associated Switch** parameter in the **Hardware / Modules** menu of the card reader module.



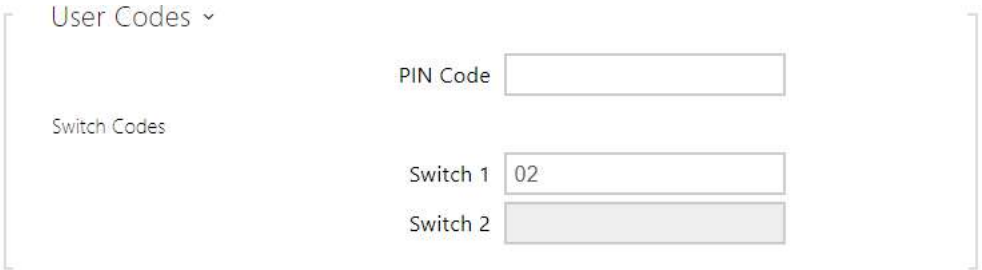
The Search in directory function works as a fulltext search in user names, phone numbers and e-mail addresses. It searches for all matches in the list. Press the button above the table to add a User. Click to show the user details. Click to set the table column display; the default table setting displays the user name, e-mail and assigned accesses. Press to remove a user and delete its details. The icons in the access column describe the active user authentications.

Every record in the Users list includes the following parameters:

- **Name** – a mandatory parameter for easier user search, for example.
- **E-mail** – user e-mail address for sending missed call information. You can enter more e-mail addresses separated with commas.



- **Entry Rules**
  - **Access Enabled** – enable authentication via this access point.
  - **Access Profiles** – select one of the profiles pre-defined in Directory / Time profiles or set the time profile for this element manually.
- **Exit Rules**
  - **Access Enabled** – enable authentication via this access point.
  - **Access Profiles** – select one of the profiles pre-defined in Directory / Time profiles or set the time profile for this element manually.
- **Validity term**
  - **Valid from** – set the beginning of the mode validity term.
  - **Valid to** – set the end of the mode validity term.
- **Access Exception** – set an exception from the access blocking and Anti-passback rules for the user.

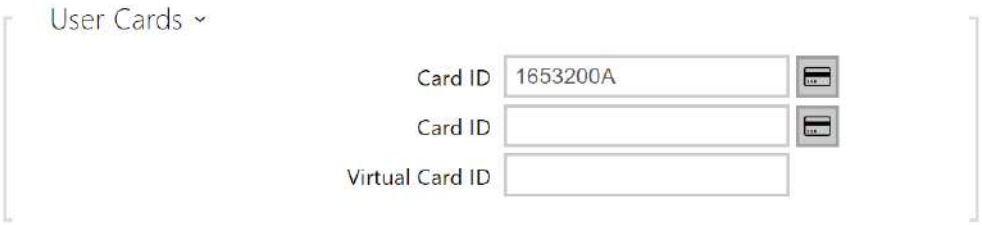


Each user can be assigned a private switch activation code. The user switch codes can be arbitrarily combined with the universal switch codes defined in the **Hardware | Switches** menu.

If the codes are identical with the codes already defined in the intercom configuration, the mark will appear at the colliding codes.

PIN Code – set the user's Personal Identification Number. The code must include 2 characters at least.

Switch1–2 – set a private user switch activation code: up to 16 characters including digits 0–9 only. The code must include at least two door unlocking characters via the intercom keypad and at least one door unlocking character via DTMF.



Each of the intercom users can be assigned two access RFID card.

- **Card ID** – set the user access card ID: 6–32 characters including 0–9, A–F. Each user can be assigned up to two access cards. When a valid card is tapped on the reader, the switch associated with the card reader gets activated. If the double authentication mode is enabled, the switch can only be activated using both a card and numeric code.
- **Virtual card ID** – set the user virtual card ID for user identification in the devices that are integrated with the **2N IP intercoms** via a Wiegand interface. Each user can be assigned just one virtual card. The virtual card ID is a sequence of 6–32 characters: 0–9, A–F. After the user is validated via the Bluetooth/biometric reader, the identifier is sent to the device integrated with the **2N IP intercom** via Wiegand.

- **Auth ID** – set a unique mobile device/user identifier. The parameter value is automatically generated for pairing. You can move Auth ID to another user or copy it to another device in the same location.
  - pair via USB reader

  -  pair via this device
  -  delete Auth ID
- **Pairing state** – display the current pairing state (Inactive, Waiting for pairing, PIN validity expired or Paired).
- **Pairing valid until** – display the date and time of the generated authorisation PIN validity end.

Pairing via Bluetooth Module in Intercom

To pair a mobile phone with the user:

- Click  at Auth ID to start pairing for the selected user account.
- A dialogue window with the PIN code is displayed.
- Find the appropriate reader in the **2N® Mobile Key** application and press Start pairing.
- Enter the code from item 2 into the input field.
- Pairing is completed.

- **User Fingerprints** – display the set count of fingerprints; up to 2 different fingerprints can be set. This section is displayed only if the biometric reader module is available.
  -  enrol via USB reader
  -  enrol via Fingerprint scanner module 3

Caution

- The fingerprint loading capacity is up to 2000 per device.

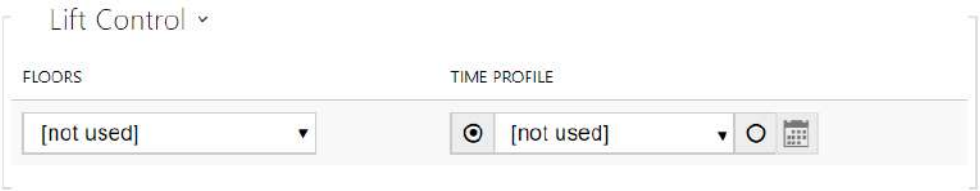
Refer to Subs. 5.2.1.1 User Fingerprint Setting Instructions for user fingerprint loading details.

2N Access Unit helps you use the recognized license plates sent in the HTTP request by the AXIS cameras equipped with additional VaxALPR to api/lpr/licenseplate (refer to the HTTP API manual for IP intercoms).
In case the function is on, the event is recorded into the LicensePlateRecognized history when a valid HTTP request has been received.

If an image is sent within the HTTP request (photo part or whole photo of the license plate detecting scene), it is saved. The last five photos are stored in the device memory and can be retrieved via an HTTP request sent to api/lpr/image available in **2N® Access Commander**.

It is advisable that each license plate should be assigned to just one entry in the directory. Multiple license plate assignments may result in the inability to assign a license plate to an entry in the directory unambiguously (the first entry assigned the specified license plate is selected and given the access rights).

- **License Plates** – set the car license plates for the selected record in the directory. A record can be assigned multiple license plates separated with commas (up to 20). The set license plates are used for recognizing license plates from external camera images (refer to the Interoperability manual for details). One license plate may include up to 10 characters. The set string length is limited to 255 characters.



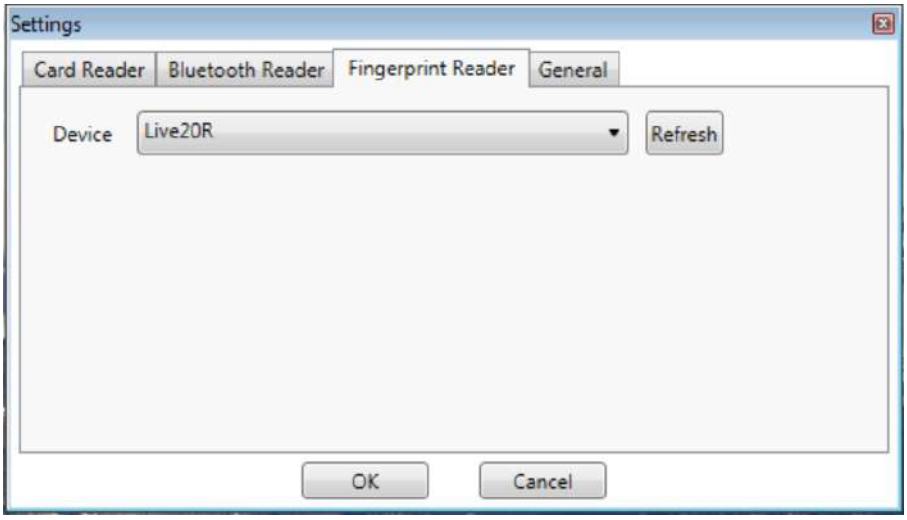
- **Floors** – select the floors available to the user.
- **Time Profile** – select one or more time profiles to be applied. Set the time profiles in the Directory / Time Profiles section.
  - mark the selection from predefined profiles or manual setting of a time profile for the given element.
  - set a time profile for the given element.

5.2.1.1 User Fingerprint Setting Instructions

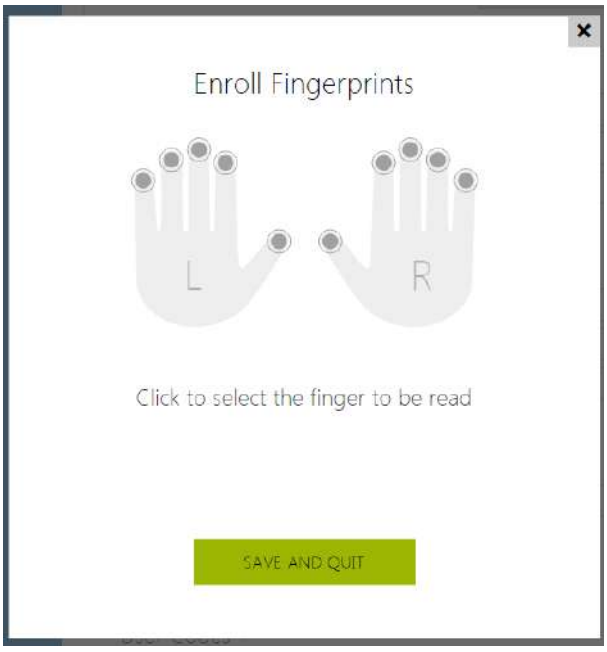
To load fingerprints, use the **2N® Access Unit Fingerprint reader** (Part No. 916019) or an external USB fingerprint scanner (Part No. 9137423E) as follows:

1a) To load fingerprints via the **2N® Access Unit Fingerprint reader**, use the web interface at the selected user and click  Load via fingerprint reader module in Directory / Users/ User fingerprints.

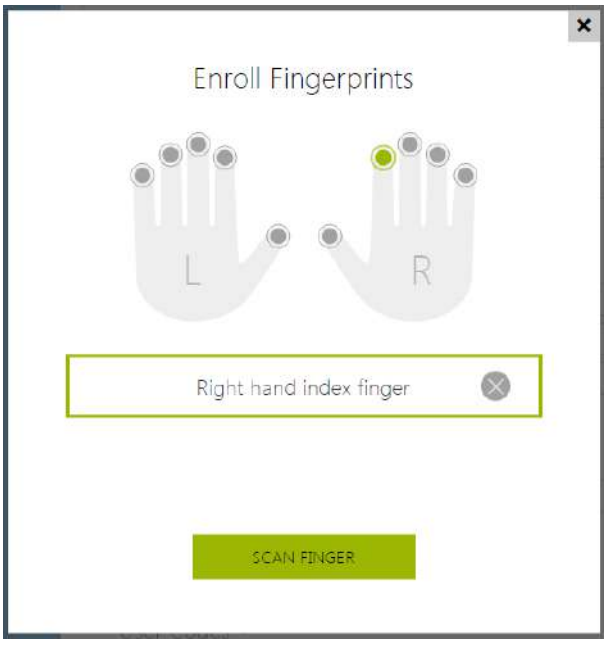
1b) To load fingerprints via an external USB fingerprint scanner, use the **2N® IP USB Driver** and select Fingerprint reader in the Settings and press OK for confirmation. Click  Load via fingerprint reader module in Directory / Users/ User fingerprints via the web interface at the selected user.



2) Click to select a finger for fingerprint loading.

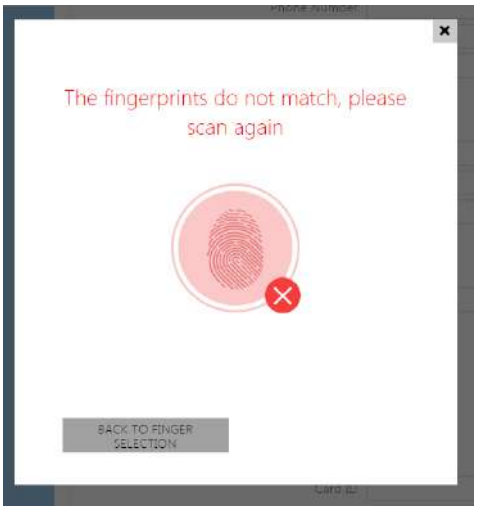


Up to two fingerprints may be saved for each user.
3) Click SCAN FINGER to load a fingerprint.

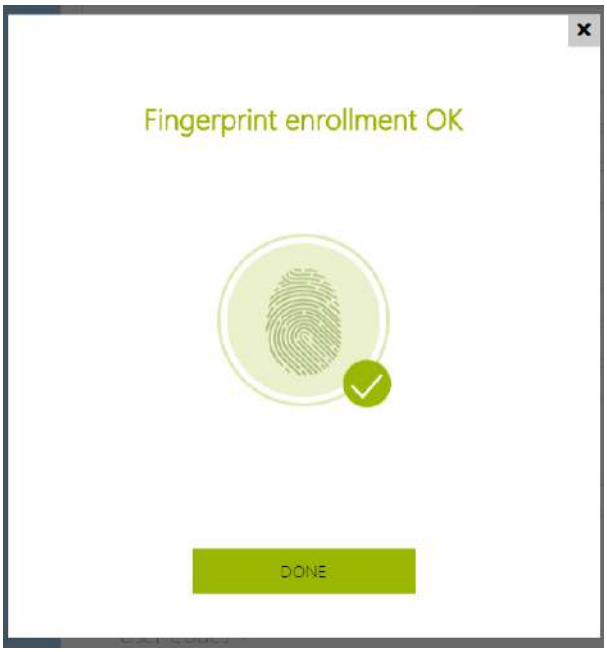


4) Place the selected finger on an external USB reader. This process is repeated three times for greater precision.

Repeat the process if any inconsistency occurs during fingerprint reading.

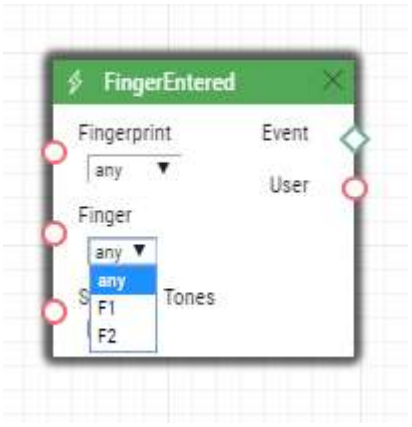


5) If fingerprint scanning is successful, click DONE to confirm the settings.

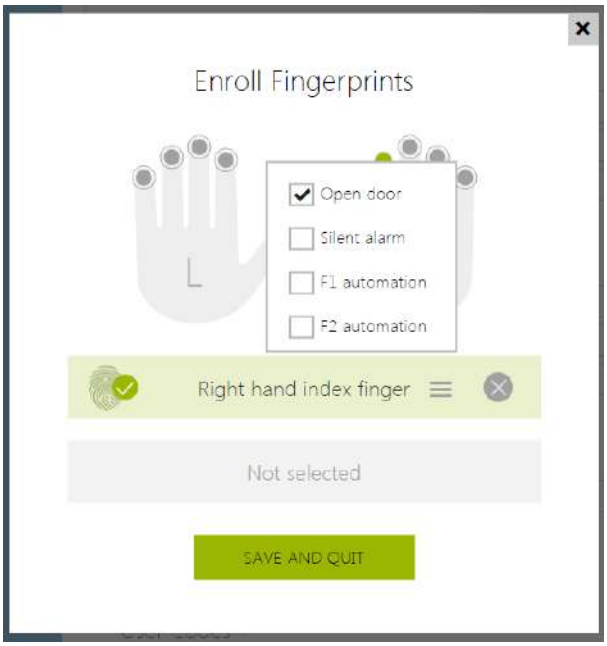


To set the finger function, click the icon to display the list of available functions:

- Door opening
- Silent alarm; configurable only if Door opening is active
- Automation F1 – generate the FingerEntered event in Automation. F1 helps distinguish the applied finger in Automation.
- Automation F2 – generate the FingerEntered event in Automation. F2 helps distinguish the applied finger in Automation.



Click SAVE AND QUIT to confirm the fingerprint enrolment and selected functions.

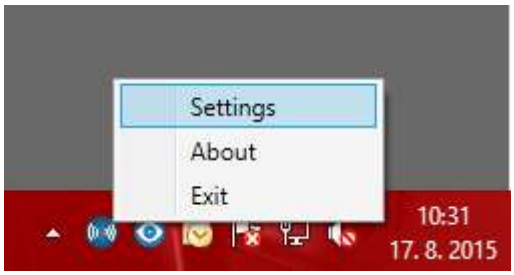


6) You can check the current settings in the User tab.

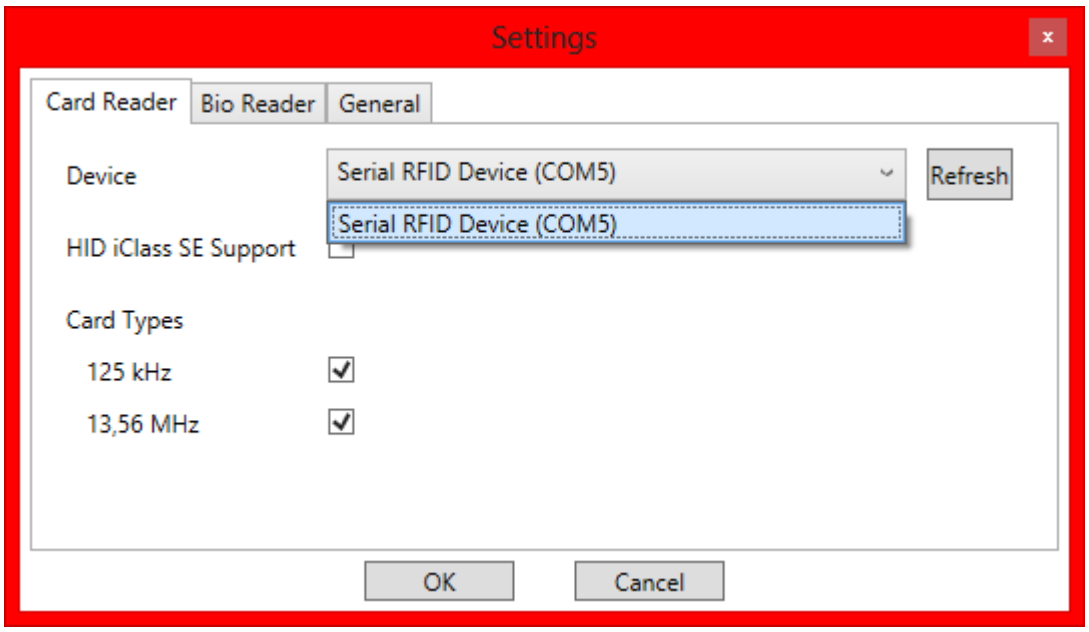
5.2.1.2 USB RFID Card Reader

It is possible to read the card ID via an RFID card reader. Proceed as follows:

- Go to the **2N® USB Driver** settings.

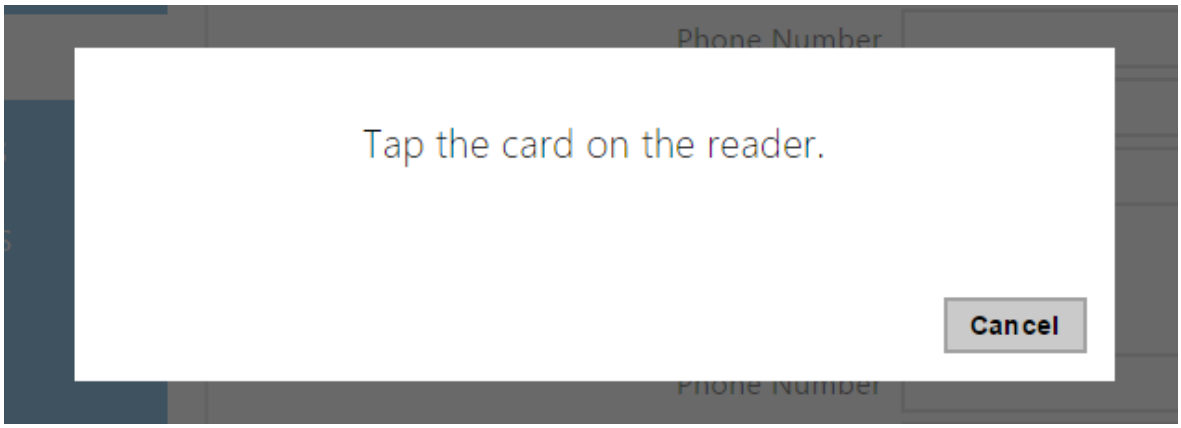


- Set up the COM port for the connected reader.



- Press the Read button via the **2N Access Unit** web interface.

- Tap the card on the card reader.



- The card ID is successfully read.

Do not forget to save the configuration.

.

5.2.2 Time Profiles

Such **2N Access Unit** functions as RFID card/numeric code access, for example, can be time-limited by being assigned a **time profile**. By assigning a time profile you can:

- block all calls to a selected user beyond the set time interval
- block calls to selected user phone numbers beyond the set time interval
- block RFID access for a user beyond the set time interval
- block numeric code access for a user beyond the set time interval
- block switch activation beyond the set time interval

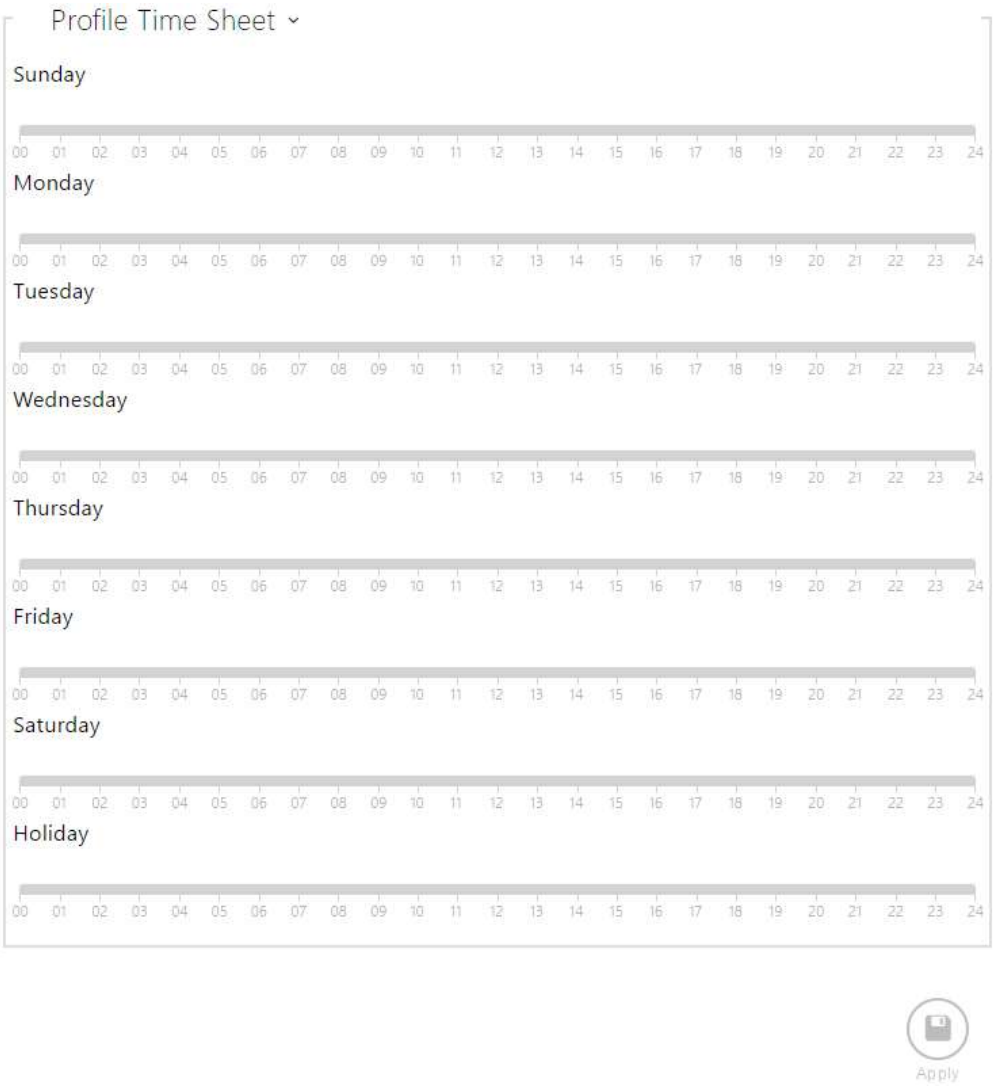
Assign a time profile according to a week time sheet to define availability of the selected function. Just set from-to and/or days in the week on which the function shall be available. **2N Access Unit** helps you create up to 20 time profiles that can be assigned to the function; refer to the Users, Access Cards and Switches settings.

The time profiles can be defined not only using the week time sheet but also manually with the aid of special activation/deactivation codes. Enter the activation/deactivation codes using the numeric keypad of your **2N Access Unit** to activate/deactivate a function after arriving in/before leaving your office, for example.

Refer to the **Directory / Time Profiles** menu for the time profile settings.

List of Parameters

- **Profile Name** – enter a profile name. This parameter is optional and helps you find items in the time profile list in the switch, card and phone number settings more easily.



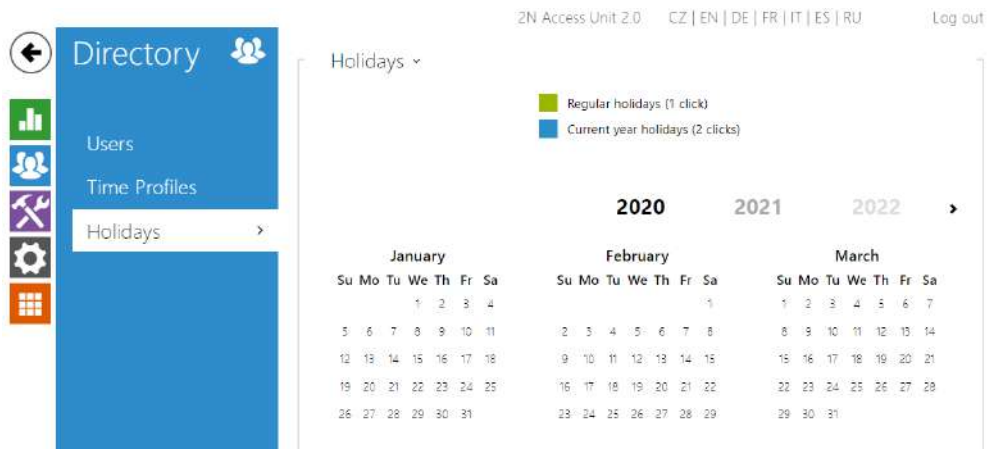
This parameter helps you set time profiles within a week period. A profile is active when it matches the set intervals.
If a day is marked as holiday (refer to **Directory** → **Holidays**), the last table row (Holiday) is applied regardless of the day in a week.

Make sure that the real time settings are correct (refer to the Date and Time subsection) to make this function work properly.

Note

- *You can set any number of intervals within a day: 8:00–12:00, 13:00–17:00, 18:00–20:00, e.g.*
- *To make a profile active for the whole day, enter one day-covering interval: 00:00–24:00.*

5.2.3 Holidays

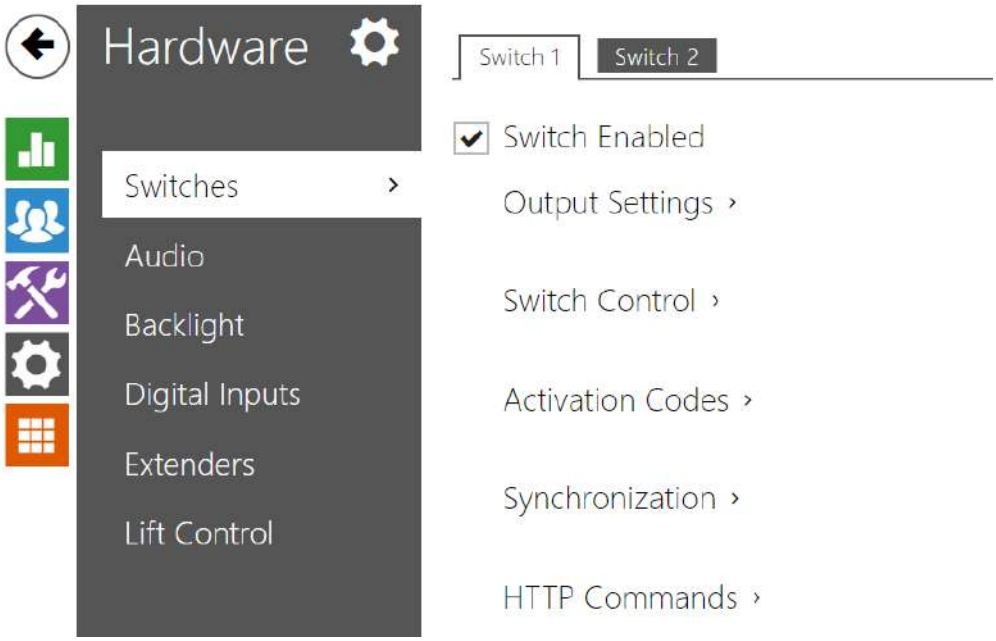


Here select the bank holidays (including Sundays). You can assign them different time intervals than to working days in their time profiles.
You can set holidays for the coming 10 years (click the year number at the top of the screen to select a year). A calendar is displayed for you to select/unselect a holiday. Fixed (annual) holidays are marked green and variable holidays (valid for the particular year only) are blue. Click a date once to select a fixed holiday, click twice to select a variable holiday and click for the third time to remove the holiday from the holiday list.

5.3 Hardware

Here is what you can find in this section

5.3.1 Switches



Switches provide a very flexible and efficient control of such peripherals connected to the Access Unit as electric door locks, lighting, additional ringing signalling, and so on. **2N Access Unit** allows you to configure to 2 independent all-purpose switches.

A switch can be activated by:

- entering a valid code via the **2N Access Unit** numeric keypad,
- tapping a valid RFID card on the reader,
- a predefined delay after another switch activation,
- by a time profile *),
- receiving an HTTP command from another LAN device,
- the Action.ActivateSwitch action via Automation *).

Switch activation can be blocked by an appropriately selected time profile if necessary.

Caution

- The options marked with *) require their respective active licences.

Switch locking and hold

The switch activation conditions are modified using two functions: switch locking and switch hold. If a switch is locked, it is permanently deactivated and cannot be operated until unlocked (locked has a higher priority than held – in case the switch is locked and held simultaneously, locking is applied). If held, the switch is in the activated state and cannot be operated until released.

Switch locking and holding can be controlled by time profiles among others. It is not recommended that a time profile be used for the locking function (the time-profile based lock control is present in the device for legacy switch compatibility reasons) because this case results in switch unlocking at the end of the time profile despite manual switch locking.
The current combination of these two functions is shown by the **Current switch function** parameter (Normal – lock and hold are off; Held – lock is off and hold is on; Locked – lock is on regardless of the hold setting).
Check after restart whether or not the lock/hold is controlled by a time profile. If so, the given function is activated/deactivated according to the time profile setting. If not, the last locking state before the device power off is set, or hold is set to inactive (the switch is not held).

If a switch is active, you can:

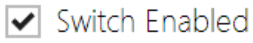
- activate any logical output of the **2N Access Unit** (relay, power output).
- activate the output to which the **2N® IP Security Relay** module is connected.
- send an HTTP command to another device.

The switch can work in the monostable or bistable mode. The switch is switched off after a timeout in the monostable mode and switched on with the first activation and off with the next activation in the bistable mode.

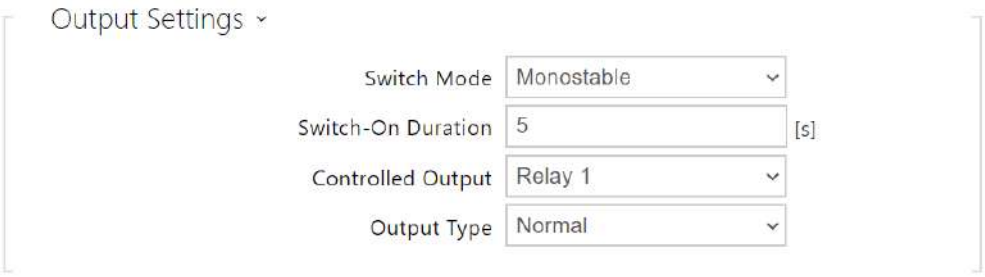
The switch signals its state by:

- a programmable beep.
- a LED indicator if available in the **2N Access Unit** model.

Switch 1–2



- **Switch enabled** – enable/disable the switch globally. When disabled, the switch cannot be activated by any of the available codes (including user switch codes), by a call or quick dial button.



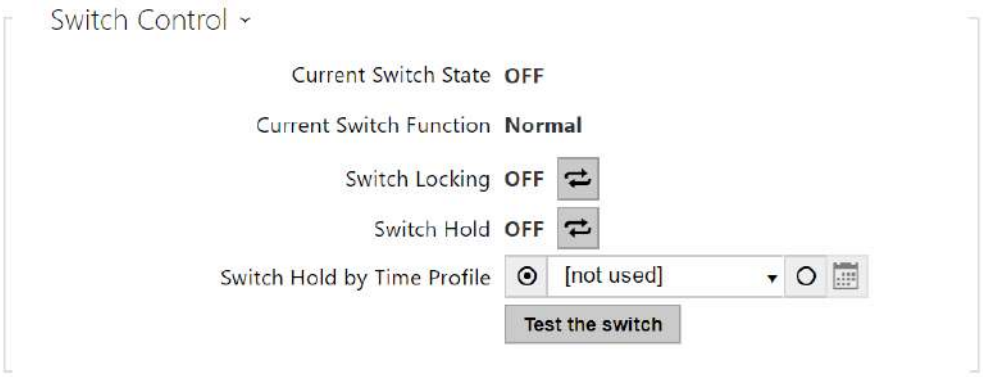
- **Switch Enabled** – enable/disable the switch globally. When disabled, the switch cannot be activated by any of the available codes (including user switch codes), by quick dial button.
- **Switch mode** – set the monostable/bistable mode for the switch. The switch is switched off after a timeout in the monostable mode and switched on with the first activation and off with the next activation in the bistable mode.
- **Switch-on duration** – set the switch-on time for a monostable switch. This value is not applied in the bistable mode.
- **Controlled output** – assign an electric output to the switch. Choose one of the available intercom outputs: relay, power output, extender output. If you select **None**, the switch will not control any electric output but can control external equipment via HTTP commands.
- **Output type** – if you use the **2N® IP Intercom - Security Relay** module, set the output type to **Security**. In the **Security** mode, the output works in the inverse mode, i.e. remains closed and controls the **2N® IP Intercom - Security Relay** module using a specific pulse sequence. If you use the inverse mode (i.e. the door is locked when voltage is applied), set the **inverse** output type. In case multiple switches are set to the same output but different output types, the following priority will be applied: 1. security, 2. inverse, 3. normal.

Info

- *A switch activation value higher than 1 s can be set for the **security** output type. A value equal to or higher than 0.1 s can be set for the **normal** and **inverse** output types.*

Security

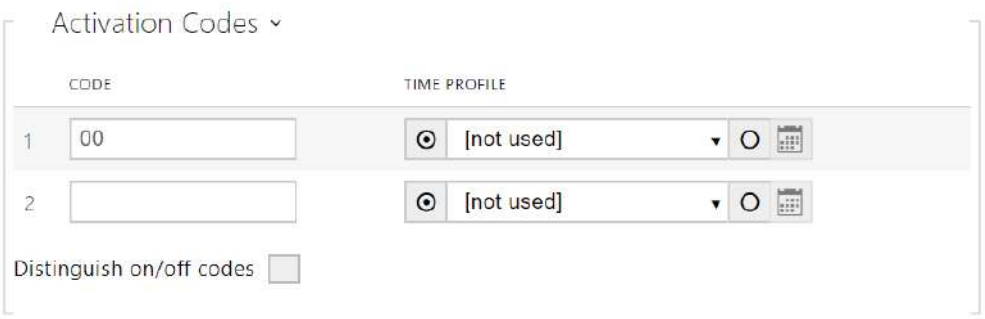
- The 12V output is used for lock connection. If, however, the unit (2N IP Intercom, 2N Access Unit) is installed where unauthorized tampering may happen, we strongly recommend that the 2N® Security Relay (Part No. 9159010) be used for enhanced installation security.



- **Current Switch State** – display the current switch state (On/Off).
- **Current Switch Function** – Display the current switch function.
  - **Normal**: the switch is not locked or held.
  - **Held**: the switch is held and unlocked.
  - **Locked**: the switch is locked (locking has priority over holding, the holding state is irrelevant in this case).
- **Switch Locking** – on: the switch is permanently in position 0 and cannot be controlled until unlocked.Off: the switch is unlocked.
- **Switch Hold** – on: the switch is permanently in position 1 and cannot be controlled until released (if the switch hold and lock are active at the same time, the switch is locked).Off: the switch not held in position 1.
- **Switch Hold by Time Profile** – assign a predefined time profile to the switch or set a time profile manually that allows for switch activation. If the assigned time profile is inactive, the switch can be activated by tapping a valid RFID card, making a call, entering a code or pressing a quick dial button.
- **Test the switch** – activate the switch manually to test its function, e.g. an electric lock or another device connected.

Caution

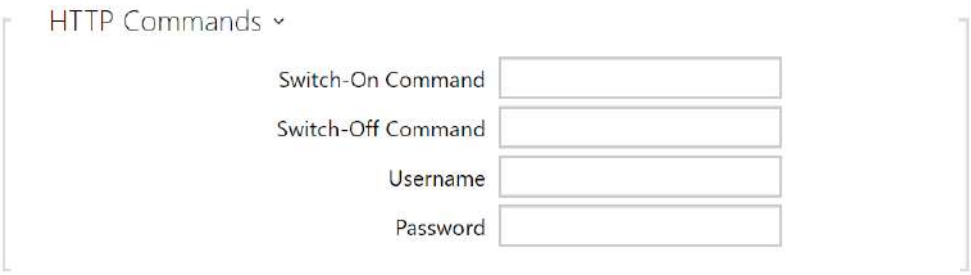
- In case the switch is locked and the device is turned off and on, the switch will be locked after the device is turned on again. The same is true when the switch is disabled and enabled again.
- In case the switch is held and the device is turned off and on, the switch will not be held after the device is turned on again. The switch is held after power on only if a switch hold time profile is set and active at the moment of the power on. The same is true when the switch is disabled and enabled again.



The table above includes a list of universal codes that help you activate switches from **2N Access Unit** keypad. Up to 10 universal codes can be defined for each switch (depending on the particular intercom model).

- **Code** – enter the numerical code for the switch. The code must include at least two door unlocking characters via the intercom keypad and at least one door unlocking character via DTMF. We recommend you to use four characters at least. Codes 00 and 11 cannot be entered and are not accepted from a numeric keypad; they are reserved for opening doors via DTMF. Confirm the code with *. The code length is up to 16 characters.
- **Time Profile** – assign a time profile to the switch code to control its validity.
- **Distinguish on/off codes** – Set a switch code mode in which odd codes (1, 3 ....) are used for switch activation and even codes (2, 4 ...) are for switch deactivation. This mode can only be used if the switch is set to the bistable mode.

- **Synchronise with** – set switch synchronisation to enable automatic switch activation after another switch activation with a predefined delay. Define the delay in the **Synchronisation Ddelay** parameter.
- **Synchronisation Delay** – set the time interval between synchronised activations of two switches. The parameter will not be applied unless the **Synchronise** function is enabled.

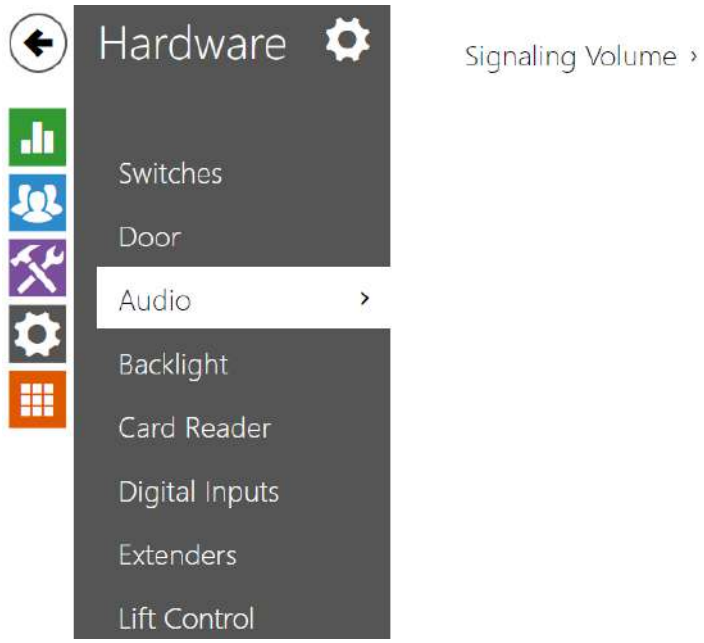


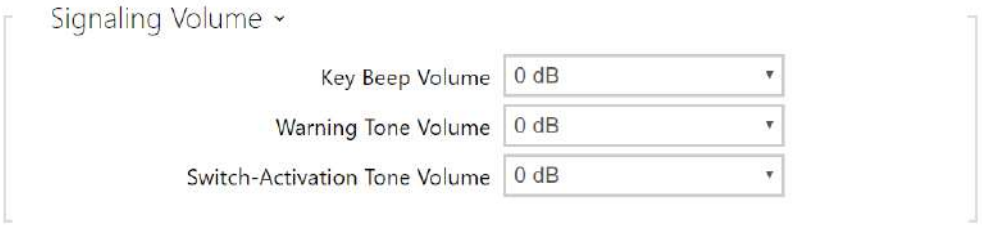
- **Switch-On Command** – set the command to be sent to the external device (WEB relay, e.g.) upon switch activation. The command is sent via the HTTP (GET request) and must be as follows: http://ip_address/path. E.g.: http://192.168.1.50/relay1=on.
- **Switch-Off Command** – set the command to be sent to the external device (WEB relay, e.g.) upon switch deactivation. The command is sent via the HTTP (GET request) and must be as follows:http://ip_address/path. E.g.: http://192.168.1.50/relay1=off
- **Username** – enter the username for the external device (WEB relay, e.g.) authentication. The parameter is obligatory only if the external device requires authentication.
- **Password** – enter the external device (WEB relay, e.g.) authentication password. The parameter is obligatory only if the external device requires authentication.

Tip

In case of use external relay **part no.: 9137410E** are used next HTTP commands:
To turn on the switch – http://ip_address/state.xml?relayState=1 (e.g.: http://192.168.1.10/state.xml?relayState=1)
To turn on for pre-defined time (default value is 1.5 s) – http://ip_address/state.xml?relayState=2 (e.g.: http://192.168.1.10/state.xml?relayState=2)
To turn off – http://ip_address/state.xml?relayState=0 (e.g.: http://192.168.1.10/state.xml?relayState=0)
In case of use external relay **part no.: 9137411E** are used next HTTP commands (Symbol X should be replaced with a number of the desired switch):
To turn on the switch – http://ip_address/state.xml?relayXState=1 (e.g.: http://192.168.1.10/state.xml?relay1State=1)
To turn on for pre-defined time (default value is 1.5 s) – http://ip_address/state.xml?relayXState=2 (e.g.: http://192.168.1.10/state.xml?relay1State=2)
To turn off – http://ip_address/state.xml?relayXState=0 (e.g.: http://192.168.1.10/state.xml?relay1State=0)

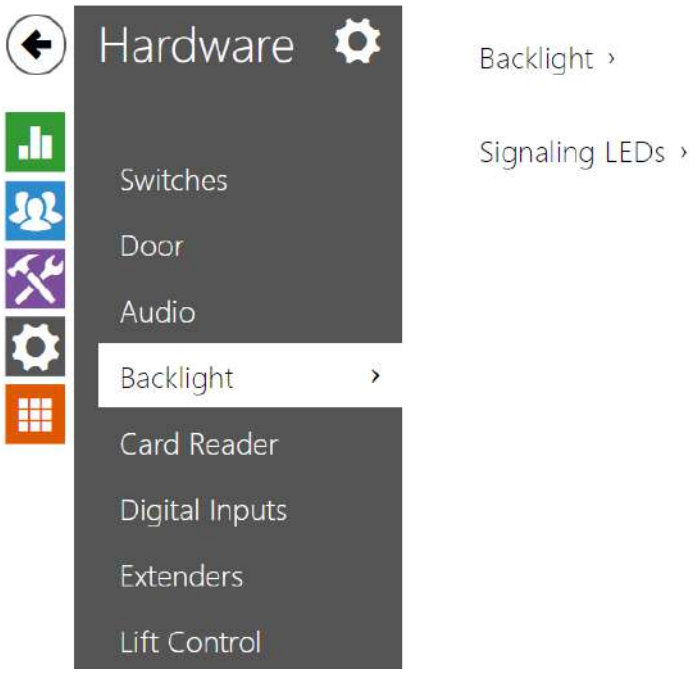
5.3.3 Audio





- **Key beep volume** – set the key beep volume. The volume values are relative against the set master volume.
- **Warning tone volume** – set the volume of warning and signalling tones described in the **Signalling of Operational Statuses** section. The volume values are relative against the set master volume.
- **Switch activation tone volume** – set the volume of the switch activation tone. The volume values are relative against the set master volume.

5.3.4 Backlight



Use this tab to set the module backlight and signalling LED brightness levels separately.

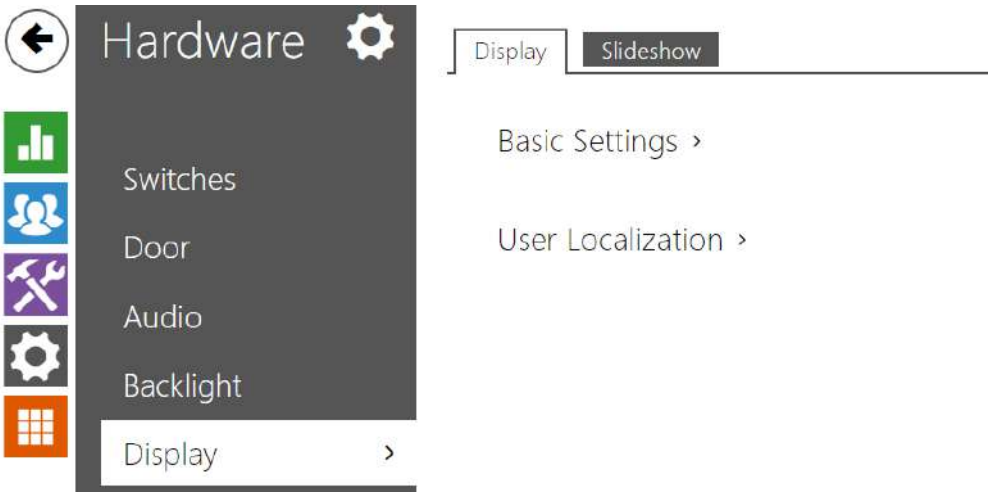
- **Backlight** – set the backlight brightness value for the day mode. Set the value as a percentage of the maximum possible LED brightness.

- **Signaling LEDs** – set the signaling LED brightness value for the day mode. Set the value as a percentage of the maximum possible LED brightness.

Note

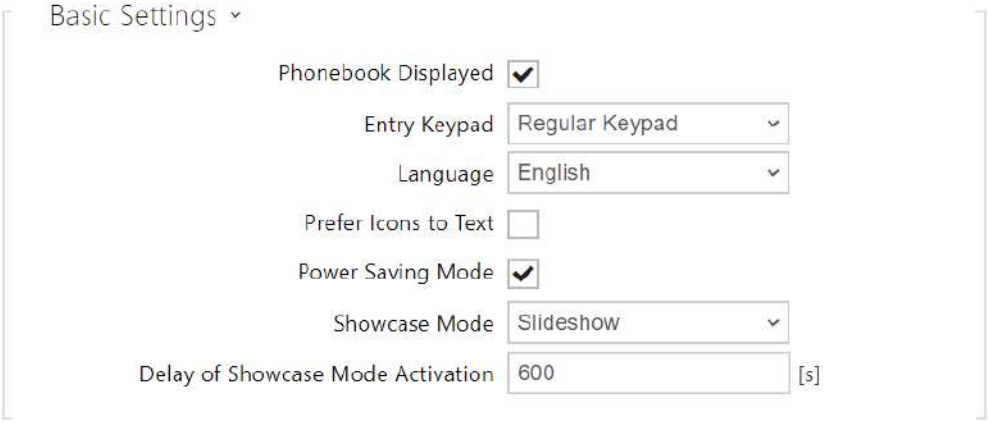
- The brightness parameters affect the function, power consumption and general appearance of your device. A high nametag and button backlight value may, if the ambient light level is low, dazzle the persons standing in front of the intercom and, in general, increase the power consumption of the device. A low LED brightness value, on the other hand, may, if the intercom is placed in direct sun, result in a lower LED on/off contrast and potential LED state identification problems.

5.3.5 Display



2N Access Unit version 2.0 can be extended to include a display module. A color LCD display provides a touch keypad function and indicates the device state (door opening, access denial etc.) and/or can work in the Showcase mode at the same time, showing sets of loaded images after a defined idle timeout. The images are automatically switched and the showing time can be set for each image.

Display



- **Phonebook Displayed** – enable/disable display of the phone book function.
- **Entry Keypad** – enable the keypad/keypad type.
  - **Disabled** – disable the keypad.
  - **Regular Keypad** – set the regular keypad type.
  - **Scramble Keypad** – enable/disable keypad button scrambling (random button transposing) before every new display to prevent other persons from watching the code entered (**Enhanced Security** licence required).
- **Language** – set the language for the texts to be displayed. Choose one of the seven pre-defined languages: **English, Spanish, German, French, Russian, Italian** and **Czech**.

- **Prefer Icons to Text** – the icons on the dosplay will be preferred to the text.
- **Power Saving Mode** – activate the power saving mode in which the display brightness is reduced. If no event occurs during two Slideshow screen activation timeouts, the power saving mode activation has been successful. Set 0 in the Slideshow screen activation timeout to disable the power saving mode. Any movement in front of the intercom camera or any display event (such as door lock activation or display touch) restores the full brightness of the display.
- **Showcase Mode** – set whether the device shall go into the showcase mode when idle. Choose various options in the showcase mode (Slideshow, Company Logo, Address).
- **Delay of Showcase Mode Activation** –set the idle timeout in the range of 1 to 600 seconds after which the device goes into the mode of representation.

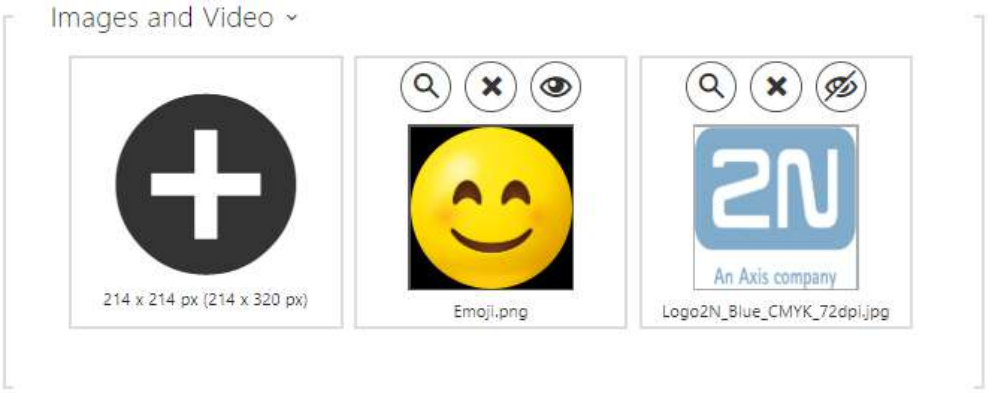
- **Original Language** – download the localisation file template for own translation. It is an XML file with all the texts to be displayed.
- **Custom Language** – remove, download and upload a localisation file of your own.

> **Note**
>
> If none of the pre-defined languages is convenient for you, proceed as follows:
> - Download the original language file (English).
> - Modify the file using a text editor (replace the English texts with your own ones).
> - Upload the modified localisation file to the intercom.
> - Set **Language Settings | Language** to **Custom.**
> - Check and correct if necessary the texts on the intercom display.

Slideshow

This tab helps you configure a list of images to be displayed in the Slideshow mode. Upload up to 8 images to be shown with a preset delay.

- **Slideshow Transition Time** – set the image displaying time in a slideshow.



Make sure that the image resolution is 214 x 214 pixels. Other sizes will be adjusted to the display resolution automatically.

Click the magnifier icon to view the loaded image, press to delete an image and click to hide a selected image/video on the device display.

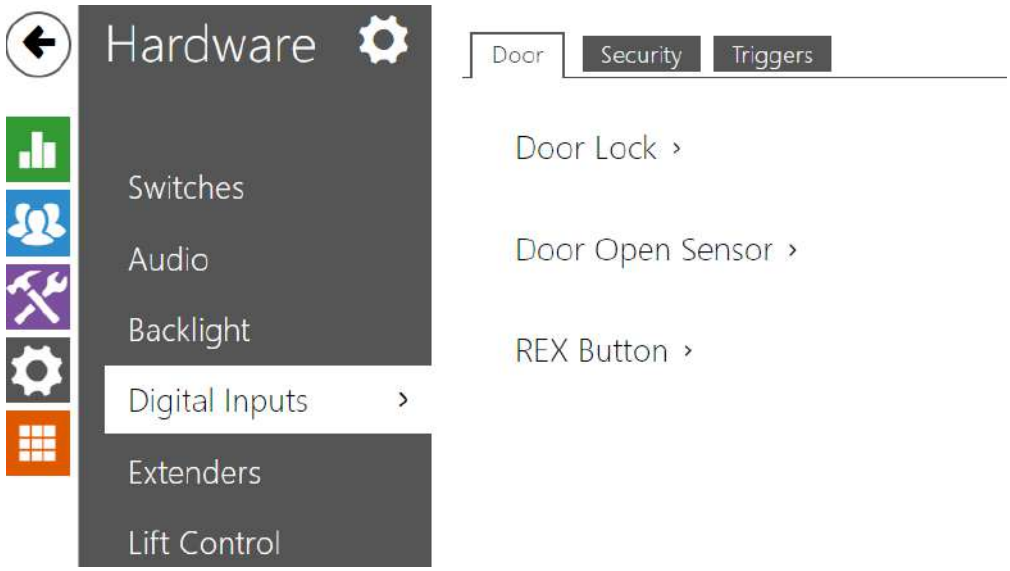
If no image is loaded, the Slideshow mode will never be activated.

Tip

- To hide the "Start with touch" display on the display, load an image of the resolution of 214 x 320 pixels.

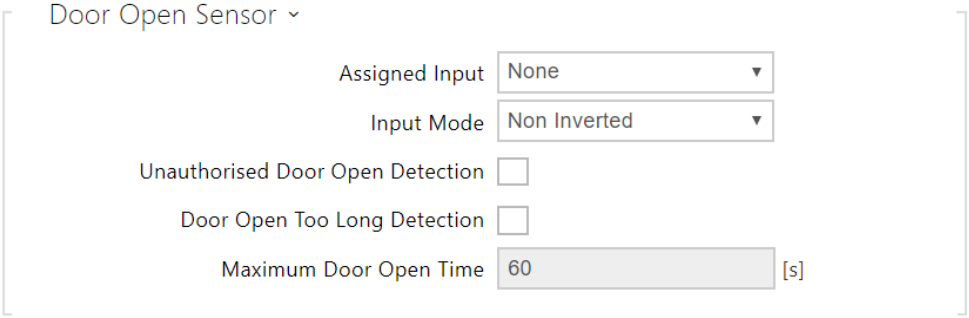
5.3.7 Digital Inputs

In this configuration section set the parameters associated with the digital inputs and their interconnections with other functions.



Door

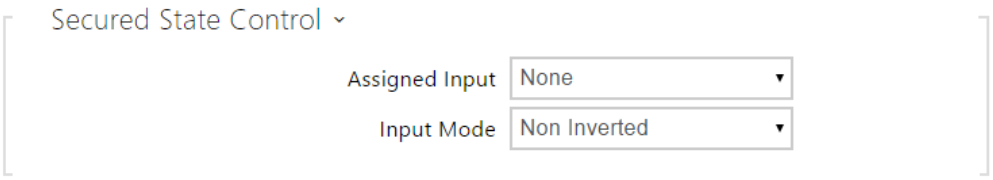
- **Assigned Switch** – select a switch for the electromagnetic door lock control. The switch state controls the door unlocking signaling (green door symbol, green LED).



- **Assigned Input** – define one (or none) of the logical inputs for open door detection.
- **Unauthorized Door Open Detection** – detect if the door is open when switch has been locked.
- **Door Open Too Long Detection** – door open too long detection.
- **Maximum Door Open Time** – maximum permitted door open duration in seconds.

- **Assigned Input** – select one (or none) of the logic inputs for the departure button function. The departure button input activation activates the selected switch. The activation time and mode are set by the selected switch parameters.
- **Input Mode** – set the active input mode (polarity).

Security



- **Assigned input** – define one (or none) of the logical inputs for secured state detection. The secured state is then signalled by a red LED on the **2N Access Unit**.
- **Input mode** – set the active level of the input (polarity).

The tamper switch equipped models help detect opening of the device cover and signal this event as **TamperSwitchActivated**. The events are written into a log and read out via HTTP API (refer to the HTTP API manual).

If the function is enabled, all the switches get blocked for 30 minutes whenever the tamper is activated. Blocking is active even after the device restart. Each port can be controlled via **Automation**. Press the **UNBLOCK** button, disable the function or reset the configuration factory values to unblock the switches.

- **Assigned input** – select the logical input to which the tamper switch is to be connected. **TamperSwitchActivated** signals the tamper switch activation.
- **Enable automatic switch blocking** – block the switches by tamper activation for 30 minutes.
- **Switch blocking state** – display and make switch blocking settings.

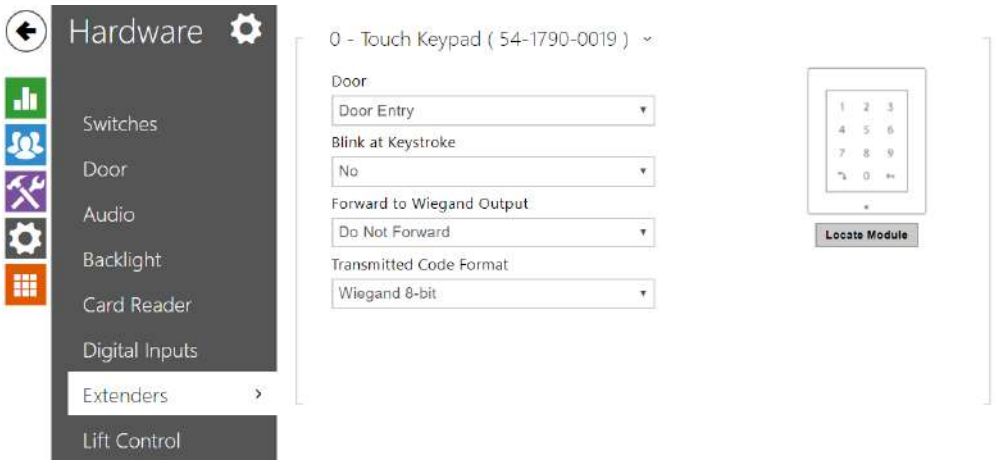
Note

- From PCB version 599v2 up, each of the models is equipped with an optical tamper switch.
- From PCB version 599v2 up, the assigned input is indicated by a module pictogram backlight. In lower PCB versions, it is indicated by the LED light on the right-hand module side.

Triggers

- **User Actions Trigger 1, 2**
  - **Assigned input** – select a logic input that will fulfil the user action function. In case the function is activated, the UserActionActivated event with parameter state=in (function deactivation is indicated by state=out) is written into the device event log. Based on this event, for example, superior systems can trigger alarm, lock the whole building or perform any other action.
  - **Input mode** – select whether a user action should be evaluated based on the inverted or normal value of the assigned input.

5.3.8 Extenders



You can enhance the **2N Access Unit** with extending modules connected to the basic unit. The following modules are available:

- Five-button module
- Keypad module
- Infopanel module
- Card reader module
- Bluetooth module
- I/O module
- Wiegand module
- OSDP module
- Inductive loop module
- Display module
- Fingerprint reader
- Touch keypad
- Touch keypad & RFID reader 125 kHz, 13.56 MHz
- Bluetooth & RFID reader 125 kHz, 13.56 MHz

The modules are chain-like interconnected. Each of the modules has its number depending on the chain position (the first module has number 0).

You can configure each module separately. The parameters are specific for the given module type.

Caution

- The connected module is not detected automatically. Restart the device to see the module in the extender list.
- In case the firmware versions of the module to be connected and the main unit are incompatible, the module will not be detected. Therefore, it is necessary to update the device firmware after the modules are connected. Use the device web

interface in the System > Maintenance > System configuration section for firmware upgrade.

Caution

- Be sure to configure the replaced modules. The configuration is tied with the module serial number.

Note

- *The extending modules are displayed in the order corresponding to their interconnection. The modules connected further from the basic unit are listed below. If more modules of the same type are connected to one intercom, it may be difficult to assign a setting to a particular module. In this case, identify the modules connected using the* ***Locate Module*** *button. The module will flash shortly several times when you press the button.*

Caution

- Having connected the card reader module to a device into which the **2N® PICard** reading keys have been uploaded, remember to pair the module with the device. Without pairing, the card reader module will not have access to the reading keys and be unable to read encrypted cards. Click **Pair Module** to pair the module.

Note

- *The modules can also be configured via the text row with a list of parameters (parameter_name=parameter_value) separated with semicolons. At present, just a few of these parameters are available. The other parameters are not public as they are rather experimental and can be modified in the future.*

Note

- Module Name has to be unique.
- Unnameable modules can be addressed via ext <module_position>.

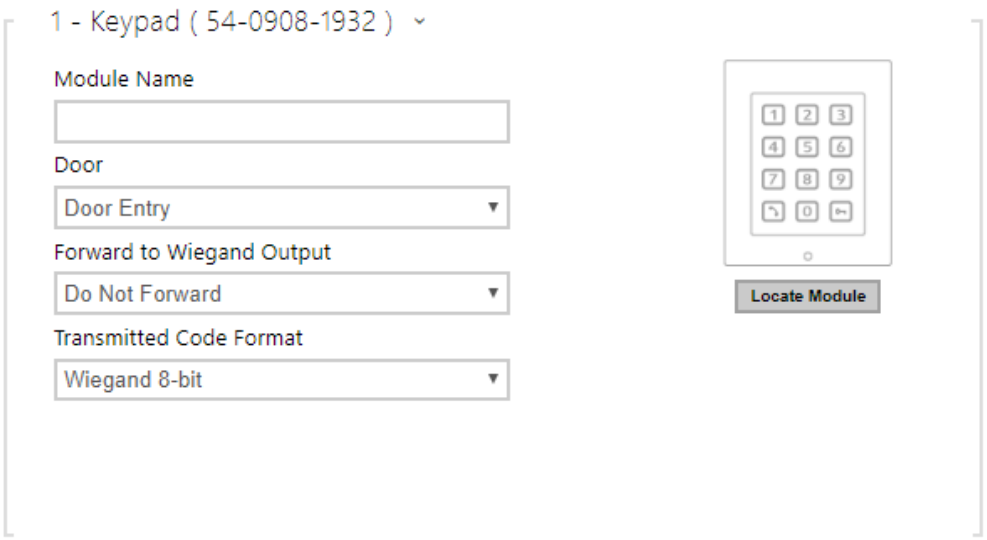
Tip

- Place the mouse cursor onto the module image to display the module's basic production and software information.

Button Module Configuration

- **Button Functions** – press the buttons to dial selected Automation functions.

Keypad Module Configuration



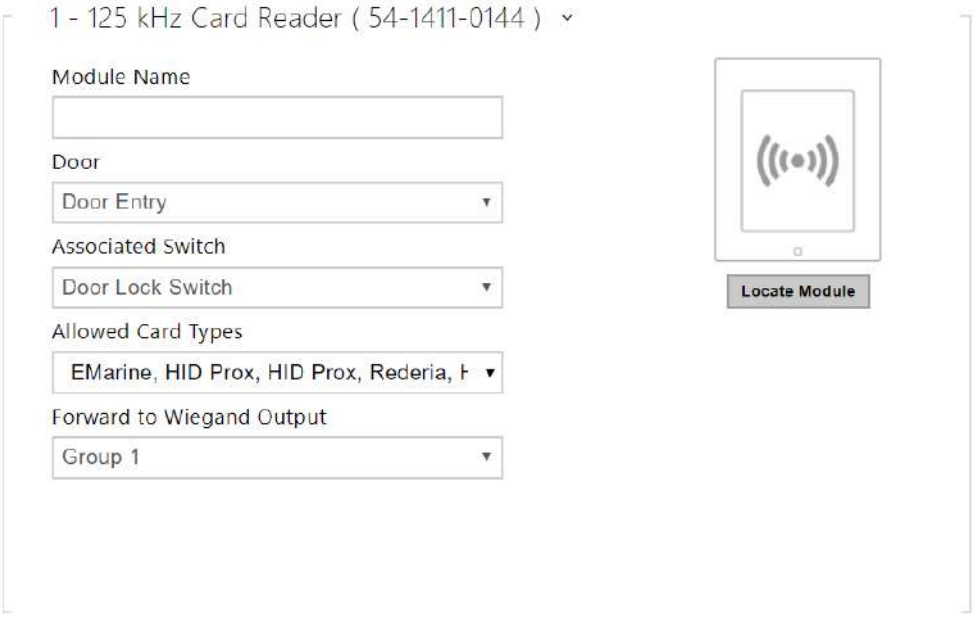
- **Module Name** – set the module name for logging events from the keypad.
- **Door** – set the reader direction (Door Entry, Door Exit) for the Attendance system purposes.

- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all pressed keys are to be forwarded.
- **Transmitted Code Format** – select a 4bit or 8bit (higher security) format for the codes to be transmitted.

Infopanel Module Configuration

- No parameters are available to the public at present.

125 kHz Card Reader Module Configuration



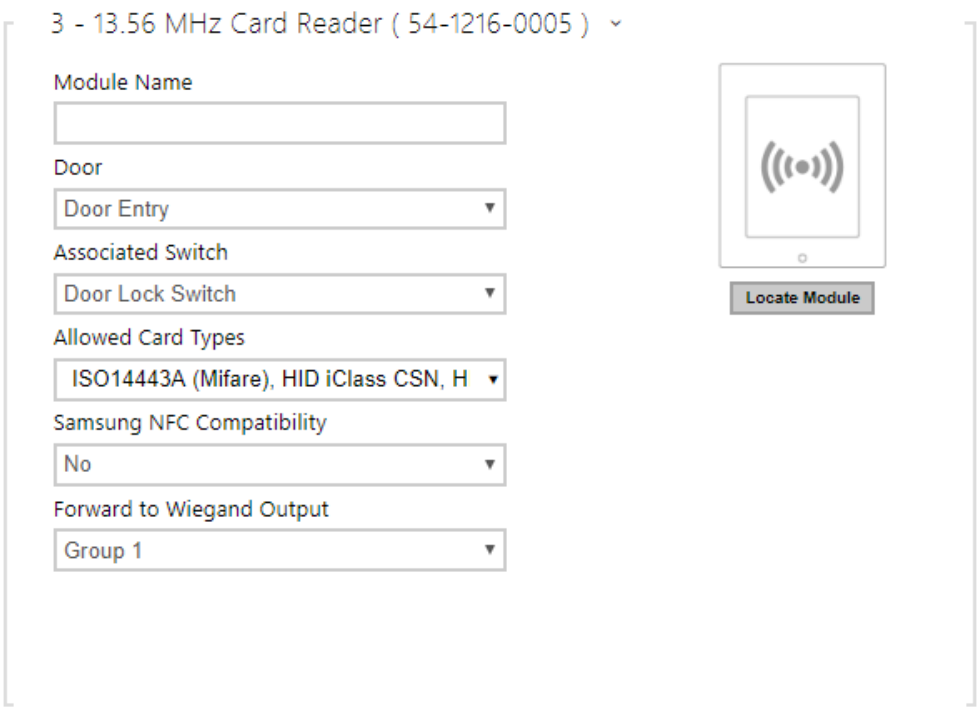
- **Module Name** – set the module name for card reader logging purposes.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.

- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports just one card type at an instant.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resent.

Tip

- To accelerate card reading, you are recommended to select the card types used by the user in the module settings.

13.56 MHz Card Reader Module Configuration



- **Module Name** – set the module name for card reader logging purposes.
- **Door** – set the reader direction (Door Entry, Door Exit) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.

- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports just one card type at an instant.
- **Samsung NFC Compatibility** – enable NFC compatibility with the Samsung phones.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resen

Tip

- To accelerate card reading, you are recommended to select the card types used by the user in the module settings.

Bluetooth Module

- **Module Name** – set the module name for logging events from the Bluetooth module.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Signal Range** – set the maximum signal range, i.e. the distance within which the Bluetooth module can communicate with the mobile phone:
  - **Short** – less than 2 m for most phones
  - **Long** – maximum possible range

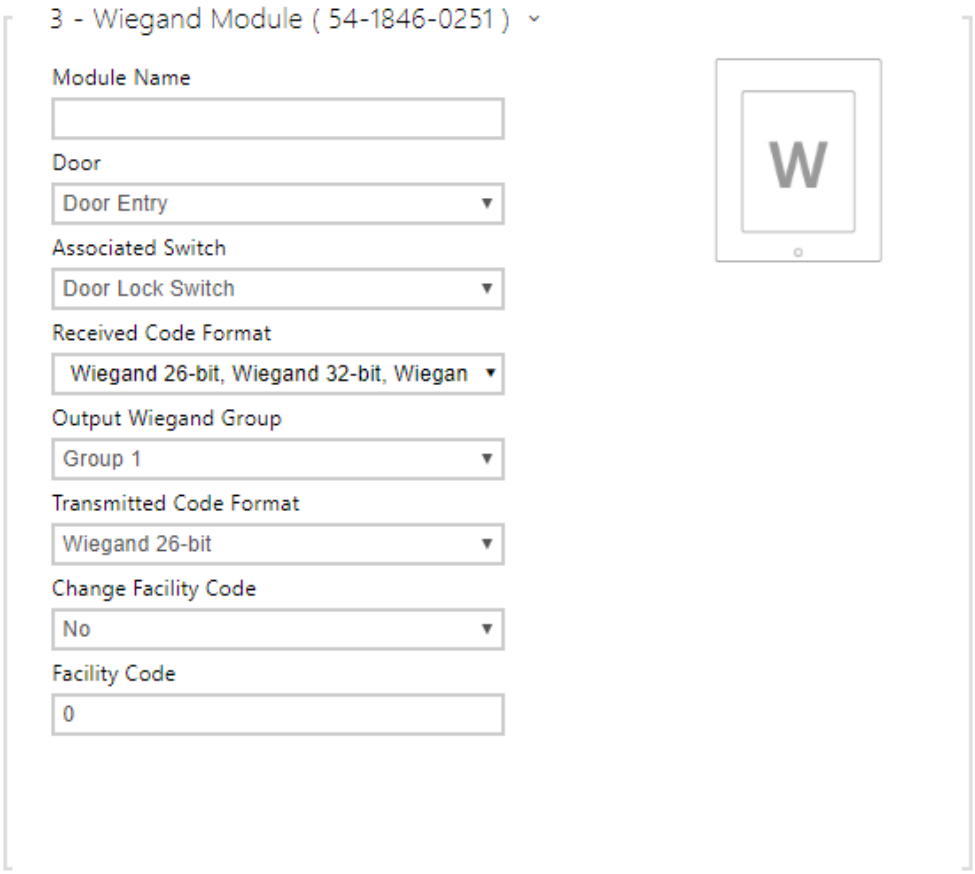
- **Launch Authentication by** – set the authentication method for a mobile phone. Set one or a combination of two/three launch authetication methods.
  - **Tap in app** – authentication has to be confirmed by tapping on an icon in the application running in a mobile phone.
  - **Interacting with Device** – touch the card reader having a phone with paired **2N® Mobile Key** to confirm authentication.

I/O Module Configuration

- **Module Name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in **Automation**.

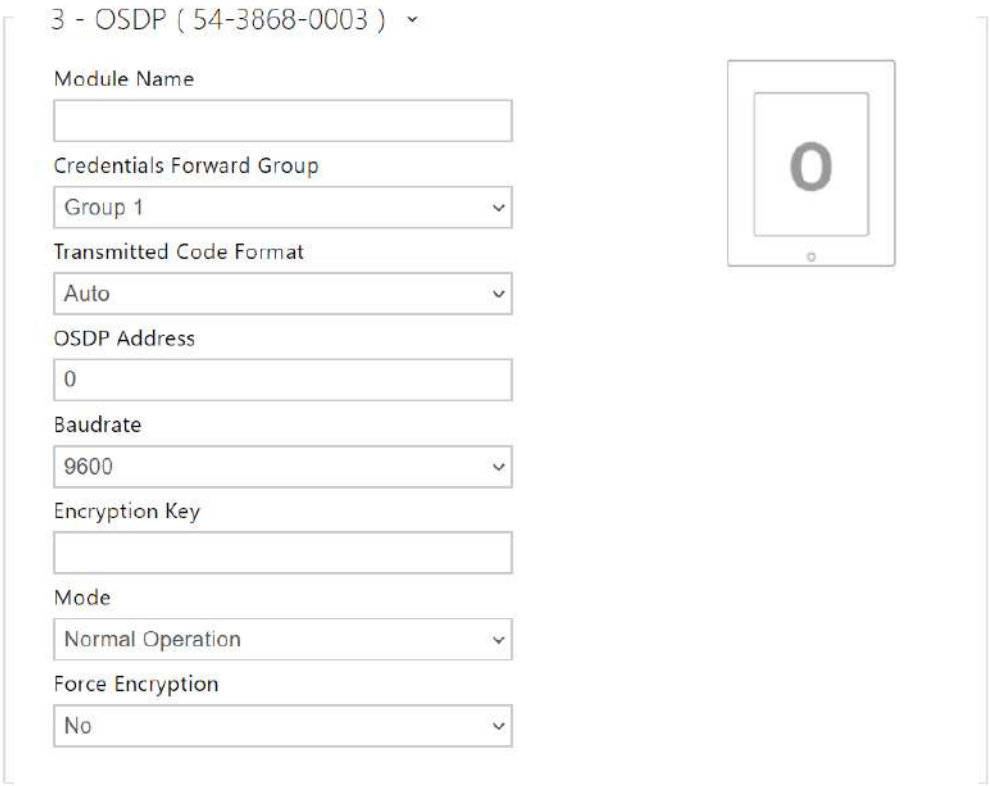
Wiegand Module Configuration

The Wiegand module is equipped with the input and output Wiegand interfaces, which are mutually independent, have separate settings and can receive and send codes at the same time. The Wiegand input helps you connect such equipment as RFID card readers, biometric readers and so on. With the Wiegand output, you can connect the intercom to the security system in your building, for example (to send IDs of the RFID cards tapped on the RFID reader or codes received on any Wiegand input). The **2N® Wiegand Isolator** is also equipped with one logical input and one logical output, which can be controlled via **Automation**.



- **Module Name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N Automation**.
- **Door** – set the reader direction (Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Received Code Format** – set the format for the codes to be received (Wiegand 26, 32, 37 and RAW).
- **Output Wiegand Group** – assign the output Wiegand to a group to which the codes from the connected card readers or Wiegand inputs can be resent.
- **Transmitted Code Format** – set the format for the codes to be transmitted (26-bit, 32-bit, 37-bit and RAW format, 35-bit, Corp. 1000, 48-bit, Corp. 1000 and Auto).
- **Change Facility Code** – set the first code part via Wiegand. This applies to Wiegand OUT for 26-bit code format. Contact your security system supplier to know if the Facility Code is requested.
- **Facility Code** – define the 2N IP device location in the security system. Enter a decimal value for the location (0–255).

OSDP Module Configuration



- **Module Name** – set the module name. The module name is used for input / output specification in **Automation**.
- **Credentials Forward Group** – assign the OSDP output to the group to which codes from the connected card readers or OSDP inputs can be resent.
- **Transmitted Code Format** – set the code format to be transmitted.
- **OSDP Address** – OSDP module address ranging from 0 to 126 on an OSDP line.
- **Baudrate** – set the communication rate in compliance with the device connected.
- **Encryption Key** – set your own key for encrypted communication.
- **Mode** – use the installation mode for encryption key remote setting on the peripheral if enabled. Once the encryption key is received, the normal operation is switched on automatically. The installation mode is signaled by a fast flashing of the LED indicator on the OSDP module.
- **Force Encryption** – set forced encryption for encrypted communication only.

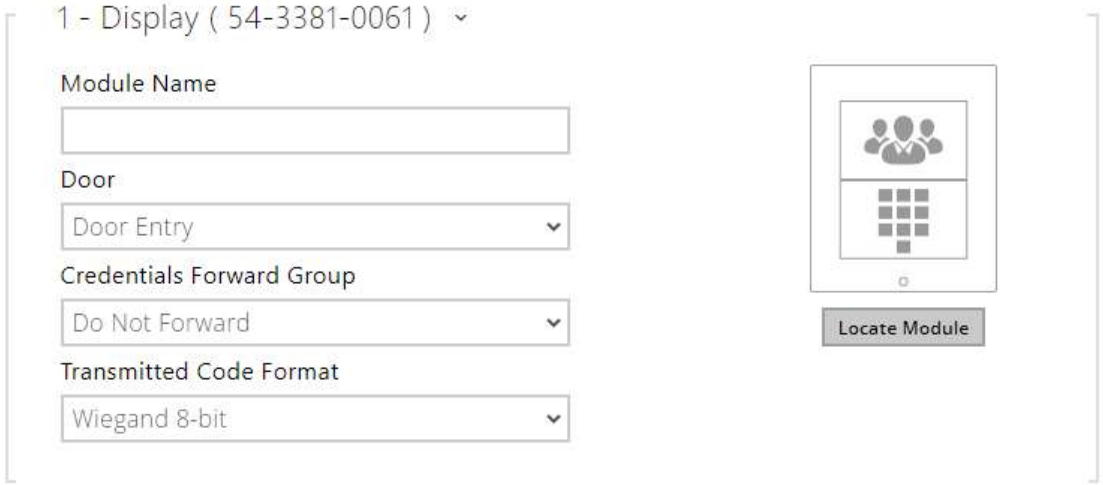
Caution

- When communication is made by the OSDP device in an unencrypted format after forced encryption is set, this communication will be rejected.

Induction Loop Module Configuration

- **Maximum Power** – set the maximum transmission power for the induction loop antenna. A higher transmission power means a wider range, but less power for other intercom functions. The convenient default value is 0.25 W under normal circumstances.

Display Module Configuration



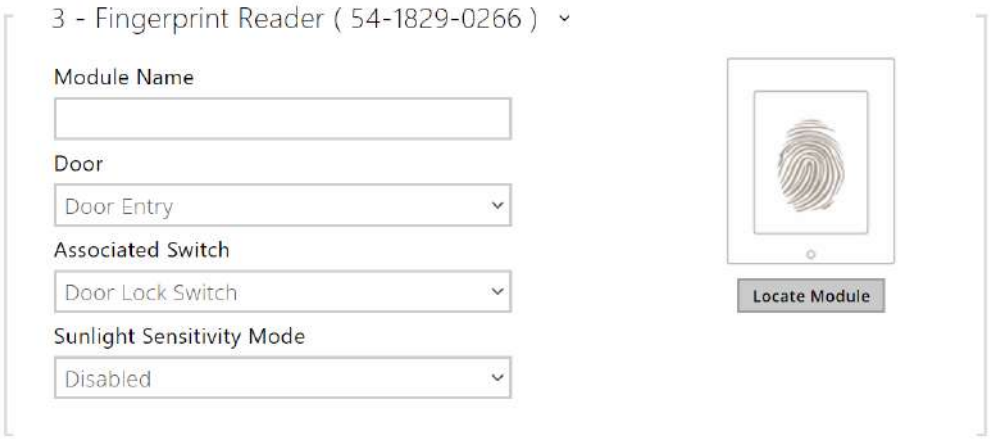
- **Module Name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N Automation**.
- **Door** – set the reader direction for the Attendance system purposes.
- **Credentials Forward Group** – set the group to which all entered access codes will be forwarded.

- **Transmitted Code Format** – selects a 4bit or 8bit (higher security) format for the codes to be transmitted.

Caution

- The display is not supported on Access Unit 1.0 from FW version 2.27.

Fingerprint Reader Module Configuration

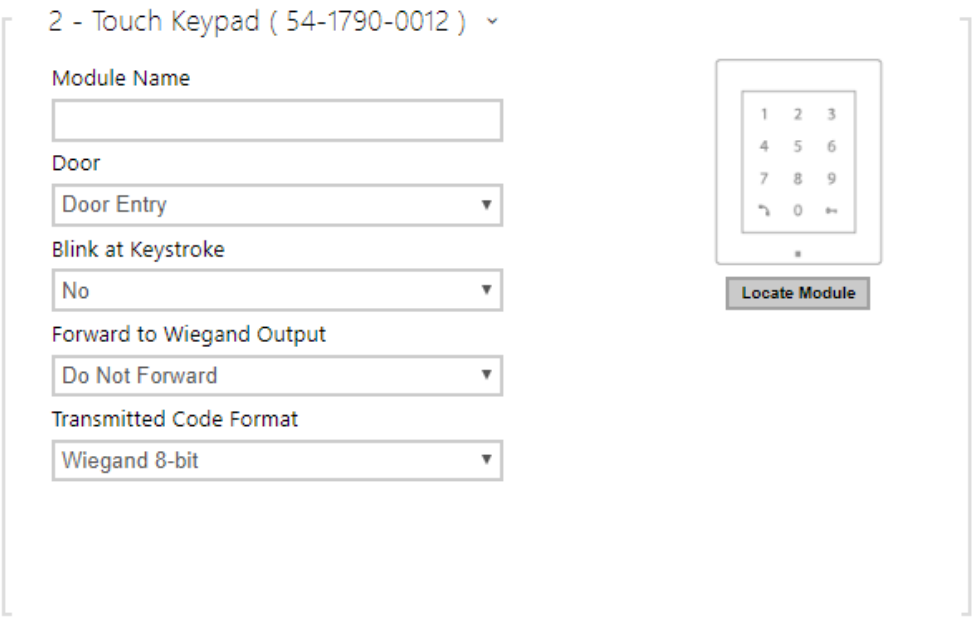


- **Module Name** – set the module name for logging events from the Fingerprint reader.
- **Door** – set the reader direction (Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Sunlight Sensivity Mode** – enable this parameter to prevent erroneous behavior of the reader if exposed to direct sunlight. Restart the device to change the setting. The mode may reduce the reading sensitivity.

Caution

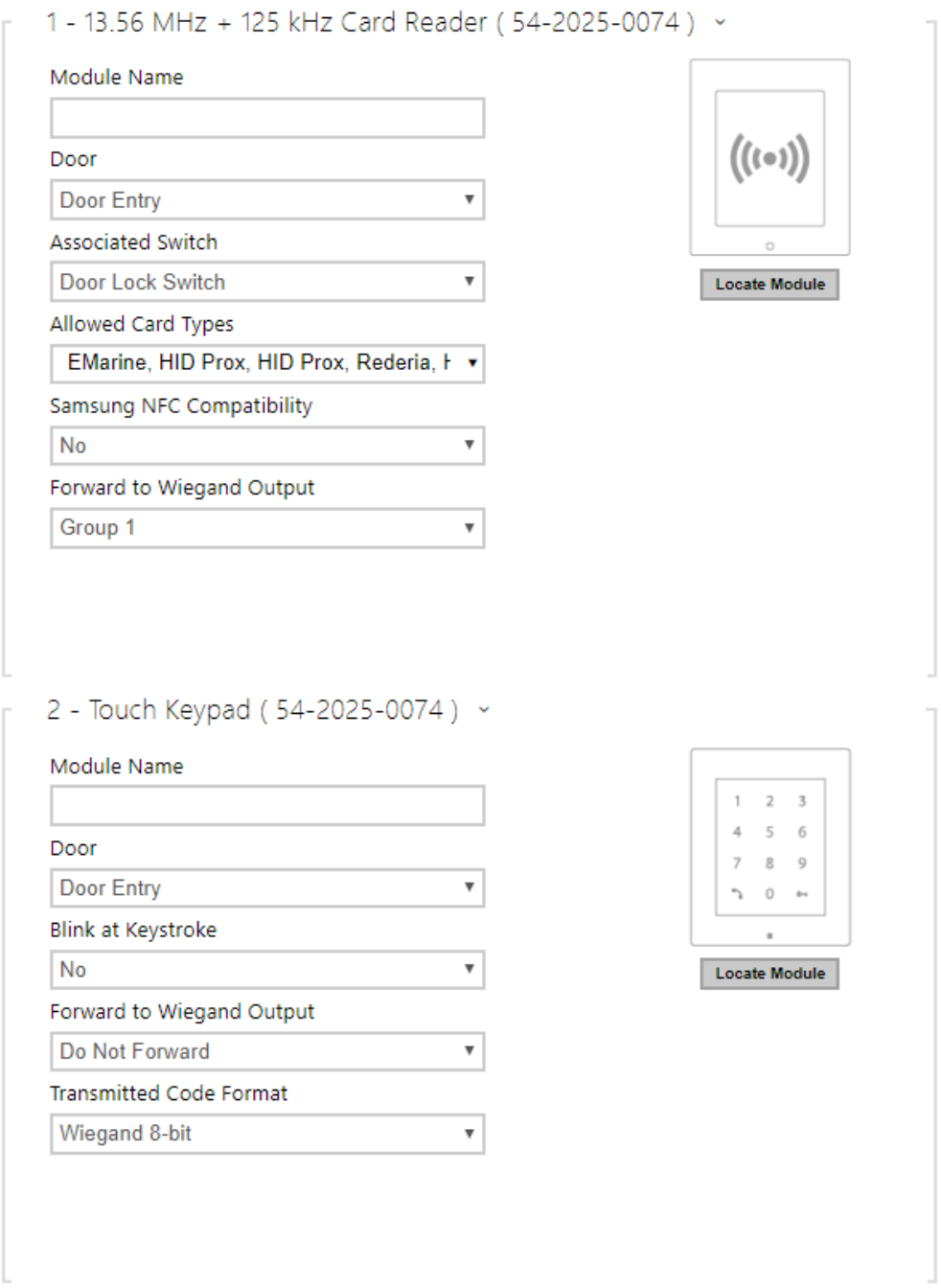
- Whenever the fingerprint reader is disconnected, the User fingerprints will be hidden in the user profile after restart. This section displays how many user fingerprints have been uploaded to the intercom memory. Once a fingerprint reader is reconnected, the User fingerprints will be displayed again.

Touch Keypad



- **Module Name** – set the module name for logging events from the keypad.
- **Door** – set the reader direction (Door Entry, Door Exit) for the Attendance system purposes.
- **Blink at Keystroke** – set keystroke light signalling for noisy environments where acoustic signals are difficult to hear.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all pressed keys are to be forwarded.
- **Transmitted Code Format** – select a 4bit or 8bit (higher security) format for the codes to be transmitted.

Touch Keypad & RFID Reader 125 kHz, 13.56 MHz



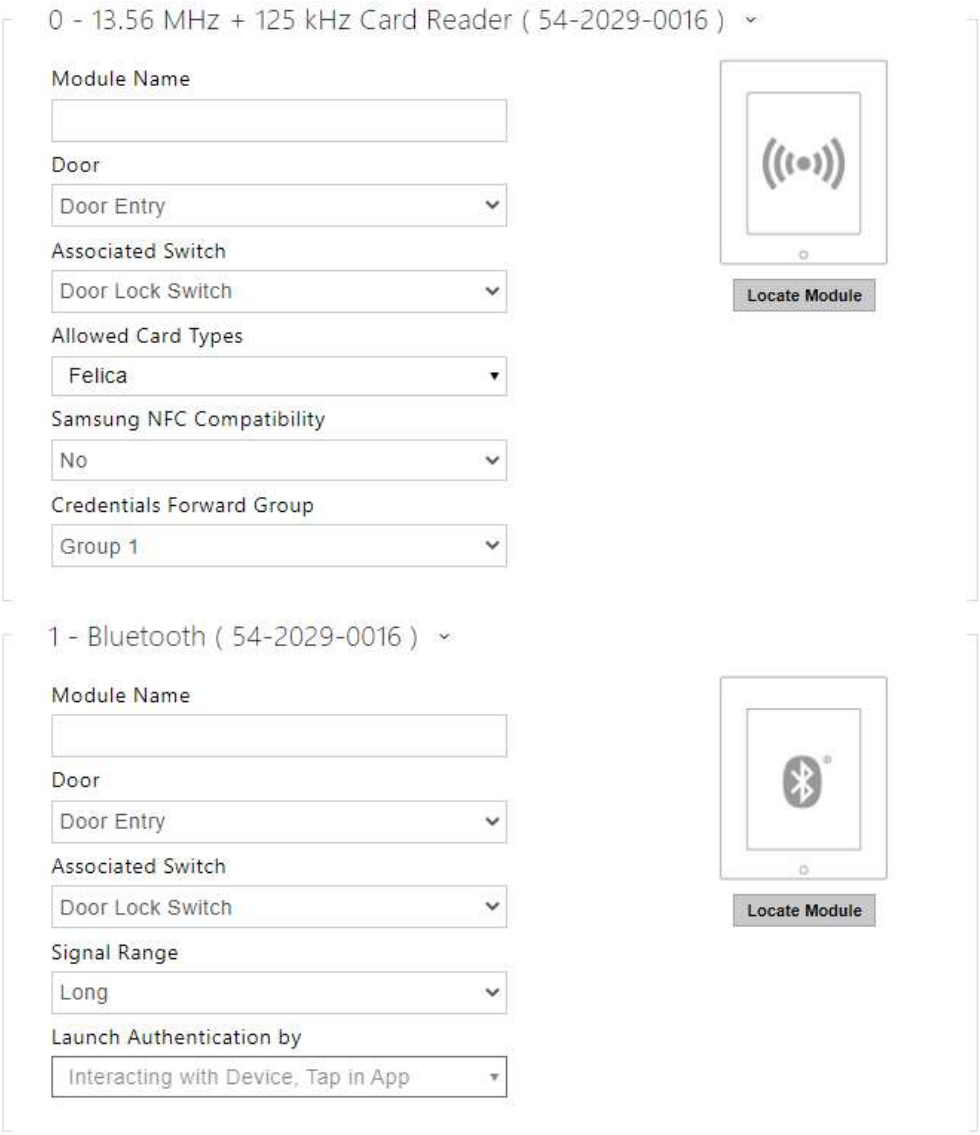
13.56 MHz (125 kHz) Card Reader (serial number)

- **Module Name** – set the module name for card reader logging purposes.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports just one card type at an instant.
- **Samsung NFC Compatibility** – enable NFC compatibility with the Samsung phones.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resent.

Touch keypad (serial number)

- **Module Name** – set the module name for logging events from the touch keypad module.
- **Door** – set the reader direction (Door Entry, Door Exit) for the Attendance system purposes.
- **Blink at Keystroke** – set keystroke light signalling for noisy environments where acoustic signals are difficult to hear.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all pressed keys are to be forwarded.
- **Transmitted Code Format** – select a 4bit or 8bit (higher security) format for the codes to be transmitted.

Bluetooth & RFID Reader 125 kHz, 13.56 MHz



13.56 MHz (125 kHz) Card Reader (serial number)

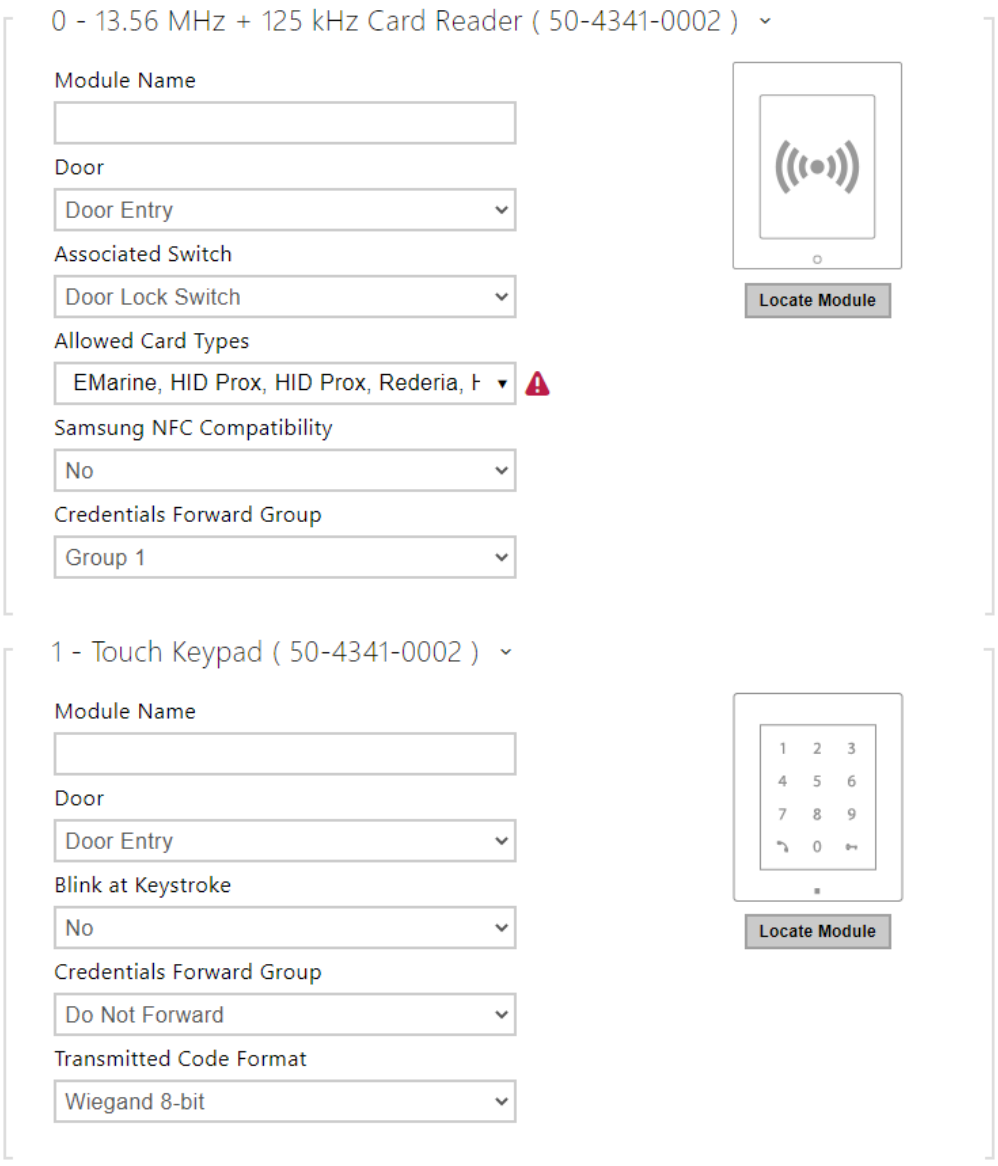
- **Module Name** – set the module name for card reader logging purposes.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.

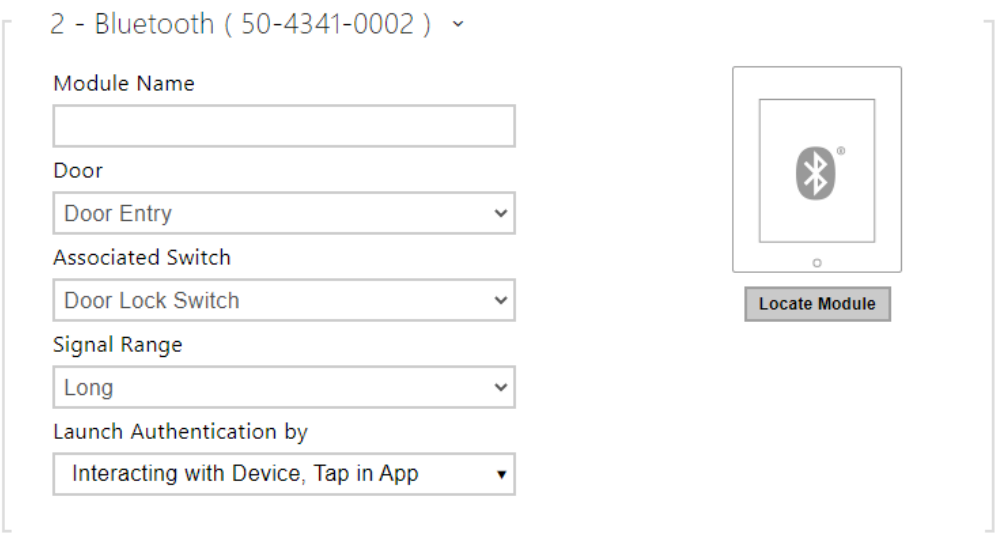
- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports just one card type at an instant.
- **Samsung NFC Compatibility** – enable NFC compatibility with the Samsung phones.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resent.

Bluetooth (serial number)

- **Module Name** – set the module name for logging events from the Bluetooth module.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Signal Range** – set the maximum signal range, i.e. the distance within which the Bluetooth module can communicate with the mobile phone:
  - **Short** – less than 2 m for most phones
  - **Long** – maximum possible range
- **Launch Authentication by** – set the authentication method for a mobile phone. Set one or a combination of two/three launch authetication methods.
  - **Tap in app** – authentication has to be confirmed by tapping on an icon in the application running in a mobile phone.
  - **Interacting with Device** – touch the card reader having a phone with paired **2N® Mobile Key** to confirm authentication.

Touch Keypad & Bluetooth & RFID Reader 125 kHz, 13.56 MHz, NFC





13.56 MHz (125 kHz) Card Reader (serial number)

- **Module Name** – set the module name for card reader logging purposes.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports just one card type at an instant.
- **Samsung NFC Compatibility** – enable NFC compatibility with the Samsung phones.
- **Credentials Forward Group** – allows you to set a group to which all received user access codes will be forwarded.

Touch keypad (serial number)

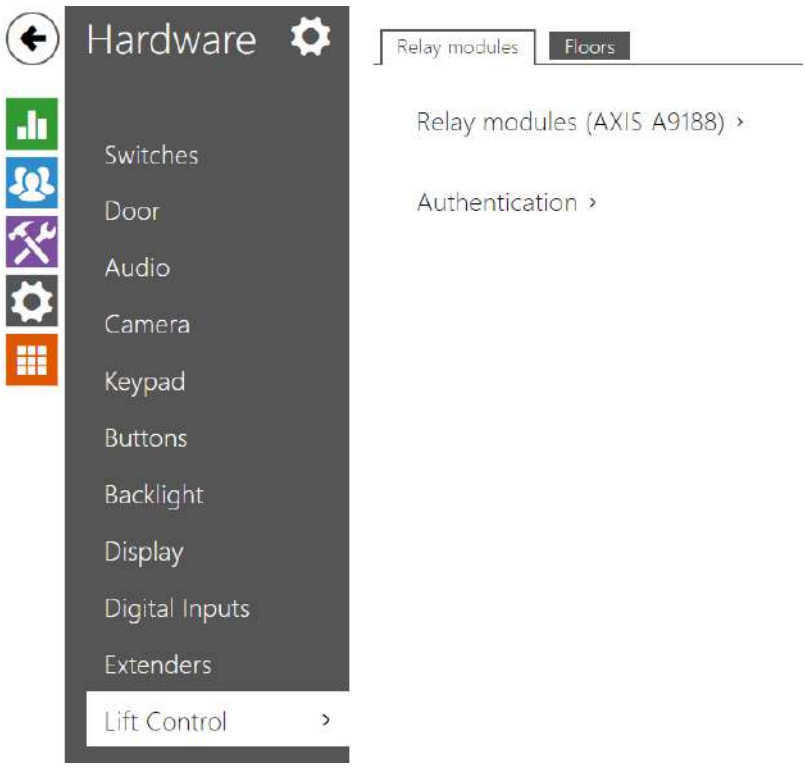
- **Module Name** – set the module name for logging events from the touch keypad module.
- **Door** – set the reader direction (Door Entry, Door Exit) for the Attendance system purposes.
- **Blink at Keystroke** – set keystroke light signalling for noisy environments where acoustic signals are difficult to hear.
- **Credentials Forward Group** – allows you to set a group to which all received user access codes will be forwarded.
- **Transmitted Code Format** – select a 4bit or 8bit (higher security) format for the codes to be transmitted.

Bluetooth (serial number)

- **Module Name** – set the module name for logging events from the Bluetooth module.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.

- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Signal Range** – set the maximum signal range, i.e. the distance within which the Bluetooth module can communicate with the mobile phone:
  - **Short** – less than 2 m for most phones
  - **Long** – maximum possible range
- **Launch Authentication by** – set the authentication method for a mobile phone. Set one or a combination of two/three launch authetication methods.
  - **Tap in app** – authentication has to be confirmed by tapping on an icon in the application running in a mobile phone.
  - **Interacting with Device** – touch the card reader having a phone with paired **2N® Mobile Key** to confirm authentication.

5.3.9 Lift Control

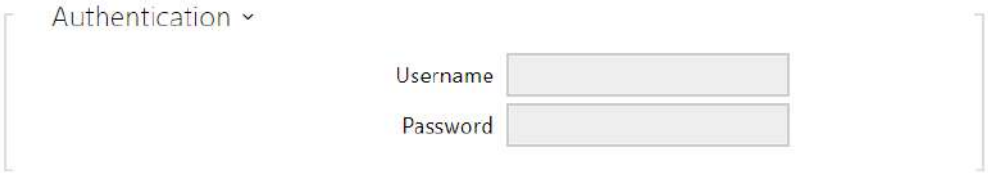


To control the floor lift access, connect the AXIS A9188 relay module to the **2N Access Unit**. Up to 5 relay modules can be connected to one **2N Access Unit**, each of which can control up to 8 floors, which makes a total of 64.

Relay Modules

- **Switch-On Duration** – set the relay module activation time (range of 1 – 600 s).

- **Enabled** – activate/deactivate the AXIS A9188 module used for lift control for up to 8 floors.
- **IP address** – AXIS A9188 IP address.
- **State** – display the state of the connected AXIS A9188 module (Error/Access denied/ Ready/Offline).
- **Serial number** – AXIS A9188 serial number.



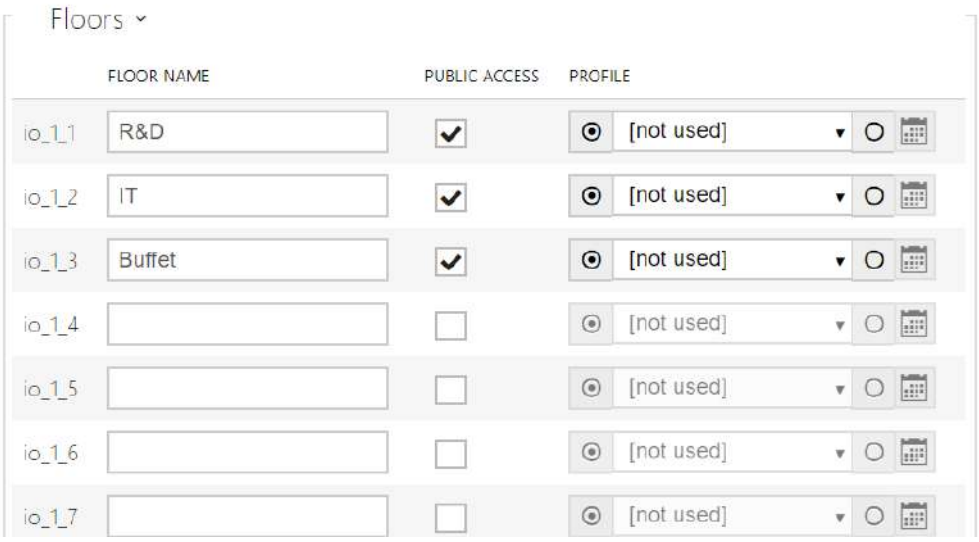
- **Username** – external device authentication username. The parameter is only mandatory if the external device requests authentication.

- **Password** – external device (WEB relay, etc.) authentication password. The parameter is only mandatory if the external device requests authentication.

Caution

- You just need one authentication username and password for all the modules.

Floors



- **Floor name** – set the floor name.
- **Public access** – activate permanent floor access without any authentication.
- **Profile** – select one or more time profiles to be applied. Set the time profiles in the Directory / Time Profiles section.
  - mark the selection from predefined profiles or manual setting of a time profile for the given element.
  - set a time profile for the given element.

Tip

Certificate generation for AXIS A9188

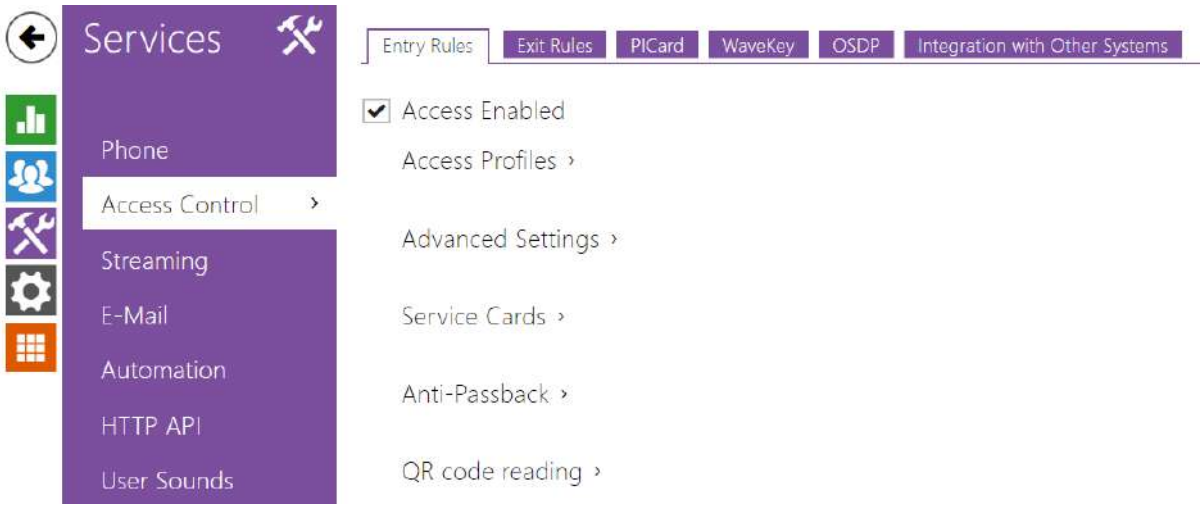
1. Retrieve the AXIS A9188 relay module in the LAN using AXIS IP Utility.
2. Enter the root/root login.
3. Select Preferences / Additional device configuration in the menu.
4. A new device configuration window gets displayed.
5. Select System Options / Security / Certificates.
6. Click Create self-signed certificate to create a certificate.
7. Complete all the required fields and click OK for confirmation.
8. Go to System Options / Security / HTTPS.
9. Select the certificate in a pop-up menu and press Save to save it.
10. Move to the **2N Access Unit** web interface, Hardware / Lift Control. Enter the login data and the relay module IP address.
11. READY gets displayed at the relay module if the connection has been successful.

5.4 Services

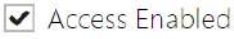
Here is what you can find in this section:

5.4.1 Access Control

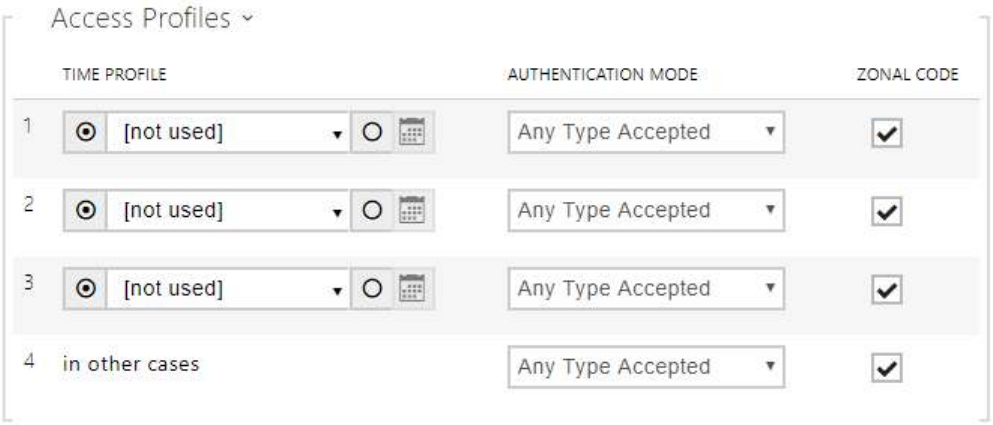
Access Control helps you manage accesses and verify user authentications.



Entry Rules



- **Access Enabled** – enable access in a direction (entry, exit). If access is disabled, the door cannot be opened from the selected side.

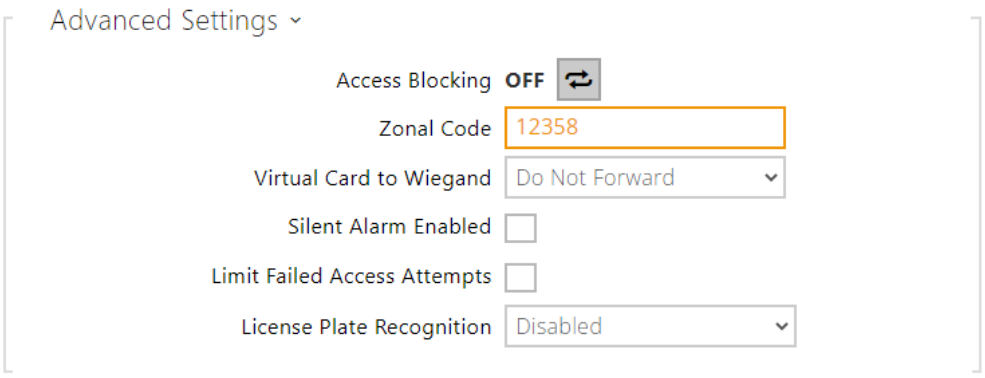


- **Time Profile** – choose one or more time profiles to be applied. Set the time profiles in Directory / Time profiles.
  -  – select one of the pre-defined profiles or set the time profile for the given element manually.

- **Authentication Mode** – set the authentication mode for the time profile in this row including multiple authentication for enhanced security. Select Access denied to ban access.
- **Zonal Code** – enable the zonal code for the time profile and authentication combination in this row. You can use the zonal code instead of the user PIN.

Caution

- If the time profile is unset, the authentication mode is ignored on the given row.



- **Access Blocking** – display the active Access Blocking setting: ON/OFF.
- **Zonal Code** – enter the switch numeric zonal code consisting of two characters at least. However, four characters at least are recommended.
- **Virtual Card to Wiegand** – select a group of Wiegand outputs to which the Virtual user card No. shall be sent after successful authentication. Can be combined with any authentication method, including codes, fingerprints, etc.
- **Silent Alarm Enabled** – a virtual code higher by 1 than the access code is assigned to each access code and used for silent alarm activation. For example, if the access code is 0000, then the silent alarm activation code is 0001. It means, for instance, that silent alarm is 0000 for access code 9999 and so on. Set the silent alarm action in the Automation section.

Caution

- In case the user authenticates itself and activates the silent alarm that is deactivated, the user access will be denied and the alarm will not be activated.

- **Limit Failed Access Attempts** – enable the maximum count of unsuccessful authentication attempts. After five unsuccessful attempts (wrong numeric code, invalid card, etc.), the access module will be blocked for 30 seconds even if authentication is valid.
- **License Plate Recognition** – choose the scenario after the license plate is recognized.

Caution

- It is advisable that each license plate should be assigned to just one entry in the directory. Multiple license plate assignments may result in the inability to assign a license plate to an entry in the directory unambiguously (the first entry assigned the specified license plate is selected and given the access rights).

  - **Disabled**
  - **Opening by License Plate –** The door is unlocked if the entry in the directory with the recognized license plate has currently the entry/exit right. Door (gate etc.) opening after a valid license plate is detected works independently of the other Authentication ways set in the Access profiles.
  - **LPR Multifactor** – this option is only available if Multifactor Authentication of License Plates beta function is activated. Enable permanent access blocking and permanently disable Bluetooth (WaveKey) authentication. Once the license plate is read, its user will be assigned a temporary (60-second) exception and the Wave Key function will be activated for the same time. Access will only be granted to the read license plate user who authenticates using another authenticating method (WaveKey/QR code) within 60 seconds. Users with a permanent exception will be granted access during the whole access blocking period, but will be able to authenticate themselves using WaveKey too within 60 seconds after their license plates are recorded.
    Every next car license plate will cancel the preceding temporary exception and, if there is a user with the newly accepted license plate, a temporary exception is assigned to this user.

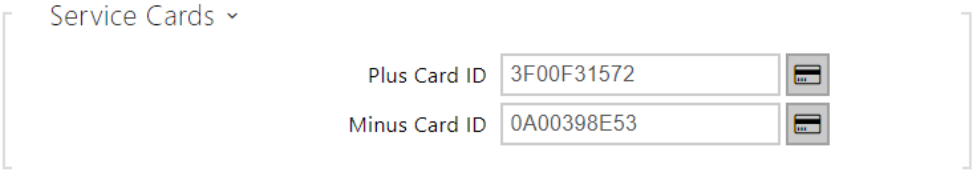
The device allows you to use the recognized license plates sent in an HTTP request by the AXIS cameras equipped with an optional application VaxALPR on api/lpr/licenseplate (refer to the HTTP API Manual for IP Intercoms).

In case the function is on, the event is recorded into the LicensePlateRecognized history when a valid HTTP request has been received. If an image is sent within the HTTP request (photo part or whole photo of the license plate detecting scene), it is saved. The last five photos are stored in

the device memory and can be retrieved via an HTTP request sent to api/lpr/image available in **2N® Access Commander**.

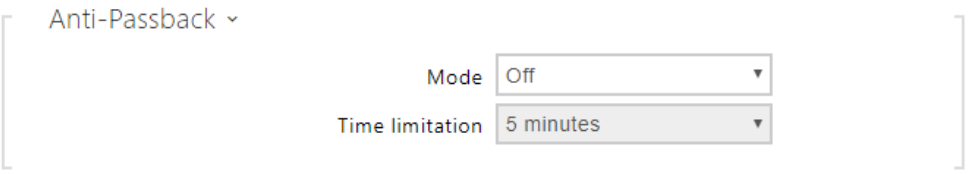
Warning

- The software factory reset or different configuration upload does not result in a change of the access blocking setting. It is only the hardware factory reset using the Reset button on the device that resets the default values.
  - The Security Relay enhances the installation security against hardware reset misuse.



The plus/minus cards are used for user card administration. When a plus card is tapped on the card reader, any other tapped card is added to the Directory list as a new user with an access card assigned. The user !Visitor #card_ID is automatically created in the device. When a minus card is tapped on the card reader, any other tapped card and its user are deleted from the Directory list.

- **Plus Card ID** – enter the service card ID for adding cards to the Installed cards: a sequence of 6 to 32 characters including 0–9, A–F.
- **Minus Card ID** – enter the service card ID for removing cards from the Installed cards: a sequence of 6 to 32 characters including 0–9, A–F.



Anti-Passback is a security function preventing users to use their access cards or other identifiers to re-enter an area without leaving it before (i.e. preventing users from sharing cards).

- **Mode** – enable/disable the Anti-Passback mode:
  - **Off** – the function is Off by default allowing the user to use the access card or another identifier to re-enter an area without leaving it before.

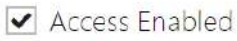
  - **Soft** – the user is allowed to use the access card or another identifier to re-enter an area without leaving it before. A new **UserAuthenticated** record with *apbBroken=**true*** will be created in the Status / Events section.
  - **Hard** – the user is not allowed to use the access card or another identifier to re-enter an area without leaving it before. A new **UserAuthenticated** record with *apbBroken=**true*** will be created in the Status / Events section.
- **Time Limitation** – select an Anti-Passback timeout during which the user cannot re-enter an area using the given authentication method (card, code, etc.) in the same direction.

- **Enabled** – enable/disable QR code reading using the device camera. If QR code reading is enabled, it is possible to enter PIN codes and individual switch codes longer than ten digits by showing the QR code to the device camera.

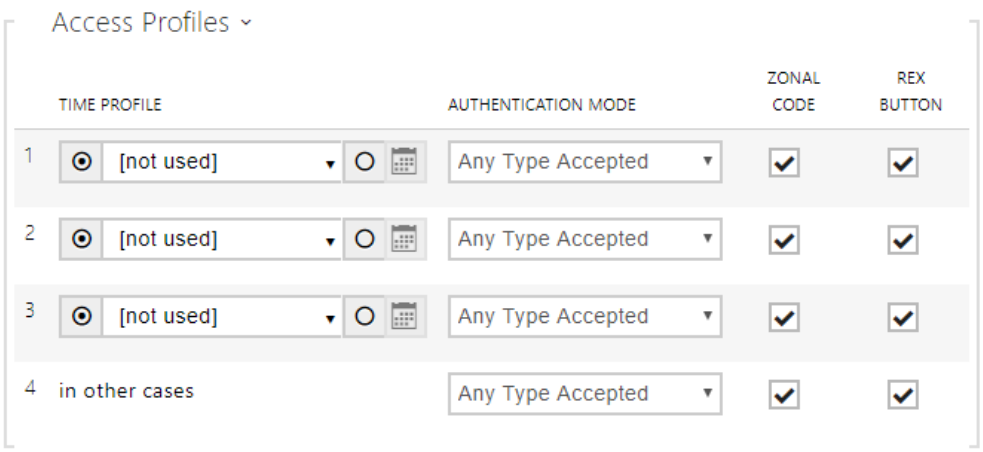
Caution

- Do not use privacy masking in combination with QR code reading to make the QR code reading function work properly.
- For increased security, limit the count of unsuccessful accesses in the Advanced Settings block above.
- The QR code reading function is only available in models equipped with the ARTPEC-7 microcontroller supplied by Axis.

Exit Rules



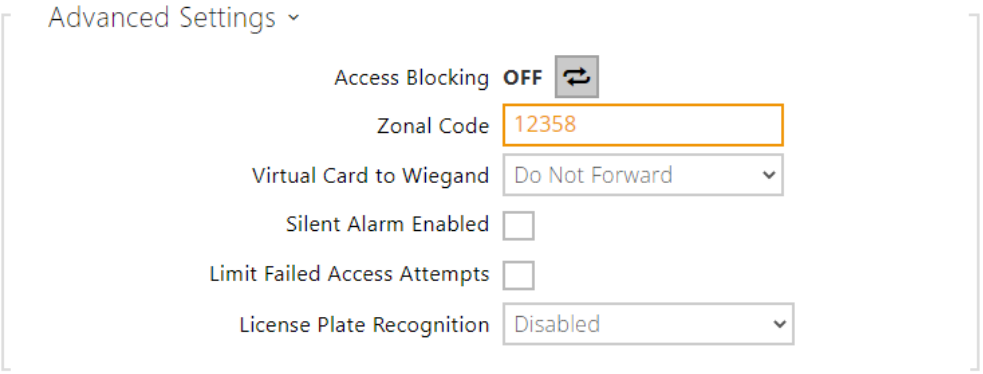
- **Access enabled** – enable access in a direction (entry, exit). If access is disabled, the door cannot be opened from the selected side.



- **Time Profile** – choose one or more time profiles to be applied. Set the time profiles in Directory / Time profiles.
  -  – select one of the pre-defined profiles or set the time profile for the given element manually.
- **Authentication Mode** – set the authentication mode for the time profile in this row including multiple authentication for enhanced security. Select Access denied to ban access.
- **Zonal Code** – enable the zonal code for the time profile and authentication combination in this row. You can use the zonal code instead of the user PIN.
- **REX Button** – enable the exit button function for the selected time profile. Set the exit button input in Hardware / Door / Door tab.

Caution

- If the time profile is unset, the authentication mode is ignored on the given row.



- **Access Blocking** – display the active Access Blocking setting: ON/OFF.

- **Zonal Code** – enter the switch numeric zonal code consisting of two characters at least. However, four characters at least are recommended.
- **Virtual Card to Wiegand** – select a group of Wiegand outputs to which the Virtual user card No. shall be sent after successful authentication. Can be combined with any authentication method, including codes, fingerprints, etc.
- **Silent Alarm Enabled** – a virtual code higher by 1 than the access code is assigned to each access code and used for silent alarm activation. For example, if the access code is 0000, then the silent alarm activation code is 0001. It means, for instance, that silent alarm is 0000 for access code 9999 and so on. Set the silent alarm action in the Automation section.

Caution

- In case the user authenticates itself and activates the silent alarm that is deactivated, the user access will be denied and the alarm will not be activated.

- **Limit Failed Access Attempts** – enable the maximum count of unsuccessful authentication attempts. After five unsuccessful attempts (wrong numeric code, invalid card, etc.), the access module will be blocked for 30 seconds even if authentication is valid.
- **License Plate Recognition** – choose the scenario after the license plate is recognized.

Caution

- It is advisable that each license plate should be assigned to just one entry in the directory. Multiple license plate assignments may result in the inability to assign a license plate to an entry in the directory unambiguously (the first entry assigned the specified license plate is selected and given the access rights).

  - **Disabled**
  - **Opening by License Plate –** The door is unlocked if the entry in the directory with the recognized license plate has currently the entry/exit right. Door (gate etc.) opening after a valid license plate is detected works independently of the other Authentication ways set in the Access profiles.
  - **LPR Multifactor** – this option is only available if Multifactor Authentication of License Plates beta function is activated. Enable permanent access blocking and permanently disable Bluetooth (WaveKey) authentication. Once the license plate is read, its user will be assigned a temporary (60-second) exception and the Wave Key function will be activated for the same time. Access will only be granted to the read license plate user who authenticates using another authenticating method (WaveKey/QR code) within 60 seconds. Users with a permanent exception will be granted access during the whole access blocking period, but will be able to authenticate themselves using WaveKey too within 60 seconds after their license plates are recorded.
    Every next car license plate will cancel the preceding temporary exception and, if there is a user with the newly accepted license plate, a temporary exception is assigned to this user.

The device allows you to use the recognized license plates sent in an HTTP request by the AXIS cameras equipped with an optional application VaxALPR on api/lpr/licenseplate (refer to the HTTP API Manual for IP Intercoms).

In case the function is on, the event is recorded into the LicensePlateRecognized history when a valid HTTP request has been received. If an image is sent within the HTTP request (photo part or whole photo of the license plate detecting scene), it is saved. The last five photos are stored in

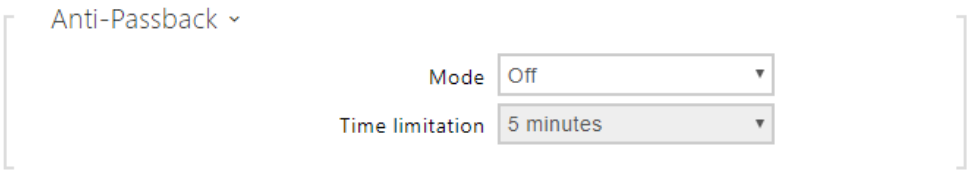
the device memory and can be retrieved via an HTTP request sent to api/lpr/image available in **2N® Access Commander**.

Warning

- The software factory reset or different configuration upload does not result in a change of the access blocking setting. It is only the hardware factory reset using the Reset button on the device that resets the default values.
  - The Security Relay enhances the installation security against hardware reset misuse.

The plus/minus cards are used for user card administration. When a plus card is tapped on the card reader, any other tapped card is added to the Directory list as a new user with an access card assigned. The user !Visitor #card_ID is automatically created in the device. When a minus card is tapped on the card reader, any other tapped card and its user are deleted from the Directory list.

- **Plus Card ID** – enter the service card ID for adding cards to the Installed cards: a sequence of 6 to 32 characters including 0–9, A–F.
- **Minus Card ID** – enter the service card ID for removing cards from the Installed cards: a sequence of 6 to 32 characters including 0–9, A–F.



Anti-Passback is a security function preventing users to use their access cards or other identifiers to re-enter an area without leaving it before (i.e. preventing users from sharing cards).

- **Mode** – enable/disable the Anti-Passback mode:
  - **Off** – the function is Off by default allowing the user to use the access card or another identifier to re-enter an area without leaving it before.
  - **Soft** – the user is allowed to use the access card or another identifier to re-enter an area without leaving it before. A new **UserAuthenticated** record with *apbBroken=**true*** will be created in the Status / Events section.

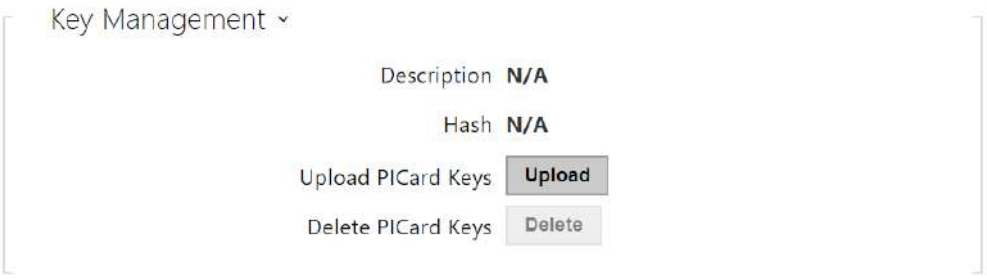
  - **Hard** – the user is not allowed to use the access card or another identifier to re-enter an area without leaving it before. A new **UserAuthenticated** record with *apbBroken=**true*** will be created in the Status / Events section.
- **Time Limitation** – select an Anti-Passback timeout during which the user cannot re-enter an area using the given authentication method (card, code, etc.) in the same direction.

PICard

The 2N® PICard technology is used for encryption of access card login data. To read the login data, the 2N devices need access to the keys generated by the 2N® PICard Commander application. The keys can subsequently be imported to 2N® Access Commander for distribution to all of the supported 2N devices.

Caution

- Refer to the 2N® PICard Commander Configuration Manual for the devices on which cards with the PICard technology can be read.



- **Description** – encryption key name.
- **Hash** – project numerical ID.
- **Upload PICard Keys** – select the key file and enter the valid password to upload the PICard key.
- **Delete PICard Keys** – delete the uploaded PICard keys.

WaveKey

The **2N IP intercoms** equipped with the Bluetooth module allow for user authentication via the **2N® Mobile Key** application available to devices with iOS 12 and higher (iPhone 4s and higher phones) or Android 6.0 Marshmallow and higher (Bluetooth 4.0 Smart supporting phones).

User Identification (Auth ID)

The **2N® Mobile Key** application authenticates itself with a unique identifier on the intercom side: **Auth ID** (128-bit number) is generated randomly for every user and **paired** with the intercom user and its mobile device.

Note

- The generated Auth ID cannot be saved in more mobile devices than one. This means that Auth ID uniquely identifies just one mobile device or its user.

You can set and edit the Auth ID value for each user in the Mobile Key section of the intercom phone book. You can move Auth ID to another user or copy it to another intercom. By deleting the Auth ID value you can block the user's access.

Encryption Keys and Locations

The **2N® Mobile Key** – intercom communication is always encrypted. **2N® Mobile Key** cannot authenticate a user without knowing the encryption key. The primary encryption key is automatically generated upon the intercom first launch and can be re-generated manually any time later. Together with AuthID, the primary encryption key is transmitted to the mobile device for pairing.

You can export/import the encryption keys and location identifier to other intercoms. Intercoms with identical location names and encryption keys form so-called **locations**. In one location, a mobile device is paired just once and identifies itself with one unique Auth ID (i.e. a user AuthID can be copied from one intercom to another within a location).

Pairing

Pairing means transmission of user access data to a user personal mobile device. The user access data can only be saved into one mobile device, i.e. a user cannot have two mobile devices for authentication, for example. However, the user access data can be saved into multiple locations in one mobile device (i.e. the mobile device is used as a key for more locations at the same time).

To pair a user with a mobile device, use the user's page in the intercom phone book. Physically, you can pair a user locally using the USB Bluetooth module connected to your PC or remotely using an integrated Bluetooth module. The results of both the pairing methods are the same.

The following data is transmitted to a mobile device for pairing:

- Location identifier
- Location encryption key
- User Auth ID

Encryption Key for Pairing

An encryption key other than that used for communication after pairing is used in the pairing mode for security reasons. This key is generated automatically upon the intercom first launch and can be re-generated any time later.

Encryption Key Administration

The intercom can keep up to 4 valid encryption keys: 1 primary and up to 3 secondary ones. A mobile device can use any of the 4 keys for communication encryption. The encryption keys are fully controlled by the system administrator. It is recommended that the encryption keys should be periodically updated for security reasons, especially in the event of a mobile device loss or intercom configuration leak.

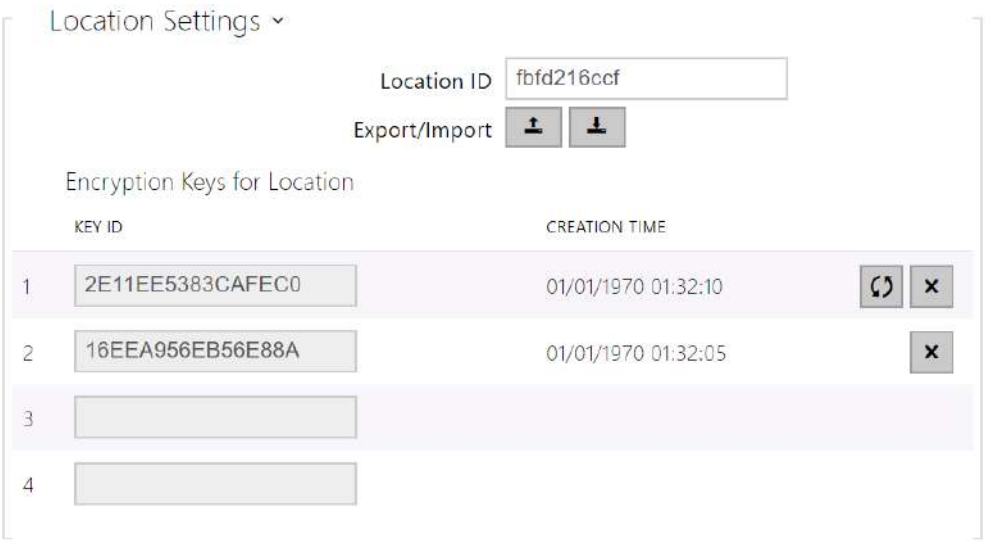
Note

- The encryption keys are generated automatically upon the intercom first launch and saved into the intercom configuration file. We recommend you to re-generate the encryption keys manually before the first use to enhance security.

The primary key can be re-generated any time. Thus, the original primary key becomes the first secondary key, the first secondary key becomes the second secondary key and so on. Secondary keys can be deleted any time.

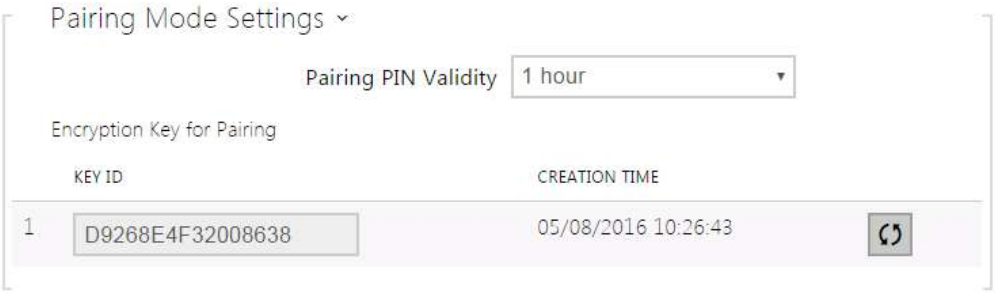
When a key is deleted, the **2N® Mobile Key** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **2N® Mobile Key** application.

List of Parameters



- **Location ID** – set a unique identifier for the location in which the selected encryption key set is valid.
- **Export** – push the button to export the location ID and current encryption keys into a file. Subsequently, the exported file can be imported to another device.

- **Import** – push the button to import the location ID and current encryption keys from a file exported from another intercom.
- **Restore primary key** – by generating a new primary encryption key you delete the oldest secondary key. Thus, the **2N® Mobile Key** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **2N® Mobile Key** application.
- **Delete primary key** – delete the primary key to prevent the users that still use this key from authentication.
- **Delete secondary key** – the **2N® Mobile Key** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **2N® Mobile Key** application.



- **Pairing PIN validity** – set the authorisation PIN validity for user mobile device pairing with the intercom.

Tip

- In the case of loss of a mobile phone with access data proceed as follows:

1. Delete the Mobile Key Auth ID value for the user to block the lost phone and avoid misuse.
2. Re-generate the primary encryption key (optionally) to avoid misuse of the encryption key stored in the mobile device.

Warning

- With the upgrade to version 2.30, the bluetooth modules will also be upgraded. When downgrading to version 2.29 and lower, they may malfunction.

OSDP

The OSDP provides secure communication for sending such login data as access card IDs or PIN codes between the connected OSDP device (control panel, door controller) and a 2N Access Unit. The goal is to enable signaling on the **2N Access Unit** based on the counterparty's response to the card signaling definition sent.

- **OSDP Signaling Enable** – definition string for access enable signaling.
- **OSDP Denied Signaling** – definition string for access denial signaling.

Note

- If identical definitions are inserted in the two parameters above, an evaluation is made with audio visual signals as if one authorized access and one unauthorized access have been used closely one after another.

The Received Messages box helps you get the definition string. When an access card is tapped on the 2N Access Unit reader, the counterparty's OSDP signaling definition is displayed for authorized / unauthorized access.

The received message is displayed in the following format:

13:46:39] led(0,0,0,0,0,0,0,0,1,1,1,2,2)
13:46:39] buz(0,2,1,1,1)
13:46:42] led(0,0,0,0,0,0,0,0,1,1,1,1,1)
13:46:42] buz(0,1,0,0,0)

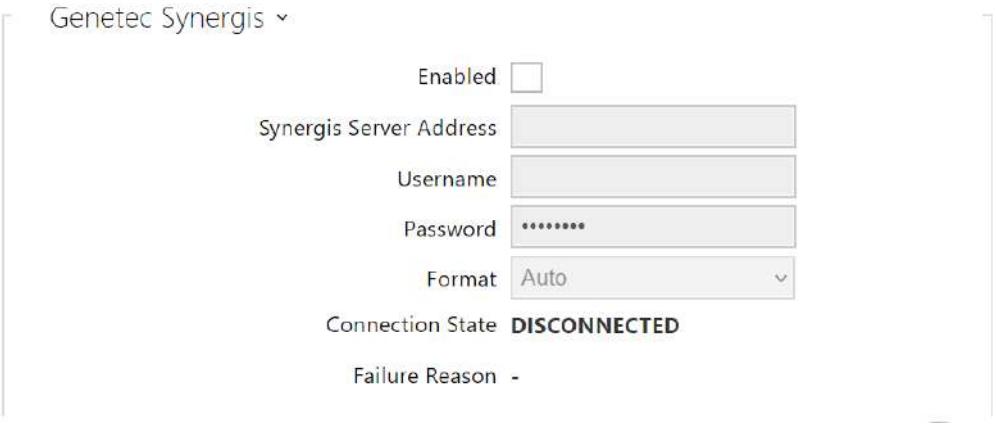
A part of the message (without the time value) is used as the definition string, whose length may not exceed 255 characters, e.g.: led(0,0,0,0,0,0,0,0,1,1,1,1,1) or buz(0,2,1,1,1). Having evaluated a match on the counterparty, the device responds with an adequate signaling. Any part of the definition can be replaced with "*", which will be interpreted as an arbitrary message content (e.g. it is possible to ensure that signaling will be activated upon any LED 0 light on the device regardless of the other message parameters).

- **Clear Log** – delete a Received messages record.

Note

- Make sure that the Door / Unused parameter is set for the card reader and keypad in Hardware / Extending modules to make the function work. The 2N Access Unit confirms the card reading by a beep and the device responds with an appropriate signaling after evaluation.

Integration with Other Systems

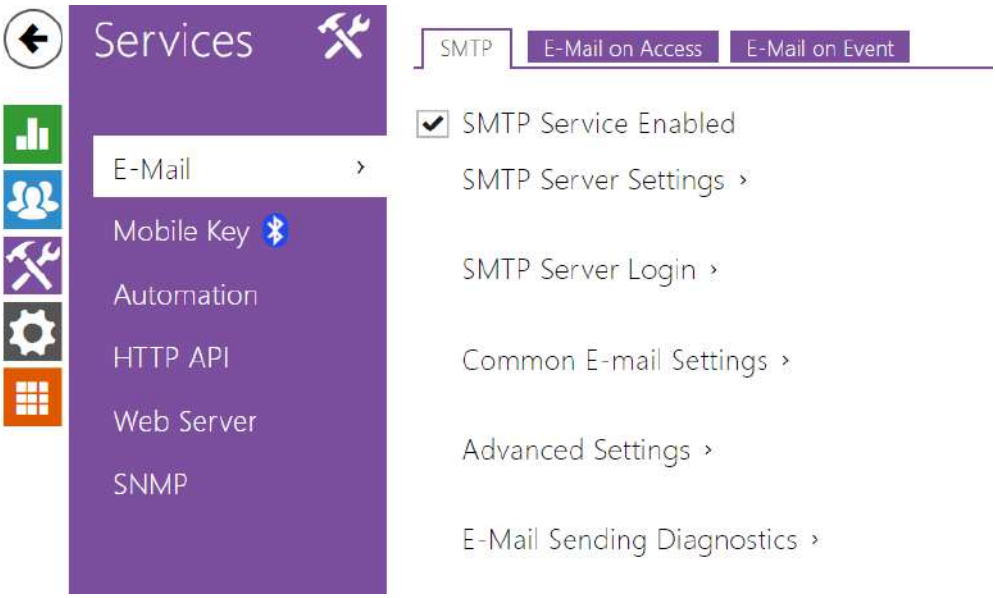


- **Enabled** – enable connection with the Genetec Synergis external security system.
- **Synergis Server Address** – Synergis server IP address or domain name.
- **Username** – authentication user name.
- **Password** – authentication password.
- **Format** – set the card reading format for sending card IDs to Genetec Synergis.
- **Forward Code** – set whether or not the set codes are to be resent. The codes may contain up to 6 digits and their ends have to be confirmed with a key.
- **Connection State** – display the current Synergis server connection state or error state description if necessary.
- **Failure Reason** – display the failure reason of the last Synergis server connection attempt – the last error response, 404 Not Found, for example.

Advanced Folder

- **Compatibility Mode** – support older card reading modes. This mode is not recommended in combination with the PICard cards. If this mode is off, the card numbers must be a perfect match for successful authorization.

5.4.2 E-mail



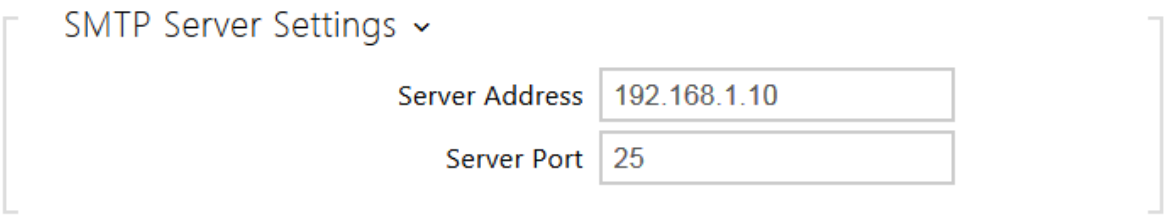
To inform the intercom users on all missed and/or successfully completed calls, configure **2N IP intercom** to send an e-mail after every call to the called user. You can compile the e-mail subject and message text of your own. If your intercom is equipped with a camera, you can automatically attach one or more snapshots taken during the call or ringing.

The intercom sends e-mails to all the users whose valid e-mail addresses are included in the users list. If the **E-mail** parameter in the user list is empty, e-mails are sent to the default e-mail address.

You can also send e-mails via Automation using the **Action.SendEmail** action.

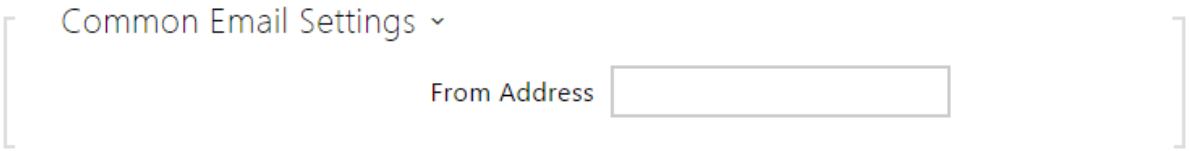
SMTP

- **SMTP service enabled** – enable/disable sending e-mails from the intercom.



- **Server address** – set the SMTP server address to which e-mails shall be sent.
- **Server port** – specify the SMTP server port. Modify the value only if the SMTP server setting is substandard. The typical SMTP port value is 25.

- **Username** – enter a valid username for login if the SMTP server requires authentication, or leave the field empty if not.
- **Password** – enter the SMTP server login password.
- **Client certificate** – specify the client certificate and private key for the intercom – SMTP server communication encryption. Choose one of the three sets of user certificates and private keys (refer to the Certificates subs.) or keep the **SelfSigned** setting, in which the certificate automatically generated upon the first intercom power up is used.



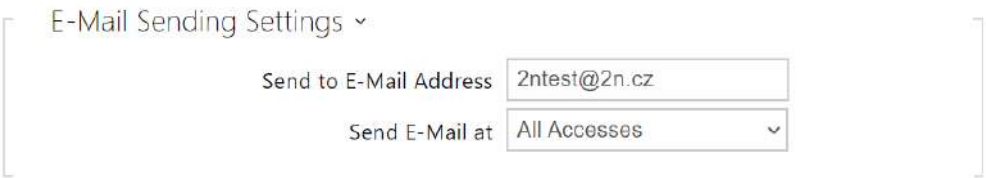
- **From address** – set the sender address for all outgoing e-mails from the device.

- **Deliver In** – set the time limit for delivering an e-mail to an inaccessible SMTP server.

Click **Apply & Test** to send a testing e-mail to the defined address with the aim to test the functionality of the current e-mail sending setting. Enter the destination e-mail address into the Test e-mail address field and press the button. The current e-mail sending state is continuously displayed in the window for you to detect an e-mail setting problem if any on the intercom or another network element.

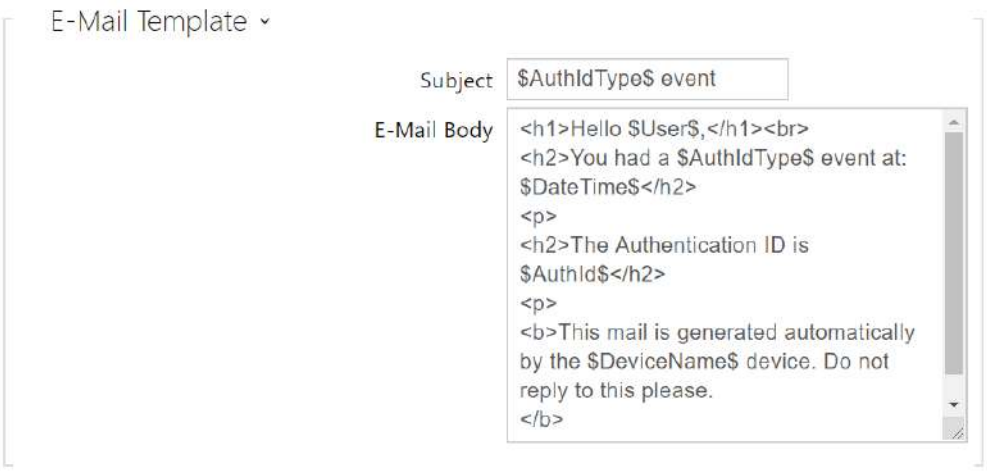
E-mail on Access

Set that an e-mail shall be sent whenever an RFID card is tapped on the card reader and/or Bluetooth/fingerprint reader identification is made.



- **Send E-Mail at** – set e-mail sending. The following options are available:
  - **Do Not Send E-mail** – no e-mail message will be sent.
  - **All Accesses** – an e-mail will be sent at all (valid/invalid) access attempts.

- **Denied Accesses** – an e-mail will only be sent if the access is denied.



- **Subject** – set the e-mail subject to be sent.
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date and time, intercom/card identification, Bluetooth/fingerprint identifier and identifier validity for information. These symbols will be replaced with the actual value before sending. SThe list of placeholders found in the template is shown in the overview table at the end of this chapter.

E-Mail Body

```
<p>Hello,
</p>
<p>User <b>$User$</b> generated a new access event on device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>)
</p>
<ul>
  <li>Authentication Type: <b>$AuthIdType$</b>
  </li>
  <li>Authentication ID: <b>$AuthId$</b>
  </li>
  <li>Validity: <b>$AuthIdValid$</b>
  </li>
  <li>Reason: <b>$AuthIdReason$</b>
  </li>
  <li>Direction: <b>$AuthIdDirection$</b>
  </li>
  <li>Date/Time: <b>$DateTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
```

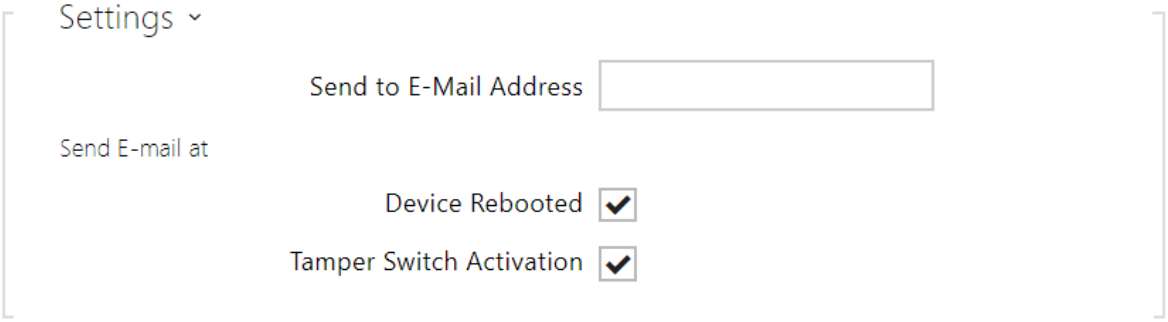
```
</p>
```

Caution

- An extended syntax can be used for the $AuthIdType$ and $AuthIdValid$ placeholders to replace the values in different languages.
- In the case of an invalid value of $AuthId$, the first half of the ID is masked, e.g.: ******11188, **********792d9044158891fa etc.
- In the case of a valid value of $AuthId$, the whole ID is masked ****.
- If the placeholder value is not found in the string, the value is used directly.

E-Mail on Event

Set that an e-mail shall be sent whenever the SIP gets lost, the device is rebooted or the tamper switch is activated on the device.



Send to E-Mail Address – set e-mail sending. The following options are available:

- **Device Rebooted**
- **Tamper Switch Activation**

Device Restart Message – set the message to be sent to the specified e-mail address whenever the device is restarted.

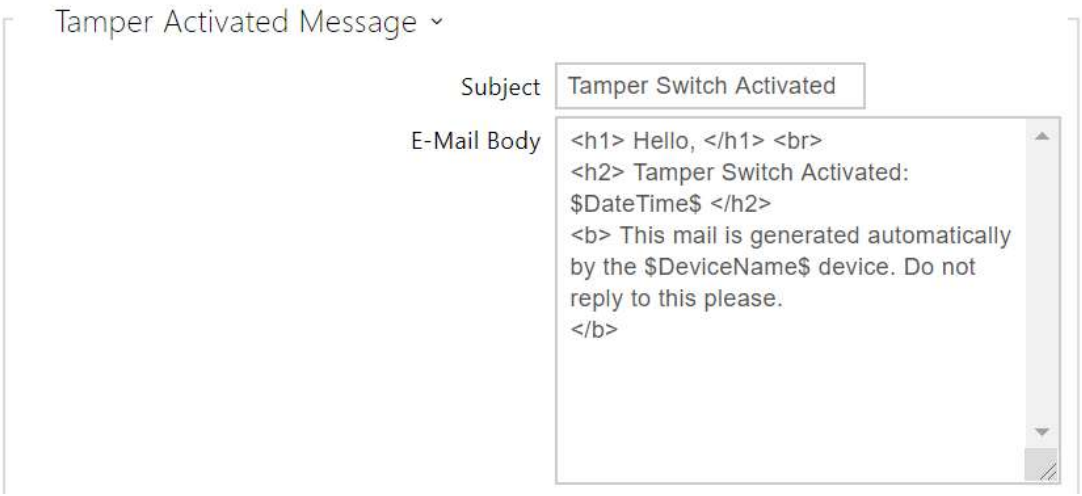
- **Subject** – set the e-mail subject to be sent.
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date & time and device ID. These symbols will be replaced with the actual value before sending. The list of placeholders found in the template is shown in the overview table at the end of this chapter.

E-Mail Body

```
<p>Hello,
</p>
<p>Device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) rebooted on <b>$DateTime$</b>
</p>
<ul>
  <li>Reason: <b>$RebootReason$</b>
  </li>
  <li>Uptime: <b>$UpTime$</b>
  </li>
  <li>Firmware version: <b>$SoftwareVersion$</b>
  </li>
  <li>Build date: <b>$BuildTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Caution

- If the placeholder value is not found in the string, the value is used directly.



Tamper Activated Message – set the message to be sent to the specified e-mail address whenever the tamper switch is activated.

- **Subject** – set the e-mail subject to be sent.
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date & time and device ID. These symbols will be replaced with the actual value before sending. The list of placeholders found in the template is shown in the overview table at the end of this chapter.

E-Mail Body

```
<p>Hello,
</p>
<p>Tamper switch of device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) was
activated on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Caution

- If the placeholder value is not found in the string, the value is used directly.

Caution

- The $DeviceName$ placeholder name is directly linked to the value of the Device name parameter in Services / Web Server / Basic Settings. We recommed that you use a name that defines the device uniquely.

List of Placeholders

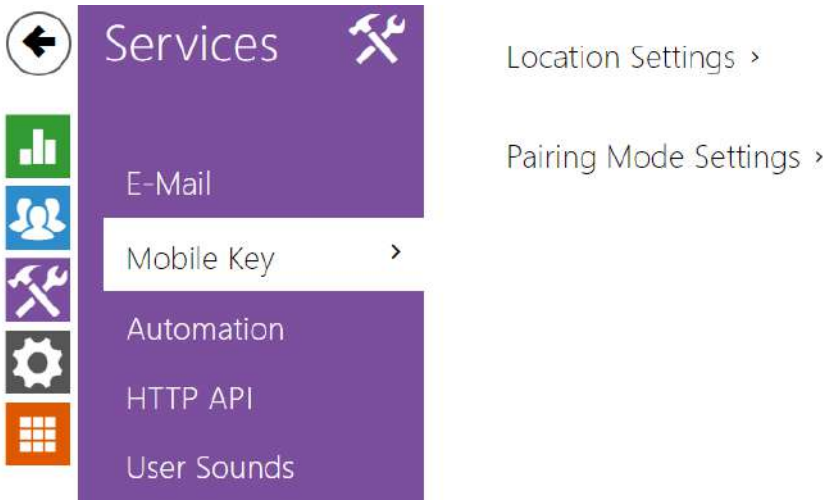
Occurrence	Placeholder	Description
Always available	$DateTime$	current date and time
	$DeviceName$	device name
	$Ip4Address$	device IP address
	$SoftwareVersion$	FW version
	$BuildTime$	build date and time
	$UpTime$	device uptime
Case dependent	$User$	username
	$RebootReason$	reboot reason
	$AuthId$	authentication ID
	$AuthIdDirection$	direction (entry/exit)
	$AuthIdType$	credential type
	$AuthIdValid$	in/valid
	$AuthIdReason$	reason of rejection

List of Placeholderrs in Events

Placeholder / Function	E-Mail on Access	E-mail on Device Rebooted	E-mail on Tamper Switch Activation	E-mail on Diagnostics Sending	Automation
$DateTime$	*	*	*	*	*

Placeholder / Function	E-Mail on Access	E-mail on Device Rebooted	E-mail on Tamper Switch Activation	E-mail on Diagnostics Sending	Automation
$DeviceName$	*	*	*	*	*
$Ip4Address$	*	*	*	*	*
$SoftwareVersion$	*	*	*	*	*
$BuildTime$	*	*	*	*	*
$UpTime$	*	*	*	*	*
$User$	*			*	*
$RebootReason$		*			
$DialNumber$				• (sends "E-Mail test")	CallStateChanged
$SipAccountNumber$					
$AuthId$	*				CardEntered, CardHeld
$AuthIdDirection$	*				CardEntered, CardHeld
$AuthIdType$	*				CardEntered, CardHeld
$AuthIdValid$	*				CardEntered, CardHeld
$AuthIdReason$	*				

5.4.3 Mobile Key



The **2N Access Unit** equipped with the Bluetooth module allow for user authentication via the **2N® Mobile Key** application available to devices with iOS 12 and higher (iPhone 4 s and higher phones) or Android 6.0 Marshmallow and higher (Bluetooth 4.0 Smart supporting phones).

User Identification (Auth ID)

The **2N® Mobile Key** application authenticates itself with a unique identifier on the **2N Access Unit** side: **Auth ID** (128-bit number) is generated randomly for every user and **paired** with the **2N Access Unit** user and its mobile device.

> **Note**
>
> - The generated Auth ID cannot be saved in more mobile devices than one. This means that Auth ID uniquely identifies just one mobile device or its user.

You can set and edit the Auth ID value for each user in the Mobile Key section of the **2N Access Unit** phone book. You can move Auth ID to another user or copy it to another intercom. By deleting the Auth ID value you can block the user's access.

Encryption Keys and Locations

The **2N® Mobile Key** – **2N Access Unit** communication is always encrypted. **2N® Mobile Key** cannot authenticate a user without knowing the encryption key. The primary encryption key is automatically generated upon the **2N Access Unit** first launch and can be re-generated

manually any time later. Together with AuthID, the primary encryption key is transmitted to the mobile device for pairing.

You can export/import the encryption keys and location identifier to other **2N Access Unit**. **2N Access Units** with identical location names and encryption keys form so-called **locations**. In one location, a mobile device is paired just once and identifies itself with one unique Auth ID (i.e. a user AuthID can be copied from one **2N Access Unit** to another within a location).

Pairing

Pairing means transmission of user access data to a user personal mobile device. The user access data can only be saved into one mobile device, i.e. a user cannot have two mobile devices for authentication, for example. However, the user access data can be saved into multiple locations in one mobile device (i.e. the mobile device is used as a key for more locations at the same time).

To pair a user with a mobile device, use the user's page in the **2N Access Unit** phone book. Physically, you can pair a user locally using the USB Bluetooth module connected to your PC or remotely using an integrated Bluetooth module. The results of both the pairing methods are the same.

The following data is transmitted to a mobile device for pairing:

- Location identifier
- Location encryption key
- User Auth ID

Encryption Key for Pairing

An encryption key other than that used for communication after pairing is used in the pairing mode for security reasons. This key is generated automatically upon the **2N Access Unit** first launch and can be re-generated any time later.

Encryption Key Administration

The **2N Access Unit** can keep up to 4 valid encryption keys: 1 primary and up to 3 secondary ones. A mobile device can use any of the 4 keys for communication encryption. The encryption keys are fully controlled by the system administrator. It is recommended that the encryption keys should be periodically updated for security reasons, especially in the event of a mobile device loss or intercom configuration leak.

Note

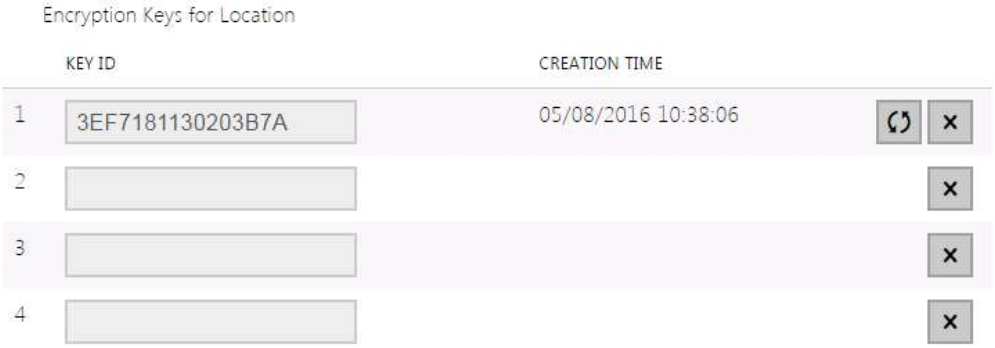
- The encryption keys are generated automatically upon the **2N Access Unit** first launch and saved into the **2N Access Unit** configuration file. We recommend you to re-generate the encryption keys manually before the first use to enhance security.

The primary key can be re-generated any time. Thus, the original primary key becomes the first secondary key, the first secondary key becomes the second secondary key and so on. Secondary keys can be deleted any time.

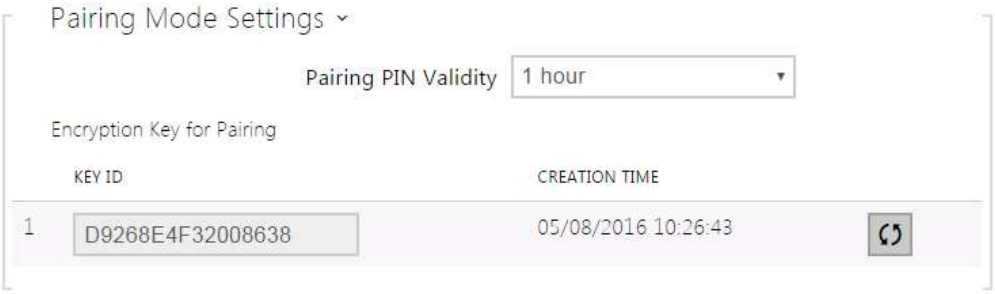
When a key is deleted, the **2N® Mobile Key** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **2N® Mobile Key** application.

List of Parameters

- **Location ID** – set a unique identifier for the location in which the selected encryption key set is valid.
- **Export** – push the button to export the location ID and current encryption keys into a file. Subsequently, the exported file can be imported to another device. Devices with identical location IDs and encryption keys form a so-called location.
- **Import** – push the button to import the location ID and current encryption keys from a file exported from another **2N Access Unit** . Devices with identical location IDs and encryption keys form a so-called location.



- **Restore primary key** – by generating a new primary encryption key you delete the oldest secondary key. Thus, the **2N® Mobile Key** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **2N® Mobile Key** application.
- **Delete primary key** – delete the primary key to prevent the users that still use this key from authentication.
- **Delete secondary key** – the **2N® Mobile Key** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **2N® Mobile Key** application.



- **Pairing PIN validity** – set the authorisation PIN validity for user mobile device pairing with the **2N Access Unit** .

Tip

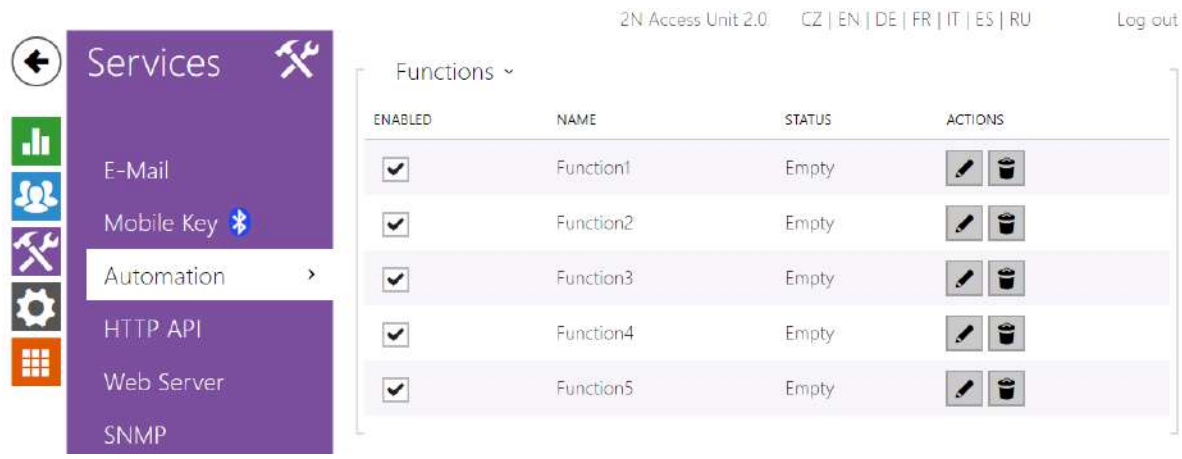
- In the case of loss of a mobile phone with access data proceed as follows:

1. Delete the Mobile Key Auth ID value for the user to block the lost phone and avoid misuse.
2. Re-generate the primary encryption key (optionally) to avoid misuse of the encryption key stored in the mobile device.

Warnung

- With the upgrade to version 2.30, the bluetooth modules will also be upgraded. When downgrading to version 2.29 and lower, they may malfunction.

5.4.4 Automation



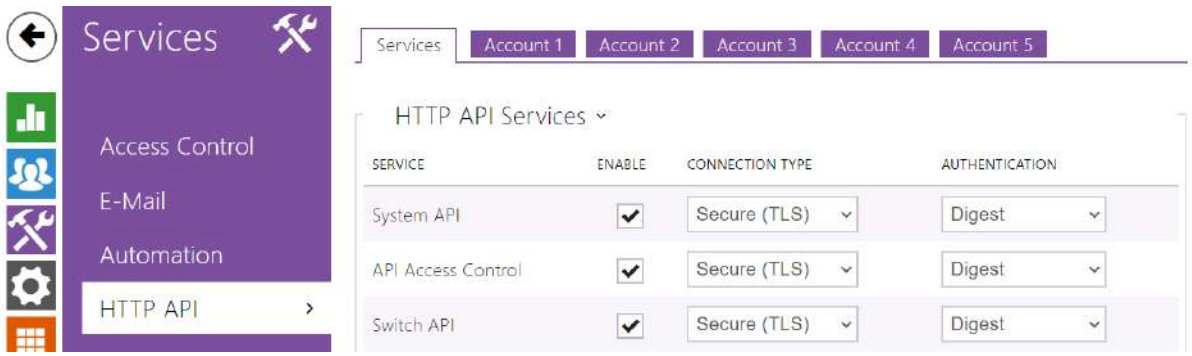
The **2N Access Unit** provides highly flexible setting options to satisfy variable user needs. There are situations in which the standard configuration settings (switch or call modes, e.g.) are insufficient and so **2N Access Unit** offers a special programmable interface, **2N Automation**. Typically, **2N Automation** is used in applications that require complex interconnections with third party systems.

Refer to the **2N Automation** Configuration Manual for the 2N IP Automation function and configuration details.

> **Note**
>
> - *The Automation function is available with the Gold or Enhanced Integration license only.*

5.4.5 HTTP API

HTTP API is an application interface designed for control of selected **2N IP Access Unit** functions via the **HTTP**. It enables **2N Access Units** to be integrated easily with third party products, such as home automation, security and monitoring systems, etc.



Services

HTTP API provides the following services:

- **System API** – provides 2N Access Unit configuration changes, status info and upgrade.
- **API Access Control** – provides access control and user authentication verification methods.
- **Switch API** – provides switch status control and monitoring, e.g. door lock opening, etc.
- **I/O API** – provides 2N Access Unit logic input/output control and monitoring.
- **Display API** – provides display control and user information display.
- **E-mail API** – provides sending of user e-mails.
- **Logging API** – provides reading of event records.
- **Automation API** – provides Secure/Unsecure communication settings and authorization requirements.

Set the transport protocol (**HTTP** or **HTTPS**) and way of authentication (**None**, **Basic** or **Digest**) for each function. Create up to five user accounts (with own username and password) in the **HTTP API** configuration for detailed access control of services and functions.3

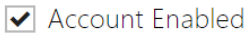
Set authentication methods for the requests to be sent to the 2N Access Unit for each service. If the required authentication is not executed, the request will be rejected. Requests are authenticated via a standard authentication protocol described in **RFC-2617**. The following three authentication methods are available:

- **None** – no authentication is required. In this case, this service is completely unsecure in the **LAN**.
- **Basic** – Basic authentication is required according to **RFC-2617**. In this case, the service is protected with a password transmitted in an open format. Thus, we recommend you to combine this option with **HTTPS** where possible.
- **Digest** – Digest authentication is required according to **RFC-2617**. This is the default and most secure option of the three above listed methods.

Refer to the 2N HTTP API Configuration Manual for the HTTP API function and configuration details.

Account 1–5

The **2N Access Unit** allows you to manage up to five user accounts for access to the **HTTP API** services. The user account includes the user name and password and a list of user privileges to **HTTP API**.

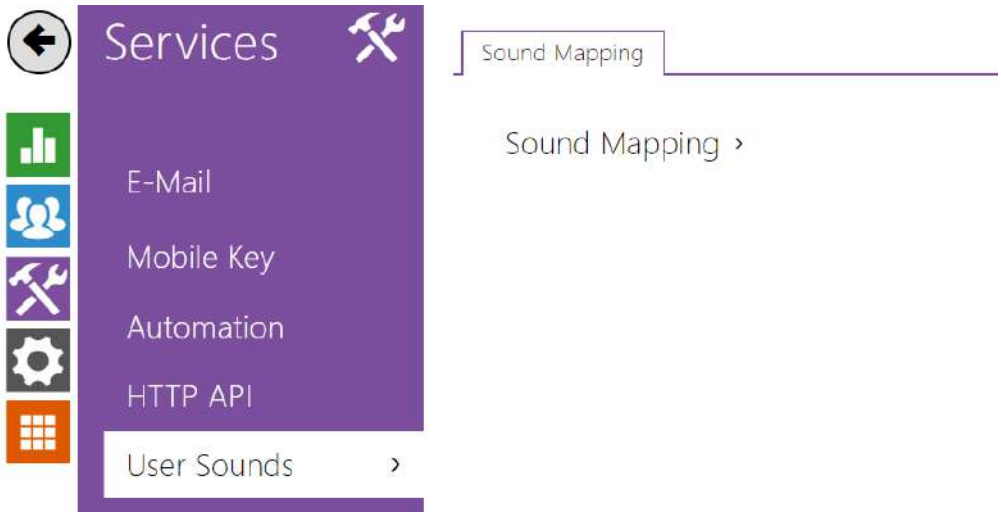


- **Account Enabled** – enable this user account.

- **Username** – enter the username fot the HTTP authentication.
- **Password** – enter the HTTP API authentication password.

You can manage the user account priviliges to the services via the table above.

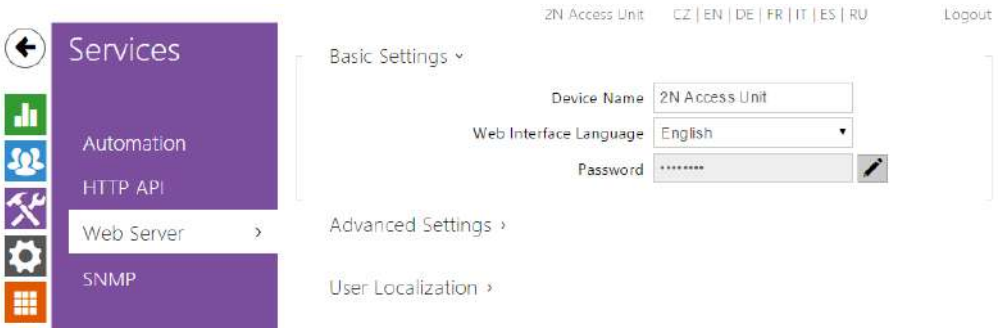
5.4.6 User Sounds



User Sounds helps you set or mute the acoustic signalling of the activated **2N Access Unit** switch. For acoustic signalling for authentication refer to 5.3.1 Door.

- **Switch 1 Activation Signaling** – set the sound to be generated when a switch 1 is activated.
- **Switch 2 Activation Signaling** – set the sound to be generated when a switch 2 is activated.

5.4.7 Web Server



You can configure your **2N Access Unit** using a standard browser with access to the integrated web server. Use the secured HTTPS protocol for communication between the browser and **2N Access Unit**. Having accessed the intercom, enter the login name and password. The default login name and password are **admin** a **2n** respectively. We recommend you to change the default password as soon as possible.

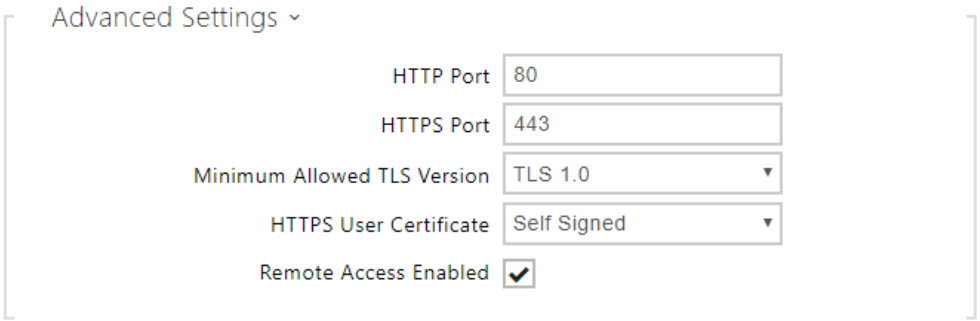
The Web Server function is used by the following **2N Access Unit** functions too:

1. HTTP commands for switch control, refer to the Switches subsection.
2. Event.HttpTrigger in **2N Automation**; refer to the respective manual.

The unsecured HTTP protocol can be used for these special communication cases.

List of Parameters

- **Device Name**– set the device name to be displayed in the right upper corner of the web interface, login window and other applications if available (**2N® IP Manager**, **2N® IP Network Scanner**, etc).
- **Web Interface Language** – set the default language for administration web server login. Use the upper toolbar buttons to change the language temporarily.
- **Password** – set the intercom access password. Press  to change the password. The 8-character password must include one lower-case letter, one upper-case letter and one digit at least.



- **HTTP port** – set the web server port for HTTP communication. The port setting will not be applied until the intercom gets restarted.
- **HTTPS port** – set the web server port for HTTPS communication. The port setting will not be applied until the intercom gets restarted.
- **Minimum Allowed TLS Version** – define the lowest TLS version to be connected to the devices.
- **HTTPS user certificate** – specify the user certificate and private key for the intercom HTTP server – user web browser communication encryption. Choose one of the three sets of user certificates and private keys (refer to the Certificates subsection) or keep the **SelfSigned** setting, in which the certificate automatically generated upon the first intercom power up is used.
- **Remote access enabled** – enable remote access to the intercom web server from off-LAN IP addresses.

- **Original Language** – download the original file containing all the user interface texts in English. The file format is XML; see below.
- **User Language** – record, load and remove, if necessary, a user file containing your own user interface text translations.

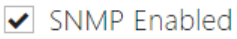
```
<?xml version="1.0" encoding="UTF-8"?>
<strings language="English" languageshort="EN">
  <!-- Global enums-->
  <s id="enum/error/1">Invalid value!</s>
  <s id="enum/bool_yesno/0">NO</s>
  <s id="enum/bool_yesno/1">YES</s>
  <s id="enum/bool_user_state/0">ACTIVE</s>
  <s id="enum/bool_user_state/1">INACTIVE</s>
  <s id="enum/bool_profile_state/0">ACTIVE</s>
  <s id="enum/bool_profile_state/1">INACTIVE</s>
  ..
  ..
  ..
</strings>
```

While translating, modify the value of **<s>** elements only. Do not modify the **id** values. The language name specified by the **language** attribute of the **<strings>** element will be available in the selections of the Web interface language parameter. The abbreviation of the language name specified by the **languageshort** attribute of the **<strings>** element will be included in the language list in the right-hand upper corner of the window and will be used for a quick language switching.

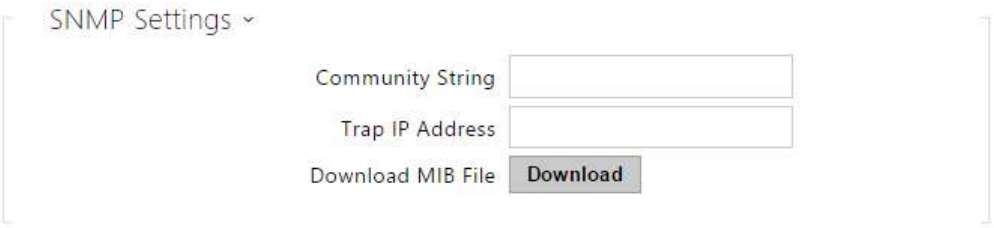
5.4.8 SNMP

The **2N Access Unit** access systems integrate a remote intercom supervision functionality via the SNMP. The **2N Access Unit** systems support the SNMP version 2c.

List of Parameters

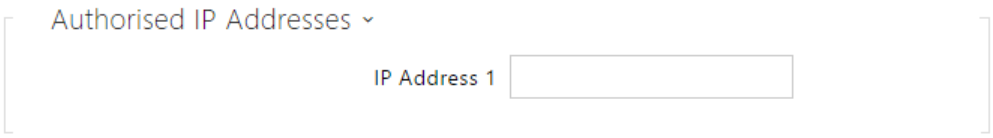


- **SNMP Enabled** – enable the SNMP function.



- **Community String** – text string representing the access key to the MIB table objects.
- **Trap IP Address** – IP address to which the SNMP traps are to be sent.
- **Download MIB File** – download the current MIB definition from a device.

- **Contact** – enter the device manager contact (name, e-mail, etc.).
- **Name** – enter the device name.
- **Location** – enter the device location (1st floor, e.g.).

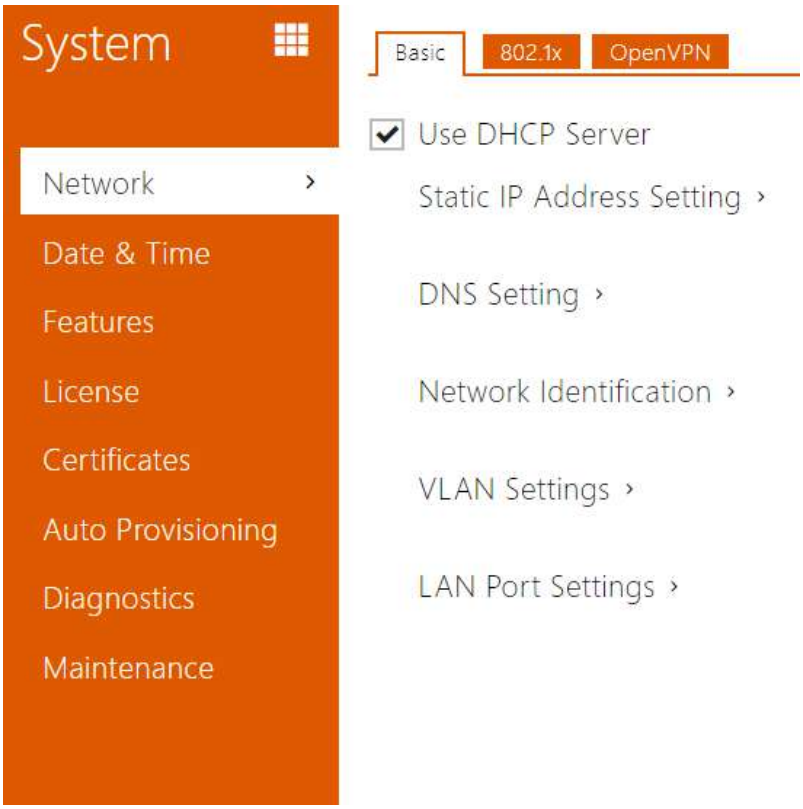


- **IP Address** – enter up to 4 valid IP addresses for SNMP agent access to block access from other addresses. If the field is empty, the device may be accessed from any IP address.

5.5 System

Here is what you can find in this section:

5.5.1 Network



As the **2N Access Unit** is connected to the LAN, make sure that its IP address has been set correctly or obtained from the LAN DHCP server. Configure the IP address and DHCP in the Network subsection.

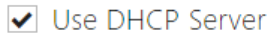
Tip

- *To know the current IP address of your **2N Access Unit**, use the **2N IP Network Scanner**, which can be freely downloaded from www.2n.com, or apply the steps described in the Installation Manual of the respective **2N Access Unit**: the **2N Access Unit** communicates its IP address to you via a voice function.*

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

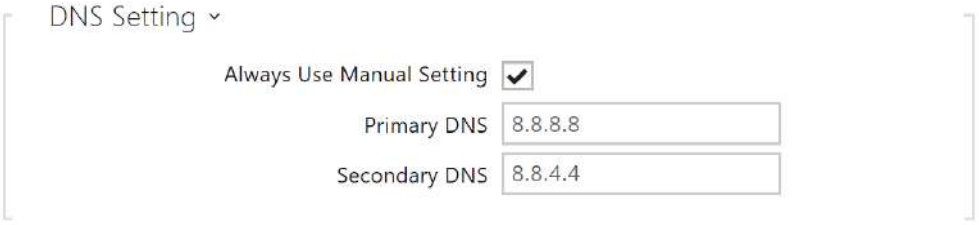
The Trace tab helps you launch capture of incoming and outgoing packets on the **2N Access Unit** network interface. The file with captured packets can be downloaded for Wireshark processing, e.g. (www.wireshark.org).

List of Parameters



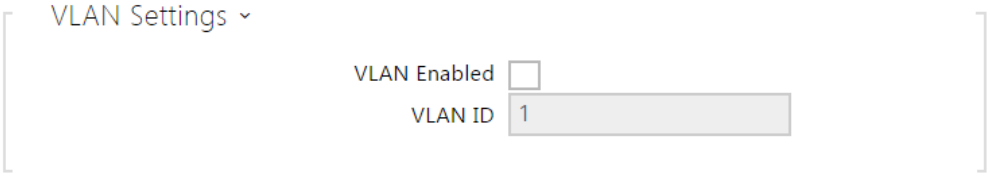
- **Use DHCP Server** – enable automatic obtaining of the IP address from the LAN DHCP server. If the DHCP server is unavailable or inaccessible in your LAN, use the manual network settings.

- **Static IP Address** – display the static IP address of the **2N Access Unit**, which is used together with the below mentioned parameters if the Use DHCP Server parameter is disabled.
- **Network Mask** – set the network mask.
- **Default Gateway** – set the address of the default gateway, which provides communication with off-LAN equipment.

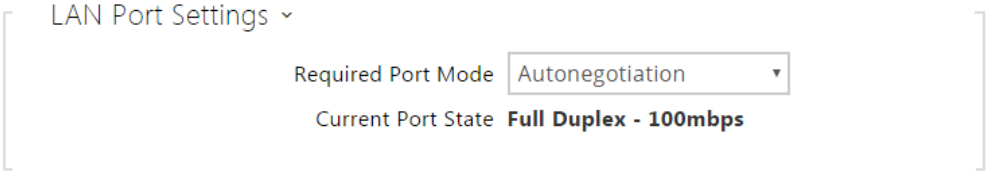


- **Primary DNS** – set the primary DNS server address for translation of domain names to IP addresses. The primary DNS value is 8.8.8.8 upon factory reset.
- **Secondary DNS** – set the secondary DNS server address, which is used in case the primary DNS is inaccessible. The secondary DNS value is 8.8.4.4 upon factory reset.

- **Hostname** – set the 2N IP intercom network identification.
- **Vendor Class Identifier** – set the vendor class identifier as a string of characters for DHCP Option 60.



- **VLAN Enabled** – enable the virtual network (VLAN) support (according to recommendation 802.1q). Set the virtual network ID too to make the function work properly.
- **VLAN ID** – select a virtual network ID in the range of 1-4094. The device shall receive only the packets tagged with this ID. A wrong setting may result in a connection loss and need to reset the device to factory values.



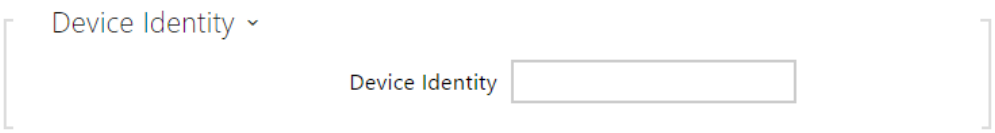
- **Required Port Mode** – set the preferred network interface port mode: Autonegotiation or Half Duplex – 10 mbps. The lower bit rate of 10 mbps may be necessary if the used network infrastructure (cabling) is not reliable for the 100mbps traffic.
- **Current Port State** – current network interface port state (Half or Full Duplex – 10 mbps or 100 mbps).

802.1x

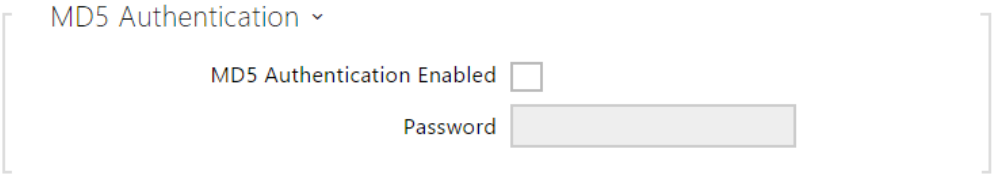
Caution

- The authentication setting changes will not apply until the device is restarted.

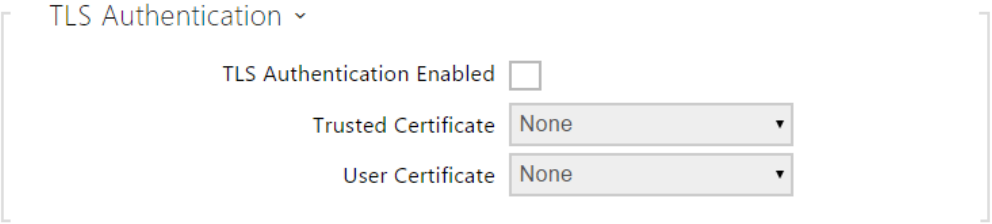
The tab is not displayed for 2N Access Unit 2.0, which does not support the 802.1x protocol.



- **Device Identity** – set the user name (identity) for authentication via EAP-MD5 and EAP-TLS.

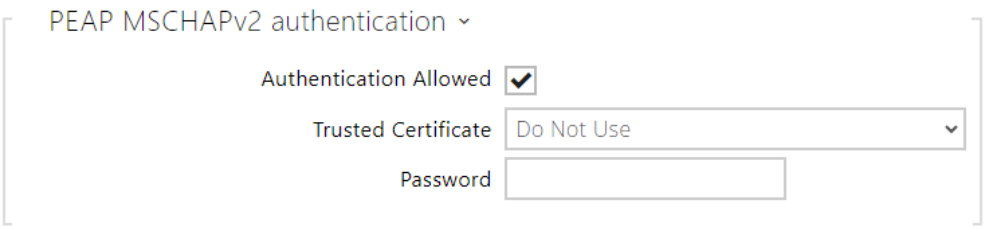


- **MD5 Authentication Enabled** – enable authentication of network devices via the 802.1x EAP-MD5 protocol. Do not enable this function if your LAN does not support 802.1x. If you do so, the **2N Access Unit** will become inaccessible.
- **Password** – enter the access password for EAP-MD5 authentication.



- **TLS Authentication Enabled** – enable authentication of network devices via the 802.1x EAP-TLS protocol. Do not enable this function if your LAN does not support 802.1x. If you do so, the **2N Access Unit** will become inaccessible.
- **Trusted Certificate** – specify the set of trusted certificates for verification of the RADIUS server public certificate validity. Choose one of three sets of certificates; refer to the Certificates subsection. If no trusted certificate is included, the RADIUS public certificate is not verified.

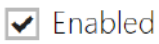
- **User Certificate** – specify the user certificate and private key for verification of the **2N Access Unit** authorisation to communicate via the 802.1x-secured network element port in the LAN. Choose one of three sets of user certificates and private keys; refer to the Certificates subsection.



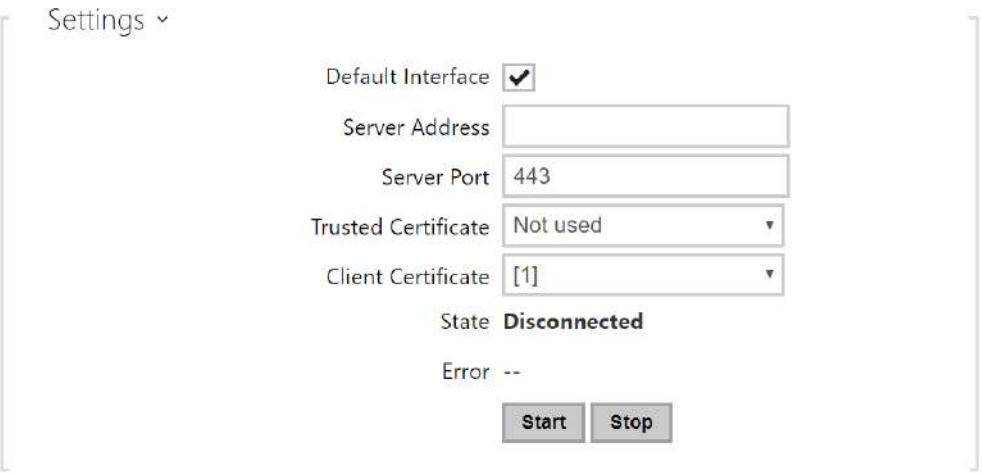
- **Authentication Allowed** – enable authentication of network devices via the 802.1x PEAP MSCHAPv2 protocol. Do not enable this function if your LAN does not support 802.1x. If you do so, the device will become inaccessible.
- **Trusted Certificate** – specify the CA certificate for verifying the RADIUS server public certificate validity. If none is available, the RADIUS server public certificate is not validated.
- **Password** – enter the access password for PEAP-MSCHAPv2 authentication.

OpenVPN

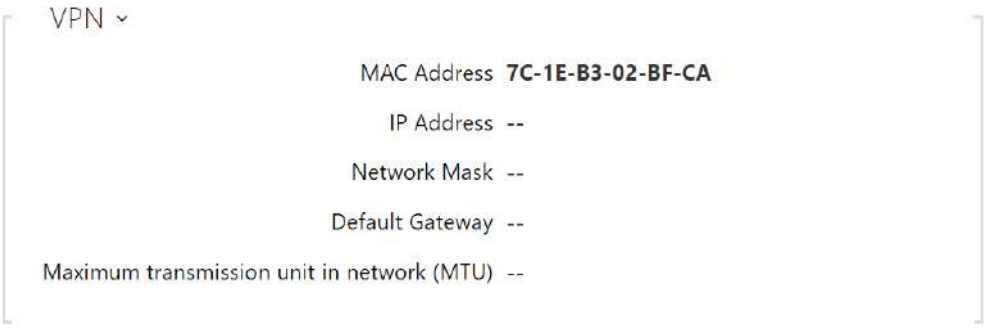
Use OpenVPN to connect the device to another network.



- **Enabled** – enables the virtual private network (VPN).



- **Default Interface** – if enabled, it directs all outgoing network traffic to the VPN interface outside the LAN mask.
- **Server Address** – OpenVPN Server Address
- **Server Port** – OpenVPN Server Port.
- **Trusted Certificate** – specify a set of certificates issued by certification authorities to verify the OpenVPN server public certificate validity. Choose one of three certificate sets, see the Certificates subsection. If no certificate issued by a certification authority is specified, the OpenVPN server public certificate is not validated.
- **Client Certificate** – specify a set of client certificates to verify the client's identity by the OpenVPN server. Choose one of three certificate sets, see the Certificates subsection. If no client certificate is specified, the OpenVPN client identity is not validated.
- **State** – display the OpenVPN connection state: Connected/Disconnected.
- **Error** – display the OpenVPN connection error type if any.
- **Start** – connect the device to OpenVPN.
- **Stop** – disconnect the device from OpenVPN.

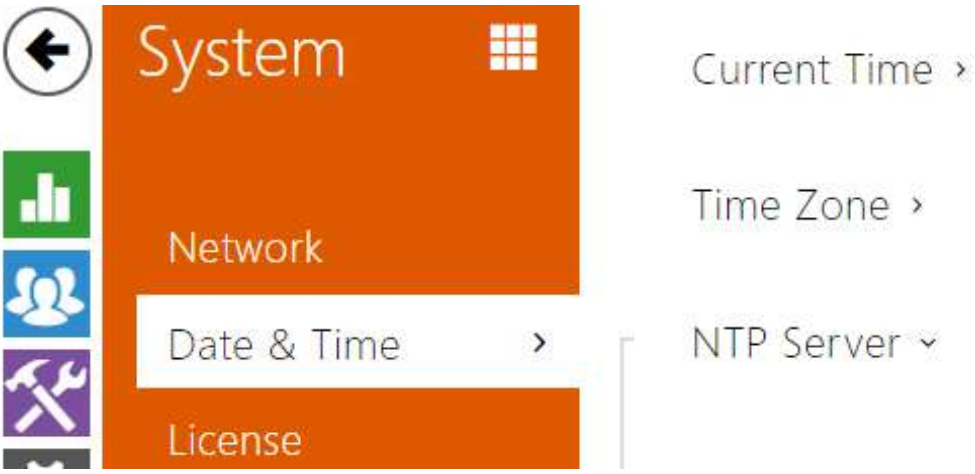


- **VPN** – display the basic information on VPN.

Tip

- Refer to FAQ for OpenVPN server and client setting details.

5.5.2 Date and Time



If you control validity of lock activation codes and similar by time profiles, make sure that the **2N Access Unit** internal date and time are set correctly.

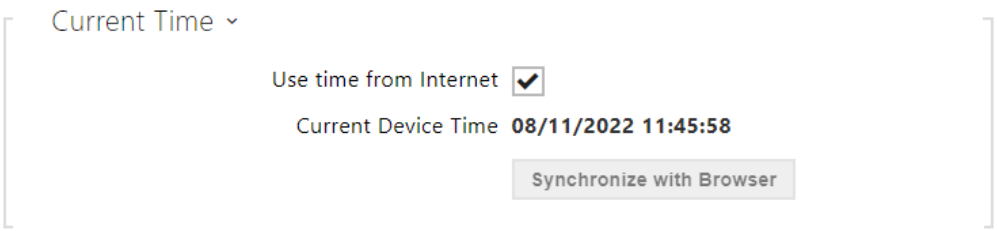
2N Access Unit is equipped with a back-up real-time clock to withstand up to several days' long power outages. Select **Use time from Internet** to synchronize **2N Access Unit** time with the internet time or click **Synchronize with browser** to synchronize the intercom time with your current PC time.

Note

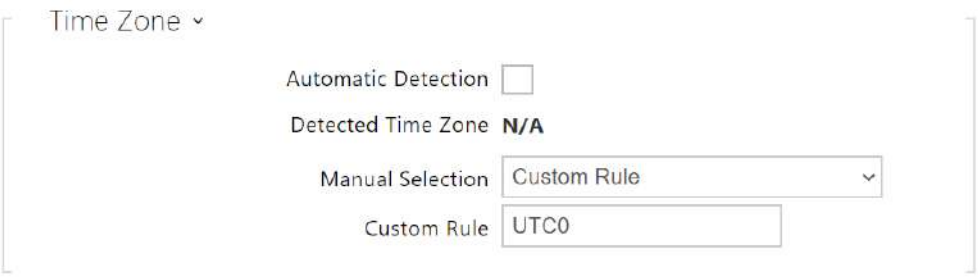
- *The **2N Access Unit** does not need the current date and time values for its basic function. However, be sure to set these values when you apply time profiles and display time of listed events (Syslog, used cards, logs downloaded by **2N IP intercom** HTTP API, etc.).*

Practically, the **2N Access Unit** real-time circuit accuracy is approximately ±0,005 %, which may mean a deviation of ±2 minutes per month. To maximize the accuracy and reliability, we recommend that you always enable the **Use time from Internet** function.

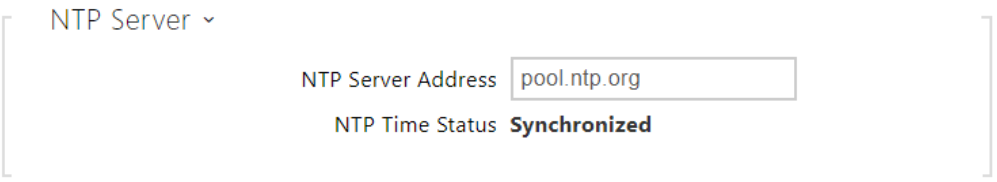
List of Parameters



- **Use time from Internet** – Enable the NTP server use for device time synchronization.
- **Synchronise with browser** – push the button to synchronise the **2N Access Unit** time value with your PC time value.

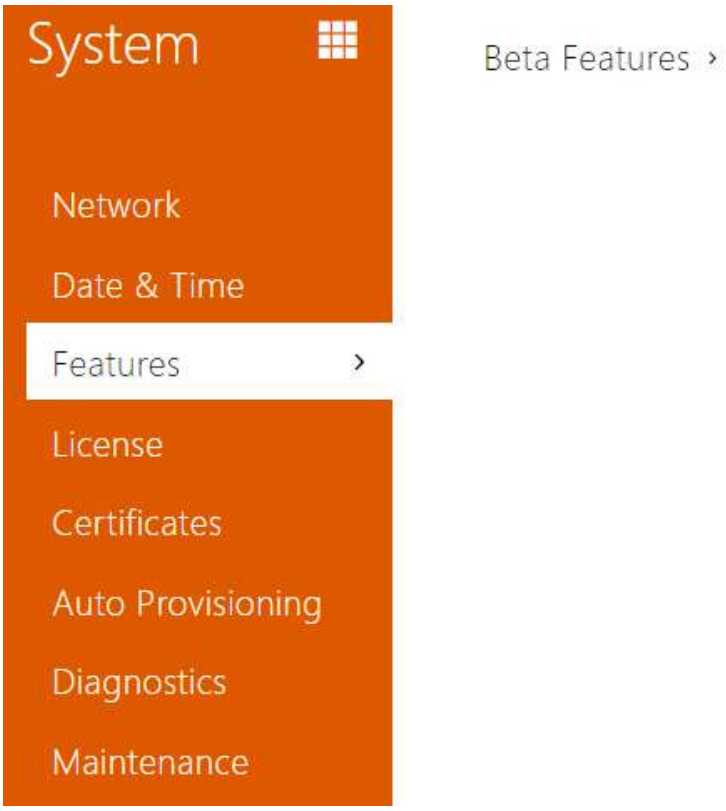


- **Automatic Detection** – define whether the time zone shall be detected automatically from My2N. In case automatic detection is disabled, the Manual selection parameter is Used (manually selected time zone or Own rule).
- **Detected Time Zone** – display the automatically found time zone. In case the function is unavailable or disabled, N/A is displayed.
- **Manual Selection** – set the installation site time zone. Set the time shift and summer/ winter time transitions.
- **Custom Rule** – if the device is installed on a site that it not included in the Time Zone parameter, set the time zone rule manually. The rule is applied only if the Time Zone parameter is set to Manual.



- **Use NTP Server** – enable the NTP server use for **2N Access Unit** time synchronization. The server IP address and domain name cannot be set if **Use time from Internet** is disabled.
- **NTP Server Address** – set the IP address/domain name of the NTP server used for your **2N Access Unit** time synchronisation.

5.5.3 Features



A list of public beta functions designed for user testing is shown here.
The list includes:

- function name,
- function status: started or stopped,
- event allowing to start/stop the function.

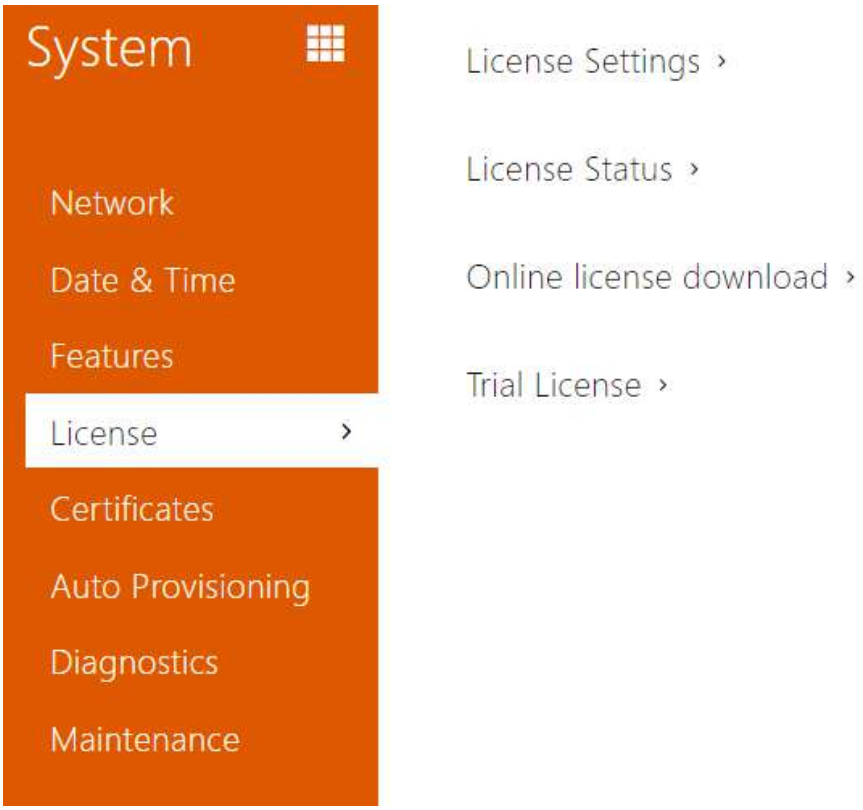
The function does not start/stop until the device is restarted. Hence, the status change request can be canceled by **Interrupt** until the restart.

Note

- There is no warranty on the testing functions and 2N TELEKOMUNIKACE a.s. shall not be held liable for any functional limitations and damage incurred as a result of functional limitations of the beta functions. The beta functions are provided for testing purposes exclusively.

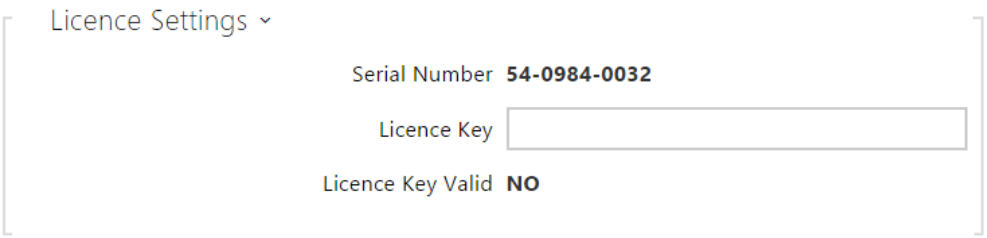
Beta Function Name	Description
Password-Protected Configuration File	This function helps you encrypt the configuration file with a password during backup (refer to 5.5.8 Maintenance). To upload the configuration file to the device, you need to enter a security password. If the password fails to match, the configuration file will not be uploaded.
Multifactor Authentication of License Plates	Once this function is activated, the Multifactor selection appears in Services > Access Control > Arrival Rules > Advanced Settings > License Plate Recognition. Access is only granted when at least two authentication methods are verified as set in the access rules. Once the license plate is recognized, remember to enter another authentication method within 60 seconds.

5.5.4 Licence



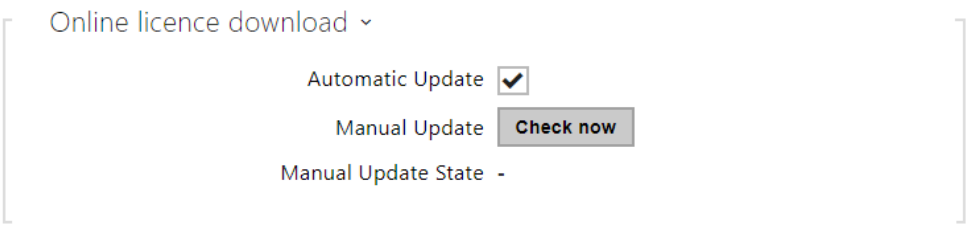
Some **2N Access Unit** functions are available with a valid licence key only. Refer to the **Function Licensing** subsection for the list of **2N Access Unit** licensing options.

List of Parameters



- **Serial Number** – display the serial number of the device for which the licence is valid.
- **Licence Key** – enter the valid licence key.
- **Licence Key Valid** – check whether the used licence key is valid.

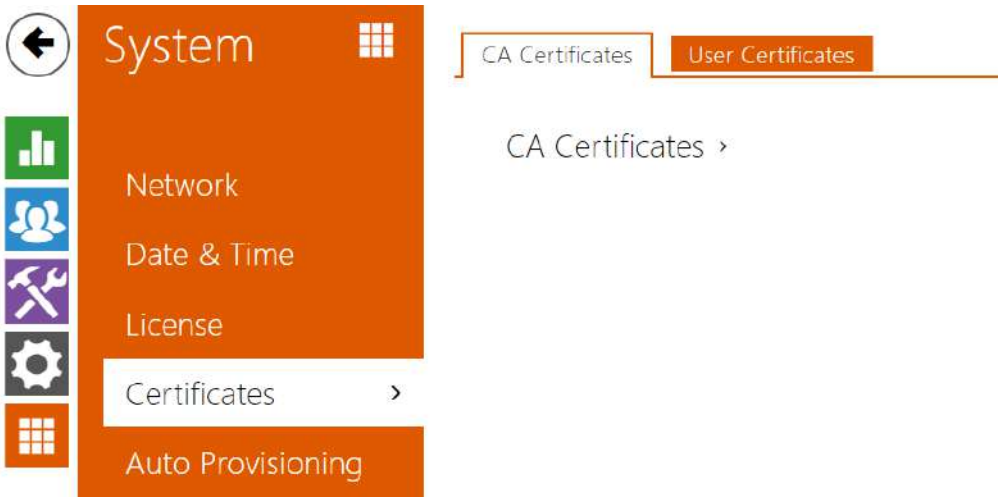
- **Standard Licenses** – display the list of factory default licenses.
  - **Enhanced Security** – check whether the functions activated by the Enhanced Security licence are available.
  - **NFC Support** – check whether the functions activated.
  - **Enhanced Intergration** – check whether the functions activated by the Enhanced Integration licence are available.
  - **Lift Control Support** – check whether the functions activated by the Lift Module license are available.



- **Automatic update** – enable automatic license key update from the 2N License server.
- **Manual update** – manual license availability check request.
- **Manual update state** – running, updated, unspecified, failed: license is not available.

- **Trial Licence State** – check the trial licence state (Non-Activated, Activated, Expired).
- **Licence Expiry** – display the remaining time of the trial licence validity.

5.5.5 Certificates



Some **2N Access Unit** network services use the Transaction Layer Security (TLS) protocol for communication with other LAN devices to prevent third parties from monitoring and/or modifying the communication contents. Unilateral or bilateral authentication based on certificates and private keys is needed for establishing connections via TLS.

The following **2N Access Unit** services use the TLS protocol:

a. Web server (HTTPS)
b. E-mail (SMTP)
c. 802.1x (EAP-TLS)
d. SIPs

Sets of CA certificates can be uploaded to the **2N Access Unit**, which are used for identity verification of the device that the intercom is communicating with, and also of User certificates and private keys for communication encryption

Each certificate-requiring service can be assigned one of the three certificate sets available; refer to the **Web Server**, **E-Mail** and **Streaming** subsections. The certificates can be shared by the services.

- **2N Access Unit** accepts the DER (ASN1) and PEM certificate formats.
- **2N Access Unit** supports the AES, DES and 3DES encryption.
- **2N Access Unit** supports the following algorithms:
  - RSA up to 2048bit user certificate keys; internally up to 4096bit keys (during connection – temporary and equivalence certificates)
  - Elliptic Curves

Caution

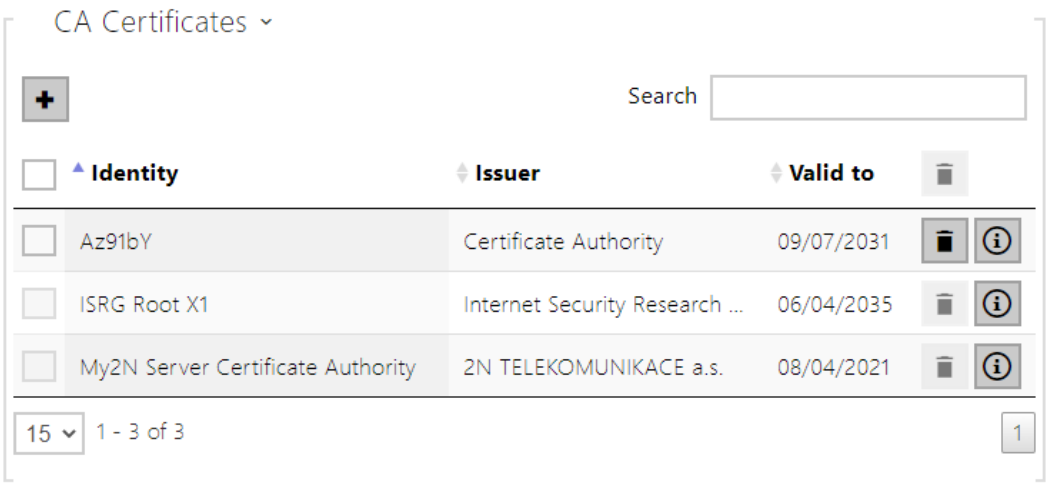
- The CA certificates must use the X.509 v3 format.

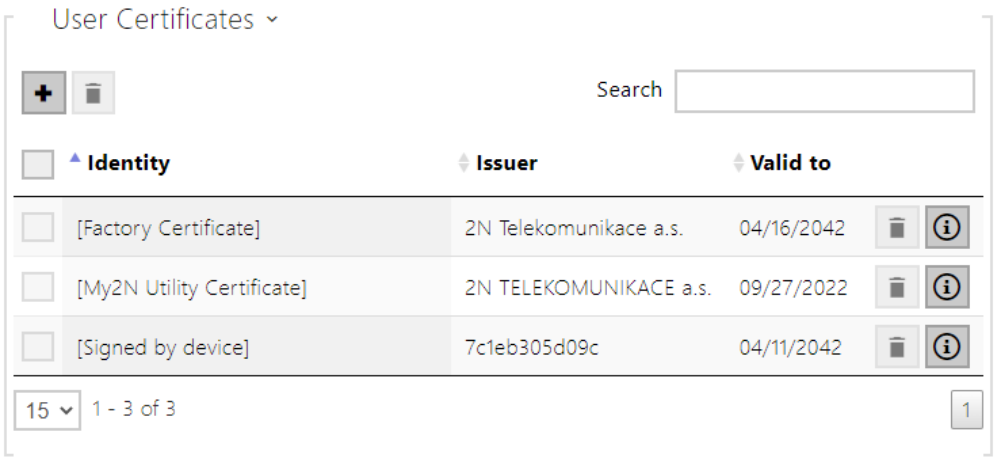
Upon the first power up, the **2N Access Unit** automatically generates the **Self Signed certificate** and **private key** for the **Web server** and **E-mail** services without forcing you to load a certificate and private key of your own.

Note

- *If you use the Self Signed certificate for encryption of the intercom web server – browser communication, the communication is secure, but the browser will warn you that it is unable to verify the **2N Access Unit** certificate validity.*

The current overview of CA and User certificate uploads is shown in the following two folders:





Press  to upload a certificate saved on your PC. Complete the certificate ID in the dialogue box to select, edit or delete the certificate. Make sure that the ID is not longer than 40 characters and contains small and capital letters, digits and the '_' and '-' characters. The ID is not mandatory. Select the certificate (or private key) file in the dialogue box and push **Load**. Click  to remove the certificate from the device. Press  to show the certificate information.

Caution

- The device changes the **Self signed certificate** into a new one after firmware update or restart. Check and compare the certificate displayed on the device with the web certificate for a match.

Caution

- For certificates based on elliptic curves use the secp256r1 (aka prime256v1 aka NIST P-256) and secp384r1 (aka NIST P-384) curves only.

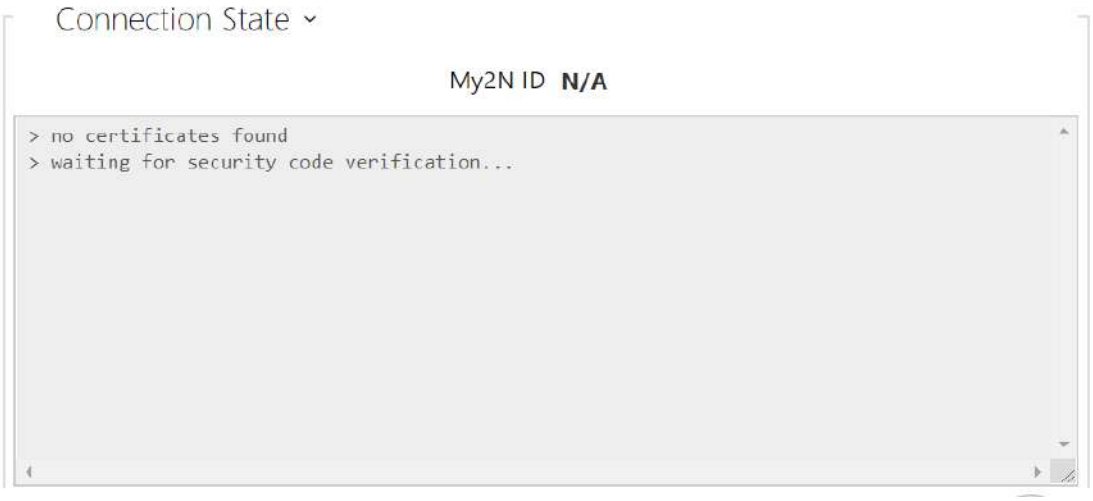
5.5.6 Auto Provisioning

The **2N Access Unit** allows you to update firmware and configuration manually or automatically from a storage on a TFTP/HTTP server selected by you according to predefined rules.

You can configure the TFTP and HTTP server address manually. The **2N Access Unit** supports automatic address identification via the local DHCP server (Option 66).

My2N

- **Serial Number** – display the serial number of the device to which the valid My2N code applies.
- **My2N Security Code** – display the full application activating code.
- **GENERATE NEW** – the active My2N Security Code will be invalidated and a new one will be generated.



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

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

Firmware

Use the Firmware tab to set automatic firmware download from a server defined by you. The **2N Access Unit** compares the server file with its current firmware file periodically and, if the server file is more recent, automatically updates firmware and gets restarted (approx. 30 s). Hence, we recommend you to update when the **2N Access Unit** traffic is very low (at night, e.g.).

The **2N Access Unit** expects the following files:

1. **MODEL**-firmware.bin – **2N Access Unit** firmware
2. **MODEL**-common.xml – common configuration for all **2N Access Unit**
3. **MODEL**-**MACADDR**.xml –specific configuration for one **2N Access Unit**

MODEL in the filename specifies the intercom model:

1. **au – 2N Access Unit**
2. **aug2 – 2N Access Unit 2.0**
3. **aum – 2N Access Unit M**

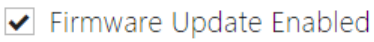
MACADDR is the MAC address of the **2N Access Unit** in the 00-00-00-00-00-00 format. Find the MAC address on the **2N Access Unit** production plate or on the **Status** tab in the web interface.

Example:

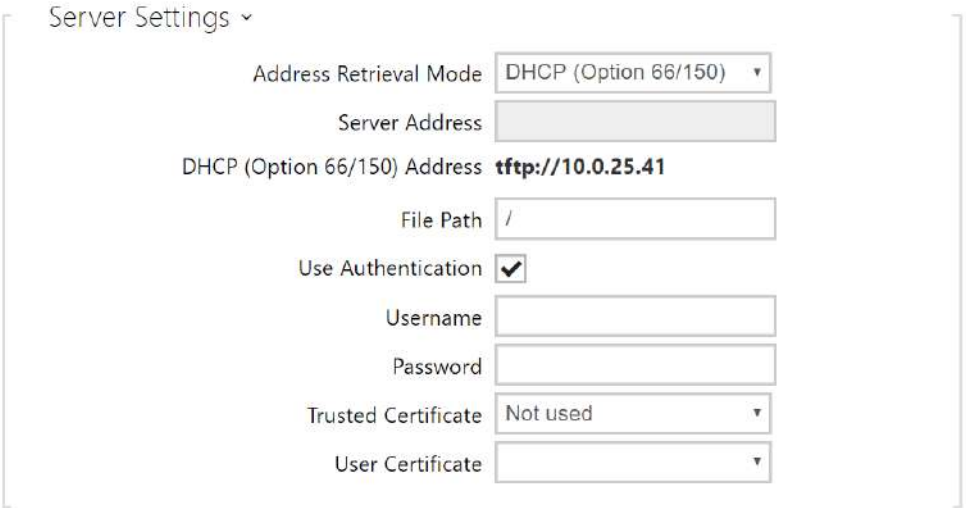
2N Access Unit with MAC address 00-87-12-AA-00-11 downloads the following files from the TFTP server:

- au-firmware.bin
- au-common.xml
- au-00-87-12-aa-00-11.xml

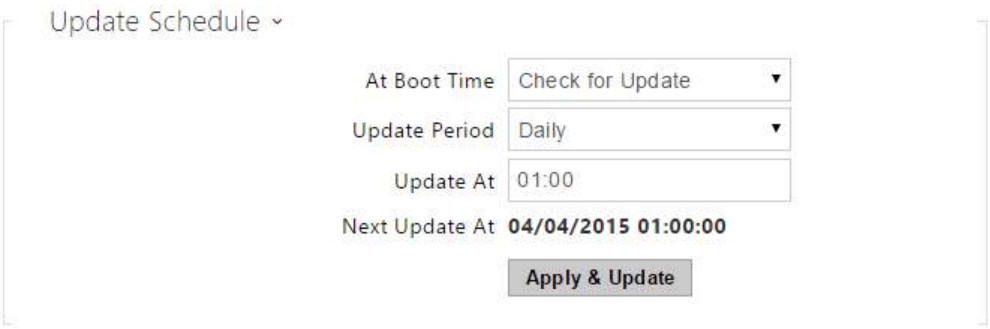
List of Parameters



- **Firmware/Configuration Update Enabled** – enable automatic firmware/configuration updating from the TFTP/HTTP server.



- **Address Retrieval Mode** – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 shall be used.
- **Server Address** – enter the TFTP (tftp://ip_address), HTTP (http://ip_address) or HTTPS (https://ip_address) server address manually.
- **DHCP (Option 66/150) Address** – check the server address retrieved via the DHCP Option 66 or 150.
- **File Path** – set the firmware/configuration filename directory or prefix on the server. The intercom expects the XhipY_firmware.bin, XhipY-common.xml and XhipY-MACADDR.xml files, where X is the prefix specified herein and Y specifies the intercom model.
- **Use Authentication** – enable authentication for HTTP server access.
- **Username** – enter the user name for server authentication.
- **Password** – enter the password for server authentication.
- **Trusted Certificate** – set the set of CA certificates for validation of the ACS public certificate.
- **User Certificate** – specify the user certificate and private key to validate the intercom right to communicate with the ACS.



- **At Boot Time** – enable check and/or execution of update upon every **2N Access Unit** start.
- **Update Period** – set the update period. Set an automatic update to take place hourly/daily/weekly/monthly, or set the period manually.
- **Update At** – set the update time in the HH:MM format for periodical updating at a low-traffic time. The parameter is not applied if the update period is set to a value shorter than 1 day.
- **Next Update At** – display the next update time.

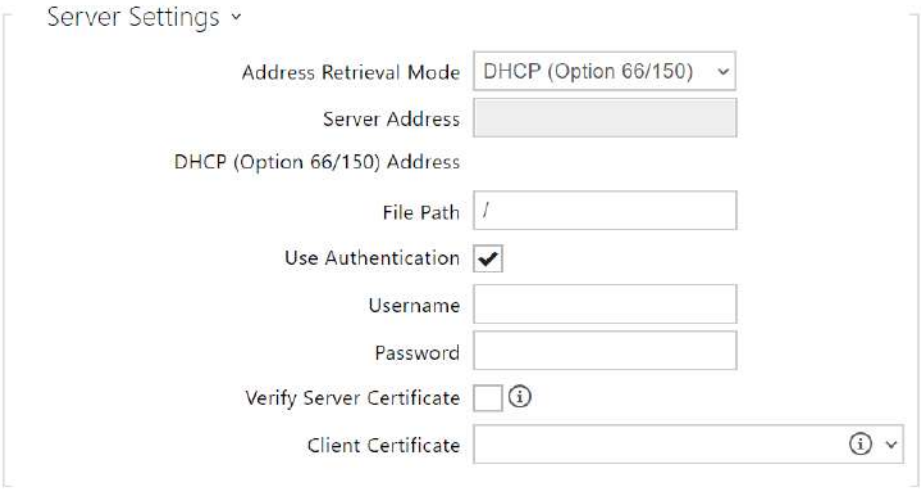
- **Last Update At** – last update time.
- **Update Result** – last update result. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail** – server communication error code or TFTP/HTTP status code.

Result	Description
In progress ...	Update in progress
Updated	The configuration/firmware update has been successful. With firmware update, the device will be restarted in a few seconds.
Firmware is up to date.	The firmware update attempt reveals that the latest firmware version has been loaded.
DHCP Option 66 has failed.	The server address loading via DHCP Option 66 or 150 has failed.
Invalid domain name	The server domain name is invalid due to wrong configuration or unavailability of the DNS server.
Server Not Found	The requested HTTP/TFTP server fails to reply.
Download failed	An unspecified error occurred during file download.
File not found	The file has not been found on the server.
File invalid	The file to be downloaded is corrupted or of a wrong type.

Configuration

Use the Configuration tab to set automatic configuration download from the server defined by you. The **2N Access Unit** periodically downloads a file from the server and gets reconfigured without getting restarted.

- **Firmware update enabled** – enable automatic firmware/configuration updating from the TFTP/HTTP server.

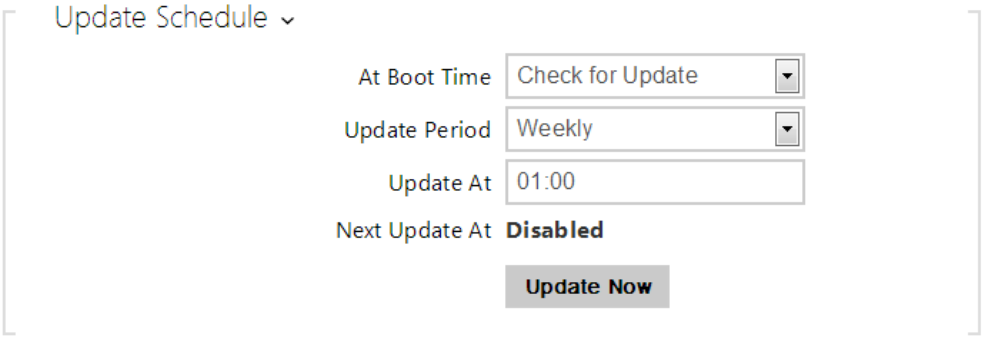


- **Address Retrieval Mode** – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 shall be used.
- **Server Address** – enter the TFTP (tftp://ip_address), HTTP (http://ip_address) or HTTPS (https://ip_address) server address manually.
- **DHCP (Option 66/150) Address** – check the server address retrieved via the DHCP Option 66 or 150.
- **File Path** – set the firmware/configuration filename directory or prefix on the server. The intercom expects the XhipY_firmware.bin, XhipY-common.xml and XhipY-MACADDR.xml files, where X is the prefix specified herein and Y specifies the intercom model.
- **Use Authentication** – enable authentication for HTTP server access.
- **Username** – enter the user name for server authentication.
- **Password** – enter the password for server authentication.
- **Verify Server Certificate** – set the set of CA certificates for validation of the ACS public certificate.

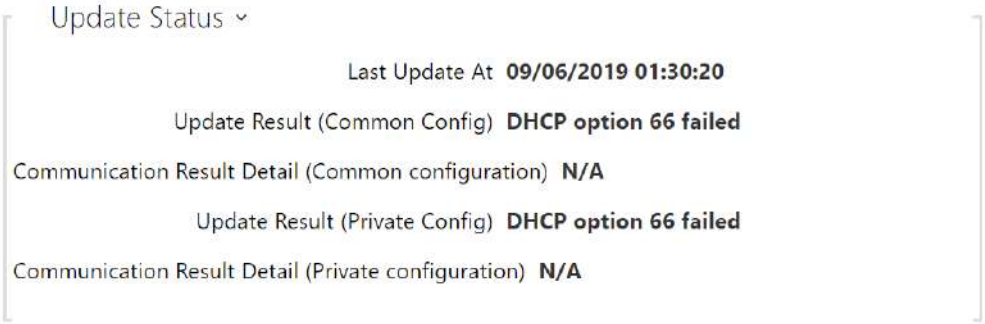
- **Client Certificate** – specify the client certificate and private key to validate the intercom right to communicate with the ACS.

Info

- The intercom contains the Factory Cert, a signed certificate used for British Telecom integration, for example.



- **At Boot Time** – enable check and, if possible, update execution upon every intercom start.
- **Update Period** – set the update period. Set an automatic update to take place hourly/daily/weekly/monthly, or set the period manually.
- **Update At** – set the update time in the HH:MM format for periodical updating at a low-traffic time. The parameter is not applied if the update period is set to a value shorter than 1 day.
- **Next Update At** – set the next update time.



- **Last Update At** – last update time.

- **Update Result (Common Config)** – last update result. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail(Common Config)** – server communication error code or TFTP/HTTP status code.
- **Update Result (Private Config)** – private configuration follows the common configuration update. The device with private configuration is identified by its MAC address. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail (Private Config)** – server communication error code or TFTP/HTTP status code.

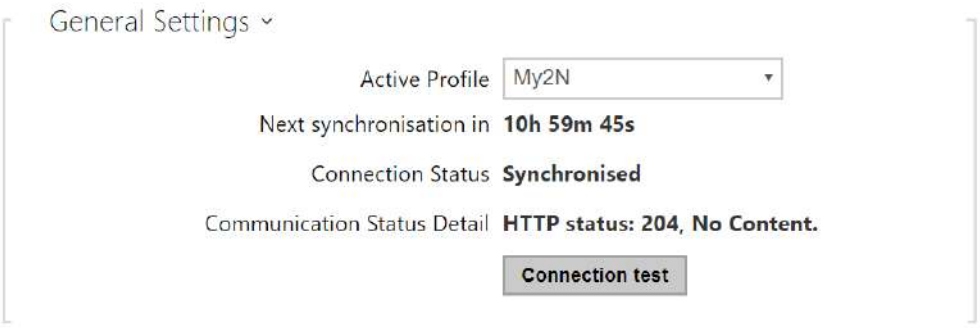
My2N / TR069

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

The TR-069 protocol is utilised by the My2N cloud service. Make sure that TR-069 is enabled and Active profile set to My2N to make your intercom log in to My2N periodically for configuration.

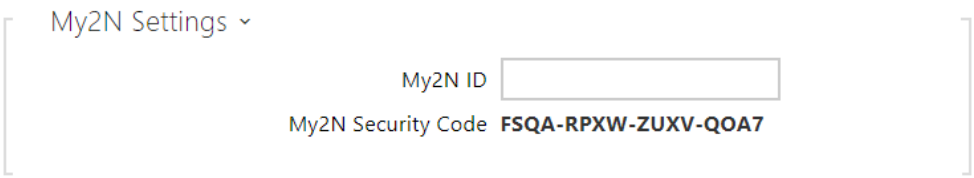
This function helps you connect the intercom to your ACS (Auto Configuration Server). In this case, the connection to My2N will be disabled in the intercom.

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

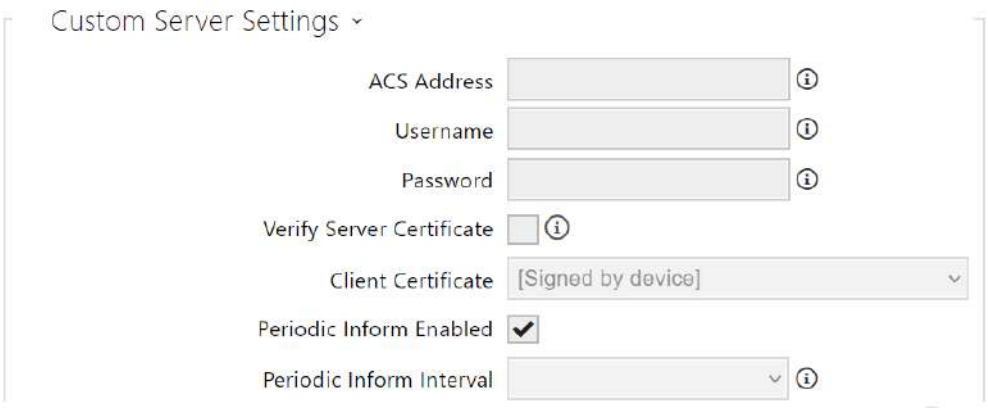


- **Active Profile** – select one of the pre-defined profiles (ACS), or choose a setting of your own and configure the ACS connection manually.

- **Next Synchronisation in** – display the time period in which the intercom shall contact a remote ACS.
- **Connection Status** – display the current ACS connection state or error state description if necessary.
- **Communication Status Detail** – server communication error code or HTTP status code.
- **Connection test** – test the TR069 connection according to the set profile, see the Active profile. The test result is displayed in the Connection status.



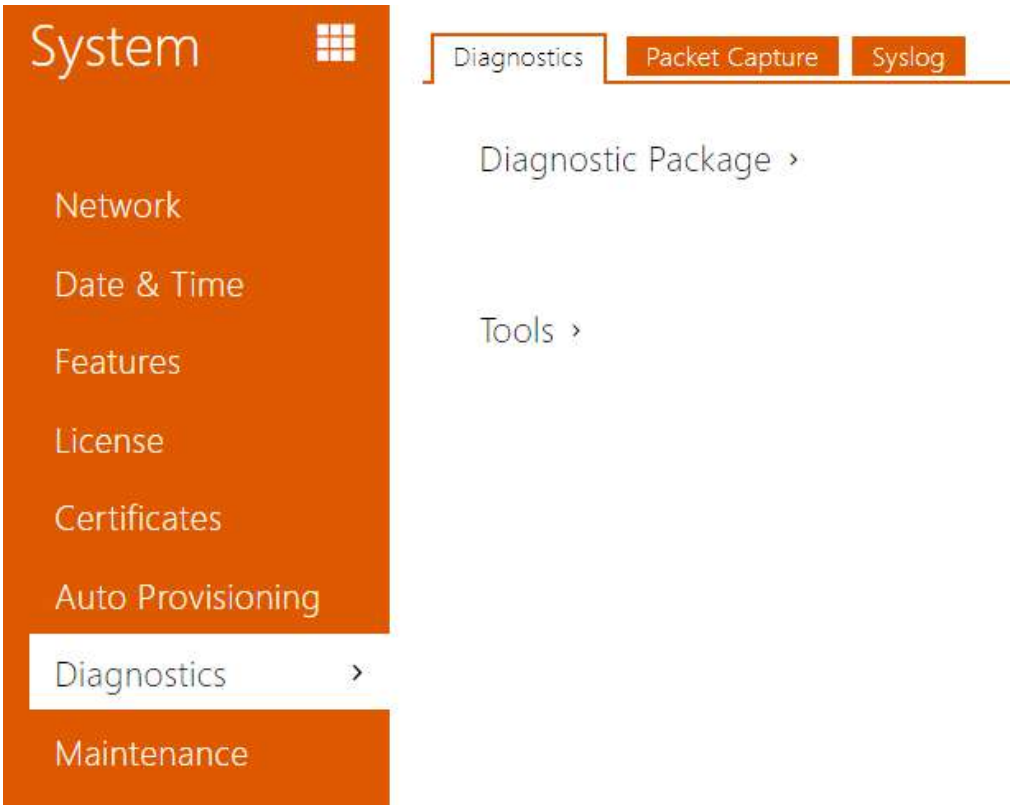
- **My2N ID** – unique identifier of the company created via the My2N portal.
- **My2N Security Code** – display the full application activating code.



- **ACS Address** – set the ACS address in the following format: ipaddress[: port], 192.168.1.1:7547, for example.
- **Username** – set the user name for intercom authentication while connecting to the ACS server.
- **Password** – set the user password for intercom authentication while connecting to the ACS server.
- **Verify Server Certificate** – set the set of CA certificates for validation of the ACS public certificate. Choose one of three sets, see the Certificates subsection. If none is selected, the ACS public certificate is not validated.

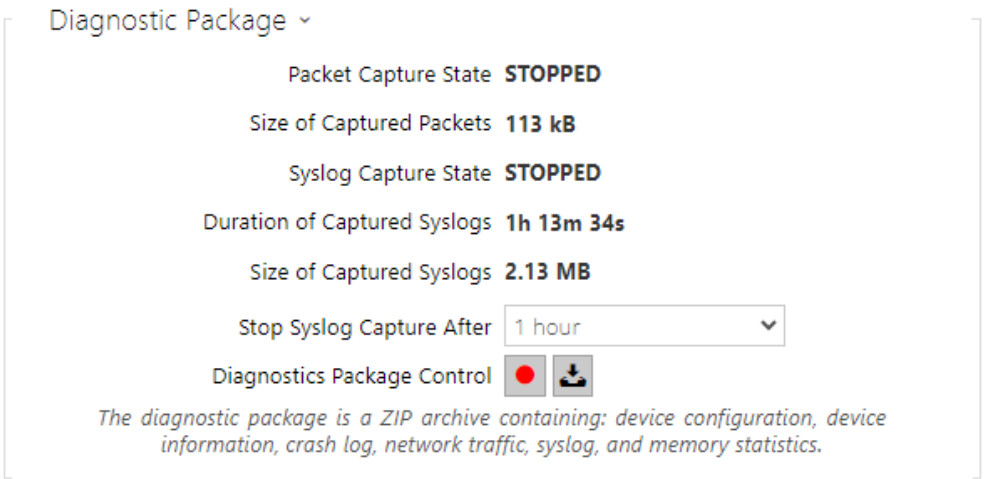
- **Client Certificate** – specify the client certificate and private key to validate the intercom right to communicate with the ACS. Choose one of three sets, refer to the Certificates subsection.
- **Periodic inform enabled** – enable periodical logging of the intercom to the ACS.
- **Periodic inform interval** – set the interval of periodical logging of the intercom to the ACS if enabled by the Periodic inform enabled parameter.

5.5.7 Diagnostics



Diagnostics

The interface helps you start capturing diagnostic logs for subsequent download and sending to the Technical Support. The captured diagnostic logs help identify and solve reported problems. The logs contain information on the device, its configuration, network traffic, crash log and memory statistics.



- **Packet Capture State** – shows whether packet capture has been started/stopped in the Packet capture folder.
- **Size of Captured Packets** – shows the size of packets captured.
- **Syslog Capture State** – shows whether syslog capture has been started/stopped in the Syslog folder.
- **Duration of Captured Syslogs** – shows the syslog capture duration in the Syslog folder.
- **Size of Captured Syslog** – shows the size of syslogs captured.
- **Stop Syslog Capture After** – set the data capture timeout.

Press  to start capturing. Repress the button to restart and rerun capturing. Press  to download the packet capture file.

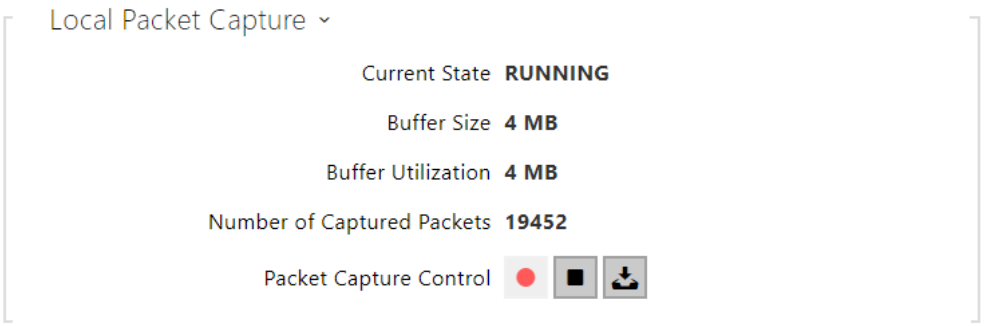
Caution

- Starting diagnostic data capture restarts packet capture if running.

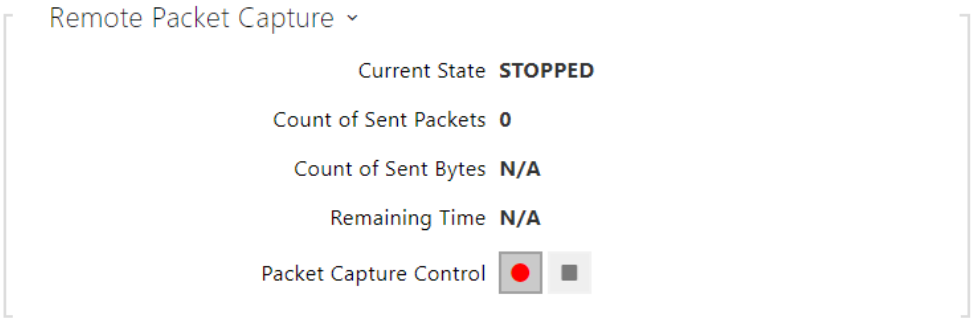
- **Verify the network address accessibility** – verify the network address accessibility via the Ping command in standard operating systems. Press Ping to display a dialogue, enter the IP address/domain name and click Ping to send test data to this address. If the selected IP address/domain name is invalid, a warning is displayed and Ping remains inactive until the given IP address becomes valid.
  The function progress and result are also displayed in the dialogue. Failed means either inaccessibility of the given IP address within 10 seconds or inability to translate the domain name into an address. If a valid response is received, the IP address from which the response came and the response waiting time in milliseconds are displayed.
  Repress Ping to send another query to the same address.

Packet Capture

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



When the local capture buffer is full, the oldest packets are rewritten automatically. We recommend that you lower the video stream transmission rate below 512 kbps while capturing packets locally. Press to start, to stop and to download the packet capture file.

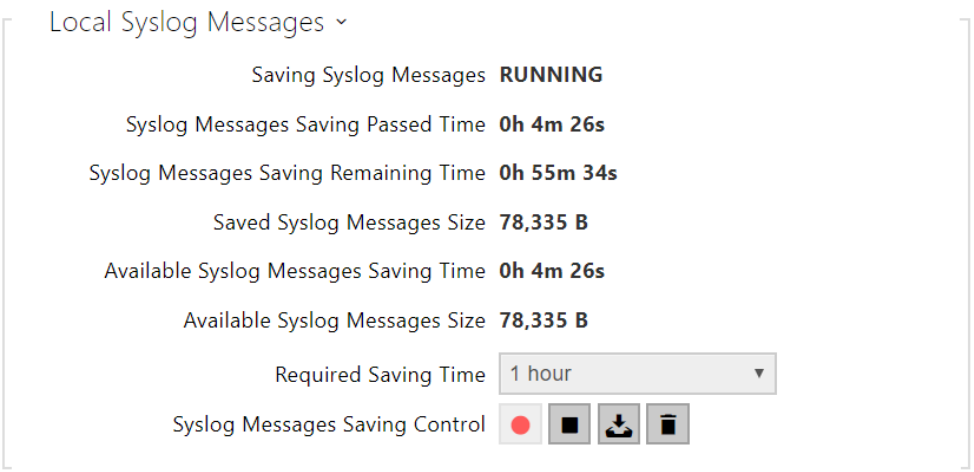


Press to start remote capturing. Specify the capturing time interval (s) for the incoming and outgoing packets. When the set time value passes, the packet capture file will be downloaded automatically to the user PC. Press to stop capturing.

Syslog

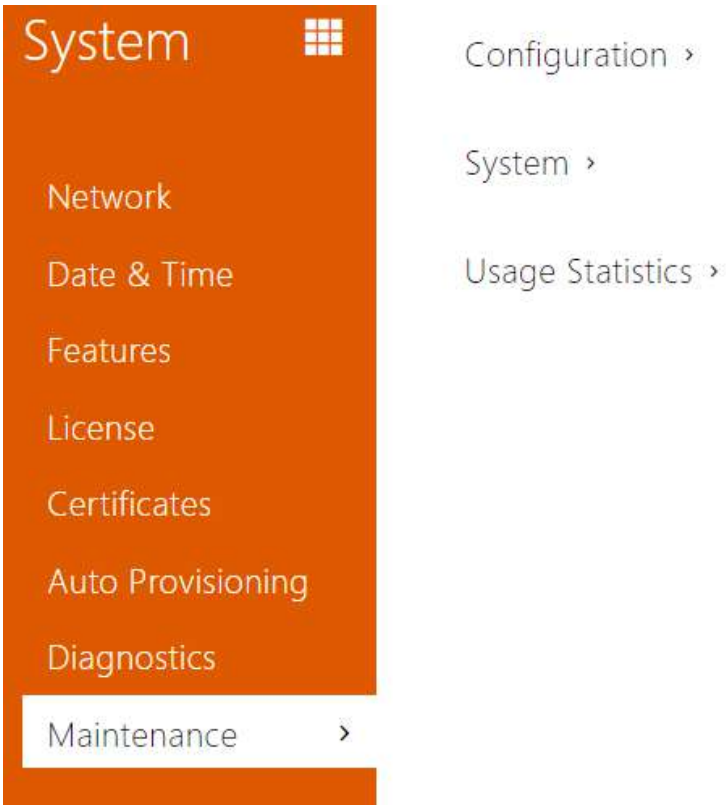
The **2N Access UUnit** allllowww yyouu to sendd sysystememm mmesssaggess tto tthe SySyslog serserverer includludingng rrelevavantt informatition on t2N Accet he dev2N Aice states andd processess fforr rrecording, anallysiss and audidit. IIt is uunnecesssaryy to cconfignfigure tthiss sservicrvice fforr ccommmon ccesss UUnitdg **2N A** opereration.
T .

- **Sendd SySyslog MMessssagges** – enabble sendiingg off syysttem messssaggess to thhe SySyslog servver.r. MMake surure thhatt tthe sservrverr addresss is sset ccorrrecctly.y. –
- **Serrver AdAddresssS** –– set thhe IP/MACIP/MAC address off the serverr on whwhich thhe SySyslogg applicattion is runnning.g.
- **Severityy LLeveel** – set the seeveerity level off the mmessagges tto be sent. Dt. Debbugg 1–31–3 level seettingg iss onnly reecommmendded to ffaccilitatte ttroublebleshhootingg foSer ththe TTechniccal SSuppoSer – t departmmentt.

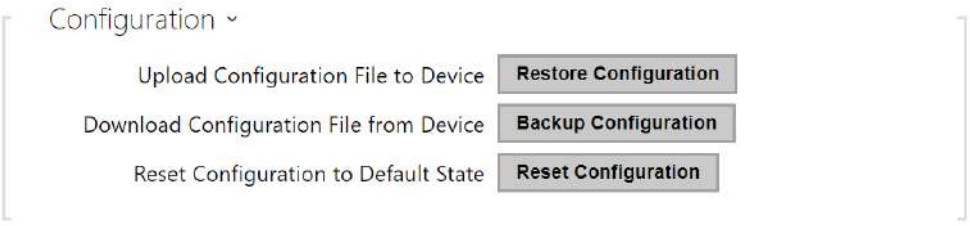


Generral overvieww off localal syslog messagesmessages.G

5.5.8 Maintenance



Use this menu to maintain your **2N Access Unit** configuration and firmware. You can back up and reset all parameters, update firmware and/or reset default settings here.



- **Restore Configuration** – reset configuration from the preceding backup. Press the button to display a dialogue window for you to select and upload the configuration file to the **2N Access Unit**. Before uploading, choose whether to apply general settings from the configuration file, import network settings and certificates.
- **Backup Configuration** – back up the complete current configuration of your **2N Access Unit** Press the button to download the configuration file to your PC.

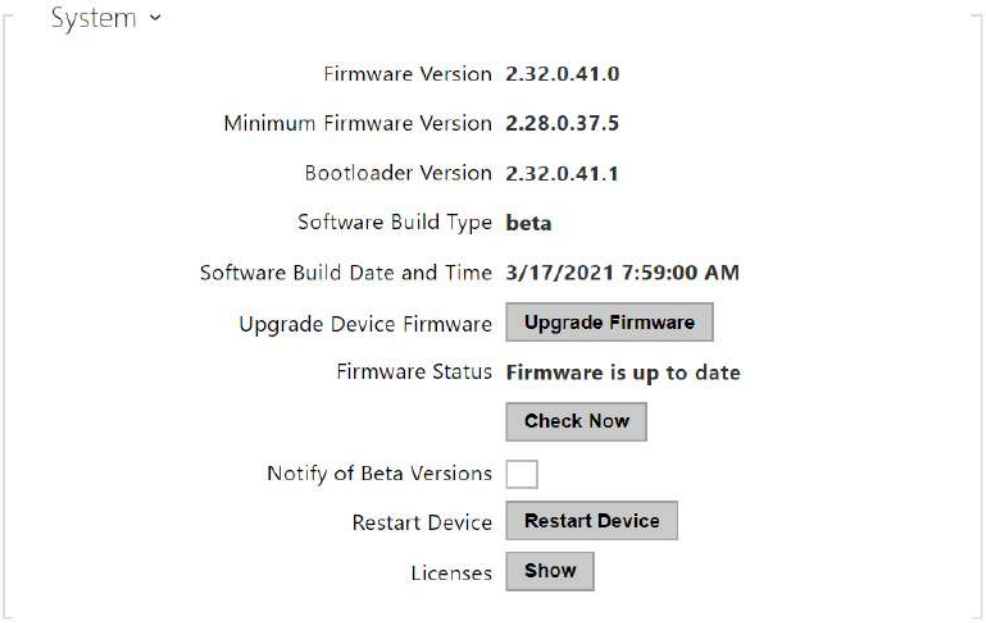
Caution

- *Treat the file cautiously as the* **2N Access Unit** *configuration may include delicate information such as user phone numbers and access codes.*

- **Reset Configuration** – reset default values for all of the **2N Access Unit** parameters except for the network settings. Use the respective jumper or push **Reset** to reset all the **2N Access Unit** parameters; refer to the Installation Manual of your intercom.

Caution

- *The default state reset deletes the license key if any. Hence, we recommend you to copy it to another storage for later use.*
- *The license key is not deleted at HW reset (i.e. reset via a device button) if the Automatic update is enabled (System/License), which updates the license key from the 2N License server. The software reset resets all parameters to the default values except for certificates and network settings.*



Note

- The device function, reliability and security depend on the firmware version installed. A regular firmware upgrade is one of the product use conditions. Errors arisen from the use of an outdated firmware version shall not be subject to complaints. The up-to-date firmware version implements client experience and personal data security requirements.

- **Upgrade Firmware** – upgrade your **2N Access Unit** firmware. Press the button to display a dialogue window for you to select and upload the firmware file to the intercom. The **2N Access Unit** will automatically get restarted and new FW will then be available. The whole upgrading process takes less than one minute. Refer to www.2n.com. for the latest FW

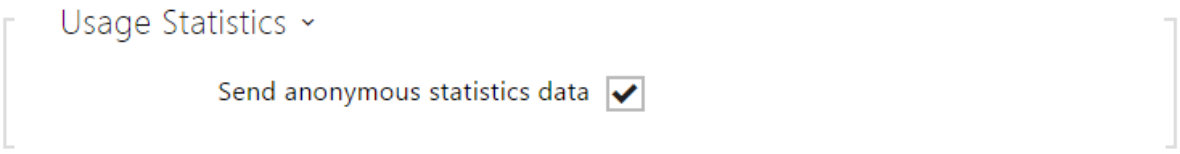
version for your intercom. FW upgrade does not affect configuration as the ***2N Access Unit*** checks the FW file to prevent upload of a wrong or corrupted file.

- **Check Firmware Online** – check online whether a new firmware version is available. If so, download the new FW version and an automatic device upgrade will follow.
- **Restart Device** – restart the **2N Access Unit**. The process takes about 30 s. When the **2N Access Unit** has obtained the IP address upon restart, the login window will get displayed automatically.

Caution

- The **2N Access Unit** configuration change writing takes 3–15 s depending on the **2N Access Unit** configuration size. Do not restart the intercom during this process.

- **License** – click Display to display a dialogue window including a list of used licenses and third party software as well as a EULA link.



- **Send anonymous statistics data** – enable sending of anonymous statistic data on device usage to the manufacturer. These data do not include any sensitive information such as passwords, access codes or phone numbers. This information helps 2N TELEKOMUNIKACE a.s. improve the software quality, reliability and performance. Your participation is voluntary and you can cancel this sending any time.

6. Supplementary Information

Here is what you can find in this section:

6.1 Troubleshooting

For the most frequently asked questions refer to faq.2n.cz.

6.2 Directives, Laws and Regulations

2N Access Unit conforms to the following directives and regulations:

- 2014/53/EU for radio equipment
- 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment
- 2012/19/EU on waste electrical and electronic equipment

Industry Canada

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

FCC

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

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

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

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

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

6.3 General Instructions and Cautions

Please read this User Manual carefully before using the product. Follow all instructions and recommendations included herein.

Any use of the product that is in contradiction with the instructions provided herein may result in malfunction, damage or destruction of the product.

The manufacturer shall not be liable and responsible for any damage incurred as a result of a use of the product other than that included herein, namely undue application and disobedience of the recommendations and warnings in contradiction herewith.

Any use or connection of the product other than those included herein shall be considered undue and the manufacturer shall not be liable for any consequences arisen as a result of such misconduct.

Moreover, the manufacturer shall not be liable for any damage or destruction of the product incurred as a result of misplacement, incompetent installation and/or undue operation and use of the product in contradiction herewith.

The manufacturer assumes no responsibility for any malfunction, damage or destruction of the product caused by incompetent replacement of parts or due to the use of reproduction parts or components.

The manufacturer shall not be liable and responsible for any loss or damage incurred as a result of a natural disaster or any other unfavourable natural condition.

The manufacturer shall not be held liable for any damage of the product arising during the shipping thereof.

The manufacturer shall not make any warrant with regard to data loss or damage.

The manufacturer shall not be liable and responsible for any direct or indirect damage incurred as a result of a use of the product in contradiction herewith or a failure of the product due to a use in contradiction herewith.

All applicable legal regulations concerning the product installation and use as well as provisions of technical standards on electric installations have to be obeyed. The manufacturer shall not be liable and responsible for damage or destruction of the product or damage incurred by the consumer in case the product is used and handled contrary to the said regulations and provisions.

The consumer shall, at its own expense, obtain software protection of the product. The manufacturer shall not be held liable and responsible for any damage incurred as a result of the use of deficient or substandard security software.

The consumer shall, without delay, change the access password for the product after installation. The manufacturer shall not be held liable or responsible for any damage incurred by the consumer in connection with the use of the original password.

The manufacturer also assumes no responsibility for additional costs incurred by the consumer as a result of making calls using a line with an increased tariff.

Electric Waste and Used Battery Pack Handling

Do not place used electric devices and battery packs into municipal waste containers. An undue disposal thereof might impair the environment!

Deliver your expired electric appliances and battery packs removed from them to dedicated dumpsites or containers or give them back to the dealer or manufacturer for environmental-friendly disposal. The dealer or manufacturer shall take the product back free of charge and without requiring another purchase. Make sure that the devices to be disposed of are complete.

Do not throw battery packs into fire. Battery packs may not be taken into parts or short-circuited either.