2N® Access Unit

Access Control

Configuration Manual

Firmware:

Version: 2.20

cie-group.com

The 2N TELEKOMUNIKACE a.s. is a Czech manufacturer and supplier of telecommunications equipment.

The product family developed by 2N TELEKOMUNIKACE a.s. includes GSM gateways, private branch exchanges (PBX), and door and lift communicators. 2N TELEKOMUNIKACE a.s. has been ranked among the Czech top companies for years and represented a symbol of stability and prosperity on the telecommunications market for almost two decades. At present, we export our products into over 120 countries worldwide and have exclusive distributors on all continents.

2N® is a registered trademark of 2N TELEKOMUNIKACE a.s. Any product and/or other names mentioned herein are registered trademarks and/or trademarks or brands protected by law.

2N TELEKOMUNIKACE a.s. administers the FAQ database to help you quickly find information and to answer your questions about 2N products and services. On www.faq.2n.cz you can find information regarding products adjustment and instructions for optimum use and procedures „What to do if...".

2N TELEKOMUNIKACE a.s. hereby declares that the 2N® product complies with all basic requirements and other relevant provisions of the 1999/5/EC directive. For the full wording of the Declaration of Conformity see the CD-ROM (if enclosed) or our website at www.2n.cz.

The 2N TELEKOMUNIKACE a.s. is the holder of the ISO 9001:2009 certificate. All development, production and distribution processes of the company are managed by this standard and guarantee a high quality, technical level and professional aspect of all our products.

Content:

1. Product Overview

Door access system **2N® Access Unit** can (with addon software and/or with **2N Helios 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

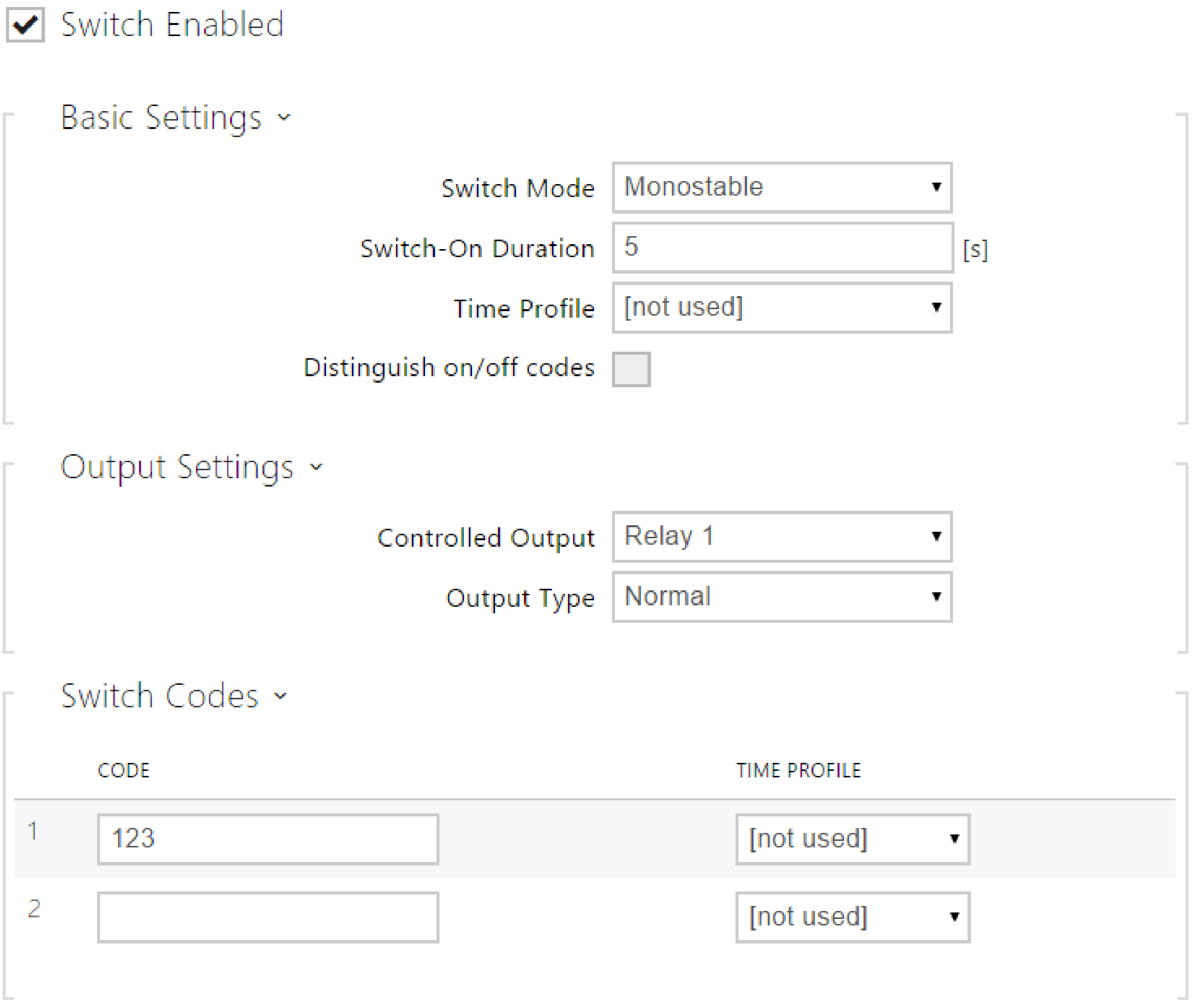
- FAQ: IP address – How to get the 2N® Access Unit IP address?

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.



☑ Switch Enabled

Basic Settings ˅

Switch Mode	Monostable ▾
Switch-On Duration	5 [s]
Time Profile	[not used] ▾
Distinguish on/off codes	□

Output Settings ˅

Controlled Output	Relay 1 ▾
Output Type	Normal ▾

Switch Codes ˅

	CODE	TIME PROFILE
1	123	[not used] ▾
2		[not used] ▾

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 provides just one licensed function – NFC (license Part. No. 916012).

This license can be used only with 2N® Access Unit which has 13 MHz card reader installed.

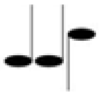
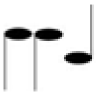
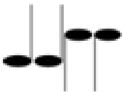
For a limited period of 800 hours it is possible to activate a trial license, which includes the NFC functionality.

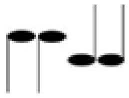
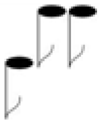
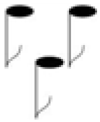
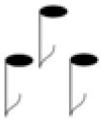
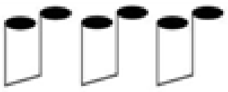
4. Signalling of Operational Statuses

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:

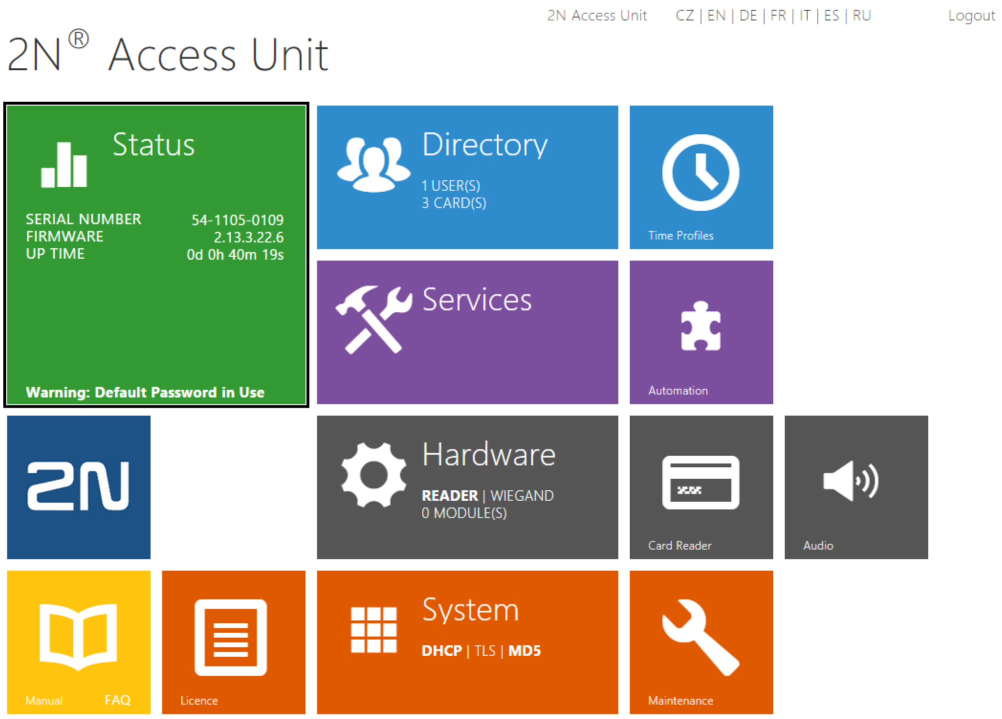
Note

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

Tones	Meaning
	**User activated** This tone signals entering of the user activation code. The activation code is used for user (user’s position) activation. Refer to the Users subsection for the activation code settings.
	**User deactivated** This tone signals entering of the user deactivation code. The deactivation code is used for user (user’s position) deactivation. Refer to the Users subsection for the deactivation code settings.
	**Profile activated** This tone signals profile activation. This function helps enable alerting of a user group in an office, for example. Refer to the Profile subsection for the activation code settings.

	**Profile deactivated** This tone signals profile deactivation. Refer to the Profile subsection for the deactivation code settings.
	**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. Intercom Configuration



2N Access Unit CZ | EN | DE | FR | IT | ES | RU Logout

2N® Access Unit

Status

SERIAL NUMBER 54-1105-0109
FIRMWARE 2.13.3.22.6
UP TIME 0d 0h 40m 19s

Warning: Default Password in Use

Directory

1 USER(S)
3 CARD(S)

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**). Select the web interface language with the **CZ, EN, DE, FR, IT, ES and RU** buttons. Press the Log out button in the right-hand upper corner to log out.

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.

Tip

- Video Tutorial: New web interface of 2N® Helios IP intercoms

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

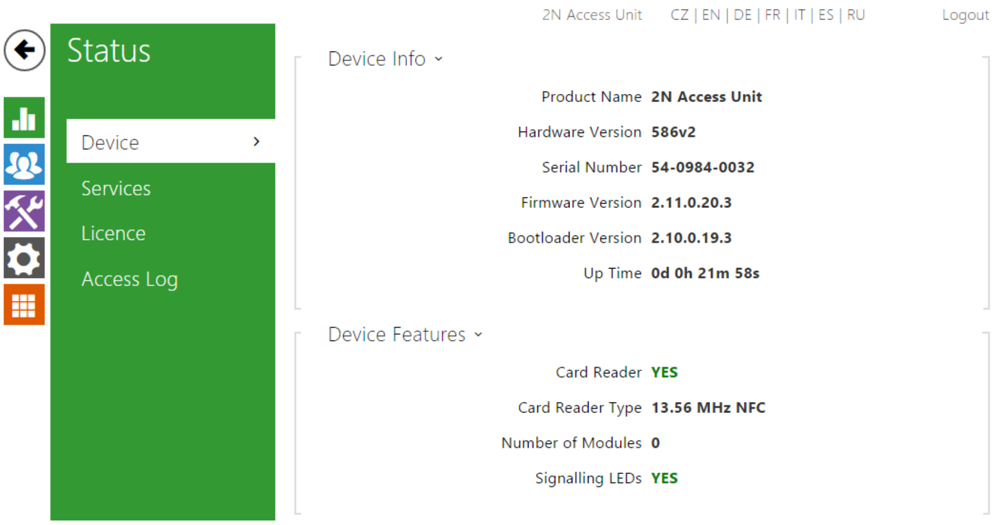
Services

- 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
- 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



Device Info

Product Name	2N Access Unit
Hardware Version	586v2
Serial Number	54-0984-0032
Firmware Version	2.11.0.20.3
Bootloader Version	2.10.0.19.3
Up Time	0d 0h 21m 58s

Device Features

Card Reader	YES
Card Reader Type	13.56 MHz NFC
Number of Modules	0
Signalling LEDs	YES

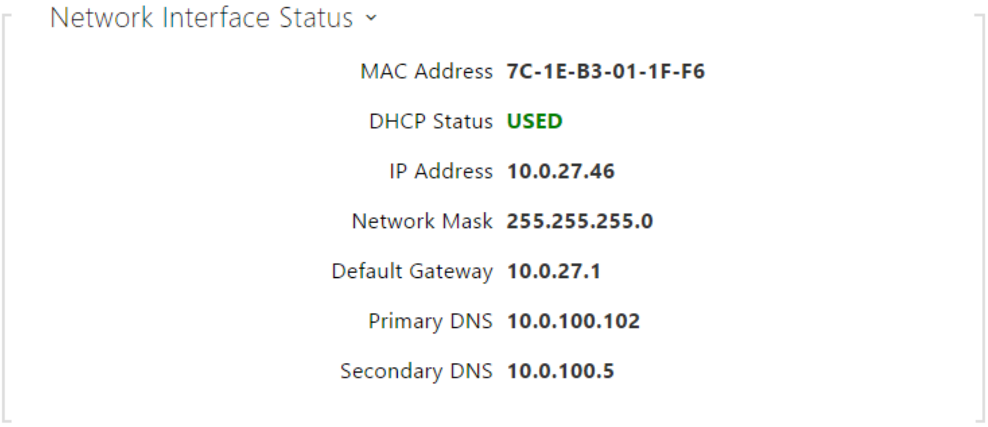
The **Status** menu provides clear status and other essential information on the 2N® Access Unit. The menu is divided into the following tabs:

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.

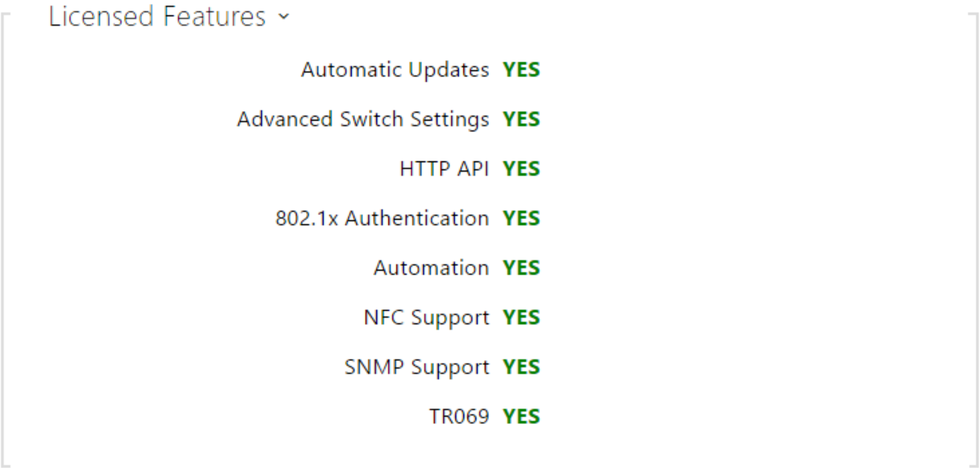


Network Interface Status

MAC Address	7C-1E-B3-01-1F-F6
DHCP Status	USED
IP Address	10.0.27.46
Network Mask	255.255.255.0
Default Gateway	10.0.27.1
Primary DNS	10.0.100.102
Secondary DNS	10.0.100.5

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).

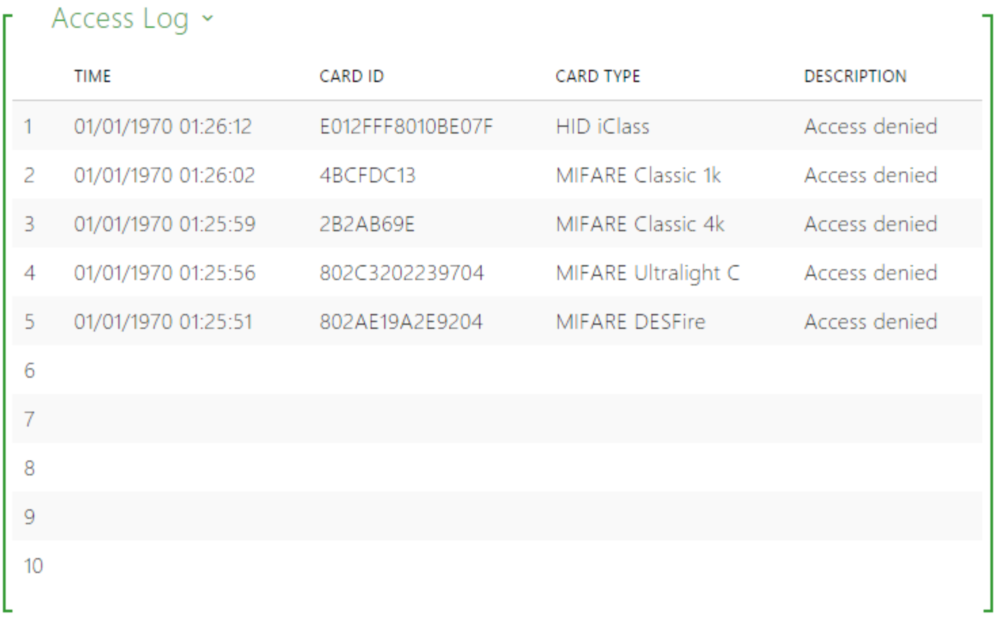


Licensed Features ˅

Automatic Updates	**YES**
Advanced Switch Settings	**YES**
HTTP API	**YES**
802.1x Authentication	**YES**
Automation	**YES**
NFC Support	**YES**
SNMP Support	**YES**
TR069	**YES**

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.).

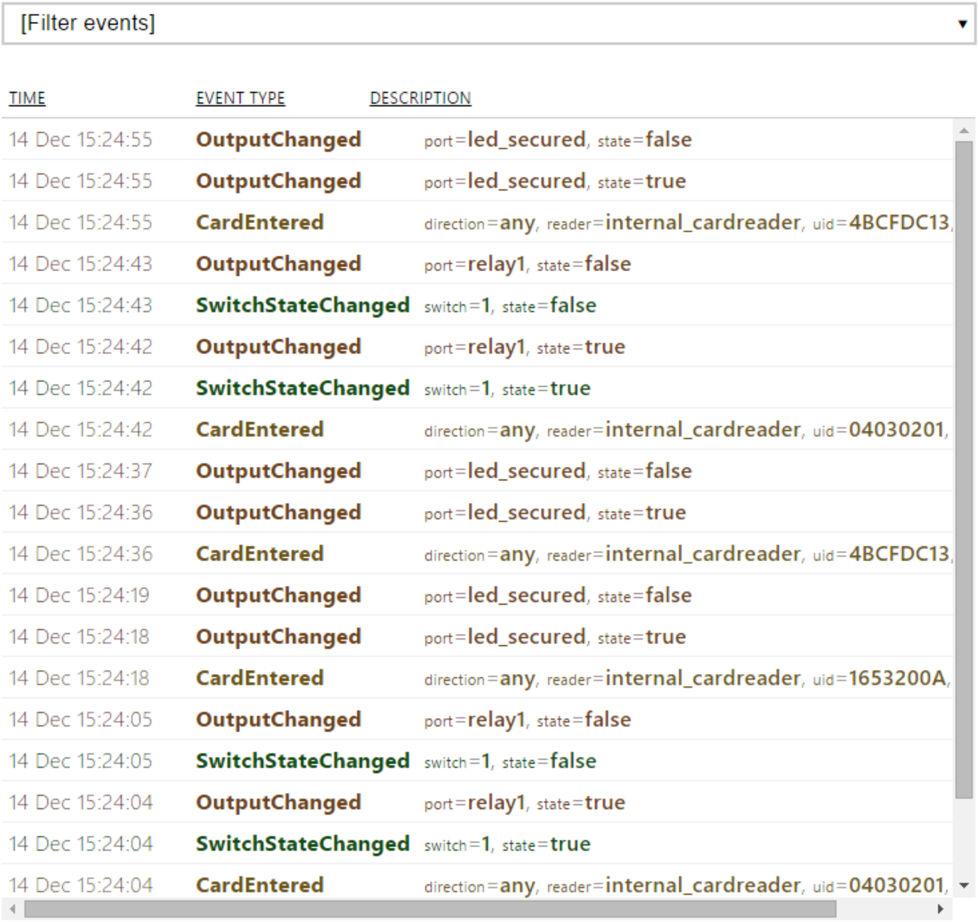


Access Log ˅

	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

This tab displays activity of the device (switches, signalling leds, pressed keys on keypad etc.). It also allows filtering between events through the 13 optional parameters.



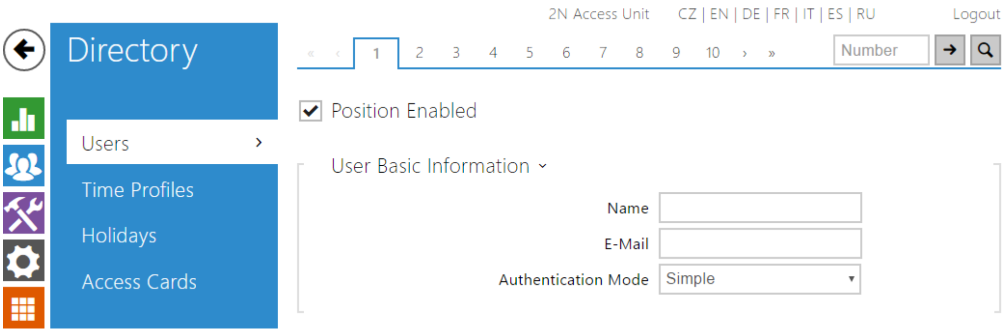
TIME	EVENT TYPE	DESCRIPTION
14 Dec 15:24:55	OutputChanged	port=led_secured, state=false
14 Dec 15:24:55	OutputChanged	port=led_secured, state=true
14 Dec 15:24:55	CardEntered	direction=any, reader=internal_cardreader, uid=4BCFDC13,
14 Dec 15:24:43	OutputChanged	port=relay1, state=false
14 Dec 15:24:43	SwitchStateChanged	switch=1, state=false
14 Dec 15:24:42	OutputChanged	port=relay1, state=true
14 Dec 15:24:42	SwitchStateChanged	switch=1, state=true
14 Dec 15:24:42	CardEntered	direction=any, reader=internal_cardreader, uid=04030201,
14 Dec 15:24:37	OutputChanged	port=led_secured, state=false
14 Dec 15:24:36	OutputChanged	port=led_secured, state=true
14 Dec 15:24:36	CardEntered	direction=any, reader=internal_cardreader, uid=4BCFDC13,
14 Dec 15:24:19	OutputChanged	port=led_secured, state=false
14 Dec 15:24:18	OutputChanged	port=led_secured, state=true
14 Dec 15:24:18	CardEntered	direction=any, reader=internal_cardreader, uid=1653200A,
14 Dec 15:24:05	OutputChanged	port=relay1, state=false
14 Dec 15:24:05	SwitchStateChanged	switch=1, state=false
14 Dec 15:24:04	OutputChanged	port=relay1, state=true
14 Dec 15:24:04	SwitchStateChanged	switch=1, state=true
14 Dec 15:24:04	CardEntered	direction=any, reader=internal_cardreader, uid=04030201,

5.2 Directory

Here is what you can find in this section:

- 5.2.1 Users
- 5.2.2 Time Profiles
- 5.2.3 Holidays

5.2.1 Users



☑ Position Enabled

Name	
E-Mail	
Authentication Mode	Simple

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 1999 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.

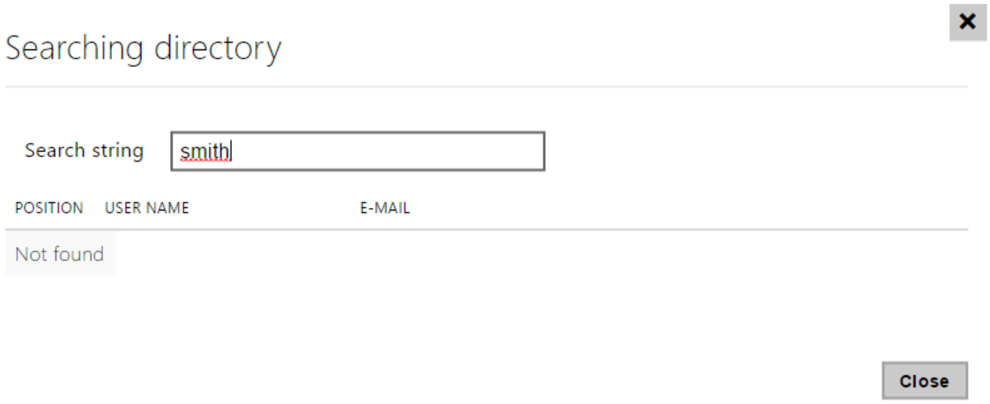
If your external card reader is connected to the intercom via the Wiegand interface, the card ID is shortened to 6 or 8 characters for transmission (depending on the transmission parameters). If you apply a card to the reader, you will receive a complete ID, which is typically longer (8 chars or more). 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.

Refer to the **Directory / Users** menu for the User list settings. Use the navigation panel for selecting user positions easily and arrows for scrolling pages. Or, you can enter the position number and push → to move to the position quickly. If you know the user's name, push 🔍 to find its position.

The Search in directory function works as a fulltext search in position numbers, user names, phone numbers and e-mail addresses. The match is found in all the positions.



Searching directory

Search string: smith

POSITION	USER NAME	E-MAIL
Not found		

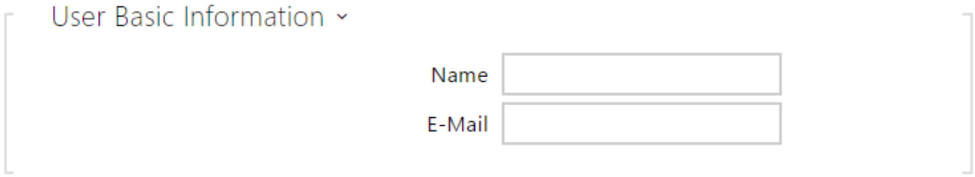
Every record in the Users list includes the following parameters:

- **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.
- **User switch codes** – enter the switch activating user codes (door lock activation, e.g.). A time profile can be assigned to each code.
- **User cards** – enter the user-defined access cards with/without a time profile. Enable/disable double authentication (valid user card + switch activating code) for each user.
- **User mobile key** – allows to authenticate users using a mobile app 2N® Mobile Key.

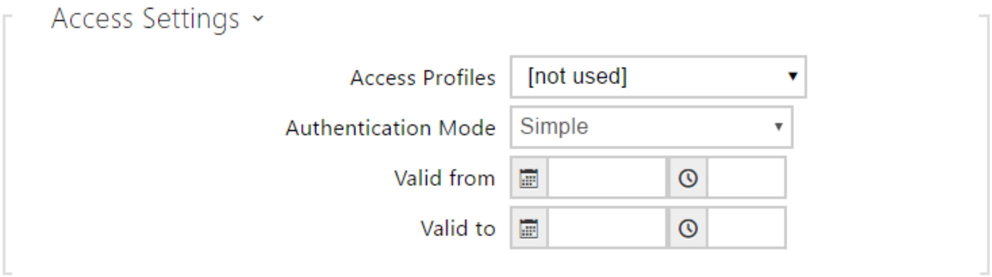
Refer to the **Directory / Users** menu for the Users settings. Use the navigation panel for selecting the user positions easily and arrows for scrolling pages. Or, you can enter the position number and push → to move to the position quickly. If you know the user's name, push 🔍 to find its position.

List of Parameters

- **Remove user** – all the user data will be deleted after the user is removed.



- **Name** – enter the user name for the selected user position. This parameter is optional and helps you find items in the user list more easily.
- **E-mail** – enter the user E-mail to which information on missed or successful calls can be sent. Refer to the E-Mail subsection for more details.

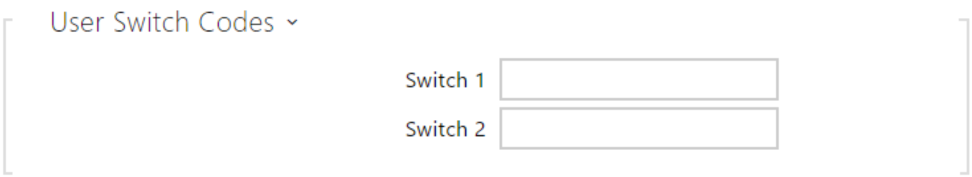


Access Profiles: [not used]

Authentication Mode: Simple

Each user is assigned an access mode for intercom authentication.

- **Acces Profiles** – assign an access profile to user Auth ID to control its validity. If the profile is inactive, the user Auth ID is considered invalid. If assigned multiple profiles at the same time, Auth ID is valid only if one of the profiles is active at least.
- **Authentication mode** – set the authentication mode for a user - either simple or a combination of the user card, numeric code and fingerprint, depending on which authentication devices are installed. To activate the switch in the multiple authentication mode, it is necessary to perform all the selected authentication actions sequentially in ten-second intervals.
- **Valid from** – set the beginning of the mode validity term.
- **Valid to** – set the end of the mode validity term.



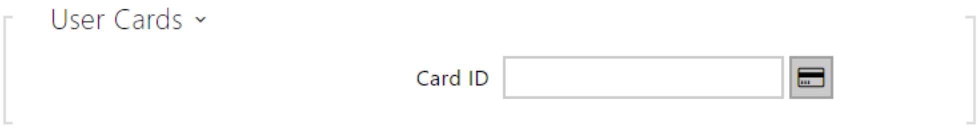
User Switch Codes ˅

Switch 1

Switch 2

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.

Code – set a private user switch activation code: up to 16 characters including digits 0–9 only.



User Cards ˅

Card ID 💳

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

- **Card ID** – set the user access card ID: 6–32 characters including 0–9, A–F. Each user can be assigned just one access card. 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.

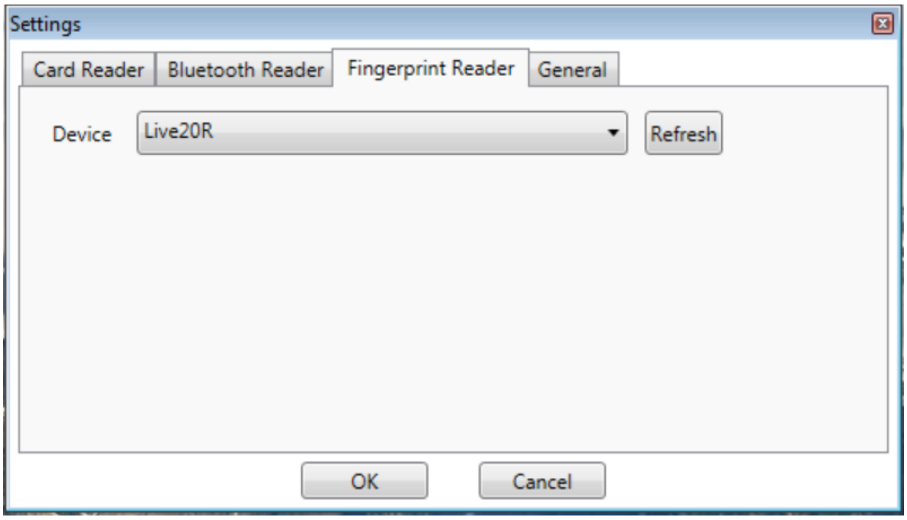
✓ **Tip**

- The user card ID can also be entered via an external USB card reader (Part No. 9137421E).
- Press 💳 and swipe the card through the USB card reader. The card number will be automatically entered into the Card ID field.
- Make sure that a PC driver is installed to make the USB card reader work properly. Refer to **www.2n.cz**.

Instructions for setting a user´s fingerprints

Fingerprint reading is possible via an external USB fingerprint reader (ordering no. 9137423E). The procedure is as follows:

1) Go to the Helios IP USB Driver settings, select the Fingerprint reader (Biometric reader) and confirm by clicking OK.

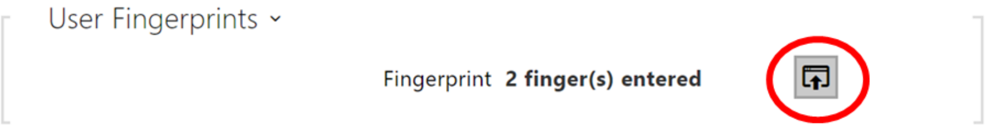


Settings

Card Reader | Bluetooth Reader | Fingerprint Reader | General

Device: Live20R

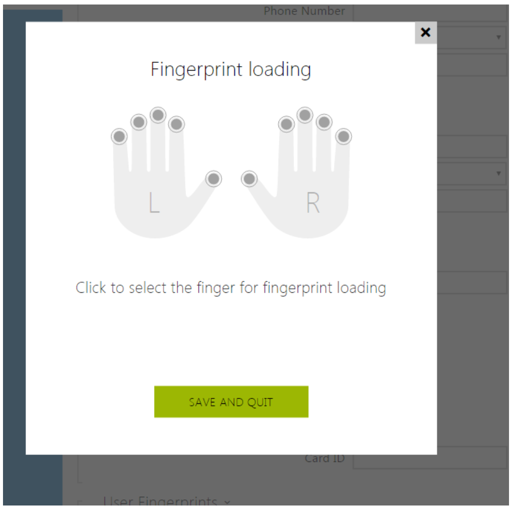
2) Click the fingerprint reading button in the user section of the **2N**® **Acces Unit´s** web interface.



User Fingerprints ⌄

Fingerprint **2 finger(s) entered**

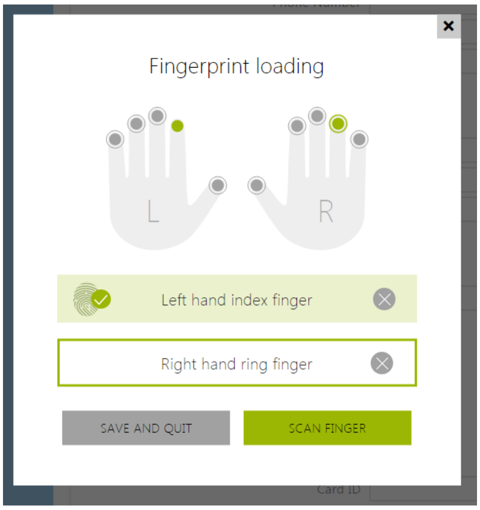
3) Click to select a finger to record a fingerprint.



Fingerprint loading

Click to select the finger for fingerprint loading

Up to two fingerprints may be saved for each user.

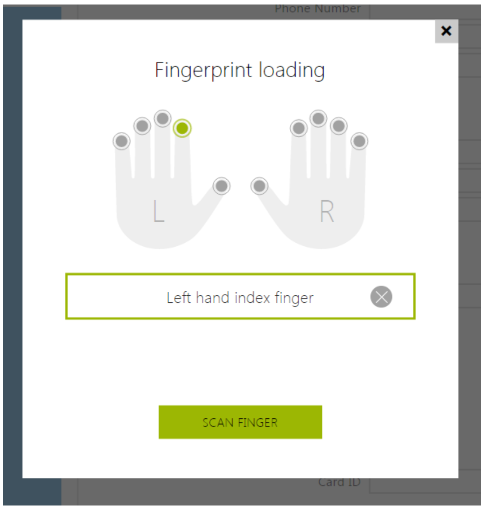


Fingerprint loading

Left hand index finger

Right hand ring finger

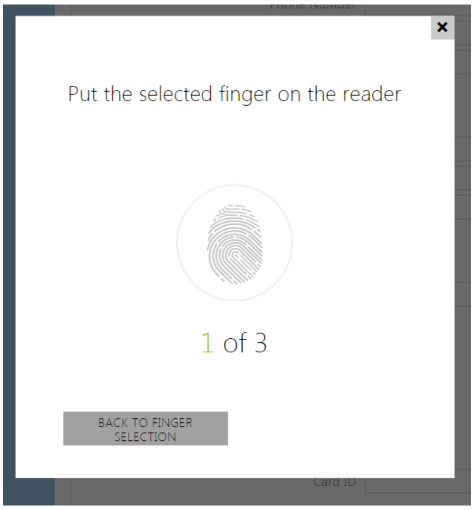
4) To record a fingerprint, click SCAN FINGER.



Fingerprint loading

Left hand index finger

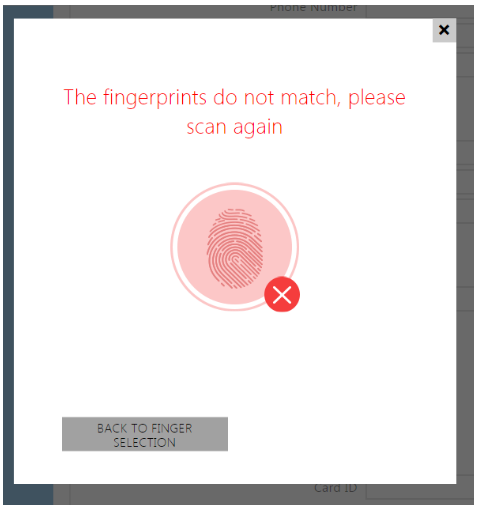
5) Place the selected finger on a external USB reader. This process is repeated three times for greater precision.



Put the selected finger on the reader

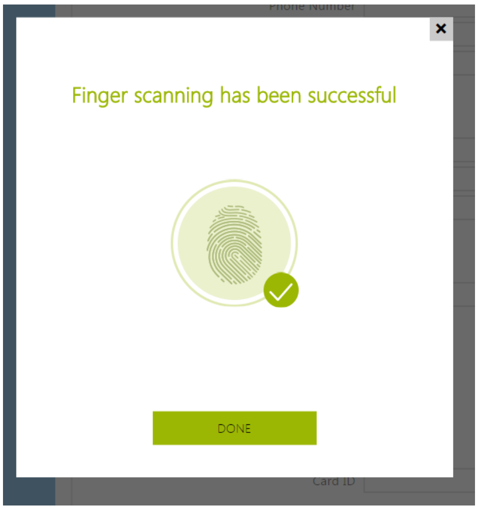
1 of 3

6) Repeat the process if any inconsistency occurs during fingerprint reading.



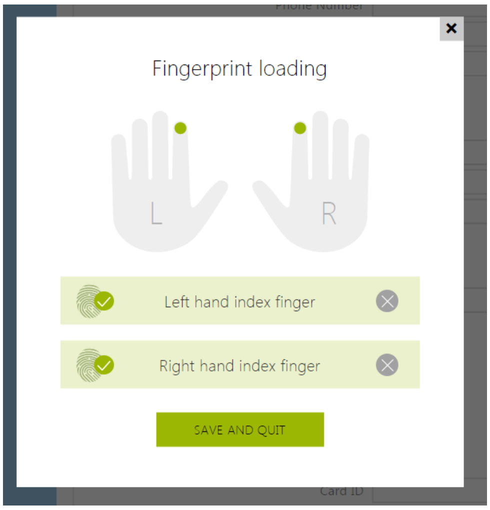
The fingerprints do not match, please scan again

7) If fingerprint scanning is successful, confirm the settings by clicking DONE.



Finger scanning has been successful

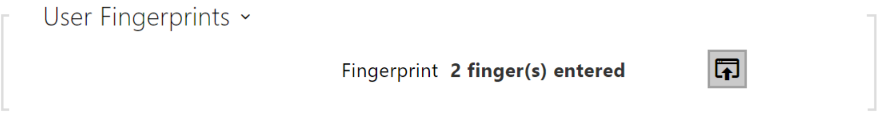
To apply the fingerprint settings, confirm the process by clicking SAVE AND QUIT.


Fingerprint loading

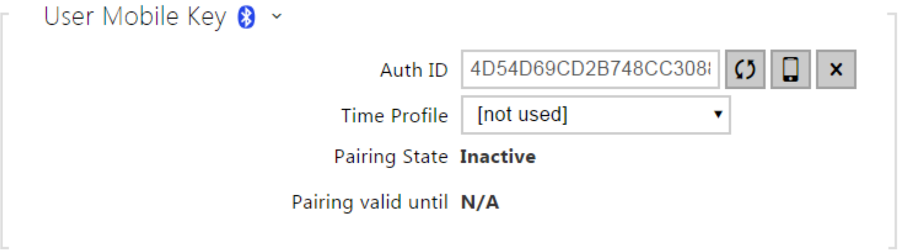
Left hand index finger

Right hand index finger

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


User Fingerprints

Fingerprint **2 finger(s) entered**


User Mobile Key

Auth ID	4D54D69CD2B748CC308
Time Profile	[not used]
Pairing State	**Inactive**
Pairing valid until	**N/A**

- 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.
- Time profile – assign a time profile to user Auth ID to control its validity. If the profile is inactive, the user Auth ID is considered invalid. If assigned multiple profiles at the same time, Auth ID is valid only if one of the profiles is active at least.
- 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

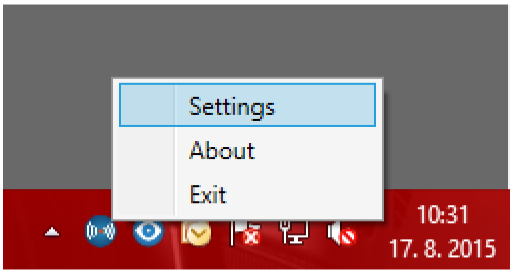
To pair a mobile phone with the user:

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

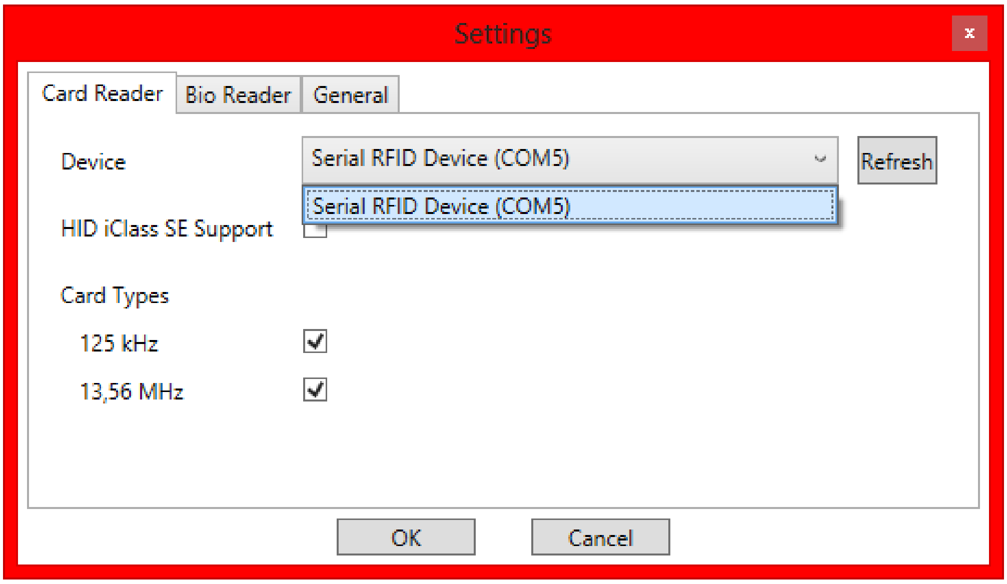
USB RFID Card Reader

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

1. Go to the **2N**® **Helios IP** USB Driver settings.



2. Set up the COM port for the connected reader.

a. 

Settings

Card Reader | Bio Reader | General

Device: Serial RFID Device (COM5)

Serial RFID Device (COM5)

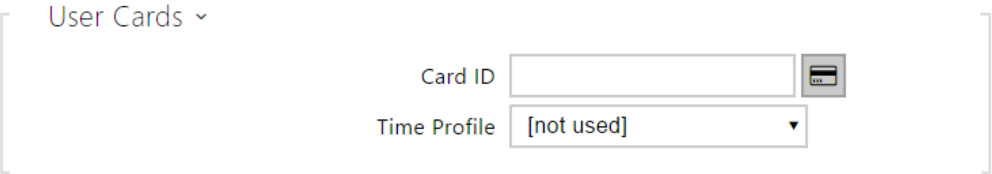
HID iClass SE Support □

Card Types

125 kHz ☑

13,56 MHz ☑

3. Press the Read button via the **2N**® **Helios IP** web interface.

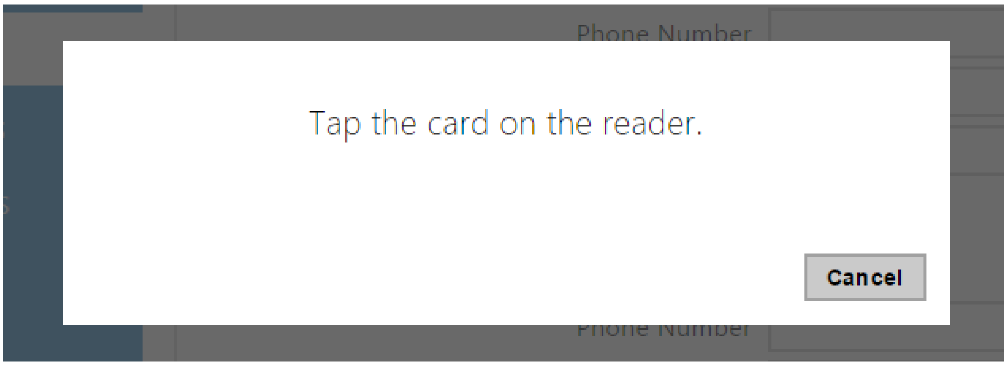


User Cards

Card ID:

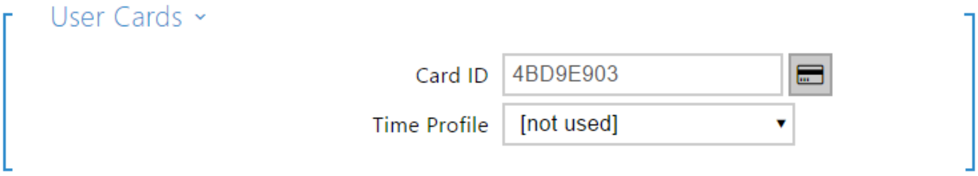
Time Profile: [not used]

4. Tap the card on the card reader.

a. 

Tap the card on the reader.

5. The card ID is successfully read.



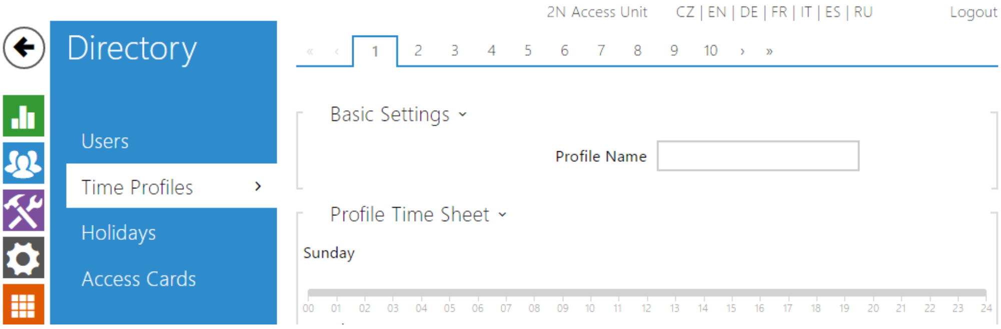
User Cards

Card ID 4BD9E903

Time Profile [not used]

6. Do not forget to save the configuration.

5.2.2 Time Profiles



Profile Name

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:

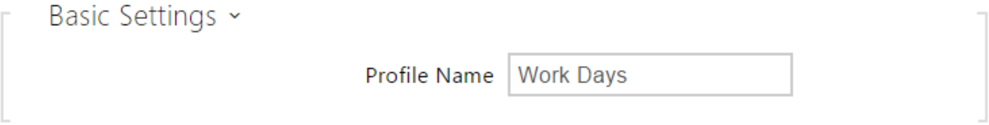
- block all calls to a selected user beyond the set time interval
- block calls to selected user phone numbers beyond the set time interval
- block RFID access for a user beyond the set time interval
- block numeric code access for a user beyond the set time interval
- block switch activation beyond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

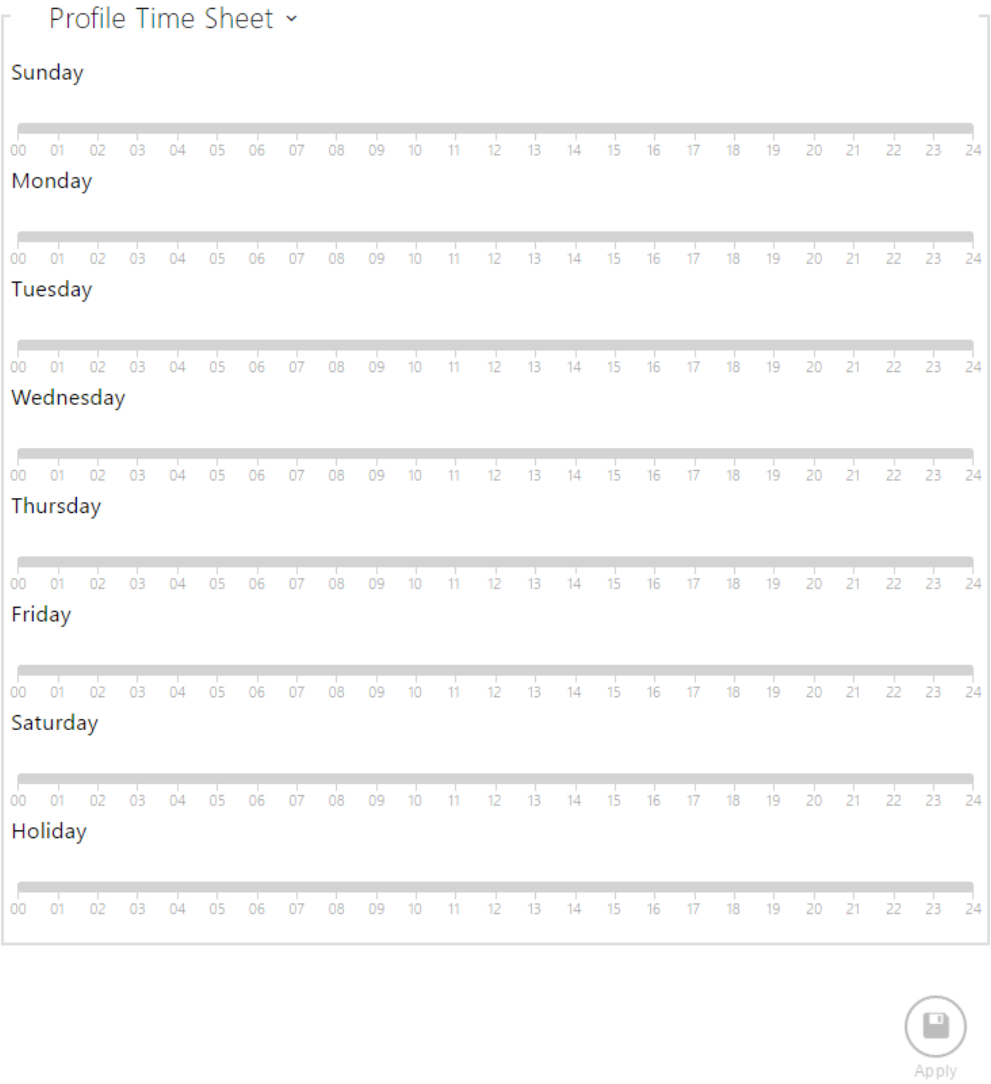
Refer to the **Directory / Time Profiles** menu for the time profile settings.

List of Parameters



Profile Name: Work Days

- **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.

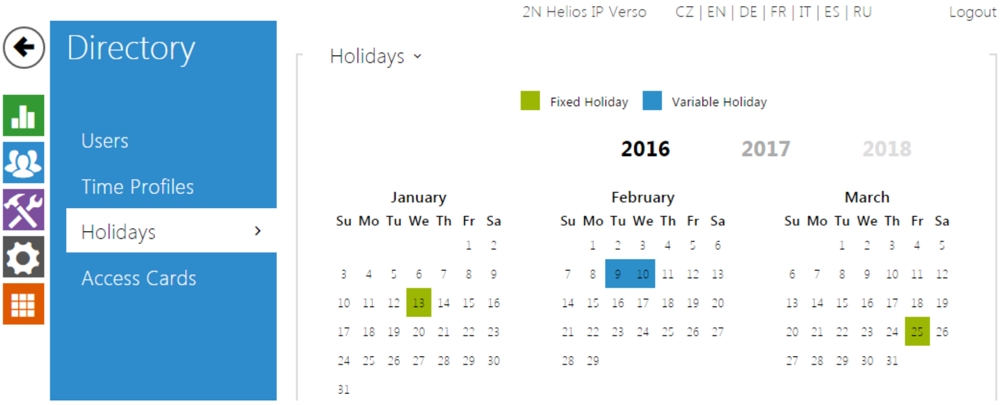
If a day is marked as holiday (refer to **Directory Holidays**), the last table row (Holiday) is applied regardless of the day in a week.

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



🟩 Fixed Holiday 🟦 Variable Holiday

January

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

February

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29					

March

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

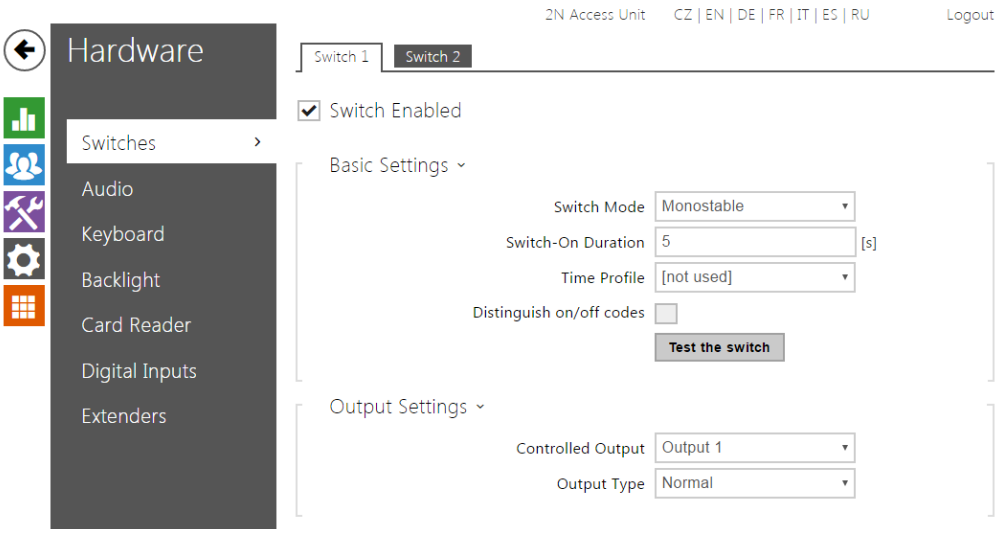
Here select the bank holidays (including Sundays). You can assign them different time intervals than to working days in their time profiles.

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



☑ Switch Enabled

Basic Settings

Switch Mode	Monostable
Switch-On Duration	5 [s]
Time Profile	[not used]
Distinguish on/off codes	□

Output Settings

Controlled Output	Output 1
Output Type	Normal

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 1).
- the Action.ActivateSwitch action via Automation.

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

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® Helios 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.

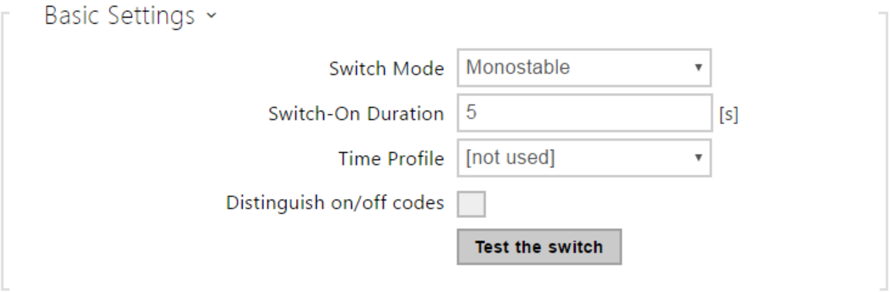
The switch signals its state by:

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

List of Parameters

☑ Switch Enabled

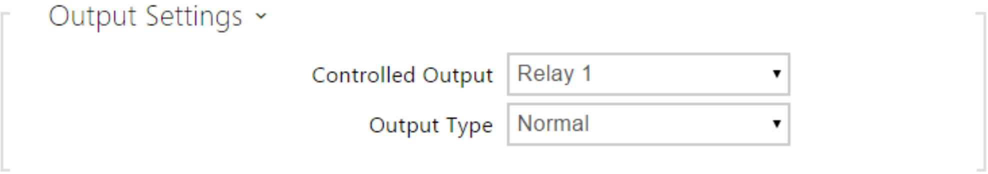
- **Switch Enabled** – enable/disable the switch globally. When disabled, the switch cannot be activated by any of the available codes (including user switch codes), by quick dial button.



Basic Settings

Switch Mode	Monostable
Switch-On Duration	5 [s]
Time Profile	[not used]
Distinguish on/off codes	□

- **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.
- **Distinguish on/off codes** – set a switch code mode in which odd codes (1, 3, etc.) are used for switch activation and even codes (2, 4, etc.) are for switch deactivation. This mode can only be used if the switch is set to the bistable mode.
- **"Test the switch" button** – activate the switch manually to test its function, e.g. an electric lock or another device connected.

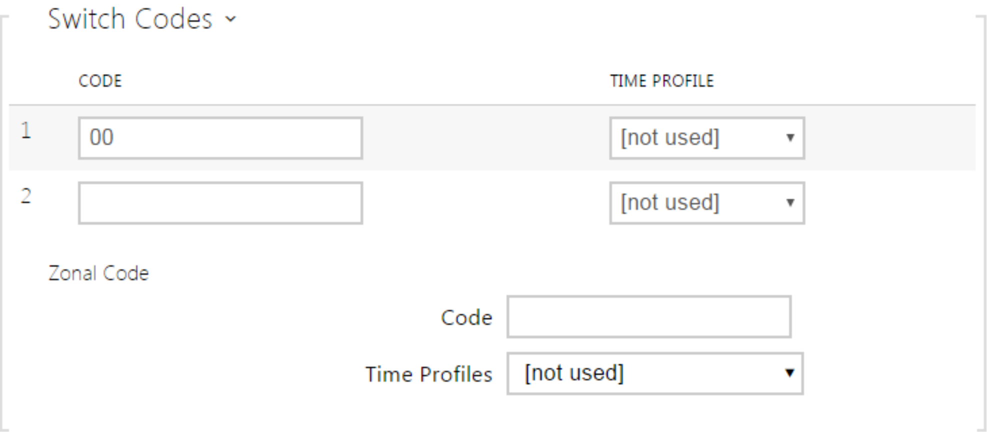


Output Settings

Controlled Output	Relay 1
Output Type	Normal

- **Controlled Output** – assign an electric output to the switch. Choose one of the available intercom outputs: relay, power output, extender output and so on. 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® Helios IP 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® Helios IP 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.


Switch Codes ˅

	CODE	TIME PROFILE
1	00	[not used]
2		[not used]

Zonal Code

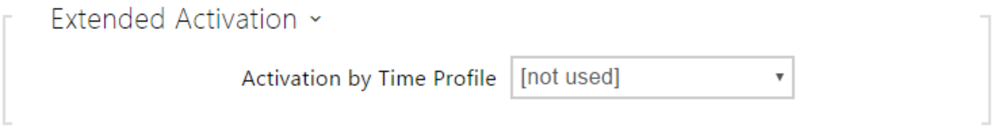
Code	
Time Profiles	[not used]

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 a numeric code for the switch. The code must include 2 characters at least but we recommend you to use four characters at least to make the code accessible from the intercom numeric keypad. Codes 00 and 11 cannot be entered from the numeric keypad. 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.

The zone code is an access code shared by a group of intercoms for switch 1 activation from the keypad.

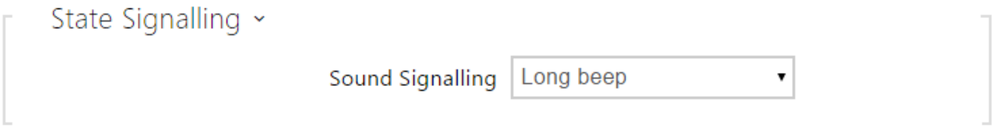
- **Code** – enter a numeric code for the switch. The code must include 2 characters at least but we recommend you to use four characters at least to make the code accessible from the intercom numeric keypad. Codes 00 and 11 cannot be entered from the numeric keypad. Confirm the code with *. The code length is up to 16 characters.
- **Time profiles** – assign a time profile to the switch code for validity control. The switch can be activated only if one of its time profiles is valid at least.



Extended Activation

Activation by Time Profile: [not used]

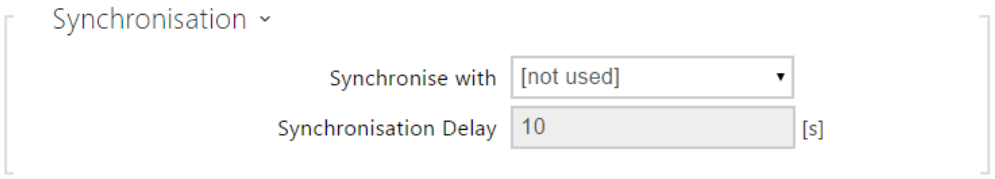
- **Activation by time profile** – activate the switch by a pre-defined time profile. The switch will remain active as long as the assigned time profile is active.



State Signalling

Sound Signalling: Long beep

- **Sound Signalling** – set the sound signalling type for switch activation. Choose the Short beep or Long beep (during the whole activation).

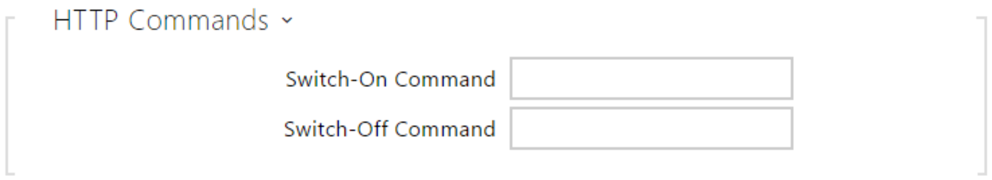


Synchronisation

Synchronise with: [not used]

Synchronisation Delay: 10 [s]

- **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.



HTTP Commands

Switch-On Command:

Switch-Off Command:

- **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**

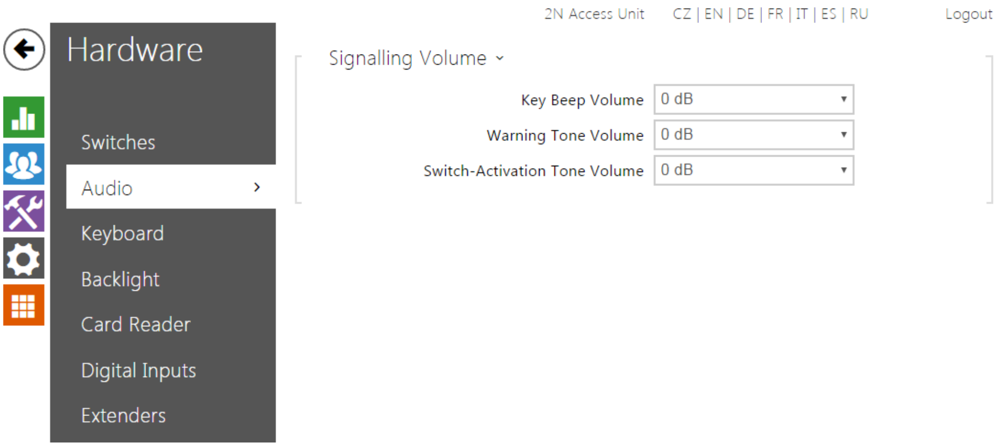
✓ In case of use external relay **part no.: 9137410E** are used next HTTP commands:

- 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)

5.3.2 Audio



Signalling Volume

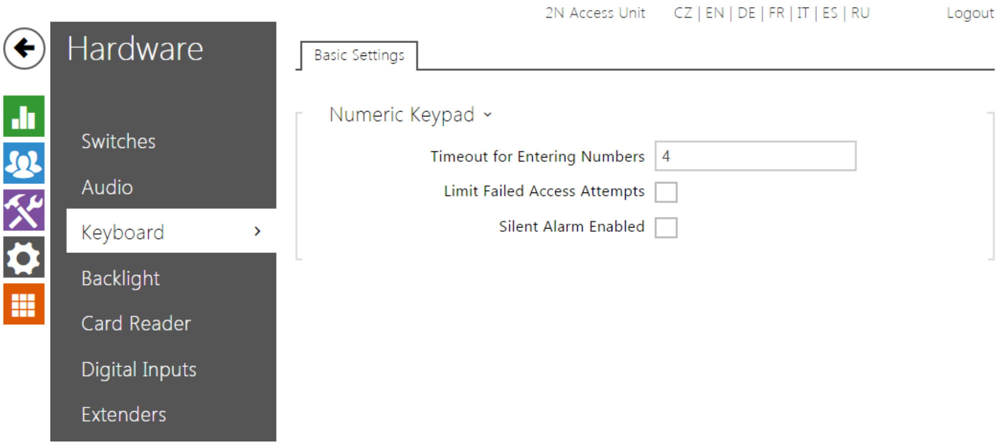
Key Beep Volume: 0 dB

Warning Tone Volume: 0 dB

Switch-Activation Tone Volume: 0 dB

- **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.

5.3.3 Keyboard



Numeric Keypad ˅

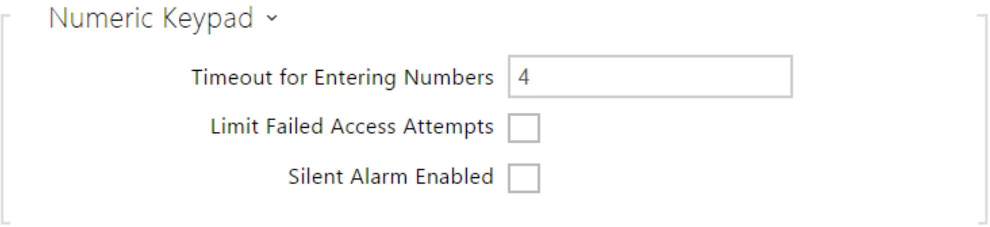
Timeout for Entering Numbers: 4

Limit Failed Access Attempts □

Silent Alarm Enabled □

List of Parameters

Basic Settings



Numeric Keypad ˅

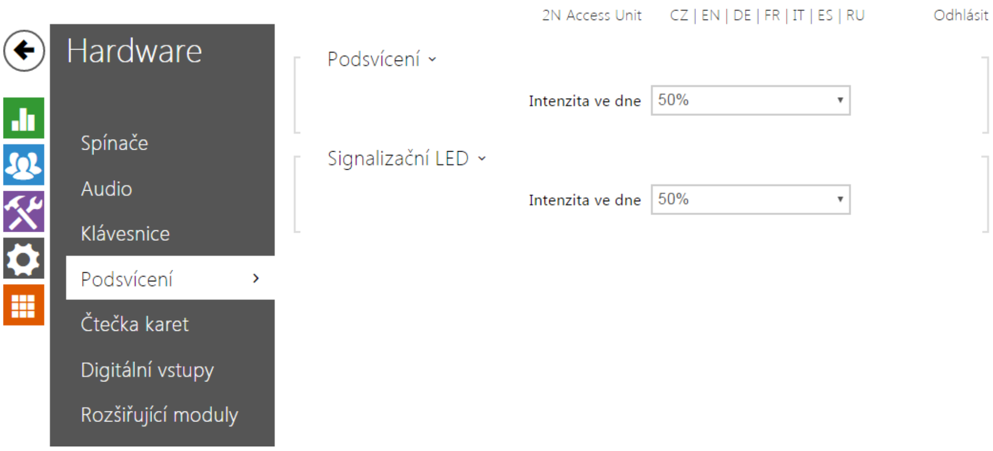
Timeout for Entering Numbers: 4

Limit Failed Access Attempts □

Silent Alarm Enabled □

- **Timeout for entering numbers** – set the maximum interdigit timeout for code dialling via the numeric keypad. If you dial a switch activation code, the dialling will be rejected after this timeout unless confirmed with * . Set the code entering limit in the range of 3–15 s.
- **Limit unsuccessful access attempts** – activate temporary code blocking. After 5 invalid access attempts, code entering is blocked for 30 seconds during which all the used codes are evaluated as invalid. The **Enhanced Security** licence is required for this function.
- **Enable silent alarm** – activate the silent alarm function. Silent alarm can be started by entering a code higher by 1 than the user switch code. If, thus, a user is assigned switch code 123, silent alarm is started with 124. The **Enhanced Security** licence is required for this function.

5.3.4 Backlight



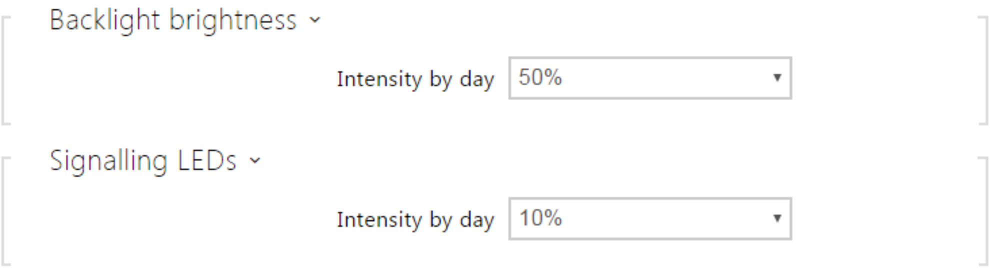
Podsvícení

Intenzita ve dne 50%

Signalizační LED

Intenzita ve dne 50%

This tab helps you control the backlight level of buttons and brightness of signalling LEDs.



Backlight brightness

Intensity by day 50%

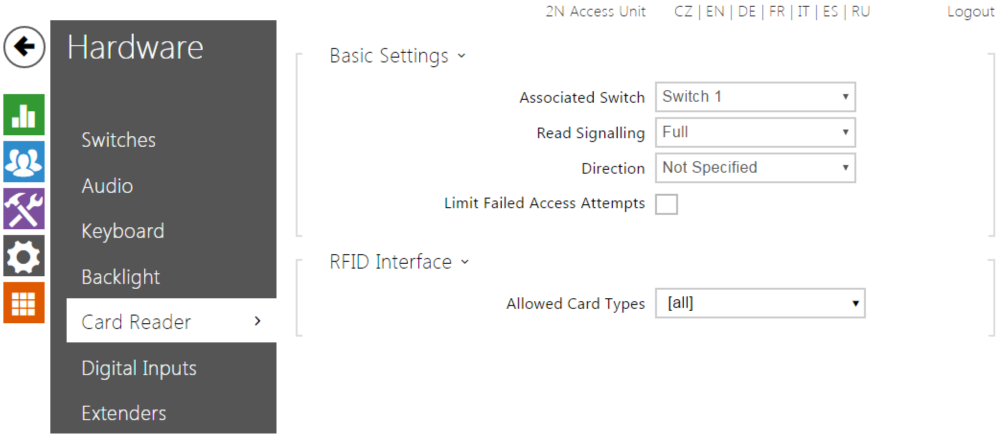
Signalling LEDs

Intensity by day 10%

- **Brightness by day** – set the LED brightness percentage value for the day mode.

> **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 Card Reader



Basic Settings

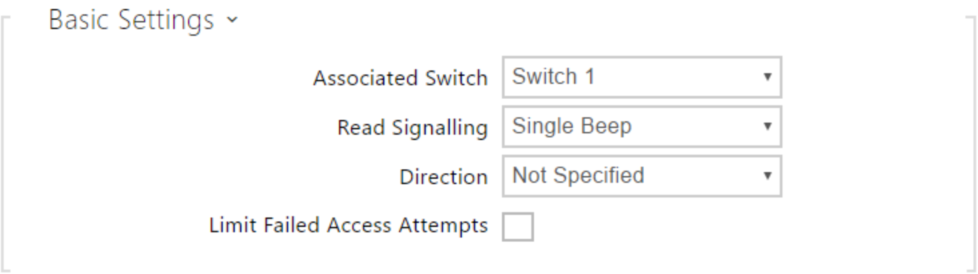
Associated Switch: Switch 1
Read Signalling: Full
Direction: Not Specified
Limit Failed Access Attempts: □

RFID Interface

Allowed Card Types: [all]

The card reader helps you control access to your building effectively using contactless RFID cards. The supported card types depend on the card reader model used.

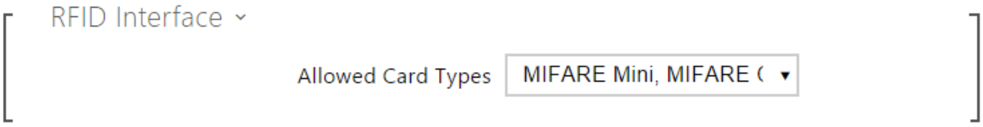
List of Parameters



Basic Settings

Associated Switch: Switch 1
Read Signalling: Single Beep
Direction: Not Specified
Limit Failed Access Attempts: □

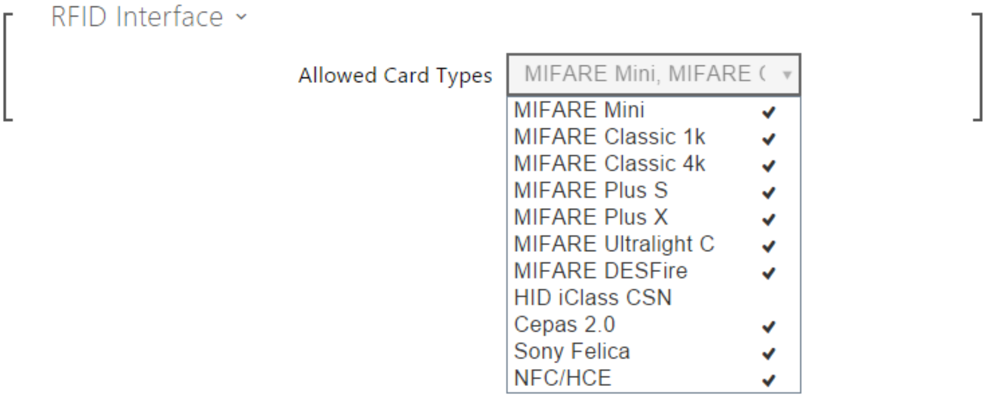
- **Associated switch** – select a switch to be activated whenever a valid card is applied. The set value is not applied when a valid user card is tapped on the reader while the double authentication mode is enabled. In this case, a numeric switch activating code is required to identify the switch to be activated.
- **Card read signalling** – set one of the card reading signalling modes: **Full** – acoustic signals distinguish valid/invalid cards, **Single beep** - one beep signals both valid and invalid cards, **None** – acoustic signalling is disabled.
- **Direction** – set direction to be writen in system: **Not Specified/In/Out**
- **Limit Failed Access Attempts** – the card reader will be blocked (reject all card) for thirty seconds after five unsuccesful access attempts



RFID Interface

Allowed Card Types: MIFARE Mini, MIFARE (

- **RFID Interface** – allows to choose the permitted types of cards (select/unselect).



RFID Interface

Allowed Card Types: MIFARE Mini, MIFARE (

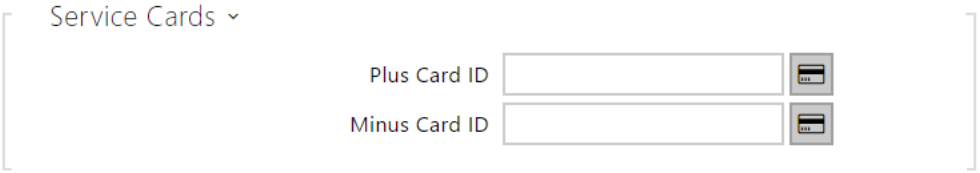
MIFARE Mini	✓
MIFARE Classic 1k	✓
MIFARE Classic 4k	✓
MIFARE Plus S	✓
MIFARE Plus X	✓
MIFARE Ultralight C	✓
MIFARE DESFire	✓
HID iClass CSN	
Cepas 2.0	✓
Sony Felica	✓
NFC/HCE	✓

Service Cards

Service cards are two common cards that are dedicated to this particular purpose by you. Be sure to complete their IDs in the Plus card ID and Minus card ID items in this section. The count of access card ID characters is given by the card type and is variable. However, it holds true that all cards of the same type have equally long IDs.

To add a card to the list, apply the plus card and then tap the card to be added on the reader. The RFID card will be added if the list in not full and does not include the card yet.

To remove a card from the list, apply the minus card and then tap the card to be removed on the reader. The RFID card record will be cancelled and access via this card will be blocked.



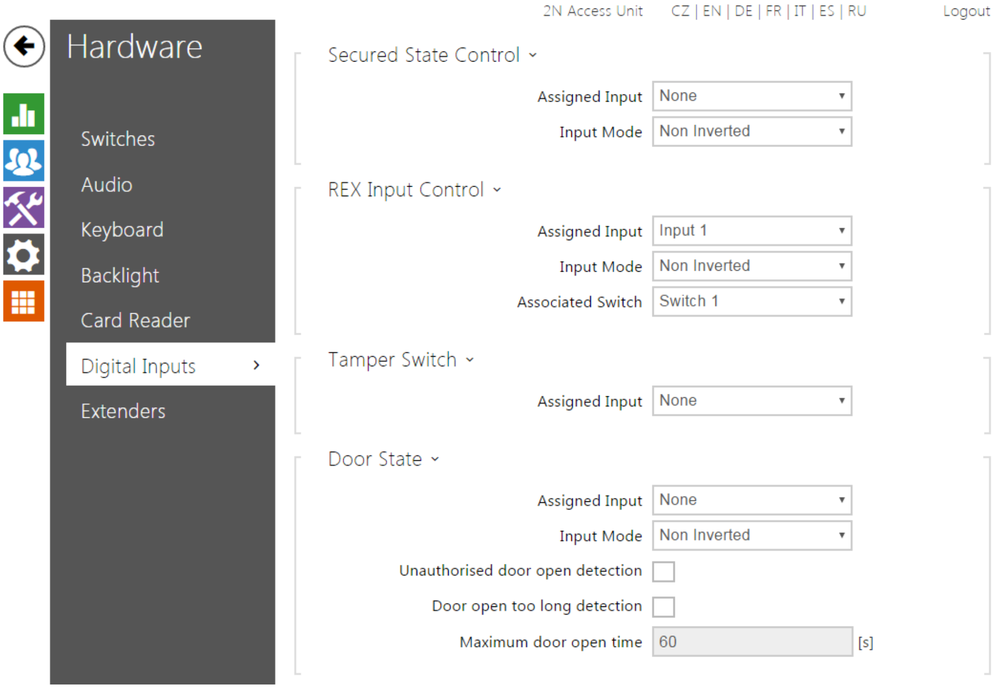
Service Cards

Plus Card ID

Minus Card ID

- **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

5.3.6 Digital Inputs



Secured State Control

Assigned Input	None
Input Mode	Non Inverted

REX Input Control

Assigned Input	Input 1
Input Mode	Non Inverted
Associated Switch	Switch 1

Tamper Switch

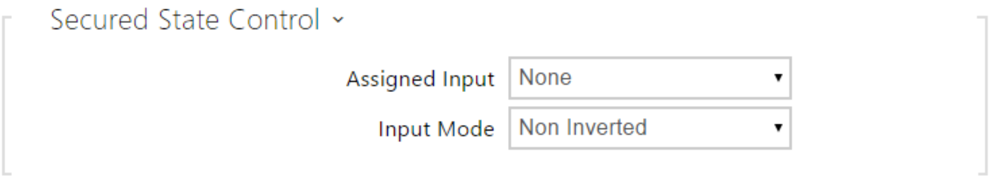
Assigned Input	None

Door State

Assigned Input	None
Input Mode	Non Inverted
Unauthorised door open detection	□
Door open too long detection	□
Maximum door open time	60 [s]

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

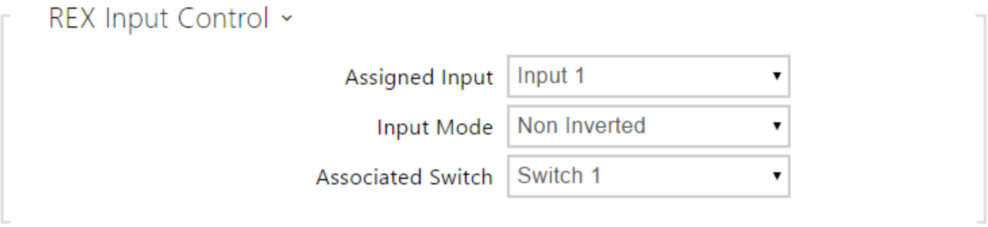
List of Parameters



Secured State Control

Assigned Input	None
Input Mode	Non Inverted

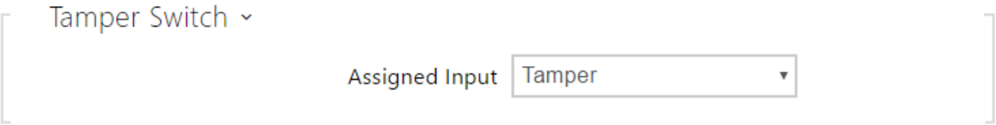
- **Assigned input** – define one (or none) of the logical inputs for secured state detection. The secured state is then signalled by a red LED on the **2N$^{®}$ Access Unit**.
- **Input mode** – set the active level of the input (polarity).



REX Input Control

Assigned Input	Input 1
Input Mode	Non Inverted
Associated Switch	Switch 1

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

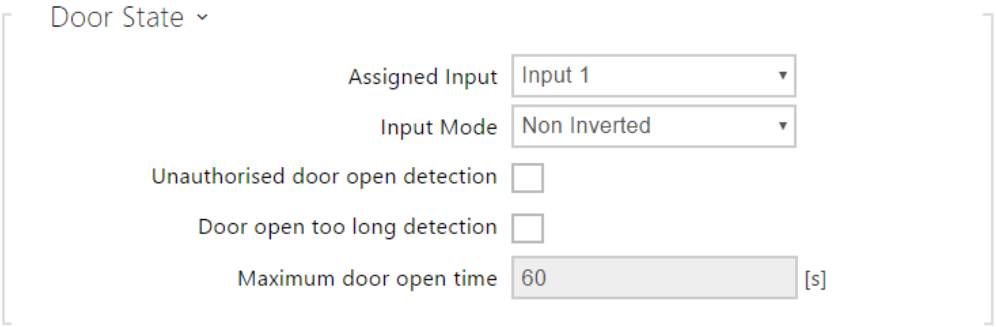


Tamper Switch

Assigned Input: Tamper

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 **2N® Helios IP HTTP API** manual).

- **Assigned input** – select the logical input to which the tamper switch is to be connected. **TamperSwitchActivated** signals the tamper switch activation.



Door State

Assigned Input: Input 1

Input Mode: Non Inverted

Unauthorised door open detection: □

Door open too long detection: □

Maximum door open time: 60 [s]

The models equipped with one digital input at least help connect an open door sensor and signal any unauthorised door opening or door closing failure with a timeout. The events are written into a log and read out using HTTP API (refer to the **2N® Helios IP HTTP API** manual).

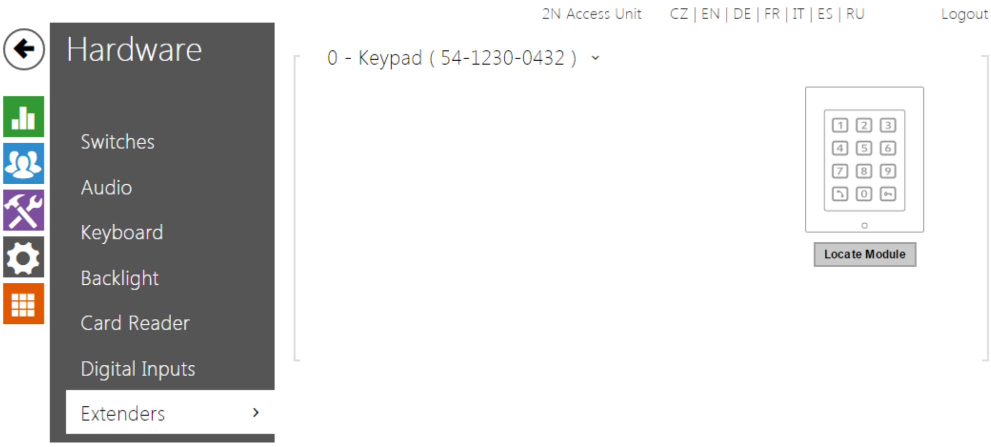
- **Assigned input** – assign one logical input to the door open sensor.
- **Input mode** – set the input active mode (polarity).
- **Unathorised door open detection** – enable **UnauthorisedDoorOpen** signalling. This event is signalled if the door opens when the electric lock is inactive.
- **Door open too long detection** – enable **DoorOpenTooLong** signalling. This event is signalled if the door is blocked open longer than as defined.
- **Maximum door open time** – set the maximum door opening timeout after which the DoorOpenTooLong state is detected.

Note

Menu Digital Inputs is available for models:

- 2N® Helios IP Verso
- 2N® Helios IP Vario and 2N® Helios IP Force if an internal card reader is installed
- 2N® Access Unit

5.3.7 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
- Fingerprint reader
- I/O module
- Wiegand module

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

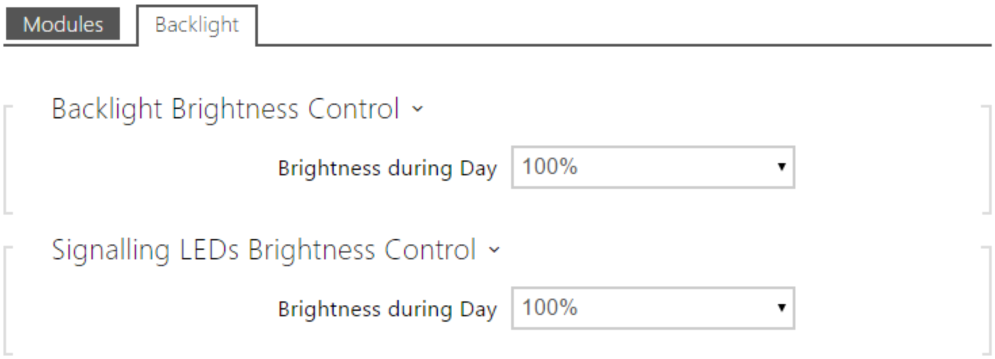
You can configure each module separately. The parameters are specific for the given module type .

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.*

Backlight Brightness

This tab helps you control the backlight level of name tags, buttons and brightness of signalling LEDs.



Backlight Brightness Control

Brightness during Day: 100%

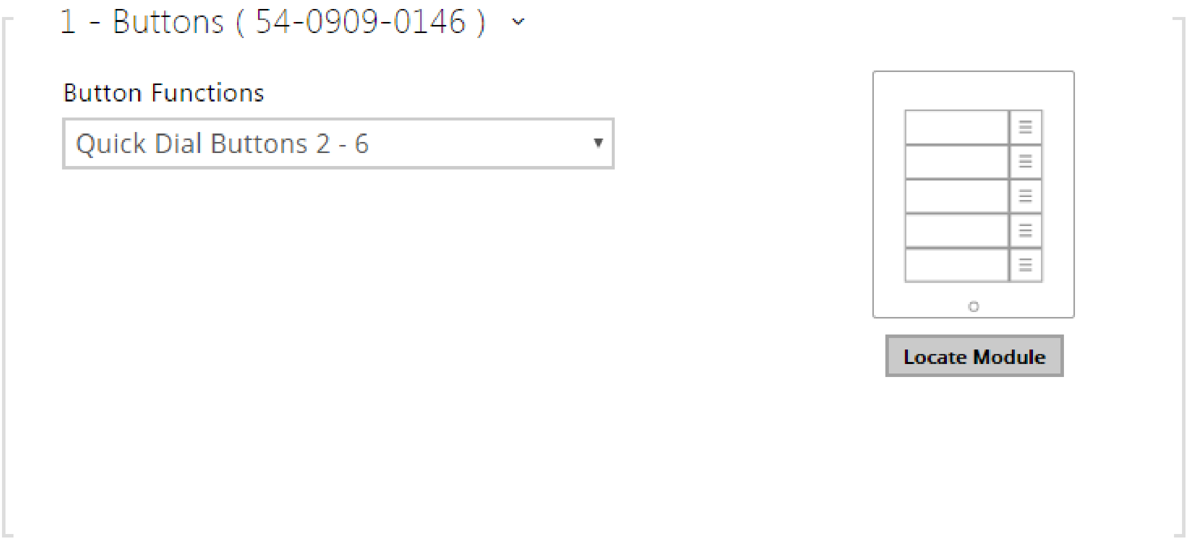
Signalling LEDs Brightness Control

Brightness during Day: 100%

Note

- The brightness parameters affect the function, power consumption and general appearance of your device. Extremely high name tag and button backlight values may, if the ambient light level is low, dazzle the persons standing in front of the **2N® Access Unit** and, in general, increase the power consumption of the device. An excessively 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.

Button Module Configuration

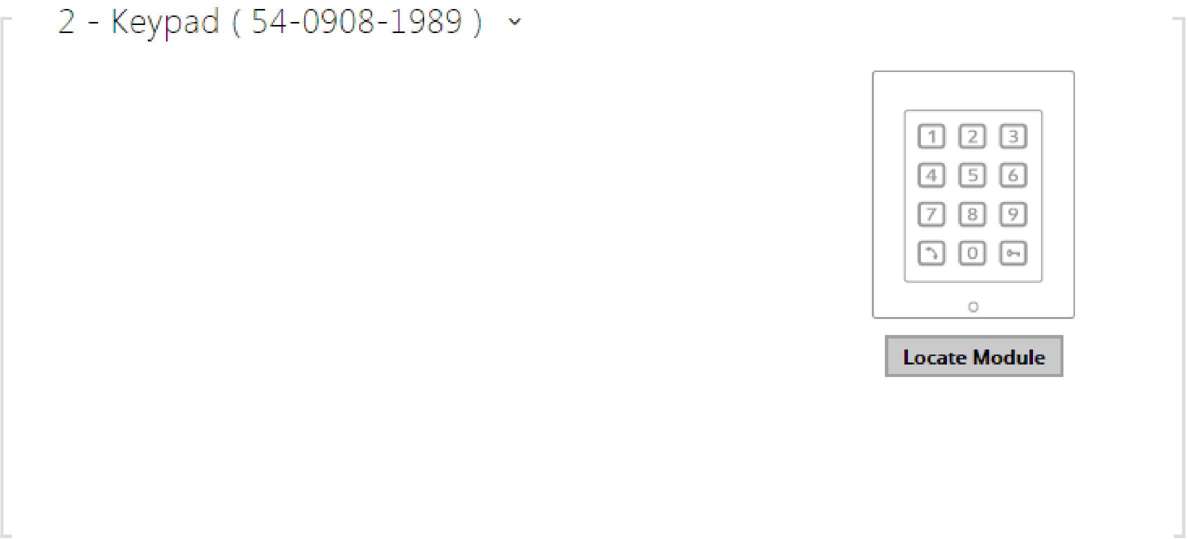


1 - Buttons (54-0909-0146)

Button Functions: Quick Dial Buttons 2 - 6

- Button functions – assign user positions to the buttons.

Keypad Module Configuration

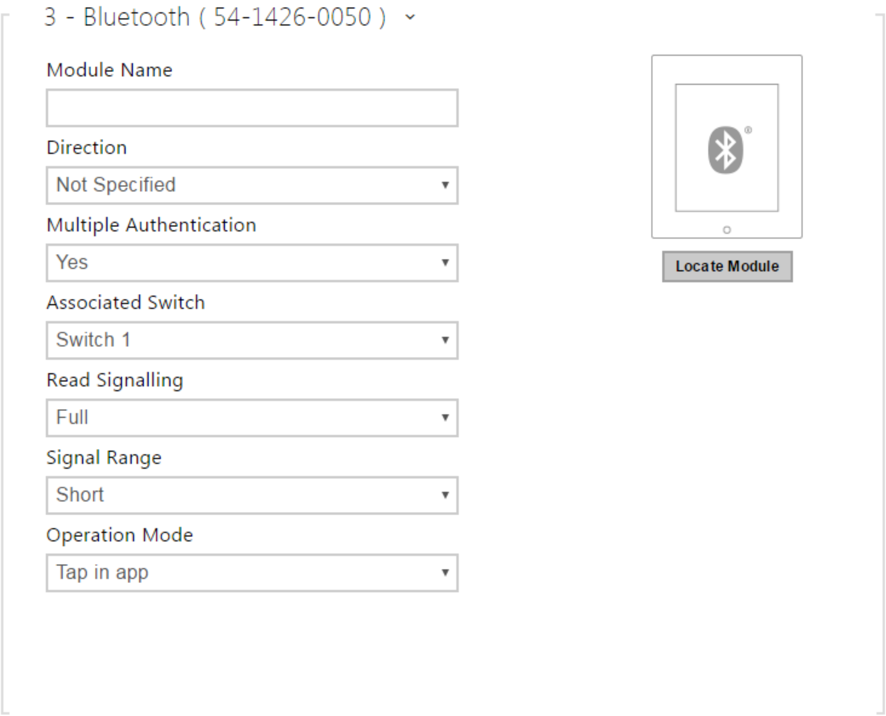


- No parameters are available to the public at present.

Infopanel Module Configuration

- No parameters are available to the public at present.

Card Reader Module Configuration



3 - Bluetooth (54-1426-0050)

Module Name

Direction: Not Specified

Multiple Authentication: Yes

Associated Switch: Switch 1

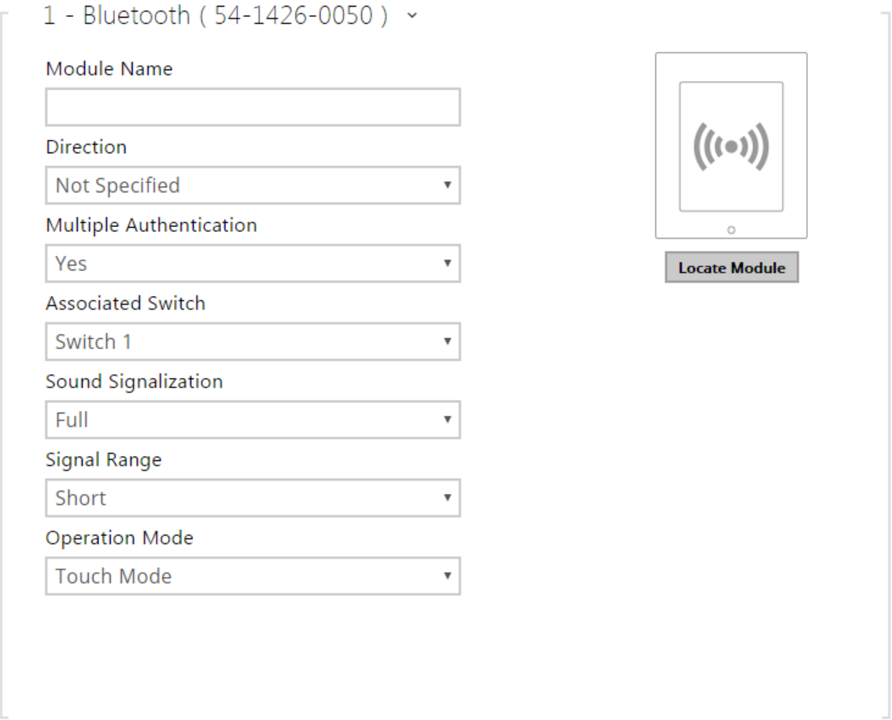
Read Signalling: Full

Signal Range: Short

Operation Mode: Tap in app

- **Module name** - set the module name for card reader logging purposes.
- **HID card format** - set the type of HID Prox card to be accepted by the card reader. The card reader supports just one card type at an instant. This setting is not applied if you do not use the HID Prox cards. (The parameters is available for 125kHz card readers only).
- **Associated switch** – set the number of the switch to be activated by tapping of a valid RFID card. The set value is not applied when a valid user card is tapped on the reader while the double authentication mode is enabled. In this case, a numeric switch activating code is required to identify the switch to be activated.
- **Card read signalling** – set one of the card reading signalling modes: **Full** – acoustic signals distinguish valid/invalid cards, **Single beep** – one beep signals both valid and invalid cards, **None** – acoustic signalling is disabled.
- **Forward to Wiegand output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resent.

Bluetooth Module



1 - Bluetooth (54-1426-0050)

Module Name

Direction: Not Specified

Multiple Authentication: Yes

Associated Switch: Switch 1

Sound Signalization: Full

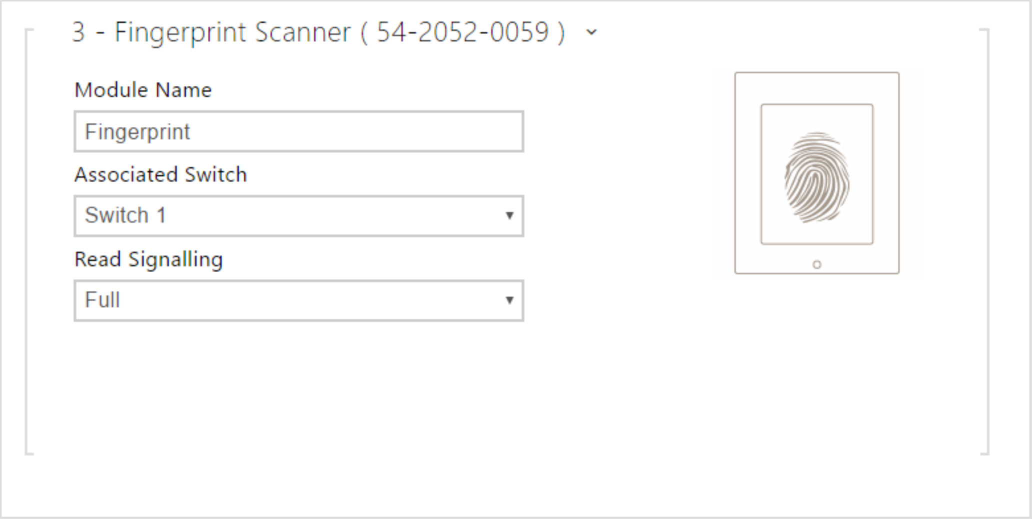
Signal Range: Short

Operation Mode: Touch Mode

- **Module name** – set the module name for logging events from the Bluetooth module.
- **Direction** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Multiple authentication** – enable multiple user authentication via this module (or, authentication is controlled by the user card settings; refer to Directory / Users). Multiple authentication can be disabled for each reader connected to the intercom.
- **Associated switch** – set the number of the switch to be activated after user authentication via this module.
- **Sound signalling** – set one of the sound signalling modes for the module:
  - **Full** – valid and invalid accesses are distinguished by sound signalling
  - **Single beep** – valid and invalid accesses are signalled by a single beep
  - **None** – module use is not signalled by any sound
- **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 50 cm for most phones
  - **Middle** – less than 2 m for most phones
  - **Long** – maximum possible range
- **Operation mode** – set the authentication method for a mobile phone:

- **Tap in app** – authentication has to be confirmed by tapping on an icon in the application running in a mobile phone
- **Touch mode** – authentication has to be confirmed by moving the hand to the Bluetooth module installed
- **Proximity mode** – authentication is executed automatically when the mobile phone is within the Bluetooth module signal reach

Fingerprint Reader Module Configuration



3 - Fingerprint Scanner (54-2052-0059)

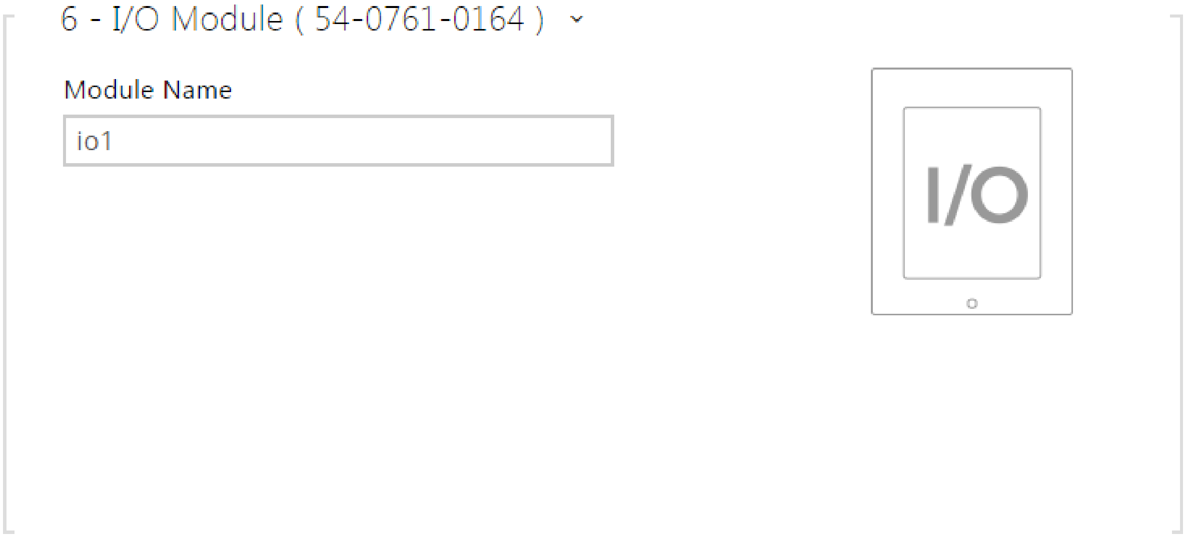
Module Name: Fingerprint

Associated Switch: Switch 1

Read Signalling: Full

- **Module name** – set the module name for logging events from the Fingerprint reader.
- **Associated switch** – set the number of the switch to be activated whenever a valid code is received .
- **Read Signalling** – set one of the card reading signalling modes
  - **Full** – acoustic signals distinguish valid/invalid cards
  - **Single Beep** – one beep signals both valid and invalid cards
  - **None** – acoustic signalling is disabled.

I/O Module Configuration



6 - I/O Module (54-0761-0164)

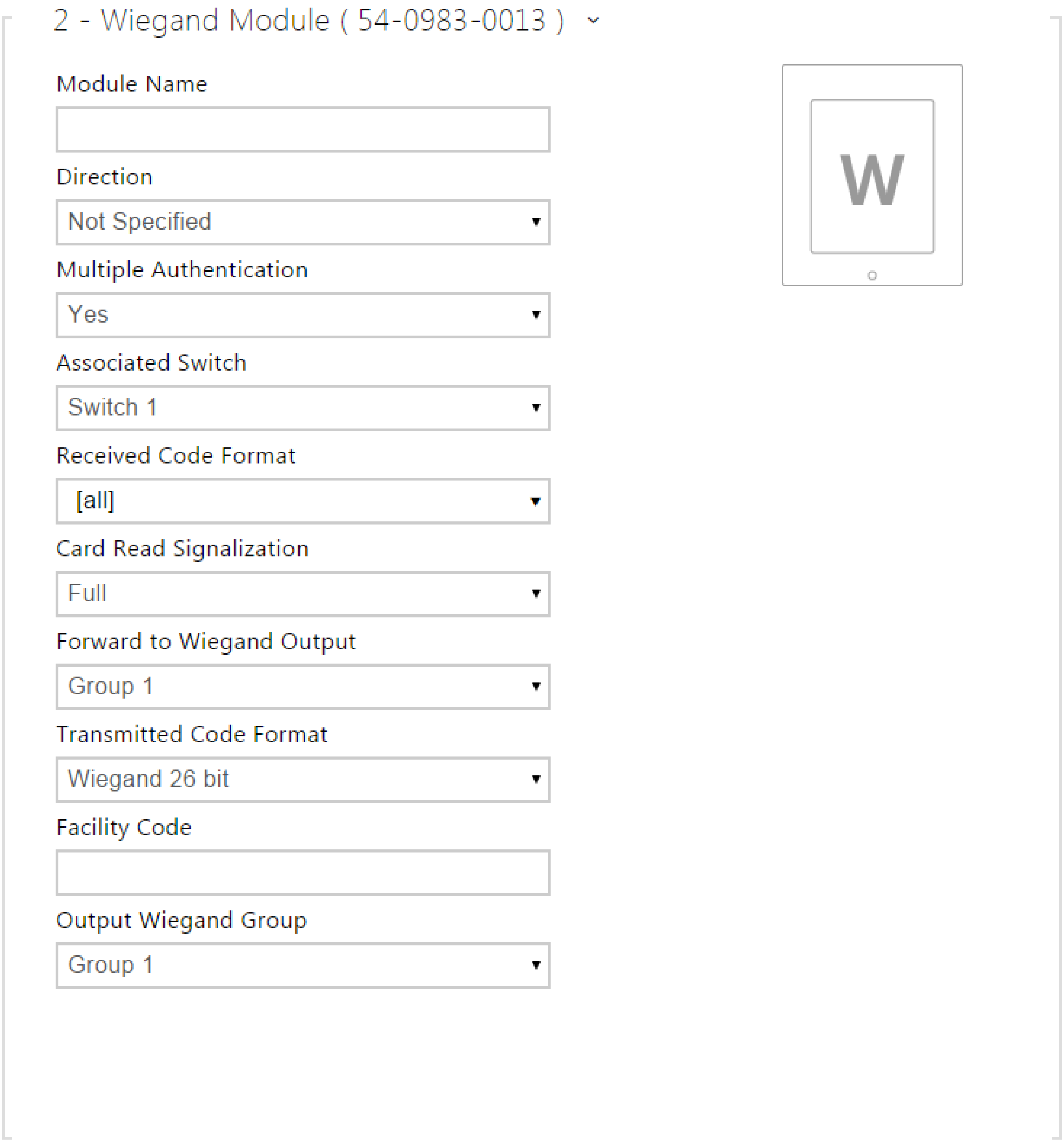
Module Name

io1

- **Module name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N® Helios IP Automation** settings.

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 **2N® Access Unit** 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 Wiegand module is also equipped with one logical input and one logical output, which can be controlled via **2N® Helios IP Automation**.



2 - Wiegand Module (54-0983-0013) ˅

Module Name	
Direction	Not Specified ▾
Multiple Authentication	Yes ▾
Associated Switch	Switch 1 ▾
Received Code Format	[all] ▾
Card Read Signalization	Full ▾
Forward to Wiegand Output	Group 1 ▾
Transmitted Code Format	Wiegand 26 bit ▾
Facility Code	
Output Wiegand Group	Group 1 ▾

- **Module name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N® Helios IPAutomation**.
- **Associated switch** – set the number of the switch to be activated whenever a valid code is received.
- **Received code format** – set the format for the codes to be received (Wiegand 26, 32, 37 and RAW).
- **Card read signalling** – set one of the card reading signalling modes: **Full** – acoustic signals distinguish valid/invalid cards, **Single beep** – one beep signals both valid and invalid cards, **None** – acoustic signalling is disabled.

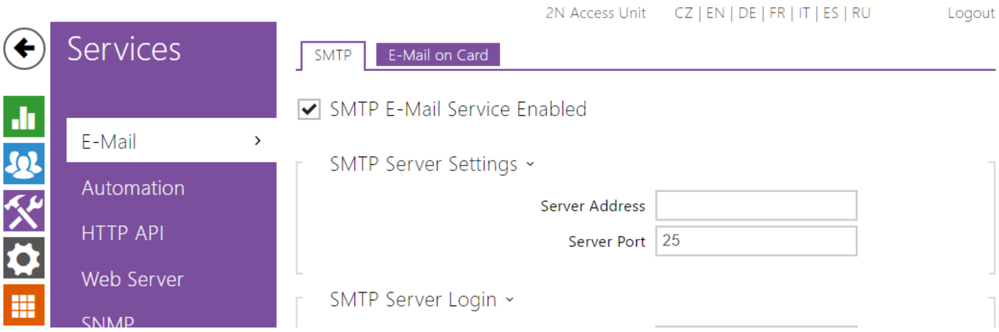
- **Forward to Wiegand output** – set the group of Wiegand outputs to which all the received codes shall be resent.
- **Transmitted code format** – set the format for the codes to be transmitted (Wiegand 26, 32, 37 and RAW).
- **Output Wiegand group** – assign the output Wiegand to a group to which the codes from the connected card readers or Wiegand inputs can be resent.

5.4 Services

Here is what you can find in this section:

- 5.4.1 E-mail
- 5.4.2 Mobile Key
- 5.4.3 Automation
- 5.4.4 HTTP API
- 5.4.5 Web Server
- 5.4.6 SNMP

5.4.1 E-mail



☑ SMTP E-Mail Service Enabled

Server Address

Server Port 25

To inform the intercom users on all missed and/or successfully completed calls, configure **2N Helios IP** 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.

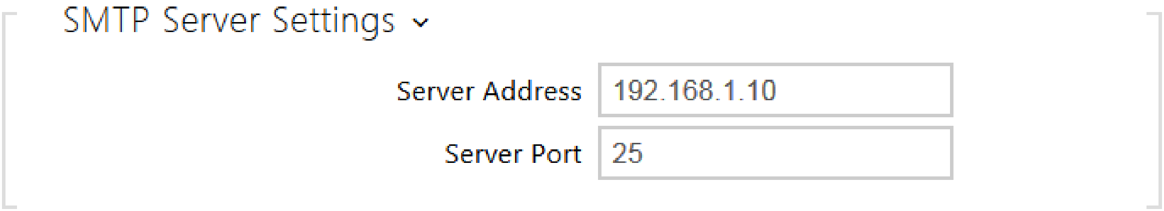
> **Note**
>
> - *The E-mail function is available with the Gold or Enhanced Integration licence only.*

List of Parameters

SMTP

☑ SMTP Service Enabled

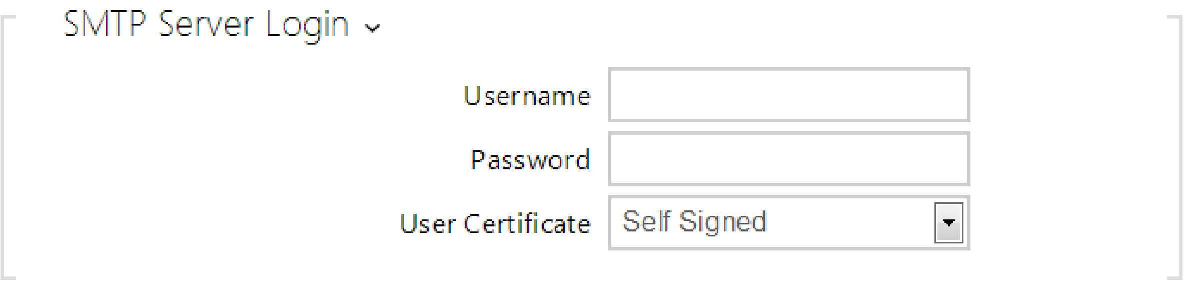
- **SMTP service enabled** – enable/disable sending e-mails from the intercom.



SMTP Server Settings ⌄

Server Address	192.168.1.10
Server Port	25

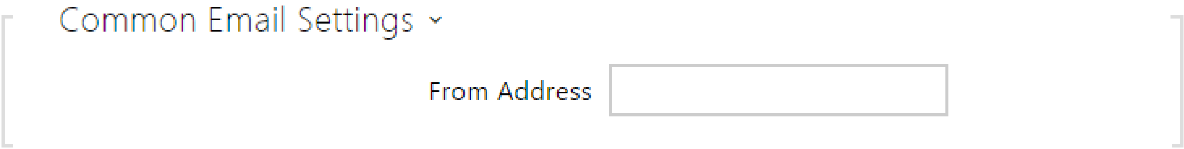
- **Server address** – set the SMTP server address to which e-mails shall be sent.
- **Server port** – specify the SMTP server port. Modify the value only if the SMTP server setting is substandard. The typical SMTP port value is 25.



SMTP Server Login ⌄

Username	
Password	
User Certificate	Self Signed ▾

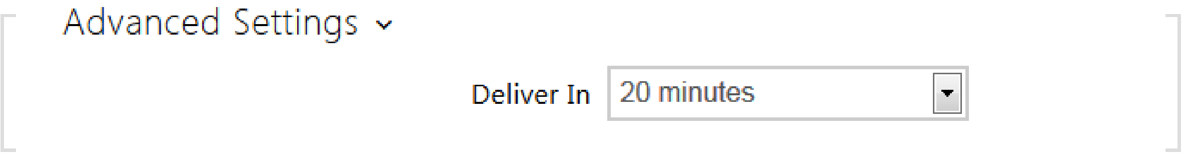
- **Username** – enter a valid username for login if the SMTP server requires authentication, or leave the field empty if not.
- **Password** – enter the SMTP server login password.
- **User certificate** – specify the user certificate and private key for the intercom – SMTP server communication encryption.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



Common Email Settings ⌄

From Address	

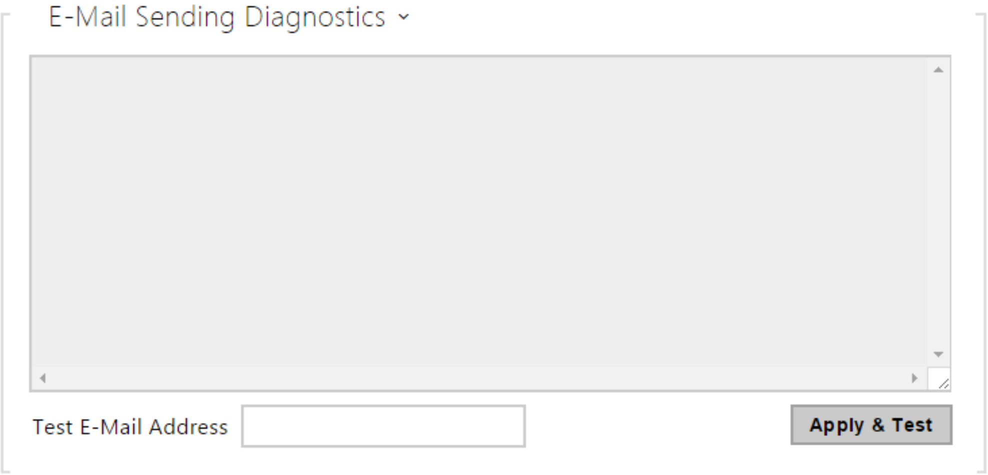
- **From address** – set the sender address for all outgoing e-mails from the device.



Advanced Settings ⌄

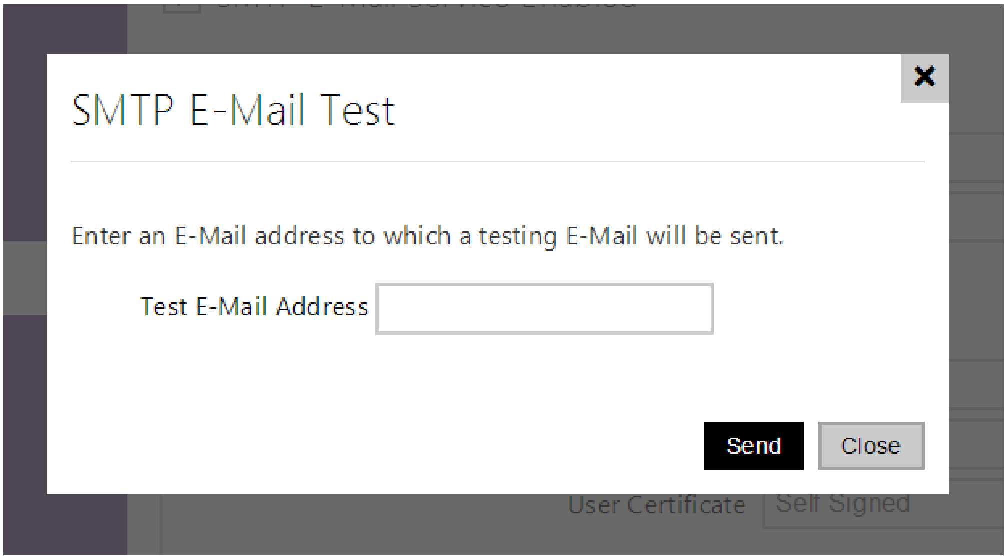
Deliver In	20 minutes ▾

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


E-Mail Sending Diagnostics ˅

Test E-Mail Address

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.

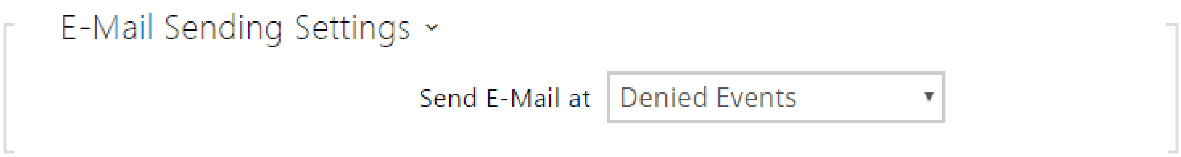

SMTP E-Mail Test

Enter an E-Mail address to which a testing E-Mail will be sent.

Test E-Mail Address

E-mail on Card

Set e-mail sending whenever a RFID card is tapped on the card reader on this tab.

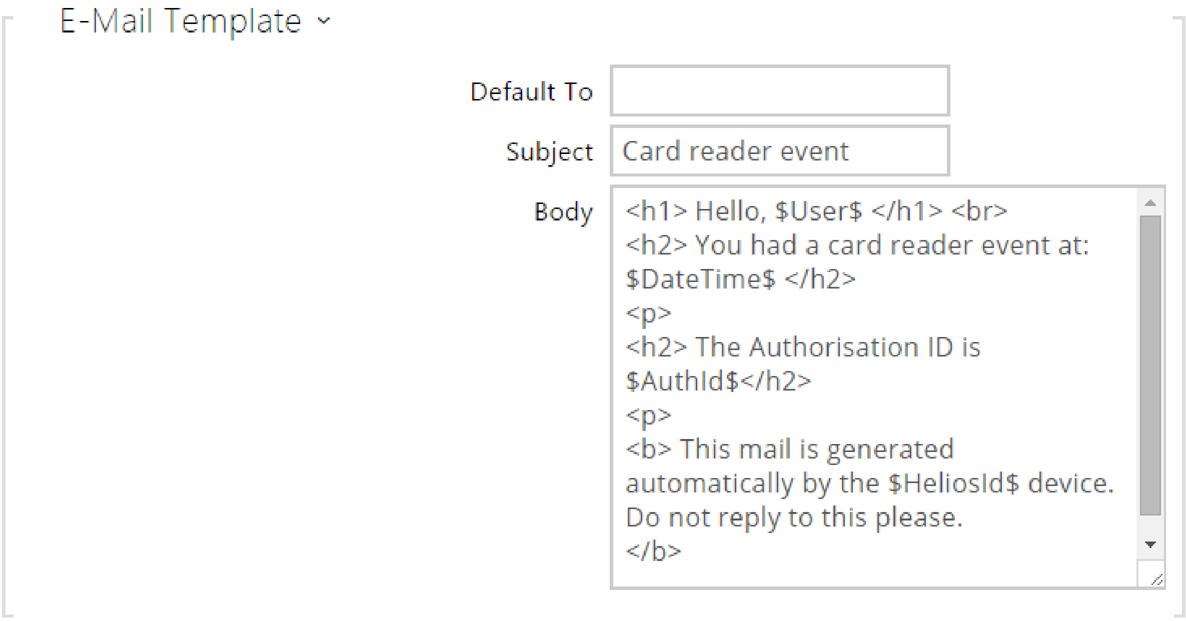


E-Mail Sending Settings ˅

Send E-Mail at: Denied Events ▾

Send E-mail at – set e-mail sending whenever a RFID card is tapped on the card reader. The following options are available:

- Denied events – e-mail shall be sent when an invalid RFID card is applied.
- All events – e-mail shall be sent when any card is applied.
- Never – e-maily shall not be sent.



E-Mail Template ˅

Default To:

Subject: Card reader event

Body:

```
<h1> Hello, $User$ </h1> <br>
<h2> You had a card reader event at:
$DateTime$ </h2>
<p>
<h2> The Authorisation ID is
$AuthId$</h2>
<p>
<b> This mail is generated
automatically by the $HeliosId$ device.
Do not reply to this please.
</b>
```

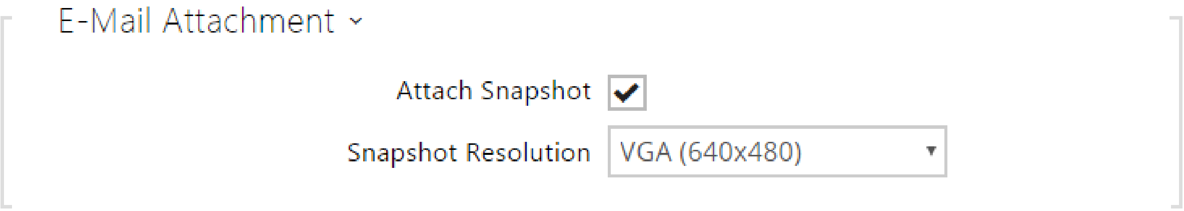
- **Default to** – the intercom sends messages to the e-mail address specified for the user when a valid user card is applied. When an invalid card is applied or no e-mail address is assigned to the user, the message shall be sent the e-mail address included here. If the receiver is included neither in the phone book nor in this parameter, no e-mail shall be sent. You can set more e-mail addresses separated with a comma if necessary.
- **Subject** – set the e-mail subject to be sent.
- **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 identification or authentication ID, which will be replaced with the actual value before sending. Refer to the table of substitute symbols below:

1.
   a. $User$ Called username

   b. $DateTime$ Current date and time

c. $AuthId$ User authentication ID

d. $HeliosId$ Intercom identification



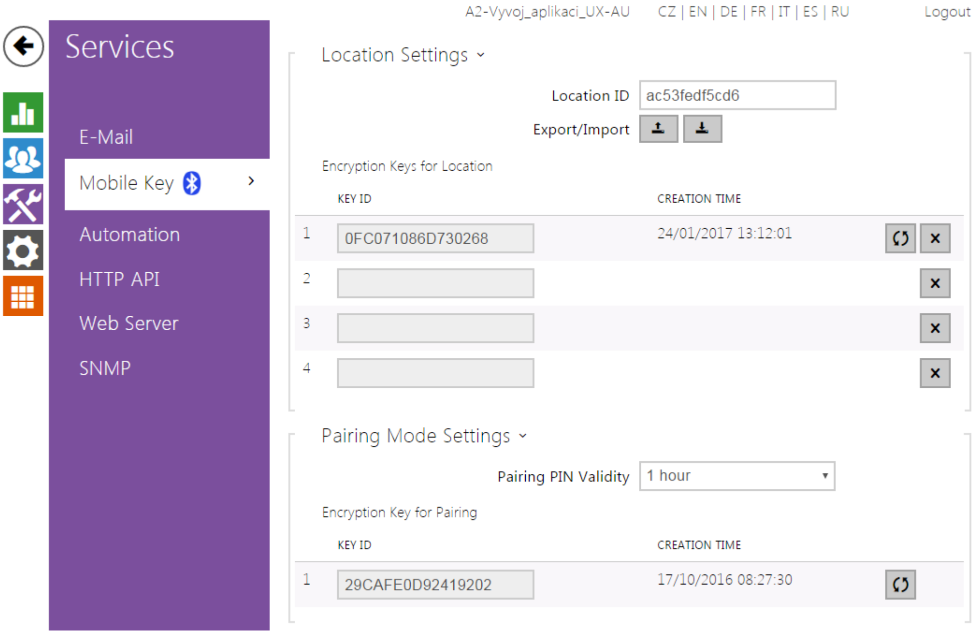
E-Mail Attachment

Attach Snapshot ☑

Snapshot Resolution VGA (640x480)

- **Attach snapshot** – enable sending of an attachment including one camera snapshot taken during ringing or calling.
- **Snapshot resolution** – set the snapshot resolution for the image to be sent.

5.4.2 Mobile Key



Location Settings

Location ID: ac53fedf5cd6

Export/Import

Encryption Keys for Location

	KEY ID	CREATION TIME
1	0FC071086D730268	24/01/2017 13:12:01
2		
3		
4		

Pairing Mode Settings

Pairing PIN Validity: 1 hour

Encryption Key for Pairing

	KEY ID	CREATION TIME
1	29CAFE0D92419202	17/10/2016 08:27:30

The 2N® Access Unit equipped with the Bluetooth module allow for user authentication via the 2N® **Mobile Key** application available to devices with iOS 8.1 and higher (iPhone 4 s and higher phones) or Android 4.4 KitKat 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.

Poznámka

- 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.

Poznámka

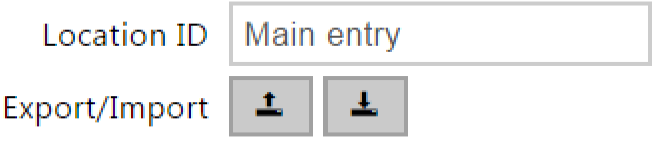
- The encryption keys are generated automatically upon the 2N® Access Unit first launch and saved into the 2N® Access Unit configuration file.

  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.

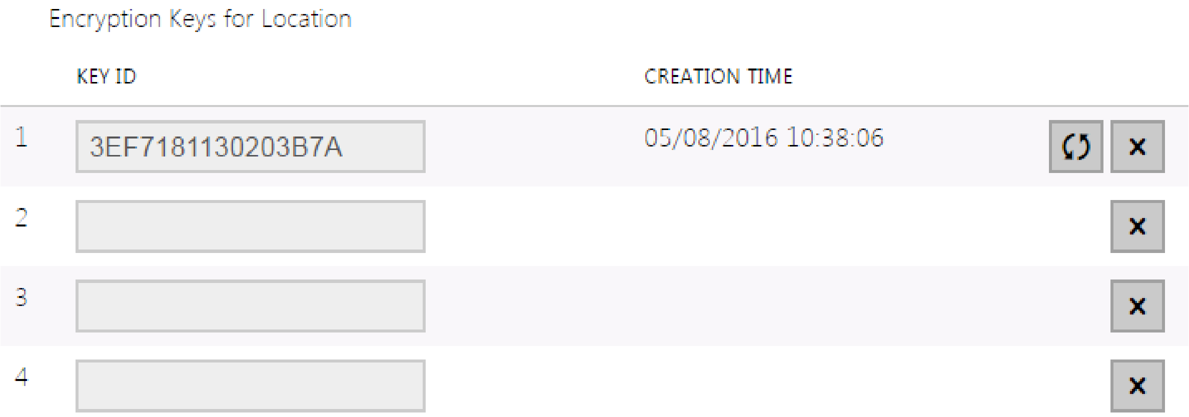
When a key is deleted, the 2N® Mobile Key users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the 2N® Mobile Key application.

List of Parameters



Location ID: Main entry

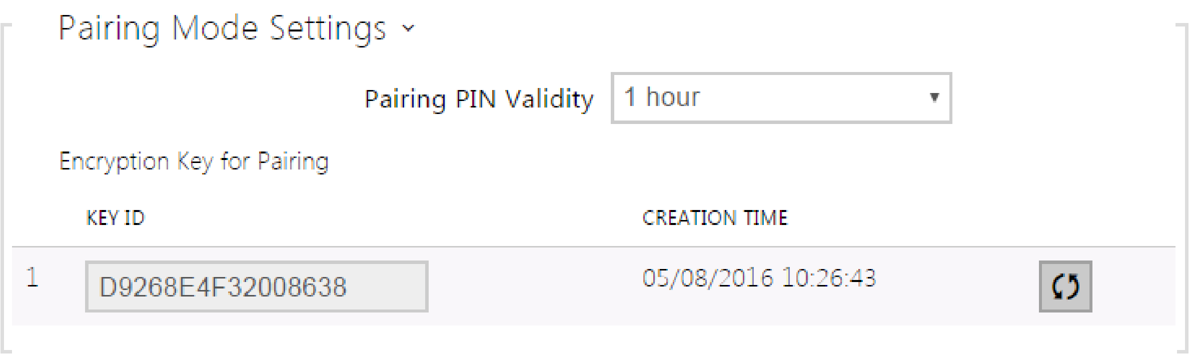
- **Location ID** – set a unique identifier for the location in which the selected encryption key set is valid.
- **Export** – push the button to export the location ID and current encryption keys into a file. Subsequently, the exported file can be imported to another device. Devices with identical location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



Encryption Keys for Location

	KEY ID	CREATION TIME	
1	3EF7181130203B7A	05/08/2016 10:38:06	⟳ ✕
2			✕
3			✕
4			✕

- **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 Mode Settings

Pairing PIN Validity: 1 hour

Encryption Key for Pairing

	KEY ID	CREATION TIME
1	D9268E4F32008638	05/08/2016 10:26:43

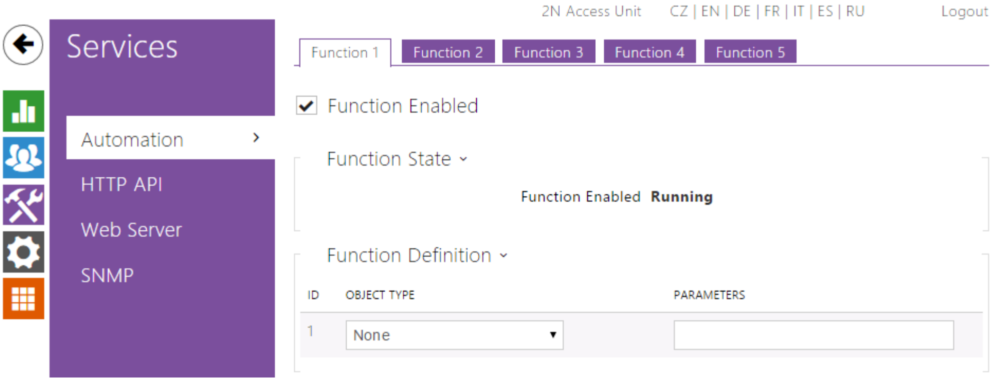
- **Pairing PIN validity** – set the authorisation PIN validity for user mobile device pairing with the **2N® Access Unit** .

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.

5.4.3 Automation



☑ Function Enabled

Function State

Function Enabled **Running**

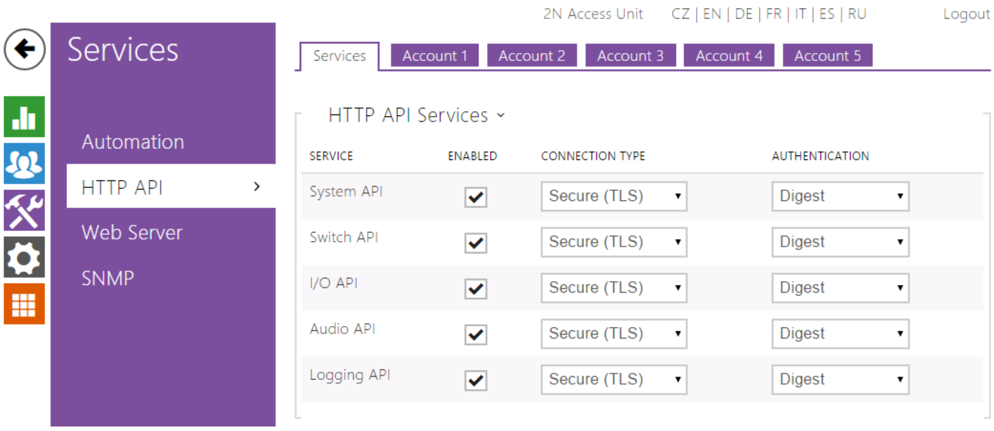
Function Definition

ID	OBJECT TYPE	PARAMETERS
1	None	

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**® **Helios IP Automation**. Typically, **2N**® **Helios IP Automation** is used in applications that require complex interconnections with third party systems.

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

5.4.4 HTTP API



HTTP API Services

SERVICE	ENABLED	CONNECTION TYPE	AUTHENTICATION
System API	☑	Secure (TLS)	Digest
Switch API	☑	Secure (TLS)	Digest
I/O API	☑	Secure (TLS)	Digest
Audio API	☑	Secure (TLS)	Digest
Logging API	☑	Secure (TLS)	Digest

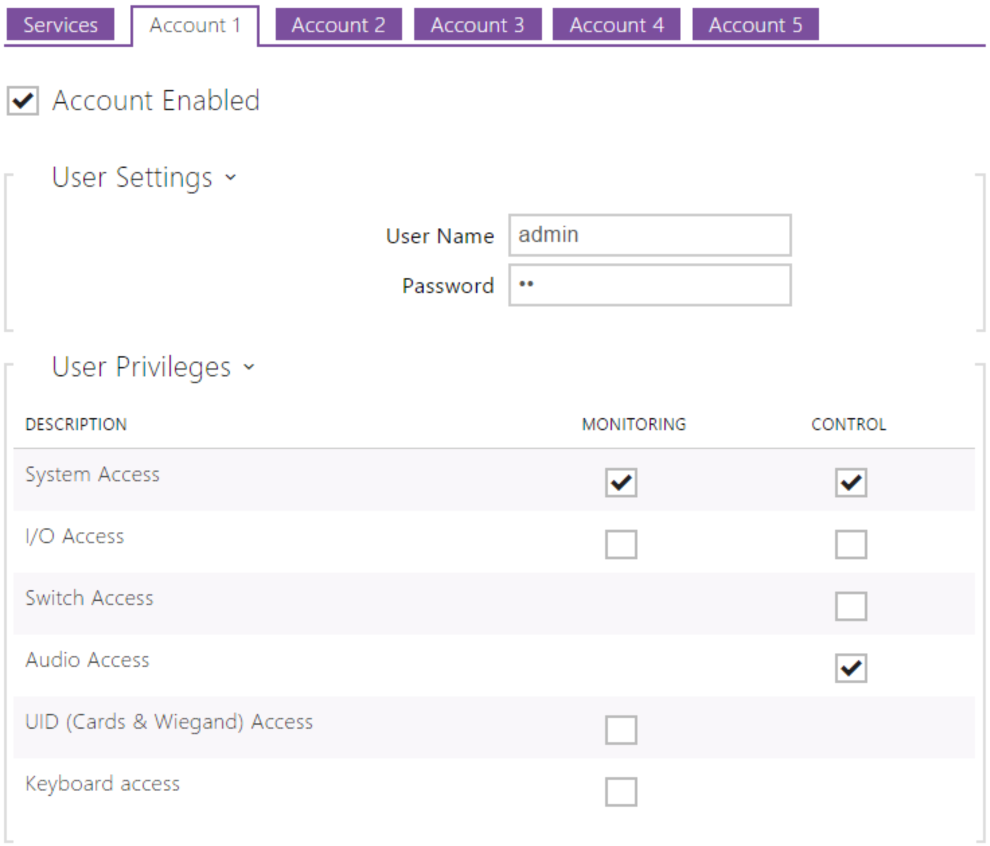
2N® **Helios IP HTTP API** is an application interface designed for control of selected **2N Helios IP** functions via the **HTTP**. It enables **2N Helios IP** intercoms to be integrated easily with third party products, such as home automation, security and monitoring systems, etc.

2N® **Helios IP HTTP API** provides the following services:

- **System API** – provides intercom configuration changes, status info and upgrade.
- **Switch API** – provides switch status control and monitoring, e.g. door lock opening, etc.
- **I/O API** – provides intercom logic input/output control and monitoring.
- **Audio API –** provides configuration of audio signalling.
- **Logging API – Logging API**

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.

Refer to the **2N® Helios IP HTTP API** Configuration Manual for the HTTP API function and configuration details.



☑ Account Enabled

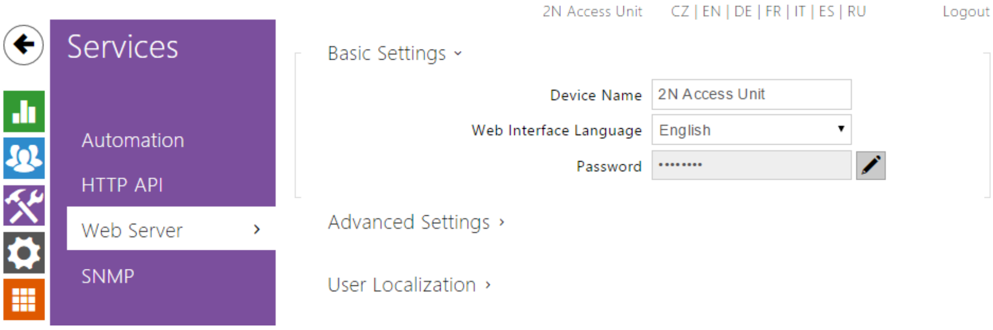
User Settings ˅

User Name	admin
Password	••

User Privileges ˅

DESCRIPTION	MONITORING	CONTROL
System Access	☑	☑
I/O Access	□	□
Switch Access		□
Audio Access		☑
UID (Cards & Wiegand) Access	□	
Keyboard access	□	

5.4.5 Web Server



Device Name: 2N Access Unit
Web Interface Language: English
Password: ••••••••

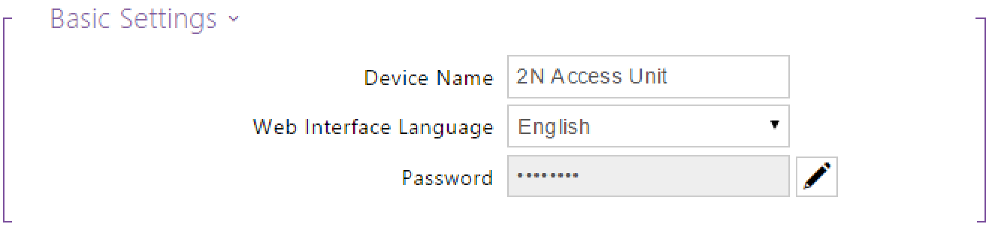
You can configure your **2N® Access Unit** using a standard browser with access to the integrated web server. Use the secured HTTPS protocol for communication between the browser and **2N® Access Unit**. Having accessed the intercom, enter the login name and password. The default login name and password 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® Helios IP Automation**; refer to the respective manual.

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

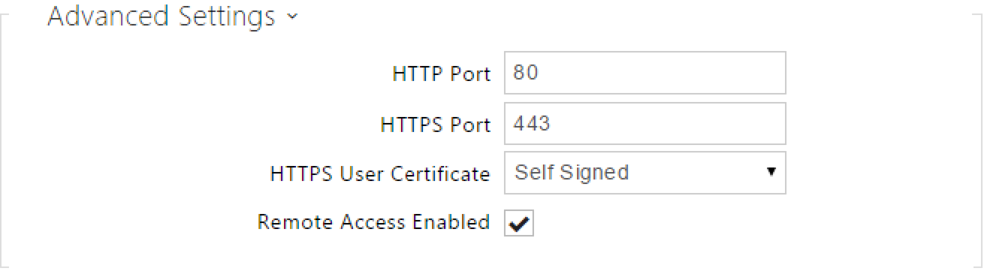
List of Parameters



Device Name: 2N Access Unit
Web Interface Language: English
Password: ••••••••

- **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® Helios IP Manager**, **2N® Helios 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.



Advanced Settings ˅

HTTP Port: 80

HTTPS Port: 443

HTTPS User Certificate: Self Signed ▾

Remote Access Enabled: ☑

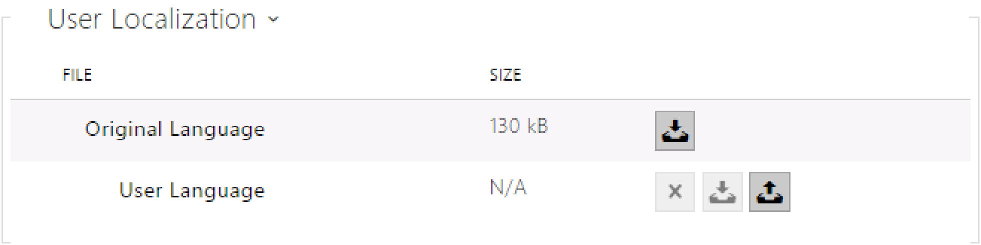
- **HTTP Port** – set the web server communication port via the unsecured HTTP.

  The port setting will not be applied until the **2N® Access Unit** gets restarted.

- **HTTPS Port** – set the web server communication port via the secured HTTPS.

  The port setting will not be applied until the **2N® Access Unit** gets restarted.

- **User Certificate** – specify the user certificate and private key for the **2N® Access Unit** 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 **Self Signed** 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.



User Localization ˅

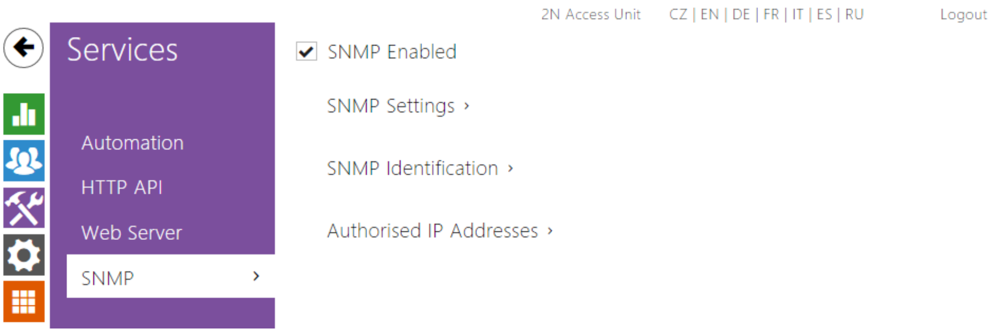
FILE	SIZE	
Original Language	130 kB	⭳
User Language	N/A	× ⭳ ⭱

- **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.

5.4.6 SNMP



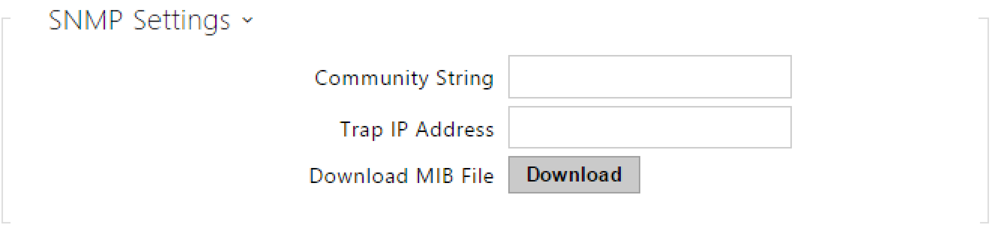
☑ SNMP Enabled

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

List of Parameters

☑ SNMP Enabled

- **SNMP Enabled** – Allows you to enable the SNMP function

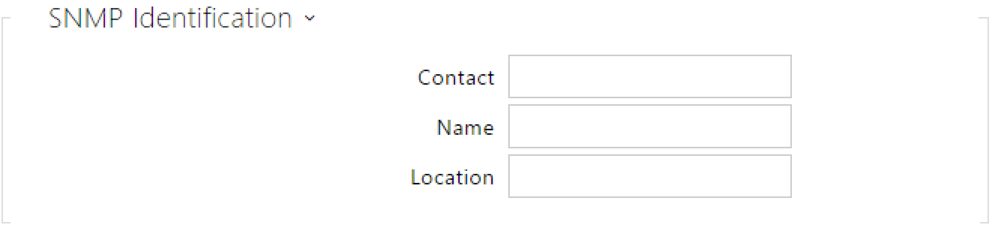


Community String

Trap IP Address

Download MIB File

- **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.



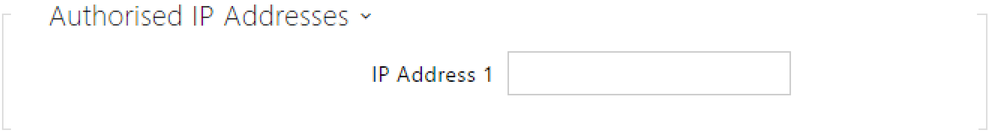
Contact

Name

Location

- **Contact** – enter the device manager contact (name, e-mail, etc.).

- **Name** – enter the device name.
- **Location** – enter the device location (1st floor, e.g.).



Authorised IP Addresses ˅

IP Address 1

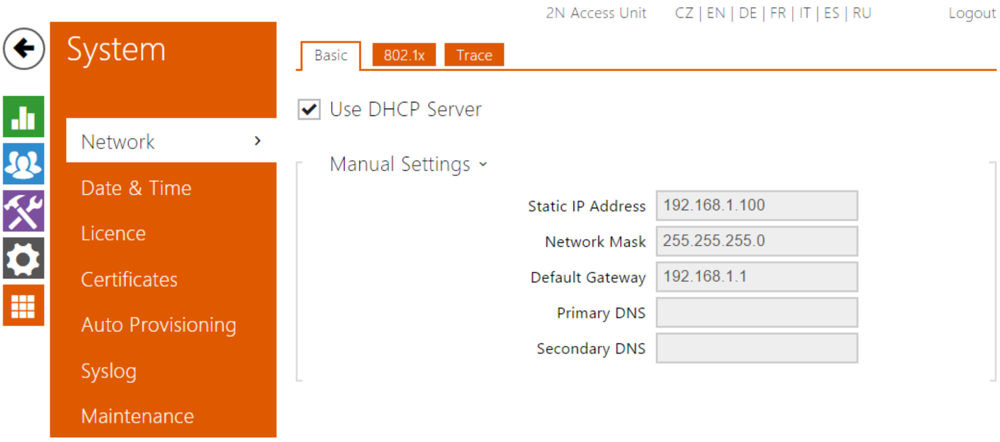
- **IP Address** – enter up to 4 valid IP addresses for SNMP agent access to block access from other addresses. If the field is empty, the device may be accessed from any IP address.

5.5 System

Here is what you can find in this section:

- 5.5.1 Network
- 5.5.2 Date and Time
- 5.5.3 Licence
- 5.5.4 Certificates
- 5.5.5 Auto Provisioning
- 5.5.6 Syslog
- 5.5.7 Maintenance

5.5.1 Network



☑ Use DHCP Server

Static IP Address	192.168.1.100
Network Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	
Secondary DNS	

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® Helios IP Scanner**, which can be freely downloaded from **www.2n.cz**, 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.*

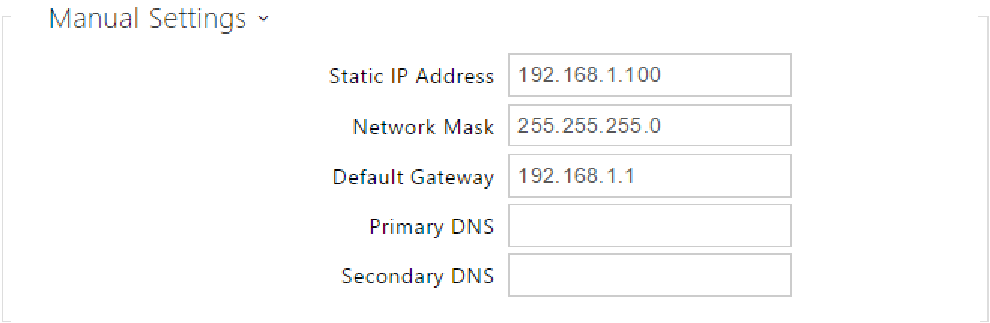
If you use the RADIUS server and 802.1x-based verification of connected equipment, you can make the intercom use the EAP-MD5 or EAP-TLS authentication. Set this function on the 802.1x tab.

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

- **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.

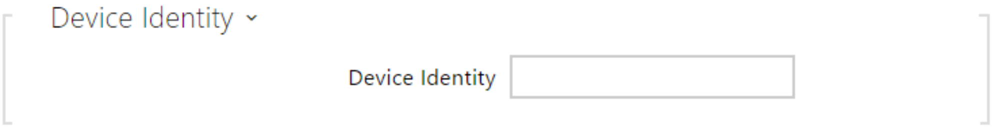


Manual Settings ˅

Static IP Address	192.168.1.100
Network Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	
Secondary DNS	

- **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.
- **Secondary DNS** – set the secondary DNS server address, which is used in case the primary DNS is inaccessible.

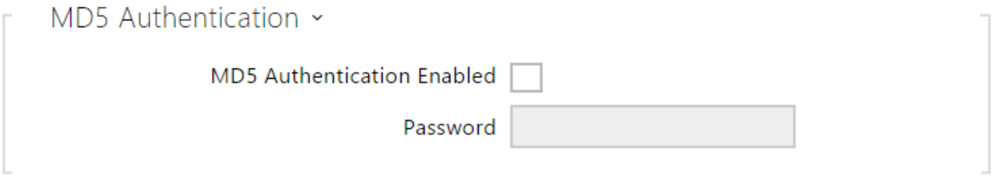
802.1x



Device Identity ˅

Device Identity	

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

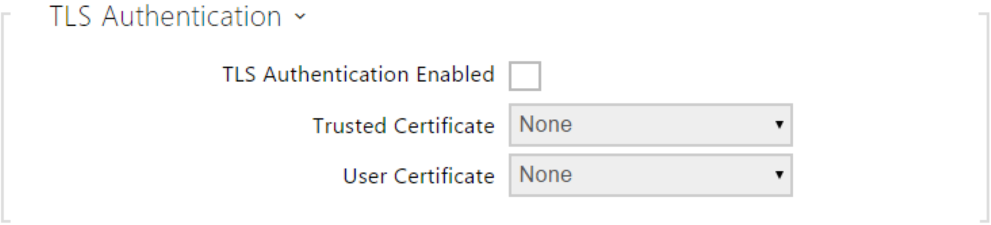


MD5 Authentication ˅

MD5 Authentication Enabled	□
Password	

- **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 ˅

TLS Authentication Enabled □

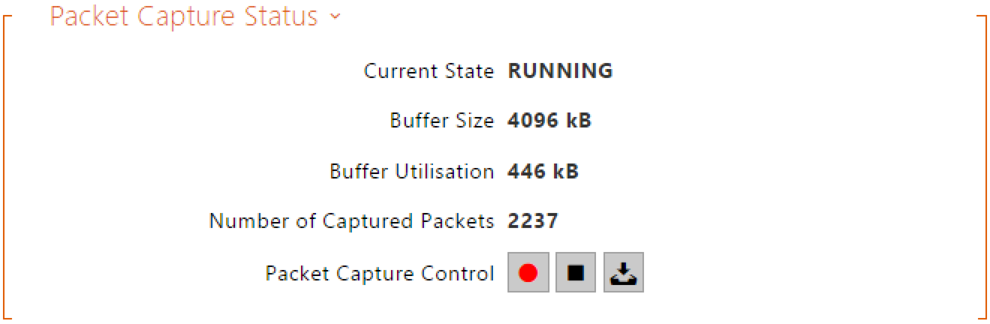
Trusted Certificate None ▾

User Certificate None ▾

- **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.

Trace

On the Trace tab, you can launch capturing of incoming and outgoing packets on the **2N® Access Unit** network interface. The captured packets are stored in a 4 MB buffer. When the buffer fills up, the oldest packets are overwritten automatically. We recommend you to lower the video stream transmission rate below 512 kbps while capturing. Press ● to start, ■ to stop and ⭳ to download the packet capture file.



Packet Capture Status ˅

Current State **RUNNING**

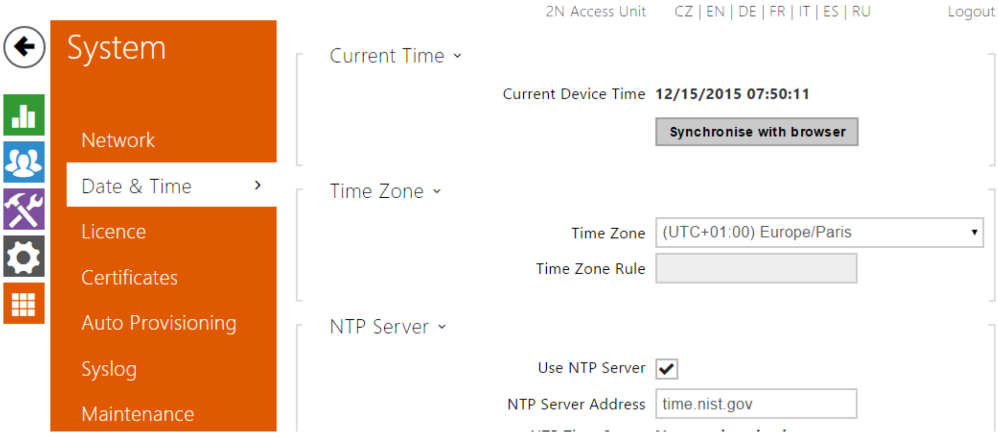
Buffer Size **4096 kB**

Buffer Utilisation **446 kB**

Number of Captured Packets **2237**

Packet Capture Control ● ■ ⭳

5.5.2 Date and Time



Current Device Time 12/15/2015 07:50:11

Time Zone (UTC+01:00) Europe/Paris

Time Zone Rule

Use NTP Server ☑

NTP Server Address time.nist.gov

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.

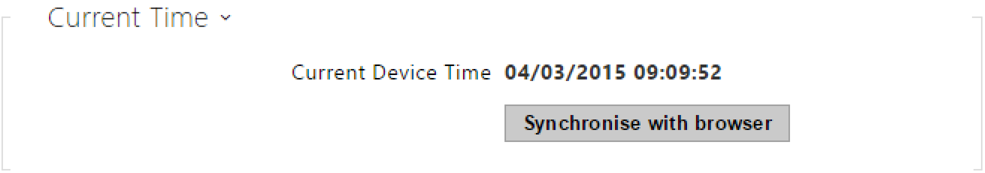
2N® **Access Unit** is equipped with a back-up real-time clock to withstand up to several days' long power outages. You can synchronise the 2N® **Access Unit** time with your PC anytime by pressing the **Synchronise** button.

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® **Helios IP** HTTP API, etc.).*

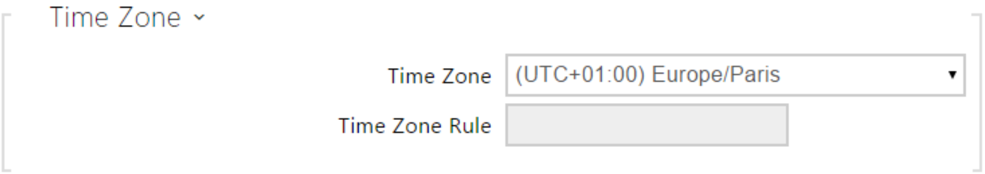
Practically, the 2N® **Access Unit** real-time circuit accuracy is approximately ±0,005 %, which may mean a deviation of ±2 minutes per month. Therefore, we recommend you to synchronise time with the NTP server to achieve the highest accuracy and reliability. The 2N® **Access Unit** sends a query to the NTP server periodically to update its time value.

List of Parameters



Current Device Time **04/03/2015 09:09:52**

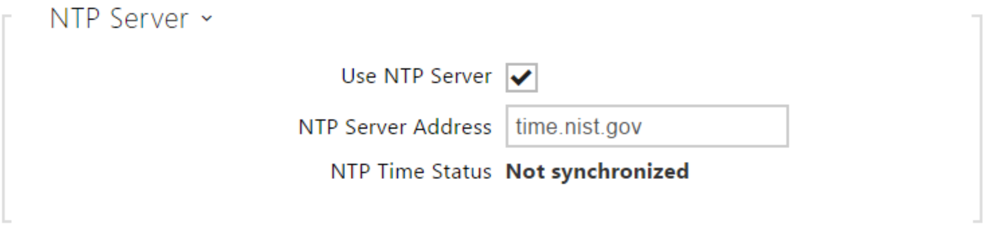
Synchronise – push the button to synchronise the **2N**® **Access Unit** time value with your PC time value.



Time Zone: (UTC+01:00) Europe/Paris ▾

Time Zone Rule:

- **Time Zone** – set the time zone for the installation site to define time shifts and winter/summer time transitions.
- **Time Zone Rule** – if the **2N**® **Access Unit** 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** (specify time shifts and winter /summer time transitions manually).



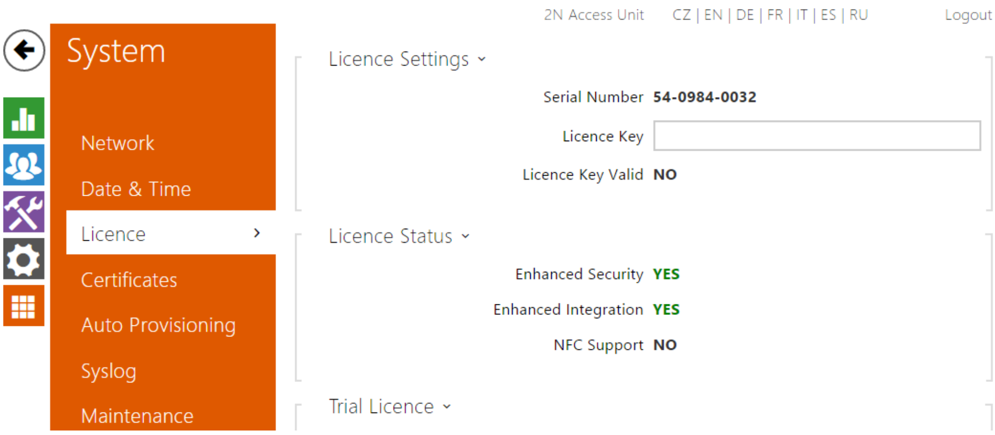
Use NTP Server ☑

NTP Server Address: time.nist.gov

NTP Time Status **Not synchronized**

- **Use NTP Server** – enable the NTP server use for **2N**® **Access Unit** time synchronisation.
- **NTP Server Address** – set the IP address/domain name of the NTP server used for your **2N**® **Access Unit** time synchronisation.

5.5.3 Licence



Licence Settings

Serial Number **54-0984-0032**

Licence Key

Licence Key Valid **NO**

Licence Status

Enhanced Security **YES**

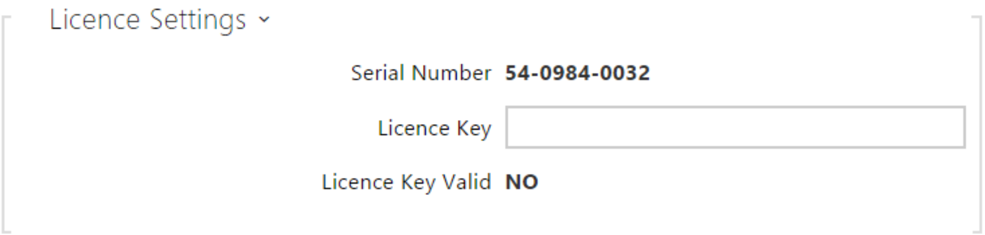
Enhanced Integration **YES**

NFC Support **NO**

Trial 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



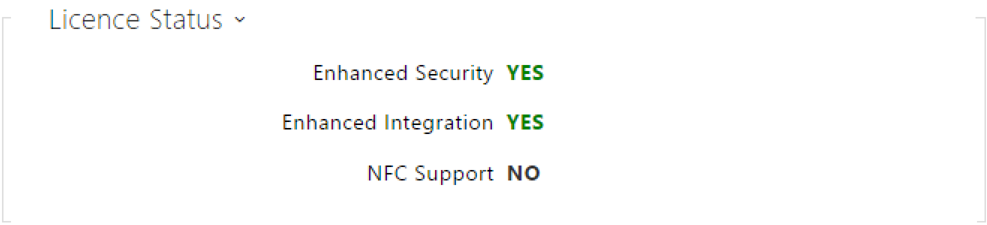
Licence Settings

Serial Number **54-0984-0032**

Licence Key

Licence Key Valid **NO**

- **Licence Key** – enter the valid licence key.
- **Licence Key Valid** – check whether the used licence key is valid.



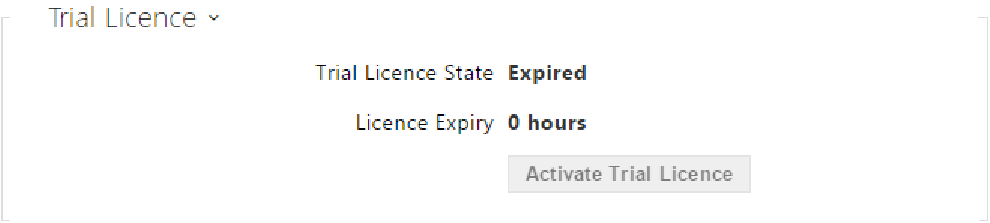
Licence Status

Enhanced Security **YES**

Enhanced Integration **YES**

NFC Support **NO**

- **Enhanced Security** – check whether the functions activated by the Enhanced Security licence are available.
- **Enhanced Intergration** – check whether the functions activated by the Enhanced Integration licence are available.
- **NFC Support** – check whether the functions activated.



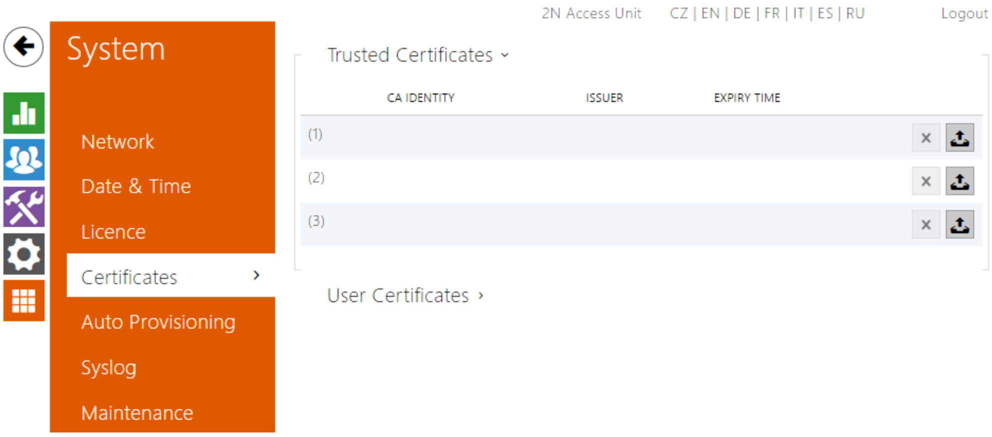
Trial Licence ˇ

Trial Licence State **Expired**

Licence Expiry **0 hours**

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

5.5.4 Certificates



	CA IDENTITY	ISSUER	EXPIRY TIME
(1)			
(2)			
(3)			

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:

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

The 2N® **Access Unit** intercoms allow you to load up to three sets of trusted certificates, which help authenticate LAN devices for communication with the 2N® **Access Unit**, plus three sets of user certificates and private keys for communication encryption.

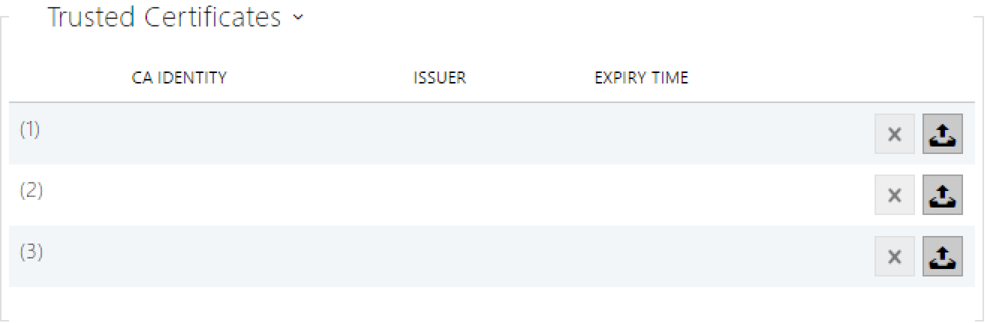
Each certificate-requiring service can be assigned one of the three certificate sets available; refer to the **Web Server**, **E-Mail** and **Streaming** subsections. The certificates can be shared by the services.

2N® **Access Unit** accepts the DER (ASN1) and PEM certificate formats.

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.

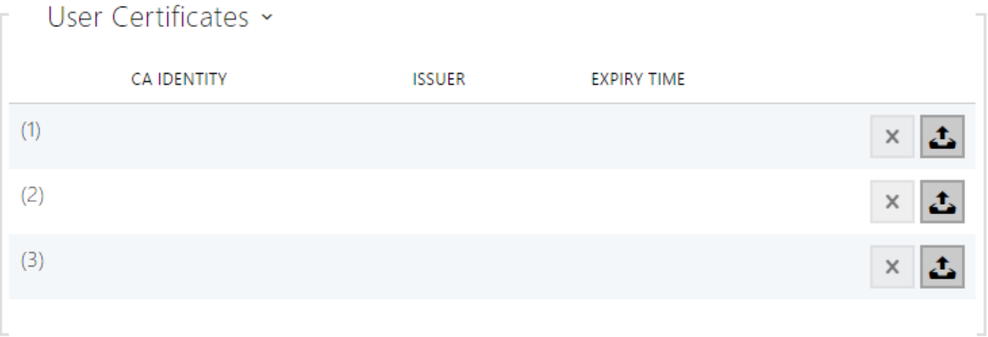
> **Note**
>
> - *If you use the Self Signed certificate for encryption of the intercom web server – browser communication, the communication is secure, but the browser will warn you that it is unable to verify the **2N® Access Unit** certificate validity.*

Refer to the tables below for the current list of trusted and user certificates:



Trusted Certificates ˅

	CA IDENTITY	ISSUER	EXPIRY TIME	
(1)				× ⬆
(2)				× ⬆
(3)				× ⬆

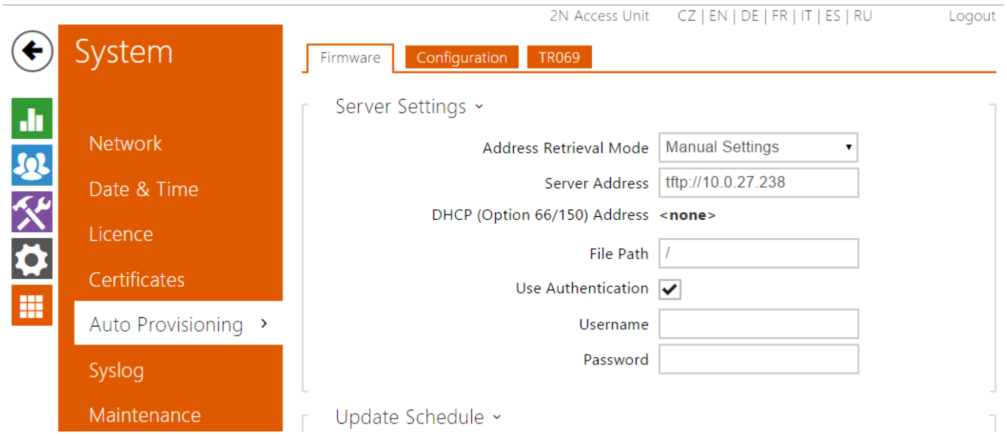


User Certificates ˅

	CA IDENTITY	ISSUER	EXPIRY TIME	
(1)				× ⬆
(2)				× ⬆
(3)				× ⬆

Press ⬆ to load a certificate saved on your PC. Select the certificate (or private key) file in the dialogue window and push **Load**. Press × to remove a certificate from the intercom.

5.5.5 Auto Provisioning


2N Access Unit CZ | EN | DE | FR | IT | ES | RU Logout

System

Network
Date & Time
Licence
Certificates
Auto Provisioning
Syslog
Maintenance

Firmware | Configuration | TR069

Server Settings

Address Retrieval Mode: Manual Settings
Server Address: tftp://10.0.27.238
DHCP (Option 66/150) Address: <none>
File Path: /
Use Authentication: ☑
Username:
Password:

Update Schedule

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).

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

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:

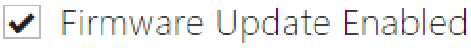
2N® Access Unit with MAC address 00-87-12-AA-00-11 downloads the following files from the TFTP server:

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

Configuration

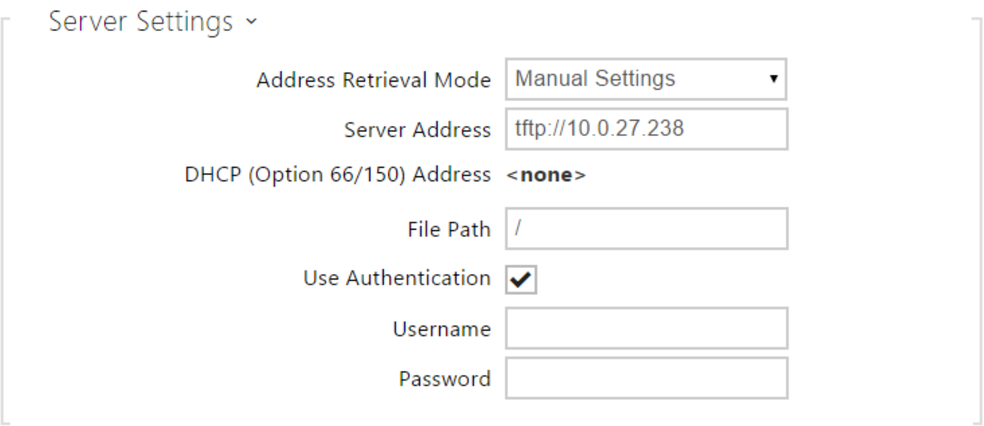
Use the Configuration tab to set automatic configuration download from the server defined by you. The **2N® Access Unit** periodically downloads a file from the server and gets reconfigured without getting restarted.

List of Parameters



☑ Firmware Update Enabled

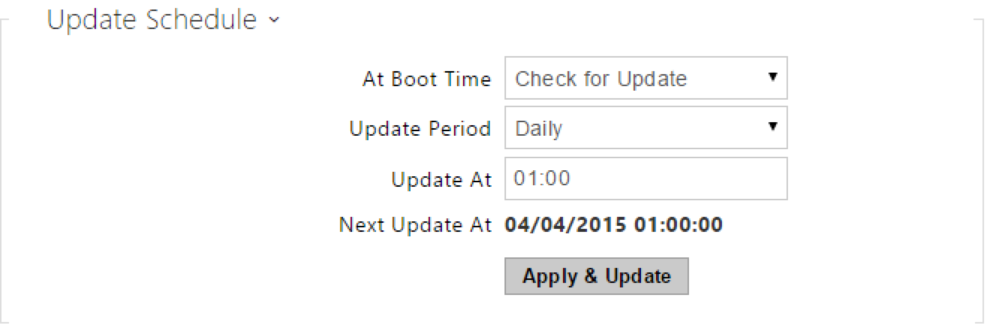
- **Firmware/Configuration Update Enabled** – enable automatic firmware /configuration updating from the TFTP/HTTP server.



Server Settings ˅

Address Retrieval Mode	Manual Settings ▾
Server Address	tftp://10.0.27.238
DHCP (Option 66/150) Address	**<none>**
File Path	/
Use Authentication	☑
Username	
Password	

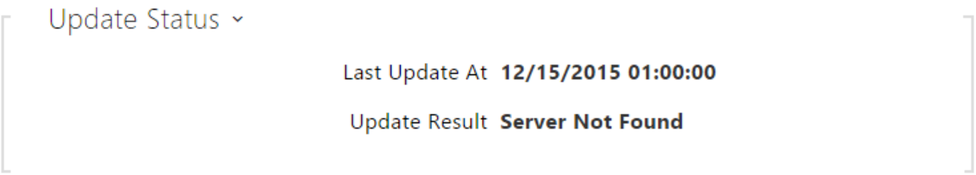
- **Address Retrieval Mode** – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 shall be used.
- **Server Address** – enter the TFTP (**tftp://ip_address**), HTTP (**http://ip_address**) or HTTPS (**https://ip_address**) 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 **2N® Access Unit** expects the au_firmware.bin, au-common.xml and au-MACADDR.xml files.
- **User Authentication** – Allows to use credentials for connect with server



Update Schedule ˅

At Boot Time: Check for Update ▾
Update Period: Daily ▾
Update At: 01:00
Next Update At: **04/04/2015 01:00:00**

- **At Boot Time** – enable check and/or execution of update upon every **2N® Access Unit** start.
- **Update Period** – set the update period: Hourly, Daily, Weekly or Monthly.
- **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.



Update Status ˅

Last Update At: **12/15/2015 01:00:00**
Update Result: **Server Not Found**

- **Last Update At** - display the last update time.

Update Result - display the last update result. The following options are available:

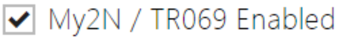
Result	Description
In progress ...	Update in progress
Updated	The configuration/firmware update has been successful. With firmware update, the device will be restarted in a few seconds.
Firmware is up to date.	The firmware update attempt reveals that the latest firmware version has been loaded.
DHCP 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.

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.

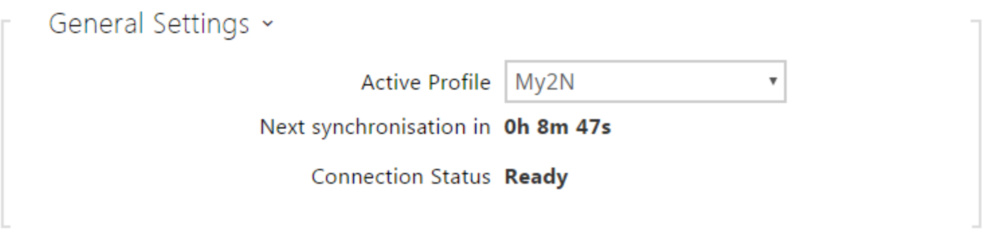
The TR-069 protocol is utilised by the My2N cloud service. Make sure that TR-069 is enabled and Active profile set to My2N to make your intercom log in to My2N periodically for configuration.

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

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



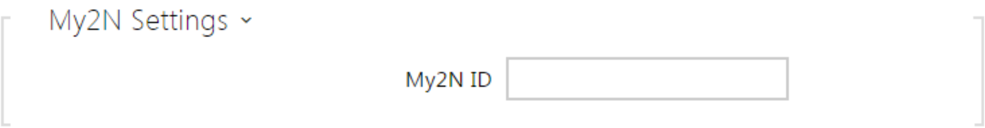
General Settings ⌄

Active Profile: My2N ▾

Next synchronisation in **0h 8m 47s**

Connection Status **Ready**

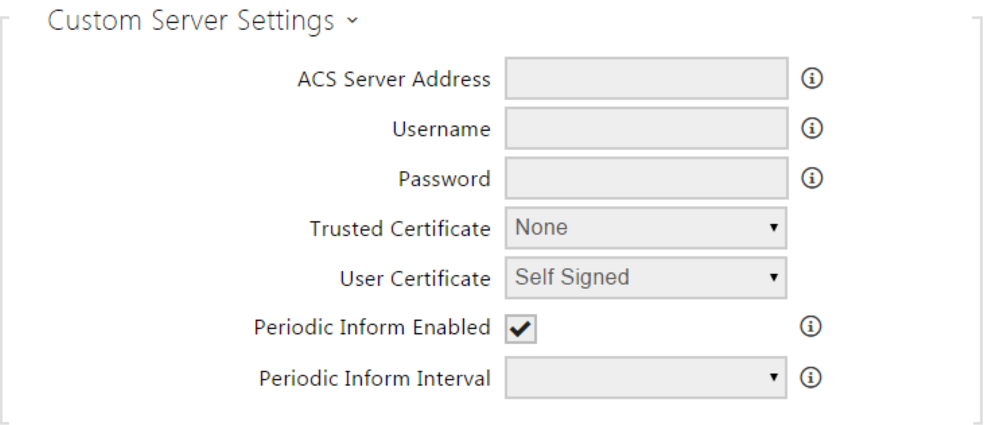
- **Active profile** – select one of the pre-defined profiles (ACS), or choose a setting of your own and configure the ACS connection manually.
- **Next synchronisation in** – display the time period in which the intercom shall contact a remote ACS.
- **Connection status** – display the current ACS connection state or error state description if necessary.



My2N Settings ⌄

My2N ID:

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



Custom Server Settings ⌄

ACS Server Address:

Username:

Password:

Trusted Certificate: None ▾

User Certificate: Self Signed ▾

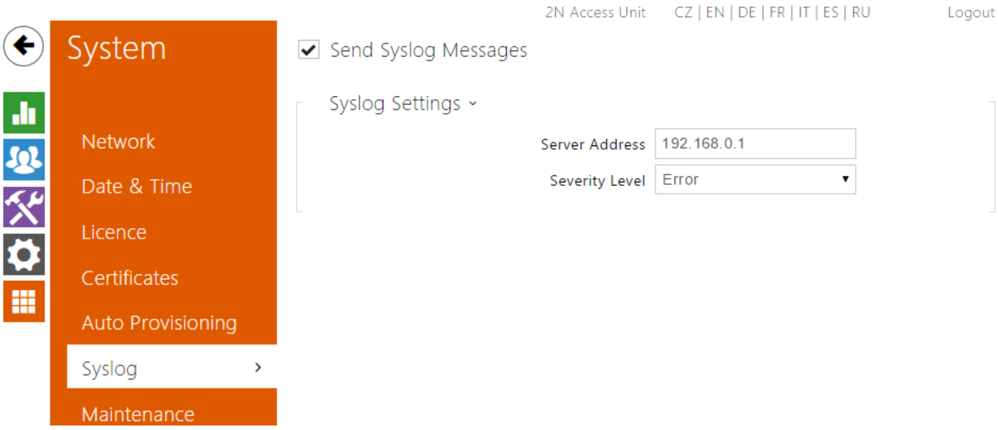
Periodic Inform Enabled: ☑

Periodic Inform Interval: ▾

- **ACS server 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.
- **Trusted 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.

- **User certificate** – specify the user 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.

5.5.6 Syslog



☑ Send Syslog Messages

Server Address: 192.168.0.1

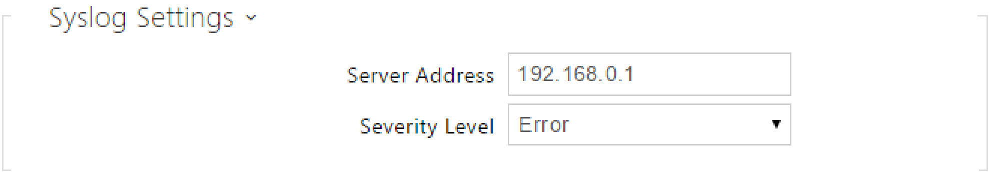
Severity Level: Error

The **2N**® **Access Unit** allow you to send system messages to the Syslog server including relevant information on the device states and processes for recording, analysis and audit. It is unnecessary to configure this service for common **2N**® **Access Unit** operation.

List of Parameters

☑ Send Syslog Messages

- **Send Syslog Messages** – enable sending of system messages to the Syslog server. Make sure that the server address is set correctly.

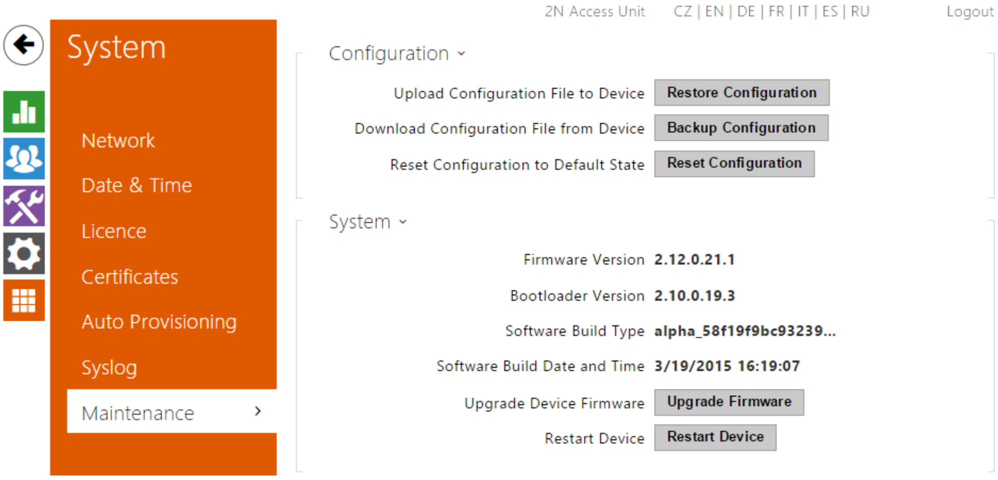


Server Address: 192.168.0.1

Severity Level: Error

- **Server Address** – set the IP/MAC address of the server on which the Syslog application is running.
- **Severity Level** – set the severity level of the messages to be sent.

5.5.7 Maintenance



Upload Configuration File to Device

Download Configuration File from Device

Reset Configuration to Default State

Firmware Version 2.12.0.21.1

Bootloader Version 2.10.0.19.3

Software Build Type alpha_58f19f9bc93239...

Software Build Date and Time 3/19/2015 16:19:07

Upgrade Device Firmware

Restart Device

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.

- 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 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. You can also choose before uploading whether the network parameters and SIP exchange connection settings from the configuration file shall be applied.
- Default State – 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 2N® Access Unit.

⚠ **Caution**

- *The default state reset deletes the licence key if any. Hence, we recommend you to copy it to another storage for later use.*

- 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 2N® Access Unit. The intercom will automatically get restarted and new FW will then be available. The whole upgrading process takes less than one minute. Refer to **www.2n.cz** for the latest FW version for your **2N® Access Unit**. FW upgrade does not affect configuration as the intercom checks the FW file to prevent upload of a wrong or corrupted file.
- 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.

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

Europe

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

Directive 1999/5/EC of the European Parliament and of the Council, of 9 March 1999 - on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits

Directive 2004/108/EC of the Council of 15 December 2004 on the harmonisation of the laws of Member States relating to electromagnetic compatibility

Commission Regulation (EC) No. 1275/2008, of 17 December 2008, implementing Directive 2005/32/EC of the European Parliament and of the Council with regard to ecodesign requirements for standby and off mode electric power consumption of electrical and electronic household and office equipment

Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No. 793/93 and Commission Regulation (EC) No. 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC

Directive 2012/19/EC of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment.

Industry Canada

This Class B digital apparatus complies with Canadian ICES-003. / Cet appareil numérique de la classe B est conforme a la norme NMB-003 du Canada.

FCC

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

cie
av solutions

Bringing
technology
to life.

CIE-Group Ltd 3 Widdowson Close Blenheim Ind Est Bulwell Nottingham NG6 8WB England
T: **+44(0)115 9770075** **F:** **+44(0)115 9770081** **E:** **info@cie-group.com** **W:** **www.cie-group.com**

Registered in England No. 2761780
@ciegroup CIE-Group facebook.com/ciegroup

plasa member

Member of BESA

ISCE supporting member

UVDB Registered

bsi. ISO 9001 Quality Management
FS 31532