2N® Access Unit

Access Control

Configuration Manual

Firmware 2.11
Version 2.11

www.2n.cz

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 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® Access Unit 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.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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, atomaticaly, 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 **2N® Access Unit** 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** voic e 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 9+ 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

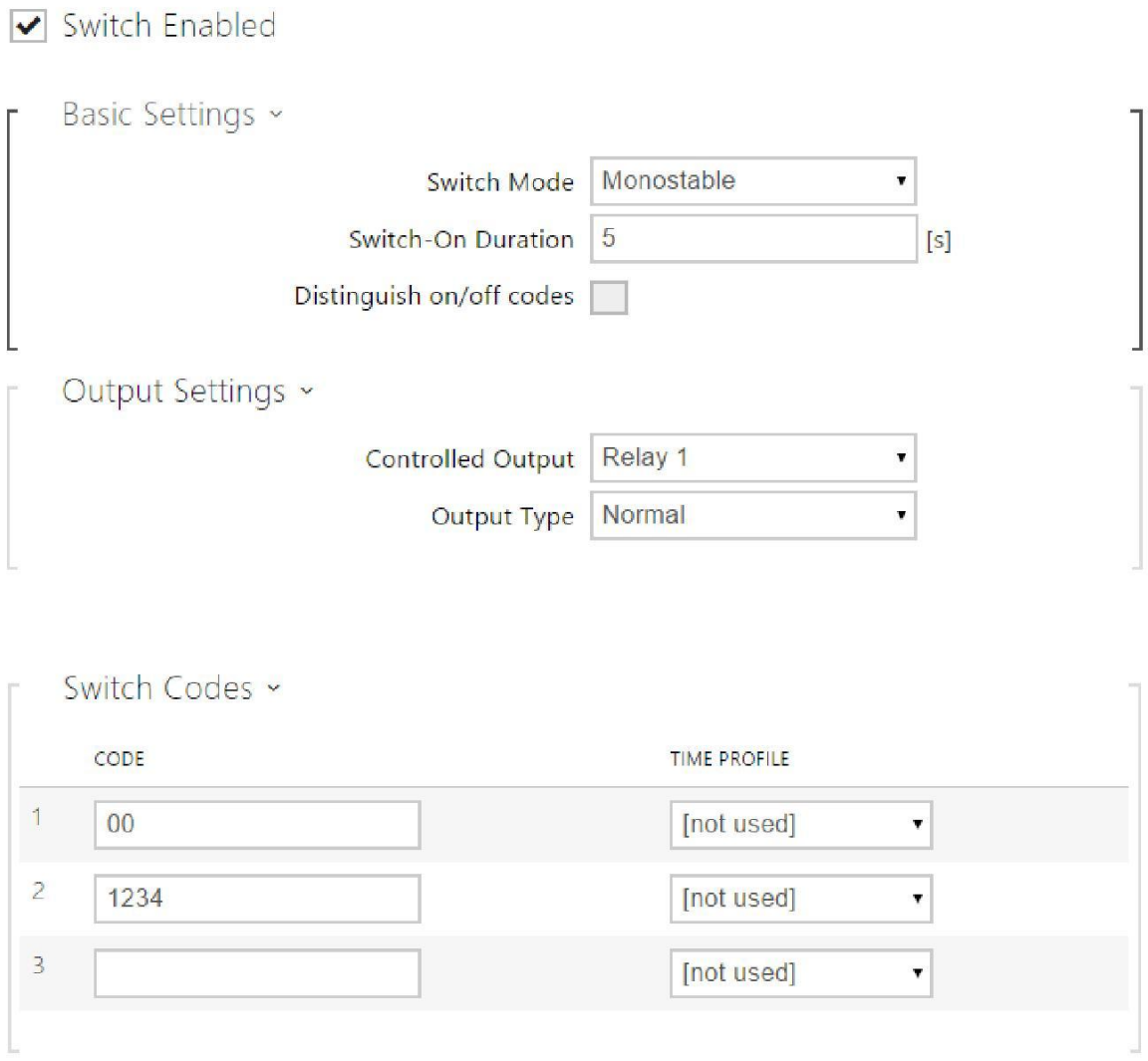
- FAQ: IP address - How to get the **2N® Access Unit** IP address?

Firmware Update

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

Electric Lock Switching Settings

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



Enable the switch in the Switch Enabled parameter on the **Hardware / Switches /**

Switch 1 tab, set the Controlled Output to the intercom output to which the electric door lock is connected. Now set one or more activation codes for the electric door lock switching.

3. Function Licensing

2N® Access Unit provides just one licensed function - NFC.

4. Signalling of Operational Statuses

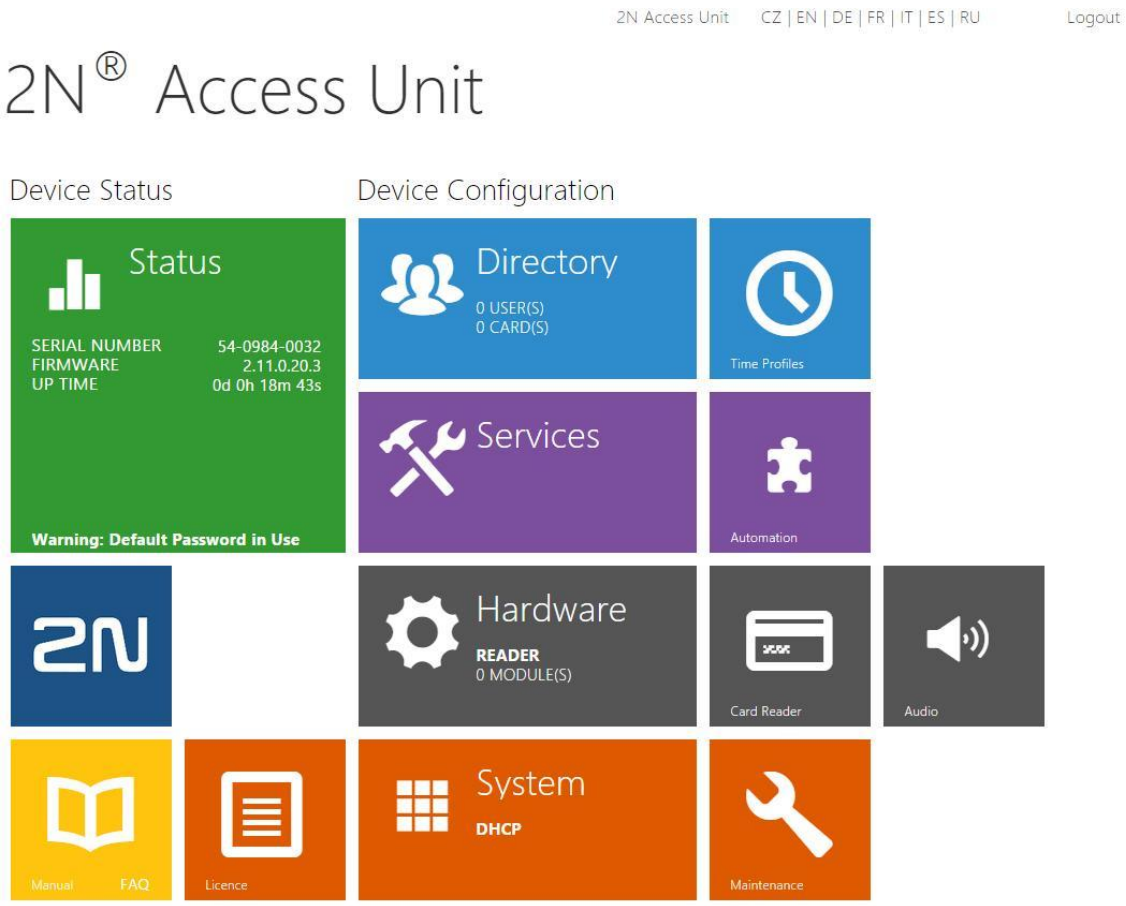
2N® Access Unit generates sounds to signal changes and switching of operational statuses. Each status change is assigned a different type of tone. See the table below for the list of signals:

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. A deactivated user may not be called but the call can, if necessary, be forwarded to a deputy if defined. 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. This function helps, for example, disable alerting of a user group in an office and routing calls either to a pre-defined phone number (porter's lodge, e.g.) or user mobile phones. 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 signalled 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. Access Unit Configuration



Start Screen

The start screen is an introductory overview screen displayed upon login to the **2N®**

Access Unit web interface. Use the button in the left-hand upper corner of the following web interface pages to return to this screen anytime.

The screen header includes the **2N® Access Unit** name (refer to the Display Name parameter in the **Services / Phone/ SIP** menu). Select the web interface language with the **CZ** and **EN** 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

- **System** – 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

Directory

- **Users** – settings for user phone numbers, quick dial buttons, access cards and switch control user codes
- **Profiles** – time profile settings
- **Access Cards** – access card settings

Hardware

- **Switches** – electric lock, lighting, etc. settings
- **Speaker** – audio, signalling tone, etc. volume settings
- **Keypad** – button and keypad settings
- **Card Reader** – card reader, Wiegand interface settings
- **Extenders** – **2N® Access Unit** extender settings

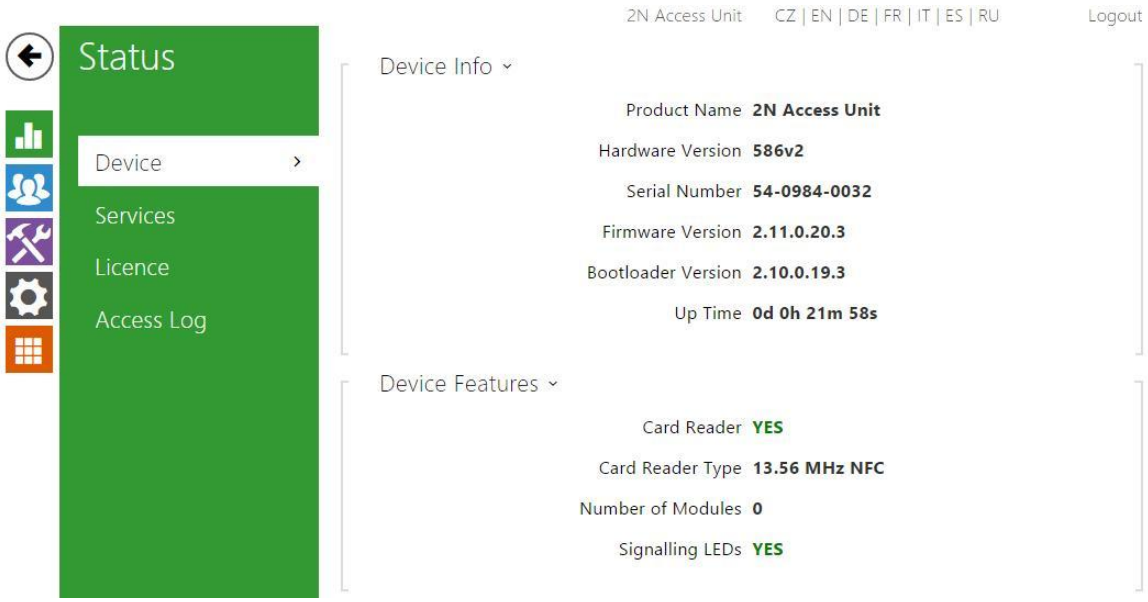
Services

- **E-Mail** – E-mail sending and SMTP connection settings
- **Automation** – flexible intercom settings according to user requirements
- **User sounds** – user sound settings and upload
- **Web server** – web server and access password settings

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
- **Update** – automatic firmware and configuration update settings
- **Syslog** – syslog message sending settings
- **Maintenance** – backup and configuration reset, firmware update

5.1 State



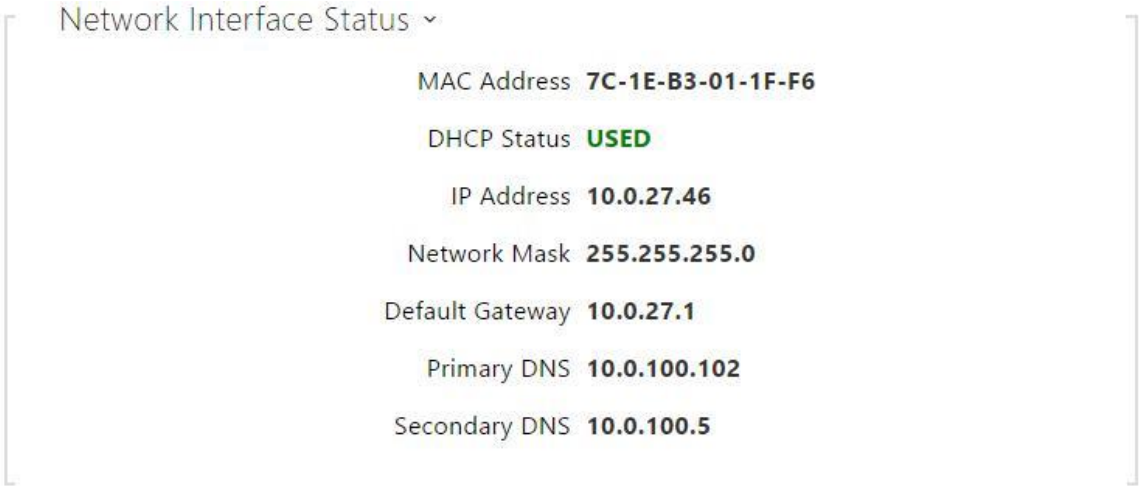
The **Status** menu provides clear status and other essential information on the **2N® Access Unit**. The menu is divided into the following tabs:

Device

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

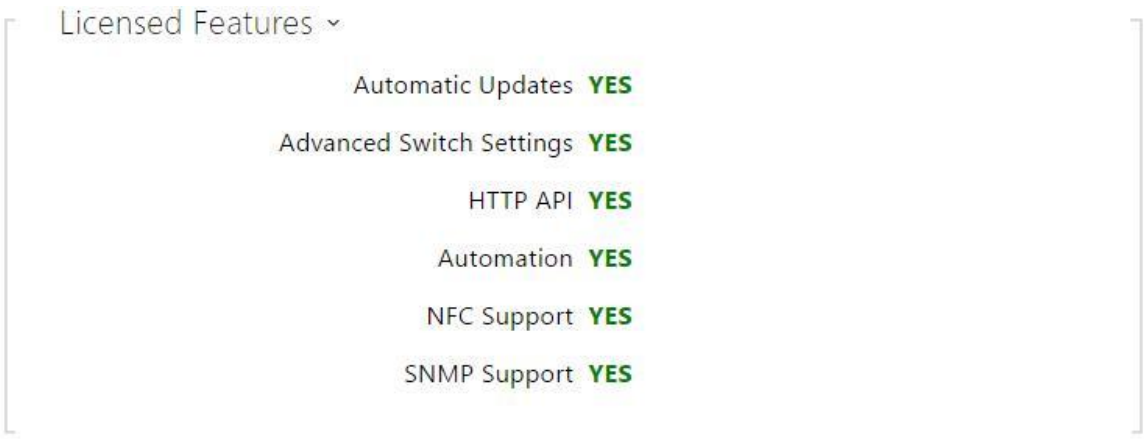
Services

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



Licence

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



Access Log

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

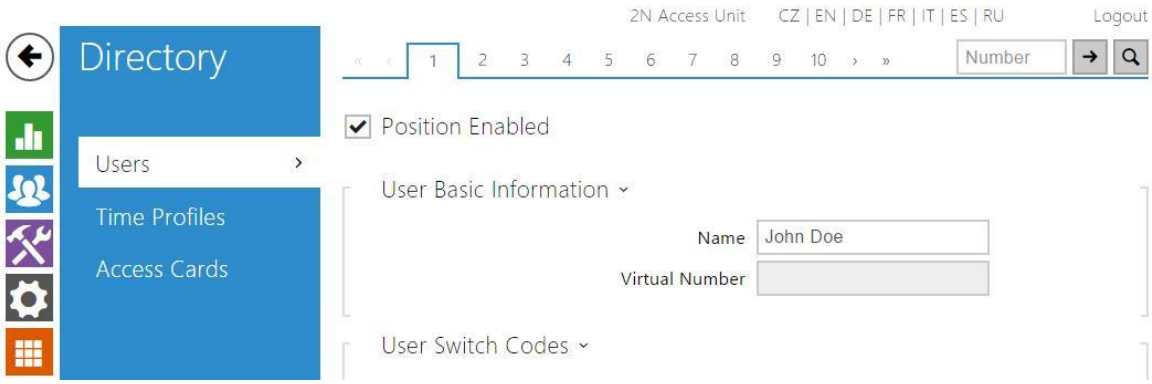
Access Log

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

5.2 Directory

Here is what you can find in this section:

5.2.1 Users



The User list is one of the crucial parts of the **2N®** **Access Unit** configuration. It contains user information relevant for such intercom functions as RFID card door unlocking, code lock switching and similar.

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.

Do not complete the phone numbers of the RFID/code access users. Enter their RFID card IDs or door unlocking numeric codes only. In this case, the quick dial button will behave as non-programmed (for calling).

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.

List of Parameters

- **Position enabled** – enable calling to this user position.

- **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.

- **Time profile** – assign a time profile to each phone number to define the number validity. If the profile in inactive, the phone number is not used and the following phone number is dialled if defined.

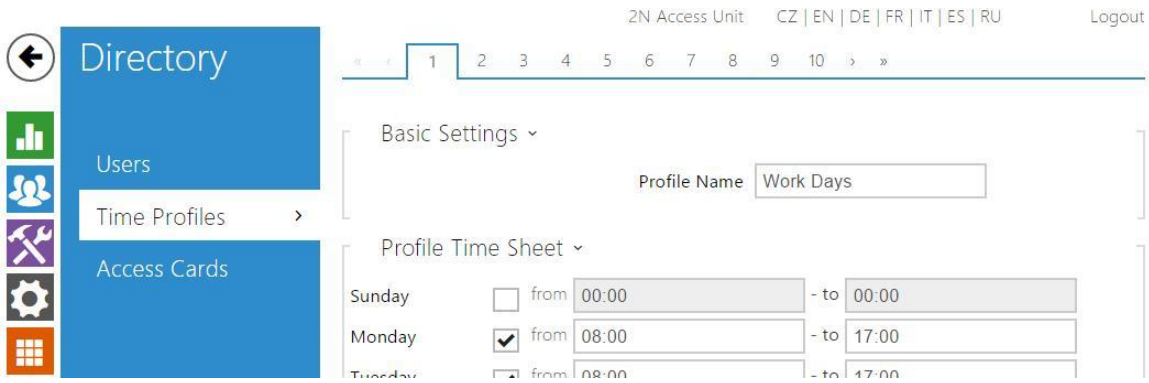
Each user can be assigned a private switch activation code. The user switch codes can be arbitrarily combined with the universal switch codes defined in the **Hardware / Switches** menu. If the codes are identical with the codes already defined in the intercom configuration, the mark will appear at the colliding codes.

- **Code** – set a private user switch activation code: up to 16 characters including digits 0–9 only.
- **Time profile** – assign a time profile to the switch code to define the code validity. If the time profile is inactive, the switch will not be activated by the code.

Each of the **2N® Access Unit** users can be assigned one access RFID card. Refer to the **Access Cards** subsection for details.

- **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.
- **Time profile** – assign a time profile to the user access card to define the card validity. If the time profile is inactive, the user access card will be detected as invalid.
- **Double authentication** – set card + numeric code authentication for a user: apply a valid user card and then enter one of the switch activating codes (no later than ten seconds after tapping) to activate the switch in this mode.

5.2.2 Time Profiles



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

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

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

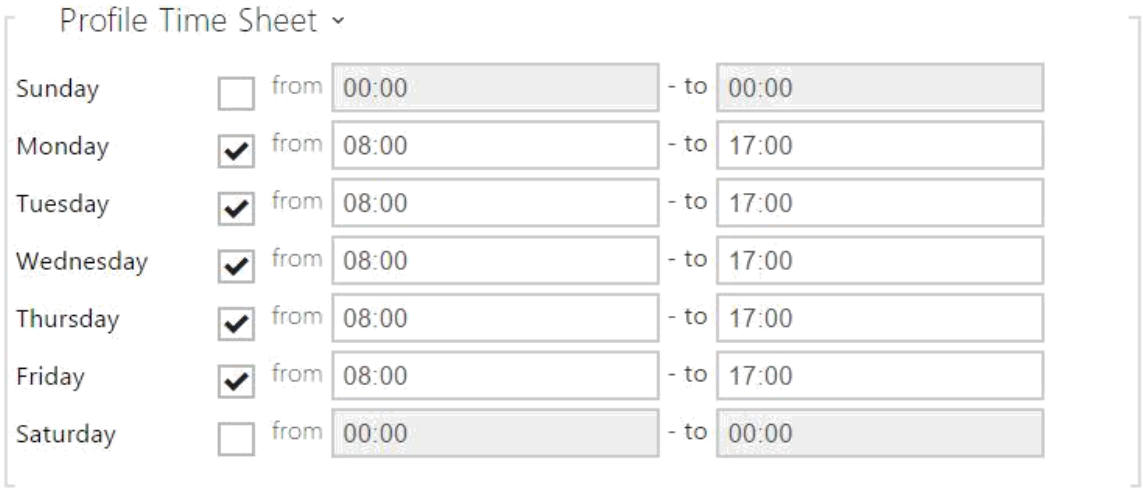
The time profiles can be defined not only using the week time sheet but also manually with the aid of special activation/deactivation codes. Enter the activation/deactivation codes using the numeric keypad of your **2N®** **Access Unit** to activate/deactivate a function after arriving in/before leaving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

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

List of Parameters

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

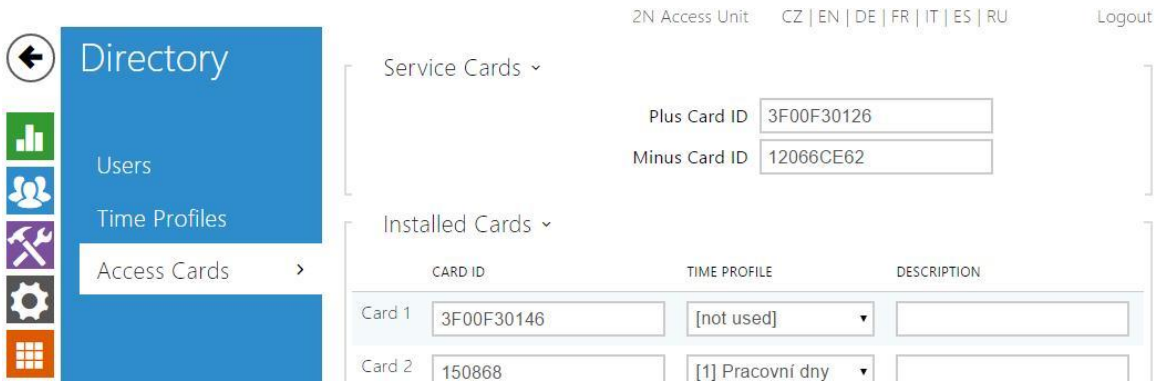
This parameter helps you set time profiles within a week period. A profile is active when it matches the set intervals. Make sure that the real time settings are correct (refer to the Date and Time subsection) to make this function work properly.



Note

- Check off a day and set the From/To fields to 00:00 to make a time profile active the whole day.

5.2.3 Access Cards



Each **2N®** **Access Unit** user can be assigned one or more access RFID cards. Typically, the card ID is included in the User list together with such user data as phone numbers, e-mail address and so on. Or, you can define the RFID cards in the Installed Cards list, which defines a limited number of cards to be assigned to visitors, for example.

You can manage – add, remove and modify items – the list of installed cards manually via the **2N®** **Access Unit** configuration interface. The main advantage of this list is the option to add/remove cards using the Service plus/minus card without accessing the configuration interface. Unlike the User list with its up to 1999 positions, the Installed Cards may contain only 20 cards.

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

The Service cards are common cards that you can define for this special purpose. Enter their IDs in the Plus Card ID and Minus Card ID fields in the **Service Cards** section.

The access card ID is a sequence of 6–32 characters including 0–9, A–F (i.e. hexadecimal number of the length of 24 to 128 bits). The number of characters in the card ID can be different in different card types. However, it holds true that cards of one and the same type have identically long IDs.

If you use an external card reader connected to the **2N®** **Access Unit** 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 an internal 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 **2N®** **Access Unit** 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 internal and external readers. Go to the **Directory / Access Cards / Records** menu to identify whether the card was tapped on an internal or external reader.

All cards applied via an internal 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 **2N® Access Unit** 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 **2N® Access Unit** setting field.

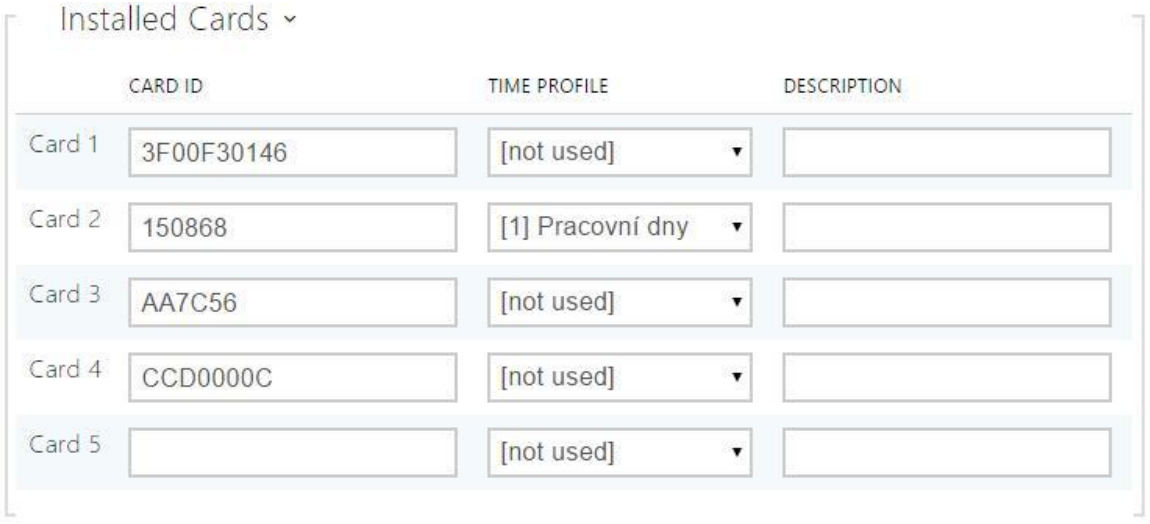
Having been read, the card ID is compared with the **2N® Access Unit** card database. If the card ID matches any of the cards in the database, the appropriate action is executed: switch activation (door unlocking, etc.). To change the switch number to be activated, use the **Associated switch** parameter in the **Hardware / Modules** menu of the card reader module.

Refer to the **Directory / Access Cards** menu for the access card settings.

List of Parameters

Cards

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



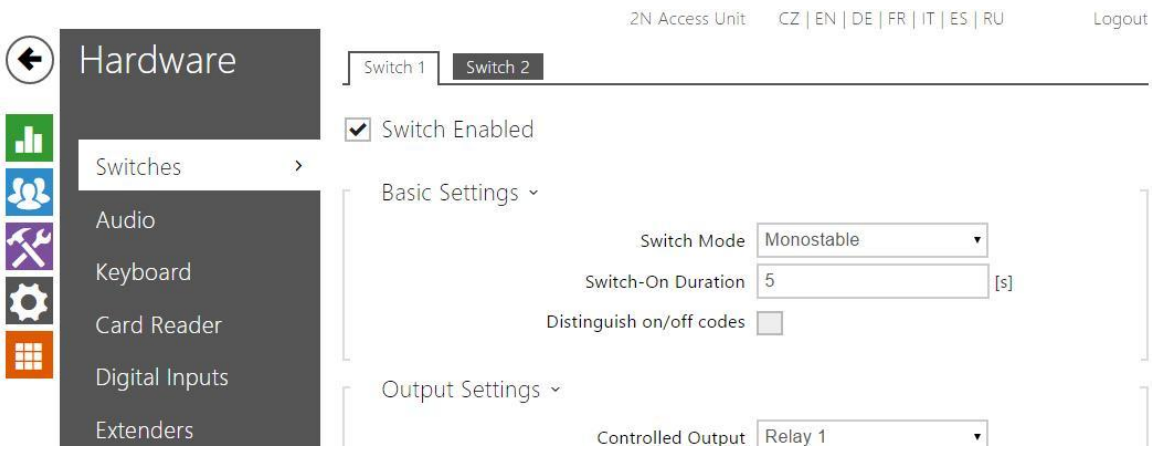
- **Card ID** – enter the access card ID: a sequence of 6–32 characters including 0–9, A–F.

- **Time profile** – assign a time profile to the user access card to define the card validity. If the time profile is inactive, the user access card will be detected as invalid.
- **Description** – enter such information as the card owner name and similar. The description gets displayed in the Records menu whenever the card is applied and helps you find the card list items more easily without affecting the **2N® Access Unit** function.

5.3 Extending Modules

Here is what you can find in this section:

5.3.1 Switches



Switches provide a very flexible and efficient control of such peripherals connected to the Access Unit as electric door locks, lighting, additional ringing signalling, and so on.
2N® Access Unit allows you to configure up to 4 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.
- an incoming or outgoing call 1).
- 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:

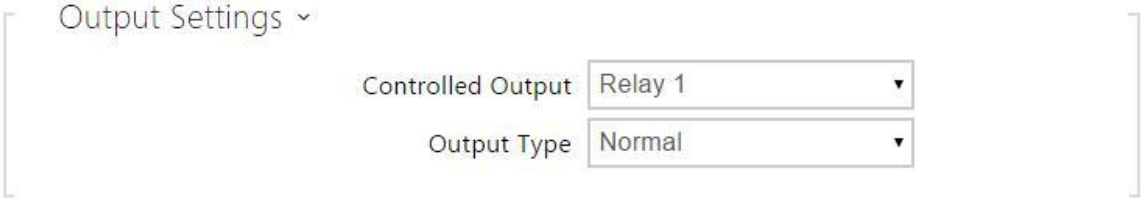
- a programmable beep or a predefined user sound.
- a LED indicator if available in the **2N® Access Unit** model.

List of Parameters

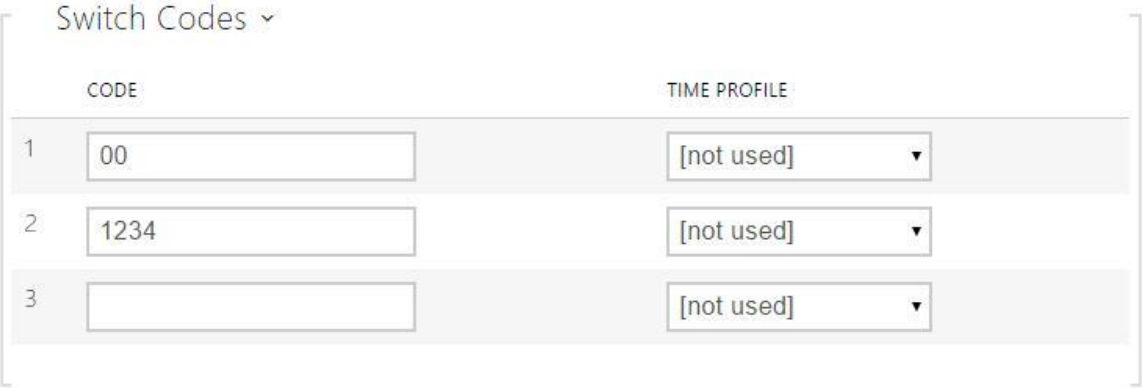
- **Switch enabled** – enable/disable the switch globally. When disabled, the switch cannot be activated by any of the available codes (including user switch codes),

by quick dial button.

- **Switch mode** – set the monostable/bistable mode for the switch. The switch is switched off after a timeout in the monostable mode and switched on with the first activation and off with the next activation in the bistable mode.
- **Switch-on duration**– set the switch-on time for a monostable switch. This value is not applied in the bistable mode.
- **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.



- **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 via a specific pulse sequence.



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

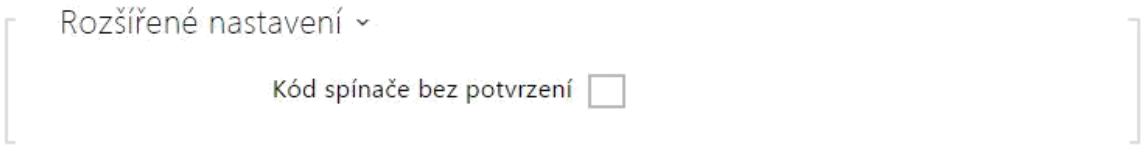
(depending on the particular intercom model).

- **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.
- **Activation by quick dial button** – assign a quick dial button to the switch. The switch is activated whenever the button is pressed.

- **Sound signalling** – set the sound signalling type for switch activation. Choose the Short beep, Long beep (during the whole activation) or User sound (refer to the User Sounds subsection).

- **Synchronise** – set switch synchronisation to enable automatic switch activation after another switch activation with a predefined delay. Define the delay in the **Synchronisation delay** 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.

- **Command sent upon activation** – 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.
- **Command sent upon deactivation** – 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

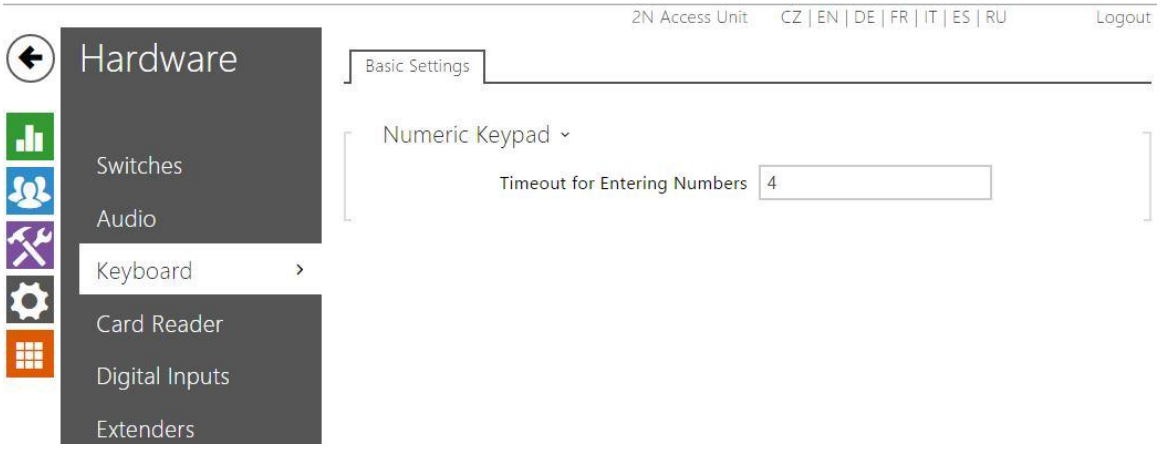


- **Legacy switch code** – enable the option to activate the **first-listed switch code** from the phone without being confirmed with *. When this box is checked, the first code does not require confirmation with *. This setting does not apply to other switch codes listed and to numeric keypad code activation, which always have to be confirmed with *. The Legacy switch code helps you set back compatibility with earlier 2N intercom models.

5.3.2 Audio


2N Access Unit
CZ | EN | DE | FR | IT | ES | RU
Logout
Hardware
Switches
Audio
Keyboard
Card Reader
Digital Inputs
Extenders
Signalling Volume
Key Beep Volume
0 dB
Warning Tone Volume
0 dB
Switch-Activation Tone Volume
0 dB

5.3.4 Keyboard



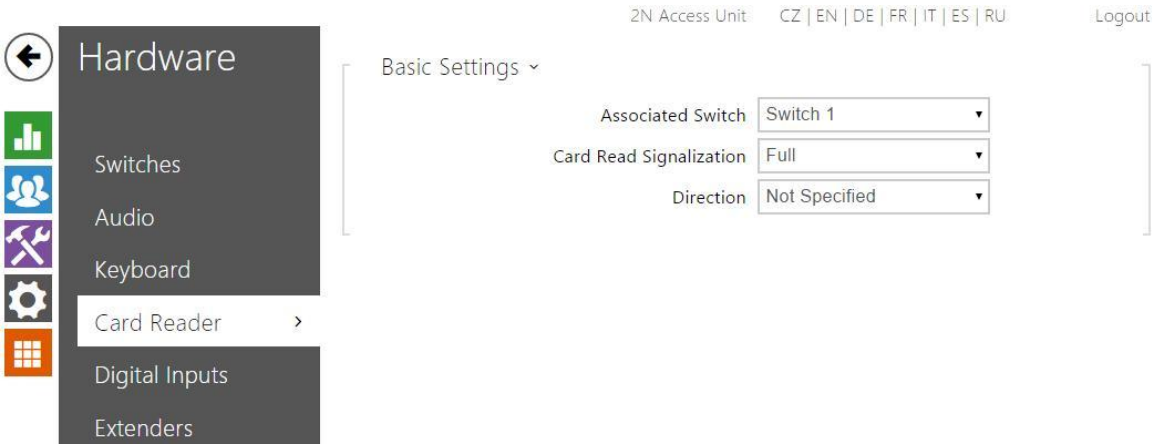
This configuration section helps you set the numeric keypad and quick dial button functions. The **2N® Access Unit** allows you to:

- set the timeout for entering codes and phone numbers

List of Parameters

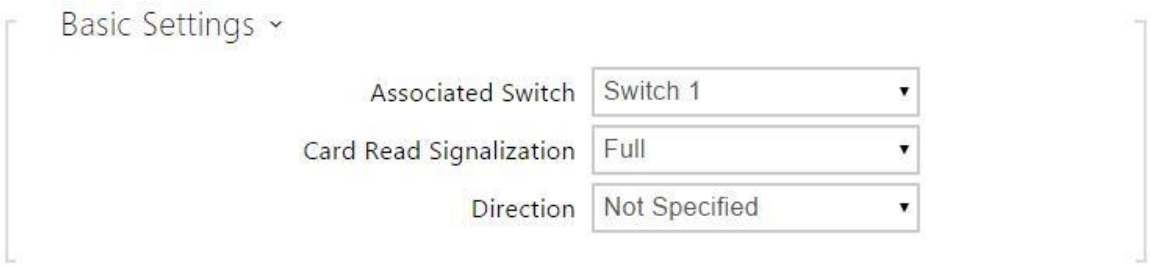
- **Timeout for entering numbers** – set the maximum interdigit timeout for code or phone number dialling via the **2N® Access Unit** numeric keypad. When the timeout elapses, the dialling is automatically confirmed as if the * key was pressed.

5.3.5 Card Reader



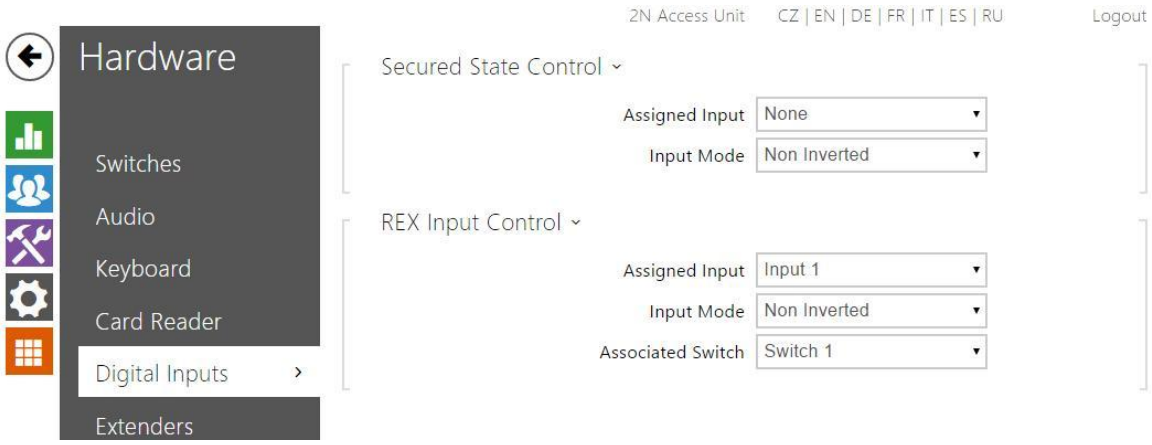
The card reader helps you control access to your building effectively using contactless RFID cards. The supported card types depend on the card reader model used.

List of Parameters



- **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**

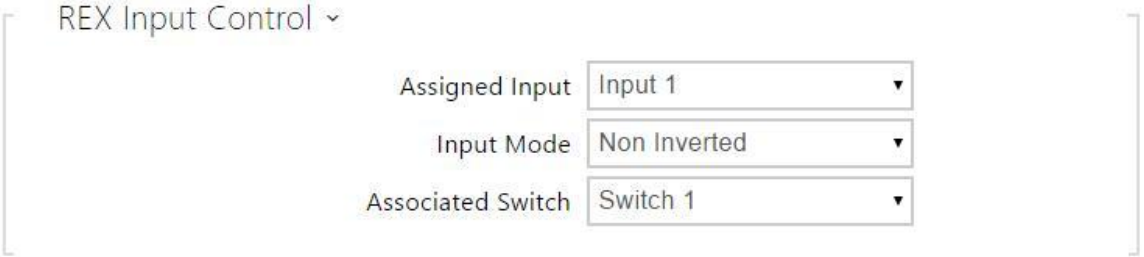
5.3.6 Digital Inputs



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

List of Parameters

- **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).



- **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.

5.3.7 Other 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
- 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).

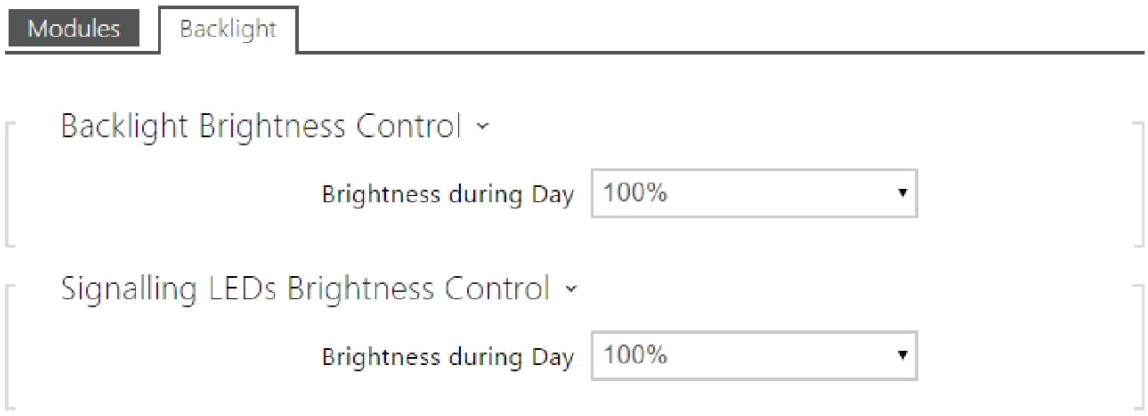
You can configure each module separately. The parameters are specific for the given module type .

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.



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

- **Button functions** – assign user positions to the buttons.

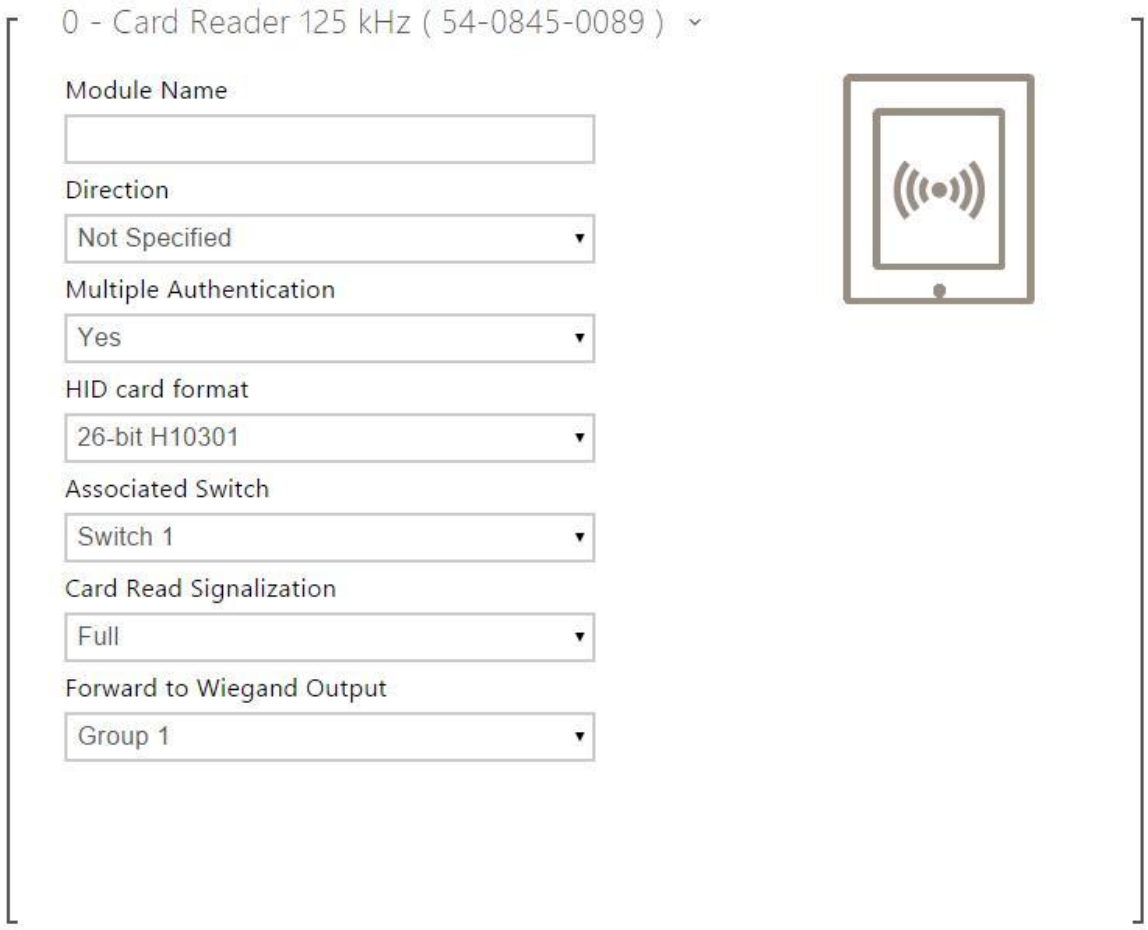
Keypad Module Configuration

- No parameters are available to the public at present.

Infopanel Module Configuration

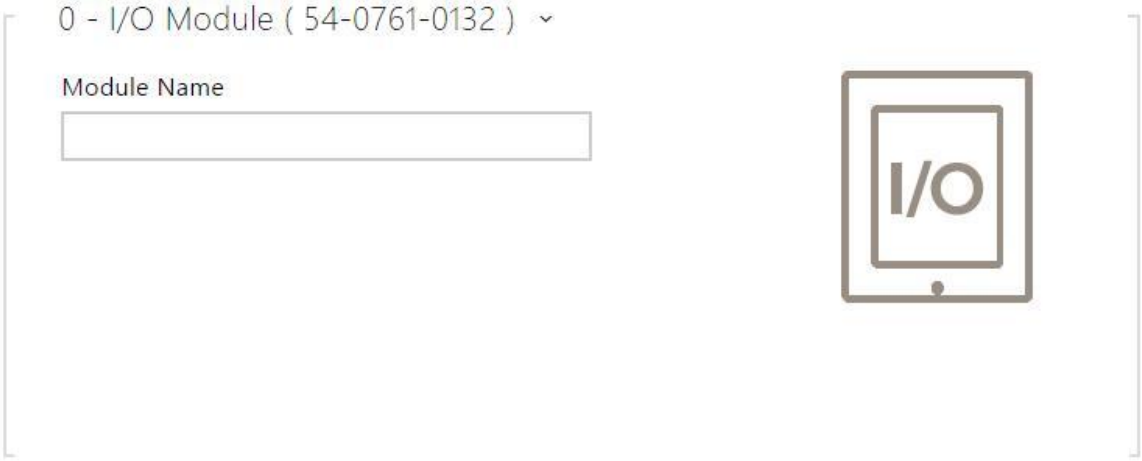
- No parameters are available to the public at present.

Card Reader Module Configuration



- **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.

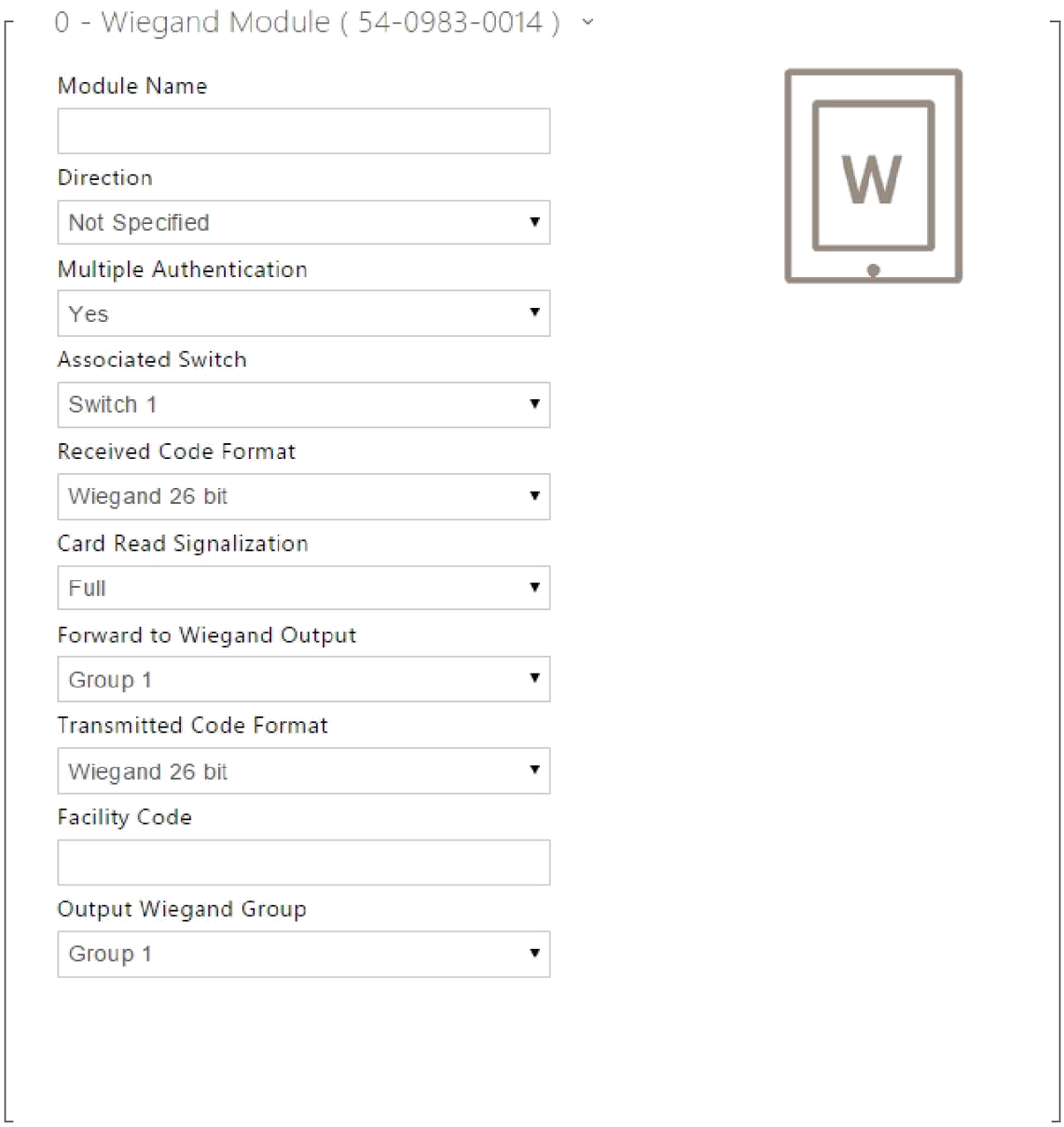
I/O Module Configuration



- **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**.

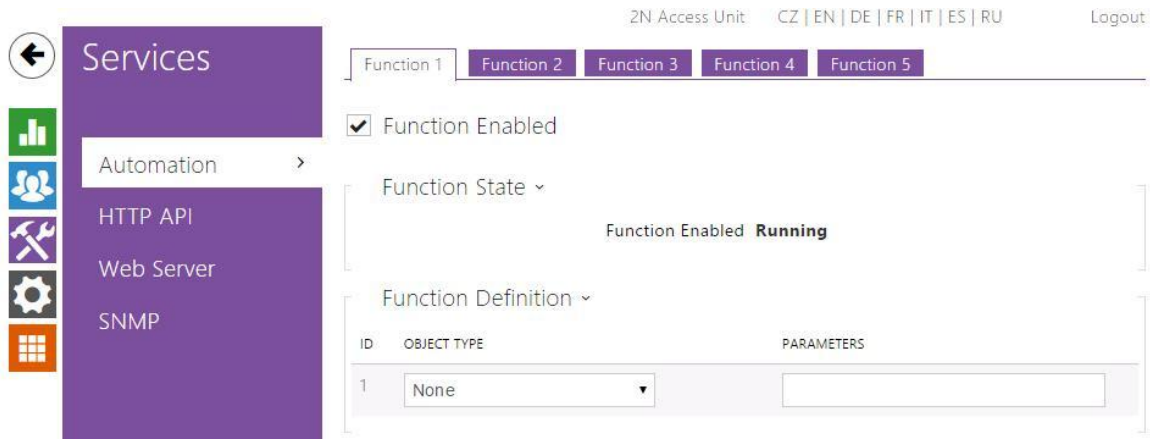


- **Module name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N® Helios IP Automation**. .
- **Associated switch** - set the number of the switch to be activated whenever a valid code is received.
- **Received code format** - set 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:

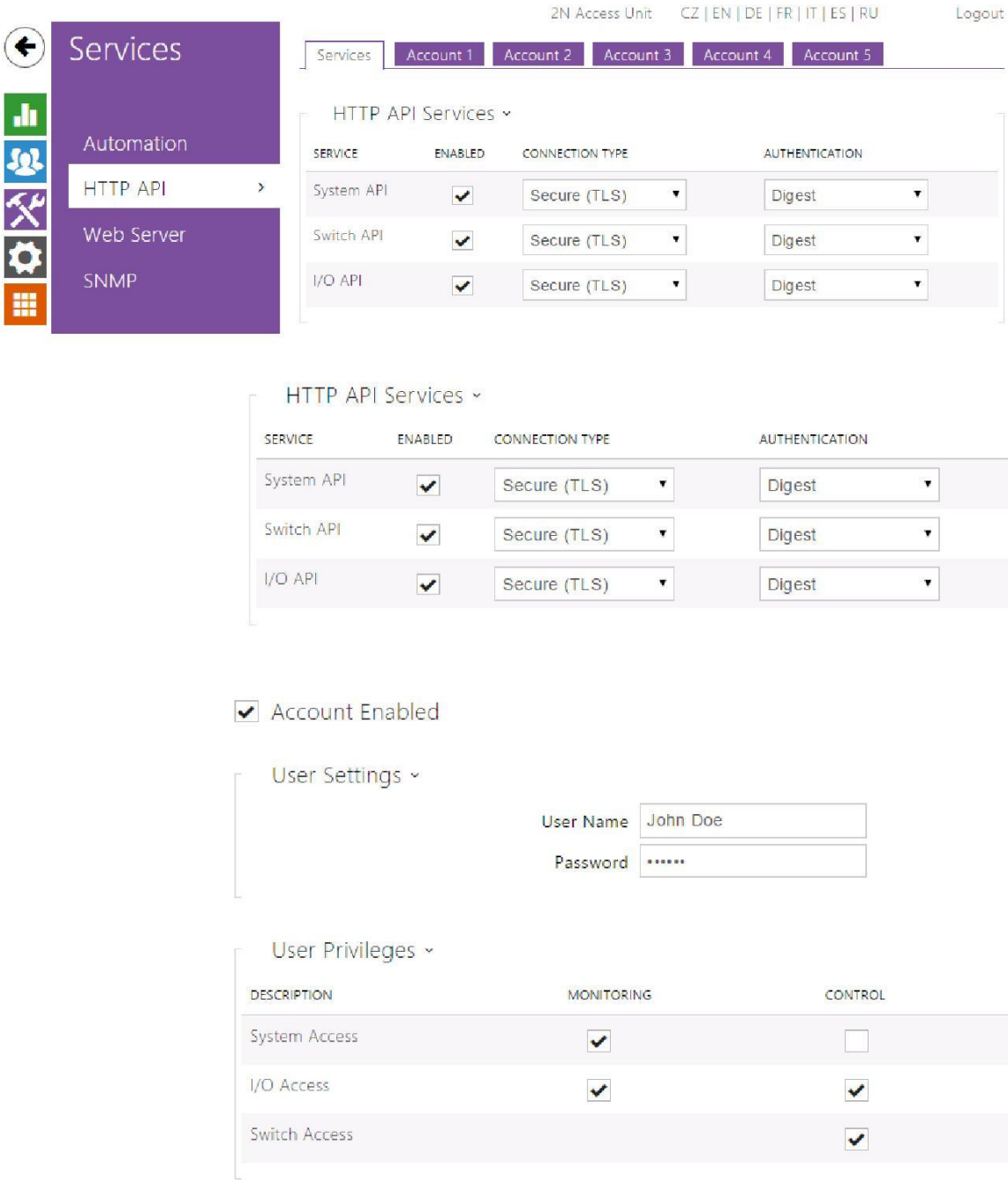
5.4.1 Automation



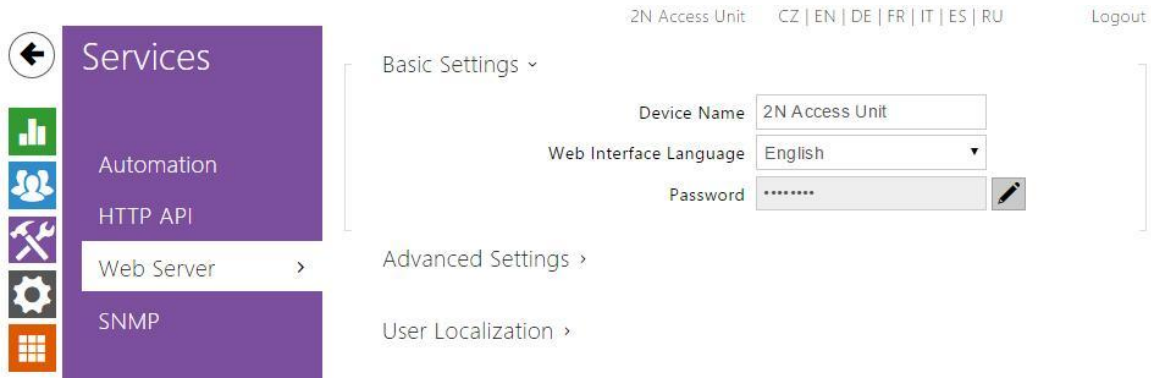
The **2N® Access Unit** provides highly flexible setting options to satisfy variable user needs. There are situations in which the standard configuration settings (switch or call modes, e.g.) are insufficient and so **2N® Acess Unit** offers a special programmable interface, **2N® Helios IP Automation**. 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.

5.4.2 HTTP API


2N Access Unit
CZ | EN | DE | FR | IT | ES | RU
Logout
Services
Automation
HTTP API
Web Server
SNMP
Services
Account 1
Account 2
Account 3
Account 4
Account 5
HTTP API Services
SERVICE
ENABLED
CONNECTION TYPE
AUTHENTICATION
System API
Switch API
I/O API
Secure (TLS)
Digest
Account Enabled
User Settings
User Name
John Doe
Password
User Privileges
DESCRIPTION
MONITORING
CONTROL
System Access
I/O Access
Switch Access

5.4.3 Web server



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

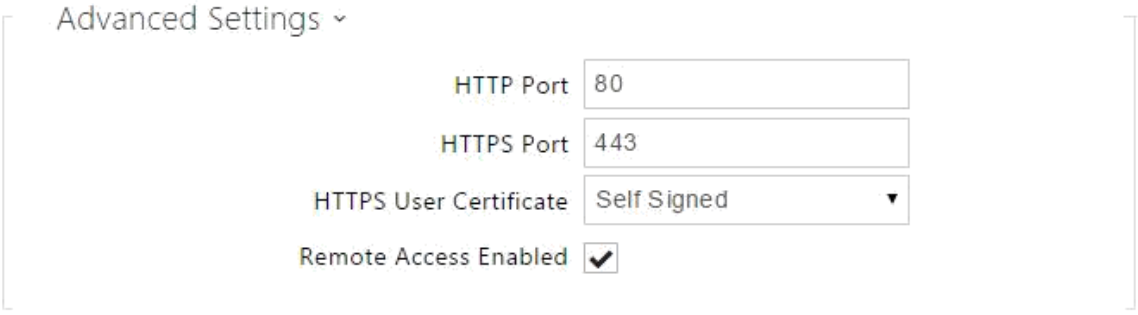
The Web Server function is used by the following **2N®** **Access Unit** functions too:

a. HTTP commands for switch control, refer to the Switches subsection.
b. Event.HttpTrigger in **2N®** **Helios IP Automation**; refer to the respective manual.

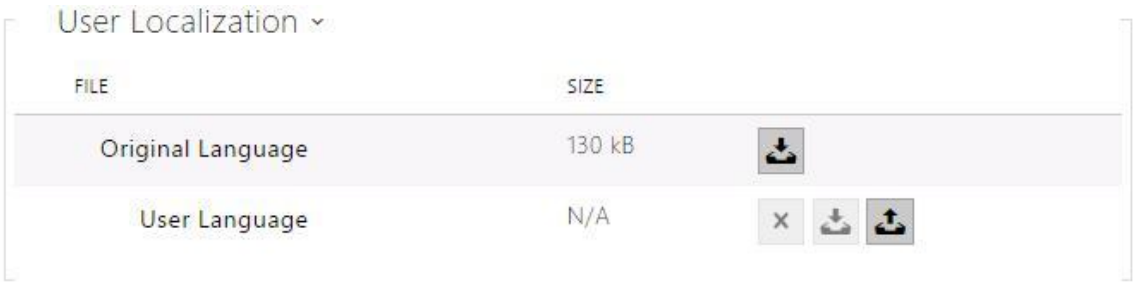
The unsecured HTTP protocol can be used for these special communication cases.

List of Parameters

- **Device name**– 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.



- **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.



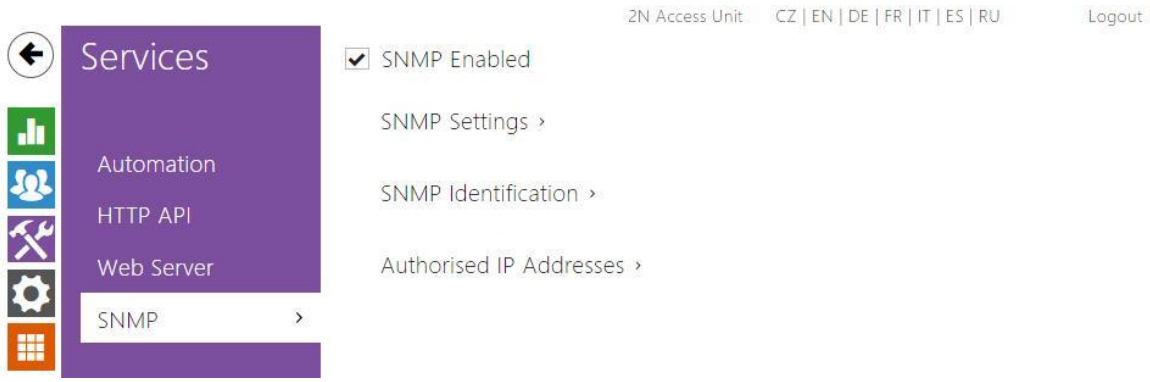
- **Original language** – download the original file containing all the user interface texts in English. The file format is XML; see below.
- **User language** – record, load and remove, if necessary, a user file containing your own user interface text translations.

```
<?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.

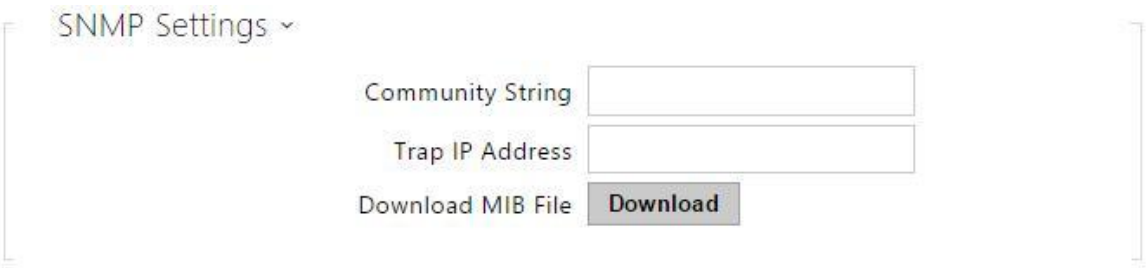
5.4.4 SNMP



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** - Allows you to enable the SNMP function



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

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

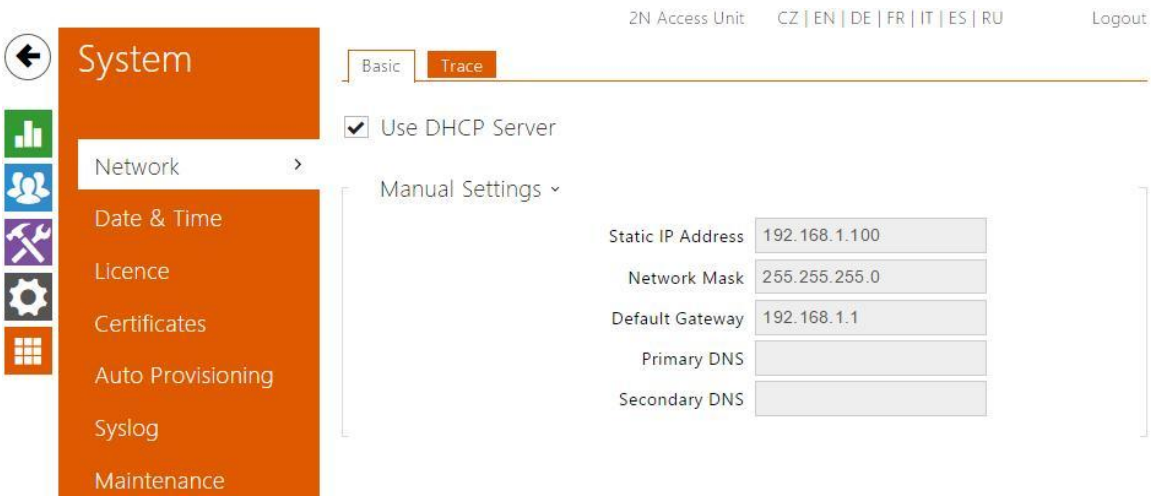
- **Name** - enter the device name.
- **Location** - enter the device location (1st floor, e.g.).

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

5.5 System

Here is what you can find in this section:

5.5.1 Network



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

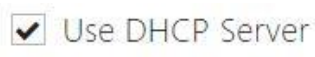
Tip

- To know the current IP address of your **2N® Access Unit**, use the **2N® 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.

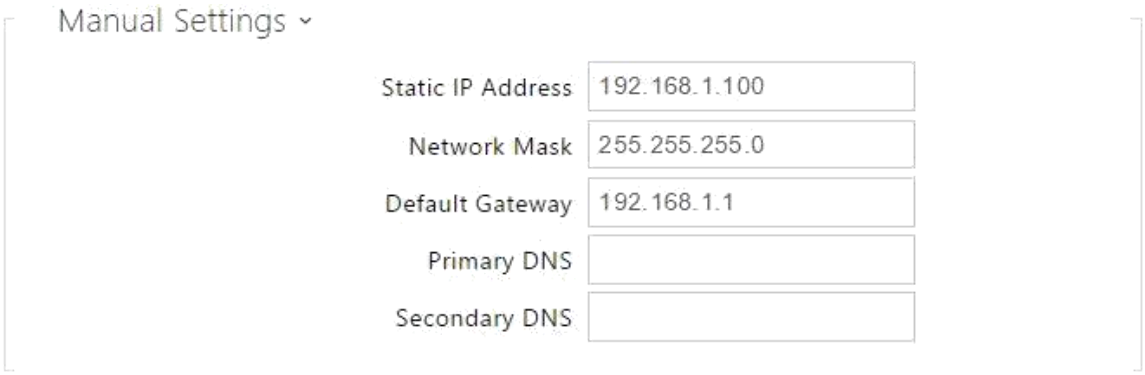
If you use the RADIUS server and 802.1x-based verification of connected equipment, you can make the intercom use the EAP-MD5 or EAP-TLS authentication. Set this function on the 802.1x tab.

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

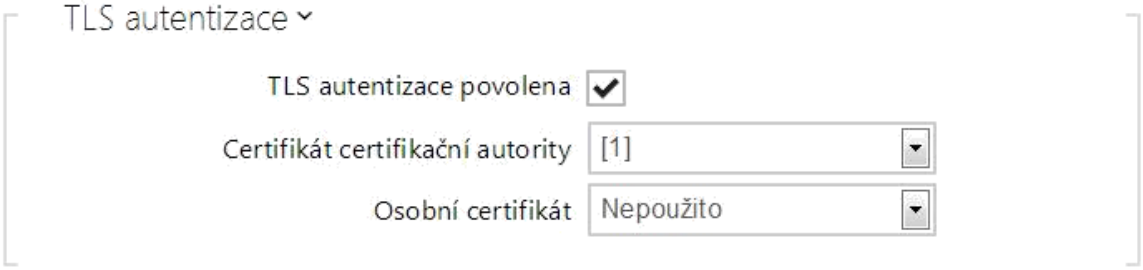


- **Static IP address** – display the static IP address of the **2N® Access Unit**, which is used together with the below mentioned parameters if the Use DHCP Server parameter is disabled.
- **Network mask** – set the network mask.
- **Default gateway** – set the address of the default gateway, which provides communication with off-LAN equipment.
- **Primary DNS** – set the primary DNS server address for translation of domain names to IP addresses.
- **Secondary DNS** – set the secondary DNS server address, which is used in case the primary DNS is inaccessible.

802.1x

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

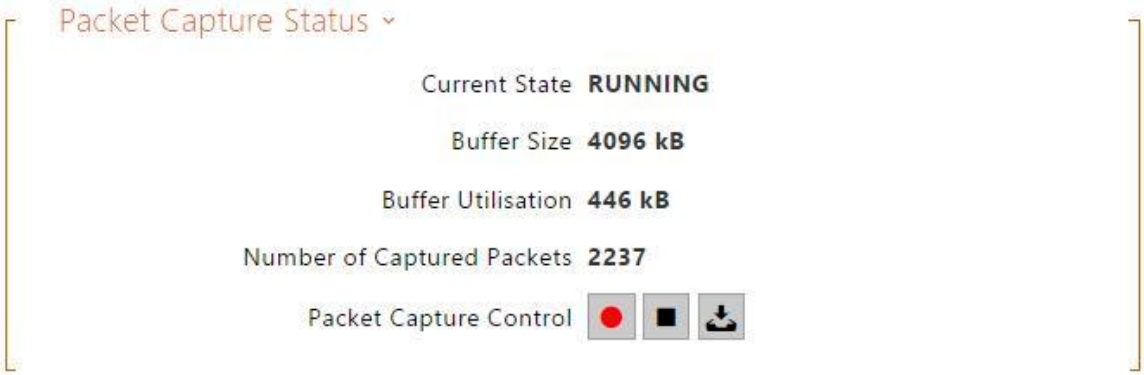
- **MD5 authentication enabled** – enable authentication of network devices via the 802.1x EAP-MD5 protocol. Do not enable this function if your LAN does not support 802.1x. If you do so, the **2N® Access Unit** will become inaccessible. ■ **Password** – enter the access password for EAP-MD5 authentication.



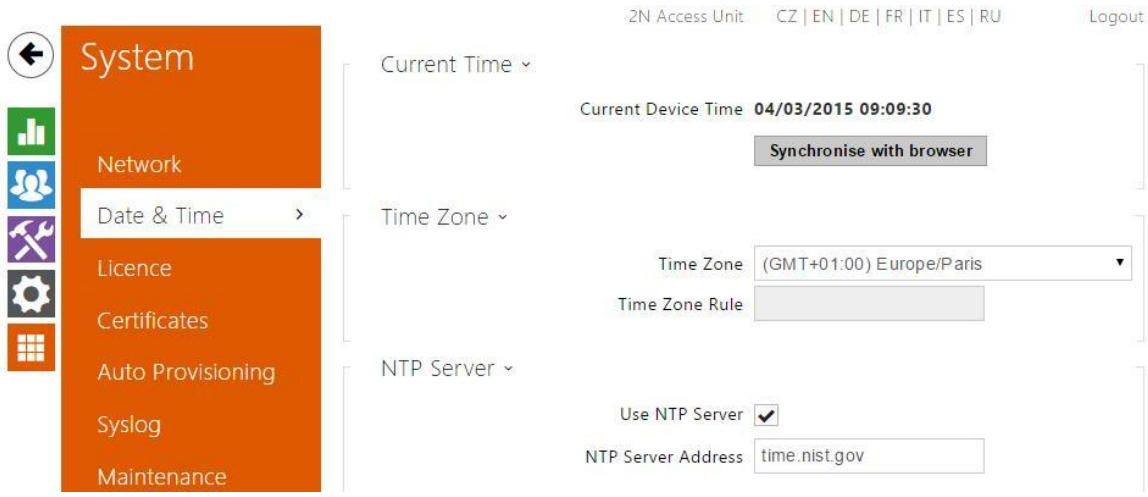
- **TLS authentication enabled** – enable authentication of network devices via the 802.1x EAP-TLS protocol. Do not enable this function if your LAN does not support 802.1x. If you do so, the **2N® Access Unit** will become inaccessible.
- **Trusted certificate** – specify the set of trusted certificates for verification of the RADIUS server public certificate validity. Choose one of three sets of certificates; refer to the Certificates subsection. If no trusted certificate is included, the RADIUS public certificate is not verified.
- **User certificate** – specify the user certificate and private key for verification of the **2N® Access Unit** authorisation to communicate via the 802.1x-secured network element port in the LAN. Choose one of three sets of user certificates and private keys; refer to the Certificates subsection.

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.



5.5.2 Date and Time



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

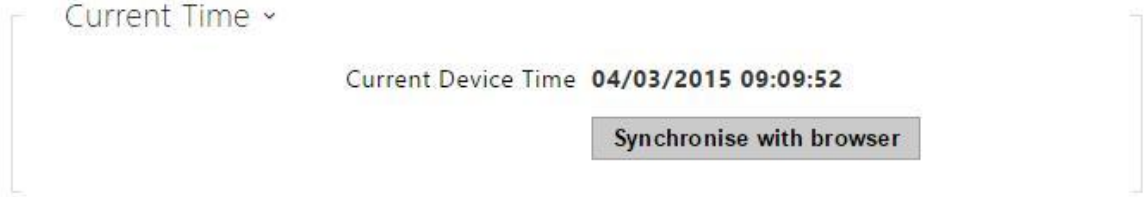
2N® Access Unit is equipped with a back-up real-time clock to withstand up to several days' long power outages. You can synchronise the **2N® Access Unit** time with your PC anytime by pressing the **Synchronise** button.

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.

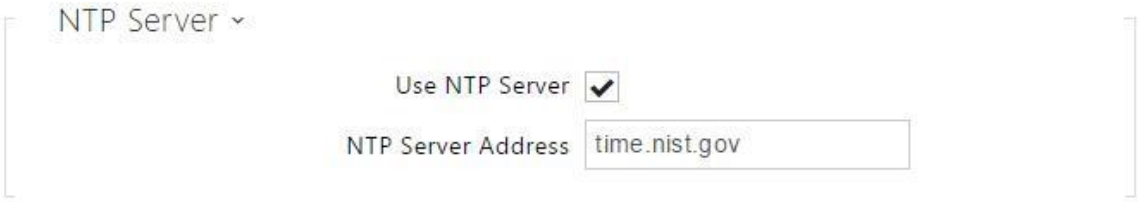
List of Parameters



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

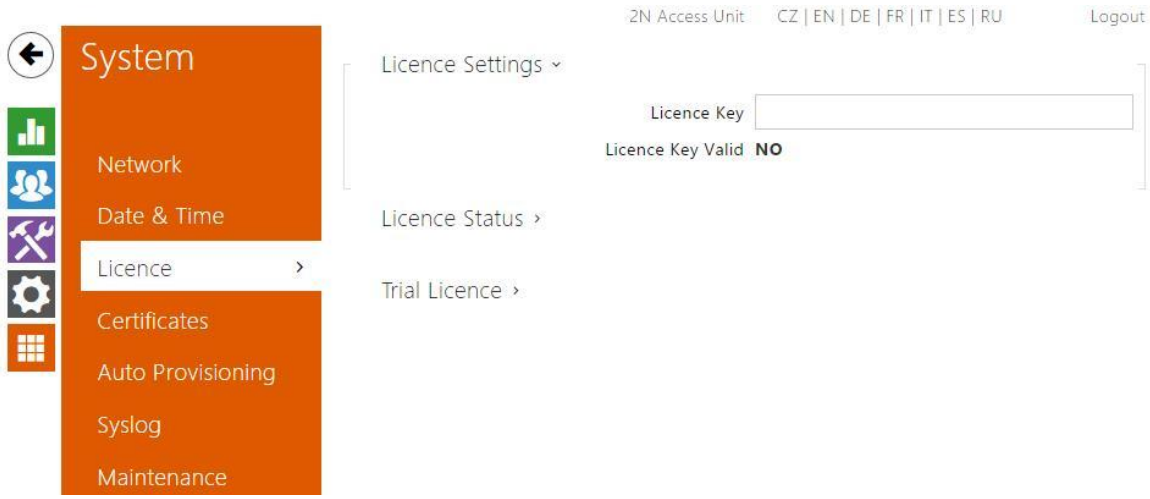
your PC time value.

- **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** – 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



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

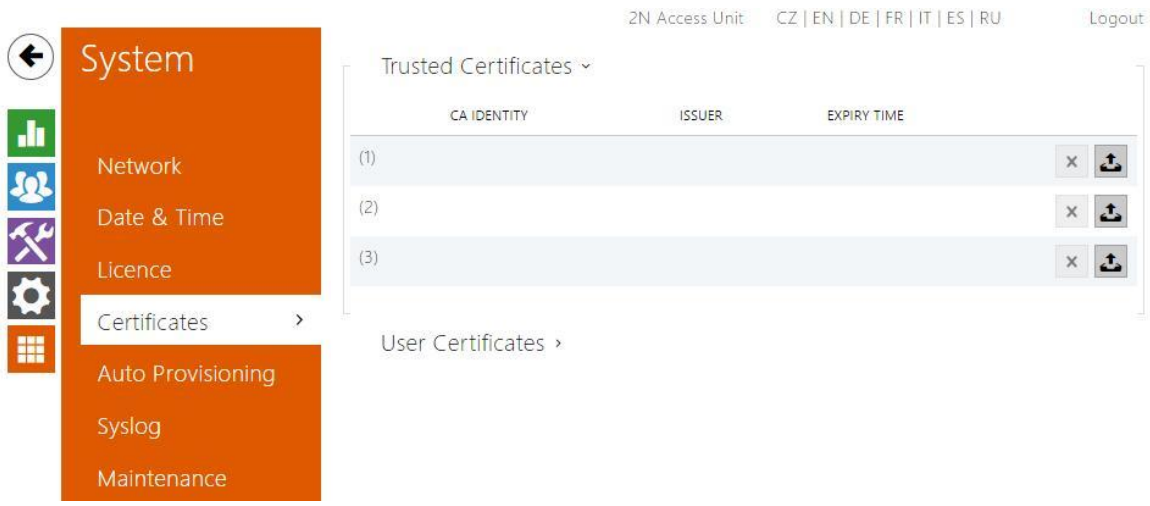
- **Current licence** – display the current licence type: Basic, Gold or Enhanced.
- **Enhanced Security** – check whether the functions activated by the Enhanced Security licence are available.
- **Enhanced Audio** – check whether the functions activated by the Enhanced Audio licence are available.
- **Enhanced Video** – check whether the functions activated by the Enhanced Video

licence are available.

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

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

5.5.4 Certificates



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

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

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

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.

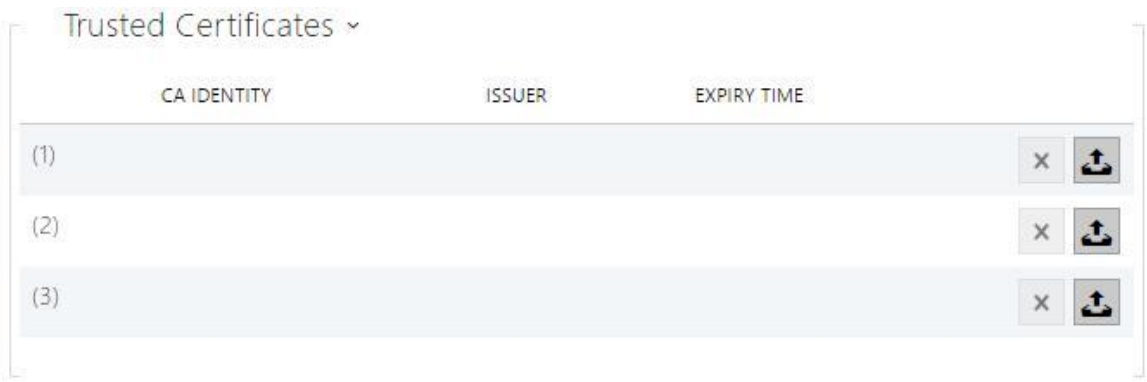
2N® **Access Unit** accepts the DER (ASN1) and PEM certificate formats.

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

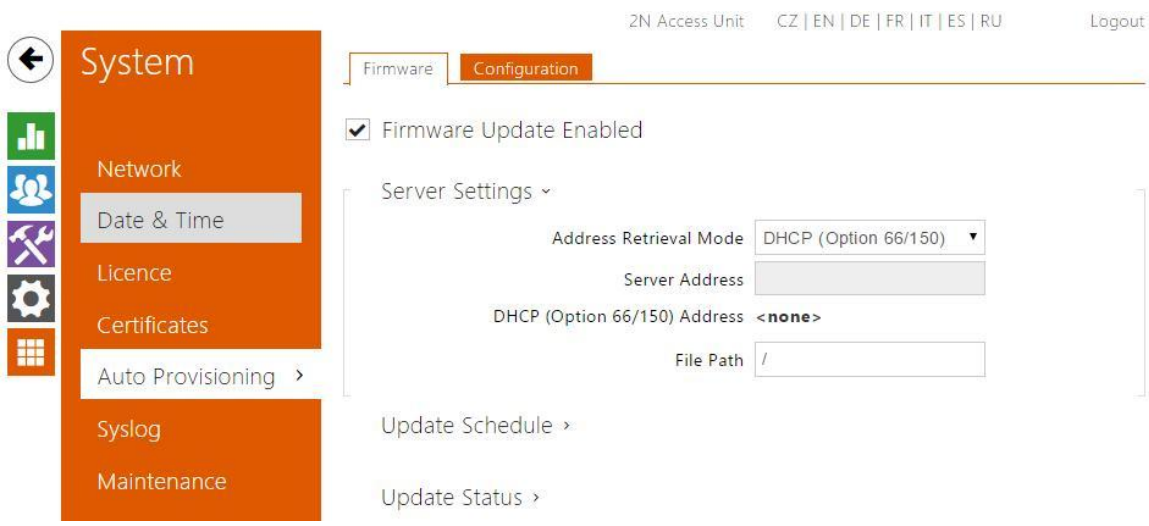
- If you use the Self Signed certificate for encryption of the intercom web server – browser communication, the communication is secure, but the browser will warn you that it is unable to verify the **2N®** **Access Unit** certificate validity.

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



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



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:

a. **MODEL**-firmware.bin – **2N®** **Access Unit** firmware
b. **MODEL**-common.xml – common configuration for all **2N®** **Access Unit**
c. **MODEL**-**MACADDR**.xml –specific configuration for one **2N®** **Access Unit**

MODEL in the filename specifies the intercom model:

a. **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:

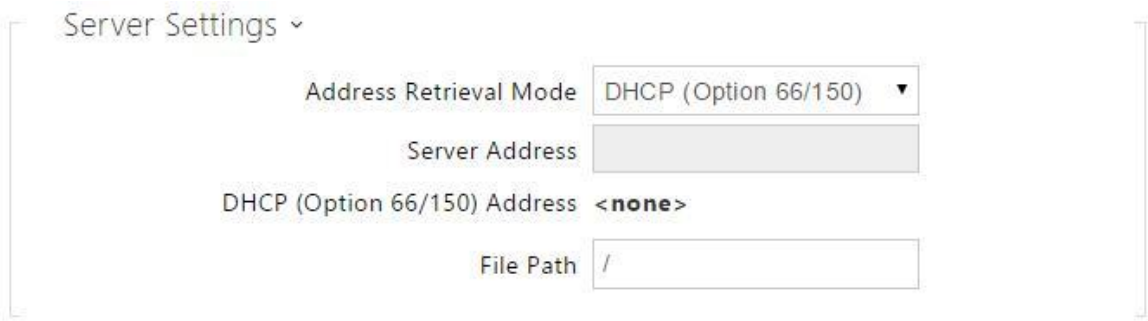
- au-firmware.bin
- au-common.xml
- au-00-87-12-aa-00-11.xml

Configuration

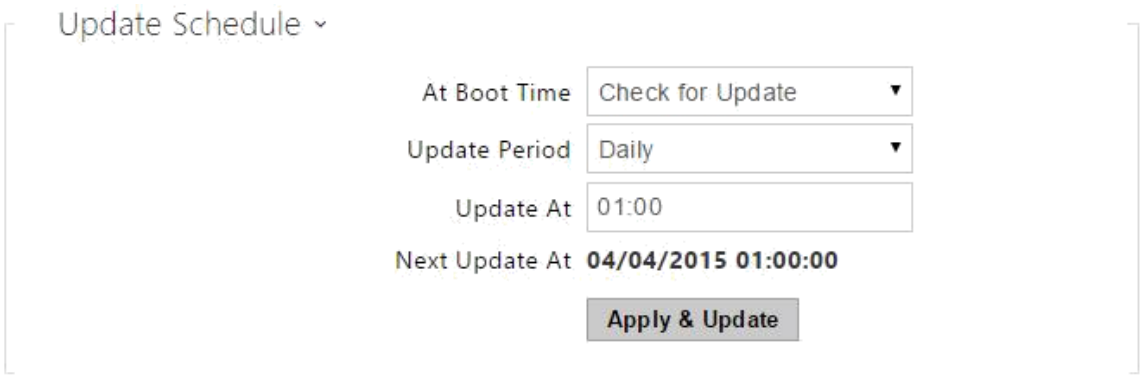
Use the Configuration tab to set automatic configuration download from the server defined by you. The **2N® Access Unit** periodically downloads a file from the server and gets reconfigured without getting restarted.

List of Parameters

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



- **Address retrieval mode** – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 shall be used.
- **Server address** – enter the TFTP (tftp://ip_address), HTTP (http://ip_address) or HTTPS (https://ip_address) server address manually.
- **DHCP (Option 66/150) address** – check the server address retrieved via the DHCP Option 66 or 150.
- **File path** – set the firmware/configuration filename directory or prefix on the server. The **2N® Access Unit** expects the au_firmware.bin, au-common.xml and au-MACADDR.xml files.

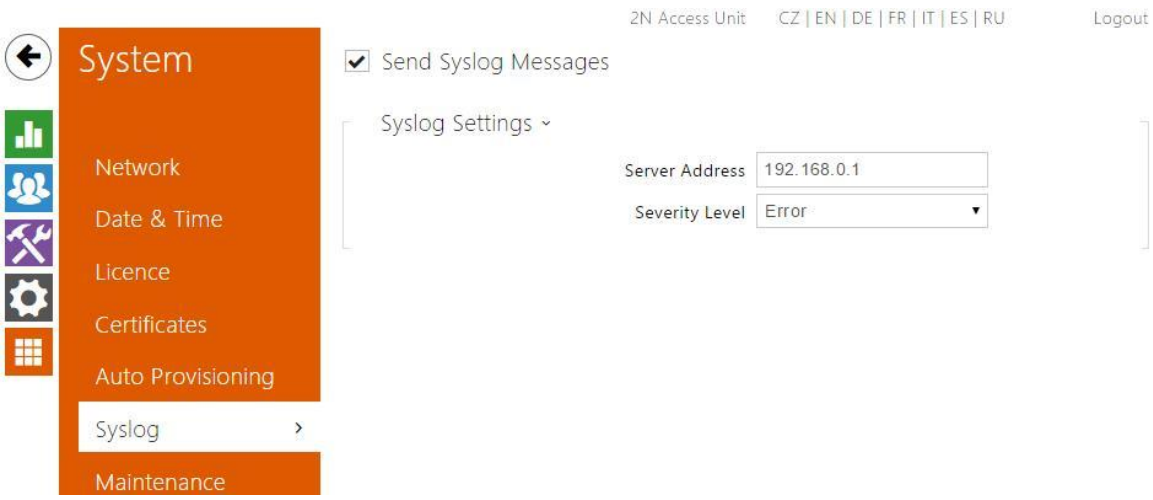


- **At boot time** – enable check and/or execution of update upon every **2N® Access Unit** start.
- **Update period** – set the update period: Hourly, Daily, Weekly or Monthly.
- **Update at** – set the update time in the HH:MM format for periodical updating at a low-traffic time. The parameter is not applied if the update period is set to a value shorter than 1 day.
- **Next update at** – display the next update time.

- **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.

5.5.6 Syslog



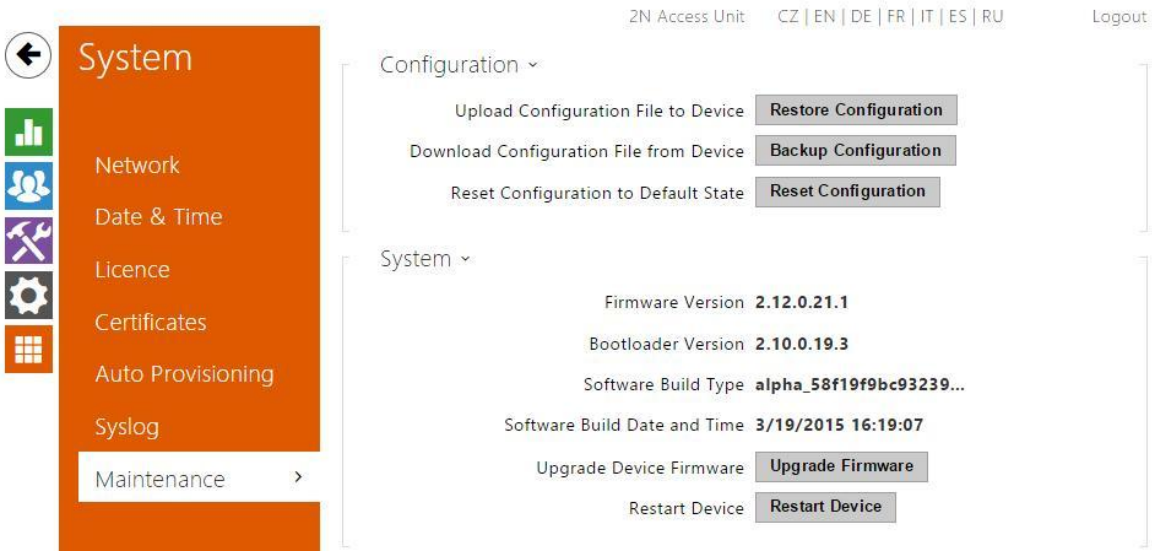
The **2N® Access Unit** allow you to send system messages to the Syslog server including relevant information on the device states and processes for recording, analysis and audit. It is unnecessary to configure this service for common **2N® Access Unit** operation.

List of Parameters

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

- **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



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.

- **Back up 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.

2N TELEKOMUNIKACE a.s.
Modřanská 621, 143 01 Prague 4, Czech Republic
Phone: +420 261 301 500, Fax: +420 261 301 599
E-mail: sales@2n.cz
Web: www.2n.cz

1758v2