2N Helios IP

IP Intercom

Configuration Manual

Version: 2.17

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® 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

The 2N Helios IP door intercoms can smartly replace traditional doorbell push-button speakerphone panels and all wiring, bells and home intercom installations in buildings with structured cabling. The intercoms provide more advanced and wider services than standard home phones. The installation is very easy, all you need is connect the intercom to the other LAN elements using a UTP cable and set necessary parameters.

Thanks to the integrated SIP protocol, the intercom can make use of all VoIP services: call forwarding at absence (to another office, VoiceMail or a cellular phone) or call transfer (from the secretary's office to the required person, e.g.).

The intercoms are equipped with a programmable number of quick dial buttons for speed calling to the users whose numbers are included in the intercom Users list. Each of the quick dial buttons can be assigned up to three phone numbers, which can be dialled in parallel or sequentially. Thanks to an integrated time sheet it is possible to configure each of the buttons in such a way that the called party is always accessible and/or calls to selected phone numbers can be barred off the working hours.

Some 2N Helios IP models are equipped with a numeric keypad, which can be used as a code lock or a standard push-button phone.

The 2N Helios IP intercoms help LAN users scan the area in front of the camera via video streaming. Thanks to the full ONVIF support, the intercoms can become part of the Video Surveillance System in your facility .

The 2N Helios IP intercoms can be equipped with an RFID card reader for authorised access control and thus become a key part of your surveillance or attendance control systems.

The 2N Helios IP intercom is equipped with a relay switch (and, optionally, other relays and outputs), which controls the electric lock or other equipment connected to the intercom. Its activation time and method can be programmed flexibly: it can be activated by a code, automatically by a call, by pressing a button, and so on.

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 intercom configuration interface address to connect to the LAN successfully. Automatic IP address retrieval from the DHCP server is set by default in the 2N Helios IP intercoms. Thus, if connected to a network in which a DHCP server configured to assign IP addresses to all new devices is available, the intercom will obtain an IP address from the DHCP server. The intercom 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 intercom voice function; refer to the Installation Manual of your intercom model.

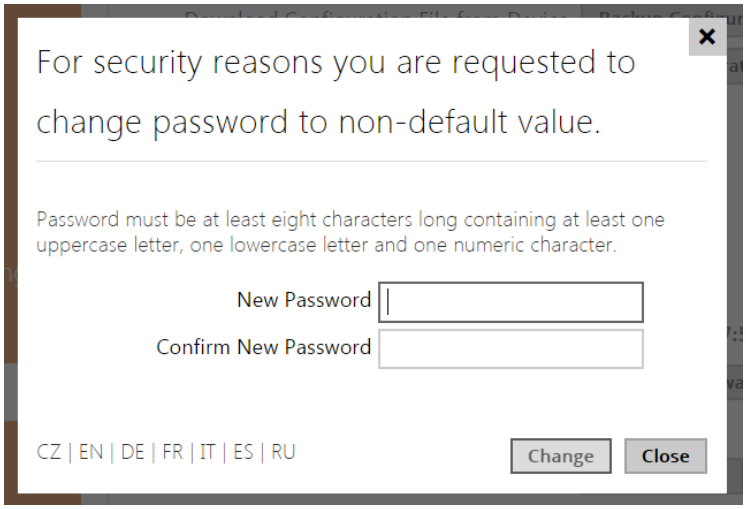
If there is no DHCP server in your LAN, use the intercom buttons to set the static IP address mode, refer to the Installation Manual of your intercom model. Your intercom address will then be 192.168.1.100. Use it for the first login and then change it if necessary.

Now enter the intercom IP address into your favourite browser. We recommend you to use the latest Chrome, Firefox or Internet Explorer 9+ versions as 2N Helios IP 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.

The intercom requires a password change upon the first login. Strong passwords are only accepted: eight characters at least including one capital letter, one small letter and one digit.



Remember the new password well or put it down just in case. Because if you forget the password, you will have to reset the intercom to default values (refer to the Installation Manual of your intercom model) and lose all your current configuration changes.

Tip

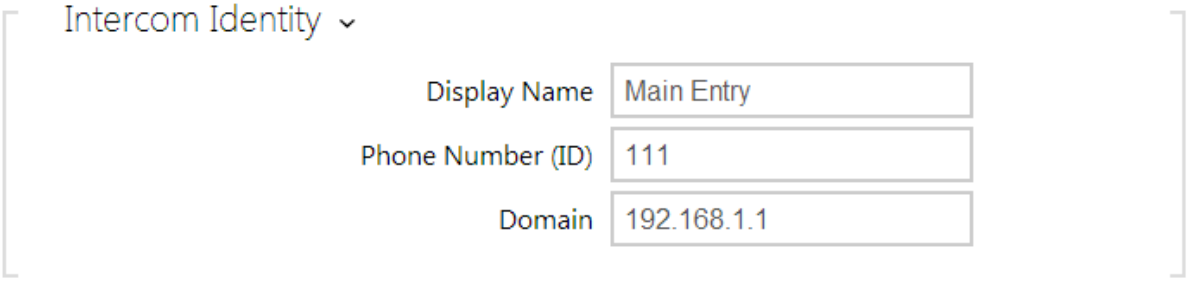
- FAQ: IP address - How to get IP address of 2N Helios IP

Firmware Update

We also recommend you to update your intercom firmware upon the first login to the intercom. Refer to **www.2n.cz** for the latest firmware version. Press the **Update Firmware** button in the **System / Maintenance** menu to upload firmware. The intercom will get restarted upon upload and only then the updating process will be complete. The process takes about 30 seconds.

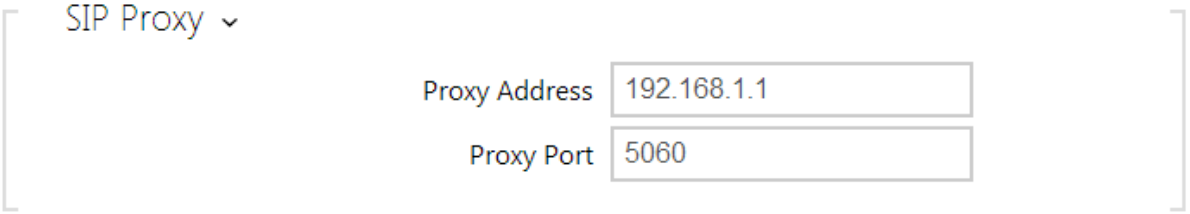
SIP Server Connection Setting

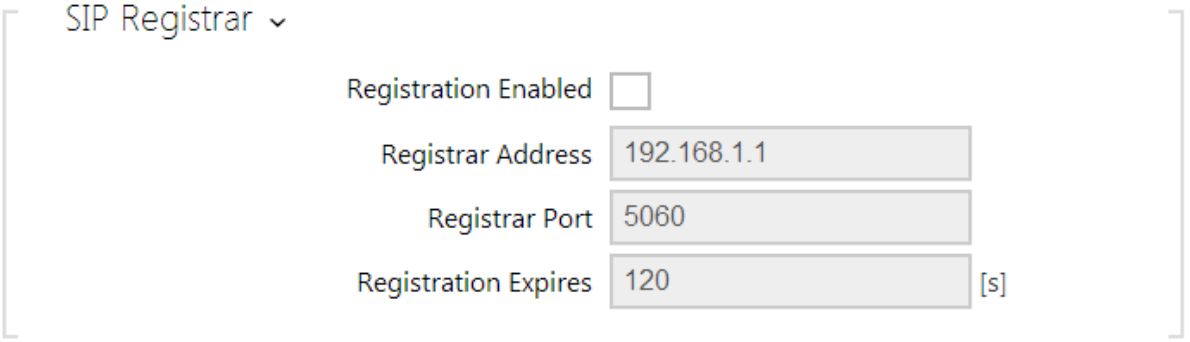
Set the following parameters in the **Services** / **Phone** / **SIP** menu to allow your intercom make calls and be accessible within your VoIP infrastructure.



- **Display name** – set the name to be displayed as CLIP on the called party's phone, in the login window and on the web interface start page.
- **Phone number (ID)** – set the intercom phone number (or another unique ID composed of characters and digits) to identify the intercom uniquely in calls and registration.
- **Domain** – set the domain name of the service with which the intercom is registered. Typically, it is equivalent to the SIP Proxy or Registrar address. If you do not use a SIP Proxy in your intercom installation, enter the intercom IP address.

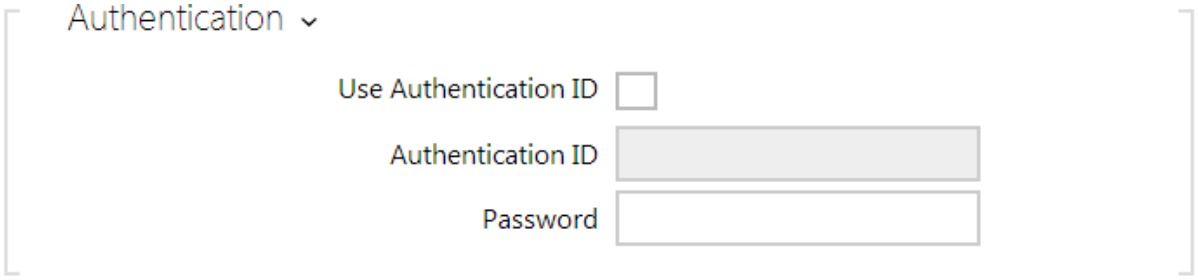
If you use a SIP server (Proxy, Registrar), set the addresses for the following network elements:





- **Proxy address** – set the SIP Proxy IP address or domain name.
- **Registrar address** – set the SIP Registrar IP address or domain name. The SIP Proxy and SIP Registrar addresses are usually identical.
- **Registration enabled** – enable intercom registration with the set SIP Registrar.

If your SIP server requires authentication of terminal equipment, enter the following parameters:



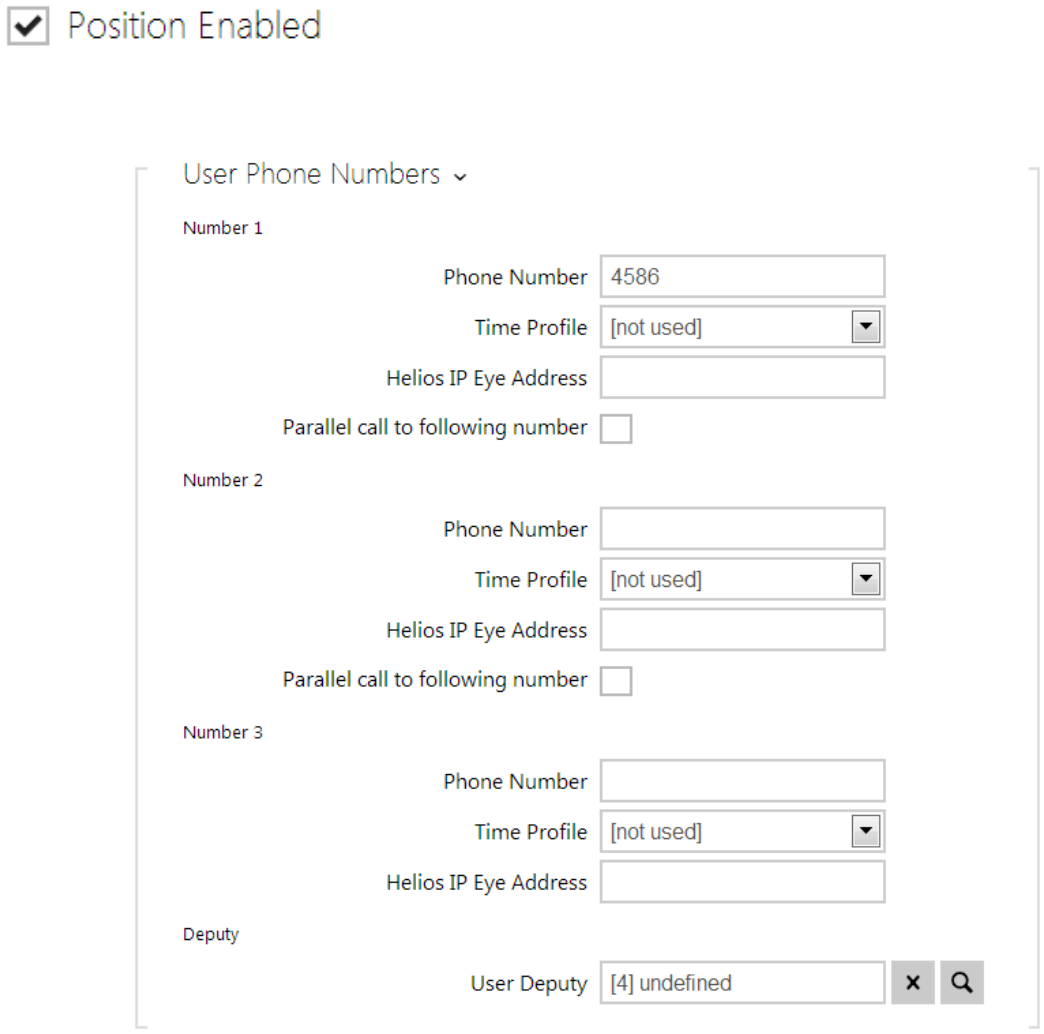
- **Password** – enter the password for intercom authentication.

Quick Dial Button Settings

All the **2N Helios IP** models are equipped with quick dial buttons. If you press a quick dial button, a call will be set up to the phone number assigned to the respective Users list position.

Select position 1, which corresponds to quick dial button 1, in the **Directory / Users** menu.

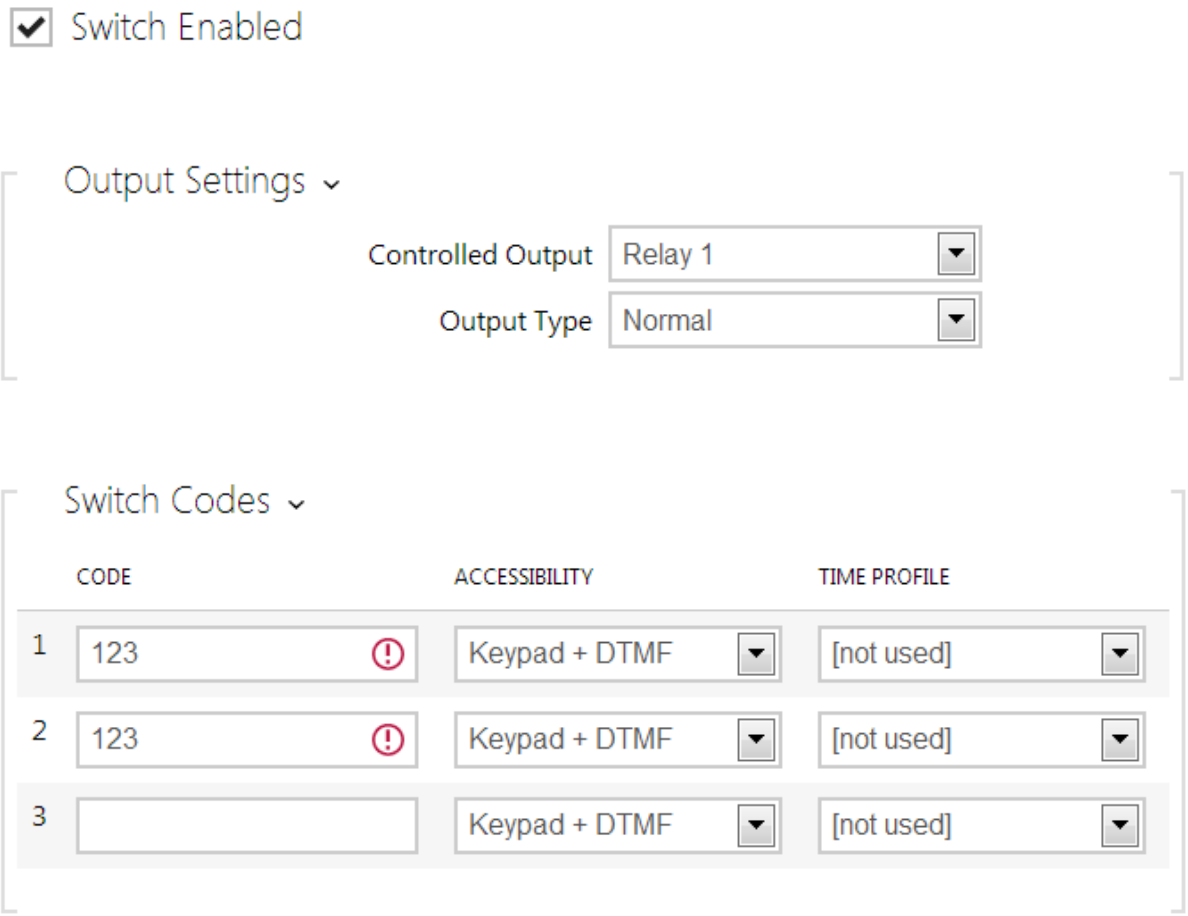
Enable the position in the **Position Enabled** field and enter the called station phone number into the **Phone Number** parameter in the **User Phone Numbers** section.



You can also use the **2N Helios IP** intercom with one or more IP phones without a SIP server. Use the **Direct SIP Call** for outgoing calls and enter the called phone SIP address (sip:phone_number@phone_ip_address) instead of the phone number.

Electric Lock Switching Settings

An electric lock can be attached to the **2N Helios IP** intercoms and controlled by a code from the intercom numeric keypad, or a code from the IP phone keypad during a call. Connect the electric lock as instructed in the Installation Manual of your intercom model.



Enable the switch in the **Switch Enabled** parameter in 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. Model Differences and Function Licensing

This manual is valid for all members of the 2N Helios IP family and so some features described herein are only available in selected 2N Helios IP models or need to be activated with a valid licence key. This section provides a short list of differences between the models and licences which affect the configuration options. If a function is not available in all the models, there is a note in the respective subsection and reference to this section.

The table below includes an overview of properties and functions of all the 2N Helios IP models.

Property/Model	2N® Helios IP						
	Verso	Vario	Force	Safety	Uni	Audio Kit	Video Kit
Part No.	9155...	9137....	9151...	9152...	9153...	9154...	9154...C
Integrated camera	optional			no			
Camera resolution	1280 x 960	640 x 480					
External analogue camera support	no						yes
External IP camera support	yes				no		yes
Internal RFID card reader	optional			no			
Display	optional		no				

Property/Model	2N® Helios IP						
	Verso	Vario	Force	Safety	Uni	Audio Kit	Video Kit
Basic unit button count	1	1, 3 or 6	1, 2 or 4	1	1 or 2	up to 16 external programmable buttons	
Button extenders	up to 145	up to 48	no				
Numeric keypad	optional			no			
Digital input	yes	optional			no	2	
Wideband audio codecs (L16, G. 722)	yes				no		yes
Amplifier power output	2 W	150 mW	1 W			10 W	
Adjustable microphone gain	no					yes	
Extended amplifier power output (10 W)	no		yes		no	no	
Tamper switch	optional	no	optional		yes	no	
Users position count	1999				2	16	
User deputy	yes				no	yes	
User activation/deactivation	yes				no	yes	
Controlled switch count	4				1	4	
Switch universal code count	10				2	10	
User profile count	20						

Property/Model	2N® Helios IP		
JPEG HTTP video	yes	no	yes
2N® Helios IP Eye support	yes	no	yes
Telephone mode	yes	no	yes

Some **2N Helios IP** functions are unavailable until a valid licence key is entered (refer to the Licence subsection). The following types of licences are available:

- Enhanced Audio (Part No. 9137905)
- Enhanced Video (Part No. 9137906)
- Enhanced Integration (Part No. 9137907)
- Enhanced Security (Part No. 9137908)
- Gold (Part No. 9137909)
- G.729 (Part No. 9137902)
- InformaCast (Part No. 9137910)
- NFC (Part No. 9137915)

The G.729 licence allows the audio codec G.729 to be used.

The InformaCast licence allows the SingleWire InformaCast protocol to be used.

The NFC licence enables authentication via NFC-equipped mobile phones for selected 13Mhz RFID card reader models.

No licenced features are available for the **2N® Helios IP Uni** model.

The table below includes the functions that need to be activated by the licence keys corresponding to the above mentioned licences. The licences can be combined arbitrarily.

Property/Licence	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	Gold (Profi)
User sounds	•					•
Automatic audio test	•					•
Noise detection	•					•

Property/Licence	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	Gold (Profi)
Audio/video streaming (RTSP Server)		•				•
External IP camera support		•				•
ONVIF support		•				•
PTZ function support		•				•
Motion detection support		•				•
Extended switch setting options			•			•
HTTP API (see note below)			•			•
Automation functions			•			•
E-mail sending (SMTP Client)			•			•
Automatic update (TFTP /HTTP Client)			•			•
FTP client			•			•
SNMP client			•			•
TR-069			•			•
802.1x support				•		•
SIPS (TLS) support				•		•
NFC support					•	•

Note

- *Full **HTTP API** function is available with the Gold or Enhanced Integration licence only. Only Camera API a Switch API is available without this licence.*

Note

- Extended switch setting options – switch activation with quick dial button; time profile for switch

Tip

- FAQ: License for 2N Helios IP – How to get it

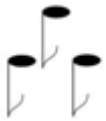
4. Signalling of Operational Statuses

2N Helios IP generates sounds to signal switching and changes 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.*

Tone	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.

Tone	Meaning
	**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.
	**Call prolongation confirmation signalling** Calls are time-limited in **2N Helios IP** for security reasons (protection against blocking). Refer to the Miscellaneous subsection for details.
	**Internal application launched** The internal application is launched upon **2N Helios IP** power up or restart. A successful launch is signalled by this tone combination.
	**Connected to LAN, IP address received** **2N Helios IP** 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 signals UTP cable disconnection from **2N Helios IP**. Disconnection is signalled by this tone combination.
	**Invalid telephone number or invalid switch activation code** **2N Helios IP** allows the user to dial an extension number directly using the keypad or enter the door unlocking code. An invalid code is signalled by this tone sequence.
	**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 Helios IP** Installation Manual for details.

Tone	Meaning
	Call end signalling **2N Helios IP** enables the user to set a call end timeout to avoid call blocking. Press a key on your VoIP phone to extend the call time during this timeout.
	**Connected VoIP phone** This short tone signals successful connection between a VoIP phone and **2N Helios IP**.

5. Intercom Configuration

Start Screen

The start screen is an introductory overview screen displayed upon login to the intercom web interface. Use the back arrow  in the left-hand upper corner of the following web interface pages to return to this screen anytime.The screen header includes the intercom 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® Helios IP configuration includes 5 main menus: State, Directory, Hardware, Services and System including submenus; see below.

Status

- Device – essentials on the intercom
- Services – information on active services and their states
- Licence – current states of licences and available intercom functions

Directory

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

Hardware

- Switches – electric lock, lighting, etc. settings
- Audio – audio, signalling, etc. volume control, microphone parameters
- Camera – internal camera, external IP camera settings
- Keyboard – button and keyboard settings
- Buttons - user speed dial settings
- Display – basic display settings
- Card Reader – card reader, Wiegand interface settings
- Extenders – 2N® Helios IP Verso extender settings

Services

- Phone – telephone and SIP connection settings
- Streaming – audio/video streaming settings (ONVIF, RTSP, Multicast, etc.)
- Onvif – Onvif settings
- E-Mail – E-mail sending and SMTP connection settings
- Automation – flexible intercom settings according to the user's requirements
- HTTP API – HTTP API authorisation settings
- User Sounds – user sound settings and upload
- Web Server – web server and access password settings

- Audio Test – automatic audio test settings
- SNMP – SNMP 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
- Auto provisioning – automatic firmware and configuration update settings
- Syslog – syslog message sending settings
- Maintenance – backup and configuration reset, firmware update

5.1 Status

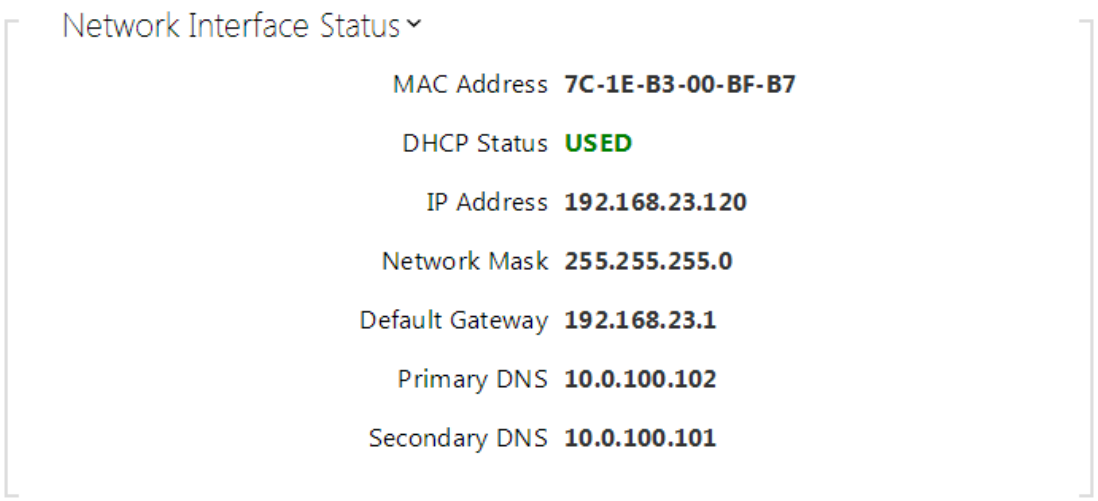
The **Status** menu provides clear status and other essential information on the intercom. The menu is divided into five tabs: **Device**, **Services, Licence, Access Log** and **Events**.

Device

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

Services

The **Services** tab displays the status of the network interface and selected services.

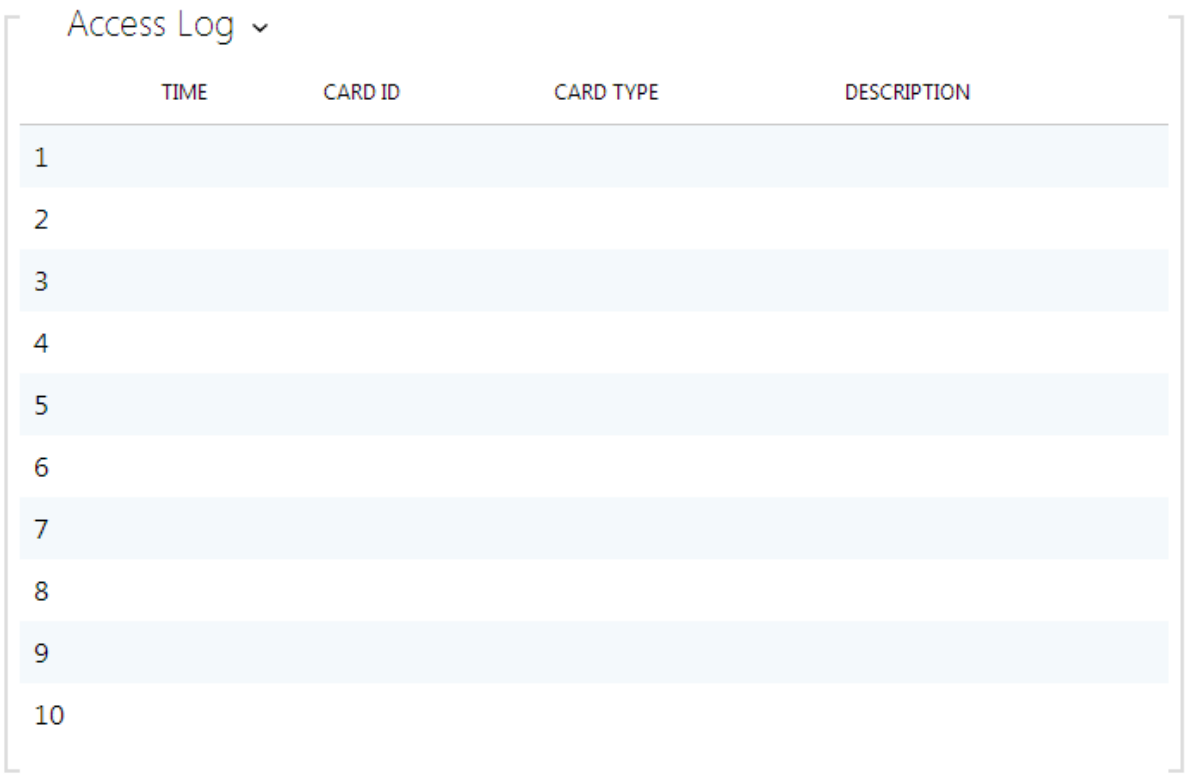


Licence

The **Licence** tab displays the list of licensed functions of the intercom including their current availability (on the basis of a valid licence key entered in the **System | Licence** menu).

Access Log

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

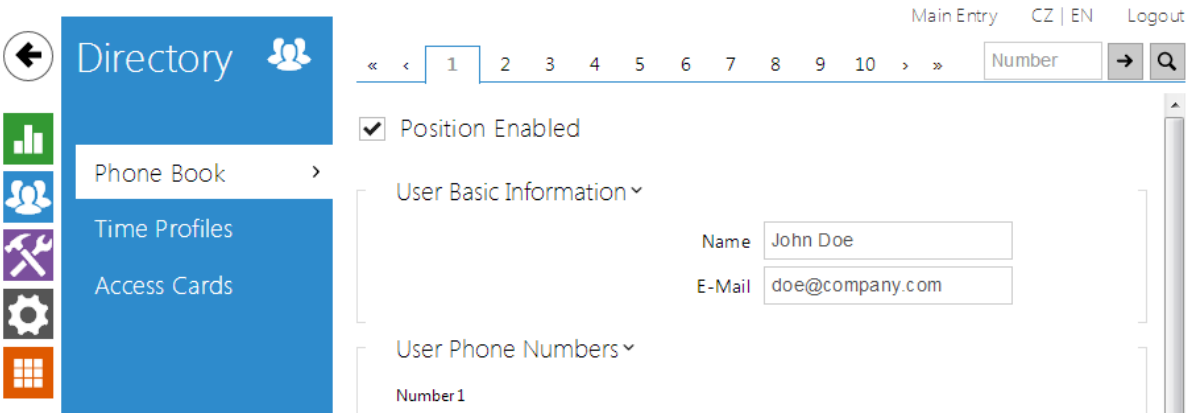


5.2 Directory

Here is what you can find in this subsection:

- 5.2.1 Users
- 5.2.2 Time Profiles
- 5.2.3 Holidays
- 5.2.4 Access Cards

5.2.1 Users



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

The Users list contains up to 1999 users (variable in the **2N Helios IP** models) – typically, each user is assigned just one item (position 1 to 1999).

The Users list includes the users that can be called via the quick dial buttons and the users that are assigned the RFID card, code, etc. access to the building.

Use the **Hardware / Buttons** menu to assign the quick dial users. By default, button 1 is assigned to position 1 in the user list, button 2 to position 2 in the phone book, etc. You can change the user and button settings as necessary. Most of the **2N Helios IP** intercoms are equipped with one or more quick dial buttons. Refer to the Installation Manual of your intercom model for the quick dial button count and extending options.

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.
- **Virtual number** – number to be used for user calling via a numeric keypad. The number can have 2 to 4 digits. Virtual numbers are not associated with user telephone numbers. They are included in an independent numbering plan allowing you to withhold user telephone numbers, especially in installations where the quick dial button count is insufficient. The visitor enters a virtual number via the numerical keypad and presses the * key. You are recommended to place a clear user/virtual number list nearby including simple instructions for use to facilitate this type of user calls. Enable this function in the **Dial by Numeric Keypad** in the **Hardware / Keyboard** menu. The following options are available:
  User phone numbers – enter up to three user numbers to be called sequentially

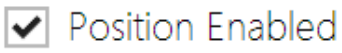
in predefined time intervals or at the same time (group calls). You can assign a time profile and the address of the PC on which the 2N® Helios IP Eye application is running to display the intercom camera image before call answering, for example.

- Disabled – no user number can be entered via the numeric keypad.
- User virtual number – enter the user virtual number via the numeric keypad and press * to start the call.
- User position number – enter the user position (01 – 1999) via the numeric keypad and press * to start the call. This original FW 2.10 option is no more recommended due to potential user management troubles.

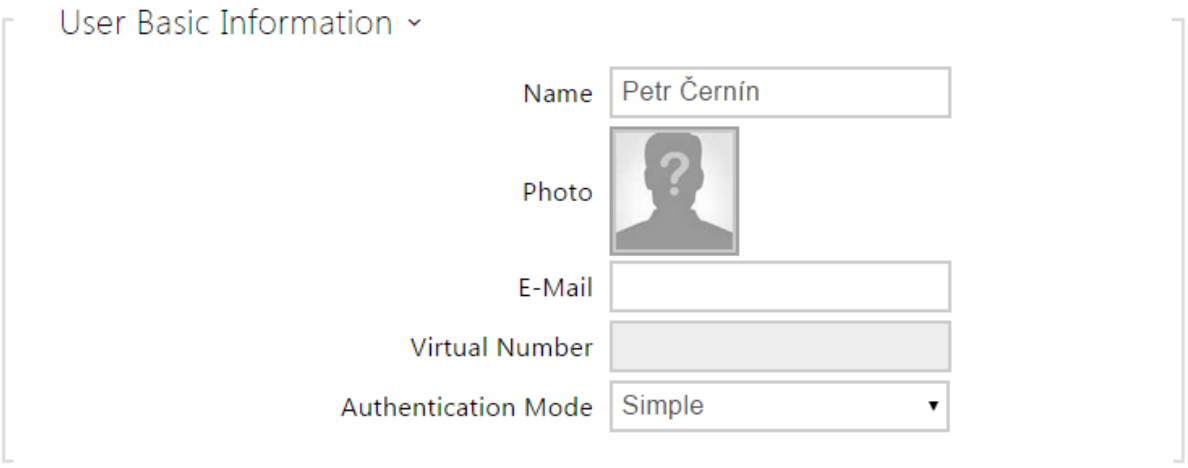
- User switch codes – enter the switch activating user codes (door lock activation, e.g.). A time profile can be assigned to each code.
- User cards – enter the user-defined access cards with/without a time profile. Enable/disable double authentication (valid user card + switch activating code) for each user.
- User activation and deactivation codes – enter the user-defined codes to activate /deactivate speed dial and virtual number calling. Calls to a deactivated user are automatically forwarded to the User deputy.

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.

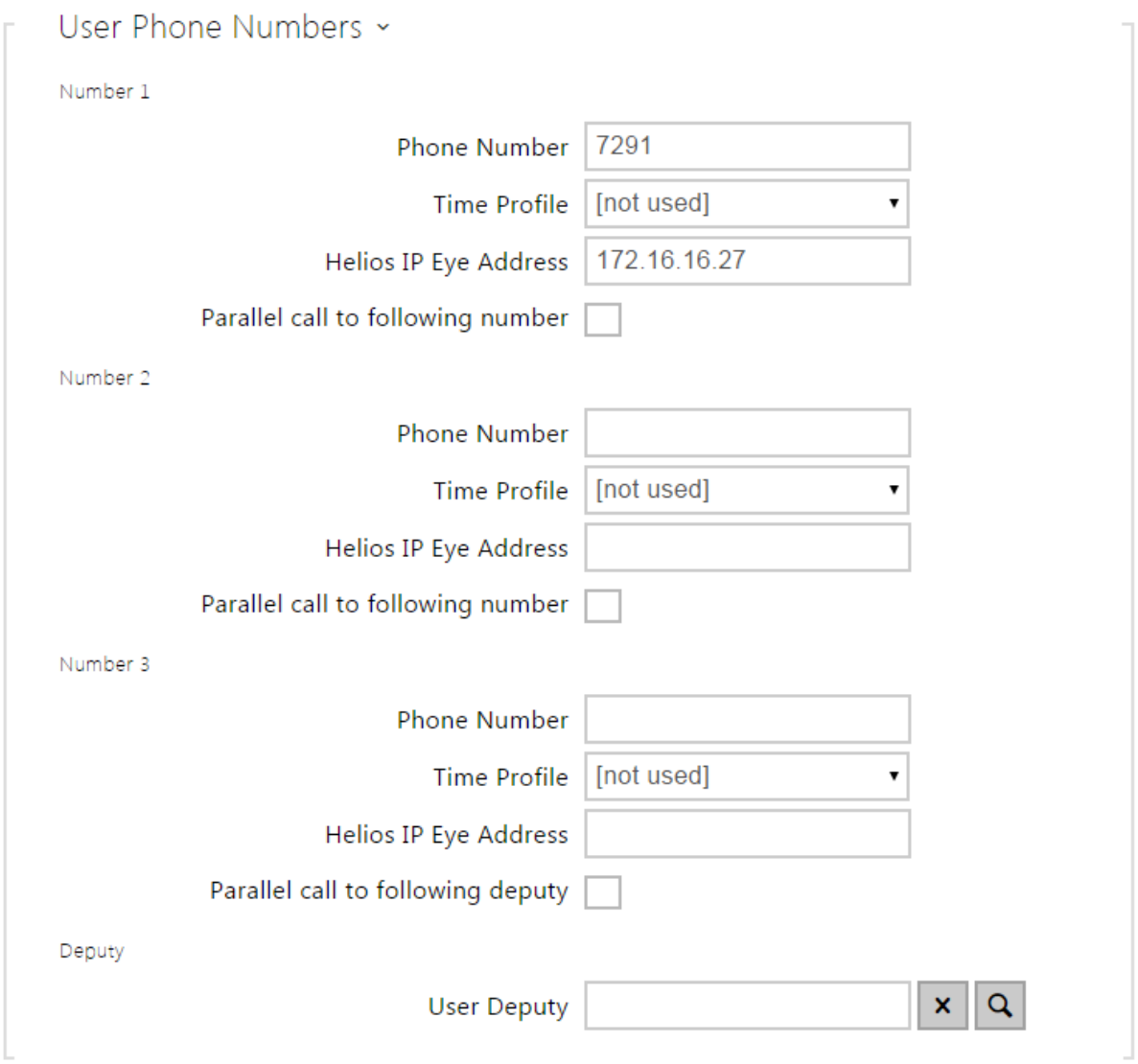
List of Parameters



- **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.
- **Photo** – add a photo for display. Click on the image to select a file with the photo saved on the disk or scan an image via a web camera connected to the PC. This parameter is available in display-equipped models only.
- **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.
- **Virtual number** – select a number to be used for user calling via a numeric keypad. Enable this function in the **Dial by Numeric Keypad** in the **Hardware / Keyboard** menu.
- **Authentication mode** - set card + numeric code authentication for a user: apply a valid user card and then enter one of the switch activating codes (within ten seconds after tapping) to activate the switch in this mode.



You can assign up to three user phone numbers to each user position. In case the user is inaccessible on one number, the following number will be dialled after a ringing timeout. Enable the **Parallel call to following number** to enable dialling multiple numbers simultaneously. The phone number validity can also be time profile-limited.

- **Phone number** – enter the phone number of the station to which the call shall be routed. Enter the address sip:[user_id@]domain[:port] for Direct SIP calling, e.g.: sip:200@192.168.22.15 or **sip:name@yourcompany**. Enter device:device_name for calls to the **2N® Helios IP Mobile** application. Set the device name in the mobile application. Enter **/1** or **/2** behind the phone number to specify which SIP account shall be used for outgoing calls (account 1 or 2).
- **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.

- **Helios IP Eye address** – set the address of the PC to be sent a special UDP message on each active user phone number call. With the aid of this message, the **2N® Helios IP Eye** application displays the camera image screen for those users who are not provided with a display-equipped videophone. Enter the address as follows: domain[:**port1**][:**port2**], e.g.: **computer.yourcompany.com** or 192.168.22.111. The **port1** and **port2** parameters are optional and are used in case there is Network Address Translation (NAT) between the PC and intercom and the addresses have to comply with the router or another NAT-executing device. The port1 (default value: 8003) parameter defines the destination port for the UDP messages sent to **2N® Helios IP Eye**. The port2 (default value: 80) parameter defines the destination port for the **2N® Helios IP Eye** – intercom HTTP communication.

Note

- *The 'Helios IP Eye Address' function is available in selected **2N Helios IP** models only (refer to the model and licence overview).*
- *When Enhanced Integration is not licensed on a device, it is possible to control the locks only when a call is in progress. If a call with user, who has **2N® Helios IP Eye** address filled in, is in progress, no licence is needed to control the locks.*

Tip

- FAQ: **2N® Helios IP Eye - How to set**

Tip

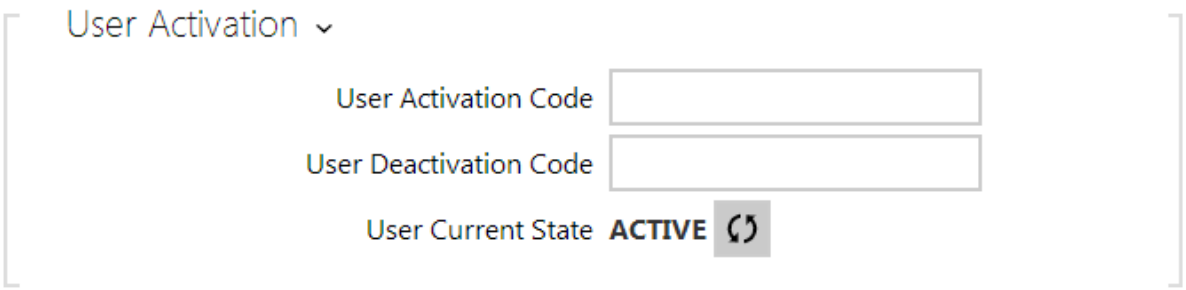
- Video Tutorial: **SW application for IP intercoms - 2N® Helios IP Eye**

- **Parallel call to following number** – enable group calling, i.e. calling to more phone numbers at the same time. You can call the first two numbers, the last two numbers, or all of the three user numbers in parallel. Answering one call automatically terminates the other calls.
- **Parallel call to following deputy** – extend group calling to include the User deputy.

- User deputy – select a user to which the user calls will be routed in the event of inaccessibility. Enter user position number or use search button. The deputy setting is applied when the user fails to answer the call to any of its phone numbers within the predefined timeout, or if the user numbers are inaccessible for other reasons (time profiles, user deactivation).

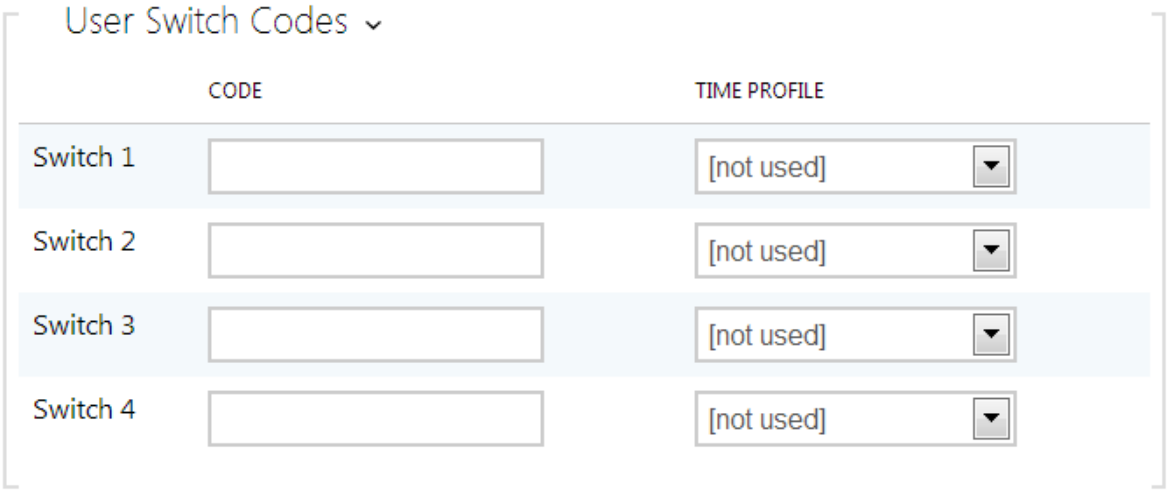
Note

- *The User Deputy function is available in selected **2N Helios IP** models only (refer to the model and licence overview).*



Each intercom user can be assigned its activation/deactivation code for call routing purposes. If a user is deactivated, calls are routed not to its phone numbers but to the predefined user deputy at inaccessibility.

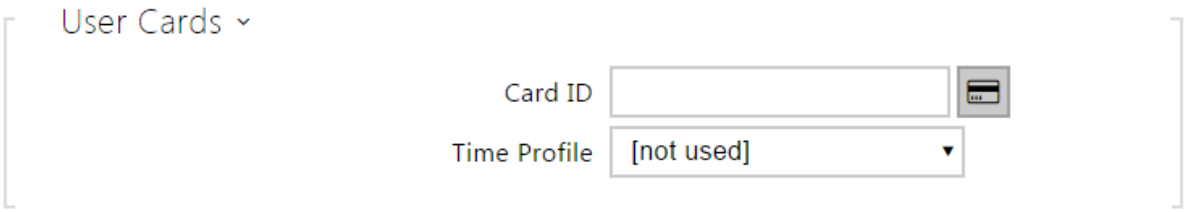
- **User activation code** – set a private user activation code: up to 16 characters including digits 0-9 only. If the user activation code is the only code defined or the activation and deactivation codes are identical, the activation code is used both for user activation and deactivation.
- **User deactivation code** – set a private user deactivation code: up to 16 characters including digits 0-9 only.
- **User current state** – select the current state of the user.



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

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 . If multiple time profiles are assigned to a code, the code is valid only if one of the profiles is active at least.

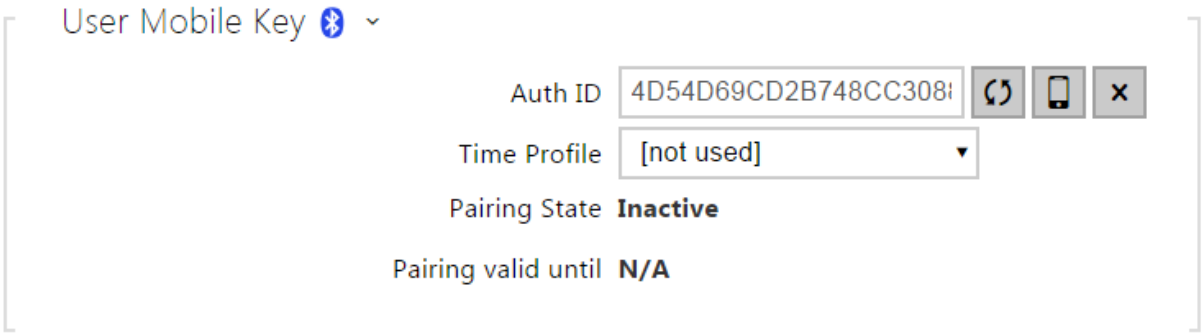


Each of the intercom users can be assigned one access RFID card. Refer to the **Access Cards** subsection for details.

- **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, th e user access card will be detected as invalid. If multiple time profiles are assigned to a card, the card is valid only if one of the profiles is active at least.

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**.



- **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

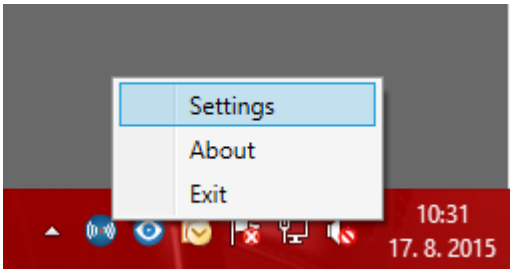
To pair a mobile phone with the user:

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.

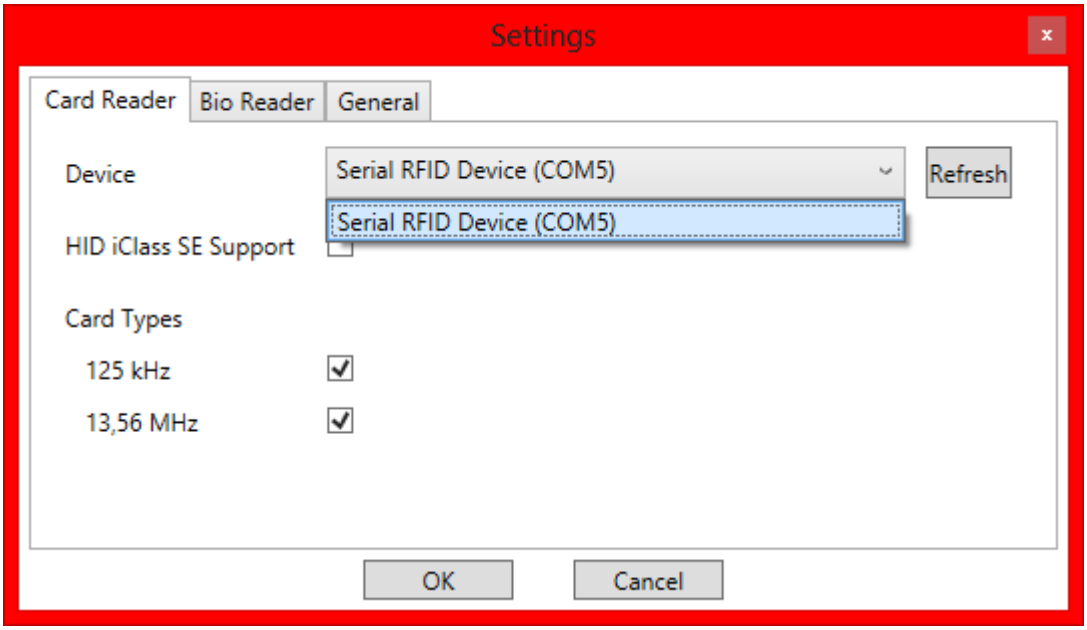
USB RFID Card Reader

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

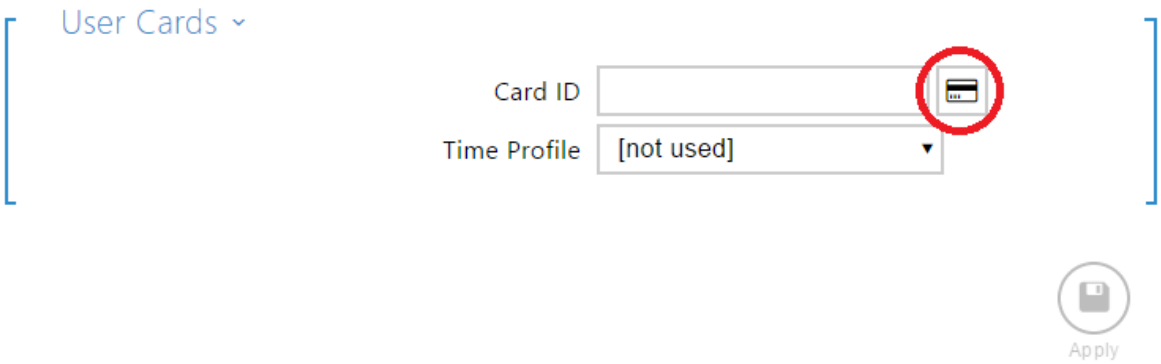
1. Go to the **2N Helios IP** USB Driver settings.



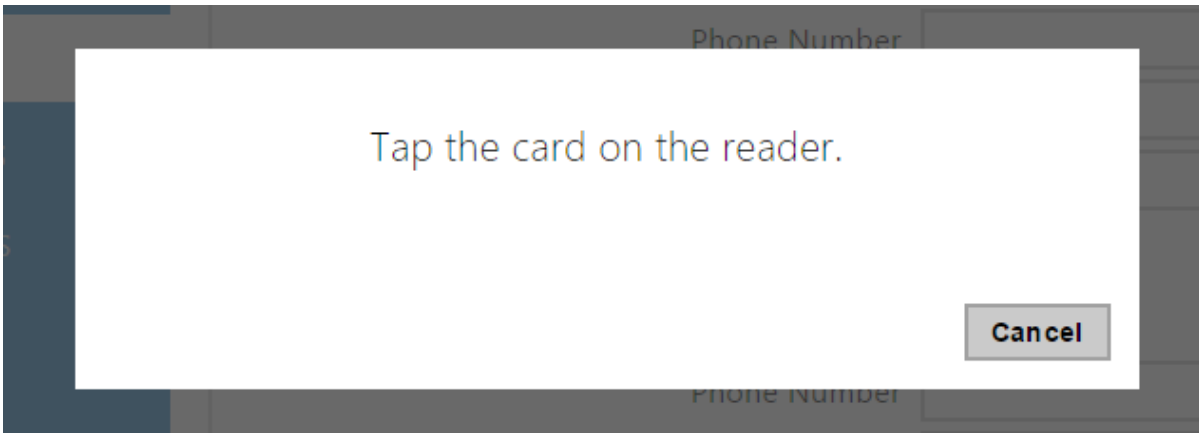
2. Set up the COM port for the connected reader.



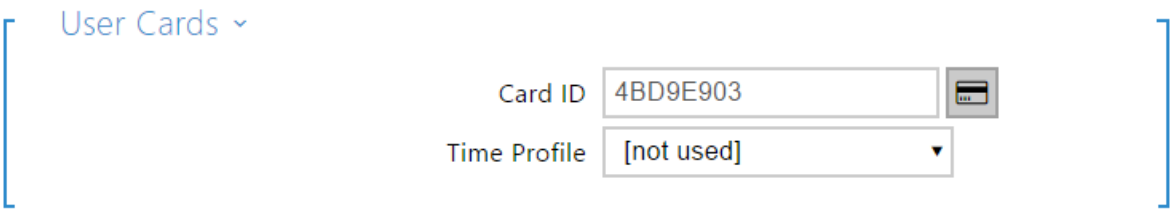
3. Press the Read button via the **2N Helios IP** web interface.



4. Tap the card on the card reader.

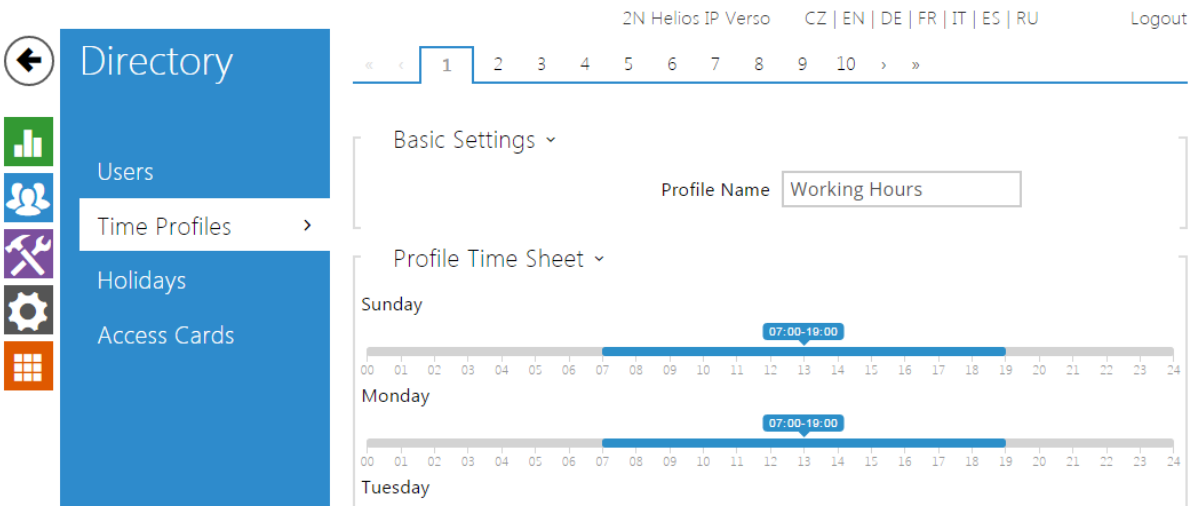


5. The card ID is successfully read.



Do not forget to save the configuration.

5.2.2 Time Profiles



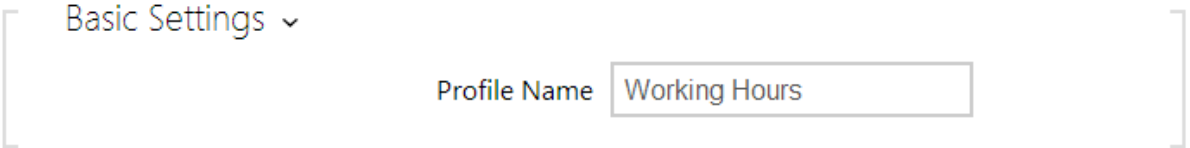
Such intercom functions as outgoing calls and RFID card/numeric code access, for example, can be time-limited by being assigned a **time profile**. By assigning a time profile you can:

- block all calls to a selected user beyond the set time interval
- block calls to selected 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

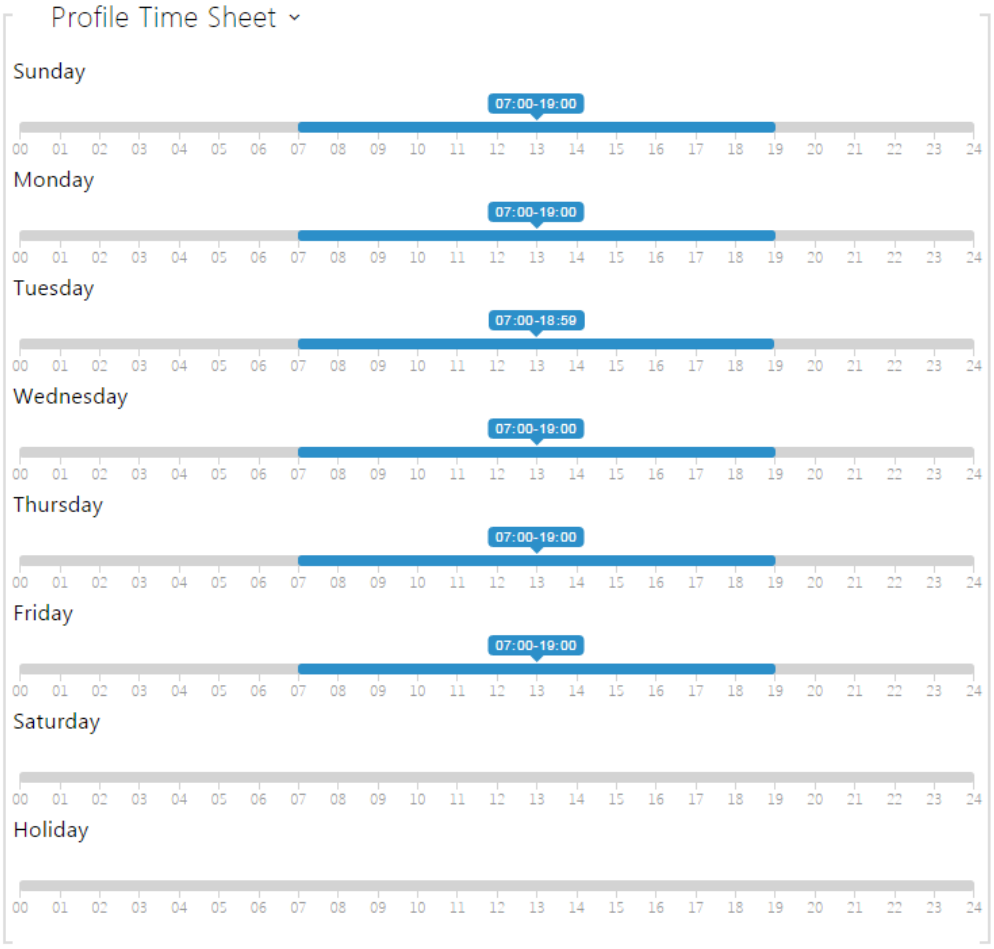
Assign a time profile according to a week time sheet to define availability of the selected function. Just set from-to or days in the week on which the function shall be available. **2N Helios IP** helps you create up to 20 time profiles (depending on the **2N Helios IP** model) that can be assigned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

The time profiles are defined not only using the week time sheet but also manually with the aid of special activation/deactivation codes that you can assign to them after arriving in/before leaving your office, for example. Enter the activation/deactivation codes using the numeric keypad of your intercom or phone (during the intercom call). 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 and select profiles in the switch, card and phone number settings more easily.



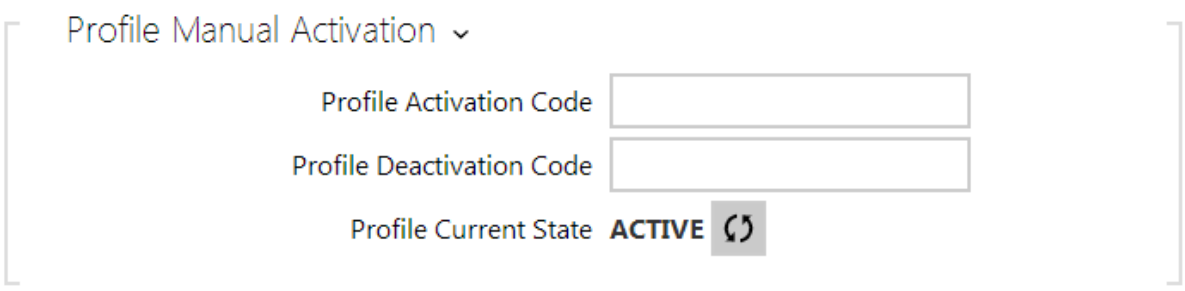
This parameter helps you set time profiles within a week period. A profile is active when it matches the set intervals.

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.*

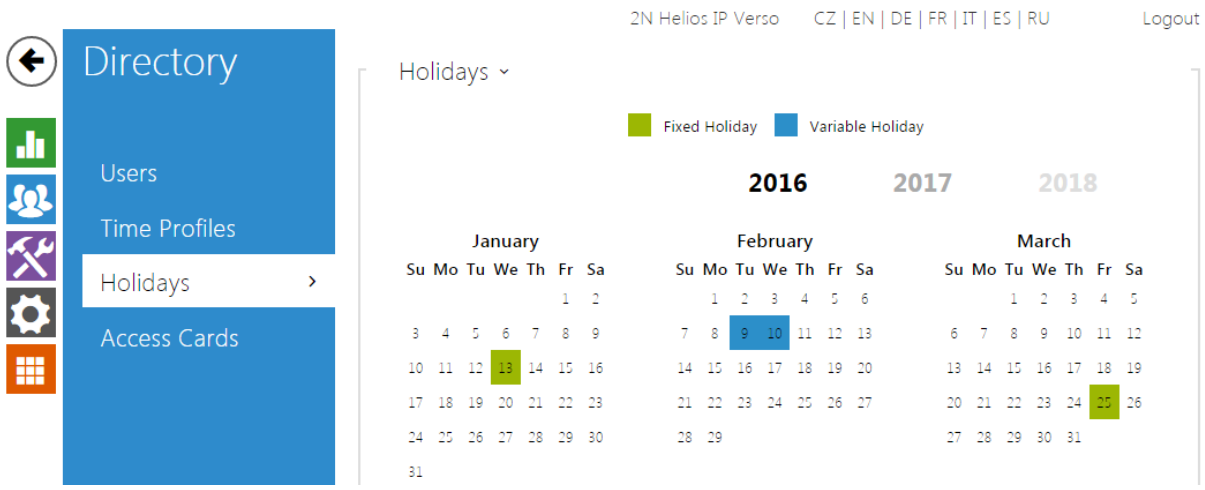


- **Profile activation code** – set the profile activation code: 16 characters including digits 0–9 only. If the activation code is the only code defined or the activation and deactivation codes are identical, then the activation code is used both for profile activation and deactivation.
- **Profile deactivation code** – set the profile deactivation code: 16 characters including digits 0–9 only.
- **Profile current state** – select the current state of the user.

Note

- *If the profile activation/deactivation code is not defined, the profile state is based on the time sheet exclusively.*
- *If you apply a time profile together with the activation/deactivation code, the profile will be active only if the time condition is met and the profile is code-activated at the same time.*

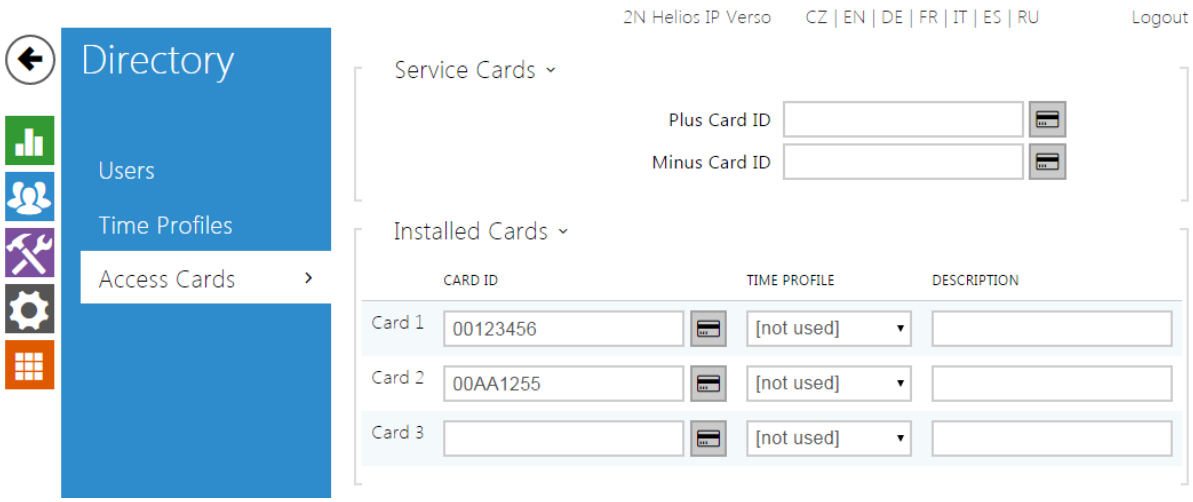
5.2.3 Holidays



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

You can set holidays for the coming 5 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.

5.2.4 Access Cards



Each intercom user can be assigned one or more access RFID cards. Typically, the card ID is included in the users 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 unassigned cards reserved for visitors, for example.

You can manage – add, remove and modify items – the list of installed cards manually via the intercom configuration interface. The main advantage of this list is the option to add/remove using the Service plus/minus cards without accessing the configuration interface. Unlike the users list with its up to 1999 positions, the Installed Cards may contain only 10 cards.

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 help you add/remove cards to/from the list. Enter their IDs in the Plus Card ID and Minus Card ID fields in the **Service Cards**: 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 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

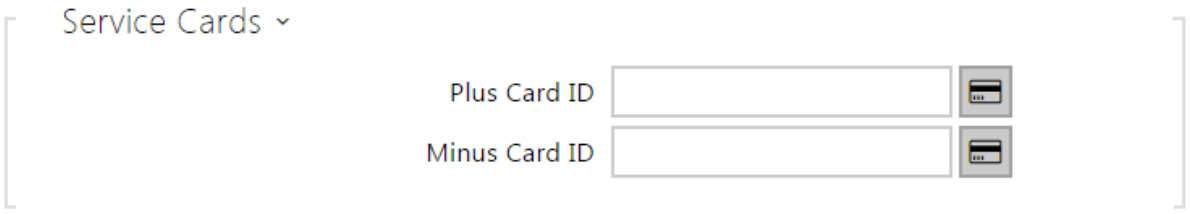
lengths, all the characters are compared. This ensures mutual compatibility of the internal and external readers. Go to the **Directory / Access Cards / Records** menu to identify whether the card was tapped on the internal or external reader.

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.

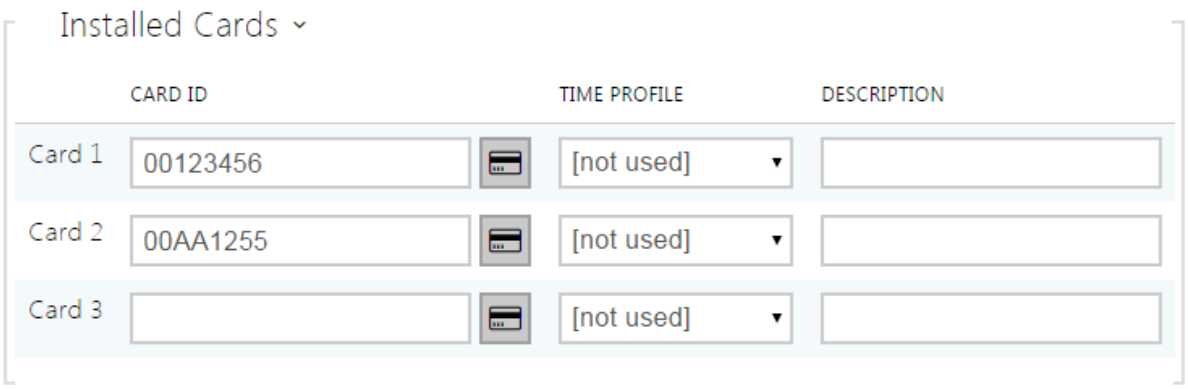
Having been read, the card ID is compared with the intercom card database. If the card ID matches any of the cards in the database, the appropriate action will be executed: switch activation (door unlocking, etc.). To change the switch number to be activated, use the **Associated Switch** parameter in the **Hardware / Card Reader** menu (**2N® Helios IP Vario, Force, Safety** models) or the **Associated Switch** parameter in the **Hardware / Modules** menu of the card reader module (**2N® Helios IP Verso** model). 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.

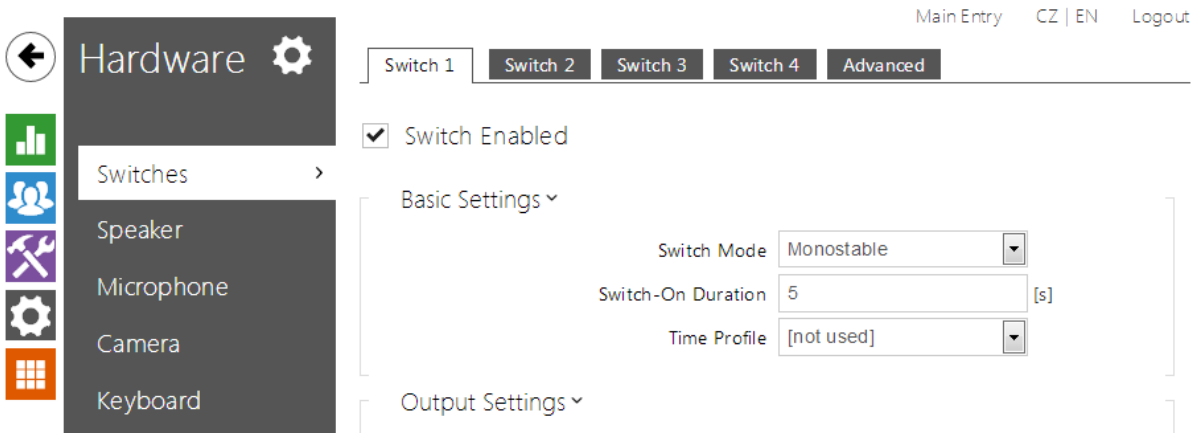


- **Card ID** – enter the access card ID: a sequence of 6–32 characters including 0–9, A–F.
- **Time profile** – assign a time profile to the user access card to define the card validity. If the time profile is inactive, the user access card will be detected as invalid.
- **Description** – enter such 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 intercom function.

5.3 Hardware

Here is what you can find in this section:

5.3.1 Switches



Switches provide a very flexible and efficient control of such intercom peripherals as electric door locks, lighting, additional ringing signalling, and so on. 2N Helios IP allows you to configure up to 4 (depending on model types) independent all-purpose switches.

A switch can be activated:

- by entering the valid code via the intercom numeric keypad or receiving a DTMF sequence during a call.
- by tapping a valid RFID card on the reader.
- with a predefined delay after another switch activation.
- by an incoming or outgoing call 1).
- by pressing a quick dial button 1).
- by receiving the HTTP command from another LAN device 1).
- via Automation using the Action.ActivateSwitch action.

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

If a switch is active, you can:

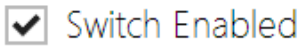
- activate any logical output of the intercom (relay, power output).
- activate the output to which the 2N® Helios IP Security Relay module is connected.
- send an HTTP command to another device.

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.

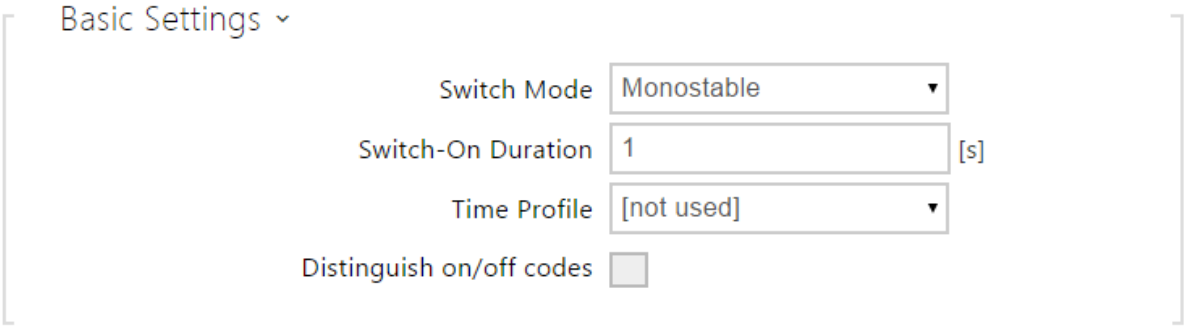
The switch signals its state:

- by a programmable beep or a predefined user sound.
- by a LED indicator if available in the intercom model.
- by an open-door icon on the display if available in the intercom model.

List of Parameters



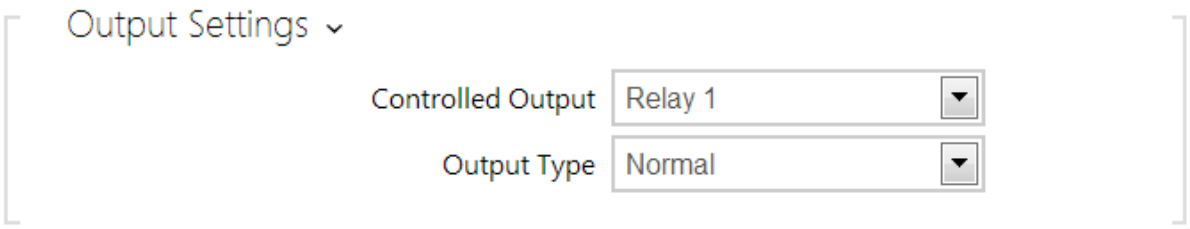
- Switch enabled – enable/disable the switch globally. When disabled, the switch cannot be activated by any of the available codes (including user switch codes), by a call or quick dial button.



- 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.
- Time profile – assign the switch a time profile to enable switch-on. If the time profile is inactive, the switch cannot be activated by a code, call or quick dial button.
- Distinguish on/off codes – set a switch code mode in which odd codes (1, 3 ....) are used for switch activation and even codes (2, 4 ...) are for switch deactivation. This mode can only be used if the switch is set to the bistable mode.

Note

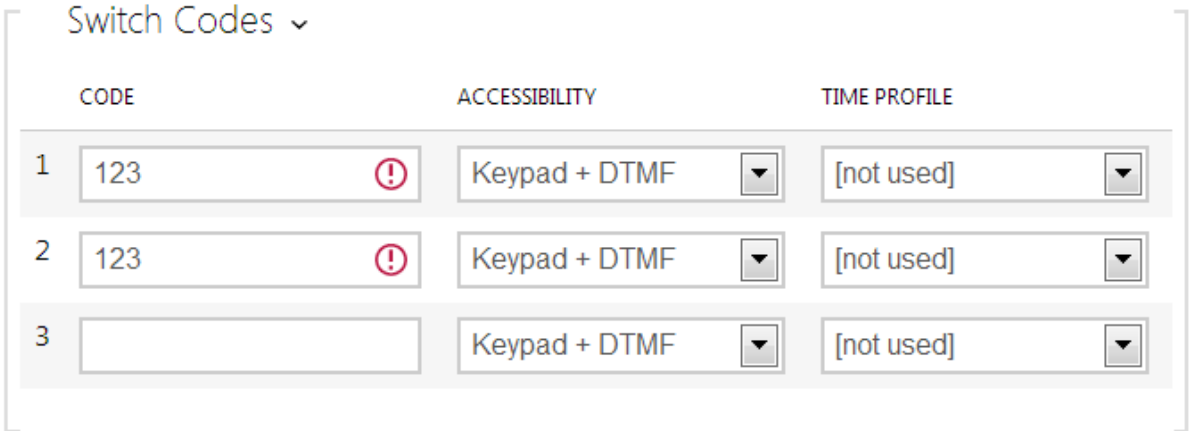
- *Switch time profiles are available with the Gold or Enhanced Integration licence only.*



- **Controlled output** – assign an electric output to the switch. Choose one of the available intercom outputs: relay, power output, extender output. If you select **None**, the switch will not control any electric output but can control external equipment via HTTP commands.
- **Output type** – if you use the **2N® 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.

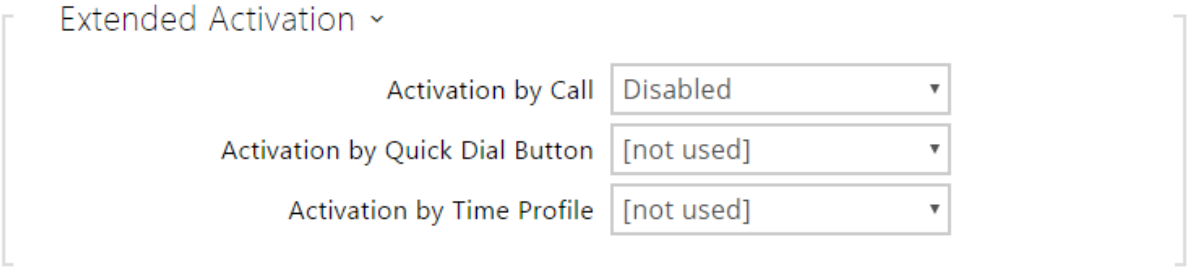
Note

- *2N® Helios IP Vario – be sure to set the internal power supply and switching relay on the configuration connector.*
- *2N® Helios IP Force – the security relay is connected to the DOOR + and - terminals.*



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

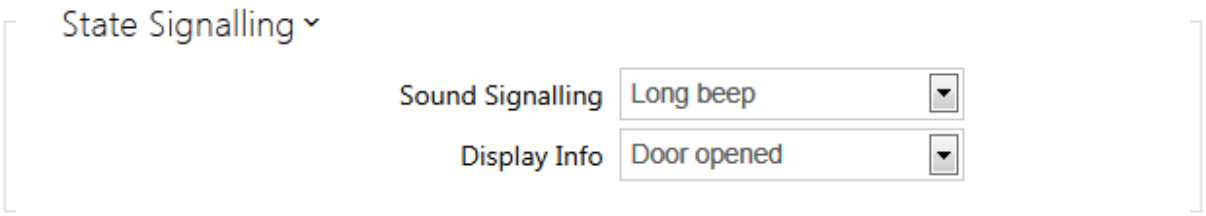
- **Code** – enter a numeric code for the switch. The code must include 2 characters at least but we recommend you to use four characters at least to make the code accessible from the intercom numeric keypad. Codes 00 and 11 can't be entered from numeric keypad. Code is confirmed with *. Code length up to 16 characters.
- **Accessibility** – block the switch activation code entering from the intercom numeric keypad or your phone.
- **Time profile** – assign a time profile to the switch code to control its validity.



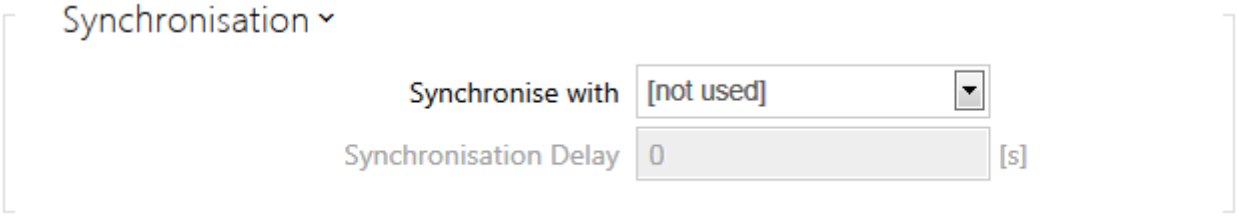
- **Activation by call** – enable switch activation by an incoming or outgoing call, for example. During an outgoing call the switch is activated after SIP message 180 Ringing is received. The called party confirms ringing by this message. The switch is active during the whole call in the bistable mode, and activated by the call beginning and deactivated after the predefined switch-on duration in the monostable mode.
- **Activation by quick dial button** – assign a quick dial button to the switch. The switch is activated whenever the button is pressed.
- **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.

Note

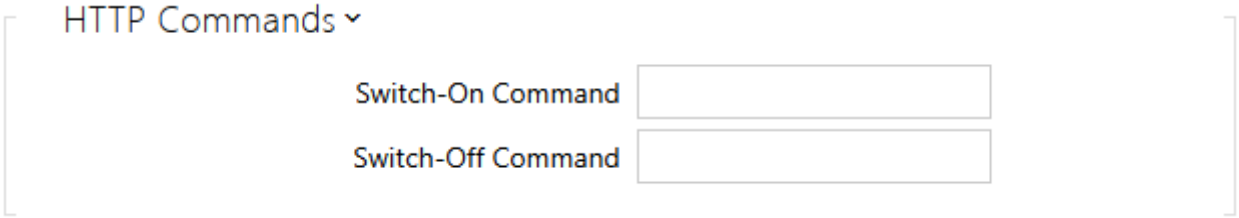
- *Activation by a quick dial button is available with the Gold or Enhanced Integration licence only.*



- Sound signalling – set the sound signalling type for switch activation. Choose the Short beep, Long beep (during the whole activation) or a User sound (refer to the User Sounds subsection).
- Display info – enable/disable signalling of an activated switch on the display.



- Synchronise with – 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 if the Synchronise function is disabled.



Note

- *The HTTP command sending is available with the Gold or Enhanced Integration licence only .*

- **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**

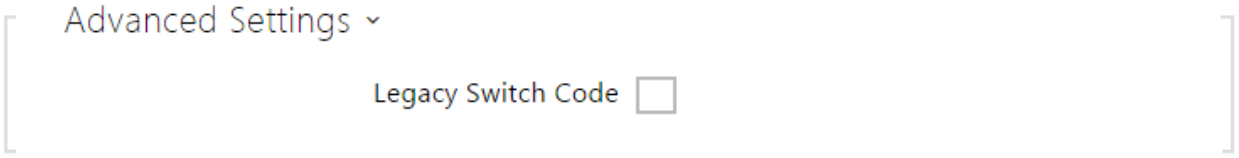
Tip

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

- **To turn on the switch** – **http://ip_address/state.xml?relayState=1** (e.g.: **http://192.168.1.10/state.xml?relayState=1**)
- **To turn on for pre-defined time (default value is 1.5 s)** – **http://ip_address/state.xml?relayState=2** (e.g.: **http://192.168.1.10/state.xml?relayState=2**)
- **To turn off** - **http://ip_address/state.xml?relayState=0** (e.g.: **http://192.168.1.10/state.xml?relayState=0**)

In case of use external relay **part no.: 9137411E** are used next HTTP commands (Symbol X should be replaced with a number of the desired switch):

- **To turn on the switch** – **http://ip_address/state.xml?relayXState=1** (e.g.: **http://192.168.1.10/state.xml?relay1State=1**)
- **To turn on for pre-defined time (default value is 1.5 s)** – **http://ip_address/state.xml?relayXState=2** (e.g.: **http://192.168.1.10/state.xml?relay1State=2**)
- **To turn off** - **http://ip_address/state.xml?relayXState=0** (e.g.: **http://192.168.1.10/state.xml?relay1State=0**)

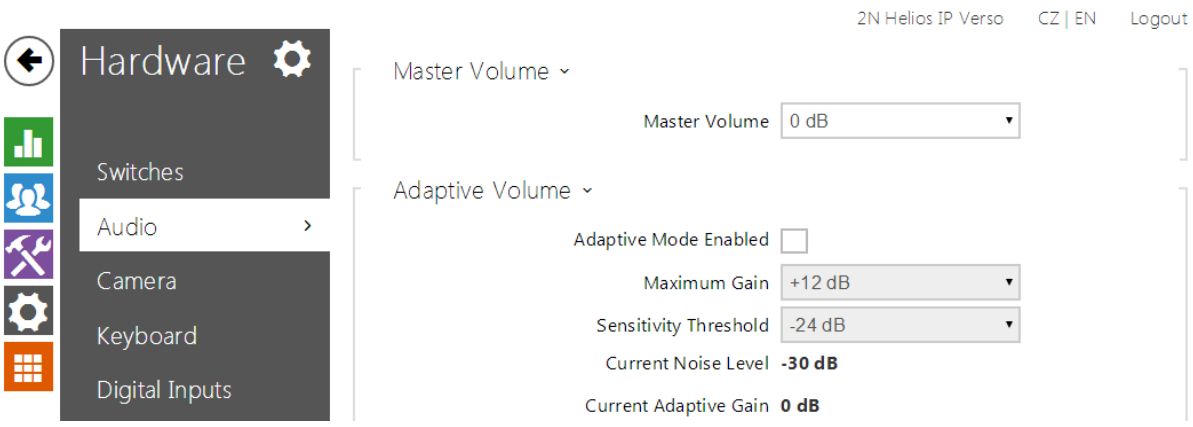


- Legacy switch code – enable the option to activate the first-listed switch code from the phone without being confirmed with *. When this box is checked, first code does not require confirmation by *. This setting does not apply to other switch codes listed and to numeric keypad code activation, those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

Note

- *The switch time profiles are available with the Gold or Enhanced Integration licence only.*

5.3.2 Audio

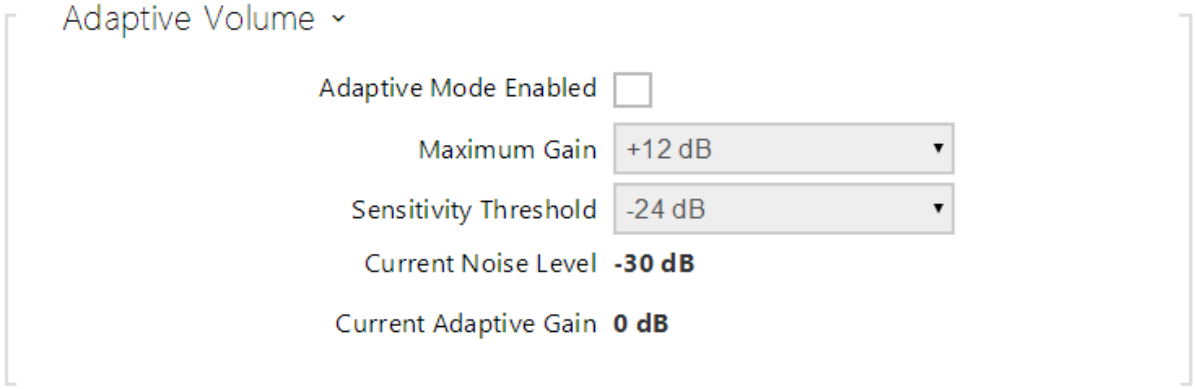


All the **2N Helios IP** models are equipped with a speaker or power amplifier output to which an external loudspeaker can be connected. Set the phone call and state signalling volume control in this configurat ion section. Set the **Master volume** to control the master volume of the device: volum e of calls, signalling tones, etc. Set this parameter according to the ambient noise level. If the noise level is not constant, use the Adaptive mode to increase the master volume temporarily depending on the ambient noise level.

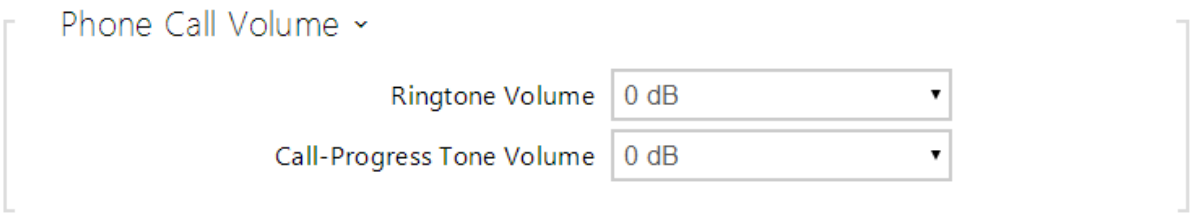
Model	Master Volume
Vario	-12 db .. +0 dB (150mW)
Force/Safety 1W	-12 dB .. +6 dB (1W)
Force/Safety 10W	-12 dB .. +20 dB (10W)
Uni	-16 dB .. +2 dB (1W)
Verso	-8 dB .. +8 dB (2W)
Audio/Video Kit	-10 dB .. +10 dB
SIP Speaker	-10 dB .. +10 dB

List of Parameters

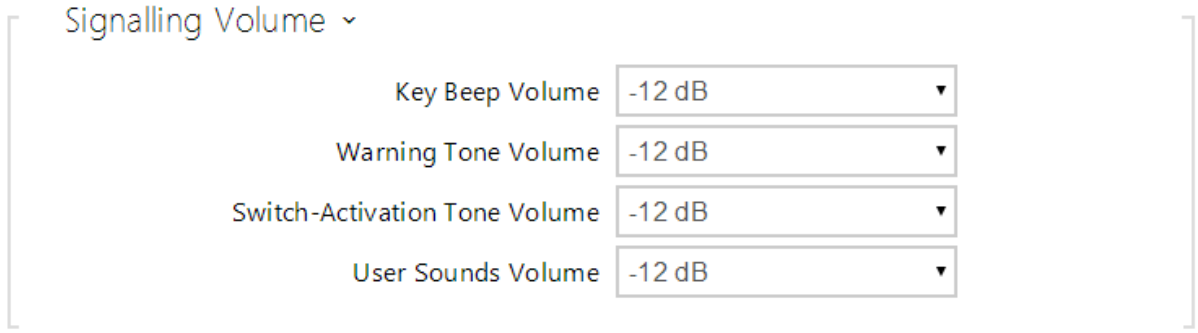
- Master volume – set the master volume for the entire system. This setting affects the volume of phone calls and all signalling tones.



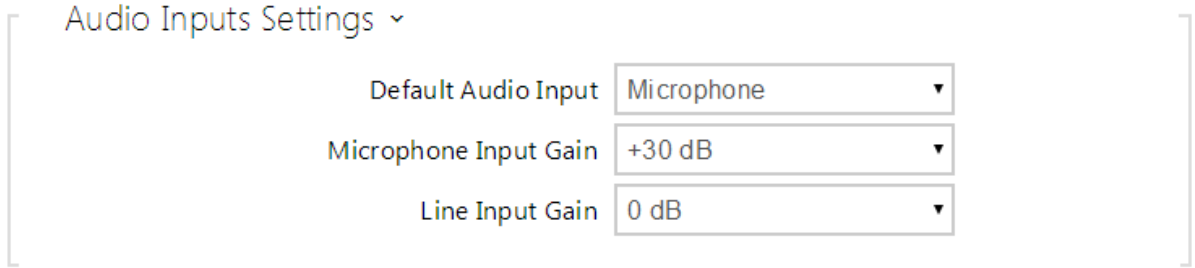
- Adaptive volume – enable the adaptive volume mode in which the speaker volume is adjusted automatically depending on the noise level of the intercom installation site.
- Maximum gain – set the maximum gain to be applied to the master volume in the adaptive mode.
- Sensitivity threshold – set the ambient noise threshold at which adaptive gain is applied.
- Current noise level – display the current ambient noise level.
- Current adaptive gain – display the current adaptive gain of the master volume. The value is determined by the difference of the Current noise level and Sensitivity threshold and never exceeds the Maximum gain value.



- **Ringtone volume** – set the incoming call signal loudness.
- **Call-progress tone volume** – set the dial, ring and busy tone volume. In case the call-progress tones are automatically generated by the PBX, this setting will not be applied.



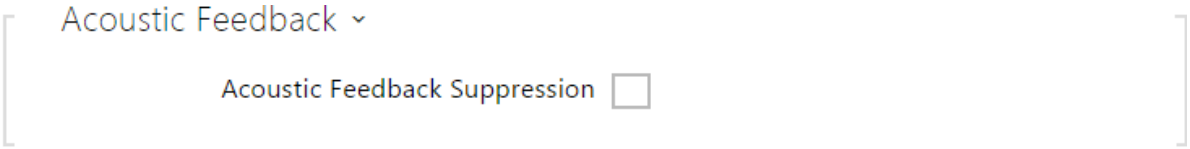
- **Key beep volume** – set the key beep volume. The volume values are relative against the set master volume.
- **Warning tone volume** – set the volume of warning and signalling tones described in the **Signalling of Operational Statuses** section. The volume values are relative against the set master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



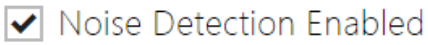
- **Default audio input** – set the default audio input (microphone, line input or audio module input) to be used for phone calls and audio streaming.

- **Microphone input gain** – set the microphone input gain.
- **Line input gain** – set the line input gain independently of the microphone gain value.

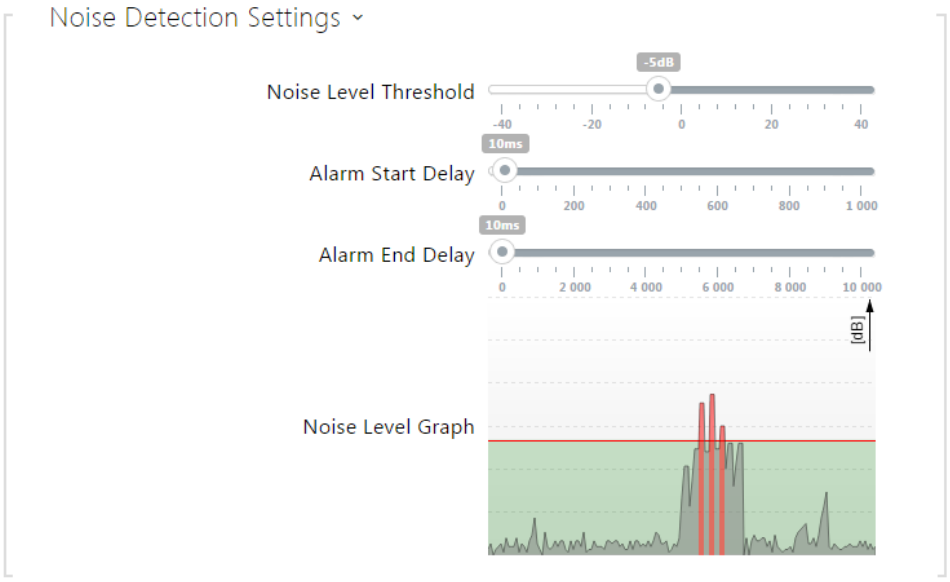
> **Tip**
>
> - Only at **2N® Helios IP Audio Kit** and **2N® Helios IP Video Kit** is possible to configure microphone gain.
> - *The microphone/line input gain setting is connected with the input signal level and type of external microphone installation. The wide gain range (0 to 39dB for a microphone input and -6dB to 24dB for a line input) should be sufficient for most installations. Set a value to ensure good audibility and eliminate excessive acoustic feedback at high loudspeaker volumes with subsequent signal saturation on the microphone/line input and thus acoustic echo cancellation (AEC) deterioration.*



- **Acoustic feedback filter** – set automatic suppression of acoustic feedback (typically whistling) between the intercom speaker and phone handset if located in close proximity to the intercom. This mode is disabled by default.

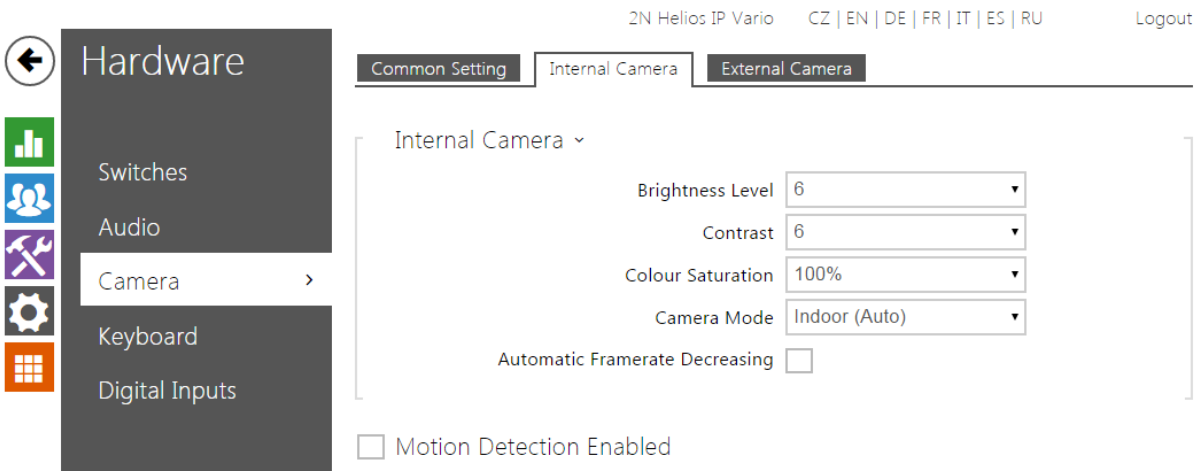


Switch on automatic detection of noise or microphone noise level threshold exceeding. Process the threshold exceeding alarm using **Event.NoiseDetected** and assign it to other user actions.



- **Noise level threshold** – set the microphone noise level threshold for alarm setting.
- **Alarm start delay** 0 set the time interval during which the signal must be above the threshold to start alarm.
- **Alarm end delay** – set the time interval during which the signal must be below the threshold to stop alarm.
- **Noise level graph** – display the signal level history. Red designates alarm activation.

5.3.3 Camera



This menu is only available in the **2N Helios IP** models that are equipped with an internal camera or can be connected to an external camera. The camera signal can be streamed directly into the call via a videophone, sent by E-mail, streamed via ONVIF /RTSP to another device (a video surveillance device, e.g.), or simply HTTP downloaded from the intercom in the JPEG format.

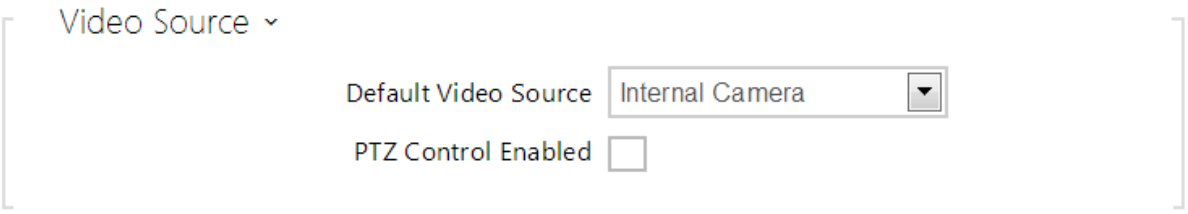
The following video signal sources can be used:

- an internal integrated camera or external analogue camera (**2N® Helios IP Video Kit** only)
- a standard external IP camera supporting RTSP stream with codecs MJPEG (640 x 480 max resolution) or H.264 (640 x 480 Base Line Profile max resolution). The recommended framerate is 15 frames per second in either case. Higher frame rates may result in undesired effects (less smooth playing).

The **Camera** menu helps you set such camera parameters as brightness, colour saturation and external IP camera login data if necessary. Refer to the **Services / Phone, Services / Streaming** and **Services / E-Mail** menus for the video call/streaming parameters.

List of Parameters

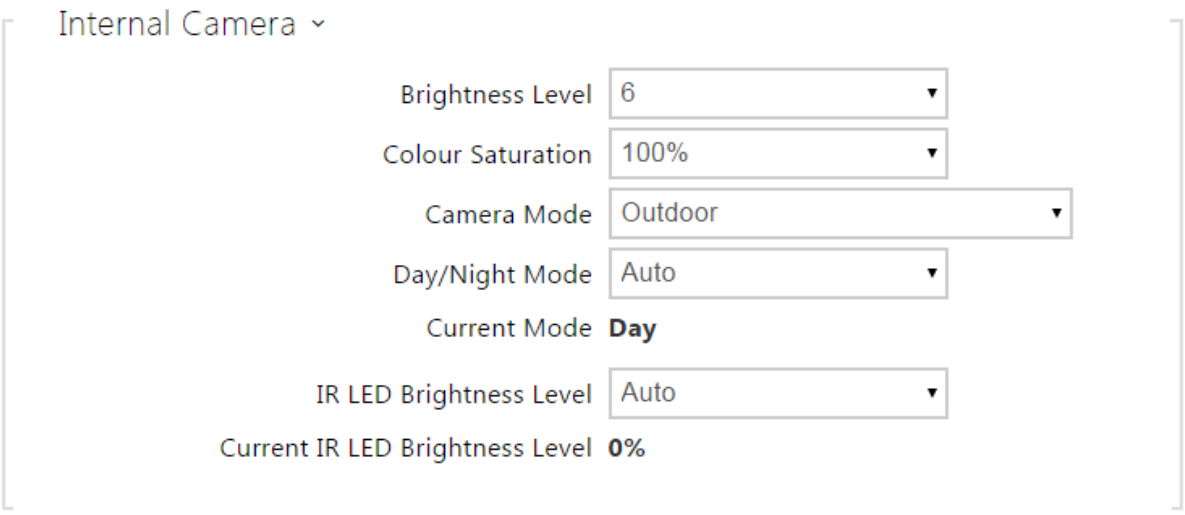
Common Settings



- **Default video source** – set the default video signal source. Choose Internal camera (or an analogue camera connected to the intercom) or External IP camera. The change of the default video signal source is applied to the RTSP stream and HTTP API. In **2N® Helios IP Eye** it is required to enable the external camera manually, even when there is no internal camera present in the device. If no internal camera is connected to the intercom, External IP camera can only be selected. If the external camera is not connected or configured properly, N/A is displayed on a blue background.
- **PTZ control enabled** – enable the PTZ (Pan-Tilt-Zoom) function to control the camera display area during the call via DTMF (for **2N® Helios IP Verso** only) from your IP phone numeric keypad. Click the * key to enable/disable the PTZ mode. The meanings of the IP phone keys in the PTZ mode are as follows:

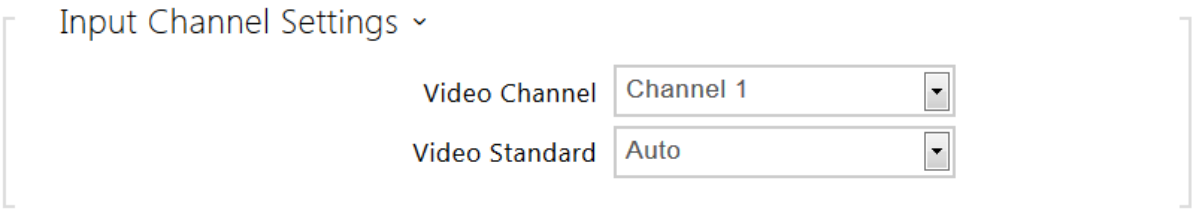
IP phone key	PTZ mode function
*	Enable/disable PTZ
1	Zoom in
3	Zoom out
2	Move cropped display up
4	Move cropped display to the left
6	Move cropped display to the right
8	Move cropped display down
5	Return to initial state

Internal Camera



- **Brightness level** – set the camera image brightness level.
- **Colour saturation** – set the camera image colour saturation.
- **Camera mode** – select suitable camera modes according to the current intercom installation conditions (indoor/outdoor use). Choose variable image flicker cancellation modes for indoor sites illuminated by artificial light. Or, set direct sunshine suppression for outdoor applications.
- **Automatic framerate decreasing** – enable automatic frame rate decreasing under worsened illumination conditions to improve image quality by lowering the frame rate.
- **Image trimming** – the **2N® Helios IP Force** camera view angle allows you to scan the largest area possible. Use this parameter to enable automatic camera image trimming to eliminate the (sometimes annoying) view of the intercom frame. Disable this function to get the maximum possible view angle. The parameter is available in the **2N® Helios IP Force** models only.
- **Day/Night mode** – set the camera day/night mode. The options are automatic (controlled by the ambient light level), or permanently day or night mode.
- **Current mode** – display the currently selected camera mode (day/night). in the day mode, the camera uses an IR suppressing filter and infrared illumination is disabled. In the night mode, the IR suppressing filter is disabled and infrared illumination is on .
- **IR LED brightness level** – set the infrared LED brightness level in the range of 0-100% in several steps. Infrared illumination is automatically activated in night mode. The IR LED brightness level settings are only available in the **2N® Helios IP Verso** and **2N® Helios IP Verso** with HD camera models.

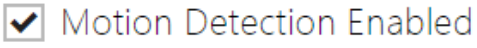
- **Current IR LED brightness level** – display the current IR LED brightness level percentage. The level can automatically be decreased below the set value so that the maximum power consumption cannot be exceeded (typically, when multiple extenders are connected and PoE supply is used).



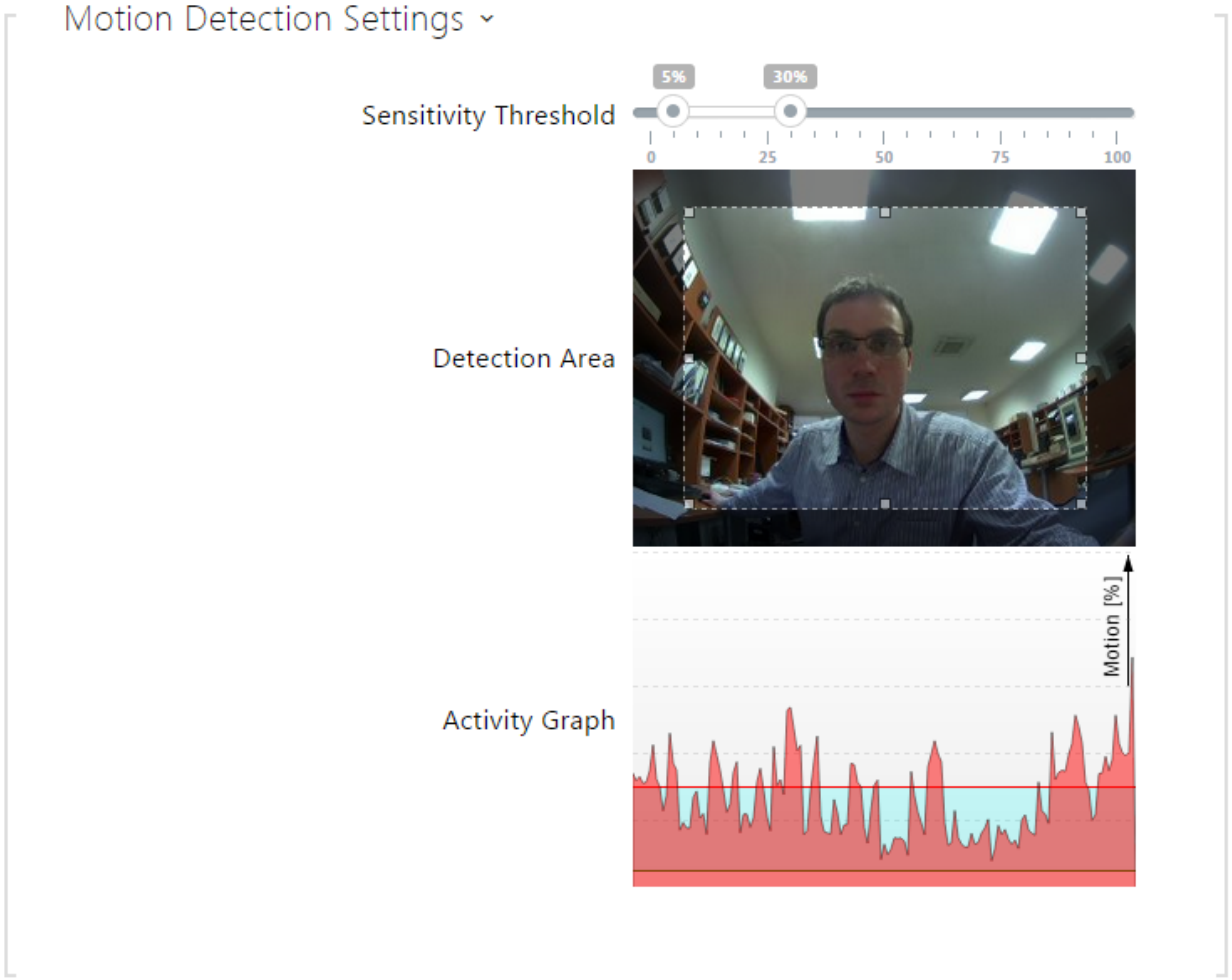
Note

- *This setting is only available in the models equipped with an external analogue camera input.*

- **Video input** – choose one of the analogue camera inputs. You can change the input by automation via the Action.SetCameraInput during operation.
- **Video standard** – set the video standard for the camera connected. Modify the value only if the automatic video standard detection does not work well (**Auto** value).

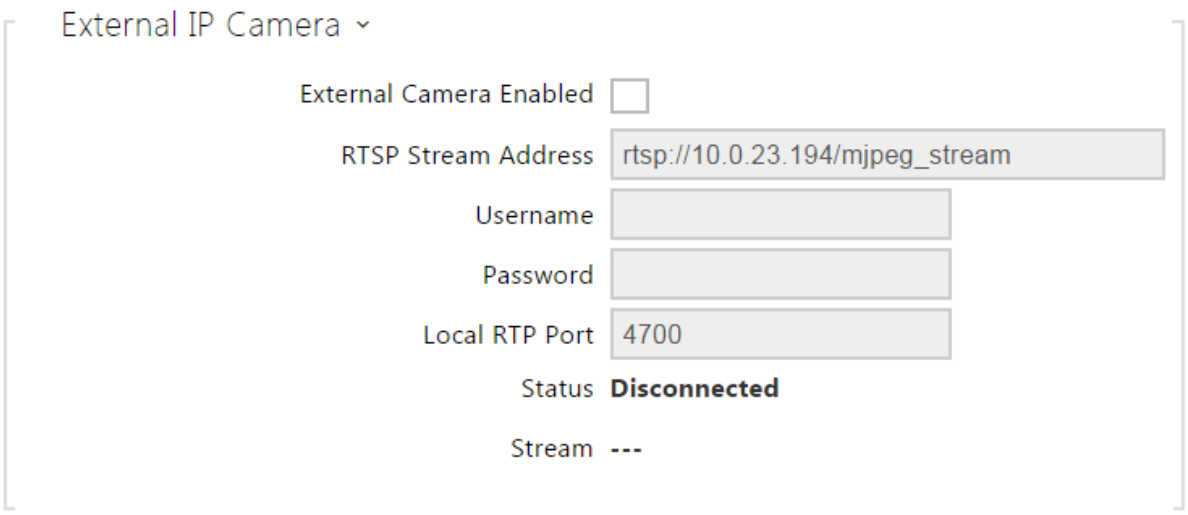


- **Motion detection enabled** – enable automatic motion detection via an internal camera. Motion is detected by monitoring of a brightness change in the selected image section in time. When objects move within the camera range, the selected part of the image detects an activity, which can be expressed in percentage. If the activity exceeds the upper limit, motion is detected and indicated as long as the activity drops below the lower limit. Select the sensitivity thresholds and detection area according to the requirements and installation site conditions.



- **Sensitivity threshold**– set the lower and upper sensitivity and hysteresis limits for the motion detecting algorithm.
- **Detection area** – set the rectangular detection area in the image.
- **Activity graph** – display the activity history (image brightness changes) including the upper/lower sensitivity thresholds.

External Camera



- **External camera enabled** – enable RTSP stream download from the external IP camera. Complete the valid RTSP stream address or the username and password to make the function work properly.
- **RTSP stream address** – enter the IP camera RTSP stream address: **rtsp://camera_ip_address/parameters**. The parameters are specific for the selected IP camera model. If you choose another **2N Helios IP** intercom for the external camera, enter **http://ip_address/mjpeg_stream** or **http://ip_address/h264_stream**.
- **Username** – enter the username for the external IP camera authentication. The parameter is obligatory only if the external IP camera requires authentication.
- **Password** – enter the external IP camera authentication password. The parameter is obligatory only if the external IP camera requires authentication.
- **Local RTP port** – set the local UTP port for RTP stream receiving.

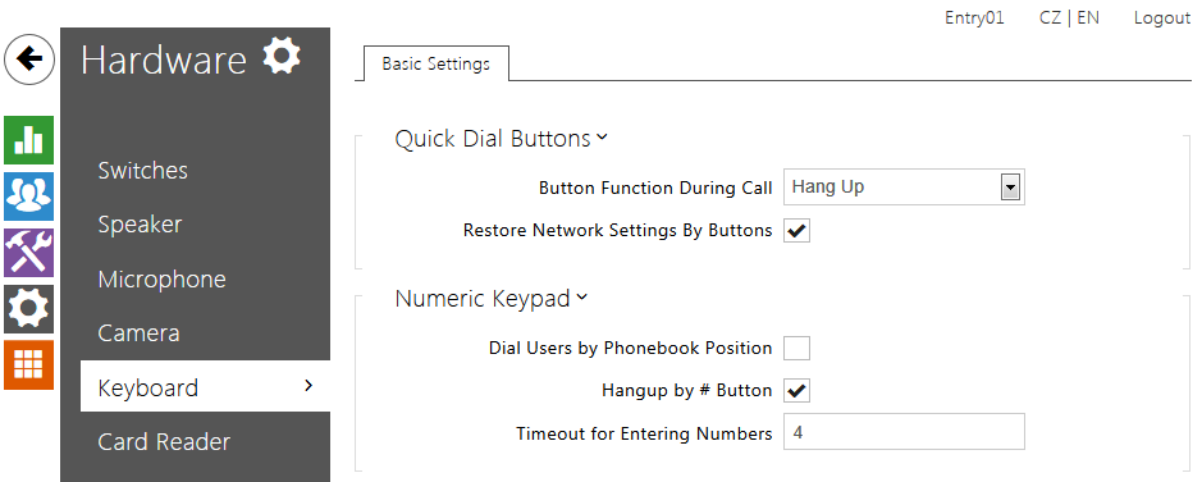
Tip

- FAQ: **External camera - How to set it in 2N® Helios IP**

The Camera Preview window displays the current image received from an external camera. If the external camera is disconnected or configured incorrectly, the N/A characters are displayed on a blue background.

The External IP Camera Log displays the RTSP communication with the selected external IP camera including failures and error states if any.

5.3.4 Keyboard

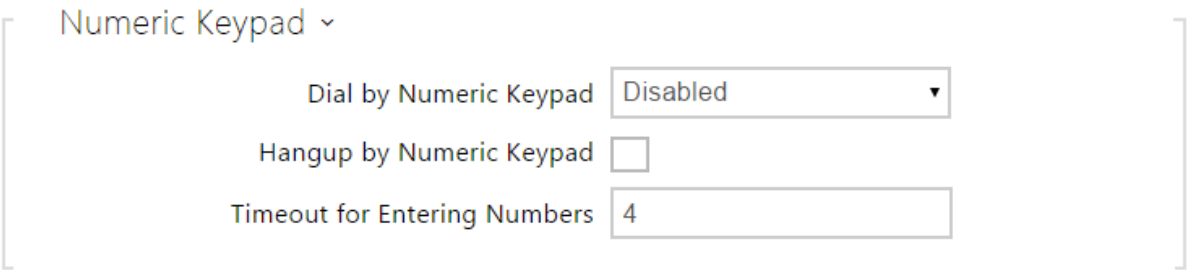


This configuration section helps you set the numeric keypad and quick dial button functions. 2N Helios IP allows you to:

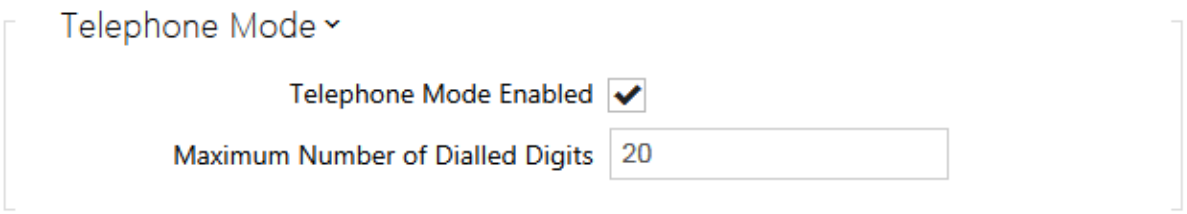
- use the numeric keypad for dialling common phone numbers
- use the numeric keypad for dialling a user position
- use the numeric keypad for entering the access code for door unlocking, e.g.
- set the # function
- set the timeout for entering codes and phone numbers
- set the function of the buttons and keys of the connected 2N® Helios IP Audio /Video Kit units

List of Parameters

Basic Settings



- **Dial by numeric keypad** – enable user calling via the numeric keypad by entering the user position/virtual number and pressing *.
- **Hang up by numeric keypad** – enable termination of the active call by the # key (or the key with a red phone at Verso). If the call was initiated by a quick dial button, the same button has to be repressed; refer to the **Button function during call** parameter.
- **Timeout for entering numbers** – set the maximum interdigit timeout for code or phone number dialling via the intercom numeric keypad. When you enter a number in the Telephone mode, i.e. after (or on the **2N® Helios IP Verso** keypad) is pressed, and keep the maximum number length as set in the **Maximum number of dialled digits**, the dialling will be confirmed automatically when this timeout expires as if (or for **2N® Helios IP Verso**) was pressed. If you dial a user position, virtual number or switch activation code, the dialling will be rejected after this timeout unless confirmed with (or in **2N® Helios IP Verso** depending on the required function). Set the code entering limit in the range of 3–15 s.



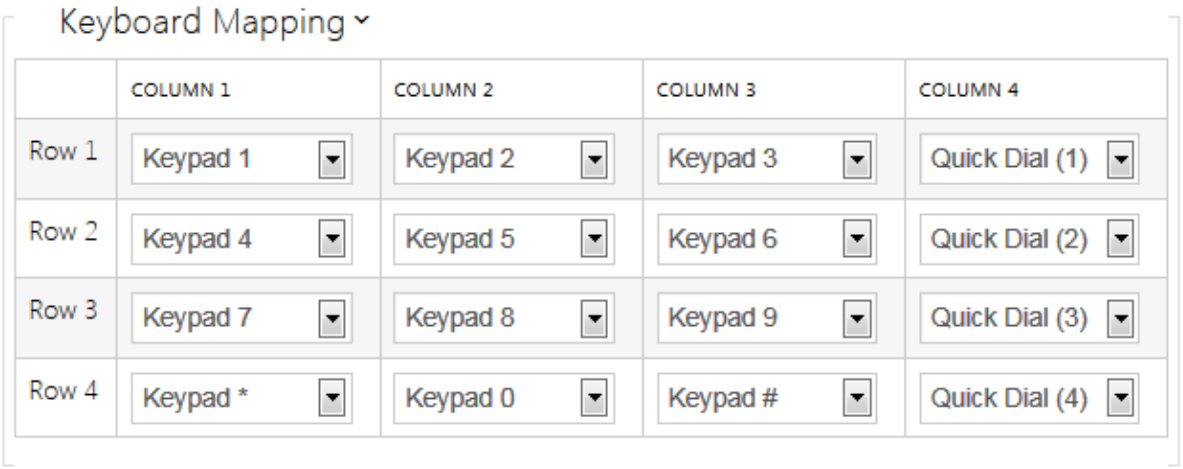
- **Telephone mode enabled** – enable call setup to phone numbers dialled via the intercom numerical keypad. Set up a call as follows: press **phone_number** (or **phone_number** for **2N® Helios IP Verso**). If you do not press (or for **2N® Helios IP Verso**) as the terminating character, the dialling will be confirmed automatically when the code entering timeout expires as if (or for **2N® Helios IP Verso**) was pressed.
- **Maximum number of dialled digits** – set the maximum count of digits for a phone number in the Telephone mode. When this limit is reached, the number is dialled automatically without pressing *.

Keyboard Mapping

The **2N® Helios IP Audio Kit** and **2N® Helios IP Video Kit** models are equipped with eight terminals for up to 16 external buttons or a keypad. The functions can be set for each button separately.

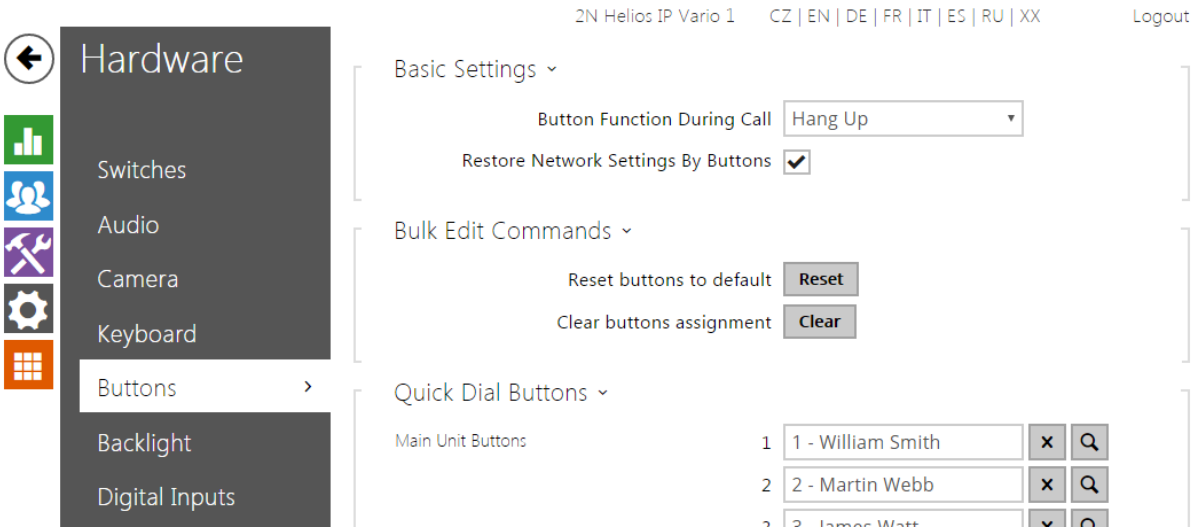
The buttons and their settings are arranged in a matrix of 4 columns x 4 rows; see the figure below.

The figure below shows the default button settings.

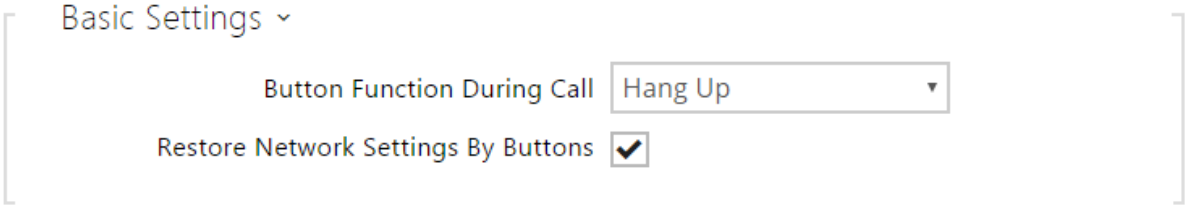


You can assign one function to each matrix position: numeric keypad keys 0 through 9, *, # or one of the quick dial buttons 1–16.

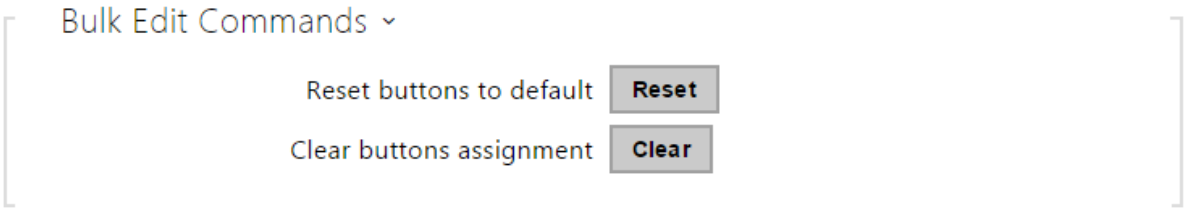
5.3.5 Buttons



Assign the **Directory** / **Users** users to the quick dial buttons. By default, all available intercom buttons are assigned to the listed users. A non-assigned button can be used for automation or switch activation, for example.

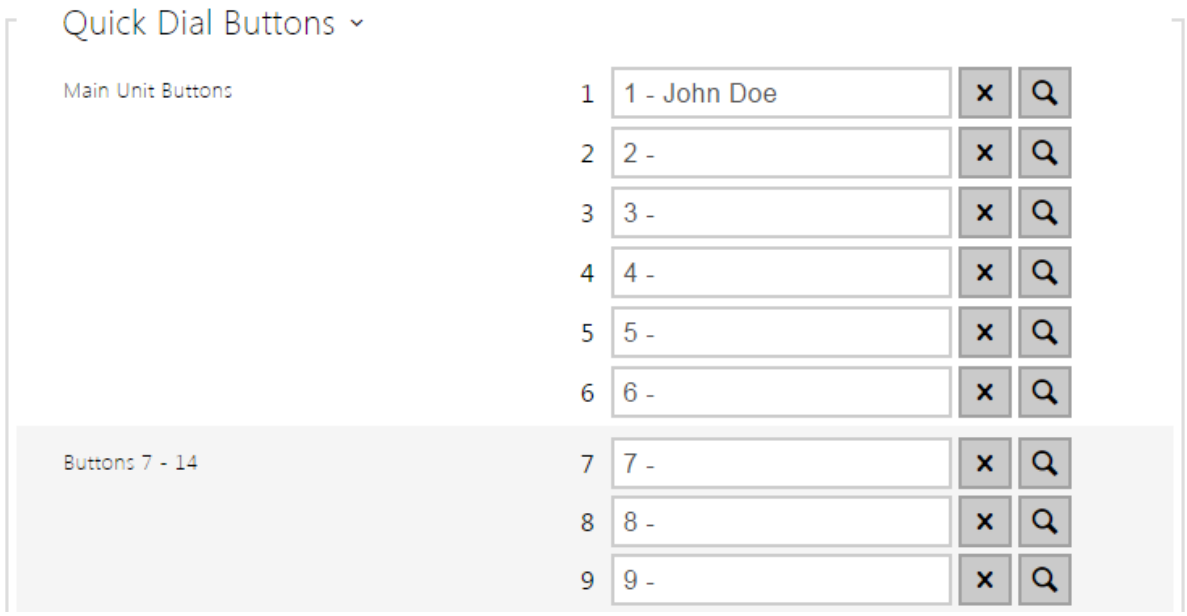


- **Button function during call** – set the quick dial button function during a call. You can only set the button that initiated the call. The following options are available:
  - **None** – button pressing does not affect the call setup or active call.
  - **Hang up** – button pressing terminates the call setup or active call.
  - **Dial the following** – button pressing initiates dialling of the following user number in the users list. This accelerates the dialling process in case the user is inaccessible on some of its phone numbers.
  - **Flash** – button pressing sends a special DTMF character (FLASH) into the current call, to which the connected PBX can response with the selected action.
- **Restore network settings by buttons** – enable restoration of the default network settings by pressing a sequence of the quick dial buttons after the intercom restart as described in the **Device Configuration** subsection in the Installation Manual of the respective model.



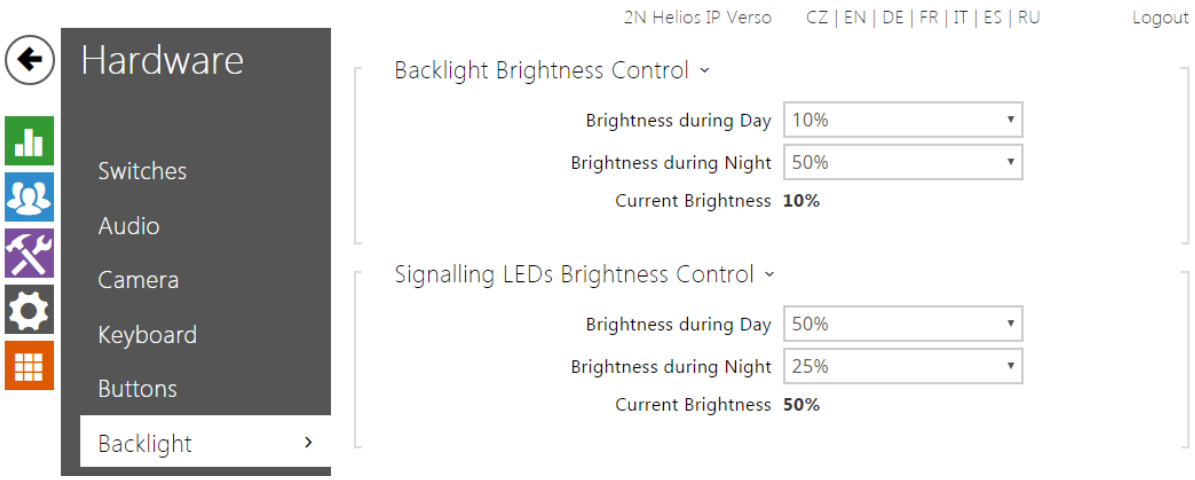
The bulk editing function is available in intercom models with more than 3 buttons.

- **Reset** – reset the default button values, i.e. assign button 1 to position 1, button 2 to position 2, etc.
- **Clear** – remove all button assignments.



Display the list of all potentially available intercom buttons including those that are physically absent. In some intercom models (**2N® Helios IP Vario** , **2N® Helios IP Verso**), the button list is divided into 8/5-item groups corresponding to the button extending modules. Enter the user list position number or click  to search a user by the name easily.

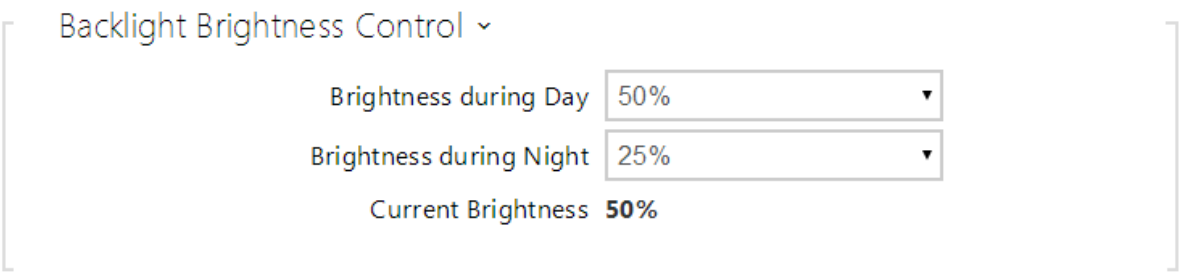
5.3.6 Backlight

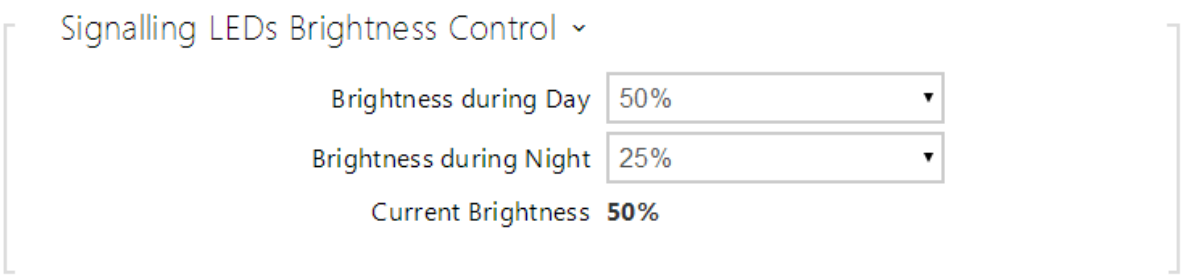


This tab helps you control the backlight level of nametags, buttons and brightness of signalling LEDs.

If equipped with an ambient light level sensor, the intercom automatically chooses the suitable backlight level within the set range of values. The selected intercoms allow you to control the backlight brightness of name tags (buttons) and signalling LEDs (illuminated pictograms). Refer to the table below:

Property/Model	Verso	Base	Vario	Force	Safety	Uni	Audio Kit	Video Kit
Backlight level control	Yes	Yes	Yes				No	
Ambient light level sensor	Yes	No	No				No	
Independent name tag and LED backlight level control	Yes	Yes	No				No	



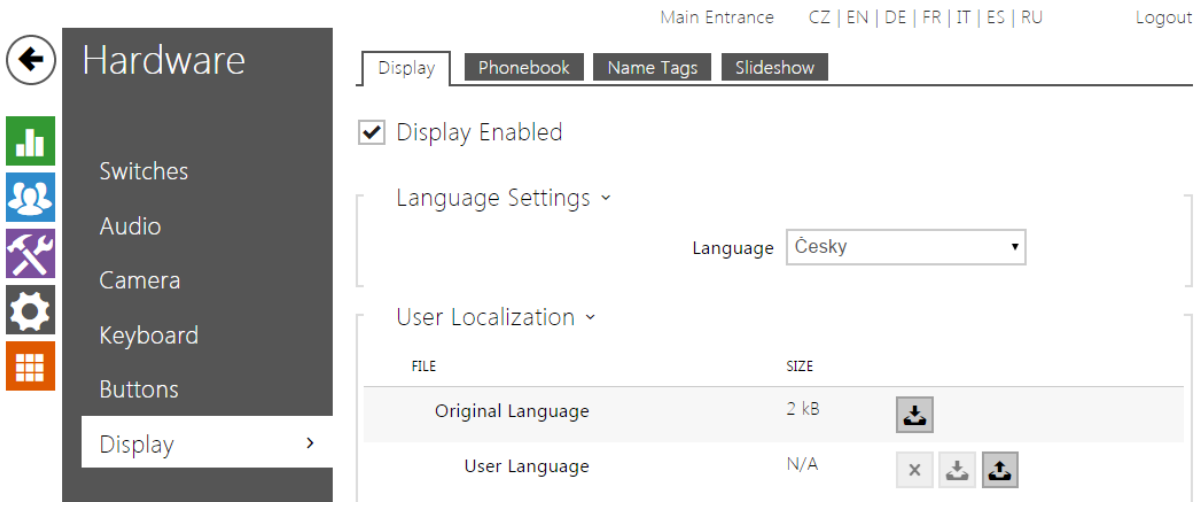


- **Brightness during day** – set the LED brightness percentage value for the day mode.
- **Brightness during night** – set the LED brightness percentage value for the night mode . If the Brightness during day and Brightness during night are set to one and the same value, the ambient light level is ignored.
- **Current brightness** – display the current LED brightness value automatically selected according to the ambient daylight level.

Poznámka

- 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.

5.3.7 Display



Some intercom models (2N® Helios IP Vario, 2N® Helios IP Verso) can be equipped with a colour LCD display. The device state is displayed (call progress, door opening, etc.) and the following modes are available:

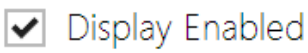
Name Tags – display up to 4 selected users from the phonebook in the digital Name Tags mode. Each of the users is assigned one of the 4 buttons located on the display sides. Press a button to activate a call to the selected user.

Phonebook – display a configurable list of users. Use the numeric keypad buttons (arrows) to go through the user list. You can create practically any count of nested groups within the user list and add any count of users to each group.

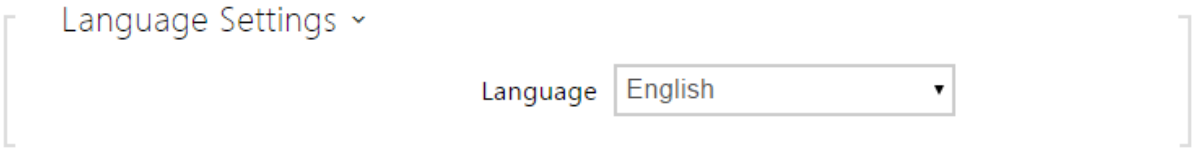
Slideshow – display a slideshow showing a set of recorded images after a defined idle time. The automatic switching time can be configured.

List of Parameters

Display (for 2N ® Helios IP Vario only)



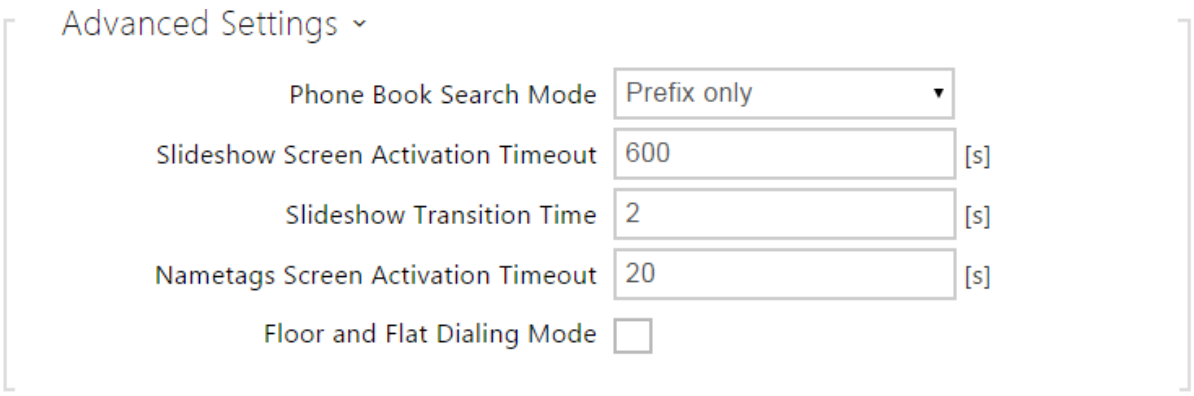
- Display enabled – enable this parameter to automatically display the name tags, phonebook and slideshow if necessary. When this parameter is disabled, the images recorded via HTTP API are displayed only (refer to the HTTP API documentation).



- **Language** – set the language for the texts to be displayed. Choose one of the seven pre-defined languages: **English, Spanish, German, French, Russian, Italian** and **Czech**. If you do not choose any of the available languages, select the **User language** and create a localisation file of your own; see below.

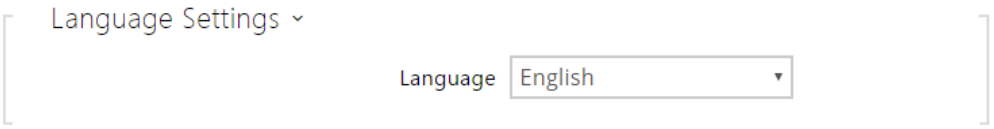
- **Original language** – download a preset XML file with all the texts to be displayed.
- **User language** – record, remove and load a localisation file of your own.
- **User font** – record, remove and load a font of your own for the texts to be displayed. Keep the TTF format and make sure that the file does not exceed 4 MB.

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

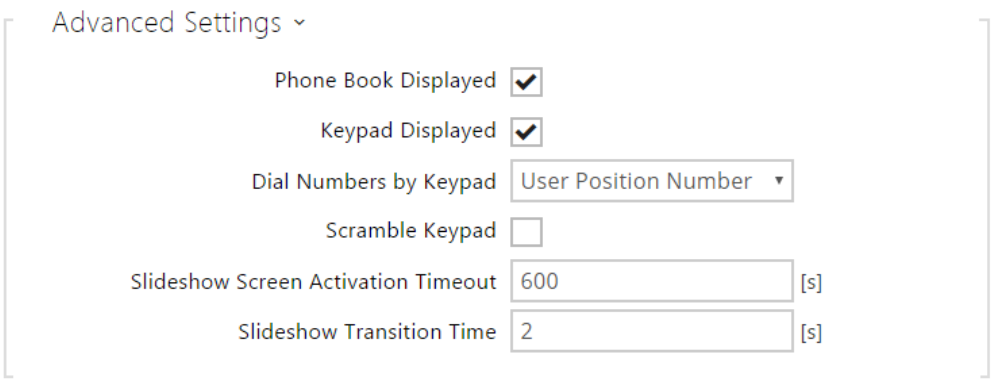


- **Phonebook search mode** – set the Phone Book searching mode. You can search users either according to the first username characters (Prefix only) or an arbitrary incidence of the selected characters in the username (Arbitrary incidence).
- **Slideshow screen activation timeout** – set the maximum idle time (i.e. during which the user does not control the device via the buttons or numeric keypad) in which the Slideshow mode will be activated automatically.
- **Slideshow transition time** – set the image displaying time in a slideshow.
- **Nametags screen activation timeout** – set the maximum idle time (i.e. during which the user does not control the device via the buttons or numeric keypad) in which the Phonebook mode will be switched to the Name Tags mode. You can also press the Back button to the left to return to the Name Tags mode.
- **Floor and flat dialling mode** – activate a special display to view floors and apartments instead of the phonebook and name tags. Enter a two-digit floor number via the numeric keypad and press one of the A - F buttons on the display sides to make the intercom dial the phonebook position defined by the selected floor number and button. The phonebook position is calculated as 6 x floor number + N, where N is 0 for A, 1 for B, 2 for C, and so on.

Display (for 2N ® Helios IP Verso only)



- **Language** – set the language for the texts to be displayed. Choose one of the seven pre-defined languages: **English, Spanish, German, French, Russian, Italian** and **Czech** .



- Phone book displayed – enable/disable display of the phone book function.
- Keypad displayed – enable/disable display of the keypad function.
- Dial numbers by keypad – set number dialling via the keypad on the display. The following options are available:
  - Disable – disable the keypad dialling function.
  - User position number – enable user dialling by its phone book position via the keypad.
  - User virtual number – enable user dialling by a virtual number via the keypad.
- Scramble keypad – enable/disable keypad button scrambling (random button transposing) before every new display to prevent other persons from watching the code entered.
- Slideshow screen activation timeout – set the maximum idle time (i.e. during which the user does not control the device via the buttons or numeric keypad) in which the Slideshow mode will be activated automatically.
- Slideshow transition time – set the image displaying time in a slideshow.

Phonebook

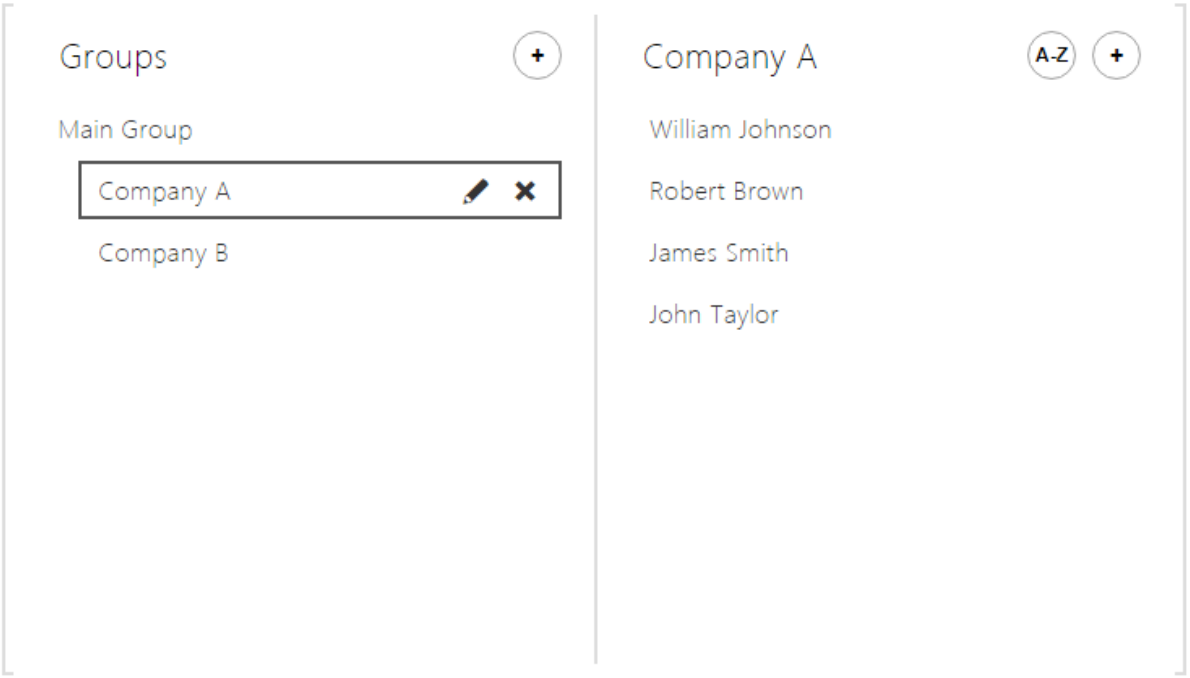
This tab helps you configure a structured list of users. You can create practically any count of groups and assign any count of users to each of the groups. One user cannot be assigned to one group more times, but one user can be assigned to more groups at the same time.

The created groups are displayed to the left. Click ⊕ to add a group. Press ✖ or DEL to remove a group including its users. Click ✎ or ENTER to rename a group. The currently selected group is marked with a black oblong. Use the mouse to move (nest) the groups created.

The users assigned to the currently selected group are displayed to the right. Click ⊕ to add a user from the phonebook. Press ✖ or DEL to remove a user.

The **Main Group** is created by default to which you can directly add users from the phonebook. The Main Group cannot be deleted or renamed.

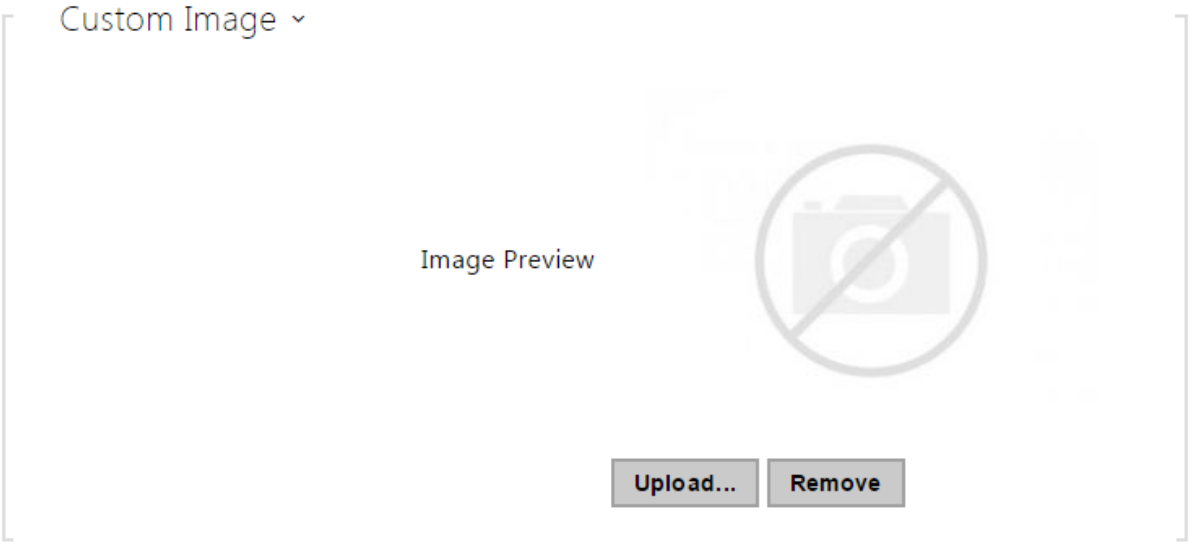
The users are displayed in the order in which they were added to the group. Move a user up/down with the mouse to change the user order. Or, press A-Z to arrange the users in a group alphabetically.



This tab helps you set the users to be displayed in the Name Tags mode. Select up to 4 users from the phonebook and assign them to the buttons on the display sides. If you do not assign any user, the Name Tags mode will be inactive. In the Name Tags mode, the user names are displayed with guidelines and arrows pointing to the right button on the display sides.

Name Tags (for 2N ® Helios IP Vario only)

If you do not like the default graphic appearance of the name tags, load a background of your own to the intercom. Make sure that the image resolution is 320 x 208 pixels. Upload your name tags to the intercom to replace the original name tags. The original user assignments, however, remain the same.



Slideshow

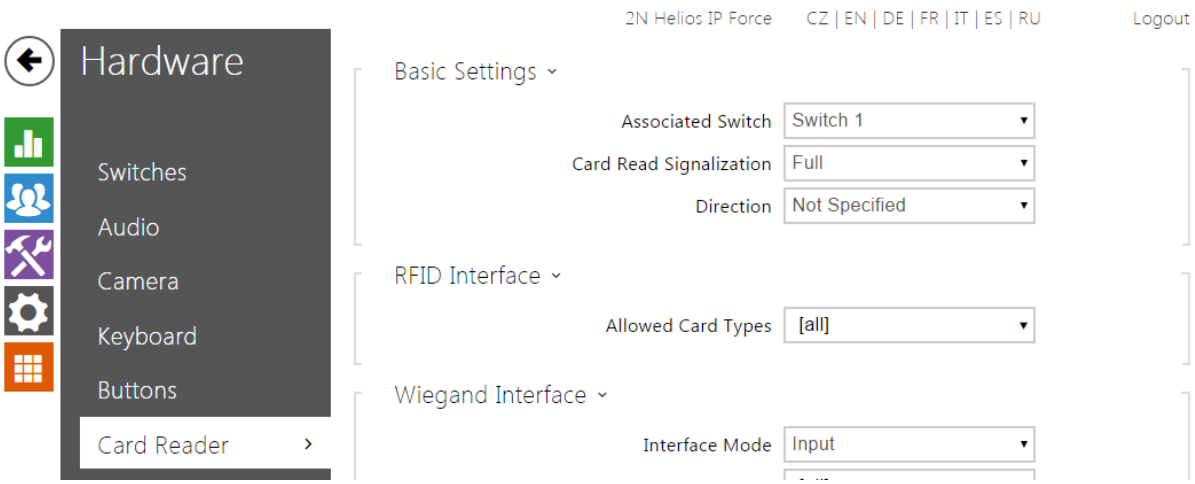
This tab helps you configure a list of images to be displayed in the Slideshow mode. Upload up to 8 images to be shown with a preset delay.

Make sure that the image resolution is 320 x 240 pixels. Other sizes will be adjusted to the display resolution automatically.

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

Slideshow Images

5.3.8 Card Reader



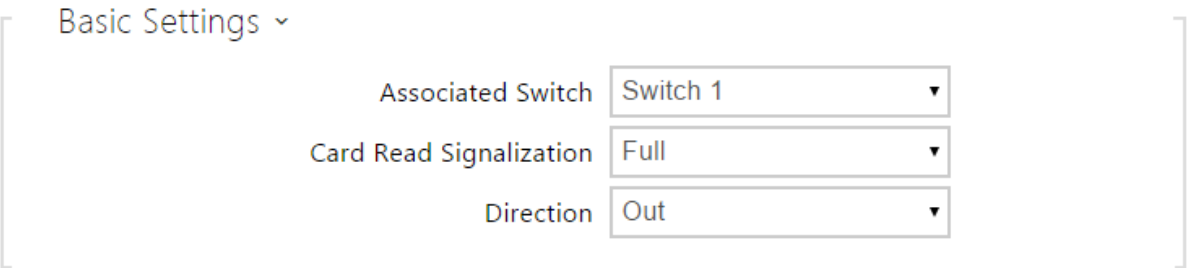
This menu is available in the **2N® Helios IP Vario** and **2N® Helios IP Force** models only.

Configure the **2N® Helios IP Verso** card reader in the **Extenders** menu.

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.

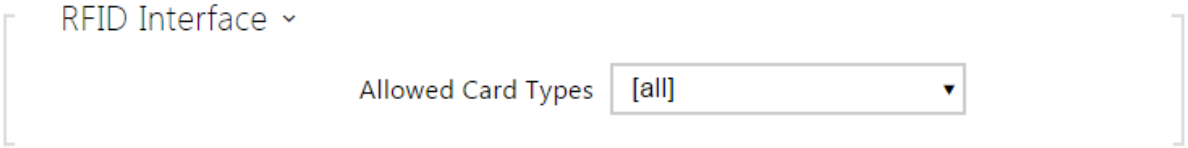
The **2N® Helios IP Vario** and **2N® Helios IP Force** card readers are equipped with an input/output Wiegand interface. The interface direction is configurable. In the input mode, the interface can be used for connection of external card readers, fingerprint readers, biometric data readers and so on. In the output mode, the interface helps connect the intercom to the security exchange, e.g. and send IDs of the cards tapped on the internal reader to this exchange.

List of Parameters

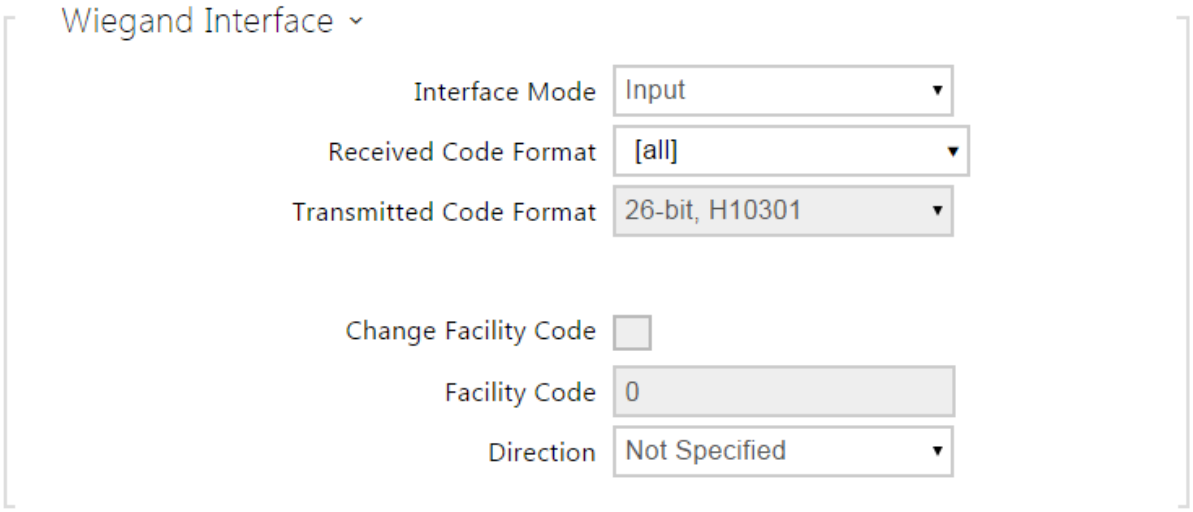


- **Associated switch** – select a switch to be activated whenever a valid card is applied. The set value is not applied when a valid user card is tapped on the reader while the double authentication mode is enabled. In this case, a numeric switch activating code is required to identify the switch to 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 the passage direction for the card reader (Not Specified, In, Out) for the attendance system purposes.



- **Allowed card types** – select one or more card types to be accepted. If no selection is made, all types of supported cards are accepted.



- **Interface mode** – enable the Wiegand function and set Wiegand IN/OUT. The IDs of the cards tapped on the internal card reader are always resent to Wiegand OUT.
- **Received code format** – select one or more message formats to be received via the Wiegand interface. If no selection is made, all supported message formats are accepted.
- **Transmitted code format** – set the sent message format: 26-bit, 32-bit, 37-bit or RAW.

26-bit message format (HID26)

Bits are sent to the Wiegand interface from the left to the right

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
E	F	F	F	F	F	F	F	F	C	C	C	C	C	C	C	C	C	C	C	C	C

22	23	24	25
C	C	C	O

E – Even parity, it is counted from bits 1 – 12

O – Odd parity, it is counted from bits 13 – 24

F – Facility code

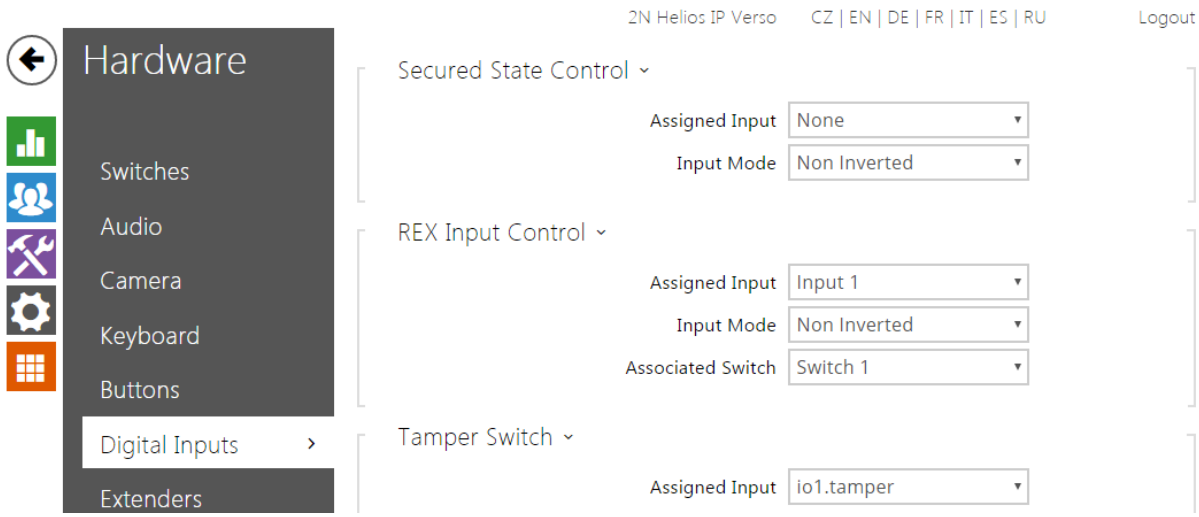
C – Card code

Note

- 37bit message is modified according to the interface specification – received and transmitted ID may differ.

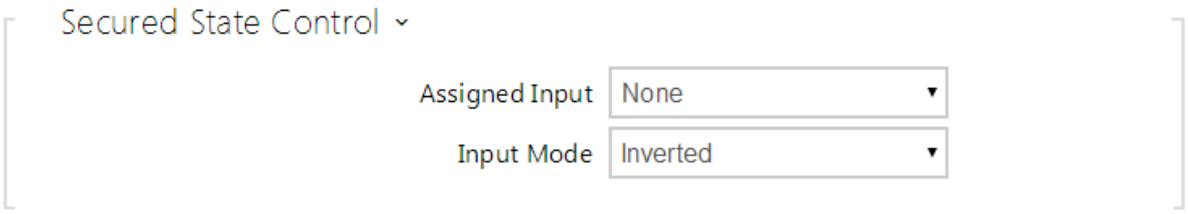
- Change facility code – set the mode in which the first 8 bits of the 24 card ID resent to the Wiegand interface are replaced with the value included in the Facility code. Facility code value is entered in the decadic number format (allowed value is 0–255). The parameter is applied only if the Wiegand is OUT.
- Facility code – enter the facility code for card ID resending to Wiegand
- Direction – set the passage direction for a Wiegand-connected card reader (Not Specified, In, Out) for the attendance system purposes.

5.3.9 Digital Inputs



In this configuration section set the parameters associated with digital inputs and their interconnections with other intercom functions. The digital inputs are available in selected intercom models or where appropriate equipment is installed (Vario/Force model card readers, e.g.).

List of Parameters

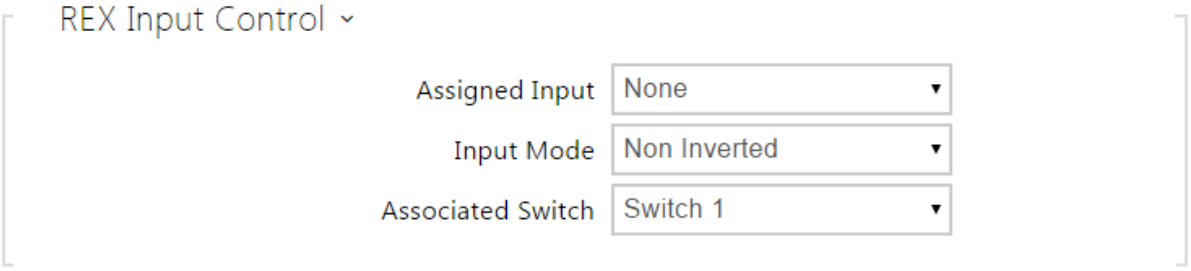


- Assigned input – define one (or none) of the logical inputs for secured state detection. The secured state is then signalled by a LED on the intercom, whose location may vary in different intercom types.
- Input mode – set the active input mode (polarity).

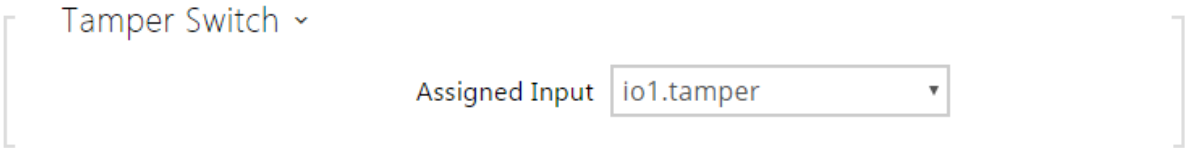
Note

- *Secured state signalling is typically used with a security PBX connected to one of the intercom digital inputs. The wire leading from the PBX is connected to the intercom directly or via an extending module. The secured state LED location is variable depending on the intercom type:*

  *The **2N® Helios IP Vario** (91371...U) intercoms are equipped with a red LED indicator located in the middle of the backlit name tags. The **2N® Helios IP Force** intercoms are equipped with a red LED indicator located in the integrated card reader window. The **2N® Helios IP Verso** intercoms are equipped with a red padlock pictogram in the left-hand upper corner of the basic module.*

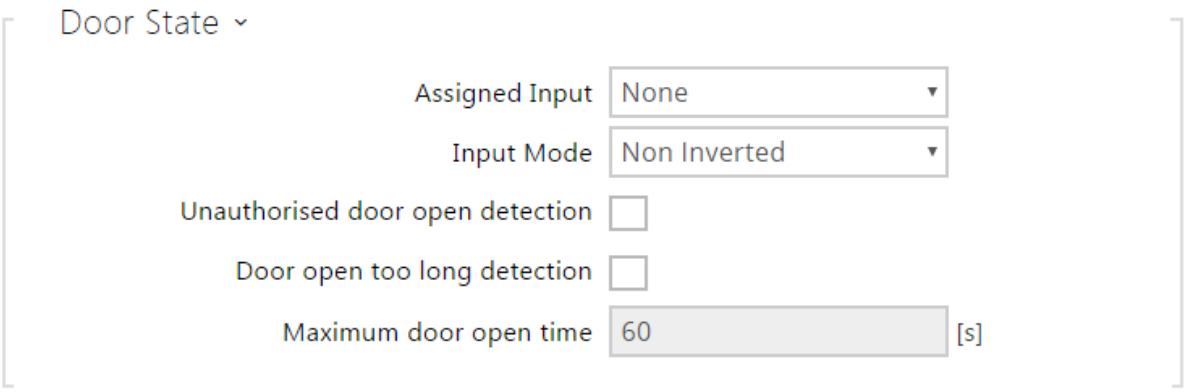


- **Assigned input** – select one (or none) of the logic inputs for the departure button function. Activation of the departure button input activates the selected switch. The activation time and mode are set by the selected switch parameters.
- **Input mode** – set the active input mode (polarity).
-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



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.



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).

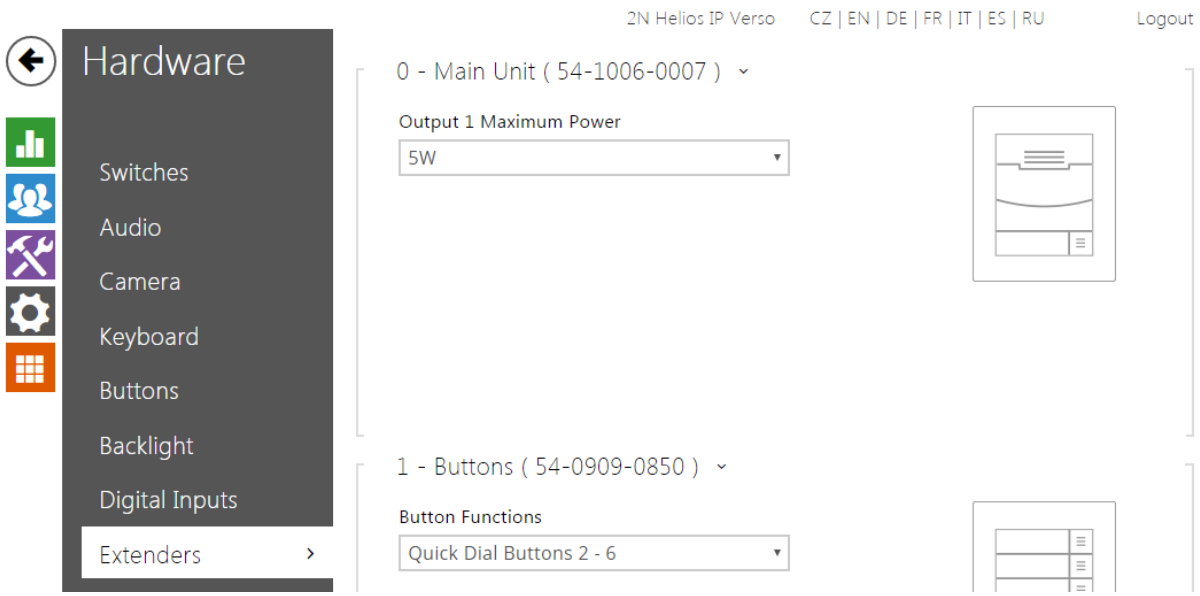
- **Assigned input** – assign one logical input to the door open sensor.
- **Input mode** – set the input active mode (polarity).
- **Unathorised door open detection** – enable **UnauthorisedDoorOpen** signalling. This event is signalled if the door opens when the electric lock is inactive.
- **Door 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*

5.3.10 Extenders



The 2N® Helios IP Verso intercoms can be enhanced with extending modules connected to the intercom basic unit. The following modules are available:

- five-button module
- keypad module
- Infopanel module
- card reader module
- Bluetooth module
- I/O module
- Wiegand module
- inductive loop module
- display module

The modules are chain-like interconnected. Each of the modules has its number depending on the chain position (the first module has number 1). The basic unit is a special type of module and has number 0.

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

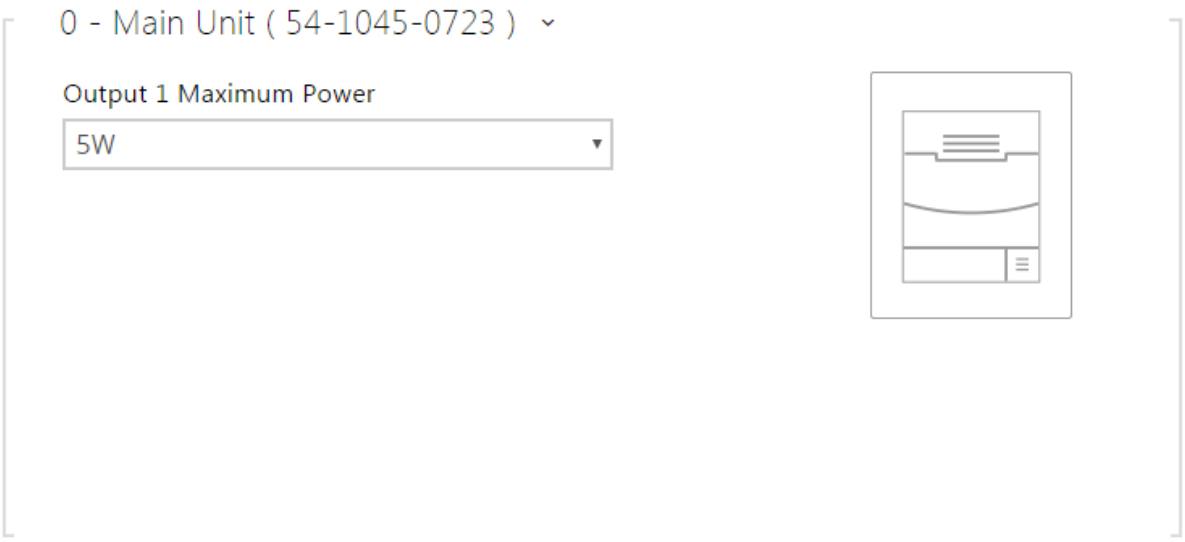
Note

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

Caution

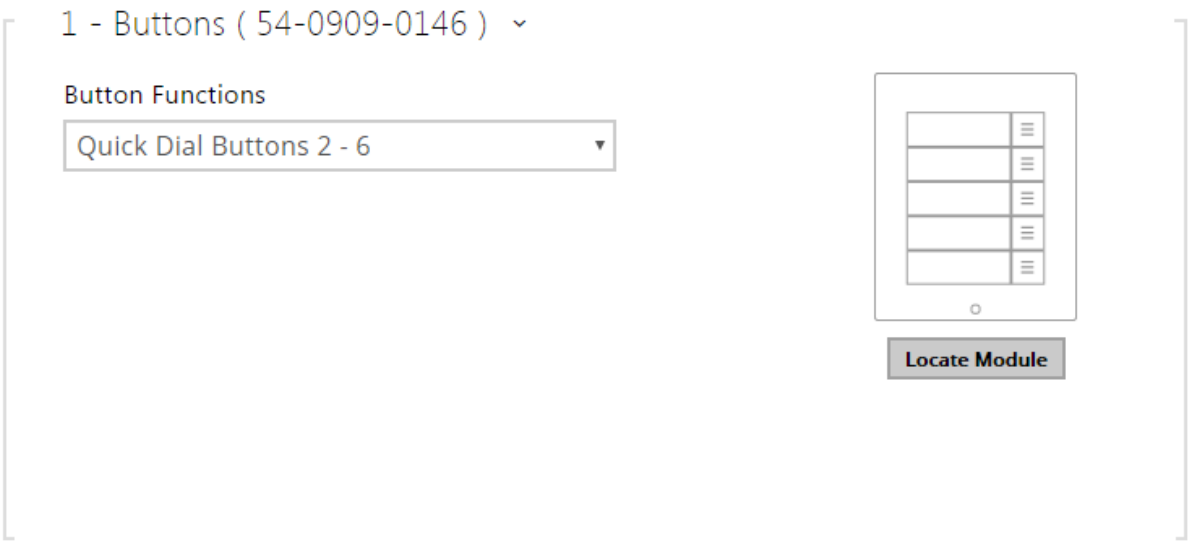
- Module Name has to be unique.

Basic Unit Module Configuration



- Output 1 maximum power – set the maximum load to be connected to the power output available on the basic unit. When the output is active, the consumption of the other modules (backlight level, etc.) can be adjusted automatically in order that the maximum allowed consumption of the intercom cannot be exceeded.

Button Module Configuration



- Button function – assign user positions to the buttons.

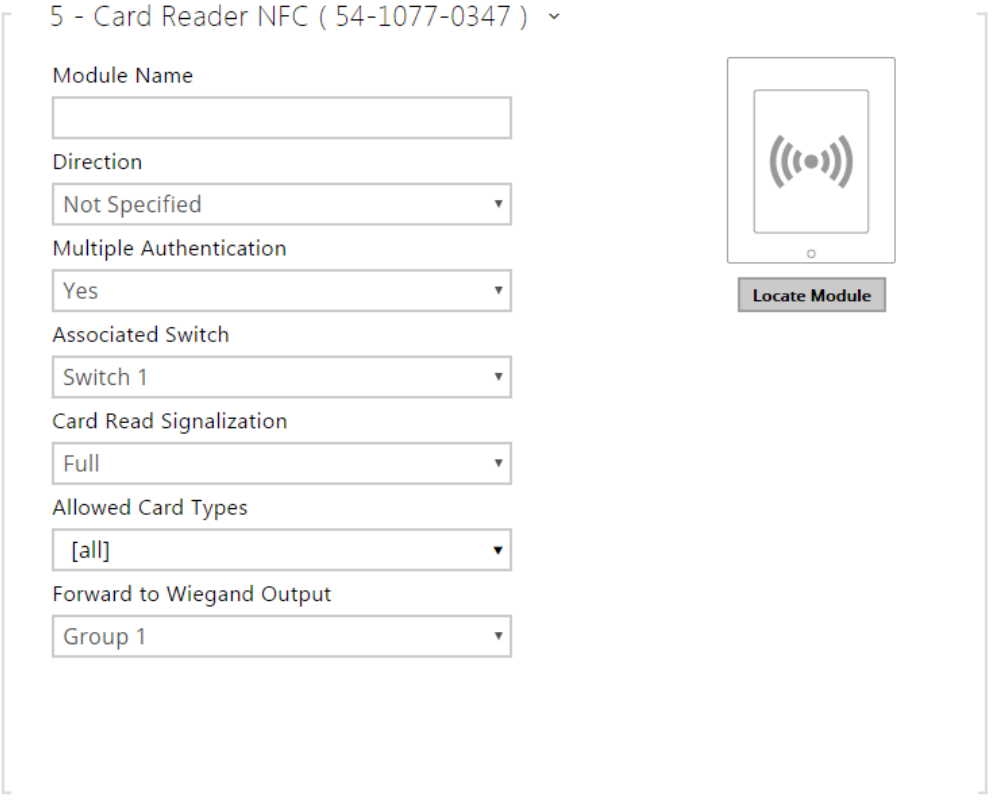
Keypad Module Configuration

- No parameters are available to the public at present.

Infopanel Module Configuration

- No parameters are available to the public at present.

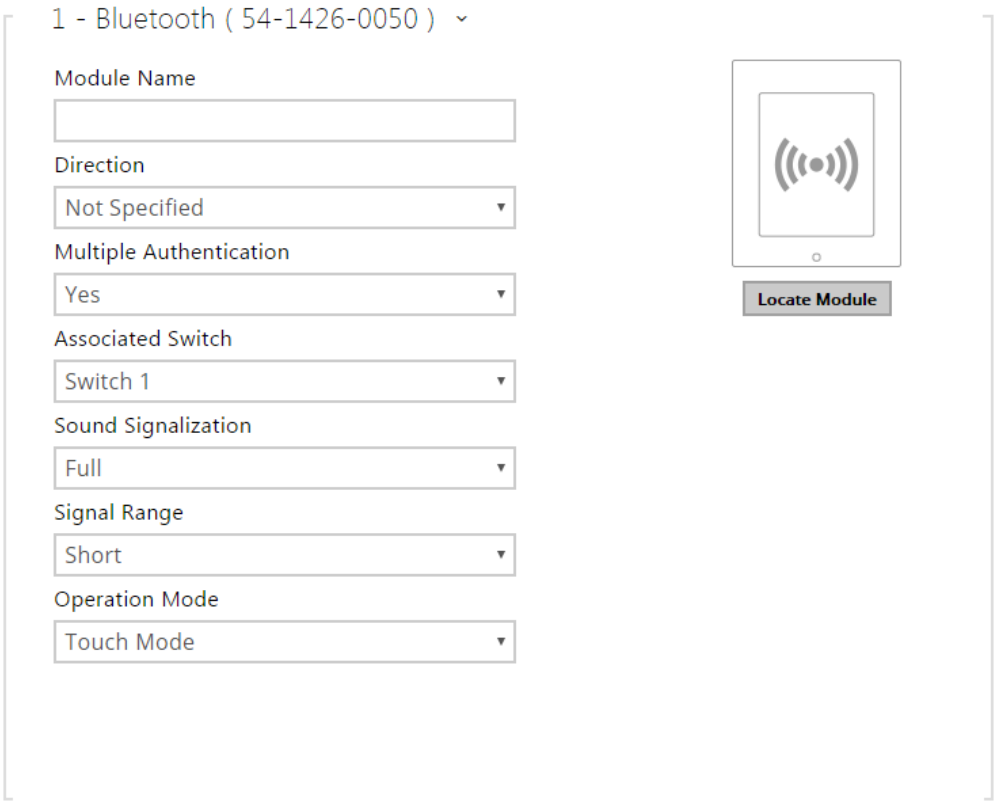
Card Reader Module Configuration



- Module name – set the module name for card reader logging purposes.
- Direction – set the passage direction for the card reader (Not Specified, In, Out) for the attendance system purposes .

- **Multiple authentication** – enable multiple user authentication via the card reader (or the user authentication option defined in **Directory / Users**). Disable multiple authentication for a card reader to cancel code authentication via the numeric keypad.
- **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
- **Allowed card types** – select one or more card types to be accepted. If no selection is made, all types of supported cards are accepted.
- **Forward to Wiegand output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resent .

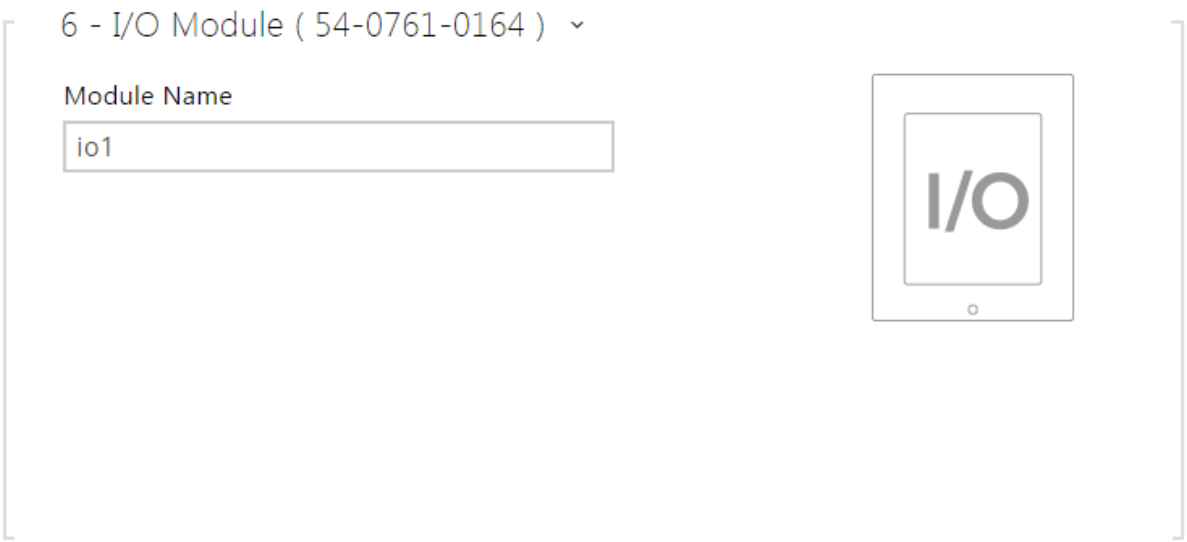
Bluetooth Module



- **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

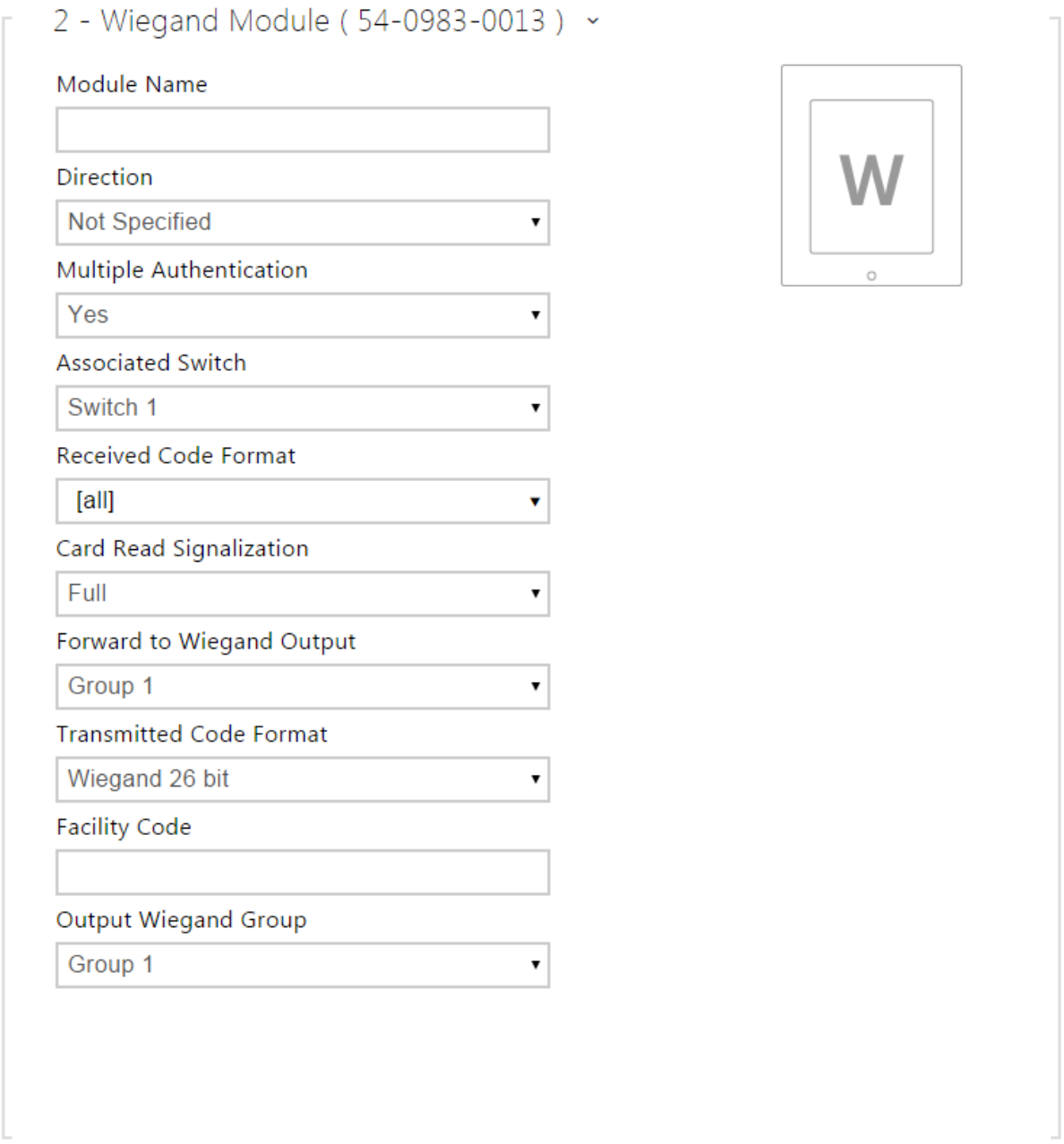
I/O Module Configuration



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

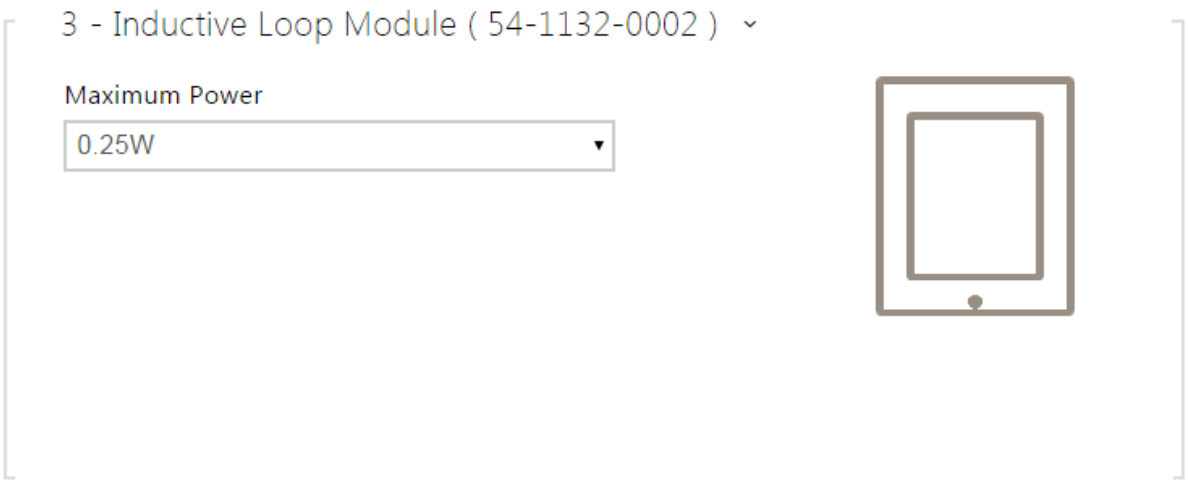
Wiegand Module Configuration

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



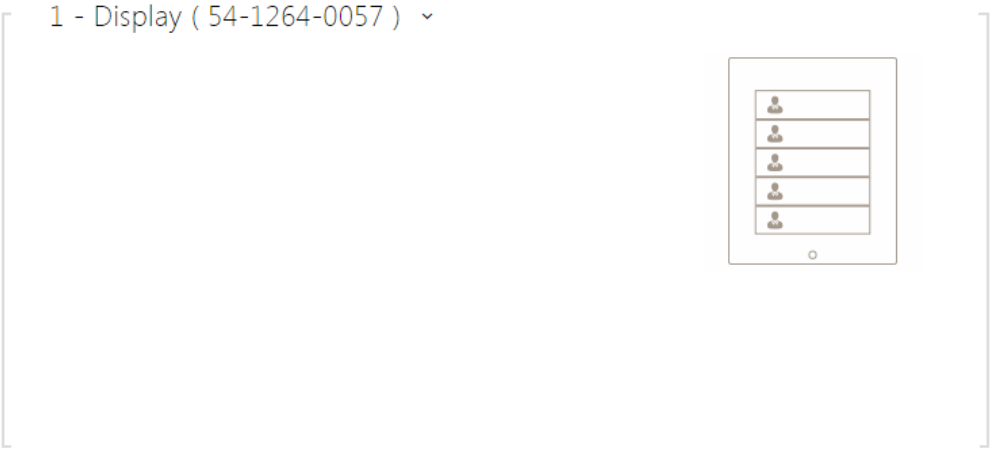
- **Module name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **Automation** settings.
- **Direction** – set the passage direction for the card reader (Not Specified, In, Out) for the attendance system purposes.
- **Multiple authentication** – enable multiple user authentication via a Wiegand-connected card reader (or the user authentication option defined in **Directory / Users**). Disable multiple authentication for a card reader to cancel code authentication via the numeric keypad.
- **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 will 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 group to which the codes from the connected card readers or Wiegand inputs can be resent.

Inductive Loop Module Configuration



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

Display Module Configuration

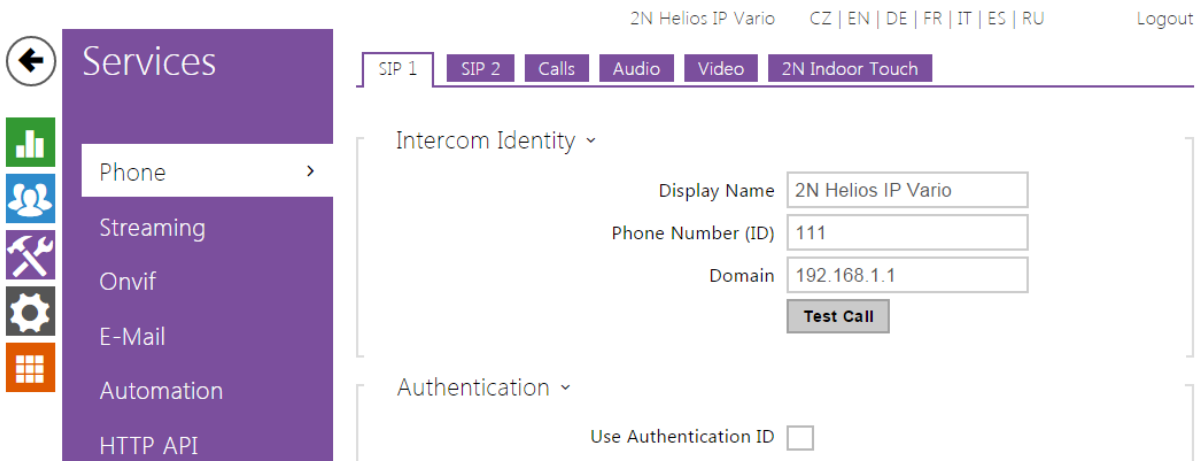


5.4 Services

Here is what you can find in this section:

- 5.4.1 Phone
- 5.4.2 Streaming
- 5.4.3 ONVIF
- 5.4.4 E-Mail
- 5.4.5 Mobile Key
- 5.4.6 Automation
- 5.4.7 HTTP API
- 5.4.8 User Sounds
- 5.4.9 Web Server
- 5.4.10 Audio Test
- 5.4.11 SNMP

5.4.1 Phone



The Phone service is one of the basic functions of the intercom: helps you establish connections with other IP network terminal equipment. The **2N Helios IP** intercoms support the extended SIP and are compatible with and certified by the leading SIP PBX and terminal equipment manufacturers (CISCO, Avaya, Broadsoft, etc.).

The intercom supports up to five parallel calls: 1 outgoing and up to 4 incoming calls. Just one of the calls can be **active** – the audio stream is interconnected with the microphone and speaker and video stream with the camera. The other calls are always **inactive** – the microphone and speaker are muted, the intercom receives the DTMF characters for the opponent to control the intercom (activate/deactivate profiles, users, etc.).

Typically, the intercoms are used for outgoing calls and incoming calls are inactive – the microphone and speaker are muted. However, you can configure your intercom to make incoming calls active and ringing; refer to the **Calls** tab. Press the * and # keys on the numeric keypad to answer and terminate an incoming call.

The **2N Helios IP** intercoms use the **G.711**, **L16, G.722** and **G.729** protocols (with a licence key) to encrypt or compress audio streams and the **H.263** or **H.264** codecs to compress video streams. Broadband codecs L16 and G.722 are available in selected **2N Helios IP** models only. Choose your preferential codecs in the Audio or Video tab.

Explanation of IP Telephony Terms

- **SIP (Session Initiation Protocol)** – is a phone call signalling transmission protocol used in IP telephony. It is primarily used for setting up, terminating and forwarding calls between two SIP devices (the intercom and another IP phone in this case). SIP devices can establish connections directly with each other (Direct SIP Call) or, typically, via one or more servers: SIP Proxy and SIP Registrar.

- SIP Proxy – is an IP network server responsible for call routing (call transfer to another entity closer to the destination). There can be one or more SIP Proxy units between the users.
- SIP Registrar – is an IP network server responsible for user registration in a certain network section. As a rule, SIP device registration is necessary for a user to be accessible to the others on a certain phone number. SIP Registrar and SIP Proxy are often installed on one and the same server.
- RTP (Real-Time Transport Protocol) – is a protocol defining the standard packet format for audio and video transmission in IP networks. 2N Helios IP uses the RTP for audio and video stream transmission during a call. The stream parameters (port numbers, protocols and codecs) are defined and negotiated via the SDP (Session Description Protocol).

The 2N® Helios IP intercoms support three ways of SIP signalling:

- via the User Datagram Protocol (UDP), which is the most frequently used unsecured signalling method
- via the Transmission Control Protocol (TCP), which is less frequent, yet recommended unsecured signalling method
- via the Transaction Layer Security (TLS) protocol, where SIP messages are secured against third party monitoring and modification

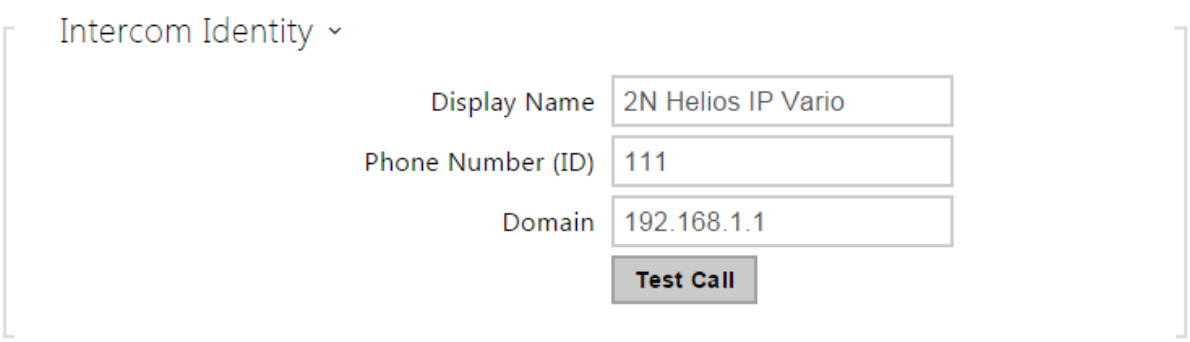
List of Parameters

The 2N Helios IP Phone settings are arranged in five tabs:

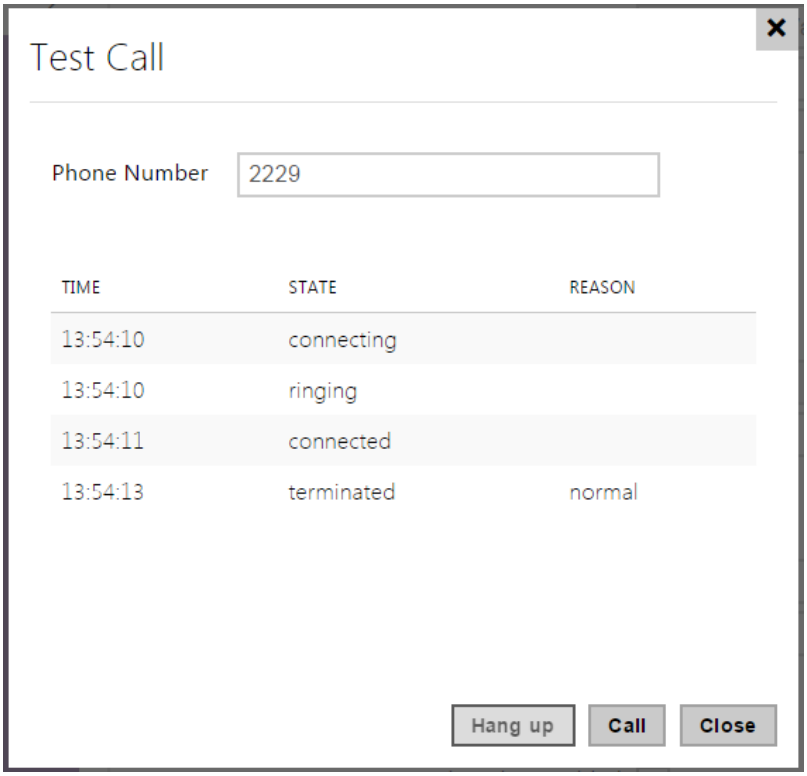
- SIP 1 and SIP 2 – complete SIP terminal settings
- Calls – incoming and outgoing call settings
- Audio – audio codec, DTMF transmission and other audio stream transmission settings
- Video – video codec, video resolution and other video stream transmission settings

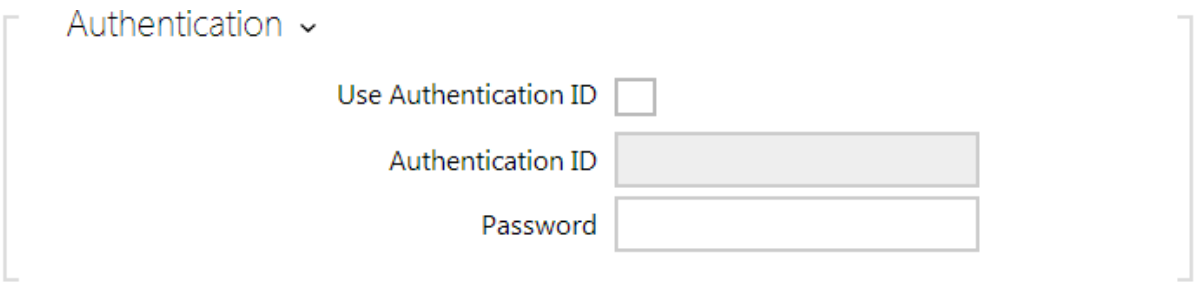
SIP 1 and SIP 2

The 2N® Helios IP intercoms allow two independent SIP accounts (SIP 1 and SIP 2 tabs) to be configured. Thus, the intercom can be registered under two phone numbers, with two different SIP exchanges and so on. Both the SIP accounts process incoming calls equivalently. Outgoing calls are primarily processed by account 1, or, if account 1 is not registered (due to SIP exchange error, e.g.), by account 2. Select the account number for the phone numbers included in the phone directory to specify the account to be used for outgoing calls (example: 2568/1 - calls to number 2568 go via account 1, sip:1234@192.168.1.1 calls to sip uri via account 2).

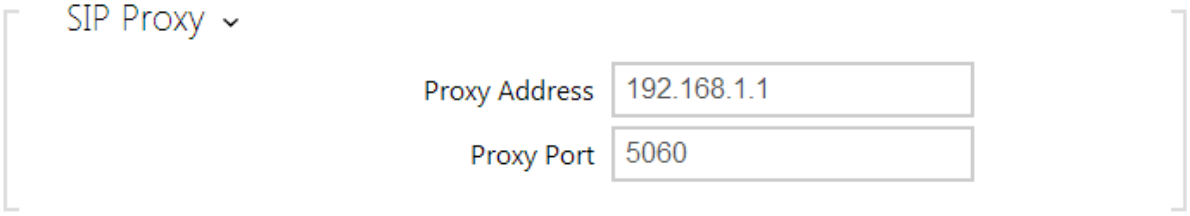


- **Display name** – set the name to be displayed as CLIP on the called party's phone.
- **Phone number (ID)** – set the intercom phone number (or another unique ID including characters and digits). Together with the domain, this number represents a unique intercom identification in calls and registration.
- **Domain** – set the domain name of the service with which the intercom is registered. Typically, it is identical with the SIP Proxy or Registrar address.
- **Test call** – display a dialogue window enabling you to make a test call to a selected phone number, see below.

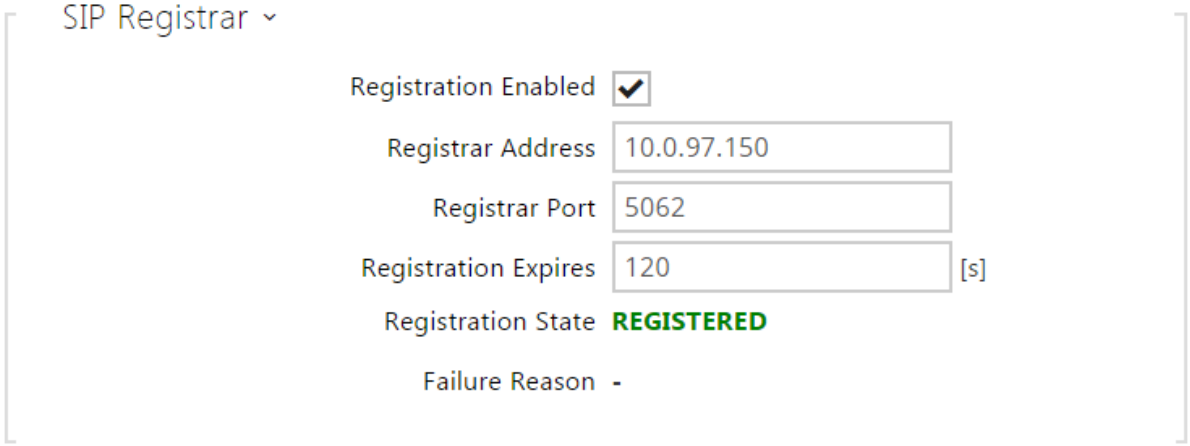




- **Use authentication ID** – enable the use of an alternative ID for intercom authentication. If disabled, the phone number defined above is used for authentication.
- **Authentication ID** – enter the alternative ID for authentication.
- **Password** – enter the password for authentication. The parameter is applied on if your PBX requires authentication.

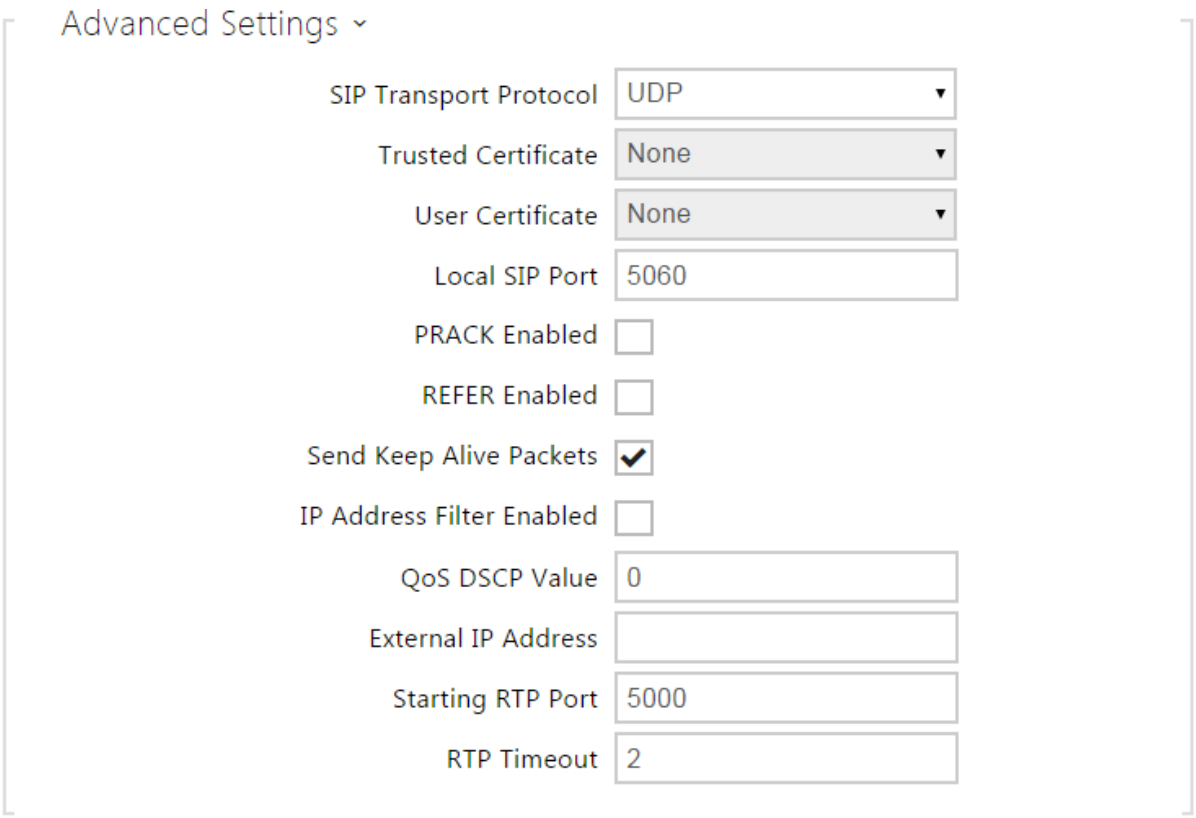


- **Proxy address** – set the SIP Proxy IP address or domain name.
- **Proxy port** – set the SIP Proxy port (typically 5060).



- **Registration enabled** – enable intercom registration with the set SIP Registrar.
- **Registrar address** – set the SIP Registrar IP address or domain name.
- **Registrar port** – set the SIP Registrar port (typically 5060).

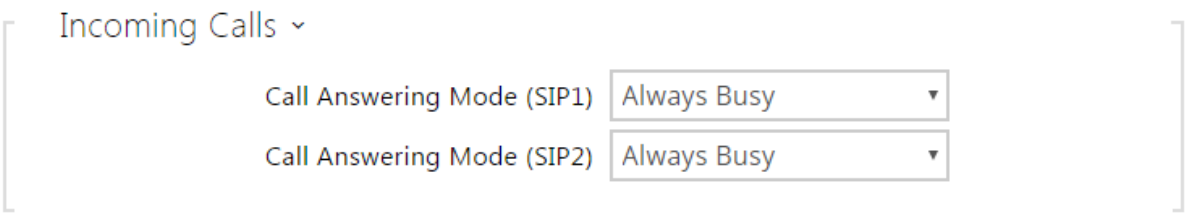
- **Registration expires** – define the registration expiry, which affects the network and SIP Registrar load by periodically sent registration requirements. The SIP Registrar can modify the expiry limit without letting you know.
- **Registration state** – display the current registration state (unregistered, registering..., registered, unregistering...).
- **Failure reason** – display the reason for the last registration attempt failure: the last error reply of the registrar, e.g. 404 Not Found.



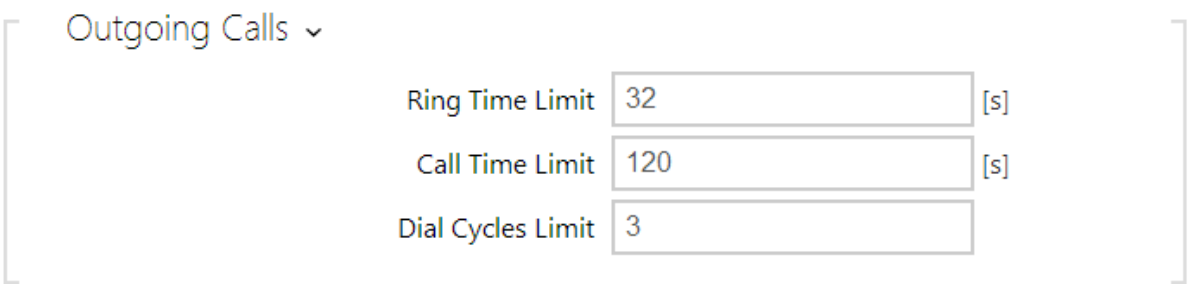
- **SIP transport protocol** – set the SIP communication protocol: UDP (default), TCP or TLS.
- **Trusted certificate** – specify one of the three sets of certificates issued by certification authorities to verify the SIP server public certificate validity, refer to the Certificates subsection. If none is included, the SIP server public certificate is not verified.
- **User certificate** – specify the user certificate and private key to verify the intercom authorisation to communicate with the SIP server. There are three sets of user certificates and private keys, refer to the Certificates subsection.
- **Local SIP port** – set the local port to be used for SIP signalling. The parameter is not applied until the intercom is restarted. The default value is 5060.
- **PRACK enabled** – enable the PRACK method for reliable confirmation of SIP messages with codes 101 - 199 .
- **REFER enabled** – enable call forwarding via the REFER method.

- **Send KeepAlive packets** – define whether the intercom shall, during a call, send periodical SIP OPTIONS requests to inquire about the state of the called station (to detect the station failure, e.g.).
- **IP address filter enabled** – enable the blocking of SIP packet receiving from addresses other than SIP Proxy and SIP Registrar. The primary purpose of the function is to enhance communication security and eliminate unauthorised phone calls.
- **QoS DSCP value** – set the SIP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header. Value is entered in decimal format. The parameter is not applied until the intercom is restarted.
- **Starting RTP port** – set the starting local RTP port in the range of the length of 60 ports to be used for audio and video transmissions. The default value is 5000 (i.e. the used range is 5060–5059). The parameter is only set for account 1 but applies to both the SIP accounts.
- **External IP address** – set the public IP address of the router to which your intercom is connected. If the intercom IP address is public, leave this field blank.
- **RTP timeout** – set the audio stream RTP packet receiving timeout during a call. If this limit is exceeded (RTP packets are not delivered), the call is terminated by the intercom. Set the parameter to 0 to disable this function. The parameter is only set for account 1 but applies to both the SIP accounts.

Calls

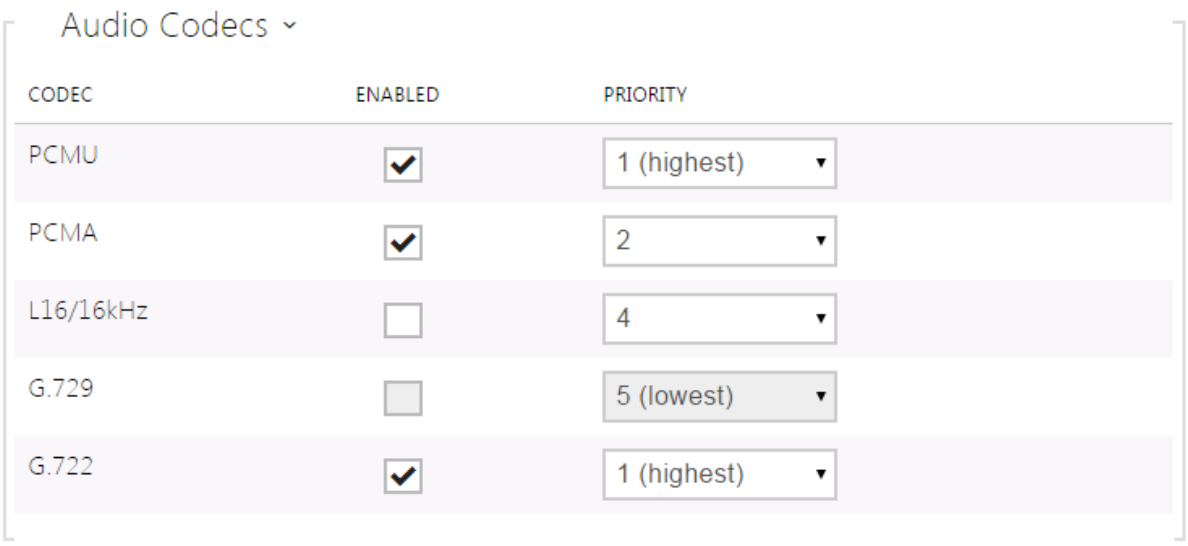


- Call answering mode – set the incoming call receiving mode: **Always Busy** - the intercom rejects incoming calls, **Manual** - the intercom alerts incoming calls and the user answers them using a numeric keypad button, and **Automatic** - the intercom answers incoming calls automatically. You can set the call receiving mode for each SIP account separately.



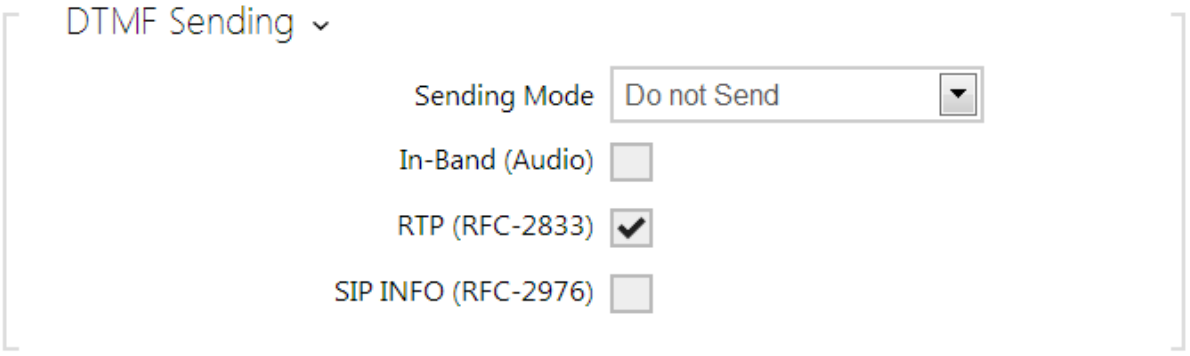
- **Ring time limit** – set the outgoing call setup and ringing time limit after which the calls shall be automatically terminated. If the calls are routed to the GSM network via GSM gateways, your are advised to set a value higher than 20 s. Minimum value 1 s, maximum value 600 s. Configure 0 to disable this time limit.
- **Call time limit** – set the call duration limit after which the call is automatically terminated. The intercom signals termination with a beep 10 s before the call end. Enter any DTMF character into the call (# on your IP phone, e.g.) to extend the call time. The limit is valid for both outgoing and incoming calls. Minimum value 1 s, maximum value 3600 s. Configure 0 to disable this time limit.
- **Dial cycles limit** – set the maximum count of user deputy dial cycles if the user dialled is inaccessible. The function helps you avoid deadlock if the **User deputy** is set to the same value in the users list.

Audio



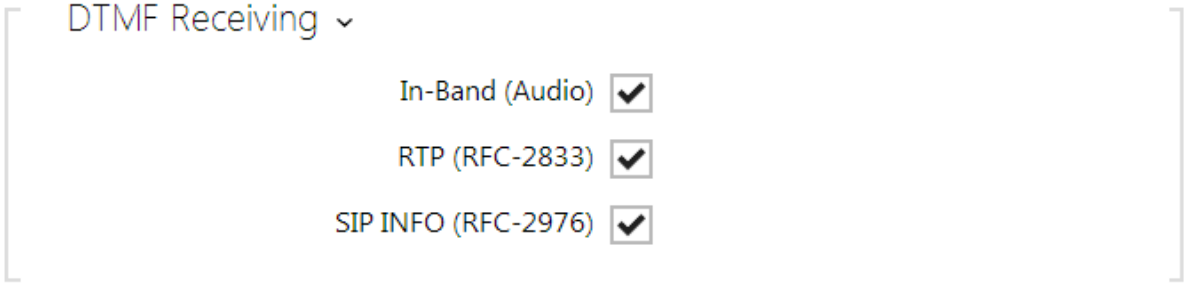
- Enable/disable the use of audio codecs for call setups and set their priorities . Broadband codecs L16 and G.722 are available in selected intercom models only . Codec G.729 is available in selected intercoms only with a valid licence G.729.

The tab below helps you define how DTMF characters shall be sent from the intercom. Check the DTMF receiving options and settings of the opponent to make the function work properly.

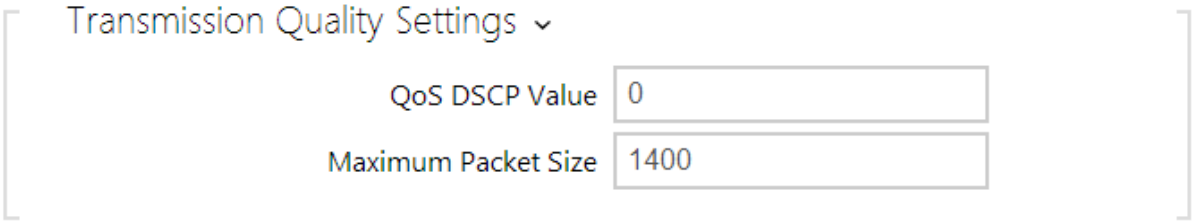


- **Sending mode** – define whether it will be possible to send DTMF during a call by pressing 0 through 9, * and # on the intercom numeric keypad. Set the sending mode for incoming/outgoing/all calls.
- **In-Band (Audio)** – enable classic DTMF dual tone sending in the audio band.
- **RTP (RFC-2833)** – enable DTMF sending via the RTP according to RFC-2833.
- **SIP INFO (RFC-2976)** – enable DTMF sending via SIP INFO messages according to RFC-2976.

The tab below helps you define how DTMF characters shall be received from the intercom. Check the DTMF receiving options and settings of the opponent to make the function work properly.



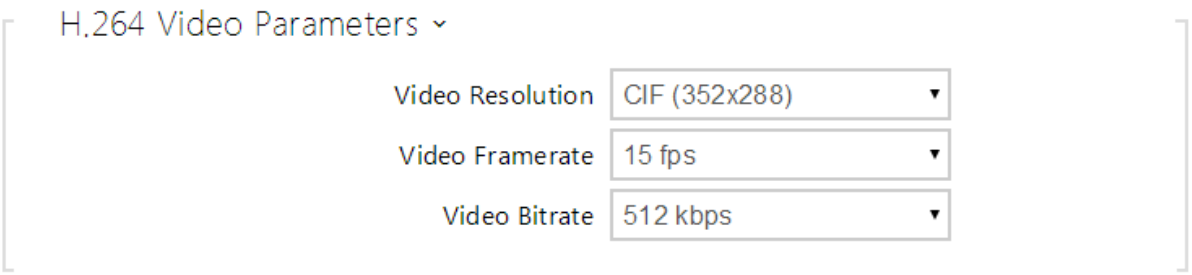
- **In-Band (Audio)** – enable classic DTMF dual tone receiving in the audio band.
- **RTP (RFC-2833)** – enable DTMF receiving via the RTP according to RFC-2833.
- **SIP INFO (RFC-2976)** – enable DTMF receiving via SIP INFO messages according to RFC-2976.

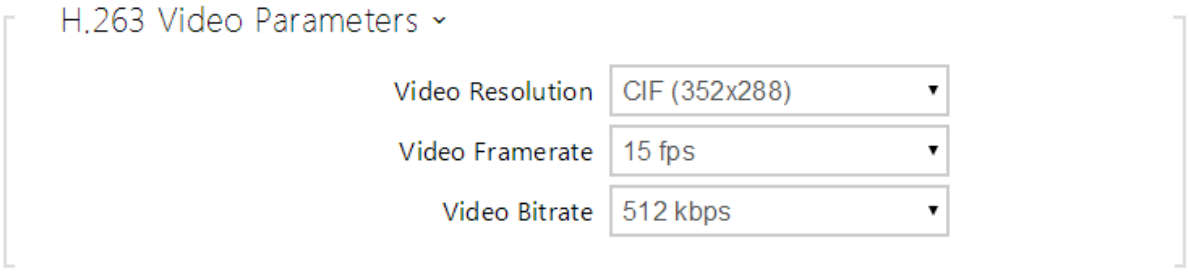


- QoS DSCP value – set the audio RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header. Value is entered in decimal format. The parameter is not applied until the intercom is restarted.
- Jitter compensation – set the buffer capacity for jitter compensation in audio packet transmissions. A higher capacity improves the transmission resistance at the cost of a greater sound delay.

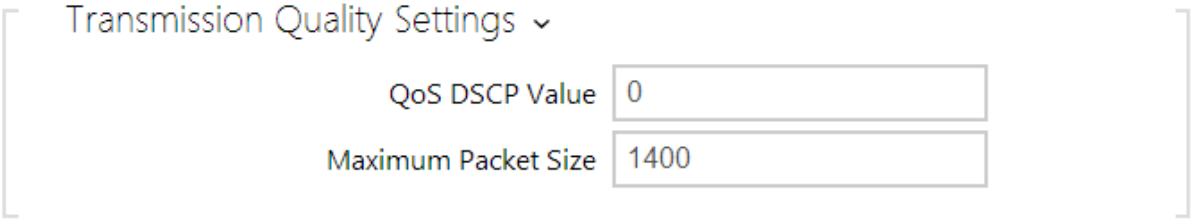
Video

- Enable/disable the use of video codecs for call setups and set their priorities.

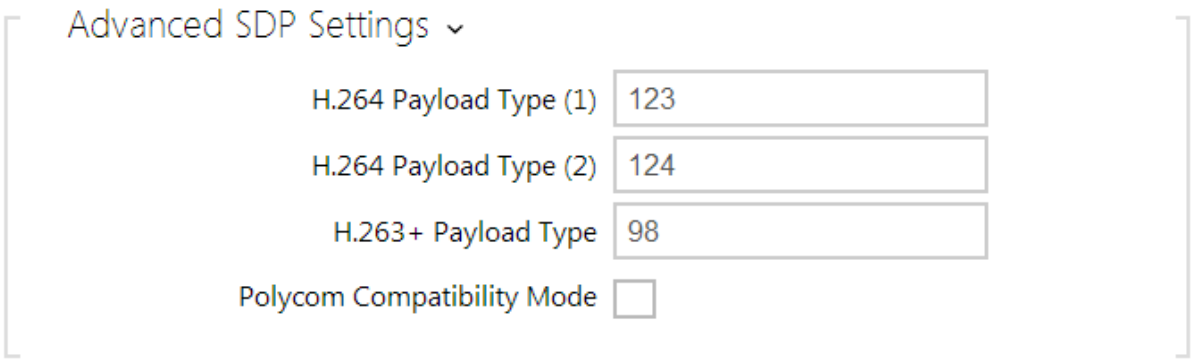




- **Video resolution** – set the video resolution for phone calls.
- **Video framerate** – set the video frame rate for phone calls.
- **Video bitrate** – set the video stream bit rate for phone calls.



- **QoS DSCP value** – set the video RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.
- **Maximum packet size** – set the size limit for the video RTP packets to be sent.



- **H.264 payload type (1)** – set the payload type for video codec H.264 (packetisation mode 1). Set a value from the range of 96 through 127, or 0 to disable this codec type.
- **H.264 payload type (2)** – set the payload type for video codec H.264 (packetisation mode 2). Set a value from the range of 96 through 127, or 0 to disable this codec type.
- **H.263+ payload type** – set the payload type for video codec H.263+ (packetisation mode 3). Set a value from the range of 96 through 127.
- **Polycom compatibility mode** – set SDP compatibility with some earlier Polycom and Cisco phone models. If this mode is on, the intercom does not send the **sendonly** flag in the SDP message in the video codec offer.

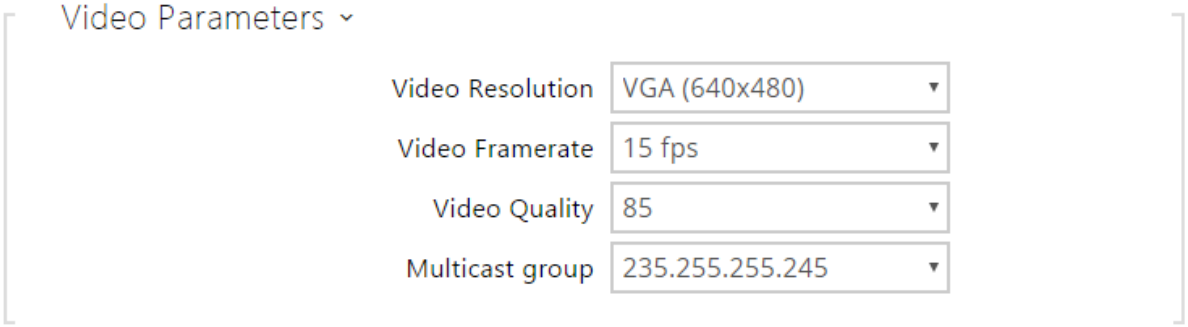
Tip

- For the Video Preview feature at the **Grandstream GXV 3275** phone (video transferred via Early Media) no configuration is needed. Check your PBX vendor whether this feature is supported by your PBX system.
- For the Video Preview feature at the **Gigaset Maxwell 10** phone (video transferred via jpg images) it is necessary to set **Connection Type** to **Unsecure** and **Authentication** to **None** at the **Camera API** in **HTTP API.**

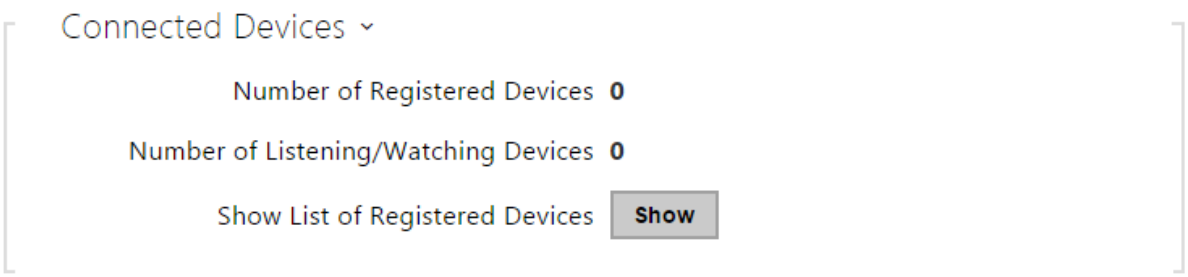
2N ® Indoor Touch Tab

This tab contains settings for connection of the **2N®** **Indoor Touch** devices the intercom. The main parameter is the access key, which secures the connection and enables you to create multiple independent groups of intercoms and **2N®** **Indoor Touch** devices within the local network. It also contains the video transmission settings.

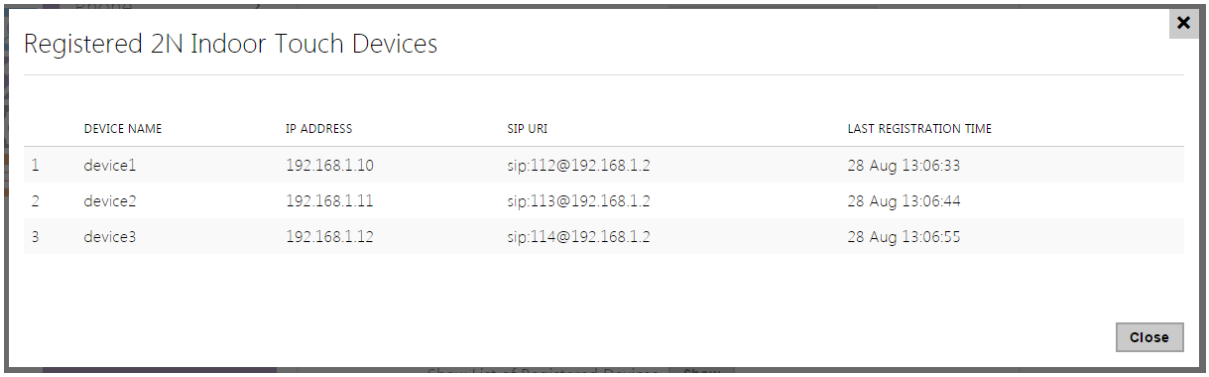
- **Access key** – set the access key to be shared by the intercom and 2N® Indoor Touch. If the access keys do not match in the intercom and 2N® Indoor Touch, the intercom cannot call the 2N® Indoor Touch device and the 2N® Indoor Touch device cannot receive video from the intercom. Each intercom can be assigned up to three access keys and thus become a member of up to three independent **2N® Indoor Touch** groups.



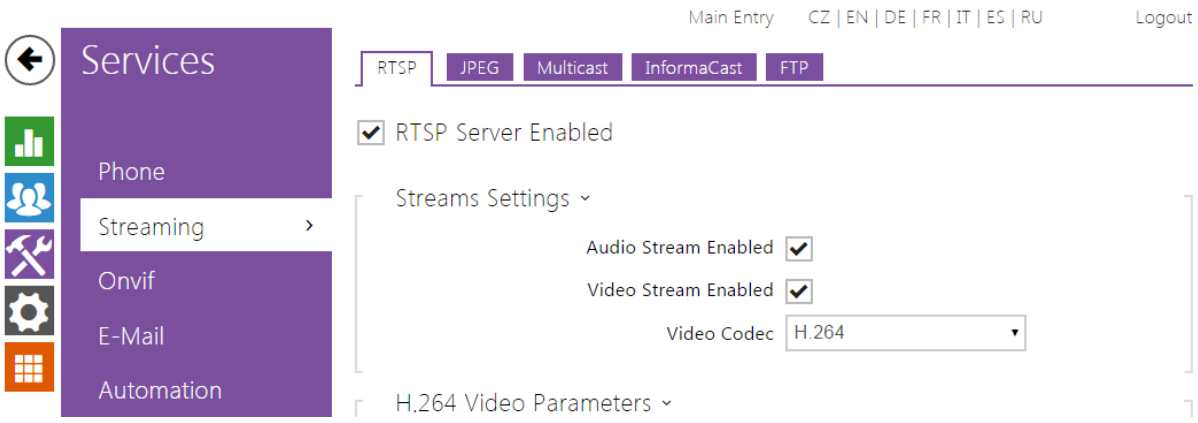
- **Video resolution** – s et the resolution of the video stream to be sent to **2N® Indoor Touch**.
- **Video framerate** – s et the framerate of the video stream to be sent to **2N® Indoor Touch**.
- **Video quality** – s et the quality of the MJPEG video stream to be sent to **2N® Indoor Touch**.
- **Multicast group** – set the multicast address to which the intercom video stream shall be sent. Select one of the 8 preset addresses or set the mode in which the intercom selects the address automatically.



- **Number of registered devices** – display the current count of **2N® Indoor Touch** devices connected to the intercom, i.e. those registered with the intercom.
- **Number of watching devices** – display the current count of **2N® Indoor Touch** devices watching video streams from the intercom.
- **Show list of registered devices** – display the list of registered **2N® Indoor Touch** devices.



5.4.2 Streaming



The **2N Helios IP** intercoms provide several audio/video streaming methods; refer to the table below:

Transmission method	Description
JPEG/HTTP	Static JPEG image transmission. Refer to the JPEG tab below.
MJPEG /HTTP	A series of consecutive JPEG images, the Server Push - multipart/x-mixed-replace method. Refer to the JPEG tab below.
RTSP + RTP /UDP	RTSP with separate RTP/UDP audio and video streams. Supported both for audio (G.711) and video (H.264, H.263, MPEG-2 and MJPEG). Refer to the RTSP tab below.
RTP/RTSP	RTP tunnelling via RTSP. Supported both for audio (G.711) and video (H.264, H. 263, MPEG-2 and MJPEG). Refer to the RTSP tab below.
RTP/RTSP /HTTP	RTSP tunnelling via HTTP. Supported both for audio (G.711) and video (H.264, H. 263, MPEG-2 and MJPEG). Refer to the RTSP tab below.
RTP/UDP-Multicast	Uncontrolled RTP packet multicast. Supported for audio (G.711) only. Refer to the Multicast tab below.

Explanation of Terms

- RTP (Real-Time Transport Protocol) – is a protocol defining the standard packet format for audio/video transmission via IP networks. 2N Helios IP employs this protocol for audio/video streaming. The RTP transport protocol is either UDP or also RTSP and HTTP.
- RTSP (Real-Time Streaming Protocol) – is a network protocol for streaming server control (controls setting up, launching and stopping of audio/video streams).
- HTTP (Hypertext Transfer Protocol) – helps transmit practically any contents and is used primarily by internet browsers for web server communication. 2N Helios IP uses the HTTP to transmit static JPEG images or MJPEG streams via the HTTP Server Push.
- IP Multicast – is a way of parallel sending of IP packets from one source to multiple stations via IP networks. 2N Helios IP uses IP multicast for sending and receiving audio streams.
- ONVIF (Open Network Video Interface Forum) – is a set of video camera search, configuration and administration specifications for the IP network. The 2N Helios IP intercoms are ONVIF compatible and fully implement the ONVIF Profile S.
- JPEG – is a standard method of lossy compression of images.
- MJPEG – is a video stream encoding format in which each image is compressed separately by JPEG. MJPEG encoding produces high-quality video at a significantly higher bit rate compared to the methods mentioned below.
- H.263 – is a video stream compression standard used in telecommunications. Unlike MJPEG, H.263 uses differences between consecutive images and provides a significantly higher level of compression to the detriment of the video stream quality.
- H.263+ – is like H.263, but supports a different bit stream packetisation method.
- MPEG-4 part 2 – is a video stream compression standard used mostly in areas other than telecommunications, but often supported by IP camera and video surveillance systems. In 2N Helios IP, the compression level and image quality are comparable with the H.263 standard.
- H.264 – is a video stream compression standard. Compared to H.263 and MPEG-4, H.264 provides an approximately identical level of video stream quality but a half bit rate. This type of compression is sometimes called MPEG-4 part 10.
- G.711 – is one of the most common audio transmission standards in telecommunications. It uses the sampling frequency of 8 kHz and data are compressed using logarithmic compression.

List of Parameters

RTSP

The 2N Helios IP intercoms integrate an RTSP server, which can be configured in this tab. The RTSP server allows for audio/video streaming. You can choose the data transmission method, video compression method/parameters and other parameters associated with transmission security and quality.

Enter the following RTSP Uri for connection to the intercom RTSP server:

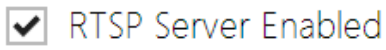
- rtsp://intercom_ip_address/

Set the video stream (video codec type, image resolution, frame rate and bit rate) parameters in the Video section.

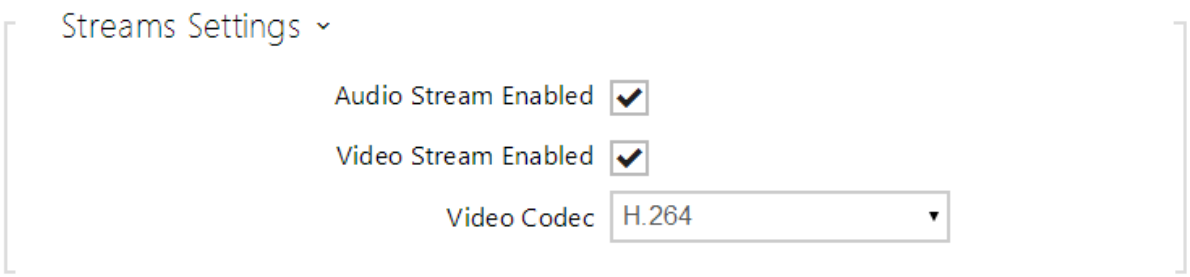
Or, use the following RTSP Uri and choose a codec type other than the currently set one:

1. a. rtsp://ip_intercom_address/h264_stream
   b. rtsp://ip_intercom_address/mpeg4_stream
   c. rtsp://ip_intercom_address/mjpeg_stream

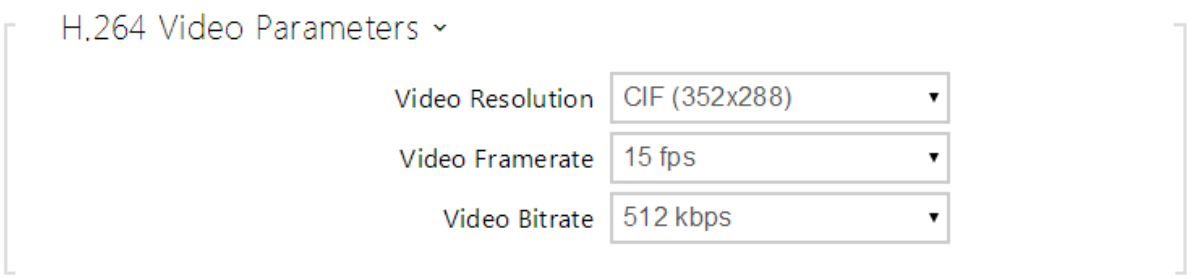
Number of RTSP streams is limited to 4 parallel streams. This number includes both audio streams without video and audio return channel directed to the intercom.

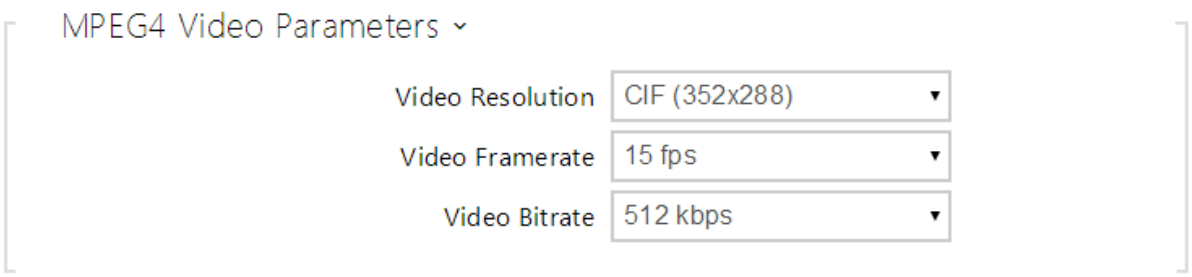


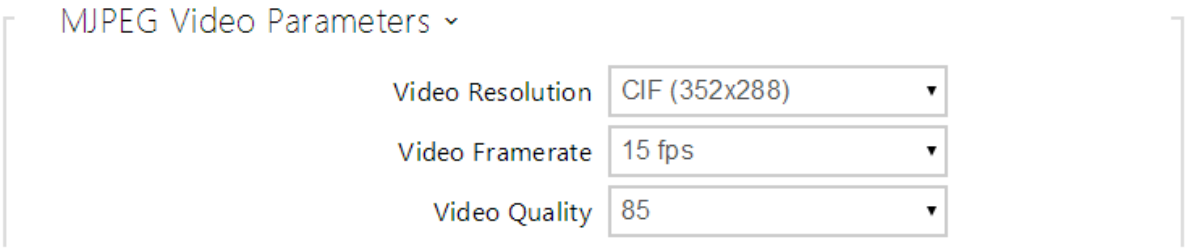
- RTSP server enabled – enable the RTSP server function in the intercom.



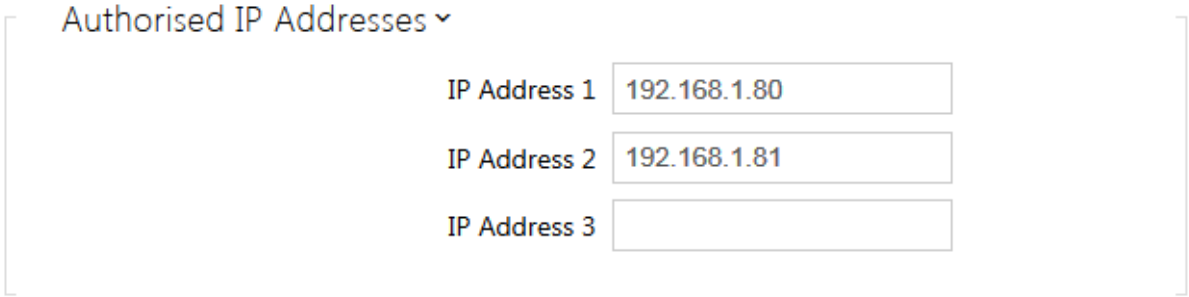
- Audio stream enabled – enable offering of audio stream while establishing connection with the RTSP server.
- Video stream enabled – enable offering of video stream while establishing connection with the RTSP server.
- Video codec – set the default video codec for RTSP streaming.



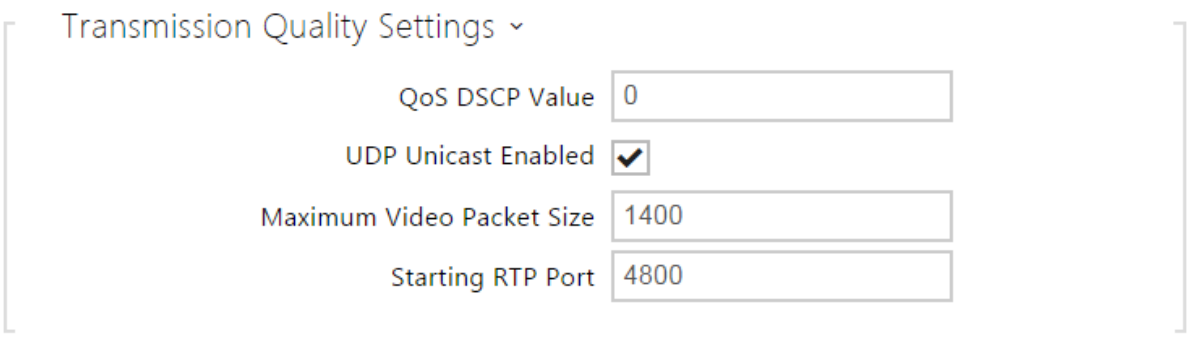




- **Video resolution** – set the default image resolution for RTSP streaming.
- **Video framerate** – set the default video frame rate for RTSP streaming.
- **Video bitrate** – set the default video bit rate for RTSP streaming.
- **Video quality** – set the video compression level (for MJPEG only) ranging between 10 (low quality, lowest bitrate) and 99 (top quality, highest bitrate).



- **IP address 1–4** – set up to 4 authorised IP addresses from which you can log in to the RTSP server. If none of the four fields is completed, any IP address can be used for login.



- **QoS DSCP value** – set the audio/video RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.
- **UDP unicast enabled** – enable audio/video stream sending via the RTP/UDP. If this mode is off, the audio/video stream data are sent via the RTP/RTSP only.
- **Maximum video packet size** – set the maximum size of the video packets to be sent via the RTP/UDP.
- **Starting RTP port** – set the starting local RTP port in the range of the length of 60 ports to be used for audio and video transmissions. The default value is 4800 (i.e. the used range is 4800–4859).

Tip

- FAQ: **VLC Player - How to watch a video from 2N® Helios IPs RTSP server**
- FAQ: **VLC Player - How to record video from 2N Helios IP**

JPEG

Here configure the simplest way of video streaming: JPEG/HTTP and MJPEG/HTTP. Send the following GET address query to download images from the intercom:

- http://intercom_ip_address/api/camera/snapshot?width=W&height=H

or (for MJPEG, HTTP Server Push):

- http://intercom_ip_address/api/camera/snapshot?width=W&height=H&fps=N

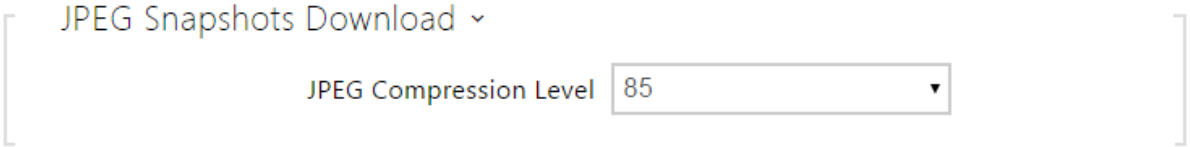
where W and H specify image resolution (supported resolutions: 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 – for 1 MPix camera equipped models only) and N gives the count of snapshots per second (1 through 10).

The following table shows the maximum number of simultaneous MJPEG/HTTP streams in which the rate of outgoing frames using the default level of JPEG compression is not reduced.

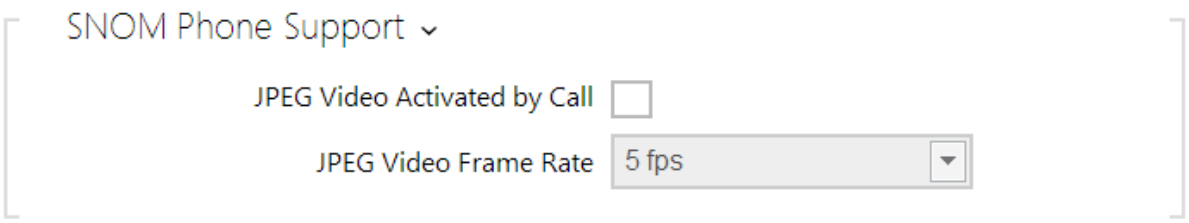
Type of intercom	Resolution	Number of streams
Force/Vario	640 x 480	15
Force HD	640 x 480	15
Force HD	1280 x 960	3
Verso	640 x 480	8
Verso	1280 x 960	2

Note

- *The HTTP Server Push method with the multipart/x-mixed-replace contents is not supported by all internet browsers. Test the function in the Firefox browser, for example.*



- **JPEG compression level** – set the JPEG compression level (1–99). The recommended value is 85. The parameter affects the image size and quality.

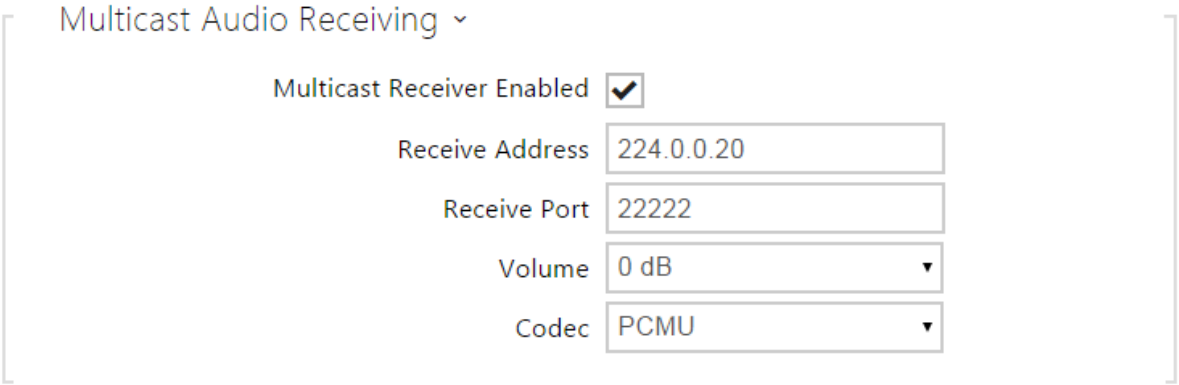


Some IP phones (SNOM 820/870) do not support video calls but are able to download and display JGEG snapshots from the predefined IP address during a call. The **2N Helios IP** intercoms do support this function: set the parameters in this tab.

- **JPEG video activated by call** – enable camera snapshot downloading by Snom 820/870 phones during a call.
- **JPEG video frame rate** – set the frame rate or time periods for camera snapshot downloading by Snom 820/870 phones.

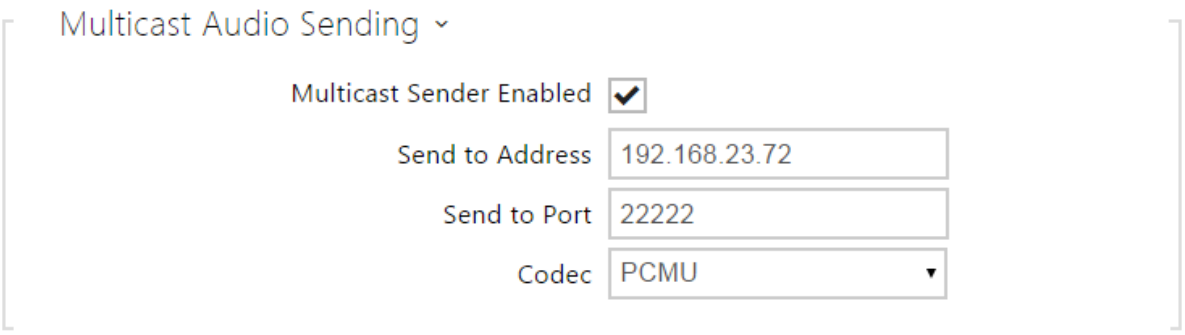
Multicast

The **2N Helios IP** intercoms allow you to stream audio signals (from the microphone or another intercom audio input) via RTP packets sent to the multicast address and receive audio streams in the same format and play them via the integrated speaker or another intercom audio output. The audio stream is encoded by G.711 u-law.



- **Multicast receiver enabled** – enable receiving of RTP packets on the selected multicast address and port. The audio stream received is played during an active call too and the sounds from the two sources get mixed.
- **Receive address** – set the multicast IP address to receive multicast RTP packets.
- **Receive port** – set the local port to receive multicast RTP packets.
- **Volume** – set the received audio stream playing volume.

- **Codec** – set the audio codec for RTP packet decoding: PCMU, PCMA, G.722, L.16. The G.722 and L16 broadband codecs are available in selected intercom models only.



- **Multicast sender enabled** – enable RTP packet sending to the selected multicast address and port.
- **Send to address** – set the destination multicast IP address for the audio stream.
- **Send to port** – set the destination port for the audio stream.
- **Codec** – set the audio codec for RTP packet decoding: PCMU, PCMA, G.722, L.16. The G.722 and L16 broadband codecs are available in selected intercom models only.

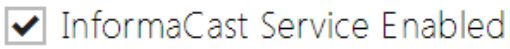
InformaCast

The **2N Helios IP** intercoms support the audio streaming Informacast protocol, which helps you set up an audio stream (unicast/multicast RTP/UDP encoded with G.711 U-law) between the intercom and an Informacast server or any other Informacast client.

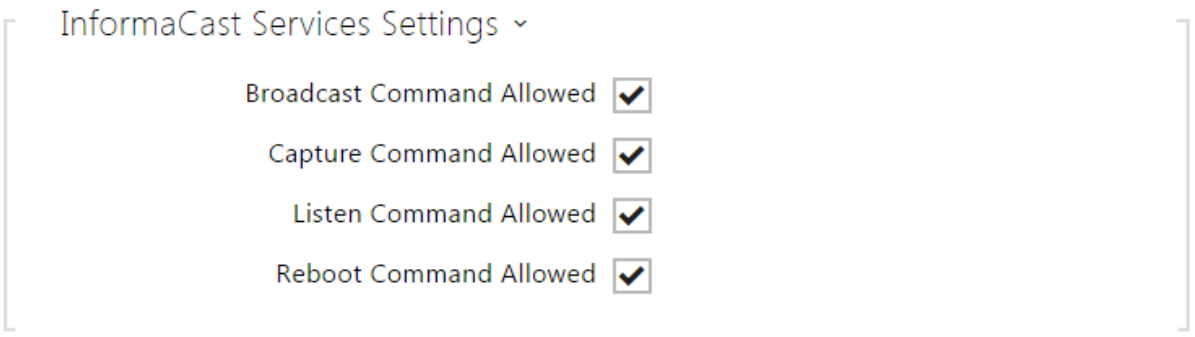
When you enable this service, the Informacast servers are found automatically in the LAN via the SLP and the intercom gets registered with them automatically. The Informacast server with which the intercom is registered can send the audio stream setting up commands to the intercom.

- **Broadcast** – the intercom receives audio from the Informacast server and plays it via an integrated speaker.
- **Capture** – the intercom records audio via an internal microphone and sends it to the Informacast server.
- **Listen** – the intercom receives audio from another Informacast client.

The intercom supports registration with up to 4 Informacast servers at the same time and setup of up to 6 parallel audio streams.



InformaCast service enabled - enable the Informacast service on your intercom side.



Broadcast enabled – enable the Broadcast command to set up an audio stream sent from the Informacast server to the intercom.

Capture enabled – enable the Capture command to set up an audio stream sent from the intercom to the Informacast server.

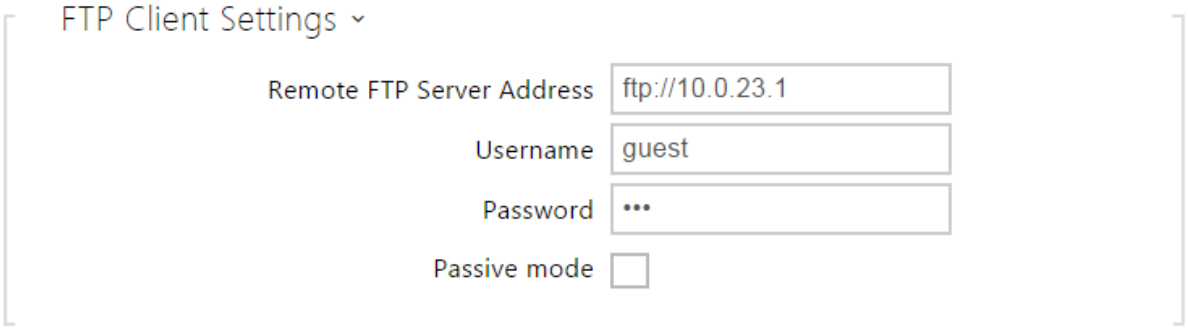
Listen enabled – enable the Listen command to set up an audio stream sent from another Informacast client to the intercom.

Reboot enabled – enable the Reboot command to allow the Informacast server to restart the intercom.

FTP

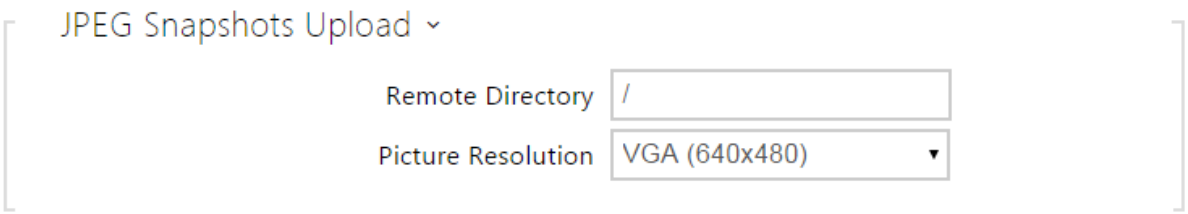
Here define access to the FTP(S) server where images from internal/external cameras can be stored in the JPEG format and selected resolution. The image filename includes the image taking date and time. Images are stored on the FTP server either automatically (periodically or at the call start) or via automation using **Action. UploadSnapshotToFTP** .

- **FTP client enabled** - enable camera image saving to the FTP server.

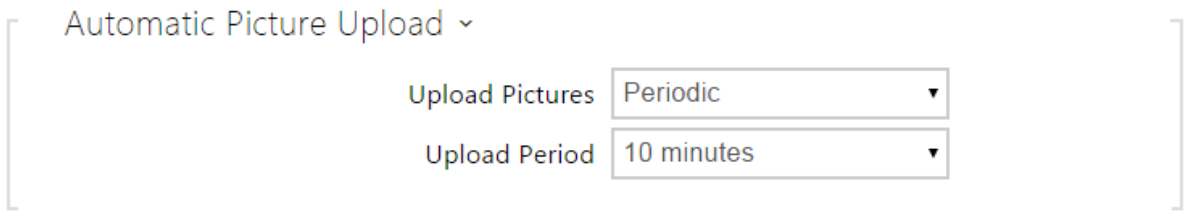


- **Remote FTP server addre ss** – set the FTP server address in the **ftp://ip_address or ftps://ip_address format**.

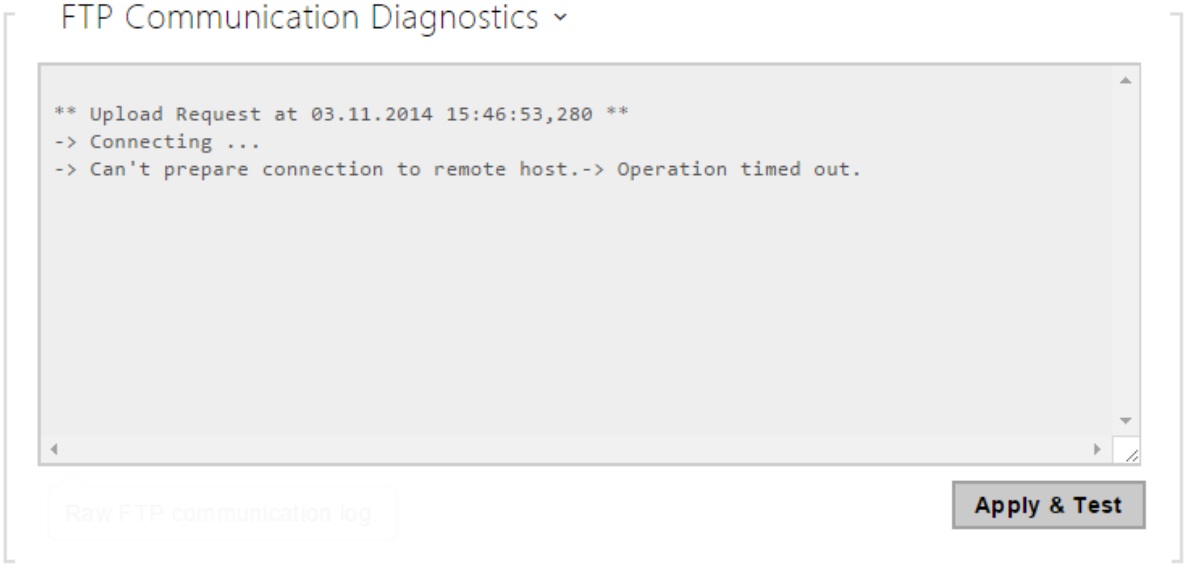
- **Username** – set the FTP server username. The parameter is mandatory if the FTP server requires user authentication.
- **Password** – set a password for the above mentioned FTP server user.
- **Passive mode** – select the passive transmission mode (as web browser).



- **Remote dir ectory** – set the FTP server directory to which the camera images shall be saved.
- **Picture resolution** – set the image resolution.

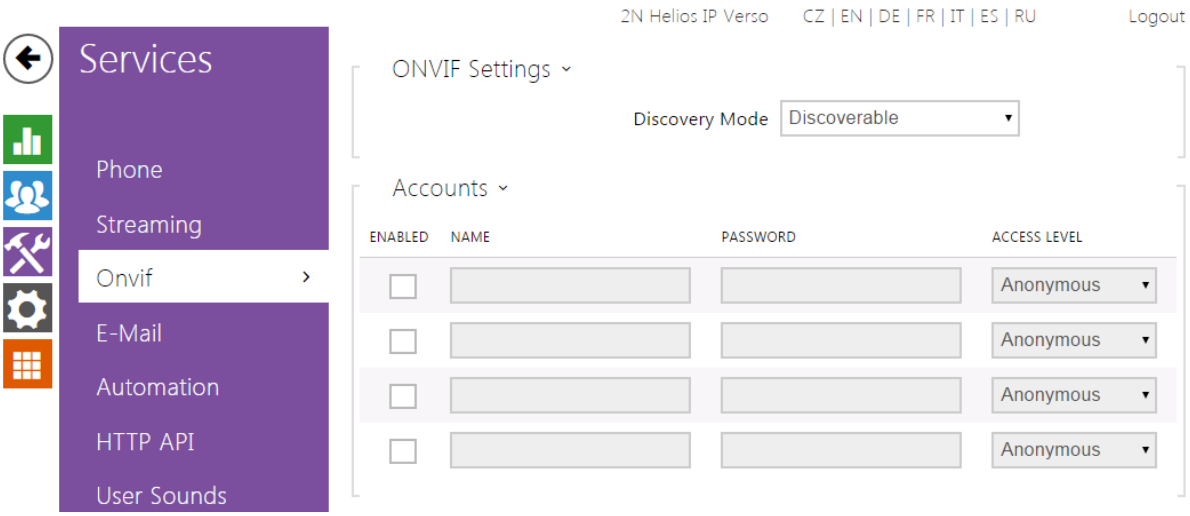


- **Upload pictures** – set automatic picture sending to the FTP server at the call start or after a preset time period. You can disable automatic sending (Automation) and send pictures via **Action.UploadSnapshotToFtp**.
- **Upload period** – set the picture sending period in steps (10 seconds to 30 minutes) when **Upload pictures** is set to **Periodic**.



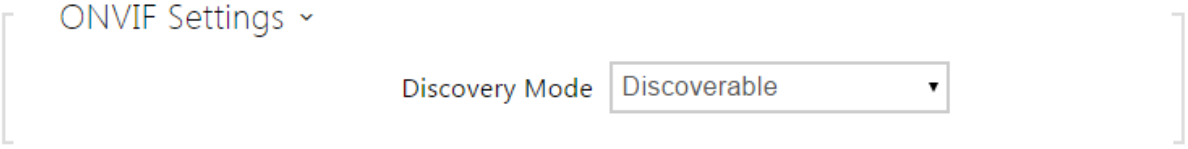
Click Apply & Test to save the current FTP server configuration, load the camera image and save the image to the FTP server. The window above displays the FTP server communication details during saving.

5.4.3 ONVIF

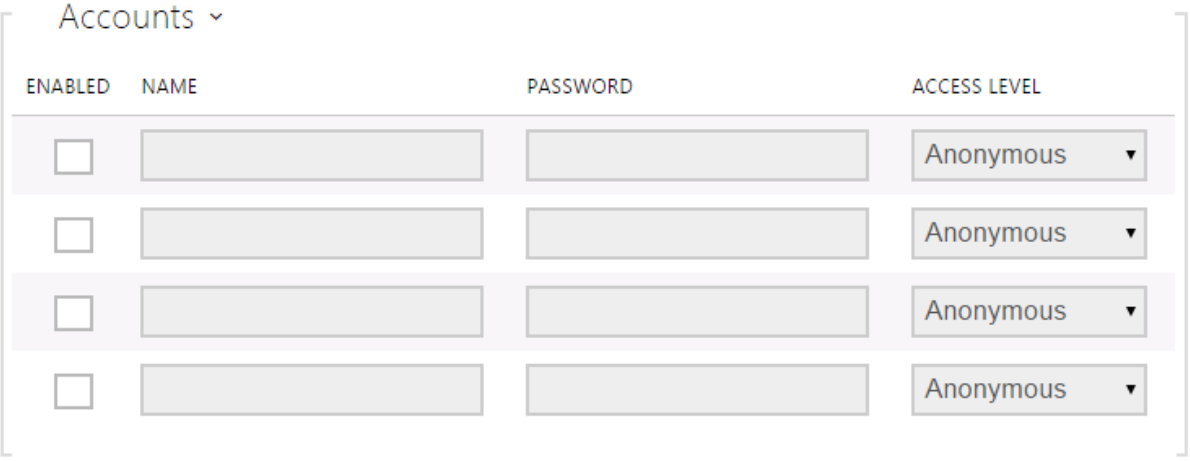


List of Parameters

The **2N Helios IP** intercoms are ONVIF compatible and fully implement the ONVIF Profile S.

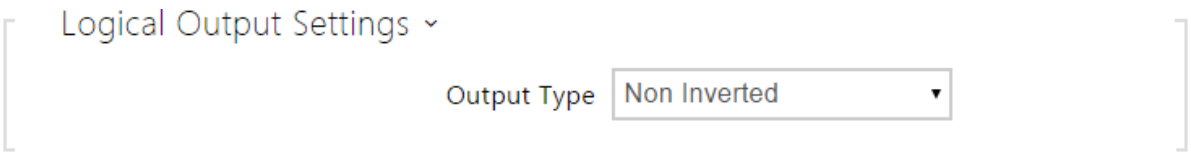


- **Discovery mode** – enable the WS-Discovery function, which allows the other ONVIF clients to search a compatible device in the LAN. Set the parameter to **Discoverable** to use your intercom as an ONVIF compatible device.



For full ONVIF functionality it is required to set at least one user account and set proper access right, according to ONVIF specification and used VMS. Without this, only basic functionality is available.

- - **Enabled** – Enables or disables the user account.
  - **Name** – set the user name for access to ONVIF.
  - **Password** – set the password for access to ONVIF.
  - **Access level** – Sets the level of user rights for the ONVIF servic e (Anonymous, User, Operator, Administrator)



- **Output type** - set the inverted logic input control mode via ONVIF.

Note

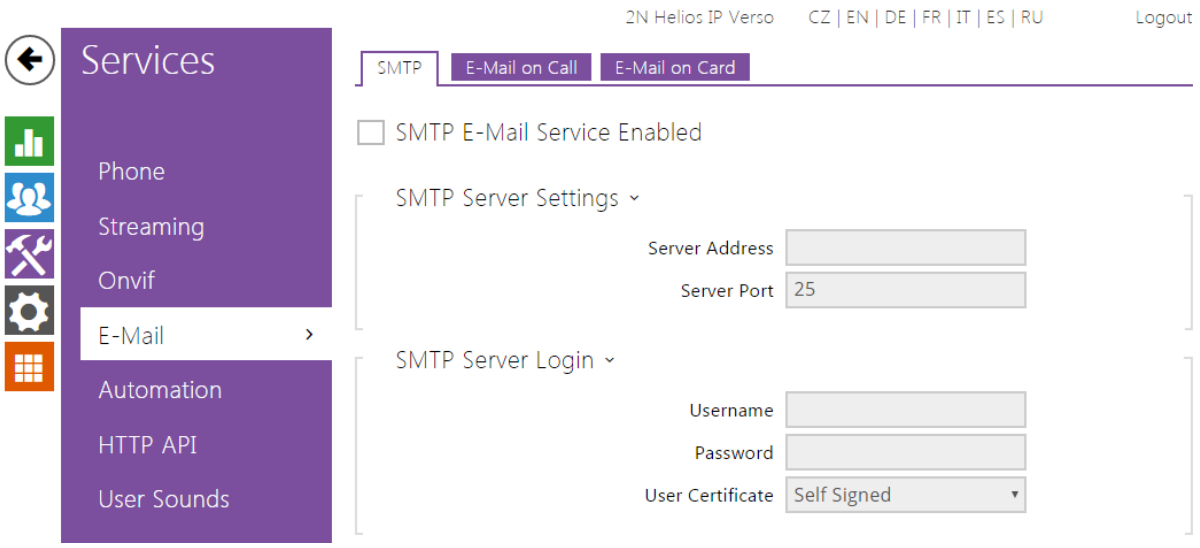
- *Check the following RTSP and JPEG functions for enable to make the ONVIF function work properly (to gain full compatibility with the third party equipment):*
  1. a. ***RTSP Server enabled*** *on the RTSP tab*
     b. ***Video stream enabled*** *on the RTSP tab*
     c. ***UDP unicast enabled*** *on the RTSP tab*
     d. ***Snapshot download enabled*** *on the JPEG tab*

Note

Preset authorisation for ONVIF

- Username: **admin**
- Password: **2n**

5.4.4 E-Mail



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.

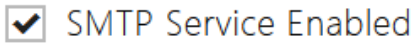
You can also send e-mails via Automation using the **Action.SendEmail** action.

Note

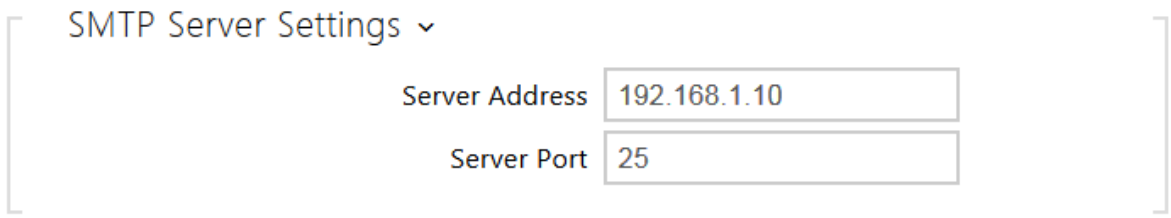
- *The E-mail function is available with the Gold or Enhanced Integration licence only.*

List of Parameters

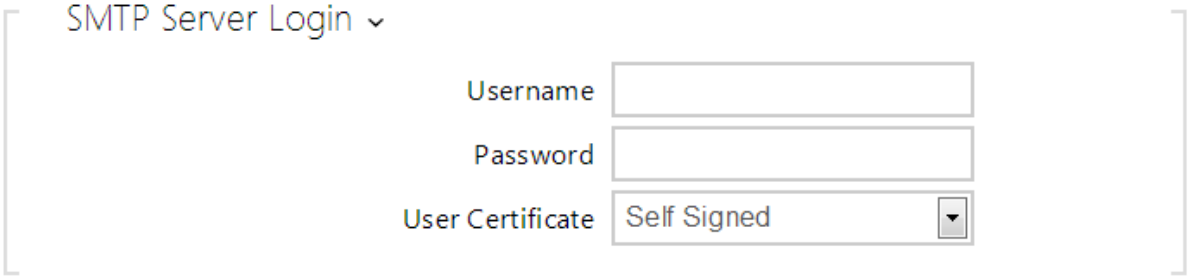
SMTP



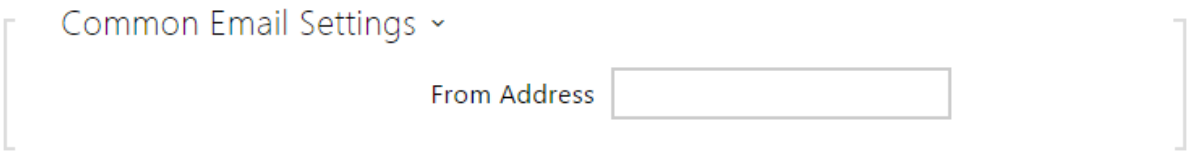
- **SMTP service enabled** – enable/disable sending e-mails from the intercom.



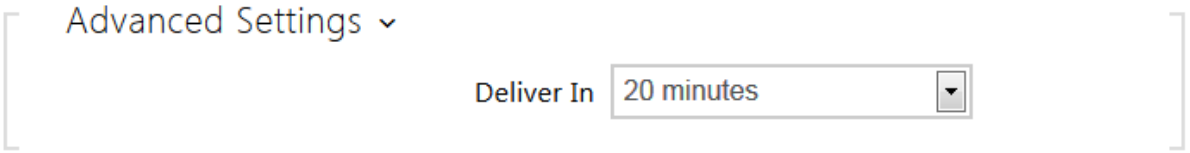
- **Server address** – set the SMTP server address to which e-mails shall be sent.
- **Server port** – specify the SMTP server port. Modify the value only if the SMTP server setting is substandard. The typical SMTP port value is 25.



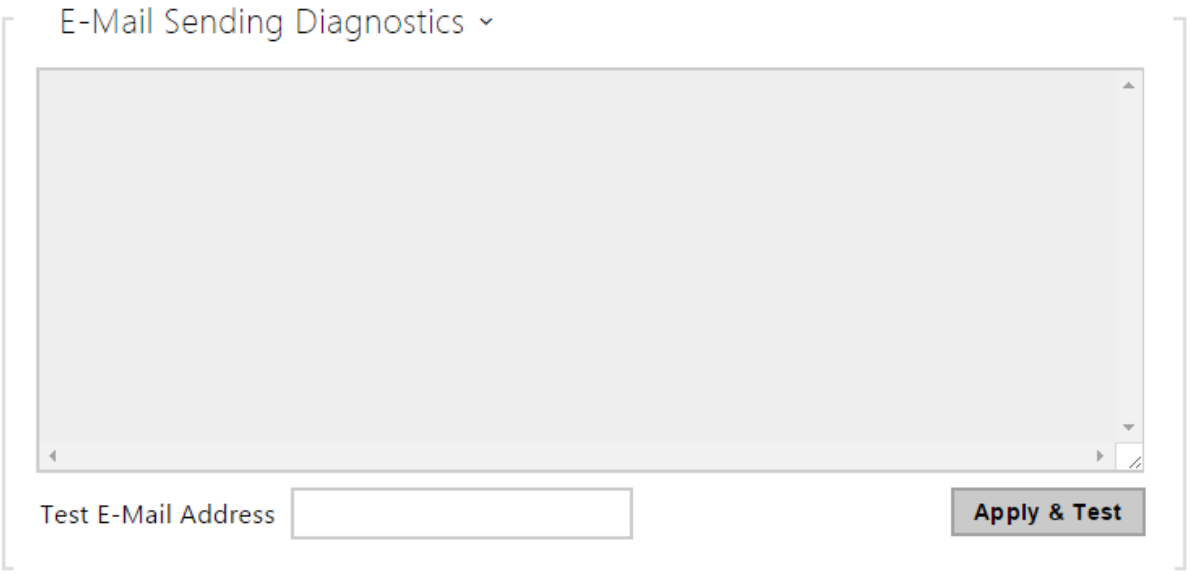
- **Username** – enter a valid username for login if the SMTP server requires authentication, or leave the field empty if not.
- **Password** – enter the SMTP server login password.
- **User certificate** – specify the user certificate and private key for the intercom – SMTP server communication encryption. 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.



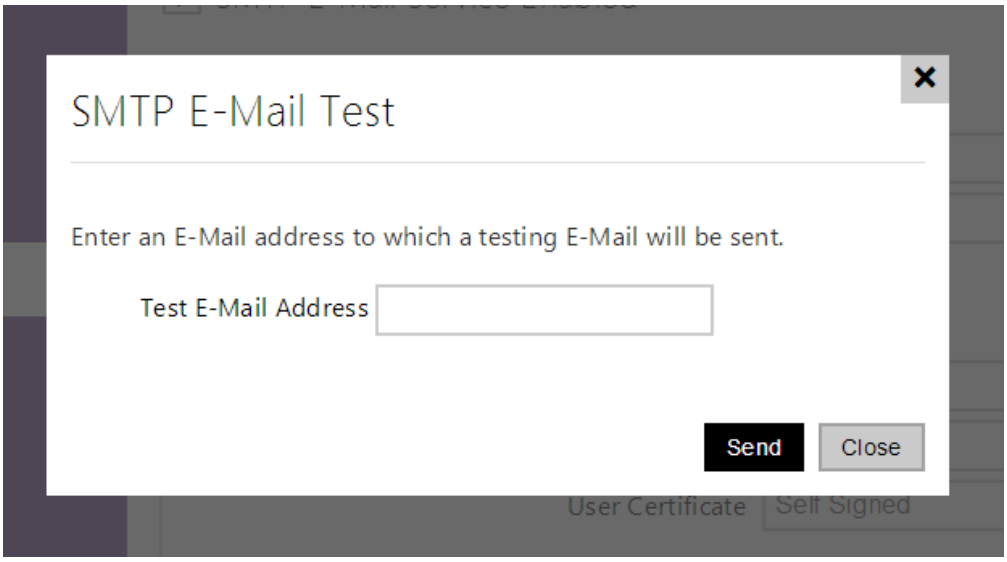
- **From address** – set the sender address for all outgoing e-mails from the device.



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

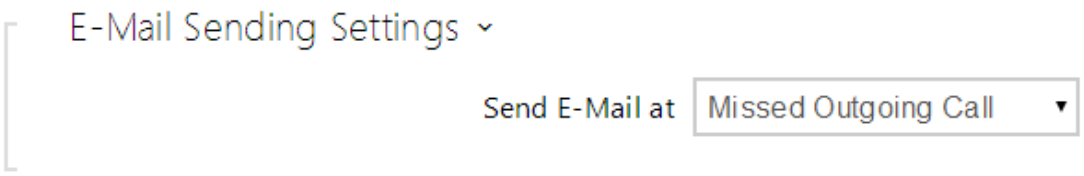


Click **Apply & Test** to send a testing e-mail to the defined address with the aim to test the functionality of the current e-mail sending setting. Enter the destination e-mail address into the Test e-mail address field and press the button. The current e-mail sending state is continuously displayed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



E-Mail on Call

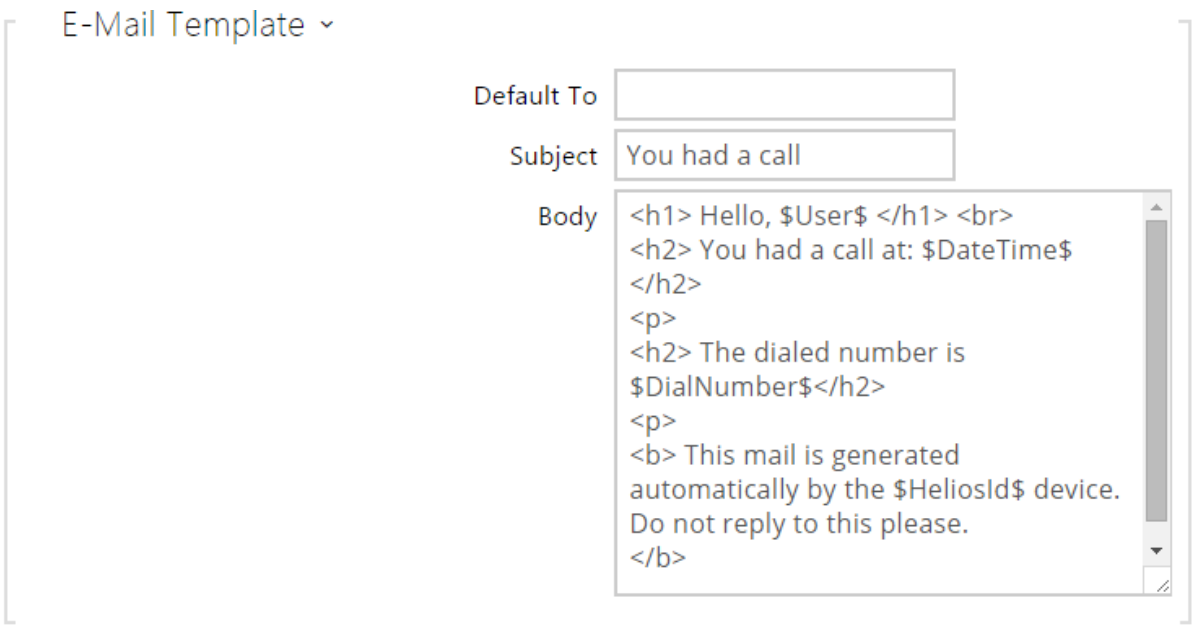
Set e-mail sending during outging calls on this tab.



- **Send e-mail at** – set e-mail sending upon outgoing phone calls. The e-mail is sent when the connection is terminated. The following options are available:
  - Any outgoing call – an e-mail will be sent upon every outgoing call.
  - Missed outgoing call – an e-mail will be sent upon every missed outgoing call.
  - Never – no e-mail messages will be sent upon outgoing calls.

Note

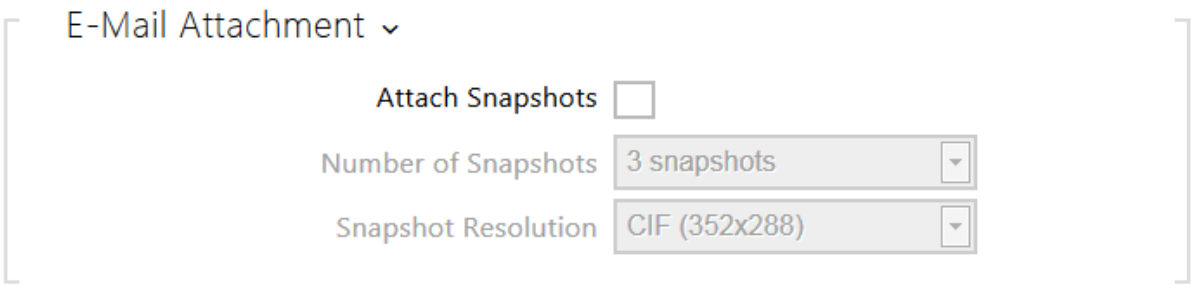
- An e-mail can always be sent via Automation.



- **Default to** – typically, the intercom sends email messages to the user addresses included in the user list. If the user's e-mail parameter is not completed, the messages are sent to the address included in this parameter. If a recipient is not included in the users list or this field, no e-mail is 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 called number, which will be replaced with the actual value before sending. Refer to the table of substitute symbols below:

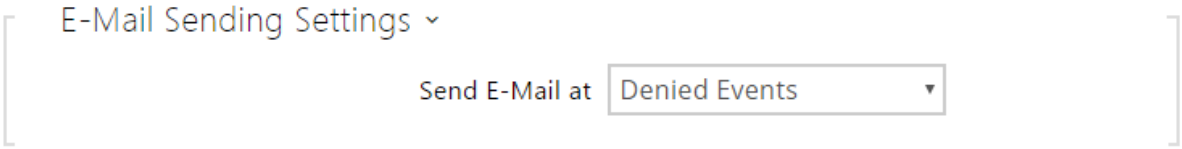
1. a. $User$ Called username
   b. $DateTime$ Current date and time
   c. $DialNumber$Called number
   d. $HeliosId$ Intercom identification



- **Attach snapshots** – enable sending of an attachment including one or more camera snapshots taken during ringing or calling.
- **Number of snapshots** – set the count of snapshots to be attached to the e-mail message.
- **Snapshot resolution** – set the snapshot resolution for the images to be sent.

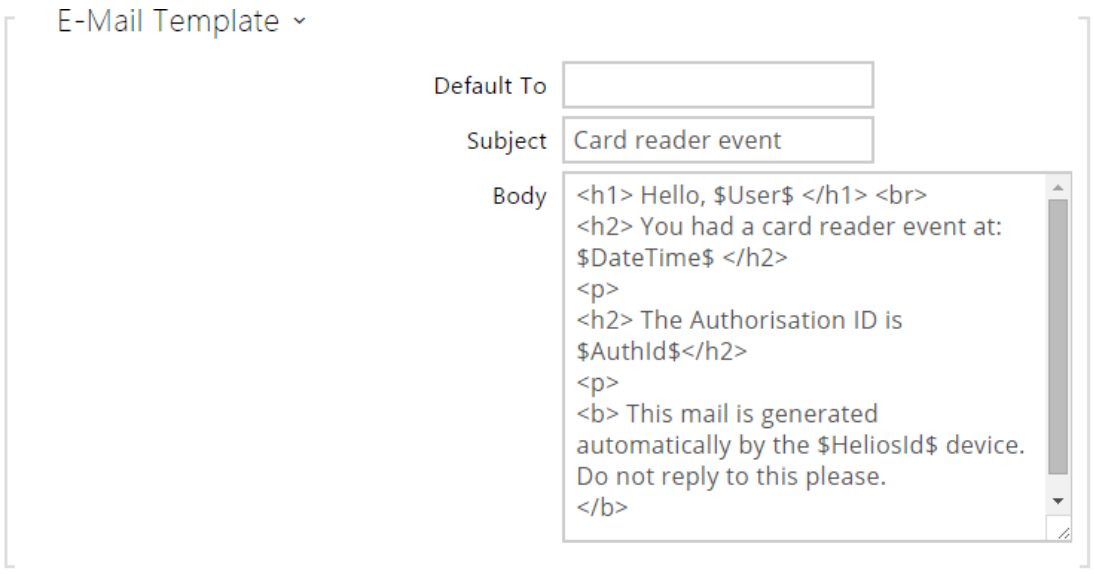
E-Mail on Card

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



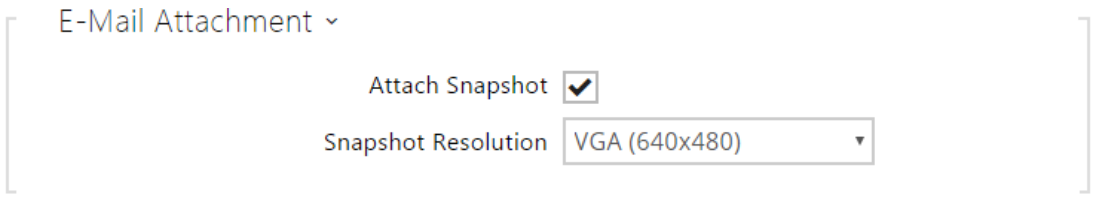
Send E-Mail at – set e-mail sending whenever a RFID card is tapped on the card reader. The following options are available:

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



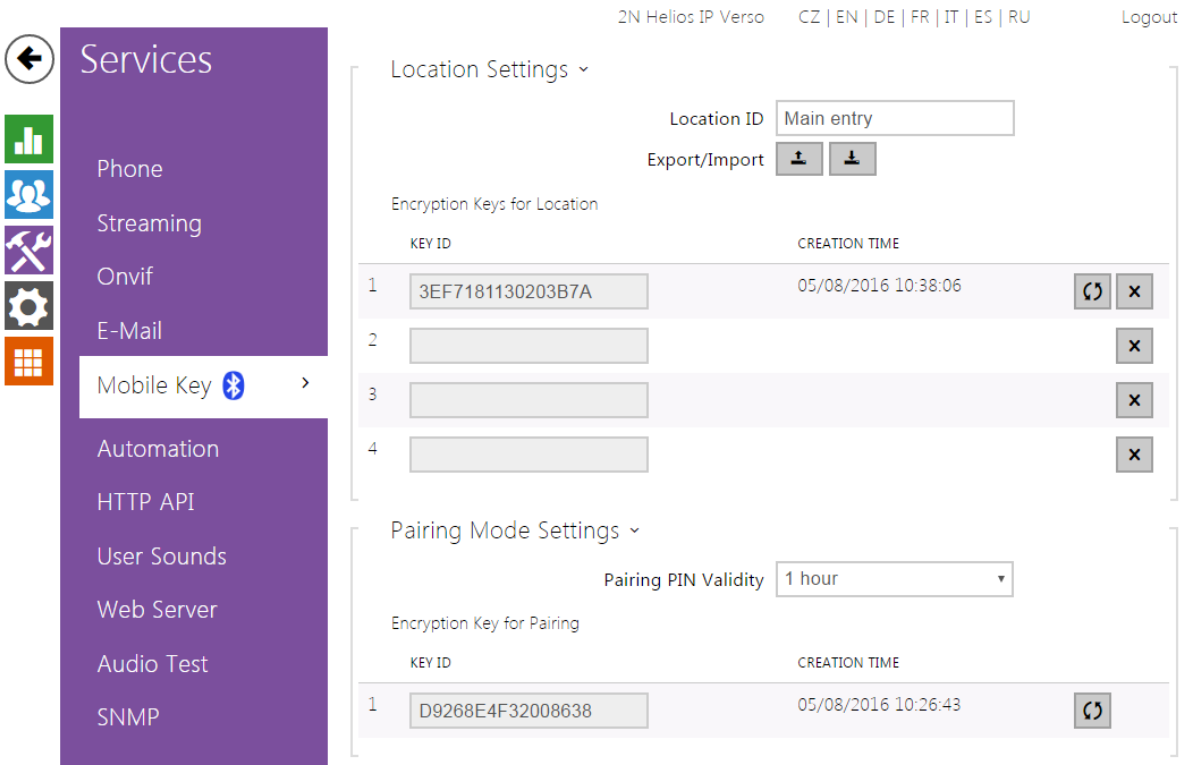
- **Default to** – the intercom sends messages to the e-mail address specified for the user when a valid user card is applied. When an invalid card is applied or no e-mail address is assigned to the user, the message shall be sent the e-mail address included here. If the receiver is included neither 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



- **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.

5.4.5 Mobile Key



The **2N Helios IP** intercoms 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 4s 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 intercom side: **Auth ID** (128-bit number) is generated randomly for every user and **paired** with the intercom 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 intercom phone book. You can move Auth ID to another user or copy it to another intercom. By deleting the Auth ID value you can block the user's access.

Encryption Keys and Locations

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

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

Pairing

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

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

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

- Location identifier
- Location encryption key
- User Auth ID

Encryption Key for Pairing

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

Encryption Key Administration

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

Poznámka

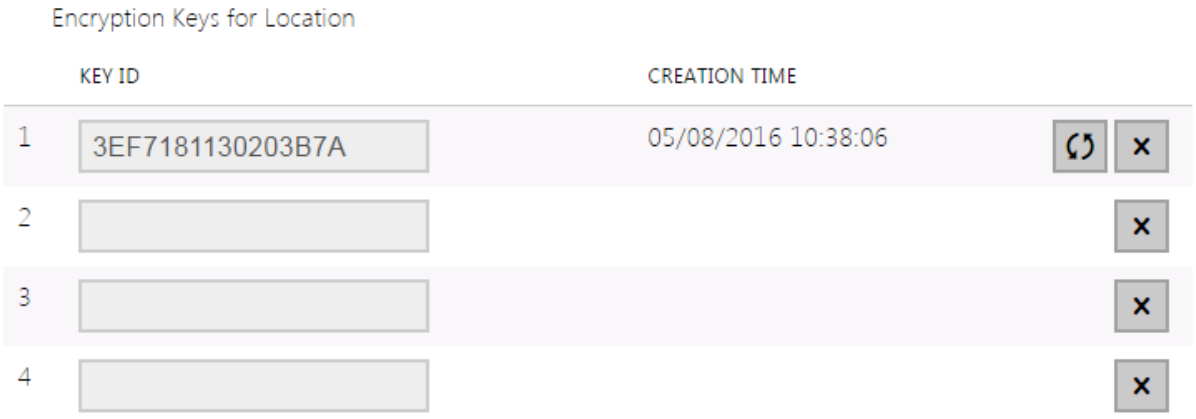
- The encryption keys are generated automatically upon the intercom first launch and saved into the intercom configuration file. We recommend you to re-generate the encryption keys manually before the first use to enhance security.

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

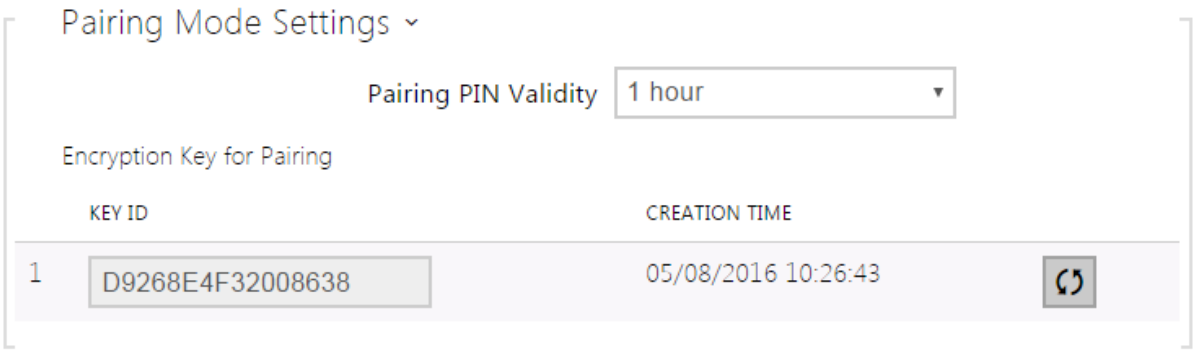
When a key is deleted, the 2N® Mobile Key users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the 2N® Mobile Key application.

List of Parameters

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



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



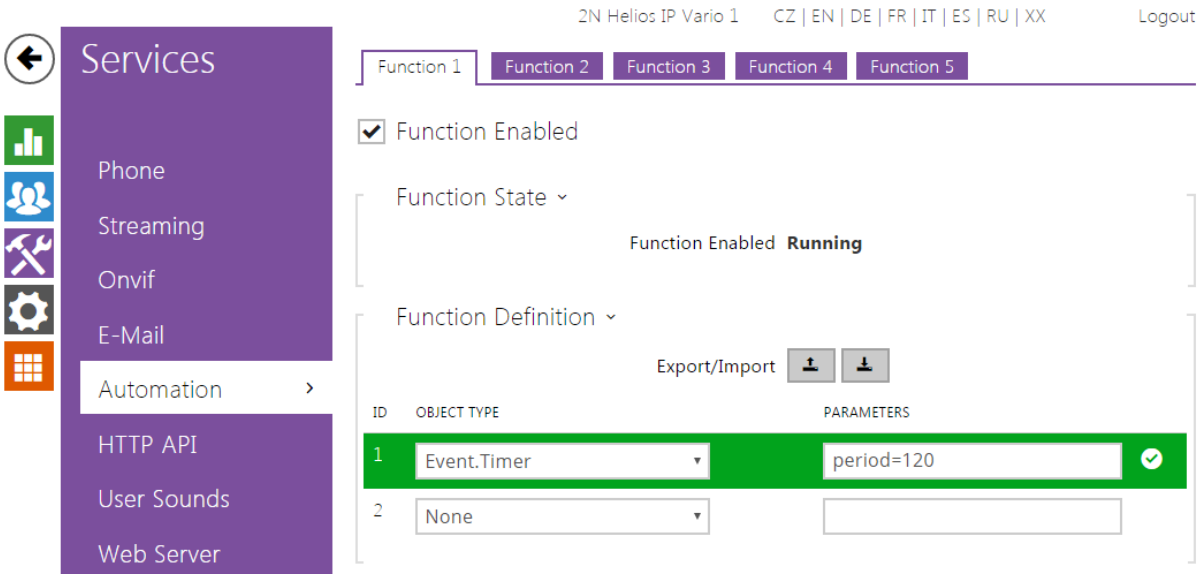
- **Pairing PIN validity** – set the authorisation PIN validity for user mobile device pairing with the intercom.

Tip

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

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

5.4.6 Automation



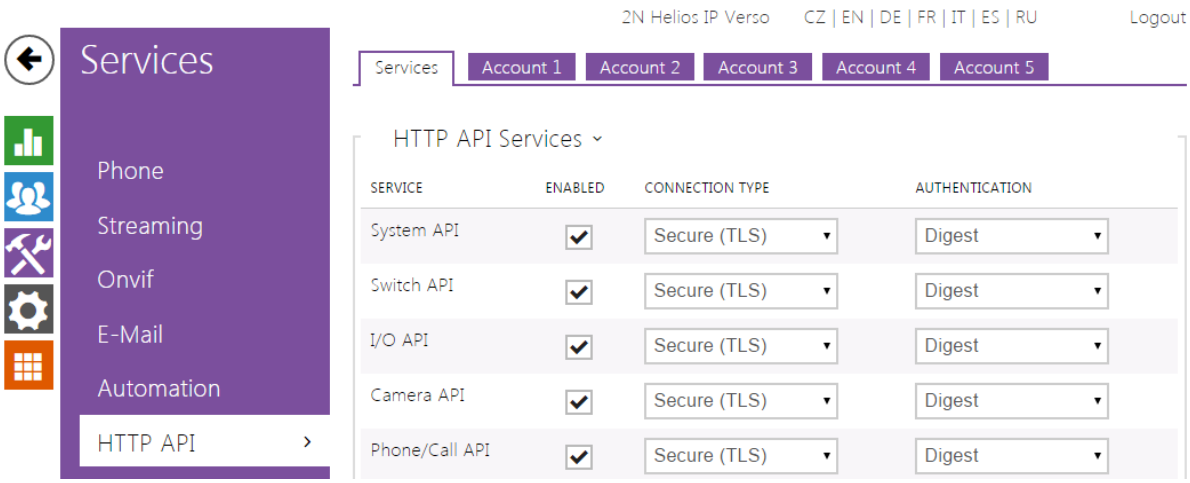
The 2N Helios IP intercom provides highly flexible setting options to satisfy variable user needs. There are situations in which the standard configuration settings (switch or call modes, e.g.) are insufficient and so 2N Helios IP offers Automation, a special programmable interface for applications that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

Refer to the Automation Configuration Manual for the Automation function and configuration details.

Note

- *The Automation function is available with the Gold or Enhanced Integration licence only.*

5.4.7 HTTP API



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.

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 audio playback control and microphone monitoring.
- Camera API – provides camera image control and monitoring.
- Display API – provides display control and user information display.
- E-mail API – provides sending of user e-mails.
- Phone/Call API – provides incoming/outgoing call control and monitoring.
- Logging API – provides reading of event records.

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 HTTP API Configuration Manual for the HTTP API function and configuration details.

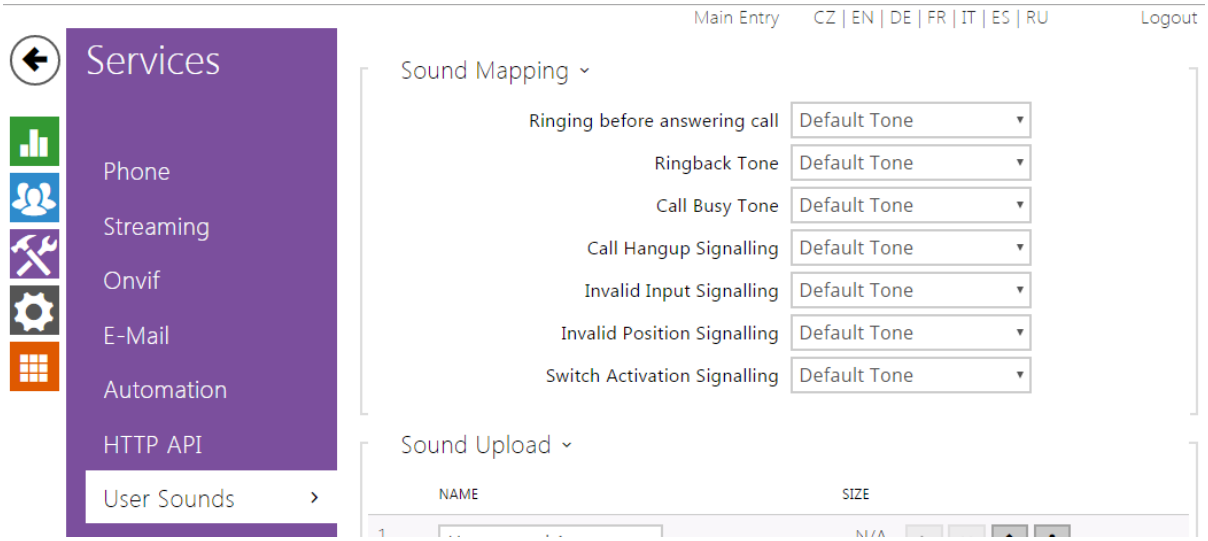
Note

- *Full HTTP API function is available with the Gold or Enhanced Integration licence only. Only Camera API is available without this licence.*

Tip

- For the Video Preview feature at Gigaset Maxwell 10 phone it's needed to set in HTTP API at the Camera API item Connection Type = Unsecure and Authetntication = None.

5.4.8 User Sounds



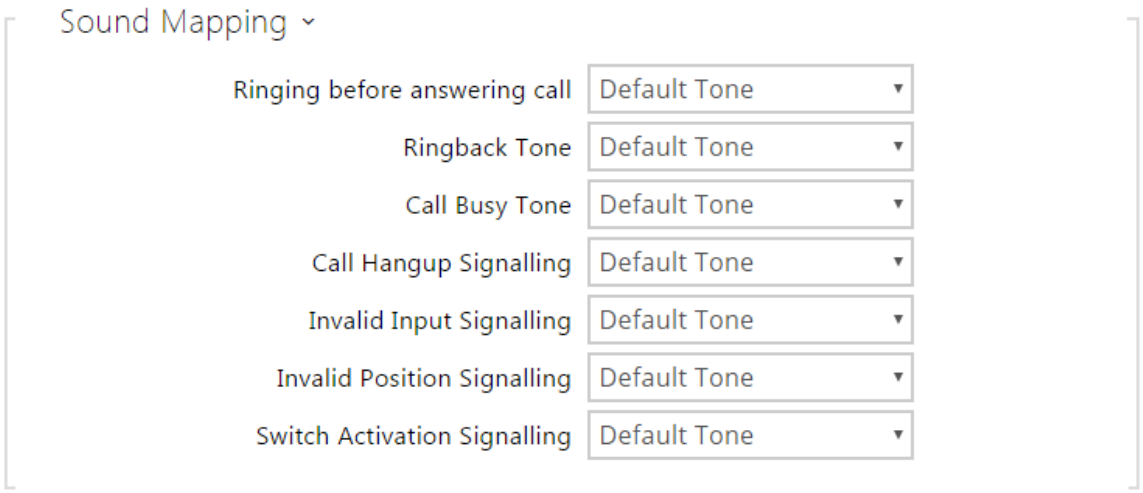
The 2N Helios IP intercoms provide standard signalling of operational statuses by tone sequences; refer to the Signalling of Operational Statuses subsection. If you find the standard sound signalling inconvenient, modify the sounds for the following statuses:

1. a. Ringing before answering call
   b. Ringback tone
   c. Call busy tone
   d. Call hang-up
   e. Invalid input
   f. Invalid user position
   g. Switch activation

You can either completely mute the above-mentioned sounds , replace them with one of the ten predefined sounds, or simply record a s ound file of your own into the intercom. The sound file must have the WAV format and use PCM encoding with 8 kHz sampling frequency and 8/16-bit sample resolution, and the file size may not exceed 256 kB. The maximum file playing time is limited to approximately 16 seconds for 8-bit and 8 seconds for 16-bit resolution.

You can also play the recorded files via Automation using the Action.PlayUserSound and, optionally, with the aid of the intercom speaker and/or directly into the phone call.

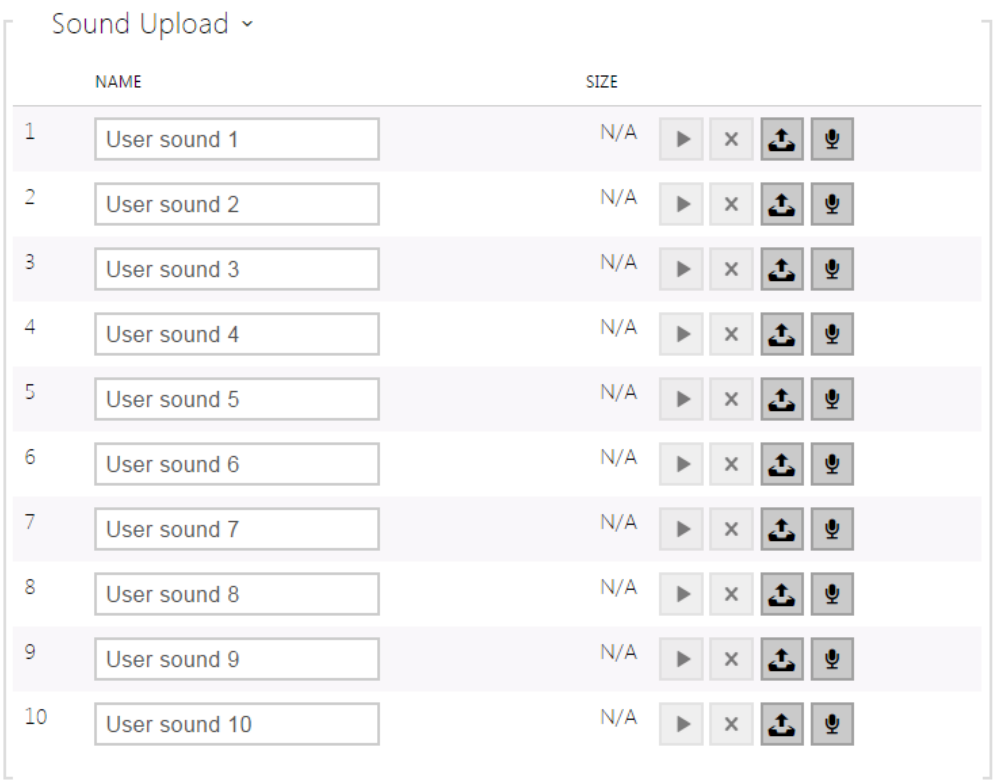
List of Parameters



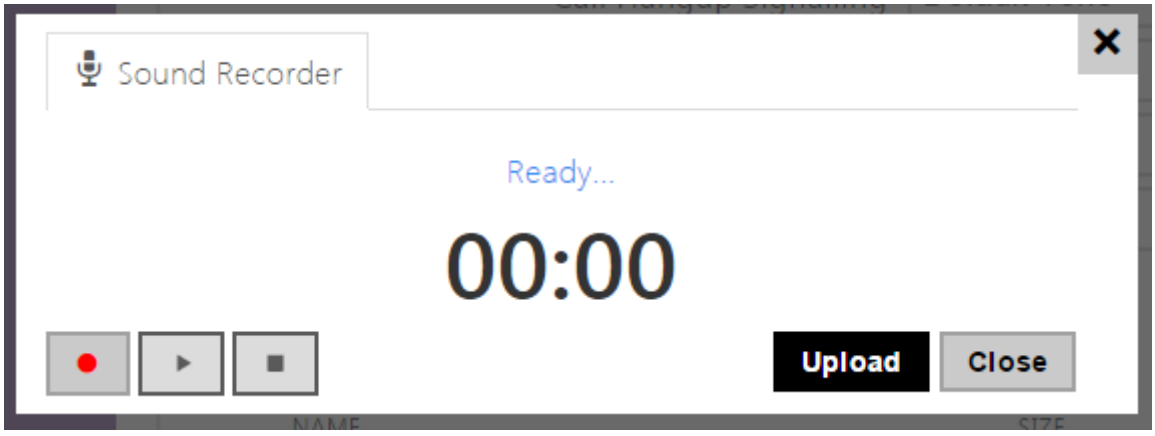
- **Ringing before answering call** – set the sound to be played before answering an incoming call (intercom ring tone).
- **Ringback tone** – set the sound to be played to the called user. The PBX ringing tone is preferred to the intercom ringing tone set here.
- **Call busy tone** – set the sound to be played when the called user is busy.
- **Call hang-up signalling** – set the sound to be played upon the call end.
- **Invalid input signalling** – set the sound to be played when an invalid code in entered (switch/user/profile activation).
- **Invalid position signalling** – set the sound to be played when a quick dial button is pressed but the corresponding user position is not programmed.
- **Switch activation signalling** – set the sound to be generated when a switch is activated. Specify signalling details for each switch; refer to the Switches subsection.

You can record up to 10 user sound files into the intercom and assign names to them for convenience.

Press ▶ to record a sound file to the intercom. Select a file from your PC via a dialogue window and push **Record**. Press × to remove a file. Press ⬆ to replay the sound file (locally on your PC).



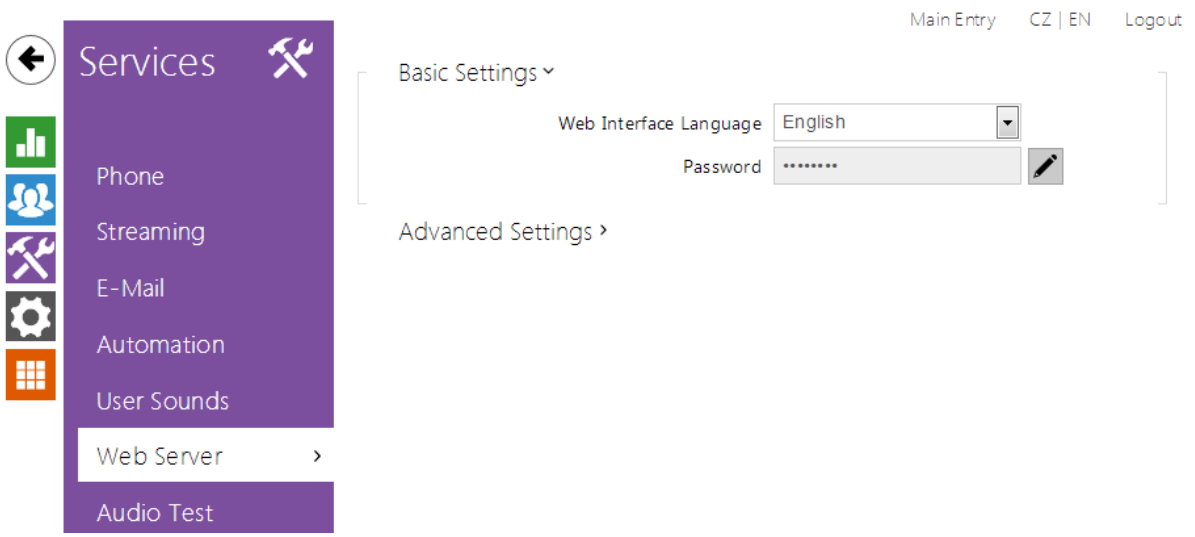
You can record a sound file using your PC microphone. Press ● to start the record and press ■ to stop the record. Press ▶ to play the sound record. Click **Upload** to save the sound into the intercom.



Note

- The sound recording function is not available in the browsers that do not support the WebRTC standard (Internet Explorer, e.g.).

5.4.9 Web Server



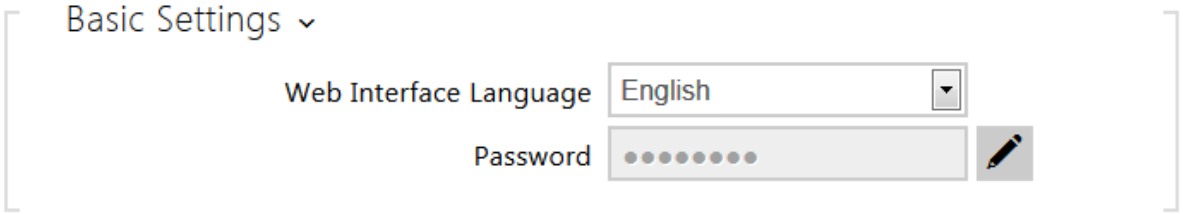
You can configure your **2N Helios IP** intercom using a standard browser which accesses the integrated web server. Use the secured HTTPS protocol for communication between the browser and intercom. Having accessed the intercom, enter the login name and password. The default login name and password are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

The **Web Server** function is used by the following intercom functions too:

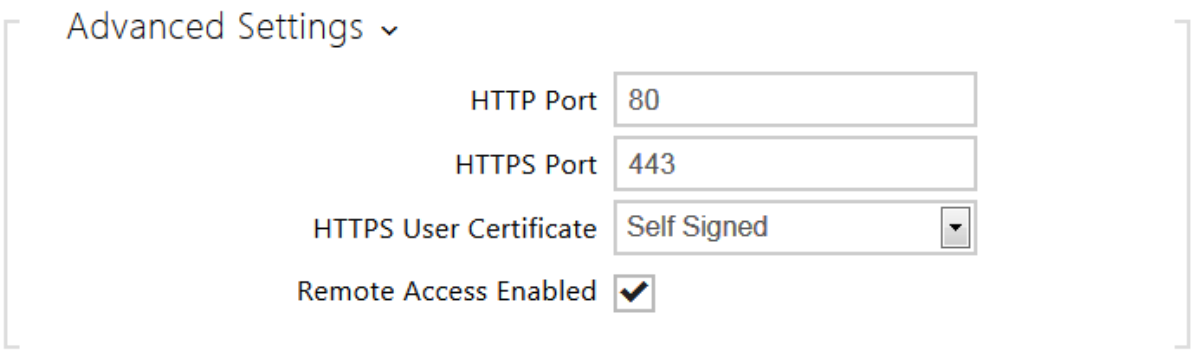
1. a. JPEG snapshot/MJPEG video download; refer to Streaming.
   b. ONVIF protocol for video streaming, refer to Streaming.
   c. HTTP commands for switch control, refer to Switches.
   d. Event.HttpTrigger in 2N Helios IP Automation, refer to the respective manual.

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 Network Scanner, etc).
- **Web interface language** – set the default language for administration web server login. Use the upper toolbar buttons to change the language temporarily.
- **Password** – set the intercom access password. Press to change the password. The 8-character password must include one lower-case letter, one upper-case letter and one digit at least.



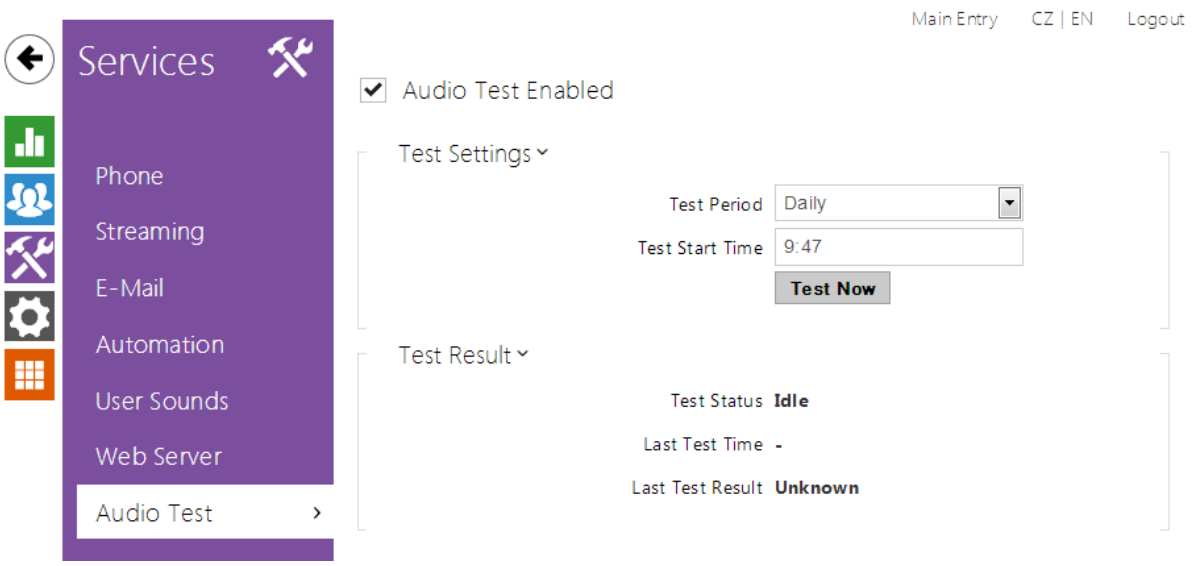
- **HTTP port** – set the web server port for HTTP communication. The port setting will not be applied until the intercom gets restarted.
- **HTTPS port** – set the web server port for HTTPS communication. The port setting will not be applied until the intercom gets restarted.
- **HTTPS user certificate**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

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

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

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

5.4.10 Audio Test

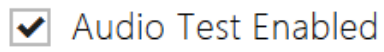


The 2N Helios IP intercoms allow you to perform periodical tests of the integrated speaker and microphone. For the test purpose, the integrated speaker generates one or more short beeps. The integrated microphone receives the generated tone and the test is successful if the tone is detected correctly.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

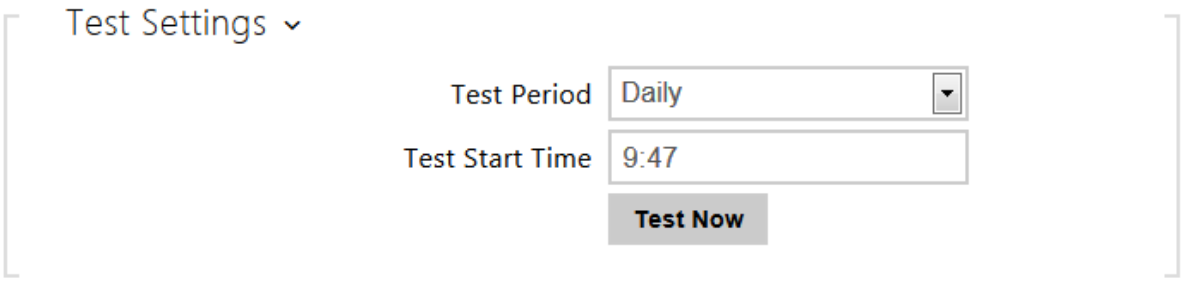
Note

- *The audio test is available with the Gold or Enhanced Audio licence only.*
- *If a call is active when the audio test starts, the audio test will be put off until the call is terminated. The audio test will be performed the moment the call is terminated.*

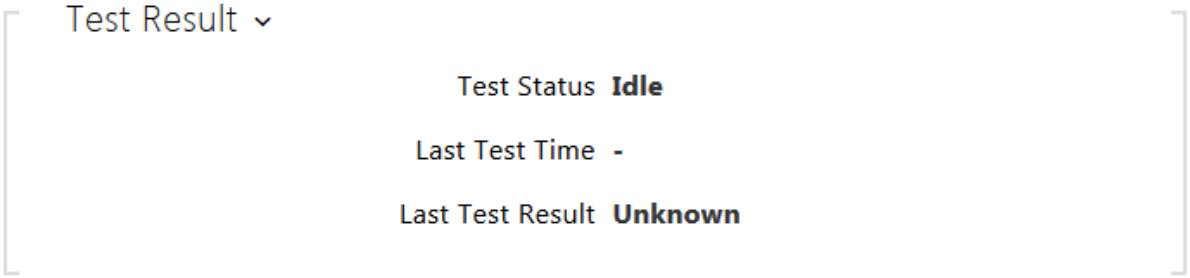
List of Parameters



- **Audio test enabled** – enable automatic execution of the audio test.

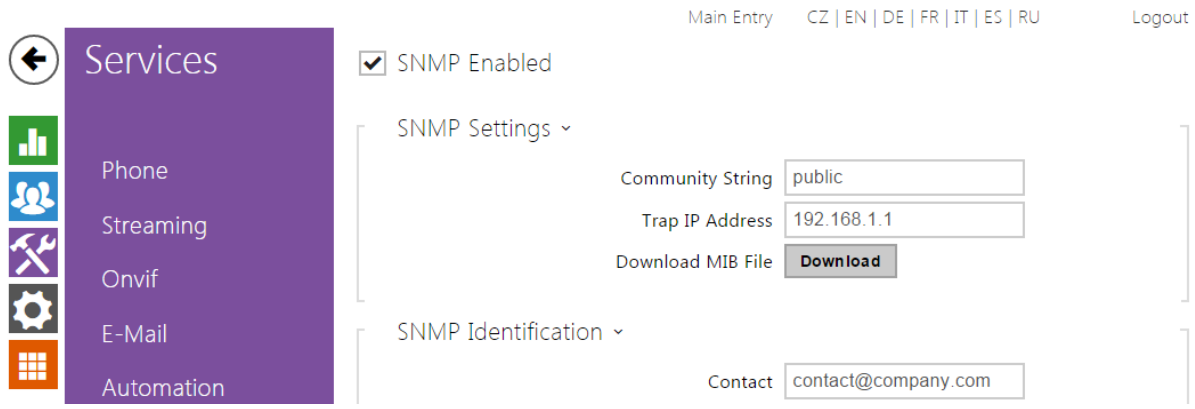


- **Test period** – set the test period: daily or weekly.
- **Test start time** – set the test starting time in the HH:MM format. We recommend you to set a time at which a low intercom traffic is expected.
- **Test now** – push the button to start the test immediately regardless of the current settings.



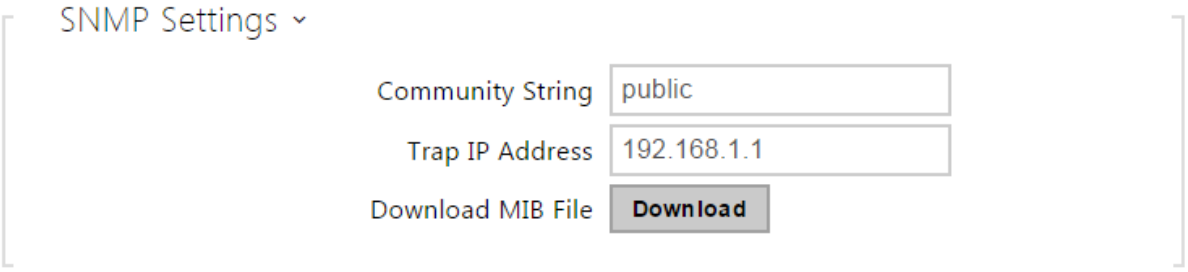
- **Test status** – this parameter displays the current test status.
- **Last test time** – this parameter displays the time of the last-performed test.
- **Last test result** – this parameter displays the result of the last-performed test.

5.4.11 SNMP



The **2N Helios IP** intercoms integrate a remote intercom supervision functionality via the SNMP. The integrated SNMP agent becomes available when the **Enhanced Integration** licence key is added. The intercoms support the SNMP version 2c.

List of Parameters

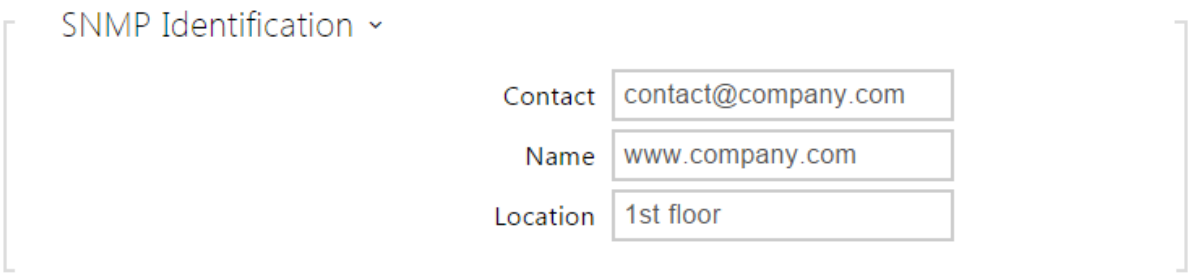


- **Community string** – text string representing the access key to the MIB table objects.
- **Trap IP address** – IP address to which the SNMP traps are to be sent.

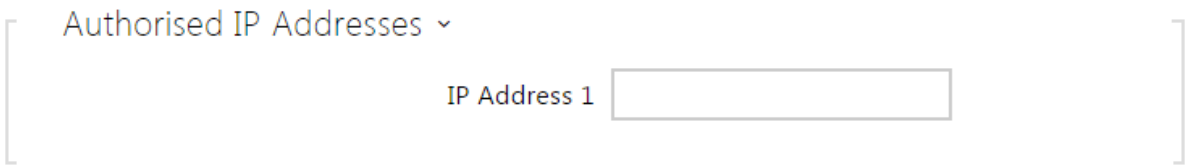
Note

- Traps are not supported at the present version. **2N Helios IP** operates with request - response messages.

- **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.).



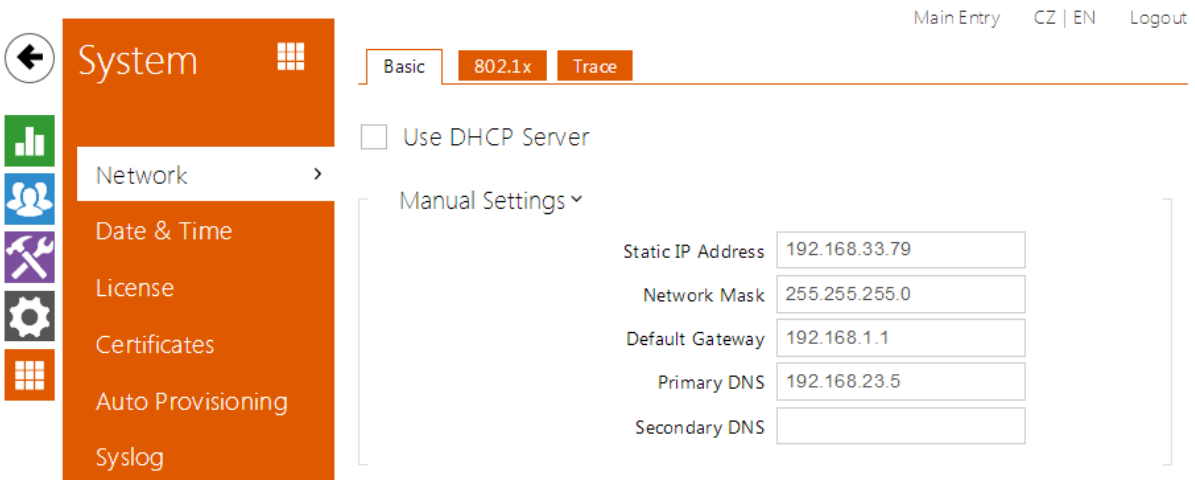
- **IP address**– enter up to 4 valid IP addresses for SNMP agent access to block access from other addresses. If the field is empty, the device may be accessed from any IP address.

5.5 System

Here is what you can find in this section:

- 5.5.1 Network
- 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



As the **2N Helios IP** intercom 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 intercom, 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 intercom: the intercom 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 in the **802.1x** tab.

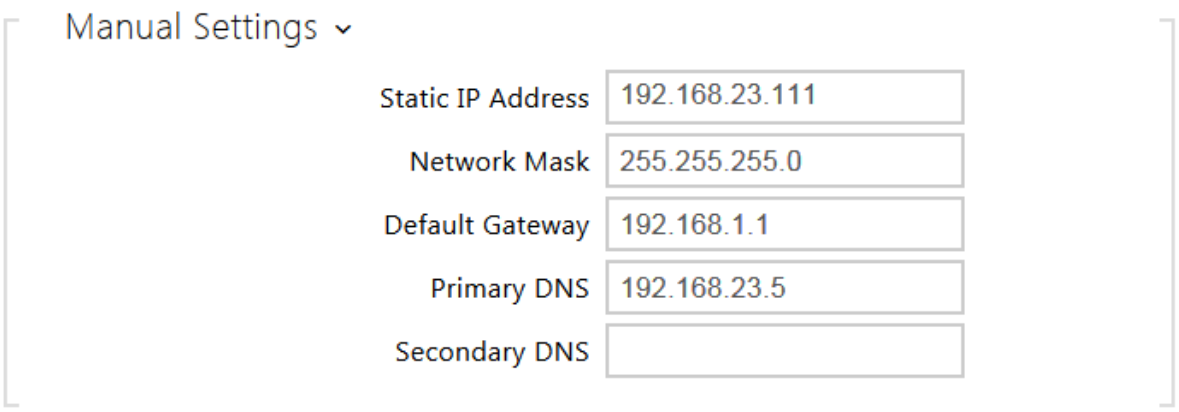
The **Trace** tab helps you launch capture of incoming and outgoing packets on the intercom network interface. The file with captured packets can be downloaded for Wireshark processing, e.g. (**www.wireshark.org**).

List of Parameters

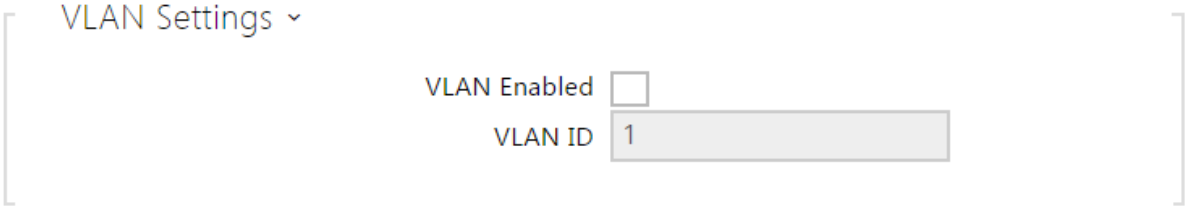
Network

Use DHCP Server

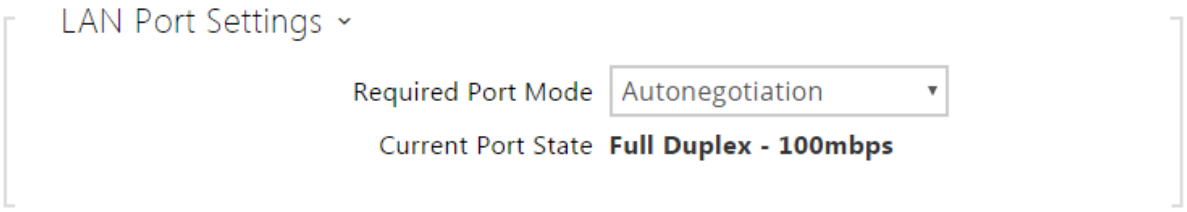
- **Use DHCP server** – enable automatic obtaining of the IP address from the LAN DHCP server. If the DHCP server is unavailable or inaccessible in your LAN, use the manual network settings.



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

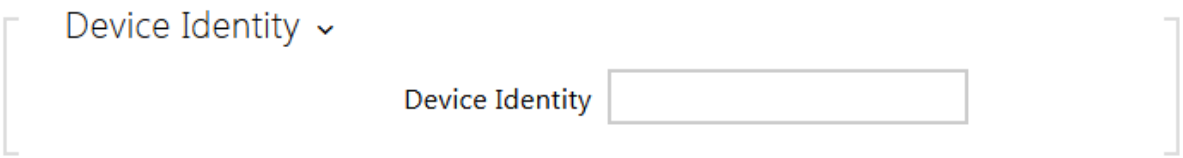


- **VLAN enabled** – enable the virtual network (VLAN) support (according to recommendation 802.1q). Set the virtual network ID too to make the function work properly.
- VLAN ID – select a virtual network ID in the range of 1-4094. The device shall receive only the packets tagged with this ID. A wrong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

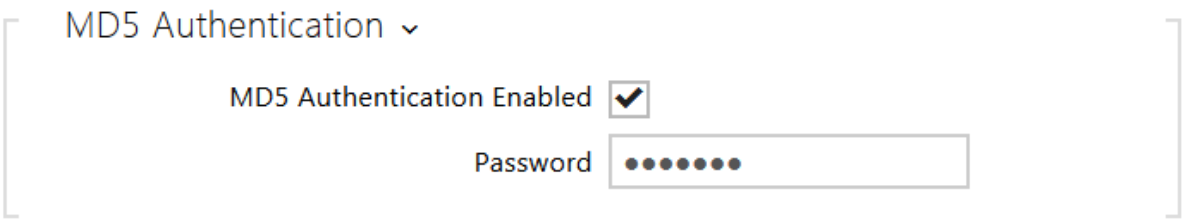


- **Required port mode** – set the preferred network interface port mode: Autonegotiation or Half Duplex - 10 mbps. The lower bit rate of 10 mbps may be necessary if the used network infrastructure (cabling) is not reliable for the 100mbps traffic.
- **Current port state** – current network interface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

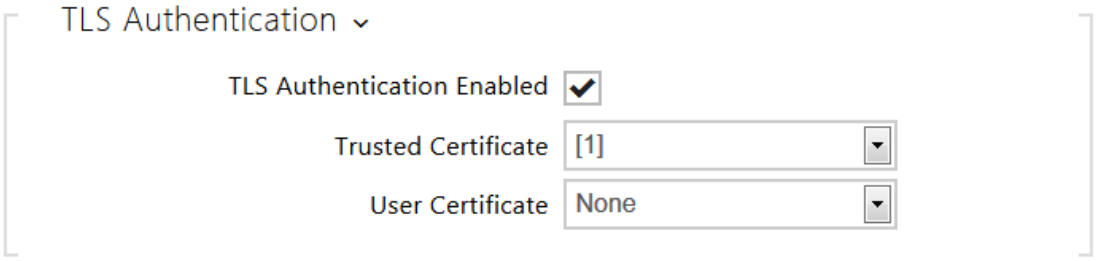
802.1x



- **Device identity** – username (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 intercom will become inaccessible.
- **Password** – enter the access password for EAP-MD5 authentication.



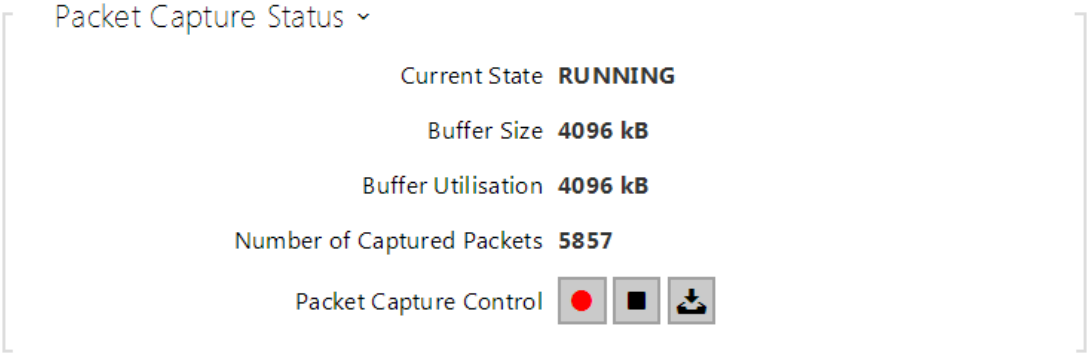
- **TLS authentication enabled** – enable authentication of network devices via the 802.1x EAP-TLS protocol. Do not enable this function if your LAN does not support 802.1x. If you do so, the intercom will become inaccessible.
- **Trusted certificate** – specify the set of trusted certificates for verification 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 intercom 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.

Note

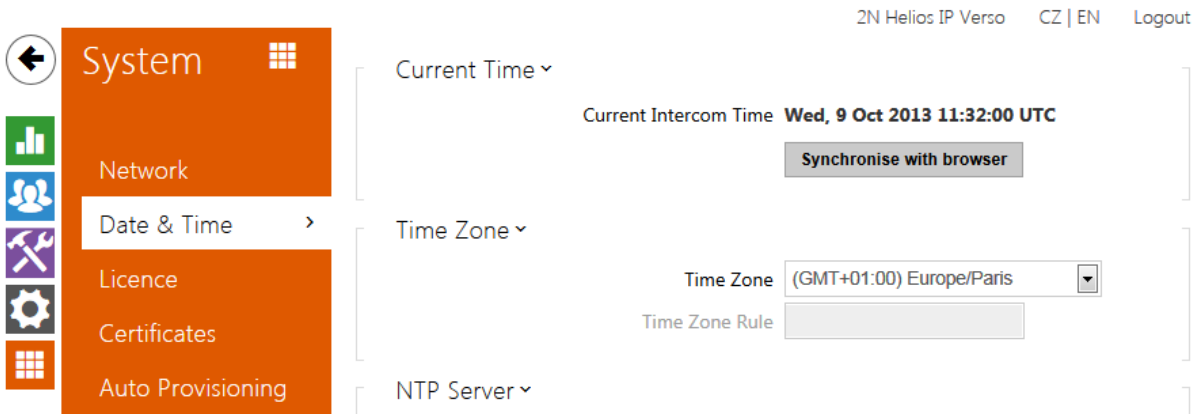
- *This function is available with the Gold or Enhanced Security licence only.*

Trace

In the **Trace** tab, you can launch capturing of incoming and outgoing packets on the intercom 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 phone numbers, lock activation codes and similar by time profiles, make sure that the intercom internal date and time are set correctly.

Most 2N Helios IP models are equipped with a back-up real-time clock to withstand up to several days' long power outages. If not equipped with this function, the intercom loses the real time data upon power outage (or restart). Therefore, if the intercom is powered up after a rather long period of time (after new intercom installation, e.g.), time is set to the default value and has to be reset. You can synchronise the intercom time with your PC anytime by pressing the Synchronise button.

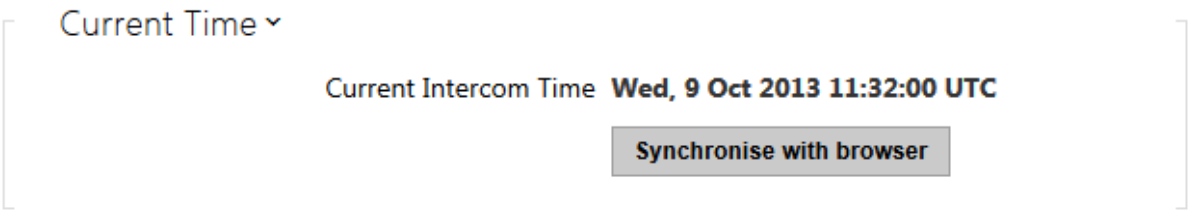
Synchronise the intercom internal time with any available SNTP server if your intercom is not equipped with a real-time clock.

Note

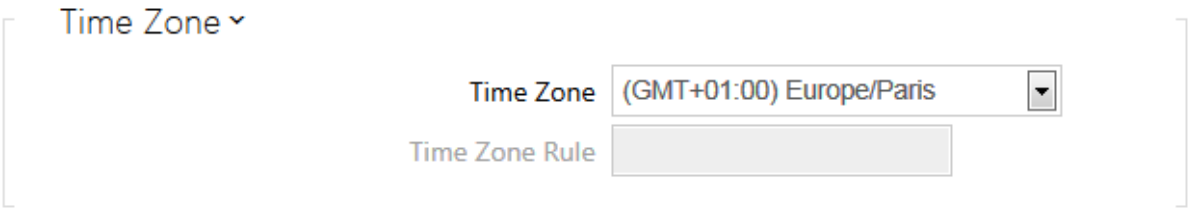
- *The intercom does not need the current date and time values for its basic function. However, be sure to set these values when you apply time profiles and display time of listed events (Syslog, used cards, logs downloaded by HTTP API, etc.).*

Practically, the intercom 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 intercom sends a query to the NTP server periodically to update its time value.

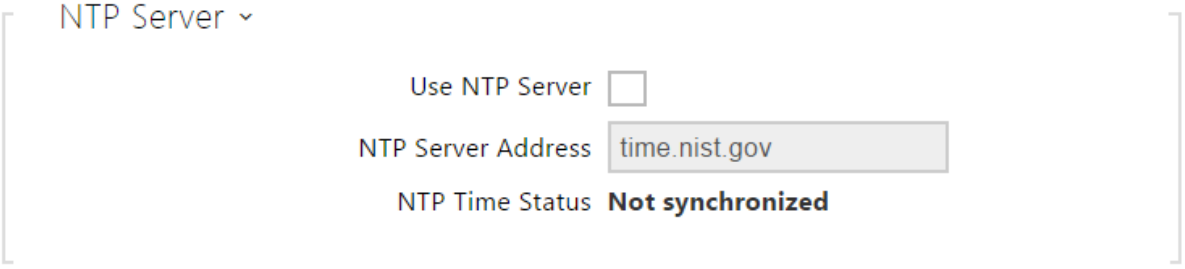
List of Parameters



Synchronise – push the button to synchronise the intercom time value with your PC time value.

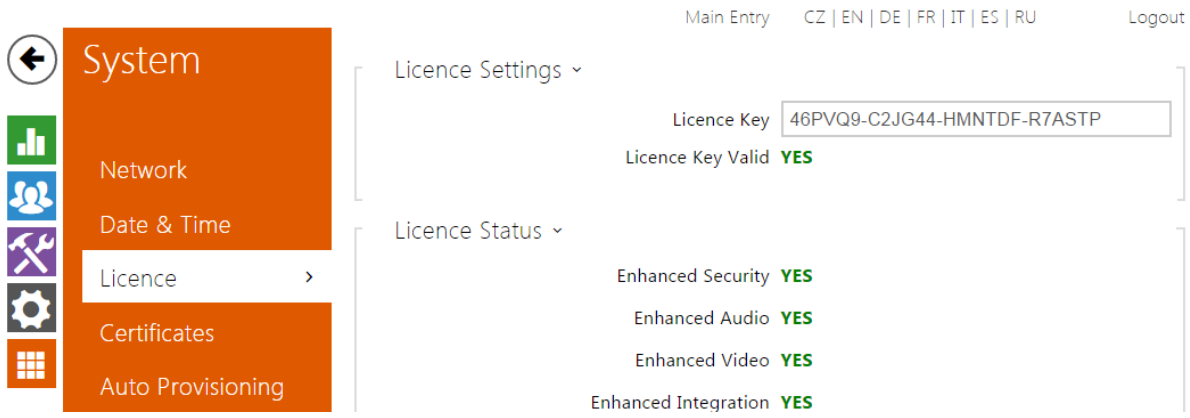


- **Time zone** – set the time zone for the installation site to define time shifts and winter/summer time transitions.
- **Time zone rule** – if the intercom is installed on a site that it not included in the **Time zone** parameter, set the time zone rule manually. The rule is applied only if the **Time zone** parameter is set to **Manual**.



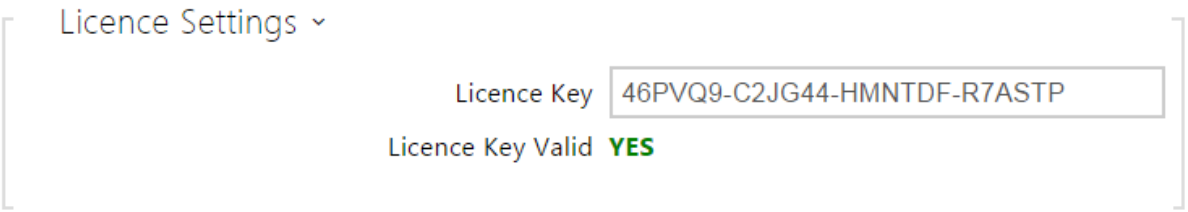
- **Use NTP server** – enable the NTP server use for intercom time synchronisation.
- **NTP server address** – set the IP address/domain name of the NTP server used for your intercom time synchronisation.
- **NTP time status** – display the state of the last local time synchronisation attempt via the NTP server (Not Synchronised, Synchronised, Error).

5.5.3 Licence

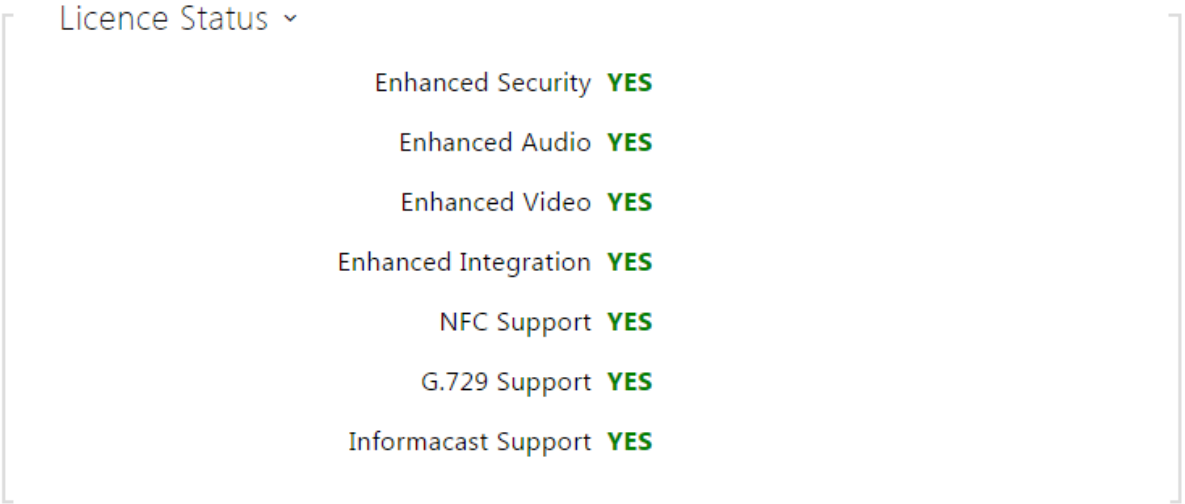


Some **2N Helios IP** functions are available with a valid licence key only. Refer to the **Model Differences and Function Licensing** subsection for the list of intercom licensing options.

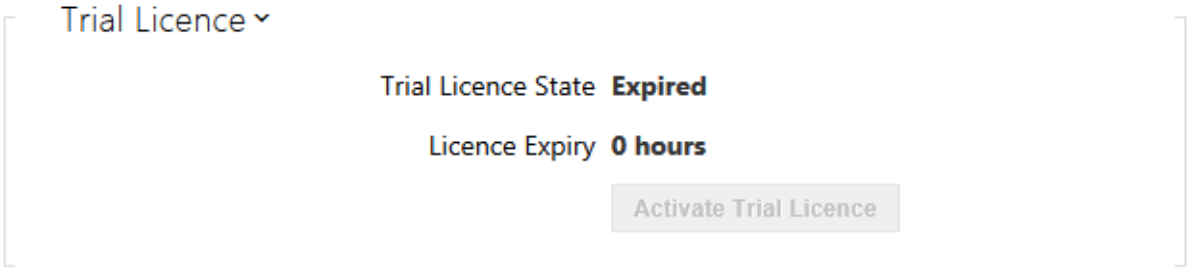
List of Parameters



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

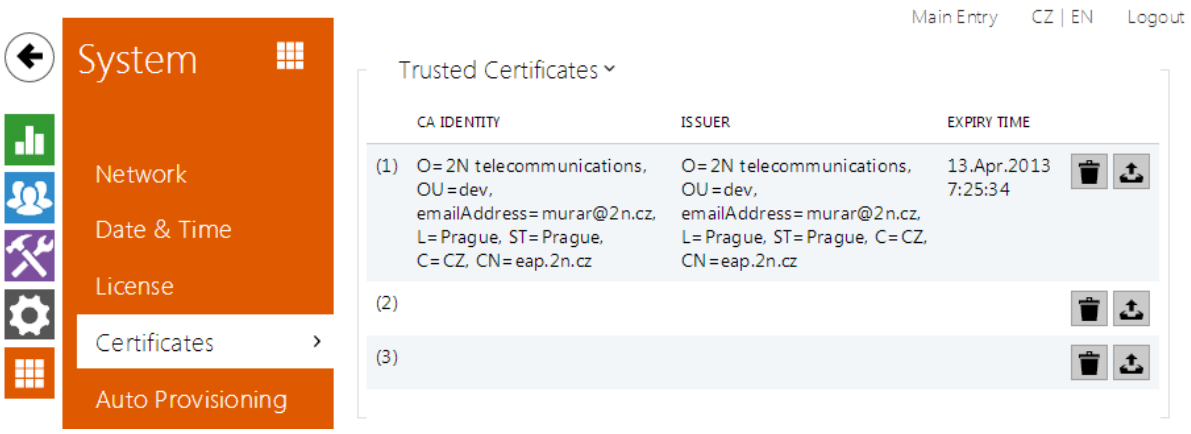


- **Enhanced security** – check whether the functions activated by the Enhanced Security licence are available.
- **Enhanced audio** – check whether the functions activated by the Enhanced Audio licence are available.
- **Enhanced video** – check whether the functions activated by the Enhanced Video licence are available.
- **Enhanced integration** – check whether the functions activated by the Enhanced Integration licence are available.
- **NFC support** – check whether the NFC user identification support is available.
- **G.729 support** – check whether the G.729 audio codec is available.
- **InformaCast support** – check whether the InformaCast support is available.



- **Trial licence state** – check the trial licence state (non-activated, activated, expired).
- **Licence expiry** – check the remaining time of the trial licence validity. 1 hour is deducted automatically from the licence remaining time upon every restart and factory reset; otherwise this time is not affected in any way.

5.5.4 Certificates



Some **2N Helios IP** 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 intercom services use the TLS protocol:

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

The **2N Helios IP** intercom allows you to load up to three sets of trusted certificates, which help authenticate LAN devices for communication with the intercom, and 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.

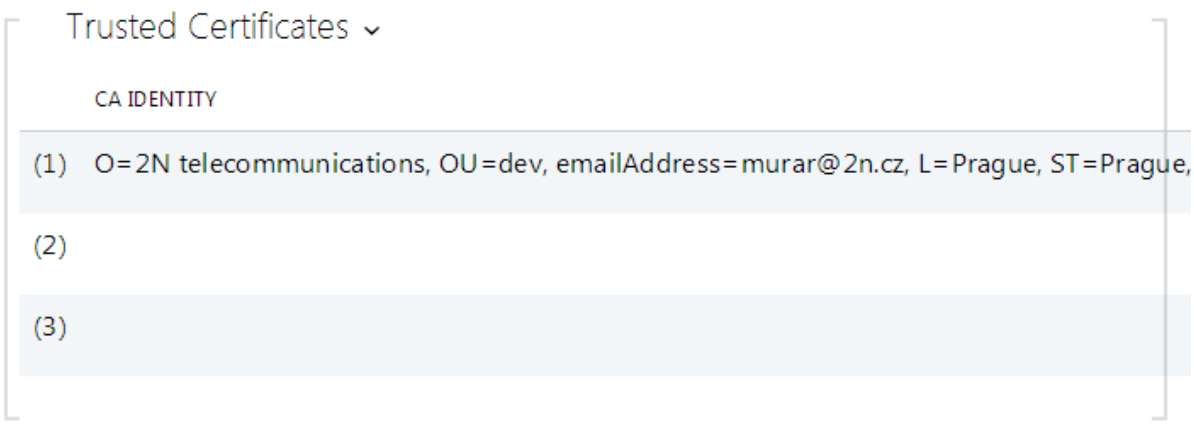
2N Helios IP accepts the DER (ASN1) and PEM certificate formats.

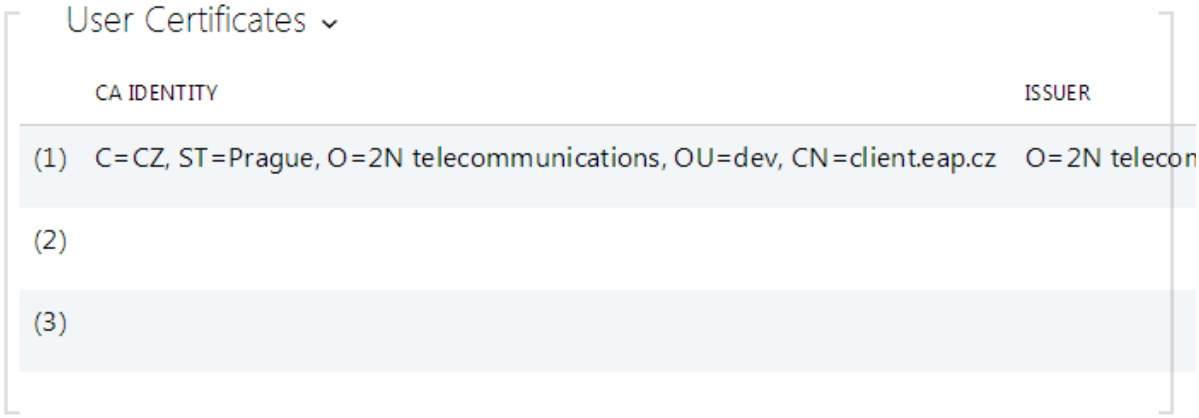
Upon the first power up, the intercom automatically generates the **Self Signed certificate and private key** for the **Web Server** and **E-Mail** without forcing you to load a certificate and private key of your own.

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 intercom certificate validity.*

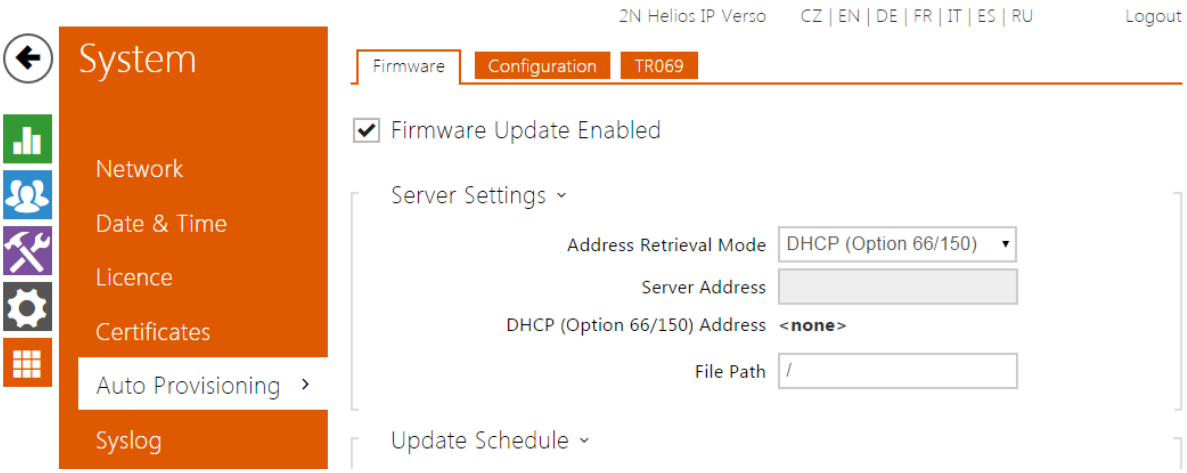
Refer to the tables below for the current list of trusted and user certificates:





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 Helios IP intercoms help you 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 Helios IP intercoms support automatic identification of the local DHCP server address (Option 66).

Firmware

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

2N Helios IP expects the following files:

1. hipMODEL-firmware.bin – intercom firmware
2. hipMODEL-common.xml – common configuration for all intercoms of one model
3. hipMODEL-MACADDR.xml – specific configuration for one intercom

MODEL in the filename specifies the intercom model:

1. v – 2N® Helios IP Vario
2. f – 2N® Helios IP Force
3. sf – 2N® Helios IP Safety

4. ak – 2N® Helios IP Audio Kit
5. vk – 2N® Helios IP Video Kit
6. ve – 2N® Helios IP Verso

MACADDR is the MAC address of the intercom in the 00-00-00-00-00-00 format. Find the MAC address on the intercom production plate or in the Intercom Status tab via the web interface.

Example:

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

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

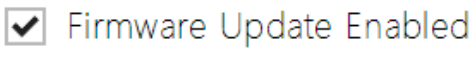
Configuration

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

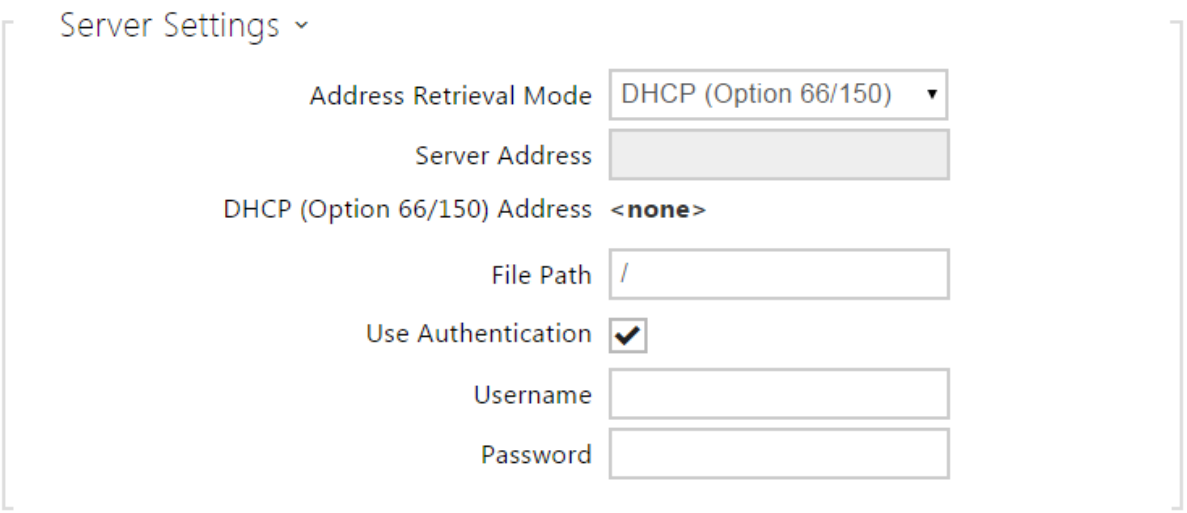
Note

- *A few seconds' interruption of the display function occurs in the display-equipped 2N® Helios IP Vario models during reconfiguration. Therefore, we recommend you to update when the intercom traffic is very low (at night, e.g.).*

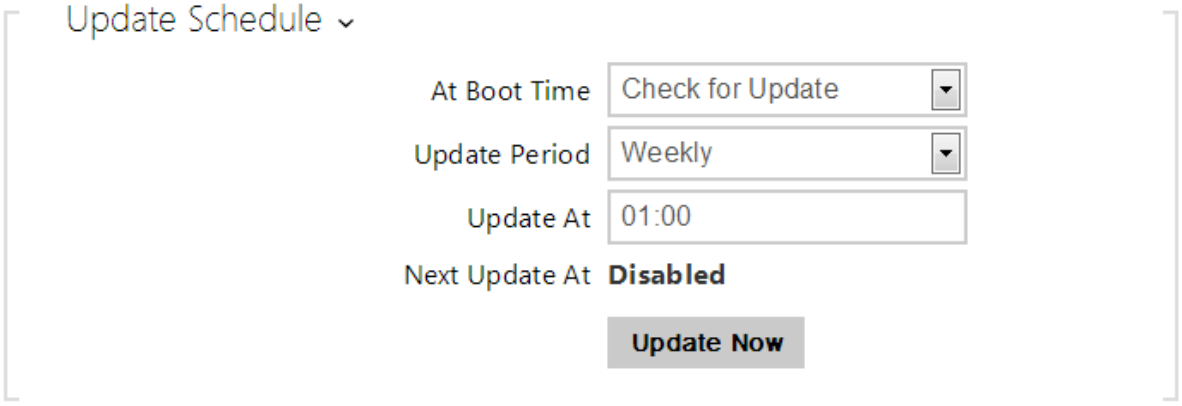
List of Parameters



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

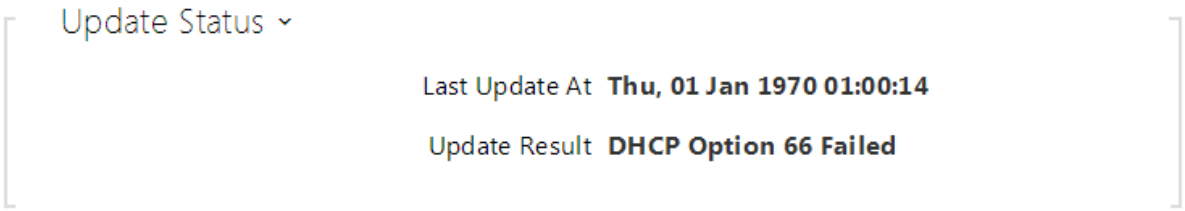


- **Address retrieval mode** – select whether the TFTP/HTTP server address shall be entered manually or a value retrieved automatically from the DHCP server using Option 66 shall be used.
- **Server address** – enter the TFTP (**tftp://ip_address**), HTTP (**http://ip_address**) or HTTPS (**https://ip_address**)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



- **At boot time** – enable check and, if possible, update execution upon every intercom start.
- **Update period** – set the update period: hourly, daily, weekly and 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** – set the next update time.



- **Last update at** – last update time .
- **Update result** – last update result. The following options are available:

Result	Description
Pending...	Update in progress
Update Succeeded	The configuration/firmware update has been successful. With firmware update, the device will be restarted in a few seconds.
Firmware Is Up To Date	A firmware update attempt reveals that the latest firmware version is used.
DHCP Option 66 Failed	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 Is Invalid	The file to be downloaded is corrupted or of a wrong type.

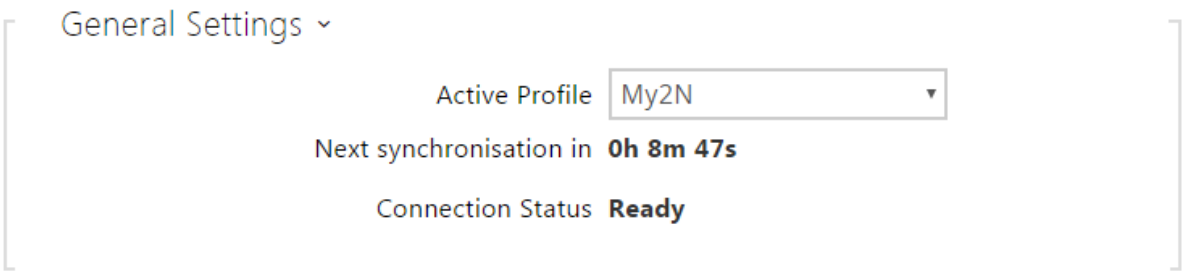
My2N / TR069

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.

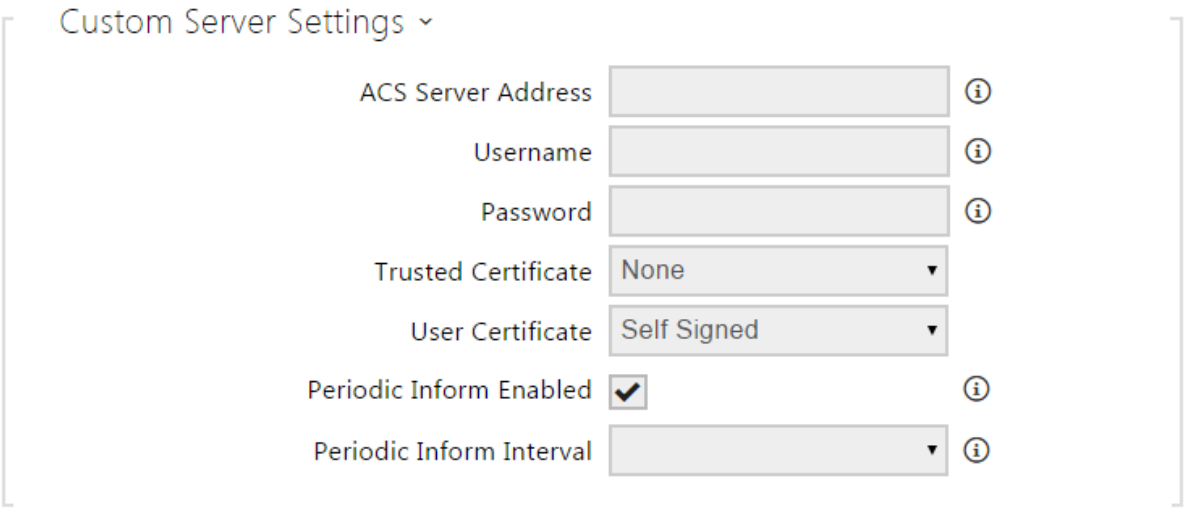
This function helps you connect the intercom to your ACS (Auto Configuration Server). In this case, the connection to My2N will be disabled in the intercom.

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



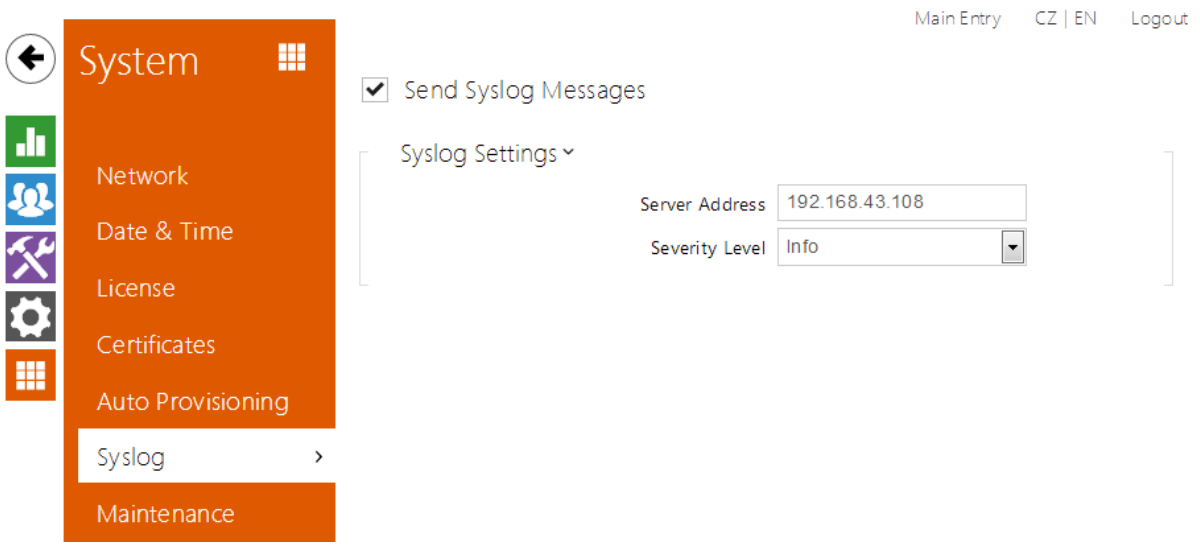
- Active profile – select one of the pre-defined profiles (ACS), or choose a setting of your own and configure the ACS connection manually.
- Next synchronisation in – display the time period in which the intercom shall contact a remote ACS.
- Connection status – display the current ACS connection state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

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



- **ACS server address** – s et the ACS address in the following format: ipaddress[: port], 192.168.1.1:7547, for example.
- **Username** – s et the user name for intercom authentication while connecting to the ACS server.
- **Password** – s et 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** – s pecify 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 interv al** – s et the interval of periodical logging of the intercom to the ACS if enabled by the **Periodic inform enabled** parameter.

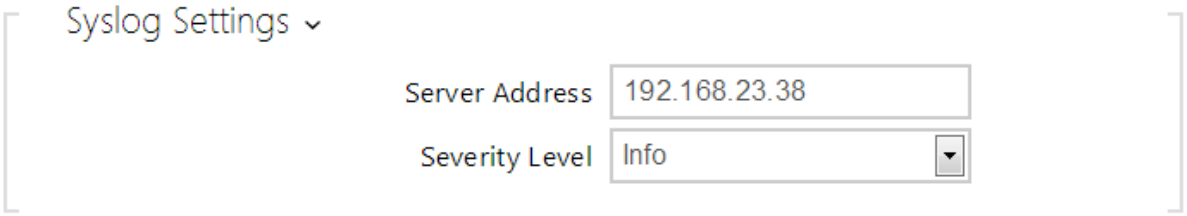
5.5.6 Syslog



The 2N Helios IP intercoms 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 unncecessary to configure this service for common intercom operation.

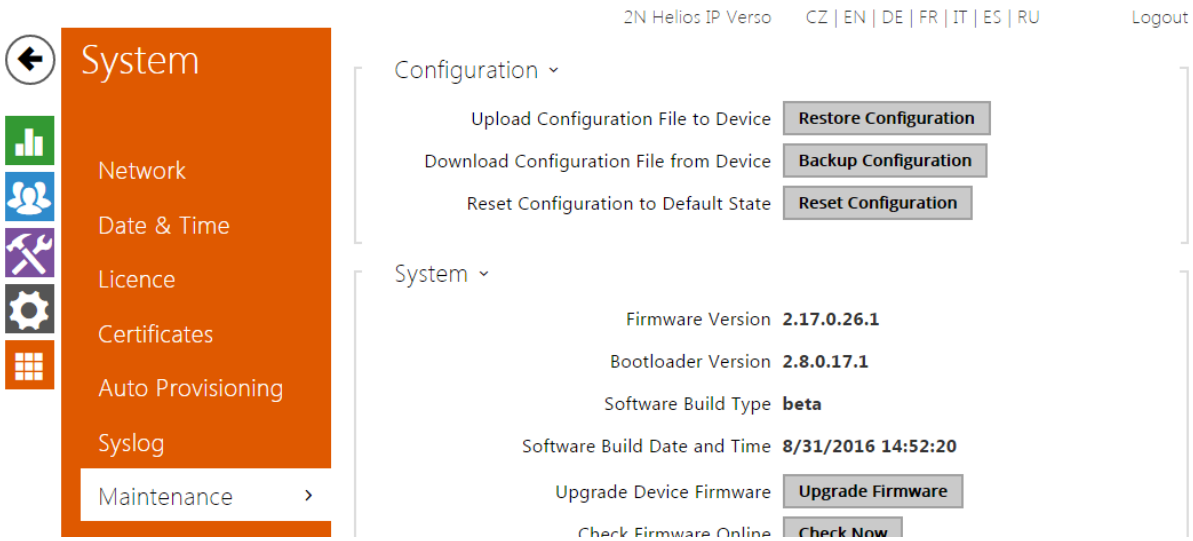
List of Parameters

- **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 intercom 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 intercom. Press the button to download the configuration file to your PC.

Caution

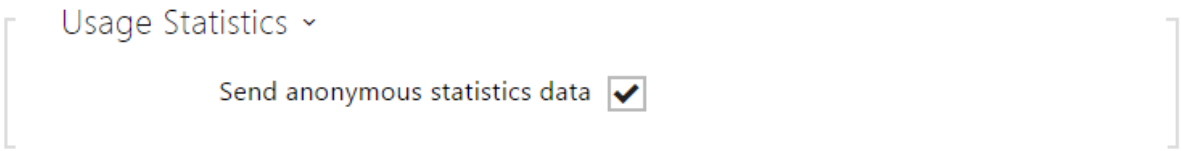
- *Treat the file cautiously as the intercom configuration may include delicate information such as user phone numbers and access codes.*

- **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 intercom. 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 intercom parameters except for the network settings. Use the respective jumper or push **Reset** to reset all the intercom parameters; refer to the Installation Manual of your intercom.

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 intercom firmware. Press the button to display a dialogue window for you to select and upload the firmware file to the intercom. 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 intercom. FW upgrade does not affect configuration as the intercom checks the FW file to prevent upload of a wrong or corrupted file.
- **Check firmware online** – check online whether a new firmware version is available. If so, download the new FW version and an automatic device upgrade will follow.
- **Restart intercom** – restart the intercom. The process takes about 30 s. When the intercom has obtained the IP address upon restart, the login window will get displayed automatically.



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

5.6 Used Ports

Service	Port	Protocol	Direction	Configurable
802.1x	-	-	In/Out	No
DHCP	68	UDP	In/Out	No
DNS	53	TCP/UDP	In/Out	No
Echo (device discovery)*	8002	UDP	In/Out	No
FTP	21	TCP	Out	No
2N® Helios IP Eye	8003	UDP	Out	No
HTTP	80	TCP	In/Out	Yes
HTTPS	443	TCP	In/Out	Yes
Multicast audio	22222	UDP	In/Out	No
Multicast video	22223	UDP	Out	No
NTP klient	123	UDP	In/Out	No
ONVIF	80	TCP	In/Out	No
RTP ports	5000 -	UDP	In/Out	Yes
RTSP server	554	UDP	In/Out	No
SingleWire Commands	80	TCP	In/Out	No
SingleWire Communication	8081	TCP	Out	No
SingleWire Discovery	427	UDP	In/Out	No

Service	Port	Protocol	Direction	Configurable
SingleWire Media	20000 -	UDP	In	No
SIP	5060	TCP/UDP	In/Out	Yes
SIPS	5061	TCP	In/Out	Yes
SMTP	25	TCP	Out	Yes
Syslog	514	UDP	Out	No
TFTP	69	UDP	Out	No

Echo – a proprietary protocol for the intercom discovery in the network. Used in applications: **2N® Helios IP Network Scanner**, **2N® Helios IP Eye**, **2N® Access Commander**.

6. Supplementary Information

Here is what you can find in this section:

- 6.1 Troubleshooting
- 6.2 Directives, Laws and Regulations
- 6.3 General Instructions and Cautions

6.1 Troubleshooting

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

6.2 Directives, Laws and Regulations

Europe

2N® Helios IP 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

v2.17