



2N[®] Helios IP

Door Access Intercom



Configuration Manual

Firmware 2.6
Version 2.6

www.2n.cz

The 2N TELEKOMUNIKACE joint-stock company is a Czech manufacturer and supplier of telecommunications equipment.



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



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



2N TELEKOMUNIKACE 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 hereby declares that the 2N[®] Helios IP 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 enclosed and 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.



The 2N TELEKOMUNIKACE company 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.

Content

1. Product Overview	4
2. Express Wizard for Basic Settings	6
3. Model Differences and Function Licensing	11
4. Signalling of Operational Statuses	14
5. Intercom Configuration	16
5.1 Status	19
5.2 Directory	21
5.3 Hardware	33
5.4 Services	59
5.5 System	87
6. Supplementary Information	104
6.1 Troubleshooting	105
6.2 Directives, Laws and Regulations	106
6.3 General Instructions and Cautions	108

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 Phone Book. 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; refer to the **Password** parameter in the **Services Web Server** menu. Remember the 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.

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.

Intercom Identity ▾

Display Name	<input type="text" value="Main Entry"/>
Phone Number (ID)	<input type="text" value="111"/>
Domain	<input type="text" value="192.168.1.1"/>

- **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:

SIP Proxy ▾

Proxy Address	<input type="text" value="192.168.1.1"/>
Proxy Port	<input type="text" value="5060"/>

SIP Registrar ▾

Registration Enabled

Registrar Address

Registrar Port

Registration Expires [s]

- **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:

Authentication ▾

Use Authentication ID

Authentication ID

Password

- **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 Phone Book position.

Select position 1, which corresponds to quick dial button 1, in the **Directory Phone Book** 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.

Position Enabled

User Phone Numbers ▾

Number 1

Phone Number

Time Profile ▾

Helios IP Eye Address

Parallel call to following number

Number 2

Phone Number

Time Profile ▾

Helios IP Eye Address

Parallel call to following number

Number 3

Phone Number

Time Profile ▾

Helios IP Eye Address

Deputy

User Deputy

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.



Switch Enabled

Output Settings ▾

Controlled Output

Output Type

Switch Codes ▾

	CODE	ACCESSIBILITY	TIME PROFILE
1	<input type="text" value="123"/> 	<input type="text" value="Keypad + DTMF"/>	<input type="text" value="[not used]"/>
2	<input type="text" value="123"/> 	<input type="text" value="Keypad + DTMF"/>	<input type="text" value="[not used]"/>
3	<input type="text"/>	<input type="text" value="Keypad + DTMF"/>	<input type="text" value="[not used]"/>

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			ne			
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	no	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	
Button extenders	up to 145	up to 48	no			programmable buttons	
Numeric keypad	optional			no			
Digital input	yes	optional			no	2	
Adaptive volume control	yes	no	yes				
Amplifier power output	2 W	150 mW	1 W			10 W	
Extended amplifier power output (10 W)	no		yes		no	no	
Tamper switch	optional	no	optional		yes	no	
Phone Book 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				2	20	
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)

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

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	Gold (Profi)
User sounds	•				•
Automatic audio test	•				•
Audio/video streaming (RTSP Server)		•			•
External IP camera support		•			•
ONVIF support		•			•
Extended switch setting options			•		•
HTTP switch control			•		•
Automation functions			•		•
E-mail sending (SMTP Client)			•		•
Automatic update (TFTP/HTTP Client)			•		•
802.1x support				•	•
SIPS (TLS) support				•	•









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 (Phone Book position) activation. Refer to the Phone Book subsection for the activation code settings.
	User deactivated This tone signals entering of the user deactivation code. The deactivation code is used for user (Phone Book 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 Phone Book subsection for the deactivation code settings.
	Profile activated This tone signals profile activation. This function helps enable alerting of a user group in an office, for example. Refer to the Profile subsection for the activation code settings.
	Profile deactivated This tone signals profile deactivation. This function helps, for example, disable alerting of a user group in an office and routing calls either to a pre-defined phone number (porter's lodge, e.g.) or user mobile phones. Refer to the Profile subsection for the deactivation code settings.

	<p>Call prolongation confirmation signalling</p> <p>Calls are time-limited in 2N® Helios IP for security reasons (protection against blocking). Refer to the Miscellaneous subsection for details.</p>
	<p>Internal application launched</p> <p>The internal application is launched upon 2N® Helios IP power up or restart. A successful launch is signalled by this tone combination.</p>
	<p>Connected to LAN, IP address received</p> <p>2N® Helios IP logs in upon the internal application launch. A successful LAN login is signalled by this tone combination.</p>
	<p>Disconnected from LAN, IP address lost</p> <p>This tone signals UTP cable disconnection from 2N® Helios IP. Disconnection is signalled by this tone combination.</p>
	<p>Invalid telephone number or invalid switch activation code</p> <p>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.</p>
	<p>Default reset of network parameters</p> <p>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.</p>
	<p>Call end signalling</p> <p>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.</p>
	<p>Connected VoIP phone – 2N® Helios IP call</p> <p>This short tone signals successful connection between a VoIP phone and 2N® Helios IP.</p>

5. Intercom Configuration

2N Helios IP Verso CZ | EN Logout

2N[®] Helios IP Verso

Intercom Status

Status

SERIAL NUMBER 54-0776-0005
FIRMWARE 2.5.0.12.2

UP TIME 0d 0h 21m 30s

PHONE NUMBER REGISTERED
5001

Intercom Configuration

Directory

1 USER(S)
2 CARD(S)

Time Profiles

Services

PHONE | E-MAIL
RTSP | JPEG | ONVIF

Streaming

Automation

2N

Camera

Hardware

INTERNAL CAMERA
6 MODULE(S)

Microphone

Speaker

Manual **FAQ**

License

System

LICENSE GOLD
DHCP | TLS | MD5

Network

Start Screen

The start screen is an introductory overview screen displayed upon login to the intercom web interface. Use the back arrow **XXX** 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.

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

- **Phone Book** – 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
- **Speaker** – audio, signalling, etc. volume control
- **Microphone** – microphone parameters, echo cancelling
- **Camera** – internal camera, external IP camera settings
- **Keyboard** – button and keyboard 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.)
- **E-Mail** – E-mail sending and SMTP connection settings
- **Automation** – flexible intercom settings according to the user's requirements
- **User Sounds** – user sound settings and upload
- **Web Server** – web server and access password settings
- **Audio Test** – automatic audio test 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



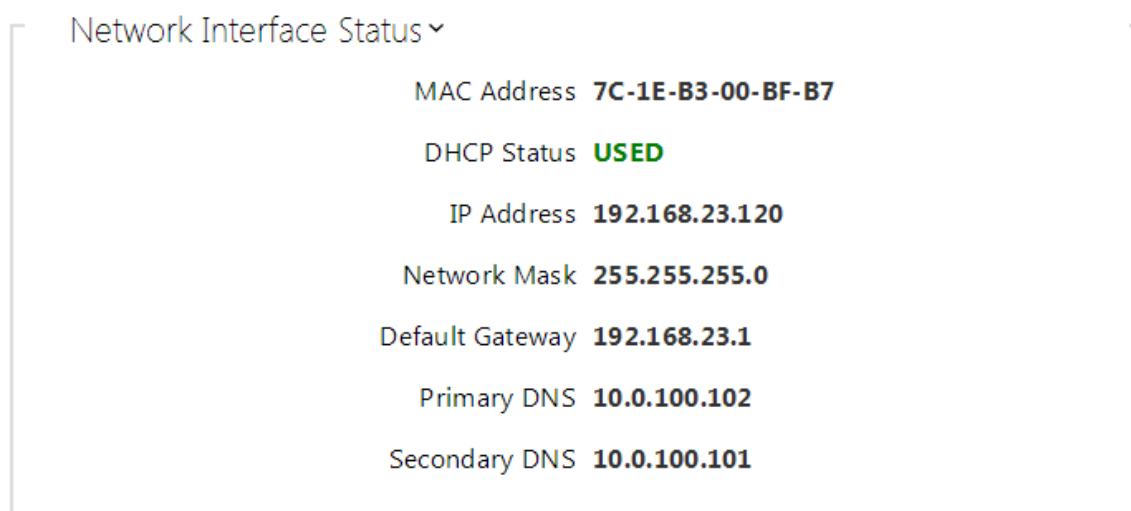
The **Status** menu provides clear status and other essential information on the intercom. The menu is divided into three tabs: **Device**, **Services** and **Licence**.

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.



Phone Status ▾

SIP Number **5001**
Registration State **REGISTERED**
Registration At **192.168.1.140**
Registration Last Time **2070-01-01 04:01:23**

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).

Licensed Features ▾

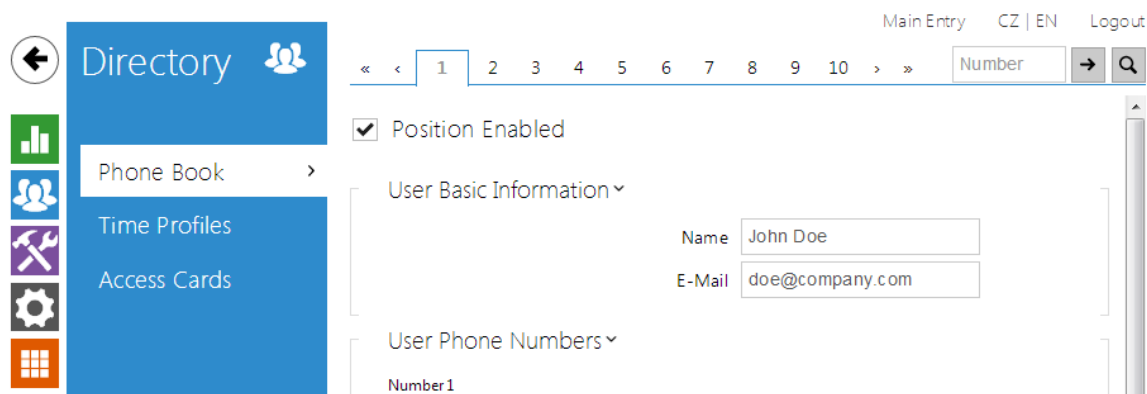
Automatic Updates **YES**
RTSP Server **YES**
G.729 Codec **NO**
Advanced Switch Settings **YES**
User Sounds **YES**
Switch Control by HTTP **YES**
SMTP Service **YES**
802.1x Authentication **YES**
Automation **YES**
Audio Test **YES**

5.2 Directory

Here is what you can find in this subsection:

- [5.2.1 Phone Book](#)
- [5.2.2 Time Profiles](#)
- [5.2.3 Access Cards](#)

5.2.1 Phone Book



The Phone Book 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 Phone Book is arranged as a table with up to 1999 positions (depending on the particular **2N® Helios IP** model): typically, each user is assigned just one position. The Phone Book includes information on the users that are accessible by quick dialling and users that are only allowed to enter the facility with their RFID cards. As the user Phone Book position substantially affects the intercom functions, please read the following text carefully and design the optimum layout according to your needs before filling the Phone Book with data.

Each intercom user has a specific Phone Book position: 1 through 1999. The user position number is very important as it also defines the **quick dial button number** assigned to the user. Therefore, place the user on the position that corresponds to the required quick dial button and complete the user phone number to make quick dialling efficient. Most **2N® Helios IP** models are equipped with one or more quick dial buttons. Refer to the Installation Manual of your intercom model for the button count, extending options and Phone Book position mapping details.

You are advised to place the users that are not supposed to be assigned any quick dial button but should have the right to enter the facility with the RFID card or numeric code onto the top positions of the Phone Book (position 100 and higher). If such user, for some reason, has to be placed on a position that corresponds to a quick dial button, leave the user phone number parameter empty and complete the door unlocking RFID card ID or numeric code only. Thus, you will make the quick dial button act as a non-programmed key.

In case the number of the users that are to be accessible by the intercom is higher than the count of the quick dial buttons installed, you can enable user dialling by entering the Phone Book position via the numeric keypad: the caller dials the position number and pushes the * key. Enable this using the **** parameter in the *** menu. If you decide to use this user calling method, you are advised to place a clear list of user names and Phone Book positions including brief instructions near the intercom.

You can also combine quick button dialling and numeric keypad dialling. In this case, reserve the Phone Book beginning positions for the quick dial buttons and complete the higher positions (from position 100 up, e.g.) with data on the users to be included in

the public user list. Then select the users to be accessible by quick dialling and copy their phone numbers to the lower Phone Book positions corresponding to the quick dial buttons.

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

List of Parameters

Position Enabled

- **Position enabled** – enable calling to this Phone Book position.

User Basic Information ▾

Name	<input type="text" value="John Doe"/>
E-Mail	<input type="text" value="doe@company.com"/>

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

User Phone Numbers ▾

Number 1

Phone Number

Time Profile ▾

Helios IP Eye Address

Parallel call to following number

Number 2

Phone Number

Time Profile ▾

Helios IP Eye Address

Parallel call to following number

Number 3

Phone Number

Time Profile ▾

Helios IP Eye Address

Deputy

User Deputy

You can assign up to three user phone numbers to each Phone Book 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.
- **Time profile** – assign a time profile to each phone number to define the number validity. If the profile is 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 Eye** application displays the camera image screen for those users who are not provided with a display-equipped videophone. Enter the address as follows: ip_address[:port1][:port2]. 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).

- **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.
- **User deputy** – select a user to which the user calls will be routed in the event of inaccessibility. 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).

User Activation ▾

User Activation Code

User Deactivation Code


User Current State **ACTIVE** 

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.

User Switch Codes ▾

	CODE	TIME PROFILE
Switch 1	<input type="text"/>	[not used] ▾
Switch 2	<input type="text"/>	[not used] ▾
Switch 3	<input type="text"/>	[not used] ▾
Switch 4	<input type="text"/>	[not used] ▾

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.

User Cards ▾

Card ID	<input type="text"/>
Time Profile	[not used] ▾

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: 6–16 characters including 0–9, A–F. Each user can be assigned just one access card.
- **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.

5.2.2 Time Profiles

The screenshot shows the 'Time Profiles' configuration page in the 2N Helios IP Manager. The page has a navigation menu on the left with options: Directory, Phone Book, Time Profiles (selected), and Access Cards. The main content area is titled 'Basic Settings' and 'Profile Time Sheet'. Under 'Basic Settings', the 'Profile Name' is set to 'Working Hours'. Under 'Profile Time Sheet', there are four rows for the days of the week, each with a checked checkbox, a 'from' time of 08:00, and a 'to' time of 17:00.

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 Phone Book, 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.

Caution

- In case you use the **2N® Helios IP** Manager for intercom configuration, we do not recommend you to modify the time profile settings via the web interface.

List of Parameters

Basic Settings ▾

Profile Name

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

Profile Time Sheet ▾

Sunday	<input checked="" type="checkbox"/>	from	<input type="text" value="08:00"/>	– to	<input type="text" value="18:00"/>
Monday	<input checked="" type="checkbox"/>	from	<input type="text" value="08:00"/>	– to	<input type="text" value="18:00"/>
Tuesday	<input checked="" type="checkbox"/>	from	<input type="text" value="08:00"/>	– to	<input type="text" value="18:00"/>
Wednesday	<input checked="" type="checkbox"/>	from	<input type="text" value="08:00"/>	– to	<input type="text" value="18:00"/>
Thursday	<input checked="" type="checkbox"/>	from	<input type="text" value="08:00"/>	– to	<input type="text" value="18:00"/>
Friday	<input type="checkbox"/>	from	<input type="text" value="00:00"/>	– to	<input type="text" value="00:00"/>
Saturday	<input type="checkbox"/>	from	<input type="text" value="00:00"/>	– to	<input type="text" value="00:00"/>

Note

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

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.

Profile Manual Activation ▾

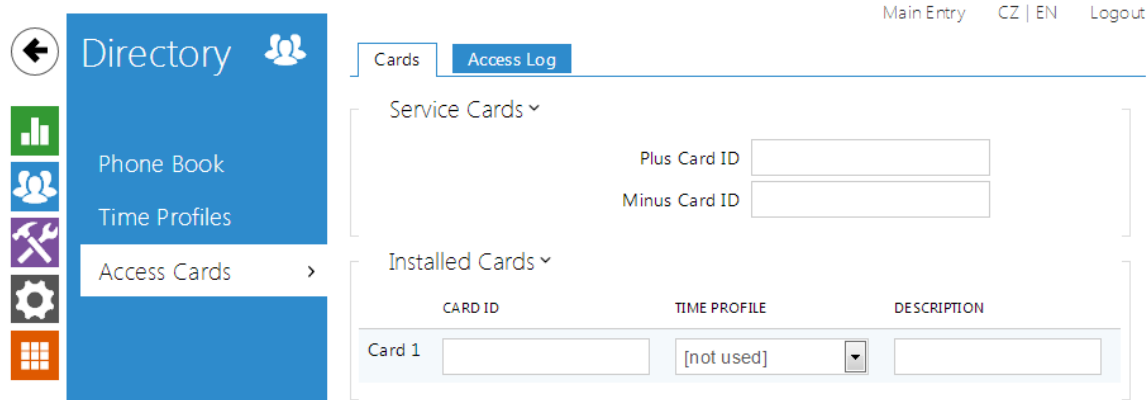
Profile Activation Code

Profile Deactivation Code

Profile Current State **ACTIVE** ↻

- **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.

5.2.3 Access Cards



Each intercom user can be assigned one or more access RFID cards. Typically, the card ID is included in the Phone Book 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 Phone Book with its up to 1999 positions, the Installed Cards may contain only 20 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 is 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**: 6–16 characters including 0–9, A–F (i.e. hexadecimal number of the length of 24 to 64 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 **Directory Access Cards Records** 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 **Records**. 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

Service Cards ▾

Plus Card ID

Minus Card ID

- **Plus card ID** – enter the service card ID for adding cards to the Installed cards: a sequence of 6–16 characters including 0–9, A–F.
- **Minus card ID** – enter the service card ID for removing cards from the Installed cards: a sequence of 6–16 characters including 0–9, A–F.

Installed Cards ▾

	CARD ID	TIME PROFILE	DESCRIPTION
Card 1	<input type="text" value="123456"/>	<input type="text" value="[not used]"/> ▾	<input type="text"/>
Card 2	<input type="text" value="456785"/>	<input type="text" value="[not used]"/> ▾	<input type="text"/>
Card 3	<input type="text" value="7954564"/>	<input type="text" value="[not used]"/> ▾	<input type="text"/>
Card 4	<input type="text"/>	<input type="text" value="[not used]"/> ▾	<input type="text"/>

- **Card ID** – enter the access card ID: a sequence of 6–16 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.

Records

The **Records** 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.).

Access Log ▾

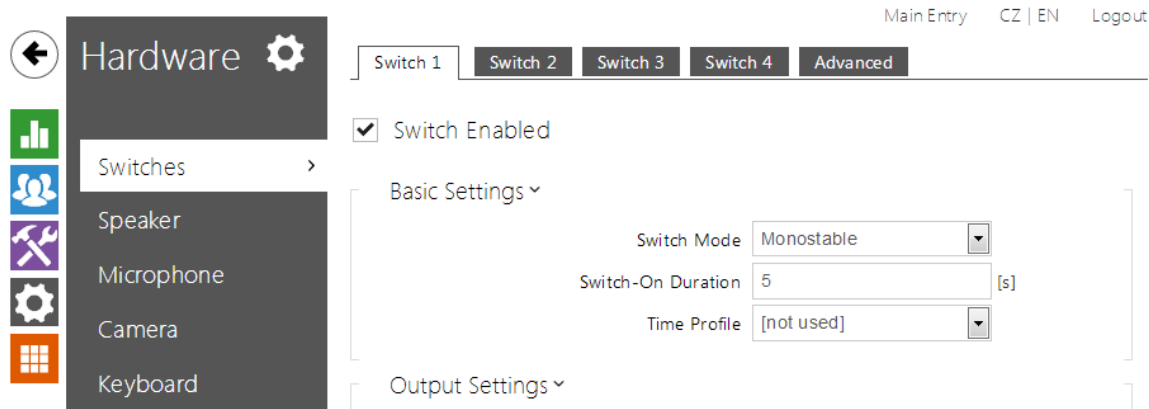
	TIME	CARD ID	CARD TYPE	DESCRIPTION
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

5.3 Hardware

Here is what you can find in this section:

- [5.3.1 Switches](#)
- [5.3.2 Speaker](#)
- [5.3.3 Microphone](#)
- [5.3.4 Camera](#)
- [5.3.5 Keyboard](#)
- [5.3.6 Display](#)
- [5.3.7 Card Reader](#)
- [5.3.8 Extenders](#)

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

- **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.

Basic Settings ▾

Switch Mode	Monostable	▾
Switch-On Duration	5	[s]
Time Profile	[not used]	▾

- **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.

Note

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

Output Settings ▾



Controlled Output	Relay 1	▾
Output Type	Normal	▾

- **Controlled output** – assign an electric output to the switch. Choose one of the available intercom outputs: relay, power output, extender output. 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.

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.

Switch Codes ▾

	CODE		ACCESSIBILITY	TIME PROFILE
1	123 		Keypad + DTMF ▾	[not used] ▾
2	123 		Keypad + DTMF ▾	[not used] ▾
3			Keypad + DTMF ▾	[not used] ▾

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 *.
- **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.

Extended Activation ▾

Activation by Call ▾

Activation by Quick Dial Button ▾

Note

- The extended switch activation is available with the Gold or Enhanced Integration licence only.

- **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.

State Signalling ▾

Sound Signalling	<input type="text" value="Long beep"/>
Display Info	<input type="text" value="Door opened"/>

- **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.

Synchronisation ▾

Synchronise with	<input type="text" value="[not used]"/>
Synchronisation Delay	<input type="text" value="0"/> [s]

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

HTTP Commands ▾

Switch-On Command	<input type="text"/>
Switch-Off Command	<input type="text"/>

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`

Advanced Settings ▾

Enable Switch Control by HTTP

Legacy Switch Code

- **Enable switch control by HTTP** – enable the HTTP switch control option. Refer to the Switch Control by HTTP details below.
- **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.

Switch Control by HTTP

Note

- The HTTP switch control function is available with the Gold or Enhanced Integration licence only .

To change the switch state, send the HTTP request (GET request) to the intercom IP address. Make sure that the function is enabled in the **Enable Switch Control by HTTP** parameter. The request format is as follows: (use any browser to try):

- `http://intercom_address/enu/lockstate.xml.p?lockXstate=Y&answer=Z`

where **X** is the switch number (1–4) and **Y** specifies the type of action: 0 – switch off, 1 – switch on, and 2 – state change.

The response to the HTTP request contains an XML message including the current states of all switches:

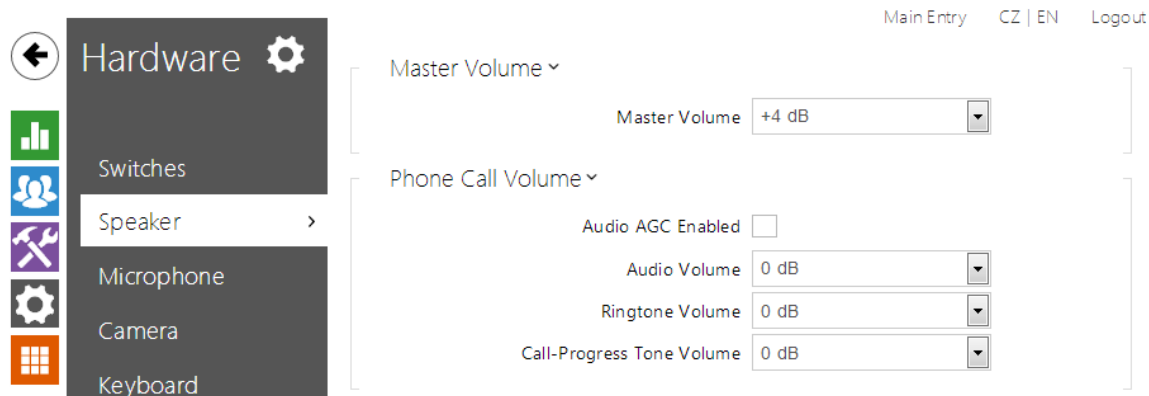
```
<result>
<lock1state>0</lock1state>
<lock2state>0</lock2state>
<lock3state>0</lock3state>
<lock4state>0</lock4state>
</result>
```

If the **answer** parameter is included in the HTTP request, the response is not in the XML format, but only contains text **Z**.

Note

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

5.3.2 Speaker



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 configuration section. The speaker volume settings are closely associated with the microphone sensitivity parameters as explained below.

Set the intercom speaker volume and microphone sensitivity values in the **Master volume**, **Phone call volume** and **Microphone sensitivity** parameters. The values can be different for different intercom models as shown in the table below:

Model	Master volume	Phone call volume	Microphone sensitivity
Vario	-6 dB .. +6 dB (150 mW)	-6 dB .. +18 dB	-6 dB .. +6 dB
Force/Safety 1W	-20 dB .. +16 dB (1 W)	-6 dB .. +18 dB	-6 dB .. +12 dB
Force/Safety 10W	-20 dB .. +20 dB (10 W)	-6 dB .. +18 dB	-6 dB .. +12 dB
Uni	-20 dB .. +16 dB (1 W)	-6 dB .. +18 dB	-6 dB .. +12 dB
Verso	-12 dB .. 12 dB (2 W)	-6 dB .. +18 dB	-6 dB .. +12 dB

The **Master volume** parameter controls the general loudness of the device, i.e. call and signal volumes, for example. Set the values with respect to the noise level of the surroundings. People tend to speak more loudly in noise environments than on quiet places and so remember that the noisier the surrounding environment, the lower the microphone sensitivity.

The **Phone call volume** parameter controls the reproduced phone call signal loudness. Adjust the value if the current master volume is still insufficient for the given environment. Values higher than +6dB may lead to some signal distortion without substantially affecting the intelligibility of speech.

The **Microphone sensitivity** parameter controls the integrated microphone signal loudness and affects the audibility of the intercom user. The microphone sensitivity value is relative against the automatic microphone sensitivity setting in the Master volume parameter.

✓ **Tip**

- If the Speaker volume and Microphone sensitivity values exceed + 12 dB if put together, the sound quality of the intercom-to-phone signal may deteriorate in some cases due to acoustic feedback between the microphone and the speaker depending on the intercom installation site conditions (mounting method, device placement, environment qualities, surrounding noise, etc.). If you hear interference in your handset during intercom communication, set the **AEC Artefacts Reduction** value to Low or High as necessary.

List of Parameters

Master Volume ▾

Master Volume 0 dB ▾

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

Adaptive Mode ▾

Adaptive Volume

Minimum Volume 0 dB ▾

Maximum Volume 0 dB ▾

ⓘ **Note**

- This setting is available in the adaptive mode supporting models only.

- **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.
- **Minimum volume** – set the minimum volume in the adaptive mode to avoid dropping below the acceptable limit.
- **Maximum volume** – set the maximum volume in the adaptive mode to avoid exceeding of the acceptable limit.

Phone Call Volume ▾

Audio AGC Enabled	<input checked="" type="checkbox"/>
Audio Volume	0 dB ▾
Ringtone Volume	0 dB ▾
Call-Progress Tone Volume	0 dB ▾

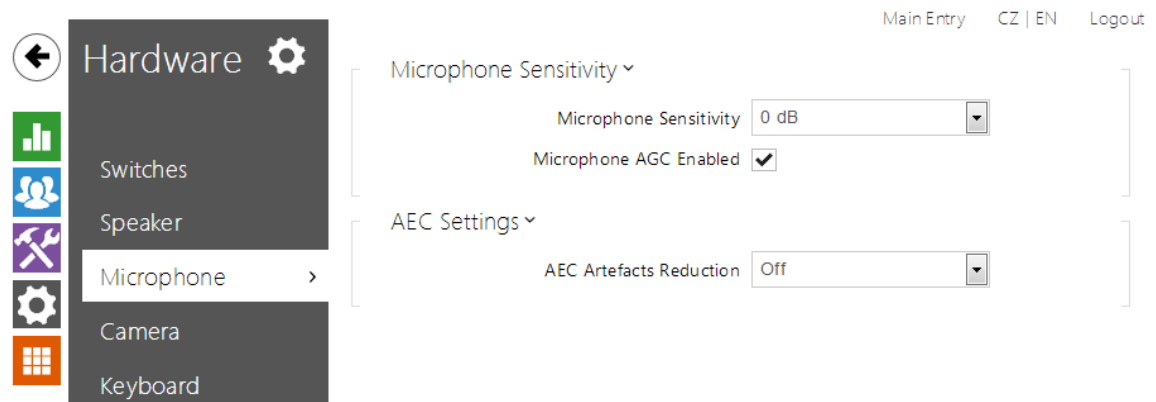
- **Audio AGC enabled** – enable the automatic gain control of the line signal.
- **Audio volume** – set the phone call volume. The volume values are relative against the set master volume.
- **Ringtone volume** – set the incoming call signal loudness.
- **Call-progress tone volume** – set the dial, ring and busy tone volume. In case the call-progress tones are automatically generated by the PBX, this setting will not be applied.

Signalling Volume ▾

Key Beep Volume	0 dB ▾
Warning Tone Volume	0 dB ▾
Switch-Activation Tone Volume	0 dB ▾

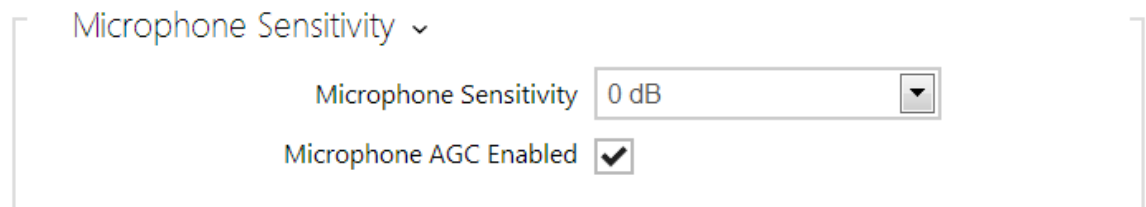
- **Key beep volume** – set the key beep volume. The volume values are relative against the set master volume.
- **Warning tone volume** – set the volume of warning and signalling tones described in the **Signalling of Operational Statuses** section. The volume values are relative against the set master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

5.3.3 Microphone

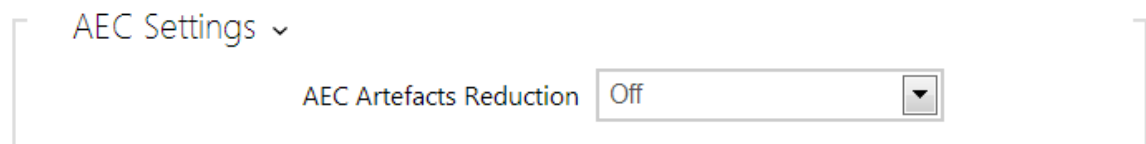


Set the microphone and line audio input volume parameters in this intercom configuration section. The microphone volume settings are closely associated with the speaker sensitivity parameters and intercom installation site conditions, which affect the general audio reproduction and recording quality. If you notice a deteriorated audio quality, please read the **Speaker** subsection carefully too to set the intercom audio parameters on your installation site properly.

List of Parameters



- **Microphone sensitivity** – set the microphone sensitivity.
- **Microphone AGC enabled** – set the automatic gain control (AGC) mode for the microphone.



- **AEC artefacts reduction** – enable cancelling of interfering noise (i.e. artefacts caused by cancellation of the local acoustic feedback on the intercom installation site); refer to the Specification of Audio Parameter Function parameter.

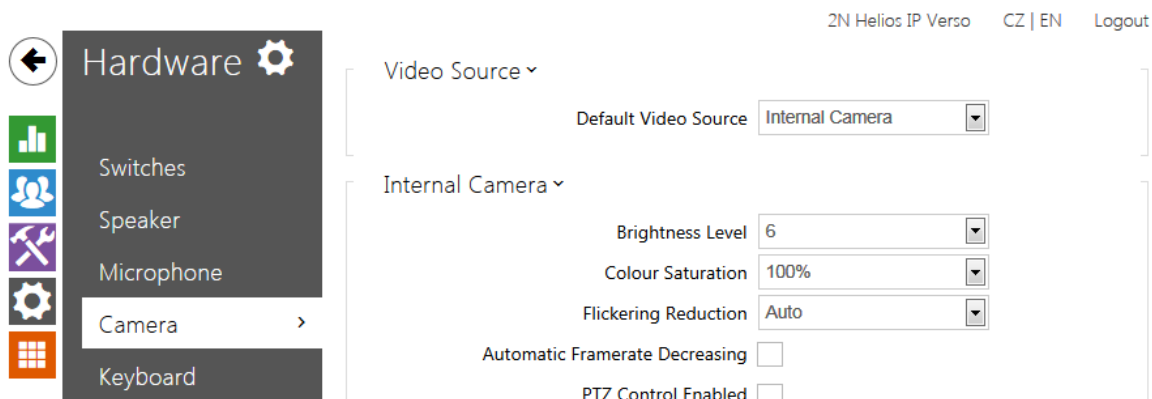
Line In Settings ▾

Default Audio Input Line Input Gain **Note**

- This setting is available in the line input supporting models only.

- **Default audio input** – set the default audio input (microphone, line input or audio module input) for phone calls and audio streaming.
- **Line input gain** – set the line input gain independently of the microphone gain setting.

5.3.4 Camera



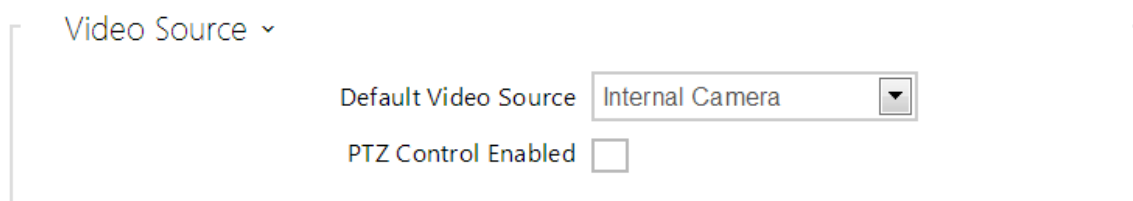
This menu is only available in the **2N® Helios IP** models that are equipped with an internal camera or can be connected to an external camera. The camera signal can be streamed directly into the call via a videophone, sent by E-mail, streamed via ONVIF/RTSP to another device (a video surveillance device,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

The following video signal sources can be used:

- internal integrated camera or external analogue camera (**2N® Helios IP Video Kit** only)
- standard external IP camera supporting MJPEG/RTSP stream with VGA (640 x 480) resolution

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



- **Default video source** – set the default video signal source. Choose an Internal camera (or an analogue camera connected to the intercom) or an External IP camera.

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

Colour Saturation

Flickering Reduction

IR LED Brightness Level

Current IR LED Brightness Level **0%**

- **Brightness level** – set the camera image brightness level.
- **Colour saturation** – set the camera image colour saturation.
- **Flickering reduction** – set reduction of image flickering caused by artificial light sources (fluorescent lamps, e.g.). Select your network frequency or keep the **Auto** setting.
- **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.
- **IR LED brightness level** - set the infrared LED brightness level in the range of 0-100% in several steps. Infrared illumination is automatically activated if the intercom detects lack of ambient light and the camera image is used. The IR LED brightness level settings are only available in the **2N® Helios IP Verso** model.
- **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).

Input Channel Settings ▾

Video Channel	Channel 0 ▾
Video Standard	Auto ▾

Note

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

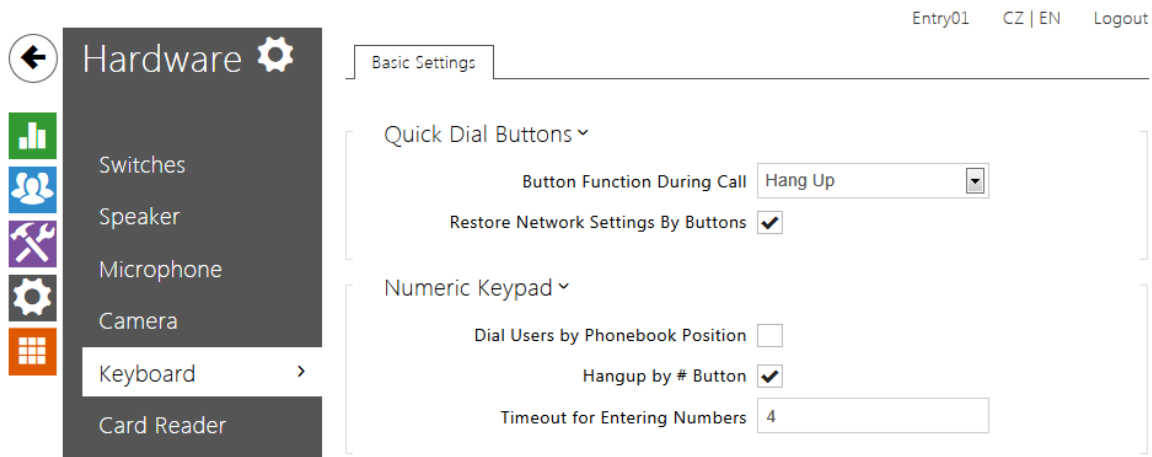
- **Video input** – choose one of the analogue camera inputs. You can change the input by automation via the Action.SetCameraInput during operation.
- **Video standard** – set the video standard for the camera connected. Modify the value only if the automatic video standard detection does not work well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

External IP Camera ▾

External Camera Enabled	<input checked="" type="checkbox"/>
RTSP Stream Address	rtsp://192.168.1.5
Username	<input type="text"/>
Password	<input type="text"/>

- **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
- **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.

5.3.5 Keyboard



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

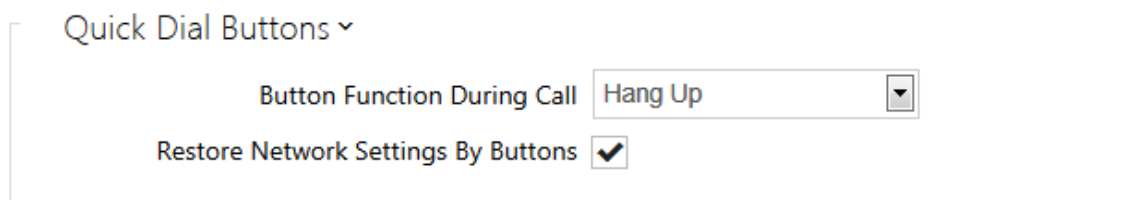
- use the numeric keypad for dialling common phone numbers
- use the numeric keypad for dialling a Phone Book position
- use the numeric keypad for entering the access code for door unlocking, e.g.
- set the # function
- set the quick dial button functions during a call
- set the timeout for entering 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

Note

- The **2N® Helios IP** models that are not equipped with a numeric keypad, do not provide all setting options mentioned herein.



- **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 Phone Book. 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 respond 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.

Numeric Keypad ▾

Dial Users by Phonebook Position

Hangup by # Button

Timeout for Entering Numbers

- **Enable calling to position number** – enable calling to a Phone Book user by dialling the user position number (2 to 4 digits) and pressing * for confirmation.
- **Hang up by # button** – enable termination of the active call by the # key. 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 the timeout elapses, the dialling is automatically confirmed as if the * key was pressed.

Telephone Mode ▾

Telephone Mode Enabled

Maximum Number of Dialed Digits

- **Telephone mode enabled** – enable the option to set up calls directly to the phone numbers dialled via the intercom numeric keypad. Enter the **telephone_number** key sequence to set up the call.
- **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 *.

LED Backlight ▾

Backlight Level 100% ▾

- **Backlight level** – set the keypad and button backlight level.

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.

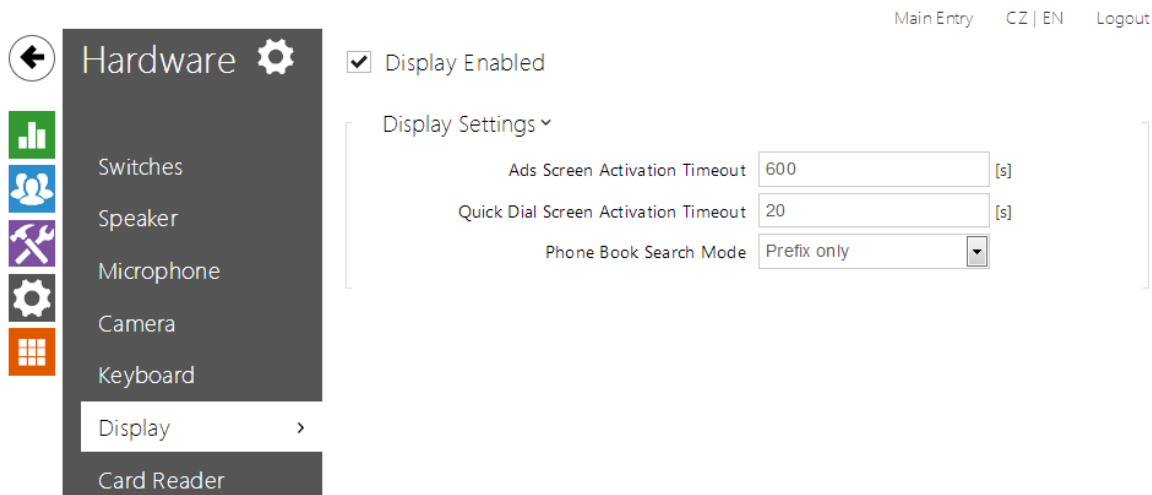
The figure below shows the default button settings.

Keyboard Mapping ▾

	COLUMN 1	COLUMN 2	COLUMN 3	COLUMN 4
Row 1	Keypad 1 ▾	Keypad 2 ▾	Keypad 3 ▾	Quick Dial (1) ▾
Row 2	Keypad 4 ▾	Keypad 5 ▾	Keypad 6 ▾	Quick Dial (2) ▾
Row 3	Keypad 7 ▾	Keypad 8 ▾	Keypad 9 ▾	Quick Dial (3) ▾
Row 4	Keypad * ▾	Keypad 0 ▾	Keypad # ▾	Quick Dial (4) ▾

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

5.3.6 Display

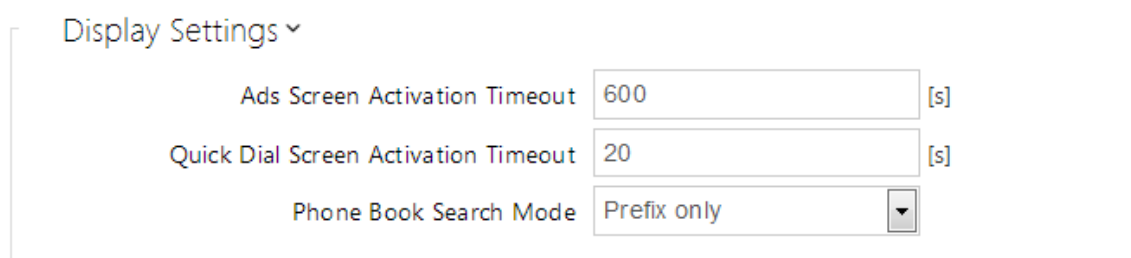


Some **2N® Helios IP Vario** models are equipped with a colour display. Configure the display exclusively via the **2N® Helios IP Manager**. In this menu, you can only switch the display on/off and set a few parameters.

List of Parameters

Display Enabled

- **Display enabled** – enable/disable the display function.



- **Ad screen activation timeout** – set the maximum idle time (i.e. time during which the user does not control the device using the buttons or numeric keypad) after which the advertisement displaying mode is switched on automatically.
- **Quick dial screen activation timeout** – set the maximum idle time (i.e. time during which the user does not control the device using the buttons or numeric keypad) after which the Phone Book is switched into the nametag displaying mode.
- **Phone Book 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).

5.3.7 Card Reader

Main Entry CZ | EN Logout

← Hardware ⚙️

- 📊 Switches
- 👤 Speaker
- 🔧 Microphone
- ⚙️ Camera
- 📺 Keyboard
- 📺 Display
- Card Reader >

Basic Settings ▾

Card Reader Enabled

Associated Switch

RFID Interface ▾

Accepted HID Cards

Wiegand Interface ▾

Interface Mode

Message Format

Change Facility Code

Facility Code

State Signalling ▾

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.

The **2N® Helios IP Vario** (91371...U) and all **2N® Helios IP Force** models are equipped with a red LED indicator. You can control the LED state via the digital inputs on the card reader. Typically, this function helps signal the secured/unsecured state via a wire from the security exchange to the intercom connected to one of the card reader inputs.

List of Parameters

Basic Settings ▾

Card Reader Enabled

Associated Switch

- **Card reader enabled** – enable the card reader function. If disabled, the card reader ignores all applied cards. If the card is disabled and the Wiegand interface is OUT, all codes of the used cards are resent to the Wiegand interface.
- **Associated switch** – select a switch to be activated whenever a valid card is applied.

RFID Interface ▾

Accepted HID Cards

Accepted HID cards – set the type of HID Prox cards to be accepted by the card reader. The card reader supports just one card type at an instant. This setting is not applied if you do not use the HID Prox cards.

Wiegand Interface ▾

Interface Mode

Message Format

Change Facility Code

Facility Code

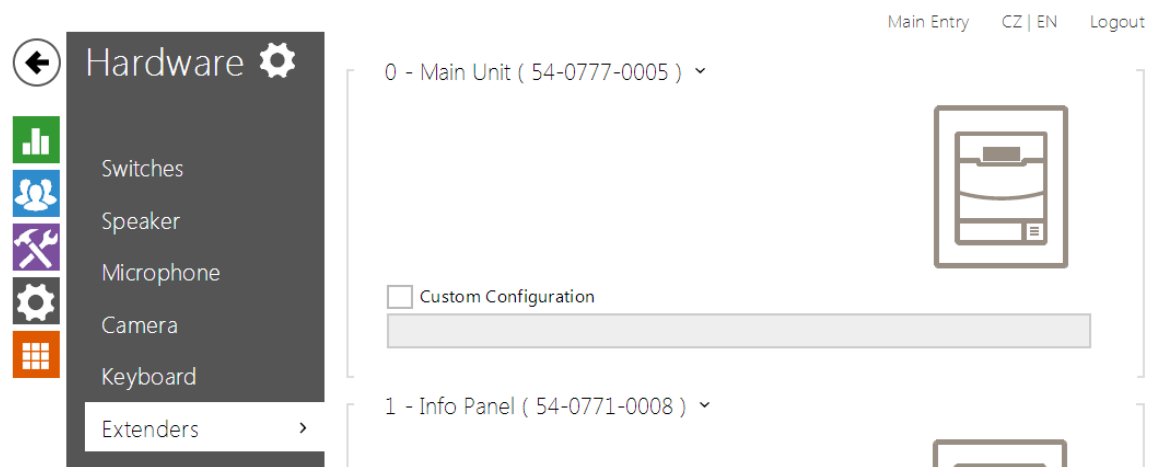
- **Interface mode** – enable the Wiegand function and set Wiegand IN/OUT. The IDs of the cards tapped on the internal card reader are always resent to Wiegand OUT.
- **Message format** – set the sent/received message format: 26-bit or 32-bit.
- **Change facility code** – set the mode in which the first 8 bits of the 24 card ID resent to the Wiegand interface are replaced with the value included in the **Facility code**. The parameter is applied only if the Wiegand is OUT.
- **Facility code** – enter the facility code for card ID resending to Wiegand.

State Signalling ▾

Red LED Control

- **Red LED control** – enable the red LED control according to the card reader digital input states. The values defines the condition under which the red LED shall be on.

5.3.8 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
- I/O module
- Wiegand module

The modules are chain-like interconnected. Each of the modules has its number depending on the chain position (the first module has number 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 modules can also be configured via the text line with a list of parameters (parameter_name=parameter_value) separated with semicolons. At present, just a few of these parameters are available. The other parameters are not public as they are rather experimental and can be modified in the future.


Basic Unit Module Configuration

0 - Main Unit (54-0777-0023) ▾

Output 1 Maximum Power

5W ▾

Custom 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

3 - Buttons (54-0769-0005) ▾

Button Functions

Quick Dial Buttons 2 - 6 ▾


Custom Configuration



- **Button function** – assign Phone Book positions to the buttons.

Keypad Module Configuration

2 - Keypad (54-0770-0014) ▾




Custom Configuration

- No parameters are available to the public at present.

Infopanel Module Configuration

1 - Info Panel (54-0771-0008) ▾



Custom Configuration

- No parameters are available to the public at present.

Card Reader Module Configuration

4 - Card Reader (54-0771-0009) ▾


Associated Switch

Switch 1 ▾

Forward to Wiegand Output

Group 1 ▾

Custom Configuration



- **Associated switch** – set the number of the switch to be activated by tapping of a valid RFID card.
- **Forward to Wiegand output** - set a group of Wiegand outputs to which all the received RFID card IDs will be resent.

I/O Module Configuration


4 - I/O Module (54-0761-0006) ▾

Module Name

io1

Custom Configuration

name=io1



- **Module name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in **2N® Helios IP 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 Wiegand module is also equipped with one logical input and one logical output, which can be controlled via **2N® Helios IP Automation**.

5 - Wiegand Module (54-0811-0005) ▾

Module Name

Associated Switch
 ▾


Received Code Format
 ▾

Forward to Wiegand Output
 ▾

Transmitted Code Format
 ▾

Output Wiegand Group
 ▾

Custom Configuration



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

5.4 Services

Here is what you can find in this section:

- [5.4.1 Phone](#)
- [5.4.2 Streaming](#)
- [5.4.3 E-Mail](#)
- [5.4.4 Automation](#)
- [5.4.5 User Sounds](#)
- [5.4.6 Web Server](#)
- [5.4.7 Audio Test](#)

5.4.1 Phone

The screenshot shows the configuration interface for the Phone service. On the left, a sidebar under 'Services' lists 'Phone', 'Streaming', 'E-Mail', 'Automation', 'User Sounds', and 'Web Server'. The 'Phone' option is selected. The main area has tabs for 'SIP', 'Calls', 'Audio', and 'Video'. Under the 'SIP' tab, there are two sections: 'Intercom Identity' and 'Authentication'. The 'Intercom Identity' section contains three input fields: 'Display Name' (Main Entry), 'Phone Number (ID)' (111), and 'Domain' (192.168.1.10). The 'Authentication' section contains three fields: 'Use Authentication ID' (unchecked checkbox), 'Authentication ID' (greyed out text input), and 'Password' (empty text input). At the top right, there are links for 'Main Entry', 'CZ | EN', and 'Logout'.

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** 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** 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. 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 four tabs:

- **SIP** – 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

Intercom Identity ▾

Display Name	Main Entry
Phone Number (ID)	111
Domain	192.168.1.1

- **Display name** – set the name to be displayed as CLIP on the called party's

phone, in the login window and web interface start page.

- **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.

Authentication ▾

Use Authentication ID	<input type="checkbox"/>
Authentication ID	<input type="text"/>
Password	<input type="text"/>

- **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.

SIP Proxy ▾

Proxy Address	<input type="text" value="192.168.1.1"/>
Proxy Port	<input type="text" value="5060"/>

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

SIP Registrar ▾

Registration Enabled	<input type="checkbox"/>
Registrar Address	<input type="text" value="192.168.1.1"/>
Registrar Port	<input type="text" value="5060"/>
Registration Expires	<input type="text" value="120"/> [s]

- **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.

Advanced Settings ▾

SIP Transport Protocol	UDP
Trusted Certificate	None
User Certificate	None
Local SIP Port	5060
Send Keep Alive Packets	<input type="checkbox"/>
IP Address Filter Enabled	<input type="checkbox"/>
QoS DSCP Value	0
Starting RTP Port	5000
RTP Timeout	60

- **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.
- **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.
- **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).
- **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.

Calls

Incoming Calls ▾

Automatic Answer

Call Activation By Activation Code ▾

Activation Code

- **Automatic answer** – enable automatic answering of incoming calls. If this function is disabled, the intercom signals incoming calls by ringing and the user can answer them by pushing the * button on the numeric keypad.
- **Call activation** – select automatic or manual microphone, speaker or camera activation during an incoming call. The parameter is applied only if the **Automatic Answer** is enabled. If you select manual activation, enter the activation code, see below.
- **Activation code** – enter the call activation code via the IP phone numeric keypad to activate the microphone, speaker and camera if available. The parameter is applied only if the manual call activation is enabled.

Outgoing Calls ▾

Ring Time Limit [s]

Call Time Limit [s]

Dial Cycles Limit

- **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, you are advised to set a value higher than 20 s.
- **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.
- **Dial cycles limit** – set the maximum count of user deputy dial cycles if the user dialled by the Phone Book position number is inaccessible. The function helps you avoid deadlock if the **User Deputy** is set to the same value in the Phone Book.

Audio

Preferred Audio Codecs ▾

Codec 1	PCMU	▾
Codec 2	PCMA	▾
Codec 3	None	▾
Codec 4	None	▾

- **Codec 1–4** – set the order of audio codecs for call setup: G.711 (PCMA or PCMU), L16 or G.729. The order defines the codec priority, i.e. the first codec has the highest priority. 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.

DTMF Sending ▾

Sending Mode	Do not Send	▾
In-Band (Audio)	<input type="checkbox"/>	
RTP (RFC-2833)	<input checked="" type="checkbox"/>	
SIP INFO (RFC-2976)	<input type="checkbox"/>	

- **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.

DTMF Receiving ▾

In-Band (Audio) RTP (RFC-2833) SIP INFO (RFC-2976)

- **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.

Transmission Quality Settings ▾

QoS DSCP Value

0

Jitter Compensation

100ms

- **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.
- **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

Video Parameters ▾

Video Resolution

CIF (352x288)

Video Framerate

15 fps

Video Bitrate

512 kbps

- **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.

Preferred Video Codecs ▾

Codec 1	H.264	▾
Codec 2	H.263+	▾
Codec 3	H.263	▾
Codec 4	None	▾

- **Codec 1–4** – set the order of video codecs for call setup: G.711 (PCMA or PCMU), L16 or G.729. The order defines the codec priority, i.e. the first codec has the highest priority. Codec G.729 is available in selected intercoms only with a valid licence G.729.

Transmission Quality Settings ▾

QoS DSCP Value	0
Maximum Packet Size	1400

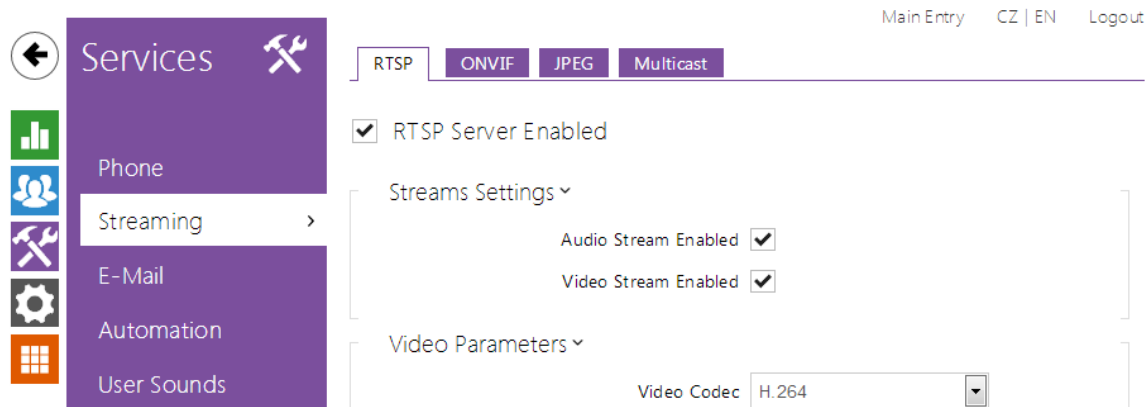
- **QoS DSCP value** – set the video RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.
- **Maximum packet size** – set the size limit for the video RTP packets to be sent.

Advanced SDP Settings ▾

H.264 Payload Type (1)	123
H.264 Payload Type (2)	124
H.263+ Payload Type	98
Polycom Compatibility Mode	<input type="checkbox"/>

- **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.

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:

- a. rtsp://ip_intercom_address/h264_stream
- b. rtsp://ip_intercom_address/mpeg_stream
- c. rtsp://ip_intercom_address/mjpeg_stream

RTSP Server Enabled

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

Streams Settings ▾

Audio Stream Enabled

Video Stream Enabled

- **Audio stream enabled** – enable offering of video stream while establishing connection with the RTSP server.
- **Video stream enabled** – enable offering of audio stream while establishing connection with the RTSP server.

Video Parameters ▾

Video Codec H.264 ▾

Video Resolution CIF (352x288) ▾

Video Framerate 15 fps ▾

Video Bitrate 512 kbps ▾

- **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.

Authorised IP Addresses ▾

IP Address 1	<input type="text" value="192.168.1.80"/>
IP Address 2	<input type="text" value="192.168.1.81"/>
IP Address 3	<input type="text"/>

- **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.

Transmission Quality Settings ▾

QoS DSCP Value	<input type="text" value="0"/>
UDP Unicast Enabled	<input type="checkbox"/>
Maximum Video Packet Size	<input type="text" value="1400"/>

- **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.

ONVIF

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

ONVIF Settings ▾

Discovery Mode	<input type="text" value="Discoverable"/>
----------------	---

- **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.

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):
 - 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 authorization for ONVIF

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

JPEG

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

- `http://intercom_ip_address/enu/sec/cameraWxH.jpg`

or (for MJPEG, HTTP Server Push):

- `http://intercom_ip_address/enu/sec/cameraWxH.jpg?fps=N`

where **W** and **H** specify image resolution (supported resolutions: 160x120, 320x240, 640x480, 176x144, 322x272, 352x288, 1280x960 – for 1MPix camera equipped models only) and **N** gives the count of snapshots per second (1 through 10).

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 Snapshots Download ▾

Snapshot Download Enabled

JPEG Compression Level ▾

- **Snapshot download enabled** – enable download of JPEG snapshots from any IP address without authentication.
- **JPEG compression level** – set the JPEG compression level (1–99). The recommended value is 85. The parameter affects the image size and quality.

SNOM Phone Support ▾

JPEG Video Activated by Call

JPEG Video Frame Rate 5 fps ▾

Some IP phones (SNOM 820/570) do not support video calls but are able to download and display JPEG 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 820/570 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 Audio Receiving ▾

Multicast Receiver Enabled Receive Address Receive Port 22222

Volume 0 dB ▾

- **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.

Multicast Audio Sending ▾

Multicast Sender Enabled Send to Address Send to Port 22222

- **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.

5.4.3 E-Mail

2N Helios IP Verso CZ | EN Logout

Services

Phone

Streaming

E-Mail >

Automation

User Sounds

E-Mail
SMTP

Basic Settings ▾

E-Mail Sending Mode

E-Mail Template ▾

Sender

Default Recipient

Message Subject

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 Phone Book. If the **E-Mail** parameter in the Phone Book 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

E-Mail

Basic Settings ▾

E-Mail Sending Mode

- **E-mail sending mode** – set the E-mail sending mode for no answer (missed call) or for all outgoing calls.

E-Mail Template ▾

Sender

Default Recipient

Message Subject

Message Body

```
<h1> Hello, $User$ </h1> <br>
<h2> You had a call at: $DateTime$ </h2>
<p>
<h2> The dialed number is
$DialNumber$</h2>
<p>
<b> This mail is generated automatically
by the $HeliosId$ device. Do not reply to
this please.
</b>
```

- **Sender** – enter the sender's E-mail.
- **Default recipient** – typically, the intercom sends E-mail messages to the user addresses included in the Phone Book. If the Phone Book E-mail parameter is not completed, the messages are sent to the address included in this parameter. If a user is not included in the Phone Book or this field, no E-mail is sent.
- **Message subject** – set the E-mail subject to be sent.
- **Message 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:
 - a. \$User\$ Called username
 - b. \$DateTime\$ Current date and time
 - c. \$DialNumber\$ Called number
 - d. \$HeliosId\$ Intercom identification

E-Mail Attachment ▾

Attach Snapshots

Number of Snapshots

Snapshot Resolution

- **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.

SMTP

SMTP Service Enabled

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

SMTP Server Settings ▾

Server Address

Server Port

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

SMTP Server Login ▾

Username

Password

User Certificate ▾

- **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.

Advanced Settings ▾

Deliver In ▾

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

5.4.4 Automation

Main Entry CZ | EN Logout

Function 1 Function 2 Function 3 Function 4 Function 5

Function Enabled

Function State Function State **Running**

Function Definition

ID	OBJECT TYPE	PARAMETERS
1	Event.Timer	period=120

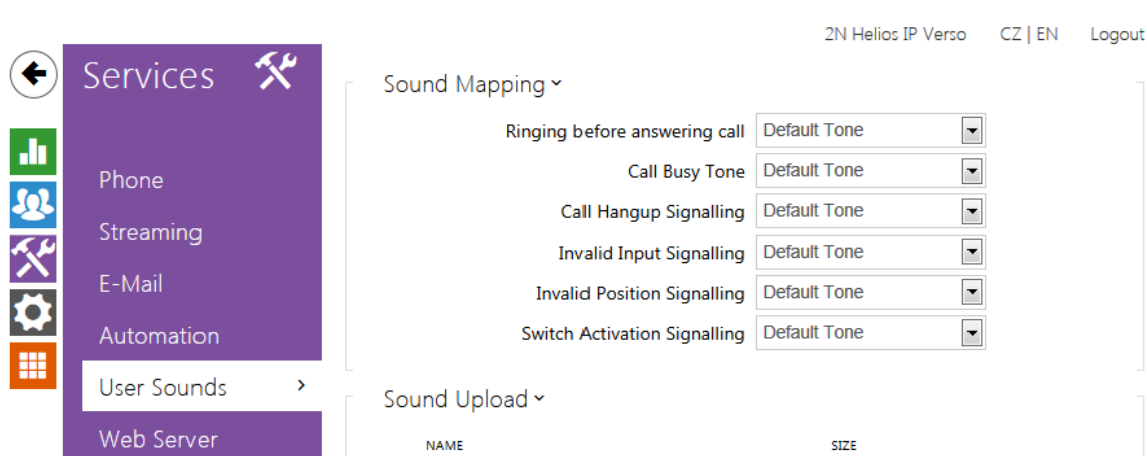
The **2N® Helios IP** intercom provides highly flexible setting options to satisfy variable user needs. There are situations in which the standard configuration settings (switch or call modes, e.g.) are insufficient and so **2N® Helios IP** offers **2N® Helios IP Automation**, a special programmable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

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

Note

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

5.4.5 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:

- a. **Ringing before answering call**
- b. **Call busy tone**
- c. **Call hang-up**
- d. **Invalid input**
- e. **Invalid Phone Book position**
- f. **Switch activation**

You can either completely mute the above-mentioned sounds or replace them with a sound file of your own simply recorded 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 128 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

Sound Mapping ▾































Ringling before answering call	Default Tone ▾
Call Busy Tone	Default Tone ▾
Call Hangup Signalling	Default Tone ▾
Invalid Input Signalling	Default Tone ▾
Invalid Position Signalling	Default Tone ▾
Switch Activation Signalling	Default Tone ▾

- **Ringling before answering call** – set the sound to be played before answering an incoming call (intercom ring tone).
- **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 is entered (switch/user/profile activation).
- **Invalid position signalling** – set the sound to be played when a quick dial button is pressed but the corresponding Phone Book 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.

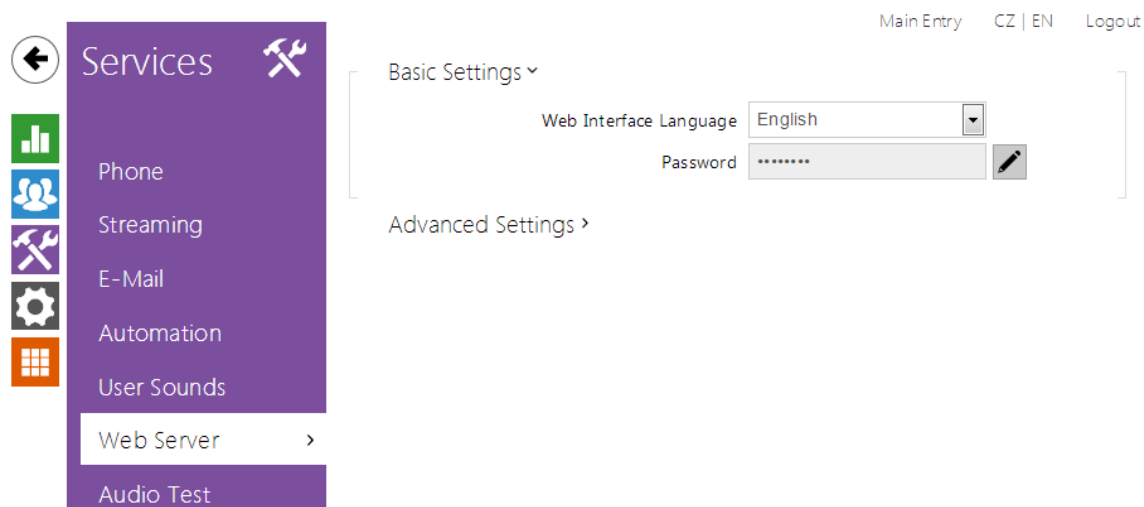
You can record up to 10 user sound files into the intercom and assign names to them for convenience.

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).

Sound Upload ▾

	NAME	SIZE	
1	<input type="text" value="Sound 1"/>	8044 B	  
2	<input type="text" value="User sound 2"/>	4720 B	  
3	<input type="text" value="User sound 3"/>	0 B	  
4	<input type="text" value="User sound 4"/>	0 B	  
5	<input type="text" value="User sound 5"/>	0 B	  
6	<input type="text" value="User sound 6"/>	0 B	  
7	<input type="text" value="User sound 7"/>	0 B	  
8	<input type="text" value="User sound 8"/>	0 B	  
9	<input type="text" value="User sound 9"/>	0 B	  
10	<input type="text" value="User sound 10"/>	0 B	  

5.4.6 Web Server



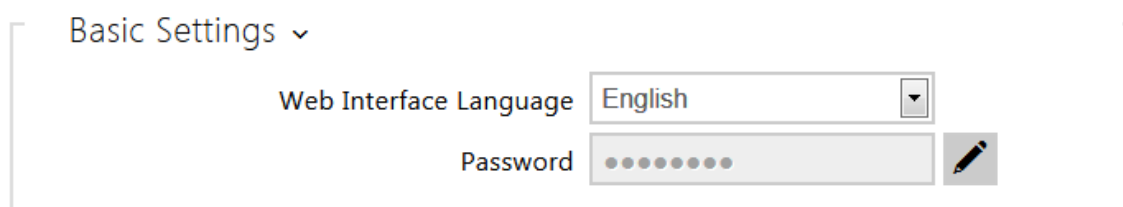
You can configure your **2N® Helios IP** intercom using a standard browser which accesses the integrated web server. Use the secured HTTPS protocol for communication between the browser and intercom. Having accessed the intercom, enter the login name and password. The default login name and password 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:

- JPEG snapshot/MJPEG video download; refer to Streaming.
- ONVIF protocol for video streaming, refer to Streaming.
- HTTP commands for switch control, refer to Switches.
- 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



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

Advanced Settings ▾

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
HTTPS User Certificate	<input type="text" value="Self Signed"/> ▾
Remote Access Enabled	<input checked="" type="checkbox"/>

- **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 **Self Signed** setting, in which the certificate automatically generated upon the first intercom power up is used.
- **Remote access enabled** – enable remote access to the intercom web server from off-LAN IP addresses.

5.4.7 Audio Test

Main Entry CZ | EN Logout

Services

- Phone
- Streaming
- E-Mail
- Automation
- User Sounds
- Web Server
- Audio Test >

Audio Test Enabled

Test Settings ▾

Test Period

Test Start Time

Test Result ▾

Test Status **Idle**

Last Test Time -

Last Test Result **Unknown**

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 **2N® Helios IP Automation**.

Note

- The audio test is available with the Gold or Enhanced Audio licence only.

List of Parameters

Audio Test Enabled

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

Test Settings ▾

Test Period	<input type="text" value="Daily"/>
Test Start Time	<input type="text" value="9:47"/>
	<input type="button" value="Test Now"/>

- **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 Result ▾

Test Status **Idle**

Last Test Time -

Last Test Result **Unknown**

- **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.

5.5 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

The screenshot shows the configuration interface for a 2N Helios IP intercom. On the left, a sidebar menu is open to the 'Network' section. The main area has three tabs: 'Basic', '802.1x', and 'Trace'. The '802.1x' tab is selected. Below the tabs, there is a checkbox for 'Use DHCP Server' which is currently unchecked. A 'Manual Settings' section is expanded, containing several input fields:

Static IP Address	192.168.33.79
Network Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	192.168.23.5
Secondary DNS	

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.

Manual Settings ▾

Static IP Address	<input type="text" value="192.168.23.111"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Primary DNS	<input type="text" value="192.168.23.5"/>
Secondary DNS	<input type="text"/>

- **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.

NAT Settings ▾

External IP Address	<input type="text" value="172.16.26.11"/>
---------------------	---

- **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.

802.1x

Device Identity ▾

Device Identity	<input type="text"/>
-----------------	----------------------

- **Device identity** – username (identity) for authentication via EAP-MD5 and EAP-TLS.

MD5 Authentication ▾

MD5 Authentication Enabled Password

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

TLS Authentication ▾




TLS Authentication Enabled Trusted Certificate User Certificate

- **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.




ⓘ Poznámka

- 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.

Packet Capture Status ▾

Current State **STOPPED**Buffer Size **4194304 B**Buffer Utilisation **0 B**Number of Captured Packets **0**Packet Capture Control   

5.5.2 Date and Time

2N Helios IP Verso CZ | EN Logout

System

- Network
- Date & Time**
- Licence
- Certificates
- Auto Provisioning

Current Time ▾

Current Intercom Time **Wed, 9 Oct 2013 11:32:00 UTC**

Time Zone ▾

Time Zone (GMT+01:00) Europe/Paris ▾

Time Zone Rule

NTP Server ▾

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 **2N[®] Helios IP** HTTP API, etc.).

Practically, the intercom real-time circuit accuracy is approximately $\pm 0,005\%$, 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

Current Time ▾

Current Intercom Time **Wed, 9 Oct 2013 11:32:00 UTC**

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

Time Zone ▾

Time Zone (GMT+01:00) Europe/Paris ▾

Time Zone Rule

- **Time zone** – set the time zone for the installation site to define time shifts and winter/summer time transitions.
- **Time zone rule** – if the 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**.

NTP Server ▾

Use NTP Server

NTP Server Address time.nist.gov

- **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.

5.5.3 Licence

2N Helios IP Verso CZ | EN Logout

The screenshot shows the 'System' menu on the left with 'Licence' selected. The main content area is divided into two sections:

- Licence Settings**: Contains a 'Licence Key' input field and 'Licence Key Valid **NO**'.
- Licence Status**: Displays the following information:
 - Current Licence **Gold**
 - Enhanced Security **YES**
 - Enhanced Audio **YES**
 - Enhanced Video **YES**
 - Enhanced Integration **YES**

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 Settings ▾

Licence Key

Licence Key Valid **NO**

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

Licence Status ▾

Current Licence **Gold**

Enhanced Security **YES**

Enhanced Audio **YES**

Enhanced Video **YES**

Enhanced Integration **YES**

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

Security licence are available.

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

Trial Licence ▾

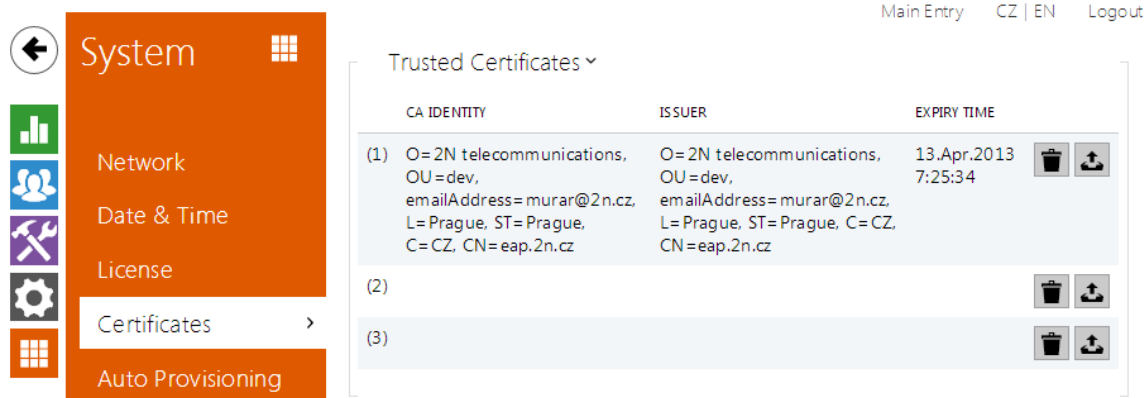
Trial Licence State **Expired**

Licence Expiry **0 hours**

Activate Trial Licence

- **Trial licence state** – check the trial licence state (non-activated, activated, expired).
- **Licence expiry** – check the remaining time of the trial licence validity.

5.5.4 Certificates



The screenshot shows the 'System' menu with 'Certificates' selected. The 'Trusted Certificates' window displays the following table:

CA IDENTITY	ISSUER	EXPIRY TIME		
(1) O=2N telecommunications, OU=dev, emailAddress=murar@2n.cz, L=Prague, ST=Prague, C=CZ, CN=eap.2n.cz	O=2N telecommunications, OU=dev, emailAddress=murar@2n.cz, L=Prague, ST=Prague, C=CZ, CN=eap.2n.cz	13.Apr.2013 7:25:34	🗑️	📄
(2)			🗑️	📄
(3)			🗑️	📄

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:

- 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.

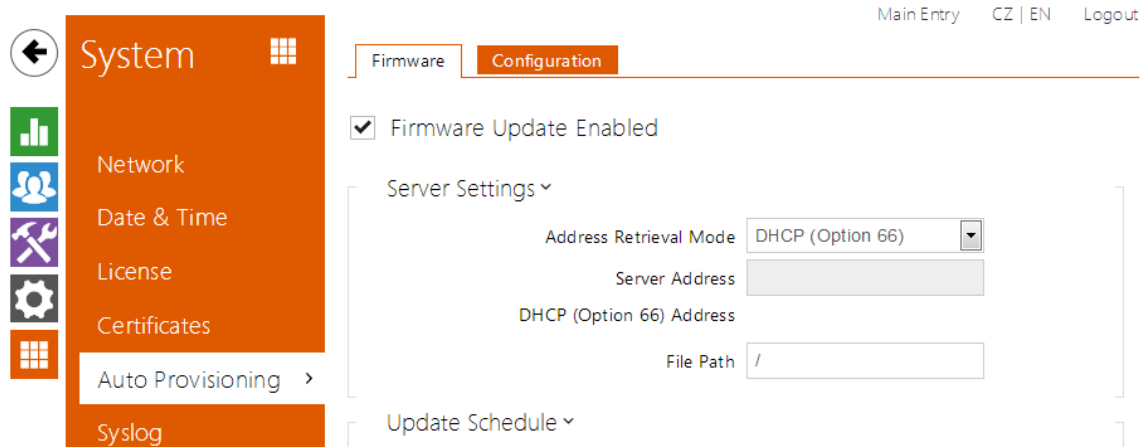
Refer to the tables below for the current list of trusted and user certificates:

Trusted Certificates ▾	
CA IDENTITY	
(1)	O=2N telecommunications, OU=dev, emailAddress=murar@2n.cz, L=Prague, ST=Prague,
(2)	
(3)	

User Certificates ▾	
CA IDENTITY	ISSUER
(1)	C=CZ, ST=Prague, O=2N telecommunications, OU=dev, CN=client.eap.cz O=2N telecon
(2)	
(3)	

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

5.5.5 Auto Provisioning



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:

- a. hip**MODEL**-firmware.bin – intercom firmware
- b. hip**MODEL**-common.xml – common configuration for all intercoms of one model
- c. hip**MODEL-MACADDR**.xml – specific configuration for one intercom

MODEL in the filename specifies the intercom model:

- a. **v** – **2N® Helios IP Vario**
- b. **f** – **2N® Helios IP Force**
- c. **sf** – **2N® Helios IP Safety**
- d. **u** – **2N® Helios IP Uni**
- e. **ak** – **2N® Helios IP Audio Kit**
- f. **vk** – **2N® Helios IP Video Kit**

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.

Poznámka

- 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

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

Server Settings ▾

Address Retrieval Mode

Server Address

DHCP (Option 66) Address

File Path

- **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) address** – check the server address retrieved via the DHCP Option 66.
- **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.

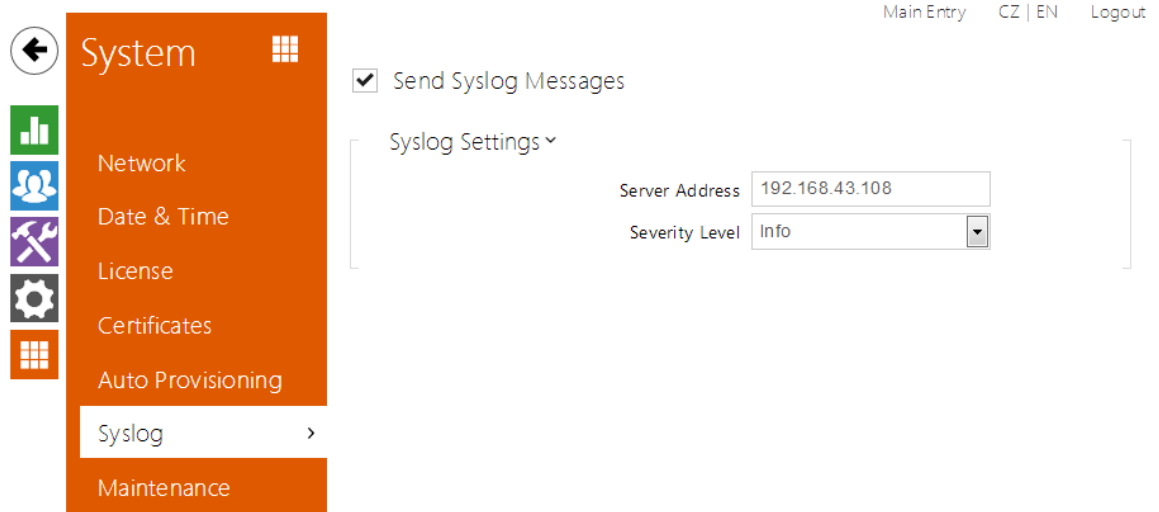
Update Schedule ▾

At Boot Time	Check for Update ▾
Update Period	Weekly ▾
Update At	01:00
Next Update At	Disabled

Update Now

- **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.

5.5.6 Syslog

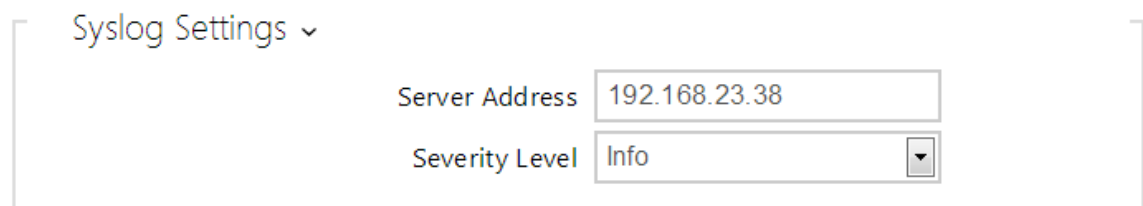


The **2N® Helios IP** intercoms allow you to send system messages to the Syslog server including relevant information on the device states and processes for recording, analysis and audit. It is unnecessary to configure this service for common intercom operation.

List of Parameters

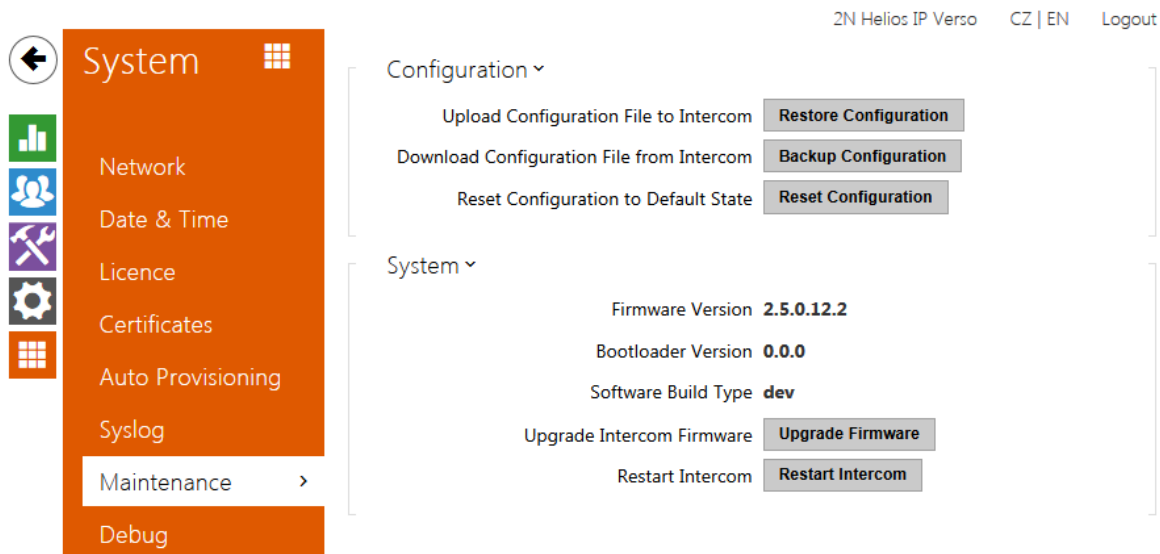
Send Syslog Messages

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



- **Server address** – set the IP 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.
- **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.

6. Supplementary Information

Zde je přehled toho, co v kapitole naleznete:

- [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 2002/96/EC of the European Parliament and of the Council of 27 January 2003 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

Tel.: +420 261 301 500, Fax: +420 261 301 599

E-mail: sales@2n.cz

Web: www.2n.cz

1759v1