2N LTE Verso Configuration Manual

v.2.49

www.2n.com

Content:

1. Product Overview

The **2N LTE door intercoms** are a successful substitute for classic Speakerphone bell button panels and complex circuitry of bells and domestic phones where structured cabling cannot be deployed. The intercoms render more sophisticated and extensive services than standard domestic phones. The intercom is easy to install - all you have to do is insert a SIM card, connect a power supply and set necessary parameters via the My2N portal.

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

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

Some **2N LTE intercom** models are equipped with a numeric keypad, which can be used as a code.

The **2N LTE 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 LTE intercoms** are 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. It is always recommended that the 2N® Security Relay (Part No. 9159010) is used for increased security.

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

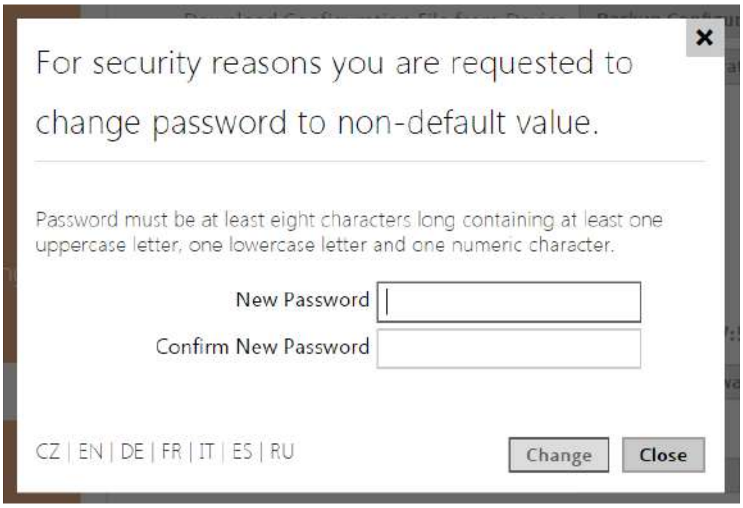
Device Setting

Make sure that your device is properly installed and connected to My2N before logging in to the intercom configuration interface. Log in to My2N at https://my2n.com and add your intercom to the **2N$^{®}$ Remote Configuration**. You have to enter your My2N security code during login - find the code in the card provided in the intercom package. Get access to the intercom web configuration interface via the 2N$^{®}$ Remote Configuration.

Use the name **admin** and password **2n** (i.e. default reset password) for your first login to the configuration interface.

We recommend you to change the default password upon your first login.

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



For security reasons you are requested to change password to non-default value.

Password must be at least eight characters long containing at least one uppercase letter, one lowercase letter and one numeric character.

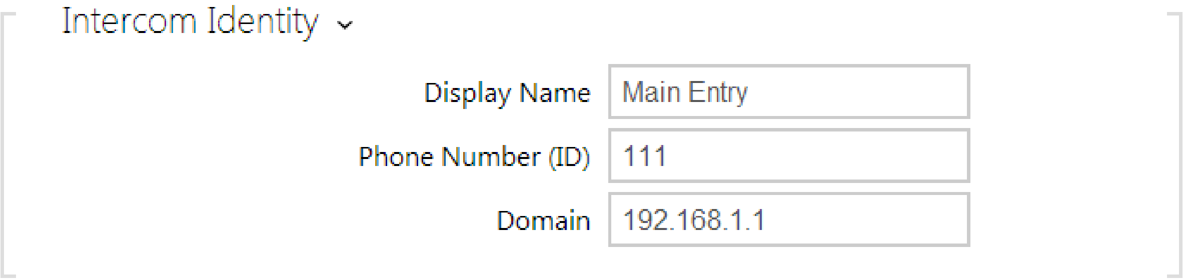
Remember the new password well or put it down just in case. Because if you forget the password, you will have to reset the intercom to default values (refer to the Installation Manual of your intercom model) and lose all your current configuration changes.

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

The intercom is automatically configured for making calls via the My2N 2N$^{®}$ Mobile Video service. To use another VoIP infrastructure, set the necessary parameters in the **Services / Phone / SIP** menu.

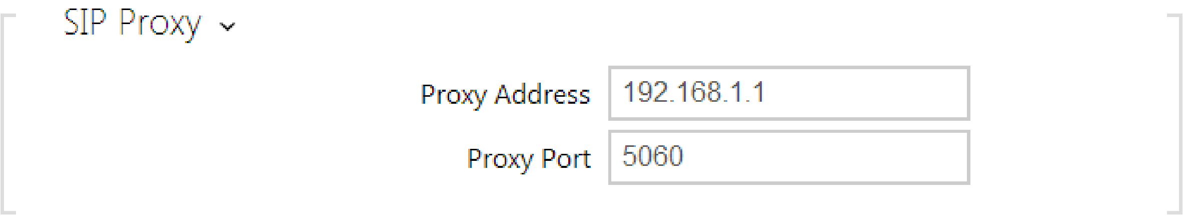


Intercom Identity

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

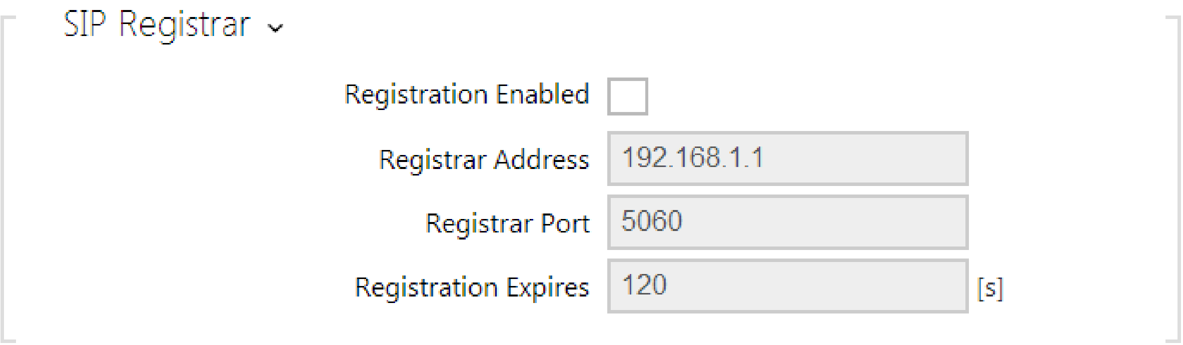
- **Display name** – set the name to be displayed as CLIP on the called party's phone, in the login window and on the web interface start page.
- **Phone number (ID)** – set the intercom phone number (or another unique ID composed of characters and digits) to identify the intercom uniquely in calls and 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: 192.168.1.1
Proxy Port: 5060

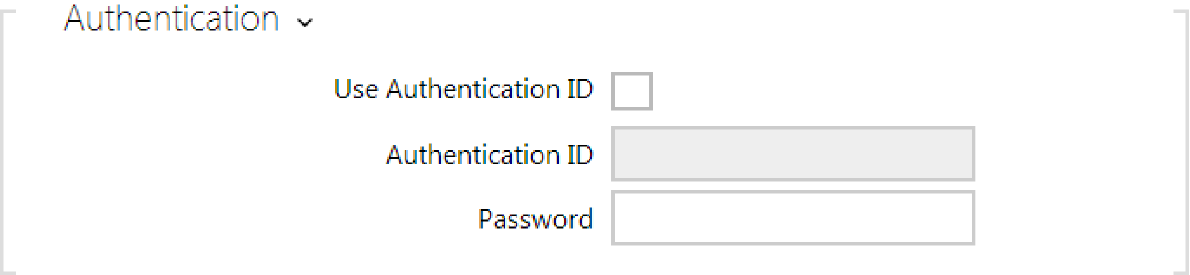


SIP Registrar

Registration Enabled: ☐
Registrar Address: 192.168.1.1
Registrar Port: 5060
Registration Expires: 120 [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:

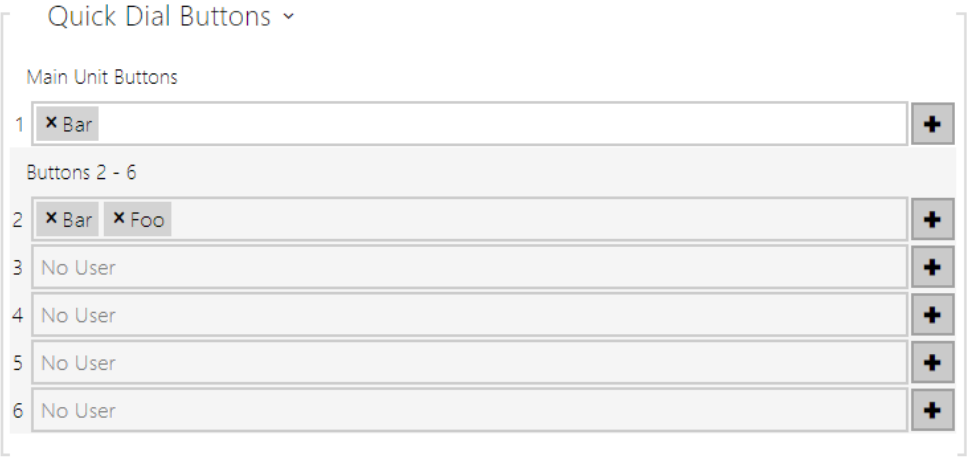


- **Password** – enter the password for intercom authentication.

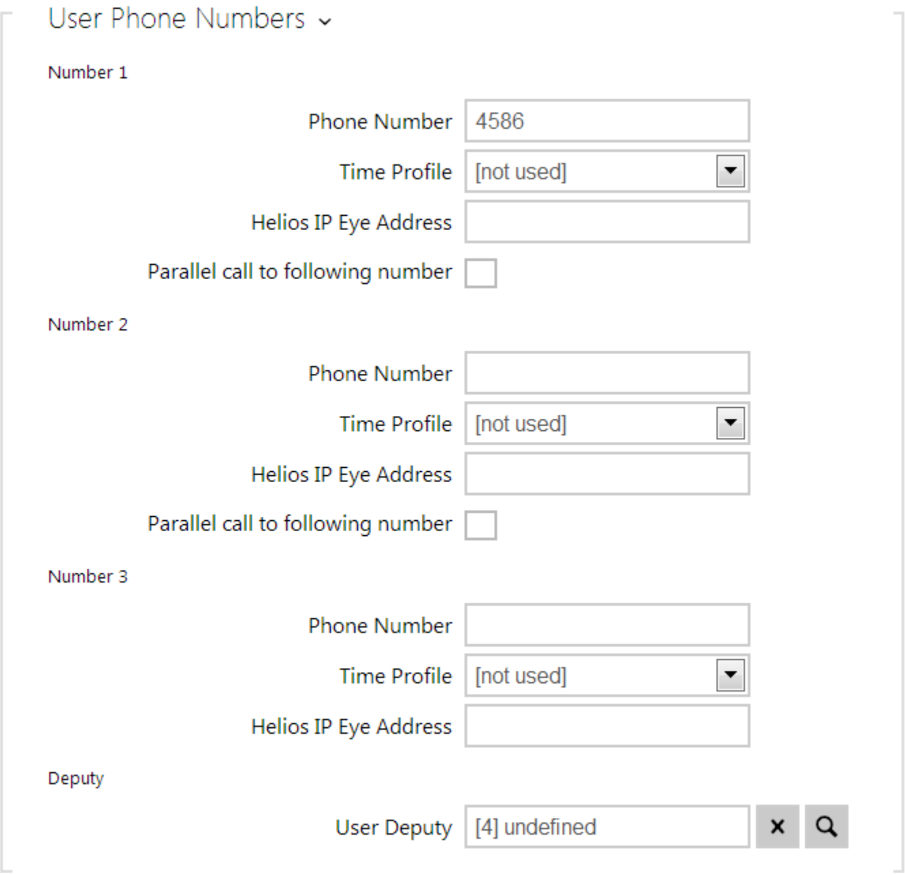
Quick Dial Button Settings

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

In the **Hardware / Buttons** menu is displayed the list of all potentially available intercom buttons including those physically absent. In some intercom models, the button list is divided into 8/5-item groups corresponding to the button extending modules. Click ✚, select the user and press Add to add a user to the editing field. To search a user in the list, use the fulltext field and the username. One quick dial button can be shared by multiple users.



1 × Bar
2 × Bar × Foo
3 No User
4 No User
5 No User
6 No User



User Phone Numbers ⌄

Number 1

Phone Number: 4586

Time Profile: [not used]

Helios IP Eye Address:

Parallel call to following number ☐

Number 2

Phone Number:

Time Profile: [not used]

Helios IP Eye Address:

Parallel call to following number ☐

Number 3

Phone Number:

Time Profile: [not used]

Helios IP Eye Address:

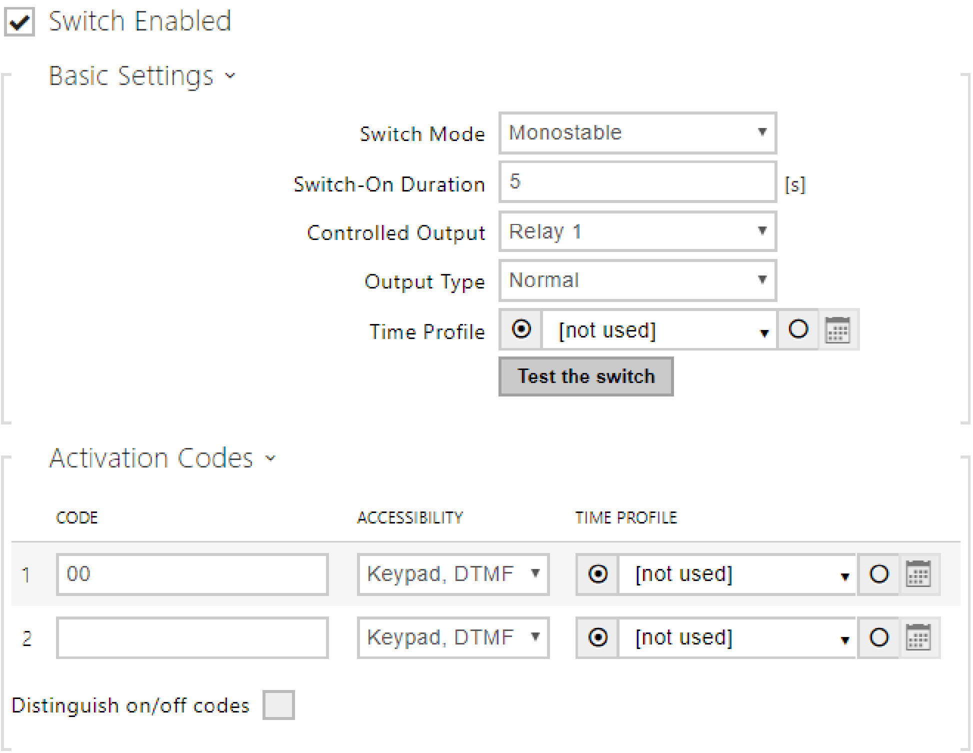
Deputy

User Deputy: [4] undefined

You can also use the **2N LTE 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 LTE** 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

Basic Settings

Switch Mode: Monostable

Switch-On Duration: 5 [s]

Controlled Output: Relay 1

Output Type: Normal

Time Profile: [not used]

Activation Codes

	CODE	ACCESSIBILITY	TIME PROFILE
1	00	Keypad, DTMF	[not used]
2		Keypad, DTMF	[not used]

Distinguish on/off codes ☐

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

Here is what you can find in this section:

- 3.1 Function Licensing

License	Features	2N IP Style	2N IP Verso 2.0	2N IP Verso	2N LTE Verso	2N IP One	2N IP Solo	2N IP Base	2N IP Force	2N IP Safety	2N IP Vario	2N IP Vario with display	2N IP Uni	2N IP Video Kit	2N IP Audio Kit
Enhanced Audio (Standard license part of the device)	User sounds	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
	Automatic audio test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
	Noise detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Enhanced Video (Included in Gold license)	Audio/video streaming (RTSP Server)	★	★	★	★ *	★	★	★	★	★	★	✓	✗	★	★
	External camera support	★	★	★	★ *	★	★	★	★	★	★	✓	✗	★	✗

License	Features	2N IP Style	2N IP Verso 2.0	2N IP Verso	2N LTE Verso	2N IP One	2N IP Solo	2N IP Base	2N IP Force	2N IP Safety	2N IP Vario	2N IP Vario with display	2N IP Uni	2N IP Video Kit	2N IP Audio Kit
	ONVIF support	★	★	★	★ *	★	★	★	★	★	★	✓	✗	★	✗
	PTZ support	★	★	★	★	★	★	★	★	★	★	✓	✗	★	✗
	Motion detection support	★	★	★	★	★	★	★	★	★	★	✓	✗	★	✗
Enhanced Integration (Included in Gold license)	Advanced switch setting options	★	★	★	★	★	★	★	★	★	★	✓	✗	★	★
	HTTP API	✓	✓	✓	✓ *	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
	Automation function	★	★	★	★	★	★	★	★	★	★	✓	✗	★	★

License	Features	2N IP Style	2N IP Verso 2.0	2N IP Verso	2N LTE Verso	2N IP One	2N IP Solo	2N IP Base	2N IP Force	2N IP Safety	2N IP Vario	2N IP Vario with display	2N IP Uni	2N IP Video Kit	2N IP Audio Kit
	E-mail sending (SMTP client)	★	★	★	★	★	★	★	★	★	★	✓	✗	★	★
	Automatic update (TFTP/HTTP client)	★	★	★	★	★	★	★	★	★	★	✓	✗	★	★
	FTP client	★	★	★	★	★	★	★	★	★	★	✓	✗	★	★
	SNMP client	★	★	★	★ *	★	★	★	★	★	★	✓	✗	★	★
	TR-069	★	★	★	★	★	★	★	★	★	★	✓	✗	★	★
	Synergis	★	★	★	★ *	★	★	★	★	★	★	✓	✗	★	★
	Lift Control	★	★	★	✗	✗	✗	✗	★	★	★	✓	✗	✗	✗

License	Features	2N IP Style	2N IP Verso 2.0	2N IP Verso	2N LTE Verso	2N IP One	2N IP Solo	2N IP Base	2N IP Force	2N IP Safety	2N IP Vario	2N IP Vario with display	2N IP Uni	2N IP Video Kit	2N IP Audio Kit
Enhanced Security (Standard license part of the device)	802.1x support	✓	✓	✓	✕	✓	✓	✓	✓	✓	✓	✓	✕	✓	✓
	SIPS (TLS) support	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕	✓	✓
	Switch Blocking by Tamper	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕	✓	✓
	SRTP support	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕	✓	✓
	Silent alarm	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕	✓	✓
	Limit unsuccessful access attempts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕	✓	✓

License	**Features**	**2N IP Style**	**2N IP Verso 2.0**	**2N IP Verso**	**2N LTE Verso**	**2N IP One**	**2N IP Solo**	**2N IP Base**	**2N IP Force**	**2N IP Safety**	**2N IP Vario**	**2N IP Vario with display**	**2N IP Uni**	**2N IP Video Kit**	**2N IP Audio Kit**
	Anti-Passback	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗
	Scrambled keypad	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
NFC (Standard license part of the device)	NFC support	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
InformaCast	InformaCast support	★	★	★	★ *	★	★	★	★	★	★	★	✗	★	★

✓ – included in device

★ – licensed function to be purchased additionally

✗ – unavailable

*) The service availability depends on the mobile provider's network configuration.

⚠ **Note**

- The license overview does not apply to the US, Canada, Mexico, Caribbean, and Central and South America.

3.1 Function Licensing

Feature Licensing

A standard license included in the device is mostly sufficient for a common use of the 2N LTE intercom. In addition, the 2N LTE intercom can be extended to include functions that are subject to a paid license.

License Types

Some 2N IP intercom functions are unavailable until a valid license key is entered (refer to the License subsection). The following types of licenses are available:

- NFC (included in device)
- Enhanced Audio (included in device)
- Enhanced Security (included in device)
- Gold (Part No. 9137909)
- InformaCast (Part No. 9137910, Axis Part No. 01381-001)

ⓘ **Info**

- The InformaCast license allows the SingleWire InformaCast protocol to be used.

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

Function	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	Licence
User sounds	•						(included in device)
Automatic audio test	•						(included in device)
Noise detection	•						(included in device)
Audio/video streaming (RTSP Server)		•					GOLD
External IP camera support		•					GOLD
ONVIF support		•					GOLD
PTZ function support		•					GOLD
Motion detection support		•					GOLD
Extended switch setting options			•				GOLD
HTTP API (see note below)			•				(included in device)
Automation functions			•				GOLD
E-mail sending (SMTP Client)			•				GOLD

Function	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	Licence
Automatic update (TFTP/HTTP Client)			•				GOLD
FTP client			•				GOLD
SNMP client			•				GOLD
TR-069			•				GOLD
802.1x support				•			(included in device)
SIPS (TLS) support				•			(included in device)
SRTP support				•			(included in device)
Silent Alarm				•			(included in device)
Limit unsuccessful access attempts				•			(included in device)
Switch Blocking				•			(included in device)
Scrambled keypad				•			(included in device)
NFC support					•		(included in device)
InformaCast support						•	InformaCast
Anti-passback				•			(included in device)

Function	Enhanced Audio	Enhanced Video	Enhanced Integration	Enhanced Security	NFC	InformaCast	Licence
Genetec Synergis			•				GOLD

What other products follow this license scheme?

2N IP intercoms, 2N® SIP Audio Converter, 2N® SIP Speaker and **2N® SIP Speaker Horn**, which already come with preloaded Gold license, so the only possible upgrades is InformaCast.

How do I get the license?

Licenses are generated by 2N according to the particular serial number. After you decide which license you want, you need to get the serial number of your unit and contact your distributor for the license key.

The license itself comes as a key, alphanumeric string, so it can be easily sent via email and copied and pasted into the intercom.

Licenses are not limited in time. Once you have a license, you have it for good.

In order to activate the license, you need to log in to the intercom web interface and paste the license key into the System / License field. When you click Save, the licensed features are immediately activated.

Licenses can be downloaded automatically in the System / License menu.

✓ **Tip**

FAQ: Lisense for 2N IP/LTE intercoms – How to get it

Can I have a demo lisence?

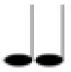
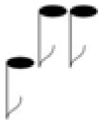
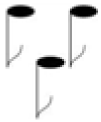
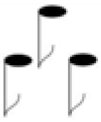
Yes, there is an option for an 800-hour trial Gold license period during which you can try the licensed features. By default, this demo is disabled - enable it via the web interface of the particular intercom in the System / License menu. There is a countdown timer showing the remaining time after which all the licensed features will be disabled again.

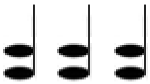
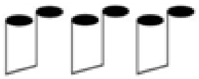
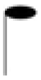
4. Signalling of Operational Statuses

2N LTE intercom 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.

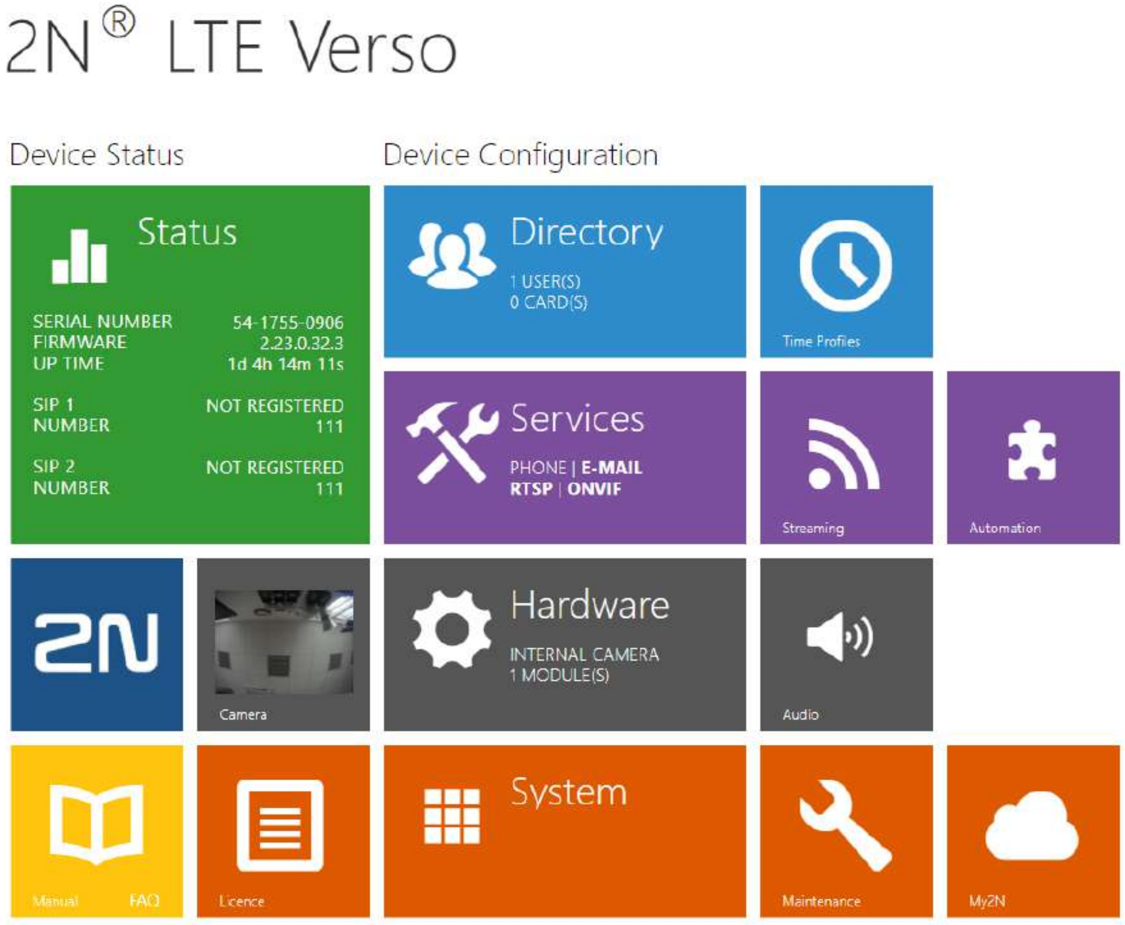
Note

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

Tone	Meaning
	**Call prolongation confirmation signalling** Calls are time-limited in **2N LTE intercoms** for security reasons (protection against blocking). Refer to the Miscellaneous subsection for details.
	**Internal application launched** The internal application is launched upon **2N LTE intercom** power up or restart. A successful launch is signalled by this tone combination.
	**Connected to data network, IP address received** **2N LTE intercom** logs in upon the internal application launch. A successful network login is signalled by this tone combination.
	**Disconnected from network, IP address lost** This tone signals data network disconnection from **2N LTE intercom**. Disconnection is signalled by this tone combination.

Tone	Meaning
	**Invalid telephone number or invalid switch activation code** **2N LTE intercom** allows the user to dial an extension number directly using the keypad or enter the door unlocking code. An invalid code is signalled by this tone sequence.
	**Default reset of network parameters** Upon power up, a 30 s timeout is set for the default reset code entering. Refer to the Device Configuration subsection in the **2N LTE intercom** Installation Manual for details.
	Call end signalling **2N LTE intercom** enables the user to set a call end timeout to avoid call blocking. Press a key on your VoIP phone to extend the call time during this timeout.
	**Connected VoIP phone** This short tone signals successful connection between a VoIP phone and **2N LTE intercom**.

5. Intercom Configuration



SERIAL NUMBER 54-1755-0906
FIRMWARE 2.23.0.32.3
UP TIME 1d 4h 14m 11s
SIP 1 NUMBER NOT REGISTERED 111
SIP 2 NUMBER NOT REGISTERED 111

Web Configuration Interface Login

The device **2N LTE Verso** is configured via the web configuration interface. You have to know the device IP address for access, which is possible only if the public IP address service is active on the SIM card. The default web configuration interface access option is the **My2N**.

The device automatically connects to the **My2N** portal after logging into the LTE mobile data network. Log in to **My2N** at https://my2n.com by adding the device to your account. The **2N Mobile Video** service helps you make basic settings and set up calls to mobile phones or 2N answering units. The **2N Remote Configuration** service also makes the device web configuration interface available.

Start Screen

The start screen is an introductory overview screen displayed upon login to the intercom web interface. Use the back arrow ← in the left-hand upper corner of the following web interface pages to return to this screen anytime.

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

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

Configuration Menu

The **2N LTE intercom** configuration includes 5 main menus: **State**, **Directory**, **Calling, Hardware**, **Services** and **System** including submenus; see below.

Status

- **Device** – essentials on the intercom
- **Services** – information on active services and their states
- **License** – current states of licenses and available intercom functions
- **Access Log** – last 10 access logs
- **Call Logs** – last 20 accomplished calls
- **Events** – last 500 events recorded by the device

Directory

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

Hardware

- **Switches** – electric lock, lighting, etc. settings
- **Audio** – audio, signalling, etc. volume control, microphone parameters
- **Camera** – internal camera, external IP camera settings
- **Keypad** – button and keypad settings
- **Buttons** - user speed dial settings
- **Backlight** – backlight intensity setting

- **Display** – basic display settings
- **Card Reader** – card reader, Wiegand interface settings
- **Digital Inputs** – digitial input settings
- **Extenders** – **2N® LTE Verso** extender settings

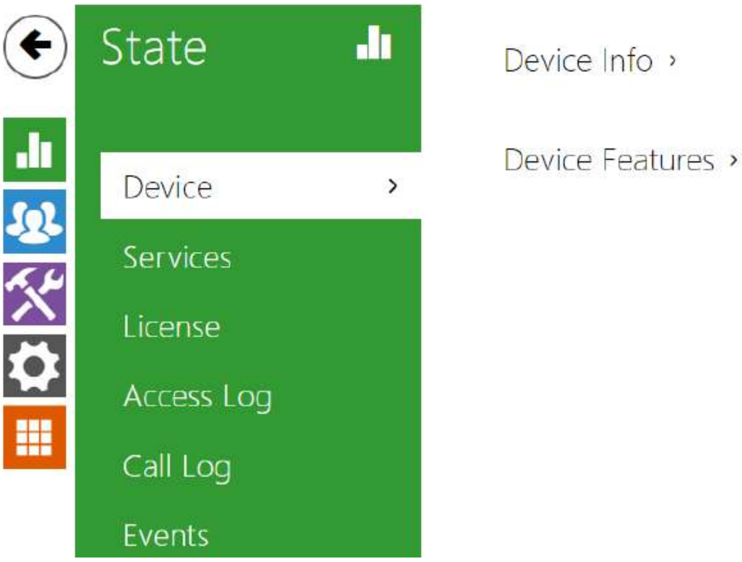
Services

- **Phone** – telephone and SIP connection settings
- **Access Control** – arrival/departure rule 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
- **HTTP API** – HTTP API authorisation settings
- **User Sounds** – user sound settings and upload
- **Web Server** – web server and access password settings
- **Audio Test** – automatic audio test settings
- **SNMP** – SNMP settings

System

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

5.1 Status

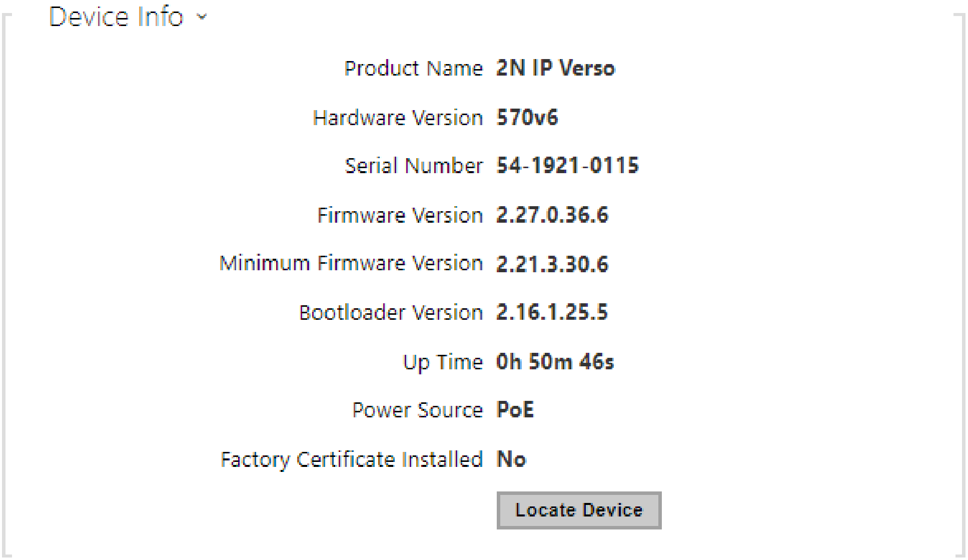


The **Status** menu provides clear status and other essential information on the intercom. The menu is divided into five tabs: **Device**, **Services, Access Log, Call Log** and **Events**.

Locate device – optical and acoustic signalling of a device. Note: Optical signalling is possible only if the device is equipped with control backlight (Verso, Base, Vario, Force, Safety and Uni). If a speaker is not integrated in the device, make sure than an external speaker is connected (Audio Kit and Video Kit) to use sound signalling.

Device

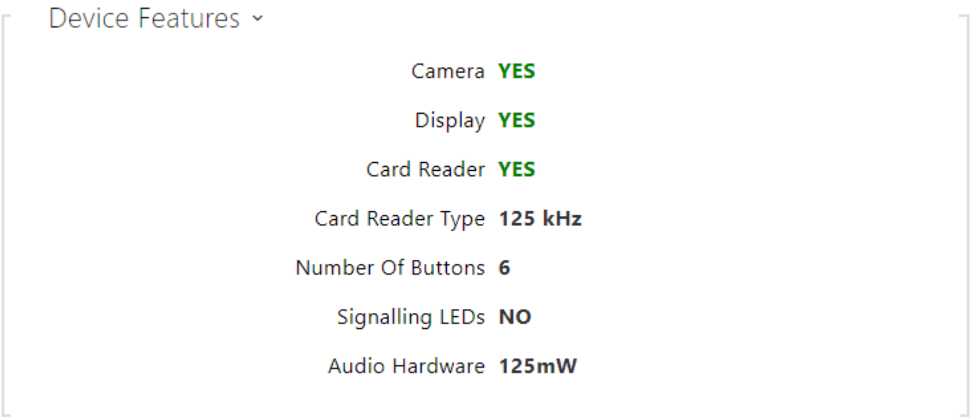
The **Device** tab displays basic information on the intercom model, its features, firmware and bootloader versions and so on.



Device Info

Product Name	2N IP Verso
Hardware Version	570v6
Serial Number	54-1921-0115
Firmware Version	2.27.0.36.6
Minimum Firmware Version	2.21.3.30.6
Bootloader Version	2.16.1.25.5
Up Time	0h 50m 46s
Power Source	PoE
Factory Certificate Installed	No

- **Factory Certificate Installed** – specify the user cerificate and private key to be used for verifying the intercom authorisation to communicate with the third party device server.
- **Locate device** – optical and acoustic signalling of a device. Optical signalling is possible only if the device is equipped with control backlight (**2N® IP Verso**, **2N® IP Solo**, **2N® IP Base**, **2N® IP Vario**, **2N® IP Force**, **2N® IP Safety** a **2N® IP Uni**). If a speaker is not integrated in the device, make sure than an external speaker is connected (**2N® IP Audio Kit** and **2N® IP Video Kit**) to use sound signalling.

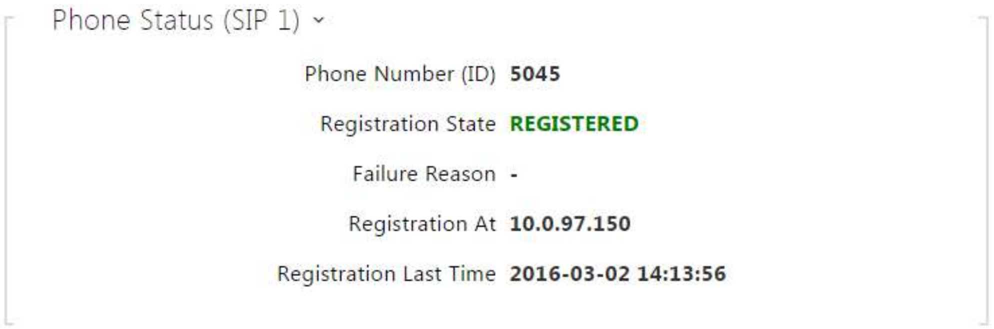


Device Features

Camera	YES
Display	YES
Card Reader	YES
Card Reader Type	125 kHz
Number Of Buttons	6
Signalling LEDs	NO
Audio Hardware	125mW

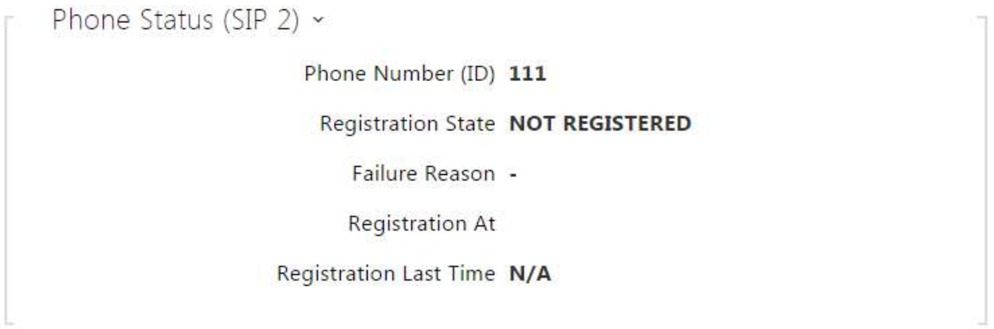
Services

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



Phone Status (SIP 1)

Phone Number (ID)	5045
Registration State	REGISTERED
Failure Reason	-
Registration At	10.0.97.150
Registration Last Time	2016-03-02 14:13:56

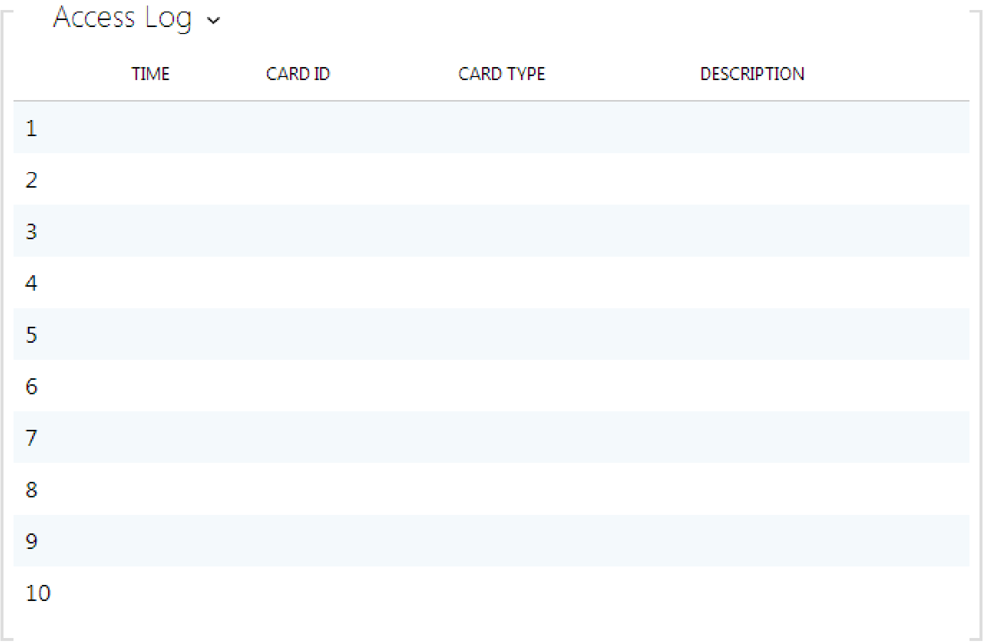


Phone Status (SIP 2)

Phone Number (ID)	111
Registration State	NOT REGISTERED
Failure Reason	-
Registration At	
Registration Last Time	N/A

Access Log

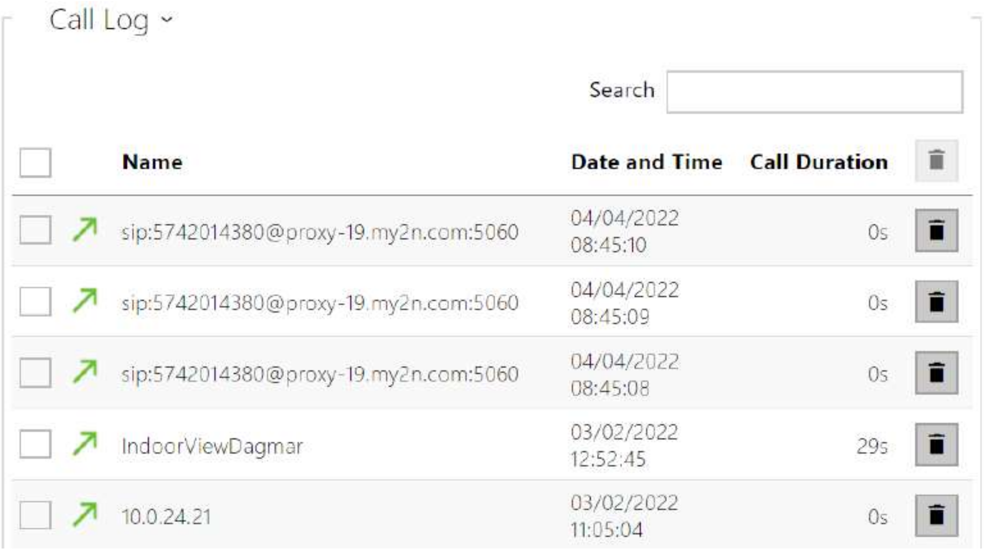
The **Access Log** tab displays the last 10 records on applied cards. Each record includes the card tapping time, card ID and type and description details (validity, card owner, etc.).



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

Call Log

The call log provides a list of all accomplished calls. Each call includes the contact type, called/ calling user ID, call date and time, call duration and status (incoming, outgoing, missed, picked up elsewhere, doorbell button). Use the search box for fulltext search in the call name. Use the check box for selecting all records for bulk deletion. The selected call record can also be deleted individually using a button 🗑. The list includes the last 20 records that are arranged from the latest call to the oldest one.



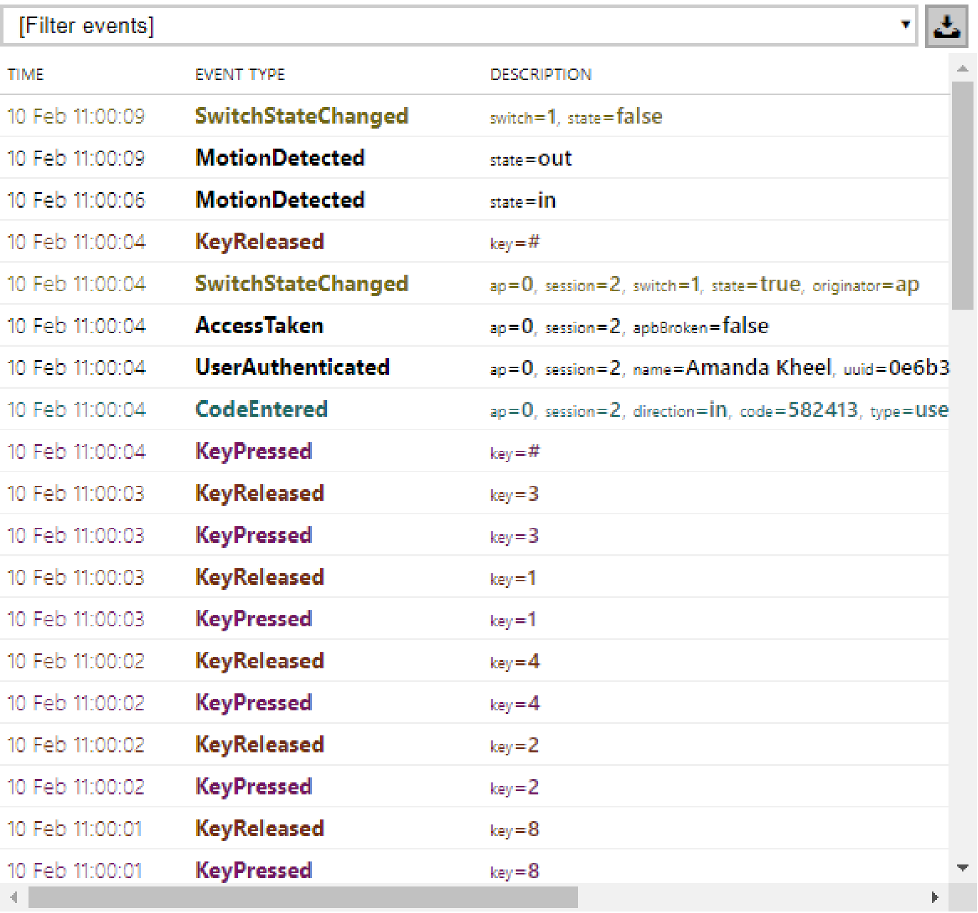
Call Log ˅

Search

☐		Name	Date and Time	Call Duration	🗑
☐	↗	sip:5742014380@proxy-19.my2n.com:5060	04/04/2022 08:45:10	0s	🗑
☐	↗	sip:5742014380@proxy-19.my2n.com:5060	04/04/2022 08:45:09	0s	🗑
☐	↗	sip:5742014380@proxy-19.my2n.com:5060	04/04/2022 08:45:08	0s	🗑
☐	↗	IndoorViewDagmar	03/02/2022 12:52:45	29s	🗑
☐	↗	10.0.24.21	03/02/2022 11:05:04	0s	🗑

Events

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



[Filter events]

TIME	EVENT TYPE	DESCRIPTION
10 Feb 11:00:09	SwitchStateChanged	switch=1, state=false
10 Feb 11:00:09	MotionDetected	state=out
10 Feb 11:00:06	MotionDetected	state=in
10 Feb 11:00:04	KeyReleased	key=#
10 Feb 11:00:04	SwitchStateChanged	ap=0, session=2, switch=1, state=true, originator=ap
10 Feb 11:00:04	AccessTaken	ap=0, session=2, apbBroken=false
10 Feb 11:00:04	UserAuthenticated	ap=0, session=2, name=Amanda Kheel, uuid=0e6b3
10 Feb 11:00:04	CodeEntered	ap=0, session=2, direction=in, code=582413, type=use
10 Feb 11:00:04	KeyPressed	key=#
10 Feb 11:00:03	KeyReleased	key=3
10 Feb 11:00:03	KeyPressed	key=3
10 Feb 11:00:03	KeyReleased	key=1
10 Feb 11:00:03	KeyPressed	key=1
10 Feb 11:00:02	KeyReleased	key=4
10 Feb 11:00:02	KeyPressed	key=4
10 Feb 11:00:02	KeyReleased	key=2
10 Feb 11:00:02	KeyPressed	key=2
10 Feb 11:00:01	KeyReleased	key=8
10 Feb 11:00:01	KeyPressed	key=8

- – tlačítko slouží k exportu všech zaznamenaných událostí do CSV souboru.

Event	Description
AccessLimited	Event generated after 5 unsuccessful user authentication atttempts (card, code, fingerprint). The access module gets blocked for 30 seconds even if the subsequent authetication is correct.
ApiAccessRequested	
AccessTaken	Card tapping in Anti-passback area.
AudioLoopTest	Generated after the audio test indicating the test result.
CallSessionStateChanged	Event describing the call direction/state, address, session number and call sequence number.
CallStateChanged	Indicates the call direction (incoming, outgoing) and opponent / SIP account identification at a call state change (ringing, connected, terminated).
CardHeld	Indicates that an RFID card has been held for more than 4s.
CardEntered	Indicates that an RFID card has been tapped.
CodeEntered	Generated whenever a code ending with * is entered via the numeric keyboard.
DeviceState	Device state indication, startup of the device, for example.
DoorOpenTooLong	Detection of a too-long opened door, settings in Hardware / Door / Door.
DoorStateChanged	Door open/closed state detection. Settings can be made in Hardware / Door / Door.
DtmfEntered	DTMF code received in call or off call locally.
DtmfPressed	DTMF code pressed in call or off call locally.

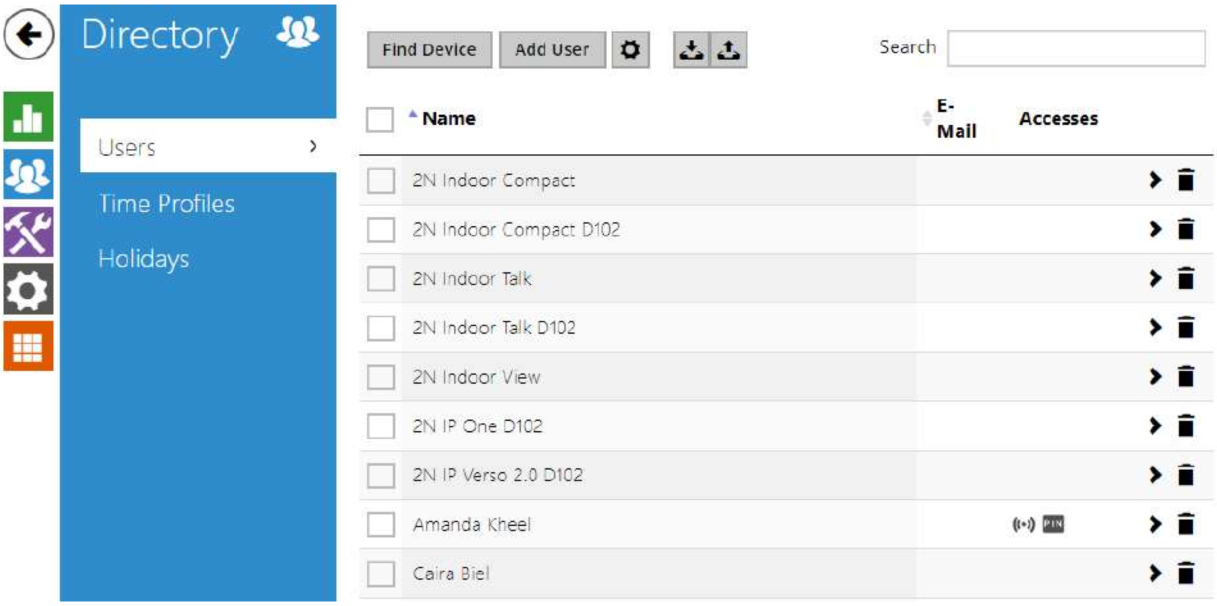
Event	**Description**
DtmfSent	DTMF code sent in call or off call locally.
FingerEntered	Fingerprint authorisation.
InputChanged	Signals a state change of the logic input.
KeyPressed	Generated whenever a button is pressed (numeric keypad digits are 0,1,2...,9 and quickdial buttons are %1,%2 ...).
KeyReleased	Generated whenever a button is released (numeric keypad digits are 0,1,2...,9 and quickdial buttons are %1,%2 ...).
LiftFloorsEnabled	Floor access via lift enabled.
LiftControlStatusChanged	Detection of Lift Control module connection/disconnection.
LoginBlocked	Event generated after 3 wrong logins to the web interface. Contains information about IP address.
MobKeyEntered	Bluetooth authorisation.
MotionDetected	Generated after motion detection, settings can be made in Hardware / Camera / Internal Camera.
NoiseDetected	Generated after noise detection, settings in Hardware / Audio.
OutputChanged	Signals a state change of the logic output.
RegistrationStateChanged	Change of the SIP Proxy registration state.
RexActivated	Event at input activation set for the REX button.

Event	Description
SilentAlarm	Silent alarm event generated whenever a code higher by one than the correct one is entered. With access code 123, the silent alarm code is 124.
SwitchesBlocked	Switches blocked by invalid access attempt.
SwitchOperationChanged	Switch operation changed (signals switch lock/hold, timer start/restart/termination – transition to permanent hold).
SwitchStateChanged	Change of the switch state, settings in Hardware / Switches.
TamperSwitchActivated	Signals tamper switch activation - device cover opening. Make sure that the tamper switch function is configured in the Digital Inputs | Tamper Switch menu.
UnauthorizedDoorOpen	Unauthorised door opening indication, settings in Hardware / Door / Door.
UserAuthenticated	User authentication.
UserRejected	Signals user authentication and subsequent door opening.
VirtualInput	Virtual input change.
VirtualOutput	Virtual output change.
CallSessionStateChanged	Informs of the current call phase (initialized, connecting, ringing, connected, terminated).

5.2 Directory

Here is what you can find in this subsection:

5.2.1 Users



	Name	E-Mail	Accesses
☐	2N Indoor Compact		
☐	2N Indoor Compact D102		
☐	2N Indoor Talk		
☐	2N Indoor Talk D102		
☐	2N Indoor View		
☐	2N IP One D102		
☐	2N IP Verso 2.0 D102		
☐	Amanda Kheel		((•)) PIN
☐	Caira Biel		

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

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

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

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

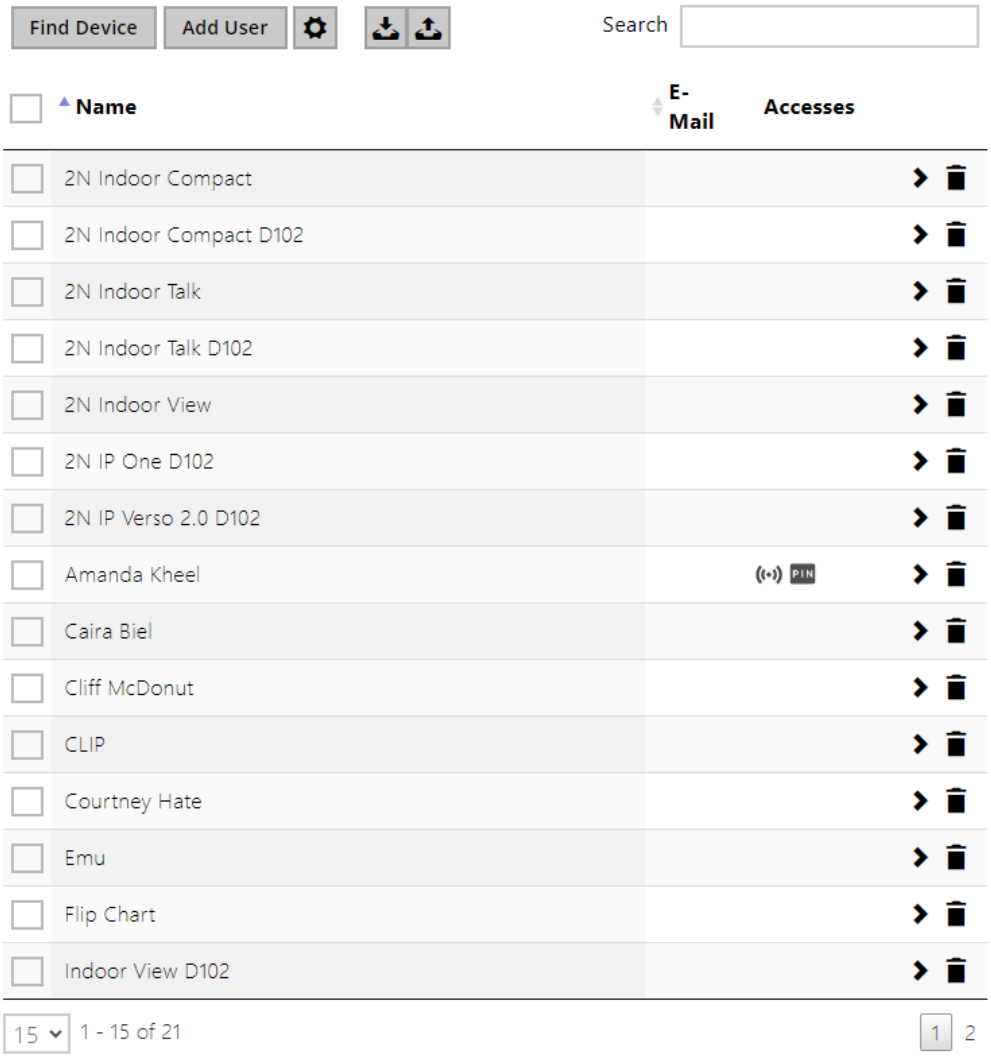
All cards applied via the reader or the Wiegand interface are recorded. Refer to the **Status / Access Log** menu for the last 10 cards including the card ID/type, card tapping time and other information if necessary. With small systems, you can make a trick to enter card IDs: tap the card on the intercom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

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

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

Warning

- You are not advised to edit the device directory that is managed by **2N Access Commander** via the device web interface. Due to synchronization with **2N Access Commander** the directory changes made via the web interface will be lost.



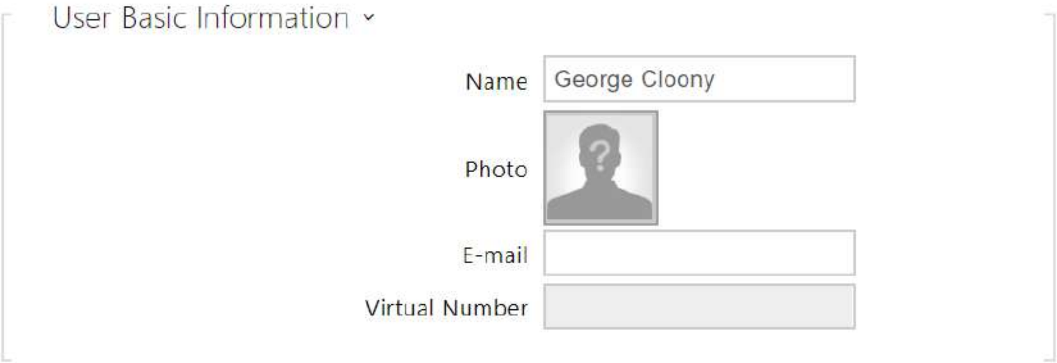
☐	Name	E-Mail	Accesses	
☐	2N Indoor Compact			› 🗑
☐	2N Indoor Compact D102			› 🗑
☐	2N Indoor Talk			› 🗑
☐	2N Indoor Talk D102			› 🗑
☐	2N Indoor View			› 🗑
☐	2N IP One D102			› 🗑
☐	2N IP Verso 2.0 D102			› 🗑
☐	Amanda Kheel		((•)) PIN	› 🗑
☐	Caira Biel			› 🗑
☐	Cliff McDonut			› 🗑
☐	CLIP			› 🗑
☐	Courtney Hate			› 🗑
☐	Emu			› 🗑
☐	Flip Chart			› 🗑
☐	Indoor View D102			› 🗑

15 1 - 15 of 21 1 2

The Search in directory function works as a fulltext search in user names, phone numbers and e-mail addresses. It searches for all matches in the list. Press the button above the table to add a User. Or, search a device in the LAN and then add the device as a new contact to the Directory.

Click › to show the user details. Click ⚙ to set the table column display; the default table setting displays the user name, e-mail and assigned accesses. Press 🗑 to remove a user and delete its details. The ((•)) ⊛ ✱ ⠿ PIN icons in the access column describe the active user authentications. The user's position in the list is sorted alphabetically.

Every record in the Users list includes the following parameters:



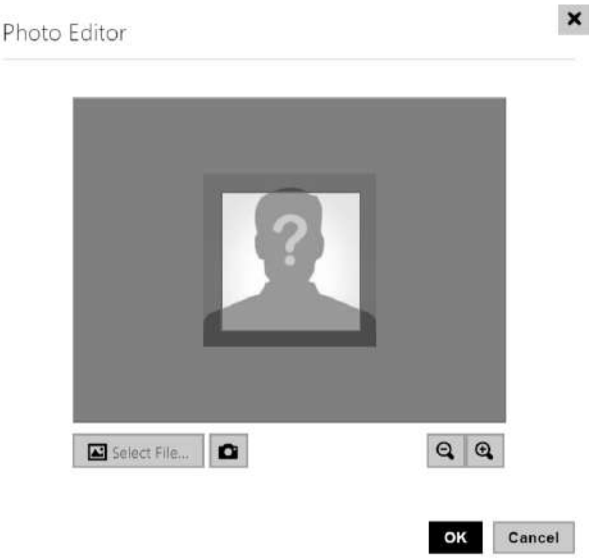
Name: George Cloony

Photo

E-mail

Virtual Number

- **Name** – mandatory parameter for easier user search, for example.
- **Photo** – load the user photo. Click the photo adding frame to display the Photo editor to load a photo from a file or create a user photo using an integrated camera. The supported photo formats are .jpg, .png and .bmp. This function is only available in display-equipped models: **2N LTE Verso**.



- **E-mail** – enter one or more email addresses separated by a comma or semicolon. The device can send emails to these addresses, e.g., missed calls, etc.
- **Virtual Number** – you can use the virtual number for calling a user via the numeric keypad on the device. The virtual number can have 1 to 7 places. The first/last place can be either a digit or a letter, the remaining positions can only be digits (A123, 456B, C12E, e.g.). Virtual numbers can be set according to apartment numbers, for example. Virtual numbers are especially convenient for installations where the speed dial buttons are

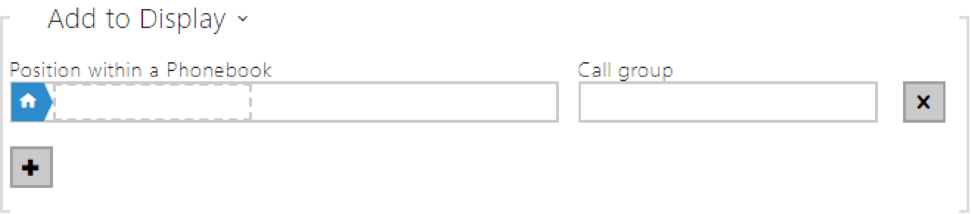
insufficient. Not being related to the actual user phone numbers, virtual numbers help protect the user phone numbers on the device.

Caution

Enable **Calling to Virtual Numbers** in **Calling > General settings > Outgoing calls**.

Note

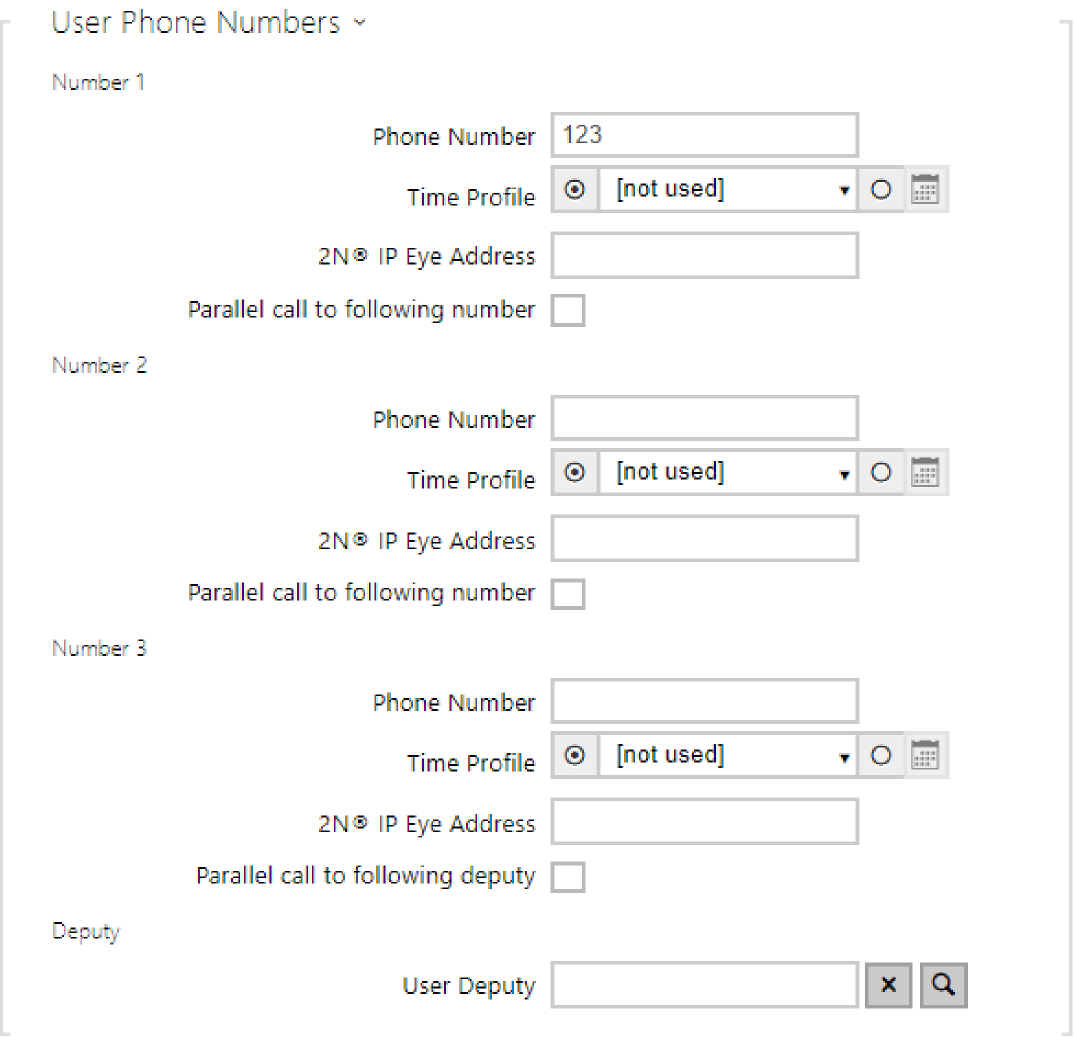
- Enter the user virtual number via the keypad and press an asterisk (*) or the call button (earpiece icon) to start a call.



- **Position within a Phonebook** – the root directory is only created by default to which users from the directory can be added directly. The root directory cannot be deleted or renamed. One user can be assigned to up to 5 root directory subgroups.
- **Call group** – enter a user group name to be displayed in the directory. By dialling the group you make calls to all of its users at the same time. When one call is answered, the other calls will be terminated automatically.

Caution

- The <, > and / characters are not allowed for the Name, Position within a Phonebook and Call group parameters.



Number 1: Phone Number 123; Time Profile ● [not used]; Parallel call to following number ☐

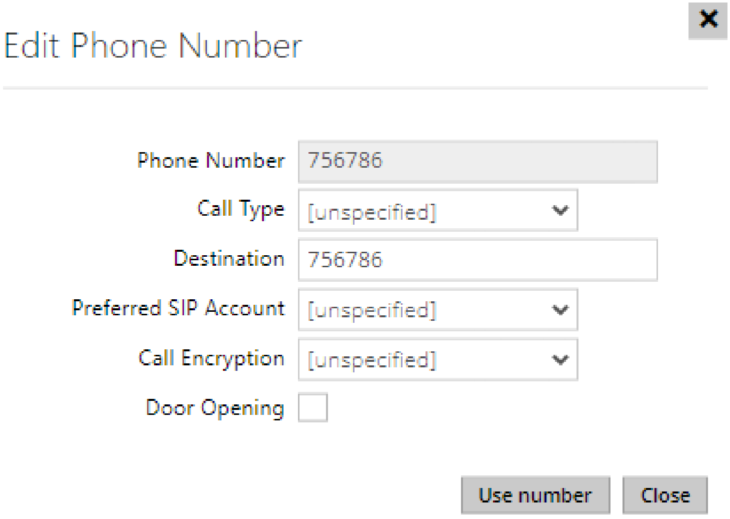
Number 2: Time Profile ● [not used]; Parallel call to following number ☐

Number 3: Time Profile ● [not used]; Parallel call to following deputy ☐

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

- **Phone number** – enter the phone number of the station to which the call shall be routed. Enter the address sip:[user_id@]domain[:port] for Direct SIP calling, e.g.: sip:200@192.168.22.15 or sip:name@yourcompany. Enter device:device_name for calls to the **2N IP Mobile** application. Set the device name in the mobile application. For calls to Crestron enter RAVA:device_name. Enter **/1** or **/2** behind the phone number to specify which SIP account shall be used for outgoing calls (account 1 or 2). Enter /**S** or /**N** to force an encrypted or unencrypted call respectively. Enter /**B** to activate door opening via Callback. Combine account selection, encryption and Callback door opening by e.g. /1S, /1B. etc. The parameter can contain up to 255 characters.

Click ✎ to edit the phone number details.



Edit Phone Number

Phone Number: 756786
Call Type: [unspecified]
Destination: 756786
Preferred SIP Account: [unspecified]
Call Encryption: [unspecified]
Door Opening: ☐

  - **Call Type** – set the scheme in the called destination URI. If you choose Without scheme ([unspecified]), the URI is completed with the data from the SIP account settings. Further settings include direct SIP calls (sip:), 2N local calls (device:), Crestron calls (rava:) or calls with VMS, e.g. AXIS Camera Station (vms:).
  - **Destination** – Set the other parts of the called destination URI. As a rule, it contains the number, IP address, domain, port or device identifier. Enter an asterisk (*) for calls to the VMS.
  - **Preferred SIP Account** – SIP account 1 or 2 is primarily used for calling.
  - **Call Encryption** – set mandatory call encryption or no encryption.
  - **Door Opening** – via callbacks.
- **Time profile** – assign a time profile to each phone number to define the number validity. If the profile in inactive, the phone number is not used and the following phone number is dialled if defined.
- **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 IP Eye** application displays the camera image screen for those users who are not provided with a display-equipped videophone. Enter the address as follows: domain[:**port1**][:**port2**], e.g.: computer.yourcompany.com or 192.168.22.111. The **port1** and **port2** parameters are optional and are used in case there is Network Address Translation (NAT) between the PC and intercom and the addresses have to comply with the router or another NAT-executing device. The port1 (default value: 8003) parameter defines the destination port for the UDP messages sent to **2N IP Eye**. The port2 (default value: 80) parameter defines the destination port for the **2N IP Eye** – intercom HTTP communication.

Note

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

Tip

FAQ: 2N IP Eye – How to set

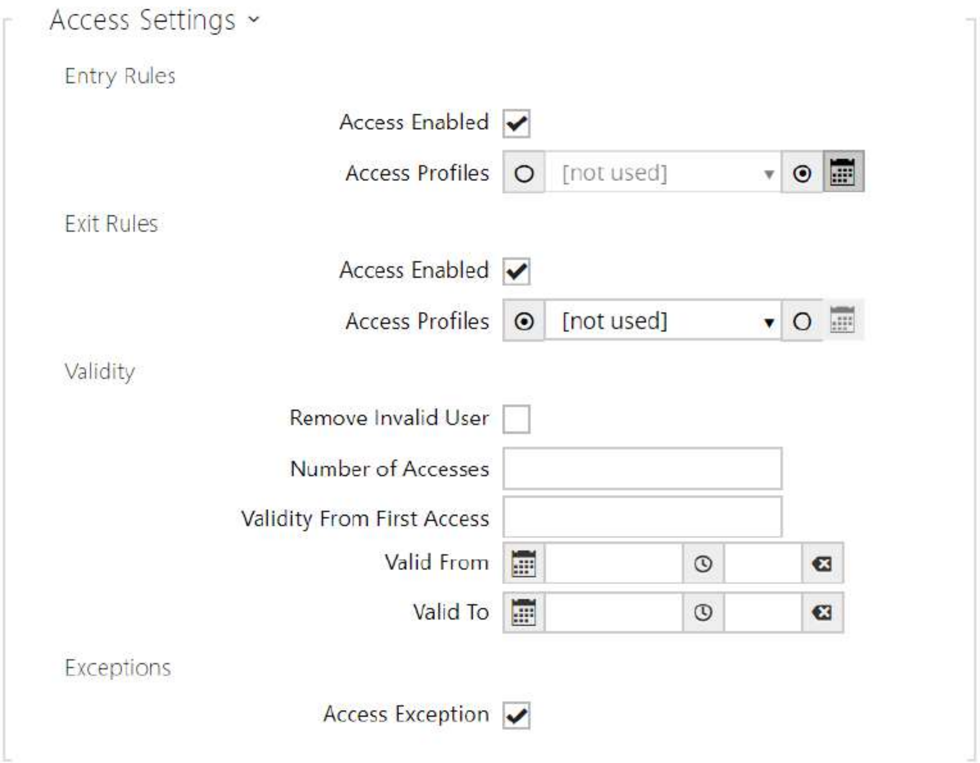
Tip

Video Tutorial: SW application for IP/LTE intercoms – 2N IP Eye

- **Parallel call to following number** – enable group calling, i.e. calling to more phone numbers at the same time. You can call the first two numbers, the last two numbers, or all of the three user numbers in parallel. Answering one call automatically terminates the other calls.
- **Parallel call to following deputy** – enable group calling, i.e. calling to more phone numbers at the same time. You can call the firs two numbers, the last two numbers, ar all of three user numbers in parallel. Once one of the calls is answered, the other calls are automatically terminated.The maximum total count of numbers to be dialled in parallel is 16, which can occur when group calling and multiple numbers assigned to a speed dial button are used simultaneously.
- **User deputy** – select a user to which the user calls will be routed in the event of inaccessibility. Enter user position number or use search button. The maximum total count of numbers to be dialled in parallel is 16, which can occur when group calling and multiple numbers assigned to a speed dial button are used simultaneously.

Note

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



Access Settings

Entry Rules

Access Enabled ☑

Access Profiles ○ [not used] ●

Exit Rules

Access Enabled ☑

Access Profiles ● [not used] ○

Validity

Remove Invalid User ☐

Number of Accesses

Validity From First Access

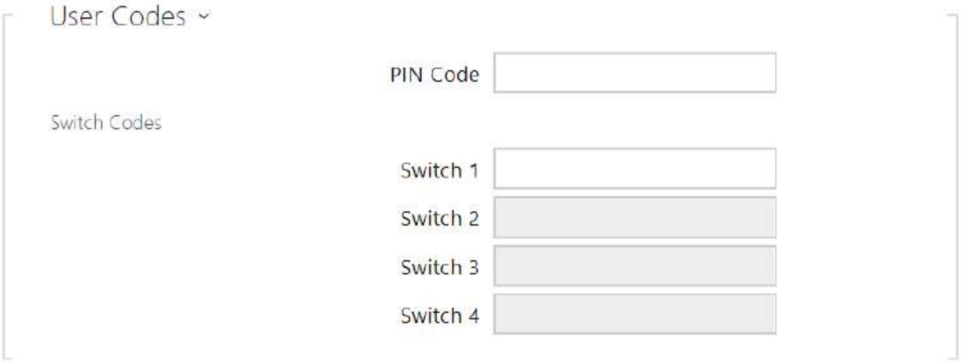
Valid From

Valid To

Exceptions

Access Exception ☑

- **Entry Rules**
  - **Access Enabled** – enable authentication via this access point.
  - **Access Profiles** – select one of the profiles pre-defined in Directory / Time profiles or set the time profile for this element manually.
- **Exit Rules**
  - **Access Enabled** – enable authentication via this access point.
  - **Access Profiles** – select one of the profiles pre-defined in Directory / Time profiles or set the time profile for this element manually.
- **Validity**
  - **Remove Invalid User** – select whether the user is removed from the device once it is invalid (i.e. it is past their validity term or the number of their authorized accesses is 0).
  - **Number of Accesses** – set the number of authorized accesses for this user. Leave empty to set indefinitely many accesses.
  - **Validity Period From First Access** – set the time that the user will be valid for from the first successful authorization. Leave empty for no relative validity period. Relative validity may shorten the validity period but never extend it. The time is set in the format HH:MM, e.g., 06:09.
  - **Valid from** – set the beginning of the mode validity term. Leave empty so that the start is not restricted. Valid From must precede Valid To.
  - **Valid to** – set the end of the mode validity term. Leave empty so that the end is not restricted. Valid To must be after Valid From.
- **Access Exception** – enable this user to bypass Access Blocking and Anti-Passback rules.



User Codes ⌄

PIN Code

Switch Codes

Switch 1

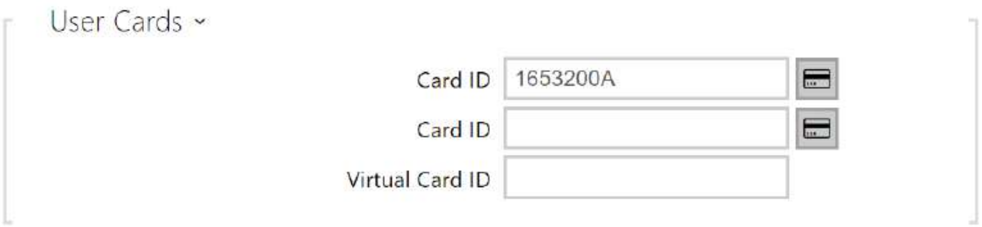
Switch 2

Switch 3

Switch 4

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

- **PIN Code** – set the user's Personal Identification Number. The code must include 2 characters at least.
- **Switch1–4** – set a private user switch activation code: up to 16 characters including digits 0–9 only. The code must include at least two door unlocking characters via the intercom keypad and at least one door unlocking character via DTMF.



User Cards ⌄

Card ID: 1653200A

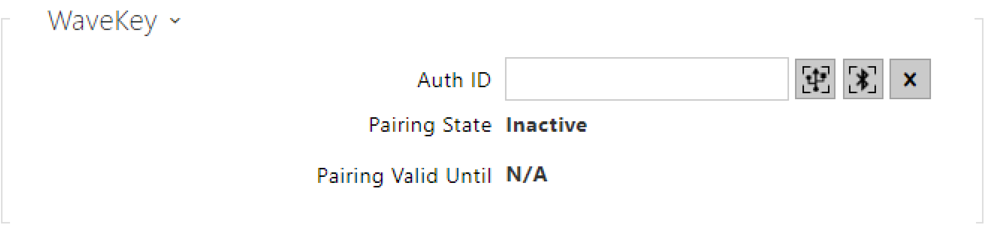
Card ID

Virtual Card ID

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

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

Bluetooth or Biometric Reader, the virtual card ID is sent to the Wiegand interface if the configuration (Services > Access Control) is set to send IDs to Wiegand.



WaveKey

Auth ID

Pairing State **Inactive**

Pairing Valid Until **N/A**

- **Auth ID** – unique WaveKey ID for access control. It's saved to the mobile device during the pairing process. The Auth ID consists of 32 hexadecimal characters.
  - pair via USB reader
  - pair via this device
  - × delete Auth ID
- **Pairing State** – display the current pairing state (Inactive, Waiting for pairing, PIN validity expired, Paired, Too many attempts).

> **Note**
>
> - After 10 unsuccessful pairing attempts, a 30 s pause is activated automatically for security reasons, during which it is impossible to make any further pairing attempts.

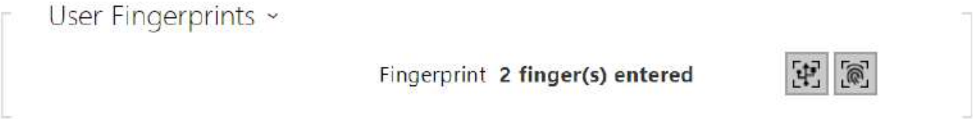
- **Pairing valid until** – date and time at which the authorization PIN validity expires or the temporary pairing suspension ends.

Pairing via Bluetooth Module in Intercom

To pair a mobile phone with the user:

- Click at Auth ID to start pairing for the selected user account.
- A dialogue window with the PIN code is displayed.
- Find the appropriate reader in the **My2N** application and press Start pairing.
- Enter the code from item 2 into the input field.
- Pairing is completed.

Refer to 5.4.2 Řízení přístupu for My2N configuration details.



Fingerprint **2 finger(s) entered**

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

Caution

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

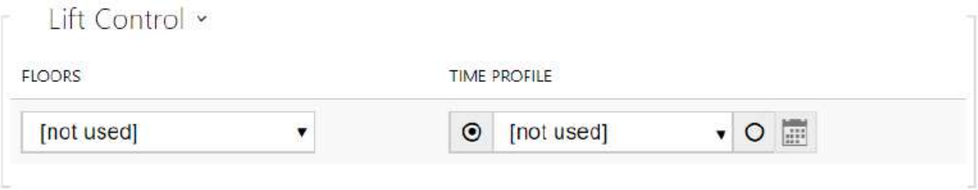
Refer to Subs. 5.2.1.1 Pokyny pro nastavení uživatelských otisků prstů for user fingerprint loading details.

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

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

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

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



[not used] ▾

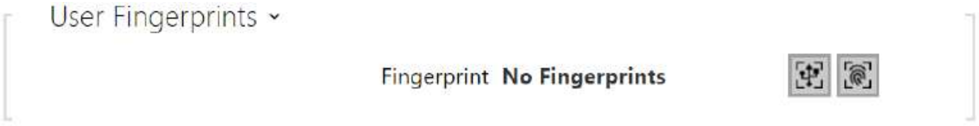
◉ [not used] ▾ ○

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

5.2.1.1 User Fingerprint Setting Instructions

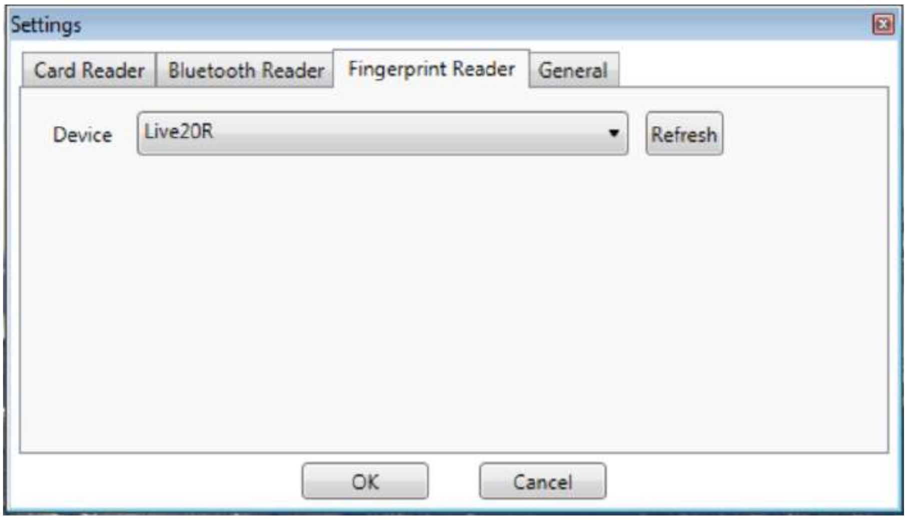
To load fingerprints, use the **2N® LTE Verso** (Part No. 9155045) fingerprint reader or an external USB fingerprint scanner (Part No. 9137423E) as follows:

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

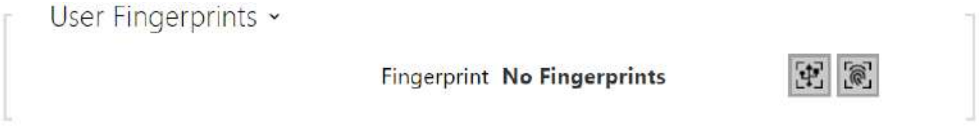


Fingerprint **No Fingerprints**

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

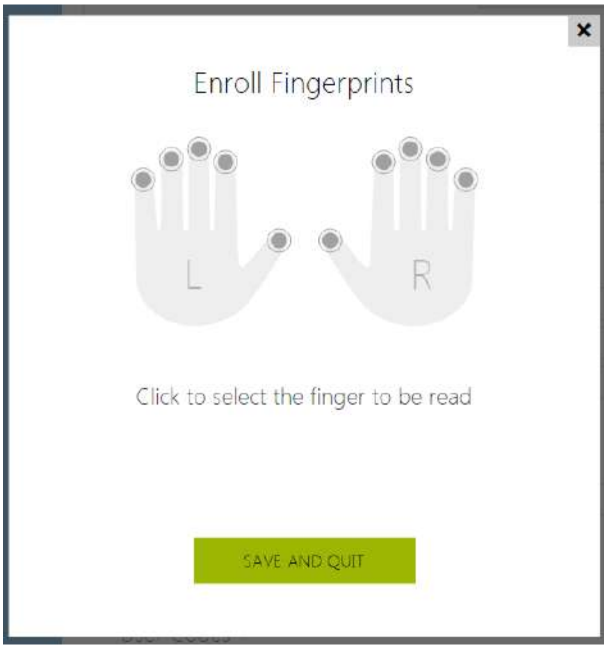


Device Live20R

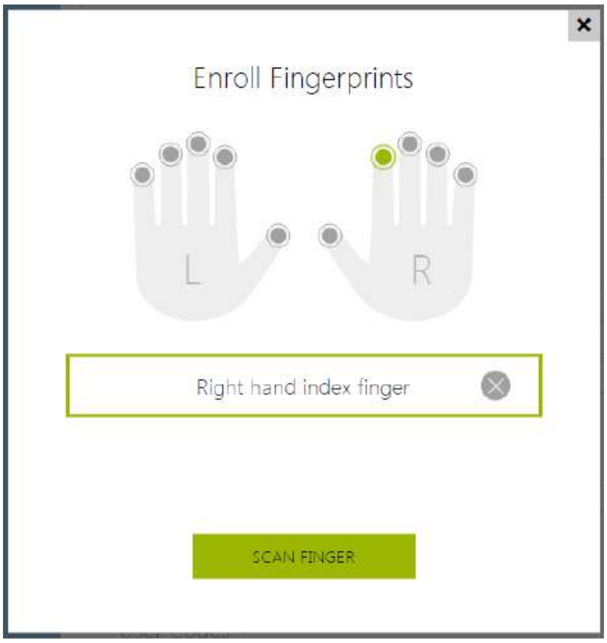


Fingerprint **No Fingerprints**

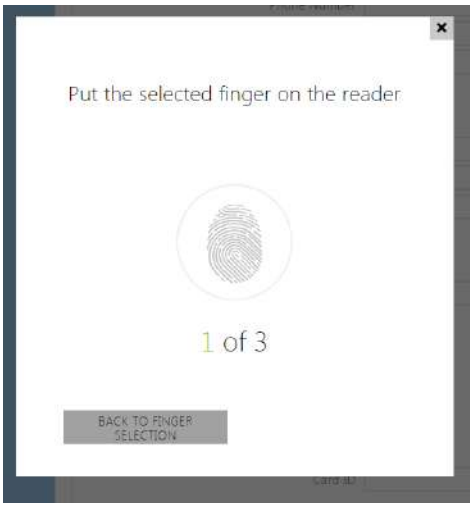
2) Click to select a finger for fingerprint loading.



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



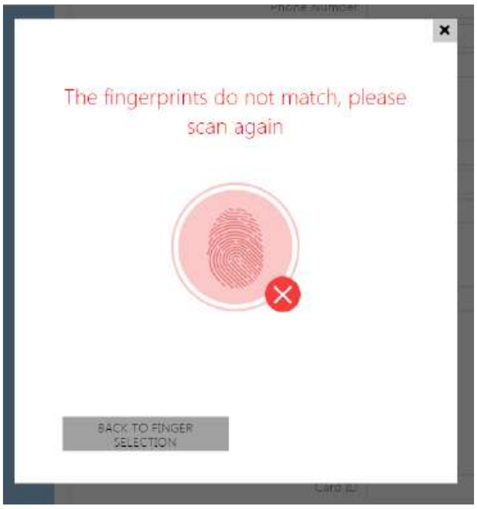
4) Place the selected finger on an external USB reader. This process is repeated three times for greater precision.



Put the selected finger on the reader

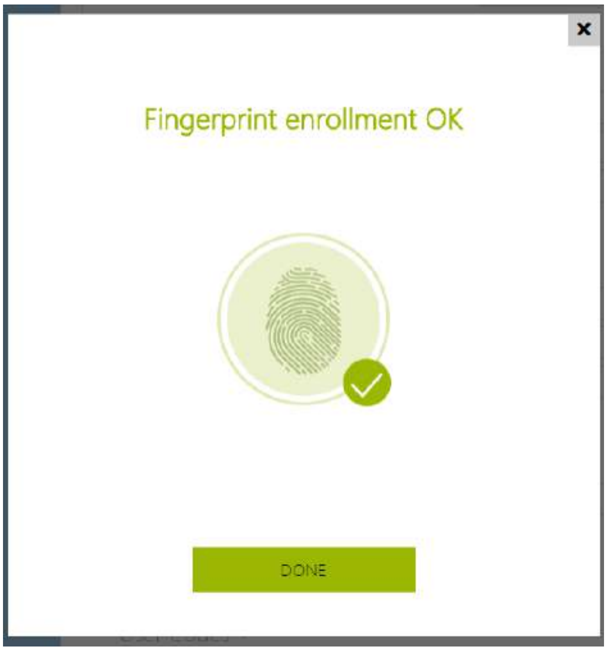
1 of 3

Repeat the process if any inconsistency occurs during fingerprint reading.



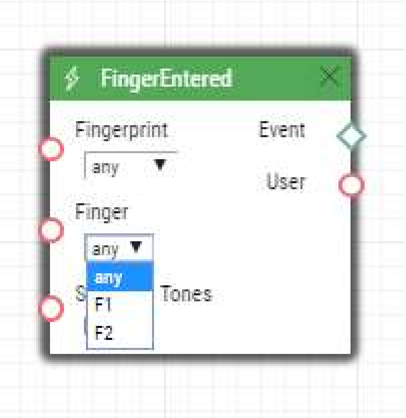
The fingerprints do not match, please scan again

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

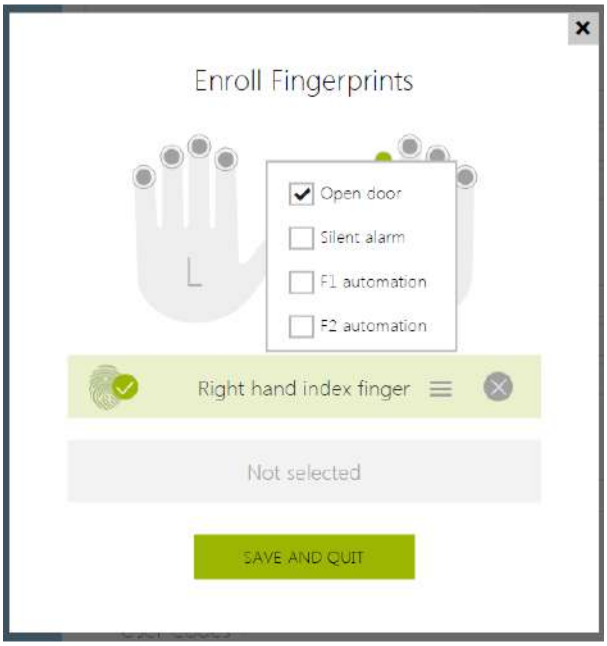


To set the finger function, click the ≡ icon to display the list of available functions:

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



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



Enroll Fingerprints

☑ Open door

☐ Silent alarm

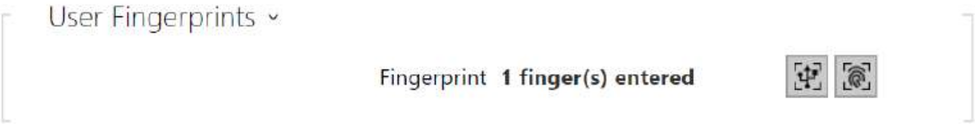
☐ F1 automation

☐ F2 automation

Right hand index finger

Not selected

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



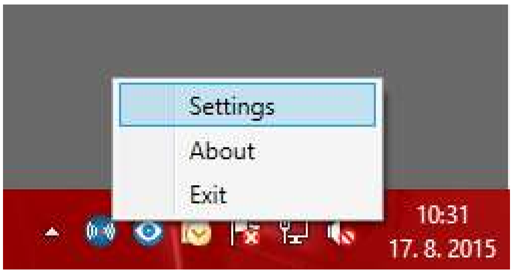
User Fingerprints

Fingerprint **1 finger(s) entered**

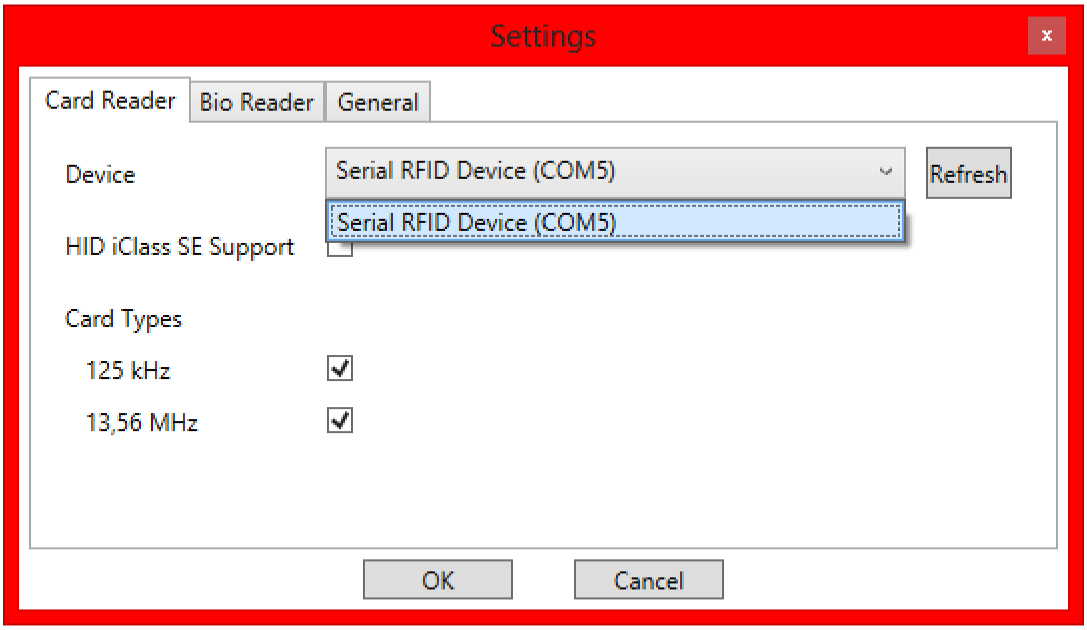
5.2.1.2 USB RFID Card Reader

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

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



- Set up the COM port for the connected reader.



Device: Serial RFID Device (COM5)

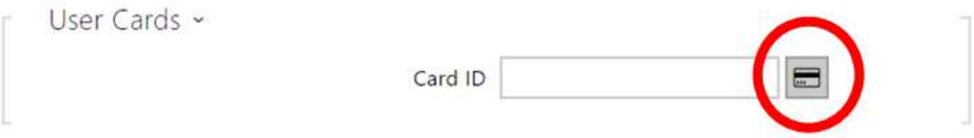
HID iClass SE Support ☐

Card Types

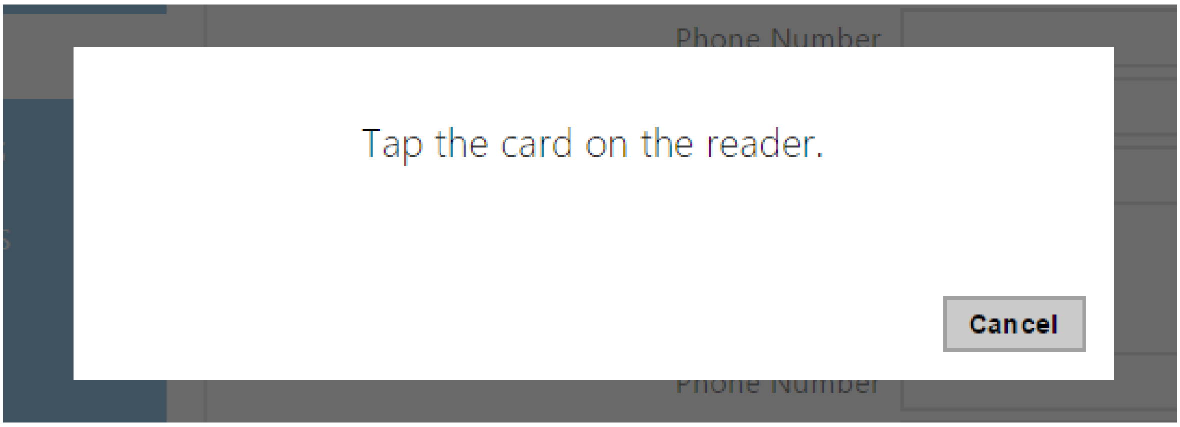
125 kHz ☑

13,56 MHz ☑

- Press the Read button via the **2N LTE intercom** web interface.

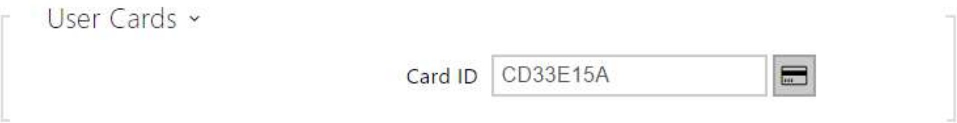


- Tap the card on the card reader.



Tap the card on the reader.

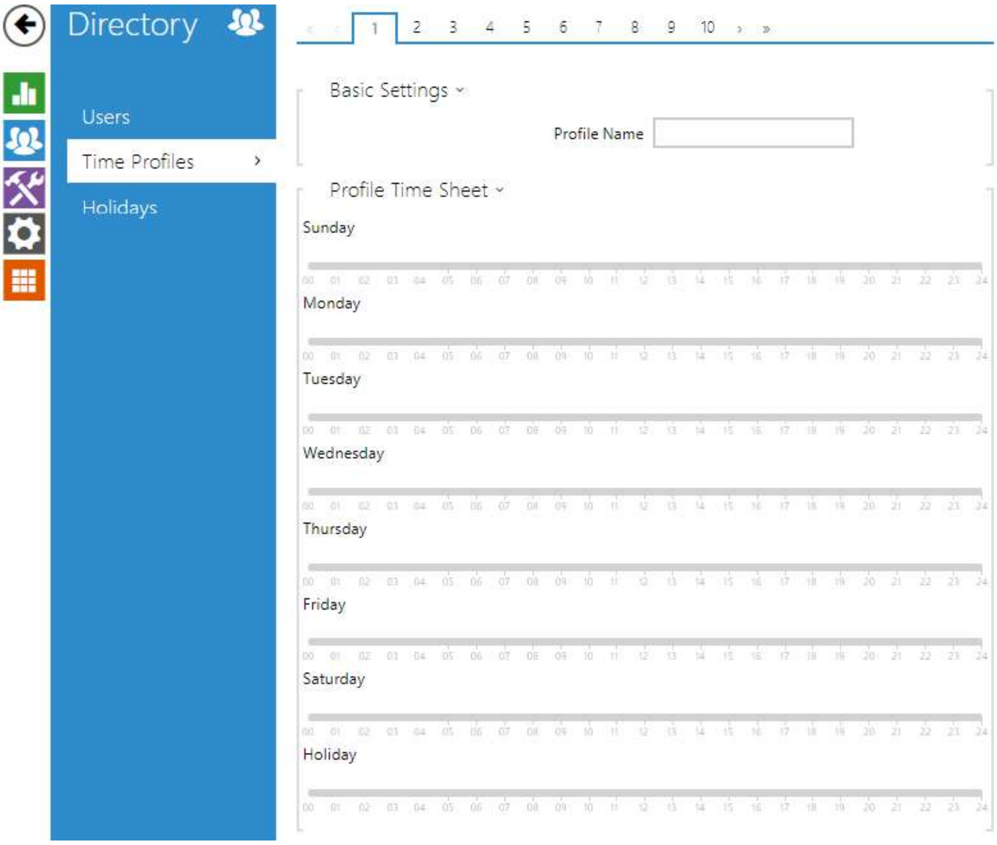
- The card ID is successfully read.



Card ID CD33E15A

- Do not forget to save the configuration.

5.2.2 Time Profiles



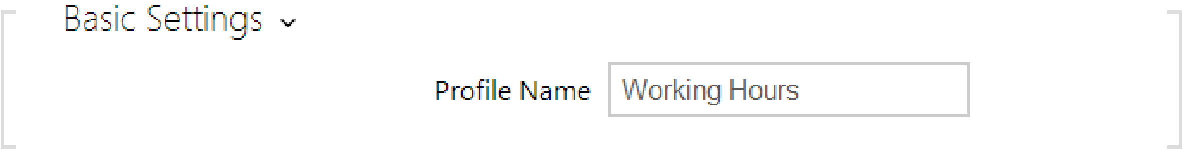
Such intercom functions as outgoing calls and RFID card/numeric code access, for example, can be time-limited by being assigned a **time profile**. By assigning a time profile you can:

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

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

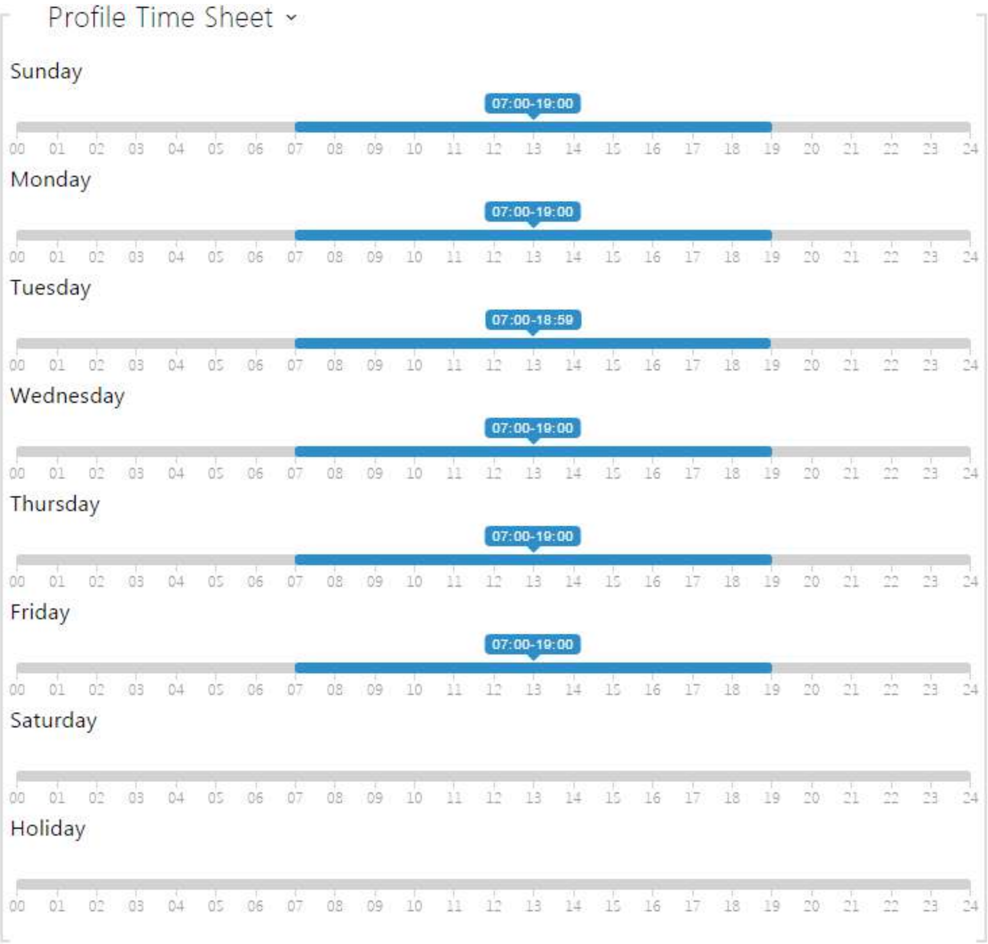
The time profiles are defined not only using the week time sheet but also manually with the aid of special activation/deactivation codes that you can assign to them after arriving in/before leaving your office, for example. Enter the activation/deactivation codes using the numeric keypad of your intercom or phone (during the intercom call). Refer to the **Directory** / **Time Profiles** menu for the time profile settings.

List of Parameters



Profile Name: Working Hours

- **Profile name** – enter a name for the time profile so that you can easily identify it when selecting it in switches, access control, phone numbers, etc.



Sunday: 07:00-19:00

Monday: 07:00-19:00

Tuesday: 07:00-18:59

Wednesday: 07:00-19:00

Thursday: 07:00-19:00

Friday: 07:00-19:00

Saturday

Holiday

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

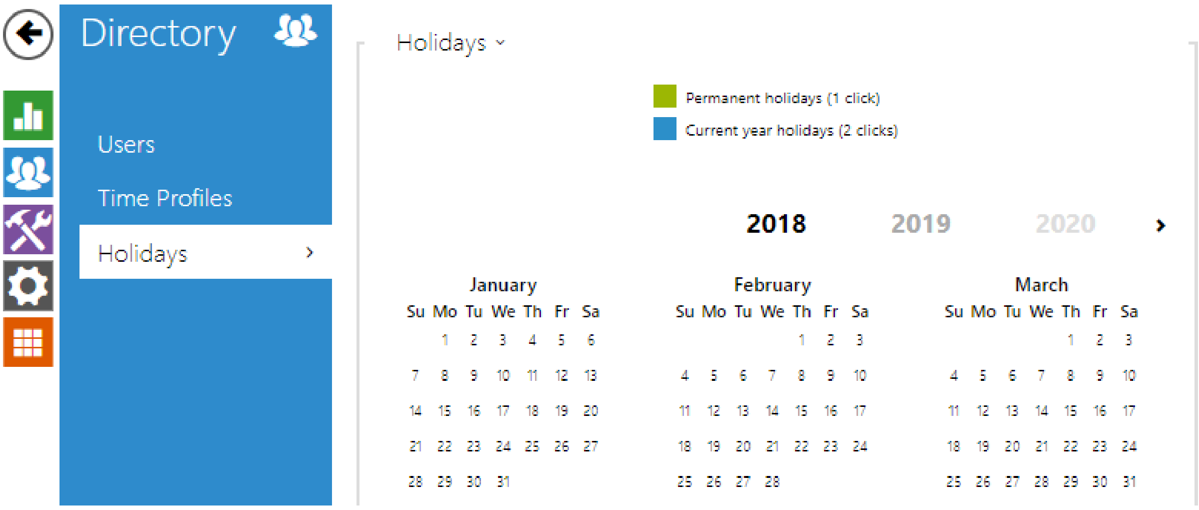
If a day is marked as holiday (refer to **Directory → Holidays**), the last table row (Holiday) is applied regardless of the day in a week.

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

ⓘ **Note**

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

5.2.3 Holidays



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

You can set holidays for the coming 10 years (click the year number at the top of the screen to select a year). A calendar is displayed for you to select/unselect a holiday. Fixed (annual) holidays are marked green and variable holidays (valid for the particular year only) are blue. Click a date once to select a fixed holiday, click twice to select a variable holiday and click for the third time to remove the holiday from the holiday list.

5.3 Calling

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

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

Typically, the intercoms are used for outgoing calls and incoming calls are inactive – the microphone and speaker are muted. However, you can configure your intercom to make incoming calls active and ringing; refer to 5.3.1 General Settings. Press the * and # keys on the numeric keypad to answer and terminate an incoming call.

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

Explanation of IP Telephony Terms

- **SIP (Session Initiation Protocol)** – is a phone call signalling transmission protocol used in IP telephony. It is primarily used for setting up, terminating and forwarding calls between two SIP devices (the intercom and another IP phone in this case). SIP devices can establish connections directly with each other (Direct SIP Call) or, typically, via one or more servers: SIP Proxy and SIP Registrar.
- **SIP Proxy** – is an IP network server responsible for call routing (call transfer to another entity closer to the destination). There can be one or more SIP Proxy units between the users.
- **SIP Registrar** – is an IP network server responsible for user registration in a certain network section. As a rule, SIP device registration is necessary for a user to be accessible to the others on a certain phone number. SIP Registrar and SIP Proxy are often installed on one and the same server.
- **RTP (Real-Time Transport Protocol)** – is a protocol defining the standard packet format for audio and video transmission in IP networks. **2N IP** intercom 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).

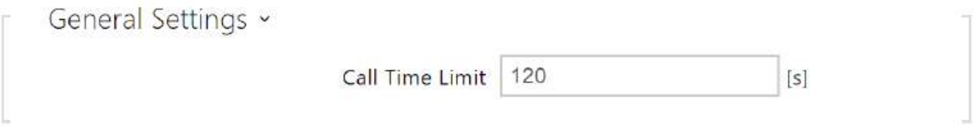
The **2N IP** intercoms support three ways of SIP signalling:

- 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 (except models **2N® IP Base**, **Uni**)

Here is what you can find in this section:

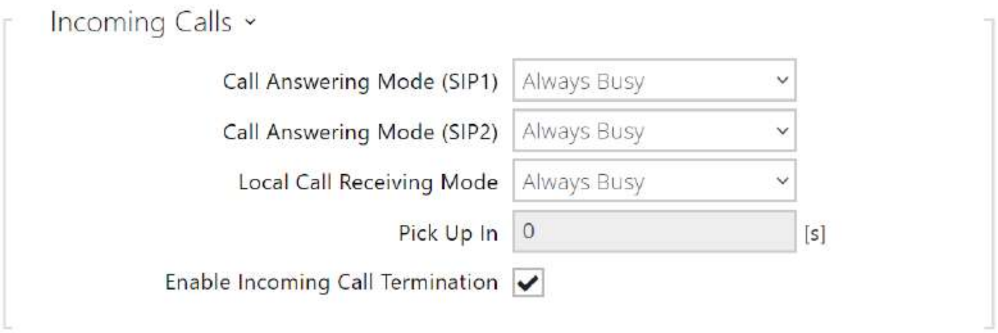
- 5.3.1 General Settings
- 5.3.2 Dialing
- 5.3.3 SIP 1 / SIP 2
- 5.3.4 Local Calls
- 5.3.5 Crestron

5.3.1 General Settings



Call Time Limit: 120 [s]

- **Call Time Limit** – set the call time limit after which the call is automatically terminated. The intercom signals termination with a 10s beep before the call end. Enter any DTMF character into the call (# on your IP phone, e.g.) to extend the call time. If the call duration is set to 0 and SRTP is not used, the call is not time limited.



Call Answering Mode (SIP1): Always Busy
Call Answering Mode (SIP2): Always Busy
Local Call Receiving Mode: Always Busy
Pick Up In: 0 [s]
Enable Incoming Call Termination: ☑

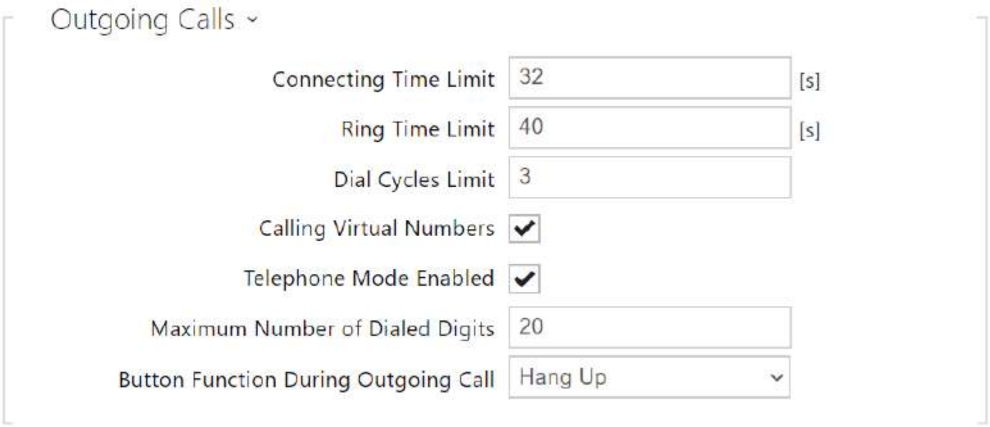
- **Call Answering Mode(SIP1, SIP2)** – set the incoming call receiving mode. The following three options are available:
    - **Always busy** – the intercom rejects incoming calls,
    - **Manual** – the intercom alerts incoming calls and the user answers them using a numeric keypad button, and

  - **Automatic** – the intercom picks up incoming calls automatically. You can set the call receiving mode for each SIP account separately.
  - **Automatic (DTMF only)** – the intercom picks up incoming calls automatically only if DTMF without connection to a microphone and speaker is received.
  - **Automatic (hidden)** – the intercom picks up incoming calls automatically without displaying the CLIP or any call pickup accompanying signs.
- **Local Call Receiving Mode** – set the incoming local call receiving mode
  - **Always busy** – the intercom rejects incoming calls,
  - **Manual** – the intercom alerts incoming calls and the user answers them using a numeric keypad button, and
  - **Automatic** – the intercom answers incoming calls automatically. You can set the call receiving mode for each SIP account separately.
  - **Automatic (hidden)** – the intercom picks up incoming calls automatically without displaying the CLIP or any call pickup accompanying signs.
- **Pick Up In** – set the timeout after which the call is automatically picked up in the automatic call answering mode. If one of the **Answering machine modes** is enabled in an Answering machine supporting device, the call is picked up after the timeout and the selected voice message is played in both the automatic and manual call answering modes. If this value is 0, the voice message is played instantaneously. Shared by all the SIP accounts.
- **Answer Incoming Call by Button** – pick up an incoming call via a selected speed dial button. Set to None to disable the function.

Caution

- The Answer Incoming Call by Button function is not displayed in the keypad-equipped **2N® IP Force** and **2N® IP Vario** models. With these models, answer incoming calls by pressing the green earpiece button on the keypad without prior configuration.

- **Enable Incoming Call Termination** – allow the users to reject or end an incoming call on the intercom. When this function is off, the earphone button will not be available for call rejection/termination and the call rejection/termination icon will not be displayed. The call can be interrupted by starting a new outgoing call from the intercom.



Outgoing Calls

Connecting Time Limit: 32 [s]

Ring Time Limit: 40 [s]

Dial Cycles Limit: 3

Calling Virtual Numbers: ☑

Telephone Mode Enabled: ☑

Maximum Number of Dialed Digits: 20

Button Function During Outgoing Call: Hang Up

Connecting Time Limit – set the maximum outgoing call connection timeout after which the calls are 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.
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. Minimum value 1 s, maximum value 600 s. Configure 0 to disable this time limit. **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. Refer to Subs. 5.4.1.1 Calling Cycle Limit for calling cycle limit settins options.

End Group Calls at First Rejection – enable the device to end all outgoing group calls if any of the called destinations rejects the call.

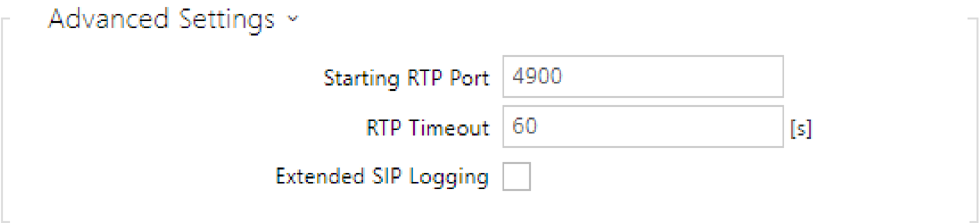
Calling Virtual Numbers – allow the calling of preset virtual numbers of users.

Floor/Apartment Dialing Mode – enable the special Floor/Apartment dialling mode. In this mode, enter the assigned user virtual number via the numeric keypad. Available for model **2N® IP Vario** only. Enter the floor/apartment code to the user Virtual number. The code may include digits and letters A–F. **Telephone Mode Enabled** – enable the option to set up calls directly to the phone numbers dialed via the intercom numeric keypad. Enter the phone number key sequence to set up the call.

Tip

- Set up a call to **2N® IP Force** and **2N® IP Vario** as follows: press * **phone_number** * (or ☎ **phone_number** ☎ for **2N® IP Verso**). If you do not press * (or ☎ for **2N® IP Verso**) as the terminating character, the dialling will be confirmed automatically when the code entering timeout expires as if * (or ☎ for **2N® IP Verso**) was pressed.

- **Maximum Number of Dialed Digits** – set the maximum count of digits for a phone number in the Telephone mode. When this limit is reached, the number is dialed automatically without pressing *.
- **Button Function During Outgoing Call** – set the quick dial button function during an outgoing call. You can only set the button that initiated the call.



Starting RTP Port: 4900
RTP Timeout: 60 [s]
Extended SIP Logging ☐

- **Starting RTP Port** – set the starting local RTP port in the range of the length of 64 ports to be used for audio and video transmissions. The default value is 4900 (i.e. the used range is 4900–4963). The parameter is only set for account 1 but applies to both the SIP accounts.
- **RTP Timeout** – set the audio stream RTP packet receiving timeout during a call. If this limit is exceeded (RTP packets are not delivered), the call is terminated by the intercom. Set the parameter to 0 to disable this function. The parameter is only set for account 1 but applies to both the SIP accounts.
- **Extended SIP Logging** – allow SIP telephony details to be recorded in syslog (for troubleshooting purposes only).

5.3.1.1 Dial Cycles Limit

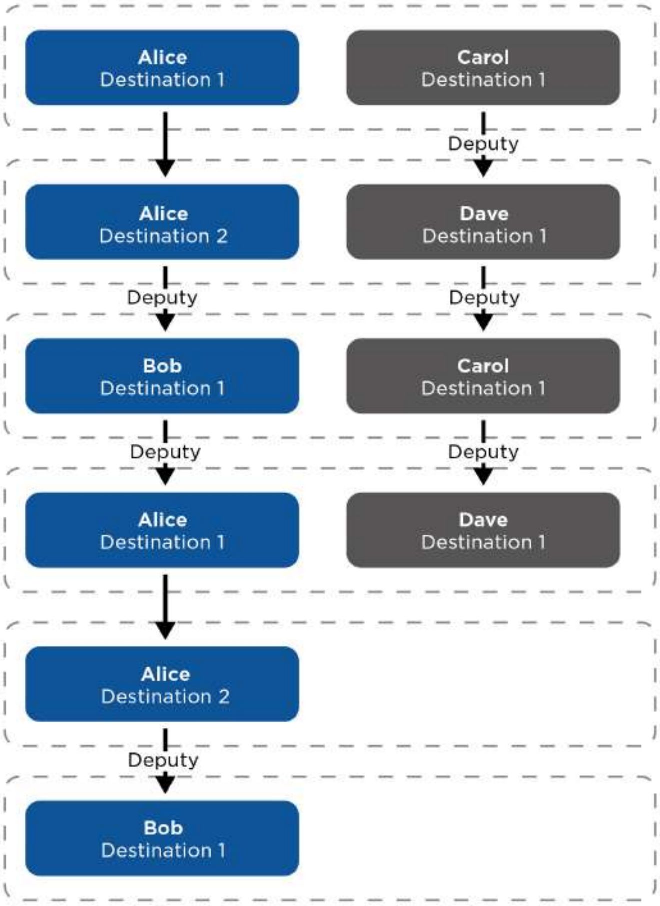
This parameter sets the maximum number of consecutive calls to a calling destination when there is a dialing cycle of deputies (the simplest example of a dialing cycle is when a user has configured itself as a deputy, another example is two users who are configured to be deputies of each other).

Example 1

The algorithm first resolves the branches independently of each other. There are users Alice and Carol configured to one button in the example below (by pressing the button two parallel calls are initiated together). The Dial Cycles Limit is set to 2. Alice has two phone numbers (calling destinations), the other users have only one calling destination. The deputies are configured as follows:

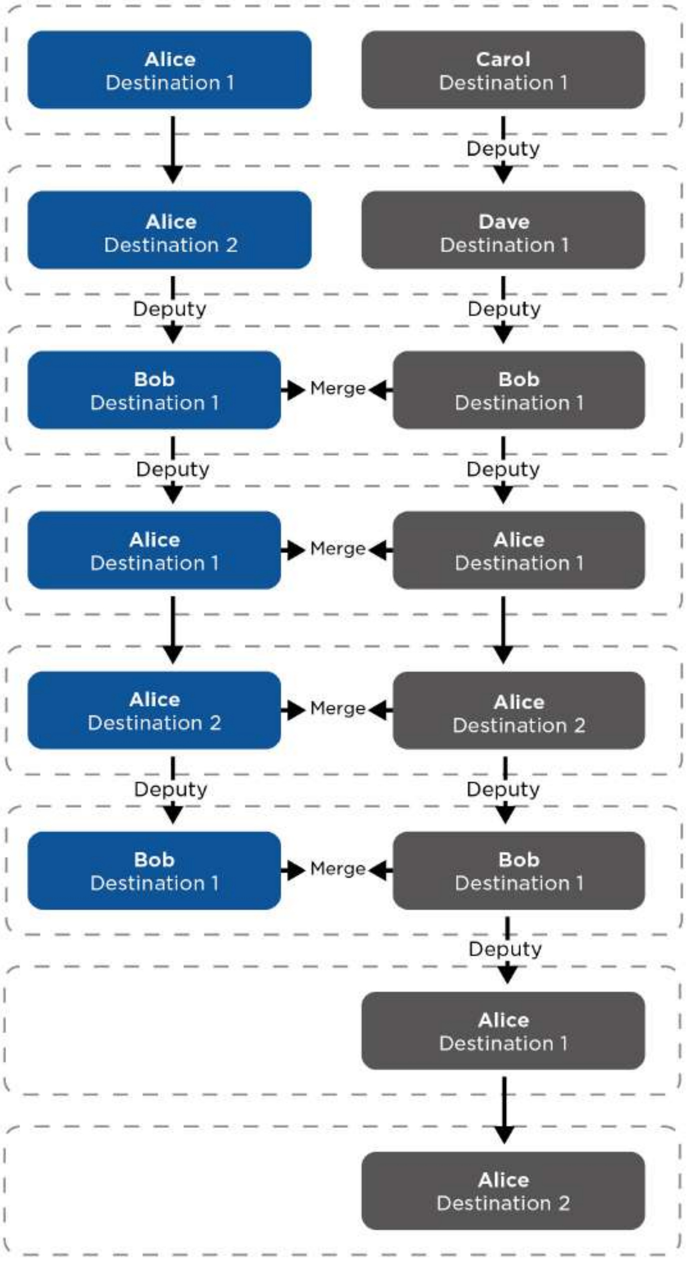
- Alice is the deputy of Bob
- Bob is the deputy of Alice
- Carol is the deputy of Dave
- Dave is the deputy of Carol

The resulting calling scheme looks like this (in case no one picks up or rejects the call):



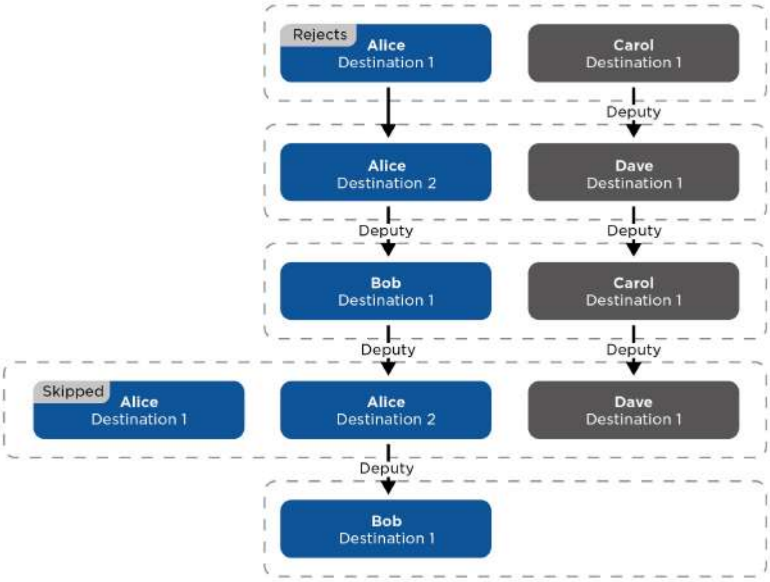
Example 2

Let’s take the previous example and change the deputy of Dave to Bob. This way the two branches are merged (only one call takes place from step 3 further on). You can also see that Alice is eventually called three times. This is caused by the fact that the Dial Cycles Limit is applied to each branch individually and in fact Alice is called only twice in the blue branch and as well only twice in the purple branch.



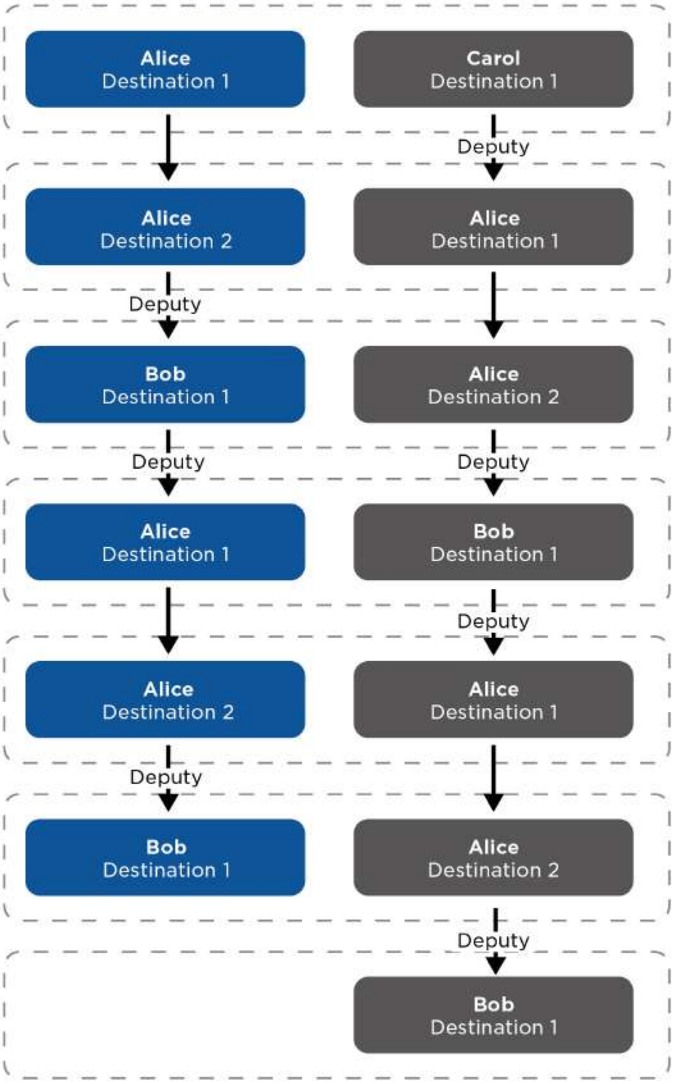
Example 3

Let's take the configuration from Example 1 and consider a situation that Alice rejects the call from her first destination. The algorithm skips dialing this destination further on (since the user actively rejected the call and it makes no sense to call them again). The calling groups in individual steps are therefore dynamically modified when one or more users reject the call from various calling destinations. Skipping of a calling destination that rejected the call applies to all branches regardless of in which branch the call was rejected.



Example 4

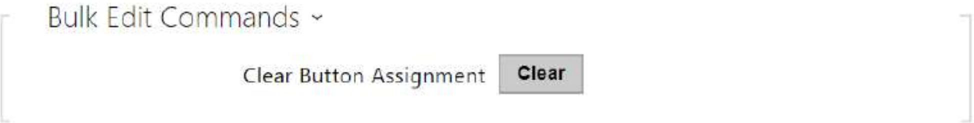
It is possible that two calling destinations of a single user are called at once. This can be achieved by configuring the scheme similarly to the example below but this situation may also arise from skipping of the destinations that rejected the call previously.


Alice
Destination 1
Carol
Destination 1
Deputy
Alice
Destination 2
Alice
Destination 1
Deputy
Bob
Destination 1
Alice
Destination 2
Deputy
Deputy
Alice
Destination 1
Bob
Destination 1
Deputy
Alice
Destination 2
Alice
Destination 1
Deputy
Bob
Destination 1
Alice
Destination 2
Deputy
Bob
Destination 1

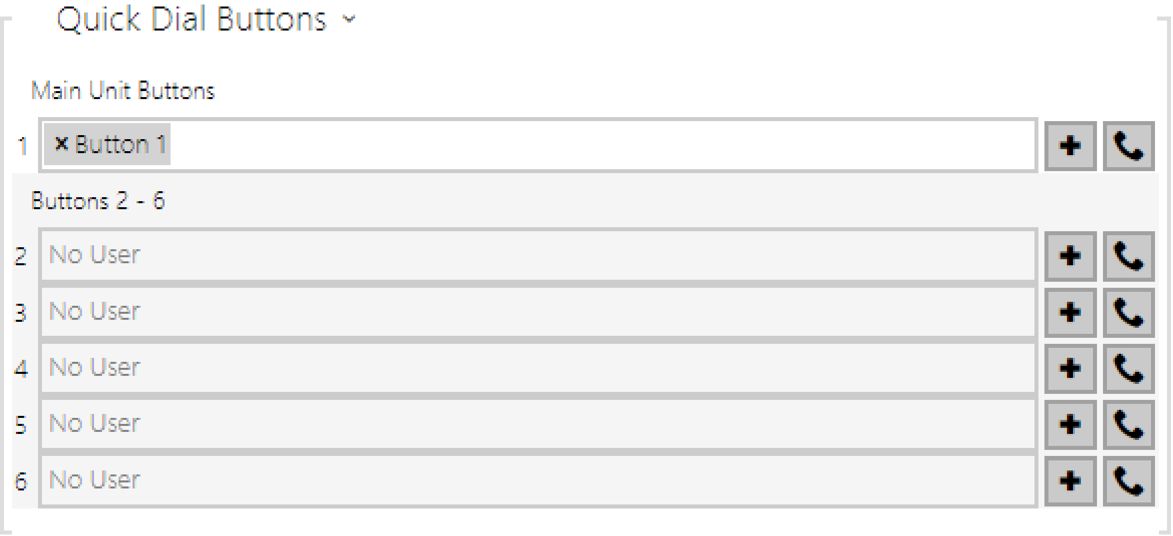
5.3.2 Dialing

Quick Dial Buttons

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



- **Clear Button Assignment** – clear all assignments of buttons to users.



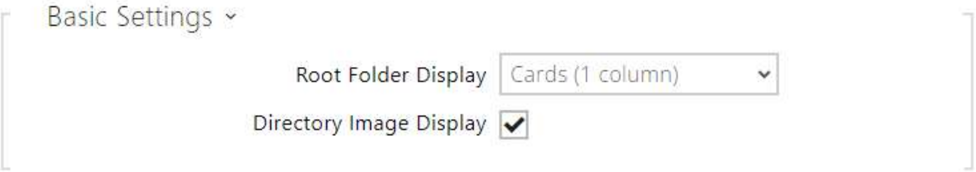
Display the list of all potentially available intercom buttons including those physically absent. In some intercom models (**2N® IP Vario**, **2N® IP Verso**), the button list is divided into 8/5-item groups corresponding to the button extending modules. Click ✚, select the user and press Add to add a user to the editing field. To search a user in the list, use the fulltext field and the username. One quick dial button can be shared by multiple users. Click ☎ to test the set quick dial button. A dialogue window is displayed including detailed information on the ongoing call (user, call direction, state, reason and last event time).

ⓘ **Info**

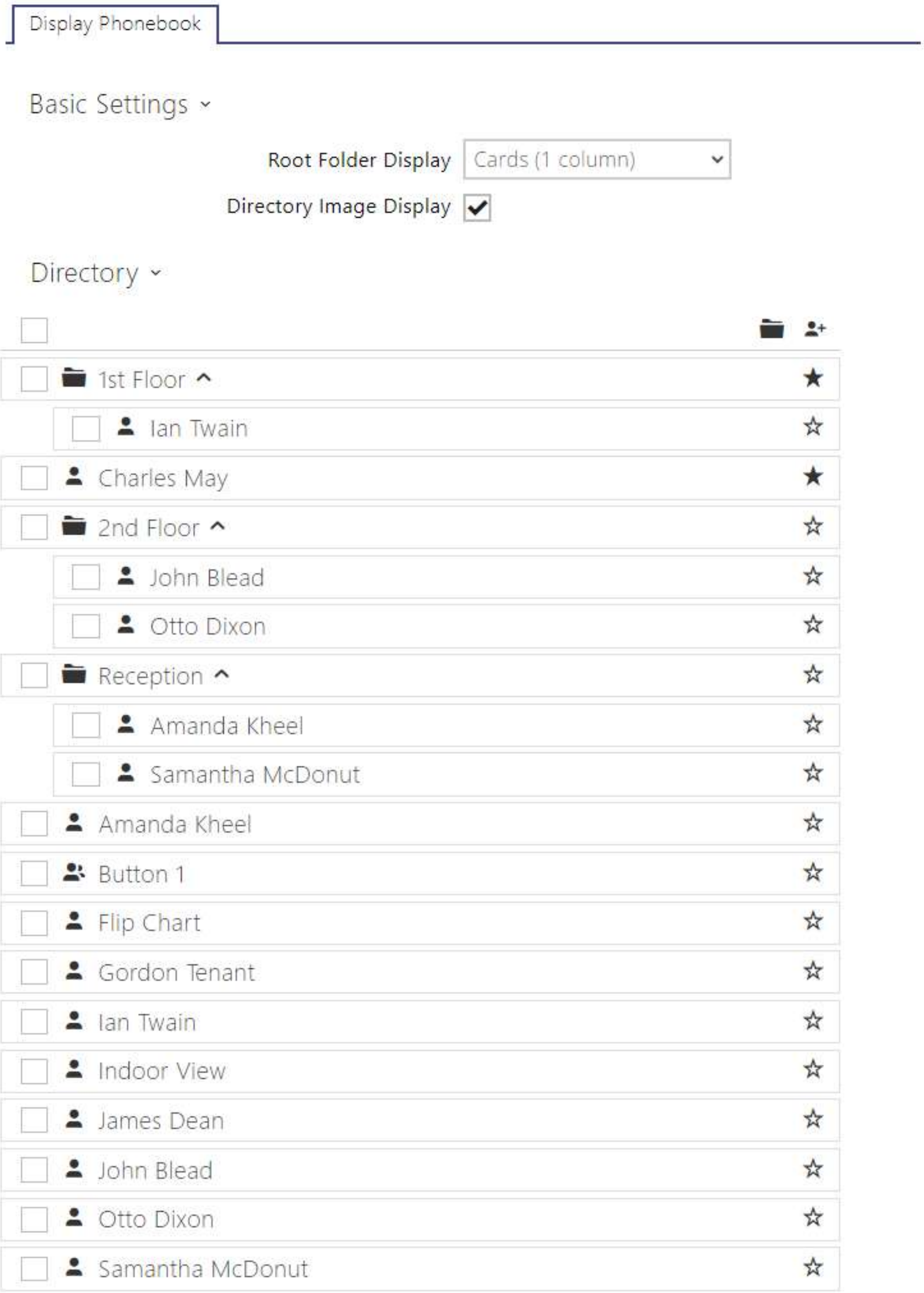
- Up to 16 users can be assigned to one speed dial button.
- The maximum total count of numbers called in parallel is 16. This can occur in the case of group call and multiple called users assigned to one quick dial button.

Directory

This tab helps you configure a structured user list to be displayed. Create any count of groups and add any count of phonebook users to groups. No user can be assigned more times to a group, but one user can be added to multiple groups at the same time.


Basic Settings
Root Folder Display: Cards (1 column)
Directory Image Display ☑

- **Root Folder Display** – Select the type of directory root folder display on the device home page. Choose Cards (larger image) or classic item list (the item list image display then obeys the Show images setting. The setting will not be applied until the user goes to another section of the graphic interface (to Search, e.g.).
- **Directory Image Display** – Choose whether or not the images in the directory display shall be shown in the item list display.



Root Folder Display: Cards (1 column)

Directory Image Display ☑

☐ 1st Floor ★
  ☐ Ian Twain ☆
☐ Charles May ★
☐ 2nd Floor ☆
  ☐ John Blead ☆
  ☐ Otto Dixon ☆
☐ Reception ☆
  ☐ Amanda Kheel ☆
  ☐ Samantha McDonut ☆
☐ Amanda Kheel ☆
☐ Button 1 ☆
☐ Flip Chart ☆
☐ Gordon Tenant ☆
☐ Ian Twain ☆
☐ Indoor View ☆
☐ James Dean ☆
☐ John Blead ☆
☐ Otto Dixon ☆
☐ Samantha McDonut ☆

The created folders and users are displayed to the left. Click 📁 to add a folder. Click 🗑 to remove a directory including users and groups. Click ✎ to rename a group. Click ✥ to move a user from the main tree to a folder.

The users assigned to the selected group are displayed to the right. Click 👤+ to add a user to the group; yet the user remains in the phonebook main tree. Press 💡 to highlight the first item in the group on the display. Click 🗑 to remove a user.

The groups and users are arranged in the alphabetical order on the display. Click ☆ to assign a priority. The directory items have 8 possible priorities. Priority ☆ 1 places the item on the top of the list. No priority puts it on the end of the list. Multiple items with identical priorities, if any, are grouped and arranged alphabetically.

⚠ **Caution**

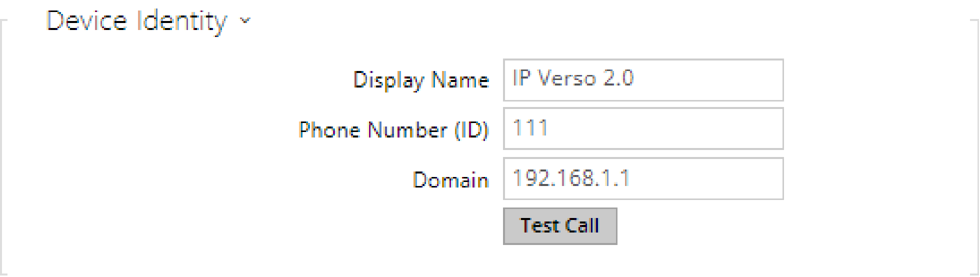
- Remember to save the phonebook changes.
- The setting (photos, root folder, content) display changes are not applied until you go to the search or dialing menu.

5.3.3 SIP 1 / SIP 2

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

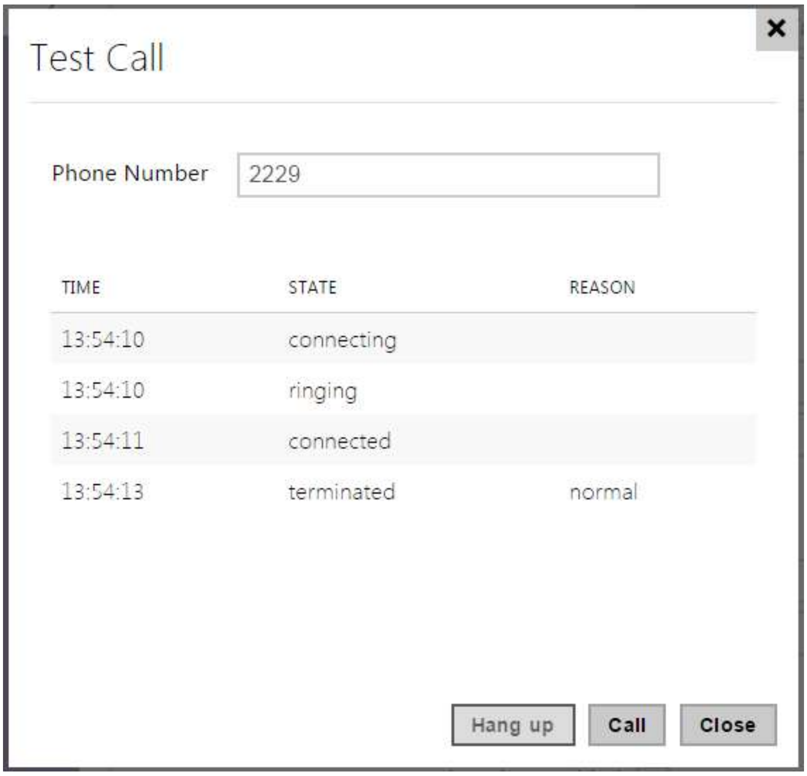
☑ SIP Account Enable

- **Enable SIP account** – allow the SIP account use for calling. If disallowed, the account cannot be used for making outgoing calls and receiving incoming calls.



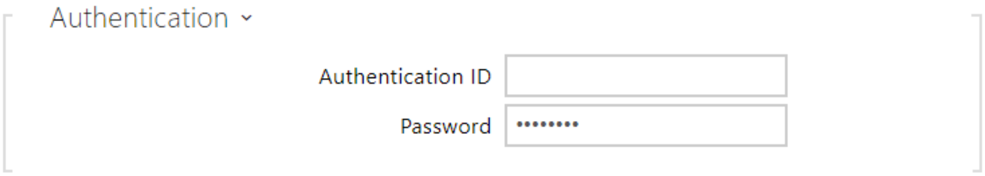
Display Name IP Verso 2.0
Phone Number (ID) 111
Domain 192.168.1.1

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



Phone Number 2229

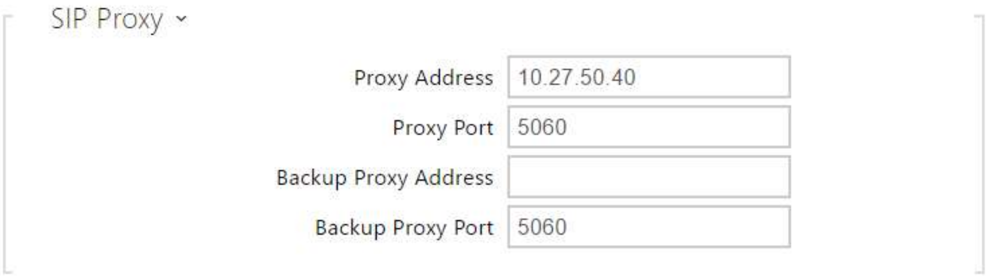
TIME	STATE	REASON
13:54:10	connecting	
13:54:10	ringing	
13:54:11	connected	
13:54:13	terminated	normal



Authentication

Authentication ID	
Password	••••••••

- **Authentication ID** – enter the alternative user ID for the device authentication. Phone Number (ID) will be used if this parameter is left empty.
- **Password** – enter the password for authentication. The parameter is applied on if your PBX requires authentication.

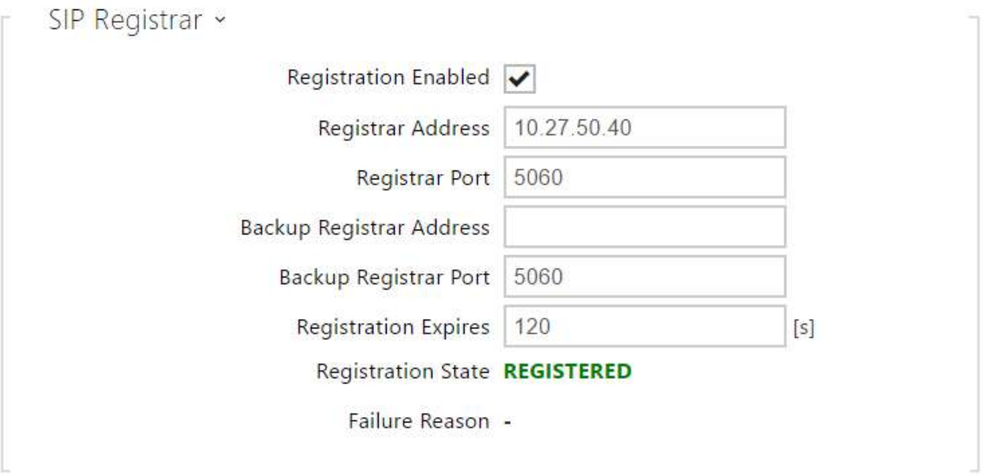


SIP Proxy

Proxy Address	10.27.50.40
Proxy Port	5060
Backup Proxy Address	
Backup Proxy Port	5060

- **Proxy Address** – set the SIP Proxy IP address or domain name.
- **Proxy Port**[*] – set the SIP Proxy port. The device uses the default port according to the transport layer (5060 or 5061) or a port obtained from DNS in case the parameter is empty or set to 0.
- **First Backup Proxy Address** – backup SIP Proxy IP address or domain name. The address is used where the main proxy fails to respond to requests. If the domain name is set and the backup SIP Proxy port number is not filled in here, the resultant backup SIP Proxy IP address will be set according to the NAPTR and SRV record data obtained from the DNS for the given name. If the DNS fails to provide such data or the backup SIP Proxy port number is set, the address from record A is used for the given name.
- **First Backup Proxy Port** – set the backup SIP Proxy port. In case the parameter is empty or set to 0, the device tries to set the port number according to the NAPTR and SRV record data obtained from the DNS. If the DNS fails to provide these records, the default port number is set based on the transport layer (5060 for UDP and TCP, 5061 for TLS).
- **Second Backup Proxy Address** – backup SIP Proxy IP address or domain name. The address is used where the main proxy fails to respond to requests. If the domain name is set and the backup SIP Proxy port number is not filled in here, the resultant backup SIP Proxy IP address will be set according to the NAPTR and SRV record data obtained from the DNS for the given name. If the DNS fails to provide such data or the backup SIP Proxy port number is set, the address from record A is used for the given name.
- **Second Backup Proxy Port** – set the backup SIP Proxy port. In case the parameter is empty or set to 0, the device tries to set the port number according to the NAPTR and SRV

record data obtained from the DNS. If the DNS fails to provide these records, the default port number is set based on the transport layer (5060 for UDP and TCP, 5061 for TLS).



SIP Registrar

Registration Enabled	☑
Registrar Address	10.27.50.40
Registrar Port	5060
Backup Registrar Address	
Backup Registrar Port	5060
Registration Expires	120 [s]
Registration State	REGISTERED
Failure Reason	-

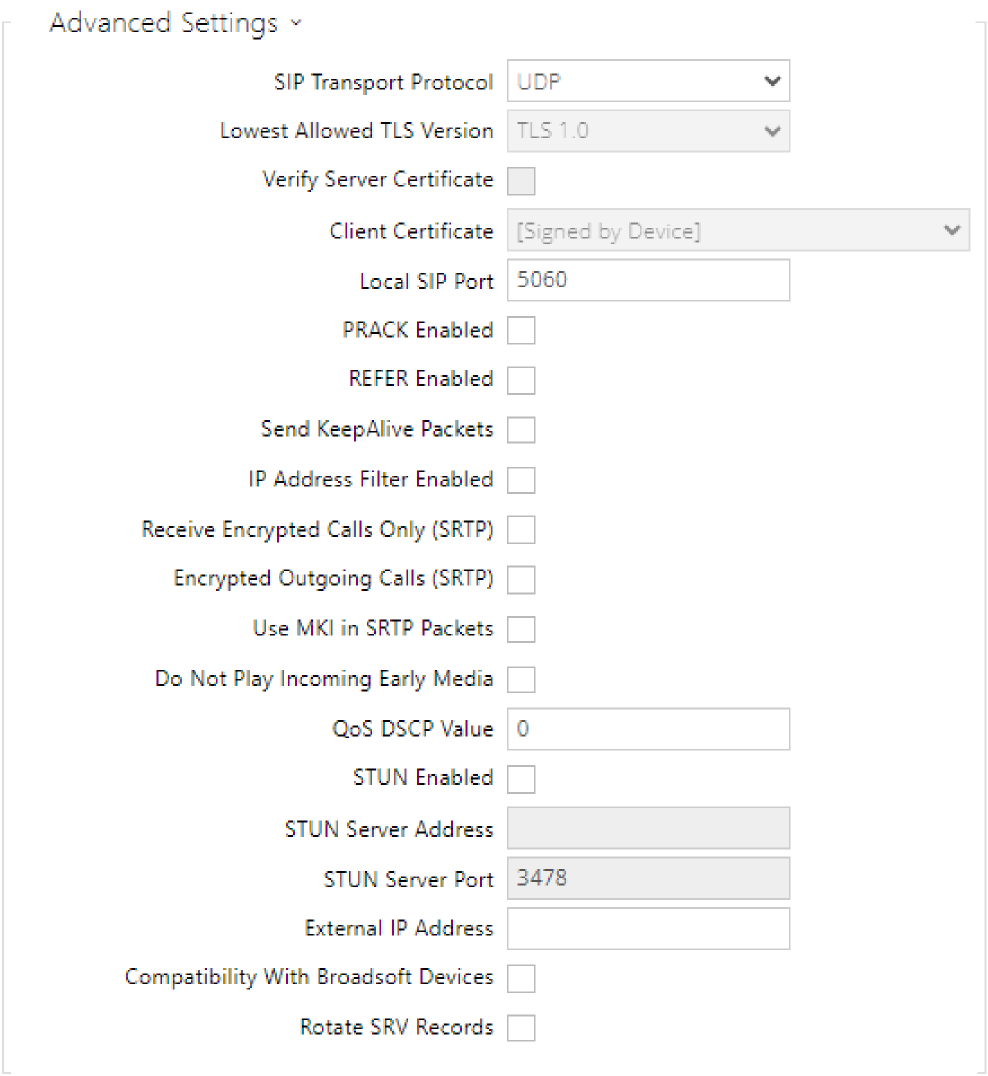
- **Registration Enabled** – enable intercom registration with the set SIP Registrar.
- **Registrar Address** – set the SIP Registrar IP address or domain name.
- **Registrar Port*** – set the SIP Registrar port. The device uses the default port according to the transport layer (5060 or 5061) or a port obtained from DNS in case the parameter is empty or set to 0.
- **Backup Registrar Address** – set the SIP registrar IP address or domain name to be used where the main registrar fails to respond to requests.
- **Backup Registrar Port*** – set the backup SIP registrar port. The device uses the default port according to the transport layer (5060 or 5061) or a port obtained from DNS in case the parameter is empty or set to 0.
- **Registration Expires** – define the registration expiry, which affects the network and SIP Registrar load by periodically sent registration requirements. The SIP Registrar can modify the expiry limit without letting you know.
- **Registration State** – display the current registration state (unregistered, registering..., registered, unregistering...).
- **Failure Reason** – display the reason for the last registration attempt failure: the last error reply of the registrar, e.g. 404 Not Found.

Tip

- To set the Outbound Proxy complete the Outbound Proxy address into the Proxy address and Registrar address parameters. Domain = Registrar address.

Caution

- If the **parameter*** is empty or set to 0, the default port is used according to the selected transport protocol (5060 for TCP or UDP, 5061 for TLS).



Advanced Settings

SIP Transport Protocol	UDP
Lowest Allowed TLS Version	TLS 1.0
Verify Server Certificate	☐
Client Certificate	[Signed by Device]
Local SIP Port	5060
PRACK Enabled	☐
REFER Enabled	☐
Send KeepAlive Packets	☐
IP Address Filter Enabled	☐
Receive Encrypted Calls Only (SRTP)	☐
Encrypted Outgoing Calls (SRTP)	☐
Use MKI in SRTP Packets	☐
Do Not Play Incoming Early Media	☐
QoS DSCP Value	0
STUN Enabled	☐
STUN Server Address	
STUN Server Port	3478
External IP Address	
Compatibility With Broadsoft Devices	☐
Rotate SRV Records	☐

- **SIP Transport Protocol** – set the SIP communication protocol: UDP (default), TCP or TLS.
- **Lowest Allowed TLS Version** – define the lowest TLS version to be connected to the devices.
- **Verify Server Certificate** – verify the SIP server public certificate against the CA certificates uploaded in the device.
- **Client Certificate** – specify the client certificate and private key used for verifying the intercom’s authority to communicate with the SIP server.

- **Local SIP Port** – set the local port to be used for SIP signalling. The parameter is not applied until the intercom is restarted. The default value is 5060.
- **PRACK Enabled** – enable the PRACK method for reliable confirmation of SIP messages with codes 101–199.
- **REFER Enabled** – enable call forwarding via the REFER method.
- **Send KeepAlive Packets** – set whether the device should periodically send STUN/CRLF packets to the registrar as well as SIP OPTIONS during calls to keep an already established connection active.
- **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.
- **Receive Encrypted Calls Only (SRTP)** – set that SRTP encrypted calls shall only be received on this account. Unencrypted calls will be rejected. At the same time, TLS is recommended as the SIP transport protocol for higher security.
- **Encrypted Outgoing Calls (SRTP)** – set that outgoing calls shall be SRTP encrypted on this account. At the same time, TLS is recommended as the SIP transport protocol for higher security.
- **Use MKI in SRTP Packets** – enable the use of MKI (Master Key Identifier) if required by the counterparty for master key identification when multiple keys rotate in the SRTP packets.
- **Adaptive Control of Video Quality** – enable the use of extended RTP profile for feedback via the RTCP (RTP/AVPF). Enable the use of interactive video quality control according to RFC-4585 allowing for adaption of the video data flow to the currently available network connection quality.
- **Do Not Play Incoming Early Media** – disable playing of the incoming audio stream before call pick-up (early media), which is sent by some PBXs or other devices. A standard local ringtone is played instead.
- **QoS DSCP Value** – set the SIP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header. Value is entered in decimal format.

✓ **Tip**

Recommended QoS DSCP Values			
	QoS decimal	**QoS hexadecimal**	**Qos DSCP decimal (ToS)**
Signaling	24 / 2624 / 26	18 / 1A18 / 1A	96 / 10496 / 104
Audio	4646	2E2E	184184
Video	4040	2828	160160

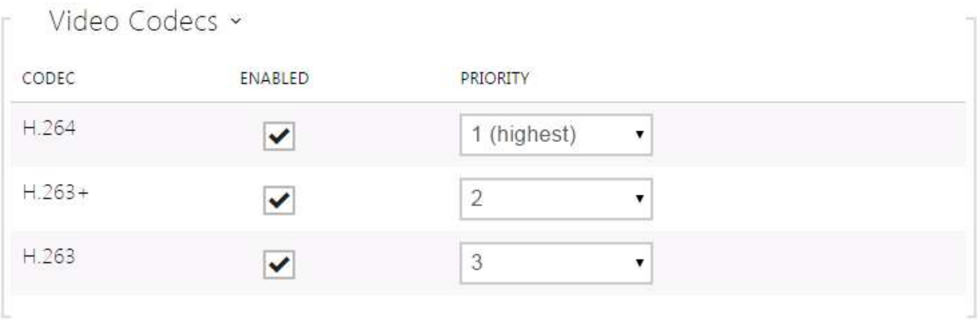
- **STUN Enable –** enable STUN functionality for the SIP account. Address and ports acquired from the configured STUN server will be used in SIP headers and SDP media negotiation.
- **STUN Server Address** – set the IP address of the STUN server that will be used for this SIP account.

- **STUN Server Port** – set the port of the STUN server that will be used for this SIP account.
- **External IP Address** – set the public IP address or name of the router to which your intercom is connected. If the intercom IP address is public, leave this field blank.
- **Compatibility with Broadsoft Devices** – set the Broadsoft PBX compatibility mode. Having received re-invite from a PBX in this mode, the intercom replies by repeating the last sent SDP with currently used codecs instead of sending a complete offer.
- **Rotate SRV Records** – allow SRV record rotation for SIP Proxy and Registrar. This is an alternative method of transition to backup servers in the event of main server failure or unavailability.

Caution

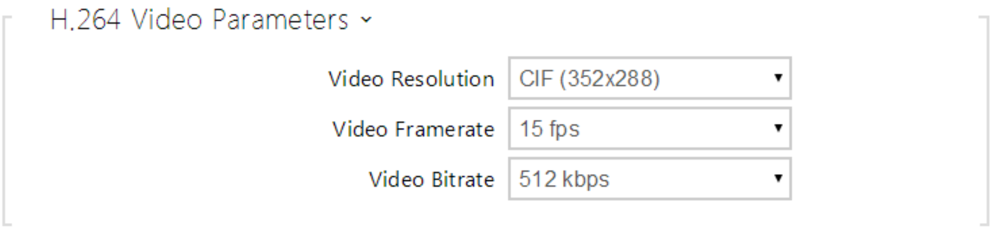
- To use the NAPTR / SRV DNS query, cancel the Proxy/Registrar port setting.

Video


Video Codecs

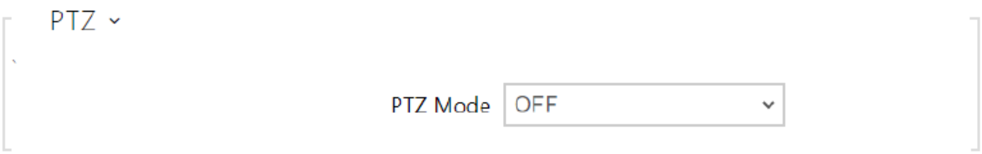
CODEC	ENABLED	PRIORITY
H.264	☑	1 (highest)
H.263+	☑	2
H.263	☑	3

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


H.264 Video Parameters

Video Resolution: CIF (352x288)
Video Framerate: 15 fps
Video Bitrate: 512 kbps

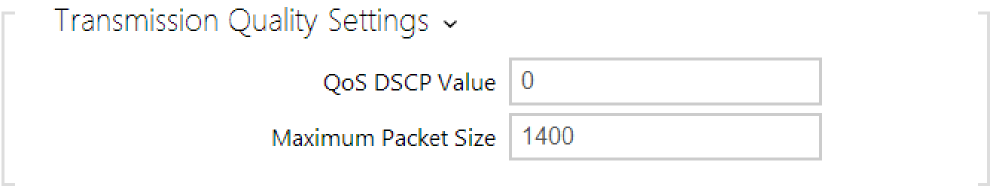
- **Video Resolution** – set the video resolution for phone calls.
- **Video Framerate** – set the video frame rate for phone calls.
- **Video Bitrate** – set the video stream bit rate for phone calls.


PTZ

PTZ Mode: OFF

- **PTZ Mode** – enable the PTZ (Pan-Tilt-Zoom) function to control the camera display area during the call via DTMF (**GOLD** license required) from your IP phone numeric keypad. If the PTZ mode is enabled, you can control the camera via your IP phone numerical keypad. Press the ***** key to enable/disable PTZ. The meanings of the IP phone keys in the PTZ mode are as follows:

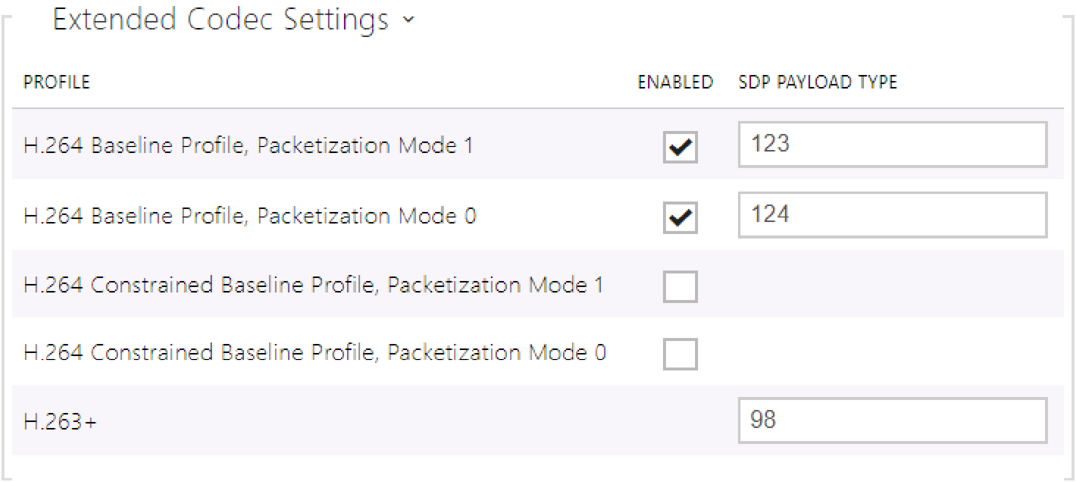
IP phone key	PTZ mode function
*****	Enable/disable PTZ
1	Zoom in
3	Zoom out
2	Move zoom region up
4	Move zoom region to the left
6	Move zoom region to the right
8	Move zoom region down
5	Return to initial state



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. The recommended QoS values valid for signaling, audio and video are shown in the table above.
- **Maximum Packet Size** – set the size limit for the video RTP packets to be sent.

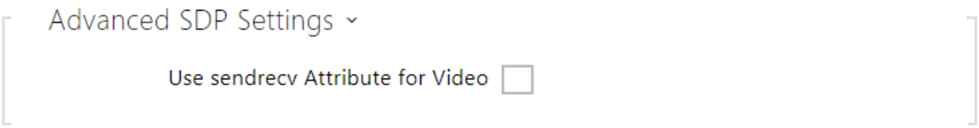


Extended Codec Settings

PROFILE	ENABLED	SDP PAYLOAD TYPE
H.264 Baseline Profile, Packetization Mode 1	☑	123
H.264 Baseline Profile, Packetization Mode 0	☑	124
H.264 Constrained Baseline Profile, Packetization Mode 1	☐	
H.264 Constrained Baseline Profile, Packetization Mode 0	☐	
H.263+		98

There can be different extended codec settings for different device types.

- **H.264 Baseline Profile, Packetization Mode 1**
- **H.264 Baseline Profile, Packetization Mode 0**
- **H.264 Main Profile, Packetization Mode 1**
- **H.264 Main Profile, Packetization Mode 0**
- **H.264 High Profile, Packetization Mode 1**
- **H.264 High Profile, Packetization Mode 0**
- **H.264 Constrained Baseline Profile, Packetization Mode 1**
- **H.264 Constrained Baseline Profile, Packetization Mode 0**
  - **Enabled** – enable the packetization mode and set the payload type for each codec. The payload type can be selected automatically in case it cannot be set manually.
  - **SDP Payload Type** – set the payload type for video codec H.264 (packetization mode 1). Set a value from the range of 96 through 127, or 0 to disable this codec option.
- **H.263+**
  - **SDP Payload Type** – set the payload type for video codec H.263+. Set a value from the range of 96 through 127.



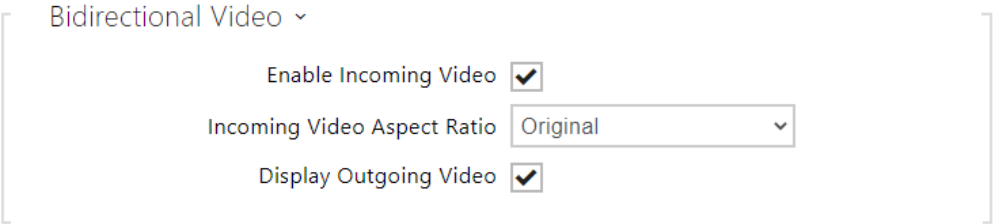
Advanced SDP Settings

Use sendrecv Attribute for Video ☐

- **Use sendrecv Attribute for Video** – the setting was earlier named Compatibility with Polycom phones. This setting provides compatibility with some third party devices (Polycom/Cisco and others). In this mode, the intercom sends sendrecv instead of sendonly in the SDP message in the codec offer for video.

Tip

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



Bidirectional Video

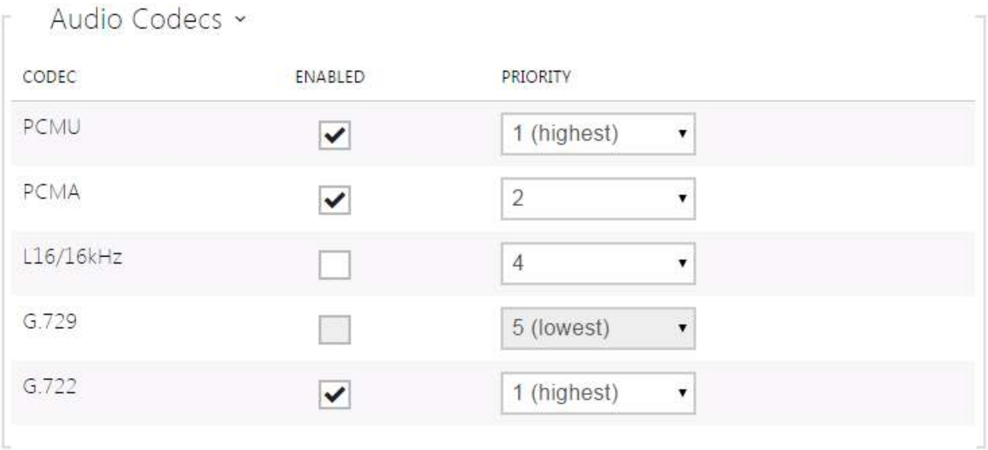
Enable Incoming Video ☑

Incoming Video Aspect Ratio: Original

Display Outgoing Video ☑

- **Enable Incoming Video** – if this mode is on, the intercom displays the opponent's video during a call if the other party allows so.
- **Incoming Video Aspect Ratio** – set the preferred incoming video aspect ratio to be displayed. If an aspect ratio other than the default one is selected, the video is cropped to fill the whole display width in the new aspect ratio.
- **Display Outgoing Video** – select whether or not the intercom shall display the preview of the video to be sent during a call.

Audio

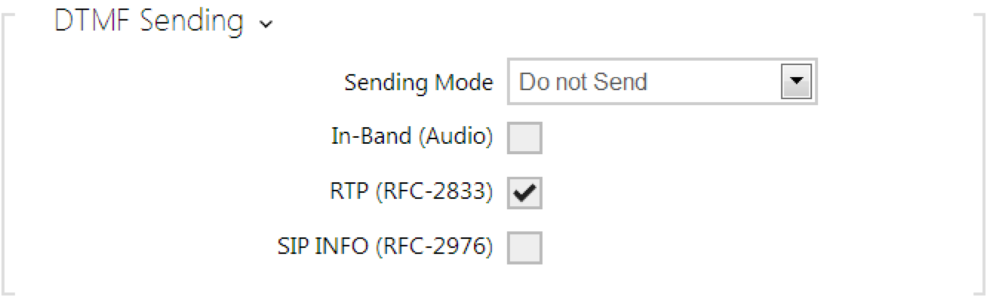


Audio Codecs

CODEC	ENABLED	PRIORITY
PCMU	☑	1 (highest)
PCMA	☑	2
L16/16kHz	☐	4
G.729	☐	5 (lowest)
G.722	☑	1 (highest)

- Enable/disable the use of audio codecs for call setups and set their priorities. Broadband codecs L16 and G.722 are available in selected intercom models only. Codec G.729 is available for all the 2N IP intercoms.

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



DTMF Sending ⌄

Sending Mode: Do not Send

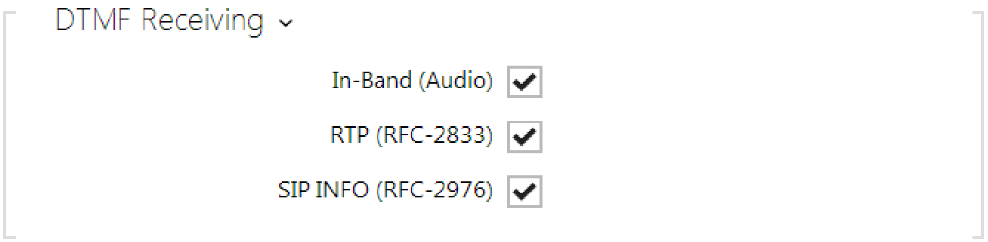
In-Band (Audio) ☐

RTP (RFC-2833) ☑

SIP INFO (RFC-2976) ☐

- **Sending Mode** – define whether it is 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.



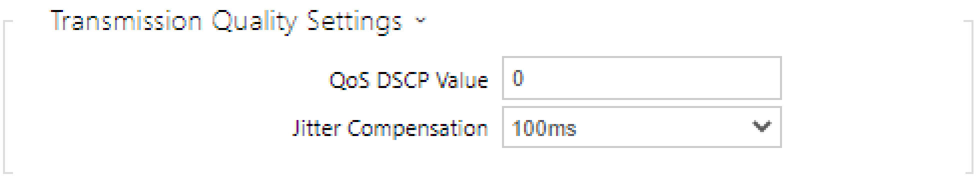
DTMF Receiving ⌄

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. Value is entered in decimal format.

The recommended QoS values valid for signaling, audio and video are shown in the table above.

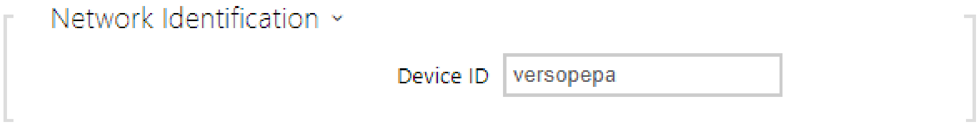
- **Jitter Compensation** – set the buffer capacity for jitter compensation in audio packet transmissions. A higher capacity improves the transmission resistance at the cost of a greater sound delay.

5.3.4 Local Calls

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

☑ Enable Local Calls

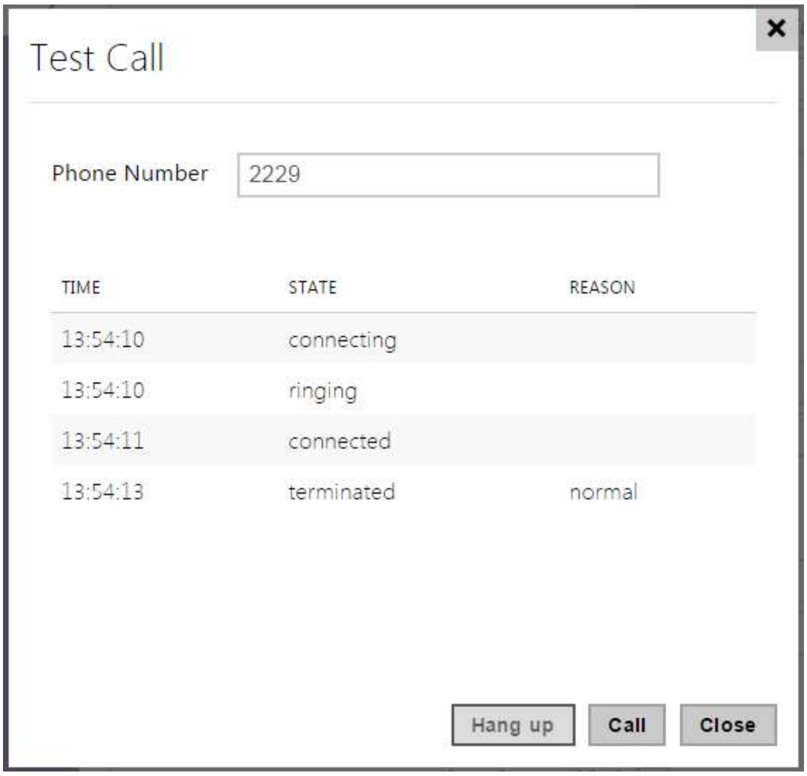
- **Enable Local Calls** – enable calls between 2N devices in the LAN. With this function off, the other LAN devices cannot locate this device, i.e. cannot call the device in the device:device_ID format.



Network Identification

Device ID: versopepa

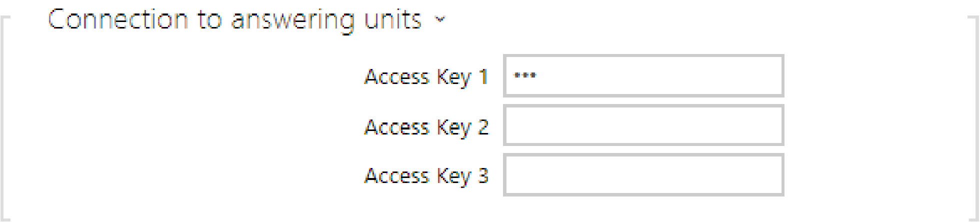
- **Device ID** – set the device ID to be displayed in the LAN device list in all the 2N devices in one and the same LAN. You can direct a call to this device by setting the user phone number as device:device_ID in these devices.
- **Test call** – display a dialogue window enabling you to make a test call to a selected phone number, see below.



Test Call

Phone Number 2229

TIME	STATE	REASON
13:54:10	connecting	
13:54:10	ringing	
13:54:11	connected	
13:54:13	terminated	normal



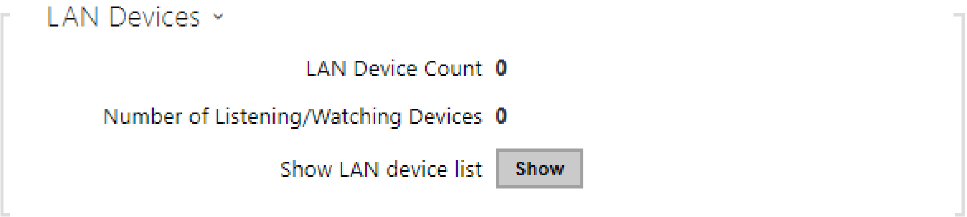
Connection to answering units

Access Key 1 •••

Access Key 2

Access Key 3

- **Access Key 1-3** – set the access key to be shared by the intercom and 2N answering unit. If the access keys do not match in the intercom and2N answering unit, the intercom cannot call the 2N answering unit and the 2N answering unit cannot receive video from the intercom. Each intercom can be assigned up to three access keys and thus become a member of up to three independent 2N answering unit groups. The Access key length is up to 63 characters.



LAN Devices

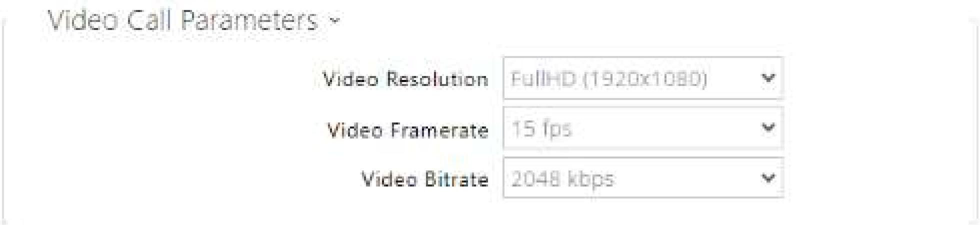
LAN Device Count: 0

Number of Listening/Watching Devices: 0

Show LAN device list: Show

- **LAN Device Count**– display the current count of local 2N answering units connected to the intercom, i.e. those registered with the intercom.
- **Number of Listening/Watching Devices** – display the current count of 2N answering units watching video streams from the intercom.
- **Show LAN device list** – display the list of local 2N devices.

Video



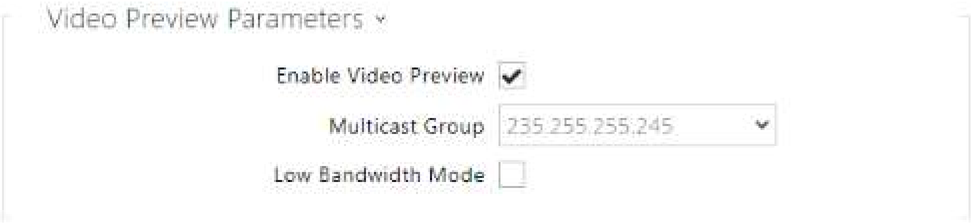
Video Call Parameters

Video Resolution: FullHD (1920x1080)

Video Framerate: 15 fps

Video Bitrate: 2048 kbps

- **Video Resolution** – set the resolution of the video stream to be sent to 2N answering unit.
- **Video Framerate** – set the framerate of the video stream to be sent to 2N answering unit.
- **Video Quality** – set the quality of the MJPEG video stream to be sent to 2N answering units.



Video Preview Parameters

Enable Video Preview: ☑

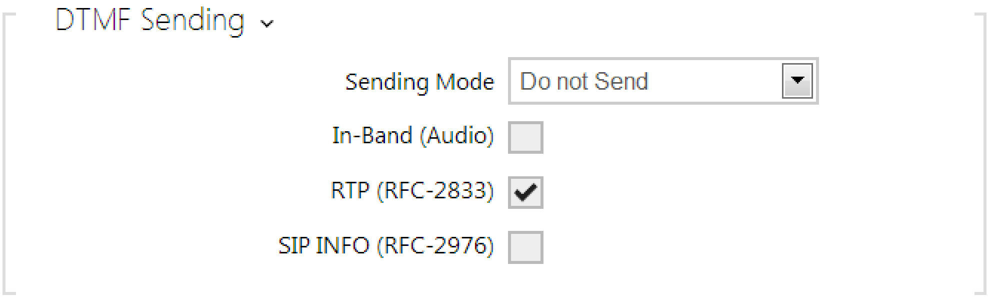
Multicast Group: 235.255.255.245

Low Bandwidth Mode: ☐

- **Enable Video Preview** – enable video preview multicast transmission.
- **Multicast Group** – set the multicast address to which the intercom video stream shall be sent. Select one of the 8 preset addresses or set the mode in which the intercom selects the address automatically.

Audio

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

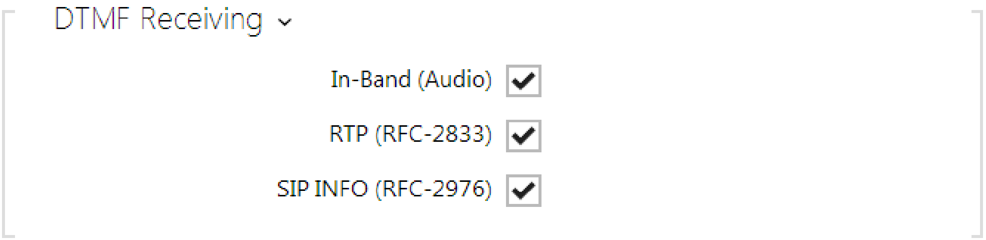


DTMF Sending

Sending Mode: Do not Send
In-Band (Audio) ☐
RTP (RFC-2833) ☑
SIP INFO (RFC-2976) ☐

- **Sending Mode** – define whether it is 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.

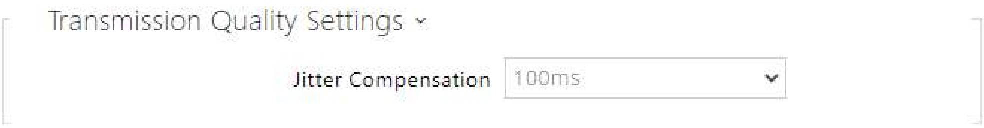
The tab below helps you define how DTMF characters shall be received from the intercom. Check the DTMF receiving options and settings of the opponent to make the function work properly.



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.



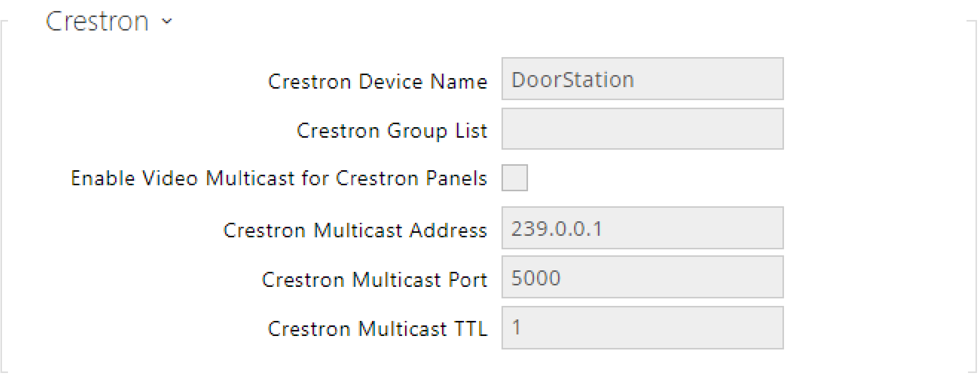
Transmission Quality Settings

Jitter Compensation: 100ms

- **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.

5.3.5 Crestron

- **Enable Crestron Network Discovery** – enable 2N IP intercom identification within the Crestron network.



Crestron Device Name: DoorStation
Crestron Group List:
Enable Video Multicast for Crestron Panels: ☐
Crestron Multicast Address: 239.0.0.1
Crestron Multicast Port: 5000
Crestron Multicast TTL: 1

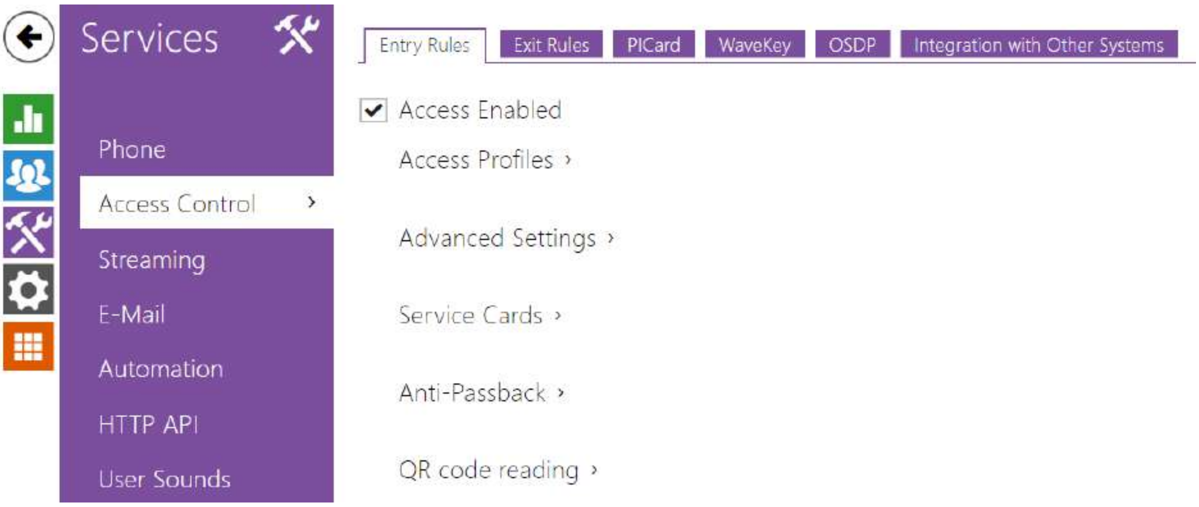
- **Crestron Device Name** – select the device name.
- **Crestron Group List** – select the group name list with comma as a separator.
- **Enable Video Multicast for Crestron panels** – enable video multicast for Crestron panels, allowing for multiple Crestron devices to receive the same video stream without wasting the local network bandwidth.
- **Crestron Multicast Address** – set the multicast address to be used for multicast video for Crestron devices.
- **Crestron Multicast Port** – set the multicast port to be used for multicast video for Crestron devices.
- **Crestron Multicast TTL** – set the Time To Live (TTL) value to be used for sending video early media for Crestron devices.

5.4 Services

Here is what you can find in this section:

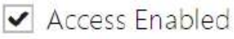
5.4.1 Access Control

Access Control helps you manage accesses and verify user authentications.



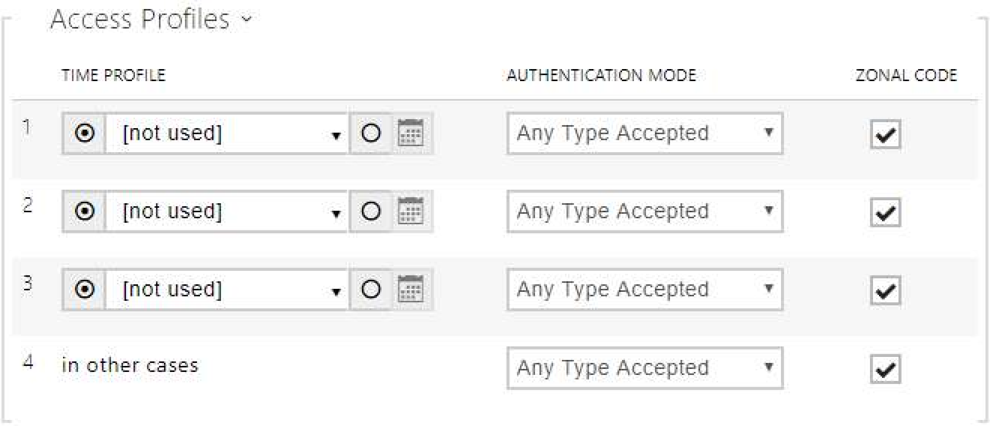
☑ Access Enabled

Entry Rules



☑ Access Enabled

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



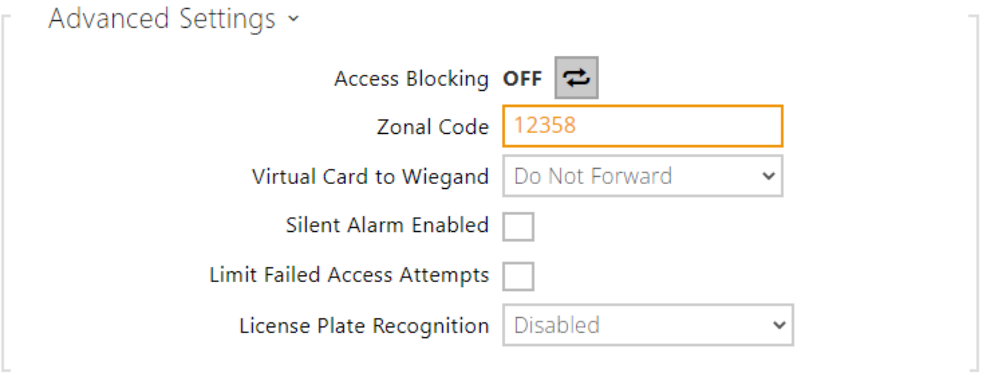
Access Profiles ˅

	TIME PROFILE	AUTHENTICATION MODE	ZONAL CODE
1	◉ [not used] ○	Any Type Accepted	☑
2	◉ [not used] ○	Any Type Accepted	☑
3	◉ [not used] ○	Any Type Accepted	☑
4	in other cases	Any Type Accepted	☑

- **Time Profile** – choose one or more time profiles to be applied. Set the time profiles in Directory / Time profiles.
  - ◉ – select global profiles from Directory > Time Profiles.
  - ○ – individual time profile for this specific element.

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

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



Advanced Settings

Access Blocking OFF

Zonal Code 12358

Virtual Card to Wiegand Do Not Forward

Silent Alarm Enabled ☐

Limit Failed Access Attempts ☐

License Plate Recognition Disabled

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

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

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

- **License Plate Recognition** – choose the scenario after the license plate is recognized.

Caution

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

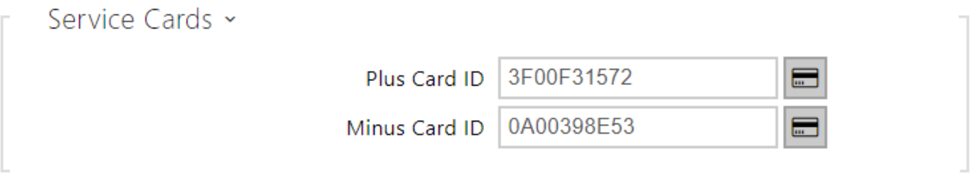
    - **Disabled**
    - **Opening by License Plate –** The door is unlocked if the entry in the directory with the recognized license plate has currently the entry/exit right.
    - **LPR Multifactor** – this option is only available if Multifactor Authentication of License Plates beta function is activated.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

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

In case the function is on, the event is recorded into the LicensePlateRecognized history when a valid HTTP request has been received. If an image is sent within the HTTP request (photo part or whole photo of the license plate detecting scene), it is saved. The last five photos are stored in the device memory and can be retrieved via an HTTP request sent to api/lpr/image available in **2N Access Commander**.

Warning

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

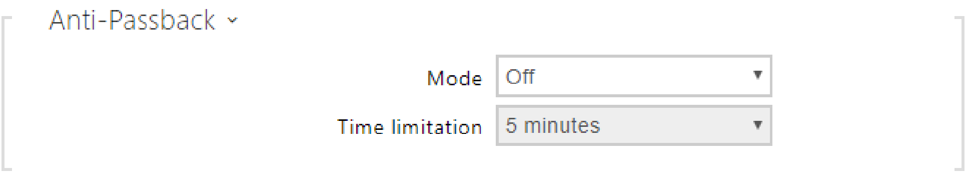

Service Cards

Plus Card ID 3F00F31572

Minus Card ID 0A00398E53

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

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

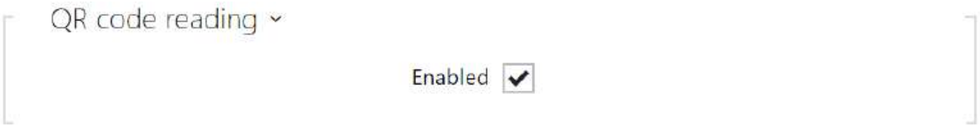

Anti-Passback

Mode Off

Time limitation 5 minutes

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

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



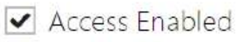
Enabled ☑

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

Caution

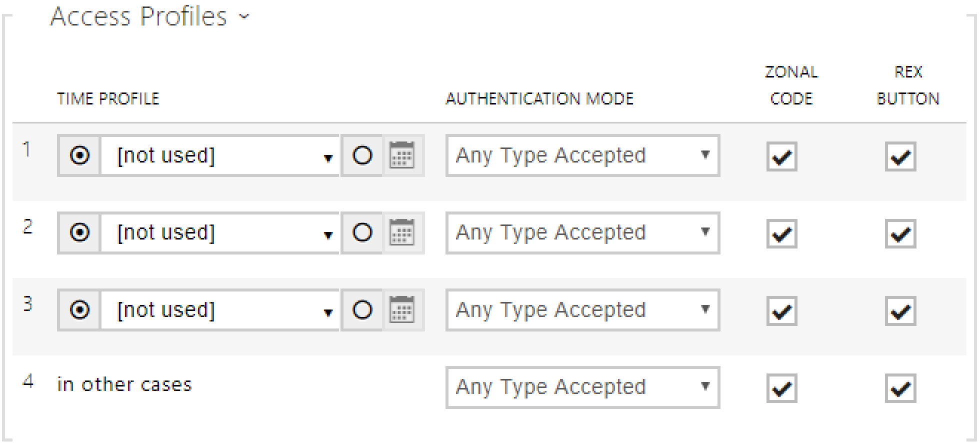
- Do not use privacy masking in combination with QR code reading to make the QR code reading function work properly.
- For increased security, limit the count of unsuccessful accesses in the Advanced Settings block above.
- The QR code reading function is only available in models equipped with the ARTPEC-7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

Exit Rules



☑ Access Enabled

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

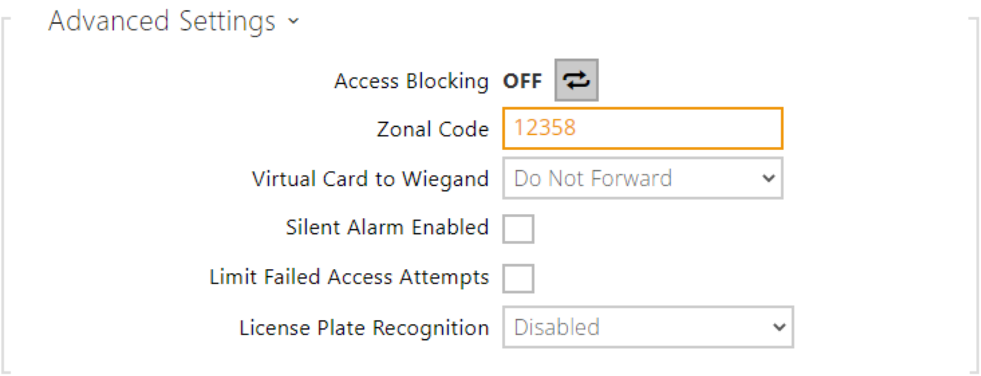


Access Profiles ˅

	TIME PROFILE		AUTHENTICATION MODE	ZONAL CODE	REX BUTTON
1	◉ [not used] ▾	○	Any Type Accepted ▾	☑	☑
2	◉ [not used] ▾	○	Any Type Accepted ▾	☑	☑
3	◉ [not used] ▾	○	Any Type Accepted ▾	☑	☑
4	in other cases		Any Type Accepted ▾	☑	☑

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

> ⚠ **Caution**
>
> - If the time profile is unset, the authentication mode is ignored on the given row.



Advanced Settings

Access Blocking OFF

Zonal Code 12358

Virtual Card to Wiegand Do Not Forward

Silent Alarm Enabled ☐

Limit Failed Access Attempts ☐

License Plate Recognition Disabled

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

Caution

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

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

Caution

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

  - **Disabled**
  - **Opening by License Plate –** The door is unlocked if the entry in the directory with the recognized license plate has currently the entry/exit right.

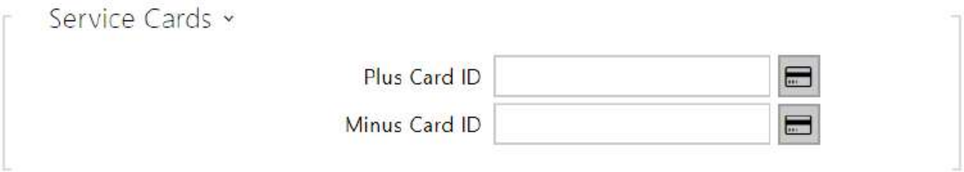
- **LPR Multifactor** – this option is only available if Multifactor Authentication of License Plates beta function is activated. Enable permanent access blocking and permanently disable Bluetooth (WaveKey) authentication. Once the license plate is read, its user will be assigned a temporary (60-second) exception and the Wave Key function will be activated for the same time. Access will only be granted to the read license plate user who authenticates using another authenticating method (WaveKey/QR code) within 60 seconds. Users with a permanent exception will be granted access during the whole access blocking period, but will be able to authenticate themselves using WaveKey too within 60 seconds after their license plates are recorded.
  Every next car license plate will cancel the preceding temporary exception and, if there is a user with the newly accepted license plate, a temporary exception is assigned to this user.

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

In case the function is on, the event is recorded into the LicensePlateRecognized history when a valid HTTP request has been received. If an image is sent within the HTTP request (photo part or whole photo of the license plate detecting scene), it is saved. The last five photos are stored in the device memory and can be retrieved via an HTTP request sent to api/lpr/image available in **2N Access Commander**.

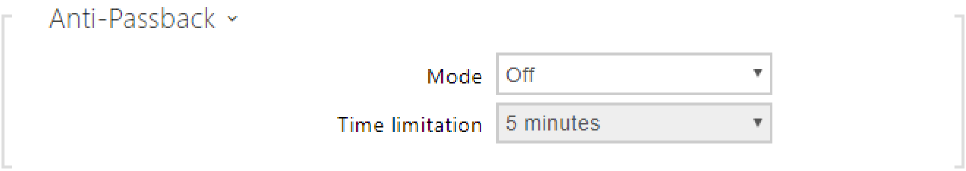
Warning

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



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

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



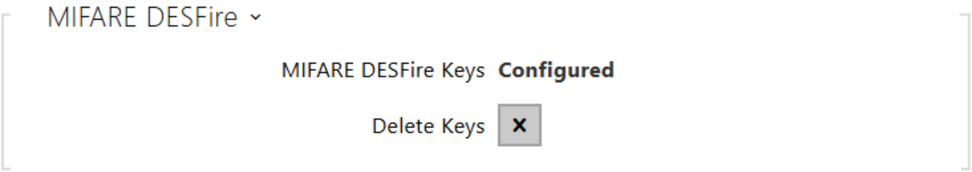
Mode: Off

Time limitation: 5 minutes

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

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

Secure Cards



MIFARE DESFire Keys: Configured

- **MIFARE DESFire Keys** – indicates the state of the configuration for MIFARE DESFire cards reading. If any of the MIFARE DESFire reading parameters is missing or invalid in the configuration, the state is *Not configured*. If all the parameters are present and valid, the state is *Configured.*

Caution

- If you use the MIFARE DESFire cards, remember to disable reading of insecure CSNs. Enable the cards in the card reader settings in Hardware > Extending modules.

MIFARE DESFire Card Configuration

1. Get ready the MIFARE DESFire card values for access control management.
2. Create an XML file with the below-mentioned structure (example of an XML structure).

   > ⚠ Keep the length and format of the values. If your data value is shorter than the required count of characters, add initial zeros from the left. Enter the values without the hexadecimal prefix.

3. Upload the XML file to the device via System > Maintenance > Configuration > Upload configuration file.
4. Once the XML file has been uploaded, the device restores the configuration. The code segment will be included in the complete configuration file of the device.

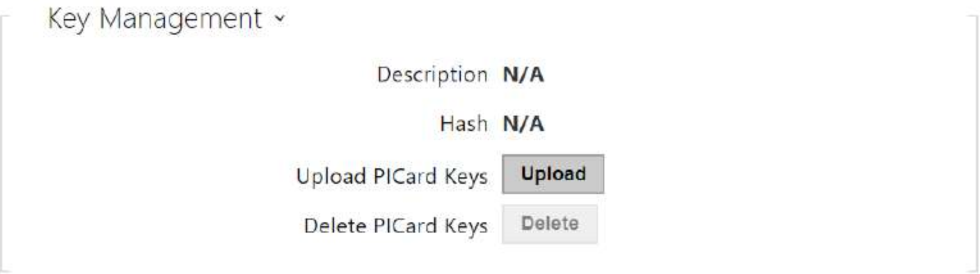
Příklad XML struktury

```
<DeviceDatabase>
    <CardReader>
        <KeyStore>
            <Keys>
                <Desfire>
                    <AID>130586</AID>
                    <KeyNo>01</KeyNo>
                    <AuthKey>B52874F4E3EEE03C349EBB74A3123458</AuthKey>
                    <KeyType>01</KeyType>
                    <AuthMode>01</AuthMode>
                    <FileNo>01</FileNo>
                    <Offset>000000</Offset>
                    <Bits>00000080</Bits>
                    <DecodeASCII>01</DecodeASCII>
                </Desfire>
            </Keys>
        </KeyStore>
    </CardReader>
</DeviceDatabase>
```

Key	Value type/format	Description
AID	3 bytes (6 hexadecimal chars)	**Application Identifier (AID):** Unique app identifier on a MIFARE DESFire card. Every card can include multiple applications and each app has files and keys of its own.

Key	Value type/format	Description
AuthKey	16 bytes (32 hexadecimal chars)	**Authentication Key:** Cryptographic key (AES 128) used for secure authentication and encrypted communication setup on the card.
KeyType	`01` (including initial zeros)	**Key Type:** Define the encryption algorithm used. At present, AES 128 is only supported, for which the value `01` is entered.
AuthMode	`00`: No authentication `01`: AES authentication	**Authentication Mode:** Enable/disable authentication using `AuthKey`. Set `01` for secure access to the files.
FileNo	`00` to `0F`	**File Number:** Identifier of a specific data file within a selected application (AID). There can be up to 32 files in one application.
Offset	2.5 bytes (5 hexadecimal chars)	**Offset:** Set the initial position (in bytes) from which the file data should be read. The value `00000` indicates the file beginning.
Bits	4 bytes (8 hexadecimal chars)	**Bits:** Define how many bits are to be read from the file (starting from the `Offset` position). Set the value in the hexadecimal format.
Decode ASCII	`01`: Enabled `00`: Disabled	**Decoding to ASCII:** Define whether or not the binary data read from the card shall be automatically interpreted and decoded as text characters in the ASCII format.

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



Description N/A
Hash N/A

- **Description** – encryption key name.

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

WaveKey

The **2N IP intercoms** equipped with the Bluetooth module allow for user authentication via the **My2N** application available to devices with iOS 12 and higher (iPhone 4s and higher phones) or Android 6.0 Marshmallow and higher (Bluetooth 4.0 Smart supporting phones).

User Identification (Auth ID)

The **My2N** application authenticates itself with a unique identifier on the intercom side: **Auth ID** (128-bit number) is generated randomly for every user and **paired** with the intercom user and its mobile device.

Note

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

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

Encryption Keys and Locations

The **My2N** – intercom communication is always encrypted. **My2N** cannot authenticate a user without knowing the encryption key. The primary encryption key is automatically generated upon the intercom first launch and can be re-generated manually any time later. Together with AuthID, the primary encryption key is transmitted to the mobile device for pairing.

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

Pairing

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

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

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

- Location identifier
- Location encryption key
- User Auth ID

Encryption Key for Pairing

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

Encryption Key Administration

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

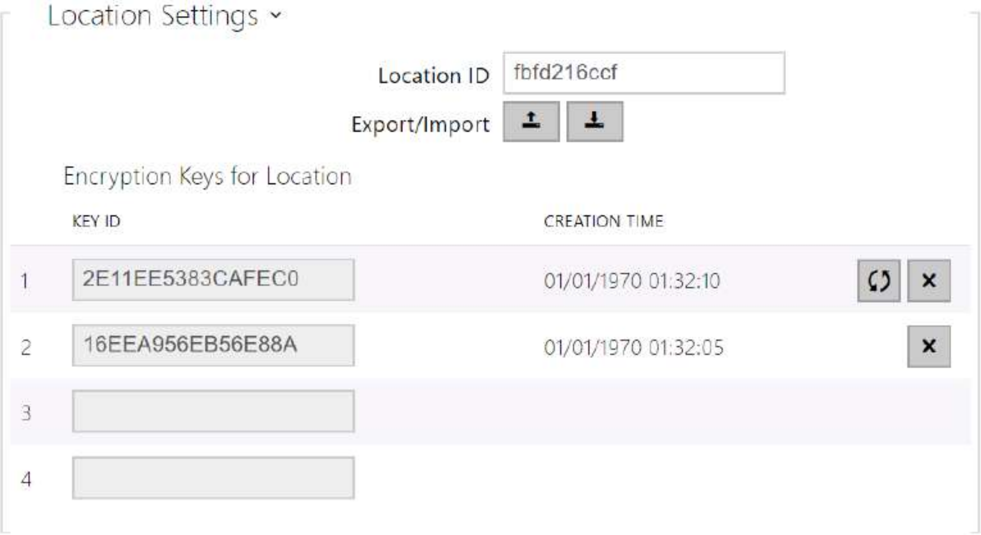
ⓘ **Note**

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

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

When a key is deleted, the **My2N** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **My2N** application.

List of Parameters


Location Settings

Location ID: fbfd216ccf

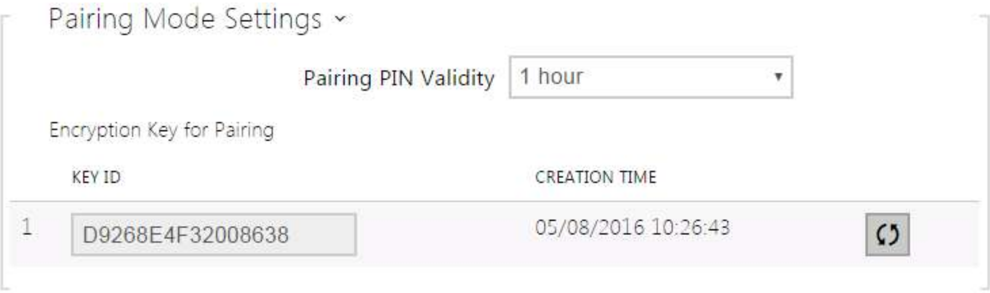
Export/Import

Encryption Keys for Location

	KEY ID	CREATION TIME
1	2E11EE5383CAFEC0	01/01/1970 01:32:10
2	16EEA956EB56E88A	01/01/1970 01:32:05
3		
4		

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

- **Restore primary key** – by generating a new primary encryption key you delete the oldest secondary key. Thus, the **My2N** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **My2N** application.
- **Delete primary key** – delete the primary key to prevent the users that still use this key from authentication.
- **Delete secondary key** – the **My2N** users that still use this key will not be able to authenticate themselves unless they have updated the encryption keys in their mobile devices before deletion. The mobile device keys are updated at every use of the **My2N** application.


Pairing Mode Settings

Pairing PIN Validity: 1 hour

Encryption Key for Pairing

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

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

Tip

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

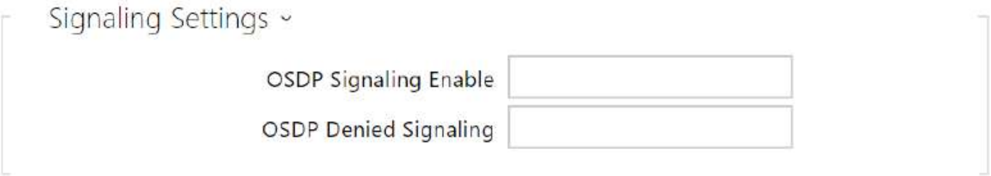
1. Delete the Mobile Key Auth ID value for the user to block the lost phone and avoid misuse.
2. Re-generate the primary encryption key (optionally) to avoid misuse of the encryption key stored in the mobile device.

Warning

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

OSDP

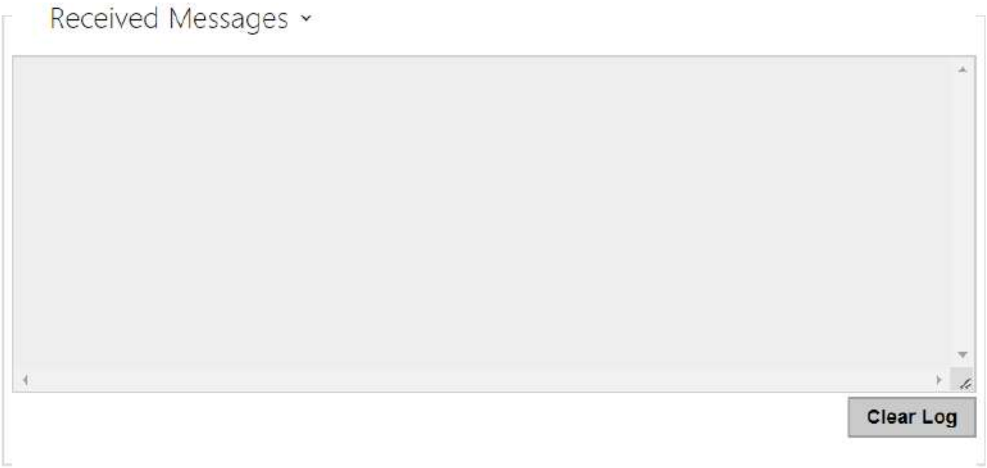
The OSDP provides secure communication for sending such login data as access card IDs or PIN codes between the connected OSDP device (control panel, door controller) and a **2N LTE intercom**. The goal is to enable signaling on the **2N LTE intercom** based on the counterparty's response to the card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



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

⚠ **Note**

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



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

The received message is displayed in the following format:

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

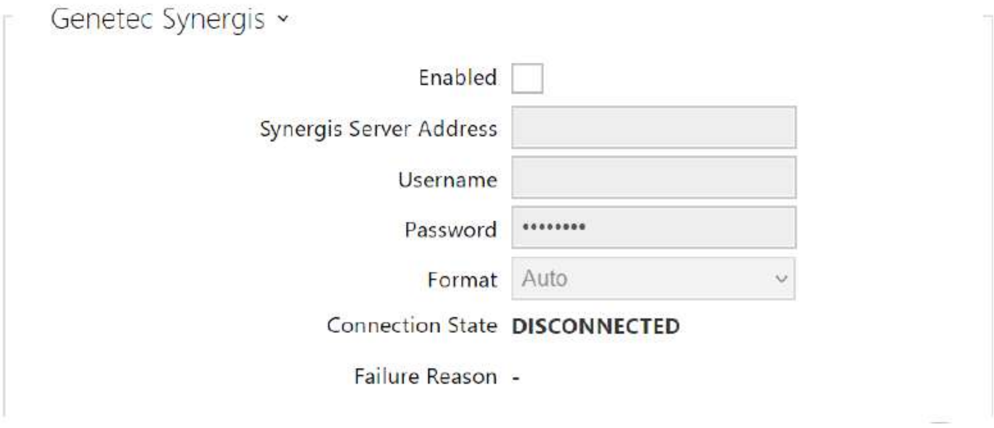
A part of the message (without the time value) is used as the definition string, whose length may not exceed 255 characters, e.g.: led(0,0,0,0,0,0,0,0,1,1,1,1,1) or buz(0,2,1,1,1). Having evaluated a match on the counterparty, the device responds with an adequate signaling. Any part of the definition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

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

⚠ **Note**

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

Integration with Other Systems

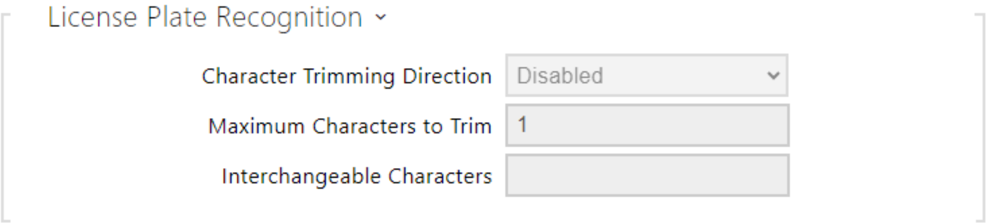


Genetec Synergis ˅

Enabled	☐
Synergis Server Address	
Username	
Password	••••••••
Format	Auto
Connection State	DISCONNECTED
Failure Reason	-

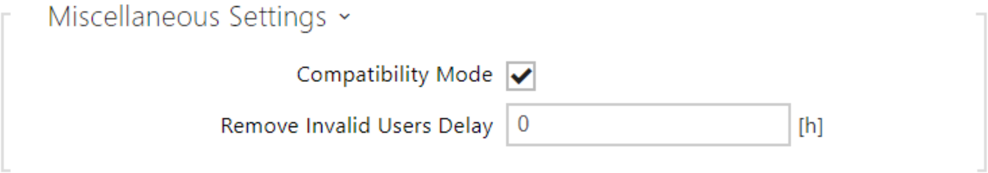
- **Enabled** – enable connection with the Genetec Synergis external security system.
- **Synergis Server Address** – Synergis server IP address or domain name.
- **Username** – authentication user name.
- **Password** – authentication password.
- **Format** – set the card reading format for sending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

Advanced Folder



Character Trimming Direction: Disabled
Maximum Characters to Trim: 1
Interchangeable Characters:

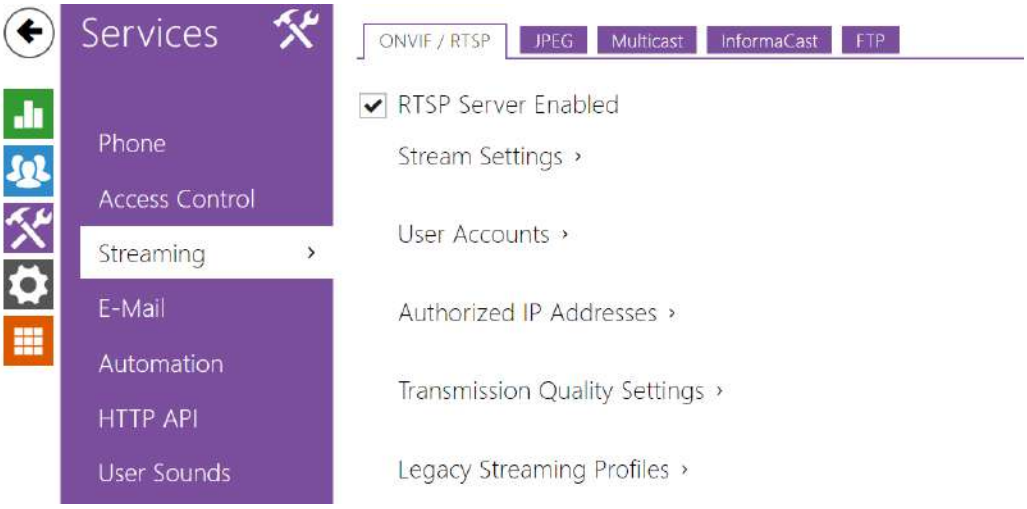
- **Character Trimming Direction** – choose whether trimming of recognized license plates is permitted, and specify the direction from which trimming may be attempted.
- **Maximum Characters to Trim** – choose the maximum number of characters to trim, either 1 or 2. Trimming occurs at the beginning or end of the string based on the selected **Character Trimming Direction**.
- **Interchangeable Characters** – define interchangeable character pairs for the purposes of the License Plate Recognition function. The first character in a pair will be replaced with the second character for the purposes of matching saved license plates. A dash separates the characters in a pair. Multiple pairs can be entered and separated by a comma. Whitespace is ignored. Example:<br>O-0, I-1<br><br>.



Compatibility Mode ☑
Remove Invalid Users Delay: 0 [h]

- **Compatibility Mode** – support older card reading modes. This mode is not recommended in combination with the PICard cards. If this mode is off, the card numbers must be a perfect match for successful authorization.
- **Remove Invalid Users Delay** – set the delay after which users with invalid access and enabled automatic removal are removed from the device directory.

5.4.2 Streaming



☑ RTSP Server Enabled

The **2N LTE 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 LTE intercom** 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 LTE intercom** 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 LTE intercom** 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 LTE intercoms** are ONVIF compatible and fully implement the ONVIF Profile T.
- **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 LTE intercoms**, 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

ONVIF/RTSP

The **2N LTE 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.

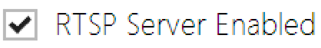
To request a stream with the defined parameters, specify the video codec type, image resolution, frames per second and bitrate in URL, e.g.: rtsp://IP_ADDRESS/media?audio=1&vcodec=h264&vres=640x480&fps=15&vbr=2048.

Parameter	Mandatory	Expected Values	Default Value	Public	Description
audio	Yes	0, 1	0	True	Selects whether audio is part of the stream or not.
vcodec	Yes	string	disabled	True	Specifies video codec (H.264, MJPEG, MPEG4). The video is not available if the codec is not specified (only audio stream).
vres	No	string	640x480	True	Specifies video resolution. Available resolutions differ based on device model and selected codec.
fps	No	integer	15	True	Specifies video frames per second. Available fps differ based on device model and selected codec.
vbr	No	integer	2048	True	Specifies video bitrate. Available vbr differ based on device model and selected codec.

Or, any of the following RTSP Uri can be used, which allows you to select another codec type regardless of the current setting:

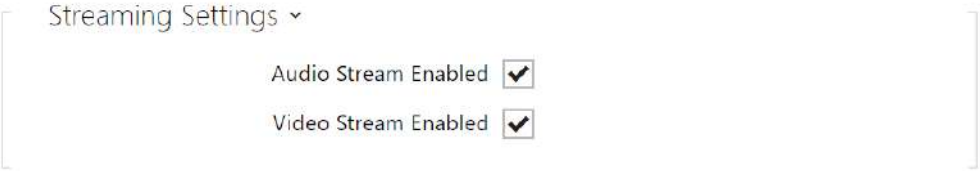
a. rtsp://ip_intercom_address/h264_stream
b. rtsp://ip_intercom_address/mpeg4_stream
c. rtsp://ip_intercom_address/mjpeg_stream

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



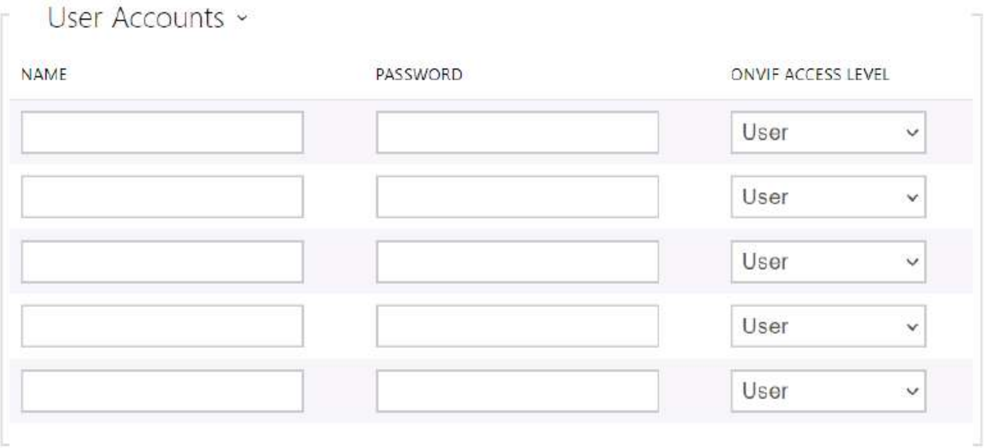
☑ RTSP Server Enabled

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



Audio Stream Enabled ☑
Video Stream Enabled ☑

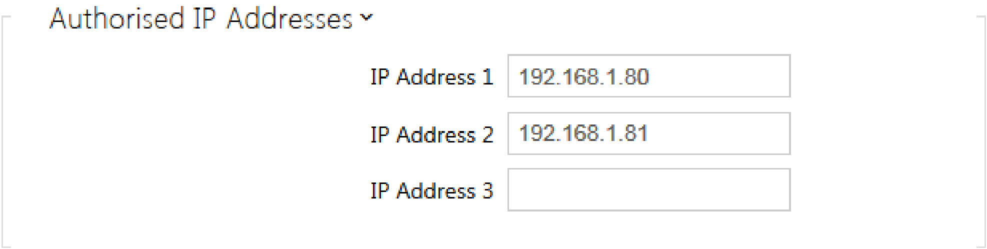
- **Audio stream enabled** – enable offering of audio stream while establishing connection with the RTSP server.
- **Video stream enabled** – enable offering of video stream while establishing connection with the RTSP server.



NAME	PASSWORD	ONVIF ACCESS LEVEL
		User
		User
		User
		User
		User

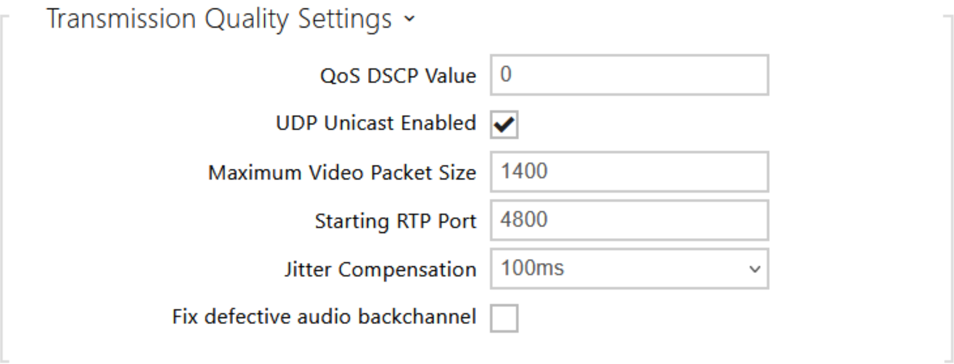
Be sure to set one user account at least and the proper access level (according to ONVIF specification and used VMS) to achieve full ONVIF functionality. Without this, the basic functionality is only available.

- **Name** – set the ONVIF access user name.
- **Password** – set the ONVIF access password.
- **Onvif Access Level** – set the user ONVIF access level (User, Operator, Administrator).



IP Address 1: 192.168.1.80
IP Address 2: 192.168.1.81
IP Address 3:

- **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: 0

UDP Unicast Enabled: ☑

Maximum Video Packet Size: 1400

Starting RTP Port: 4800

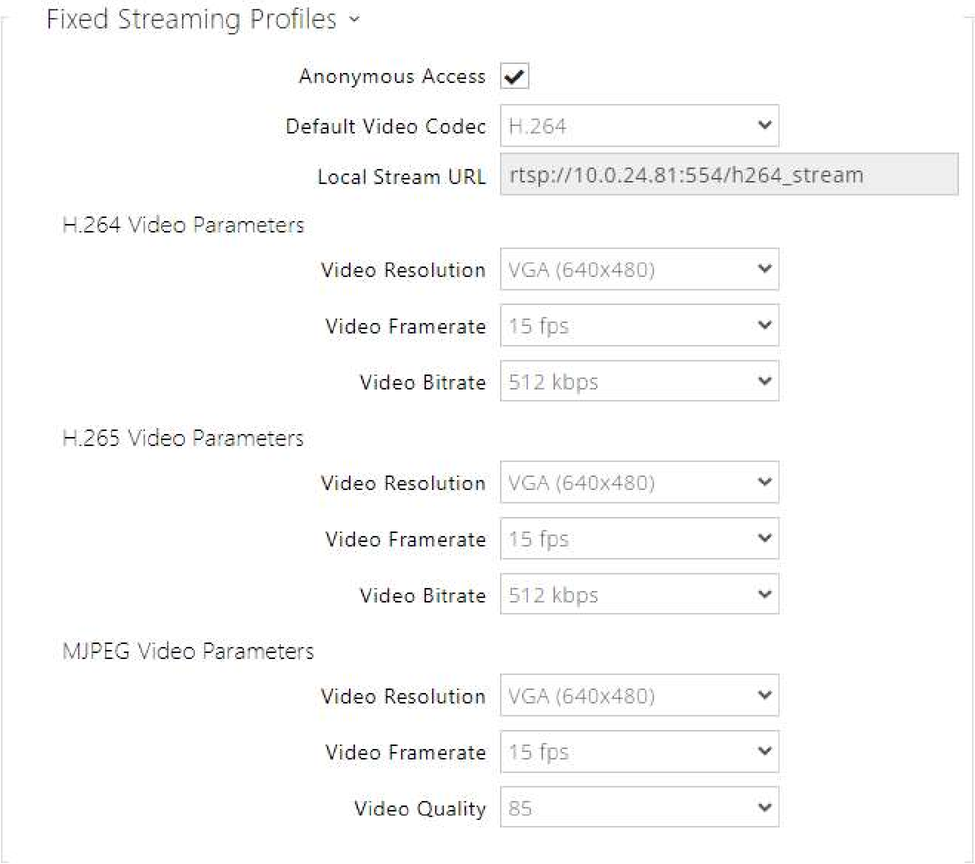
Jitter Compensation: 100ms

Fix defective audio backchannel: ☐

- **QoS DSCP Value** – set the audio/video RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.
- **UDP Unicast Enabled** – enable audio/video stream sending via the RTP/UDP. If this mode is off, the audio/video stream data are sent via the RTP/RTSP only.
- **Maximum Video Packet Size** – set the maximum size of the video packets to be sent via the RTP/UDP.
- **Starting RTP Port** – set the starting local RTP port in the range of the length of 60 ports to be used for audio and video transmissions. The default value is 4800 (i.e. the used range is 4800–4859).
- **Jitter Compenstantion** – 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.
- **Fix defective audio backchannel** – enables a feature that fixes RTP timestamps that some VMSes send incorrectly. These invalid timestamps cause dropouts and choppy audio in the played-back audio.

Tip

- FAQ: VLC Player – How to watch a video from 2N IP intercom RTSP server
- FAQ: VLC Player – How to record video from 2N IP intercom



Fixed Streaming Profiles

Anonymous Access ☑

Default Video Codec: H.264

Local Stream URL: rtsp://10.0.24.81:554/h264_stream

H.264 Video Parameters

Video Resolution: VGA (640x480)

Video Framerate: 15 fps

Video Bitrate: 512 kbps

H.265 Video Parameters

Video Resolution: VGA (640x480)

Video Framerate: 15 fps

Video Bitrate: 512 kbps

MJPEG Video Parameters

Video Resolution: VGA (640x480)

Video Framerate: 15 fps

Video Quality: 85

- **Anonymous Access** – enable access to the original RTSP server streams without user authentication. If this field is unselected, the RTSP client must authenticate itself as one of the ONVIF users while accessing the server.
- **Default Video Codec** – set the default video codec for RTSP streaming.
- **Local Stream** – display the local stream URL depending on the codec selection.

- **Video Resolution** – set the default image resolution for RTSP streaming.
- **Video Framerate** – set the default video frame rate for RTSP streaming.
- **Video Bitrate** – set the default video bit rate for RTSP streaming.
- **Video Quality**– set the video compression level (for MJPEG only) ranging between 50 (low quality, lowest bitrate) and 95 (top quality, highest bitrate).

JPEG

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

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

or (for MJPEG, HTTP Server Push):

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

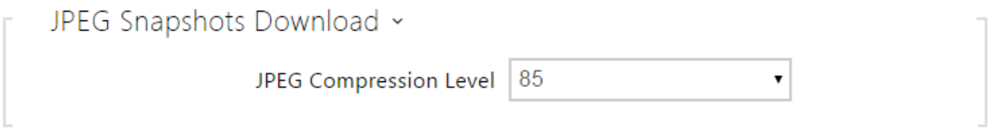
where **W** and **H** specify image resolution (supported resolutions: 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 – for 1 MPix camera equipped models only) and **N** gives the count of snapshots per second (1 through 10).

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

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

Note

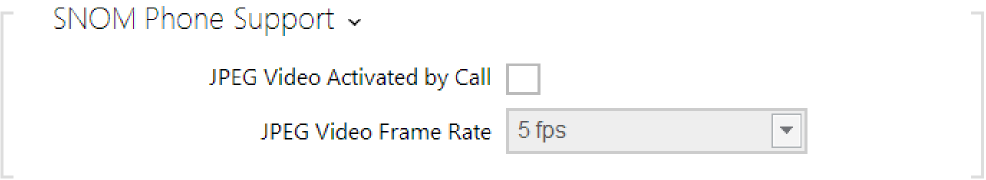
- *The HTTP Server Push method with the multipart/x-mixed-replace contents is not supported by all internet browsers. Test the function in the Firefox browser, for example.*



JPEG Snapshots Download

JPEG Compression Level 85

- **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 ☐

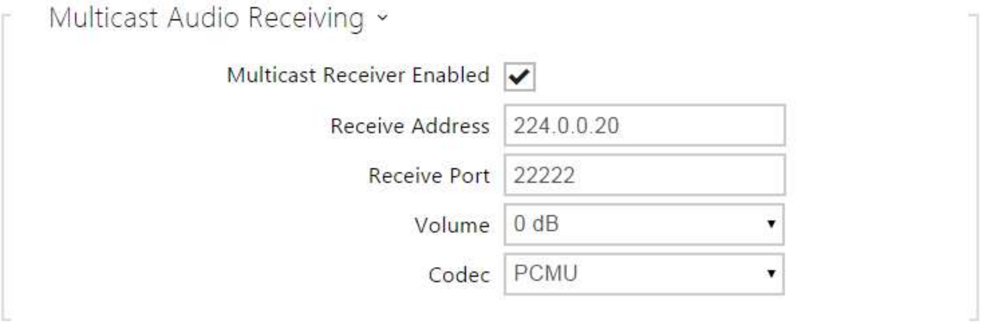
JPEG Video Frame Rate: 5 fps

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

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

Multicast

The **2N LTE 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 ☑

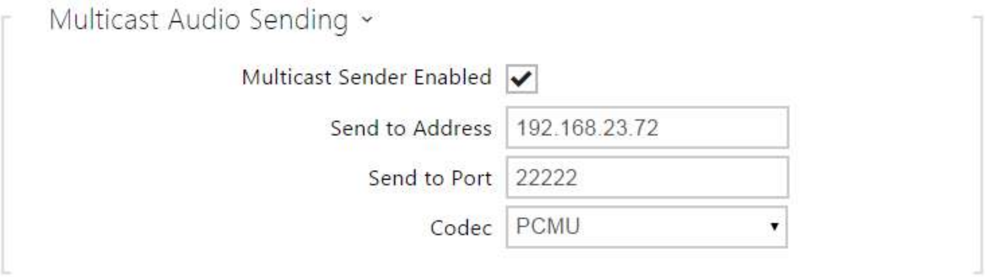
Receive Address: 224.0.0.20

Receive Port: 22222

Volume: 0 dB

Codec: PCMU

- **Multicast receiver enabled** – enable receiving of RTP packets on the selected multicast address and port. The audio stream received is played during an active call too and the sounds from the two sources get mixed.
- **Receive address** – set the multicast IP address to receive multicast RTP packets.
- **Receive port** – set the local port to receive multicast RTP packets.
- **Volume** – set the received audio stream playing volume.
- **Codec**– set the audio codec for RTP packet decoding: PCMU, PCMA, G.722, L.16. The G.722 and L16 broadband codecs are available in selected intercom models only.



Multicast Audio Sending

Multicast Sender Enabled ☑

Send to Address: 192.168.23.72

Send to Port: 22222

Codec: PCMU

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

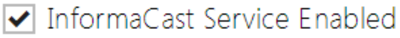
InformaCast

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

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

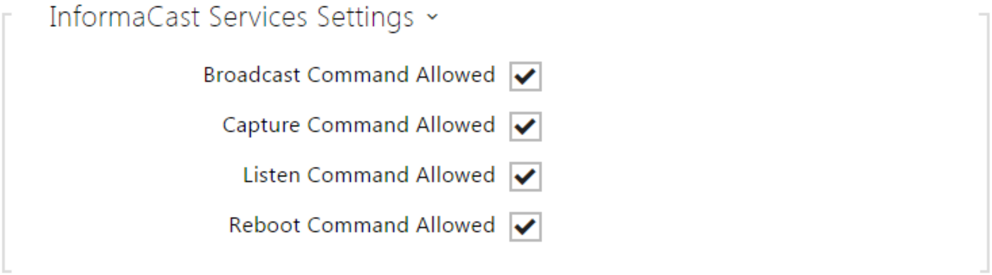
- **Broadcast** – the intercom receives audio from the Informacast server and plays it via an integrated speaker.
- **Capture** – the intercom records audio via an internal microphone and sends it to the Informacast server.
- **Listen** – the intercom receives audio from another Informacast client.

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



☑ InformaCast Service Enabled

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



InformaCast Services Settings ˅

Broadcast Command Allowed ☑

Capture Command Allowed ☑

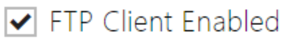
Listen Command Allowed ☑

Reboot Command Allowed ☑

- **Broadcast enabled**– enable the Broadcast command to set up an audio stream sent from the Informacast server to the intercom.
- **Capture enabled**– enable the Capture command to set up an audio stream sent from the intercom to the Informacast server.
- **Listen enabled**– enable the Listen command to set up an audio stream sent from another Informacast client to the intercom.
- **Reboot enabled**– enable the Reboot command to allow the Informacast server to restart the intercom.

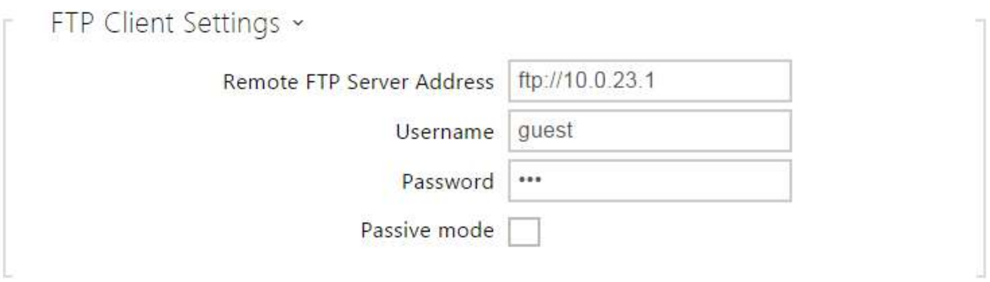
FTP

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



☑ FTP Client Enabled

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



FTP Client Settings ˅

Remote FTP Server Address: ftp://10.0.23.1

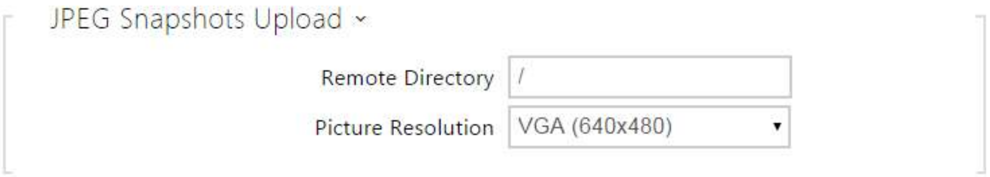
Username: guest

Password: •••

Passive mode ☐

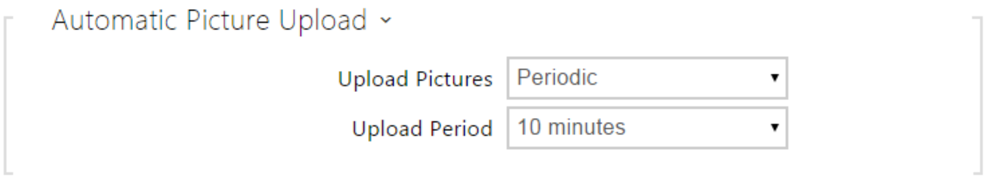
- **Remote FTP server address** – set the FTP server address in the ftp://ip_address or ftps://ip_address format.

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


JPEG Snapshots Upload

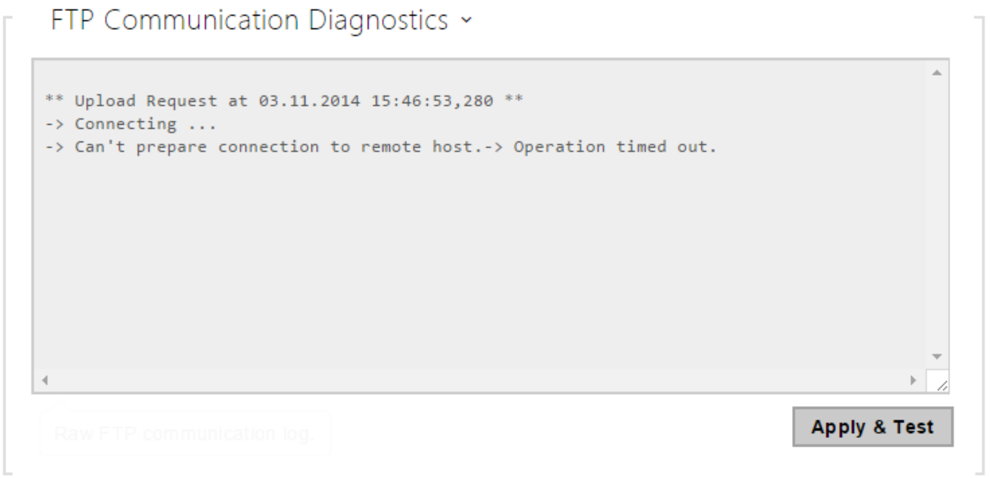
Remote Directory: /
Picture Resolution: VGA (640x480)

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


Automatic Picture Upload

Upload Pictures: Periodic
Upload Period: 10 minutes

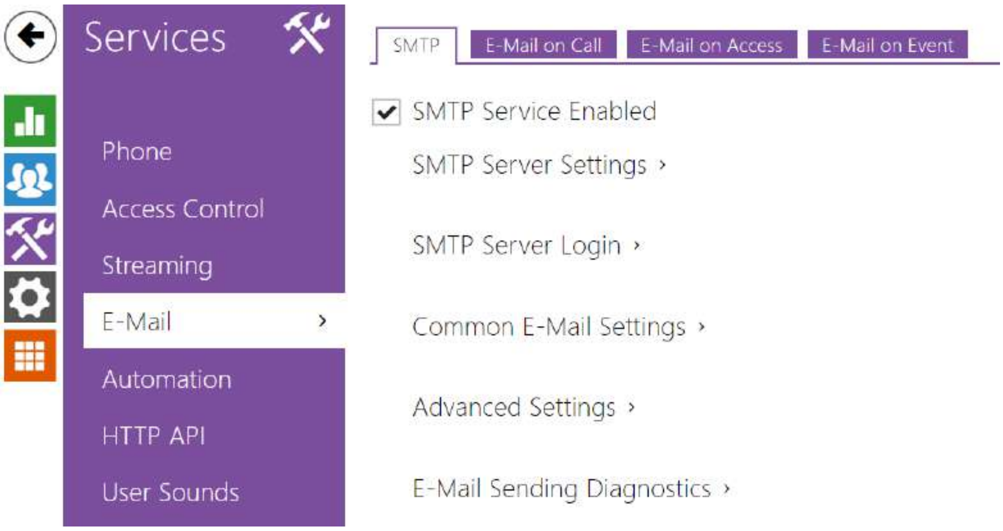
- **Upload pictures** – set automatic picture sending to the FTP server at the call start or after a preset time period. You can disable automatic sending (Automation) and send pictures via **Action.UploadSnapshotToFtp**.
- **Upload period** – set the picture sending period in steps (10 seconds to 30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


FTP Communication Diagnostics

```
** Upload Request at 03.11.2014 15:46:53,280 **
-> Connecting ...
-> Can't prepare connection to remote host.-> Operation timed out.
```

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

5.4.3 E-Mail



☑ SMTP Service Enabled

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

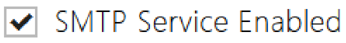
The intercom sends e-mails to all the users whose valid e-mail addresses are included in the users list. If the **E-Mail** parameter in the user list is empty, e-mails are sent to the default e-mail address.

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

Note

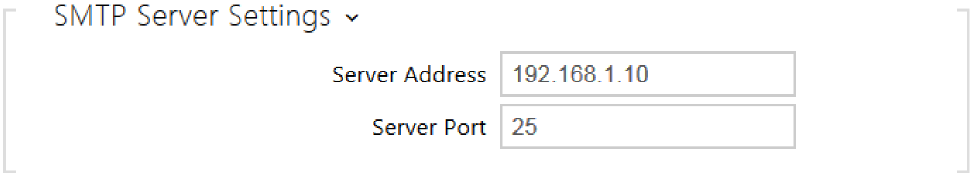
- *The e-mail function is available with the Gold license only.*

SMTP



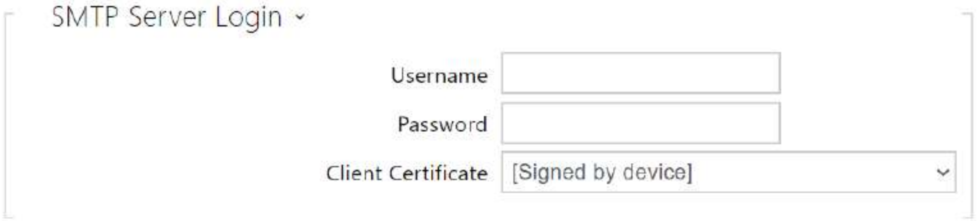
☑ SMTP Service Enabled

- **SMTP Service Enabled** – enable/disable sending e-mails from the intercom.



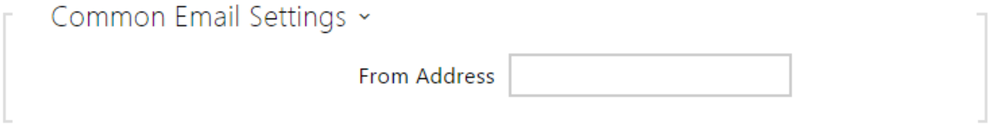
Server Address: 192.168.1.10
Server Port: 25

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

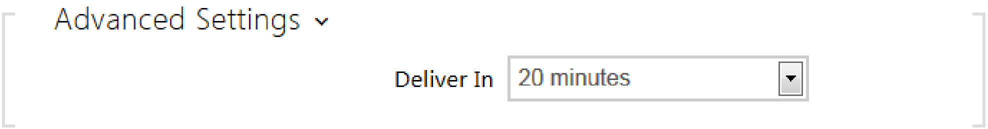


Client Certificate: [Signed by device]

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

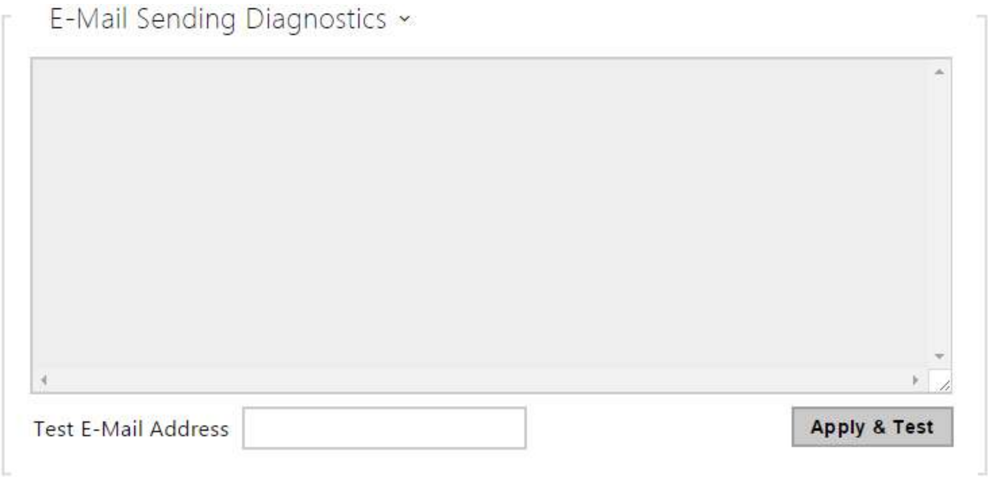


- **From Address** – set the sender address for all outgoing e-mails from the device.

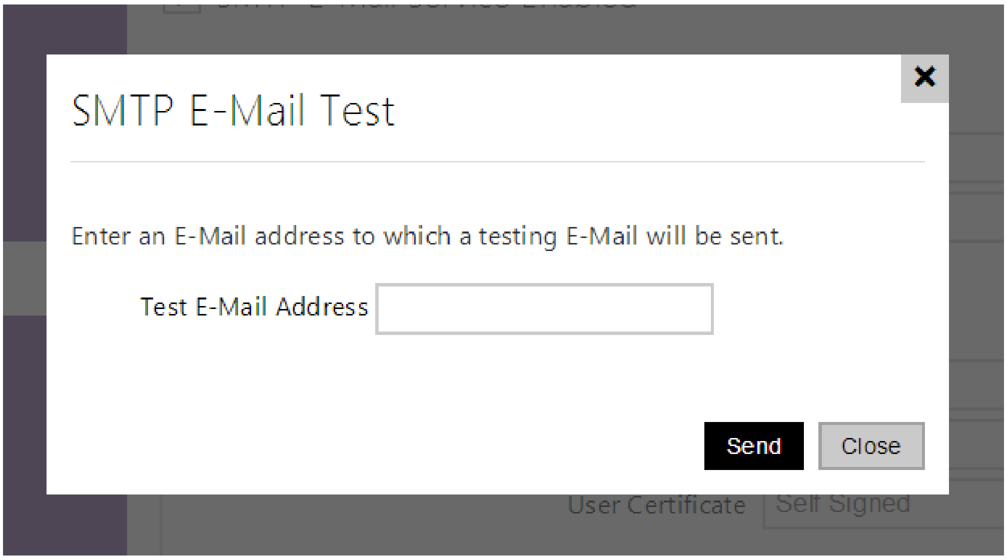


Deliver In: 20 minutes

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



Click **Apply & Test** to send a testing e-mail to the defined address with the aim to test the functionality of the current e-mail sending setting. Enter the destination e-mail address into the Test e-mail address field and press the button. The current e-mail sending state is continuously displayed in the window for you to detect an e-mail setting problem if any on the intercom or another network element. One camera shot is always attached to the e-mail even in cameraless models where the image is sent with N/A.



SMTP E-Mail Test

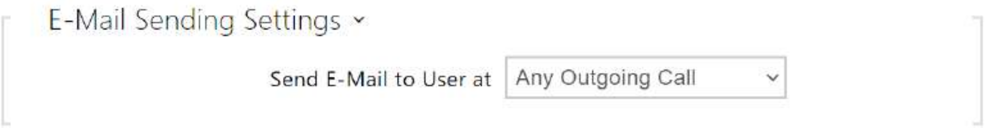
Enter an E-Mail address to which a testing E-Mail will be sent.

Test E-Mail Address

User Certificate: Self Signed

E-Mail on Call

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



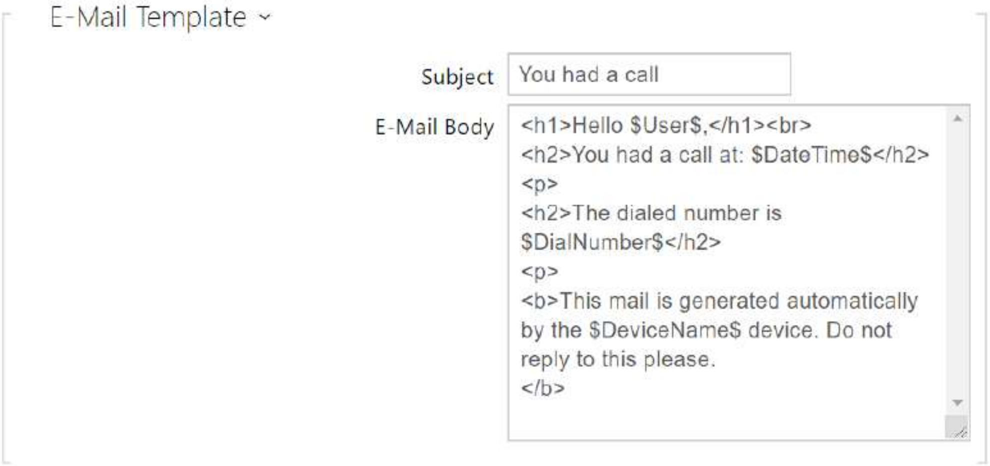
E-Mail Sending Settings

Send E-Mail to User at: Any Outgoing Call

- **Send E-Mail to User at** – set e-mail sending in the event of an accomplished / missed outoging call. The e-mail is sent when the connection is terminated. The following options are available:
    - **Do Not Send E-mail** – no e-mail messages will be sent upon outgoing calls.
    - **Any Outgoing Call** – an e-mail will be sent upon every outgoing call.
    - **Missed Outgoing Call** – an e-mail will be sent upon every missed outgoing call.

ⓘ **Note**

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



Subject: You had a call

E-Mail 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 $DeviceName$ device. Do not
reply to this please.
</b>
```

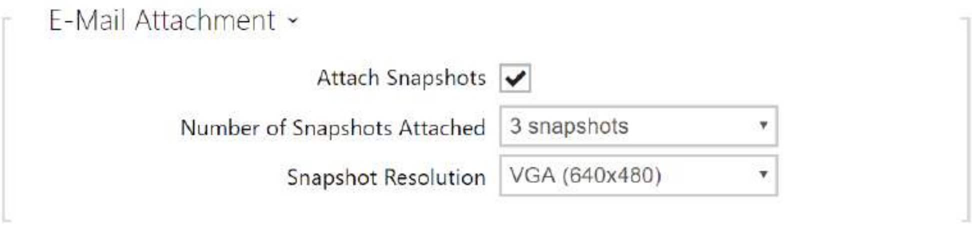
- **Subject** – set the e-mail subject to be sent.
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date and time, intercom identification or called number, which will be replaced with the actual value before sending. The list of placeholders included in the template is shown in a table at the end of the section.

E-Mail Body

```
<p>Hello <b>$User$</b>
</p>
<p>You had a call on: <b>$DateTime$</b>
  <br>The number dialed was: <b>$DialNumber$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Caution

- If the call is made to multiple users, the placeholder symbol for the name of the called user $User$ is empty.



Attach Snapshots ☑

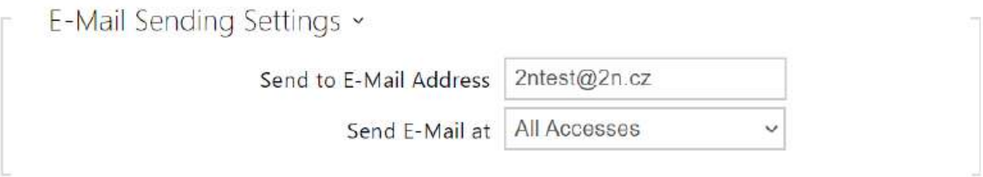
Number of Snapshots Attached: 3 snapshots

Snapshot Resolution: VGA (640x480)

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

E-Mail on Access

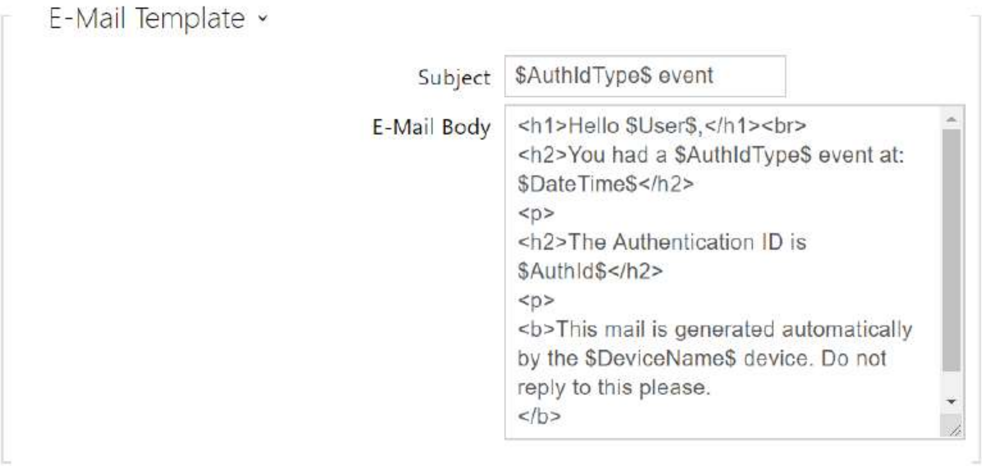
Set that an e-mail shall be sent whenever an RFID card is tapped on the card reader and/or Bluetooth/fingerprint reader identification is made.



Send to E-Mail Address: 2ntest@2n.cz

Send E-Mail at: All Accesses

- **Send to E-mail Address** – administrator e-mail address.
- **Send E-Mail at** – set e-mail sending. The following options are available:
    - **Do Not Send E-mail** – no e-mail message will be sent.
    - **All Accesses** – an e-mail will be sent at all (valid/invalid) access attempts.
    - **Denied Accesses** – an e-mail will only be sent if the access is denied.



Subject: $AuthIdType$ event

E-Mail Body:

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

- **Subject** – set the e-mail subject to be sent.
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date & time, intercom/card identification, Bluetooth/fingerprint identifier and identifier validity for information. These

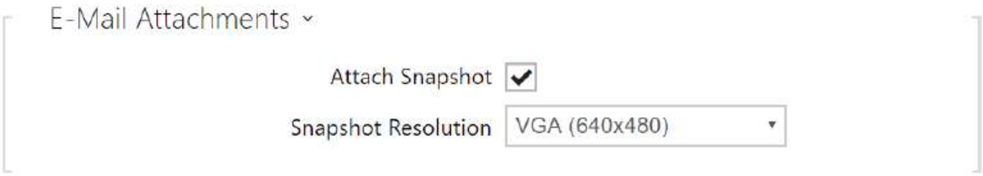
symbols will be replaced with the actual value before sending. The list of placeholders included in the template is shown in a table at the end of the section.

E-Mail Body

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

Caution

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


E-Mail Attachments

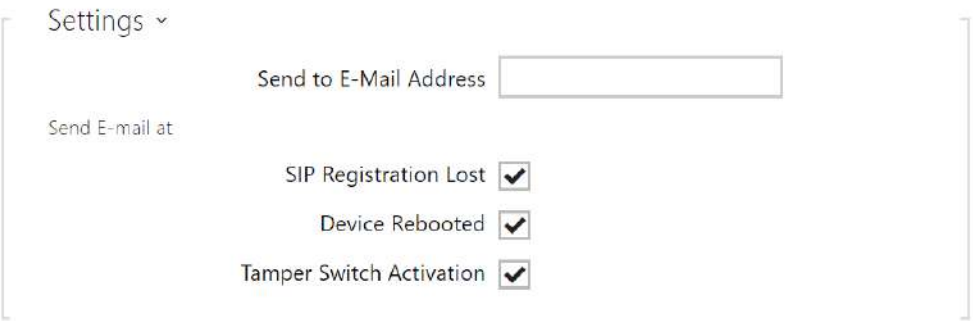
Attach Snapshot ☑

Snapshot Resolution VGA (640x480)

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

E-Mail on Event

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



Send to E-Mail Address

Send E-mail at

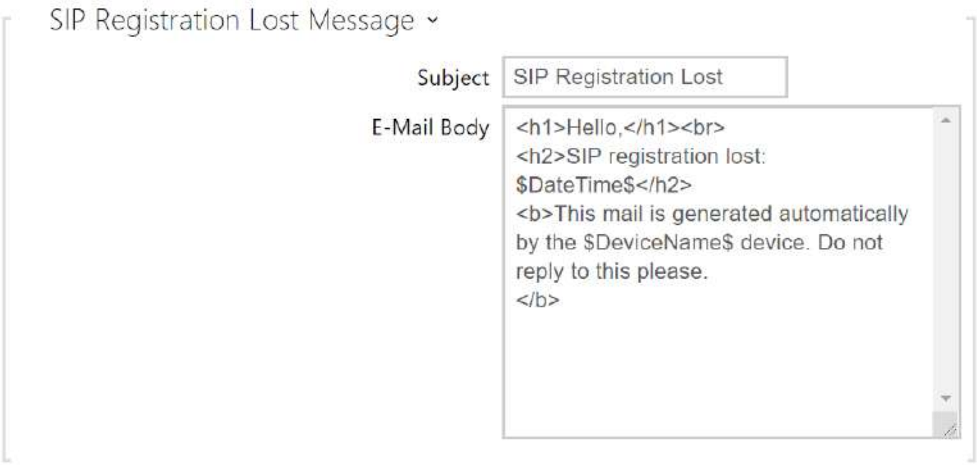
SIP Registration Lost ☑

Device Rebooted ☑

Tamper Switch Activation ☑

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

- **SIP Registration Lost**
- **Device Rebooted**
- **Tamper Switch Activation**



Subject: SIP Registration Lost

E-Mail Body:

```
<h1>Hello,</h1><br>
<h2>SIP registration lost:
$DateTime$</h2>
<b>This mail is generated automatically
by the $DeviceName$ device. Do not
reply to this please.
</b>
```

SIP Registration Lost Message – set the message to be sent to the specified e-mail address whenever the SIP registration gets lost.

- **Subject** – set the e-mail subject to be sent.

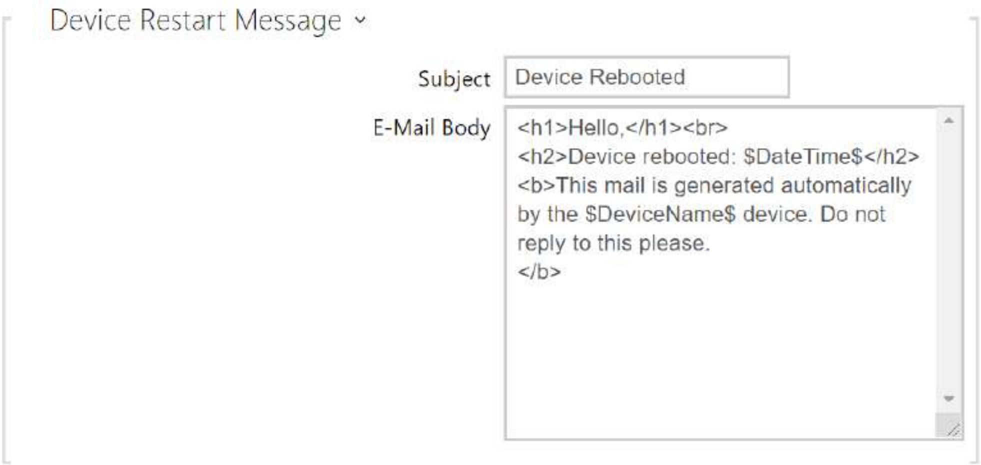
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date & time and device ID. These symbols will be replaced with the actual value before sending. The list of placeholders found in the template is shown in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

E-Mail Body

```
<p>Hello,
</p>
<p>SIP account <b>$SipAccountNumber$</b> of device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>) got unregistered on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

⚠ **Caution**

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



Subject: Device Rebooted

E-Mail Body:

```
<h1>Hello,</h1><br>
<h2>Device rebooted: $DateTime$</h2>
<b>This mail is generated automatically
by the $DeviceName$ device. Do not
reply to this please.
</b>
```

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

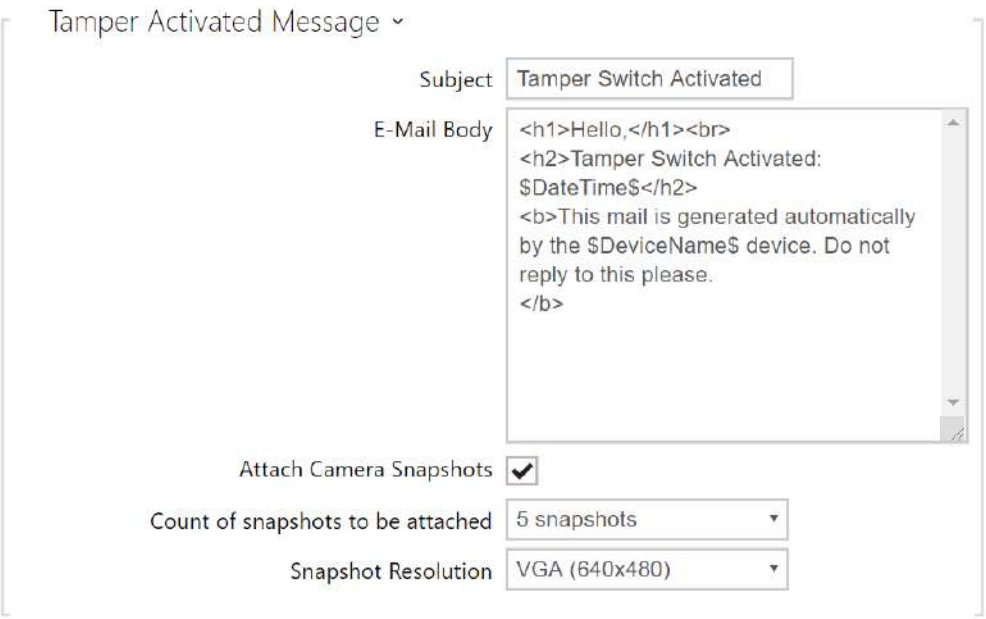
- **Subject** – set the e-mail subject to be sent.
- **E-Mail Body** – edit the text to be sent. Use the HTML formatting marks in the text. You can insert special symbols substituting the username, date & time and device ID. These symbols will be replaced with the actual value before sending. The list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

E-Mail Body

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

Caution

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



Tamper Activated Message

Subject: Tamper Switch Activated

E-Mail Body:

```
<h1>Hello,</h1><br>
<h2>Tamper Switch Activated:
$DateTime$</h2>
<b>This mail is generated automatically
by the $DeviceName$ device. Do not
reply to this please.
</b>
```

Attach Camera Snapshots ☑

Count of snapshots to be attached: 5 snapshots

Snapshot Resolution: VGA (640x480)

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

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

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

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

E-Mail Body

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

Caution

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

Caution

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

List of Placeholders

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

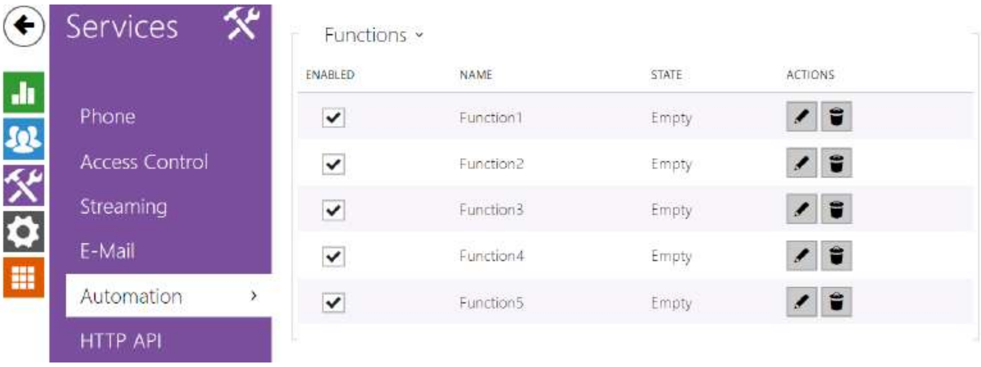
List of Placeholders in Events

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

Placeholder / Function	E-Mail on Access	E-Mail on Call	E-mail on SIP Registration Lost	E-mail on Device Rebooted	E-mail on Tamper Switch Activation	E-mail on Diagnostics Sending	Automation
$AuthIdValid$	*						CardEntered, CardHeld
$AuthIdReason$	*						

5.4.4 Automation

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



ENABLED	NAME	STATE	ACTIONS
☑	Function1	Empty	✎ 🗑
☑	Function2	Empty	✎ 🗑
☑	Function3	Empty	✎ 🗑
☑	Function4	Empty	✎ 🗑
☑	Function5	Empty	✎ 🗑

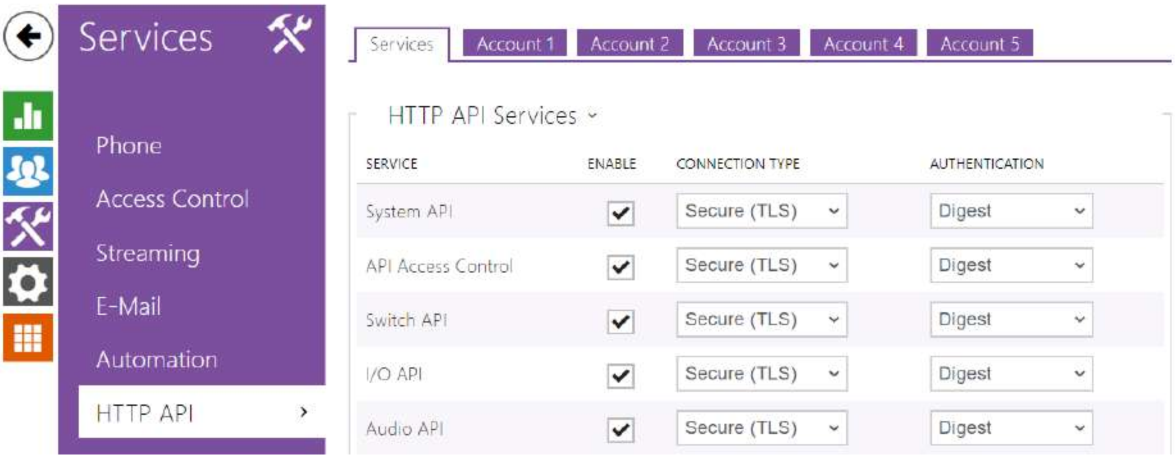
The **2N LTE intercom** provides highly flexible setting options to satisfy variable user needs. There are situations in which the standard configuration settings (switch or call modes, e.g.) are insufficient and so **2N LTE intercom** offers **Automation**, a special programmable interface for applications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

Click the ✎ icon at the function to be created or changed to access the Automation interface.

Note

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

5.4.5 HTTP API



HTTP API Services

SERVICE	ENABLE	CONNECTION TYPE	AUTHENTICATION
System API	☑	Secure (TLS)	Digest
API Access Control	☑	Secure (TLS)	Digest
Switch API	☑	Secure (TLS)	Digest
I/O API	☑	Secure (TLS)	Digest
Audio API	☑	Secure (TLS)	Digest

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

HTTP API provides the following services:

- **System API** – provides intercom configuration changes, status info and upgrade.
- **API Access Control** – provides access control and user authentication verification methods.
- **Switch API** – provides switch status control and monitoring, e.g. door lock opening, etc.
- **I/O API** – provides intercom logic input/output control and monitoring.
- **Audio API** - provides audio playback control and microphone monitoring.
- **Camera API** – provides camera image control and monitoring.
- **Display API** – provides display control and user information display.
- **E-mail API** – provides sending of user e-mails.
- **Phone/Call API** – provides incoming/outgoing call control and monitoring.
- **Logging API** – provides reading of event records.
- **Automation API** – provides Secure/Unsecure communication settings and authorization requirements.

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

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

- **None** – no authentication is required. In this case, this service is completely unsecure in the **LAN**.

- **Basic** – Basic authentication is required according to **RFC-2617**. In this case, the service is protected with a password transmitted in an open format. Thus, we recommend you to combine this option with **HTTPS** where possible.
- **Digest** – Digest authentication is required according to **RFC-2617**. This is the default and most secure option of the three above listed methods.

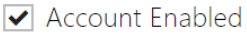
Refer to the HTTP API Configuration Manual for the HTTP API function and configuration details.

✓ **Tip**

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

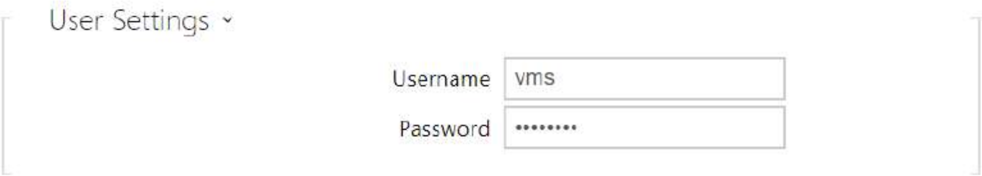
Account 1–5

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



☑ Account Enabled

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

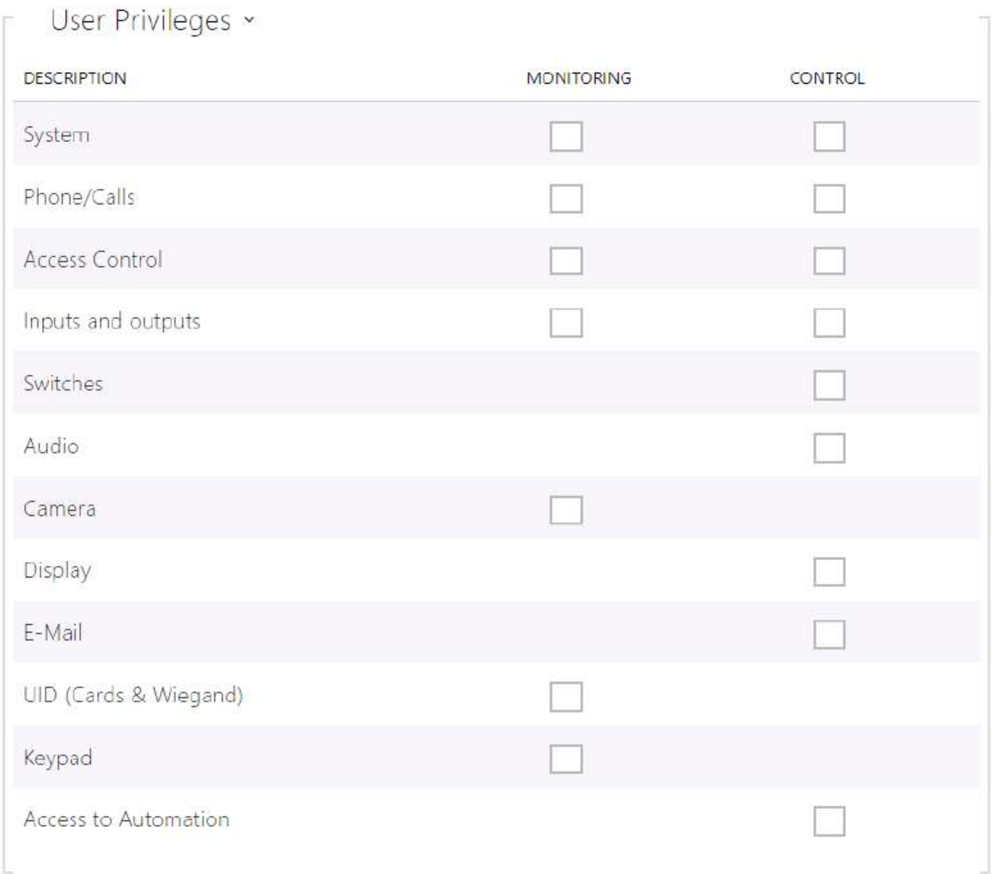


User Settings

Username: vms

Password: ••••••••

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



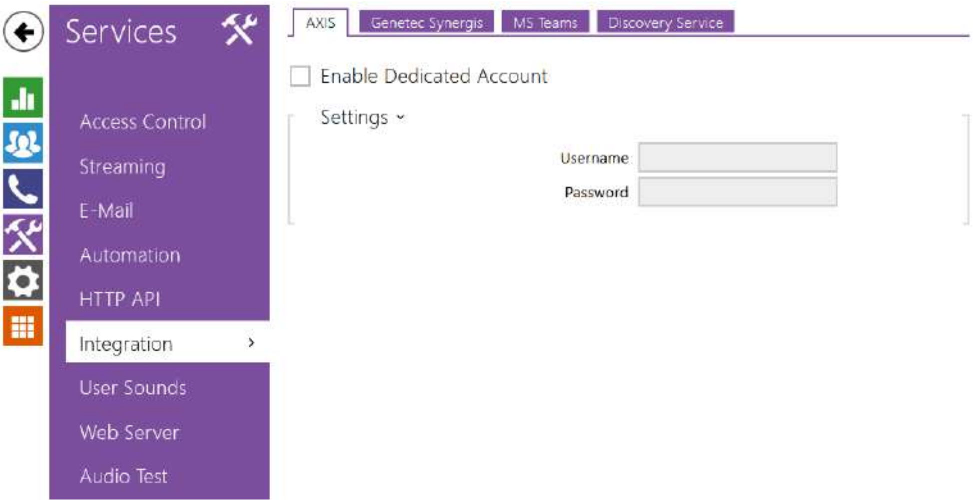
User Privileges

DESCRIPTION	MONITORING	CONTROL
System	☐	☐
Phone/Calls	☐	☐
Access Control	☐	☐
Inputs and outputs	☐	☐
Switches		☐
Audio		☐
Camera	☐	
Display		☐
E-Mail		☐
UID (Cards & Wiegand)	☐	
Keypad	☐	
Access to Automation		☐

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

5.4.6 Integration

The Integration service provides interconnection of the device and third party equipment.

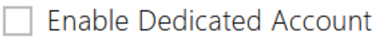


☐ Enable Dedicated Account

Username

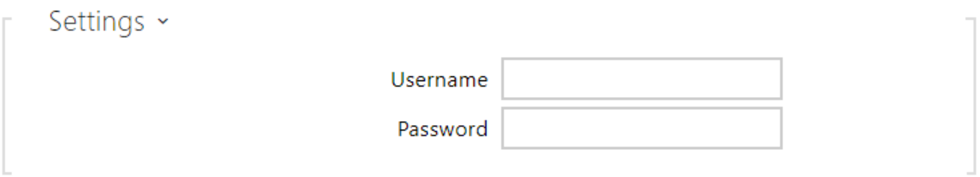
Password

AXIS



☐ Enable Dedicated Account

- **Enable Dedicated Account** – enable calling to the Axis Camera Station (ACS). A special URI in the format vms:* is used for ACS calls.



Username

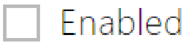
Password

- **Username** – Dedicated AXIS integration account username.
- **Password** – Dedicated AXIS integration account password.

Hint

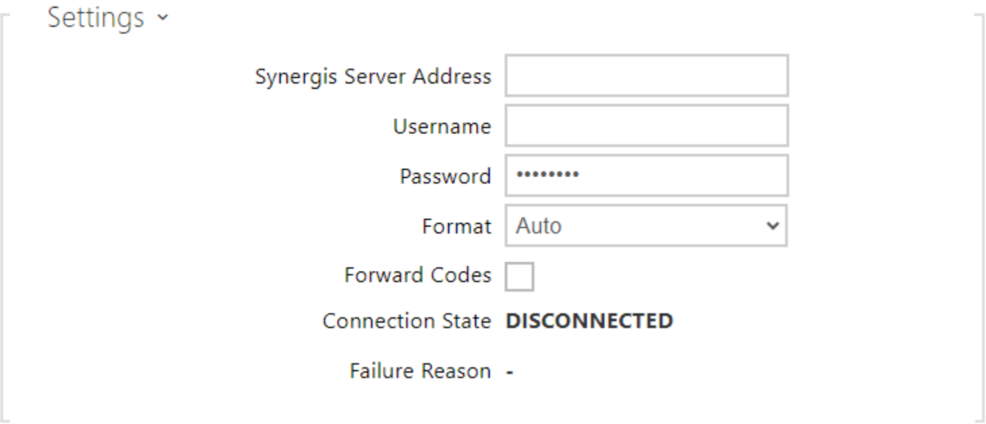
The administrator account can be used for AXIS integrations. You can use the dedicated secondary AXIS integration account if you do not want to share the administrator account with other parties or systems.

Genetec Synergis



☐ Enabled

- **Enabled** – enable connection with the Genetec Synergis external security system.



Synergis Server Address

Username

Password ••••••••

Format Auto

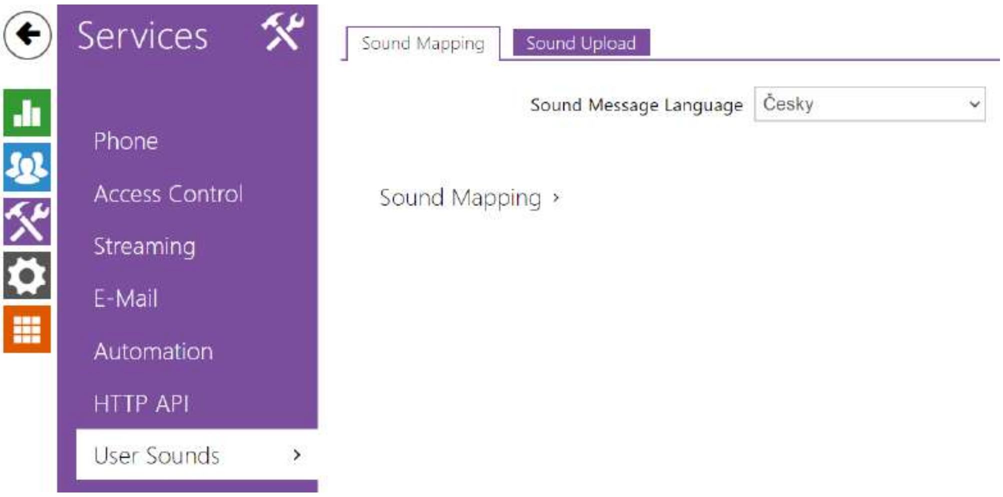
Forward Codes ☐

Connection State **DISCONNECTED**

Failure Reason -

- **Synergis Server Address** – set the IP address/domain name for the Synergis Server.
- **Username** – set the username for authentication.
- **Password** – set the password for authentication.
- **Format** – set the code format to be sent.
- **Forward Codes** – determine whether or not the set codes shall be forwarded. The codes may have up to 6 digits and have to be confirmed with the confirmation key before sending.

5.4.7 User Sounds



Sound Message Language Česky

The **2N LTE 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:

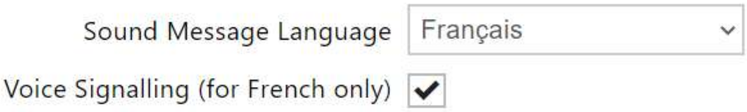
a. **Ringing before answering call**
b. **Ringback tone**
c. **Call busy tone**
d. **Call hang-up**
e. **Invalid input**
f. **Invalid user position**
g. **Switch activation**

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

Frequency	Bits for sample	Sound length	Quality
16 kHz	16 bit	up to 8 s	1 best
16 kHz	8 bit	up to 16 s	2
8 kHz	16 bit	up to 16 s	3 (not recommended combination)
8 kHz	8 bit	up to 32 s	4 low

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

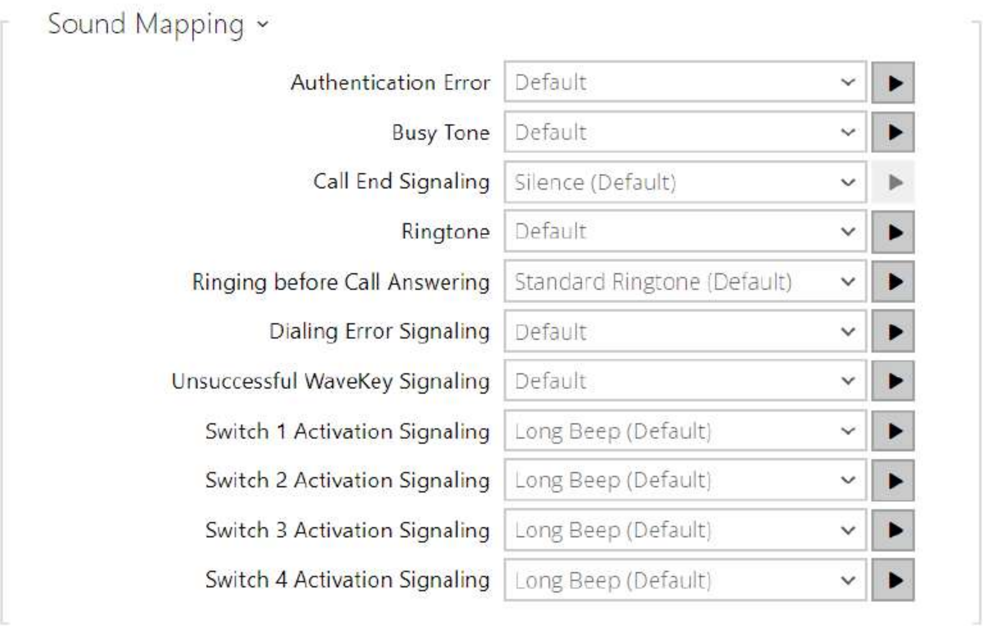


Sound Message Language: Français

Voice Signalling (for French only) ☑

- **Sound Message Language** – Select a language of spoken meassages. If there is a translation available for a mapped sound, the messagewill be played in specified language. The language defaults to English or to a language-neutral sound if there is no translation.
- **Voice Signalling (for French only)** – In order to meet the applicable legislation in French speaking regions, voice signaling in French is available for handicapped persons for the following actions: call setup, call connection and door unlocking.

Sound Mapping



Authentication Error	Default
Busy Tone	Default
Call End Signaling	Silence (Default)
Ringtone	Default
Ringing before Call Answering	Standard Ringtone (Default)
Dialing Error Signaling	Default
Unsuccessful WaveKey Signaling	Default
Switch 1 Activation Signaling	Long Beep (Default)
Switch 2 Activation Signaling	Long Beep (Default)
Switch 3 Activation Signaling	Long Beep (Default)
Switch 4 Activation Signaling	Long Beep (Default)

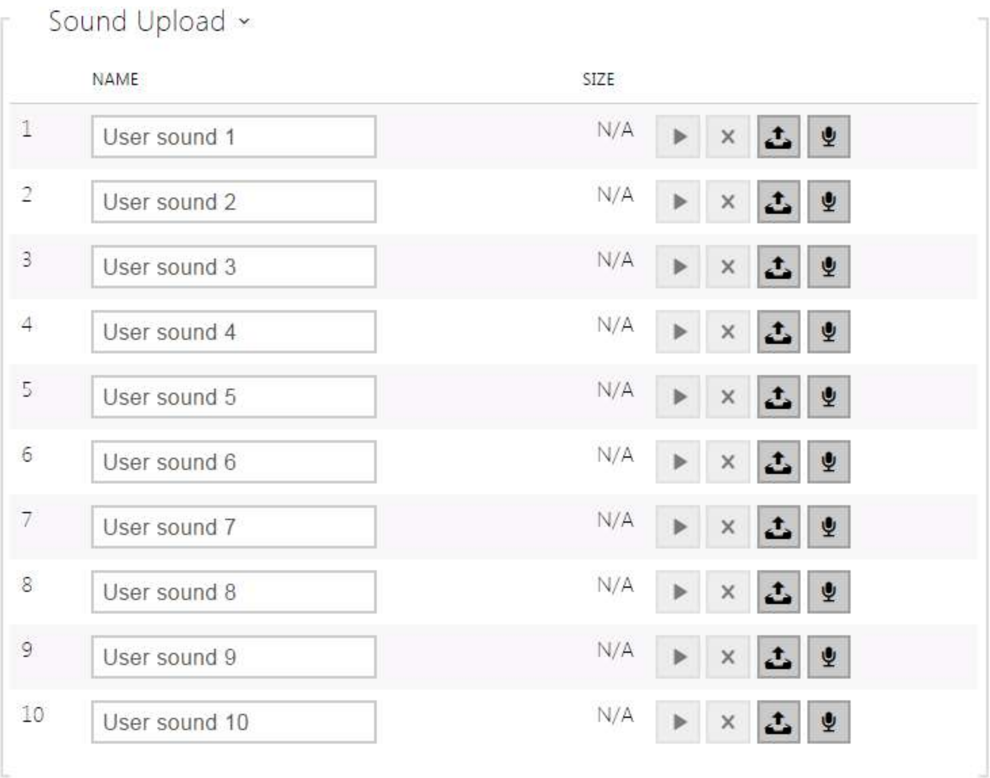
- **Authentication Error** – set the sound to be played when an invalid code in entered (switch/user/profile activation).
- **Busy tone** – set the sound to be played when the called user is busy.
- **Call End signalling** – set the sound to be played upon the call end.
- **Ringtone** – set the sound to be played when the called user id ringing.
- **Ringing before Call Answering** – set the sound to be played before answering an incoming call (intercom ringtone).
- **Dialing Error Signaling** – set the sound to be played when a quick dial button is pressed but the corresponding Phonebook position is not programmed.
- **Unsuccessful WaveKey Signaling** – set the sound to be played if no phone opens the door during the search.
- **Switch 1–4 activation signalling** – set the sound to be generated when a switch is activated. Specify signalling details for each switch; refer to the Switches subsection.

> ⚠ **Caution**
>
> - If the assigned sound cannot be played, the sound is either set to "Silence".

Sound Upload

You can upload up to 10 user sound files of the length of 60 s into the device and assign names to them for convenience.

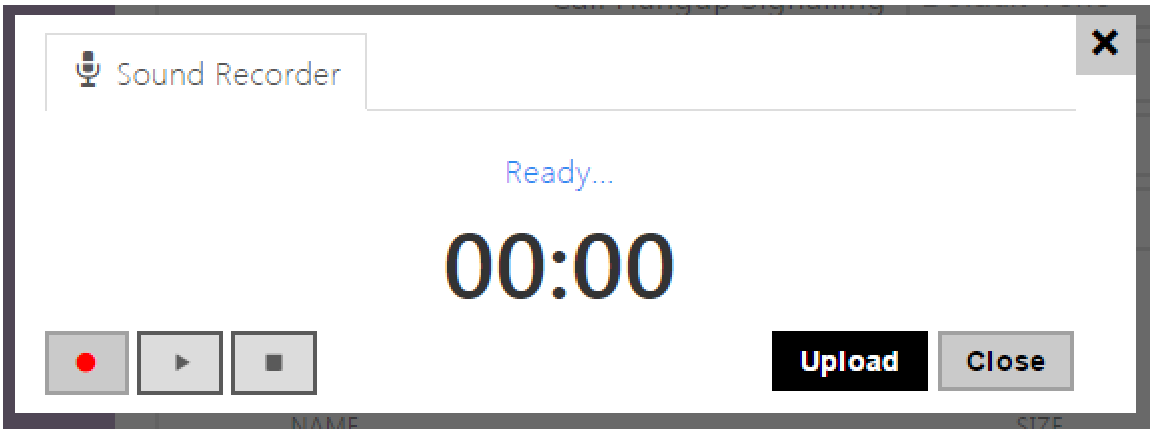
Press ⬆ to upload a sound file to the intercom. Select a file from your PC via a dialogue window and push **Upload**. Press ✕ to remove a file. Press ▶ to replay the sound file (locally on your PC).



Sound Upload

	NAME	SIZE
1	User sound 1	N/A
2	User sound 2	N/A
3	User sound 3	N/A
4	User sound 4	N/A
5	User sound 5	N/A
6	User sound 6	N/A
7	User sound 7	N/A
8	User sound 8	N/A
9	User sound 9	N/A
10	User sound 10	N/A

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



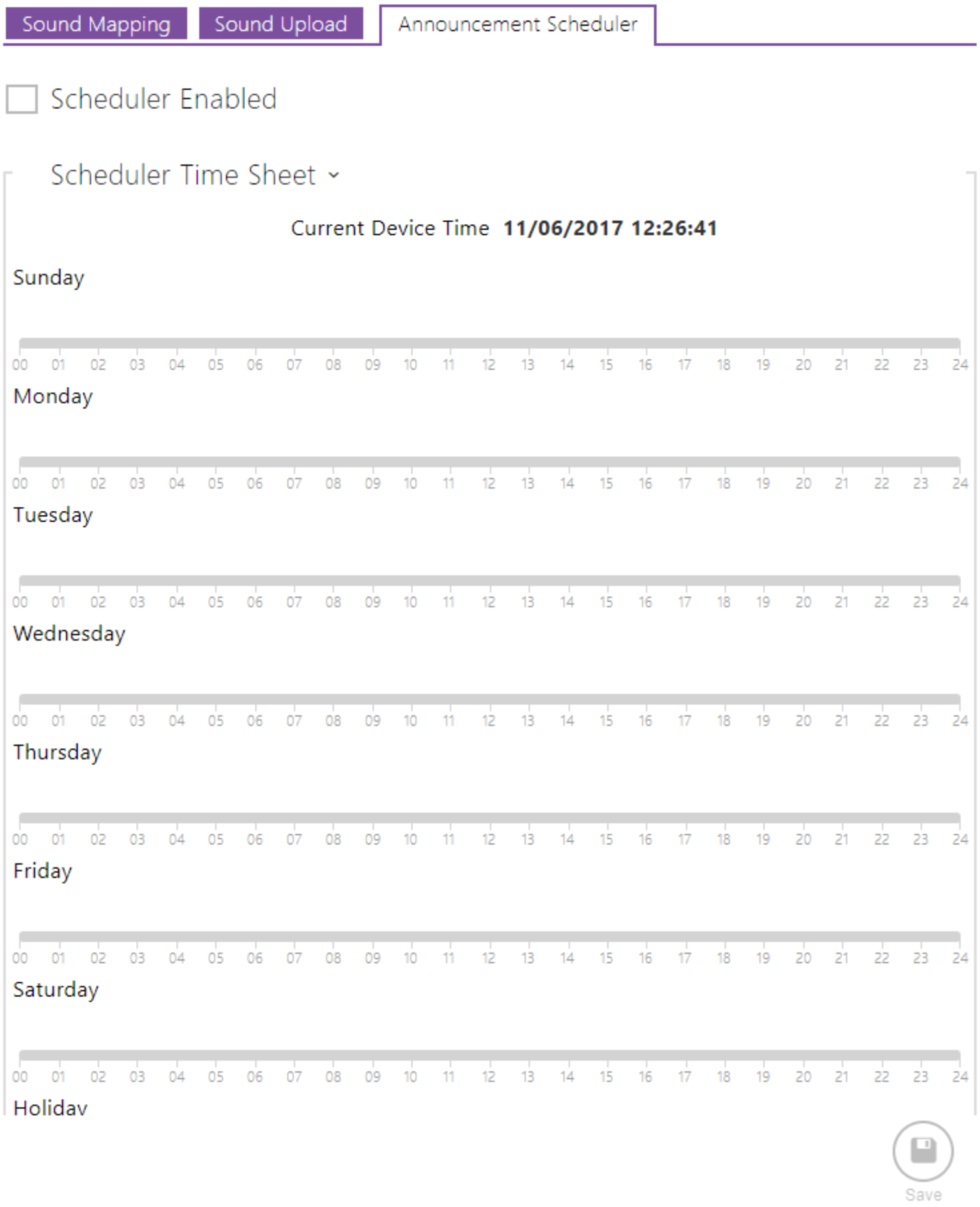
Sound Recorder

Ready...

00:00

Announcement Scheduler

The Announcement Scheduler helps you play user sounds periodically at a preset time. You can set days in a week on which the sound shall be played. Click the required day time axis point to add sound playing. While adding, set the exact time, select the user sound and adjust the sound volume. The **Announcement Scheduler** tab is only available to the **2N SIP Audio** products.



Current Device Time **11/06/2017 12:26:41**

- **Scheduler enabled** – activate playing of preset user sounds as scheduled.

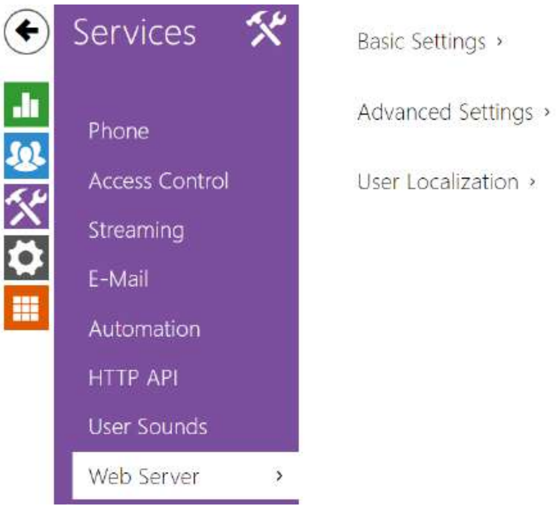
Tip

- Refer to https://wiki.2n.cz/hip/inte/latest/en/10-media-applications/audacity for user sound creating details.

Note

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

5.4.8 Web Server



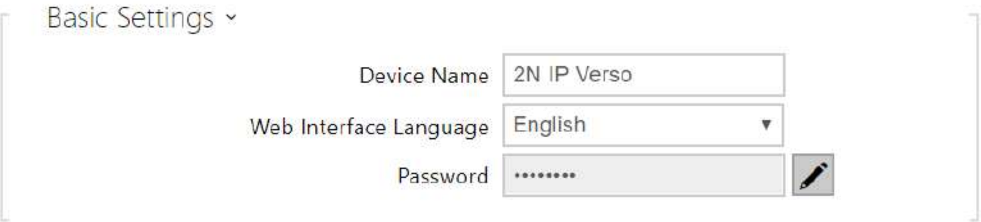
You can configure your **2N LTE intercom** using a standard browser which accesses the integrated web server. Use the secured HTTPS protocol for communication between the browser and intercom. Having accessed the intercom, enter the login name and password. The default login name and password are **admin**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

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

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

List of Parameters



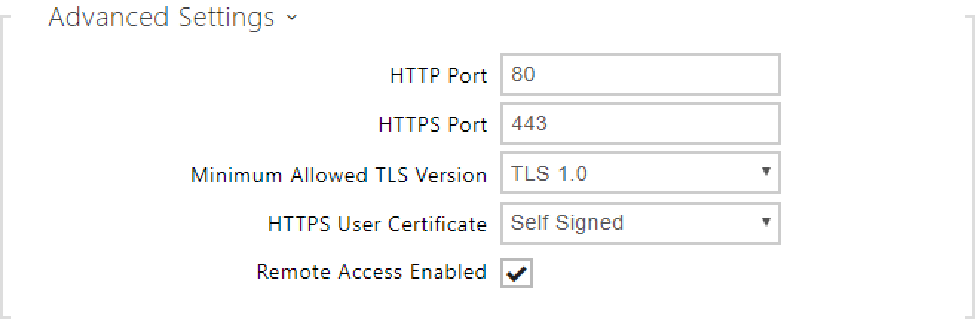
Basic Settings

Device Name: 2N IP Verso

Web Interface Language: English

Password: ••••••••

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



Advanced Settings

HTTP Port: 80

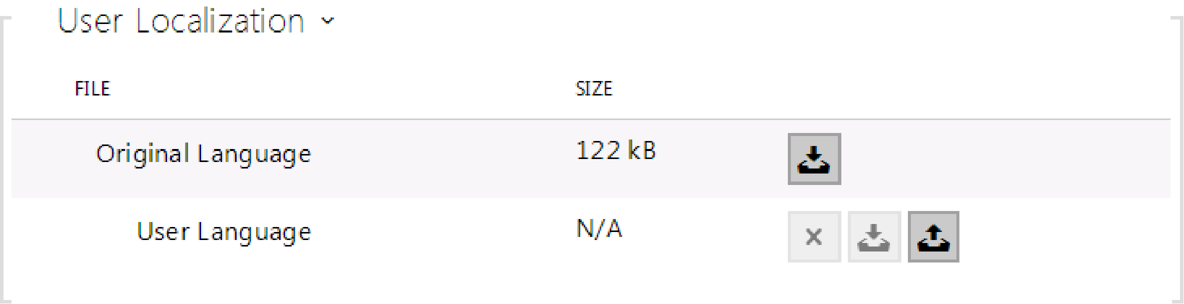
HTTPS Port: 443

Minimum Allowed TLS Version: TLS 1.0

HTTPS User Certificate: Self Signed

Remote Access Enabled: ☑

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

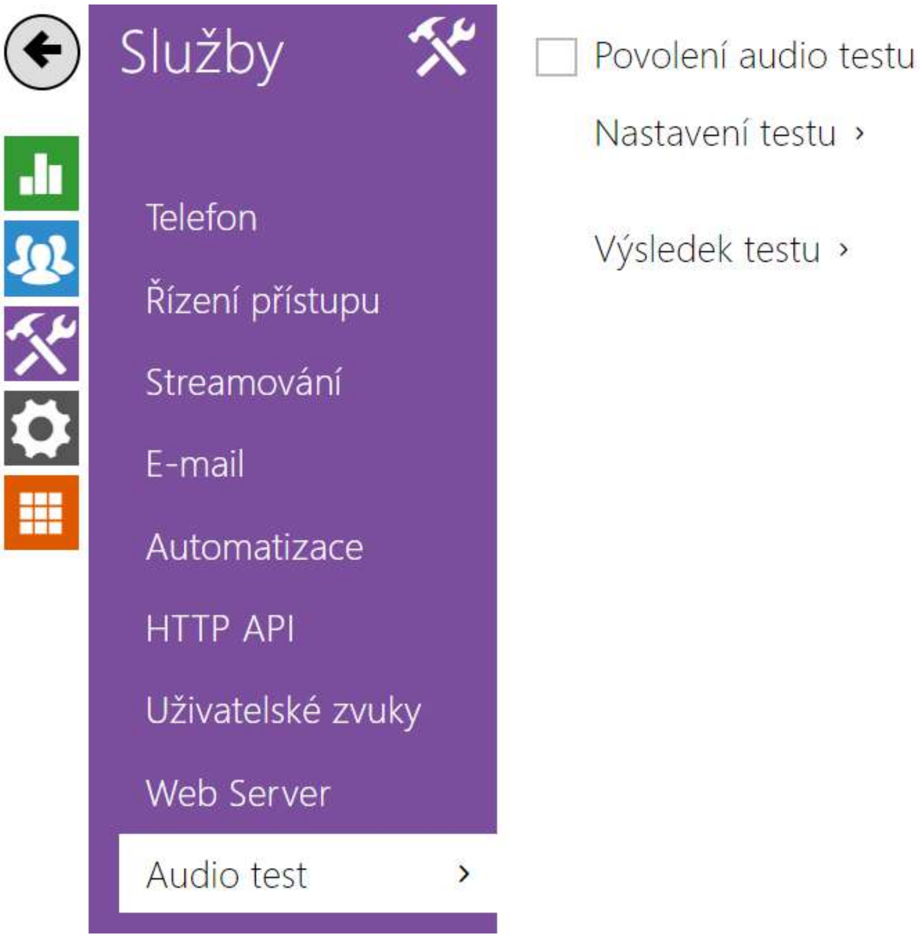


- **Original language** – download the original file containing all the user interface texts in English. The file format is XML; see below.
- **User language** – record, load and remove, if necessary, a user file containing your own user interface text translations.

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

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

5.4.9 Audio Test



☐ Povolení audio testu

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

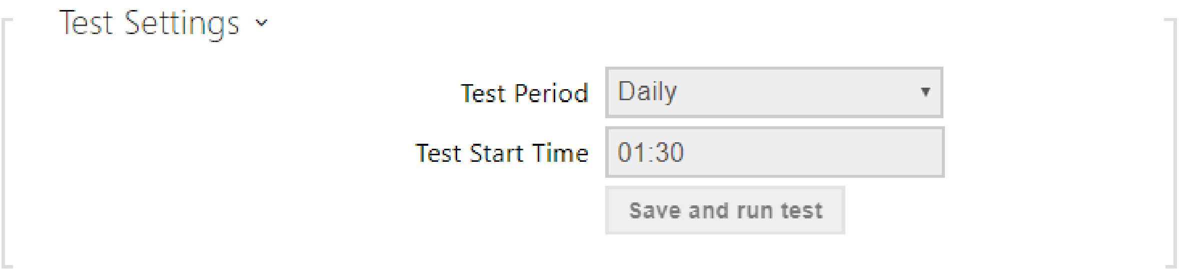
ⓘ **Note**

- *If a call is active when the audio test starts, the audio test will be put off until the call is terminated. The audio test will be performed the moment the call is terminated.*

List of Parameters

☑ Audio Test Enabled

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

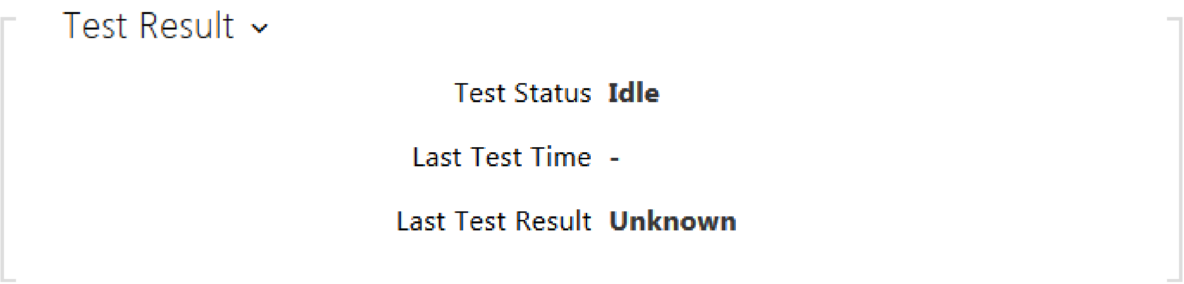


Test Settings

Test Period: Daily

Test Start Time: 01:30

- **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.
- **Save and run** – push the button to start and save the test immediately regardless of the current settings.



Test Result

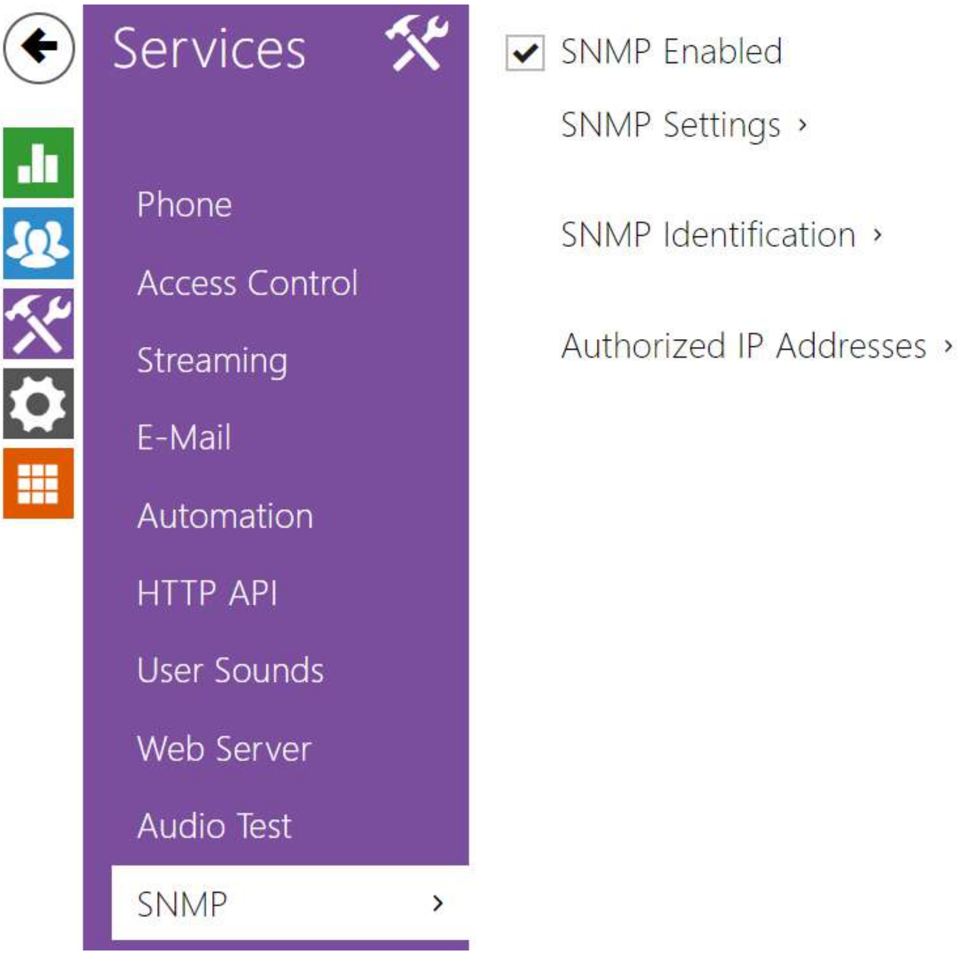
Test Status **Idle**

Last Test Time -

Last Test Result **Unknown**

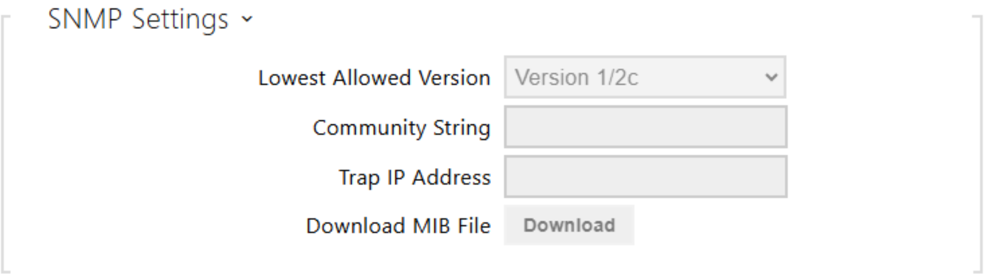
- **Test status** – this parameter displays the current test status.
- **Last test time** – this parameter displays the time of the last-performed test.
- **Last test result** – this parameter displays the result of the last-performed test.

5.4.10 SNMP



The **2N LTE intercoms** integrate a remote intercom supervision functionality via the SNMP.

List of Parameters


SNMP Settings

Lowest Allowed Version: Version 1/2c

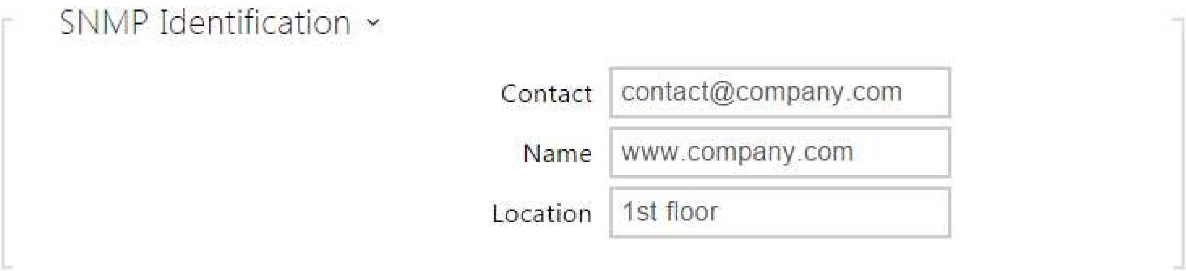
Community String:

Trap IP Address:

Download MIB File: Download

- **Lowest Allowed Version** – selects the lowest SNMP version accepted by the device. SNMPv3 enforces encryption.
- **Community String** – text string representing the access key to the MIB table objects.

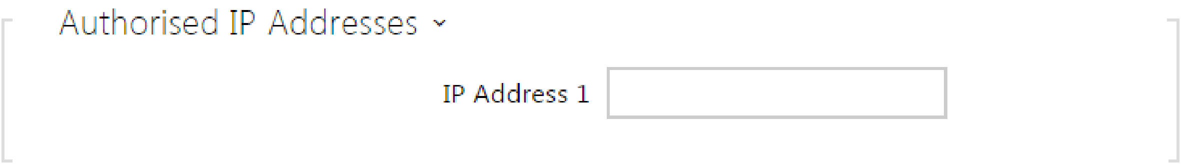
- **Trap IP Address** – IP address to which the SNMP traps are to be sent.
- **Download MIB File** – download the current MIB definition from a device.



SNMP Identification

Contact: contact@company.com
Name: www.company.com
Location: 1st floor

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



Authorised IP Addresses

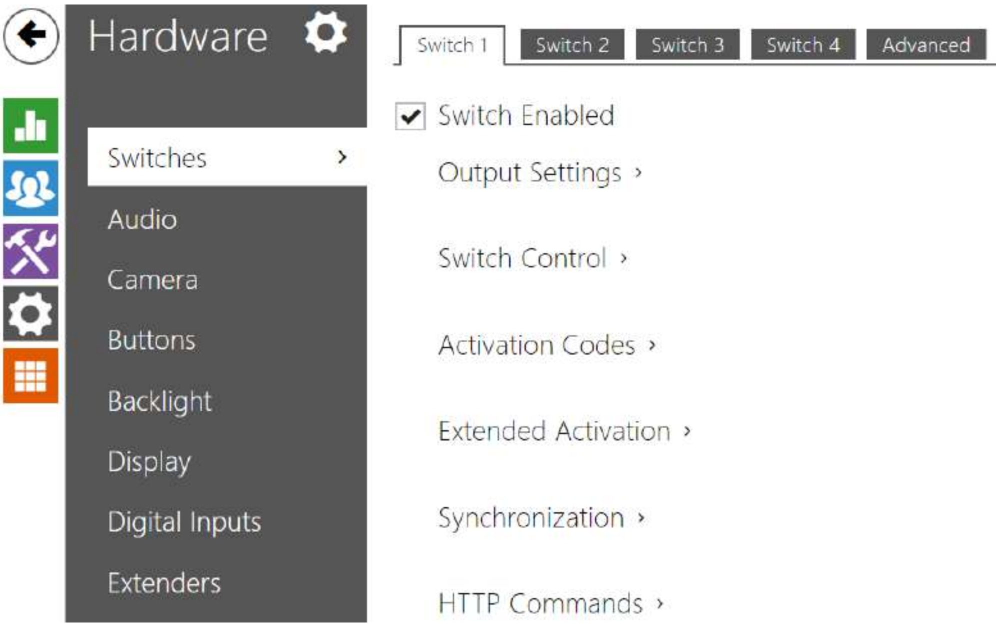
IP Address 1:

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

5.5 Hardware

Here is what you can find in this section:

5.5.1 Switches



☑ Switch Enabled

Switches provide a very flexible and efficient control of such intercom peripherals as electric door locks, lighting, additional ringing signalling, and so on. **2N LTE intercoms** 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,
- by pressing a quick dial button *),
- by a time profile *),
- by receiving the HTTP command from another LAN device,
- via Automation using the Action.ActivateSwitch action *).

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

⚠ **Caution**

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

Switch locking and hold

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

Switch locking and holding can be controlled by time profiles among others. It is not recommended that a time profile be used for the locking function (the time-profile based lock control is present in the device for legacy switch compatibility reasons) because this case results in switch unlocking at the end of the time profile despite manual switch locking.

The current combination of these two functions is shown by the **Current switch function** parameter (Normal – lock and hold are off; Held – lock is off and hold is on; Locked – lock is on regardless of the hold setting).

Check after restart whether or not the lock/hold is controlled by a time profile. If so, the given function is activated/deactivated according to the time profile setting. If not, the last locking state before the device power off is set, or hold is set to inactive (the switch is not held).

If a switch is active, you can:

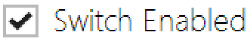
- activate any logical output of the intercom (relay, power output).
- activate the output to which the **2N IP/LTE Intercom – Security Relay** module is connected.
- send an HTTP command to another device.

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:

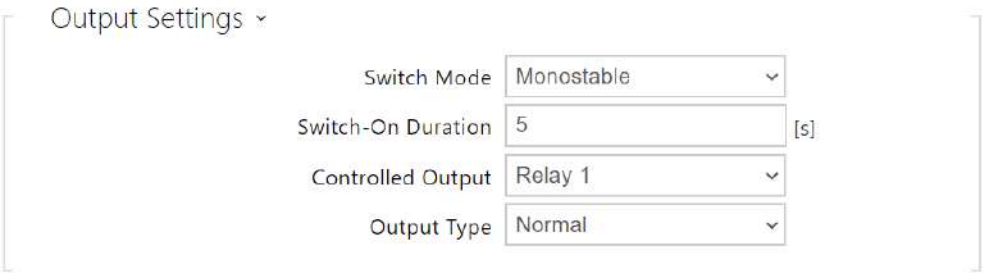
- by a programmable beep or a predefined user sound.
- by a LED indicator if available in the intercom model.
- by an open-door icon on the display if available in the intercom model.

Switch 1–4



☑ 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.



Output Settings

Switch Mode: Monostable

Switch-On Duration: 5 [s]

Controlled Output: Relay 1

Output Type: Normal

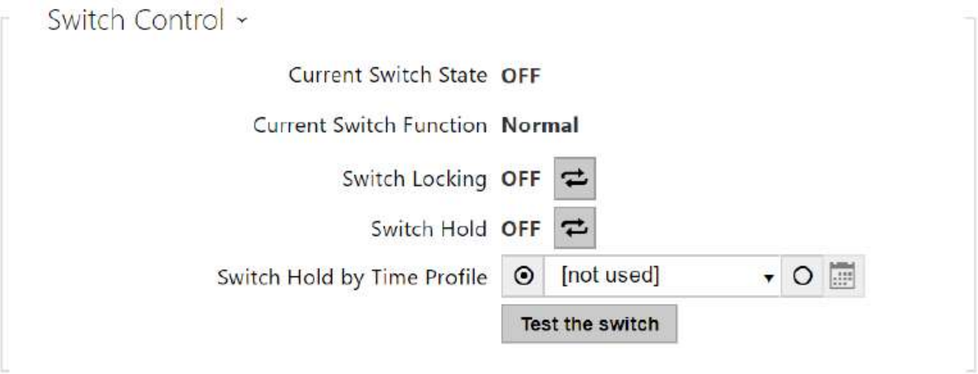
- **Switch mode** – set the monostable/bistable mode for the switch. The switch is switched off after a timeout in the monostable mode and switched on with the first activation and off with the next activation in the bistable mode.
- **Switch-on duration** – set the switch-on time for a monostable switch. This value is not applied in the bistable mode.
- **Controlled Output** – assign a physical output to the switch. Choose one of the available device outputs: relay, active output, extender output. If you select None, the switch will not control any physical output but can control external equipment via HTTP commands.
- **Output Type** – If you are using a Security Relay, set the output type to **Security**. In **Security** mode, the output works in inverse mode, i.e., remains closed and controls the Security Relay module using a specific pulse sequence. If you use the Inverse mode (i.e. the door is locked when voltage is applied), set the **Inverse** output type. In case multiple switches are set to the same output but different output types, the following priority will be applied: 1. Security, 2. Inverse, 3. Normal.

Info

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

Security

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

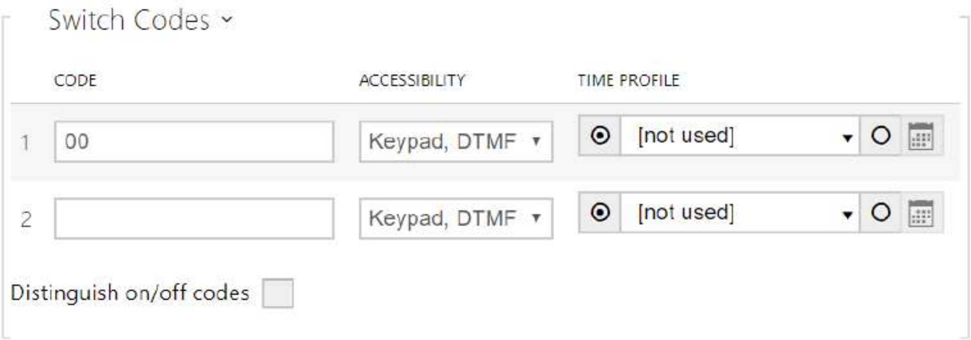


Current Switch State OFF
Current Switch Function Normal
Switch Locking OFF
Switch Hold OFF
Switch Hold by Time Profile ● [not used]

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

Caution

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



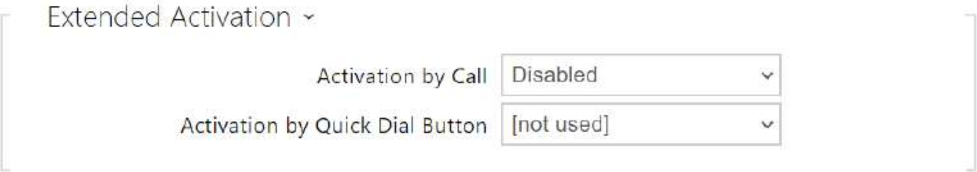
Switch Codes

	CODE	ACCESSIBILITY	TIME PROFILE
1	00	Keypad, DTMF	● [not used]
2		Keypad, DTMF	● [not used]

Distinguish on/off codes ☐

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

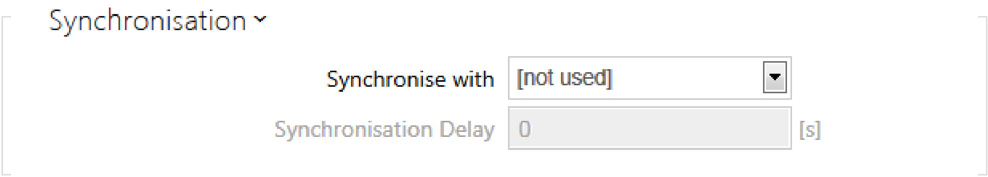


Extended Activation

Activation by Call: Disabled

Activation by Quick Dial Button: [not used]

- **Activation by call** – allows automatic switch activation by incoming or outgoing calls. The switch is activated either for a preset switch-on duration or for the entire call duration in bistable mode.
- **Activation by quick dial button** – assign a quick dial button to the switch. The switch is activated whenever the button is pressed.

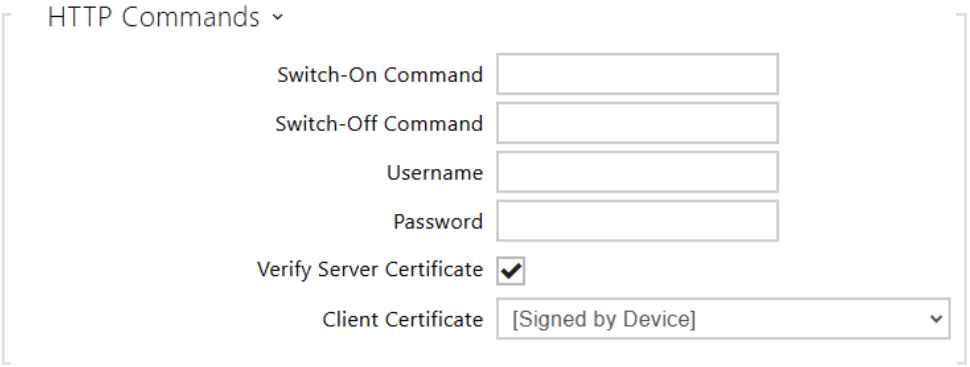


Synchronisation

Synchronise with: [not used]

Synchronisation Delay: 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:

Switch-Off Command:

Username:

Password:

Verify Server Certificate: ☑

Client Certificate: [Signed by Device]

- **Switch-On Command** – set the URL for the HTTP or HTTPS GET request sent on switch activation. The command format is http://ip_address/path. E.g. http://192.168.1.50/relay1=on.
- **Switch-Off Command** – set the URL for the HTTP or HTTPS GET request sent on switch deactivation. The command format is http://ip_address/path. E.g. http://192.168.1.50/relay1=on.
- **Username** – set the username for the HTTP commands sent on switch activation and deactivation. Required only if authentication is required.
- **Password** – set the password for the HTTP commands sent on switch activation and deactivation. Required only if authentication is required.

- **Verify Server Certificate** – enable this to verify the server public certificate against the CA certificates uploaded to the device.
- **Client Certificate** – specify the client certificate and private key to be used for server certificate verification.

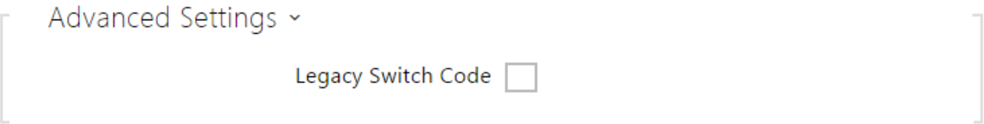
Note

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

Tip

With an external relay, **Part No. 9137410E**, the following HTTP commands are used:
To turn on the switch – http://ip_address/state.xml?relayState=1 (e.g.: http://192.168.1.10/state.xml?relayState=1)
To turn on for pre-defined time (default value is 1.5 s) – http://ip_address/state.xml?relayState=2 (e.g.: http://192.168.1.10/state.xml?relayState=2)
To turn off -http://ip_address/state.xml?relayState=0 (e.g.: http://192.168.1.10/state.xml?relayState=0)
With an external relay, **Part No. 9137411E**, the following HTTP commands are used (replace the X symbol with the relay number):
To turn on the switch – http://ip_address/state.xml?relayXState=1 (e.g.: http://192.168.1.10/state.xml?relay1State=1)
To turn on for pre-defined time (default value is 1.5 s) – http://ip_address/state.xml?relayXState=2 (e.g.: http://192.168.1.10/state.xml?relay1State=2)
To turn off -http://ip_address/state.xml?relayXState=0 (e.g.: http://192.168.1.10/state.xml?relay1State=0)

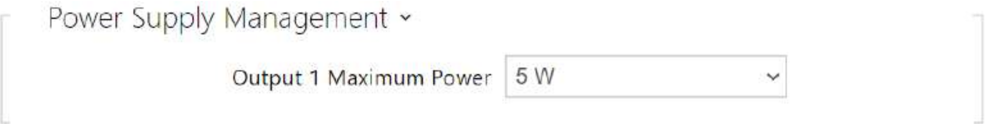
Advanced



Advanced Settings

Legacy Switch Code ☐

- **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.

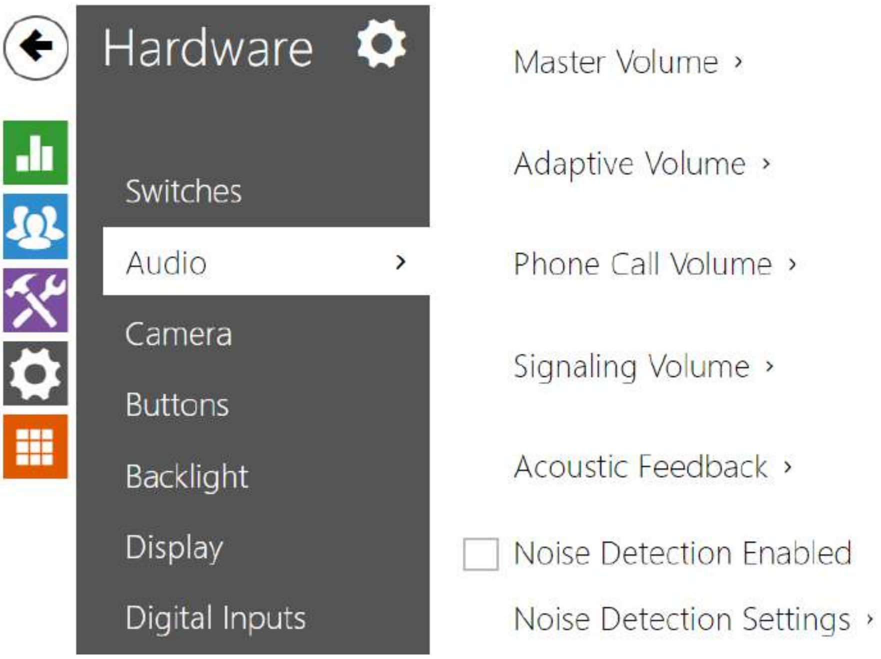


Power Supply Management

Output 1 Maximum Power 5 W

  - **Output 1 Maximum Power** – set the maximum output 1 power value.

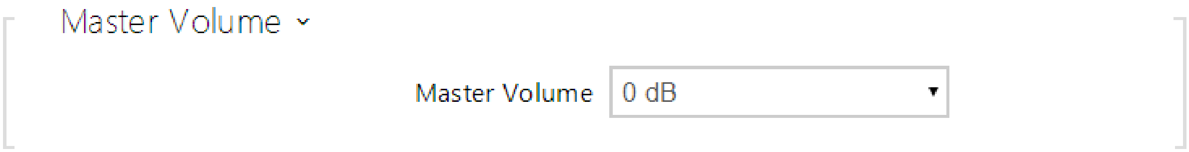
5.5.2 Audio



All the **2N LTE intercom** 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. Set the **Master volume** to control the master volume of the device: volume of calls, signalling tones, etc. Set this parameter according to the ambient noise level. If the noise level is not constant, use the Adaptive mode to increase the master volume temporarily depending on the ambient noise level.

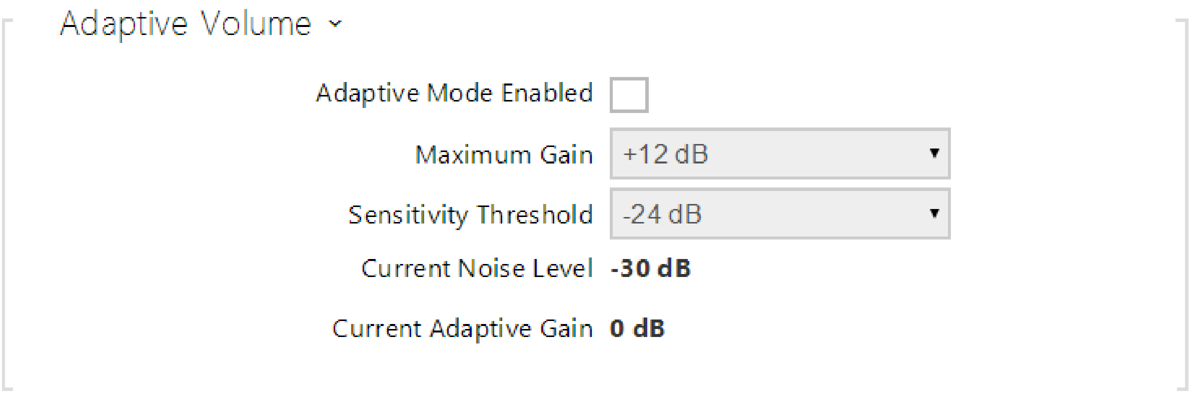
Model	Master Volume
2N LTE Verso	-8 dB .. +8 dB (2W)

List of Parameters



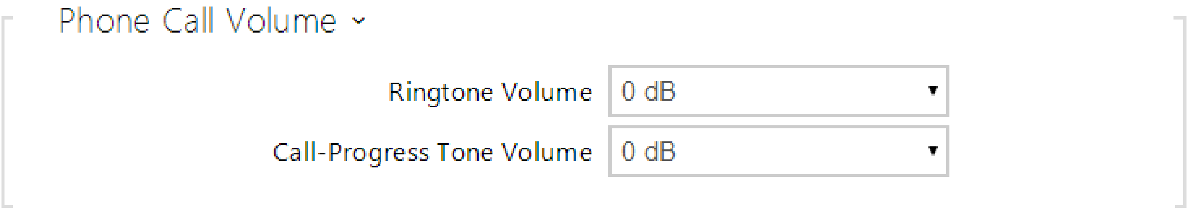
Master Volume: 0 dB

- **Master volume** – set the master volume based on the desired call volume, then adjust other sound volumes as needed. This setting affects the volume of all sounds.



Adaptive Mode Enabled ☐
Maximum Gain: +12 dB
Sensitivity Threshold: -24 dB
Current Noise Level: **-30 dB**
Current Adaptive Gain: **0 dB**

- **Adaptive volume** – enable Adaptive Volume mode, which gradually increases the device volume based on the difference between the measured Current Noise Level and selected Sensitivity Threshold, up to the set Maximum Gain value. This setting further increases Master Volume.
- **Maximum gain** – set the Maximum Gain that can be applied on top of the Master Volume once the Current Noise Level surpasses the Sensitivity Threshold.
- **Sensitivity threshold** – set the ambient noise threshold that determines when the volume starts increasing.
- **Current noise level** – display the current ambient noise level.
- **Current adaptive gain** – display the current adaptive gain of the master volume. The value is determined by the difference of the Current noise level and Sensitivity threshold and never exceeds the Maximum gain value.

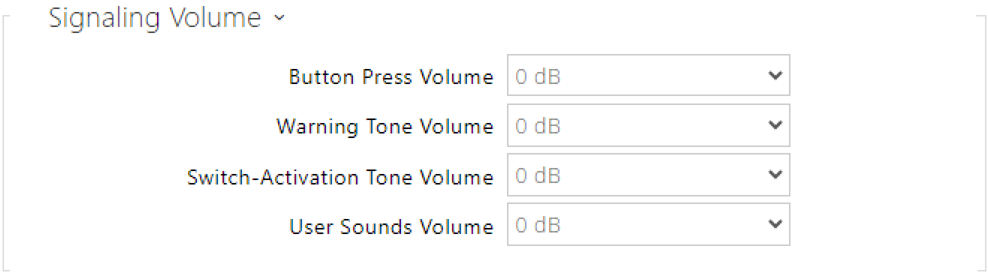


Phone Call Volume

Ringtone Volume: 0 dB

Call-Progress Tone Volume: 0 dB

- **Ringtone volume** – set the volume of the incoming call ringtone. The value is relative to the master volume.
- **Call-progress tone volume** – set the volume for dial, ringing, and busy tones. This setting will not be applied if ringback tones are generated externally. The value is relative to the master volume.



Signaling Volume

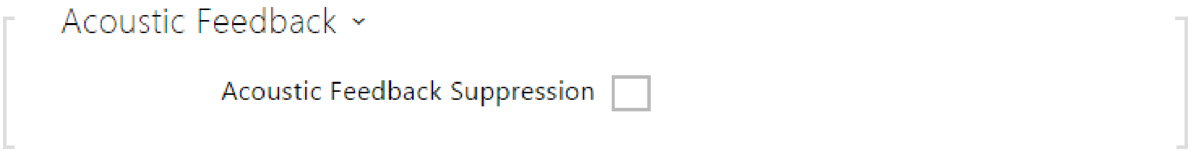
Button Press Volume: 0 dB

Warning Tone Volume: 0 dB

Switch-Activation Tone Volume: 0 dB

User Sounds Volume: 0 dB

- **Button Press Volume** – set the Button Press Volume. The volume values are relative against the set master volume.
- **Warning tone volume** – set the volume of warning and signaling tones described in the Signaling of Operational Statuses section. The value is relative to the master volume.
- **Switch activation tone volume** – set the volume of switch activation tone. The value is relative to the master volume.
- **User sounds volume** – set the volume of user sounds played by automation. The value is relative to the master volume.



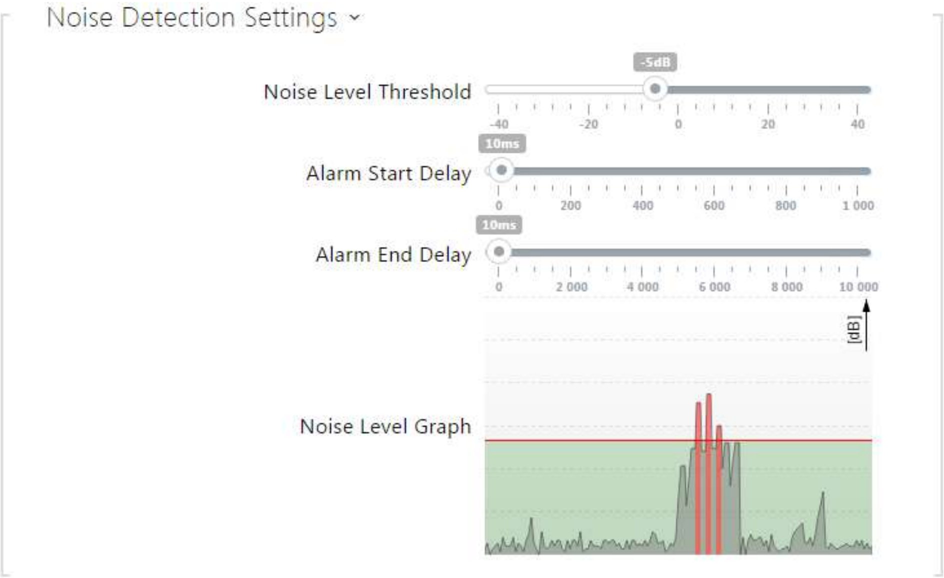
Acoustic Feedback

Acoustic Feedback Suppression ☐

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

☑ Noise Detection Enabled

- **Noise Detection Enabled** – switch on automatic detection of noise or microphone noise level threshold exceeding. Process the threshold exceeding alarm using **Event.NoiseDetected** and assign it to other user actions.



Noise Detection Settings ˅

Noise Level Threshold -5dB

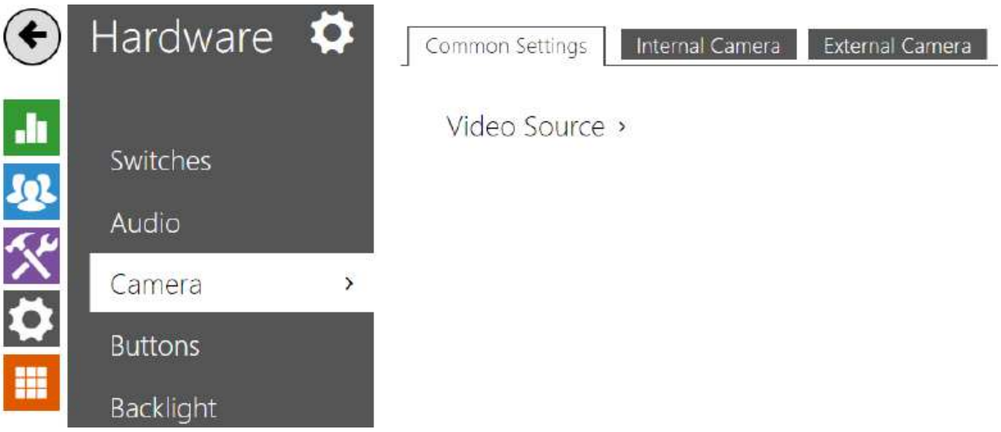
Alarm Start Delay 10ms

Alarm End Delay 10ms

Noise Level Graph

- **Noise Level Threshold** – set the microphone noise level threshold for alarm setting.
- **Alarm Start Delay** – set the time interval during which the signal must be above the threshold to start alarm.
- **Alarm End Delay** – set the time interval during which the signal must be below the threshold to stop alarm.
- **Noise Level Graph** – display the signal level history. Red designates alarm activation.

5.5.3 Camera



This menu is only available in the **2N LTE intercom** 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.

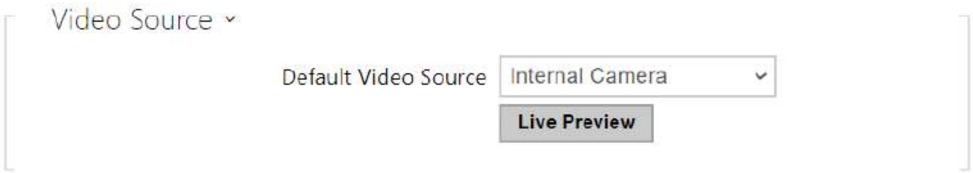
The following video signal sources can be used:

- a standard external IP camera supporting RTSP stream with codecs MJPEG (640 x 480 max resolution) or H.264 3.0 (640 x 480 Base Line Profile max resolution). The recommended framerate is 15 frames per second in either case. Higher frame rates may result in undesired effects (less smooth playing).

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

List of Parameters

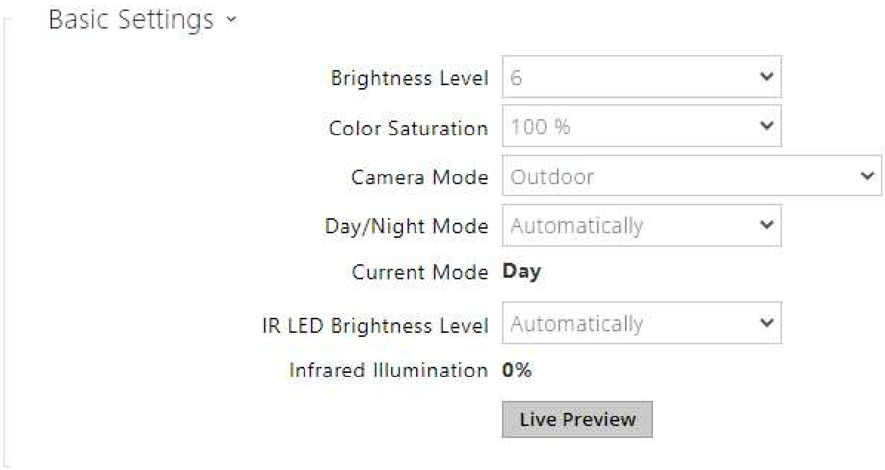
Common Settings



Default Video Source: Internal Camera

- **Default video source** – set default camera source. Choose between the internal camera (or an analog camera connected to the intercom) or an external camera. The change of the default video signal source is applied to the RTSP stream and HTTP API. In **2N IP Eye** it is required to enable the external camera manually, even when there is no internal camera present in the device. If no internal camera is connected to the intercom, External IP camera can only be selected. If the external camera is not connected or configured properly, N/A is displayed on a blue background.
- **Live Preview** – display a live preview from a 2N IP intercom camera.

Internal Camera

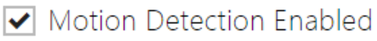


Brightness Level: 6
Color Saturation: 100 %
Camera Mode: Outdoor
Day/Night Mode: Automatically
Current Mode: Day
IR LED Brightness Level: Automatically
Infrared Illumination: 0%

- **Brightness Level** – set the camera image brightness. This setting allows brightening or darkening the entire image.
- **Color Saturation** – set the camera image color saturation.
- **Camera Mode** – set the appropriate combination of exposure mode and power line frequency if flicker is visible in the camera image. Choose variable image flicker

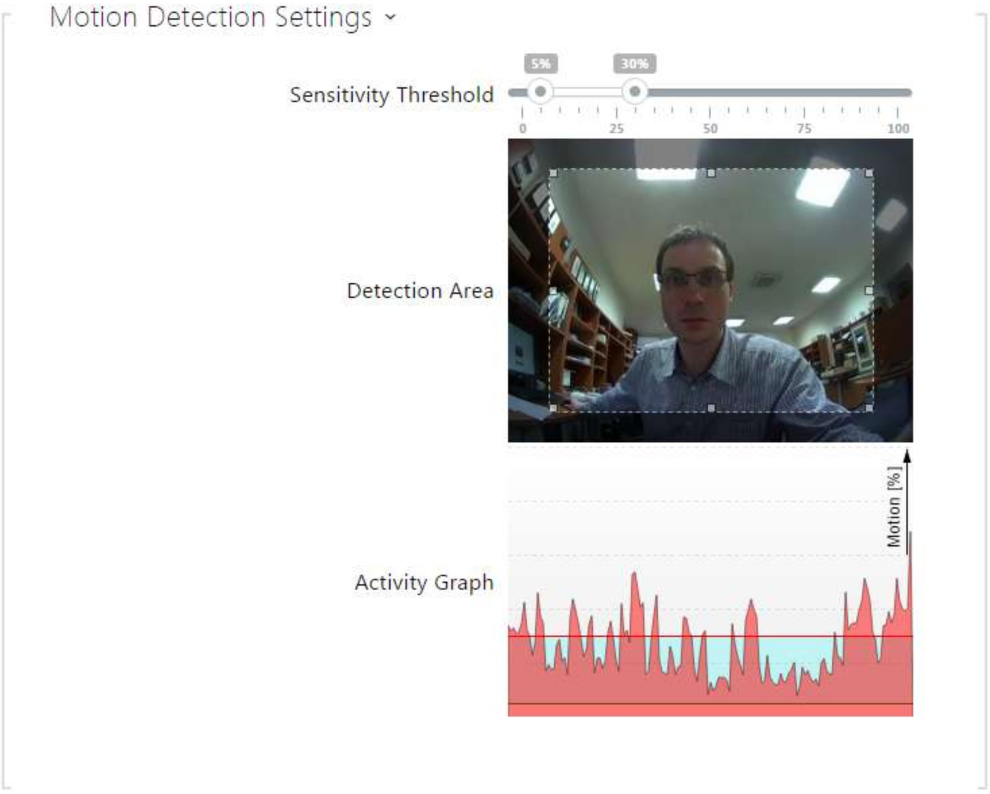
cancellation modes for indoor sites illuminated by artificial light. Or, set direct sunshine suppression for outdoor applications.

- **Day/Night Mode** – set to Always Day to enable the IR suppression filter and disable IR illumination. Set to Always Night to do the opposite and turn the image black and white. Automatic mode switches between the two based on ambient light levels.
- **Current mode** – display the currently selected camera mode (day/night). in the day mode, the camera uses an IR suppressing filter and infrared illumination is disabled. In the night mode, the IR suppressing filter is disabled and infrared illumination is on.
- **IR LED brightness level** – set the IR LED brightness level. IR illumination is only used in Night Mode, which is automatically activated in low ambient light conditions by default.
- **IR Illumination** – 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).
- **Live Preview** – display a live preview from a 2N IP intercom camera.



☑ Motion Detection Enabled

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

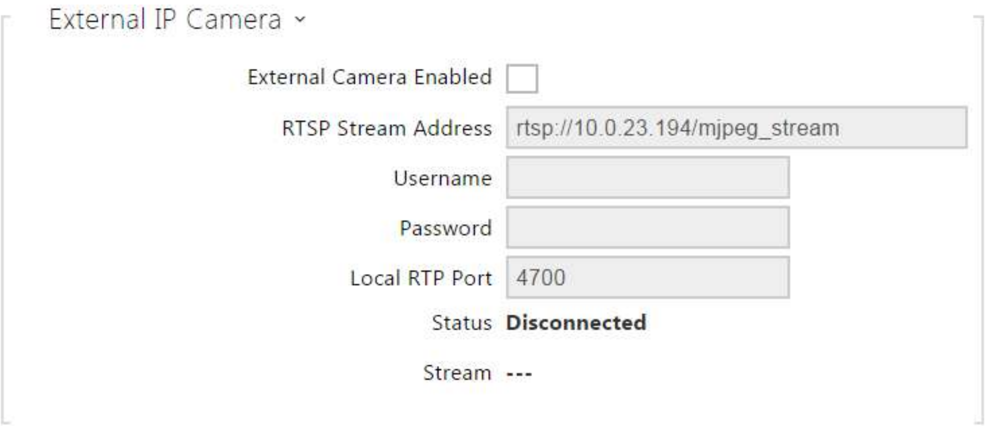


Motion Detection Settings

Sensitivity Threshold 5% 30%

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

External Camera



External IP Camera

External Camera Enabled ☐

RTSP Stream Address rtsp://10.0.23.194/mjpeg_stream

Username

Password

Local RTP Port 4700

Status **Disconnected**

Stream ---

- **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, refer to the parameter table below. The parameters are specific for the selected IP camera model. If you choose another **2N LTE intercom** for the external camera, enter http://ip_address/mjpeg_stream or http://ip_address/h264_stream.

Parameter	Description	Values / Example

vcodec	Video Codec	vcodec=h264 for codec H.264
		vcodec=mjpeg for codec MJPEG

vres	Video Resolution	vres=640x480 for VGA
fps	Video Framerate	fps=15 (1 to 30 fps, MJPEG video codec limit is 15 fps).
vbr	Bitrate	vbr=768 for 768 kbps
audio	Audio	• audio=1 (enabled) • audio=0 (disabled)

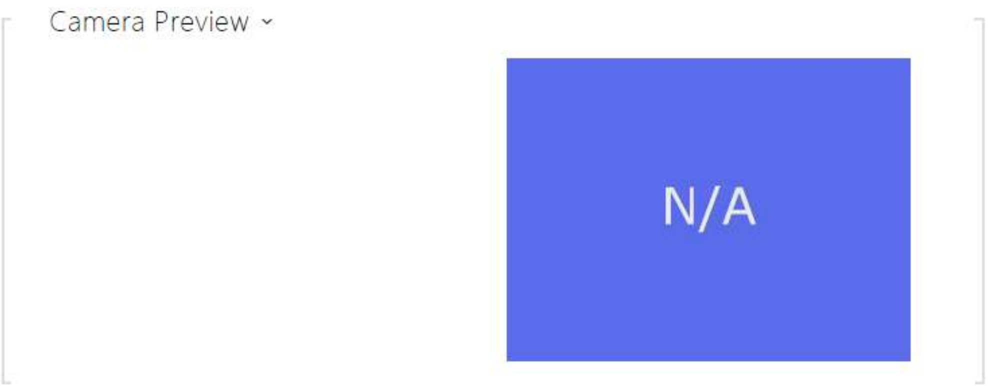
Parameter	Description	Values / Example

zipstream	Zipstream	zipstream=off (disabled)
		zipstream=low
		zipstream=medium
		zipstream=high
		zipstream=higher

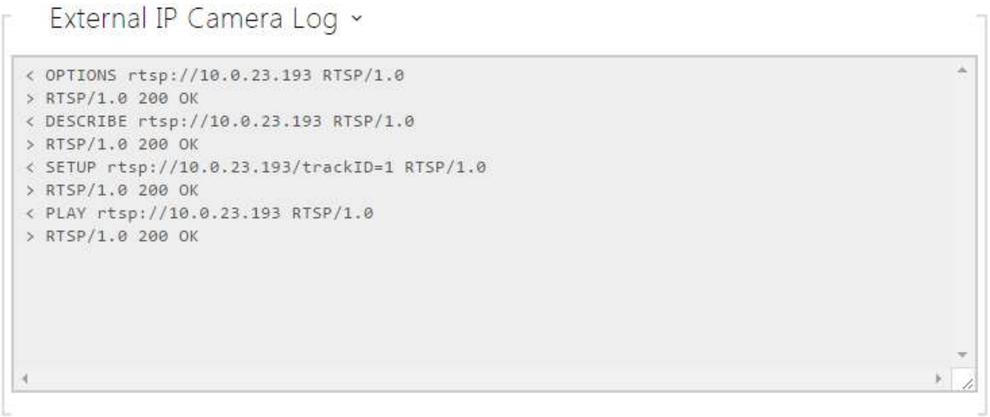
- **Username** – enter the username for the external IP camera authentication. The parameter is obligatory only if the external IP camera requires authentication.
- **Password** – enter the external IP camera authentication password. The parameter is obligatory only if the external IP camera requires authentication.
- **Local RTP port** – set the local UTP port for RTP stream receiving.

Tip

- FAQ: External camera - How to set it in 2N IP/LTE intercom



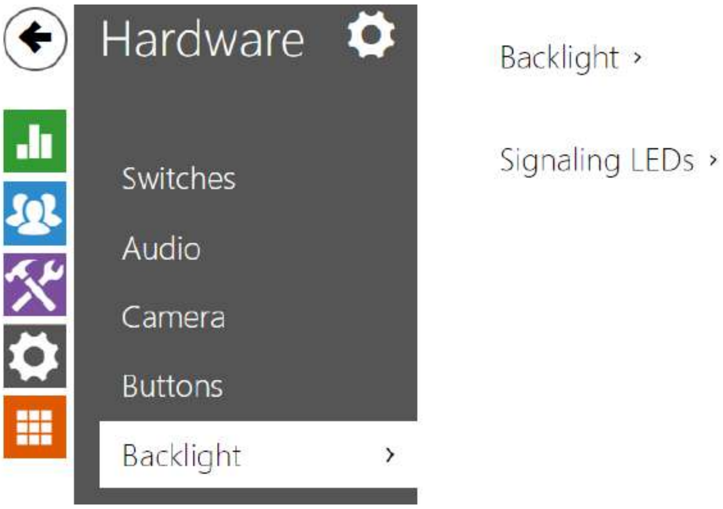
The Camera Preview window displays the current image received from an external camera. If the external camera is disconnected or configured incorrectly, the N/A characters are displayed on a blue background.



```
< OPTIONS rtsp://10.0.23.193 RTSP/1.0
> RTSP/1.0 200 OK
< DESCRIBE rtsp://10.0.23.193 RTSP/1.0
> RTSP/1.0 200 OK
< SETUP rtsp://10.0.23.193/trackID=1 RTSP/1.0
> RTSP/1.0 200 OK
< PLAY rtsp://10.0.23.193 RTSP/1.0
> RTSP/1.0 200 OK
```

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

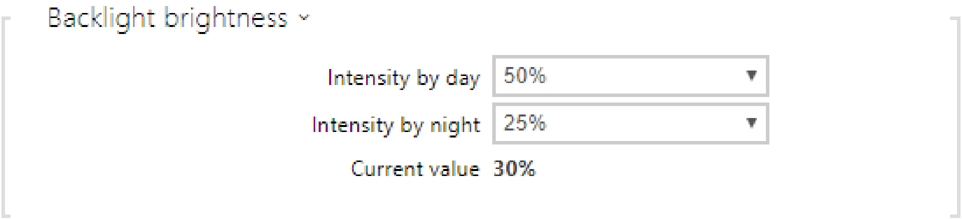
5.5.4 Backlight



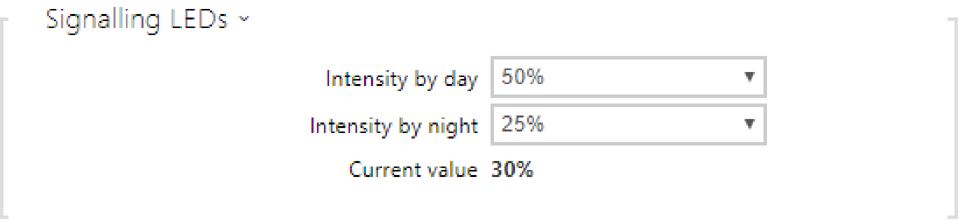
This tab helps you control the backlight level of nametags, buttons and brightness of signalling LEDs.

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

Property/Model	2N® LTE Verso
Backlight level control	**Yes**
Ambient light level sensor	**Yes**
Independent name tag and LED backlight level control	**Yes**


Backlight brightness ˅

Intensity by day 50%
Intensity by night 25%
Current value 30%


Signalling LEDs

Intensity by day 50%

Intensity by night 25%

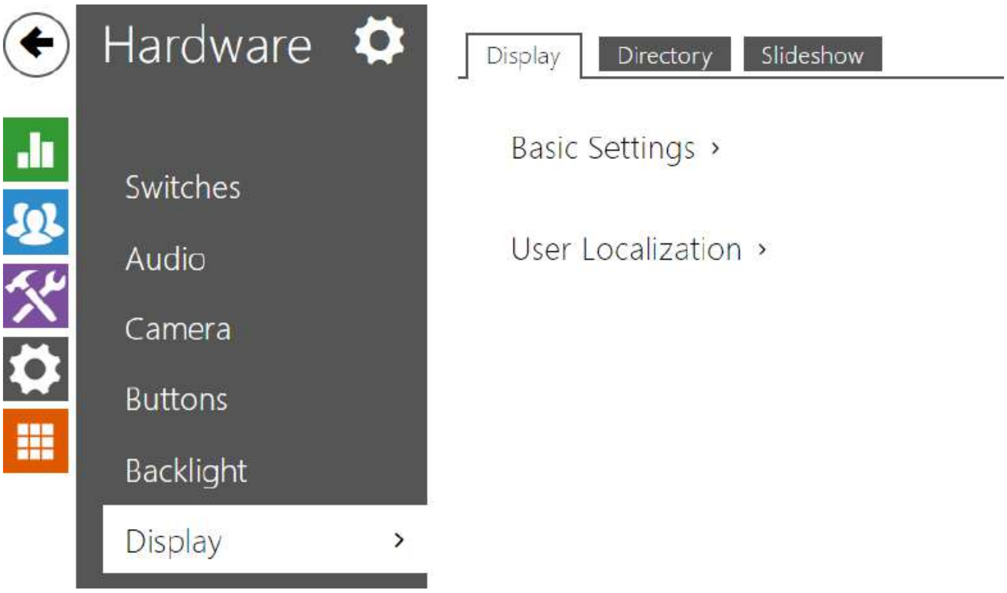
Current value 30%

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

Note

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

5.5.5 Display

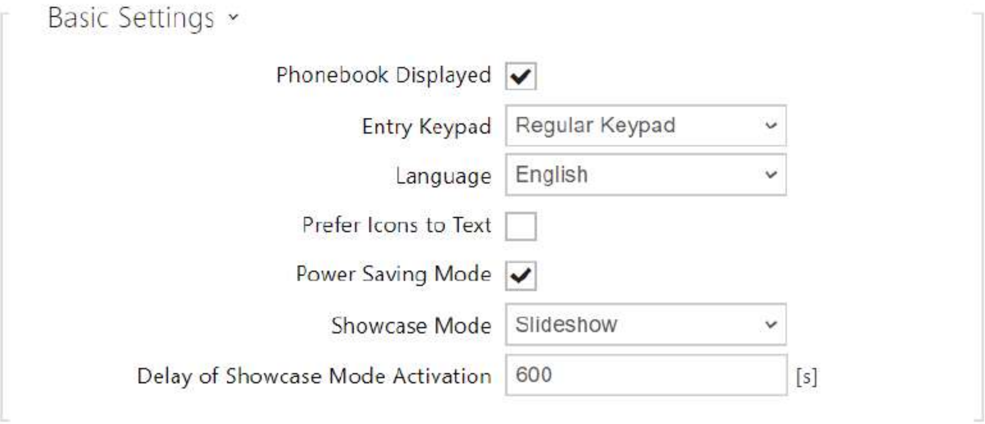


Some intercom models **2N LTE Verso** can be equipped with a colour LCD display. The device state is displayed (call progress, door opening, etc.) and the following modes are available:

Display – enable the display and language settings for **2N LTE Verso.**

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

Display



Basic Settings

Phonebook Displayed ☑

Entry Keypad: Regular Keypad

Language: English

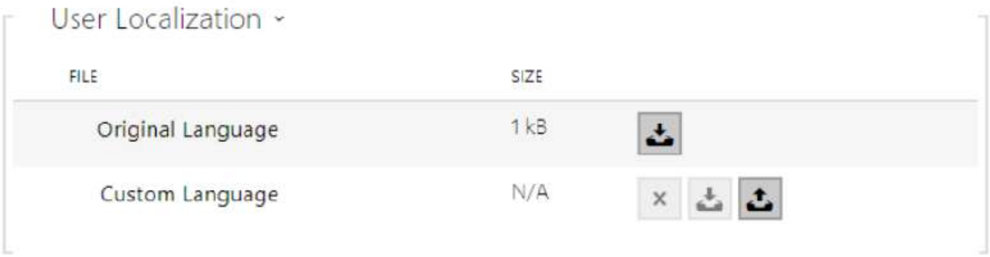
Prefer Icons to Text ☐

Power Saving Mode ☑

Showcase Mode: Slideshow

Delay of Showcase Mode Activation: 600 [s]

- **Phone book displayed** – enable/disable display of the phone book function.
- **Entry Keypad** – enable the keypad/keypad type.
  - **Disabled** – disable the keypad.
  - **Regular keypad** – set the regular keypad type.
  - **Scramble keypad** – enable/disable keypad button scrambling (random button transposing) before every new display to prevent other persons from watching the code entered (**Enhanced Security** licence required).
- **Language** – set the language for the texts to be displayed. Choose one of the predefined languages: English, Czech, German, Italian, French, Spanish, Russian, Finnish, Danish, Polish, Dutch, Portuguese, Turkish, Norwegian, Swedish, Thai, Hebrew or a custom language.
- **Prefer Icons to Text** – the icons on the dosplay will be preferred to the text.
- **Power saving mode** – activate the power saving mode in which the display brightness is reduced. If no event occurs during two Slideshow screen activation timeouts, the power saving mode activation has been successful. Set 0 in the Slideshow screen activation timeout to disable the power saving mode. Any movement in front of the intercom camera or any display event (such as door lock activation or display touch) restores the full brightness of the display.
- **Showcase Mode** – set whether the device shall go into the showcase mode when idle. Choose various options in the showcase mode (Slideshow, Company Logo, Address).
- **Showcase Mode Delay** – set the idle timeout in the range of 1 to 600 seconds after which the device goes into the Showcase Mode. There is always a fixed 15-second timeout for the device to return to the homescreen.



User Localization

FILE	SIZE
Original Language	1 kB
Custom Language	N/A

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

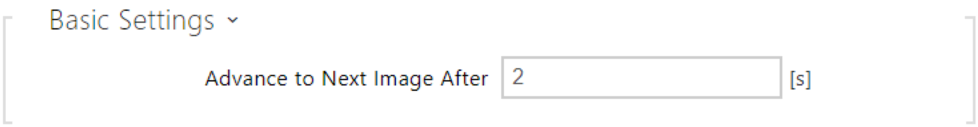
Note

If none of the pre-defined languages is convenient for you, proceed as follows:

- Download the original language file (English).
- Modify the file using a text editor (replace the English texts with your own ones).
- Upload the modified localisation file to the intercom.
- Set **Language Settings | Language** to **Custom.**
- Check and correct if necessary the texts on the intercom display.

Slideshow

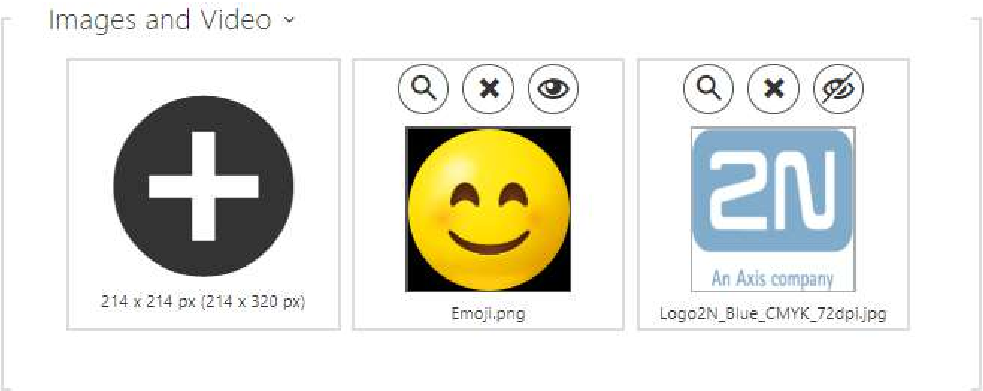
This tab helps you set the image and video list for the Slideshow mode. Up to 8 images and videos can be uploaded for the Slideshow to be switched with a predefined delay.



Basic Settings ˅

Advance to Next Image After: 2 [s]

- **Advance to Next Image After** – set the image displaying time in a slideshow.



Valid for **2N LTE Verso**

Make sure that the image / video resolution is 214 x 214 or 214 x 320 pixels up to 2 MB. Other sizes will be adjusted to the display resolution automatically.

Click the magnifier icon 🔍 to view the loaded image, press ✖ to delete an image and click 👁 to hide a selected image/video on the device display. Click the variable image/video icon 👁 to set a time profile 📅 for the display. If no time profile is active, the slideshow will have no time profile conditioned content. In the same case, the slideshow will always have a content that is not conditioned by a time profile. If no image is loaded, the Slideshow mode will never be activated.

✔ **Tip**

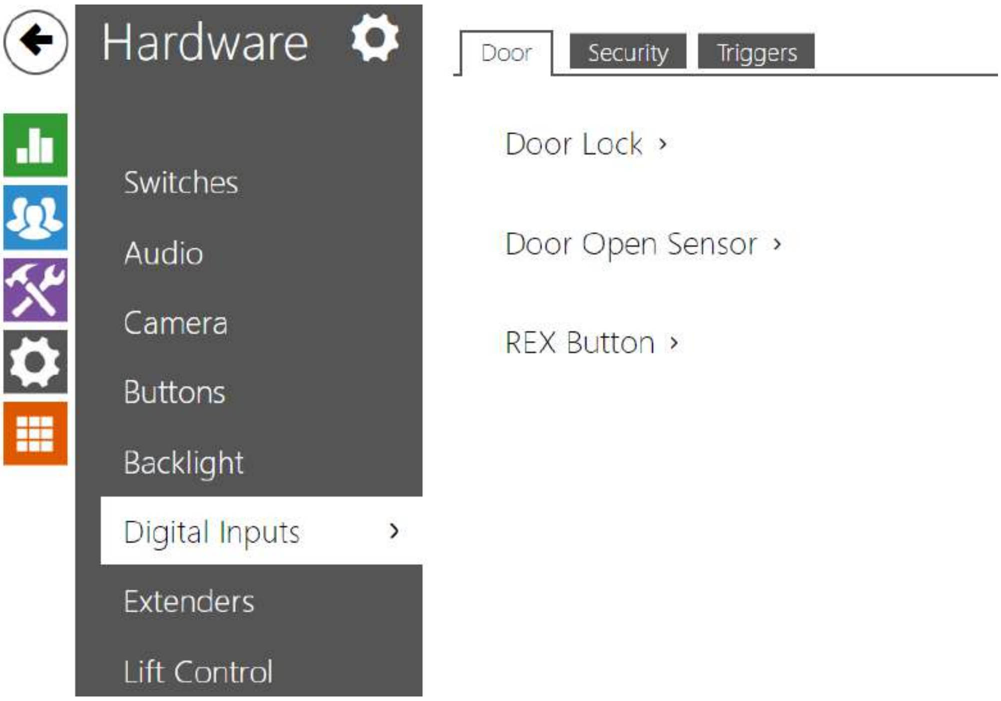
- To hide the "Start with touch" display on the 2N LTE Verso model display, load an image of the resolution of 214 x 320 pixels.

Caution

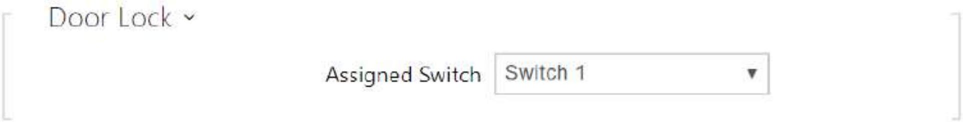
- Video with a 214 x 320 resolution cannot be uploaded in FW versions lower than 2.35.

5.5.6 Digital Inputs

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

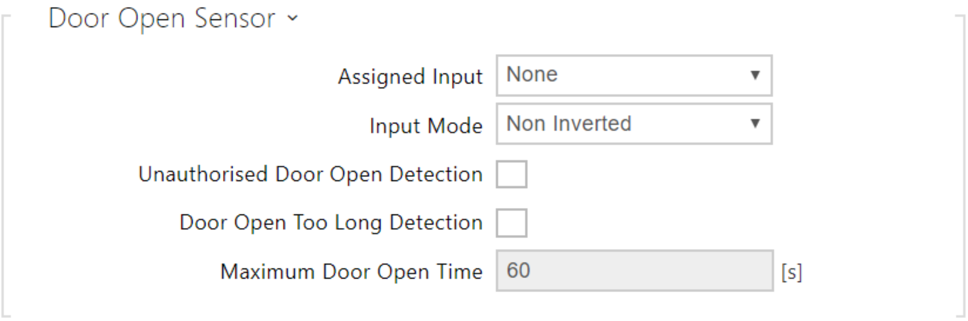


Door



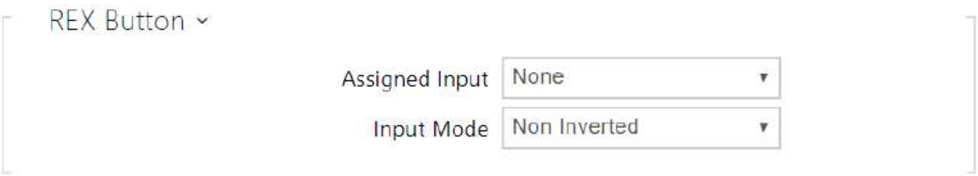
Assigned Switch: Switch 1

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



Assigned Input: None
Input Mode: Non Inverted
Unauthorised Door Open Detection ☐
Door Open Too Long Detection ☐
Maximum Door Open Time: 60 [s]

- **Assigned Input** – define one (or none) of the logic inputs for open door detection.
- **Unauthorized Door Open Detection** – detect that the door has been opened without the assigned door switch being activated first.
- **Door Open Too Long Detection** – door open too long detection.
- **Maximum Door Open Time** – duration for which the door can remain open before the Door Open Too Long event is triggered.

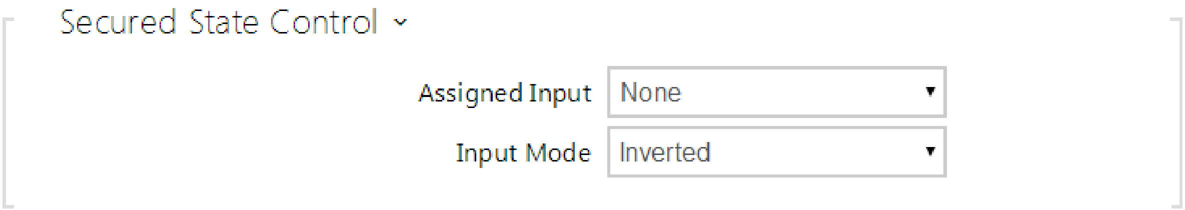


Assigned Input: None

Input Mode: Non Inverted

- **Assigned Input** – select a logical input for the exit button function. Activation of the exit button input activates the assigned door lock switch, the switch-on duration and mode of which are configured in the settings of the selected switch.
- **Input Mode** – set the active input mode (polarity).

Security



Assigned Input: None

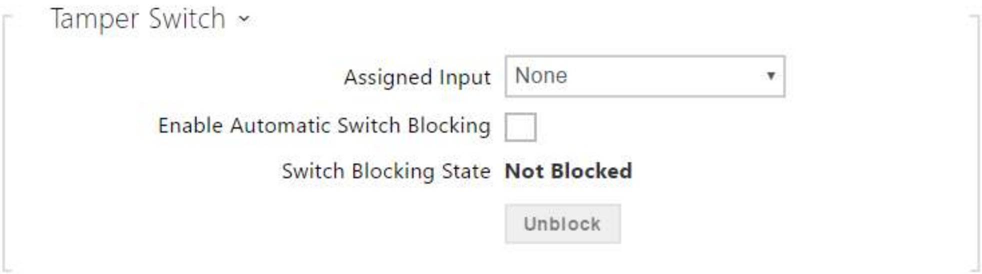
Input Mode: Inverted

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

Note

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

  The ***2N LTE Verso*** *intercoms are equipped with a red padlock pictogram in the left-hand upper corner of the basic module.*



Assigned Input: None

Enable Automatic Switch Blocking: ☐

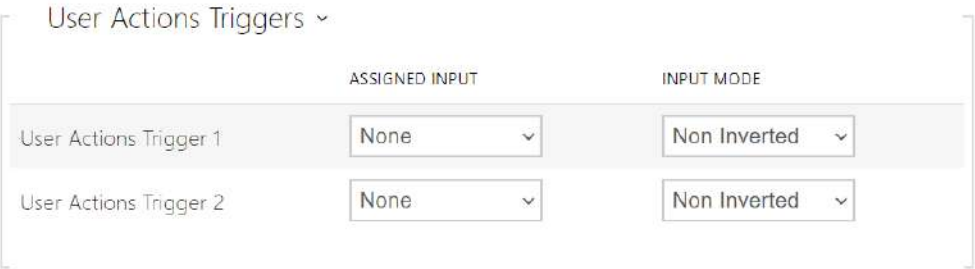
Switch Blocking State: **Not Blocked**

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

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

- **Assigned input** – select the logic input to which the tamper switch is to be connected. **TamperSwitchActivated** signals the tamper switch activation.
- **Automatic Switch Blocking** – Blocks the switches by tamper activation for 30 minutes.
- **Switch Blocking State** – display and make switch blocking settings.

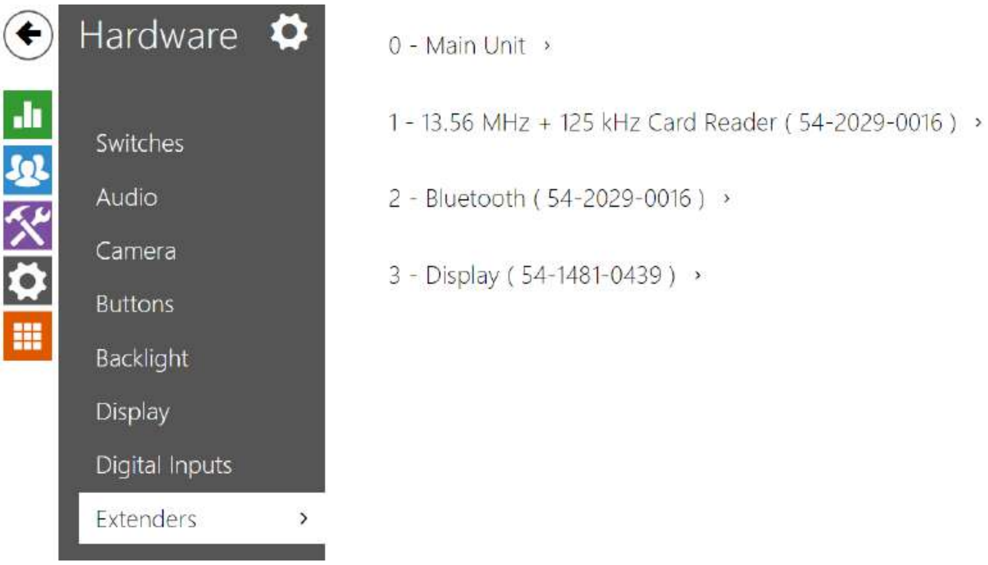
Triggers


User Actions Triggers

	ASSIGNED INPUT	INPUT MODE
User Actions Trigger 1	None	Non Inverted
User Actions Trigger 2	None	Non Inverted

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

5.5.7 Extenders



0 - Main Unit

1 - 13.56 MHz + 125 kHz Card Reader (54-2029-0016)

2 - Bluetooth (54-2029-0016)

3 - Display (54-1481-0439)

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

- Five-button module
- Keypad module
- Infopanel module
- Card reader module
- Bluetooth module

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

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

⚠ **Caution**

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

⚠ **Caution**

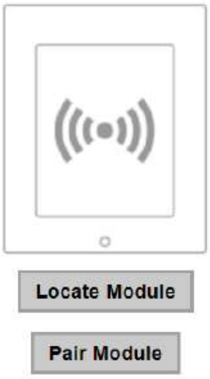
- Be sure to configure the replaced modules. The configuration is tied with the module serial number.

Note

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

Caution

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



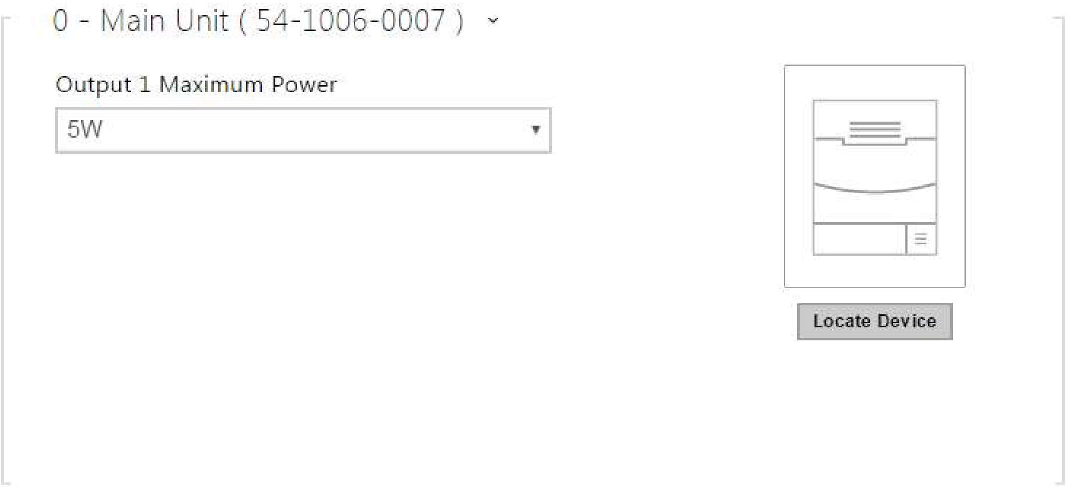
Caution

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

Tip

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

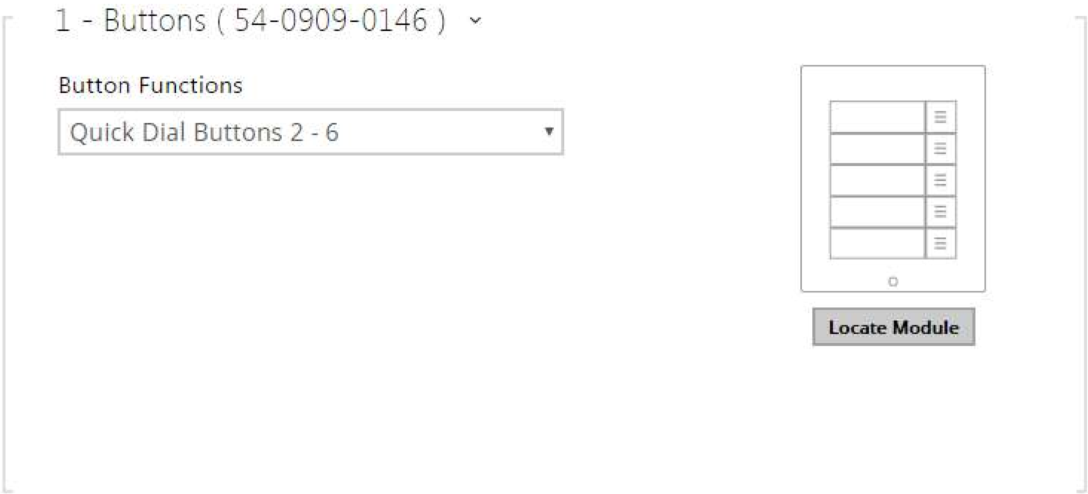
Main Unit Module Configuration



Output 1 Maximum Power
5W

- **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.
- **Locate Device** – optical and acoustic signalling of a device. Note: Optical signalling is possible only if the device is equipped with control backlight (Verso, Base, Vario, Force, Safety and Uni). If a speaker is not integrated in the device, make sure than an external speaker is connected (Audio Kit and Video Kit) to use sound signalling.

Button Module Configuration

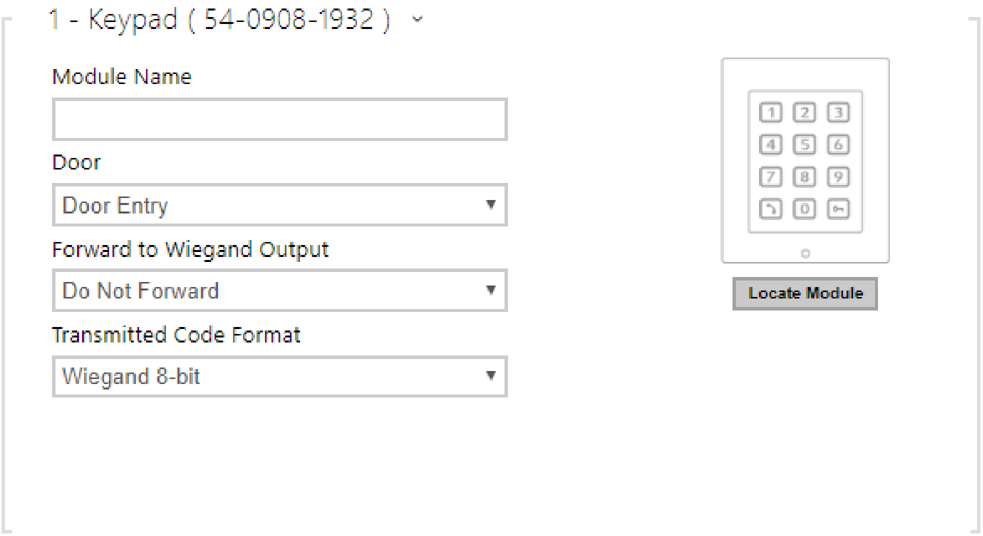


1 - Buttons (54-0909-0146)

Button Functions: Quick Dial Buttons 2 - 6

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

Keypad Module Configuration



1 - Keypad (54-0908-1932)

Module Name

Door: Door Entry

Forward to Wiegand Output: Do Not Forward

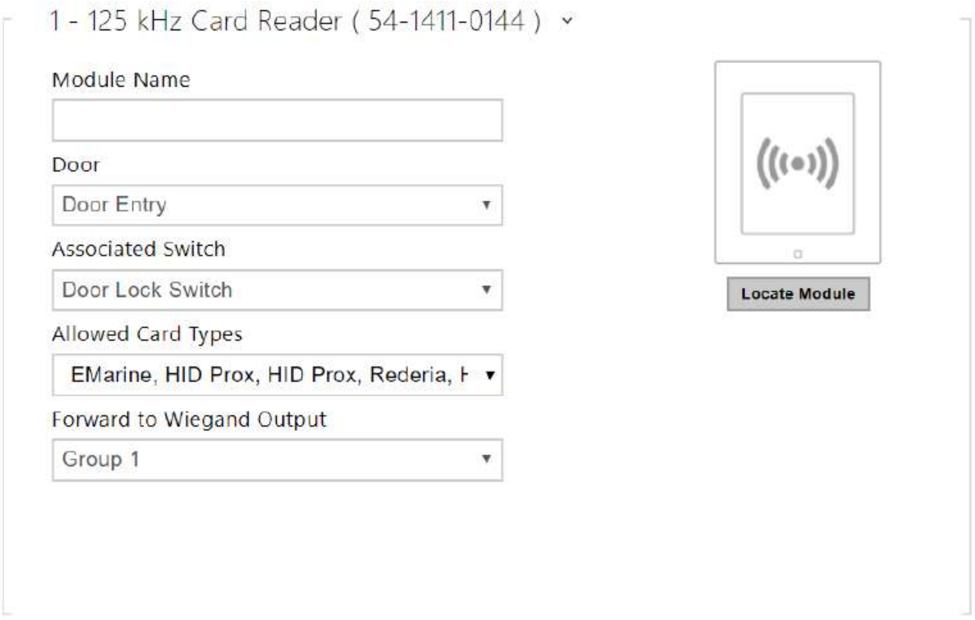
Transmitted Code Format: Wiegand 8-bit

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

Infopanel Module Configuration

- No parameters are available to the public at present.

125 kHz Card Reader Module Configuration



1 - 125 kHz Card Reader (54-1411-0144)

Module Name:

Door: Door Entry

Associated Switch: Door Lock Switch

Allowed Card Types: EMarine, HID Prox, HID Prox, Rederia,

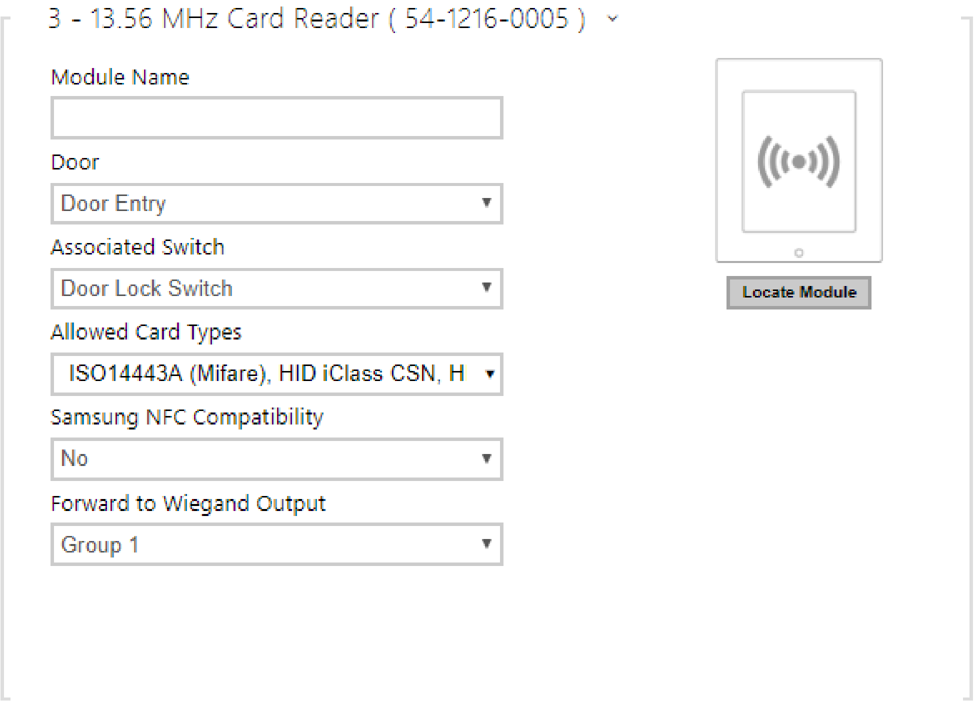
Forward to Wiegand Output: Group 1

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

✓ **Tip**

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

13.56 MHz Card Reader Module Configuration


3 - 13.56 MHz Card Reader (54-1216-0005)

Module Name

Door: Door Entry

Associated Switch: Door Lock Switch

Allowed Card Types: ISO14443A (Mifare), HID iClass CSN, H

Samsung NFC Compatibility: No

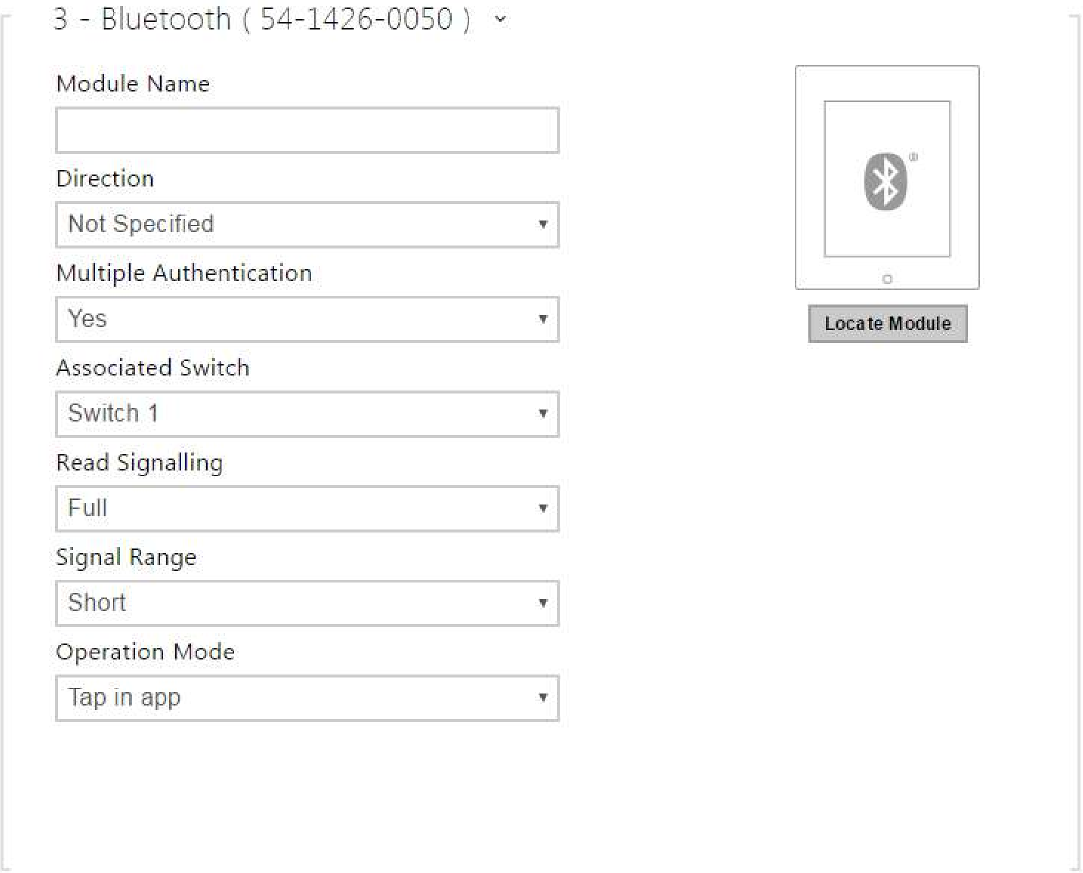
Forward to Wiegand Output: Group 1

- **Module Name** – set the module name for card reader logging purposes.
- **Door** – set the reader direction (Door Entry, Door Exit) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports just one card type at an instant.
- **Samsung NFC Compatibility** – enable NFC compatibility with the Samsung phones.
- **Forward to Wiegand Output** – set a group of Wiegand outputs to which all the received RFID card IDs will be resen

Tip

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

Bluetooth Module



3 - Bluetooth (54-1426-0050)

Module Name

Direction: Not Specified

Multiple Authentication: Yes

Associated Switch: Switch 1

Read Signalling: Full

Signal Range: Short

Operation Mode: Tap in app

- **Module Name** – set the module name for logging events from the Bluetooth module.
- **Direction** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Multiple Authentication** – enable multiple user authentication via this module (or, authentication is controlled by the user card settings; refer to Directory / Users). Multiple authentication can be disabled for each reader connected to the intercom.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Read Signalling** – set one of the sound signalling modes for the module:
  - **Full**– valid and invalid accesses are distinguished by sound signalling
  - **Single beep**– valid and invalid accesses are signalled by a single beep
  - **None**– module use is not signalled by any sound
- **Signal Range** – set the signal range (5 = maximum, 1 = minimum), i.e. the distance over which the Bluetooth module can communicate with a mobile phone. It is recommended

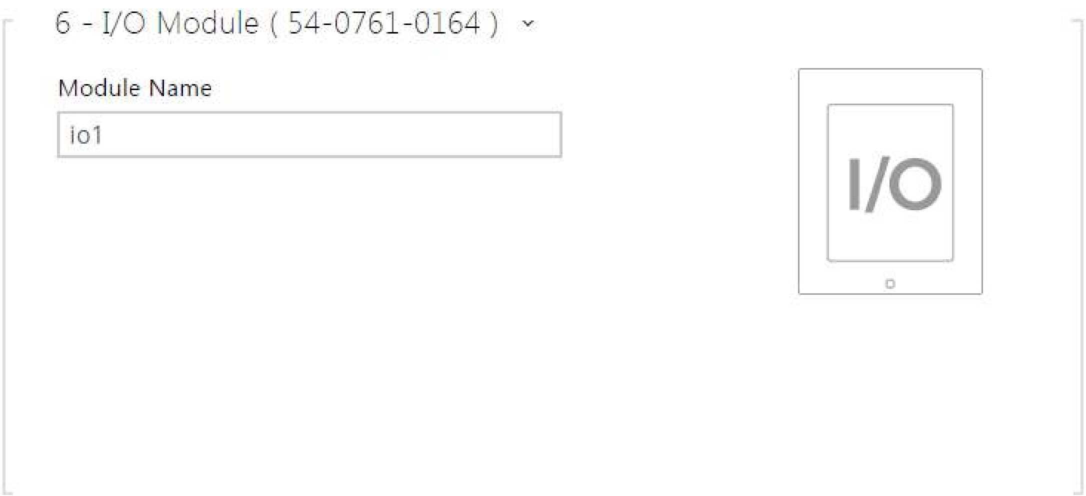
that the actual signal range is tested while setting, as it is affected by a number of factors (installation layout, mobile phone type and position in particular).

- **Operation Mode** – set the authentication method for a mobile phone:
    - **In App** – authentication has to be confirmed by tapping on an icon in the application running in a mobile phone.
    - **Touch mode** – touch the card reader having a phone with paired **My2N** to confirm authentication.

Warning

- An upgrade to version 2.30 is followed by upgrades in the Bluetooth modules. A downgrade to version 2.29 and lower may make the Bluetooth modules non-functional.

I/O Module Configuration



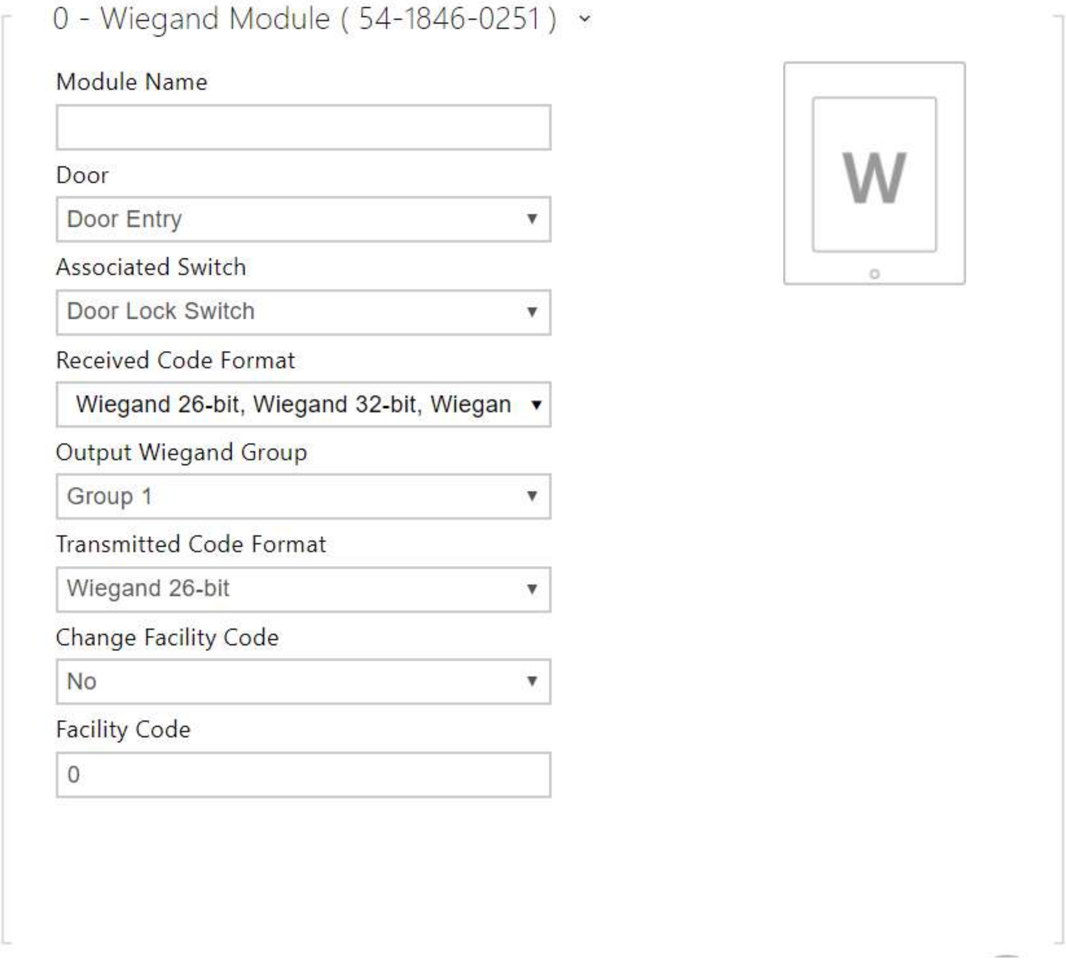
6 - I/O Module (54-0761-0164)

Module Name: io1

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

Wiegand Module Configuration

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



0 - Wiegand Module (54-1846-0251)

Module Name

Door: Door Entry

Associated Switch: Door Lock Switch

Received Code Format: Wiegand 26-bit, Wiegand 32-bit, Wiegan

Output Wiegand Group: Group 1

Transmitted Code Format: Wiegand 26-bit

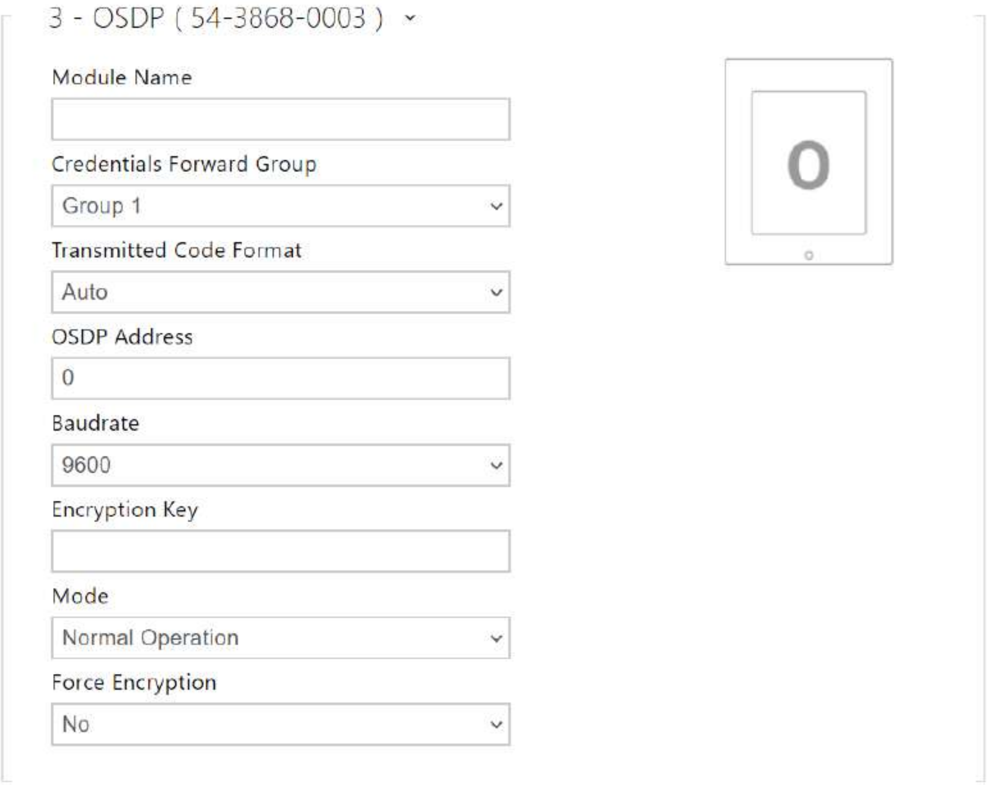
Change Facility Code: No

Facility Code: 0

- **Module Name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N Automation**.
- **Door** – set the reader direction (Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Received Code Format** – set the format for the codes to be received (Wiegand 26, 32, 37 and RAW).
- **Output Wiegand Group** – assign the output Wiegand to a group to which the codes from the connected card readers or Wiegand inputs can be resent.
- **Transmitted Code Format** – set the format for the codes to be transmitted (26-bit, 32-bit, 37-bit and RAW format, 35-bit, Corp. 1000, 48-bit, Corp. 1000 and Auto).

- **Change Facility Code** – set the first code part via Wiegand. This applies to Wiegand OUT for 26-bit code format. Contact your security system supplier to know if the Facility Code is requested.
- **Facility Code** – define the 2N IP device location in the security system. Enter a decimal value for the location (0–255).

OSDP Module Configuration



3 - OSDP (54-3868-0003)

Module Name

Credentials Forward Group: Group 1

Transmitted Code Format: Auto

OSDP Address: 0

Baudrate: 9600

Encryption Key

Mode: Normal Operation

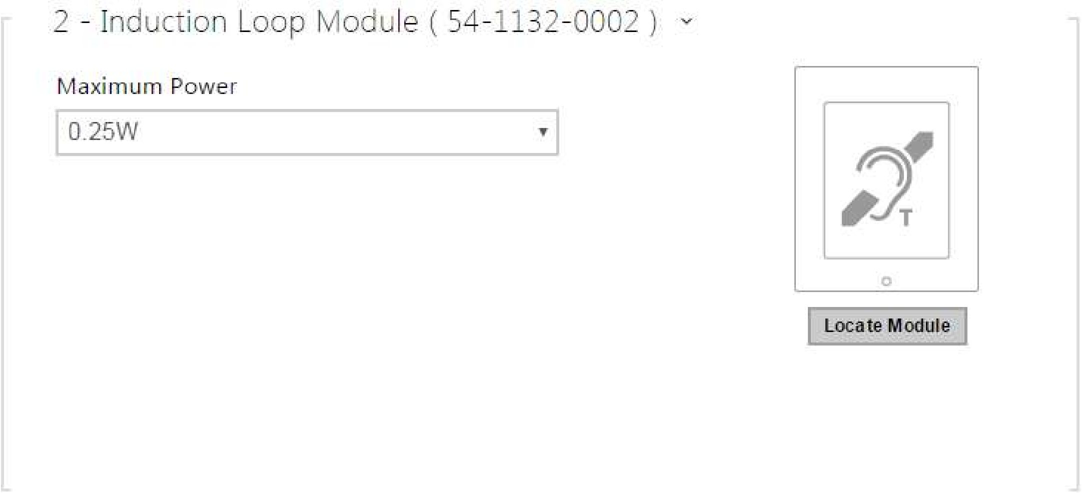
Force Encryption: No

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

Caution

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

Induction Loop Module Configuration



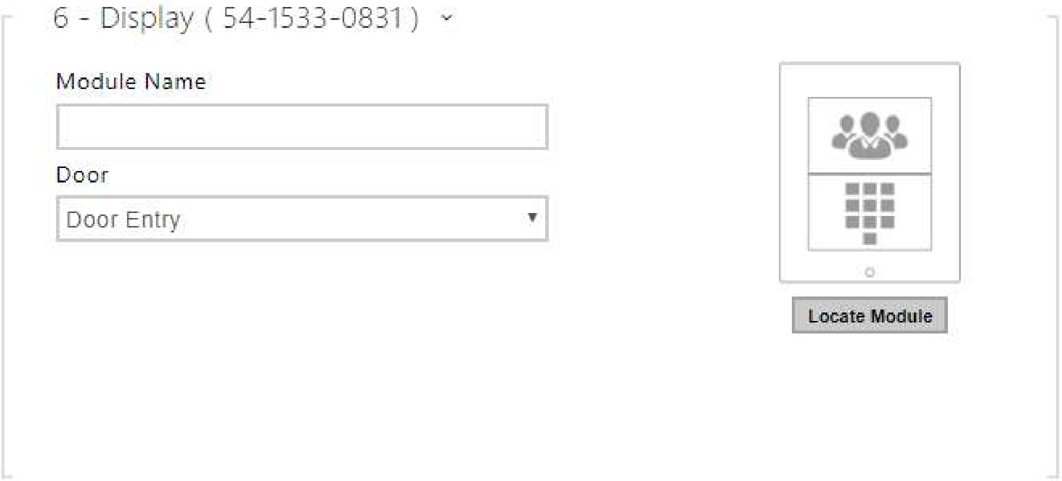
2 - Induction Loop Module (54-1132-0002)

Maximum Power

0.25W

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

Display Module Configuration



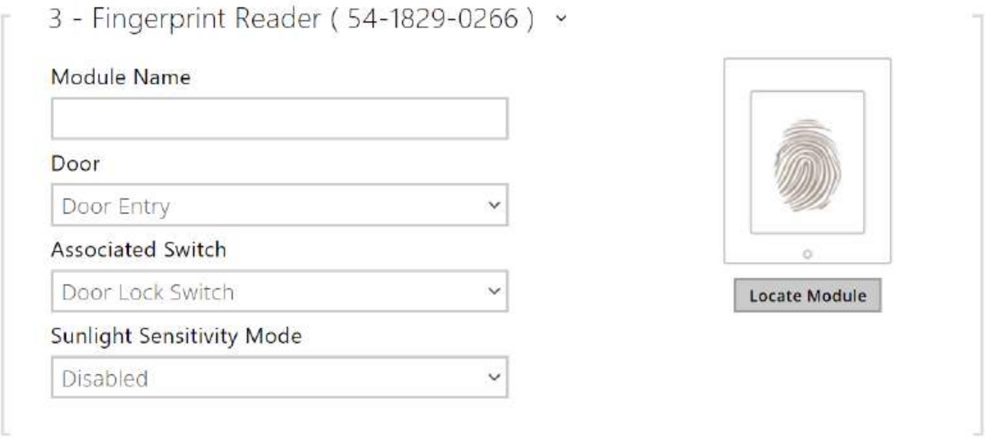
6 - Display (54-1533-0831)

Module Name

Door: Door Entry

- **Module Name** – set the module name for input/output specification in the SetOutput, GetInput and InputChanged objects in the **2N Automation**.
- **Door** – set the reader direction (Arrival, Departure) for the Attendance system purposes.

Fingerprint Reader Module Configuration



3 - Fingerprint Reader (54-1829-0266)

Module Name

Door: Door Entry

Associated Switch: Door Lock Switch

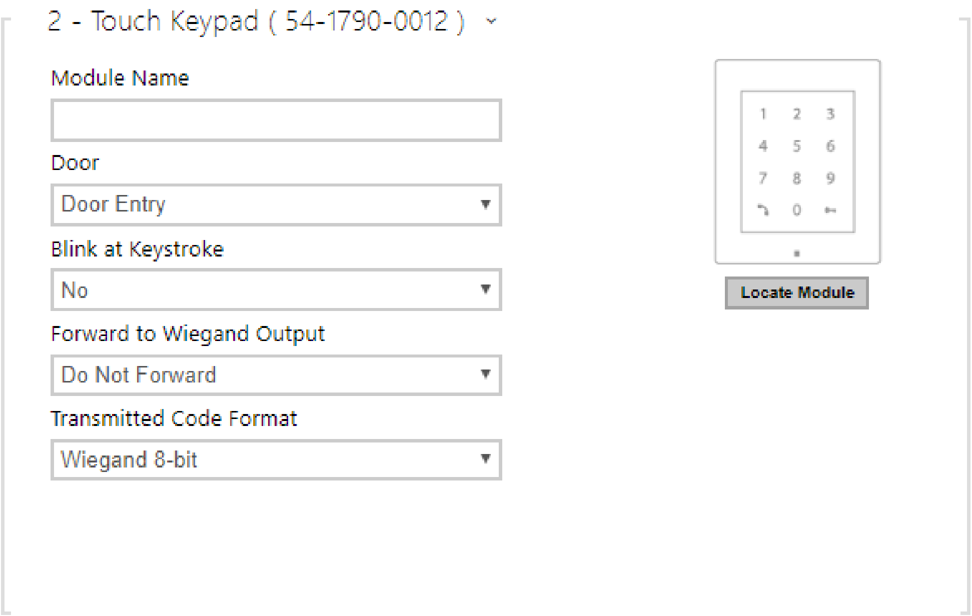
Sunlight Sensitivity Mode: Disabled

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

Caution

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

Touch Keypad



2 - Touch Keypad (54-1790-0012)

Module Name

Door: Door Entry

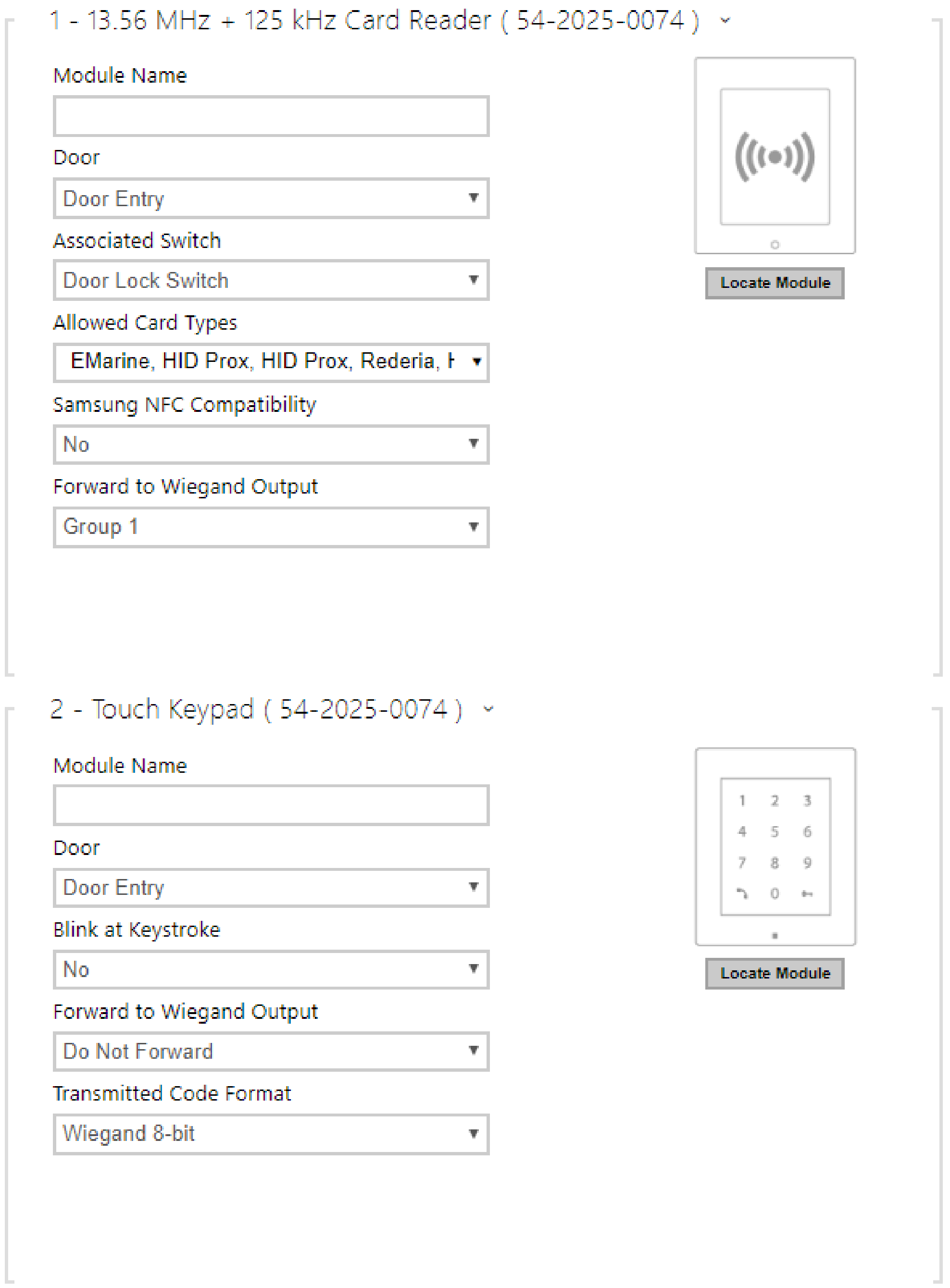
Blink at Keystroke: No

Forward to Wiegand Output: Do Not Forward

Transmitted Code Format: Wiegand 8-bit

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

Touch Keypad & RFID Reader 125 kHz, 13.56 MHz



1 - 13.56 MHz + 125 kHz Card Reader (54-2025-0074)

Module Name:

Door: Door Entry

Associated Switch: Door Lock Switch

Allowed Card Types: EMarine, HID Prox, HID Prox, Rederia,

Samsung NFC Compatibility: No

Forward to Wiegand Output: Group 1

2 - Touch Keypad (54-2025-0074)

Module Name:

Door: Door Entry

Blink at Keystroke: No

Forward to Wiegand Output: Do Not Forward

Transmitted Code Format: Wiegand 8-bit

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

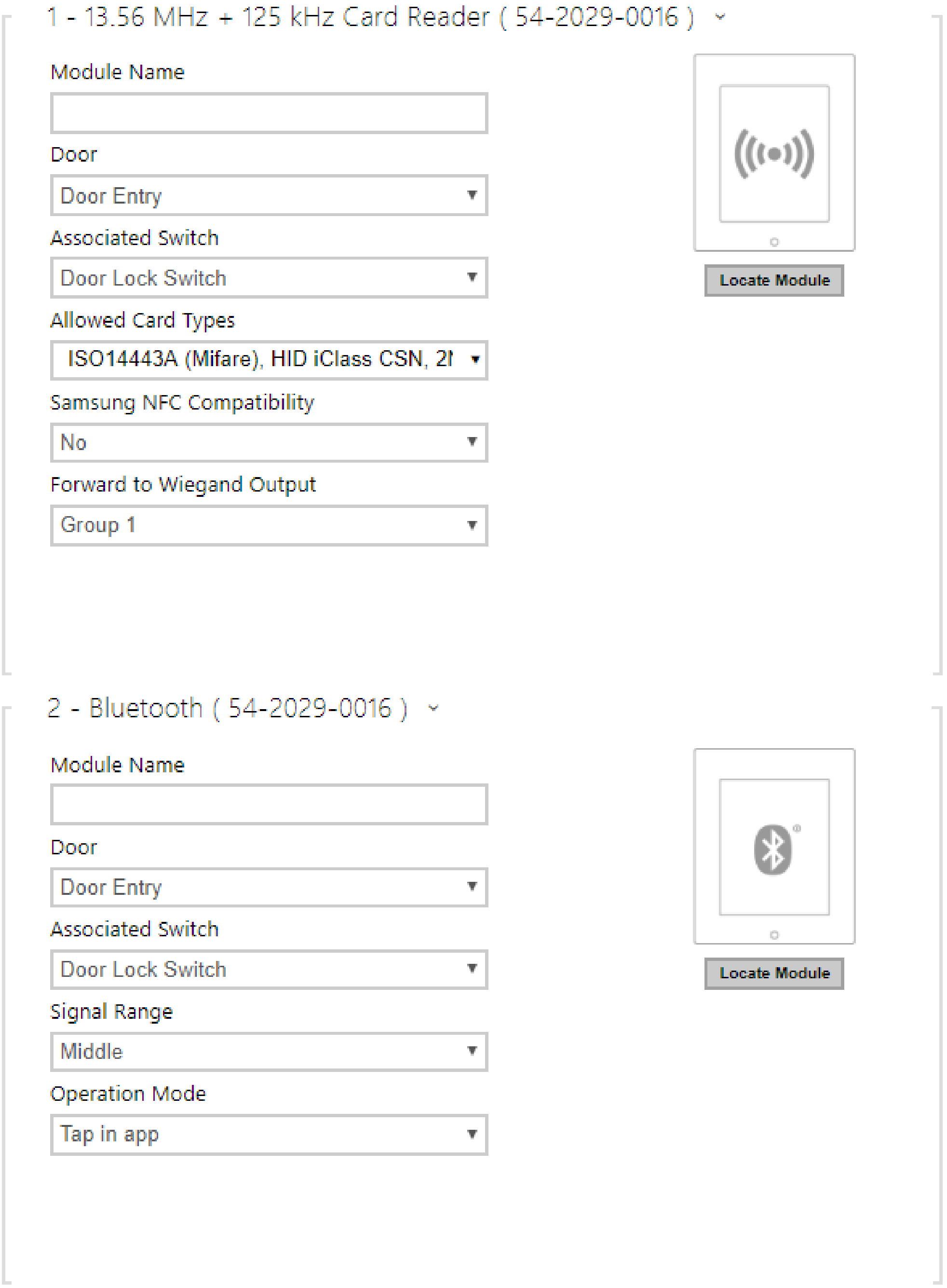
- **Module Name** – set the module name for card reader logging purposes.

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

Touch keypad (serial number)

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

Bluetooth & RFID Reader 125 kHz, 13.56 MHz



1 - 13.56 MHz + 125 kHz Card Reader (54-2029-0016)

Module Name

Door: Door Entry

Associated Switch: Door Lock Switch

Allowed Card Types: ISO14443A (Mifare), HID iClass CSN, 2N

Samsung NFC Compatibility: No

Forward to Wiegand Output: Group 1

2 - Bluetooth (54-2029-0016)

Module Name

Door: Door Entry

Associated Switch: Door Lock Switch

Signal Range: Middle

Operation Mode: Tap in app

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

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

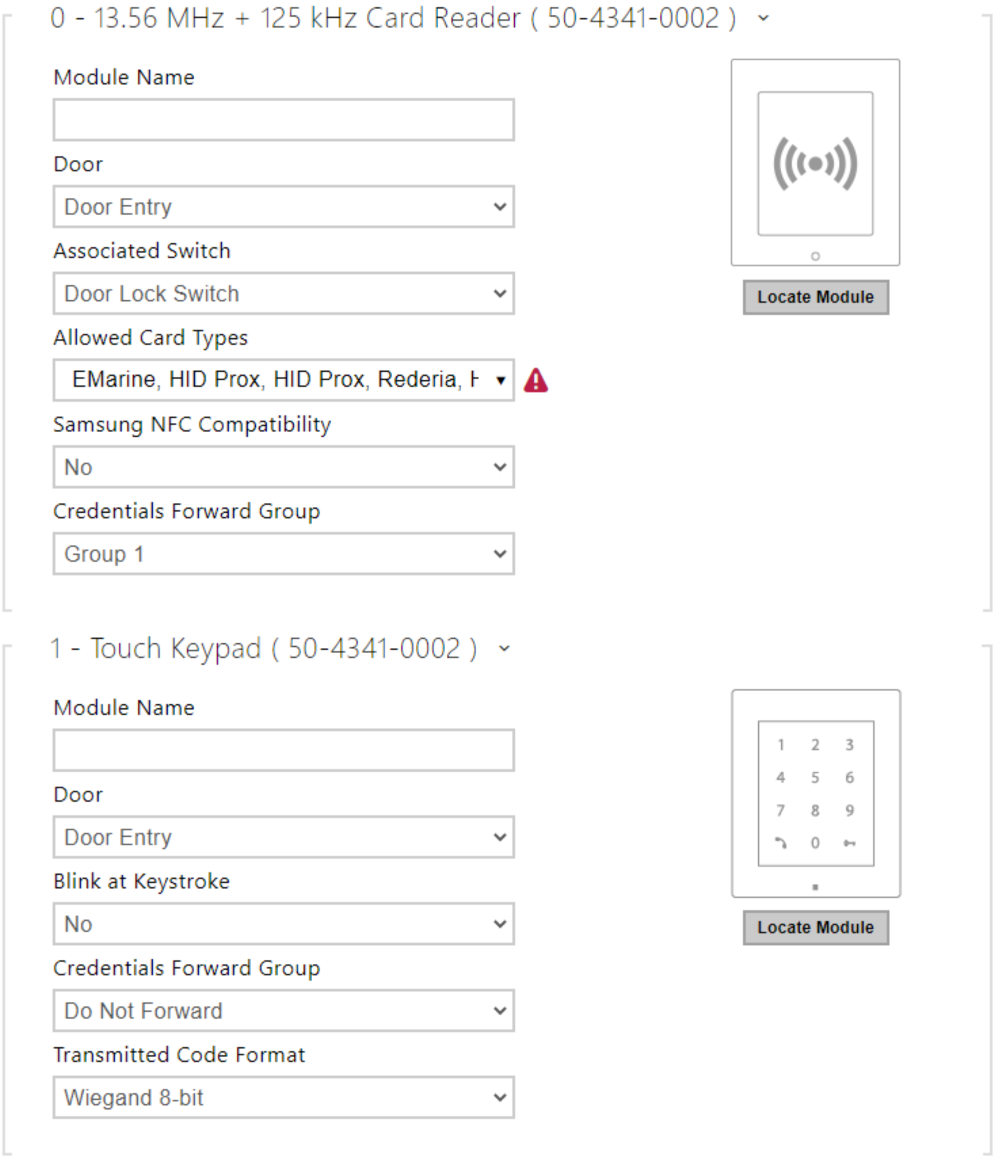
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Allowed Card Types** – set the type of a card to be accepted by the card reader. The card reader supports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

Bluetooth (serial number)

- **Module Name** – set the module name for logging events from the Bluetooth module.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.
- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Signal Range** – set the signal range (5 = maximum, 1 = minimum), i.e. the distance over which the Bluetooth module can communicate with a mobile phone. It is recommended that the actual signal range is tested while setting, as it is affected by a number of factors (installation layout, mobile phone type and position in particular).

- **Start Authentication** – set the authentication method using a mobile phone:
  - **Interacting with Device** – authentication has to be confirmed by a press on the reader in the presence of a phone with paired **My2N**.
  - **In App** – authentication has to be confimed by tapping on an icon in the application running in the phone.
  - **Via Motion Detection** – authentication is launched by motion detection in the presence of a phone with paired **My2N**.
- **Motion Detection Profile** – set the motion detection profile to be obeyed by the module for authentication using a mobile phone.

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



0 - 13.56 MHz + 125 kHz Card Reader (50-4341-0002)

Module Name:

Door: Door Entry

Associated Switch: Door Lock Switch

Allowed Card Types: EMarine, HID Prox, HID Prox, Rederia,

Samsung NFC Compatibility: No

Credentials Forward Group: Group 1

1 - Touch Keypad (50-4341-0002)

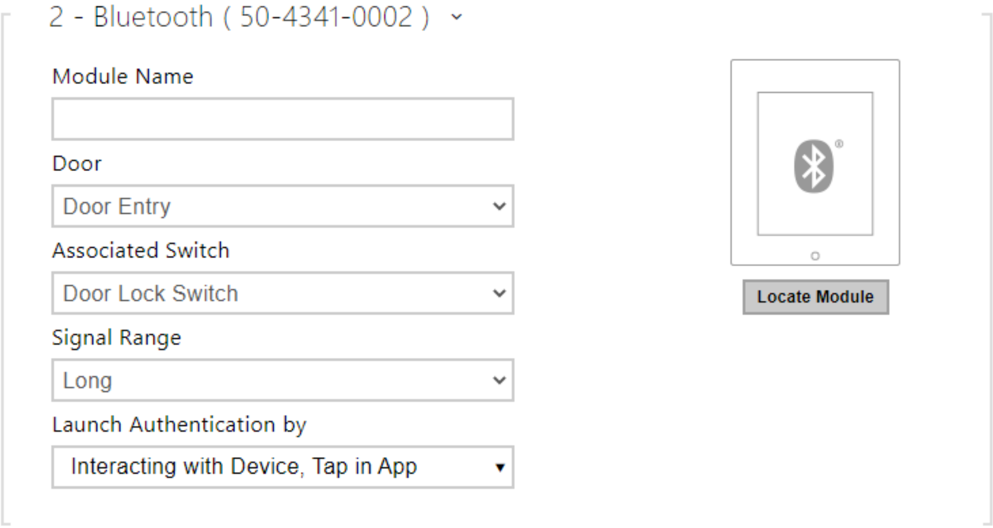
Module Name:

Door: Door Entry

Blink at Keystroke: No

Credentials Forward Group: Do Not Forward

Transmitted Code Format: Wiegand 8-bit



2 - Bluetooth (50-4341-0002)

Module Name

Door: Door Entry

Associated Switch: Door Lock Switch

Signal Range: Long

Launch Authentication by: Interacting with Device, Tap in App

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

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

Touch keypad (serial number)

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

Bluetooth (serial number)

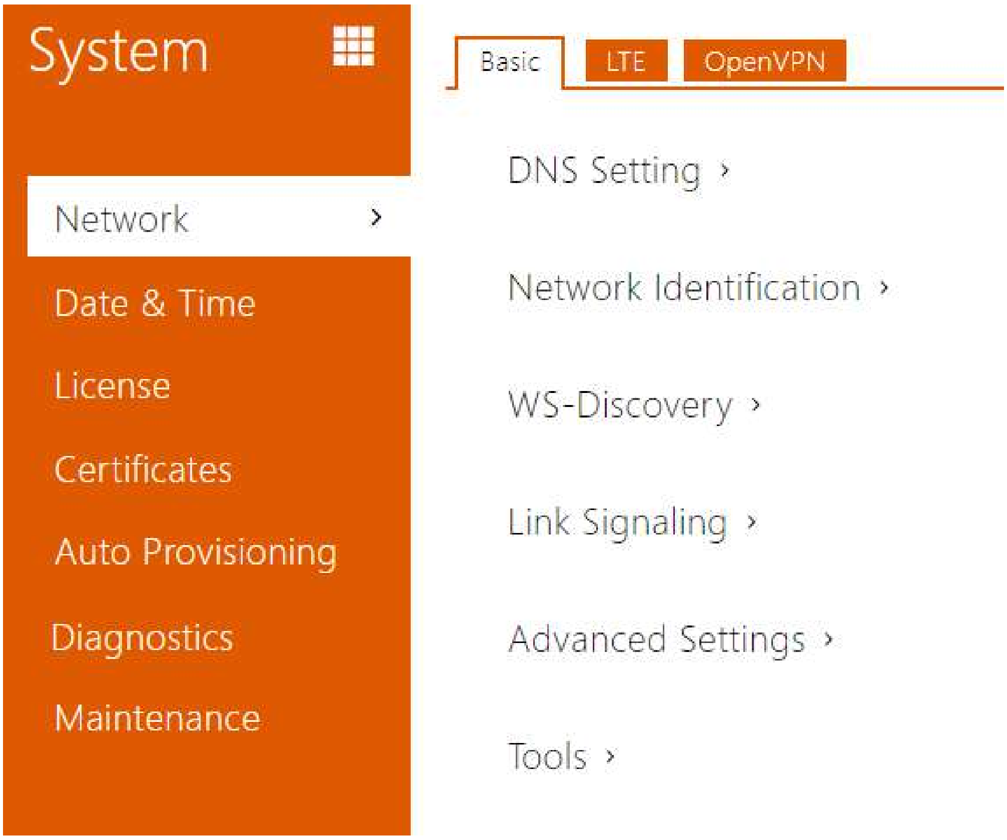
- **Module Name** – set the module name for logging events from the Bluetooth module.
- **Door** – set the reader direction (Not specified, Arrival, Departure) for the Attendance system purposes.

- **Associated Switch** – set the switch to be activated after user authentication via this module. If you set Door Lock Switch, the authentication rules specified in Hardware / Door will be used.
- **Signal Range** – set the signal range (5 = maximum, 1 = minimum), i.e. the distance over which the Bluetooth module can communicate with a mobile phone. It is recommended that the actual signal range is tested while setting, as it is affected by a number of factors (installation layout, mobile phone type and position in particular).
- **Start Authentication** – set the authentication method using a mobile phone. Set one or a combination of two/three authetication launch methods.
    - **In App** – authentication has to be confirmed by tapping on an icon in the application running in a mobile phone.
    - **Interacting with Device** – touch the card reader having a phone with paired **My2N** to confirm authentication.
    - **Via Motion Detection** – authentication will be launched by motion detection via a phone with the paired **My2N** application.

5.6 System

Here is what you can find in this section:

5.6.1 Network

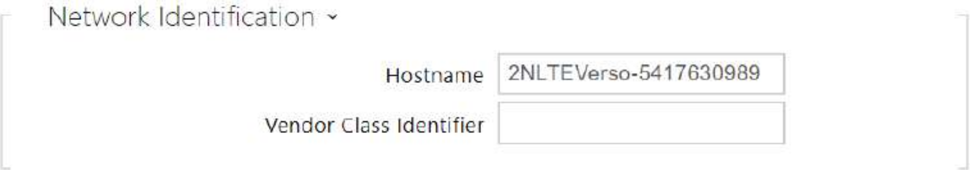


The **2N LTE intercom** gets connected to the LTE network via a SIM card. The access data (APN, access name and password) are configured automatically. To change the LTE access data configuration, use SMS (refer to the Installation manual) or the LTE tab of the web configuration interface (see below).

List of Parameters

Network

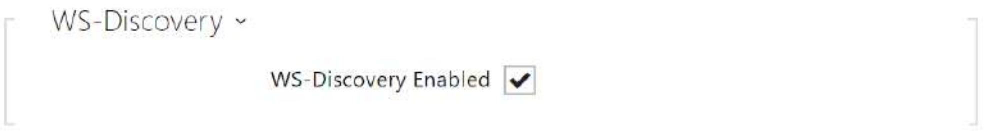
Basic



Hostname: 2NLTEVerso-5417630989

Vendor Class Identifier:

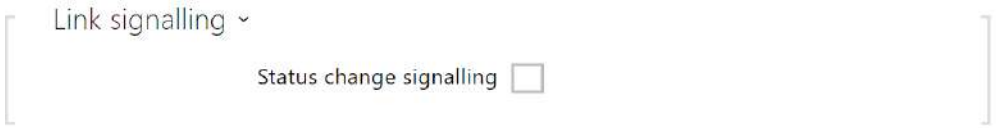
- **Hostname** – set the **2N LTE intercom** network identification.
- **Vendor Class Identifier** – set the vendor class identifier as a string of characters for DHCP Option 60.



WS-Discovery

WS-Discovery Enabled ☑

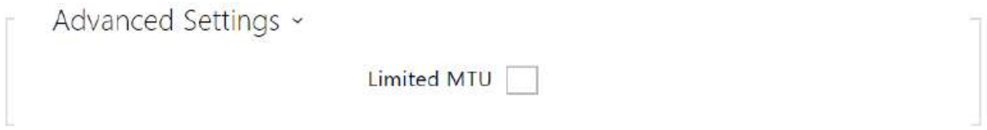
- **WS-Discovery Enabled** – enable the WS-Discovery function, which allows the other ONVIF clients to search a compatible device in the LAN. Enable this function to use a device as an ONVIF compatible one.



Link signalling

Status change signalling ☐

- **Link signalling** – Enable signalling of subsequent network connection state changes. If this signalling is disabled, only the first change until the connected state is signalled acoustically. Unselect this only if acoustic signalling were a problem.

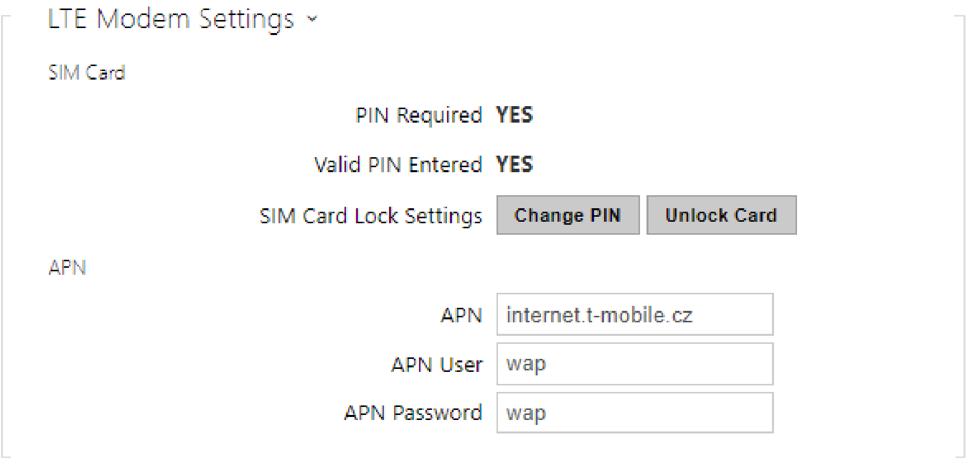


Advanced Settings

Limited MTU ☐

- **Limited MTU** – enable the shortened MTU (Maximum Transmission Unit) support to make the device work properly in the networks that only support shorter MTU.

LTE



PIN Required YES

Valid PIN Entered YES

SIM Card Lock Settings

APN internet.t-mobile.cz

APN User wap

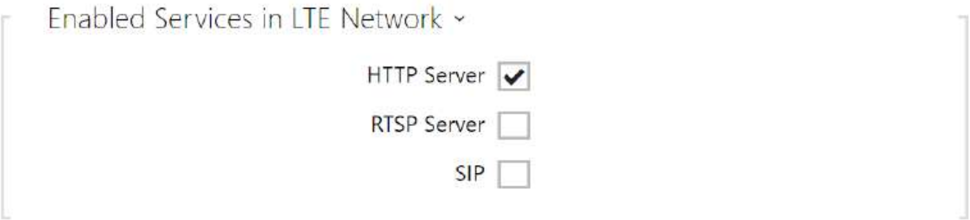
APN Password wap

- **SIM Card**
  - **PIN Required** – informs whether the SIM card PIN code security is requested.
  - **Valid PIN Entered** – informs of the set PIN code state. Once the SIM card is locked, the device web inteface is onle accessible using the 2N® LTE Verso debug module and this value is NO. Unlock the SIM card to recover common access to the device.
  - **SIM Card Lock Settings** – change the PIN code and set PIN request for the SIM card used.
    - **Change PIN** – enter the original and new PIN codes to change the PIN code. The PIN code can include 4–8 digits.
    - **Unlock / Lock Card** – enter the valid PIN to activate / deactivate the SIM card PIN request.

⚠ Caution

- If you enter an invalid code three times in succession, the SIM card will be locked. The unlock the SIM card, remove the SIM card from the device and insert it in a mobile phone to enter the PUK code. Having unlocked the SIM card, re-insert the SIM card in the device and log in.

- **APN**
  - **APN** – mobile provider's APN.
  - **APN User** – user name for APN verification if requested.
  - **APN Password** – password for APN verification if requested.



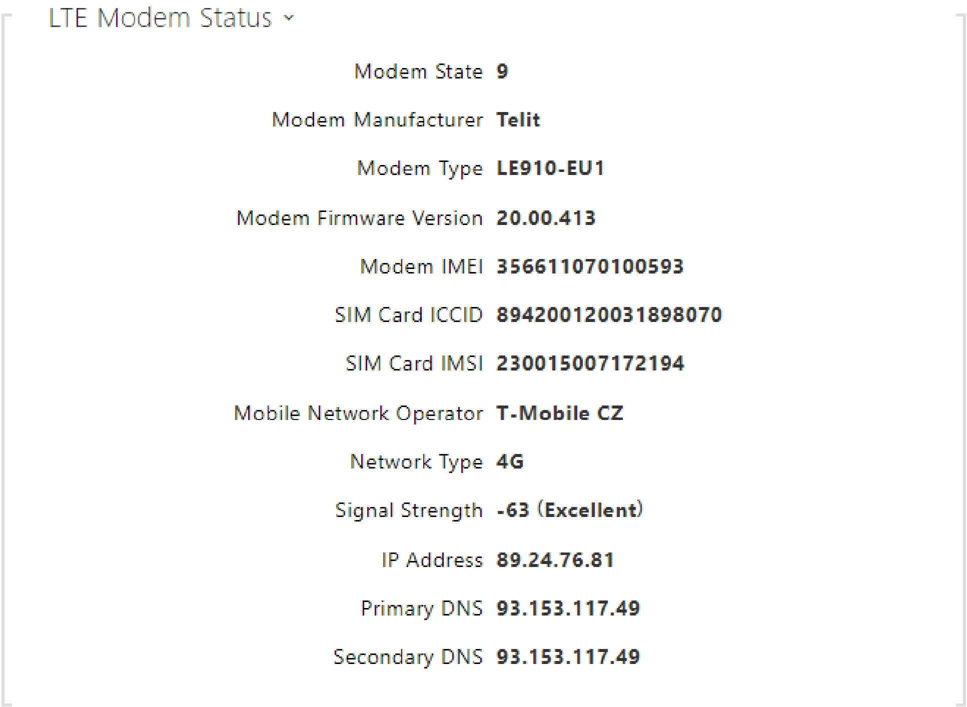
Enabled Services in LTE Network

HTTP Server ☑

RTSP Server ☐

SIP ☐

- **HTTP Server** – enable the web server availability in the public Internet.
- **RTSP Server** – enable the RTSP server availability in the public Internet.
- **SIP** – enable the SIP TCP server availability in the public Internet.



LTE Modem Status

Modem State	**9**
Modem Manufacturer	**Telit**
Modem Type	**LE910-EU1**
Modem Firmware Version	**20.00.413**
Modem IMEI	**356611070100593**
SIM Card ICCID	**894200120031898070**
SIM Card IMSI	**230015007172194**
Mobile Network Operator	**T-Mobile CZ**
Network Type	**4G**
Signal Strength	**-63 (Excellent)**
IP Address	**89.24.76.81**
Primary DNS	**93.153.117.49**
Secondary DNS	**93.153.117.49**

- **Modem State** – value 9 – connected to the data network.
- **Modem Manufacturer** – LTE modem manufacturer.
- **Modem Type** – LTE modem type.
- **Modem Firmware Version** – LTE modem firmware version.
- **Modem IMEI** – LTE modem IMEI.
- **SIM Card ICCID** – SIM card ICCID.
- **SIM Card IMSI** – SIM card IMSI.
- **Mobile Provider** – mobile provider's name.
- **Network Type** – network technology (value 4 – LTE/4G).
- **Signal Strength** – signal strength in dBm.

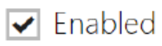
  - **Excellent** >= −80
  - **Good** >= −90
  - **Fair** >= −100
  - **Weak** < −100
- **IP Address** – IP address assigned by the provider's mobile network (typically non-public and unavailable from the public Internet).
- **Primary DNS** – primary DNS address for translation of domain names to IP addresses.
- **Secondary DNS** – secondary DNS address if the primary DNS is unavailable.

Caution

- **LTE® Verso** supports T-Mobile and AT&T for the US.

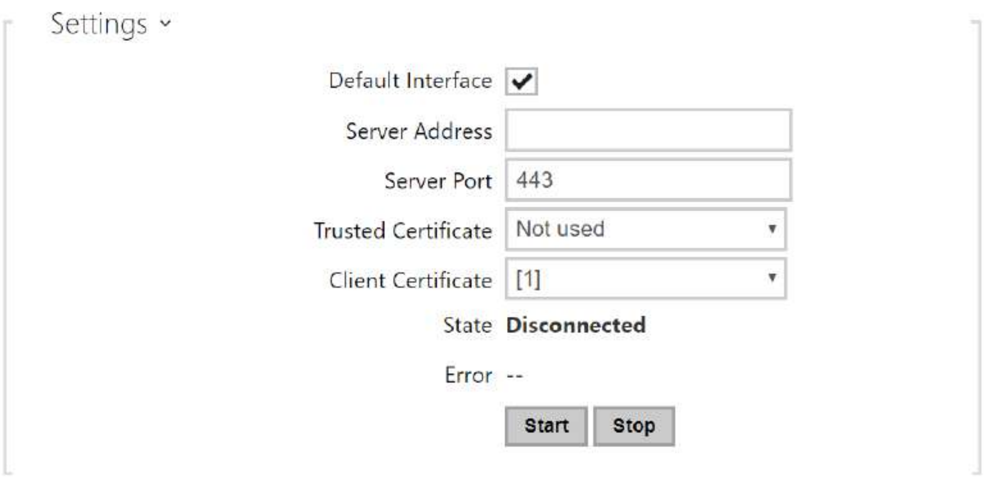
OpenVPN

Use OpenVPN to connect the device to another network.



☑ Enabled

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



Default Interface ☑

Server Address

Server Port 443

Trusted Certificate Not used

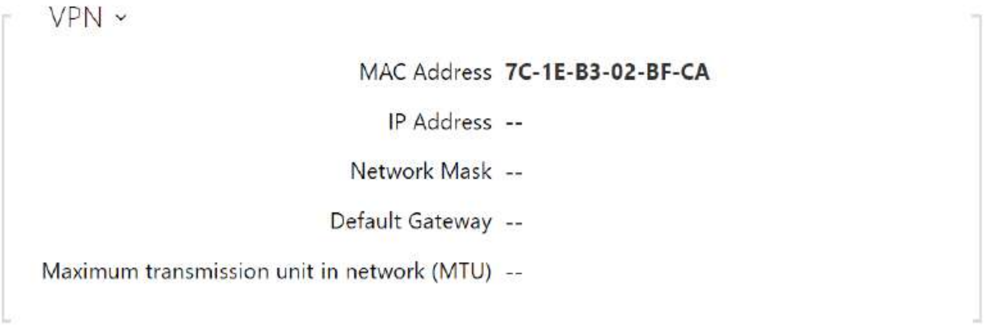
Client Certificate [1]

State **Disconnected**

Error --

- **Default Interface** – if enabled, it directs all outgoing network traffic to the VPN interface outside the LAN mask.
- **Server Address** – OpenVPN Server Address
- **Server Port** – OpenVPN Server Port.

- **Trusted Certificate** – specify a set of certificates issued by certification authorities to verify the OpenVPN server public certificate validity. Choose one of three certificate sets, see the Certificates subsection. If no certificate issued by a certification authority is specified, the OpenVPN server public certificate is not validated.
- **Client Certificate** – specify a set of client certificates to verify the client's identity by the OpenVPN server. Choose one of three certificate sets, see the Certificates subsection. If no client certificate is specified, the OpenVPN client identity is not validated.
- **State** – display the OpenVPN connection state: Connected/Disconnected.
- **Error** – display the OpenVPN connection error type if any.
- **Start** – connect the device to OpenVPN.
- **Stop** – disconnect the device from OpenVPN.



VPN

MAC Address **7C-1E-B3-02-BF-CA**

IP Address --

Network Mask --

Default Gateway --

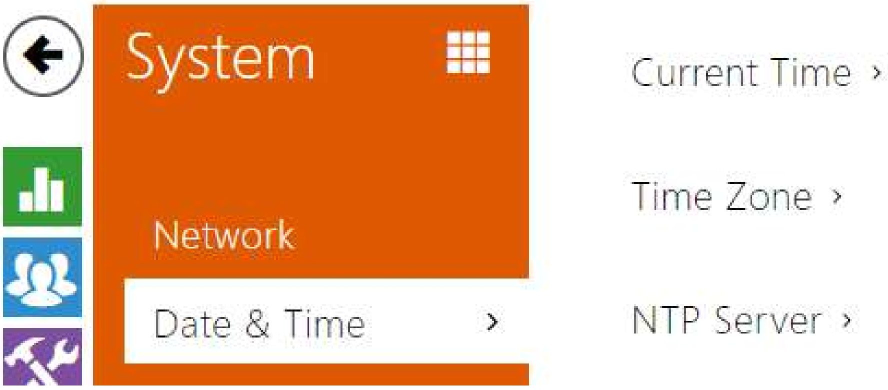
Maximum transmission unit in network (MTU) --

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

Tip

- Refer to the FAQ section for details on the OpenVPN server and client settings.

5.6.2 Date and Time



If you control validity of phone numbers, lock activation codes and similar by time profiles, make sure that the intercom internal date and time are set correctly.

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

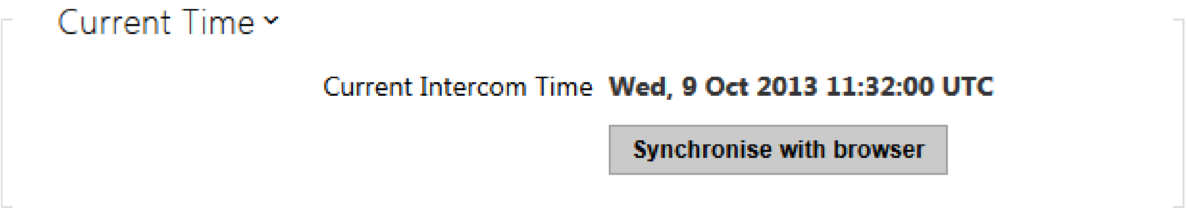
Synchronise the intercom internal time with any available SNTP server if your intercom is not equipped with a real-time clock.

Note

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

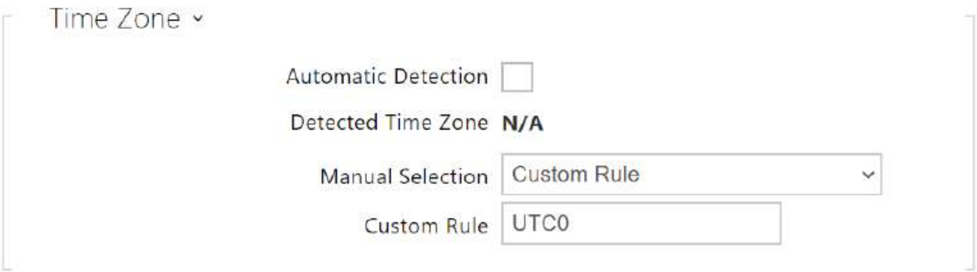
The device time error can be up to ±2 minutes per month under normal operation conditions. Therefore, we recommend you to synchronise time with the NTP server to achieve the highest accuracy and reliability. The intercom sends a query to the NTP server periodically to update its time value.

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

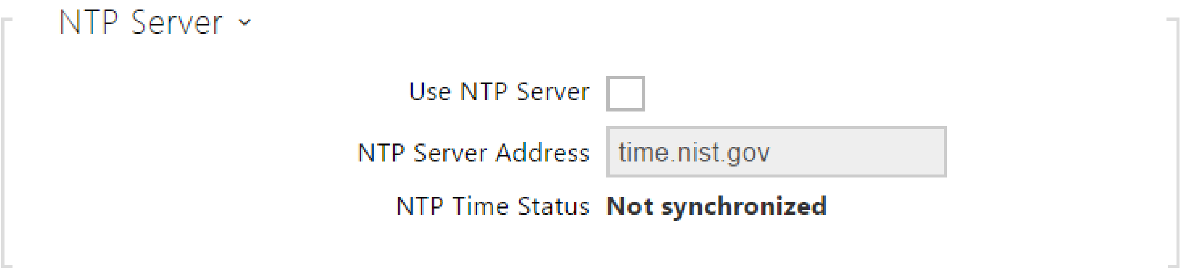
Automatic Detection ☐

Detected Time Zone **N/A**

Manual Selection Custom Rule

Custom Rule UTC0

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


NTP Server

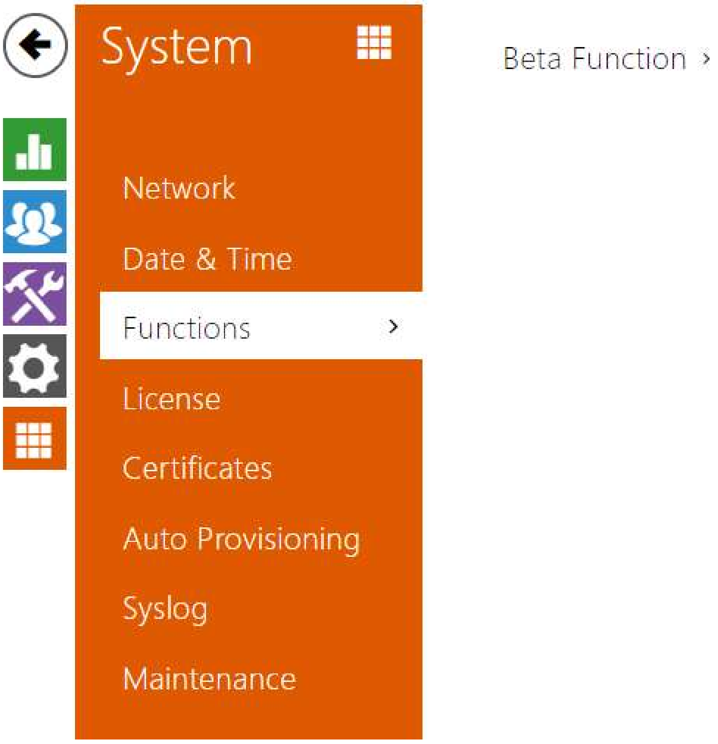
Use NTP Server ☐

NTP Server Address time.nist.gov

NTP Time Status **Not synchronized**

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

5.6.3 Functions



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

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

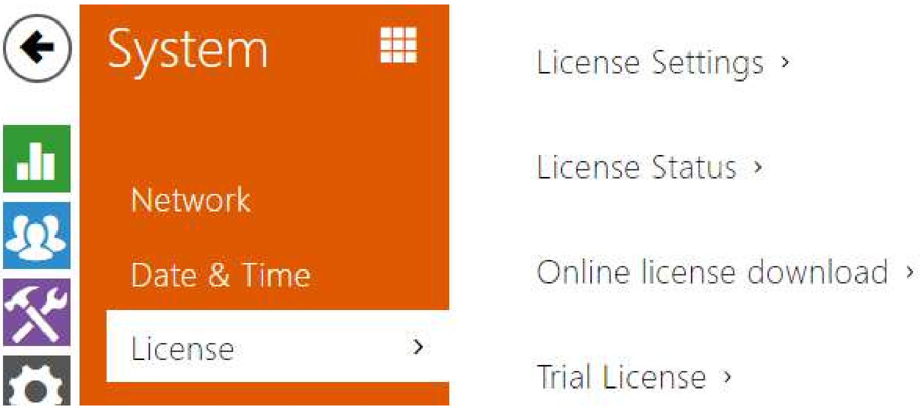
The function does not start/stop until the device is restarted. Hence, the status change request can be canceled by **Interrupt** until the restart.

Note

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

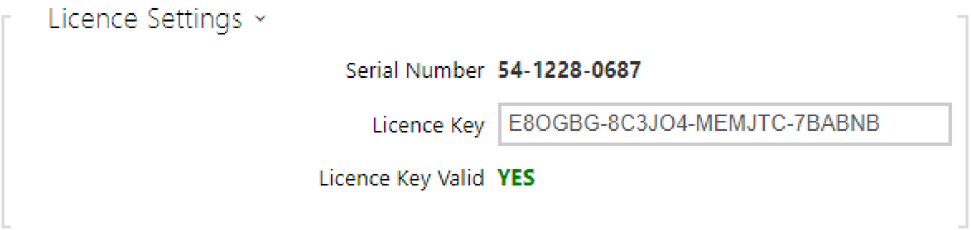
Beta Function Name	Description
Password-Protected Configuration File	This function helps you encrypt the configuration file with a password during backup (refer to 5.5.7 Údržba). To upload the configuration file to the device, you need to enter a security password. If the password fails to match, the configuration file will not be uploaded.
Multifactor Authentication of License Plates	Once this function is activated, the Multifactor selection appears in Services > Access Control > Arrival Rules > Advanced Settings > License Plate Recognition. Access is only granted when at least two authentication methods are verified as set in the access rules. Once the license plate is recognized, remember to enter another authentication method within 60 seconds.
Noise Cancelling	The function cancels ambient noise in the microphone when voice is detected.

5.6.4 License

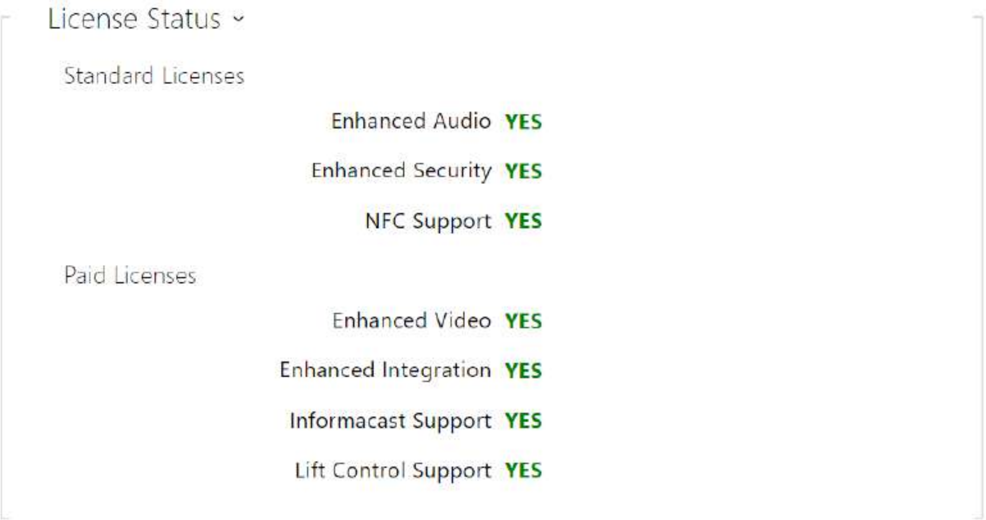


Some **2N LTE intercom** functions are available with a valid licence key only. Refer to the **Model Differences and Function Licensing** subsection for the list of intercom licensing options.

List of Parameters


Licence Settings
Serial Number 54-1228-0687
Licence Key E8OGBG-8C3JO4-MEMJTC-7BABNB
Licence Key Valid YES

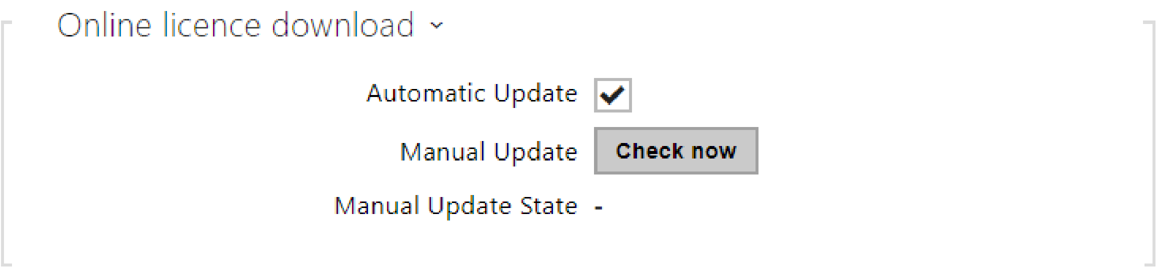
- **Serial Number** – display the serial number of the device for which the licence is valid.
- **Licence Key** – enter the valid licence key.
- **Licence Key Valid** – check whether the used licence key is valid.


License Status
Standard Licenses
Enhanced Audio YES
Enhanced Security YES
NFC Support YES
Paid Licenses
Enhanced Video YES
Enhanced Integration YES
Informacast Support YES
Lift Control Support YES

- **Standard Licenses** – display the list of factory default licenses.
  - **Enhanced Audio** – check whether the functions activated by the Enhanced Audio license are available.
  - **Enhanced Security** – check whether the functions activated by the Enhanced Security license are available.
  - **NFC support**– check whether the NFC user identification support is available.
- **Paid Licenses** – display the list of licenses available with a valid license key only.
  - **Enhanced Video** – check whether the functions activated by the Enhanced Video license are available.
  - **Enhanced Integration** – check whether the functions activated by the Enhanced Integration license are available.
  - **InformaCast support** – check whether the InformaCast support is available.
  - **Lift Control Support** – check whether the functions activated by the Lift Module license are available.

Tip

- Function Licensing

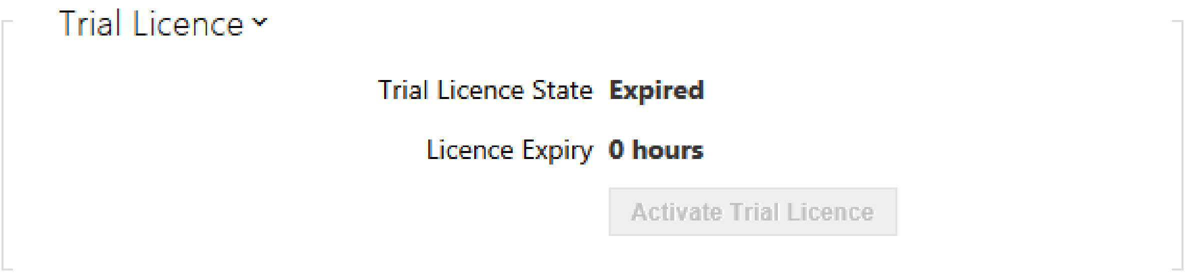


Automatic Update ☑

Manual Update

Manual Update State -

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



Trial Licence State **Expired**

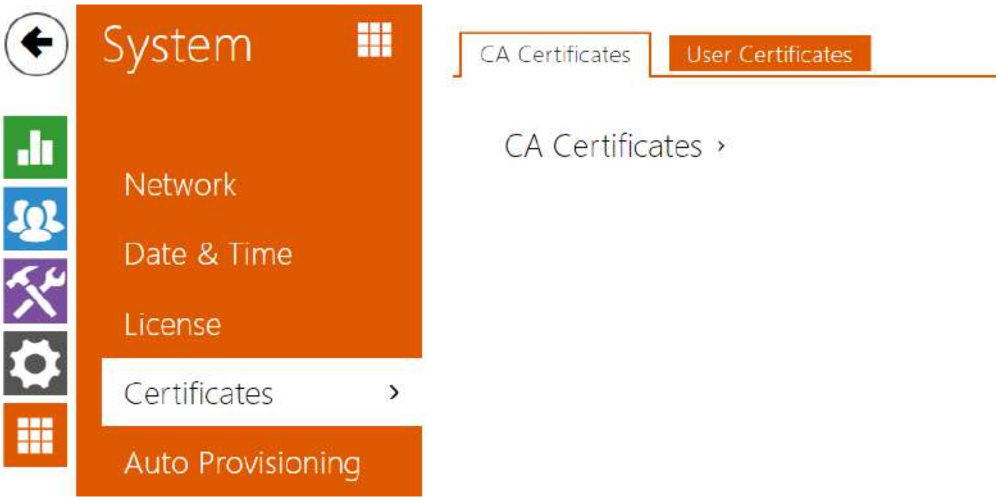
Licence Expiry **0 hours**

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

⚠ **Caution**

- The SW reset does not delete the license key and result in the device restart. If disabled before the SW reset, the automatic license update is enabled automatically and a query is sent to the license server. If the automatic license update is enabled, the query to the license server is sent as planned.
- The HW reset deletes the license key and the subsequent device restart in a randomly short time generates a query to the license server.
    - Request interval – randomly 1-100 minutes after the start and then in 8 hours in trial license devices or in 8 hours for 7 days after the restart in time-unlimited license devices.

5.6.5 Certificates



Some **2N LTE intercom** 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

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

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

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

Caution

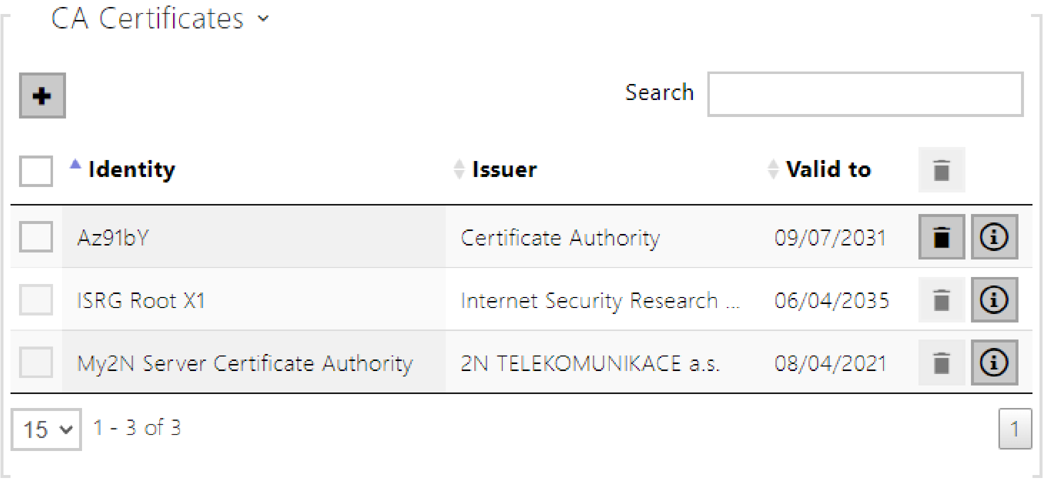
- The CA certificates must use the X.509 v3 format.

Upon the first power up, the 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

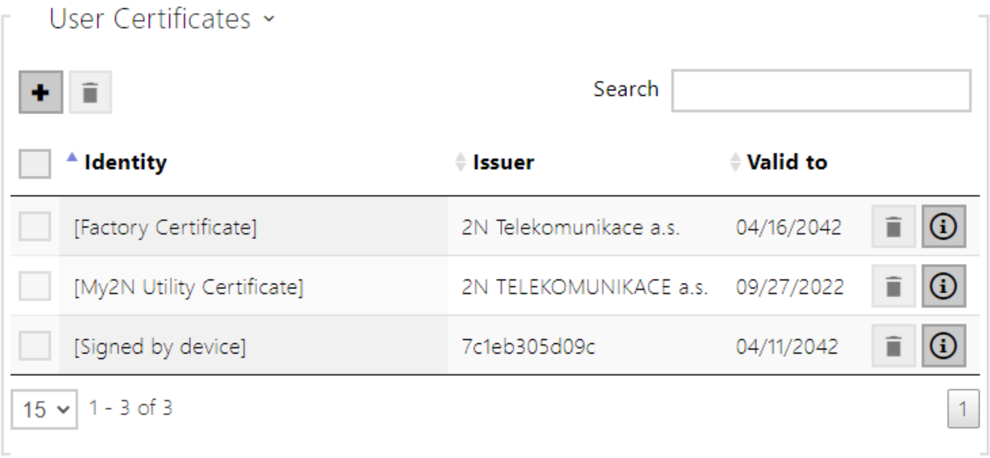
- *If you use the Self Signed certificate for encryption of the intercom web server – browser communication, the communication is secure, but the browser will warn you that it is unable to verify the intercom certificate validity.*

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



CA Certificates

☐	Identity	Issuer	Valid to
☐	Az91bY	Certificate Authority	09/07/2031
☐	ISRG Root X1	Internet Security Research ...	06/04/2035
☐	My2N Server Certificate Authority	2N TELEKOMUNIKACE a.s.	08/04/2021



User Certificates

☐	Identity	Issuer	Valid to
☐	[Factory Certificate]	2N Telekomunikace a.s.	04/16/2042
☐	[My2N Utility Certificate]	2N TELEKOMUNIKACE a.s.	09/27/2022
☐	[Signed by device]	7c1eb305d09c	04/11/2042

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

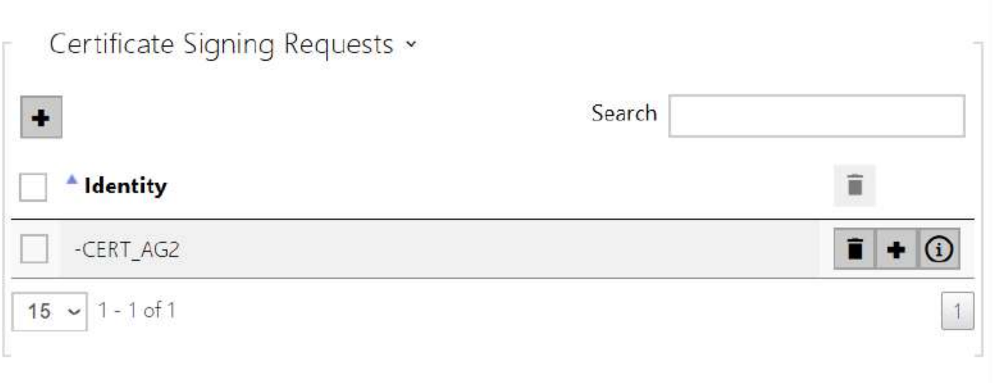
⚠ **Caution**

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

⚠ **Caution**

- It is possible that certificate with private RSA key longer than 2048 bits will be rejected and following message will be displayed: **Private key file or private key password was not accepted by device !**
- For certificates based on elliptic curves use the secp256r1 (aka prime256v1 aka NIST P-256) and secp384r1 (aka NIST P-384) curves only.

CSR (Certificate Signing Request)



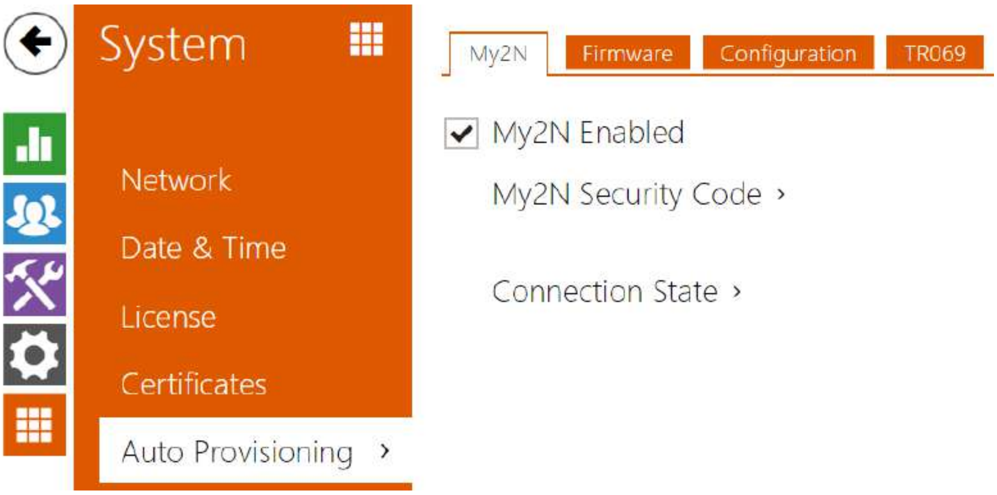
You can create a CSR (Certificate Signing Request) of your own in the web configuration interface to be submitted to the certification authority (CA) for signing. This process ensures that the certificate is properly paired with the private key generated when the CSR was created and is only stored in your device.

1. Click ➕ to create a new Certificate Signing Request.
2. A dialog box opens for you to fill in the following:
    - **Common Name (CN)** – enter the IP address/domain name under which the **2N IP Intercom** web interface is accessible.
    - **SAN: mDNS** – enable adding **mDNS (Multicast DNS)** as a Subject Alternative Name (SAN) to the certificate. It is used for the domain name based access in the LAN.
    - **SAN: IP** – enable adding an **IP address** as a Subject Alternative Name (SAN) to the certificate. It is used for the IP address based access.
    - **Public Key Algorithm** – define the type of the algorithm used for public key generation in the certificate.
    - **CSR ID** – unique Certificate Signing Request identifier.
    - **Country (C)** – two-letter code of the country in which the organization is registered (according to ISO 3166-1 alpha-2).
    - **State/Country/Region (S)** – state/region in which the organization is registered (unabridged).
    - **City/Locality (L)** – name of the city/locality in which the organization is registered (unabridged).
    - **Organization (O)** – legal name of the organization including all prefixes (Inc., Corp., Ltd.).
    - **Organizational Unit (OU)** – name of the department/unit within the organization.
    - **E-mail** – e-mail address of the contact person or certificate administrator.
3. Click **Generate** to create a Certificate Signing Request. Download and store safely the created CSR file.

4. Submit the created CSR file to the certification authority (CA), which issues a digital certificate on its basis.
5. Upload the issued digital certificate back to the CSR file in the web interface. Click + in the given certificate request row for upload.

Press 🗑 to remove the CSR. Press ⓘ to display the CSR parameters.

5.5.6 Auto Provisioning



☑ My2N Enabled

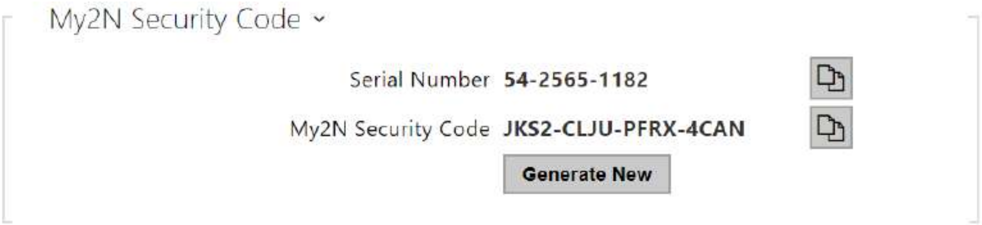
The **2N LTE intercoms** help you update firmware and configuration manually, or automatically from a storage on a TFTP/HTTP server selected by you according to predefined rules.

You can configure the TFTP and HTTP server address manually. The **2N LTE intercoms** support automatic identification of the local DHCP server address (Option 66).

> ⚠ **Caution**
>
> - The login password is saved in the configuration file. If the password is 2n (default), the valid configuration part is only uploaded. This means that the configuration is uploaded, but the password remains the same, not assuming the value included in the file.

My2N

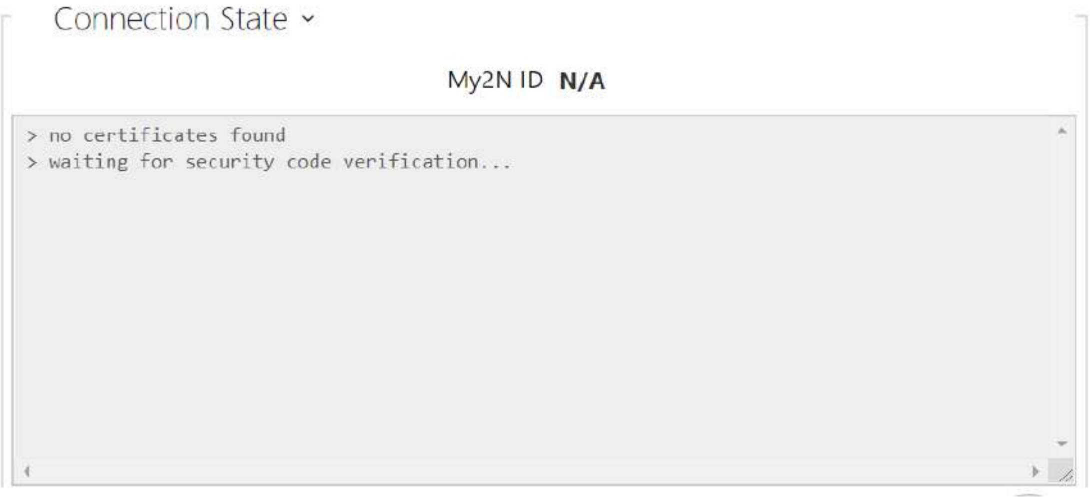
☑ My2N Enabled



Serial Number 54-2565-1182

My2N Security Code JKS2-CLJU-PFRX-4CAN

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



My2N ID N/A

```
> no certificates found
> waiting for security code verification...
```

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

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

Firmware

Use the **Firmware** tab to set automatic firmware download from a server defined by you. The 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 LTE intercom expects the following files:

1. hip**MODEL**-firmware.bin – intercom firmware
2. hip**MODEL**-common.xml – common configuration for all intercoms of one model

3. hip**MODEL**-**MACADDR**.xml – specific configuration for one intercom

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:

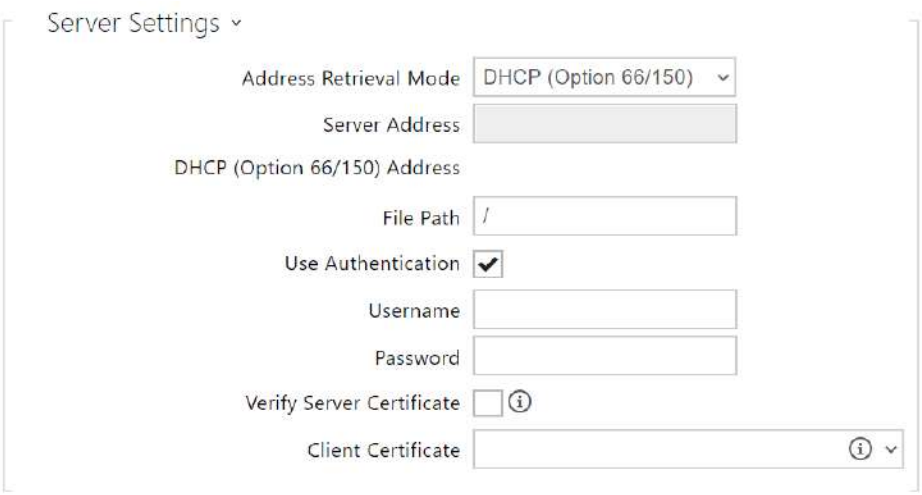
2N® LTE Verso with MAC address 00-87-12-AA-00-11 downloads the following files from the TFTP server:

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

List of Parameters

☑ Firmware Update Enabled

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



Server Settings

Address Retrieval Mode: DHCP (Option 66/150)

Server Address:

DHCP (Option 66/150) Address

File Path: /

Use Authentication: ☑

Username:

Password:

Verify Server Certificate: ☐

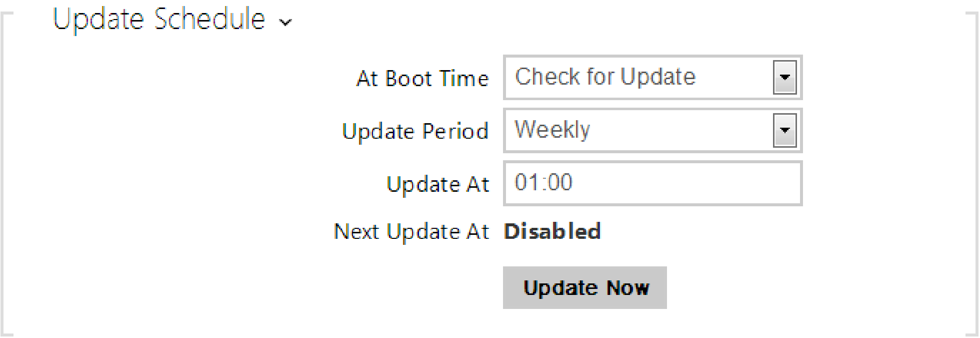
Client Certificate:

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

- **Use authentication** – enable authentication for HTTP server access.
- **Username** – enter the user name for server authentication.
- **Password** – enter the password for server authentication.
- **Verify Server Certificate** – set the set of CA certificates for validation of the ACS public certificate.
- **Client Certificate** – specify the client certificate and private key to validate the intercom right to communicate with the ACS.

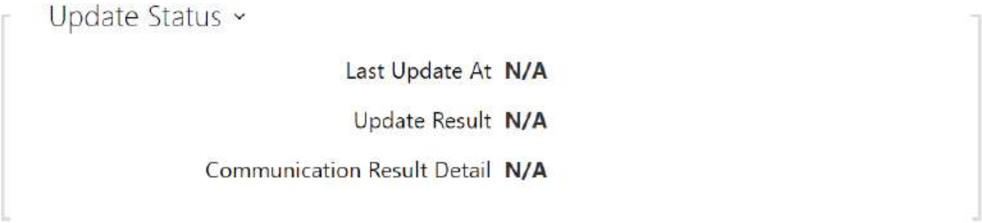
Info

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



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

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



Last Update At: **N/A**
Update Result: **N/A**
Communication Result Detail: **N/A**

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

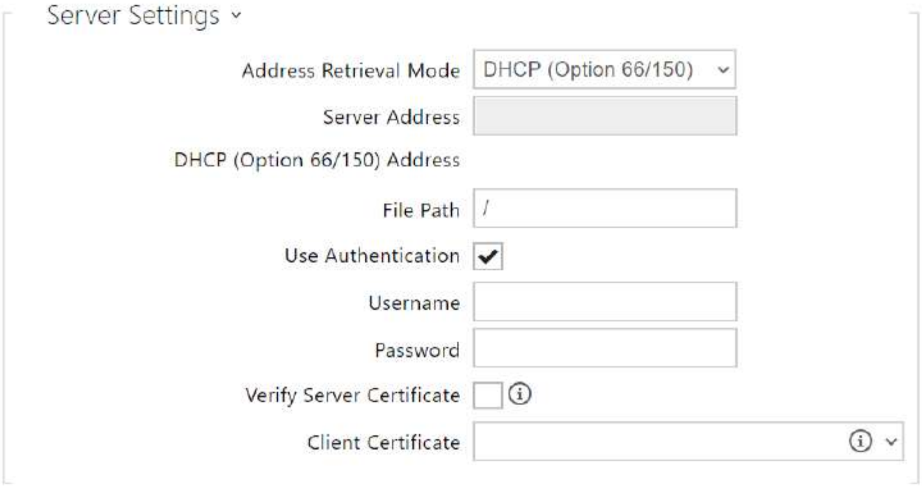
Result	Description
Invalid server address	The server address is invalid.
Unsupported protocol	The protocol is not supported. HTTP(s) and TFTP are supported only.
Invalid file path	The provisioning file location is invalid.
DHCP option 66 failed	The server address loading via DHCP Option 66 or 150 has failed.
Invalid domain name	The server domain name is invalid due to wrong configuration or unavailability of the DNS server.
Server not found	The requested HTTP/TFTP server fails to reply.
Authentication failed	The HTTP credentials are invalid.
File not found	The file has not been found on the server.
Request waiting in queue...	The provisioning request is queuing...
In progress...	Update is in progress.
File is invalid	The file to be downloaded is corrupted or of a wrong type.
Firmware is up to date	The firmware update attempt reveals that the latest firmware version has been loaded.
Update Succeeded	The configuration/firmware update has been successful. With firmware update, the device will be restarted in a few seconds.
Internal error	An unspecified error occurred during file download.

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.

☑ Automatic Configuration Update

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



Server Settings

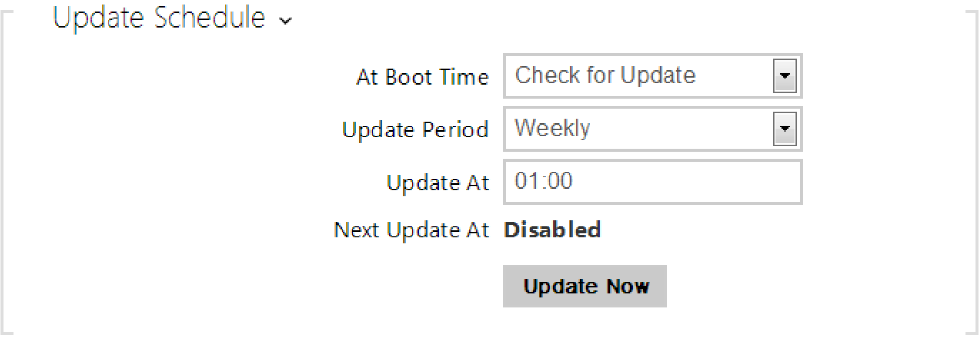
Address Retrieval Mode: DHCP (Option 66/150)
Server Address
DHCP (Option 66/150) Address
File Path: /
Use Authentication ☑
Username
Password
Verify Server Certificate ☐
Client Certificate

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

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

Info

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



Update Schedule

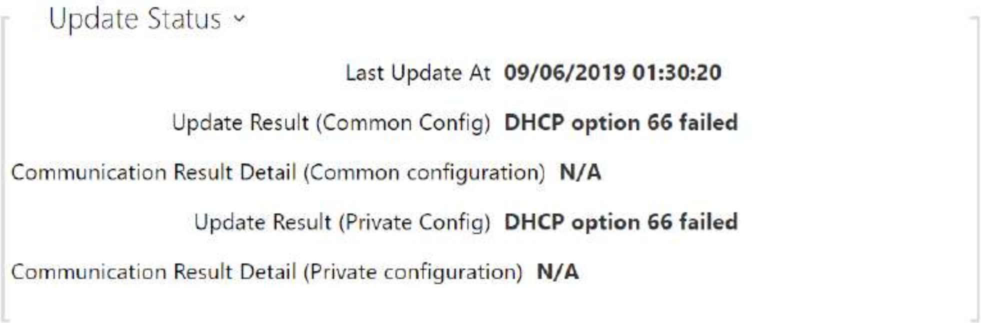
At Boot Time: Check for Update

Update Period: Weekly

Update At: 01:00

Next Update At: **Disabled**

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



Update Status

Last Update At: **09/06/2019 01:30:20**

Update Result (Common Config): **DHCP option 66 failed**

Communication Result Detail (Common configuration): **N/A**

Update Result (Private Config): **DHCP option 66 failed**

Communication Result Detail (Private configuration): **N/A**

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

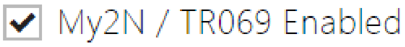
- **Update Result (Common Config)** – last update result. The following options are available: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Communication Result Detail(Common Config)** – server communication error code or TFTP/HTTP status code.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

My2N / TR069

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

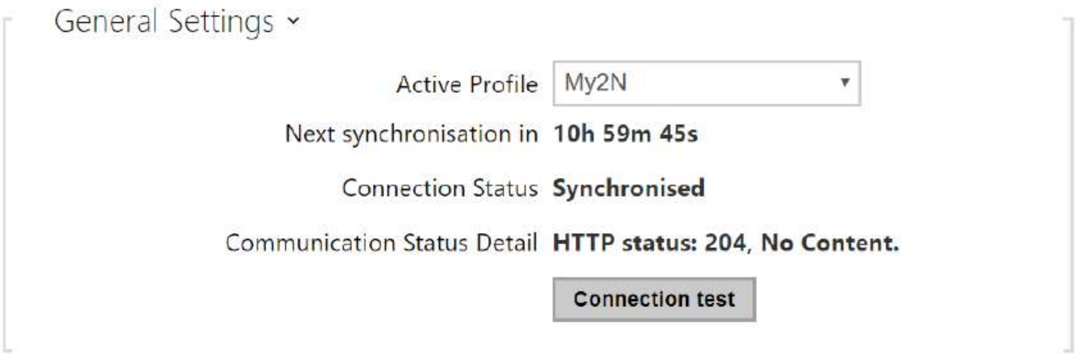
The TR-069 protocol is utilised by the My2N cloud service. Make sure that TR-069 is enabled and Active profile set to My2N to make your intercom log in to My2N periodically for configuration.

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



☑ My2N / TR069 Enabled

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



General Settings

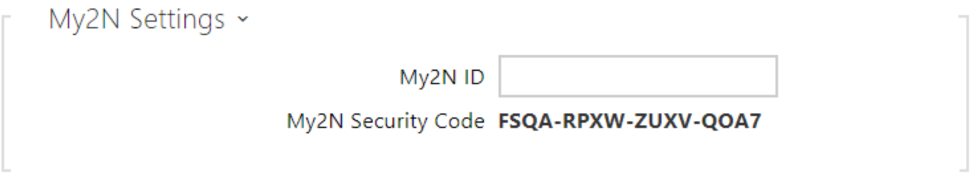
Active Profile: My2N

Next synchronisation in: 10h 59m 45s

Connection Status: Synchronised

Communication Status Detail: HTTP status: 204, No Content.

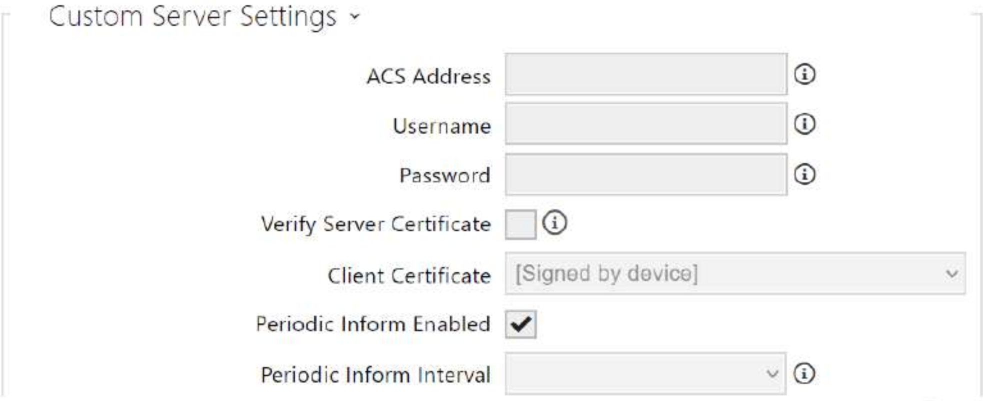
- **Active profile** – select one of the pre-defined profiles (ACS), or choose a setting of your own and configure the ACS connection manually.
- **Next synchronisation in** – display the time period in which the intercom shall contact a remote ACS.
- **Connection status** – display the current ACS connection state or error state description if necessary.
- **Communication Status Detail** – server communication error code or HTTP status code.
- **Connection test** – test the TR069 connection according to the set profile, see the Active profile. The test result is displayed in the Connection status.



My2N ID

My2N Security Code **FSQA-RPXW-ZUXV-QOA7**

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



ACS Address

Username

Password

Verify Server Certificate ☐

Client Certificate [Signed by device]

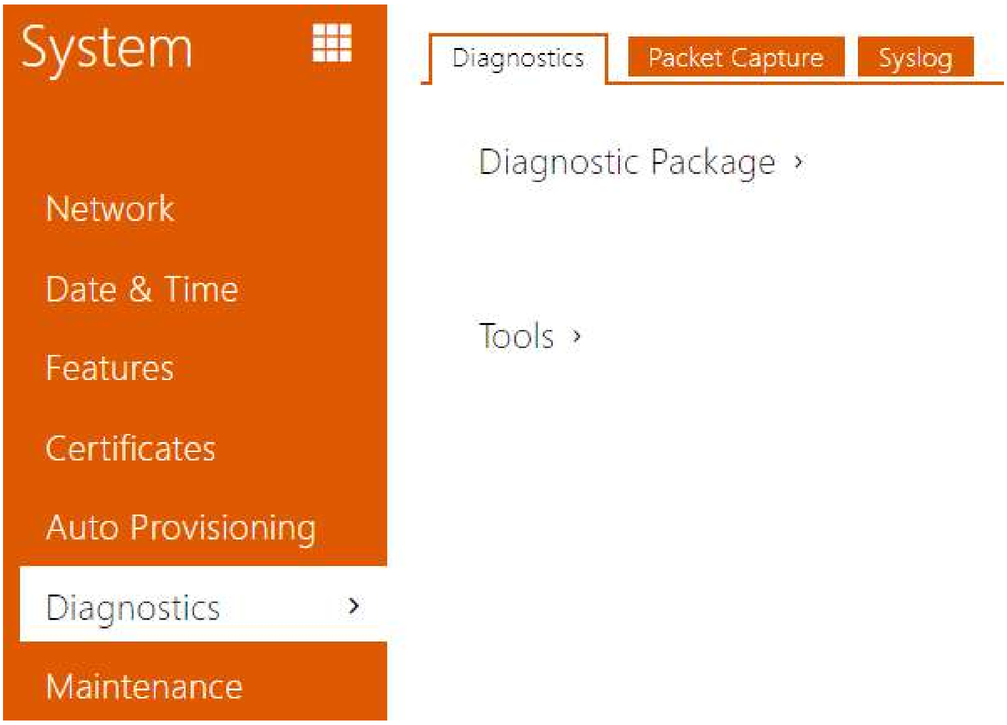
Periodic Inform Enabled ☑

Periodic Inform Interval

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

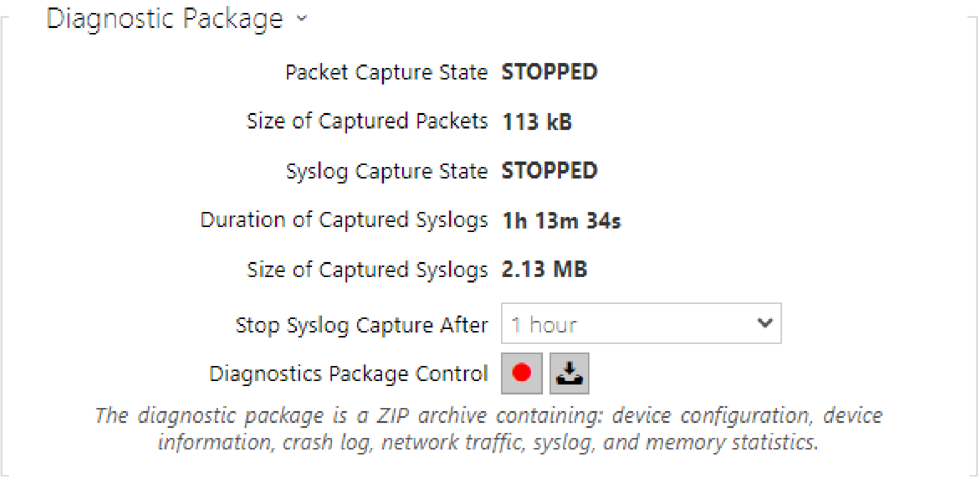
- **Client Certificate** – specify the user certificate and private key to validate the intercom right to communicate with the ACS. Choose one of three sets, refer to the Certificates subsection.
- **Periodic inform enabled** – enable periodical logging of the intercom to the ACS.
- **Periodic inform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

5.6.7 Diagnostics



Diagnostics

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



Packet Capture State	STOPPED
Size of Captured Packets	113 kB
Syslog Capture State	STOPPED
Duration of Captured Syslogs	1h 13m 34s
Size of Captured Syslogs	2.13 MB
Stop Syslog Capture After	1 hour
Diagnostics Package Control	●

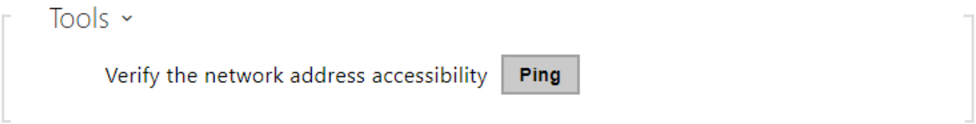
The diagnostic package is a ZIP archive containing: device configuration, device information, crash log, network traffic, syslog, and memory statistics.

- **Packet Capture State** – shows whether packet capture has been started/stopped in the Packet capture folder.

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

Press ● to start capturing. Repress the button to restart and rerun capturing. Press 📥 to download the packet capture file. Hash export for secure output adds the hash format from the syslog to the values in the configuration file. The hash format is added as **DiscreteHash.**

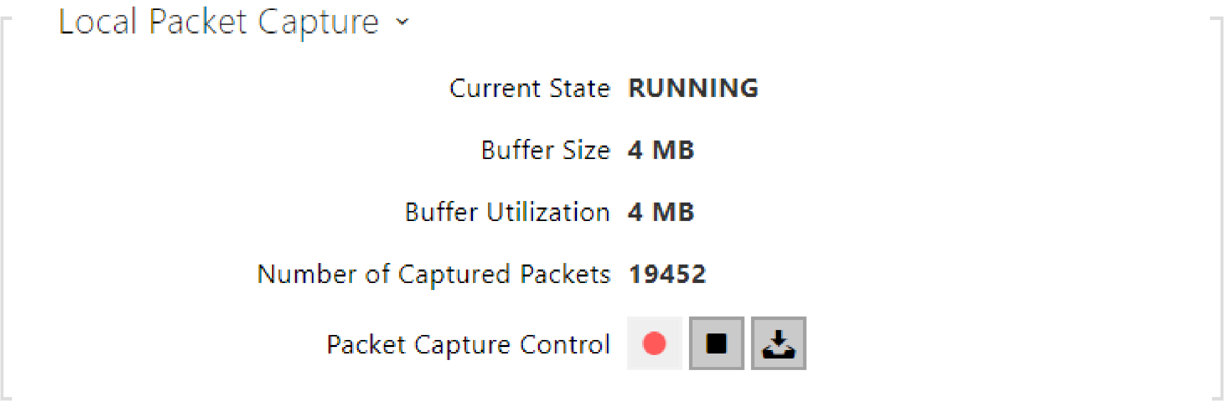
> ⚠ **Caution**
>
> - Starting diagnostic data capture restarts packet capture if running.
> - Encrypt the file with a password for additional security. This password will be needed when restoring the configuration to decrypt the file and access its contents. Make sure you do not lose your password and store it in a safe place.



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

Packet Capture

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



Local Packet Capture

Current State RUNNING

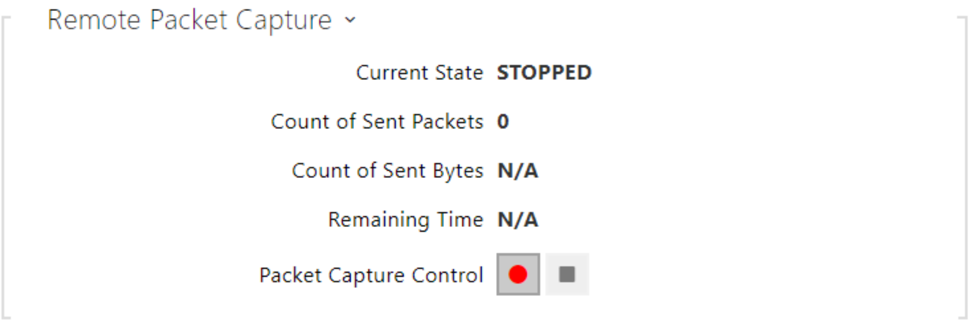
Buffer Size 4 MB

Buffer Utilization 4 MB

Number of Captured Packets 19452

Packet Capture Control ● ■ ⤓

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



Remote Packet Capture

Current State STOPPED

Count of Sent Packets 0

Count of Sent Bytes N/A

Remaining Time N/A

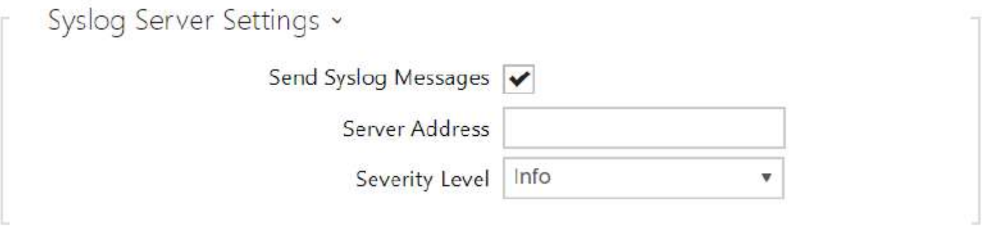
Packet Capture Control ● ■

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

Syslog

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

Such sensitive data as access codes, card identifiers, login data, etc. are stored in the encrypted format (hash) in the syslog. The assignment of the hash values to real values can be performed according to the configuration file.

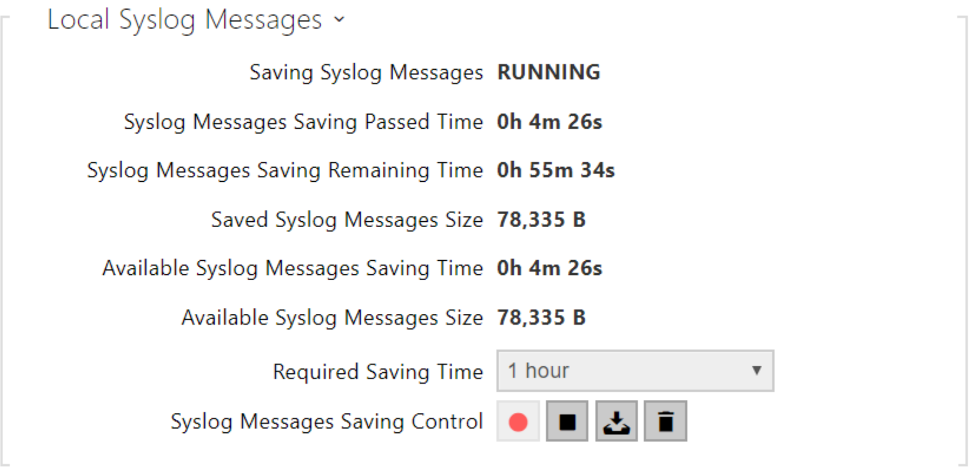


Send Syslog Messages ☑

Server Address

Severity Level Info

- **Send Syslog Messages** – enable sending of syslog messages to the Syslog server. Make sure that the server address is valid.
- **Server Address** – set the IP[:port] or MAC address of the server running the application to capture syslog messages.
- **Severity Level** – set the severity level of the messages to be sent. Debug 1–3 level setting is only recommended to facilitate troubleshooting for the Technical Support department.



Saving Syslog Messages **RUNNING**

Syslog Messages Saving Passed Time **0h 4m 26s**

Syslog Messages Saving Remaining Time **0h 55m 34s**

Saved Syslog Messages Size **78,335 B**

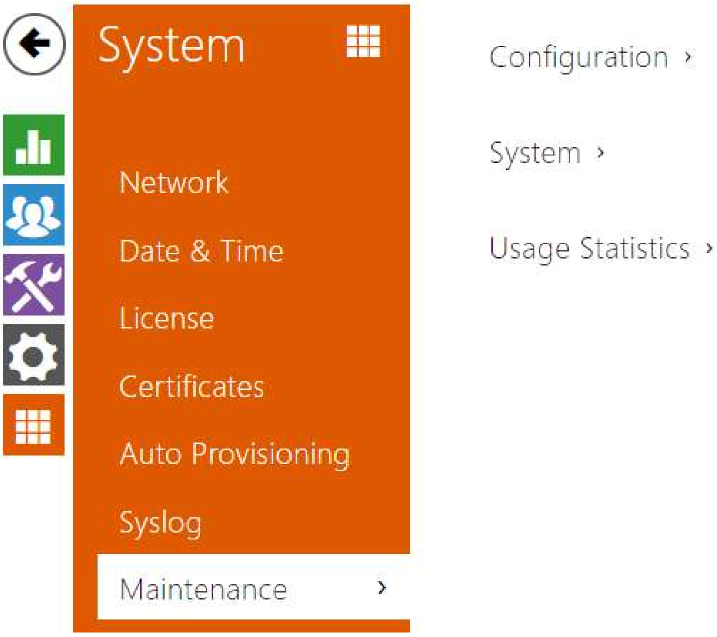
Available Syslog Messages Saving Time **0h 4m 26s**

Available Syslog Messages Size **78,335 B**

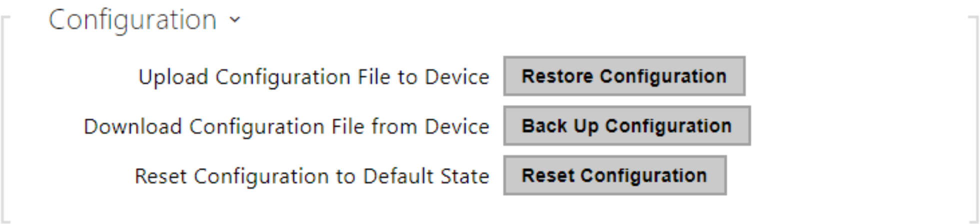
Required Saving Time 1 hour

General overview of local syslog messages.

5.6.8 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.


Configuration ˅
Upload Configuration File to Device
Restore Configuration
Download Configuration File from Device
Back Up Configuration
Reset Configuration to Default State
Reset Configuration

- **Restore configuration** – reset configuration from the preceding backup. Press the button to display a dialogue window for you to select and upload the configuration file to the intercom. Before uploading, choose whether to apply general settings from the configuration file, import a directory, import network settings and certificates or SIP PBX connection setttings.

  Caution

  - The login password is saved in the configuration file. If the password is not encoded or default (*2n* encoded), the valid configuration part is only uploaded. This means that the configuration is uploaded, but the password remains the same, not assuming the value included in the file.

- **Backup configuration** – back up the complete current configuration of your intercom. Press the button to download the configuration file to your PC.

Caution

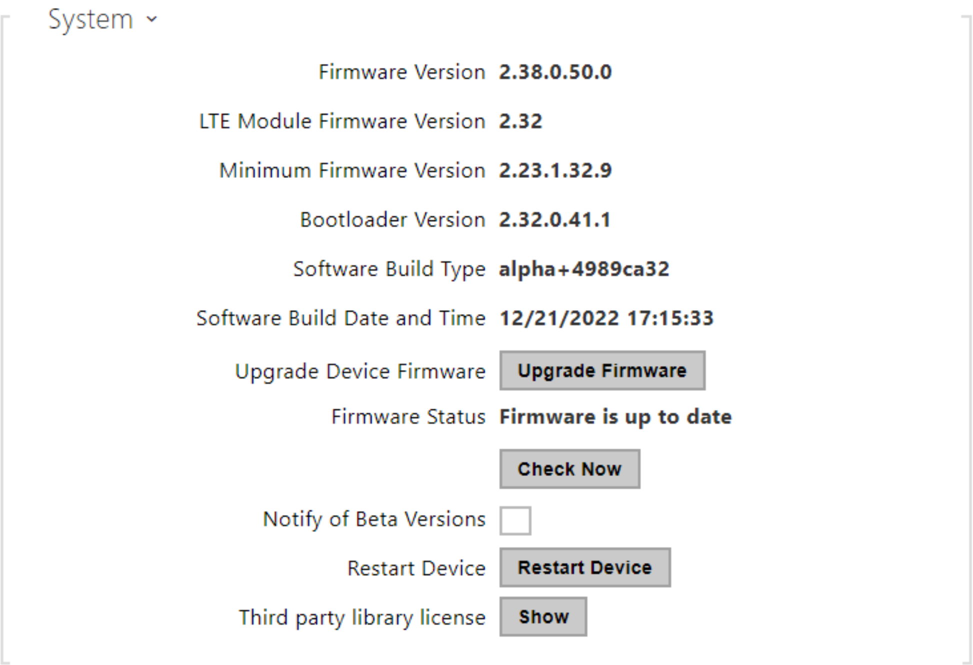
- *Treat the file cautiously as the intercom configuration may include delicate information such as user phone numbers and access codes.*

- **Reset configuration** – reset all the device parameters to the default values. Resetting the network parameters and certificates requires additional confirmation in the confirmation dialog box.
  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.*
- *The license key is not deleted at HW reset (i.e. reset via a device button) if the Automatic update is enabled (System/License), which updates the license key from the 2N License server..*

- **Allow Network Setting at Startup** – 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.



Firmware Version 2.38.0.50.0
LTE Module Firmware Version 2.32
Minimum Firmware Version 2.23.1.32.9
Bootloader Version 2.32.0.41.1
Software Build Type alpha+4989ca32
Software Build Date and Time 12/21/2022 17:15:33
Firmware Status Firmware is up to date
Notify of Beta Versions ☐

Note

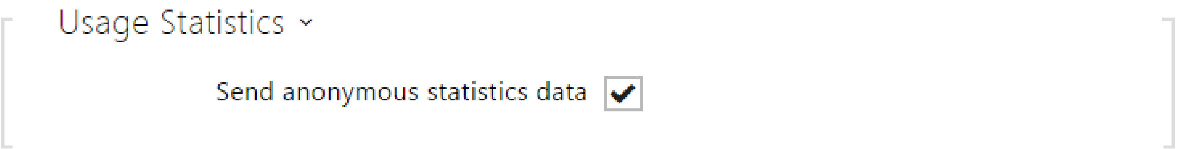
- The device function, reliability and security depend on the firmware version installed. A regular firmware upgrade is one of the product use conditions. Errors arisen from the use of an outdated firmware version shall not be subject to complaints. The up-to-date firmware version implements client experience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

- **Upgrade firmware** – upgrade your 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 2N.com. for the latest FW version for your intercom. FW upgrade does not affect configuration as the intercom checks the FW file to prevent upload of a wrong or corrupted file.
- **Check Now** – check online whether a new firmware version is available. If so, download the new FW version and an automatic device upgrade will follow.
- **Restart Device** – restart the intercom. The process takes about 30 s. When the intercom has obtained the IP address upon restart, the login window will get displayed automatically.

Caution

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

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



Send anonymous statistics data ☑

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

5.7 Used Ports

Service	Port	Protocol	Direction	Configurable	Configuration
802.1x	–	–	In/Out	No	–
DHCP	68	UDP	In/Out	No	–
DNS	53	TCP/UDP	In/Out	No	–
Echo (device discovery)*	8002	UDP	In/Out	No	–
FTP	21	TCP	Out	No	–
2N® IP Eye	8003	UDP	Out	No	–
HTTP	80	TCP	In/Out	Yes	Web server
HTTPS	443	TCP	In/Out	Yes	Web server
Multicast audio	22222	UDP	In/Out	Yes	Streaming
Multicast audio for **2N® Mobile video**	8006	UDP	Out	No	
Multicast video for **2N® Mobile video**	8008	UDP	Out	No	
NTP klient	123	UDP	In/Out	No	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	No	–
RTP ports	4900+	UDP	In/Out	Yes	Phone
RTSP server	554	UDP	In/Out	No	–
SingleWire Commands	80	TCP	In/Out	No	–
SingleWire Communication	8081	TCP	Out	No	–

Service	Port	Protocol	Direction	Configurable	Configuration
SingleWire Discovery	427	UDP	In/Out	No	–
SingleWire Media	20000+	UDP	In	No	–
SIP	5060, 5062	TCP/UDP	In/Out	Yes	Phone
SIPS	5061	TCP	In/Out	Yes	Phone
SMTP	25	TCP	Out	Yes	E-Mail
Syslog	514	UDP	Out	No	–
TFTP	69	UDP	Out	No	–

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

6. Supplementary Information

Here is what you can find in this section:

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

6.1 Troubleshooting

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

6.2 Directives, Laws and Regulations

2N® IP Intercom conforms to the following directives and regulations:

- 2014/35/EU for electrical equipment designed for use within certain voltage limits
- 2014/30/EU for electromagnetic compatibility
- 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment
- 2012/19/EU on waste electrical and electronic equipment

Industry Canada

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

FCC

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

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

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

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

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

Caution

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

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 environmentalfriendly 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.