MyBell

2-Wire 1-button Kit

EN - Instructions and warnings for installation and use

Nice

v0.2

Part One

MyBell 2-Wire 1-button Station

Part Two

MyBell 2-Wire Indoor Monitor

Part One

MyBell 2-Wire 1-button Station

1 IMPORTANT SAFEGUARDS AND WARNINGS

- ⚠ **CAUTION! – Any use other than that specified herein or in environmental conditions other than those stated in this manual is to be considered improper and is strictly forbidden!**
- ⚠ **CAUTION! – Important instructions: keep this manual in a safe place to enable future product maintenance and disposal procedures.**
- ⚠ **CAUTION! – All installation and connection operations must be performed exclusively by suitably qualified and skilled personnel with the unit disconnected from the mains power supply.**
- ⚠ **CAUTION! – This manual contains important instructions and warnings for personal safety. Read carefully all parts of this manual. If in doubt, suspend installation immediately and contact Nice Technical Assistance.**

- The product packaging materials must be disposed of in full compliance with local regulations.
- Never apply modifications to any part of the device. Operations other than those specified can cause malfunctions. The manufacturer declines all liability for damage caused by makeshift modifications to the product.
- Never place the device near the sources of heat or expose to naked flames. These actions can damage the product and cause malfuntions.
- This product isn't intended for use by people (including children) with reduced physical, sensory or mental capabilities or who lack experience and knowledge, unless they are supervised by a person responsible for their safety.
- This product isn't a toy. Keep away from children and animals!
- The device is designed to operate in an electrical home installation. Faulty connection or use can result in a fire or electric shock.
- Even when the device is turned off, voltage can be present at its terminals. Any maintenance introducing changes to the configuration of connections or the load must be always performed with a disabled fuse.
- Don't use in damp or wet locations, near a bathtub, sink, shower, swimming pool, or anywhere else where water or moisture are present.

2 DEVICE DESCRIPTION

The device is an SIP-compliant dooor phone. It can be connected with an indoor monitor for remote access, control and monitoring. The device enables audio and video communication with visitors as well as door unlocking feature. For security purpose, it also enables entrance door or gate monitoring.

Table A1 - MyBell 2-Wire 1-button Station - Device description

Feature	Description
Operation System	Linux
Body Material	plastic
Camera	2M pixels, automatic lighting
Wi-Fi	no
Ethernet	1xRJ45, 10/100 Mbps, adaptive
Power over Ethernet (PoE)	802.3af
RS485 Port	1
Relay Output	1
Relay Input	2
TF Card Slot	1
Microphone	1
Speaker	1
Installation	wall-mounted
Dimensions	146 x 70 x 23 mm
Working Humidity	10~90%
Working Temperature	-40°C ~ +60°C
Storage Temperature	-40°C ~ +70°C
Button	one call button
Light Sensor	1
Wiegand Port	yes
RF Card Reader	13.56 MHz, NFC
Tamper Alarm	yes
BLE	yes
IP Rating	IP65
Audio	SIP v1 (RFC2543), SIP v2 (RFC3261)
Narrowband Audio Codec	G.711a, G.711μ
Wideband Audio Codec	G.722
DTMF	in-band, out-of-band DTMF (RFC2833), SIP Info
Echo Cancellation	yes
Voice Activation Detection	yes
Comfort Noise Generator	yes
SIP and ONVIF Compliance	yes
Video Sensor	1/2.8", CMOS
Pixels	CIF, VGA, 4CIF, 720p, 1080p
Video Codec	H.264

Table A1 - MyBell 2-Wire 1-button Station - Device description

Feature	Description
Video Resolution	up to 1920 x 1080
Maximum Image Transfer Rate	1080p – 30 fps
Viewing Angle	123°(H) / 69°(V)
White LEDs for picture lighting during dark hours	yes
Compatible with 3rd Party Video Components, such as NVRs	yes
Relays Controlled Individually by DTMF Tones	yes
Camera Permanently Operational	yes
Auto Night Mode with LED Illumination	yes
White Balance	auto
Minimum Illuminaton	0.1 LUX
Supported Networking Protocols	IPv4, HTTP, HTTPS, FTP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP
Auto-Provisioning	yes
Web Management Portal	yes
Configuration Backup / Restore	yes
Entry Log Export	yes
Access Table Export / Import	yes
Firmware Upgrade	yes
System Logs (Including Door Access Logs)	yes
Application Scenario	• apartment/flat intercom with door access control • remote site entry over Internet

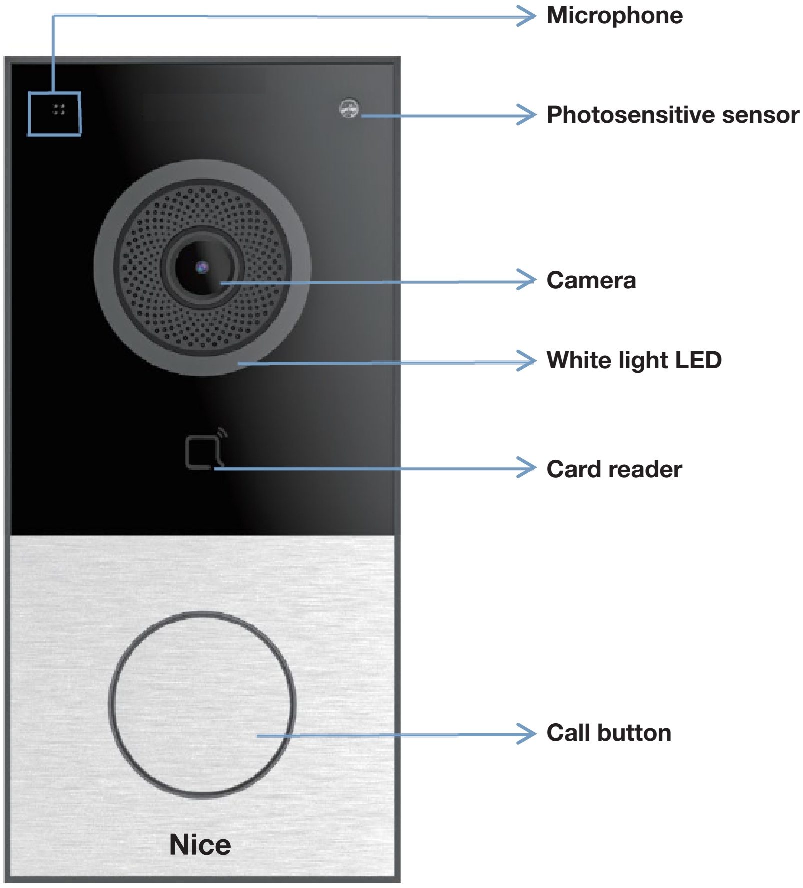
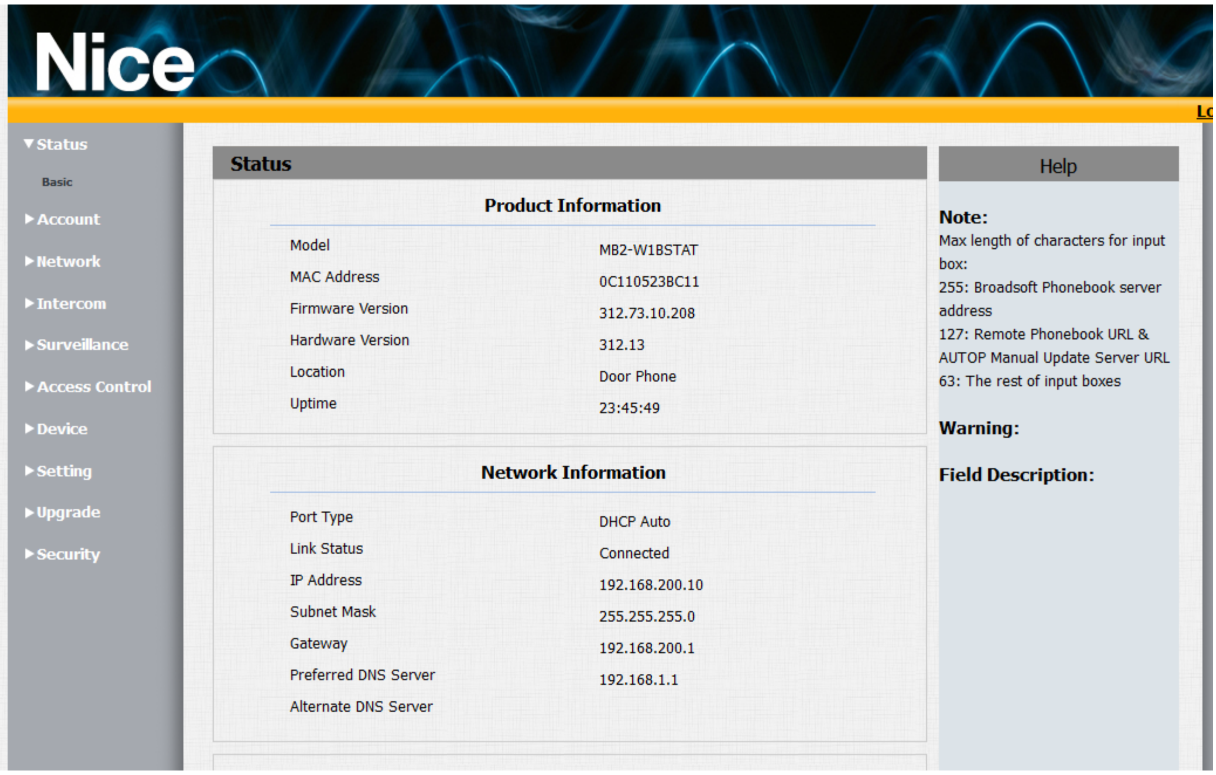


Table A2 - MyBell 2-Wire 1-button Station - Configuration menu

Section	Description
Status	Basic information such as product information, network information, and account information.
Account	SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer.
Network	DHCP & Static IP settings, RTP port setting, device deployment.
Intercom	Intercom settings, call log, etc.
Surveillance	Motion detection, RTSP, MJPEG, ONVIF, live stream.
Access Control	Input control, relay, card settings, face recognition setting, private PIN code, wiegand connection.
Device	Light, tab & button display, LCD and voice settings.
Settings	Time & language, action settings, door settings, schedule for access control.
Upgrade	Firmware upgrade, device reset & reboot, configuration file auto-provisioning, and fault Diagnosis.
Security	Password modification.



Status

Product Information

Model	MB2-W1BSTAT
MAC Address	0C110523BC11
Firmware Version	312.73.10.208
Hardware Version	312.13
Location	Door Phone
Uptime	23:45:49

Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.200.10
Subnet Mask	255.255.255.0
Gateway	192.168.200.1
Preferred DNS Server	192.168.1.1
Alternate DNS Server	

Help

Note:
Max length of characters for input box:
255: Broadsoft Phonebook server address
127: Remote Phonebook URL & AUTOP Manual Update Server URL
63: The rest of input boxes

Warning:

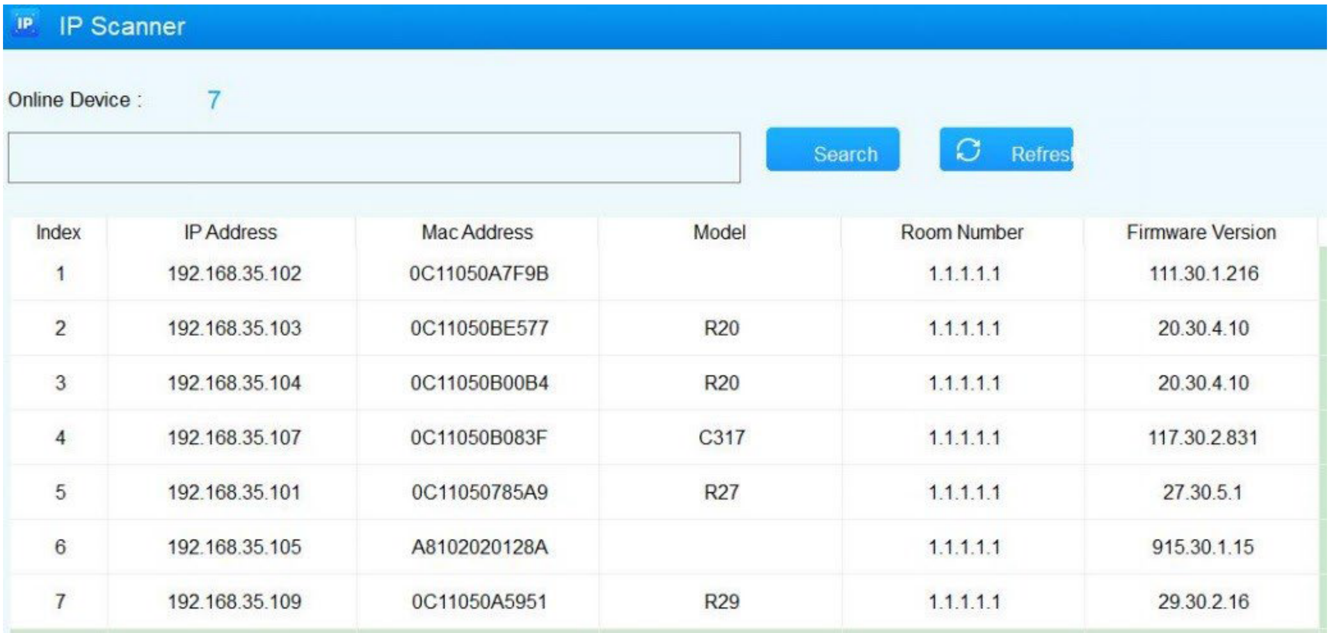
Field Description:

4 ACCESS TO DEVICE

The door phone system settings can be accessed on the device and by the web interface.

4.1 - Obtain device IP address

To check the device IP address, hold the pushbutton for 5 seconds or search the device IP using IP scanner in the same LAN network.
To search device IP using IP scanner click **Scan tab.**

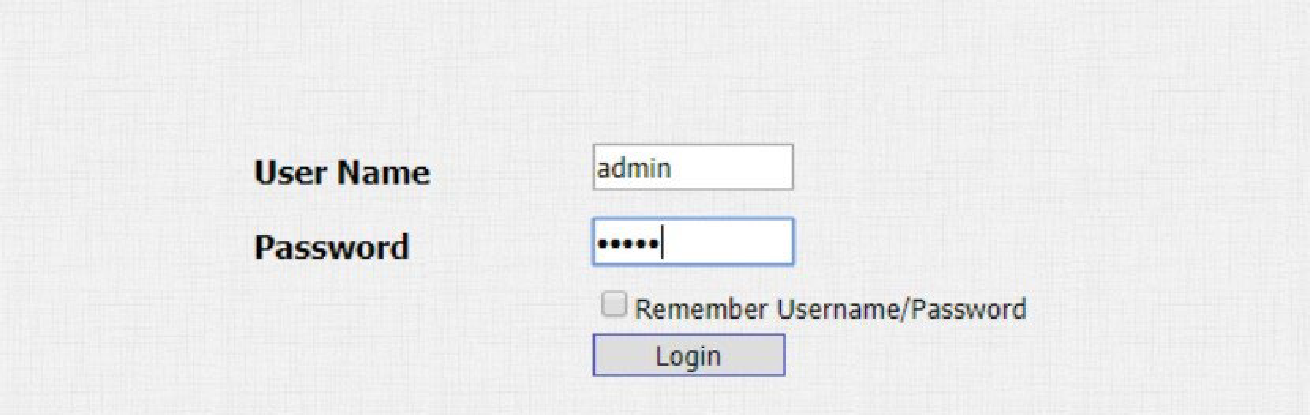


Online Device : 7

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C11050785A9	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A8102020128A		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C11050A5951	R29	1.1.1.1.1	29.30.2.16

4.2 - Access to device settings by web interface

To log in to the device web interface to configure and adjust parameters, you can also enter the device IP address in the web browser.
The default username and password are “**admin** / **admin**”. Make sure to enter them in correct case.



User Name: admin

Password: •••••

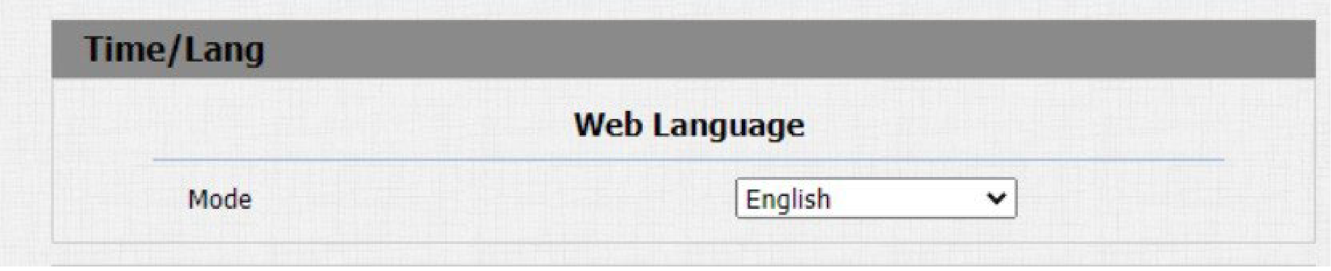
5 LANGUAGE AND TIME CONFIGURATION

5.1 - Language configuration

You can configure language on the device or by the web interface during the initial device setup or later.

To configure the language by the web interface:

Setting > Time/Lang > Web Language



Time/Lang

Web Language

Mode: English

Settings:

- **Mode:** choose the suitable web language. The default web language is normally English.

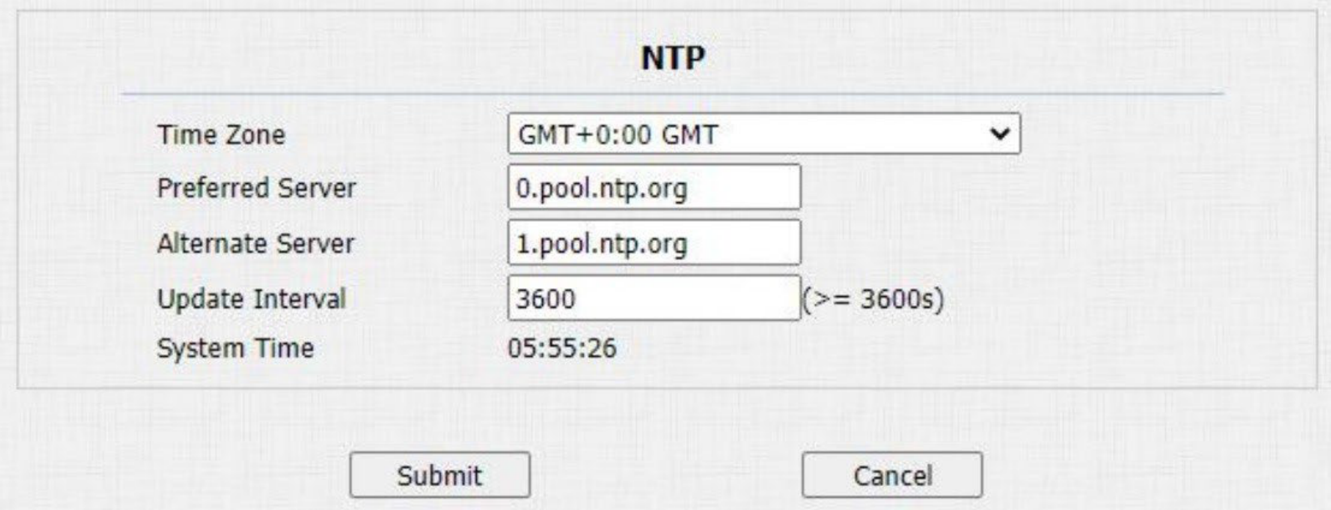
5.2 - Time configuration

The obtained NTP server address can be used to synchronize time and date automatically. Once a time zone is selected, the device notifies the NTP server of that and the NTP server synchronizes the time zone setting in the device.

You can configure time settings, including time zone or date and time format on the device or by the web interface.

To configure the time by the web interface:

Setting > Time/Lang > NTP



NTP

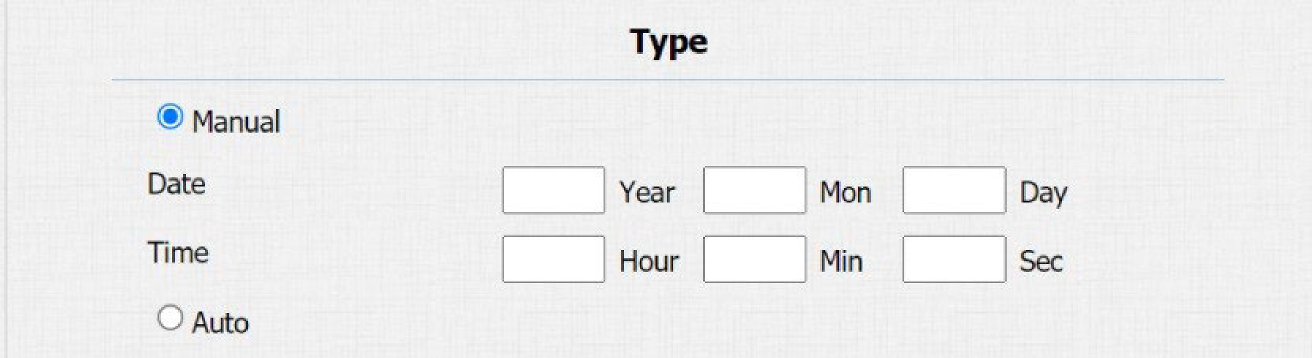
Time Zone	GMT+0:00 GMT
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	05:55:26

Settings:

- **Preferred/Alternate Server:** enter the NTP server address. The secondary server starts operating when the primary server is invalid.
- **Update Interval:** configure the interval between two consecutive NTP requests.

5.2.1 - Manual time configuration

To configure time settings manually select the **Manual** checkbox and input time data.



Type

● Manual

Date: Year Mon Day

Time: Hour Min Sec

○ Auto

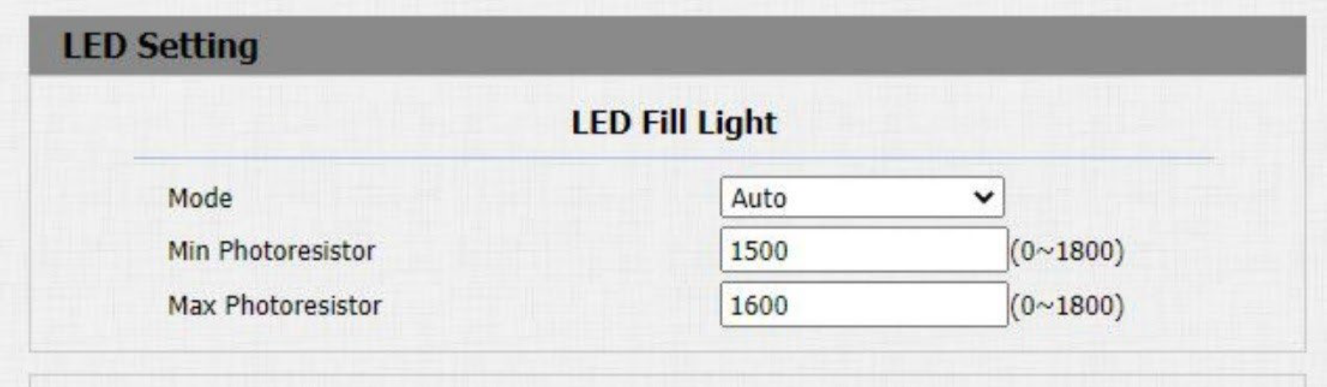
6 LED CONFIGURATION

6.1 - Infrared LED configuration

Infrared LED is mainly designed to reinforce light for facial recognition at night or in a dark environment, you can configure the infrared LED in the device and on the web interface.

To configure infrared by the web interface:

Device > LED Setting > LED Fill Light



LED Setting

LED Fill Light

Mode: Auto

Min Photoresistor: 1500 (0~1800)

Max Photoresistor: 1600 (0~1800)

Settings:

- **Mode:**
  - **Auto** – the Infrared LED light is turned on automatically according to the setting.
  - **Always OFF** – the Infrared LED light is turned off. The default infrared mode is **Always OFF**.
  - **Specific Time** – the infrared LED light is turned on according to the time schedule.
- **Min/Max Photoresistor:** set the minimum and maximum photoresistor value based on the detected photo-resistor value to control the ON/OFF status of the LED light.
  You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off.
  The default minimum and maximum photoresistor value ranges from **0** to **1000**.

Note

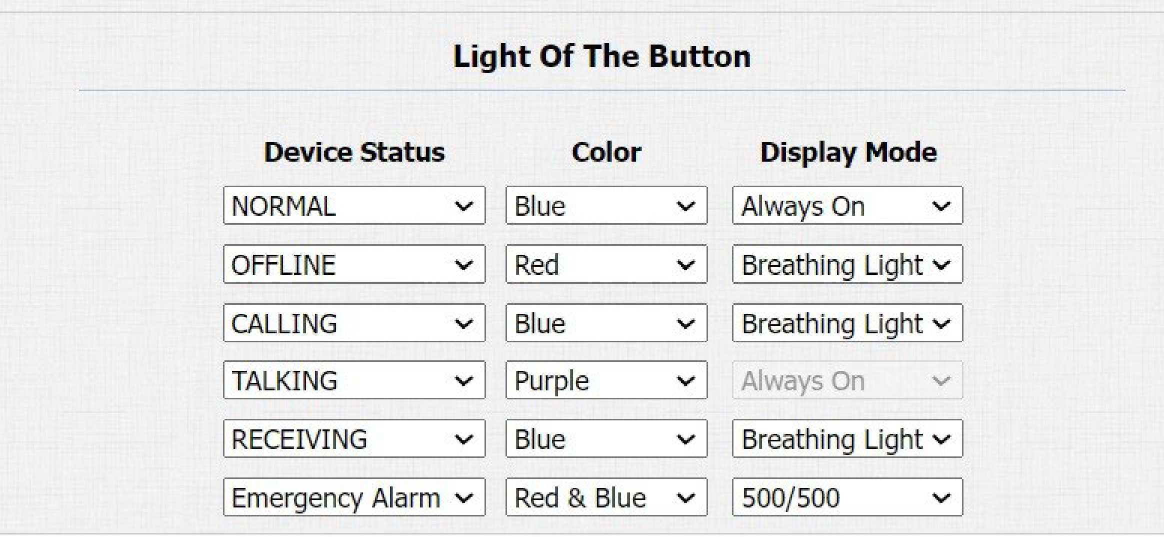
To display **Start Time** and **End Time** the **Specific Time** for LED mode needs to be selected.

6.2 - LED display status

LED display adjustment is used to indicate the light changes of the call button in 5 statuses: **normal (idle)**, **offline**, **calling**, **talking**, and **receiving a call**. The LED status enables you to verify the current mode of the device.

To configure the LED display status by the web interface:

Device > LED Setting > Light of the Button



Light Of The Button

Device Status	Color	Display Mode
NORMAL	Blue	Always On
OFFLINE	Red	Breathing Light
CALLING	Blue	Breathing Light
TALKING	Purple	Always On
RECEIVING	Blue	Breathing Light
Emergency Alarm	Red & Blue	500/500

Table A3 - MyBell 2-Wire 1-button Station - Default LED display status

Color	Status	Description
Blue	Always on	Normal status.
	Flashing	Calling.
Red	Flashing	Network is unavailable.
Green	Always on	Talking on a call.
	Flashing	Receiving a call.
Purple	Flashing	Upgrading.

Table A4 - MyBell 2-Wire 1-button Station - LED diplay status configuration	
Setting	**Description**
State	There are five states: **Normal**, **Offline**, **Calling**, **Talking** and **Receiving**.
LED Color	It supports three colors: **Red**, **Purple** and **Blue**.
LED Display Mode	It enables the configuration of different blink frequencies.

Note

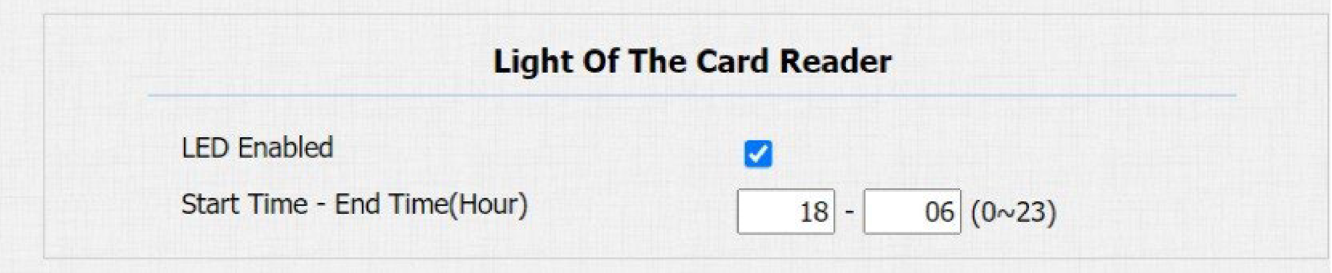
- The **State** and **Color** can't be changed.
- The **LED Color** of upgrading mode can't be adjusted.

6.3 - LED configuration on card reader area

You can enable or disable the LED lighting on the card reader area by the web interface. If you don't want the LED light on the card reader area to stay on, set the timing for the exact time span during which the LED light can be disabled to reduce electrical power consumption.

To configure the LED on card reader area by the web interface:

Device > LED Setting > Light of the Card Reader



Light Of The Card Reader

LED Enabled ☑

Start Time - End Time(Hour) 18 - 06 (0~23)

Setting:

- **Time (H):** enter the valid time span for the LED lighting. If the time span is set from 8-0 (**Start time-End time**) the LED light stays on from **8:00** am to **12:00** pm during one day (24 hours).

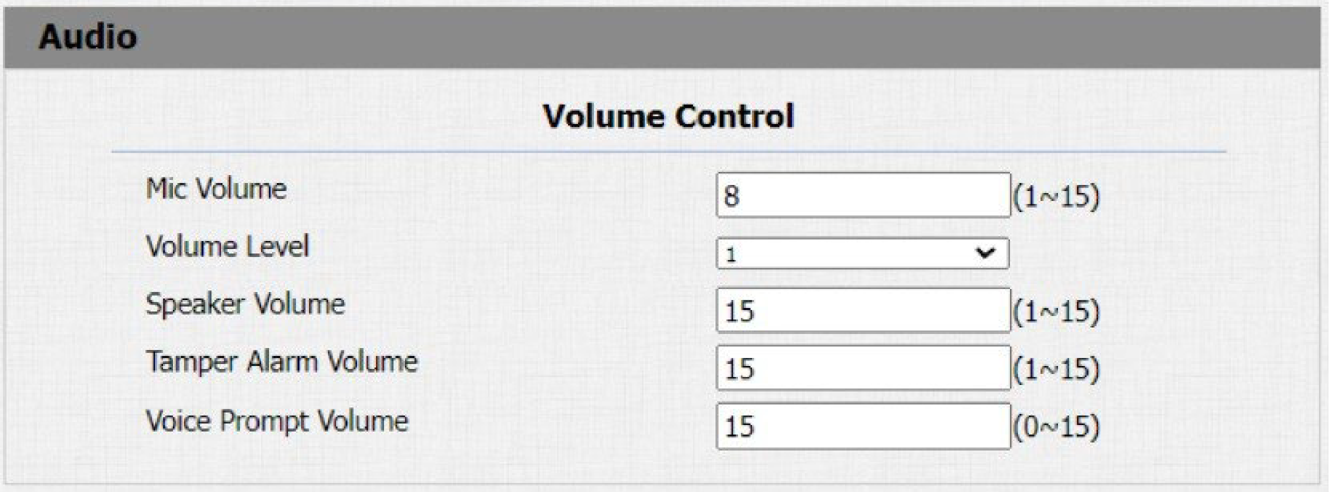
7 VOLUME AND TONE CONFIGURATION

You can configure microphone volume, AD volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone. You can also upload the tone to enrich your personalized user experience.

7.1 - Volume configuration

To configure the volume by the web interface:

Device > Audio



Audio

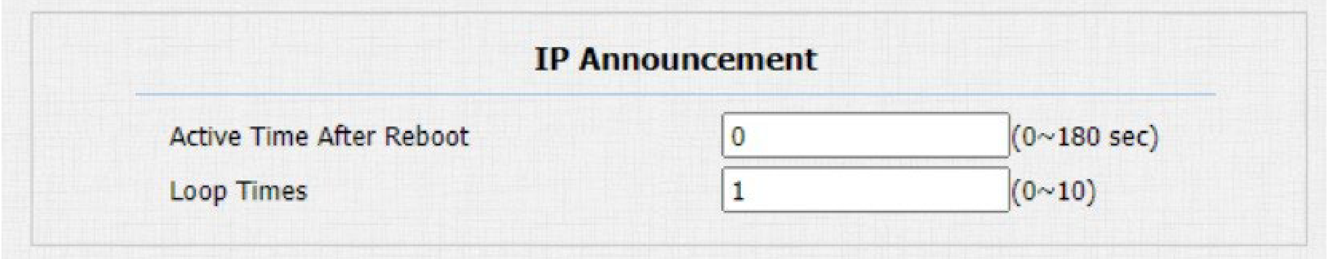
Volume Control

Mic Volume	8	(1~15)
Volume Level	1	
Speaker Volume	15	(1~15)
Tamper Alarm Volume	15	(1~15)
Voice Prompt Volume	15	(0~15)

7.2 - IP announcement configuration

To configure the device IP announcement by the web interface:

Device > Audio > IP announcement



IP Announcement

Active Time After Reboot	0	(0~180 sec)
Loop Times	1	(0~10)

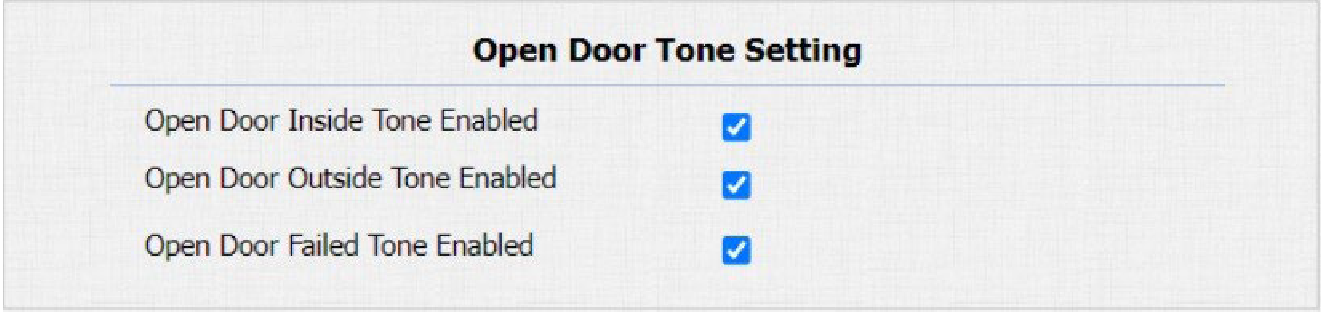
Setting:

- **Expiration (After Reboot) (Sec):** select IP announcement time after the device reboot. For example, if you set it as 30 seconds, you must press the call button within 30 seconds for the IP announcement after the device is rebooted. Otherwise, the IP announcement expires. If you set it as 0 seconds, then you can press the call button any time after the reboot for the IP announcement.
- **Loop Times:** set the IP announcement loop times.

7.3 - Open door tone configuration

To enable or disable the open door tone and control the prompt words that accompany the tone by the web interface:

Device > Audio > Open Door Tone Setting



Open Door Tone Setting

Open Door Inside Tone Enabled	☑
Open Door Outside Tone Enabled	☑
Open Door Failed Tone Enabled	☑

Setting:

- **Open Door Inside Tone:** tick this checkbox to enable the open door inside tone. It is what you can hear when you open the door by pressing the Exit button inside.
- **Open Door Outside Tone:** tick this checkbox to enable the open door outside tone. It is what you can hear when you are granted door access by various access methods on the door phone.

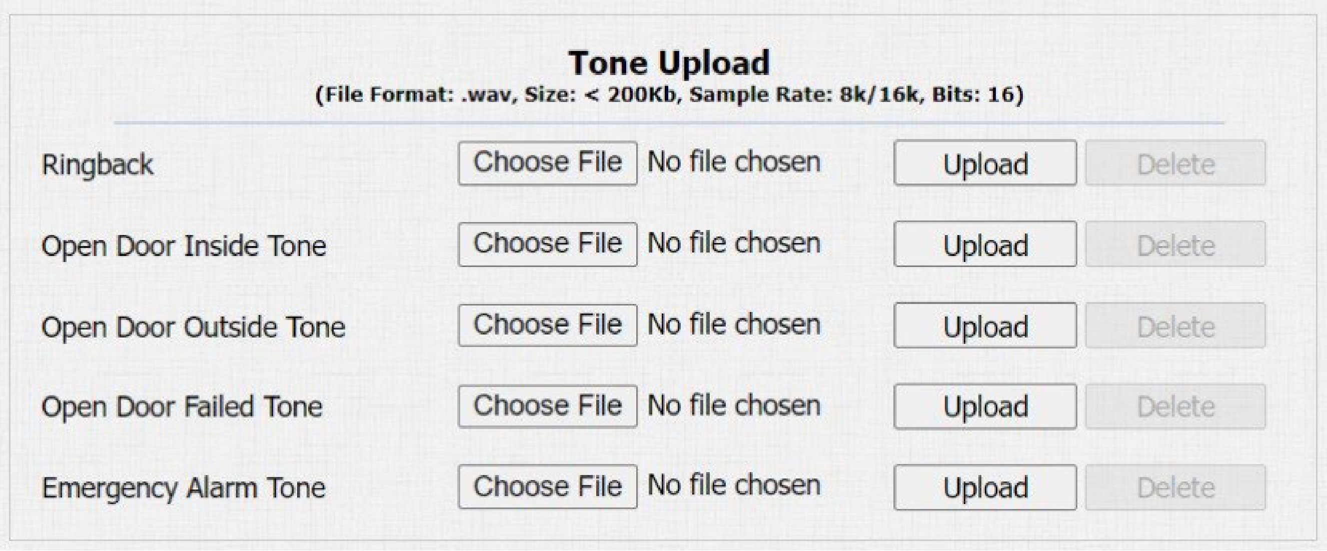
7.4 - Uploading tone files

7.4.1 - Uploading ringback tone

Ringback tone can be customised. Follow the prompt about the file size and format.

To upload the ringback tone by the web interface:

Device > Audio > Tone Upload



Tone Upload

(File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16)

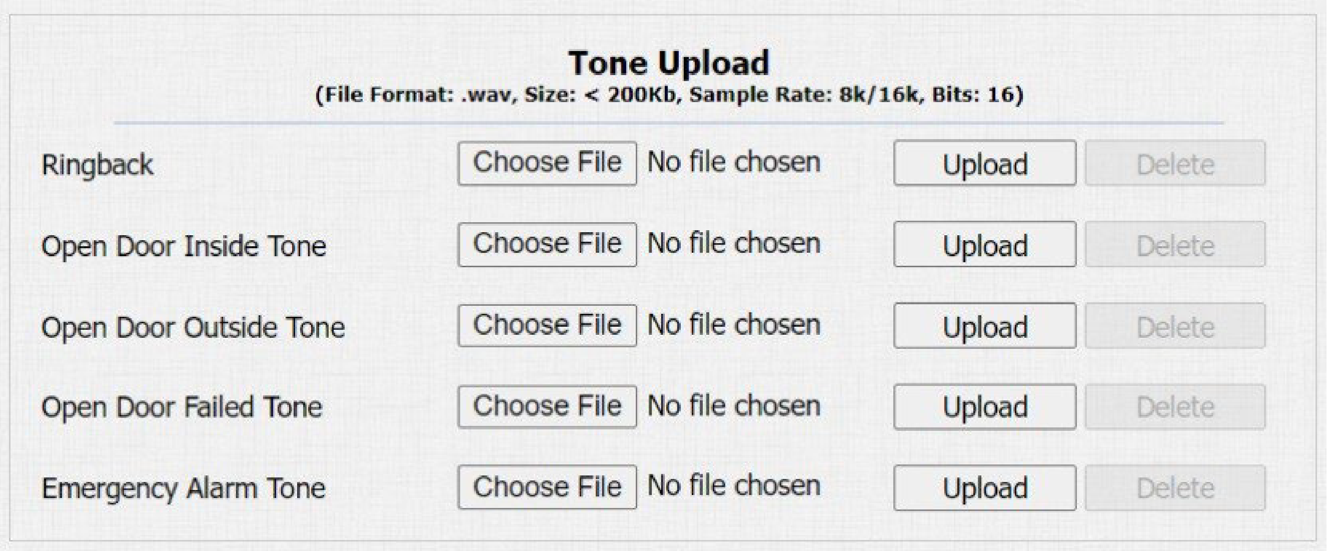
Ringback	Choose File	No file chosen	Upload	Delete
Open Door Inside Tone	Choose File	No file chosen	Upload	Delete
Open Door Outside Tone	Choose File	No file chosen	Upload	Delete
Open Door Failed Tone	Choose File	No file chosen	Upload	Delete
Emergency Alarm Tone	Choose File	No file chosen	Upload	Delete

7.4.2 - Uploading open door tone

The outside tone is used to signal opening the door by card or DTMF. The inside tone is used to signal opening the door by triggered input interface. Follow the prompt about the file size and format.

To upload the tone for open door failure and success by the web interface:

Device > Audio > Tone Upload



Tone Upload

(File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16)

Ringback	Choose File	No file chosen	Upload	Delete
Open Door Inside Tone	Choose File	No file chosen	Upload	Delete
Open Door Outside Tone	Choose File	No file chosen	Upload	Delete
Open Door Failed Tone	Choose File	No file chosen	Upload	Delete
Emergency Alarm Tone	Choose File	No file chosen	Upload	Delete

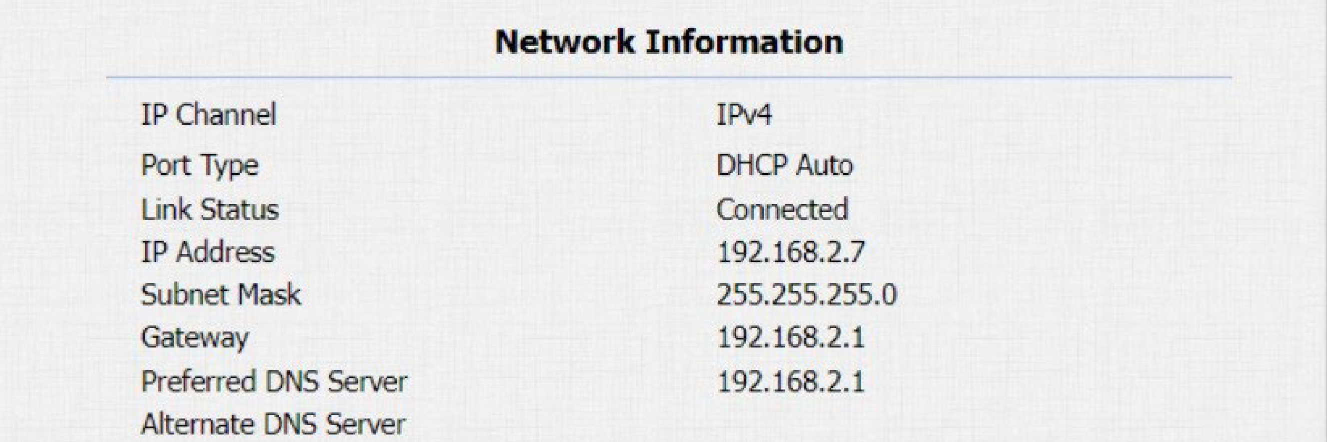
Settings:

- **Open Door Outside Tone:** warning tone that goes off when you open the door from the outside. It is what you can hear when you are granted door access by access methods on the door phone.
- **Open Door Inside Tone:** warning tone that goes off when you open the door from the inside. It is what you can hear when you open the door by pressing the Exit button inside.

8.1 - Network status

To check the network status by the web interface:

Status > Network Information



Network Information

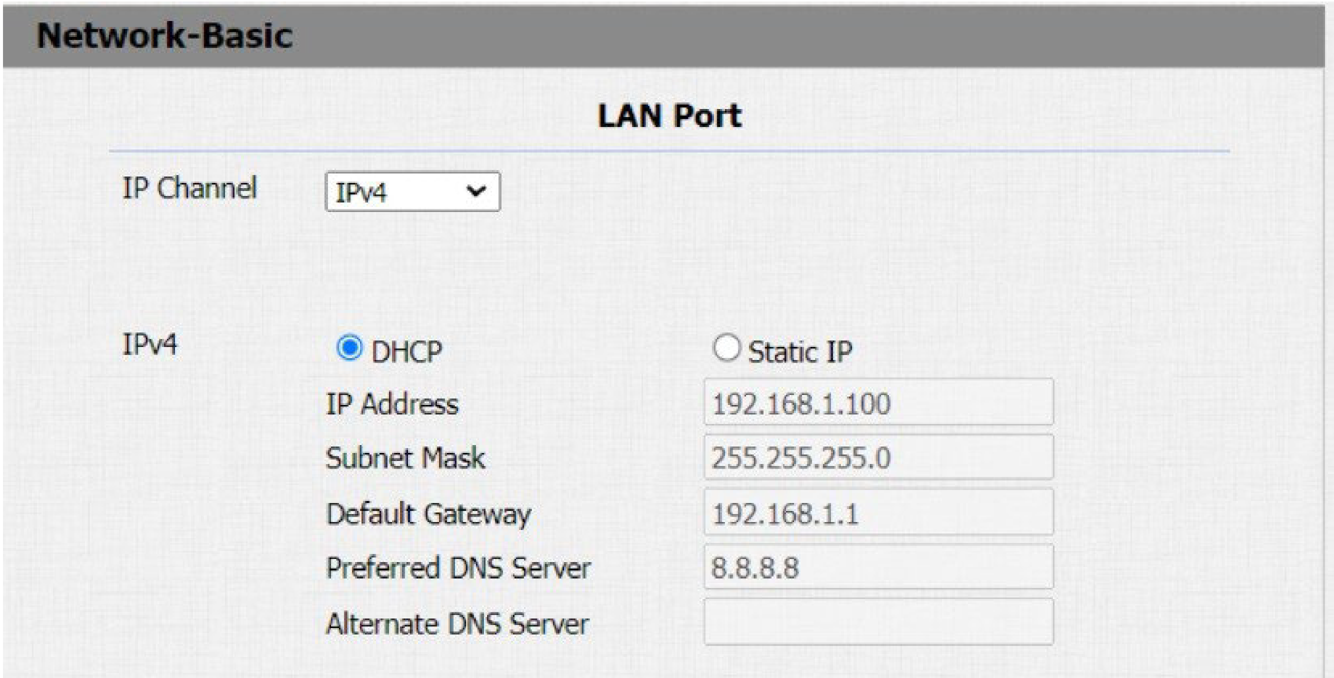
IP Channel	IPv4
Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.2.7
Subnet Mask	255.255.255.0
Gateway	192.168.2.1
Preferred DNS Server	192.168.2.1
Alternate DNS Server	

8.2 - Device network configuration

You can check the door phone network connection info and configure the default Dynamic Host Configuration Protocol (DHCP) mode and static IP connection for the device on the device or by the web interface.

To configure the device network by the web interface:

Network > Basic



Network-Basic

LAN Port

IP Channel: IPv4

IPv4: ● DHCP ○ Static IP

IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Table A5 - MyBell 2-Wire 1-button Station - Network configuration

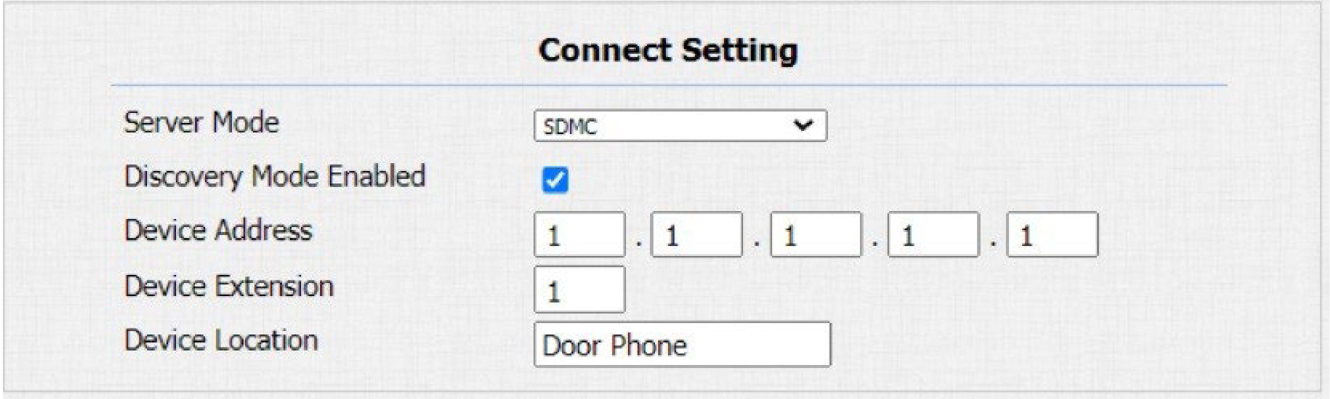
Setting	Description
DHCP	Select the **DHCP** mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, the door phone is assigned by the DHCP server with IP address, subnet mask, default gateway, and Domain Name Server (DNS) address automatically.
Static IP	Select the static IP mode by ticking the **DHCP** checkbox. When the **Static IP** mode is selected, the IP address, subnet mask, default gateway, and DNS servers addresses need to be configured manually according to your network environment.
IP Address	Set up the IP Address if the **Static IP** mode is selected.
Subnet Mask	Set up the subnet mask according to your network environment.
Default Gateway	Set up the correct gateway according to the IP address of the default gateway.
Preferred and Alternate DNS Server	Set up the preferred or alternate DNS server according to your network environment. The preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary address. The door phone connects to the alternate server when the preferred server is unavailable.

8.3 - Device deployment in network

Before they are properly configured, the door phones need to be deployed in the network environment in terms of their location, operation mode, address, and extension numbers for device control and the convenience of management.

To deploy the device in the network by the web interface:

Network > Advanced > Connect Setting



Connect Setting

Server Mode: SDMC

Discovery Mode Enabled: ☑

Device Address: 1 . 1 . 1 . 1 . 1

Device Extension: 1

Device Location: Door Phone

Table A6 - MyBell IP 2-Wire 1-button Station - Device deployment in network	
Setting	**Description**
Server Mode	It's set up automatically according to the device connection with a specific server in the network, such as **SDMC** or **Cloud** and **None**. **None** is the default factory setting indicating the device isn't in any server type and you can choose **Cloud, SDMC** in the discovery mode.
Discovery Mode Enabled	Enable the discovery mode of the device so that it can be discovered by other devices in the network, and disable it if you want to conceal the device so as not to be discovered by other devices.
Device Address	Specify the device address by entering the device location information in a sequence from left to right: **Community, Unit, Stair, Floor, Room**.
Device Extension	Enter the device extension number for the device you installed.
Device Location	Enter the location in which the device is installed and used.

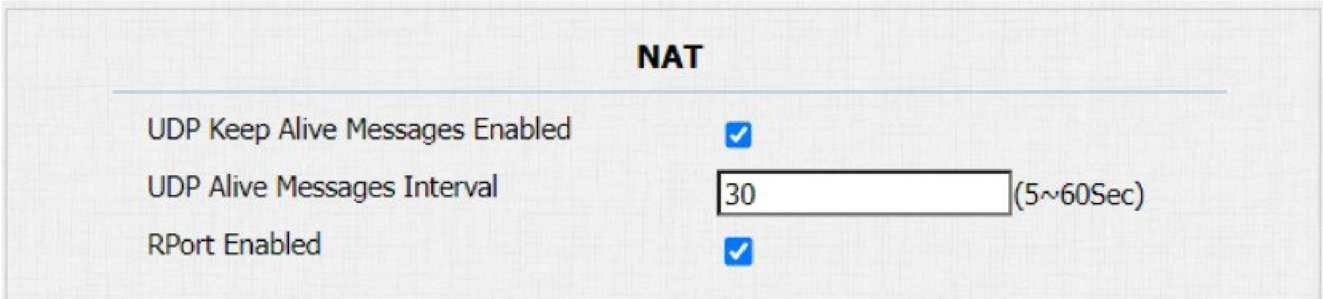
8.4 - NAT configuration

Network Address Translation (NAT) enables hosts in the organization private intranet to connect transparently to hosts in the public domain.

There is no need for internal hosts to have registered Internet addresses. It's a way to translate an internal private network IP address into a legal network IP address technology.

To configure the NAT by the web interface:

Account > Advanced > NAT



NAT

UDP Keep Alive Messages Enabled: ☑

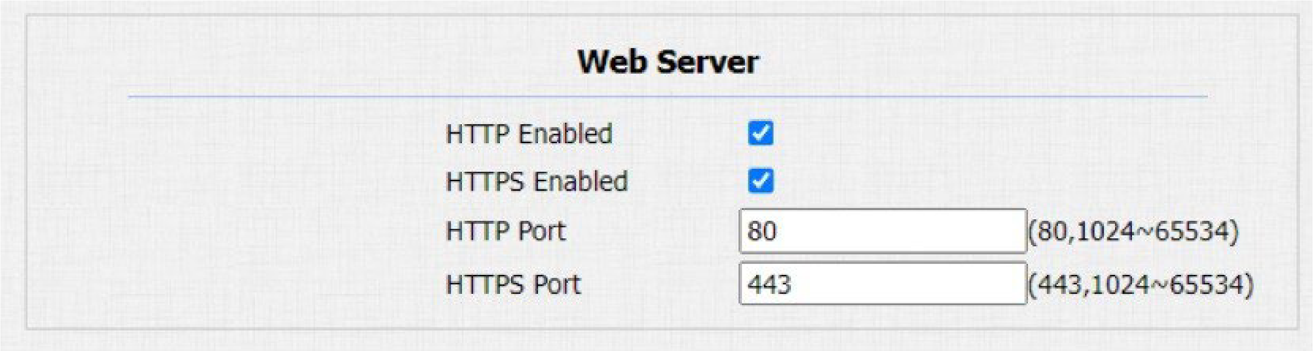
UDP Alive Messages Interval: 30 (5~60Sec)

RPort Enabled: ☑

Table A7 - MyBell 2-Wire 1-button Station - NAT configuration	
Setting	**Description**
UDP Keep Alive Messages	If enabled, the device sends out the message to the SIP server and the SIP server recognizes if the device is online.
UDP Alive Msg Interval	Set the message sending time interval from 5 to 60 seconds. The default time is 30 seconds.
RPort	Enable the RPort when the SIP server is in Wide Area Network (WAN).

8.5 - Device web HTTP configuration

This function manages device website access. The door phone supports two remote access methods: HTTP and HTTPS (encryption).
To configure the device web HTTP by the web interface:
Network > Advanced > Web Server



Web Server

HTTP Enabled ☑
HTTPS Enabled ☑
HTTP Port 80 (80,1024~65534)
HTTPS Port 443 (443,1024~65534)

Settings:

- **HTTP Enabled:** if **enabled**, the HTTP access to the device web page is allowed, if **disabled** it's not allowed. The default setting is **enabled**.
- **HTTPS Enabled:** if **enabled**, the HTTPS access to the device web page is allowed, if **disabled** it's not allowed. The default setting is **enabled**.
- **HTTP Port:** set up the port for HTTP access method. The default port is **80**.
- **HTTPS Port:** set up the port for HTTPS access method. The default port is **443**.

9 INTERCOM CALL CONFIGURATION

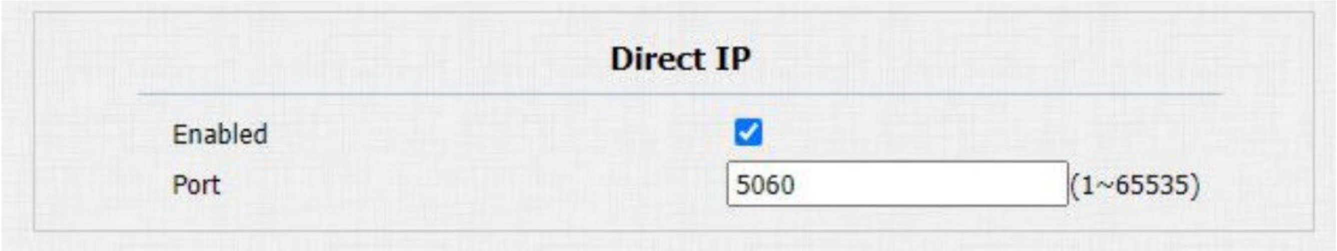
The intercom calls in the device can be configured to allow you to perform various customized intercom calls such as IP calls and SIP calls for different application scenarios.

9.1 - IP call and IP call configuration

IP calls can be made directly on the intercom device by entering the IP number. You can also disable the direct IP calls so that no IP calls can be made.

To configure IP and IP call by the web interface:

Intercom > Basic > Direct IP



Direct IP

Enabled ☑

Port 5060 (1~65535)

Settings:

- **Enabled:** if you don't allow direct IP calls to be made on the device, untick this checkbox to disable this function.
- **Port:** set up the IP direct call port. The the default port is **5060**.

9.2 - SIP call and SIP call configuration

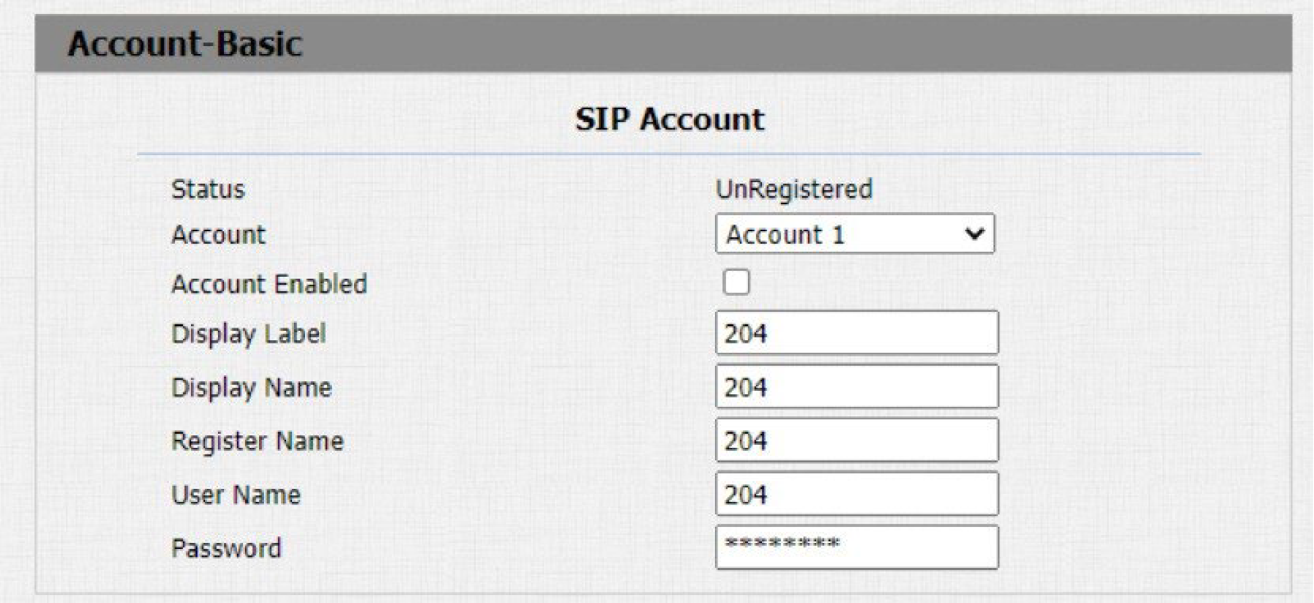
You can make a Session Initiation Protocol (SIP) call in the same way as you make the IP calls using the device. However, SIP call settings related to its account, server, and transport type need to be configured first.

9.2.1 - SIP account registration

The door phones support two SIP accounts that can be registered according to your applications and you can switch between them (for example, if one of them fails). The SIP account can be configured on the device or by the web interface. **Register Name**, **User Name**, and **Password** are obtained from the SIP account administrator.

To configure the SIP account by the web interface:

Web Account > Basic > SIP Account



Account-Basic

SIP Account

Status UnRegistered

Account Account 1

Account Enabled □

Display Label 204

Display Name 204

Register Name 204

User Name 204

Password ********

Table A8 - MyBell 2-Wire 1-button Station - SIP account registration

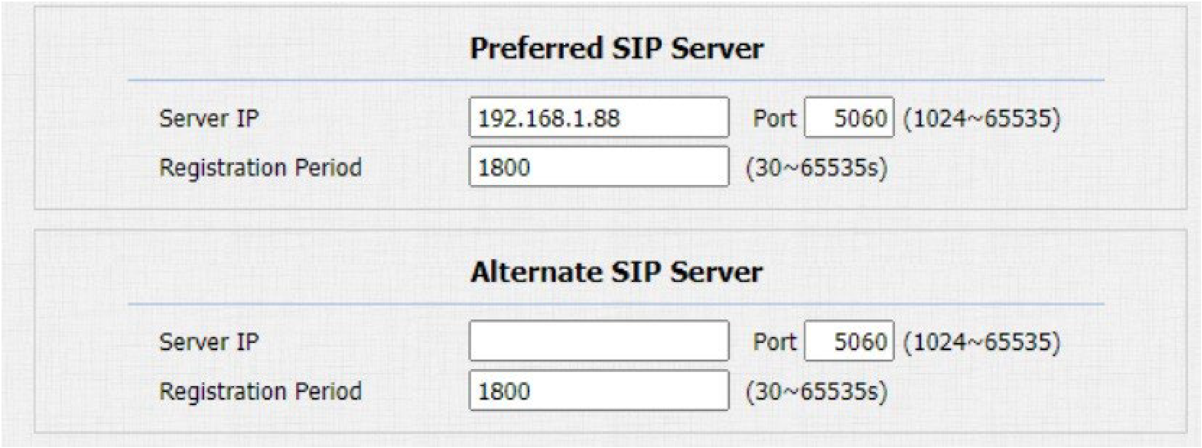
Setting	Description
Status	Check to see if the SIP account is registered.
Account	Select the account to be configured (Account 1 or 2).
Account Enabled	**Enable** or **Disable** to activate or deactivate the registered SIP account.
Display Label	Configure the device label to be shown on the device screen.
Display Name	Configure the name, for example, the device name to be shown on the device being called to.

9.2.2 - SIP server configuration

SIP servers can be set up for devices to enable call sessions through SIP servers between intercom devices.

To configure the SIP server by the web interface:

Account > Basic > SIP Server



Preferred SIP Server

Server IP: 192.168.1.88 Port: 5060 (1024~65535)

Registration Period: 1800 (30~65535s)

Alternate SIP Server

Server IP: Port: 5060 (1024~65535)

Registration Period: 1800 (30~65535s)

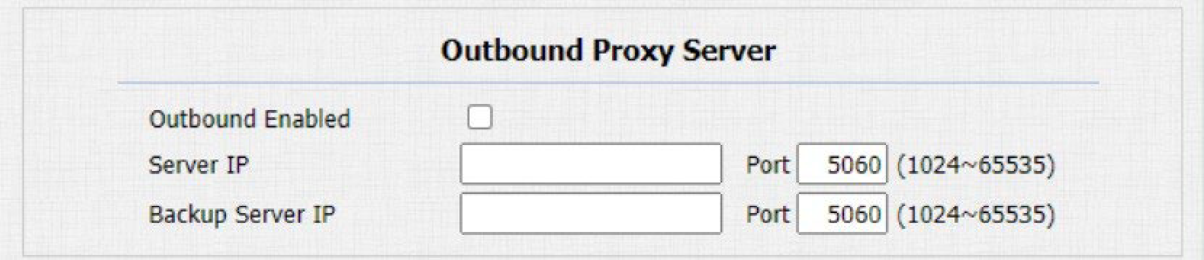
Table A9 - MyBell 2-Wire 1-button Station - SIP server configuration	
Setting	**Description**
Preferred SIP Server	Enter the primary SIP server IP address number or its URL.
Alternate SIP Server	Enter the backup SIP server IP address number or its URL.
Port	Set up the SIP server port for data transmission.
Registration Period	Set up the SIP account registration time span. The SIP re-registration starts automatically if the account registration fails during the registration time span. The registration period range is 30-65535 seconds. The default period is 1800 seconds.

9.3 - Outbound proxy server configuration

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server to establish a call session through port-based data transmission.

To configure the outboubound proxy server by the web interface:

Account > Basic > Outbound Proxy Server



Outbound Proxy Server

Outbound Enabled □

Server IP: Port: 5060 (1024~65535)

Backup Server IP: Port: 5060 (1024~65535)

Settings:

- **Preferred/Alternate Server IP:** enter the SIP address of the primary/backup outbound proxy server.
- **Port:** enter the Port number for establishing call session by the primary/backup outbound proxy server.

9.4 - Data transmission type configuration

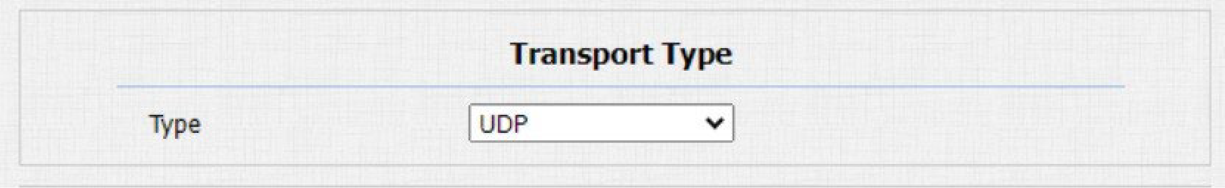
SIP messages can be transmitted in the following data transmission protocols:

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- Transport Layer Security (TLS)
- DNS-SRV

You can also identify the server from which the data comes.

To configure the data transmission type by the web interface:

Account > Basic > Transport Type



Transport Type

Type: UDP

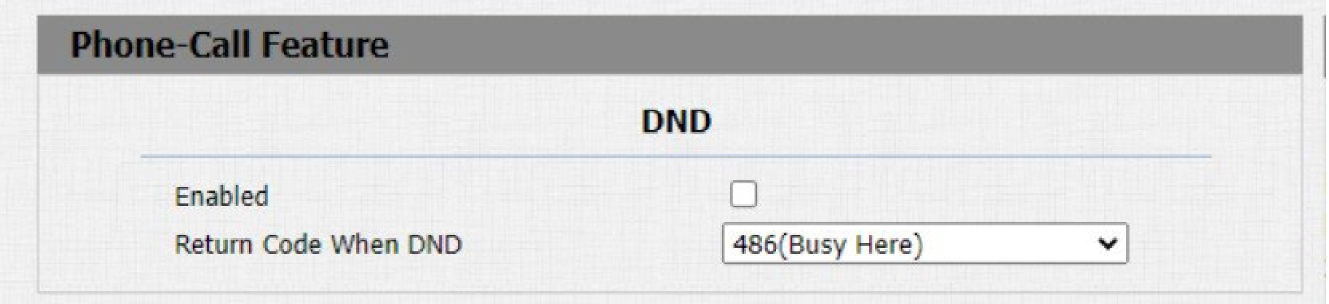
Table A10 - MyBell 2-Wire 1-button Station - Data transmission type configuration	
Setting	**Description**
UDP	Select **UDP** for unreliable but efficient transport layer protocol. UDP is the default transport protocol.
TCP	Select **TCP** for reliable but less-efficient transport layer protocol.
TLS	Select **TLS** for secure and reliable transport layer protocol.
DNS-SRV	Select **DNS-SRV** to obtain a DNS record for specifying the location of services. SRV records the server address and the server port. SRV can also be used to configure the priority and weight of the server address.

10.1 - Do not disturb feature configuration

Do not disturb (**DND**) setting eliminates distraction by unwanted incoming SIP calls. You can configure the DND-related settings by the device web interface to block SIP calls you don't intend to answer. You can also define the code to be sent to the SIP server when you want to reject the call.

To configure the DND feature by the web interface:

Intercom > Call Feature



Phone-Call Feature

DND

Enabled □

Return Code When DND: 486(Busy Here)

Setting:

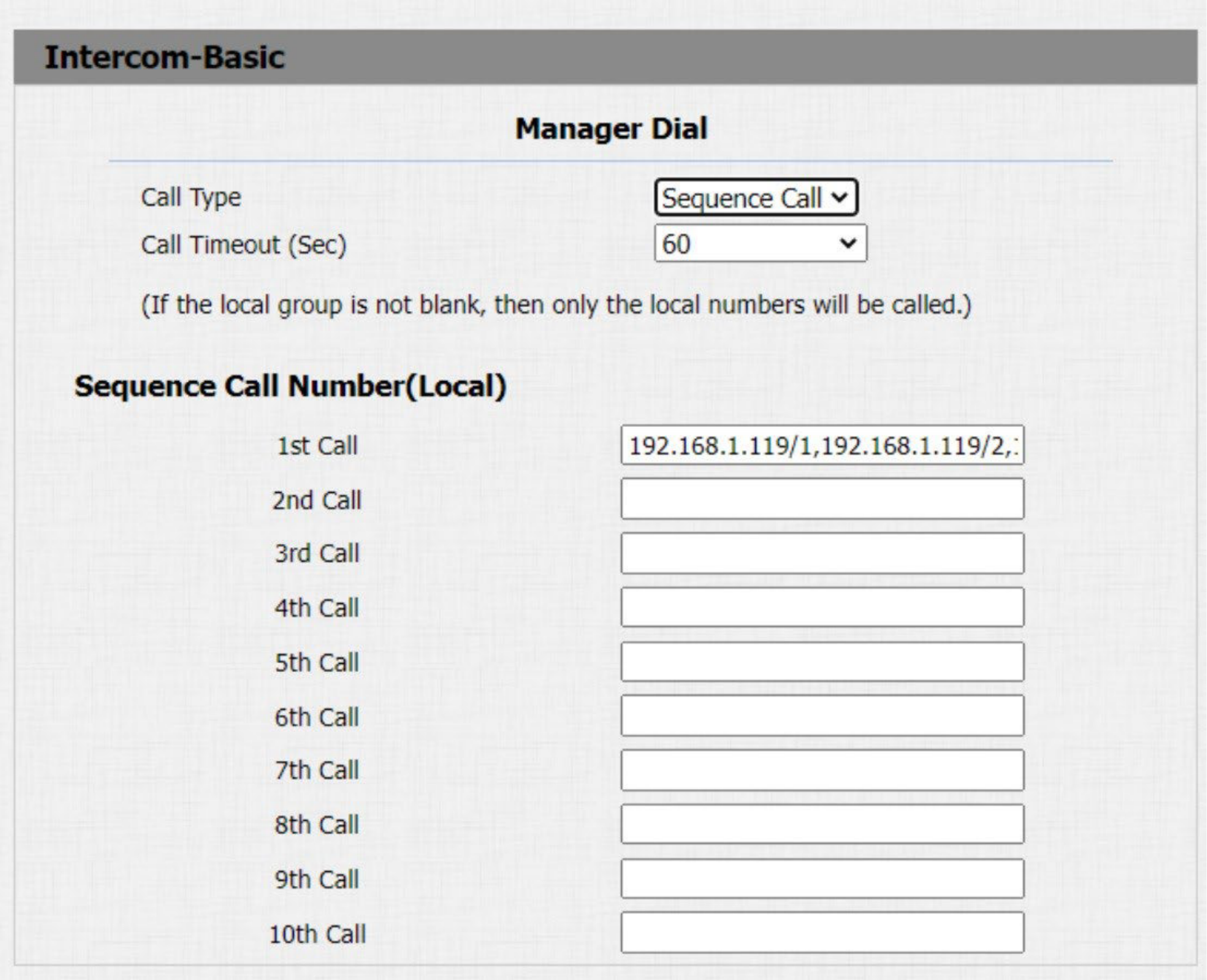
- **Return Code When DND**: select code to be sent to the caller side via SIP server when you rejected the incoming call.

10.2 - Manager dial call configuration

Manager dial call includes two types of calls: sequence call and group call. It enables quick initiation of pre-configured numbers by pressing the **Manager** key on the door phone.

To configure the manager dial call by the web interface:

Intercom > Basic > Manager Dial



Intercom-Basic

Manager Dial

Call Type: Sequence Call

Call Timeout (Sec): 60

(If the local group is not blank, then only the local numbers will be called.)

Sequence Call Number(Local)

1st Call	192.168.1.119/1,192.168.1.119/2,:
2nd Call	
3rd Call	
4th Call	
5th Call	
6th Call	
7th Call	
8th Call	
9th Call	
10th Call	

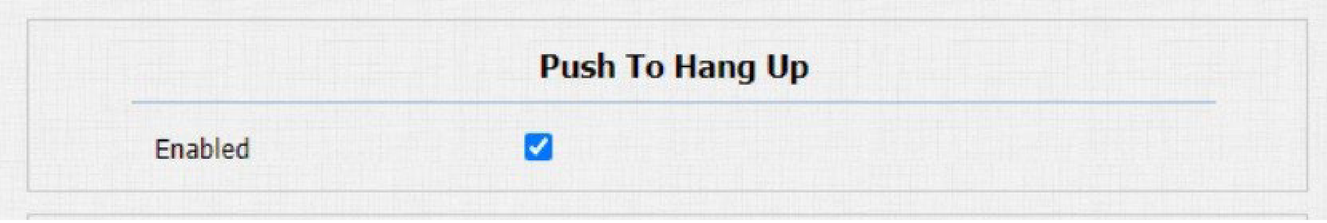
Table A11 - MyBell 2-Wire 1-button Station - Manager dial call configuration

Setting	Description
Call Type	Select the **Group Call** or **Sequence Call** (robin call) for the manager dial call.
Sequence Call	Sequence call is used to initiate multiple numbers when your press the **Manager** key. If the previous callee doesn't answer within the set time, the call is transferred to the next callee. Once the call is answered, it isn't transferred anymore.
Group Call	Group call is used to initiate calls to multiple numbers at the same time when you press the **Manager** key.
Sequence Call Number (Local)	You can enter up to five sequence call numbers in each line.

10.3 - Call hang up configuration

To enable the pushbutton call hang up by the web interface:

Intercom > Basic



Push To Hang Up

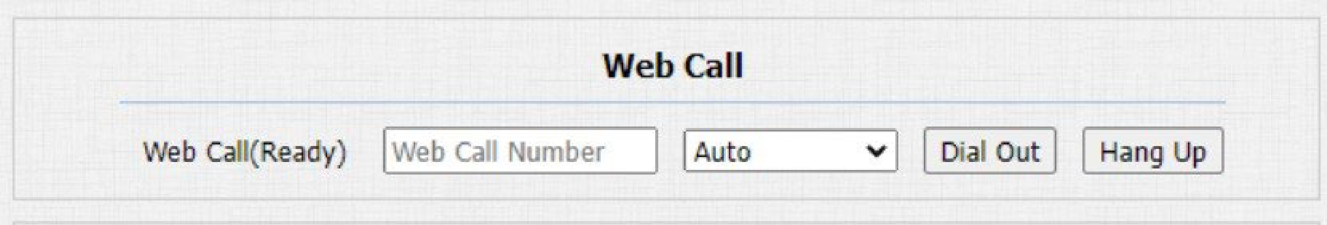
Enabled ☑

10.4 - Web call configuration

You can also make a call remotely by the device web interface, for example, for testing purposes.

To make the call by the web interface:

Upgrade > Diagnose > Web Call



Web Call

Web Call(Ready) [Web Call Number] [Auto ▾]

Setting:

- **Web Call (Ready):** enter the IP/SIP number to dial out.

10.5 - Auto answer configuration

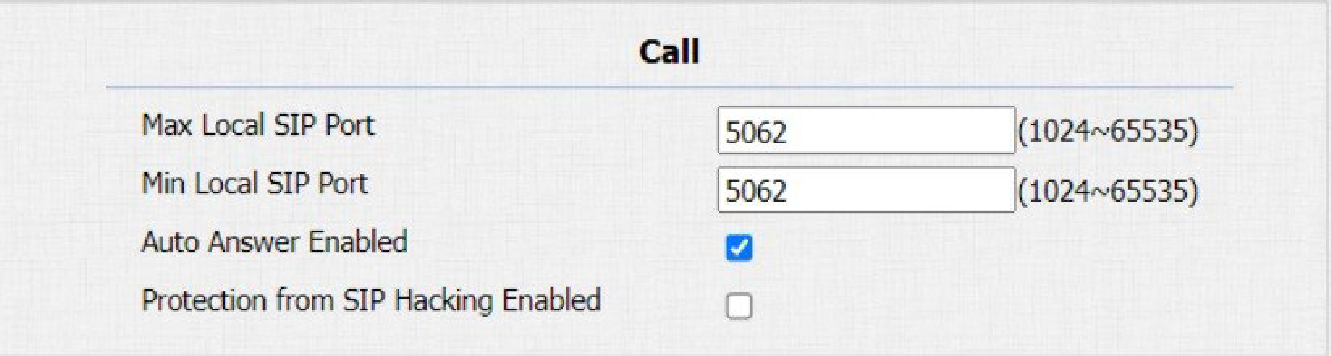
You can define the time of the door phone response for the incoming SIP/IP call automatically by setting up the time-related parameters. You can also define the mode in which the calls are answered (video or audio).

To enable the auto answer by the web interface:

Account > Advanced > Call

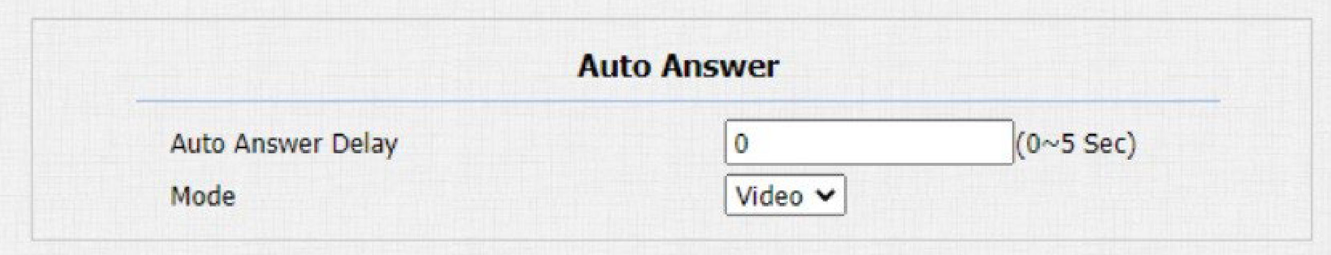
To configure the related parameters by the web interface:

Intercom > Call Feature > Auto Answer



Call

Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)
Auto Answer Enabled	☑	
Protection from SIP Hacking Enabled	□	



Auto Answer

Auto Answer Delay	0	(0~5 Sec)
Mode	Video ▾	

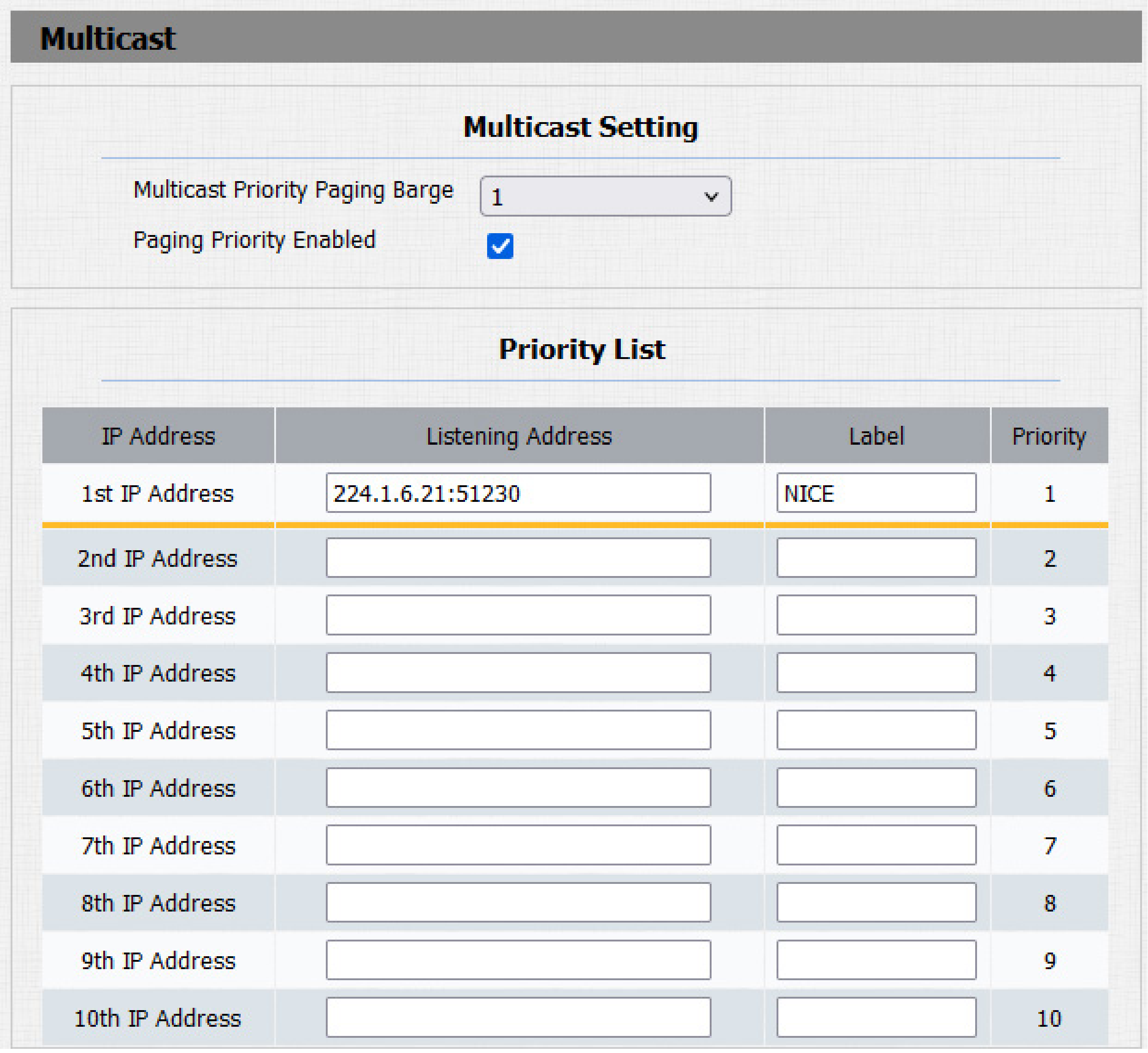
Table A12 - MyBell 2-Wire 1-button Station - Auto answer configuration	
Setting	**Description**
Auto Answer	Turn on the Auto Answer function by choosing **Enable**.
Auto Answer Delay	Set up the delay time (from 0 to 5 seconds) before the call is answered automatically. For example, if you set the delay time to 1 second, then the call is answered automatically in 1 second.
Mode	Set up the video or audio mode for answering the call automatically.

10.6 - Multicast configuration

Multicast is a one-to-many communication within a range. The door phone can act as a listener and can receive audio from the broadcasting source.

To configure the multicast by the web interface:

Intercom > Multicast



Multicast

Multicast Setting

Multicast Priority Paging Barge: 1

Paging Priority Enabled: ☑

Priority List

IP Address	Listening Address	Label	Priority
1st IP Address	224.1.6.21:51230	NICE	1
2nd IP Address			2
3rd IP Address			3
4th IP Address			4
5th IP Address			5
6th IP Address			6
7th IP Address			7
8th IP Address			8
9th IP Address			9
10th IP Address			10

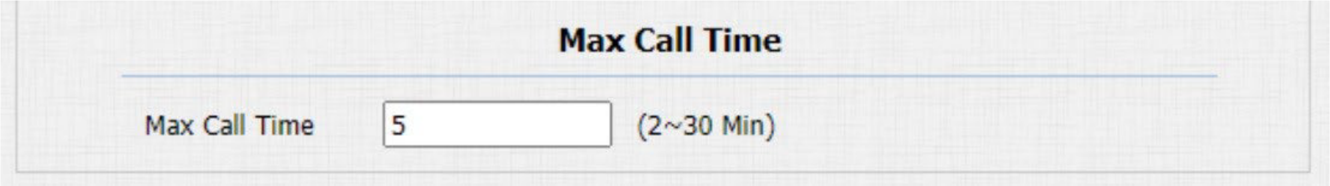
Table A13 - MyBell 2-Wire 1-button Station - Multicast configuration	
Setting	**Description**
Multicast Priority Paging Barge	Configure the amount of multicast calls with higher priority than an SIP call. If you disable Paging Priority by unticking the checkbox, the SIP call has higher priority than the multicast call.
Paging Priority Enabled	If enabled, multicast calls are perfomed in order of priority.
Listening Address	Enter the multicast IP address from which you want to listen to the call. The multicast IP address needs to be the same as the part listened to and the multicast port can't be the same for each IP address. Multicast IP addresses range from 224.0.0.0 to 239.255.255.255.

10.7 - Maximum call duration configuration

The door phone enables you to configure the call time duration for a call received from the calling device. When the set call duration is reached, the door phone ends the call automatically.

To configure the maximum call duration by the web interface:

Intercom > Call Feature > Max Call Time



Max Call Time

Max Call Time 5 (2~30 Min)

Setting:

- **Max Call Time:** enter the call time duration according to your need (ranging from 2-30 min). The default call time duration is 5 min.

Note

Maximum call time for the device is related with maximum call time for the SIP server. When using the SIP account to make a call, please pay attention to the maximum call time for the SIP server. If it's shorter than the maximum call time for the device, the shorter one applies.

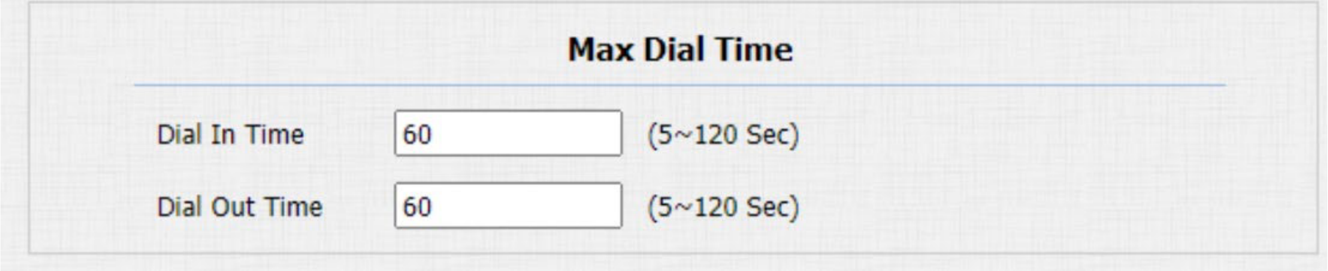
10.8 - Maximum dial duration configuration

Maximum dial duration refers to the maximum time allowed for both dial-in and dial-out calls.

- Dial-in time is the maximum time before the door phone automatically hangs up if there's no answer.
- Dial-out time is the maximum time before the door phone automatically hangs up when the intercom device being called doesn't answer.

To configure the maximum dial duration by the web interface:

Intercom > Call Feature > Max Dial Time



Max Dial Time

Dial In Time 60 (5~120 Sec)

Dial Out Time 60 (5~120 Sec)

Settings:

- **Dial In Time:** enter the dial-in time duration for your door phone (ranging from 5-120 seconds).
  Example: if you set the dial-in time duration to 60 seconds in your door phone, the door phone hangs up the incoming call automatically if the call isn't answered in 60 seconds. The default dial-in time is 60 seconds.
- **Dial Out Time:** enter the dial-out time duration for your door phone (ranging from 5-120 seconds).
  Example, if you set the dial-out time duration to 60 seconds in your door phone, the door phone hangs up the call it dialed out automatically if the call isn't answered by the device being called.

Note

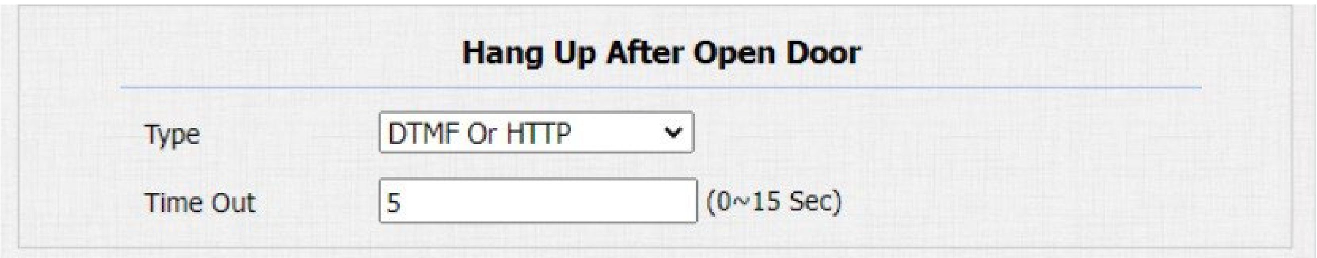
Maximum dial time for the device is related with maximum dial time for the SIP server. When using the SIP account to make a call, please pay attention to the maximum dial time for the SIP server. If it's shorter than the maximum dial time for the device, the shorter one applies.

10.9 - Hang up after open door

This feature is used to hang up the call automatically after the door is opened during a call. The hang up button doesn't have to be clicked to end the call.

To configure the hang up after open door feature by the web interface:

Setting>Door>Hang Up After Open Door



Hang Up After Open Door

Type DTMF Or HTTP

Time Out 5 (0~15 Sec)

Settings:

- **Type:** select the open door type. Door can be unlocked by the following commands:
  - **DTMF**
  - **HTTP**
  - **DTMF or HTTP**
  - **Input, DTMF, or HTTP**
- **Timeout:** the timeout value can be set up from 1 second to 15 seconds. The call automatically ends within this set time after the door is opened.

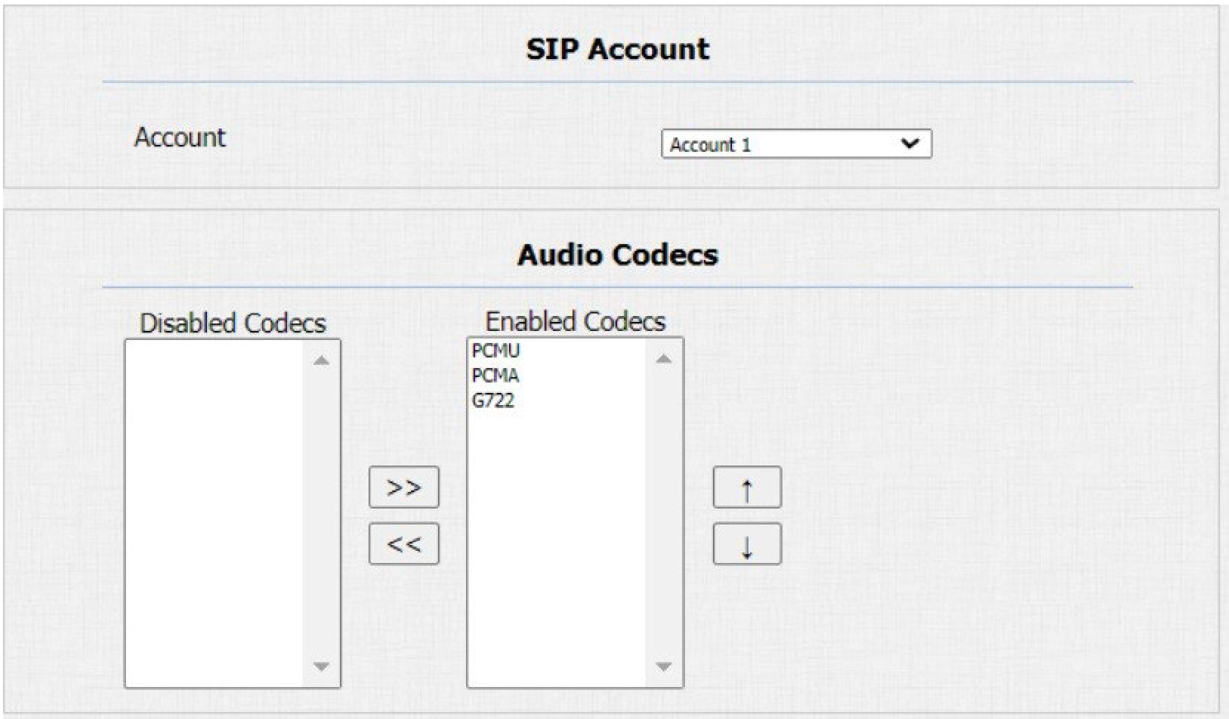
11 AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS

11.1 - Audio codec configuration

The door phone supports four types of Codec (PCMU, PCMA and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly, according to the network environment.

To configure the audio codec by the web interface:

Account > Advanced



SIP Account

Account: Account 1

Audio Codecs

Disabled Codecs

Enabled Codecs: PCMU, PCMA, G722

Please refer to the bandwidth consumption and sample rate for the codec types from the Table A14 below:

Table A14 - MyBell 2-WIre 1-button Station - Bandwidth consumption and sample rate for codec types

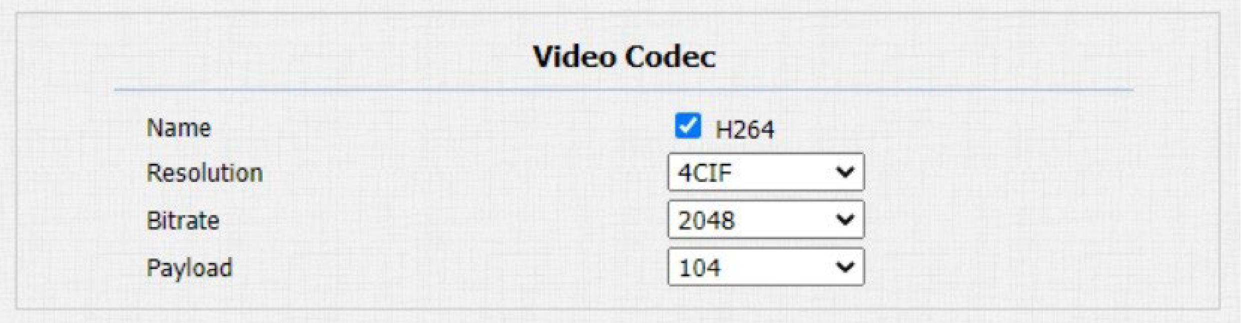
Codec type	Bandwidth consumption	Sample rate
PCMA	64 kbit/s	8 kHZ
PCMU	64 kbit/s	8 kHZ
G722	64 kbit/s	16 kHZ

11.2 - Video codec configuration

The door phone supports the H.264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

To configure the video codec by the web interface:

Account > Advanced



Video Codec

Name: ☑ H264

Resolution: 4CIF

Bitrate: 2048

Payload: 104

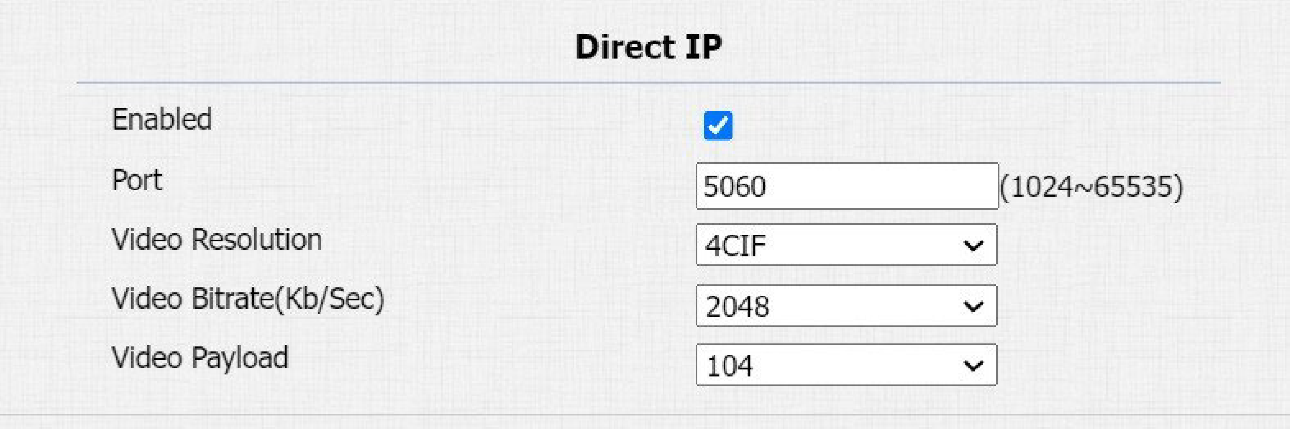
Table A15 - MyBell 2-Wire 1-button Station - Video codec configuration

Setting	Description
Name	Check to select the H.264 video codec format for the door phone video stream. The default video codec is H.264.
Resolution	Select the codec resolution for the video quality from the following options: **CIF, VGA, 4CIF, 720P,** according to your network environment. The default codec resolution is 4CIF.
Bitrate	Select the video stream bitrate (ranging from 320 to 2048). The bigger the bit rate, the more data is transmitted every second, making the video quality clearer. The default codec bitrate is 2048.
Payload	Select the payload type (ranging from 90 to 119) to set up the audio/video configuration file. The default payload is 104.

11.3 - Video codec configuration for IP direct calls

You can choose the IP call video quality by selecting the proper codec resolution according to your network condition.
To configure video codec for IP direct calls by the web interface:

Intercom > Basic > Direct IP



Direct IP

Enabled ☑

Port 5060 (1024~65535)

Video Resolution 4CIF

Video Bitrate(Kb/Sec) 2048

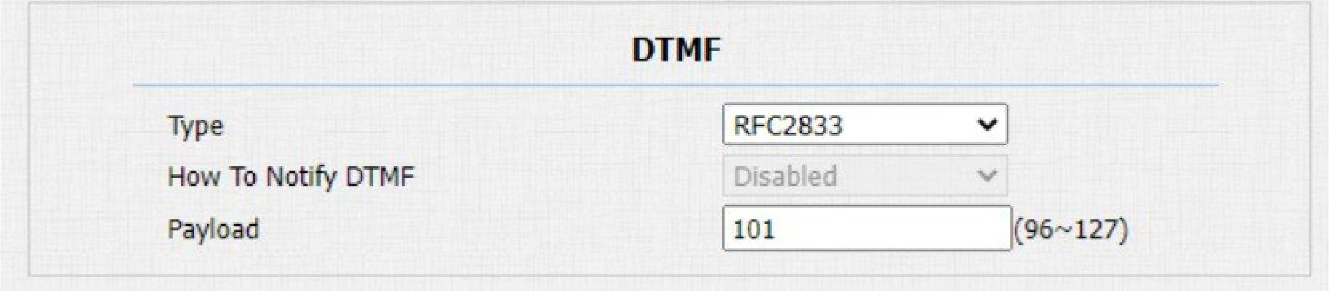
Video Payload 104

Table A16 - MyBell 2-Wire 1-button Station - Video codec configuration for IP direct calls	
Setting	**Description**
Video Resolution	Select the codec resolution for the video quality from the following options: **CIF, VGA, 4CIF, 720P.** The default resolution is 4CIF.
Video Bitrate	Select the video bitrate form the following options: **64 kbps, 128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps,** according to your network environment. The default bitrate is 2048 kpbs.
Video Payload	Select the payload type (ranging from 90 to 118) to set up the audio/video configuration file. The default payload is 104.

11.4 - DTMF data transmission configuration

To enable door access through DTMF code or some other applications you need to properly configure DTMF to establish a DTMF-based data transmission between the door phone and other intercom devices for third-party integration.
To configure the DTMF data transmission by the web interface:

Account > Advanced > DTMF



DTMF

Type RFC2833

How To Notify DTMF Disabled

Payload 101 (96~127)

Table A17 - MyBell 2-Wire 1-button Station - DTMF data transmission configuration	
Setting	**Description**
Type	Select a DTMF type from the following options: **Inband, RFC 2833, Info, Info+Inband, Info+RFC 2833.** It needs to be matched with the type adopted by the third party device for receiving signal data.
Notifying DTMF	Select from the following types: **Disabled, DTMF, DTMF-Relay, Telephone-Event.** It neeeds to be matched with the type adopted by the third party device. You need to set it up only when the third party device adopts the **Info** mode.
Payload	Set the payload according to the data transmission payload agreed on between the sender and receiver during the data transmission.

12 ACCESS TO WHITE LIST CONFIGURATION

The door phone can store up to 500 contacts, allowing access permission to the indoor monitor or other devices. The Access White List feature works for group and contact management.

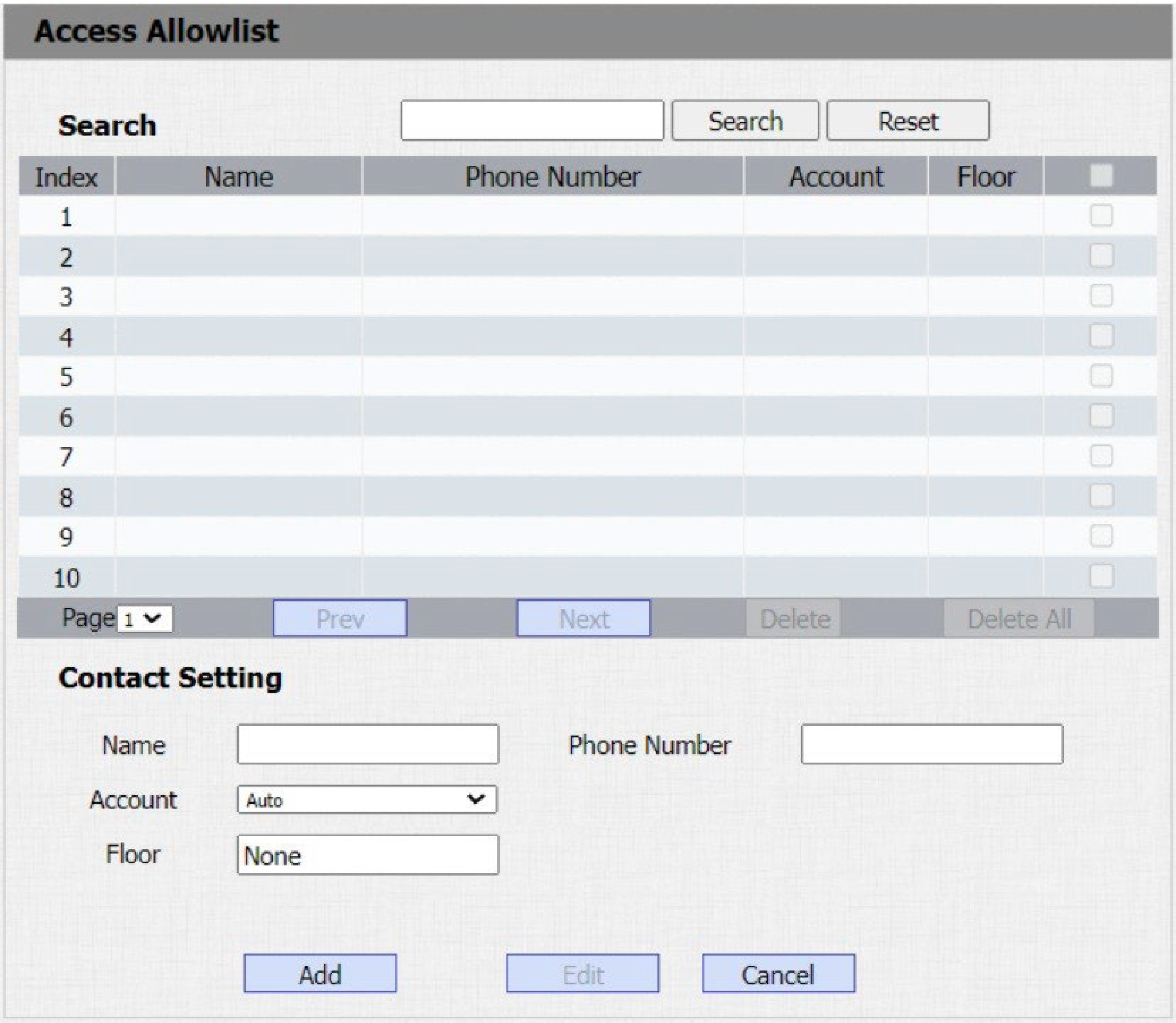
To configure the White List access feature by the web interface:

Access Control > Access Allowlist

12.1 - Managing contacts

To search, display, edit, and delete the contacts in your phone book by the web interface:

Access Control > Access Allowlist



Access Allowlist

Search

Index	Name	Phone Number	Account	Floor	□
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□
9					□
10					□

Page 1

Contact Setting

Name

Phone Number

Account: Auto

Floor: None

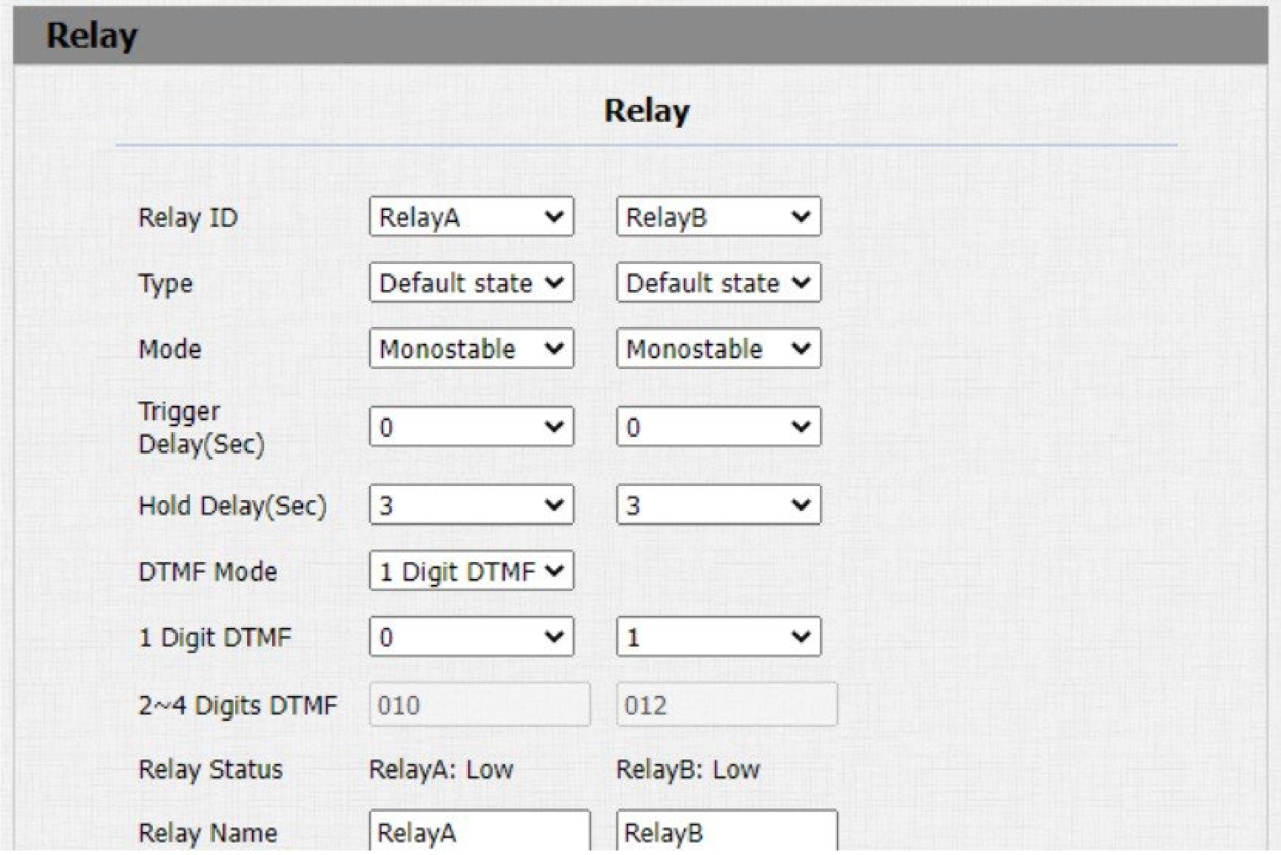
Setting:

- **Account:** select the SIP account to be used to call out. This featurte isn't available for the IP direct call.

13.1 - Relay switch configuration

To configure the relay switches and DTMF for the door access by the web interface:

Access Control > Relay



Relay

Relay

Relay ID	RelayA	RelayB
Type	Default state	Default state
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	3	3
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	0	1
2~4 Digits DTMF	010	012
Relay Status	RelayA: Low	RelayB: Low
Relay Name	RelayA	RelayB

Table A18 - MyBell 2-Wire 1-button Station - Relay switch configuration

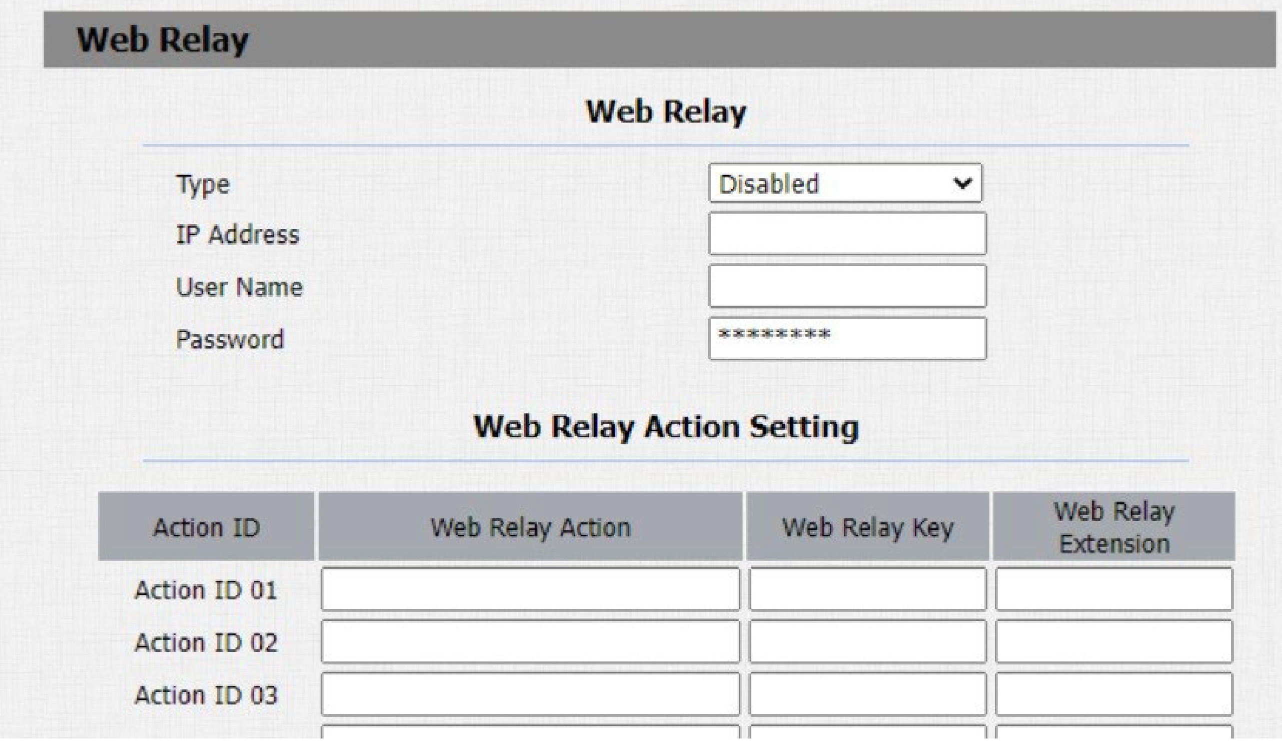
Setting	Description
Type	• **Default State Relay Status:** • **Low** – the door is closed. • **High** – the door is opened. • **Invert State Relay Status:** • **High** – the door is closed. • **Low** – the door is opened.
Mode	• **Monostable** – the relay status is reset automatically within the relay delay time after the relay is triggered. • **Bistable** – relay status is reset after the relay is triggered again.
Trigger Delay (seconds)	Set the relay trigger delay time (range: 1-10 seconds). Example: if you set the delay time to **5 seconds**, the relay is triggered 5 seconds after you press the **Unlock** tab.
Hold Delay (seconds)	Set the relay hold delay time (range: 1-10 seconds). Example: if you set the delay time to **5 seconds**, the relay resumes the initial state after maintaining the triggered state for 5 seconds.
DTMF Mode	Select the number of DTMF digits for the door access control (range: 1-4 digits). You can select **1 Digit DTMF** or **2-4 Digit DTMF** code.
1 Digit DTMF	If the **DTMF Mode** is set as **1 Digit**, configure the 1-digit DTMF code. Choose characters from: **0-9** and *****, **#**.
2~4 Digit DTMF	Set the DTMF code according to the **DMTF Mode** setting. Example: you need to set the 3-digit DTMF code if the **DTMF Mode** is set as **3 Digit**.
Relay Status	• **Low** (default) – normally closed (NC). • **High** – normally open (NO).
Relay Name	Name the relay switch as needed, for example, based on its location.

Note

- Only the external devices connected to the relay switch need to be powered by power adapters. The relay switch doesn't supply power.
- If you set the **DTMF Mode** as **1 Digit DTMF**, you can't edit the DTMF code in the **2~4 Digits DTMF** field.
  If you set the **DTMF Mode** as **2-4** in **2~4 Digits DTMF**, you can't edit the DTMF code in the **1 Digit DTMF** field.

13.2 - Web relay configuration

You can control the door access using the network-based web relay on the device and by the device web interface.
Web relay needs to be configured by the web interface.
To configure the web relay by the web interface:
Access Control > Web Relay
IP Address, **User Name** and **Password** are provided by the web relay manufacturer.



Web Relay

Web Relay

Type: Disabled

IP Address

User Name

Password: ********

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01			
Action ID 02			
Action ID 03			

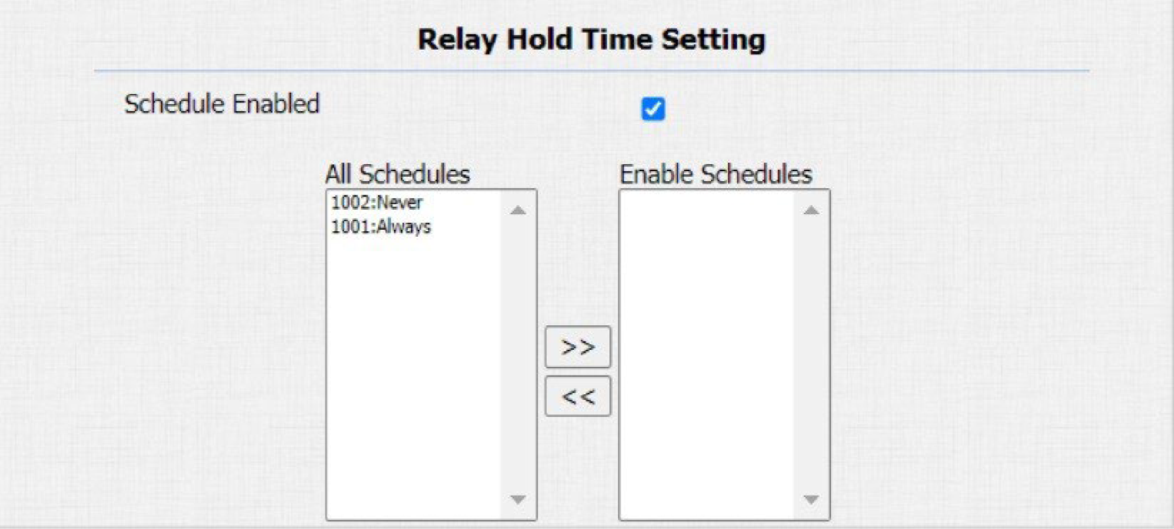
Table A19 - MyBell 2-Wire 1-button Station - Web relay configuration	
Setting	**Description**
Type	Select from the three options: • **Web relay** – enable the web relay. • **Disabled** – disable the web relay. • **Both** – enable both local relay and web relay.
Password	The password is authenticated through HTTP and you can define the passwords using **http get** option in **Action**.
Web Relay Action	Enter the specific **Web Relay Action** command provided by the web manufacturer for different actions by the web relay. Without adding the IP, username and password, you can enter the HTTP command in the **Web Relay Action** to configure multiple web relays. See the HTTP command examples below: • If you don't enter the IP address in the **IP Address** field, enter the complete HTTP command, for exaple: Http://admin:admin@192.168.1.2/state.xml?relayState=2. (HTTP://:@IP address>/state.xml?relayState=2) • If you entered the IP address in the **IP Address** field, enter the omitted HTTP command, for example: state.xml?relayState=2.
Web Relay Key	It can be null or you can enter the configured DTMF code. When the door is unlocked by the DTMF code, the action command is sent to the web relay automatically.
Web Relay Extension	It can be null or you can enter the relay extension information. That can be an SIP Account username of an intercom device such as an indoor monitor, so that the specific action command is sent when **Unlock** is performed on the intercom device. This setting is optional.

13.3 - Door access schedule management

Configure and make a schedule for the user-based door access using RF card, Private PIN, and Facial recognition.

13.3.1 - Relay schedule configuration

Set the specific relay as always open at a set time. This feature is designed for some specific scenarios, for example, the time after school, or morning work time.
To configure the relay schedule by the web interface:
Access Control > Relay > Relay Hold Time Setting



Relay Hold Time Setting

Schedule Enabled ☑

All Schedules: 1002:Never, 1001:Always

Enable Schedules:

Setting:

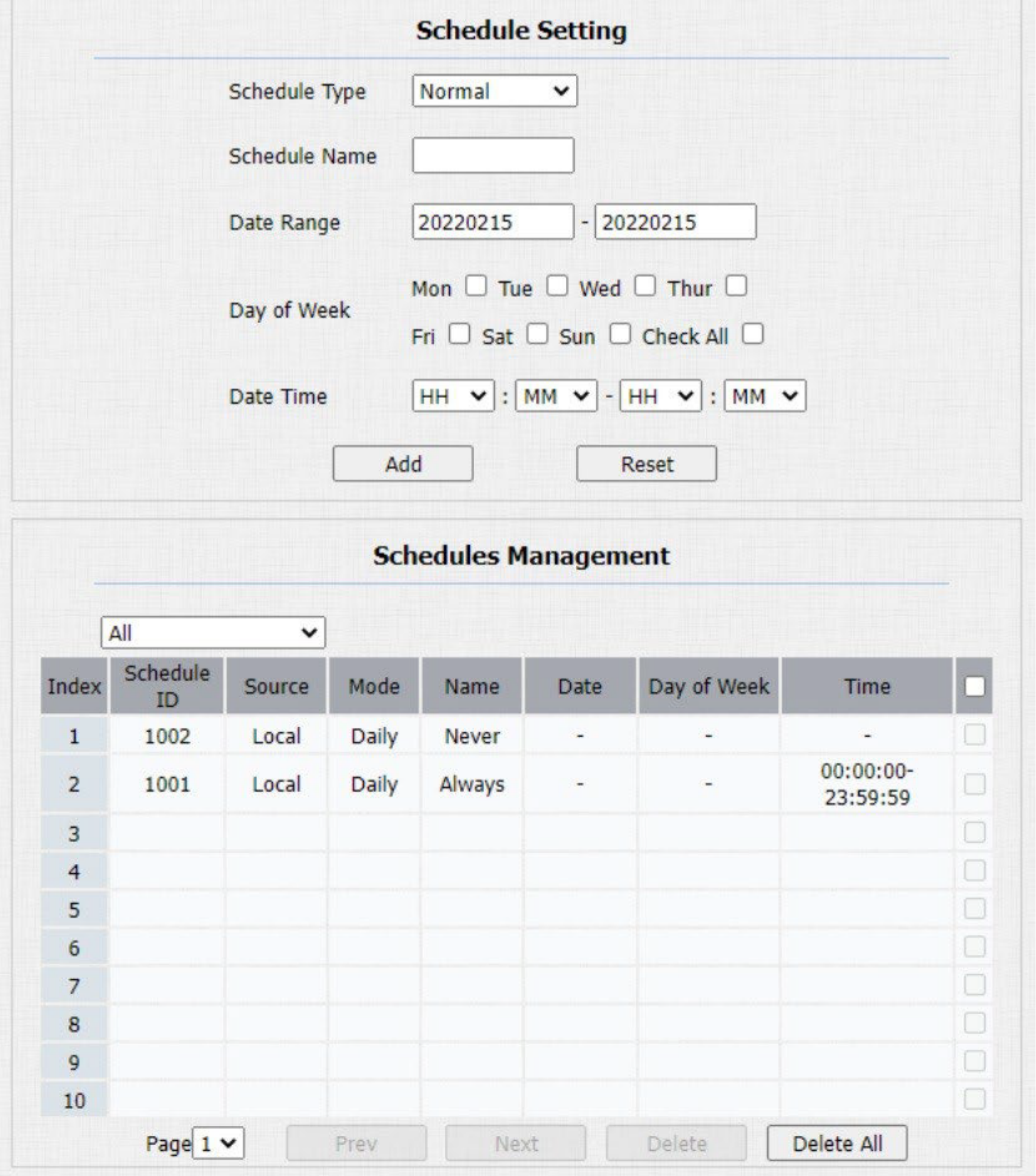
- **Schedule Enabled:** it is disabled by default. Enable it only to select the schedule. For creating the schedule, please refer to door access schedule configuration.

13.3.2 - Creating door access schedule

You can create the daily or weekly door access schedule as well as a schedule that allows you to plan door access for a longer time.

To create the door access scheduele by the web interface:

Setting > Schedules



Schedule Setting

Schedule Type: Normal

Schedule Name:

Date Range: 20220215 - 20220215

Day of Week: Mon □ Tue □ Wed □ Thur □ Fri □ Sat □ Sun □ Check All □

Date Time: HH : MM - HH : MM

Schedules Management

All

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	□
1	1002	Local	Daily	Never	-	-	-	□
2	1001	Local	Daily	Always	-	-	00:00:00-23:59:59	□
3								□
4								□
5								□
6								□
7								□
8								□
9								□
10								□

Page 1

Settings:

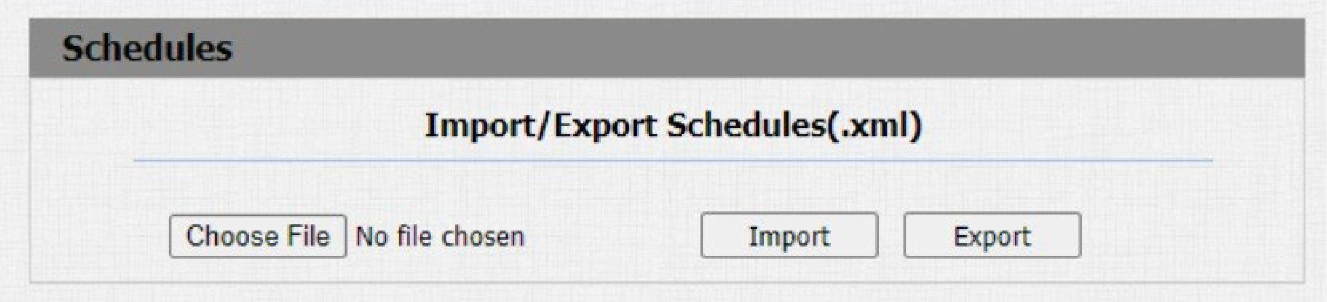
- **Mode:** choose from the three time periods: **Daily**, **Weekly**, and **Normal**. The default mode is **Daily**.
- **Day:** set the corresponding day of the week. This configuration is only displayed when the **Week** or **Normal** type is selected.

13.3.3 - Import and export door access schedule

You can import or export the schedules to maximize the door access schedule management efficiency.

To import or export the door access scheduele by the web interface:

Setting > Schedules > Import/Export Schedule(.xml)

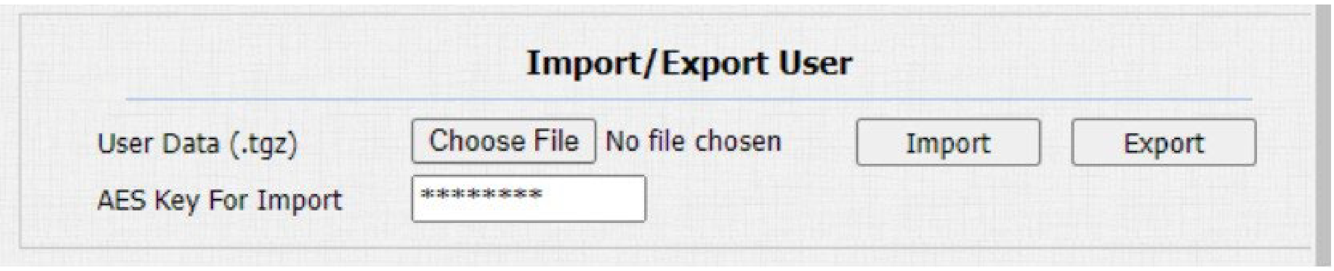


13.4 - Import and export user data

The door phone supports User Data of access control to be shared among the MyBell door phones through import and export. You can also export the facial data out of the door phone and then import it to a third-party device.

To import or export the user data by the web interface:

Access Control > User



User Data (.tgz)

AES Key For Import ********

Setting:

- **AES Key For Import:** enter the AES code before importing the AES-encrypted **.tgz** file to the door phone.

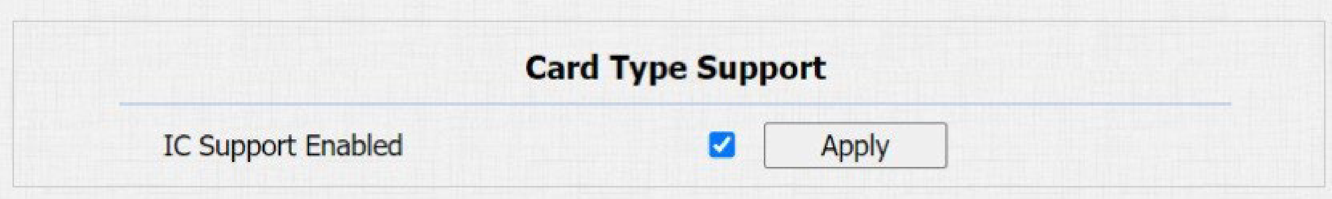
14 DOOR UNLOCK CONFIGURATION

This door phone enables three types of door access: using PIN code, RF card, and Facial recognition. You can configure them on the device and by the web interface or you can import or export the configured files to maximize the RF card configuration efficiency.

14.1 - IC card control configuration

To configure the IC card control by the web interface:

Access Contol > Card Setting > Card Type Support



Card Type Support

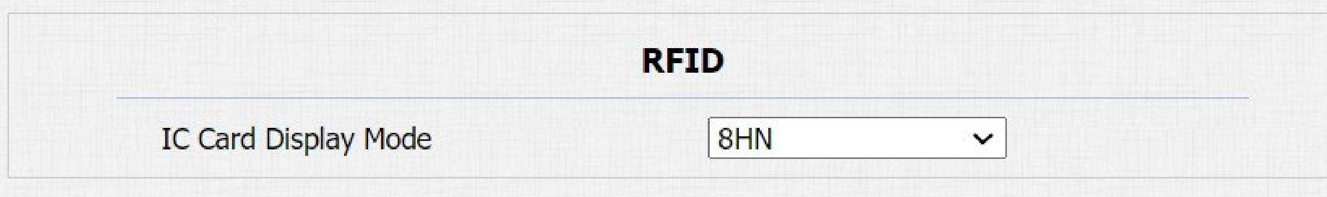
IC Support Enabled ☑ Apply

14.2 - Access card format configuration

To integrate the RF card door access feature with the third-party intercom system, change the RF card code format to identical to that applied in the third-party system.

To configure the access card format by the web interface:

Intercom > Card Setting



RFID

IC Card Display Mode: 8HN

Setting:

- **IC Card Display Mode:** Select the card code format of the IC card for the door access from the following format options: **8H10D, 6H3D 5D(W26), 6H8D, 8HN, 8HR, 6H3D 5D-R(W26), 8HR10D**.
  The default card code format in the door phone is **8HN**.

14.3 - RF card for door unlock configuration

To manage the card number and corresponding parameters by the web interface:

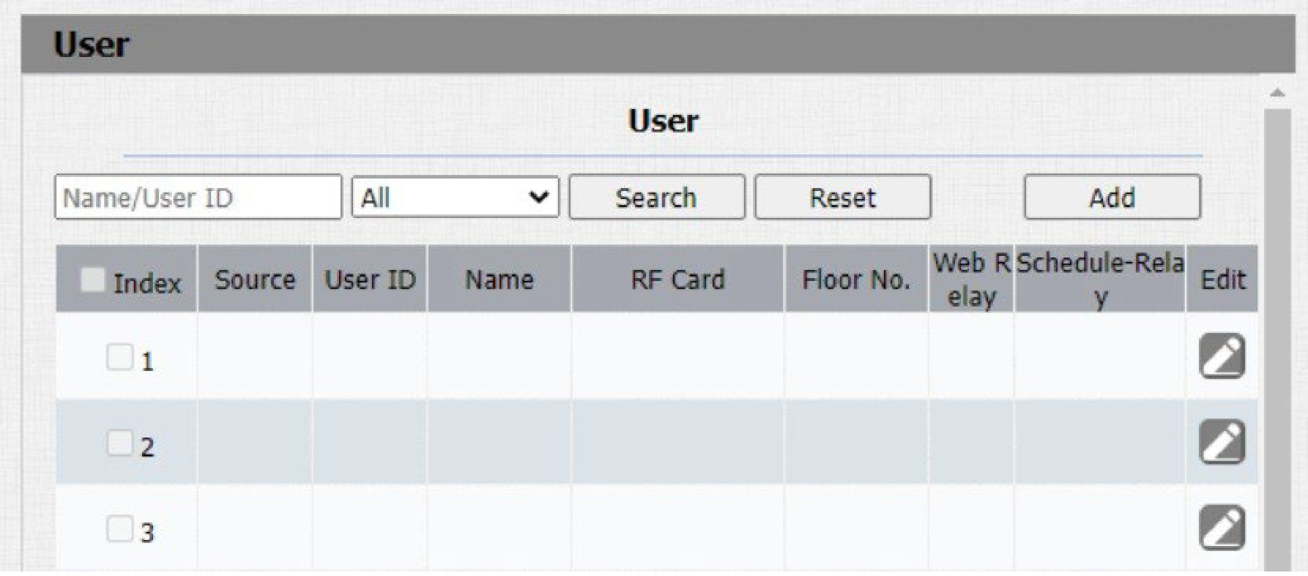
Intercom > Card Setting

14.4 - RF card configuration by web interface

You can tap the RF card on the reader and click **Obtain** to add RF card for the user.

To configure the RF card by the web interface:

Access Control > User

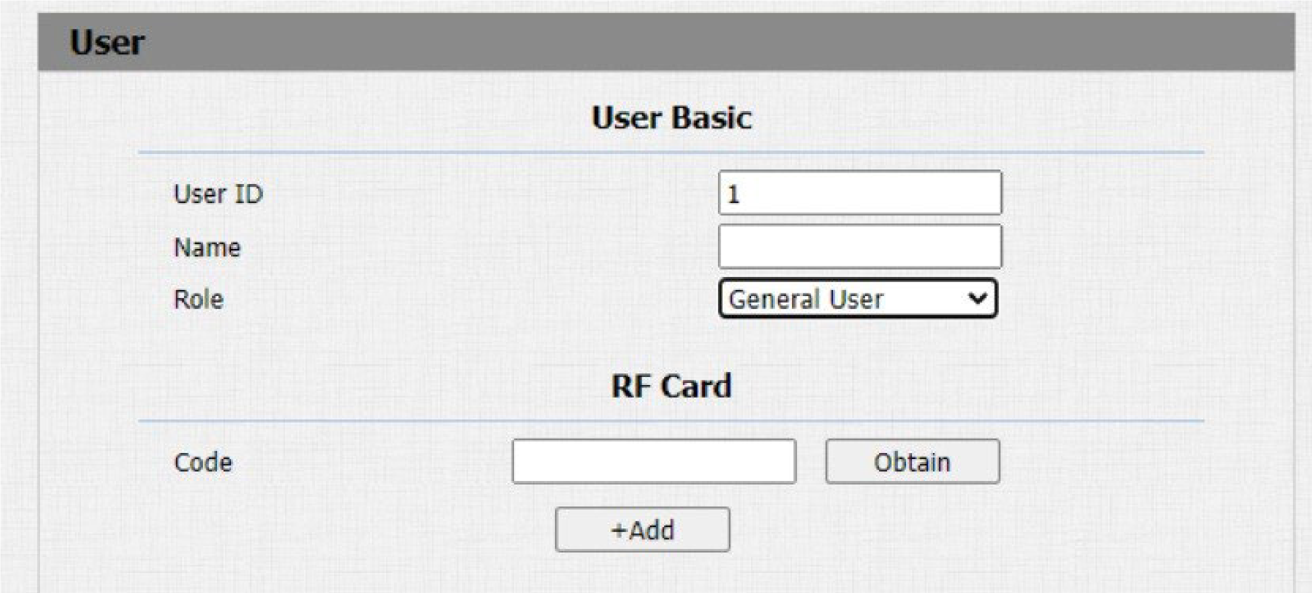


User

User

Name/User ID | All | Search | Reset | Add

□ Index	Source	User ID	Name	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
□ 1								✎
□ 2								✎
□ 3								✎



User ID: 1

Name:

Role: General User

Code:

Table A20 - MyBell 2-Wire 1-button Station - RF card configuration	
Setting	**Description**
User ID	The **User ID** can be maximum 11 digits long and can't be reused for other users. The **User ID** can be generated automatically or manually.
Role	Select **General Users** for the residents and **Administrator** for the administrator.
Code	Tap the card on the reader area and click **Obtain**.

Note

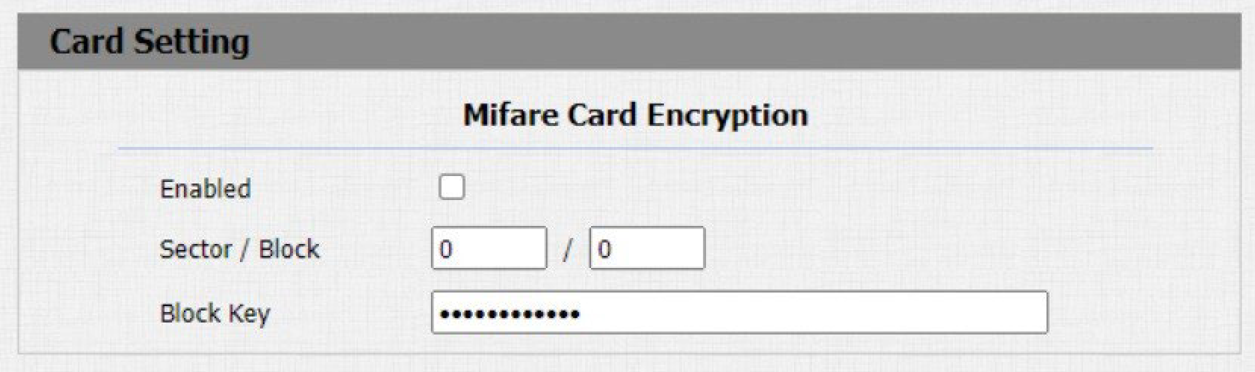
- RF cards with 13.56 MHz frequency can be used for door access on the door phone.

14.5 - Mifare card encryption configuration

The door phone can read the encrypted Mifare cards for greater security.

To encrypt the Mifare card by the web interface:

Access Control > Card setting > Mifare/Defire Card Encryption



Enabled ☐

Sector / Block: 0 / 0

Block Key: •••••••••••••

Settings:

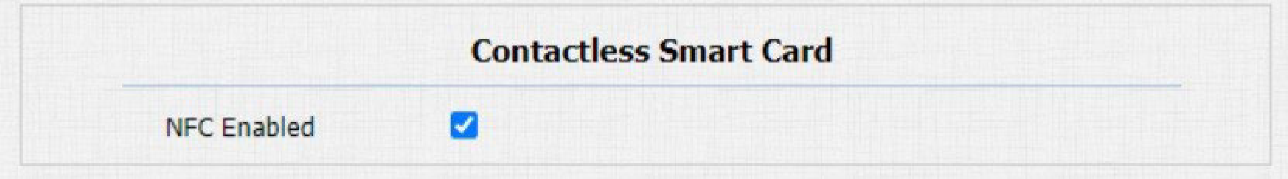
- **Sector/Block:** enter the sector and block that you want the card number to be written into for the Mifare card. For example, you can write the card number into sector 3 and block 3 in the card.
- **Block Key:** enter the block password for access.

14.6 - NFC function configuration

Near Field Communication (NFC) uses radio waves for data transmission interaction and can enable door access. Place the mobile phone close to the door phone to unlock the door.

To configure the NFC card by the web interface:

Intercom > Card Setting



NFC Enabled ☑

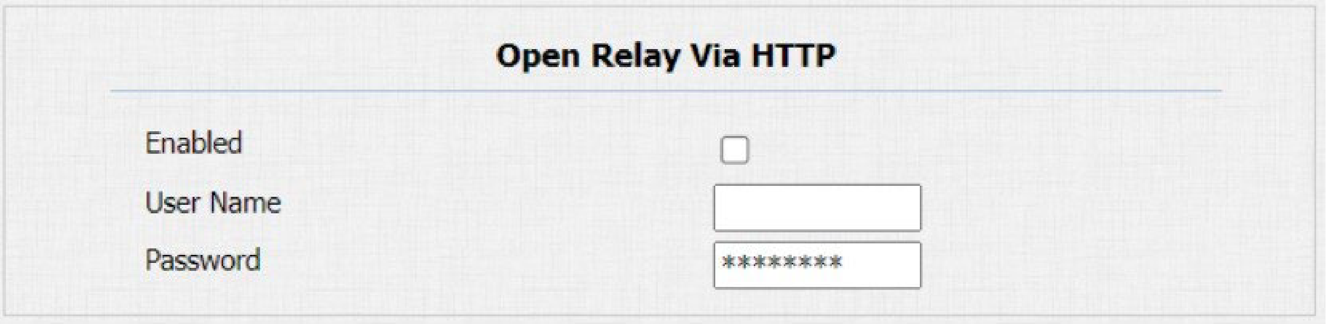
Note

- **NFC Enabled**: NFC feature is enabled by default. The device must be connected to Yubii Home for the NFC application.

14.7 - Open relay configuration through HTTP for door access

To unlock the door remotely, type in the created HTTP command (URL) in the web browser to trigger the relay.
To configure open relay through HTTP by the web interface:

Access Control > Relay > Open Relay Via HTTP



Open Relay Via HTTP

Enabled	□
User Name	
Password	*********

Settings:

- **User Name:** enter the username of the device web interface. Example: **admin**.
- **Password:** enter the password for the HTTP command. Example: **12345**.

Please refer to the following example:

http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

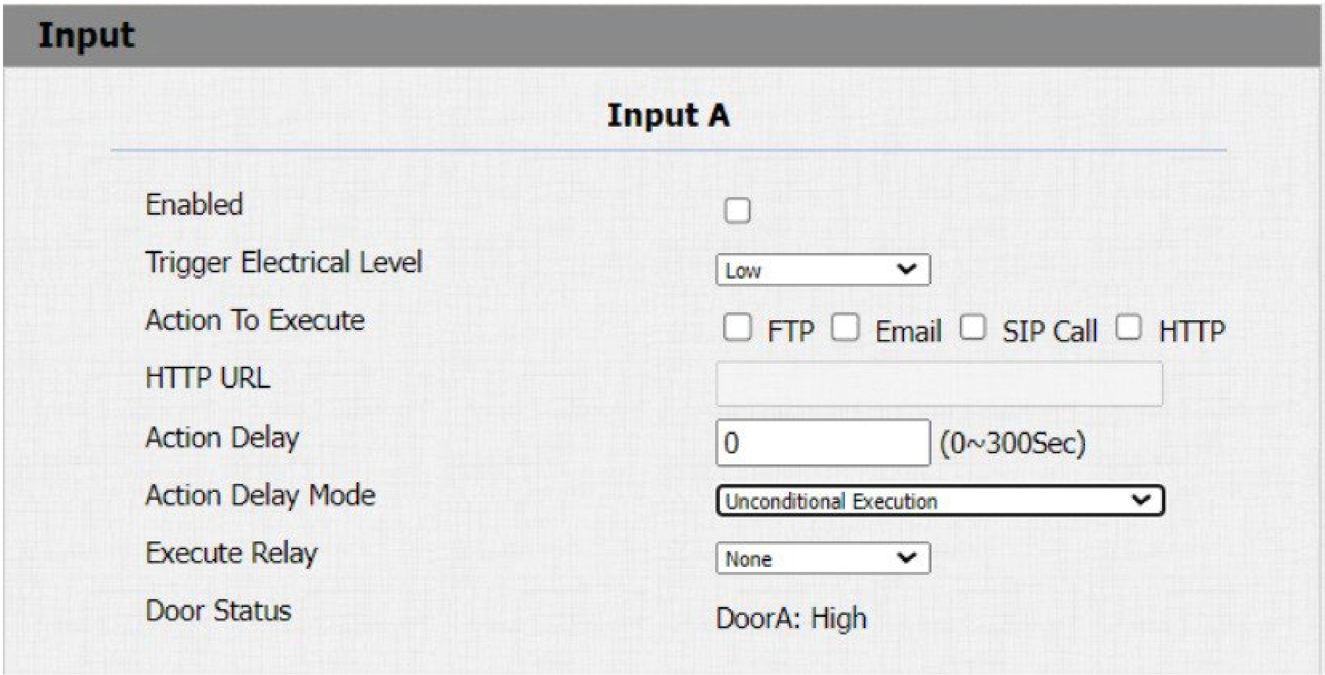
Note

- **DoorNum** in the HTTP command above refers to the number of the relay to be triggered for the door access, in this case, relay 1.

14.8 - Exit button for door unlock configuration

To open the door from the inside using the **Exit** button installed by the door, configure the door phone input to trigger the relay for the door access.
To configure the exit button for door unlock by the web interface:

Access Control > Input



Input

Input A

Enabled	□
Trigger Electrical Level	Low
Action To Execute	□ FTP □ Email □ SIP Call □ HTTP
HTTP URL	
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution
Execute Relay	None
Door Status	DoorA: High

Table A21 - MyBell 2-Wire 1-button Station - Exit button for door unlock configuration

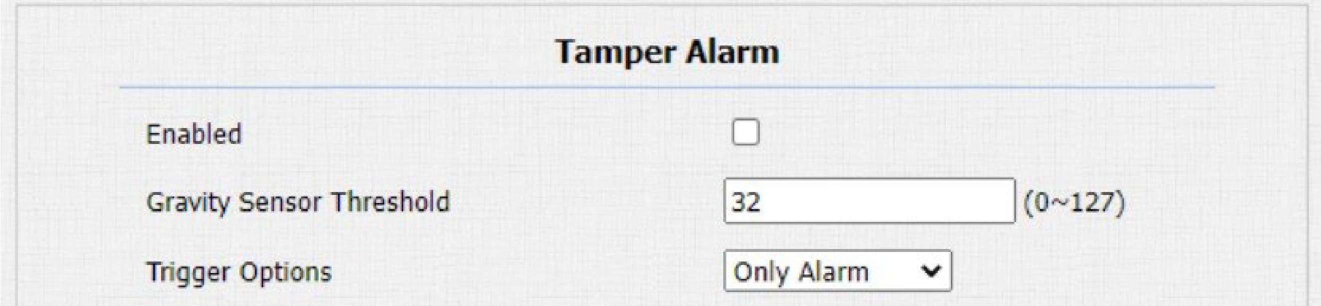
Setting	Description
Trigger Electrical Level	Select the **Trigger Electrical Level** option from **High** and **Low**, according to the operation on the exit button.
Action To Execute	Select the method to carry out the action from the following options: **FTP**, **Email, HTTP**, **TFTP**.
HTTP URL	If you select **HTTP** to carry out the action, enter the URL.
Action Delay	Set up the delay time for the action execution. For example, if you set the action delay time to 5 seconds, the corresponding action is carried out 5 seconds after pressing the button.
Action Delay Mode	• **Unconditional Execution** –the action is carried out when the input is triggered. • **Execute If Input Still Triggered** – the action is carried out if the input stays triggered. For example, if the door stays open after triggering input, an action such as an email is sent to notify the receiver.
Execute Relay	Set up the relays to be triggered by the actions.

15.1 - Tamper alarm configuration

The tamper alarm function protects against unauthorized removal of devices. It triggers an alarm and sends calls to a designated location. If the door phone gravity value changes from its original setup during installation, the tamper alarm is triggered.

To configure the tamper alarm by the web interface:

Security > Basic > Tamper Alarm



Tamper Alarm

Enabled	□
Gravity Sensor Threshold	32 (0~127)
Trigger Options	Only Alarm

Settings:

- **Trigger Options:** select the options to be activated when the gravity sensor is triggered.

15.2 - Client certificate configuration

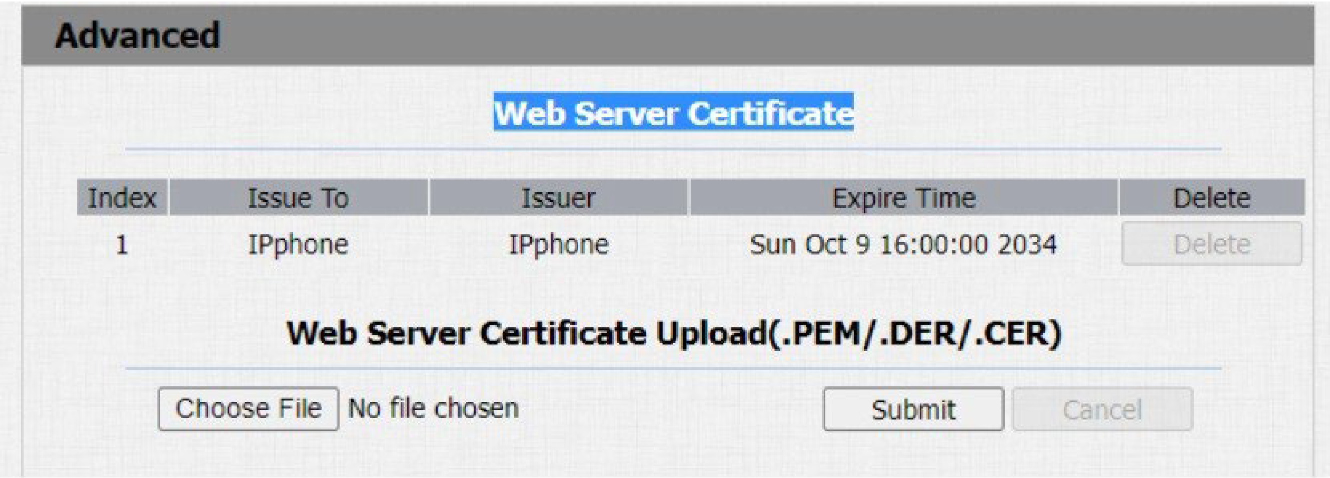
Certificates can ensure communication integrity and privacy when deploying the door phones. When the user needs to establish the SSL protocol, it is necessary to upload corresponding certificates for verification.

15.2.1 - Web Server certificate

This certificate is sent to the client for authentication when the client requires an SSL connection with the door phone. Currently, the certificate format accepted by the door phone is a **.pem** file.

To upload the Web Server certificate by the web interface:

Security > Advanced > Web Server Certificate



Advanced

Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

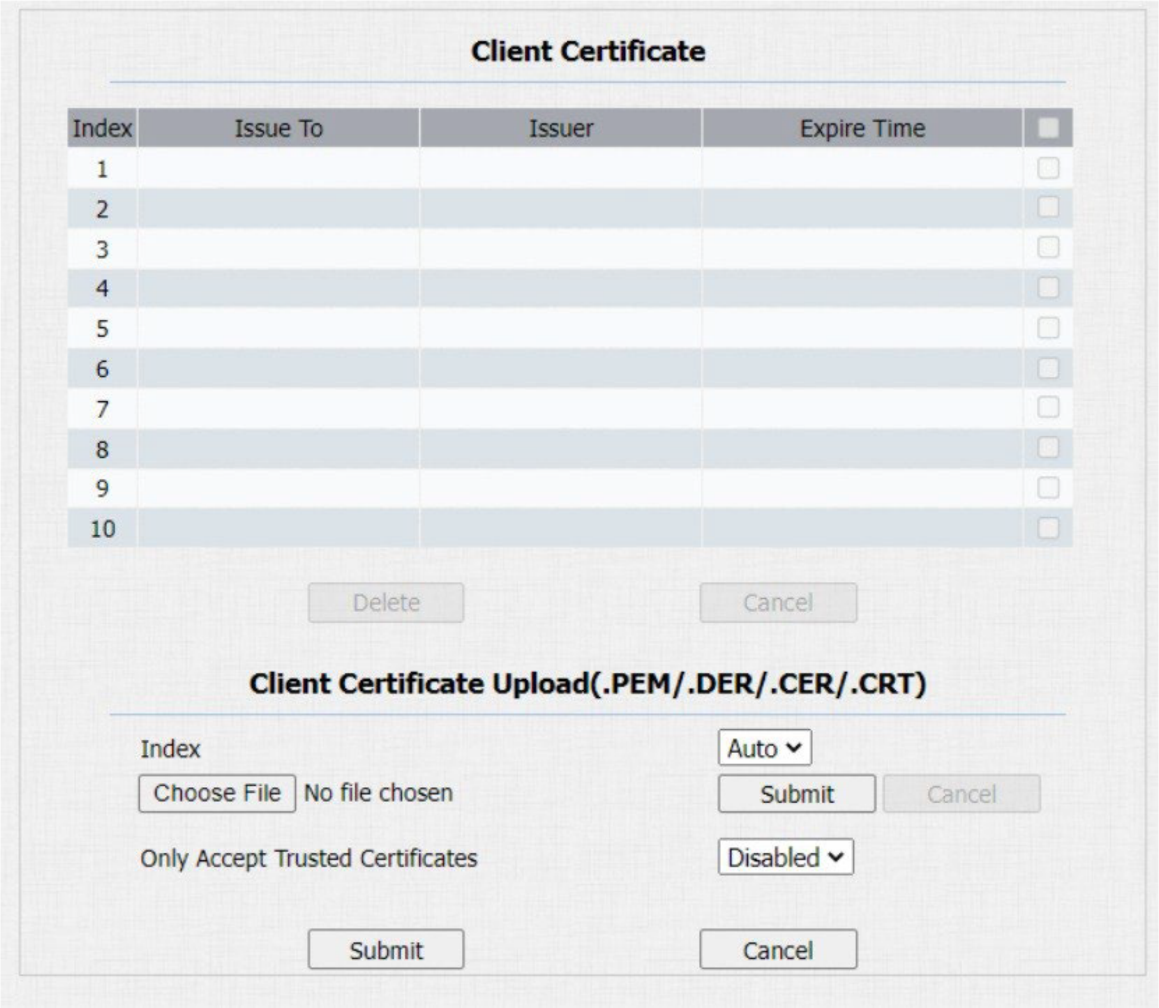
Web Server Certificate Upload(.PEM/.DER/.CER)

15.2.2 - Client certificate configuration

When the door phone requires an SSL connection with the server, the phone must verify the server to make sure it can be trusted. The server sends its certificate to the door phone. Then the door phone verifies this certificate according to the client certificate list.

To upload and configure the client certificates by the web interface:

Security > Advanced > Web Server Certificate



Client Certificate

Index	Issue To	Issuer	Expire Time	□
1				□
2				□
3				□
4				□
5				□
6				□
7				□
8				□
9				□
10				□

Client Certificate Upload(.PEM/.DER/.CER/.CRT)

Index: Auto

Choose File No file chosen

Only Accept Trusted Certificates: Disabled

Table A22 - MyBell 2-Wire 1-button Station - Client certificate configuration	
Setting	**Description**
Index	Select the desired value from the drop-down Index list. • **Auto** value – the uploaded certificate is displayed in numeric order. • Value from **1 to 10** – the uploaded certificate is displayed according to the seleced value.
Select File	Click **Choose file** to browse the local drive and locate the desired certificate (**.pem** files only).
Only Accept Trusted Certificates	• **Enabled** – if the authentication is successful, the phone verifies the server certificate based on the client certificate list. • **Disabled** – the phone doesn't verify the server certificate, whether the certificate is valid or not.

15.3 - Motion detection

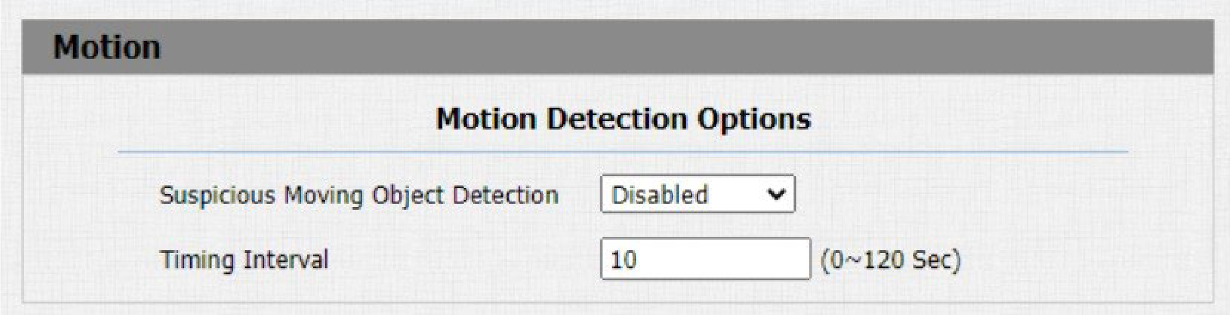
Motion detection is commonly used for unattended surveillance video and automatic alarms. The CPU compares images collected by the camera at different frame rates using a specific algorithm. If there is a change in the picture, such as someone walking by or the lens moving, the calculation and comparison result exceeds the threshold. It indicates that the processing is automatic.

15.3.1 - Motion detection configuration

When the motion detection action is triggered, you can set up the motion detection time interval, sensitivity and notification type by the web interface:

To configure the motion detection by the web interface:

Surveillance > Motion > Motion Detection Options

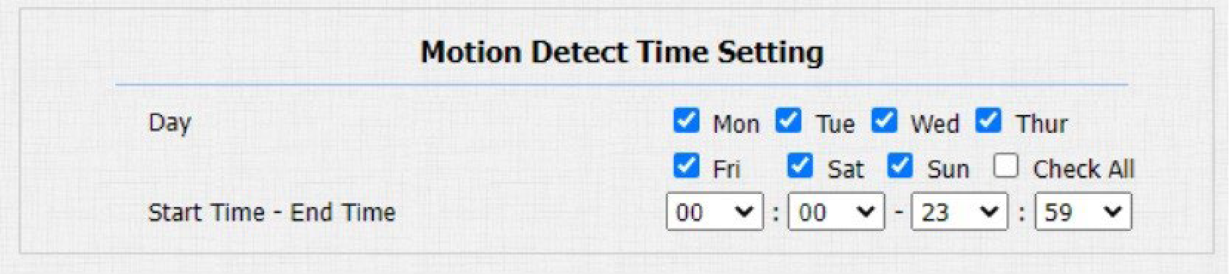


Motion

Motion Detection Options

Suspicious Moving Object Detection: Disabled

Timing Interval: 10 (0~120 Sec)



Motion Detect Time Setting

Day ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun □ Check All

Start Time - End Time 00 : 00 - 23 : 59

Settings:

- **Suspicious Moving Object Detection:**
  - **Disabled** – disable the motion detection.
  - **IR detection** – enable the IR sensor-based motion detection for the suspicious moving objects.
  - **Video detection** – enable the video-based motion detection during the monitoring for the suspicious moving object.
- **Time Interval:** set the time interval for the motion detection. If you set the time interval to 10 seconds, the motion detection time span is 10 seconds.
  Example: 10-second time interval is set and the first captured movement is the starting point of the motion detection. If the movement begins in the 7th second of the 10-second interval, the alarm is triggered in the 7th second (the first trigger point). Motion detection action (sending out the notification) can be triggered anytime between the 7th and 10th second. The 10-second interval is a complete cycle of the motion detection. The first trigger point can be calculated as **Time interval minus three**.

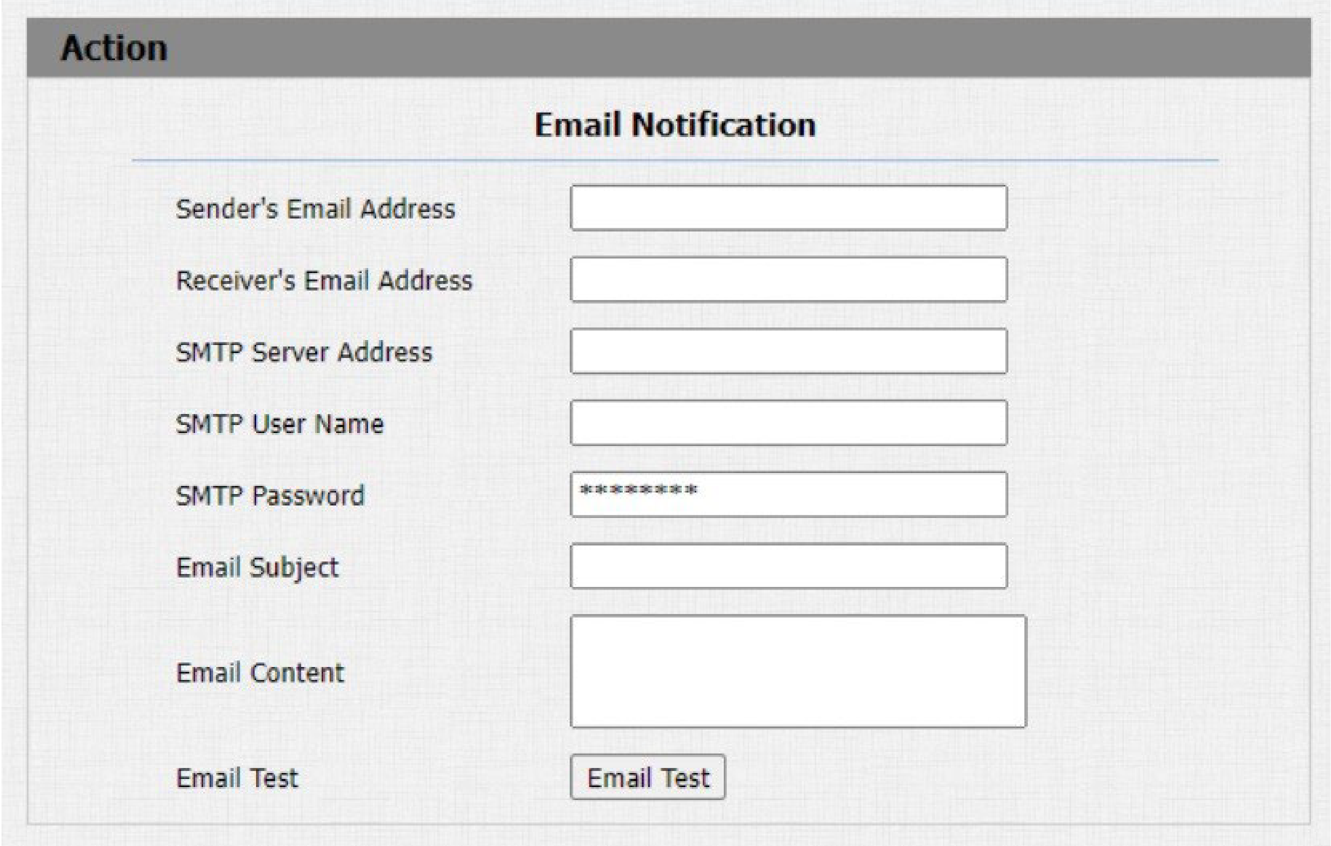
15.4 - Security notification configuration

15.4.1 - Email notification configuration

To receive the security notification by email you need to configure the email notification by the web interace. The email notification shows as captures.

To configure the email notification by the web interface:

Setting > Action > Email Notification



Action

Email Notification

Sender's Email Address

Receiver's Email Address

SMTP Server Address

SMTP User Name

SMTP Password ********

Email Subject

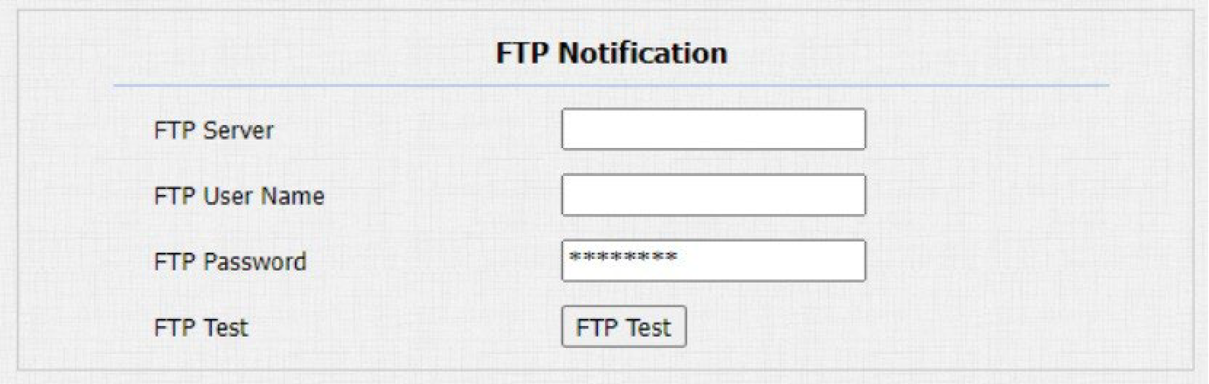
Email Content

Email Test

Table A23 - MyBell 2-Wire 1-button Station - Email notification configuration	
Setting	**Description**
Sender's email address	Enter the sender email address from which the email notification is sent.
Receiver's Email Address	Enter the receiver email address.
SMTP Server Address	Enter the SMTP server address of the sender.
SMTP User Name	Enter the SMTP username, it's usually the same as the sender email address.
SMTP Password	Configure the SMTP service password, it's the same as the sender email password.
Email Test	Click the **Email Test** button to test if you can receive the Email.

15.4.2 - FTP notification configuration

To receive the security notifications through FTP, configure the FTP notifications by the web interface:
Setting > Action > FTP Notification



FTP Notification

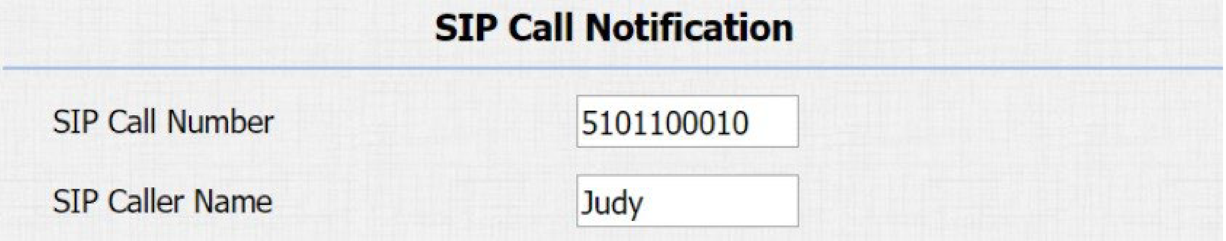
FTP Server	
FTP User Name	
FTP Password	*********
FTP Test	FTP Test

Settings:

- **FTP Server:** enter the URL address of the FTP server for the FTP notification.
- **FTP Test:** click the **FTP Test** button to run the test and see if the FTP notification can be sent and received by the FTP server.

15.4.3 - SIP call notification configuration

When the feature action is triggered, you can also use the door phone to make an SIP call.
To configure the SIP call notifications by the web interface:
Setting > Action > SIP Call Notification

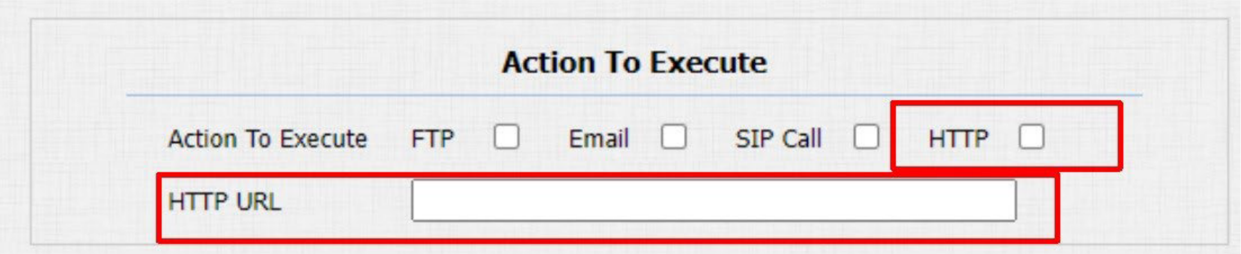


SIP Call Notification

SIP Call Number	5101100010
SIP Caller Name	Judy

15.4.4 - HTTP URL notification configuration

The door phone supports sending the HTTP notifications to the third party when specific features are enabled.
To configure the HTTP URL notification by the web interface:
Surveillance > Motion > Motion Detection Options



Action To Execute

Action To Execute FTP □ Email □ SIP Call □ HTTP □

HTTP URL

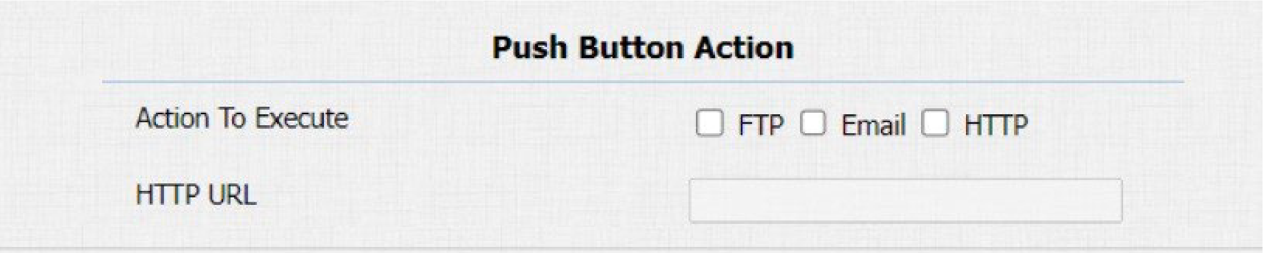
Setting:

- **HTTP:** tick this checkbox to enable HTTP URL notification.
- **HTTP URL:** if you choose the HTTP mode, enter the URL in the following format: **http://http server IP address/any information**.

15.5 - Security action configuration

15.5.1 - Pushbutton action configuration

Pressing the pushbutton triggers the preconfigured action type on the door phone. The notification can be sent out by Email, FTP notification or SIP call.
To configure the pushbutton action by the web interface:
Intercom > Basic



Push Button Action

Action To Execute □ FTP □ Email □ HTTP

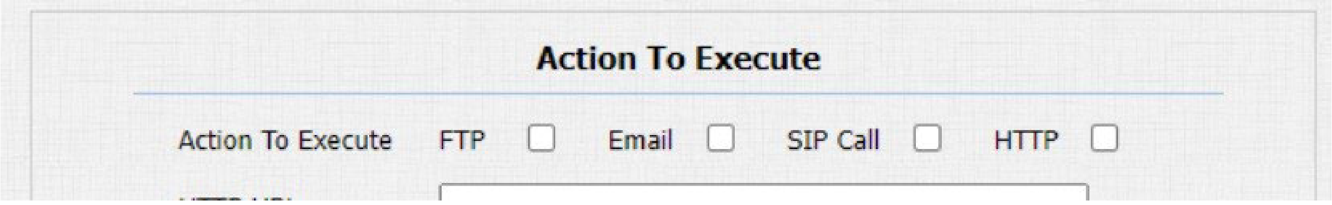
HTTP URL

Setting:

- **Action To Execute:** choose which action is executed after triggering.

15.5.2 - Motion action configuration

When the **Motion Detection** feature is working, you can set it to trigger an action.
To configure the motion action by the web interface:
Surveillance > Motion



Action To Execute

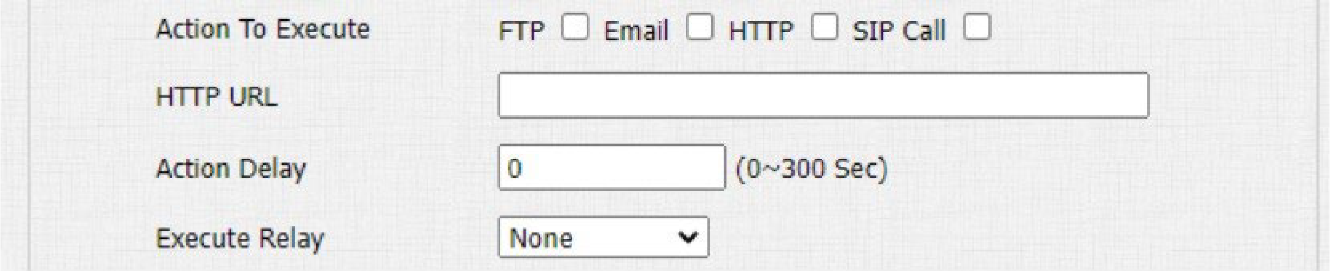
Action To Execute FTP □ Email □ SIP Call □ HTTP □

Setting:

- **Action To Execute:** choose which action is executed after triggering.

15.5.3 - Input action configuration

Working input interface can trigger an action.
To configure the input action by the web interface:
Access Control > Input



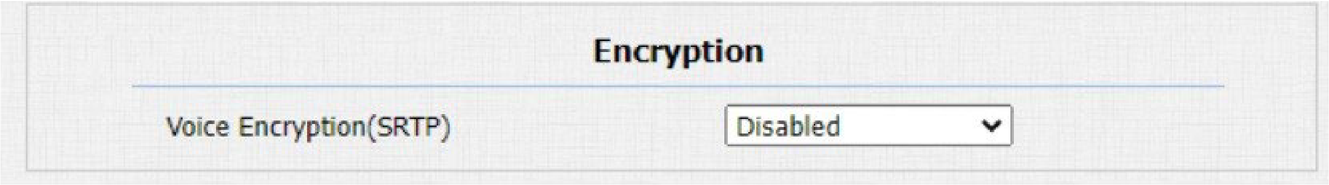
Action To Execute	FTP □ Email □ HTTP □ SIP Call □
HTTP URL	
Action Delay	0 (0~300 Sec)
Execute Relay	None

Setting:

- **Action to Execute:** choose which action is executed after triggering.
- **Action Delay Mode:**
  - **Unconditional Execution** – the action is carried out when the input is triggered.
  - **Execute If Input Still Triggered** – the action is carried out if the input stays triggered. For example, if the door stays open after triggering input, an action such as an email is sent to notify the receiver.

15.6 - Voice encryption

Secure Real-time Transport Protocol (SRTP) is a protocol defined on the basis of Real-time Transport Protocol (RTP). The data of the transmission protocol provides encryption, message authentication, integrity assurance and replay protection.
To configure voice encryption by the web interface:
Account > Advanced > Encryption



Encryption

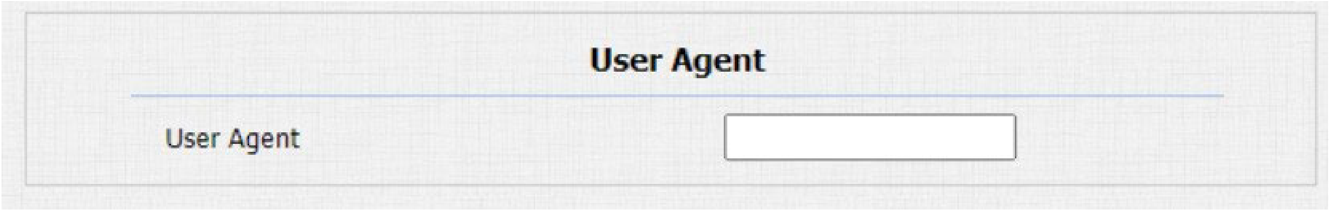
Voice Encryption(SRTP) Disabled

Setting:

- **Voice Encryption (SRTP):** choose **Disabled**, **Optional** or **Compulsory** for SRTP. If it's **Optional** or **Compulsory**, the voice during the call is encrypted, and you can grab the RTP packet to view.

15.7 - User agent

User agent is used for the identification purpose during the analysis on the SIP data packet.
To configure the user agent by the web interface:
Account > Advanced > User Agent



User Agent

User Agent

Setting:

- **User Agent:** enter another specific value, the default value is the brand name.

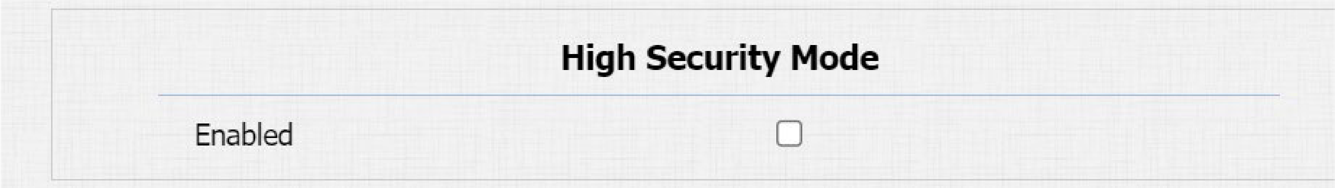
15.8 - High security mode

The high security mode is designed to enhance the security. For example, it optimizes the password storage method.

Please note that once this mode is enabled, you can't downgrade the device from the version with this mode to an old one without it.

To configure the high security mode by the web interface:

Security > Basic > High Security Mode



High Security Mode

Enabled □

Important notes

1. This mode is disabled by default when the device is upgraded to a new version with high security from an older version without the high security mode. However, if the device is reset to its factory settings, this mode is enabled by default.
2. Enabling this mode makes the old version tools unusable. To continue using them, you need to upgrade them to the following versions:
   - PC Manager: 1.2.0.0.
   - IP Scanner: 2.2.0.0.
   - Upgrade Tool: 4.1.0.0.
   - SDMC: 6.0.0.34.
3. The supported HTTP format varies depending on whether the high secure mode is enabled or disabled.
   - When the mode is turned on, the device only supports new HTTP formats for door opening.
     - http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
     - http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
   - When the mode is off, the device supports the above two new formats as well as the old one:
     - http://deviceIP/fcgi/do?ction=OpenDoor&UserName=username&Password=password&DoorNum=1
4. You can't import or export **.tgz** format configuration files between a new version device and an old version device without the high security mode.

16.1 - RTSP stream monitoring

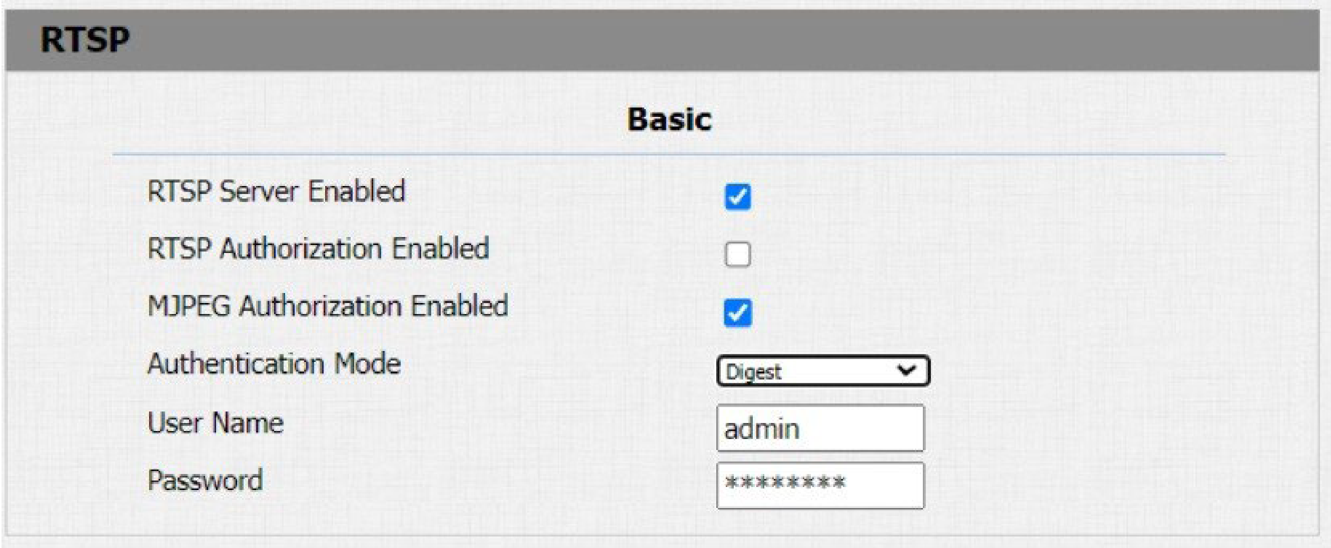
The door phones support the RTSP stream. It enables intercom devices, such as indoor monitors or third-party monitoring units, to monitor or obtain the real-time audio/video (RTSP stream) from the door phone using the correct URL.

16.1.1 - RTSP basic configuration

Before using this function, you need to set up the RTSP function in terms of RTSP Authorization.

To configure the RTSP by the web interface:

Surveillance > RTSP > RTSP Basic



RTSP

Basic

RTSP Server Enabled ☑

RTSP Authorization Enabled □

MJPEG Authorization Enabled ☑

Authentication Mode: Digest

User Name: admin

Password: *********

Settings:

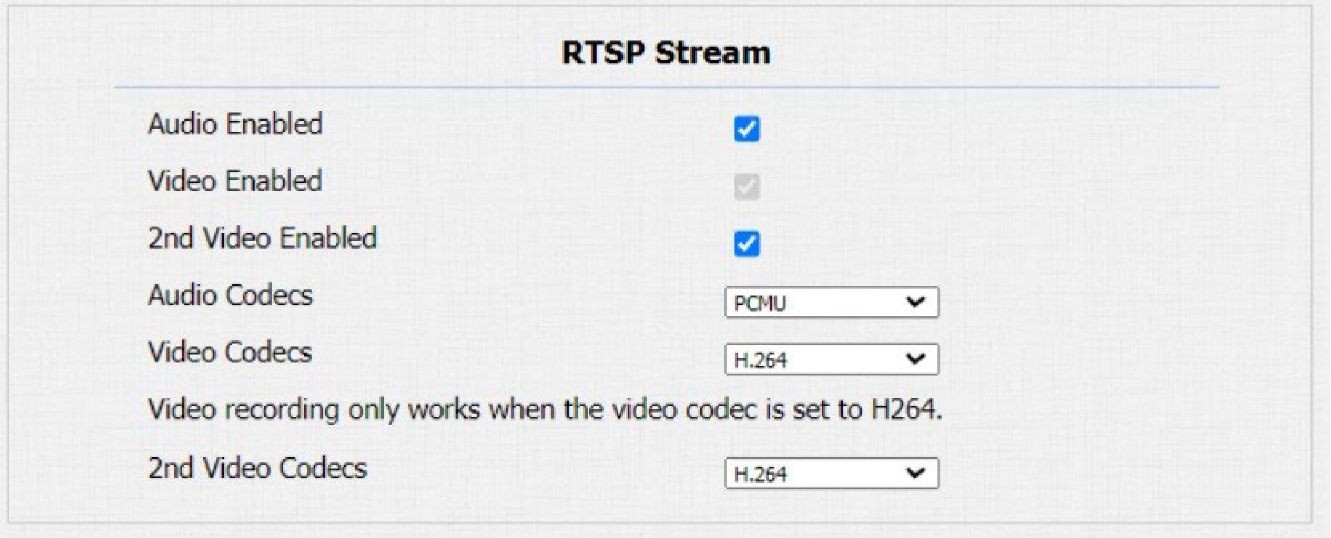
- **RTSP Server Enable:** tick this checkbox to turn on the RTSP function, and untick it to turn it off.
- **RTSP Authorization Enabled:** if enabled, you need to enter **RTSP Authentication Mode**, **RTSP User Name** and **RTSP Password** for authorization on the intercom device such as indoor monitor.
- **RTSP Authentication Mode:** select the RTSP authentication mode from: **Basic** and **Digest**. The default authentication mode is **Basic**.

16.1.2 - RTSP stream configuration

You can select the video codec for the RTSP stream and configure features such as video resolution and bitrate for H.264 codec based on your network environment.

To configure the RTSP stream by the web interface:

Surveillance > RTSP > RTSP stream



RTSP Stream

Audio Enabled ☑

Video Enabled ☑

2nd Video Enabled ☑

Audio Codecs: PCMU

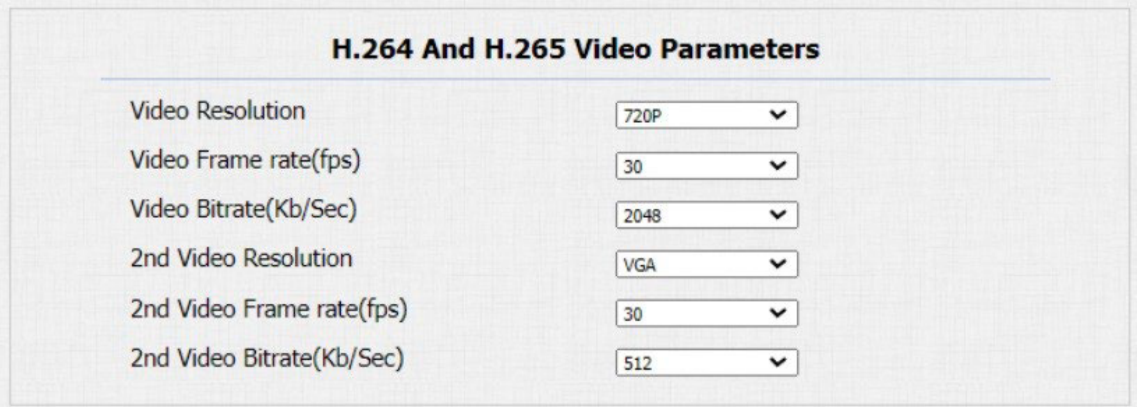
Video Codecs: H.264

Video recording only works when the video codec is set to H264.

2nd Video Codecs: H.264

Table A24 - MyBell 2-Wire 1-button Station - RTSP stream configuration

Setting	Description
Audio Enabled	Tick to enable RTSP audio so that the door phone can also send audio information to the monitor by RTSP.
Video Enabled	After enabling the RTSP feature, the video RTSP is enabled by default and can't be modified.
2nd Video Enabled	The door phones support 2 RTSP streams, you can enable the second one here.
Audio Codec	Choose a suitable audio codec for RTSP audio.
Video Codec	Choose a suitable video codec for RTSP video.



H.264 And H.265 Video Parameters

Video Resolution	720P
Video Frame rate(fps)	30
Video Bitrate(Kb/Sec)	2048
2nd Video Resolution	VGA
2nd Video Frame rate(fps)	30
2nd Video Bitrate(Kb/Sec)	512

Table A25 - MyBell 2-Wire 1-button Station - RTSP stream video parameters configuration

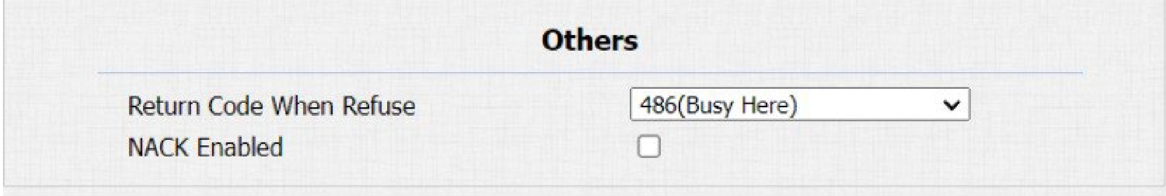
Setting	Description
Video Resolution	Select the video resolution from the following options: **CIF, VGA, 4CIF, 720P, 1080P.** The default video resolution is 4CIF. The video from the door phone can fail to be displayed on the indoor monitor if the resolution is set higher than 4CIF.
Video Framerate	The default video frame rate is 30 fps.
Video Bitrate	Select the video bitrate from the following options: **64 kbps, 128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps,** according to your network environment. The default video bit-rate is 2048 kpbs.
2nd Video Resolution	Select the video resolution for the second video stream channel. The default video resolution is VGA.
2nd Video Framerate	Select the video framerate for the second video stream channel. The default video frame rate is 25 fps.
2nd Video Bitrate	Select the video bitrate for the second video stream channel. The default video bit-rate is 512 kpbs.

16.2 - NACK

Negative Acknowledgment (NACK) indicates a failure or error in data transmission or processing. It is used to request retransmission or to signal the failure to the sender, ensuring data integrity.

To enable NACK by the web interface:

Intercom > Call Feature > Others



Others

Return Code When Refuse	486(Busy Here)
NACK Enabled	☐

Setting:

- **NACK Enabled:** it can be used to prevent losing the data packet in case of weak network environment, when discontinued and mosaic video image occurrs.

16.3 - MJPEG image capturing

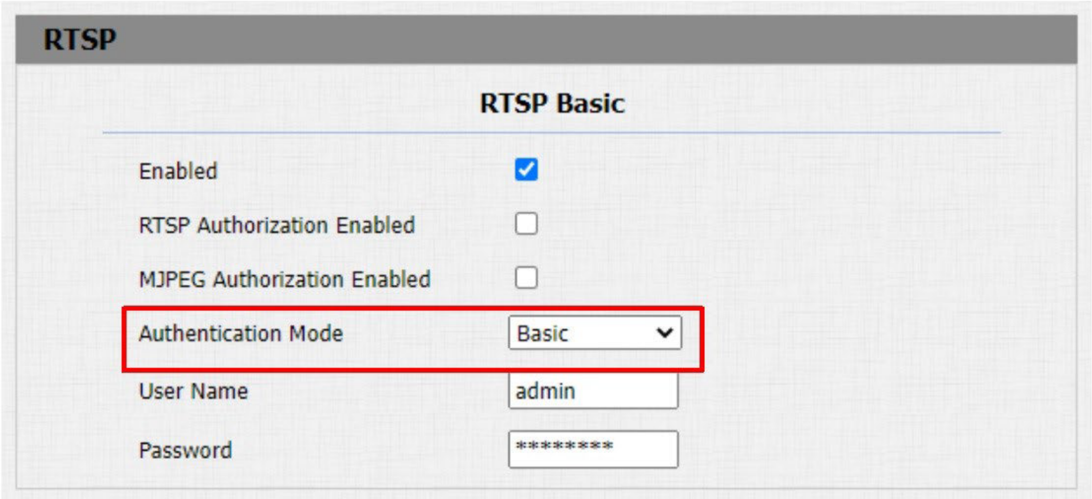
The door phone can capture the monitoring image in **MJPEG** format.

To enable the MJPEG function and set the image quality by the web interface:

Surveillance > RTSP > Basic

and

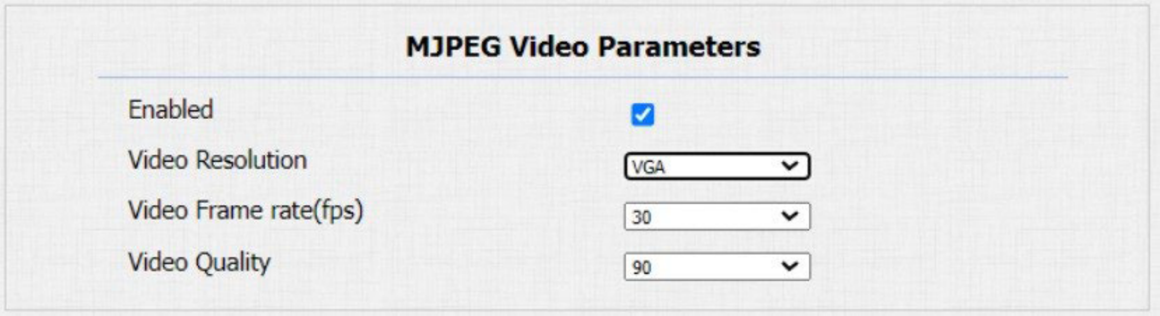
Surveillance > RTSP > MJPEG Video Parameters



RTSP

RTSP Basic

Enabled	☑
RTSP Authorization Enabled	☐
MJPEG Authorization Enabled	☐
Authentication Mode	Basic
User Name	admin
Password	********



MJPEG Video Parameters

Enabled ☑

Video Resolution VGA

Video Frame rate(fps) 30

Video Quality 90

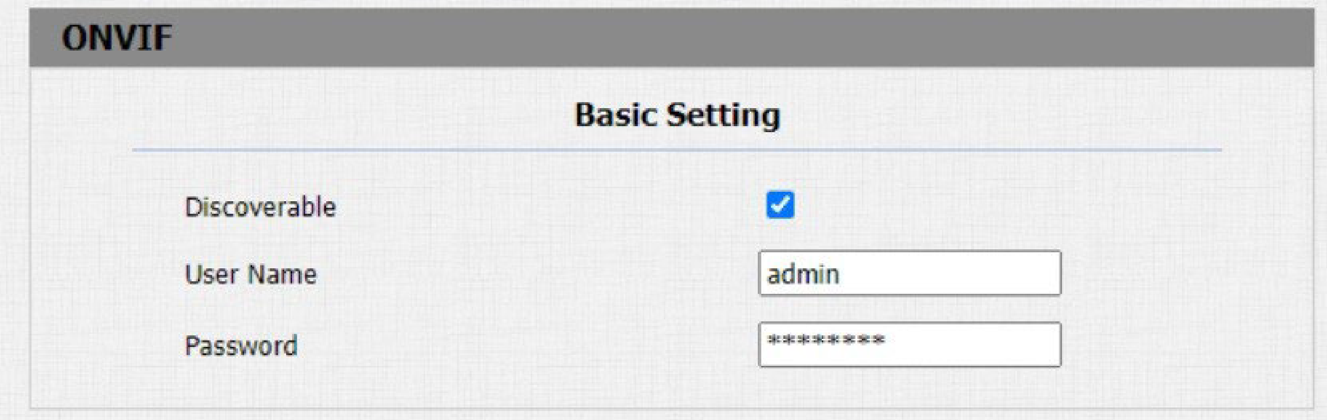
Table A26 - MyBell 2-Wire 1-button Station - MJPEG video configuration	
Setting	**Description**
Enabled	Tick this checkbox to access device video or real-time screenshots through a browser HTTP address such as: • http://device IP:8080/video.cgi (dynamic video). • http://device IP:8080/jpeg.cgi (static screenshot).
Video Resolution	Select the video resolutions from the following options: **CIF, VGA, 4CIF, 720P, 180P.** The default video resolution is VGA. The video from the door phone can fail to be displayed on the indoor monitor if the resolution is set higher than VGA.
Video Framerate	The default video frame rate is 30 fps.
Video Quality	The video bitrate range is 50 to 90.

16.4 - ONVIF configuration

Real-time video from the door phone camera can be searched and obtained by the indoor monitor or by third-party devices such as Network Video Recorder (NVR) after setting up the ONVIF function.

To configure the ONVIF function by the web interface:

Surveillance > ONVIF



ONVIF

Basic Setting

Discoverable ☑

User Name admin

Password ********

Table A27 - MyBell 2-Wire 1-button Station - ONVIF configuration	
Setting	**Description**
Discoverable	Select to enable the Discoverable ONVIF mode to enable other devices to search the video from the door phone camera.
User Name	Enter the username. The deafult username is **admin.**
Password	Enter the password. The deafult password is **admin.**

After the configuration is complete, you can enter the ONVIF URL on the third party device to view the video stream.

For example: **http://IP address:80/onvif/device_service**.

Note

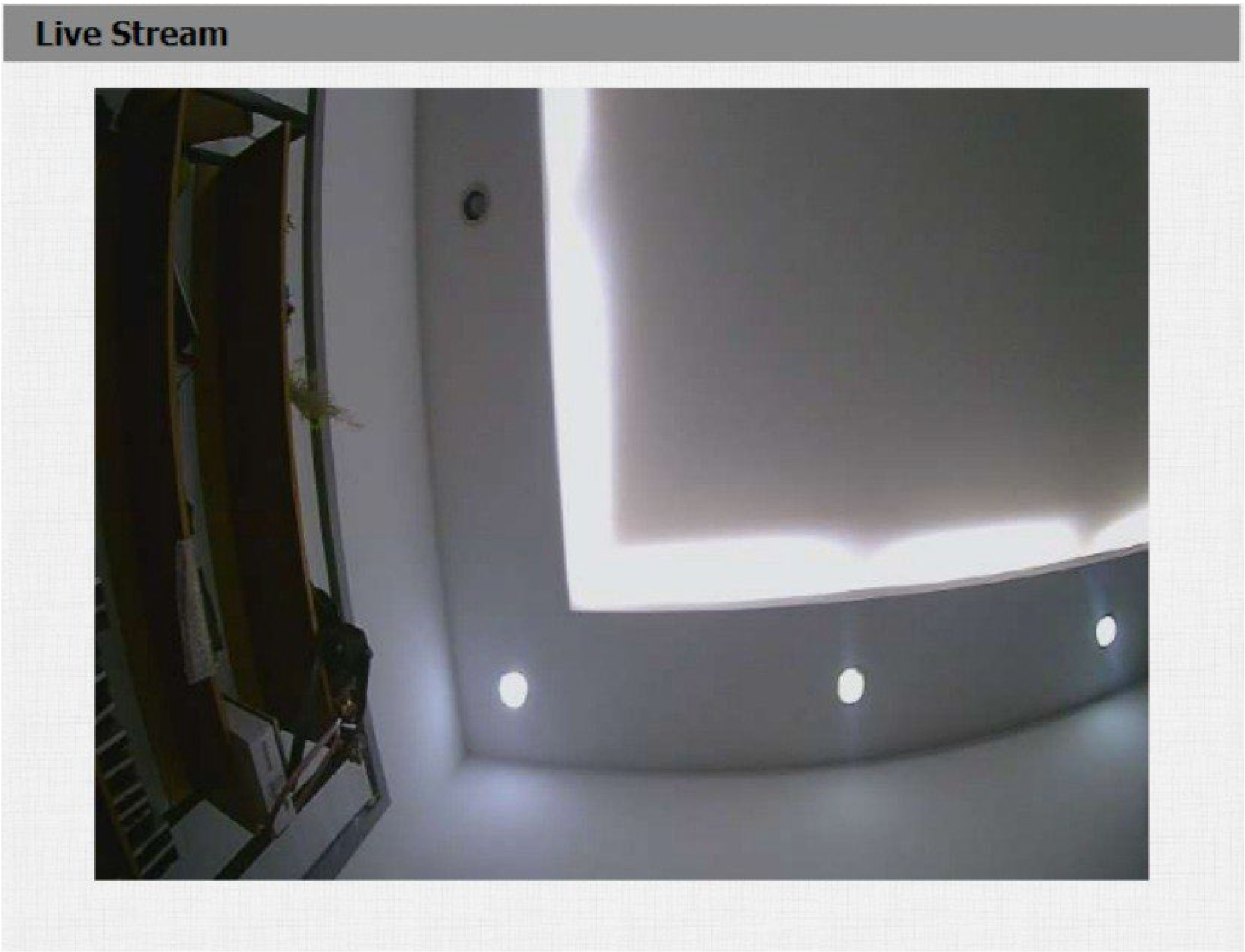
Enter the specific IP address of the door phone in the URL.

16.5 - Live stream

To check the real-time video from the door phone go to the device web interface or enter the correct URL in the web browser to obtain it directly. The URL: **http://IP_address:8080/video.cgi**.

To check the real-time video by the web interface:

Surveillance > Live Stream



Live Stream

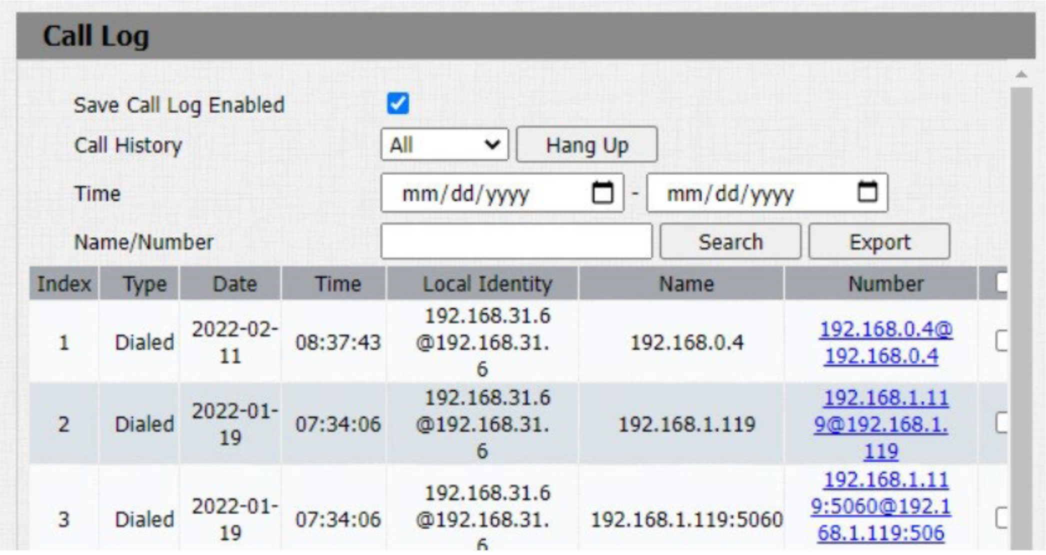
17 LOGS

17.1 - Call logs

To check the calls from a certain period of time, icluding the dial-out calls, received calls, and missed calls, check and search the call log.

To check the call logs by the web interface:

Intercom > Call Log



Call Log

Save Call Log Enabled ☑

Call History: All ▾ | Hang Up

Time: mm/dd/yyyy - mm/dd/yyyy

Name/Number: | Search | Export

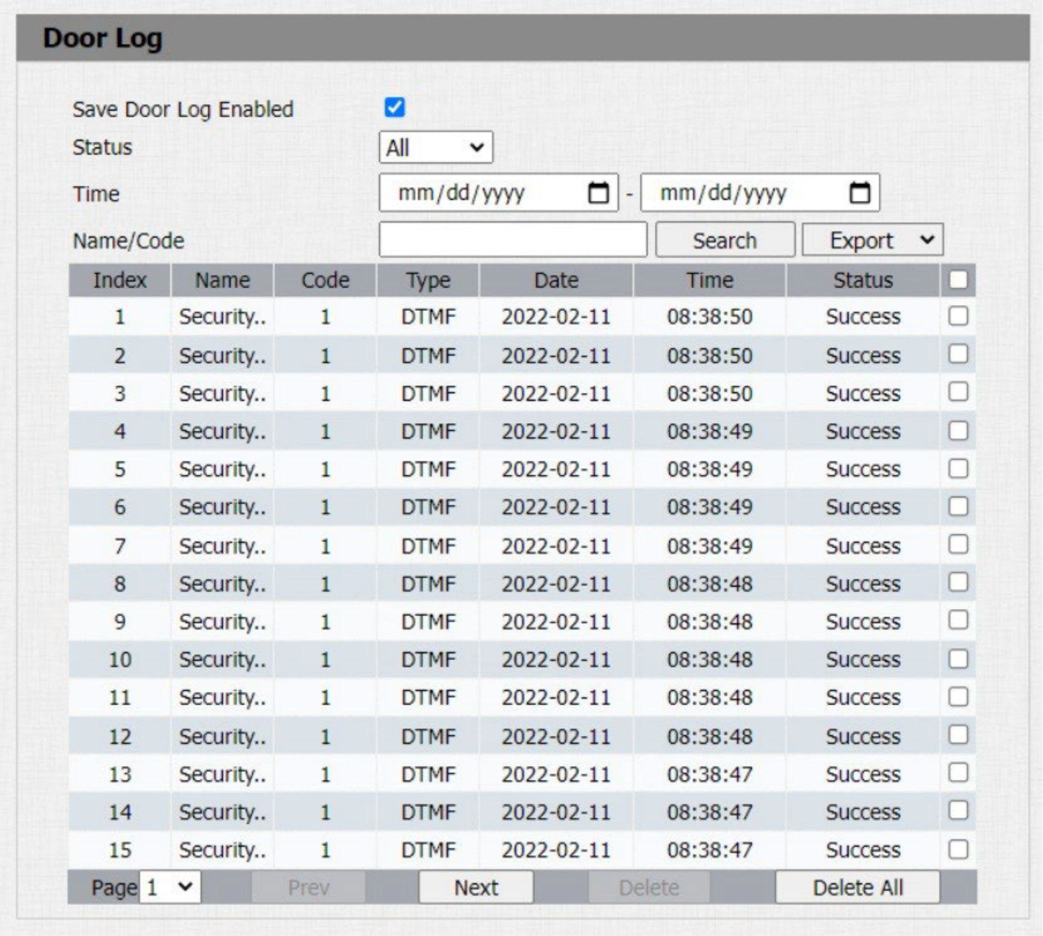
Index	Type	Date	Time	Local Identity	Name	Number	□
1	Dialed	2022-02-11	08:37:43	192.168.31.6@192.168.31.6	192.168.0.4	192.168.0.4@192.168.0.4	□
2	Dialed	2022-01-19	07:34:06	192.168.31.6@192.168.31.6	192.168.1.119	192.168.1.119@192.168.1.119	□
3	Dialed	2022-01-19	07:34:06	192.168.31.6@192.168.31.6	192.168.1.119:5060	192.168.1.119:5060@192.168.1.119:506	□

Table A28 - MyBell 2-Wire 1-button Station - Call logs configuration	
Setting	**Description**
Call History	Select call history from the following options: **All, Dialed, Received, Missed** for the specific type of call log to be displayed.
Time	Select the specific time span of the call logs you want to search, check or export.
Name/Number	Select the **Name** or **Number** option to search the call log by the name or by the SIP or IP number.

17.2 - Door logs

To search and check the various types of door access history in the door logs by the web interface:

Access Control > Door Log



Door Log

Save Door Log Enabled ☑

Status: All ▾

Time: mm/dd/yyyy - mm/dd/yyyy

Name/Code: | Search | Export ▾

Index	Name	Code	Type	Date	Time	Status	□
1	Security..	1	DTMF	2022-02-11	08:38:50	Success	□
2	Security..	1	DTMF	2022-02-11	08:38:50	Success	□
3	Security..	1	DTMF	2022-02-11	08:38:50	Success	□
4	Security..	1	DTMF	2022-02-11	08:38:49	Success	□
5	Security..	1	DTMF	2022-02-11	08:38:49	Success	□
6	Security..	1	DTMF	2022-02-11	08:38:49	Success	□
7	Security..	1	DTMF	2022-02-11	08:38:49	Success	□
8	Security..	1	DTMF	2022-02-11	08:38:48	Success	□
9	Security..	1	DTMF	2022-02-11	08:38:48	Success	□
10	Security..	1	DTMF	2022-02-11	08:38:48	Success	□
11	Security..	1	DTMF	2022-02-11	08:38:48	Success	□
12	Security..	1	DTMF	2022-02-11	08:38:48	Success	□
13	Security..	1	DTMF	2022-02-11	08:38:47	Success	□
14	Security..	1	DTMF	2022-02-11	08:38:47	Success	□
15	Security..	1	DTMF	2022-02-11	08:38:47	Success	□

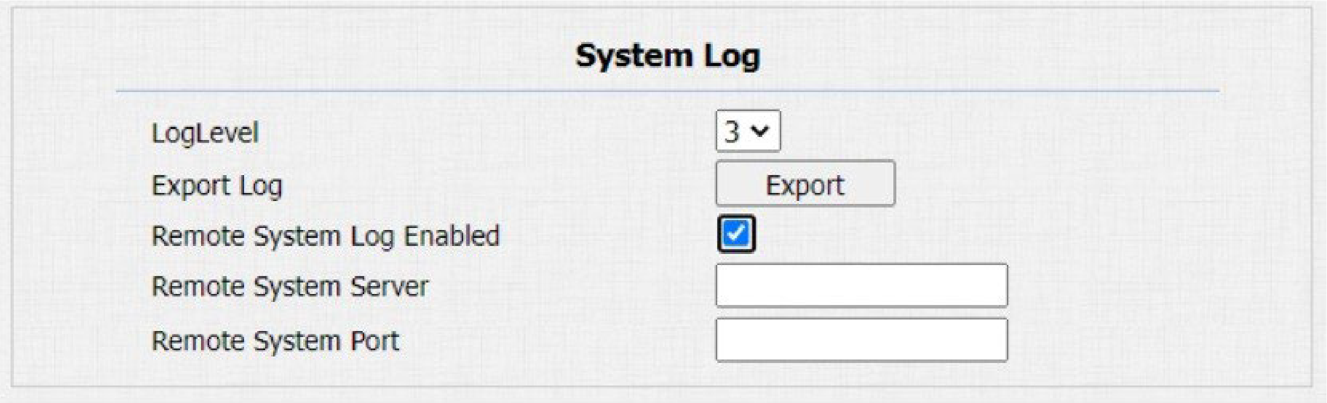
Table A29 - MyBell 2-Wire 1-button Station - Door logs configuration	
Setting	**Description**
Status	**All** – to check all door logs. **Success** – to check successfully opened door logs. **Failed** – to check door logs for opening failure.
Time	Set the time range for the door logs you want to check.
Name	• Locally added key or card – the corresponding name is displayed. • Unknown key or card – it displays as **Unknown**.
Code	• Door opened using PIN code – the corresponding PIN code is displayed. • Door opened using RF card – the corresponding card number is displayed. • Door opened using HTTP command – this field is empty.
Type	• Door opened using PIN code – **Password** is displayed. • Door opened using RF card – **Card** is displayed. • Door opened using HTTP command – **HTTP** is displayed.

18.1 - System log

System logs can be used for debugging purposes.

To export the system logs out to a local PC or to a remote server for debugging by the device web interface:

Upgrade > Diagnose > System Log



System Log

LogLevel: 3

Export Log: Export

Remote System Log Enabled: ☑

Remote System Server:

Remote System Port:

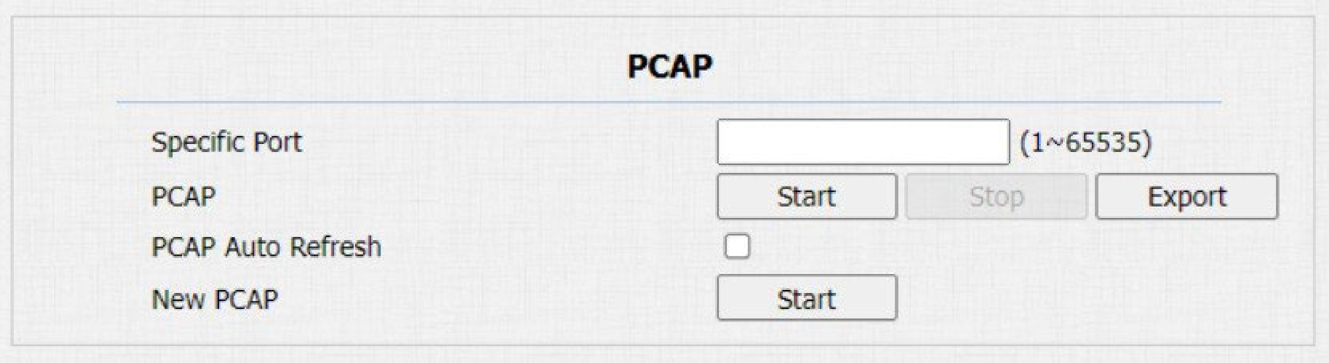
Table A30 - MyBell 2-Wire 1-button Station - System log	
Setting	**Description**
LogLevel	Select log level from 1 to 7. The technical staff instructs about the specific log level to be entered for debugging purpose. The default log level is **3**. The higher the level, the more complete the log.
Export Log	Click the **Export** button to export temporary debug log file to a local PC.
Remote System Server	Enter the remote server address to receive the device log, the remote server address is provided by the technical support.

18.2 - PCAP configuration

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes. PCAP needs to be set up properly before using it.

To configure PCAP by the web interface:

Upgrade > Diagnose > PCAP



PCAP

Specific Port: (1~65535)

PCAP: Start Stop Export

PCAP Auto Refresh: □

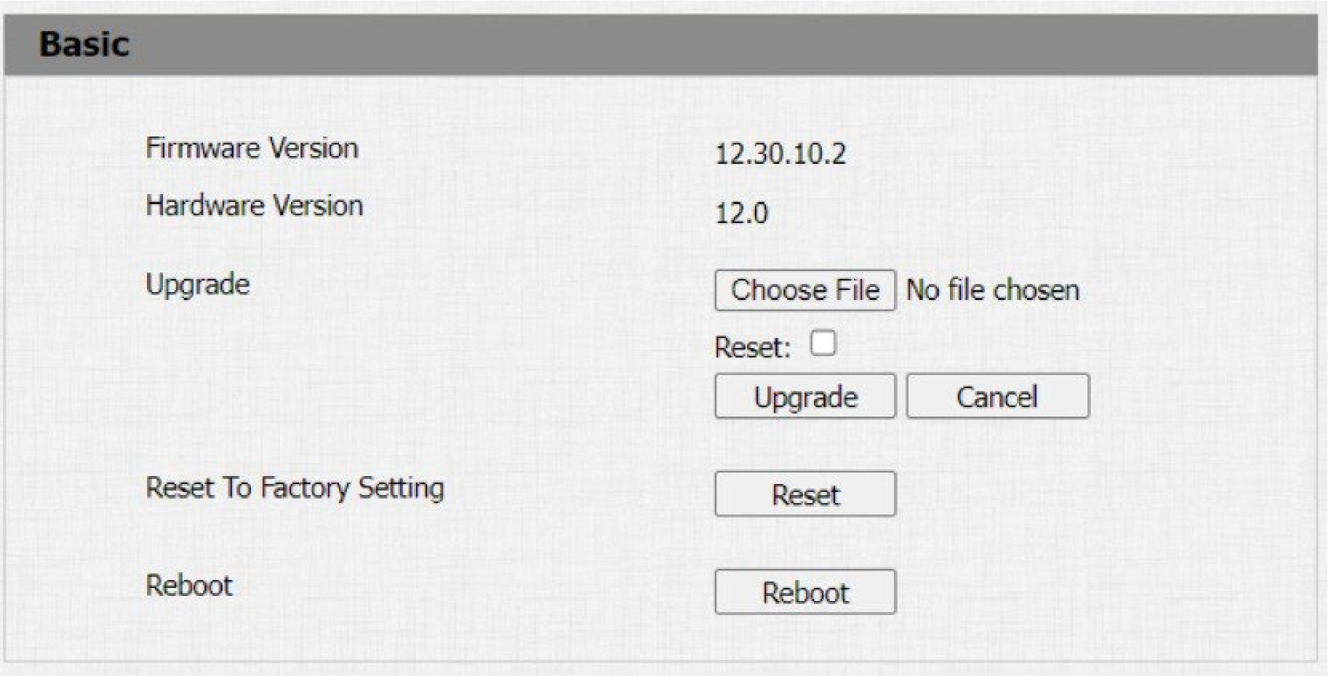
New PCAP: Start

Table A31 - MyBell 2-Wire 1-button Station - PCAP configuration	
Setting	**Description**
Specific Port	Select the specific port from 1 to 65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
PCAP	Click the **Start** and **Stop** buttons to capture a certain range of data packets before clicking the **Export** button to export the data packets to your Local PC.
PCAP Auto Refresh	If set to **Enable**, the PCAP continues to capture data packets even after the data packets reach their maximum capacity of 1 MB. If set to **Disable**, the PCAP stops data packet capturing when the captured data packet reaches the maximum capturing capacity of 1 MB.
New PCAP	Click **Start** to capture a bigger data package.

19 FIRMWARE UPGRADE

To upgrade the devices by the web interface:

Upgrade > Basic



Basic

Firmware Version	12.30.10.2
Hardware Version	12.0
Upgrade	Choose File No file chosen Reset: □ Upgrade Cancel
Reset To Factory Setting	Reset
Reboot	Reboot

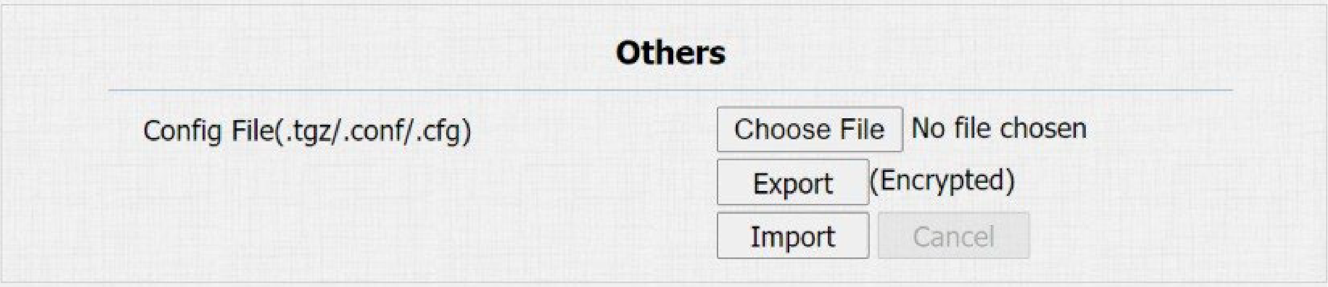
Note

Don't disconnect the device from the internet and power supply when the firmware upgrade is in progress. It might cause upgrade failure or system breakdown.

20 BACKUP

To import or export encrypted configuration files to your local PC by the web interface:

Upgrade > Diagnose > Others



Others

Config File(.tgz/.conf/.cfg) No file chosen

(Encrypted)

Setting:

- **Export Config File:** export the current config file.
- **Export/Import:** export the current config file (Encrypted) or import the new config file.

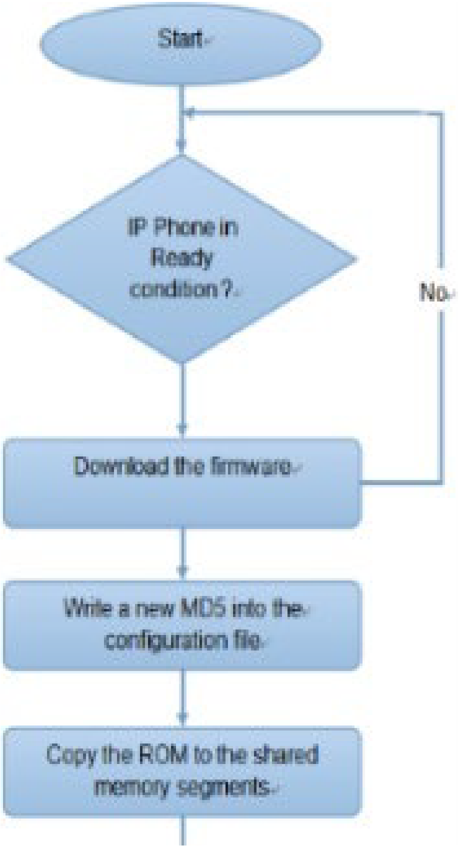
21 AUTO-PROVISIONING THROUGH CONFIGURATION FILE

Configure and upgrade the door phone by the web interface through one-time auto-provisioning and scheduled auto-provisioning through configuration files. In such case, performing manual configurations of the door phone isn't necessary.

21.1 - Provisioning principle

Auto-provisioning is a feature used to configure or upgrade devices in batch using third-party servers. DHCP, PNP, TFTP, FTP, and HTTPS protocols are used by the intercom devices to access the URL address of the third-party server which stores configuration files and firmware used to update the firmware and the corresponding settings on the device.

See the flow chart below:


Start
IP Phone in Ready condition ?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments

21.2 - Configuration files for auto-provisioning

Configuration files have the two following formats for auto-provisioning:

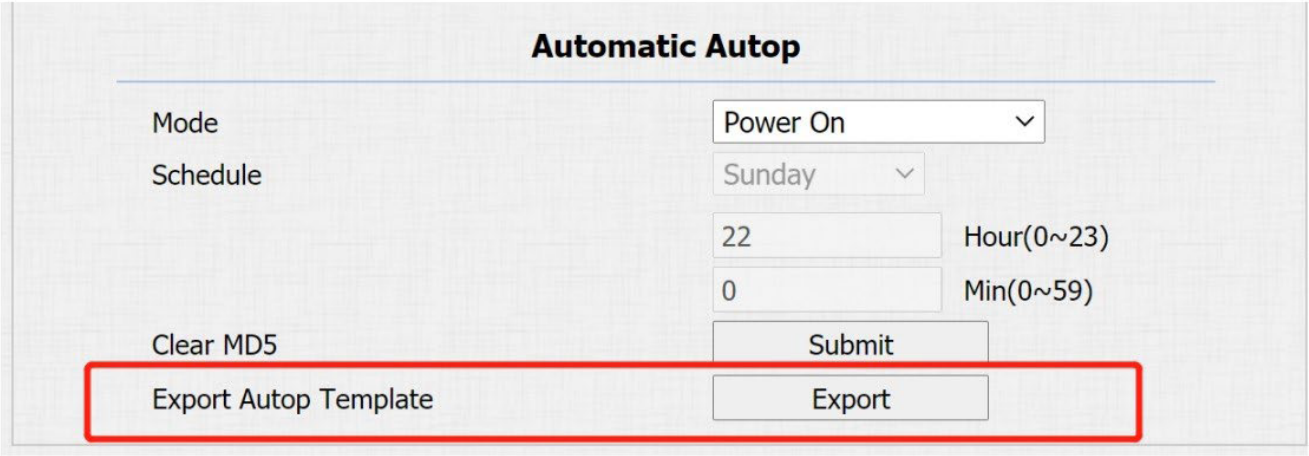
- **General configuration provisioning** – a general file is stored in a server from which all the related devices can download the same configuration file to update settings on the devices. For example, **.cfg**.
- **MAC-based configuration provisioning** – MAC-based configuration files are used for auto-provisioning on a specific device as distinguished by its unique MAC number. The configuration files named with the device MAC number are matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

If a server has these two types of configuration files, the IP devices first access the general configuration files before accessing the MAC-based configuration files.

To get the Autop configuration file template by the web interface:

Upgrade > Advanced > Automatic Autop



Automatic Autop

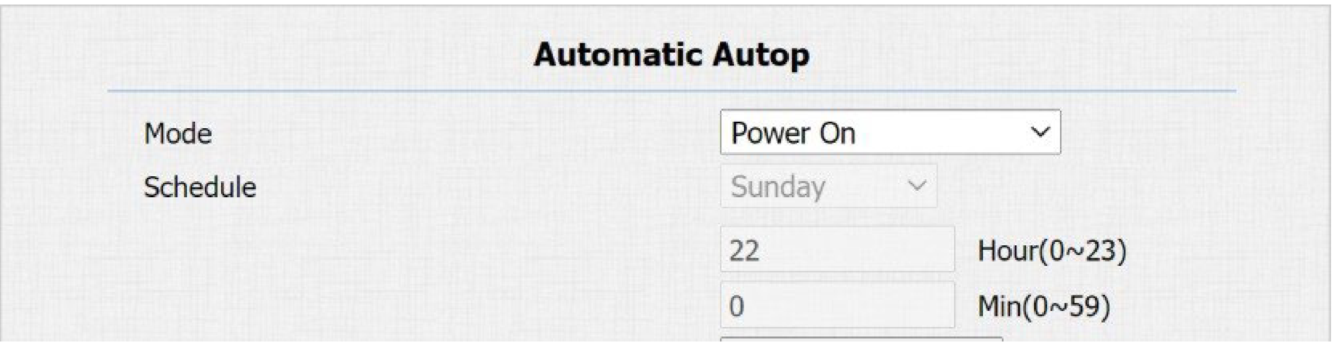
Mode	Power On
Schedule	Sunday
	22 Hour(0~23)
	0 Min(0~59)
Clear MD5	Submit
Export Autop Template	Export

21.3 - Autop schedule

The device provides you with different Autop methods that enable the indoor monitor to perform provisioning for itself in a specific time according to your schedule.

To configure the Autop schedule by the web interface:

Upgrade > Advanced > Automatic Autop



Automatic Autop

Mode: Power On

Schedule: Sunday

22 Hour(0~23)

0 Min(0~59)

Settings:

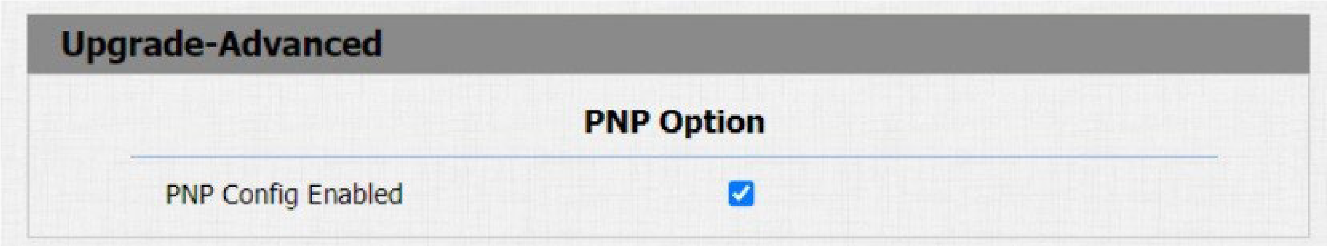
- **Mode:**
  - **Power on** – the device performs Autop every time it boots up.
  - **Repeatedly** – the device performs Autop according to the schedule you set up.
  - **Power On + Repeatedly** – combines the Power On Mode and the Repeatedly mode. It enables the device to perform Autop every time it boots up or according to the schedule you set up.
  - **Hourly Repeat** – the device performs Autop every hour.
- **Schedule:** if the **Repeatedly** mode is selected, you can set up the time schedule for the Autop.

21.4 - PNP configuration

Plug and Play (PNP) is a combination of hardware and software support that enables the computer system to recognize and adapt to hardware configuration changes with little or no user intervention.

To configure the PNP by the web interface:

Upgrade > Advanced > PNP Option



Upgrade-Advanced

PNP Option

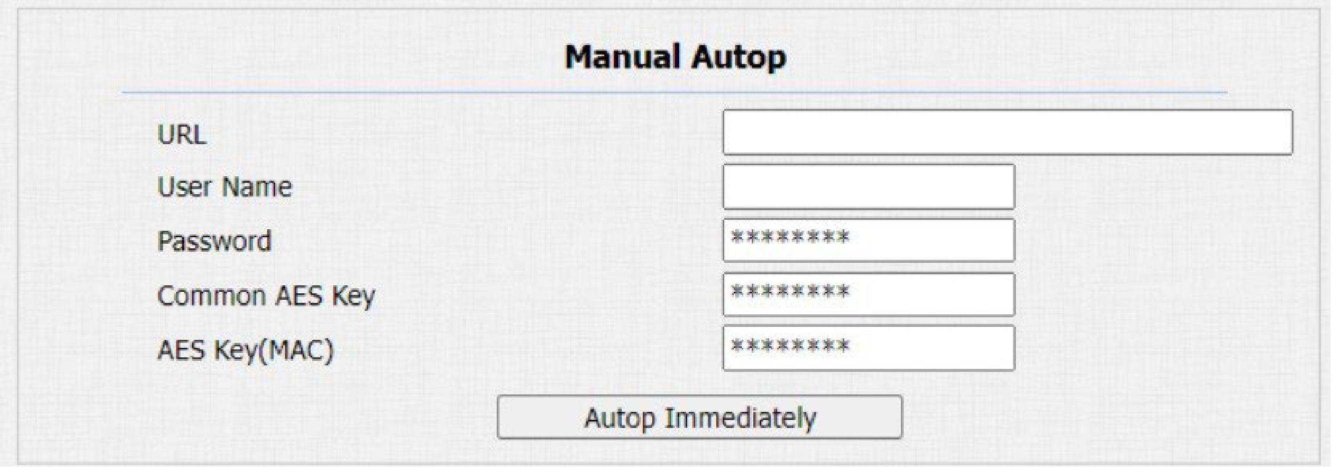
PNP Config Enabled ☑

21.5 - Static provisioning configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provisioning schedule is set up, the door phone performs the auto-provisioning at a specific time according to the schedule. TFTP, FTP, HTTP, and HTTPS protocols can be used for upgrading the device firmware and configuration.

To configure the static provisioning by the web interface:

Upgrade > Advanced > Manual Autop



Manual Autop

URL:

User Name:

Password: ********

Common AES Key: ********

AES Key(MAC): ********

Table A32 - MyBell 2-Wire 1-button Station - Static provisioning configuration	
Setting	**Description**
URL	Set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
User Name	Set up a username if it is required to acces the server, otherwise leave it blank.
Password	Set up a password if it is required to acces the server, otherwise leave it blank.
Common AES Key	Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
AES Key (MAC)	Set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

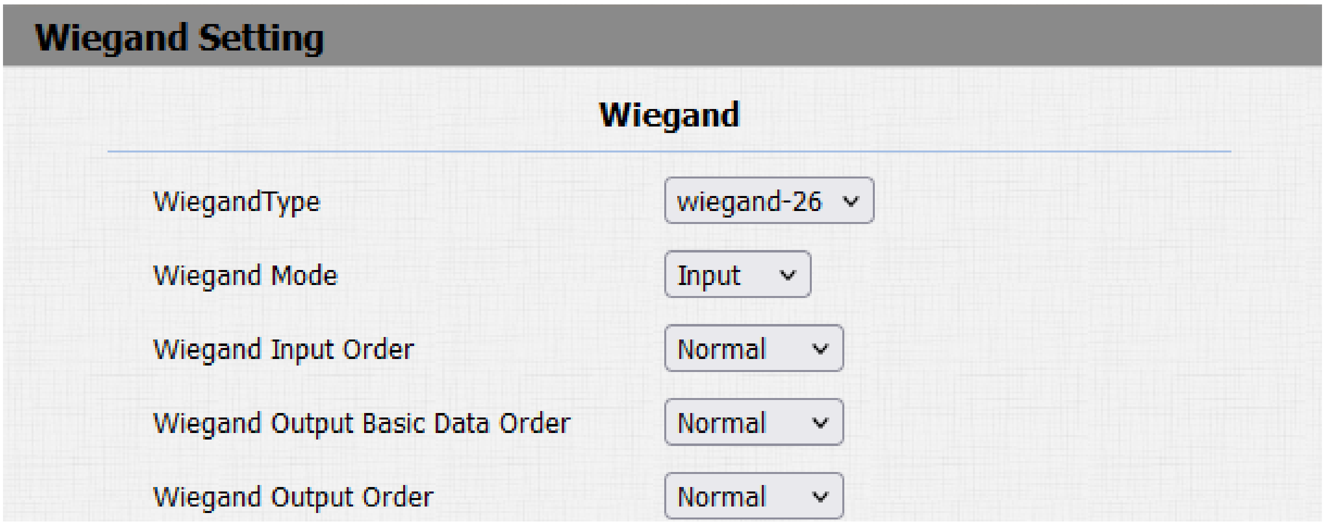
- AES encryption should be configured only when the config file is encrypted with AES, otherwise leave this field blank.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/ (allows anonymous login)
    - ftp://username:password@192.168.0.19/ (requires a user name and password)
  - HTTP: http://192.168.0.19/ (use the default port 80)
    - http://192.168.0.19:8080/ (use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/ (use the default port 443)
- MyBell doesn't provide user specified server.
- Please prepare the TFTP/FTP/HTTP/HTTPS servers by yourself.

22 INTEGRATION WITH THIRD PARTY DEVICE

22.1 - Wiegand integration

To integrate the door phone with third-party devices by Wiegand, configure the Wiegand by the web interface:

Access Control > Card Setting > Wiegand



Wiegand Setting

Wiegand

WiegandType	wiegand-26
Wiegand Mode	Input
Wiegand Input Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Order	Normal

Table A33 - MyBell 2-Wire 1-button Station - Wiegand integration

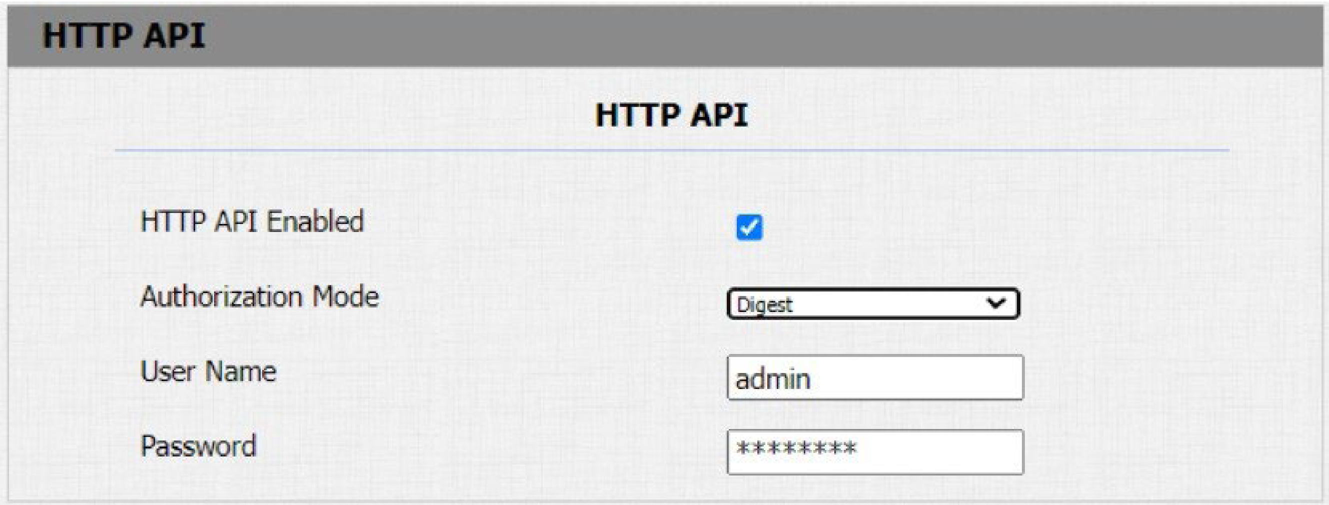
Setting	Description
Wiegand Display Mode	Select Wiegand Card code format from the following options: **8H10D, 6H3D5D, 6H8D, 8HN, 8HR, 6H3D5D-R(W26), 8HR10Dv.**
Wiegand Card Reader Mode	Select the Wiegand data transmission format from the following options: **Wiegand 26, Wiegand 34, Wiegand 58**. The transmission format needs to be the same for the door phone and the device.
Wiegand Transfer Mode	Select the transfer mode from the following options: • **Input** – door phone is used as a reciever. • **Output** – Wiegand output is converted to card number before it is sent from the door phone to the reciever. • **Convert to Card No.OutputWiegand**. The user card number corresponding to the facial recognition access is sent out in binary system.
Wiegand Input Data Order	Set the Wiegand input data sequence to **Normal** or **Reversed**. If you select **Reversed**, the input card number is reversed.
Wiegand Output Data Order	Set the Wiegand output data sequence to **Normal** or **Reversed**. If you select **Reversed**, the output card number is reversed.
Wiegand Output CRC	If enabled, the parity check function is on and it ensures that signal-based data can be transmitted correctly according to the established data transmission format.

22.2 - HTTP API integration

HTTP API is used for a network-based integration of the third-party device with the intercom device.

To perform the HTTP API integration by the web interface:

Security > HTTP API



HTTP API

HTTP API

HTTP API Enabled	☑
Authorization Mode	Digest
User Name	admin
Password	********

Table A34 - MyBell 2-Wire 1-button Station - HTTP API integration

Setting	Description
Enabled	If disabled, any request to initiate the integration is denied and HTTP 403 forbidden status is returned.
Authorization Mode	Select the authorisation type from the following options: **None, Normal, Allowlist, Basic, Digest, Token.** The options are explained in detail in Table A34 below.
User Name	Enter the username when **Basic** or **Digest** authorization mode is selected. The default username is **Admin**.
Password	Enter the password when **Basic** or **Digest** authorization mode is selected. The default password is **Admin**.
1st IP-5th IP	Enter the IP address of the third party devices when **Allowlist** authorization mode is selected.

Table A35 - MyBell 2-Wire 1-button Station - Authorization modes

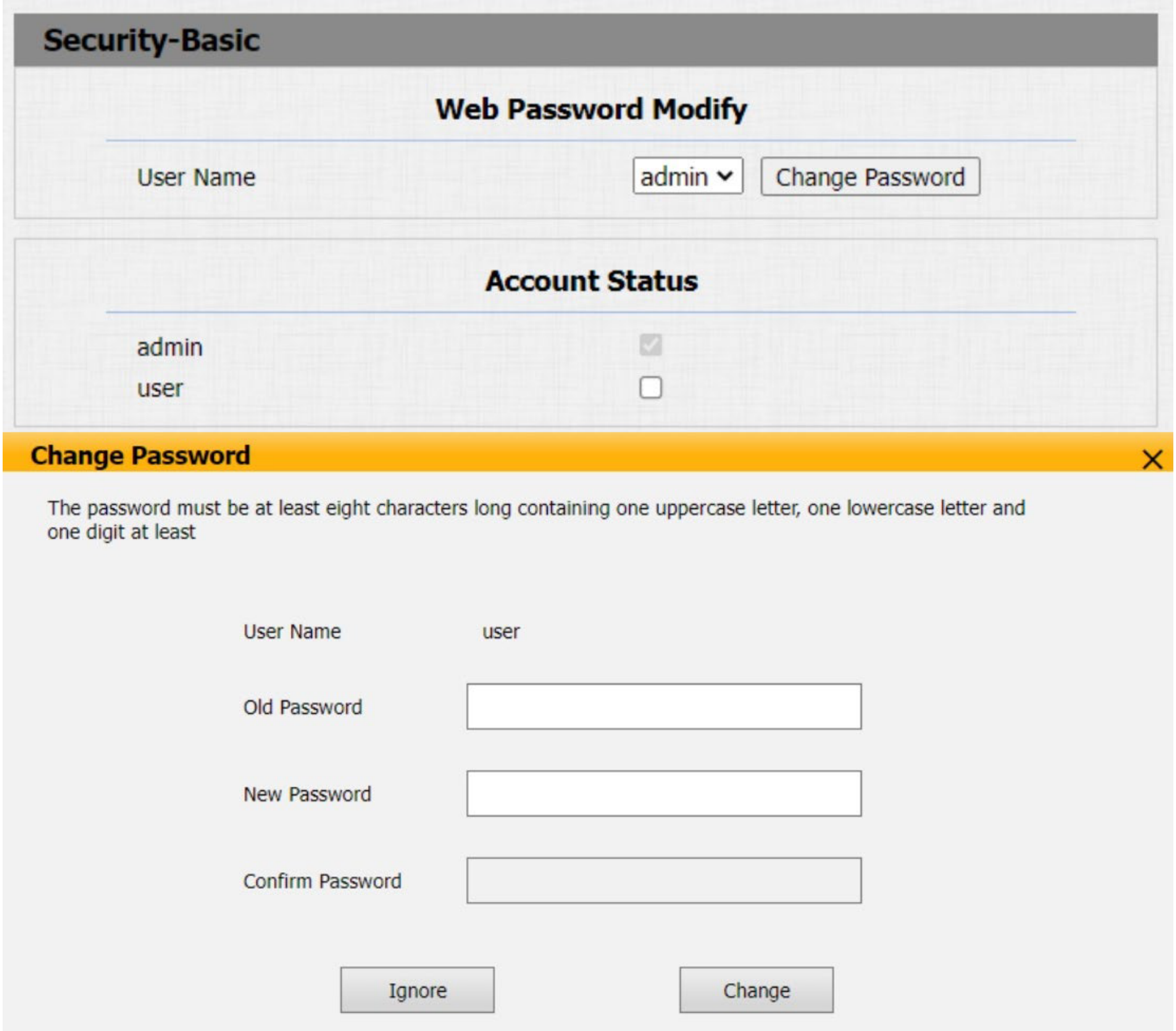
Authorization Mode	Description
None	No authentication is required for HTTP API as it's only used for demo testing.
Normal	This mode is used by the developers only.
Allowlist	You only need to enter the IP address of the third party device for authentication. The **Allowlist** is suitable for operation on the LAN.
Basic	You need to enter the **User Name** and the **Password** for authentication. In the **Authorization** field of the HTTP request header use **Base64** encode method to encode the **User Name** and **Password**.
Digest	Password encryption method only supports the Message-Digest Algorithm (MD5). MD5 in the **Authorization** field of the HTTP request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
Token	This mode is used by the developers only.

23.1 - Device web interface password modification

To change the default web password by the web interface:

Security > Basic

Select **admin** for the administrator account and **user** for the user account. Click the **Change Password** button to change the password.



User Name admin

admin ☑

user ☐

The password must be at least eight characters long containing one uppercase letter, one lowercase letter and one digit at least

User Name user

Old Password

New Password

Confirm Password

Settings:

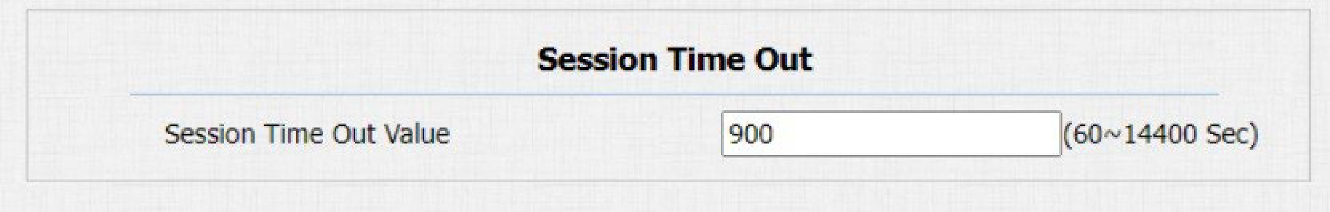
- **User Name:** modify the Admin or user password if needed.
- **User:** enable the user account if needed.

23.2 - Web interface automatic logout conifguration

You can set up the web interface automatic log-out time. After this time re-loging is required for security purposes or for the convenience of operation.

To configure the web interface automatic logout by the web interface:

Security > Basic > Session Time Out



Session Time Out Value 900 (60~14400 Sec)

Settings:

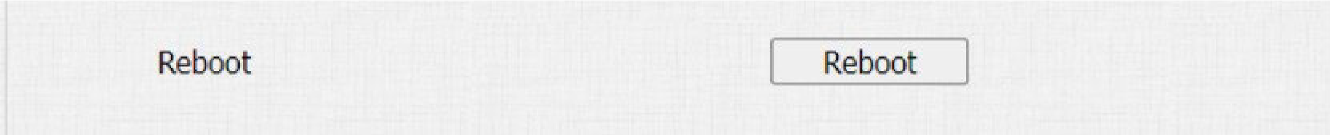
- **Session Time Out Value:** you can choose the session timeout between 60 and 14400 seconds. If there's no operation over the set time, you need to log in to the website again.

24 SYSTEM REBOOT AND RESET

24.1 - Reboot

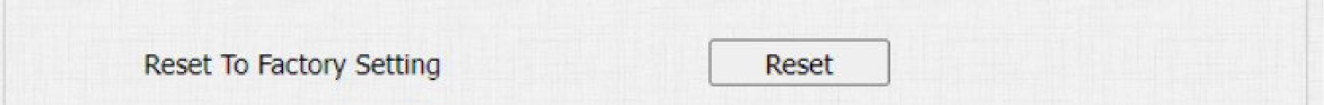
To reboot the device system by the web interface:

Upgrade > Basic



24.2 - Reset

To reset the device system to the factory settings by the web interface:
Upgrade > Basic



Part Two

MyBell 2-Wire Indoor Monitor

1 IMPORTANT SAFEGUARDS AND WARNINGS

- ⚠ **CAUTION! – Any use other than that specified herein or in environmental conditions other than those stated in this manual is to be considered improper and is strictly forbidden!**
- ⚠ **CAUTION! – Important instructions: keep this manual in a safe place to enable future product maintenance and disposal procedures.**
- ⚠ **CAUTION! – All installation and connection operations must be performed exclusively by suitably qualified and skilled personnel with the unit disconnected from the mains power supply.**
- ⚠ **CAUTION! – This manual contains important instructions and warnings for personal safety. Read carefully all parts of this manual. If in doubt, suspend installation immediately and contact Nice Technical Assistance.**

- The product packaging materials must be disposed of in full compliance with local regulations.
- Never apply modifications to any part of the device. Operations other than those specified can cause malfunctions. The manufacturer declines all liability for damage caused by makeshift modifications to the product.
- Never place the device near the sources of heat or expose to naked flames. These actions can damage the product and cause malfuntions.
- This product isn't intended for use by people (including children) with reduced physical, sensory or mental capabilities or who lack experience and knowledge, unless they are supervised by a person responsible for their safety.
- This product isn't a toy. Keep away from children and animals!
- The device is designed to operate in an electrical home installation. Faulty connection or use can result in a fire or electric shock.
- Even when the device is turned off, voltage can be present at its terminals. Any maintenance introducing changes to the configuration of connections or the load must be always performed with a disabled fuse.
- Don't use in damp or wet locations, near a bathtub, sink, shower, swimming pool, or anywhere else where water or moisture are present.

2 DEVICE DESCRIPTION

The MyBell 2-Wire Indoor Monitor multifunctional communicator, with a Linux operating system, provides audio and video communication with door phones via SIP 2.0 protocol. It delivers the ultimate touch screen experience in an unobtrusive, space-saving design featuring a brilliant 7-inch capacitive touch screen display.

Table A1 - MyBell 2-Wire Indoor Monitor - Device description

Feature	Description
Operation system	Linux
RAM	64 MB
ROM	128 MB
Front panel	plastic
Wi-Fi	IEEE802.11b/g/n, @2.4GHz
Ethernet	yes
Power over Ethernet (PoE)	no
Power supply	24 V DC
RS485 port	supported
Alarm input	8
Relay output	1
Bell in	1
I/O	8
Microphone	-58dB
Speaker	4Ω / 2W
2-wire ports	2 pairs
Ethernet ports	1xRJ45, 10/100Mbps adaptive
Installation	wall-mounted & desktop
Dimension	200.2x132.2x27.2mm
Working humidity	10~90%
Working temperature	-10°C ~ +45°C
Storage temperature	-20°C ~ +70°C
Touch screen display mode	normally white, transmissive
Display	7-inch (176 mm) TFT LCD
Screen	7-inch capacitive touch screen
Screen resolution	800 x 480
Screen contrast ratio	500:1
Luminance	220 cd/m^2
Viewing angle	50° Left, 50° Right, 40° Upper, 50° Lower
Touch Screen	projected capacitive
Audio	SIP v1 (RFC2543), SIP v2 (RFC3261)
Narrowband audio codec	G.711a, G.711μ, G.729
Broadband audio codec	G.722
DTMF	Out-of-band DTMF (RFC2833), SIP Info
Echo cancellation	yes
Supported networking protocols	IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP

Table A1 - MyBell 2-Wire Indoor Monitor - Device description

Feature	Description
Video streaming format	H.264
Auto-Provisioning	yes
Web management portal	yes
Web-based packet dump	yes
Configuration backup / restore	yes
Firmware upgrade	yes
System logs (including door access logs)	yes
Application scenario	Old villas retrofit, Old apartment retrofit

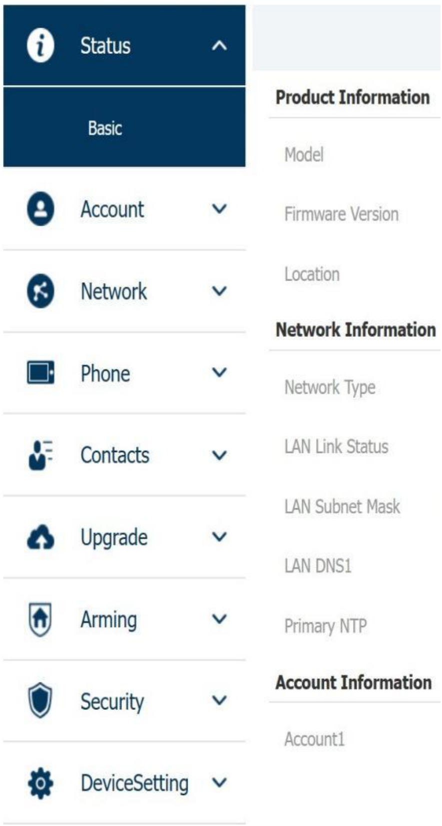


Table A2 - MyBell 2-Wire Indoor Monitor - Configuration Menu

Section	Description
Status	This section gives you basic information such as product information, network information, and account information.
Account	This section concerns SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer.
Network	This section mainly deals with DHCP & Static IP setting, RTP port setting, and device deployment.
Phone	This section includes time & language, call feature, screen display, multicast, audio intercom feature, monitor, relay, lift import & export, door log, and web relay.
Contacts	This section allows the user to configure the local contact list stored in the device.
Upgrade	This section covers a firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.
Arming	This section covers the configuration including arming zone setting, arming mode, disarm code, and alarm action.
Security	This section is for a password modification, account status & session time out configuration, and service location switching.
Device Setting	This section includes the RTSP and power output.

4 ACCESS TO THE DEVICE

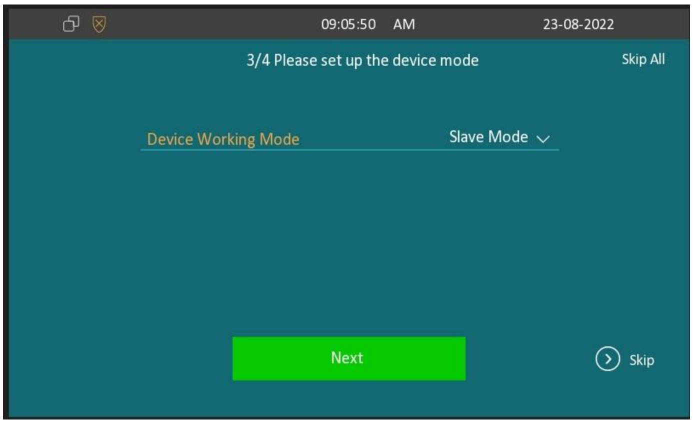
You can access MyBell 2-Wire Indoor Monitor system settings either on the device directly or using the device web interface.

4.1 - Device start-up selection

When you first start up MyBell 2-Wire Indoor Monitor, you need to perform start-up initialization, which includes a series of settings, such as language, time zone, networking method and network connection mode. Later you can also set time, language and network related setting.

Table A3 - MyBell 2-Wire Indoor Monitor - Configuration of the network connection mode

Setting	Description
Auto Mode	One of the devices is randomly selected as the master device. The master device provides the network to the sub-devices connected to it.
Master Mode	The device works as a master device for the house, the other devices connect with the master device and get the network from the master device
Slave Mode	The device works as a sub-device for the house and gets the network from the master device.



09:05:50 AM 23-08-2022

3/4 Please set up the device mode

Device Working Mode: Slave Mode

4.2 - Device home screen type selection

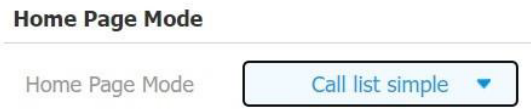
The device supports two different home screen display modes:

- **Call list simple**
- **Classic**

To configure home page mode by the web interface:

Phone > Key/ Display

Choose one suitable mode for your scenarios.



Home Page Mode

Home Page Mode: Call list simple

4.3 - Access to the device setting on the device

4.3.1 - Access to the device basic setting

You can access the device basic setting and advance setting where you can configure different types of functions as needed.

To access the device basic setting:

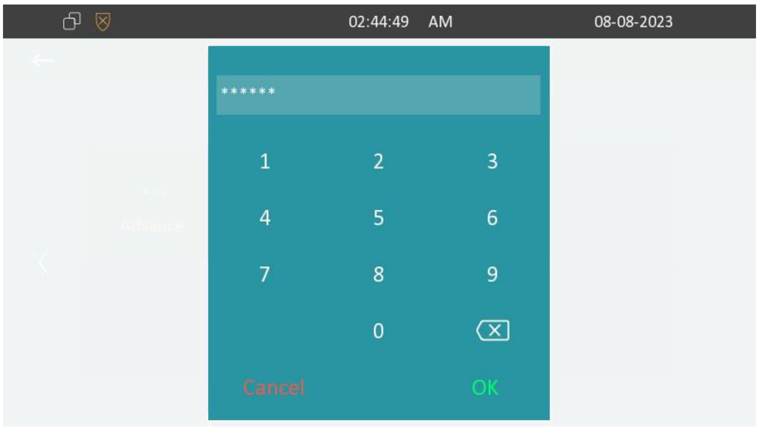
More > Settings

4.3.2 -Access to the device advanced setting

To access the device advanced basic setting:

More > Advance Settings

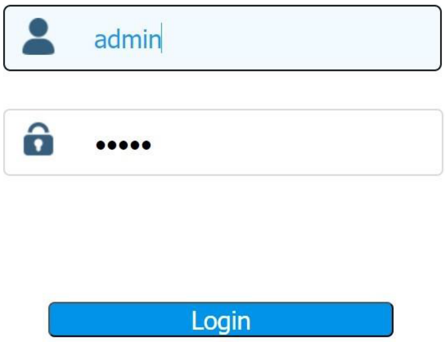
Press password **123456** (by default) to enter the advance setting.



4.4 - Access to the device setting by the web interface

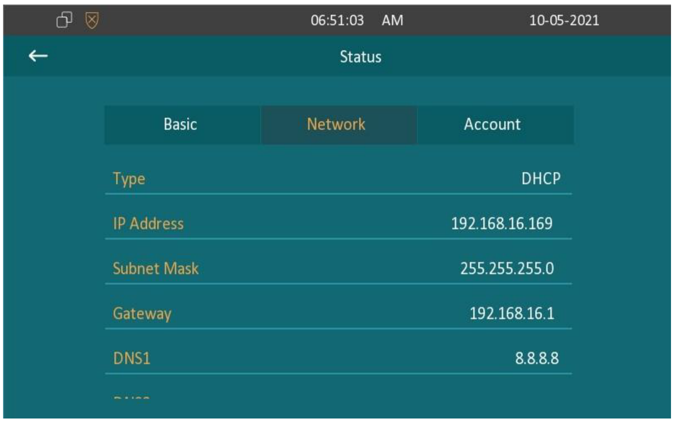
You can enter the device IP address in the web browser to log into the device web interface where you can configure settings.

The default username and password are **admin**.



admin

•••••



Type DHCP

IP Address 192.168.16.169

Subnet Mask 255.255.255.0

Gateway 192.168.16.1

DNS1 8.8.8.8

5 LANGUAGE AND TIME SETTING

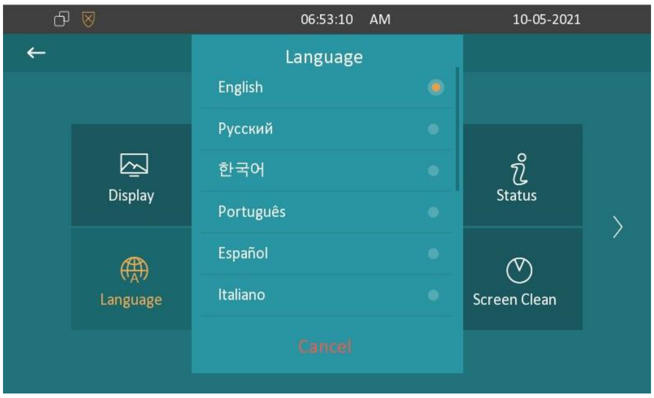
5.1 - Language setting

Set up the language during an initial device setup or later on the device or by the web interface according to your preference.

5.1.1 - Language setting on the device

To configure the language display on the device:

Settings > Language



Language

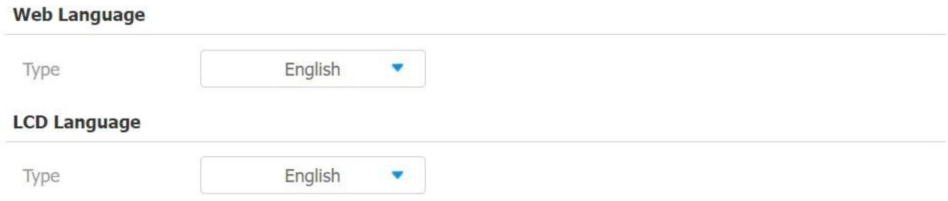
- English ●
- Русский ○
- 한국어 ○
- Português ○
- Español ○
- Italiano ○

5.1.2 - Language setting by the web interface

You can select device language, device language icons, and customize interface text including configuration names and prompt text.

To configure the language display using the web interface:

Phone > Time/Lang



Web Language

Type	English

LCD Language

Type	English

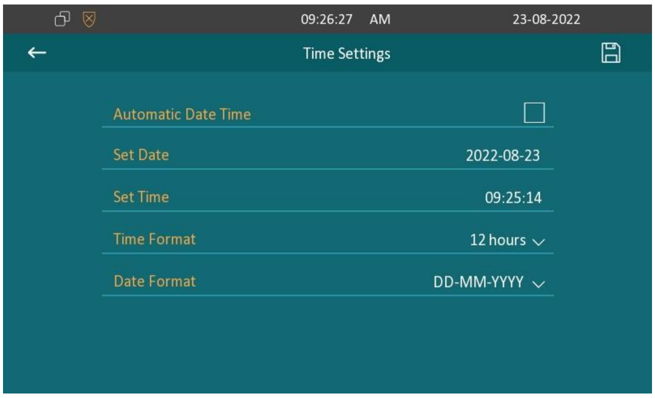
5.2 - Time setting

Time settings, including time zone, date and time format, can be configured either on the device or by the web interface.

5.2.1 - Time setting on the device

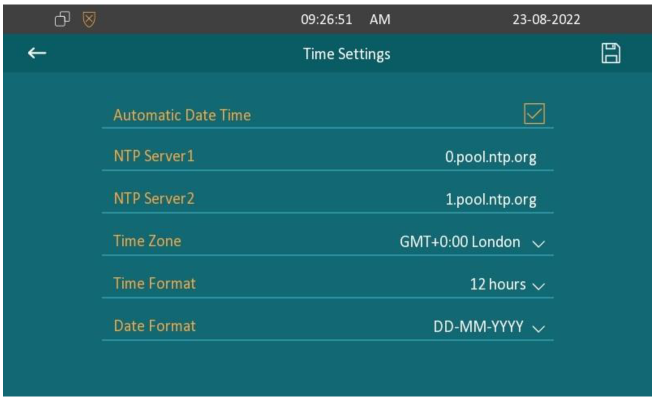
To configure time on the device:

More > Setting > Time



Time Settings

Automatic Date Time	□
Set Date	2022-08-23
Set Time	09:25:14
Time Format	12 hours
Date Format	DD-MM-YYYY



Time Settings

Automatic Date Time	☑
NTP Server1	0.pool.ntp.org
NTP Server2	1.pool.ntp.org
Time Zone	GMT+0:00 London
Time Format	12 hours
Date Format	DD-MM-YYYY

Parameter Set-up

- **Automatic Date Time** - the NTP-based automatic date time is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol (NTP) server. You can also set it up manually by ticking the check box and then entering the time and date you want and pressing the **Save** tab to save the setting.
- **NTP Server1&2** - Enter the NTP server you obtained in the NTP server field.

Note.

When the NTP-based automatic date time is switched off, settings related to the NTP server are non-editable.

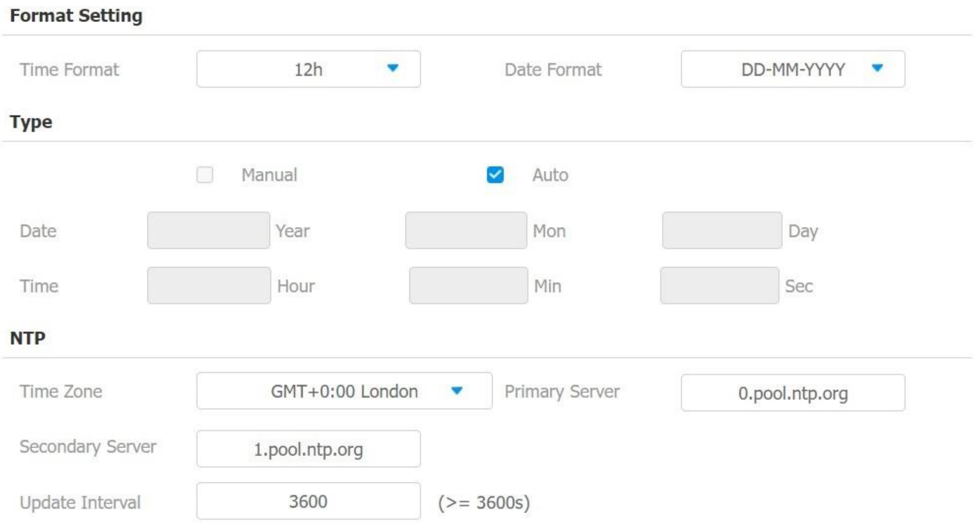
When the NTP-based automatic date time is switched on, time and date are denied editing.

5.2.2 - Time setting by the device web interface

You can synchronize automatically your time and date by setting up the NTP server address that you obtained. When a time zone is selected, the device notifies the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

To configure time by the device web interface:

Phone > Time/Lang



Format Setting

Time Format: 12h
Date Format: DD-MM-YYYY

Type

☐ Manual ☑ Auto

Date: Year, Mon, Day
Time: Hour, Min, Sec

NTP

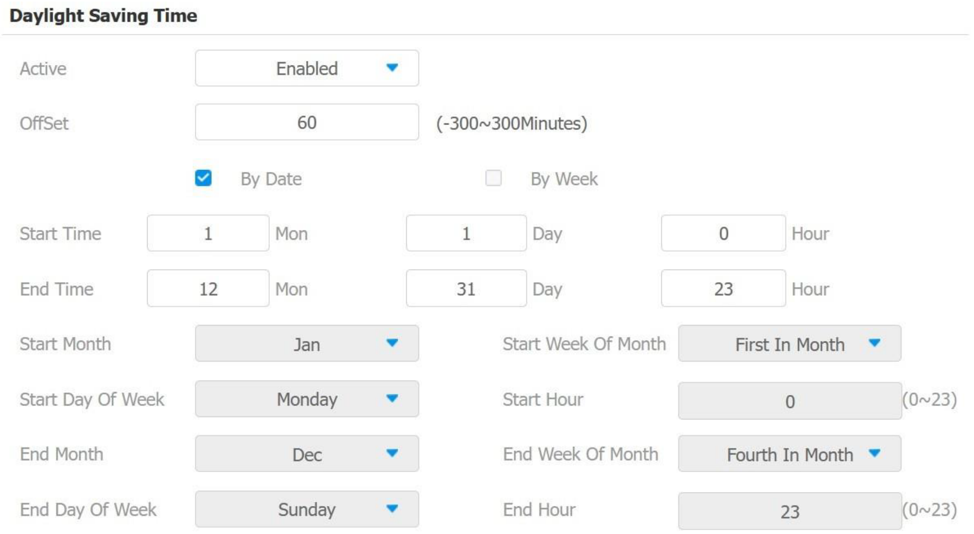
Time Zone: GMT+0:00 London
Primary Server: 0.pool.ntp.org
Secondary Server: 1.pool.ntp.org
Update Interval: 3600 (>= 3600s)

5.2.3 - Daylight saving time setting

The daylight Saving Time is the practice of advancing clocks (typically by one hour) during warmer months so that darkness falls at a later clock time. You can modify the time settings to achieve longer evenings or daytime, especially in summer.

To configure the daylight saving time by the device web interface:

Phone > Time/Lang



Daylight Saving Time

Active: Enabled
OffSet: 60 (-300~300Minutes)

☑ By Date ☐ By Week

Start Time: 1 Mon, 1 Day, 0 Hour
End Time: 12 Mon, 31 Day, 23 Hour
Start Month: Jan
Start Week Of Month: First In Month
Start Day Of Week: Monday
Start Hour: 0 (0~23)
End Month: Dec
End Week Of Month: Fourth In Month
End Day Of Week: Sunday
End Hour: 23 (0~23)

Table A4 - MyBell 2-Wire Indoor Monitor - Configuration of the daylight saving time

Setting	Description
Active	To enable or disable the daylight saving time. You can also configure it to make the device adjust the daylight saving time automatically.
Offset	To set the offset value. The default value is 60 minutes, which sets the clocks an hour ahead of the standard time.
By Date	To set the date schedule for the daylight saving time
By Week	To set the schedule for the daylight saving time according to the week and month

6 SCREEN DISPLAY CONFIGURATION

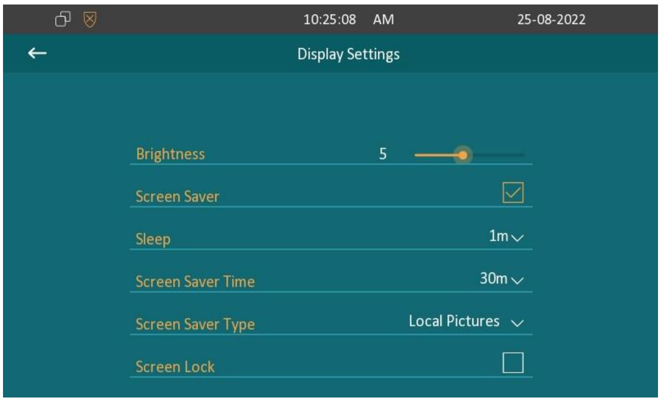
The device enables you to enjoy a variety of screen displays to enrich your visual experience through settings customized to your preference.

6.1 - Screen display setting on the device

You can configure a variety of features of the screen display such as brightness or a screen saver.

To configure a screen display on the device:

More > Setting > Display



10:25:08 AM 25-08-2022

Display Settings

Brightness 5

Screen Saver ☑

Sleep 1m

Screen Saver Time 30m

Screen Saver Type Local Pictures

Screen Lock □

Table A5 - MyBell 2-Wire Indoor Monitor - Configuration of the daylight saving time

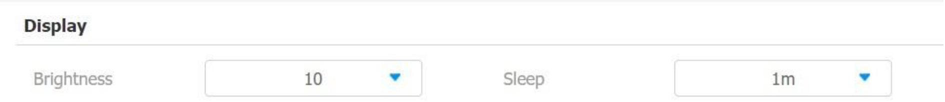
Setting	Description
Brightness	Press on the brightness setting and move the yellow dot to adjust the screen brightness. The default brightness is 5.
Sleep	Set the sleep timing based on the screen saver. The time range is from 15 second to 30 minutes. • If the screen saver is enabled, the sleep time is the screen saver start time. For example, if you set the sleep timing to 1 minute, the screen saver starts automatically when the device has no operation for 1 min. • If the screen saver is disabled, the sleep time is the screen turn-off time. For example, if you set the sleep timing to 1 minute, the screen is turned off automatically when the device has no operation for 1 min.
Screen Lock	Tick the screen lock if you want to lock the screen after the screen is turned off (turn dark). You are required to enter the system code to unlock the screen or you can unlock the screen by facial recognition.
Screen Saver Time	Set the screen saver duration. The time range is from 15 minutes to 2 hours.
Screen Saver Type	Select screen saver type • **Local Pictures:** Display picture uploaded to the indoor monitor as the screen saver. • **Clock:** Display the clock as the screen saver.

6.2 - Screen display setting by the web interface

6.2.1 - Brightness and time setting by the device web interface

To configure brightness and sleep by the device web interface:

Phone > Key/Display > Display



Display

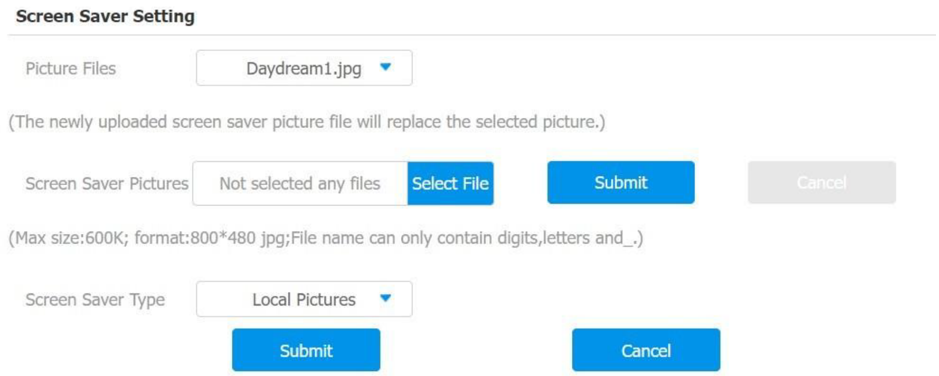
Brightness 10

Sleep 1m

6.2.2 - Screen saver configuration

To upload a screen saver by the web interface:

Phone > Display Setting > Screen Saver Setting



Screen Saver Setting

Picture Files Daydream1.jpg

(The newly uploaded screen saver picture file will replace the selected picture.)

Screen Saver Pictures Not selected any files

(Max size:600K; format:800*480 jpg;File name can only contain digits,letters and_.)

Screen Saver Type Local Pictures

Table A6 - MyBell 2-Wire Indoor Monitor - Configuration of the screen saver

Setting	Description
Picture File	Choose a picture file you want to use for the screen saver.
Screen Saver Pictures	Choose a picture from the PC and upload the picture to the indoor monitor.
Screen Saver Type	Select screen saver type • **Local Pictures:** Display picture uploaded to the indoor monitor as the screen saver. • **Clock:** Display the clock as the screen saver.

Note.

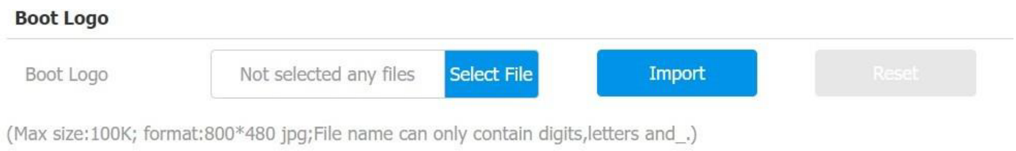
- The previous pictures with a specific ID order is overwritten when repetitive designation of pictures to the same ID order occurrs.
- The pictures uploaded should be in .jpg format with 600 k maximum.

6.3 - Uploading a device booting image

You can upload the booting image to be displayed during the device's booting process if needed.

To upload a booting image:

Phone > Logo > Boot Log



Boot Logo

Boot Logo: Not selected any files

(Max size:100K; format:800*480 jpg;File name can only contain digits,letters and_.)

Note.

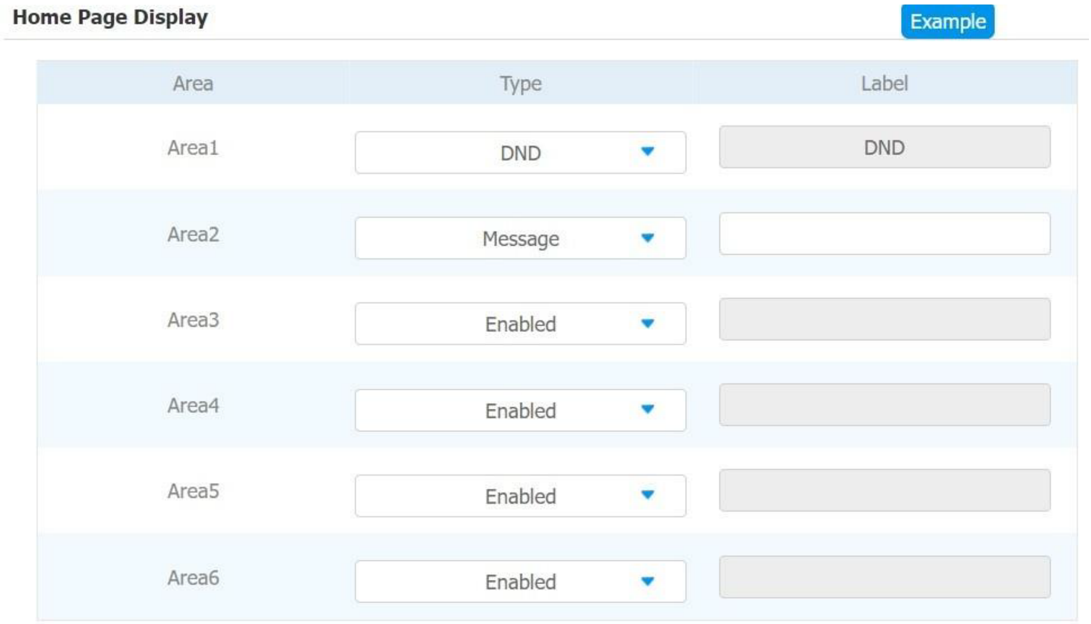
- The pictures uploaded should be in .png format with 50 k maximum.

6.4 - Icon screen display configuration

You can customize icon display on the Home screen and More screen for the convenience of your operation.

To customize icon display:

Phone > Key/Display



Home Page Display

Area	Type	Label
Area1	DND	DND
Area2	Message	
Area3	Enabled	
Area4	Enabled	
Area5	Enabled	
Area6	Enabled	

Setting

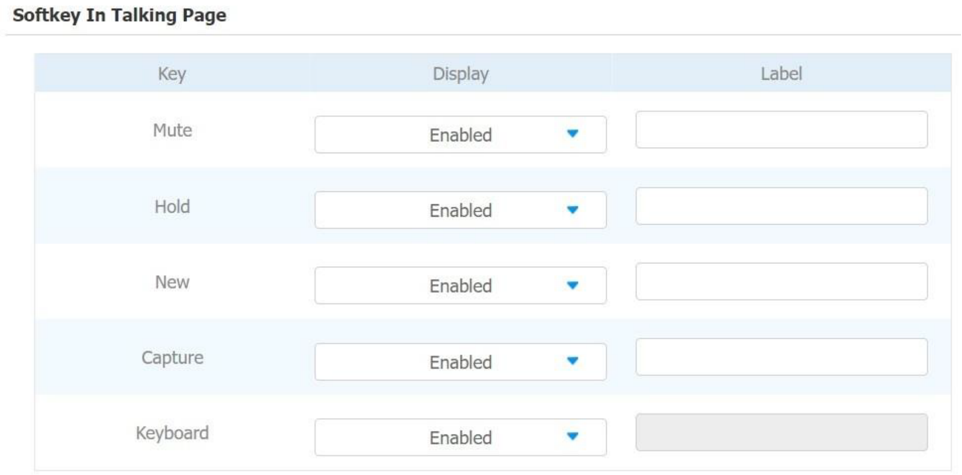
- **Type**: click to select among icon options (DND, Message, Contact, Call, Display, Status, Setting, Sound, Arming, SOS, Relay, Lift, Smart Living, Unlock, N/A). When N/A is selected, the icon displayed in the corresponding area disappears.
- **Label:** click to rename the icon if needed, while DND icon can't be renamed.
- You can configure 2 icons in area 1 and 2, or toggle whether to display area 3, 4, 5 and 6.
- You can configure 8 icons on the More screen.

6.5 - Functional buttons display

You can enable various types of functional buttons, which appear on the screen when you talk. You can also name the button if needed.

To configure functional buttons display:

Phone > Key/Display > Softkey In Talking Page



Softkey In Talking Page

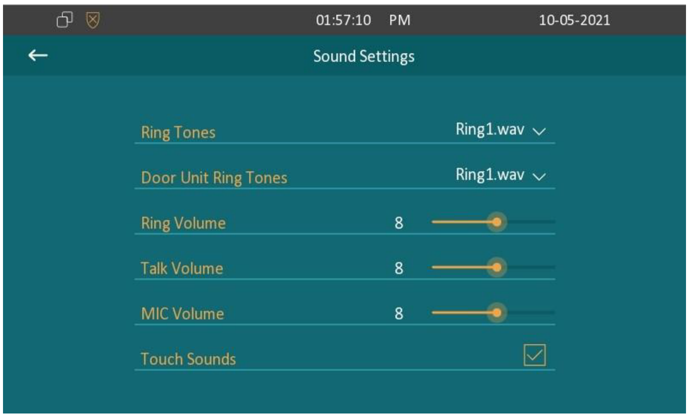
Key	Display	Label
Mute	Enabled	
Hold	Enabled	
New	Enabled	
Capture	Enabled	
Keyboard	Enabled	

7 SOUND AND VOLUME CONFIGURATION

7.1 - Configuring volume on the device

To configure volume on the device:

More > Setting > Sound



01:57:10 PM 10-05-2021

Sound Settings

Ring Tones	Ring1.wav
Door Unit Ring Tones	Ring1.wav
Ring Volume	8
Talk Volume	8
MIC Volume	8
Touch Sounds	☑

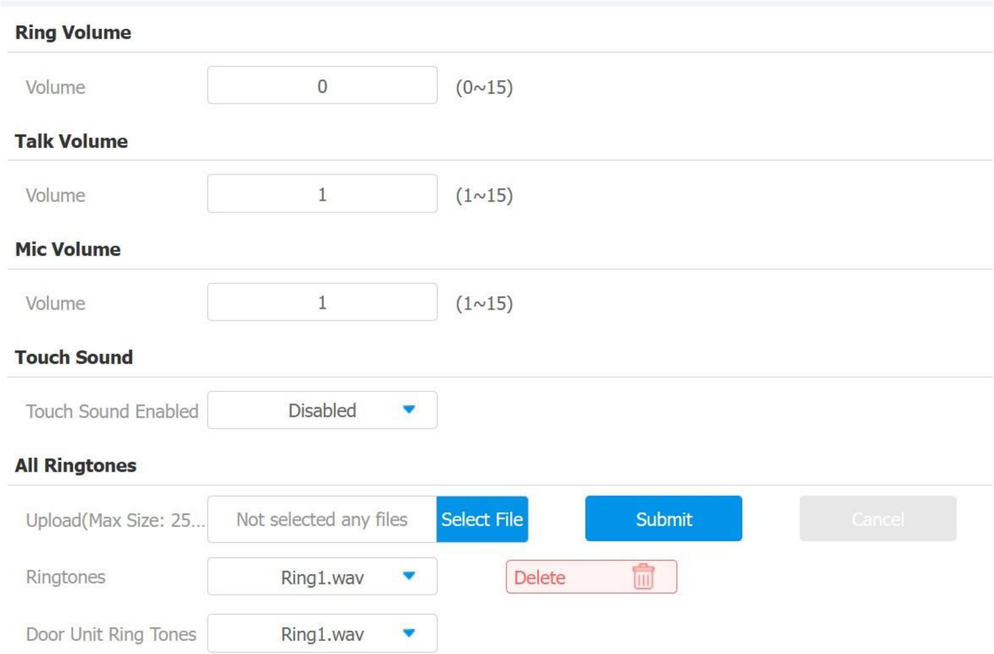
With **Door Unit Ring Tones** you can set ring tone when receiving calls from door units.

7.2 - Configuring volume by the web interface

By the web interface, you can set the ring volume or mic volume. You can also upload ringtones.

To configure volume by the web interface:

Phone > Audio



Ring Volume

Volume	0	(0~15)

Talk Volume

Volume	1	(1~15)

Mic Volume

Volume	1	(1~15)

Touch Sound

Touch Sound Enabled	Disabled

All Ringtones

Upload(Max Size: 25...	Not selected any files	Select File · Submit · Cancel
Ringtones	Ring1.wav	Delete
Door Unit Ring Tones	Ring1.wav	

With **Door Unit Ring Tones** you can set ring tone when receiving calls from door units.

Note.

Doorbell sound files to be uploaded must be in .WAV format with 250 k maximum.

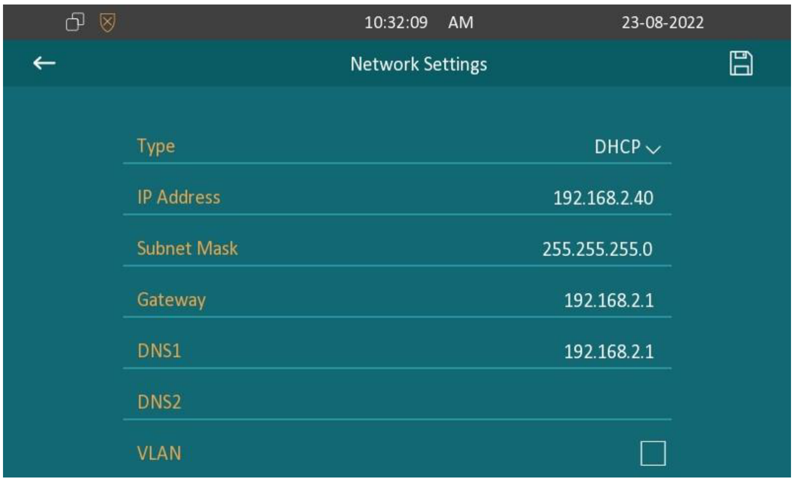
8 NETWORK CONFIGURATION

You can check the indoor monitor network connection info and configure the default Dynamic Host Configuration Protocol (DHCP) mode and a static IP connection for the device either on the device or by the device web interface.

8.1 - Configuring network connection on the device

To check and configure the network connection on the device:

More > Setting > Advance > Network



10:32:09 AM 23-08-2022

Network Settings

Type	DHCP
IP Address	192.168.2.40
Subnet Mask	255.255.255.0
Gateway	192.168.2.1
DNS1	192.168.2.1
DNS2	
VLAN	□

Table A7 - MyBell 2-Wire Indoor Monitor - Configuration of the network on the device

Setting	Description
Type	Select the **DHCP** mode or **Static IP** mode. DHCP mode is the default network connection. If the DHCP mode is selected, the indoor monitor is assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically. When Static IP mode is selected, the IP address, subnet mask, default gateway, and DNS servers address have to be configured manually according to your actual network environment.
IP Address	Set up the IP Address if the **Static IP** mode is selected.
Subnet Mask	Set up the subnet mask according to your actual network environment.
Gateway	Set up the gateway according to the IP address.
LAN DNS 1/2	Set up a preferred or alternate Domain Name Server (DNS) according to your actual network environment. The preferred DNS is the primary DNS address while the alternate DNS is the secondary DNS address. The indoor monitor connects to the alternate server when the primary DNS server is unavailable.

Note.

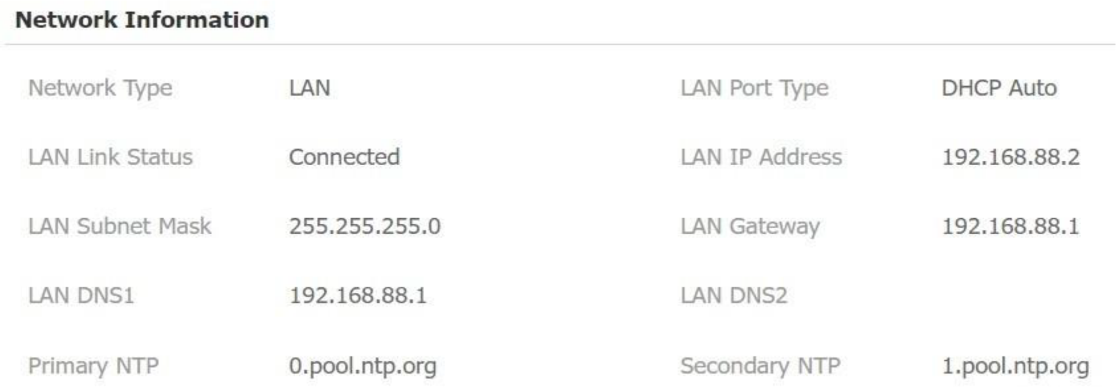
You can press **Status** icon and then press **Network** tab on the Setting screen to check the device network status.

The default system code is **123456** .

8.2 - Configuring network connection by the web interface

To check the network connection by the web interface:

Status > Network Information

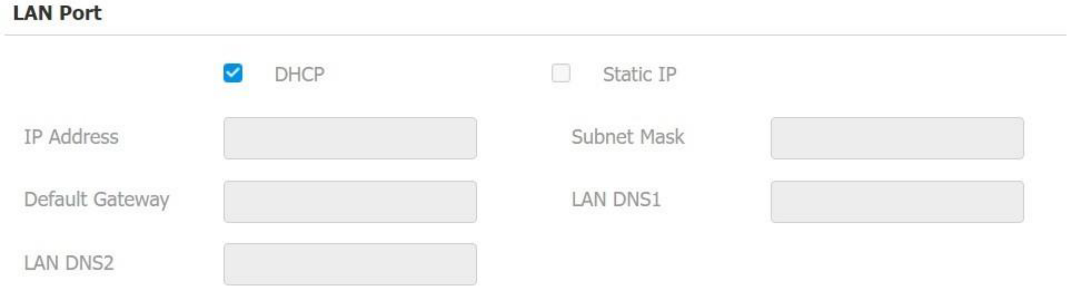


Network Information

Network Type	LAN	LAN Port Type	DHCP Auto
LAN Link Status	Connected	LAN IP Address	192.168.88.2
LAN Subnet Mask	255.255.255.0	LAN Gateway	192.168.88.1
LAN DNS1	192.168.88.1	LAN DNS2	
Primary NTP	0.pool.ntp.org	Secondary NTP	1.pool.ntp.org

To configure the network connection by the web interface:

Network > Basic



LAN Port

☑ DHCP ☐ Static IP

IP Address		Subnet Mask	
Default Gateway		LAN DNS1	
LAN DNS2			

Table A8 - MyBell 2-Wire Indoor Monitor - Configuration of the network by the web interface

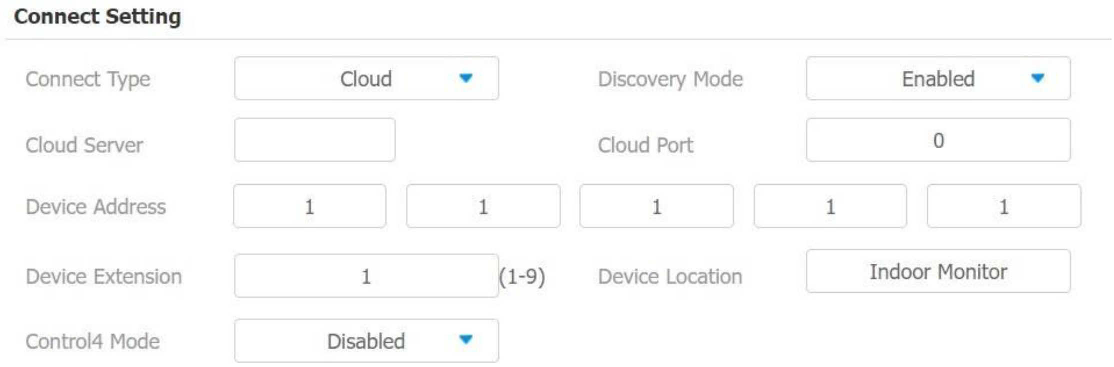
Setting	Description
DHCP	Select the **DHCP** mode by ticking the DHCP box. The DHCP mode is the default network connection. If the DHCP mode is selected, the indoor monitor is assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS address automatically.
Static IP	When the **Static IP** mode is selected, then the IP address, subnet mask, default gateway, and DNS address have to be configured manually according to your actual network environment.
IP Address	Set up the IP Address if the **Static IP** mode is selected.
Subnet Mask	Set up the subnet mask according to your actual network environment.
Gateway	Set up the gateway according to the IP address.
LAN DNS 1/2	Set up a preferred or alternate Domain Name Server (DNS) according to your actual network environment. The preferred DNS is the primary DNS address while the alternate DNS is the secondary DNS address. The indoor monitor connects to the alternate server when the primary DNS server is unavailable.

8.3 - Device deployment in the network

Indoor monitors should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address, and extension numbers for the convenience of management.

To deploy the device in the network by the web interface:

Network > Advanced > Connect Setting



Connect Setting

Connect Type	Cloud		Discovery Mode	Enabled	
Cloud Server			Cloud Port	0	
Device Address	1	1	1	1	1
Device Extension	1	(1-9)	Device Location	Indoor Monitor	
Control4 Mode	Disabled				

Table A9 - MyBell 2-Wire Indoor Monitor - The device deployment in the network

Setting	Description
Connect Type	It's set up automatically according to the actual device connection with a specific server in the network such as **SDMC Cloud or None**. None is the default factory setting indicating the device isn't in any server type, therefore you are allowed to choose Cloud, SDMC in the discovery mode.
Cloud Server	If you deploy your devices in a local cloud server, enter the local server RPS address. The device data redirects to the local server automatically.
Cloud Port	Enter the local cloud server port for the data transmission.
Discovery Mode	Turn on the discovery mode of the device so that it can be discovered by other devices in the network, and disable it if you want to conceal the device so as not to be discovered by other devices.
Device Address	Specify the device address by entering device location info from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
Device Extension	Enter the device extension number for the device you installed.
Device Location	Enter the location in which the device is installed and used to distinguish the device from others.

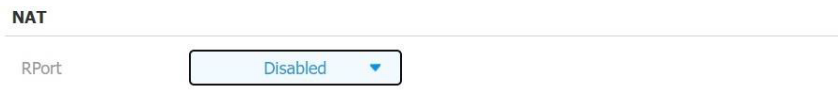
8.4 - Device NAT setting

Network Address Translation (NAT) enables hosts in an organization private intranet to connect transparently to hosts in the public domain.

There is no need for internal hosts to have registered Internet addresses. It is a way to translate an internal private network IP address into a legal network IP address technology.

To set up NAT by the web interface:

Account > Advanced > NAT



NAT

RPort	Disabled

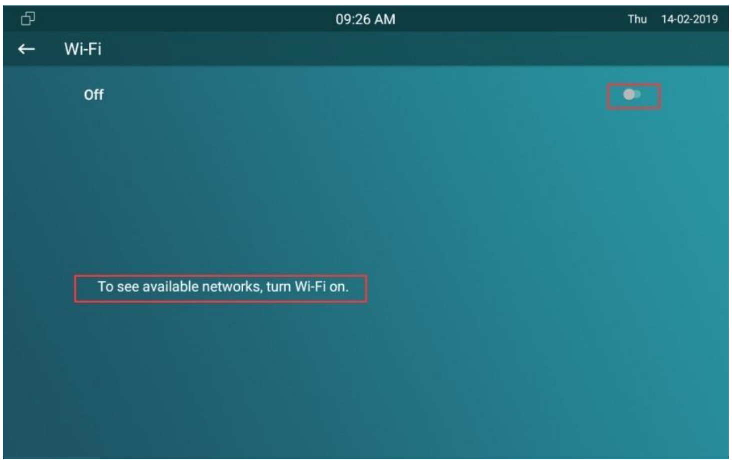
RPort option checks the RPort when the SIP server is in Wide Area Network (WAN).

8.5 - Device Wi-Fi setting

In addition to a wired connection, the device also supports Wi-Fi connection.

To set Wi-Fi on the device screen:

More > Setting > Advance > Network



09:26 AM Thu 14-02-2019

Wi-Fi

Off

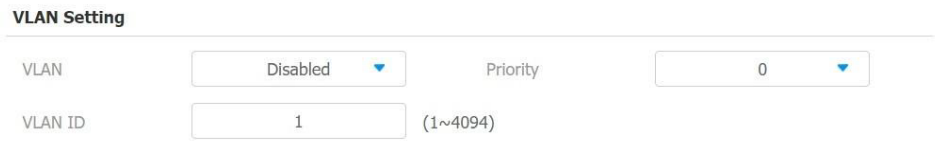
To see available networks, turn Wi-Fi on.

8.6 - VLAN setting

Virtual Local Area Network (VLAN) is a logical group of nodes from the same IP domain, regardless of their physical network segment. It separates the layer 2 broadcast domain through switches or routers, sending tagged packets only to ports with matching VLAN IDs. Utilizing VLANs enhances security by limiting ARP attacks to specific hosts and improves a network performance by minimizing unnecessary broadcast frames, thereby conserving bandwidth for increased efficiency.

To configure the VLAN function by the device web interface:

More > Setting > Advance > VLAN Setting



VLAN Setting

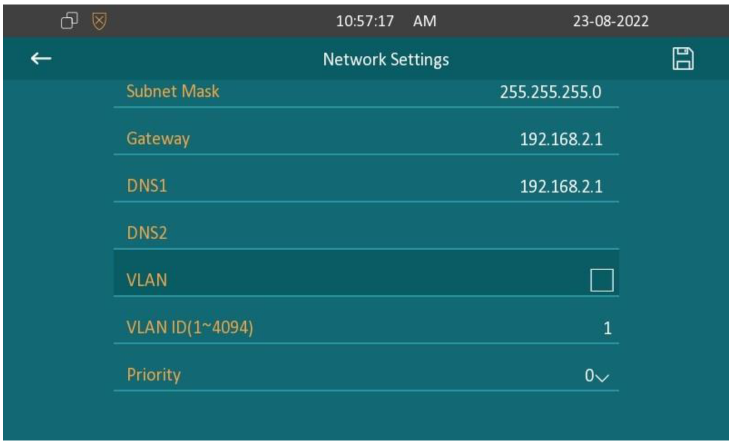
VLAN	Disabled	Priority	0
VLAN ID	1	(1~4094)	

Setting:

- **Priority:** VLAN Priority lets you assign a priority to outbound packets containing the specified VLAN-ID (VID). Packets containing the specified VID are marked with the priority level configured for the VID classifier.
- **VLAN ID:** Set the same VLAN ID as the switch or router.

To configure the VLAN function on the device:

More > Setting > Advance > Network



10:57:17 AM 23-08-2022

Network Settings

Subnet Mask	255.255.255.0
Gateway	192.168.2.1
DNS1	192.168.2.1
DNS2	
VLAN	□
VLAN ID(1~4094)	1
Priority	0

9 PHONE BOOK CONFIGURATION

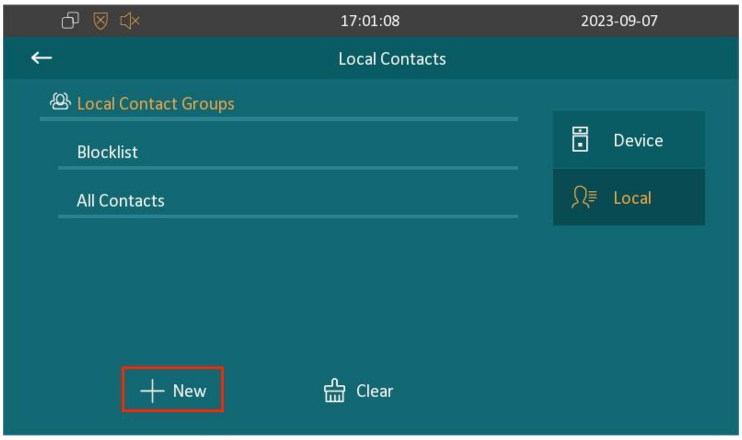
9.1 - Configuring the phone book on the device

You can create contacts and contact groups for users.

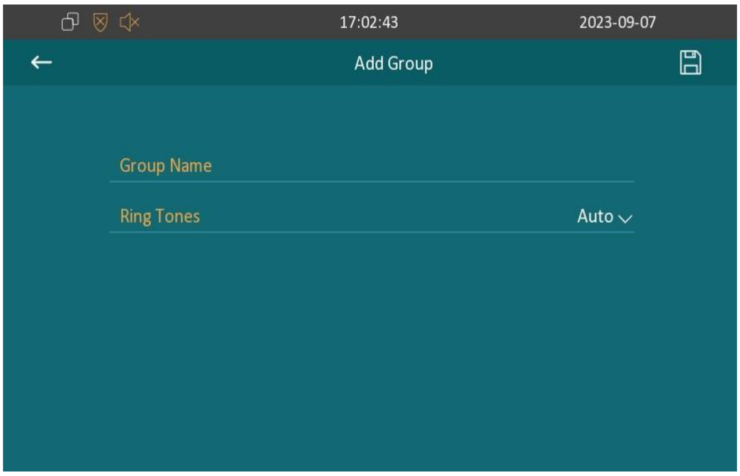
9.1.1 - Adding a contact group on the device

To add a contact group on the device screen:

More > Contacts > New



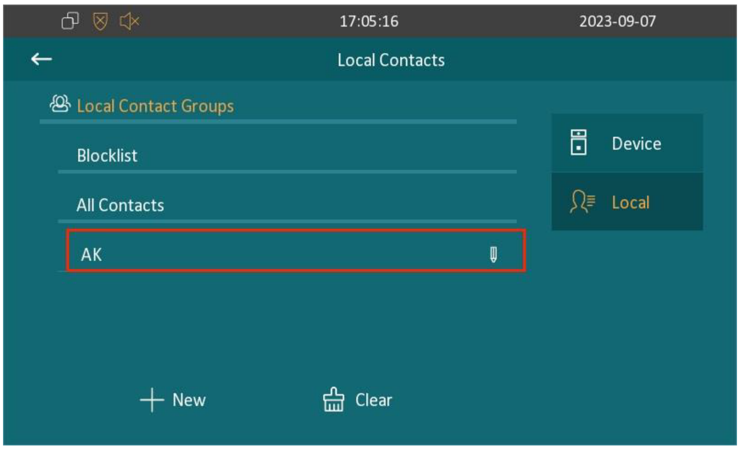
Enter a group name and press **Save** tab.

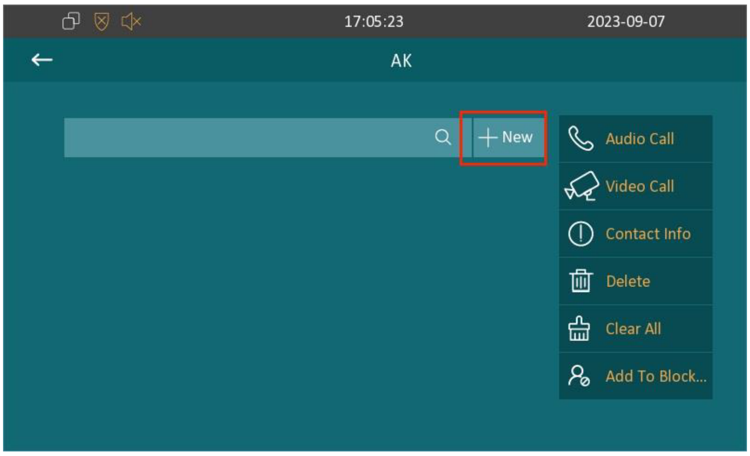


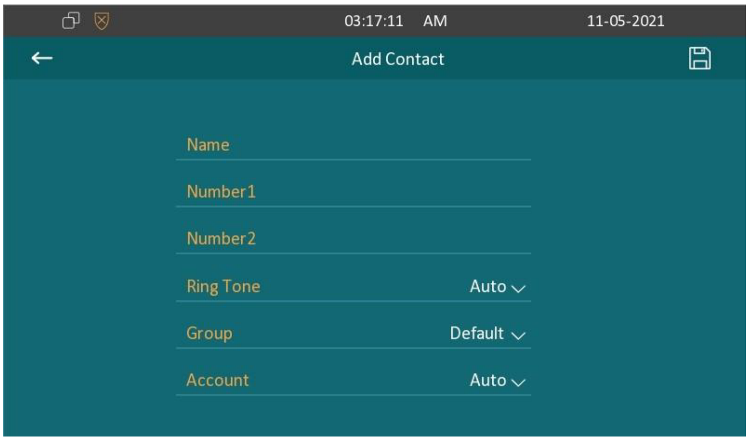
9.1.2 - Adding contacts on the device

To add a contact on the device screen:

More > Contacts > the desired group > New







Name

Number1

Number2

Ring Tone: Auto

Group: Default

Account: Auto

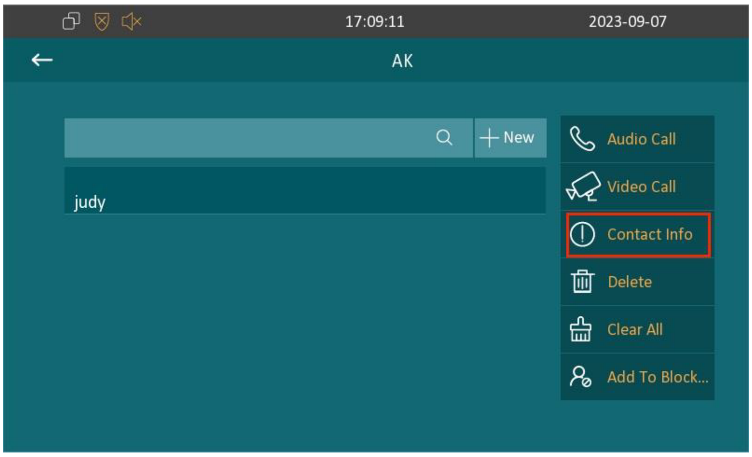
Setting:

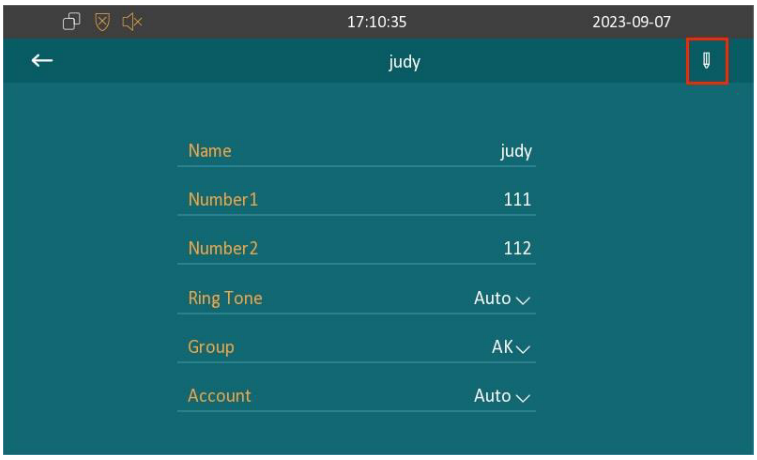
- **Number:** Enter the IP or SIP number.
- **Group:** Select Default or any other groups that were created.

9.1.3 - Editing contacts on the device

To edit a contact on the device screen:

The desired contact > Contact Info > Edit





Name: judy

Number1: 111

Number2: 112

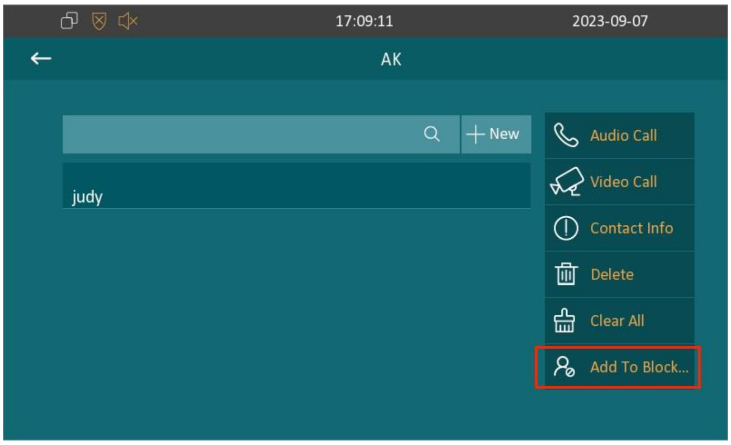
Ring Tone: Auto

Group: AK

Account: Auto

9.1.4 - Blocklist setting on the device

You can choose from the contact list the contact you want to add to the block list.
Configure the blocklist setting on the Contacts screen.



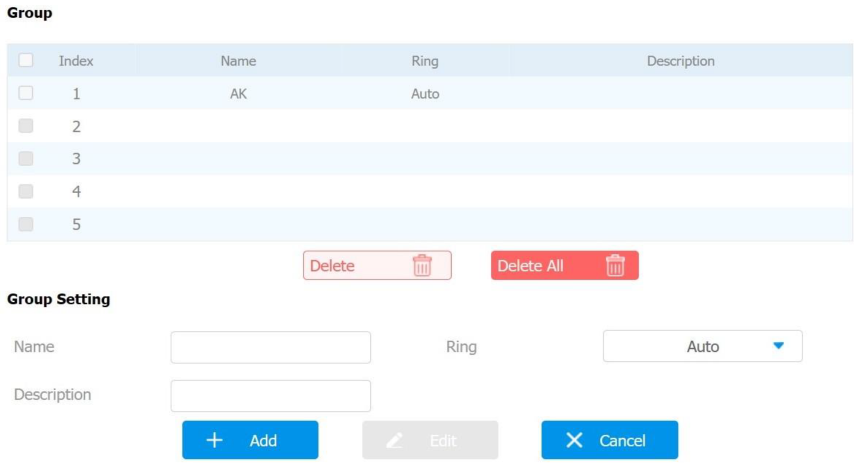
Note.
You can delete contacts regardless of whether it is on the All Contacts screen or the Blocklist screen.

9.2 - Phone book configuration by the web interface

9.2.1 - Contact group management by the web interface

You can create and edit a contact group for contacts. The contact group is used when you add a user.
To add or edit a contact group by the web interface:

Contacts > Local Contacts



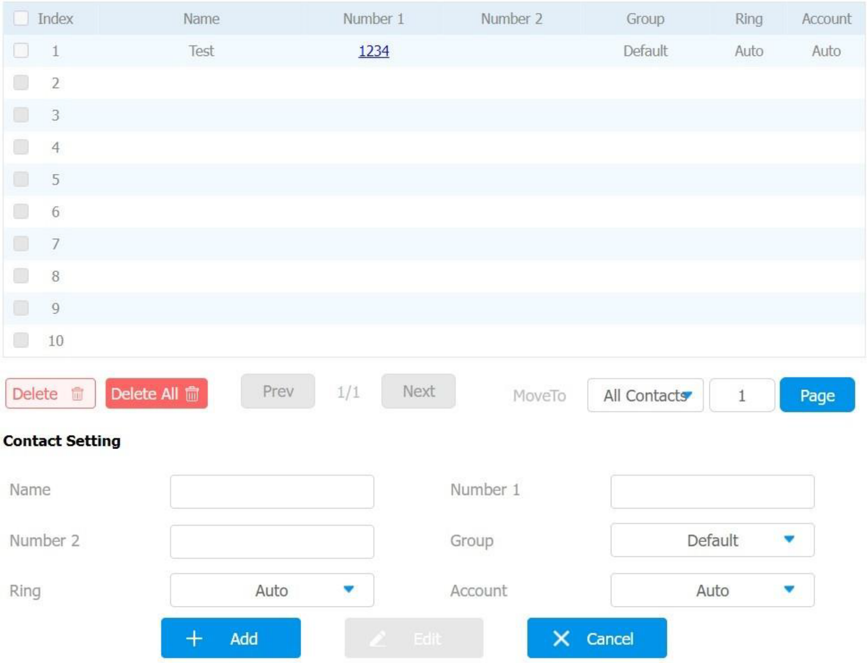
Group

□	Index	Name	Ring	Description
□	1	AK	Auto	
□	2			
□	3			
□	4			
□	5			

Group Setting

Name		Ring	Auto
Description			

The existing contacts are show in the below list after they are added.



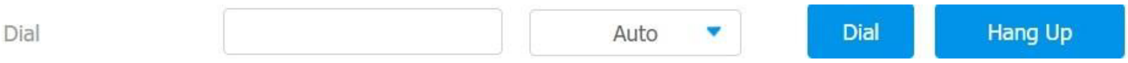
□	Index	Name	Number 1	Number 2	Group	Ring	Account
□	1	Test	1234		Default	Auto	Auto
□	2						
□	3						
□	4						
□	5						
□	6						
□	7						
□	8						
□	9						
□	10						

Contact Setting

Name		Number 1	
Number 2		Group	Default
Ring	Auto	Account	Auto

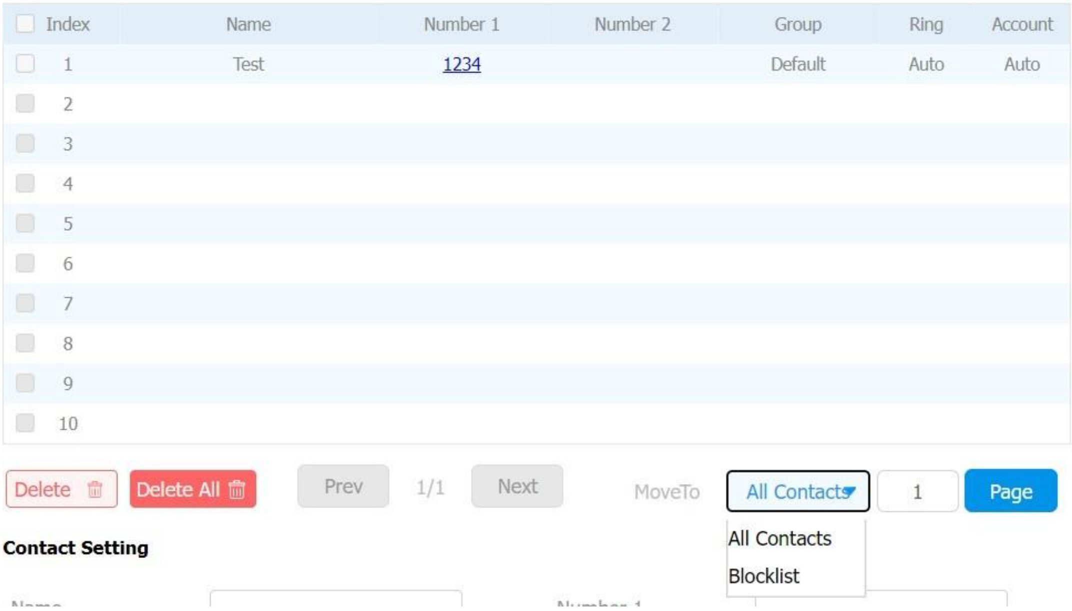
Table A10 - MyBell 2-Wire Indoor Monitor - Contact management by the web interface	
Setting	**Description**
Number	Enter the contact number (SIP or IP number) to be saved.
Group	Select Default, a Blocklist group or a group created.
Account	Select Account 1 or Account 2.

You can dial out a number using the contact phone number.
To dial out a number:
Contacts > Local Contacts.



9.2.2 - Blocklist setting by the web interface

You can set the blocklist directly in the contact list by the web interface or set it when editing a contact.
To block a contact by the web interface:
Contacts > Local Contacts > Local Contacts List

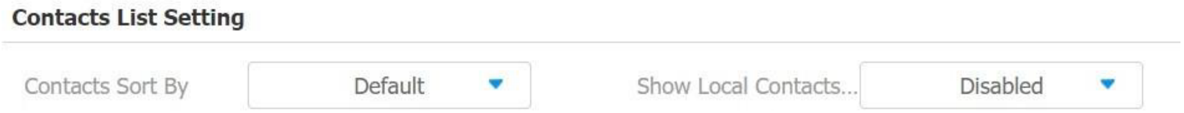


□ Index	Name	Number 1	Number 2	Group	Ring	Account
□ 1	Test	1234		Default	Auto	Auto
□ 2						
□ 3						
□ 4						
□ 5						
□ 6						
□ 7						
□ 8						
□ 9						
□ 10						

Note.
If you want to remove the contact from the blocklist by the web interface, you can change the group to **Default** when editing the contact.

9.2.3 - Contact display

You can configure the contact display order and control whether to display the discovery device on the device.
To configure the contact display by the web interface:
Contacts > Local Contacts



Contacts List Setting

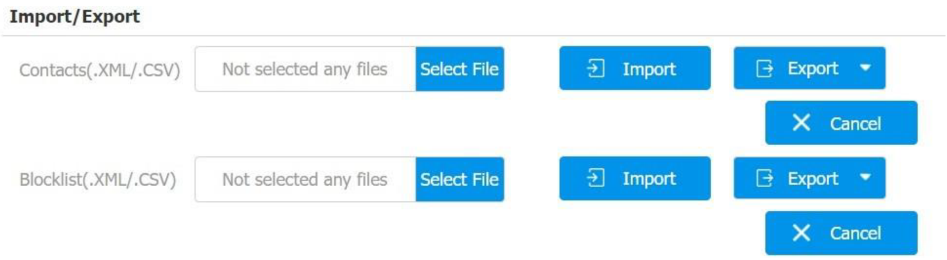
Contacts Sort By: Default
Show Local Contacts...: Disabled

Setting:

- **Contacts Sort By:** There are three modes **Default, ASCII Code** and **Created** Time for showing the contact list.
- **Show Local Contacts Only:** If the function is enabled, the contact on device shows only a local phonebook, the contact for discovery mode is hidden.

9.2.4 - Contacts import and export by the web interface

If there are too many contacts to manage them one by one manually, you can import and export them in batch using the device web interface.
To import and export contacts by the web interface:
Contacts > Local Contacts



Note.

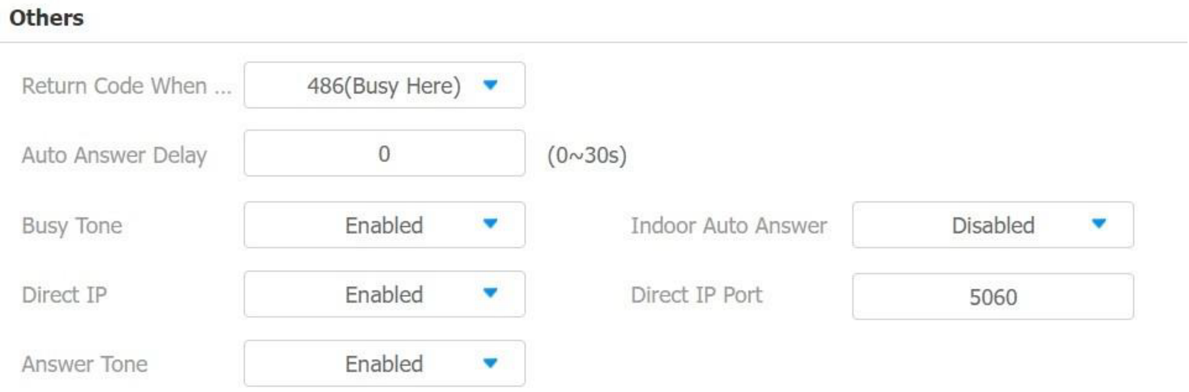
The contact file can only be imported or exported in .xml or .csv format.

10.1 - IP call & IP call configuration

IP calls and SIP calls can be made directly on the device by entering the IP number. You can also disable the direct IP calls so that no IP calls can be made.

To configure IP calls:

Phone > Call Feature > Others



Others

Return Code When ...	486(Busy Here) ▾		
Auto Answer Delay	0	(0~30s)	
Busy Tone	Enabled ▾	Indoor Auto Answer	Disabled ▾
Direct IP	Enabled ▾	Direct IP Port	5060
Answer Tone	Enabled ▾		

Setting:

- **Direct IP:** If you don't want direct IP calls to be made by the device, you can untick the check box to disable this function.
- **Direct IP Port:** The direct IP port is **5060** by default. The range for direct IP port is from 1 to 65535. If you enter any other values within the range, you need to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

10.2 - SIP call &SIP call configuration

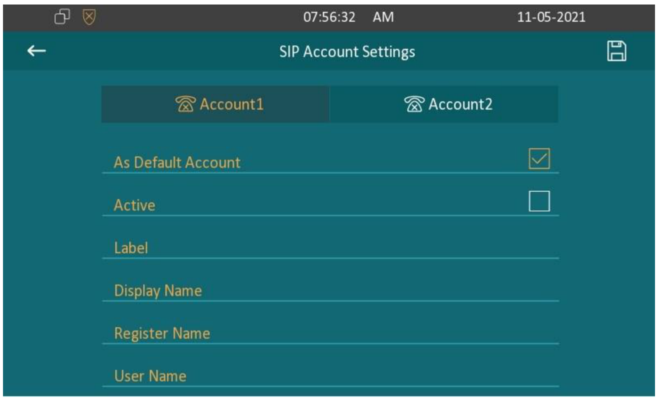
You can make a Session Initiation Protocol (SIP) call in the same way as you make the IP calls using the device. However, SIP call settings related to its account, server, and transport type need to be configured first

10.2.1 - SIP account registration

The indoor monitors support two SIP accounts that can be registered according to your applications. You can, for example, switch between them if one of the accounts fails and becomes invalid. The SIP account can be configured on the device or by the web interface.

To configure the SIP account on the device screen:

More > Setting > Advance > SIP Account



07:56:32 AM 11-05-2021

SIP Account Settings

Account1 | Account2

As Default Account ☑

Active □

Label

Display Name

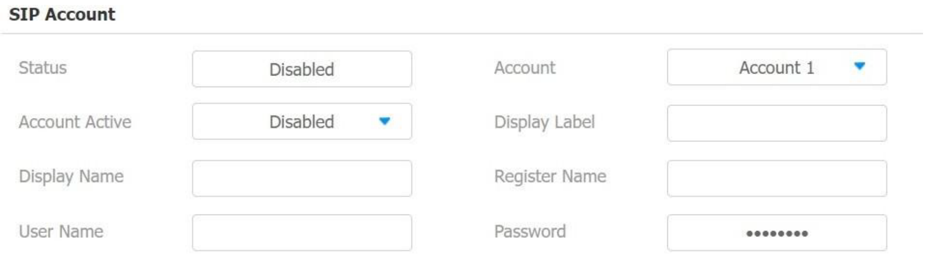
Register Name

User Name

To configure the SIP account by the web interface:

Account > Basic > SIP Account

Register Name, User Name, and **Password** are obtained from the SIP account administrator.



SIP Account

Status	Disabled	Account	Account 1 ▾
Account Active	Disabled ▾	Display Label	
Display Name		Register Name	
User Name		Password	••••••••

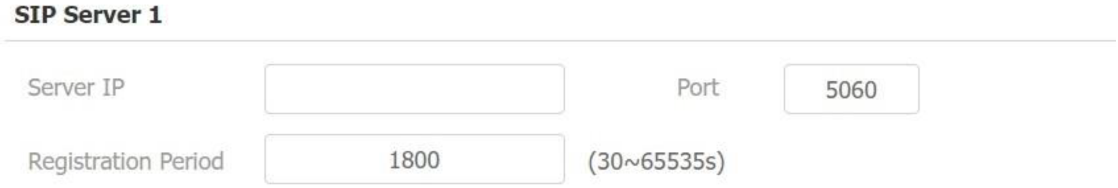
Table A11 - MyBell 2-Wire Indoor Monitor - Configuration of a SIP account by the web interface	
Setting	**Description**
Status	It enables to see if the SIP account is registered.
Account	Select Account 1 or Account 2.
Account Enabled	Enables to activate the registered SIP account.
Display Label	Configure the name, for example, the device name to be shown on the device being called to. Configure the device label to be shown on the device screen.
Display Name	Configure the name, for example, the device name to be shown on the device being called to.

10.2.2 - SIP server configuration

SIP servers can be set up for devices to achieve call sessions through SIP servers between intercom devices.

To set the SIP account by the web interface:

Account > Basic > SIP Server



SIP Server 1

Server IP

Port 5060

Registration Period 1800 (30~65535s)

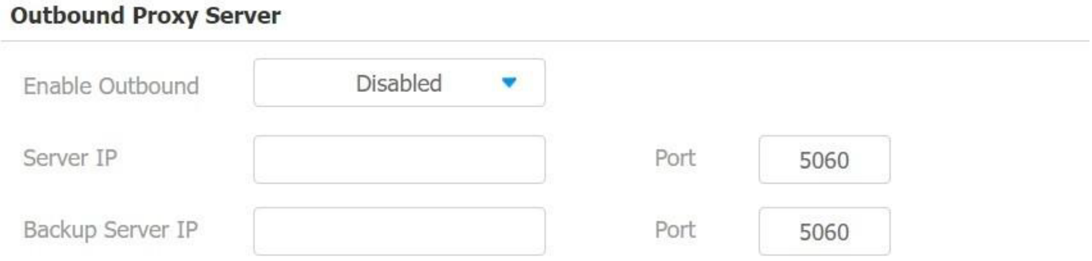
Table A12 - MyBell 2-Wire Indoor Monitor - Configuration of a SIP server by the web interface	
Setting	**Description**
Server IP	Enter the server IP address number or its URL.
Port	Set up the SIP server port for data transmission.
Registration Period	Set up the SIP account registration time span. A SIP re-registration starts automatically if the account registration fails during the registration time span. The default registration period is 1800 and it can range from 30 to 65535 seconds.

10.2.3 - Outbound proxy server configuration

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server to establish call sessions by port-based data transmission.

To configure the outbound proxy server by the web interface:

Account > Basic > Outbound Proxy Server



Outbound Proxy Server

Enable Outbound Disabled

Server IP

Port 5060

Backup Server IP

Port 5060

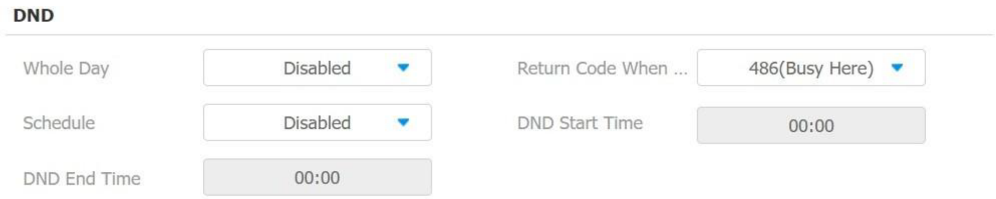
Table A13 - MyBell 2-Wire Indoor Monitor - Configuration of an outbound proxy server by the web interface	
Setting	**Description**
Server IP	Enter the IP address of the outbound proxy server.
Backup Server IP	Set up a backup server IP for the backup outbound proxy server.
Port	Enter the port number to establish a call session through the outbound proxy server or the backup one.

10.3 - DND

Do not disturb (DND) setting enables you not to be disturbed by any unwanted incoming SIP calls. You can set up DND-related settings by the device web interface to block SIP calls you don't intend to answer. You can also define the code to be sent to the SIP server when you want to reject the call.

To configure DND by the web interface:

Phone > Call Feature > DND



DND

Whole Day: Disabled

Return Code When ...: 486(Busy Here)

Schedule: Disabled

DND Start Time: 00:00

DND End Time: 00:00

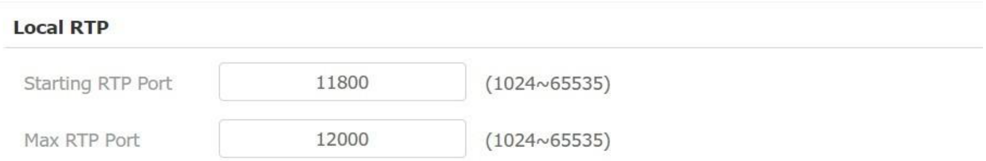
Table A14 - MyBell 2-Wire Indoor Monitor - Configuration of DND	
Setting	**Description**
DND	Check the Whole Day or Schedule to enable the DND function. The DND function is disabled by default.
Schedule	Enable the DND schedule for your indoor monitor. To configure a specific time to enable the DND feature. If you choose Schedule for DND, the whole day is checked on the device.
Return Code When DND	Select what code should be sent to the calling device through the SIP server: • 404 for Not found • 480 for Temporary Unavailable • 486 for Busy Here • 603 for Decline

10.4 - Configuring the device local RTP

For the device network data transmission purpose, the device needs to be set up with a range of Real- time Transport Protocol (RTP) ports for establishing an exclusive range of data transmission in the network.

To set up device local RTP by the web interface:

Network > Advanced > Local RTP



Local RTP

Starting RTP Port: 11800 (1024~65535)

Max RTP Port: 12000 (1024~65535)

Setting:

- **Starting RTP Port:** Enter the port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port:** Enter the port value to establish the endpoint for the exclusive data transmission range.

10.5 - Configuring a data transmission type

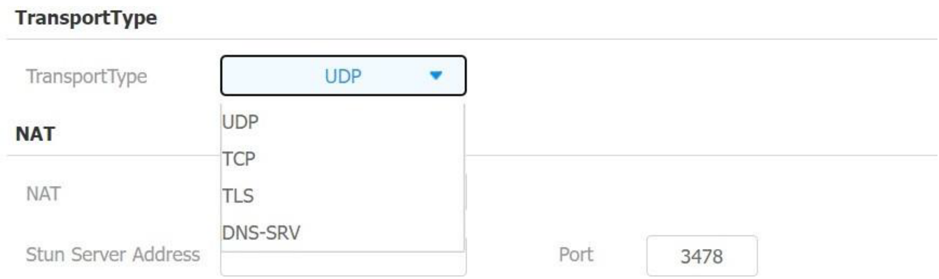
SIP messages can be transmitted in the following data transmission protocols:

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- Transport Layer Security (TLS)
- DNS-SRV.

In the meantime, you can also identify the server from which the data comes.

To set up data transmission type by the web interface:

Account > Basic > Transport Type



TransportType

TransportType: UDP

NAT

NAT

Stun Server Address

Port: 3478

Table A15 - MyBell 2-Wire Indoor Monitor - Configuration of a data transport type	
Setting	**Description**
UDP	Select UDP for unreliable but a very efficient transport layer protocol. UDP is the default transport protocol.
TCP	Select TCP for a reliable but less-efficient transport layer protocol.
TLS	Select TLS for a secured and reliable transport layer protocol.
DNS-SRV	Select DNS-SRV to obtain a DNS record for specifying the location of services. SRV records the server address and the server port. SRV can also be used to configure the priority and the weight of the server address.

11 DOOR ACCESS CONTROL CONFIGURATION

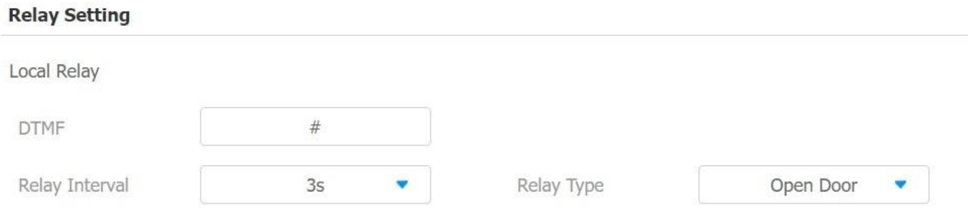
11.1 - Relay switch setting

11.1.1 - Local relay setting

Local relays in the device can be used to trigger the relay for the door access and trigger a chime bell as needed in different scenarios.

To configure a local relay by the device web interface:

Phone > Relay > Relay Setting > Local Relay



Relay Setting

Local Relay

DTMF: #

Relay Interval: 3s ▼ Relay Type: Open Door ▼

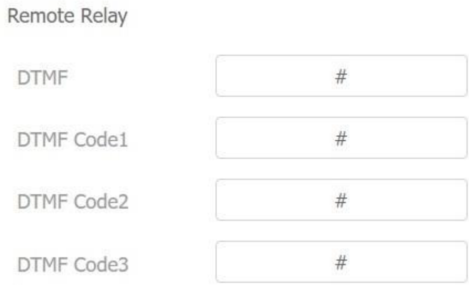
Table A16 - MyBell 2-Wire Indoor Monitor - Local relay setting	
Setting	**Description**
DTMF	Set the DTMF code for the local relay.
Relay Interval	Set the relay delay time after the relay is triggered.
Relay Type	Set a relay action type choosing one of the following optoions: • Chime Bell - when there is a call, a chime bell rings • Open Door - when press the unlock icon, the local relay opens • Other Switches (Reset By Event) - when the call is answered, the relay is reset

11.1.2 - Remote relay switch setting

You can use the unlock tab during the call to open the door. And you are required to set up the same DTMF code in the door phone and indoor monitor.

To configure a remote switch relay by the device web interface:

Phone > Relay > Relay Setting > Remote Relay



Remote Relay

DTMF: #

DTMF Code1: #

DTMF Code2: #

DTMF Code3: #

Setting:

- **DTMF Code:** To set DTMF code for the remote relay, which is **#** by default.

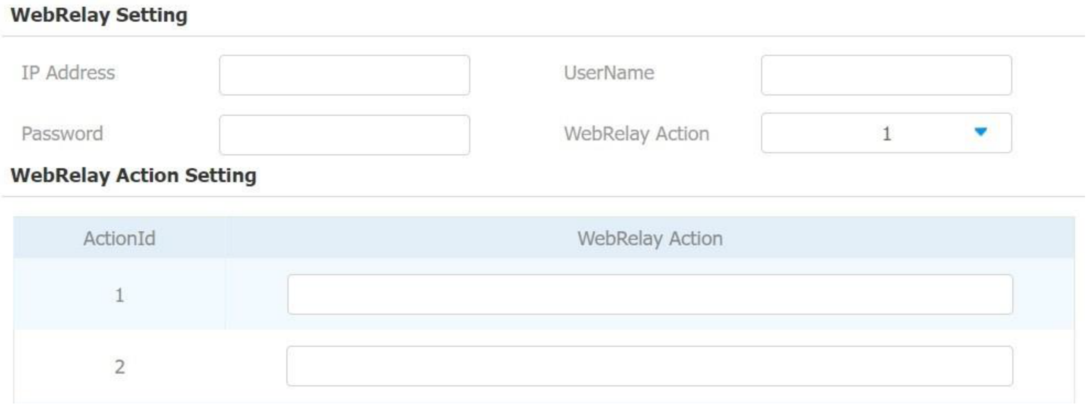
11.2 - Web relay setting

You can also control the door access using the network-based web relay.

To configure a web relay by the device web interface:

Phone > Relay > Web Relay

IP Address, User Name , and **Password** are provided by the web relay service provider.



WebRelay Setting

IP Address: UserName:

Password: WebRelay Action: 1 ▼

WebRelay Action Setting

ActionId	WebRelay Action
1	
2	

Setting:

- **Password:** The passwords are authenticated through HTTP and you can define the passwords using HTTP Get in Action.
- **Web Relay Action:** Enter the specific web relay action command provided by the web manufacturer for different actions of the web relay.

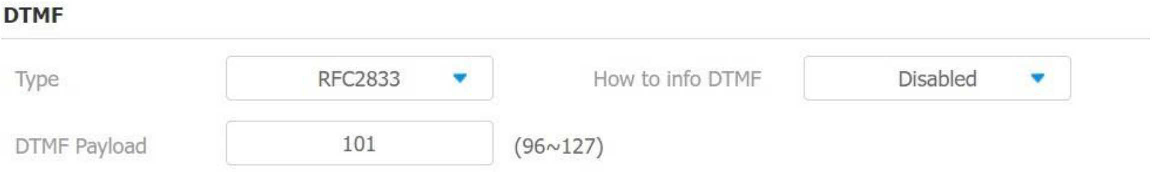
11.3 - Door unlock configuration

11.3.1 - Door unlock by DTMF code

DTMF codes can be configured by the web interface where you can set up identical DTMF codes on the corresponding intercom devices, which allows residents to enter the DTMF code on the soft keypad or press the DTMF code attached unlock tab on the screen, for example, to unlock the door for visitors during a call.

To configure a door unlock by the DTMF code using the device web interface:

Account > Advanced > DTMF



DTMF

Type: RFC2833

How to info DTMF: Disabled

DTMF Payload: 101 (96~127)

Table A17 - MyBell 2-Wire Indoor Monitor - Configuration of door unlock by DTMF code	
Setting	**Description**
Type	Select a DTMF type from the following options: • Info • RFC 2833 • Info+RFC 2833
How to info DTMF	Select among the following options: • Disable • DTMF • DTMF-Relay • Telephone-Event
DTMF Payload	Select the payload 96-127 for data transmission identification.

Note.

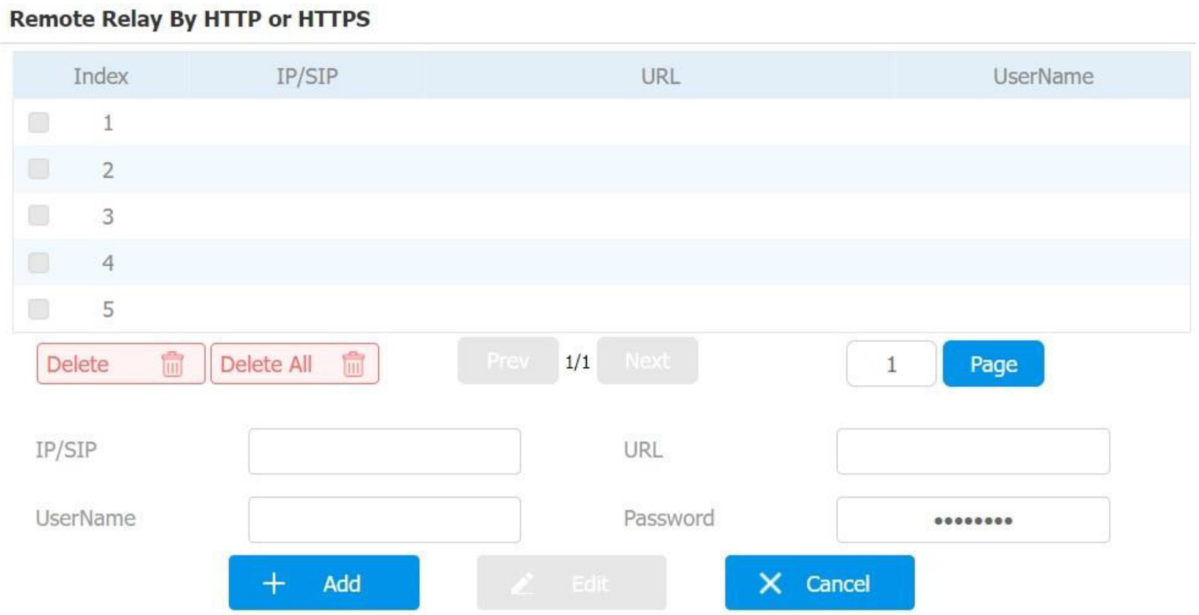
Please refer to the Relay Switch Setting for the specific DTMF code setting. Intercom devices involved need to be consistent in the DTMF type, otherwise, the DTMF code can't be applied.

11.3.2 - Door unlock through the HTTP command

You can unlock the door remotely without approaching the device physically for door access by typing the created HTTP command (URL) in the web browser to trigger the relay when you aren't available by the door.

To configure a door unlock by the HTTP code using the device web interface:

Phone > Relay > Remote Relay By HTTP or HTTPS



Remote Relay By HTTP or HTTPS

	Index	IP/SIP	URL	UserName
□	1			
□	2			
□	3			
□	4			
□	5			

IP/SIP:

URL:

UserName:

Password: ••••••••

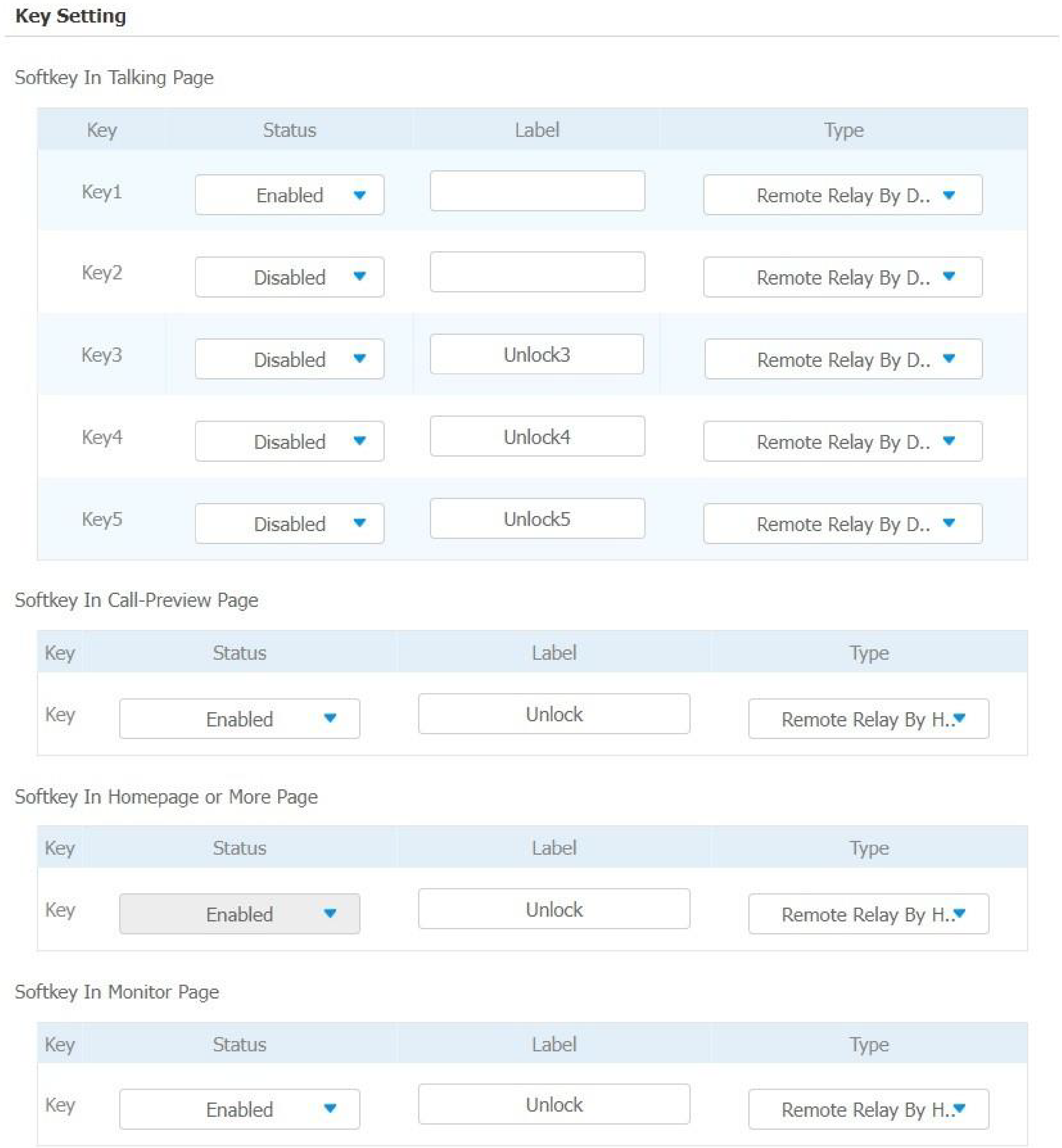
Table A18 - MyBell 2-Wire Indoor Monitor - Configuration of door unlock by HTTP command	
Setting	**Description**
IP/SIP	To configure an IP address or a SIP account to trigger a certain remote relay of doorphone by sending an HTTP message.
Username	Enter the device username to be used as a part of an HTTP command to trigger the local relay.
Password	Enter the device password to be used as part of a HTTP command to trigger the local relay. Please refer to the following example: http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note.
DoorNum in the HTTP command above refers to the relay number #1 to be triggered.

11.3.3 - Unlock by icon button

To configure a door unlock by the icon button using the device web interface:

Phone > Relay > Key Setting



Key Setting

Softkey In Talking Page

Key	Status	Label	Type
Key1	Enabled		Remote Relay By D..
Key2	Disabled		Remote Relay By D..
Key3	Disabled	Unlock3	Remote Relay By D..
Key4	Disabled	Unlock4	Remote Relay By D..
Key5	Disabled	Unlock5	Remote Relay By D..

Softkey In Call-Preview Page

Key	Status	Label	Type
Key	Enabled	Unlock	Remote Relay By H..

Softkey In Homepage or More Page

Key	Status	Label	Type
Key	Enabled	Unlock	Remote Relay By H..

Softkey In Monitor Page

Key	Status	Label	Type
Key	Enabled	Unlock	Remote Relay By H..

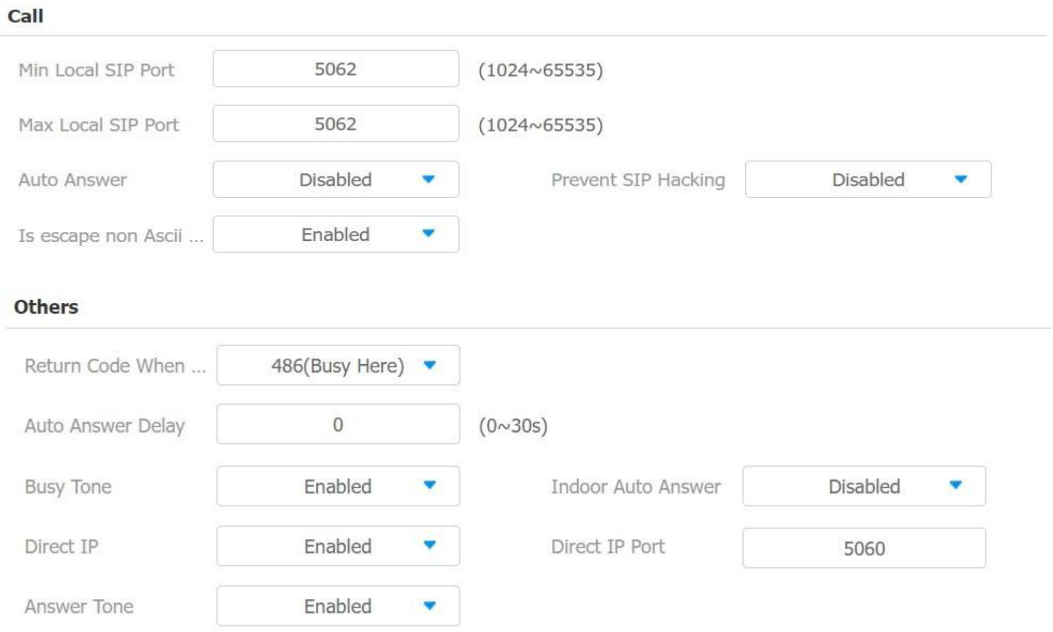
12.1 - Call auto-answer configuration

The device answer all incoming calls if call auto-answer is enabled and receives live stream if live stream is enabled.
To enable or disable a call-auto answer by the device web interface:

Account > Advanced > Call > Auto Answer

To configure the corresponding auto answer settings by the device web interface:

Phone > Call Feature > Others



Call

Min Local SIP Port	5062	(1024~65535)	
Max Local SIP Port	5062	(1024~65535)	
Auto Answer	Disabled	Prevent SIP Hacking	Disabled
Is escape non Ascii ...	Enabled		

Others

Return Code When ...	486(Busy Here)		
Auto Answer Delay	0	(0~30s)	
Busy Tone	Enabled	Indoor Auto Answer	Disabled
Direct IP	Enabled	Direct IP Port	5060
Answer Tone	Enabled		

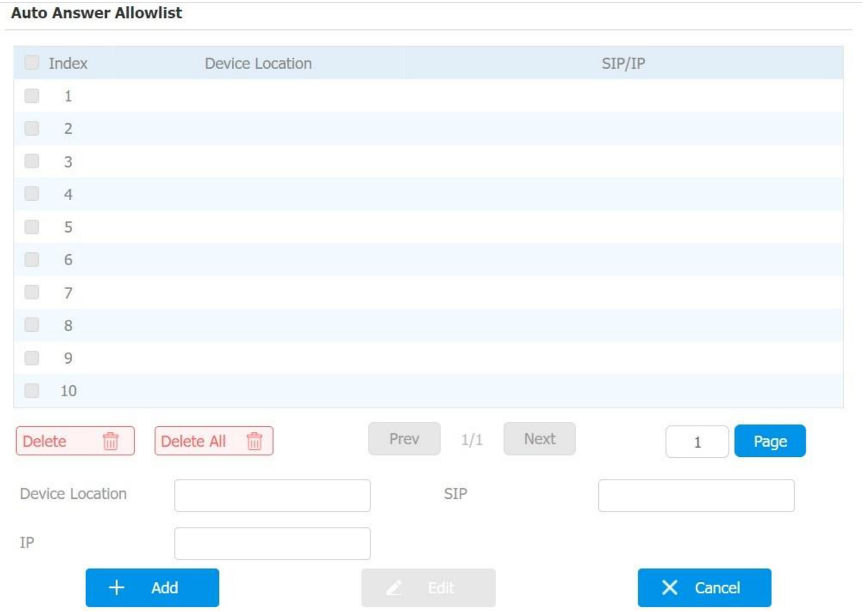
Table A19 - MyBell 2-Wire Indoor Monitor - Configuration of call auto-answer

Setting	Description
Auto Answer	Turn on the **Auto Answer** function by ticking the square box. It applies to all intercom devices.
Auto Answer Delay	Set up the delay time (from 0 to 30 seconds) before the call can be answered automatically. For example, if you set the delay time to 1 second, the call is answered in 1 second automatically.
Indoor Auto Answer	Enable it if you want to auto-answer the call from the indoor monitor only.

12.2 - Auto-answer allow list setting

Auto-answer can only be applicable to the SIP or IP numbers that are already added in the auto-answer allow list of your indoor monitor. Therefore, you are required to configure or edit the numbers in the allow list using the web interface.
To configure a call-auto answer allow list setting by the device web interface:

Phone > Call Feature > Auto Answer AllowList

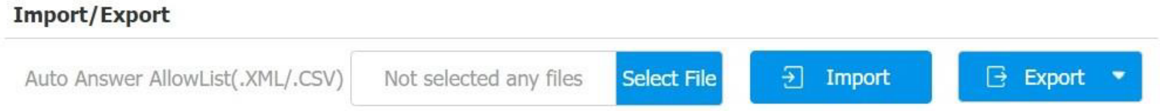


Auto Answer Allowlist

□ Index	Device Location	SIP/IP
□ 1		
□ 2		
□ 3		
□ 4		
□ 5		
□ 6		
□ 7		
□ 8		
□ 9		
□ 10		

Device Location		SIP	
IP			

SIP/IP numbers can be imported to or exported out of the indoor monitor in batch.
To import to or export out SIP/IP by the device web interface:
Phone > Call Feature > Import/Export



Import/Export

Auto Answer AllowList(.XML/.CSV) Not selected any files

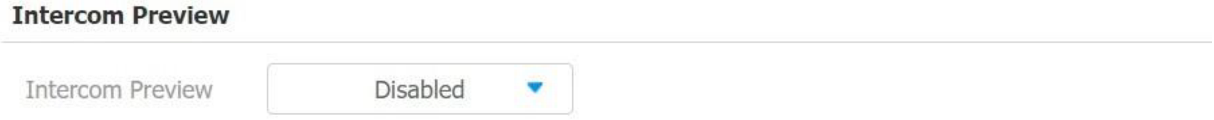
Note.

- SIP/IP number files to be imported or exported need to be in either .xml or .csv format.
- SIP/IP numbers need to be set up in the phone book of the indoor monitor before they can be valid for the auto-answer function.

12.3 - Intercom preview setting

If you want to see the image at the door station before answering the incoming call, you can enable the intercom preview function.
To enable the intercom preview function by the device web interface:

Phone > Intercom > Intercom Preview



Intercom Preview

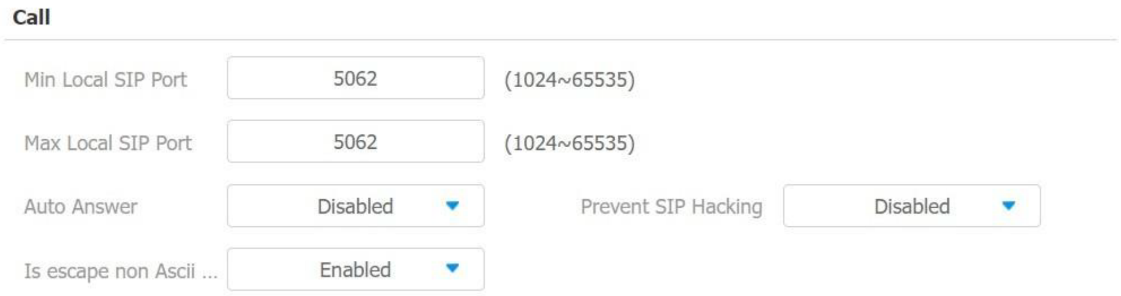
Intercom Preview: Disabled

Note.
A group call isn't available when you enable the intercom preview function.

12.4 - SIP hacking protection

Internet phone eavesdropping is a kind of network attack, which aims to eavesdrop on the communication sessions of others in an unauthorized way. Attackers can use this method to capture and read content containing sensitive and confidential information. SIP hacking prevents SIP call from hacking on the Internet.
To enable the SIP hacking protection by the device web interface:

Account > Advanced > Call



Call

Min Local SIP Port: 5062 (1024~65535)

Max Local SIP Port: 5062 (1024~65535)

Auto Answer: Disabled Prevent SIP Hacking: Disabled

Is escape non Ascii ...: Enabled

Setting:

- **Prevent SIP Hacking:** this feature is only available for SIP calls, not IP calls.

12.5 - Emergency call setting

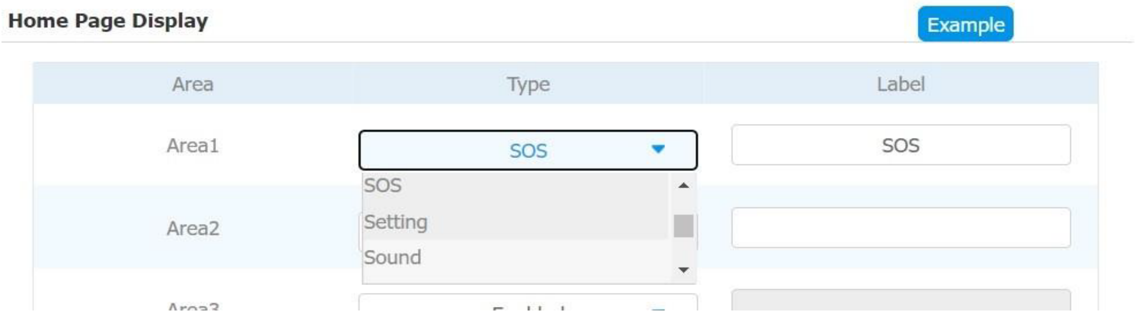
Emergency call is used to call out three emergency contacts when you are in urgent status. It's especially useful for the elders and children. Press the SOS key, the indoor monitor initiates automatically the target SOS numbers.

12.5.1 - SOS icon display

To display SOS softkey by the device web interface:

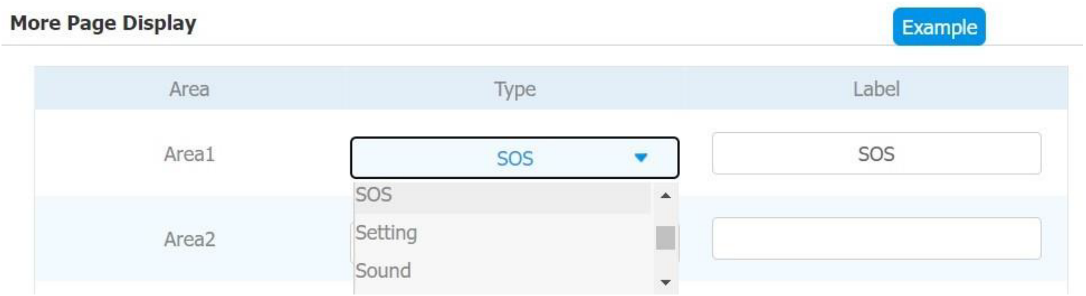
Phone > Key/Display

The icon appears on the main interface or more interfaces after configuring.



Home Page Display

Area	Type	Label
Area1	SOS	SOS
Area2		
Area3		



More Page Display

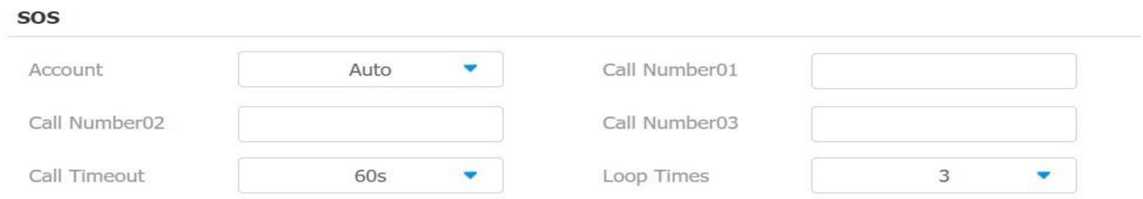
Example

Area	Type	Label
Area1	SOS	SOS
Area2		

12.5.2 - SOS number settings by the web interface

To set up SOS numbers by the device web interface:

Phone > Intercom



SOS

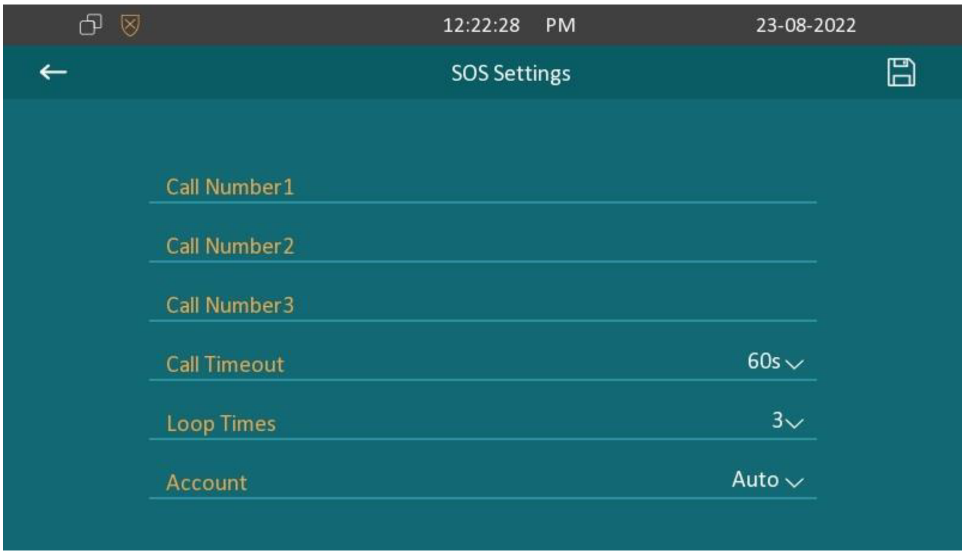
Account	Auto	Call Number01	
Call Number02		Call Number03	
Call Timeout	60s	Loop Times	3

Table A20 - MyBell 2-Wire Indoor Monitor - Configuration of SOS numbers	
Setting	**Description**
Account	Select the account you want to make SOS from account 1 or account 2.
Call Number	To set up 3 SOS numbers. Once users press SOS key on the home screen (SOS display key shall be set on the web manually), indoor monitors call out the numbers in order.
Call Timeout	Set up the timeout for each number. Once users call out, if the other side doesn't answer within the timeout, indoor monitors continue to call the next number.
Loop Times	To set up times of re-dialing.

12.5.3 - SOS number settings on the device

To set up SOS numbers on the device:

More > Setting > Advance > SOS



12:22:28 PM 23-08-2022

SOS Settings

Call Number1

Call Number2

Call Number3

Call Timeout 60s

Loop Times 3

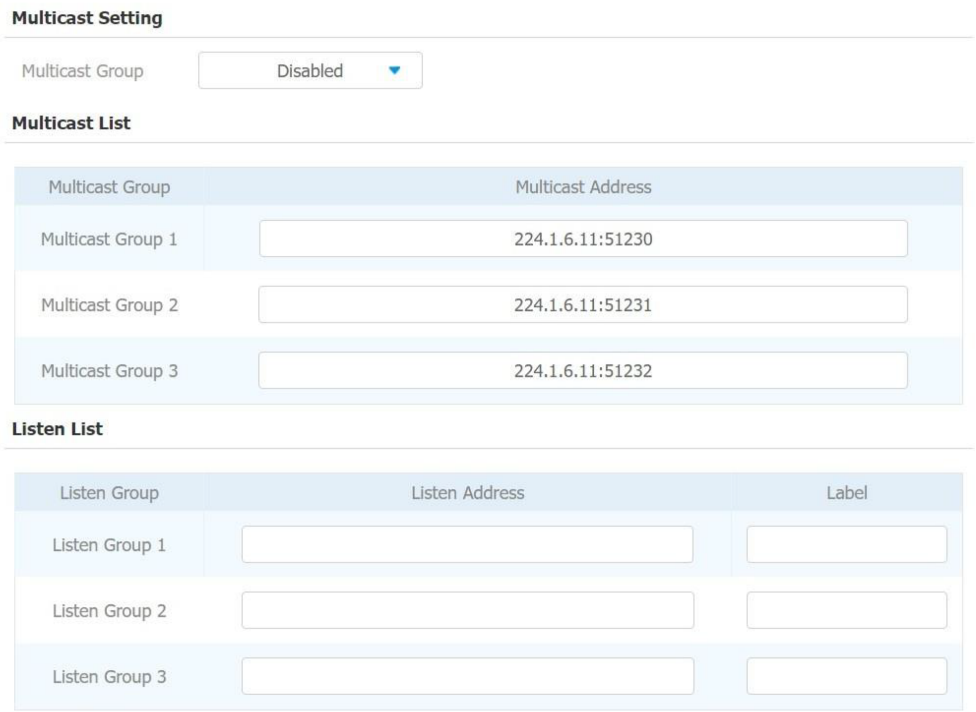
Account Auto

12.6 - Multicast configuration

Multicast is a one-to-many communication within a range.

To set up multicast communication on the device:

Phone > Multicast



Multicast Setting

Multicast Group: Disabled

Multicast List

Multicast Group	Multicast Address
Multicast Group 1	224.1.6.11:51230
Multicast Group 2	224.1.6.11:51231
Multicast Group 3	224.1.6.11:51232

Listen List

Listen Group	Listen Address	Label
Listen Group 1		
Listen Group 2		
Listen Group 3		

Table A21 - MyBell 2-Wire Indoor Monitor - Configuration of multicast

Setting	Description
Multicast Group	To set the indoor monitor in one of the groups or disable this function.
Multicast List	To fill in the settings of the multicast group. An indoor monitor establish multicast calls to other indoor monitors which are set in multicast group.
Listen List	To fill in the settings of the listen group. Indoor monitor receives multicast calls if some indoor monitors call the listen group.
Label	To show the label name on the calling interface.

12.7 - Call forwarding setting

Call Forward is a feature used to redirect an incoming call to a specific third party. Users can redirect the incoming call based on different scenarios.

12.7.1 - Call forwarding configuration on the device

To set up call forwarding on the device:

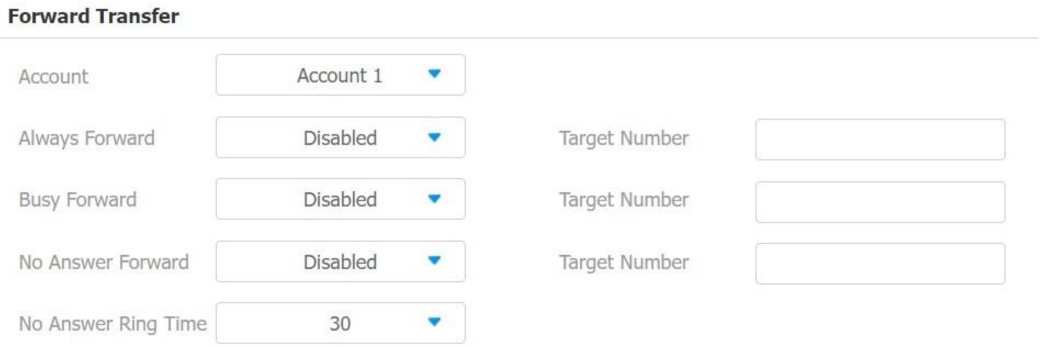
More > Setting > Advance > Direct IP

Table A22 - MyBell 2-Wire Indoor Monitor - Configuration of call forwarding on the device	
Setting	**Description**
No Answer Forward	To enable no answer forwarding function. Incoming calls are forwarded to a specific number if the indoor monitor isn't answered.
Busy Forward	To enable the busy forward function. Incoming calls are forwarded to a specific number if the device is busy.
Forward Target	To enter the specific forward number if the device enables **No Answer Forward.**
No Answer Ring Time	Set the number of seconds to wait for call pick-up before transferring to a designated number (0-120 seconds).

12.7.2 - Call Forwarding Configuration by the web interface

To set up forward function using the device web interface:

Phone > Call Feature > Forward Transfer



Forward Transfer

Account	Account 1		
Always Forward	Disabled	Target Number	
Busy Forward	Disabled	Target Number	
No Answer Forward	Disabled	Target Number	
No Answer Ring Time	30		

Table A23 - MyBell 2-Wire Indoor Monitor - Configuration of call forwarding by the web interface	
Setting	**Description**
Account	To choose which account shall implement the call forwarding feature.
Always Forward	To enable the always forwarding function. All incoming calls are automatically forwarded to a specific number.
Busy Forward	To enable the busy forwarding function. Incoming calls are forwarded to a specific number if the device is busy.
No Answer Forward	To enable the no answer forwarding function. Incoming calls are forwarded to a specific number if the device isn't picked up within no answer ring time.
Target Number	To enter the specific forward number if the device enables always forward/busy forward / no answer forward.
No Answer Ring Time	Set the number of seconds to wait for call pick-up before transferring to a designated number (0-120 seconds).

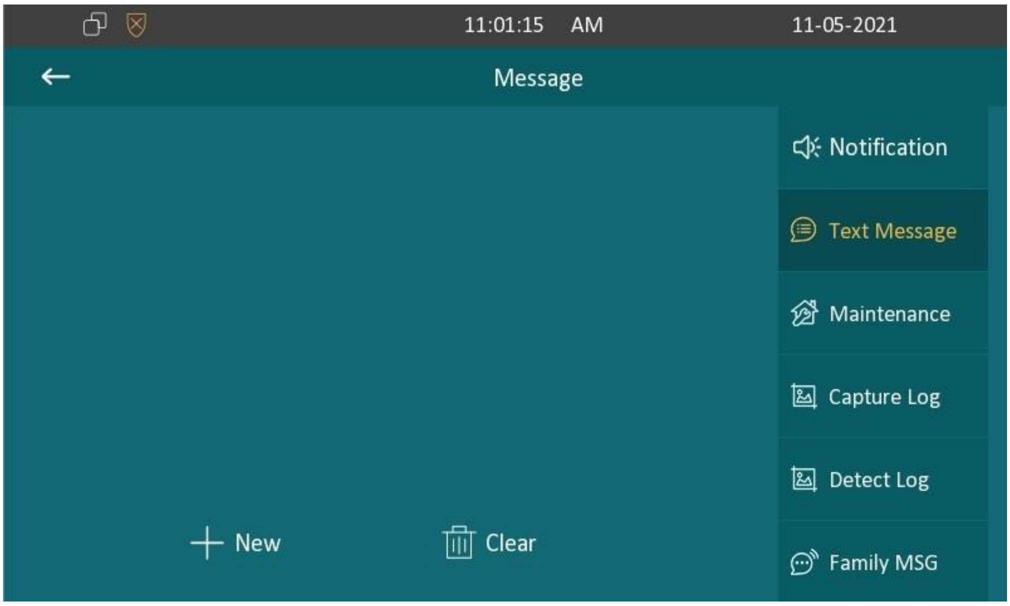
13 INTERCOM MESSAGE SETTING

13.1 - Managing Text Messages

You can check, create and clear messages as needed on the indoor monitor Messages screen. Click **New** to create a new text message and **Clear** icon to delete the existing messages.

To manage text messages on the device:

Message > Text Message

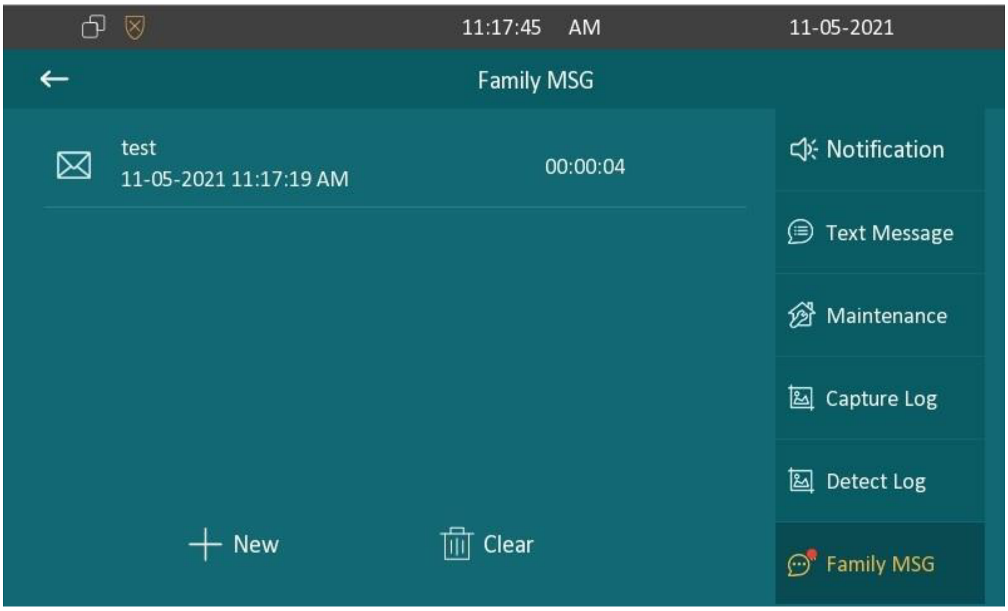


13.2 - Managing Voice Messages

You can create, delete and view the audio messages recorded by family members on the device screen.

To manage voice messages on the device:

Message > Family MSG



test
11-05-2021 11:17:19 AM 00:00:04

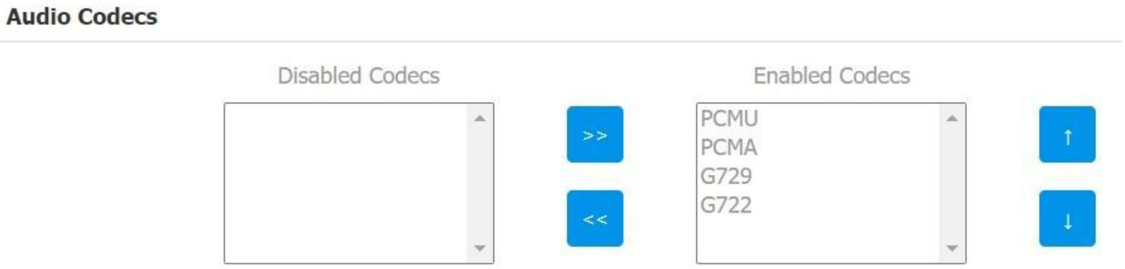
14 AUDIO & VIDEO CODEC CONFIGURATION FOR SIP CALLS

14.1 - Audio codec configuration

The indoor monitor supports four types of Codec (PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To configure audio codec by the web interface:

Account> Advanced > Audio Codecs



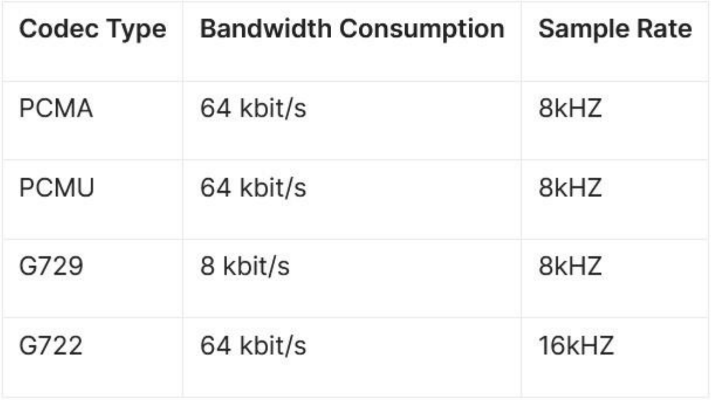
Audio Codecs

Disabled Codecs

Enabled Codecs

PCMU
PCMA
G729
G722

Please refer to the bandwidth consumption and sample rate for the four codecs types below:



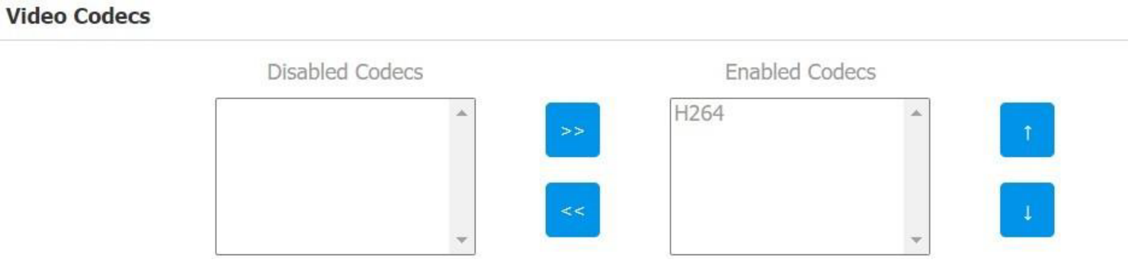
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

14.2 - Video codec configuration

The indoor monitor supports the H264 codec that provides better video quality at a much lower bit rate.

To configure video codec by the web interface:

Account> Advanced > Video Codecs



Video Codecs

Disabled Codecs

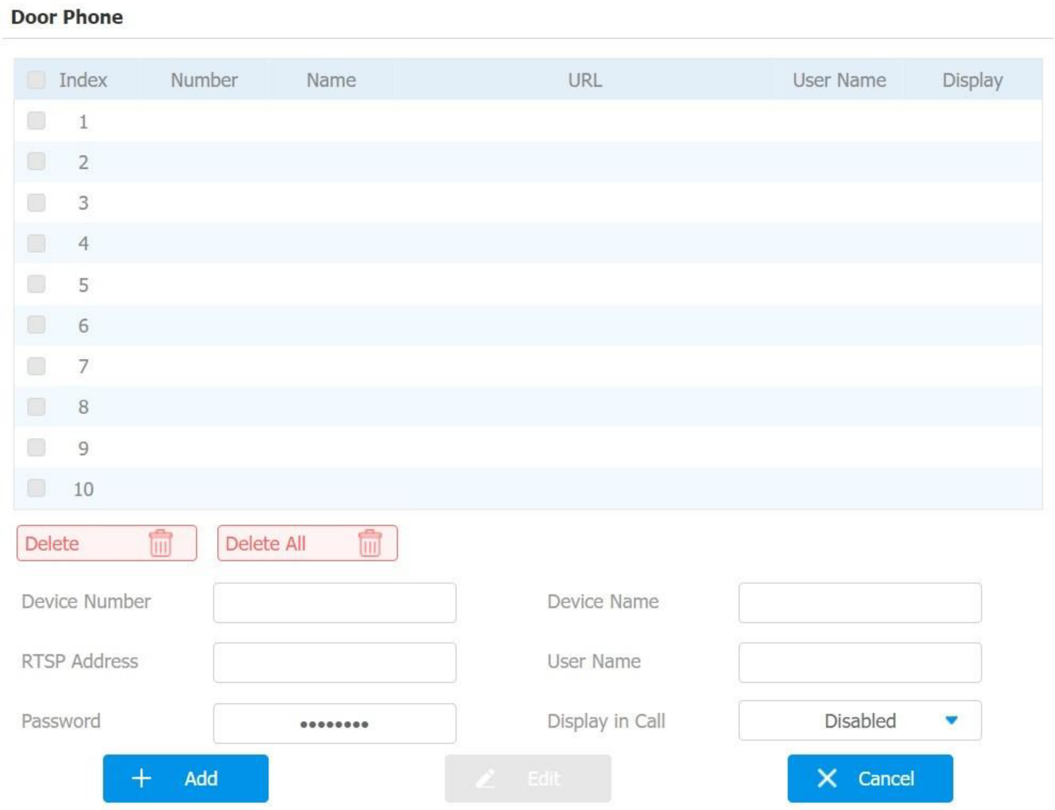
Enabled Codecs

H264

15.1 - Monitor setting

To configure the monitor setting by the web interface:

Phone > Monitor > Door Phone



Door Phone

□ Index	Number	Name	URL	User Name	Display
□ 1					
□ 2					
□ 3					
□ 4					
□ 5					
□ 6					
□ 7					
□ 8					
□ 9					
□ 10					

Device Number:

Device Name:

RTSP Address:

User Name:

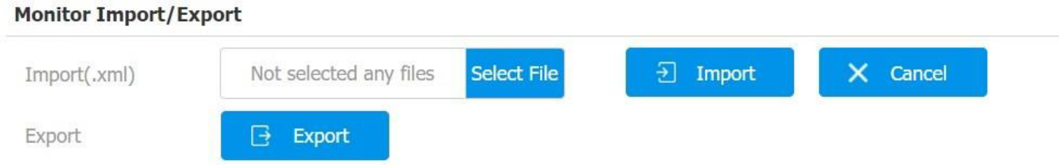
Password: ••••••••

Display in Call: Disabled

Table A24 - MyBell 2-Wire Indoor Monitor - Monitor setting

Setting	Description
Device Number	To enter the IP address or SIP number of a corresponding camera.
Device Name	To enter the device name of the doorphone, which could be set by users.
RTSP Address	To set RTSP URL for the doorphone. The RTSP format of the doorphone is rtsp://device IP/live/ch00_0
User Name	Enter the username if needed. The username of third-party camera is provided by the third-party camera service provider.
Password	Enter the password if needed. The password of third-party camera is provided by the third-party camera service provider.
Display in Call	Enable or disable to display this monitor during the call. If enabled, when there is an incoming call from the monitor, the video is displayed.

You can also import or export the monitor list in batch using the same interface. Import file only supports .xml format.



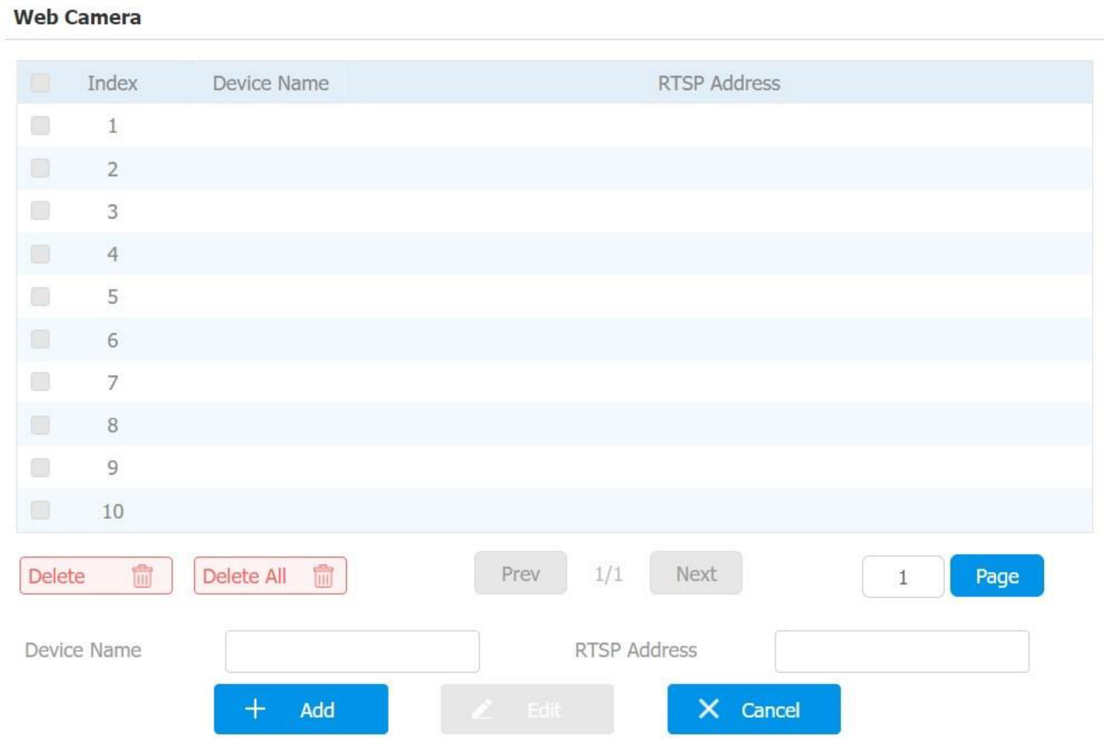
Monitor Import/Export

Import(.xml): Not selected any files

15.1.1 - Web camera setting by the web interface

To configure the monitor information for third-party cameras by the web interface:

Phone > Monitor > Web Camera



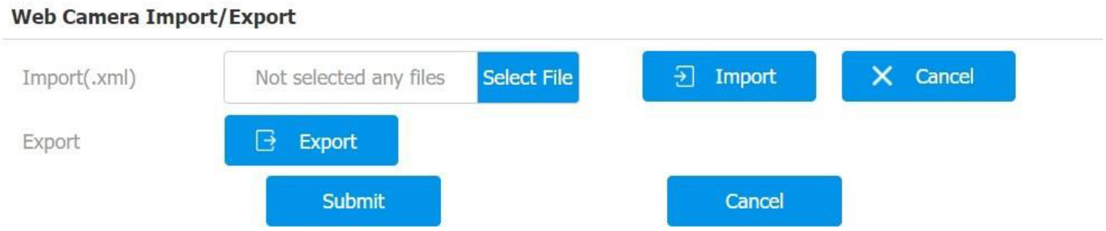
Web Camera

□	Index	Device Name	RTSP Address
□	1		
□	2		
□	3		
□	4		
□	5		
□	6		
□	7		
□	8		
□	9		
□	10		

Setting:

- **Device Name:** to enter the name of the third-party camera.
- **RTSP Address:** to set the RTSP URL for the third-party camera.

You can also import or export the monitor list in batch on the same interface. The import file only supports .xml format.

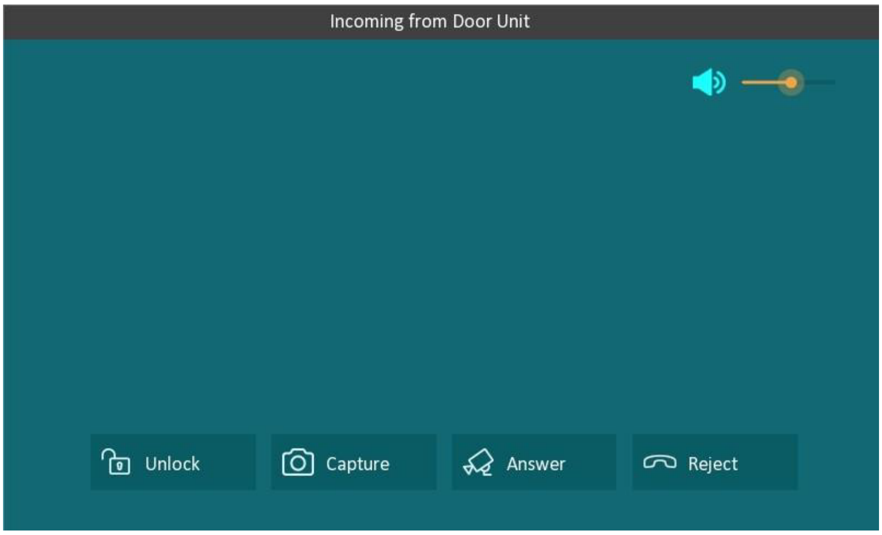


Web Camera Import/Export

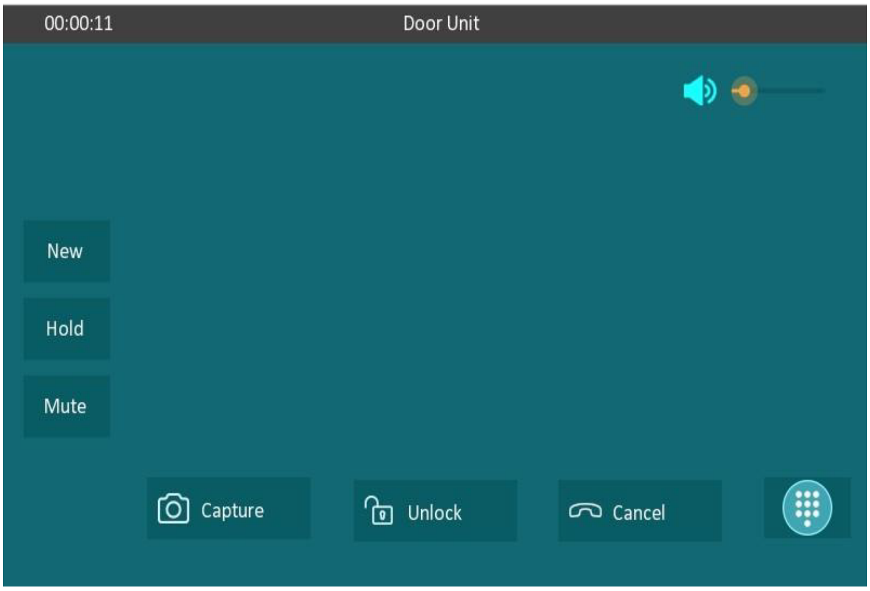
Import(.xml) Not selected any files

15.1.2 - Web camera setting on the device

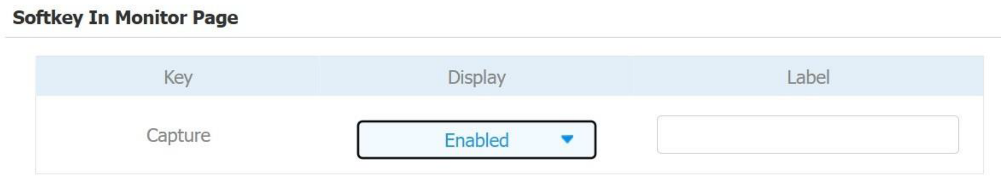
To capture video images press **Capture** during a monitor or video call.



Incoming from Door Unit

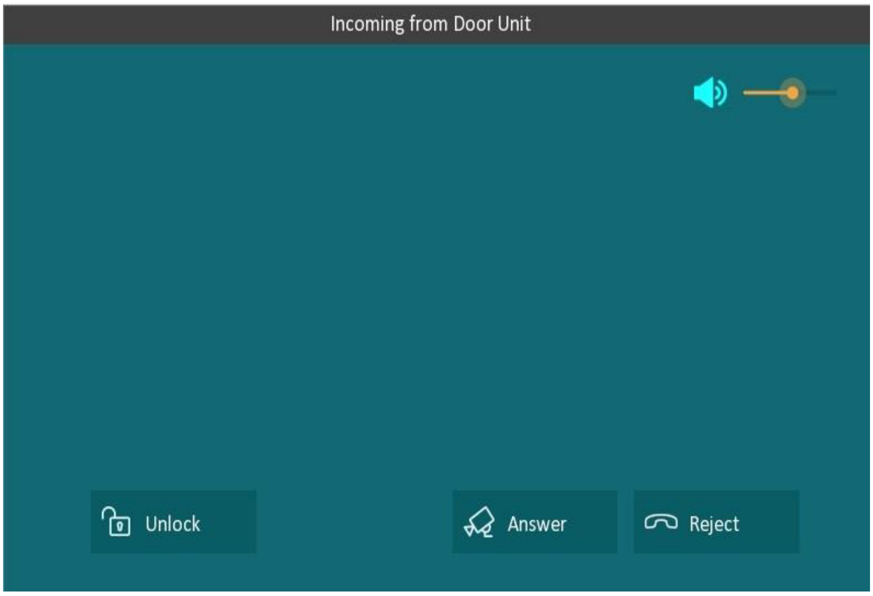


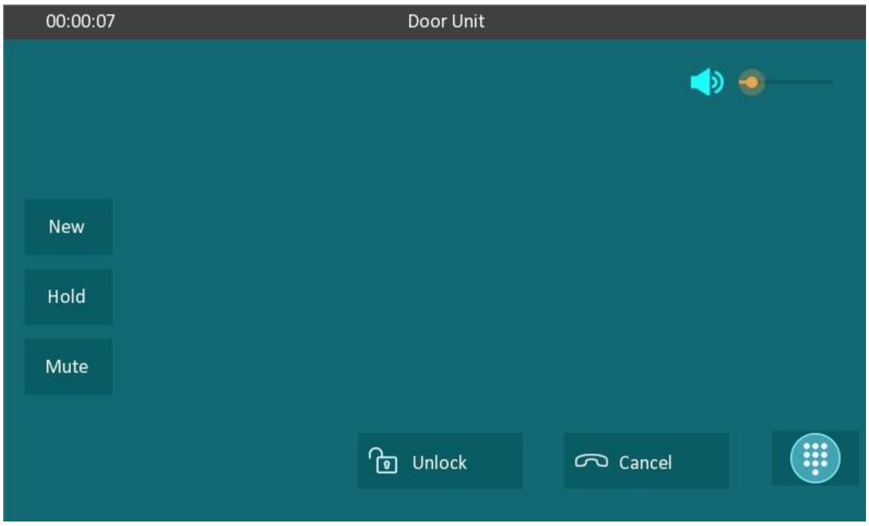
You can also disable the capture function on device web interface.
To disable the capture function by the web interface:
Phone > Key/Display > Softkey In Monitor Page



Softkey In Monitor Page

Key	Display	Label
Capture	Enabled ▾	



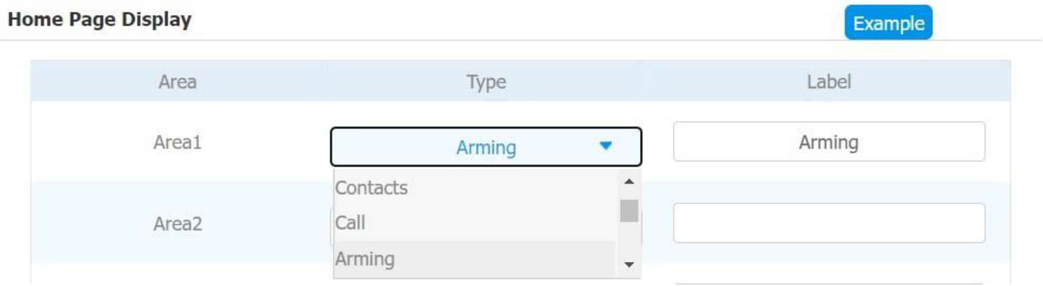


15.2 - Alarm and arming configuration

The alarm feature is used to connect some alarm detection devices to protect your home safety. MyBell 2-Wire Indoor Monitors support 8 alarm connectors, which means you can connect 8 different alarm sensors in different rooms of your house. For example, by connecting a smoker sensor in your kitchen when the leaking gas is detected, the indoor monitor rings and sends the alarm message to the target, like community property. Before checking the alarm feature on the device screen, you need to set up the **Arming icon** on the home page or more page.

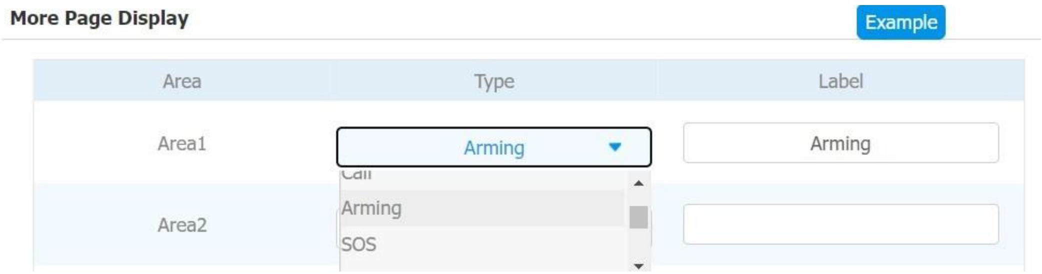
To set up the **Arming icon**:

Phone > Key/Display



Home Page Display

Area	Type	Label
Area1	Arming	Arming
Area2		



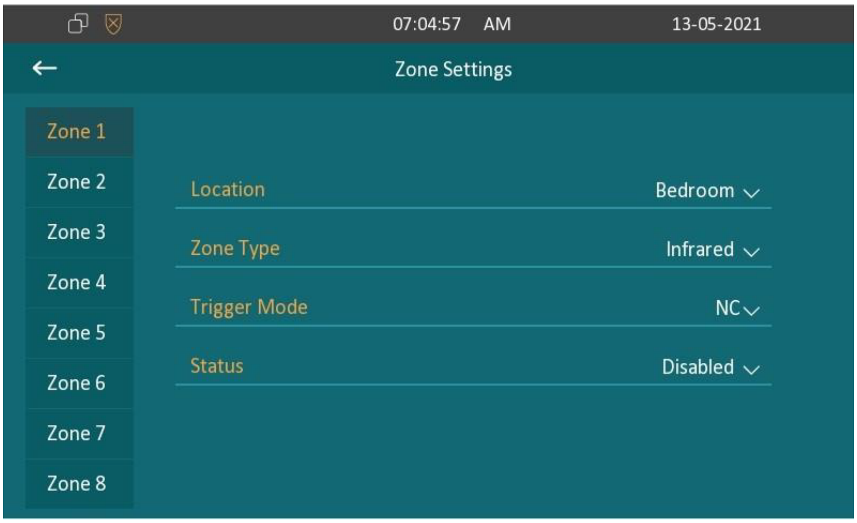
More Page Display

Area	Type	Label
Area1	Arming	Arming
Area2		

15.2.1 - Alarm and arming configuration on the device

To set up a location-based alarm sensor on the device:

More > Setting > Advance > Arming > Zone Setting



07:04:57 AM 13-05-2021

Zone Settings

Zone 1

Location: Bedroom

Zone Type: Infrared

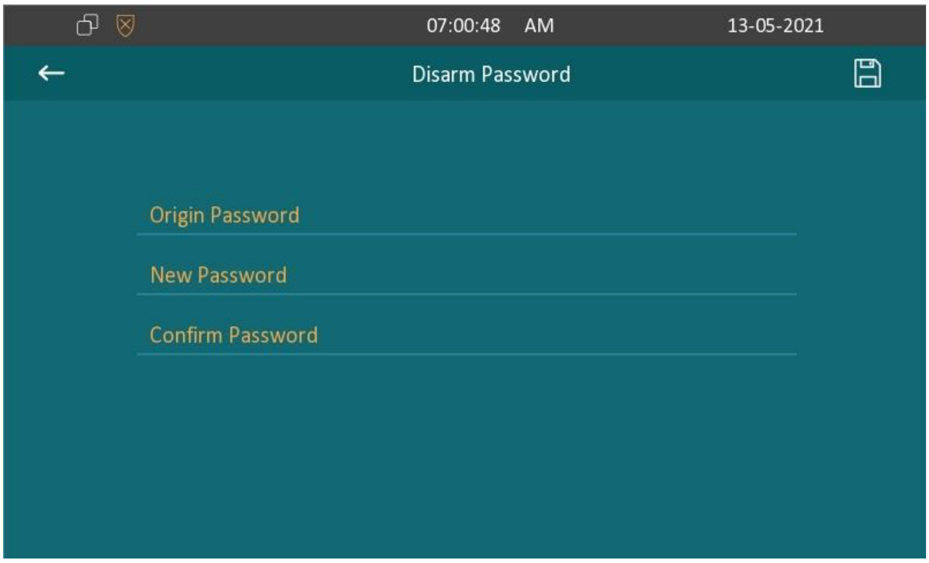
Trigger Mode: NC

Status: Disabled

Table A25 - MyBell 2-Wire Indoor Monitor - Monitor setting

Setting	Description
Location	Set up the location according to where the alarm sensor is stalled. You can select among ten location types: **Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study**, and **Bathroom**.
Zone Type	Set up the alarm sensor types. You can select among the following sensor types: **Infrared, Drmagnet, Smoke, Gas, Urgency.**
Trigger Mode	Set the sensor trigger mode between NC and NO according to your need.
Status	Set the alarm sensor status among three options: • **Enable** - if you want to enable the alarm, however, you are required to set the alarm again after an alarm is disarmed. • **Disable** - if you want to disable the alarm. • **24H** - if you want the alarm sensor to stay enabled for 24 hours without the need to set up the alarm manually again after the alarm is disarmed.

To configure the disarm code, press **Arming** on the device home screen. Change the current password and save it.



07:00:48 AM 13-05-2021

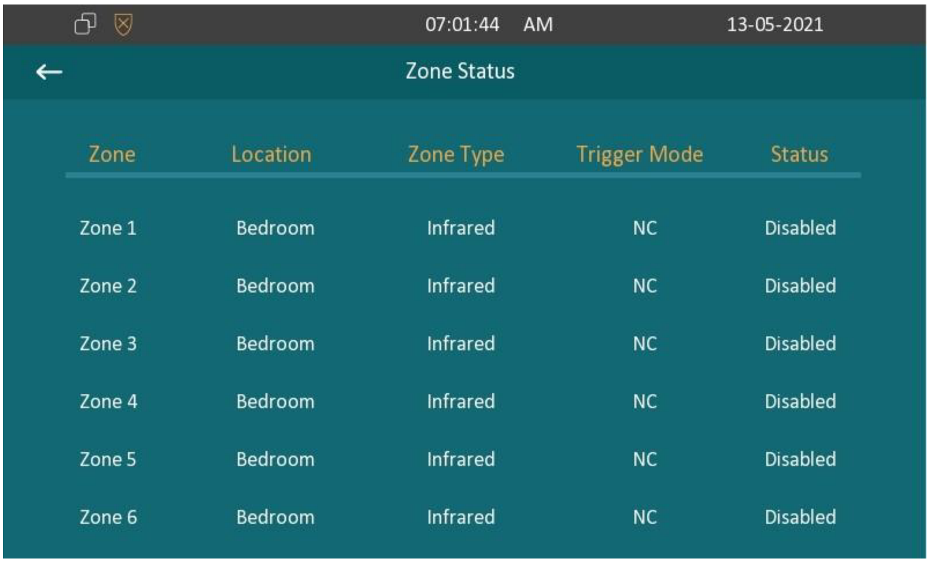
Disarm Password

Origin Password

New Password

Confirm Password

To check the zone status on the device:
Arming > Zone Status



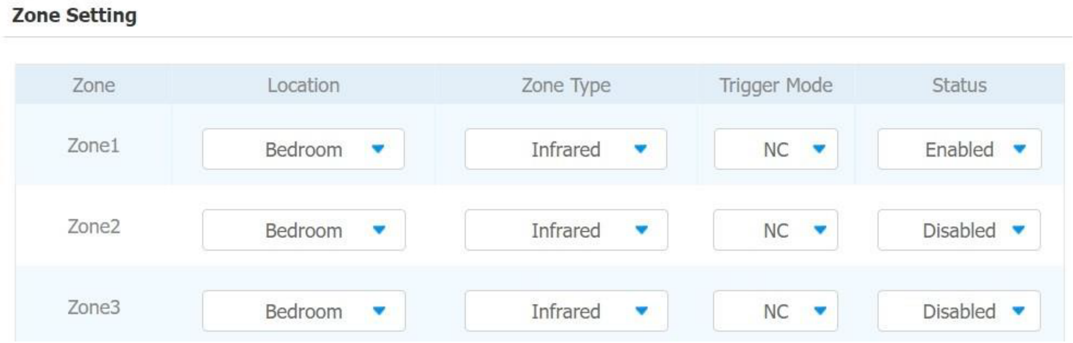
07:01:44 AM 13-05-2021

Zone Status

Zone	Location	Zone Type	Trigger Mode	Status
Zone 1	Bedroom	Infrared	NC	Disabled
Zone 2	Bedroom	Infrared	NC	Disabled
Zone 3	Bedroom	Infrared	NC	Disabled
Zone 4	Bedroom	Infrared	NC	Disabled
Zone 5	Bedroom	Infrared	NC	Disabled
Zone 6	Bedroom	Infrared	NC	Disabled

15.2.2 - Alarm and arming configuration by the web interface

To set up a location-based alarm sensor by the web interface:
Arming> Zone Setting > Zone Setting



Zone Setting

Zone	Location	Zone Type	Trigger Mode	Status
Zone1	Bedroom	Infrared	NC	Enabled
Zone2	Bedroom	Infrared	NC	Disabled
Zone3	Bedroom	Infrared	NC	Disabled

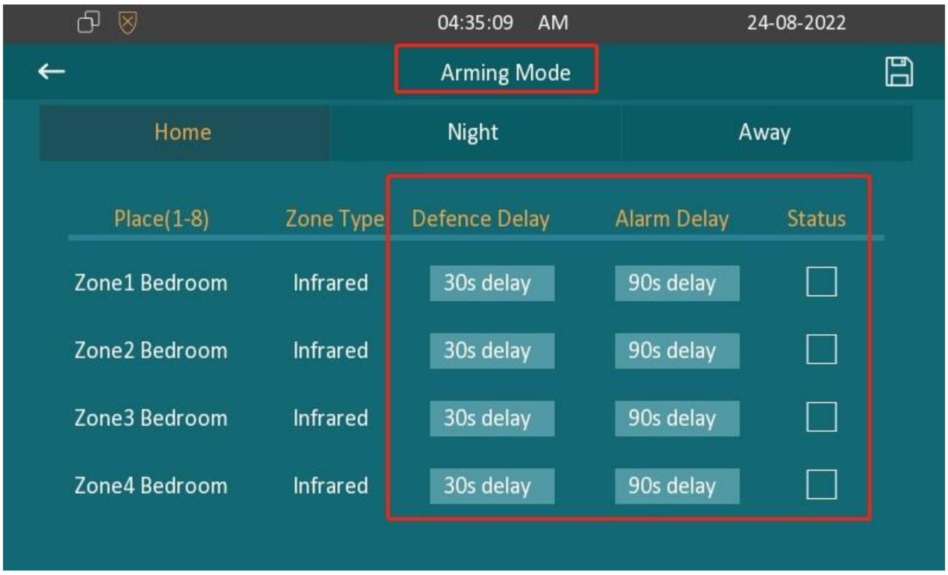
For more information about options in the zone seetting see the table A25 in section 15.2.1.

15.3 - Location-based alarm configuration

15.3.1 - Location-based alarm on the device

To configure the location-based alarm:

Arming > Arming Mode



04:35:09 AM 24-08-2022

Arming Mode

Home | Night | Away

Place(1-8)	Zone Type	Defence Delay	Alarm Delay	Status
Zone1 Bedroom	Infrared	30s delay	90s delay	□
Zone2 Bedroom	Infrared	30s delay	90s delay	□
Zone3 Bedroom	Infrared	30s delay	90s delay	□
Zone4 Bedroom	Infrared	30s delay	90s delay	□

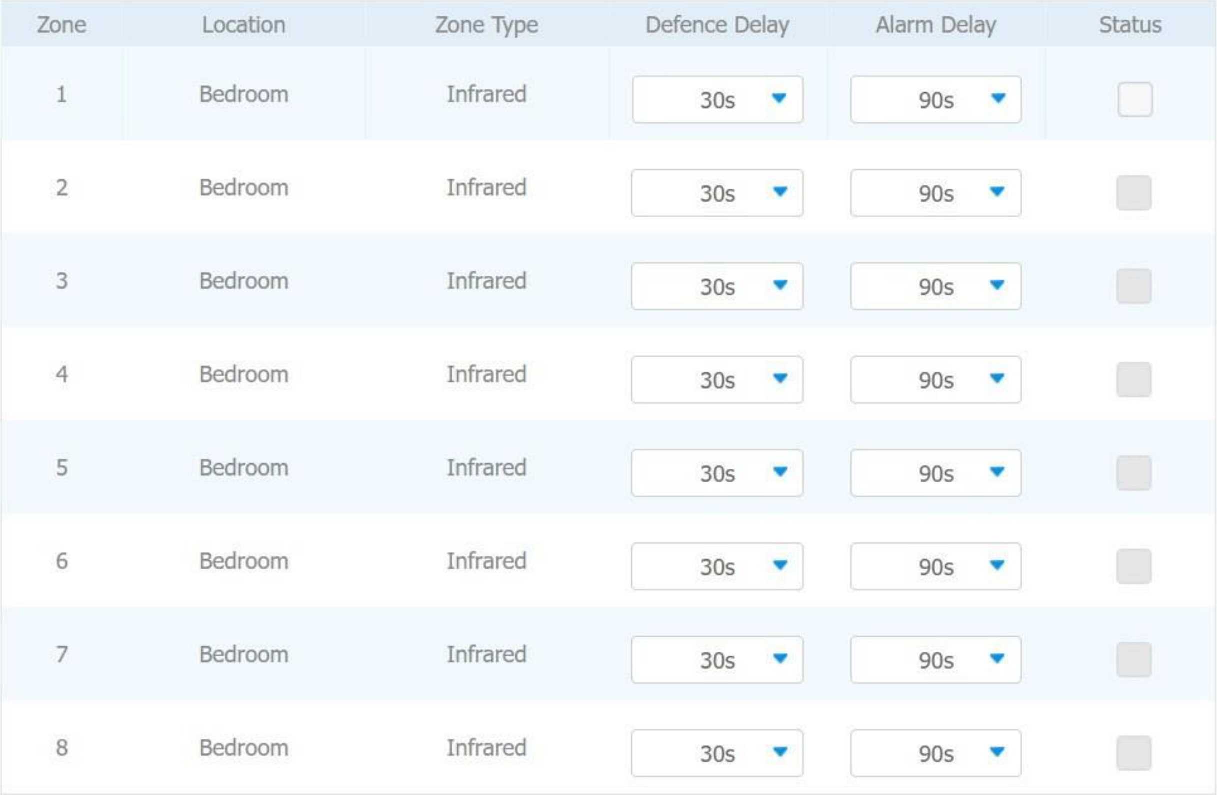
Table A26 - MyBell 2-Wire Indoor Monitor - Configuration of the arming mode

Setting	Description
Place	To display the location of the detection device.
Zone Type	To display the type of detection device.
Defence delay	When the arming mode is enabled, there is 30 seconds delay for the alarm mode to be activated.
Alarm delay	When the sensor is triggered, there is 90 seconds delay to announce the notification.
Status	To enable or disable Arming mode on the corresponding zone.

15.3.2 - Location-based alarm by the web interface

To configure the location-based alarm by the web interface:

Arming > Arming Mode



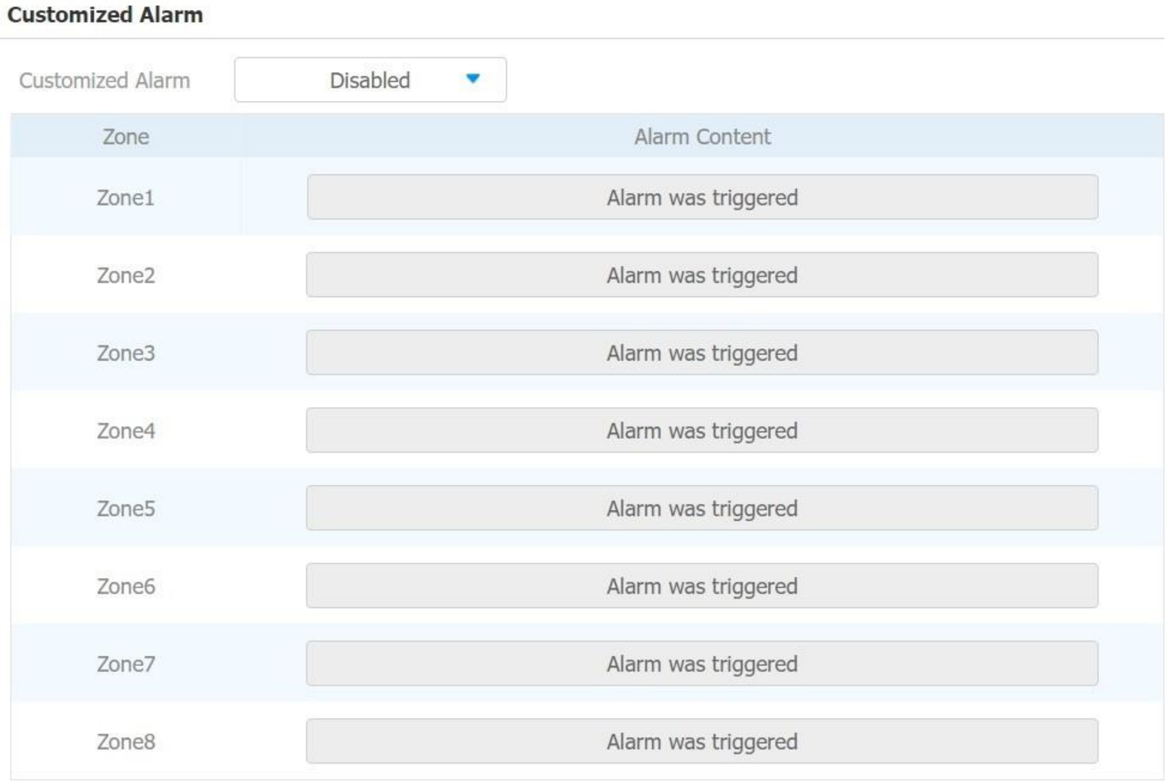
Zone	Location	Zone Type	Defence Delay	Alarm Delay	Status
1	Bedroom	Infrared	30s	90s	□
2	Bedroom	Infrared	30s	90s	□
3	Bedroom	Infrared	30s	90s	□
4	Bedroom	Infrared	30s	90s	□
5	Bedroom	Infrared	30s	90s	□
6	Bedroom	Infrared	30s	90s	□
7	Bedroom	Infrared	30s	90s	□
8	Bedroom	Infrared	30s	90s	□

15.4 - Configuring the alarm text

You can customize your alarm text shown on the screen when an alarm is triggered. Enter the alarm text for the alarm at each location according to your need.

To customize your alarm text alarm:

Arming> Zone Setting > Customized Alarm



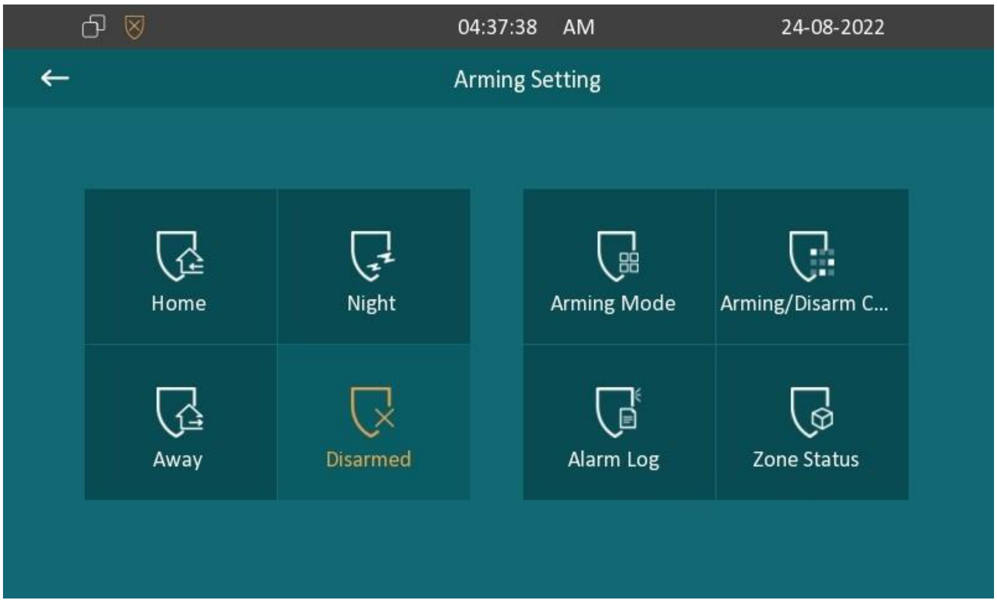
Customized Alarm

Customized Alarm: Disabled

Zone	Alarm Content
Zone1	Alarm was triggered
Zone2	Alarm was triggered
Zone3	Alarm was triggered
Zone4	Alarm was triggered
Zone5	Alarm was triggered
Zone6	Alarm was triggered
Zone7	Alarm was triggered
Zone8	Alarm was triggered

15.5. - Configuring the arming mode

You can switch the arming mode, disarm the alarm on the **Arming** screen by pressing their respective icons. Press **Disarm** icon if you want to clear the Arming Mode.

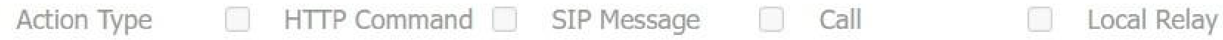


15.6 - Configuring alarm action

The triggering of the alarm sensor can be accompanied by the actions you configured in the forms of an HTTP command, SIP Message, Call, and Local Relay for different security purposes.

To select and set up actions by the web interface:

Arming > Alarm Action



Action Type □ HTTP Command □ SIP Message □ Call □ Local Relay

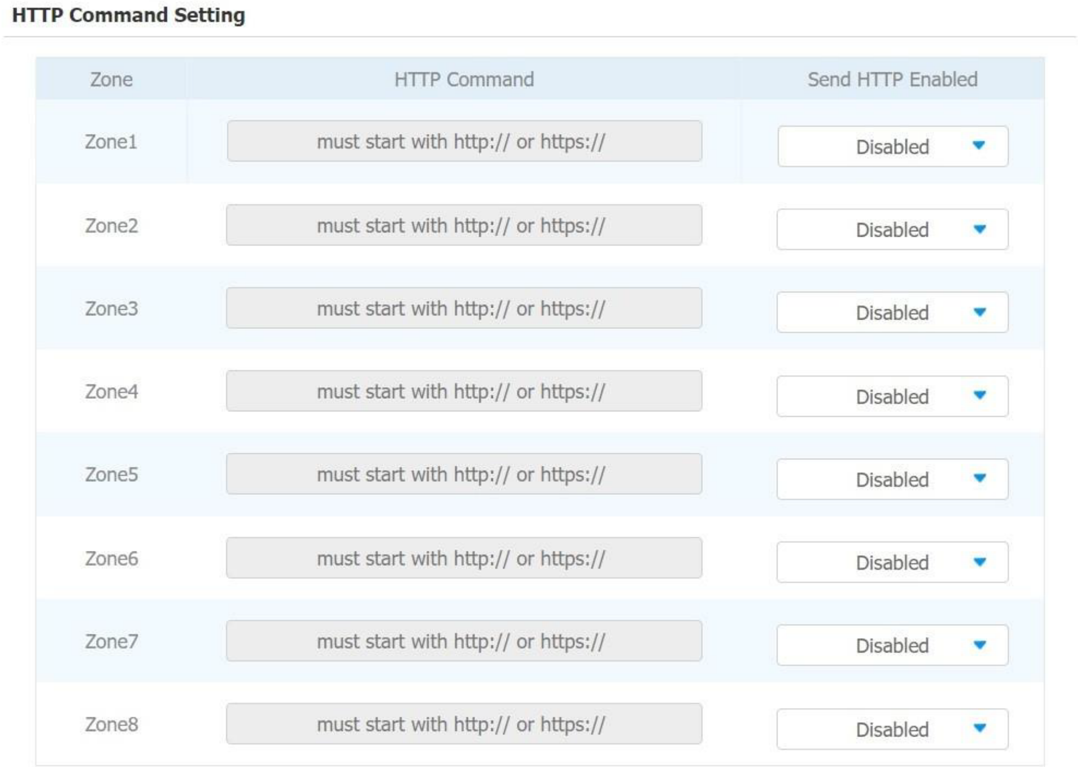
15.6.1 - Configuration of alarm action through HTTP command

You can set up the HTTP Command action by checking **Enable** in the **Send HTTP** field.

Then enter the HTTP command provided by the manufacturer of the device on which the action is to be carried out.

To set the HTTP Command up:

Arming > Alarm Action > HTTP Command Setting



HTTP Command Setting

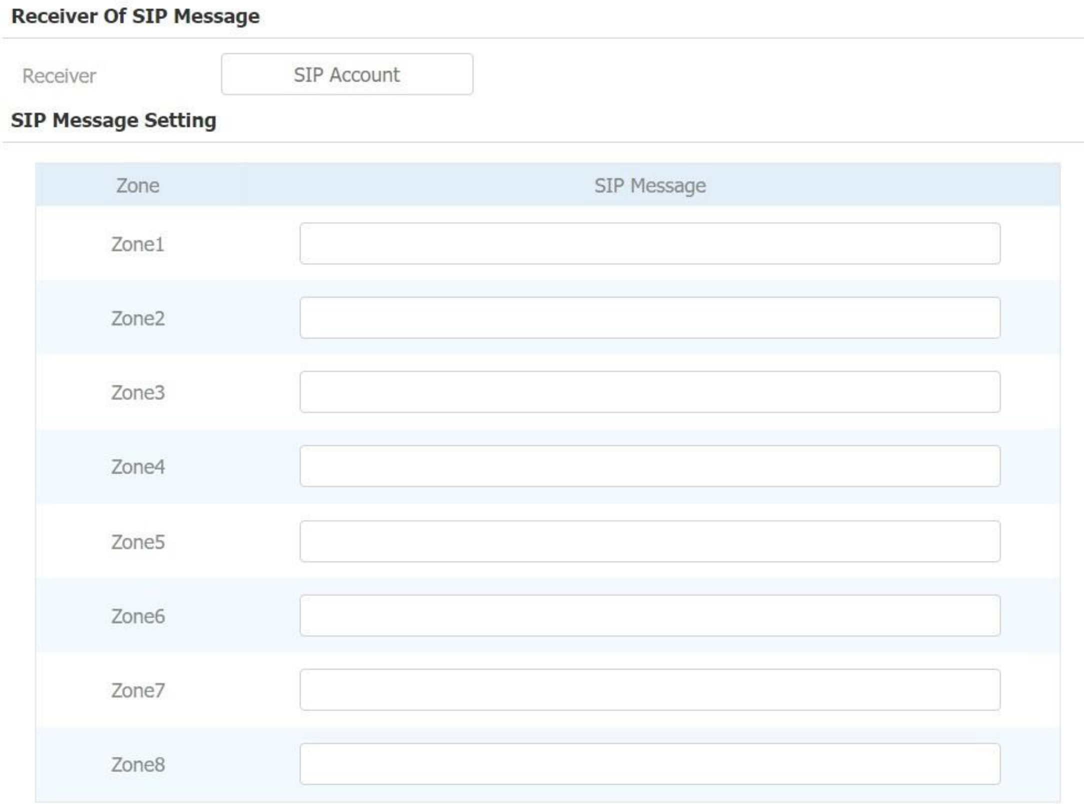
Zone	HTTP Command	Send HTTP Enabled
Zone1	must start with http:// or https://	Disabled
Zone2	must start with http:// or https://	Disabled
Zone3	must start with http:// or https://	Disabled
Zone4	must start with http:// or https://	Disabled
Zone5	must start with http:// or https://	Disabled
Zone6	must start with http:// or https://	Disabled
Zone7	must start with http:// or https://	Disabled
Zone8	must start with http:// or https://	Disabled

15.6.2 - Configuration of alarm action through SIP message

You can set up the SIP message action receiver using the same web interface. Enter the SIP account to which you want to send the configured SIP message as an action when the alarm is triggered.

To set the SIP message action receiver:

Arming > Alarm Action > Receiver Of SIP Message



Receiver Of SIP Message

Receiver: SIP Account

SIP Message Setting

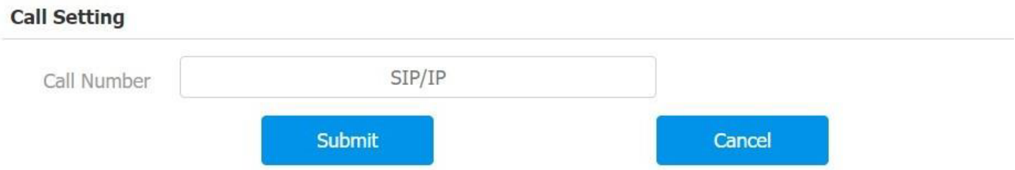
Zone	SIP Message
Zone1	
Zone2	
Zone3	
Zone4	
Zone5	
Zone6	
Zone7	
Zone8	

15.6.3 - Configuring the alarm action through SIP message

To set up the call action, you can enter the SIP or IP number of the device to be called as an action, then enable the Alarm Siren for the arming zone as needed.

To set a call action:

Arming > Alarm Action > Call Setting



Call Setting

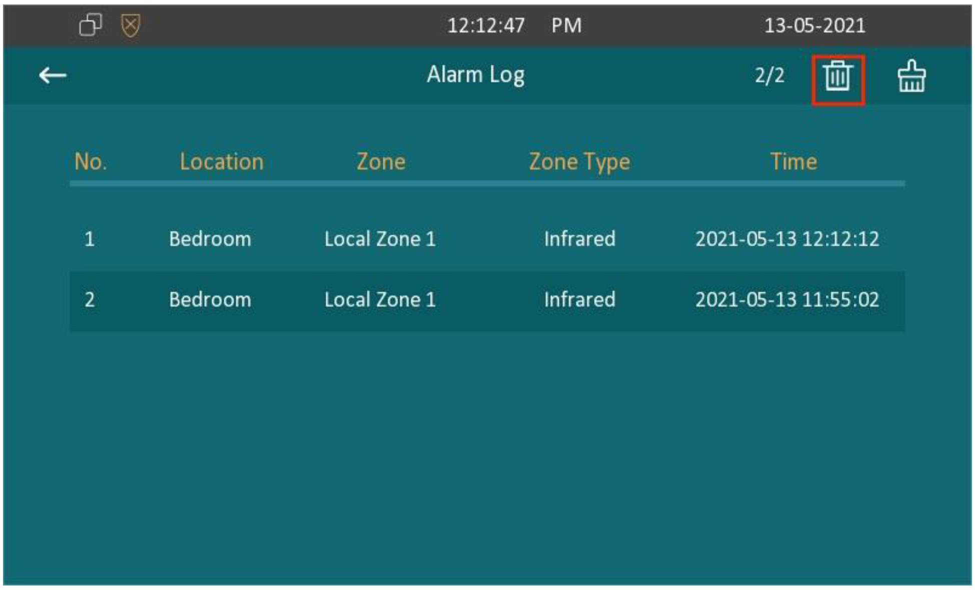
Call Number: SIP/IP

15.7 - Checking alarm logs

To check alarm logs:

Arming > Alarm Log

You can delete the existing alarm log by clicking the **Delete** icon.



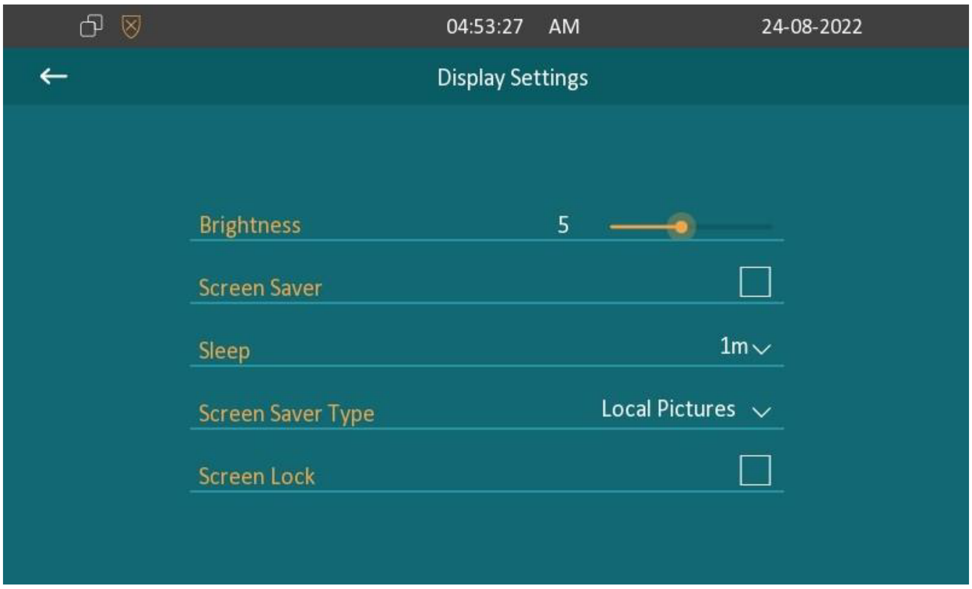
No.	Location	Zone	Zone Type	Time
1	Bedroom	Local Zone 1	Infrared	2021-05-13 12:12:12
2	Bedroom	Local Zone 1	Infrared	2021-05-13 11:55:02

15.8 - Screen unlock setting

The device screen is locked over sleep time. You are required to wake up the device through a PIN code.

To set screen unlock:

More > Setting > Display



Brightness 5

Screen Saver □

Sleep 1m

Screen Saver Type Local Pictures

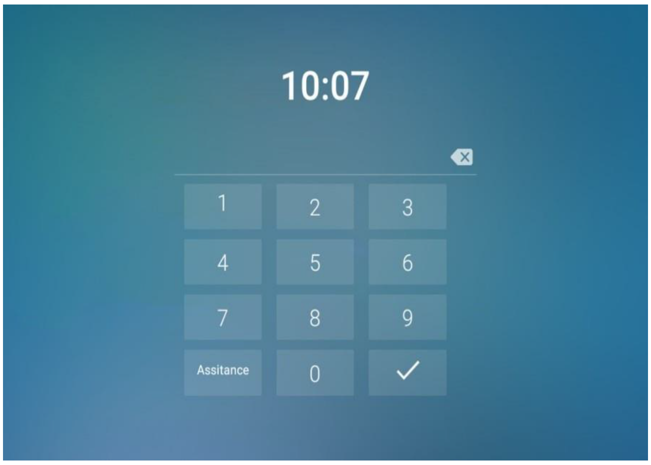
Screen Lock □

15.9 - Screen unlock by PIN code

You can unlock the device screen by entering the pre-configured PIN code when the screen is locked.

Note.

The default unlock PIN is **123456.**



15.10 - Location-based alarm configuration

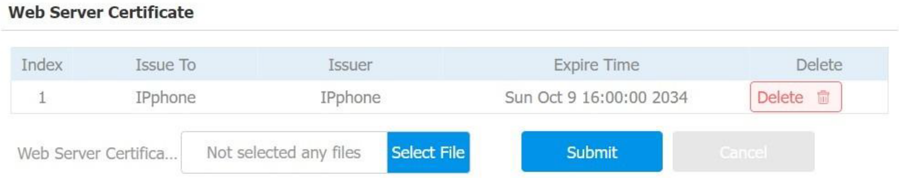
Certificates can ensure communication integrity and privacy when deploying the MyBell 2-Wire Indoor Monitors. So, when the user needs to establish the SSL protocol, it's necessary to upload corresponding certificates for verification.

15.10.1 - Web server certificate

This certificate sends to the client for authentication when the client requires an SSL connection with the device. Currently, the format of the certificate needs to *.PEM file. to be accepted by the device.

To upload web server certificate to the device web interface:

Security > Advanced > Web Server Certificate



Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

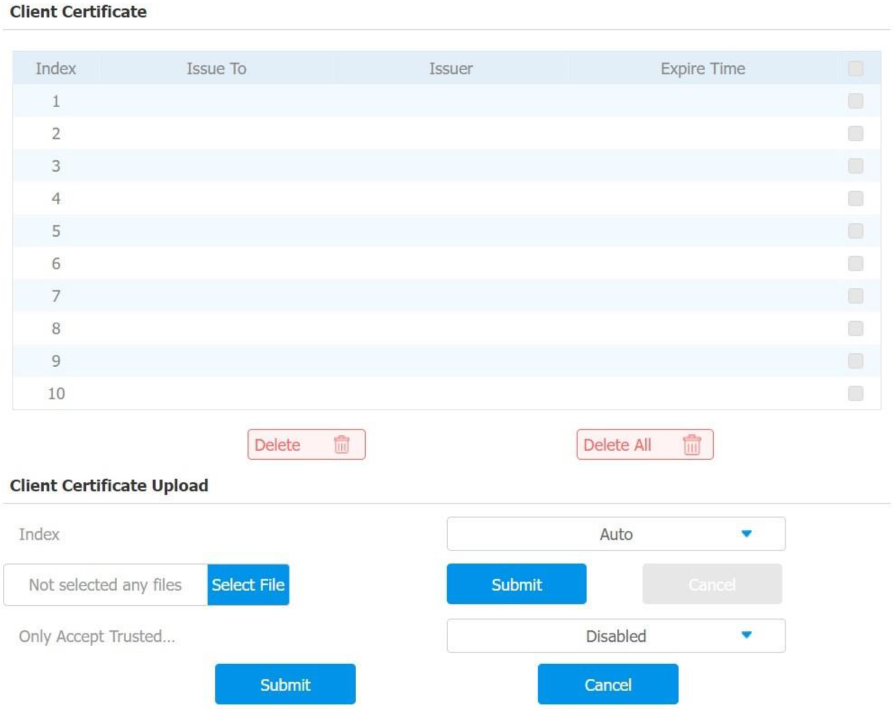
Web Server Certifica... Not selected any files

15.10.2 - Client certificate

When the device requires an SSL connection with the server, the phone needs to verify the server to make sure it can be trusted. The server sends its certificate to the device. The device verifies this certificate according to the client certificate list.

To upload and configure client certificates to the device web interface:

Security > Advanced > Client Certificate



Client Certificate

Index	Issue To	Issuer	Expire Time	□
1				□
2				□
3				□
4				□
5				□
6				□
7				□
8				□
9				□
10				□

Client Certificate Upload

Index: Auto

Not selected any files

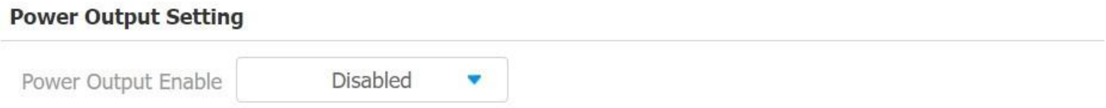
Only Accept Trusted...: Disabled

Table A27 - MyBell 2-Wire Indoor Monitor - Configuration of the client certificate	
Setting	**Description**
Index	Select the desired value from drop-down list of Index. If you select the **Auto** value, the uploaded certificate is displayed in numeric order. If you select values from 1 to 10, the uploaded certificate is displayed according to the value selected.
Select File	Click to choose file by browsing the local drive, and locate the desired certificate (*.pem only).
Only Accept Trusted Certificates	If **Enabled**, as long as the authentication succeeds, the device verifies the server certificate based on the client certificate list. If you select **Disabled**, the device verifies the server certificate no matter whether the certificate is valid or not.

15.11 - Power output setting

To enable the power output function for the PON interface using the device web interface:

Device Setting > Basic > Power Output Setting



Power Output Setting

Power Output Enable: Disabled

Note.

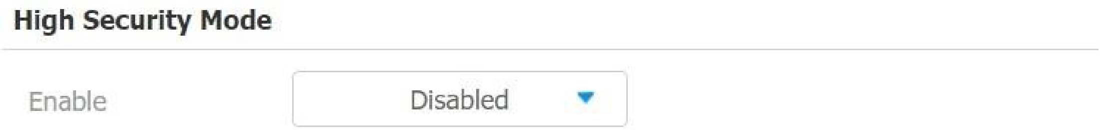
When the Power Output function is enabled, and the PON interface is connected with some particular exchangers, which can cause the device to reboot repeatedly.

15.12 - High security mode

High security mode is designed to enhance the security. For example, it optimizes the password storage method.

To configure the high security mode by the web interface

Security > Basic > High Security Mode



High Security Mode

Enable: Disabled

Important notes.

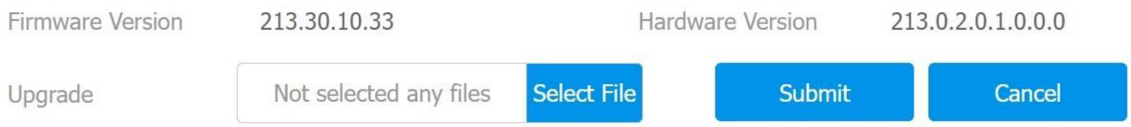
- Once the high security mode is enabled, you can't downgrade the device from the version with this mode to an old one without it.
- This mode is disabled by default when the device is upgraded to a new version with high security from an older version without the high security mode. However, if the device is reset to its factory settings, this mode is enabled by default.
- Enabling this mode makes the old version tools unusable. To continue using them, you need to upgrade them to the following versions:
  - PC Manager: 1.2.0.0
  - IP Scanner: 2.2.0.0
  - Upgrade Tool: 4.1.0.0
  - SDMC: 6.0.0.34
- The supported HTTP format varies depending on whether the high secure mode is enabled or disabled.
  When the mode is turned on, the device only supports new HTTP formats for door opening.
  - http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
  - http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

  When the mode is off, the device supports the above two new formats as well as the old one:
  - http://deviceIP/fcgi/do?ction=OpenDoor&UserName=username&Password=password&DoorNum=1
- You can't import or export tgz. format configuration files between a new version device and an old version device without the high security mode.

16 FIRMWARE UPGRADE

To upgrade the device by the device web interface:

Upgrade > Basic



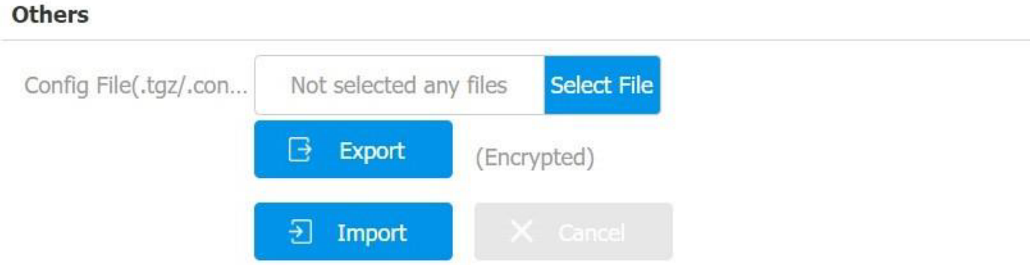
Firmware Version	213.30.10.33	Hardware Version	213.0.2.0.1.0.0.0
Upgrade	Not selected any files		

Note.

Firmware files should be .rom format for an upgrade.

To import or export encrypted configuration files to your Local PC:

Upgrade > Advanced > Others



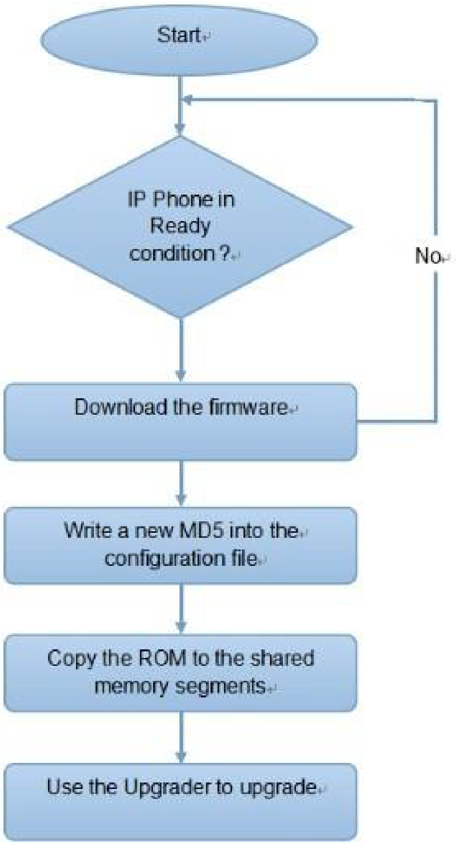
Others

Config File(.tgz/.con... Not selected any files

18 AUTO-PROVISIONING

Auto-provisioning is a feature used to configure or upgrade devices in batch using third-party servers. DHCP, PNP, TFTP, FTP, and HTTPS protocols are used by MyBell intercom devices to access the URL address of the third-party server which stores configuration files and firmware used to update the firmware and the corresponding settings on the device.

See the flow chart below:


Start
IP Phone in Ready condition ?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments
Use the Upgrader to upgrade

18.1 - Introduction to the configuration files for auto-provisioning

Configuration files have two following formats for auto-provisioning:

- **General configuration provisioning** - a general file is stored in a server from which all the related devices can download the same configuration file to update settings on the devices. For example, cfg.
- **MAC-based configuration provisioning** - MAC-based configuration files are used for auto-provisioning on a specific device as distinguished by its unique MAC number. The configuration files named with the device MAC number are matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note.

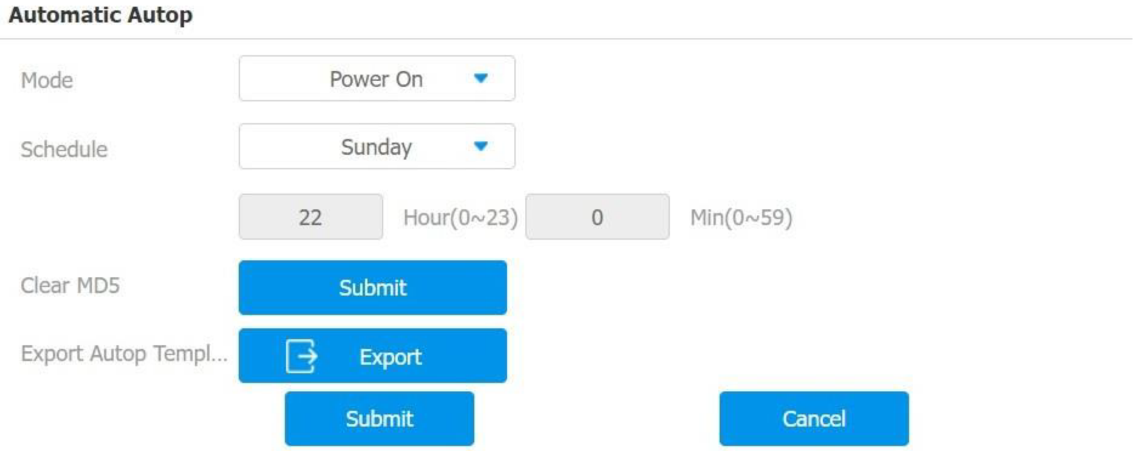
If a server has these two types of configuration files, then IP devices first access the general configuration files before accessing the MAC-based configuration files.

18.2 - Autop schedule

The device provides you with different Autop methods that enable the indoor monitor to perform provisioning for itself in a specific time according to your schedule.

To set up the schedule by the device web interface:

Upgrade > Advanced > Automatic Autop



Automatic Autop

Mode: Power On

Schedule: Sunday

22 Hour(0~23) 0 Min(0~59)

Clear MD5: Submit

Export Autop Templ...: Export

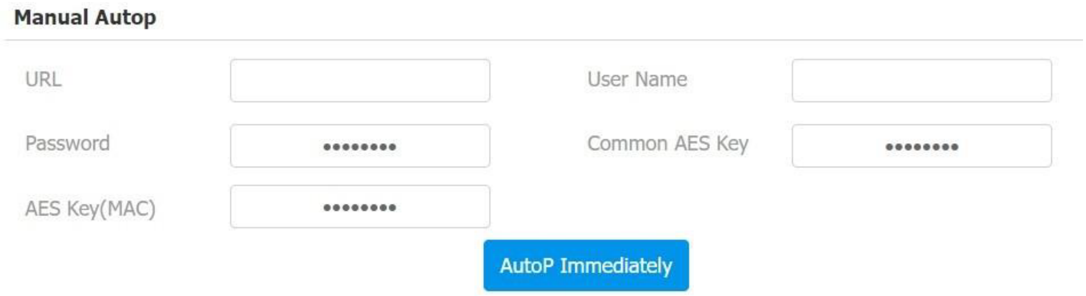
Table A30 - MyBell 2-Wire Indoor Monitor - Configuration of the automatic autop	
Setting	**Description**
Power On	Select **Power On** if you want the device to perform Autop every time it boots up.
Repeatedly	Select **Repeatedly** if you want the device to perform autop according to the schedule you set up.
Power On + Repeatedly	Select **Power On + Repeatedly** if you want to combine **Power On** mode and **Repeatedly** mode, which enable the device to perform Autop every time it boots up or according to the schedule you set up.
Hourly Repeat	Select **Hourly Repeat** if you want the device to perform Autop every hour.

18.3 - Static provisioning configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device performs the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS protocols can be used for upgrading the device firmware and configuration.

To configure static provisioning:

Upgrade > Advanced > Manual Autop



Manual Autop

URL

User Name

Password ••••••••

Common AES Key ••••••••

AES Key(MAC) ••••••••

Table A31 - MyBell 2-Wire Indoor Monitor - Configuration of the static provisioning	
Setting	**Description**
URL	Set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
Common AES Key	Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
AES Key (MAC)	Set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note.

- AES encryption should be configured only when the config file is encrypted with AES.
- User specified server isn't provided. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/ (allows anonymous login)
  - ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/ (use the default port 80)
  - http://192.168.0.19:8080/ (use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/ (use the default port 443)
- The general configuration file for the in-batch provisioning is with the format cfg. For example, r000000000313.cfg (9 zeros in total). While the MAC-based configuration file for the specific device provisioning is with the format MAC_Address of the device.cfg, for example, 0C 110504AE5B.cfg.

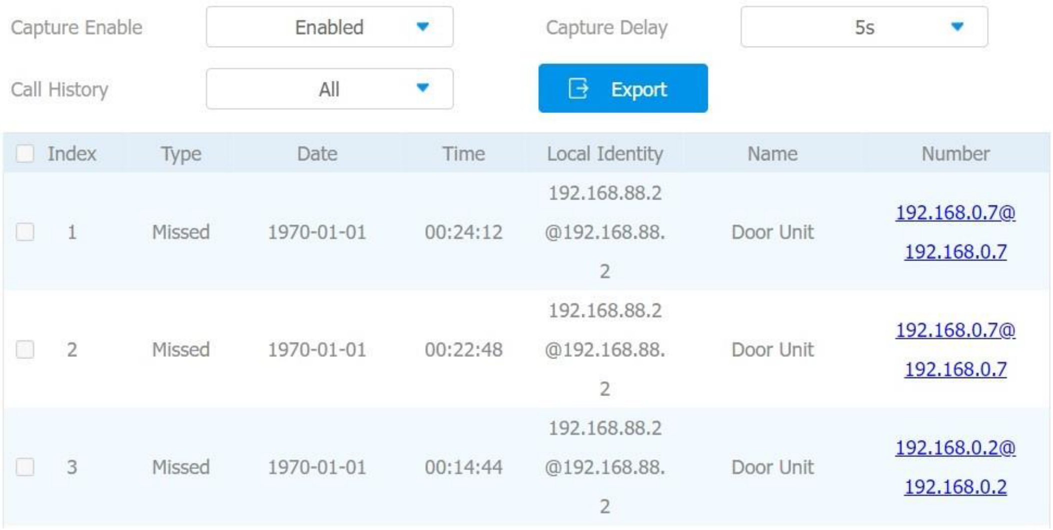
18.4 - Call log

If you want to check the dial-out calls, received calls, and missed calls in a certain period, you can search the call log by the device web interface and export the call log from the device if needed.

You can also set up the call-related picture capturing if needed.

To check call logs by the device web interface:

Contacts > Call Log



Capture Enable: Enabled ▾

Capture Delay: 5s ▾

Call History: All ▾

Export

□	Index	Type	Date	Time	Local Identity	Name	Number
□	1	Missed	1970-01-01	00:24:12	192.168.88.2@192.168.88.2	Door Unit	192.168.0.7@192.168.0.7
□	2	Missed	1970-01-01	00:22:48	192.168.88.2@192.168.88.2	Door Unit	192.168.0.7@192.168.0.7
□	3	Missed	1970-01-01	00:14:44	192.168.88.2@192.168.88.2	Door Unit	192.168.0.2@192.168.0.2

Table A32 - MyBell 2-Wire Indoor Monitor - Configuration of the call log

Setting	Description
Call History	Select call history (All, Dialed, Received, Missed, and Forwarded) for the specific type of call log to be displayed.
Capture Enabled	Enable it so that the picture of the calling party (e.g., picture of a visitor) can be captured in the video preview.
Capture Delay	Set the image capturing starting time when the device goes into a video preview (5-10 seconds).

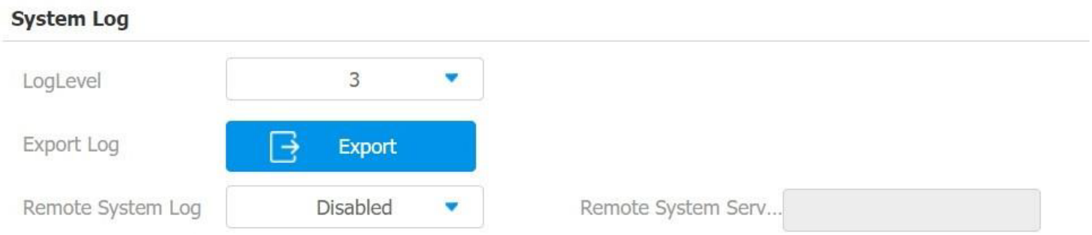
19 DEBUG

19.1 - System Log for debugging

System logs can be used for debugging purposes.

To export the system logs out to a local PC or to a remote server for debugging by the device web interface:

Upgrade > Advanced > System Log



System Log

LogLevel: 3

Export Log: Export

Remote System Log: Disabled

Remote System Serv...

Setting:

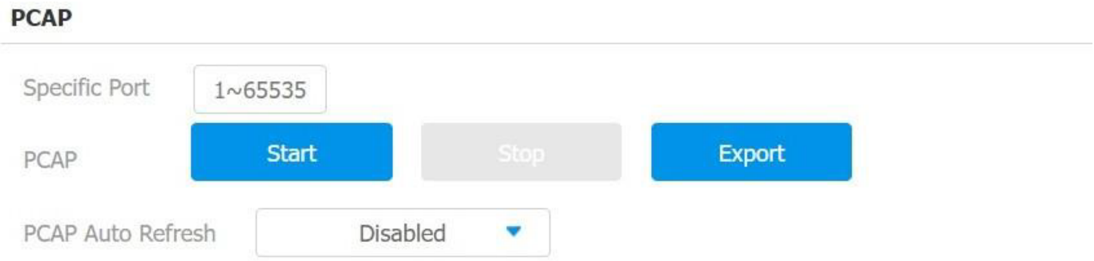
- **LogLevel:** Select log levels from 1 to 7 levels. The default log level is 3. The higher the level is, the more complete the log is.
- **Remote System Server:** Enter the remote server address to receive the device logs.

19.2 - PCAP for debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes. PCAP needs to be set up before using it.

To set up PCAP by the device web interface:

Upgrade > Advanced > PCAP



PCAP

Specific Port: 1~65535

PCAP: Start Stop Export

PCAP Auto Refresh: Disabled

Table A33 - MyBell 2-Wire Indoor Monitor - Configuration of the PCAP

Setting	Description
Specific Port	Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
PCAP	Click the Start tab and Stop tab to capture a certain range of data packets before clicking Export tab to export the data packets to your Local PC.
PCAP Auto Refresh	If set to **Enable**, PCAP continues to capture data packets even after the data packets reach their 50 MB maximum in capacity. If set to **Disable**, PCAP stops data packet capturing when the data packet captured reaches the maximum capturing capacity of 1 MB.

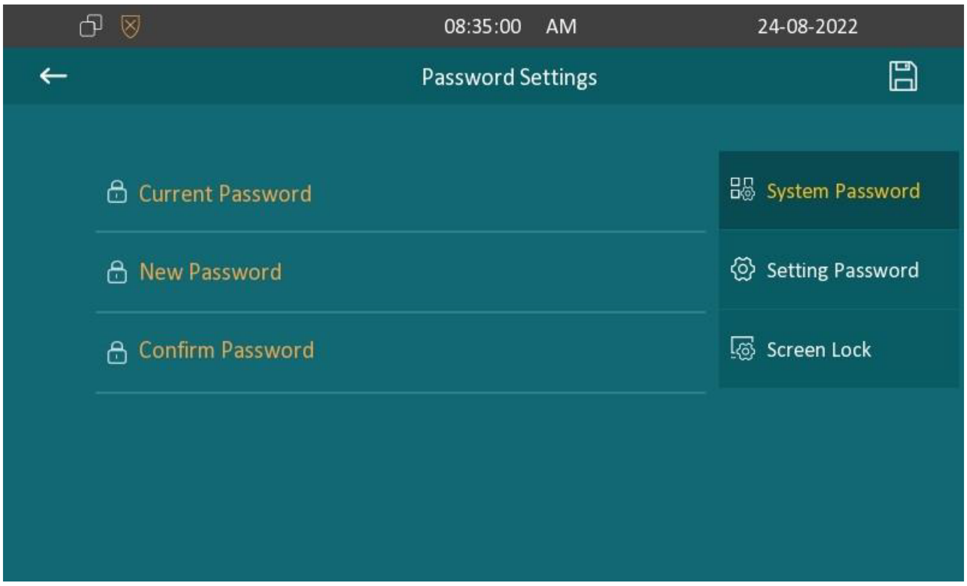
20 PASSWORD MODIFICATION

20.1 - Modification of the device advanced setting password

This password is used to enter the advanced settings of the device, including password settings, account numbers, SOS numbers, and network settings. The default password is **123456**.

To modify the advanced setting password on the device screen:

More > Setting > Advance > Password



08:35:00 AM 24-08-2022

Password Settings

Current Password

New Password

Confirm Password

Table A34 - MyBell 2-Wire Indoor Monitor - Modification of the password on the device

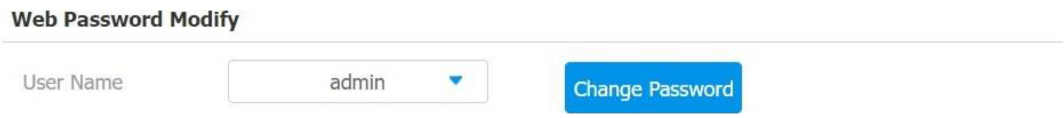
Setting	Description
Setting Password	Used to access the basic setting
System Password	Used to access advance settings
Screen lock	Used to unlock the screen

20.2 - Modification of the device web interface password

To modify the password by the web interface:

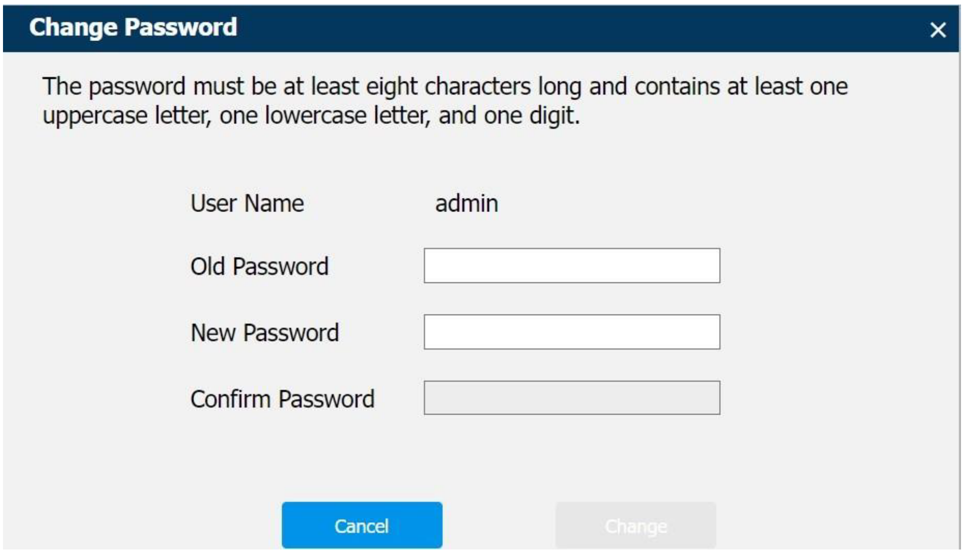
Security > Basic > Web Password Modify

Select **Admin** for the administrator account and **User** for the user account. Click the Change Password tab to change the password.



Web Password Modify

User Name admin



Change Password

The password must be at least eight characters long and contains at least one uppercase letter, one lowercase letter, and one digit.

User Name admin

Old Password

New Password

Confirm Password

Note.

The default password for the admin account is **admin.**

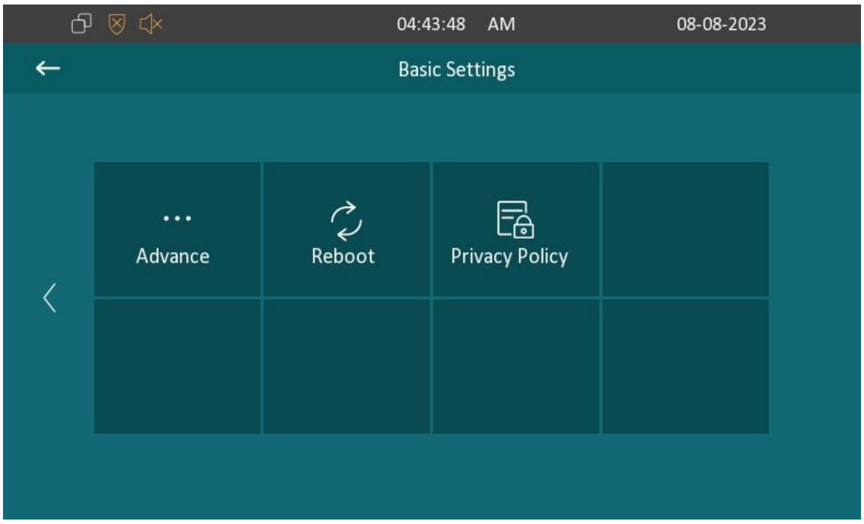
The default password for the user account is **user.**

21 SYSTEM REBOOT & RESET

21.1 - Reboot on the device

To reboot the system on the device screen:

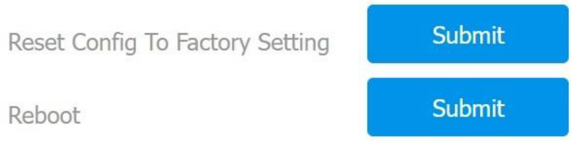
Setting > Reboot



21.2 - Reboot by the web interface

To reboot the system by the web interface:

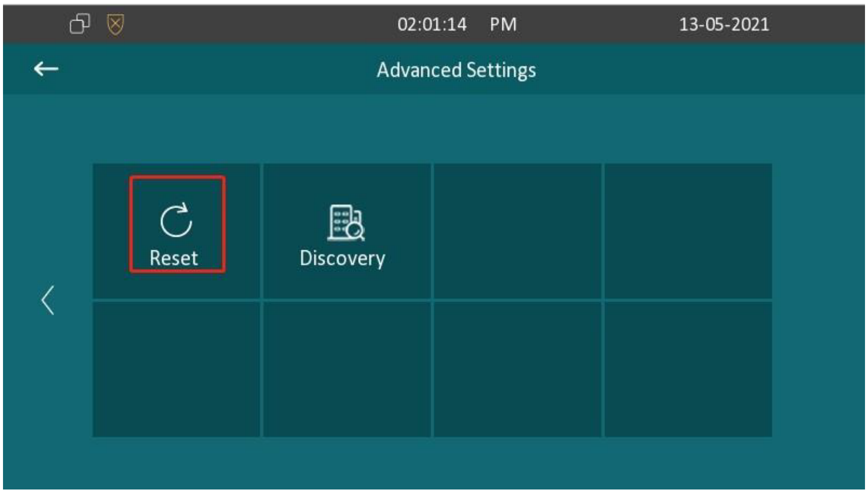
Upgrade > Basic



21.3 - Reset on the device

To reset the whole device system to the factory setting:

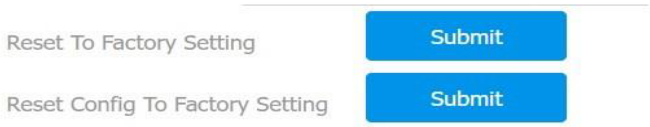
More > Setting > Advance



21.4 - Reset by the web interface

To reset the whole device system to the factory setting by the web interface:

Upgrade > Basic



You can click **Reset Config To Factory Setting** on the same page.

22 REGULATIONS

22.1 - Warranty

We warrant this product to be free from defects in material and workmanship under normal and proper use for one year from the purchase date of the original purchaser. We will, at its option, either repair or replace any part of the products that prove defective due to improper workmanship or materials. THIS LIMITED WARRANTY DOES NOT COVER ANY DAMAGE TO THIS PRODUCT THAT RESULTS FROM IMPROPER INSTALLATION, ACCIDENT, ABUSE, MISUSE, NATURAL DISASTER, INSUFFICIENT OR EXCESSIVE ELECTRICAL SUPPLY, ABNORMALMECHANICAL OR ENVIRONMENTAL CONDITIONS, OR ANY UNAUTHORIZED DISASSEMBLY, REPAIR OR MODIFICATION. This limited warranty shall not apply if: (i) the product was not used in accordance with any accompanying instructions, or (ii) the product was not used for its intended function. This limited warranty also does not apply to any product on which the original identification information has been altered, obliterated or removed, that has not been handled or packaged correctly, that has been sold as second-hand or that has been resold contrary to Country and other applicable export regulations.

22.2 - Declaration of conformity

Hereby, Nice S.p.A. declares that MyBell 2-Wire 1-button Kit is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: http://www.niceforyou.com/en/support

22.3 - WEEE Directive Compliance

Device labelled with this symbol should not be disposed with other household wastes. It shall be handed over to the applicable collection point for the recycling of waste electrical and electronic equipment.

IS0929A00EN_25-10-2024

Nice

Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com