MyBell

IP 1-button Station

EN - Instructions and warnings for installation and use

v0.2

CONTENT

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.

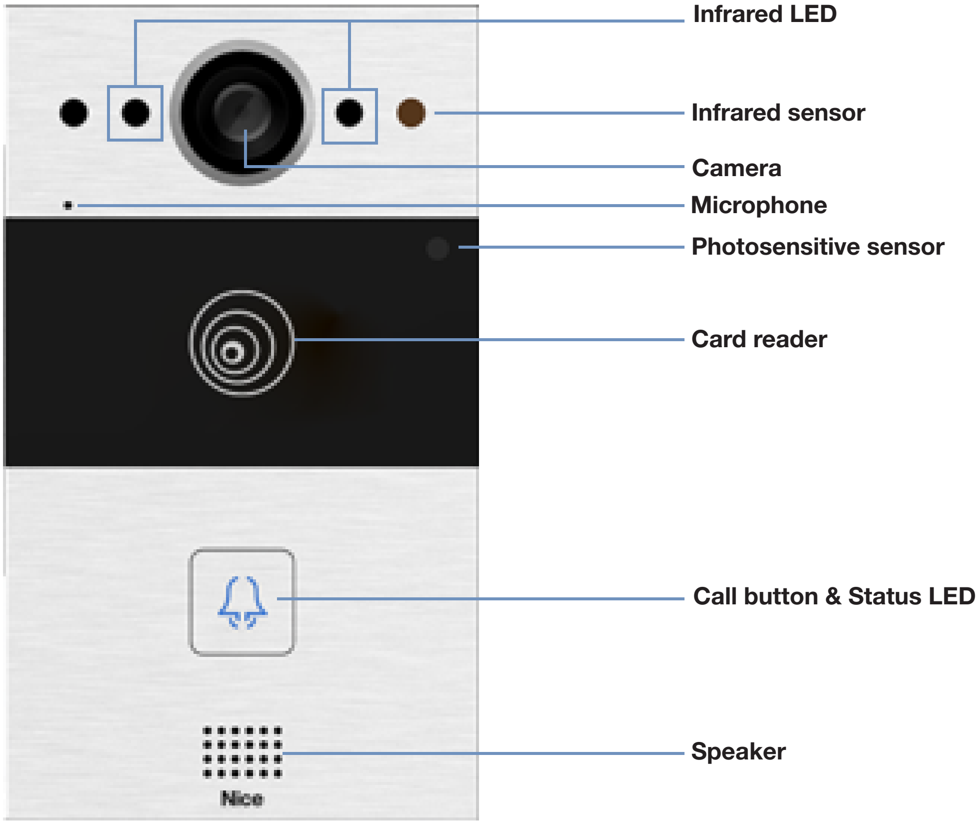
2 DEVICE DESCRIPTION

The device can be connected with indoor monitors for remote access control and communication. It enables audio and video calls with visitors and the door unlock funcion.

Table A1 - MyBell IP 1-button Station - Device description

Feature	Description
Operation System	Linux
Camera	2M pixels, automatic lighting
Front Panel	aluminium alloy
Wi-Fi	no
Ethernet	1xRJ45, 10/100 Mbps, adaptive
Power over Ethernet (PoE)	802.3af
Power Supply	12 V DC / 1.5 A
RS485 Port	1
Relay Output	2
Relay Input	2
Microphone	1
Speaker	1
Ethernet Ports	1 x RJ45
Installation	flush-mounted or wall-mounted
Dimensions	145 x 85 x 22 mm
Working Humidity	10~90%
Working Temperature	-30°C ~ +60°C
Storage Temperature	-40°C ~ +70°C
Button	single speed-dial button with blue backlight
Light Sensor	yes
Motion Sensor	yes
Wiegand Port	yes
RF Card Reader	13.56 MHz and 125 kHz, NFC
Tamper Alarm	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
Two-way Audio Communication over IP Networks	yes
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

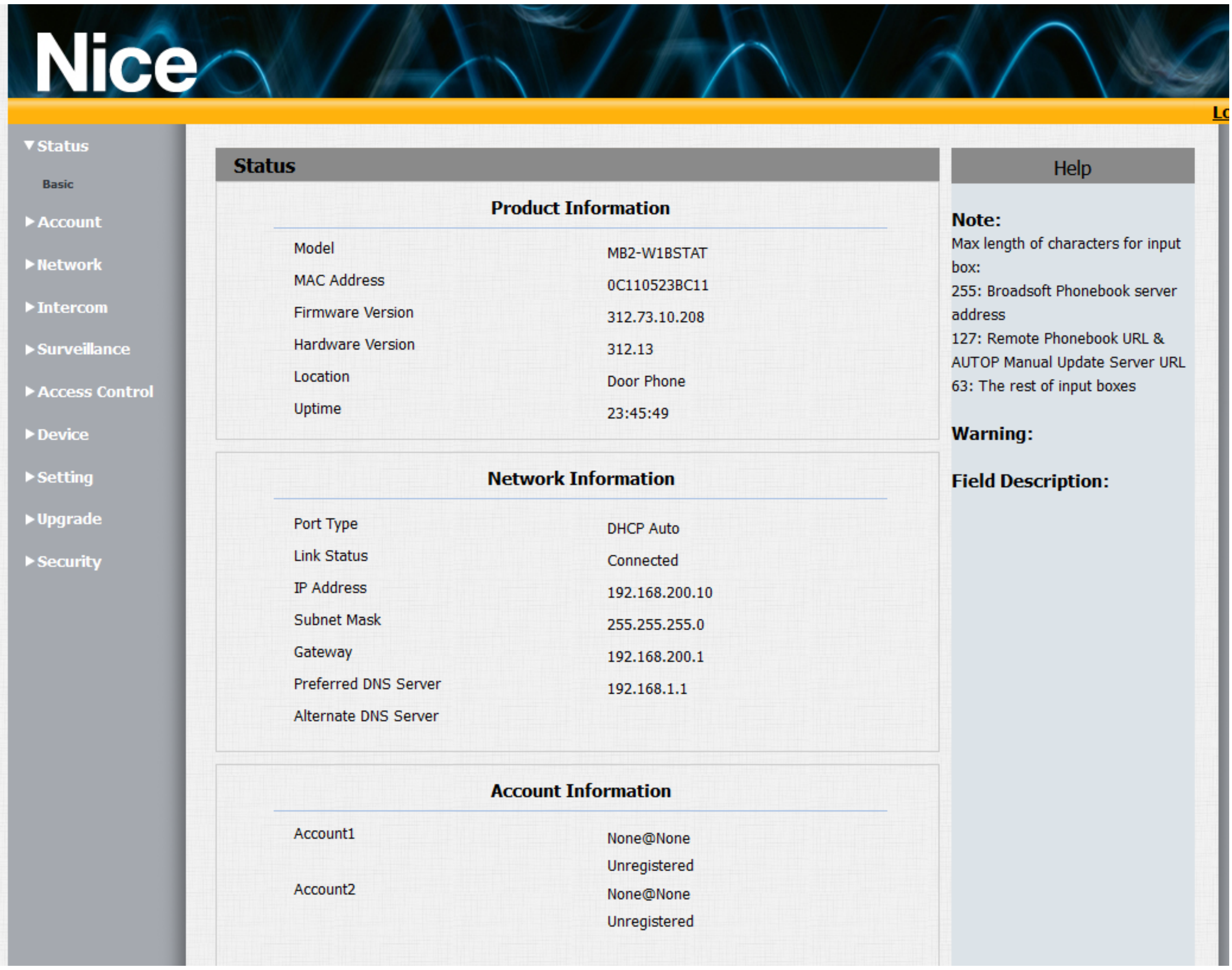
Table A1 - MyBell IP 1-button Station - Device description	
Feature	**Description**
Video Resolution	up to 1920 x 1080
Maximum Image Transfer Rate	1080p – 30 fps
Viewing Angle	110°(H) / 58°(V)
High Intensity IR LEDs for Picture Lightning During Dark Hours with Internal Light Sensor	yes
Compatible with 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, TLS, ICMP, DHCP, ARP
Auto-Provisioning	yes
Web Management Portal	yes
Web-based Packet Dump	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	• office door phone with on-site or hosted IP-PBX • remote site entry over Internet • apartment/flat intercom with door access control



3 CONFIGURATION MENU

Table A2 - MyBell IP 1-button Station - Configuration menu

Section	Description
Status	Basic information such as product information, network information, and account information.
Intercom	Intercom settings, call log, etc.
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.
Phone	Light, LCD, voice and tab & button display settings.
Contacts	Group and contact settings.
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	

Account Information

Account1	None@None Unregistered
Account2	None@None Unregistered

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:

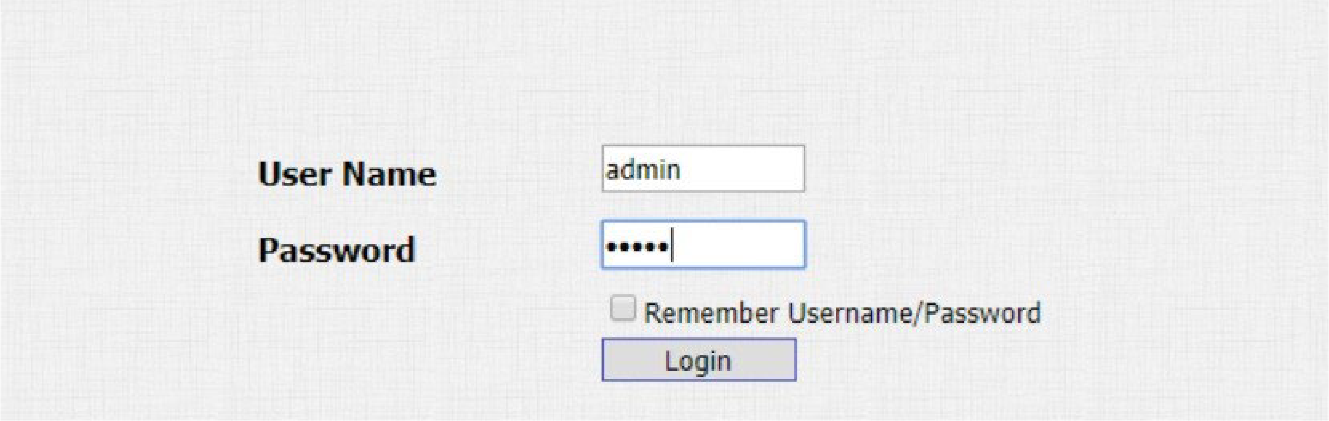
4 ACCESS TO DEVICE

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.

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 •••••

□ Remember Username/Password

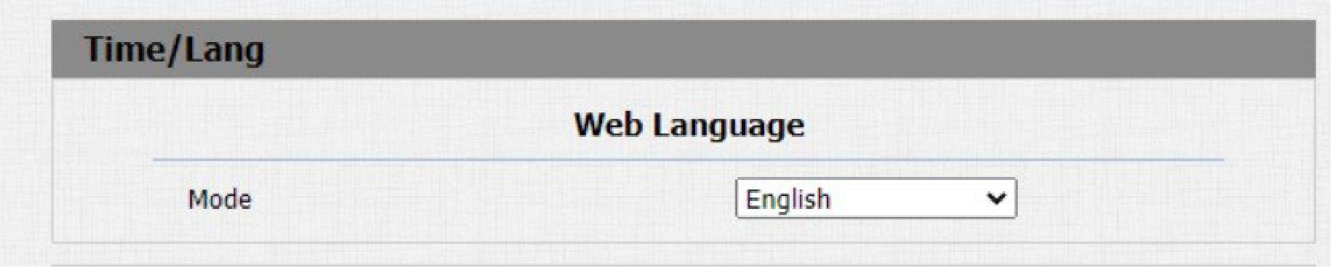
5 LANGUAGE AND TIME CONFIGURATION

5.1 - Language configuration

You can configure language during the initial device setup or later.

To configure language:

Phone > Time/Lang > Web Language



Time/Lang

Web Language

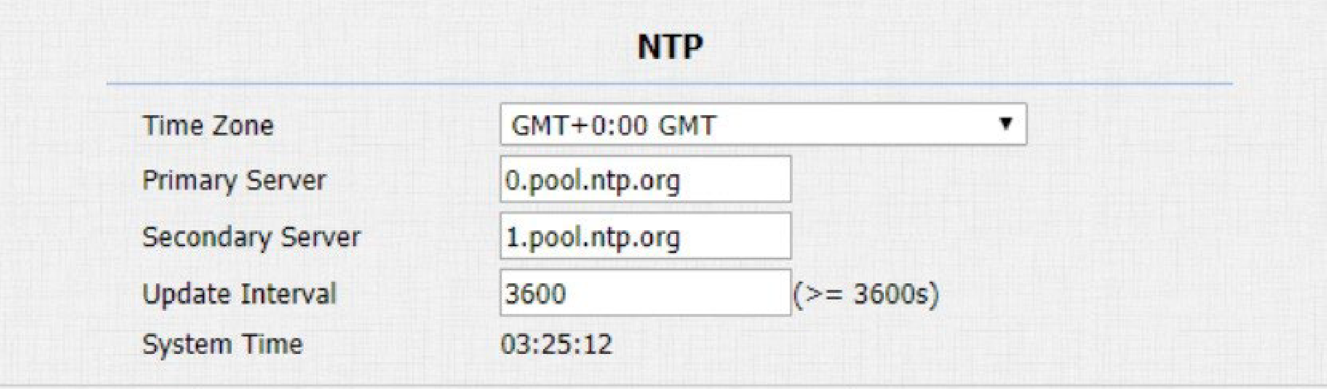
Mode: English

5.2 - Time configuration

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:

Phone > Time/Lang > NTP



NTP

Time Zone: GMT+0:00 GMT

Primary Server: 0.pool.ntp.org

Secondary Server: 1.pool.ntp.org

Update Interval: 3600 (>= 3600s)

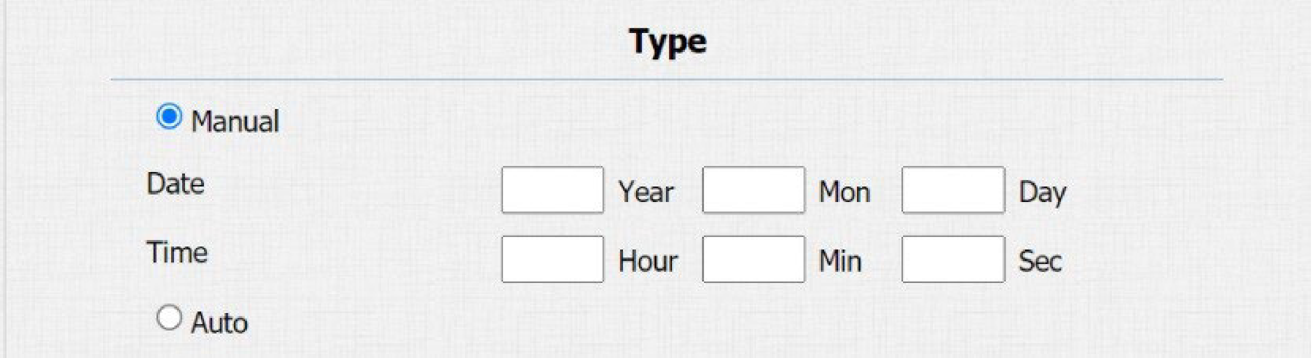
System Time: 03:25:12

Settings:

- **Primary/Secondary 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

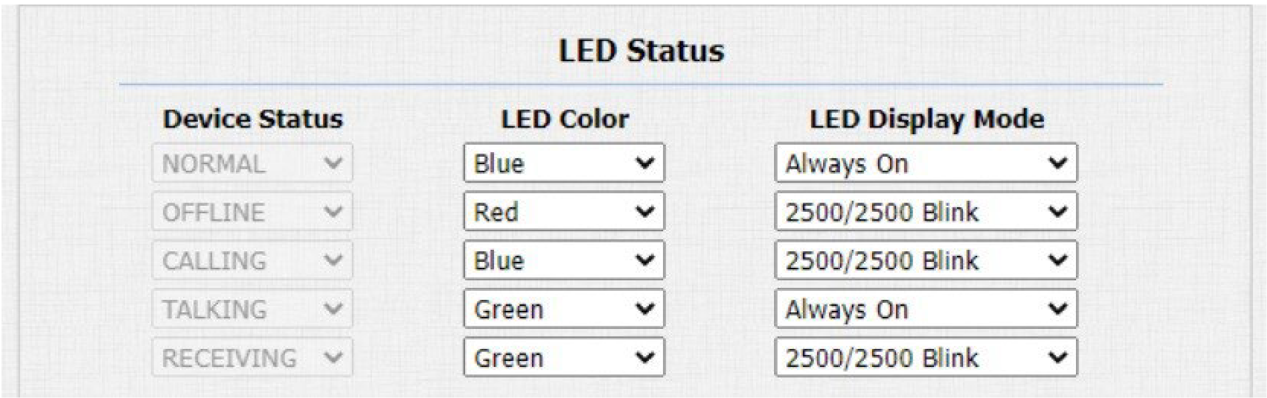
6 LED CONFIGURATION

6.1 - 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:

Intercom > LED Setting > LED Status



LED Status

Device Status	LED Color	LED Display Mode
NORMAL	Blue	Always On
OFFLINE	Red	2500/2500 Blink
CALLING	Blue	2500/2500 Blink
TALKING	Green	Always On
RECEIVING	Green	2500/2500 Blink

Table A3 - MyBell IP 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.
Pink	**Flashing**	Upgrading.

Table A4 - MyBell IP 1-button Station - LED status configuration

Setting	Description
State	There are five states: **Normal**, **Offline**, **Calling**, **Talking** and **Receiving**.
LED Color	It supports three colors: **Red**, **Green** and **Blue**.
LED Display Mode	It enables the configuration of different blink frequencies.

Note

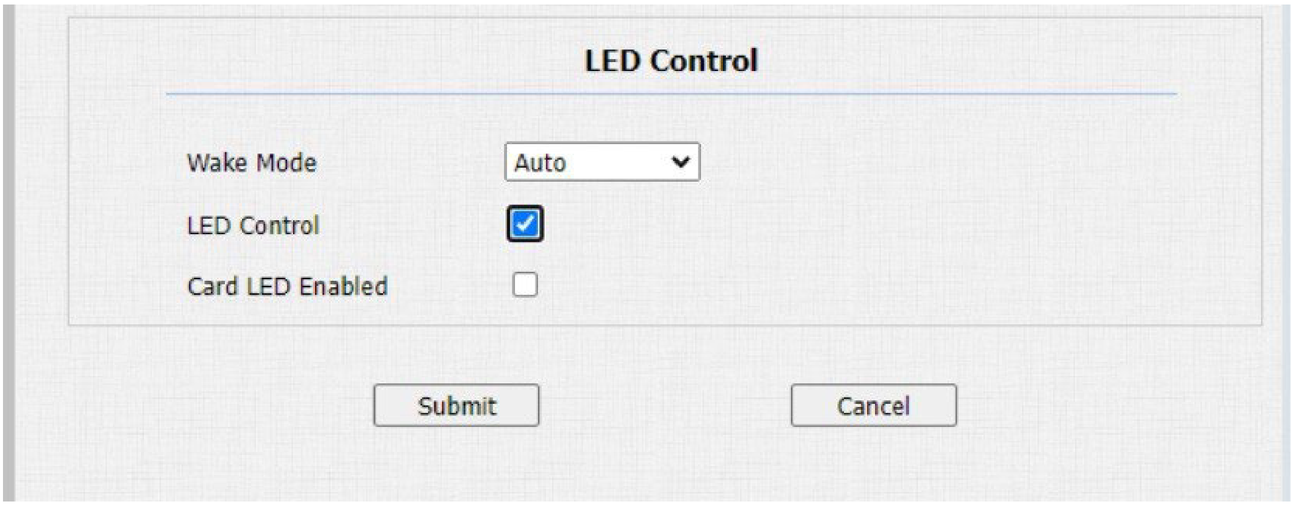
- The **State** and **Color** can't be changed.
- The **LED Color** of upgrading mode can't be adjusted.

6.2 - LED display configuration from HTTP URL

You can enter the HTTP URL in the browser to manage the LED color and frequency.

To enable this function by the web interface:

Intercom > LED Setting > LED Control



LED Control

Wake Mode: Auto

LED Control ☑

Card LED Enabled □

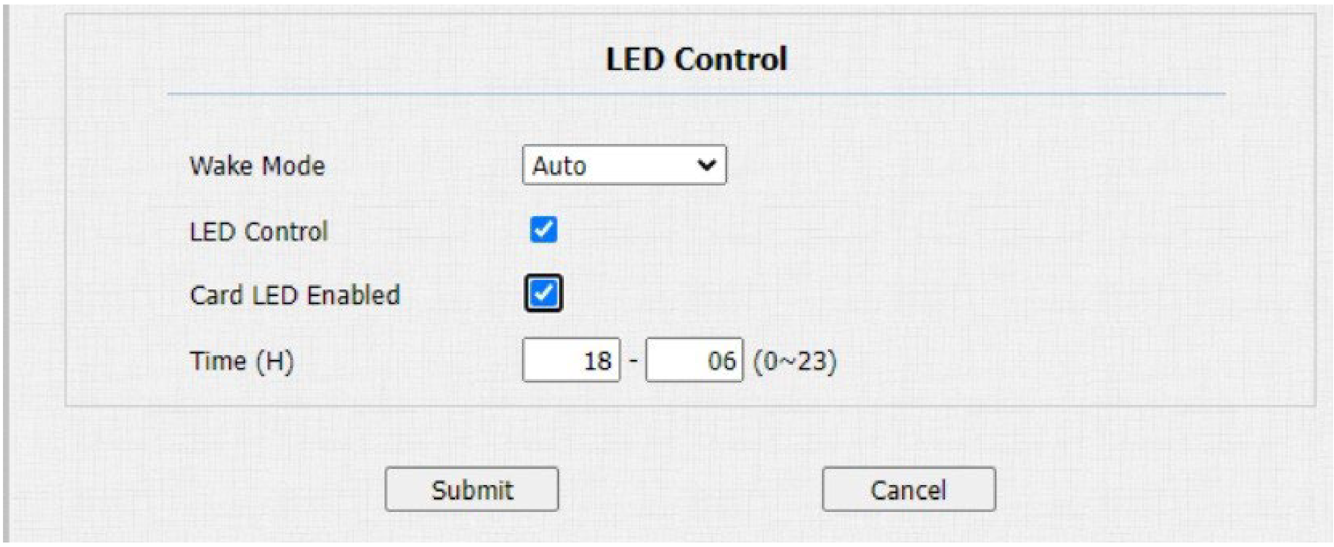
Table A5 - MyBell IP 1-button Station - LED display configuration from HTTP URL	
Setting	**Description**
HTTP URL Format	http://PhoneIP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500
Status	1=Idle 2=Offline 3=Calling 4=Talking 5=Receiving
Color	1=Green 2=Blue 3=Red
Mode	0=Always On 1=Always Off 500/1000/1500/2000/25000/3000

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:

Intercom > LED Setting > LED Control



LED Control

Wake Mode: Auto

LED Control: ☑

Card LED Enabled: ☑

Time (H): 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).

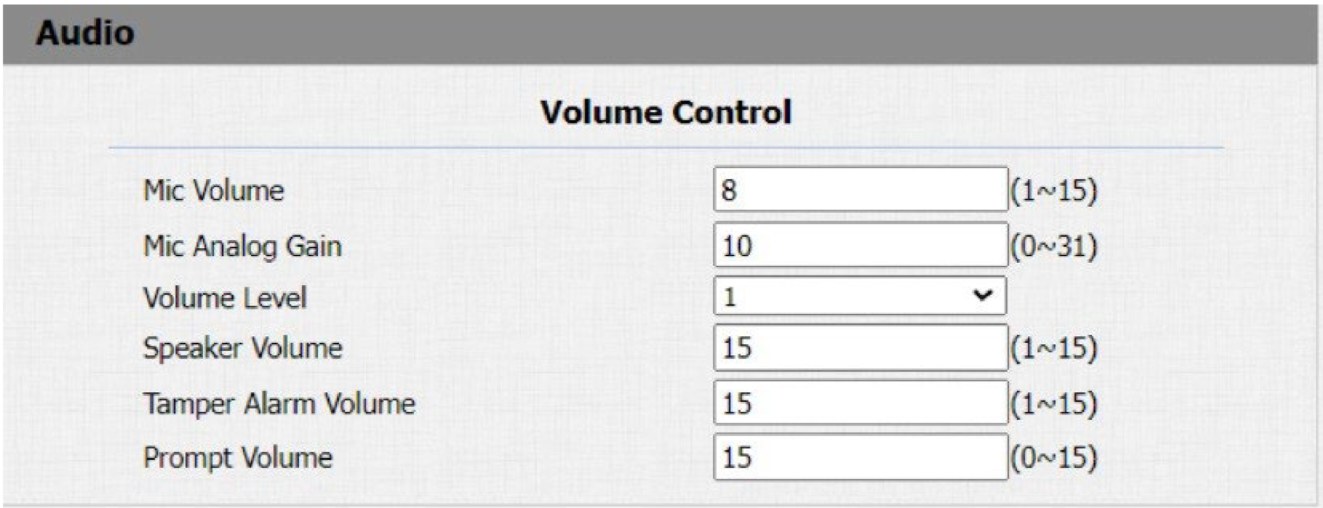
7 VOLUME AND TONE CONFIGURATION

7.1 - Volume configuration

You can configure the microphone volume for open-door notification and set up the tamper alarm volume in case of unwanted removal of the access control terminal.

To configure the volume by the web interface:

Phone > Audio > Volume Control



Audio

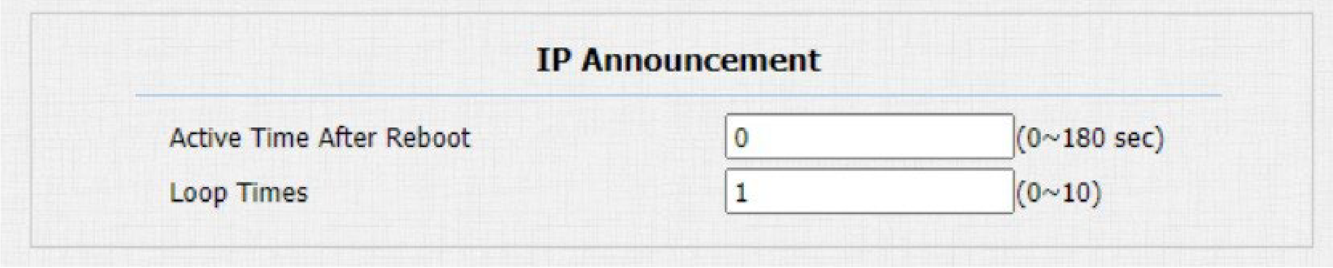
Volume Control

Mic Volume	8	(1~15)
Mic Analog Gain	10	(0~31)
Volume Level	1	
Speaker Volume	15	(1~15)
Tamper Alarm Volume	15	(1~15)
Prompt Volume	15	(0~15)

7.2 - IP announcement configuration

To configure the IP announcement by the web interface:

Phone > Audio > IP announcement



IP Announcement

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

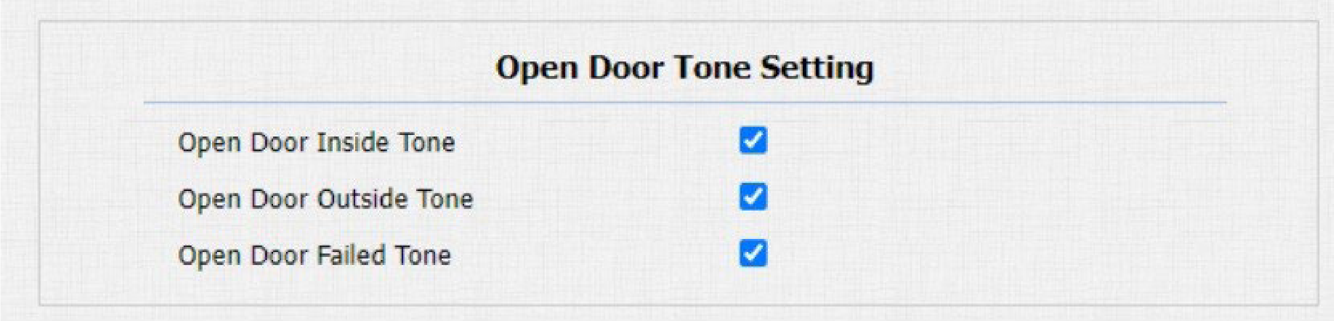
Setting:

- **Active Time After Reboot:** select IP announcement time after the device reboot.
  - If it's set to **30** seconds, you need to press the call button within 30 seconds after the reboot for the IP announcement. Otherwise, the IP announcement expires.
  - If it's set to **0** seconds, you need to press the call button any time after the reboot for the IP announcement.

7.3 - Open door tone configuration

To control the prompt words that accompany the tone by the web interface:

Phone > Audio > Open Door Tone Setting



Open Door Tone Setting

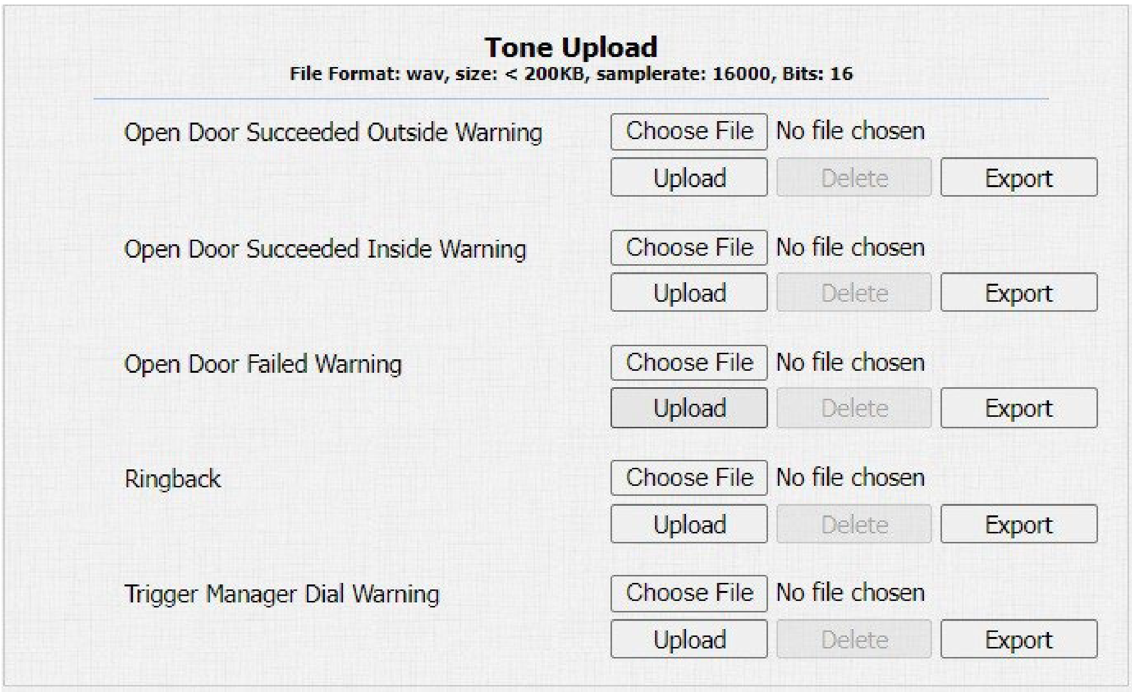
Open Door Inside Tone	☑
Open Door Outside Tone	☑
Open Door Failed Tone	☑

7.4 - Uploading tone files

7.4.1 - Uploading ringback tone

To upload the ringback tone by the web interface:

Phone > Audio > Tone Upload



Tone Upload

File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

Open Door Succeeded Outside Warning: No file chosen

Open Door Succeeded Inside Warning: No file chosen

Open Door Failed Warning: No file chosen

Ringback: No file chosen

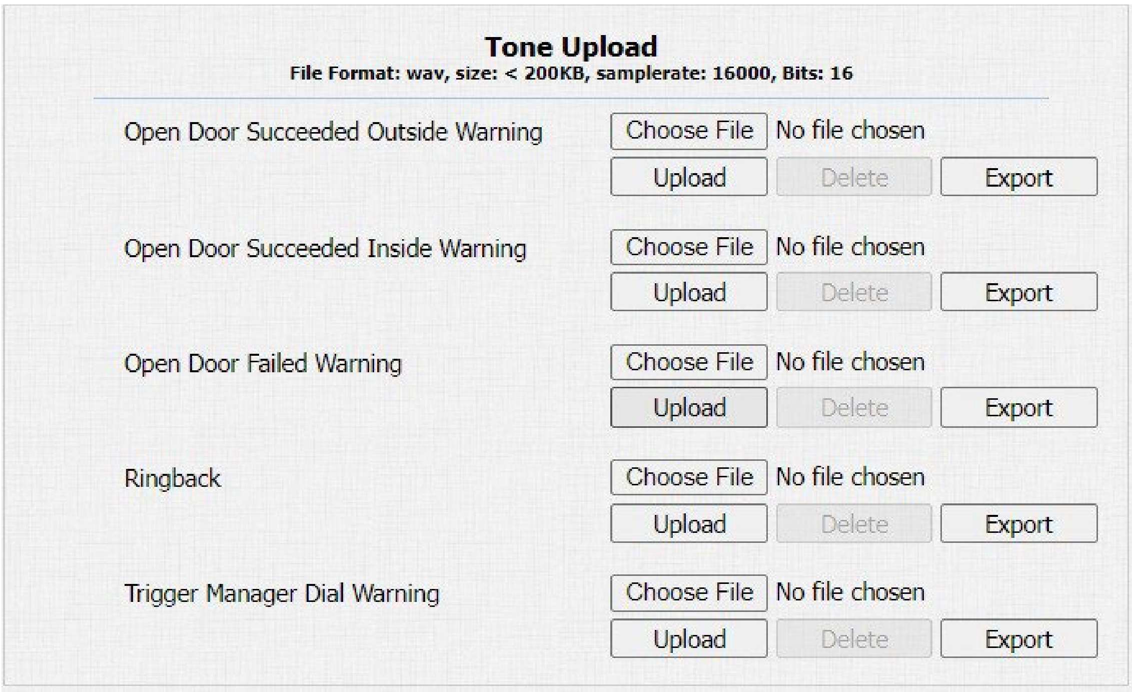
Trigger Manager Dial Warning: No file chosen

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:

Phone > Audio > Tone Upload



Tone Upload

File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

Open Door Succeeded Outside Warning: No file chosen

Open Door Succeeded Inside Warning: No file chosen

Open Door Failed Warning: No file chosen

Ringback: No file chosen

Trigger Manager Dial Warning: No file chosen

Settings:

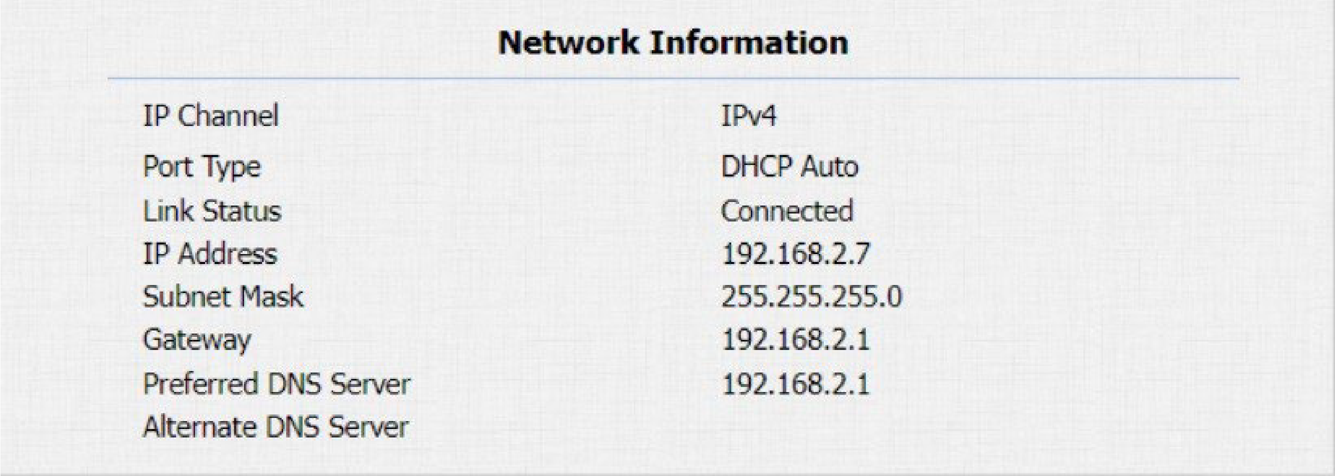
- **Open Door Succeeded Outside Warning:** warning tone that goes off when you open the door from the outside.
- **Open Door Succeeded Inside Warning:** warning tone that goes off when you open the door from the inside.

8 NETWORK CONFIGURATION

8.1 - Network status

To check the network status by the web interface:

Status > Basic > Network Information



Network Information

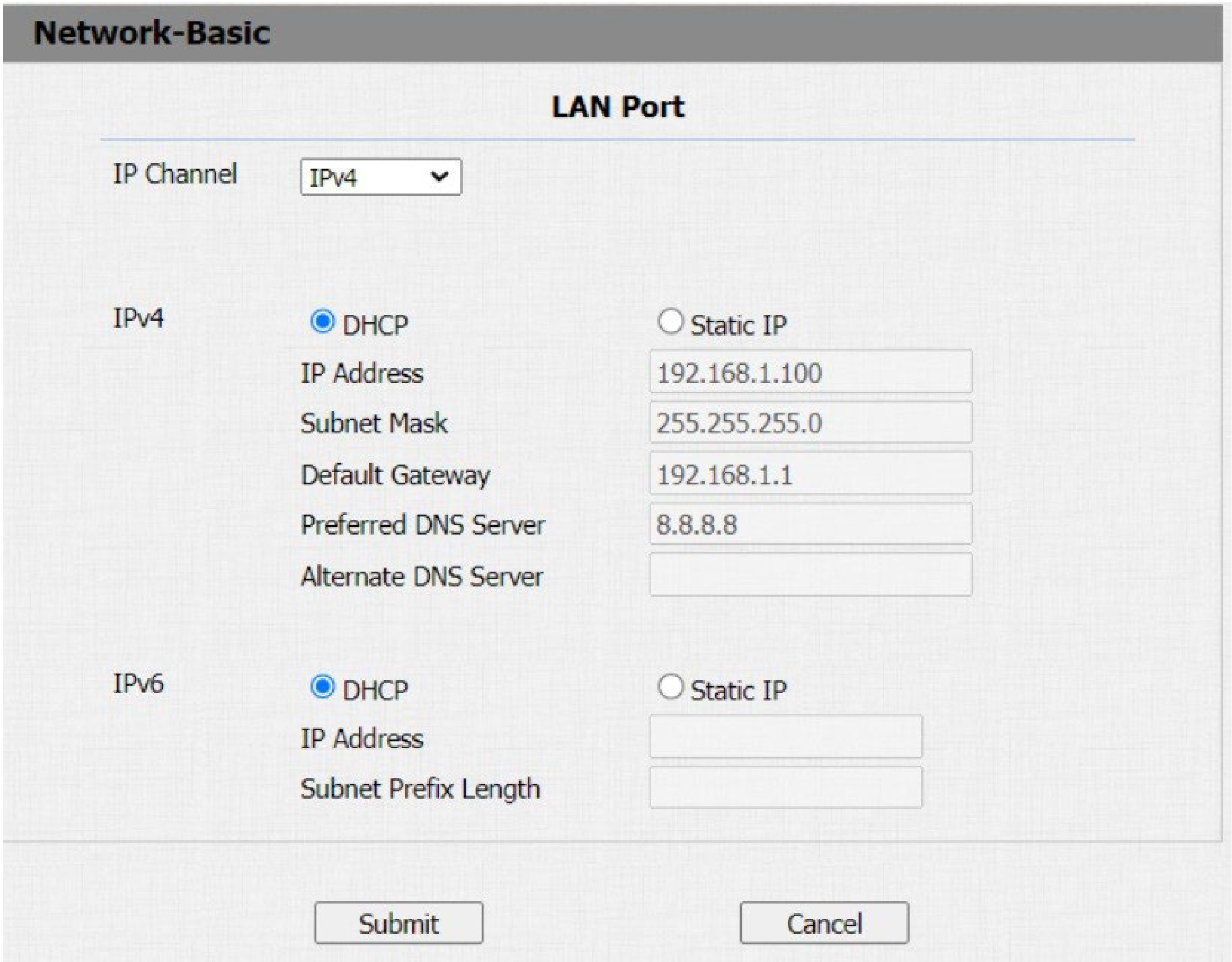
IP Channel	IPv4
Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.2.7
Subnet Mask	255.255.255.0
Gateway	192.168.2.1
Preferred DNS Server	192.168.2.1
Alternate DNS Server	

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	

IPv6: ● DHCP ○ Static IP

IP Address	
Subnet Prefix Length	

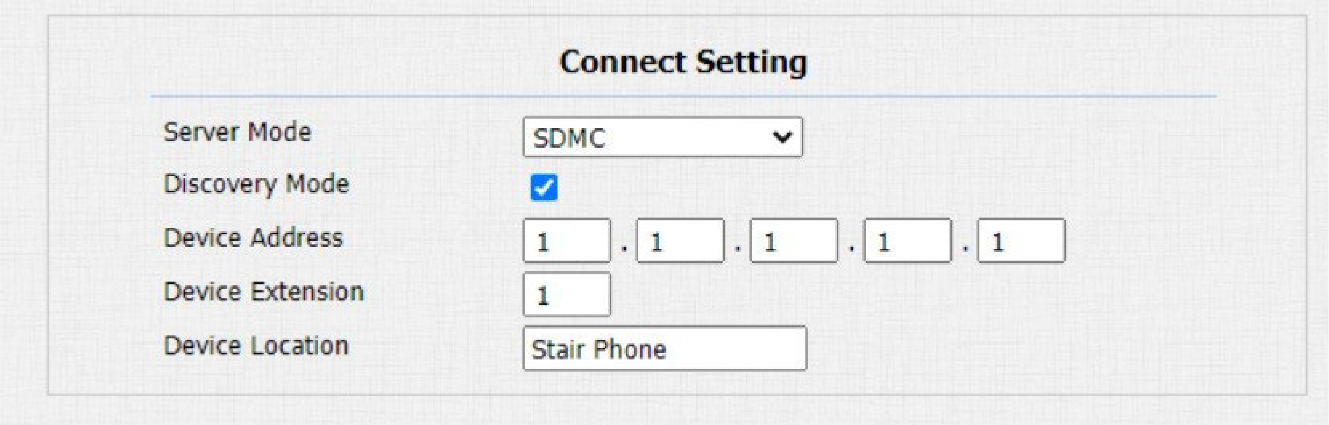
Table A6 - MyBell IP 1-button Station - Network configuration	
Setting	**Description**
DHCP	Select the **DHCP mode** by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, the door phone is assigned by the DHCP server with IP address, subnet mask, default gateway, and Domain Name Server (DNS) 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.
Subnet Prefix Length	Enter the subnet prefix length if needed.

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	☑
Device Address	1 . 1 . 1 . 1 . 1
Device Extension	1
Device Location	Stair Phone

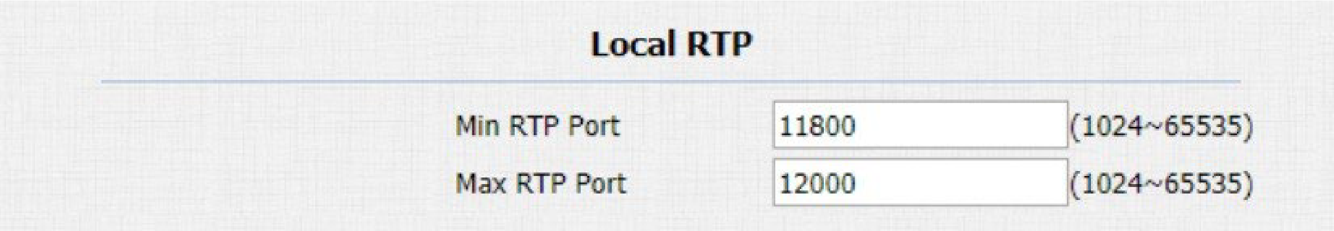
Table A7 - MyBell IP 1-button Station - Device deployment in network	
Setting	**Description**
Server Mode	It's set up automatically according to the device connection with a specific server in the network, such as **SDMC** or **Cloud** and **None**. **None** is the default factory setting indicating the device isn't in any server type and you can choose **Cloud, SDMC** in the discovery mode.
Discovery Mode	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 - Device local RTP configuration

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

To configure the device local RTP by the web interface:

Network > Advanced > Local RTP



Local RTP

Min RTP Port	11800	(1024~65535)
Max RTP Port	12000	(1024~65535)

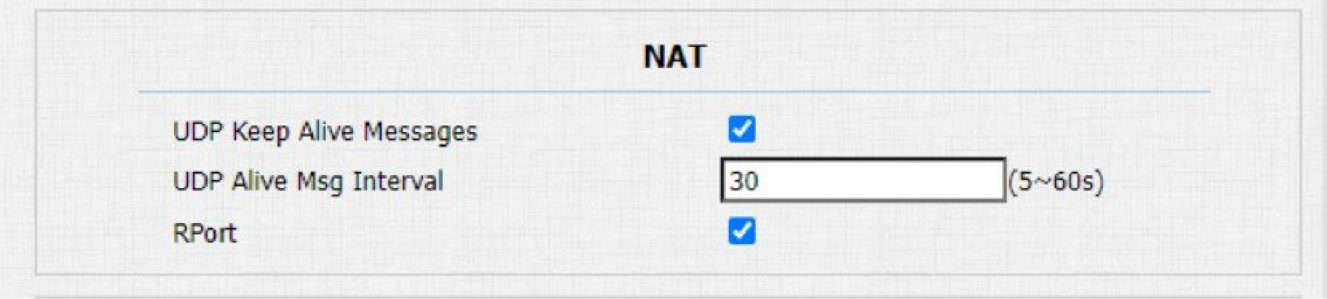
8.5 - NAT configuration

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 ☑

UDP Alive Msg Interval 30 (5~60s)

RPort ☑

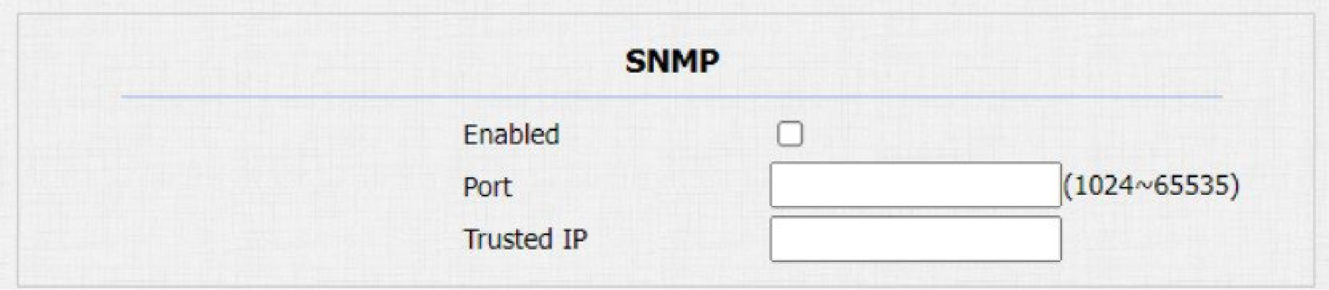
Table A8 - MyBell IP 1-button Station - NAT configuration	
Setting	**Description**
UDP Keep Alive Messages	If enabled, the device sends out the message to the SIP server and the SIP server recognizes if the device is online.
UDP Alive Msg Interval	Set the message sending time interval from 5 to 60 seconds. The default time is 30 seconds.
RPort	Enable the RPort when the SIP server is in Wide Area Network (WAN).

8.6 - SNMP configuration

Simple Network Management Protocol (SNMP) is a protocol for managing IP network devices. It enables network administrators to monitor devices and receive alerts for attention-worthy conditions. SNMP provides variables describing system configuration, organized in hierarchies and described by Management Information Bases (MIBs).

To configure the SNMP by the web interface:

Network > Advanced > SNMP



SNMP

Enabled □

Port (1024~65535)

Trusted IP

Setting:

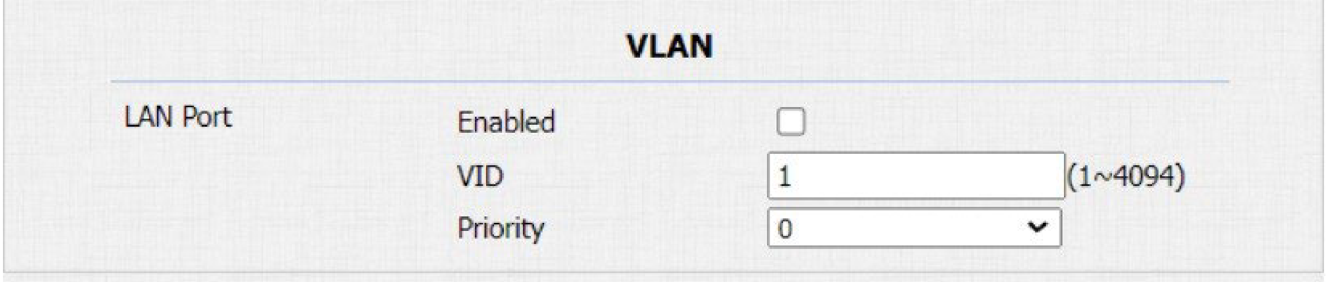
- **Trusted IP:** configure allowed SNMP server address. It could be an IP address or any valid URL domain name.

8.7 - VLAN configuration

A 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 using switches or routers, sending tagged packets only to ports with matching VLAN IDs. Using VLANs enhances security by limiting ARP attacks to specific hosts and improves network performance by minimizing unnecessary broadcast frames, conserving bandwidth for increased efficiency.

To configure the VLAN by the web interface:

Network > Advanced > VLAN interface



VLAN

LAN Port

Enabled □

VID 1 (1~4094)

Priority 0

Settings:

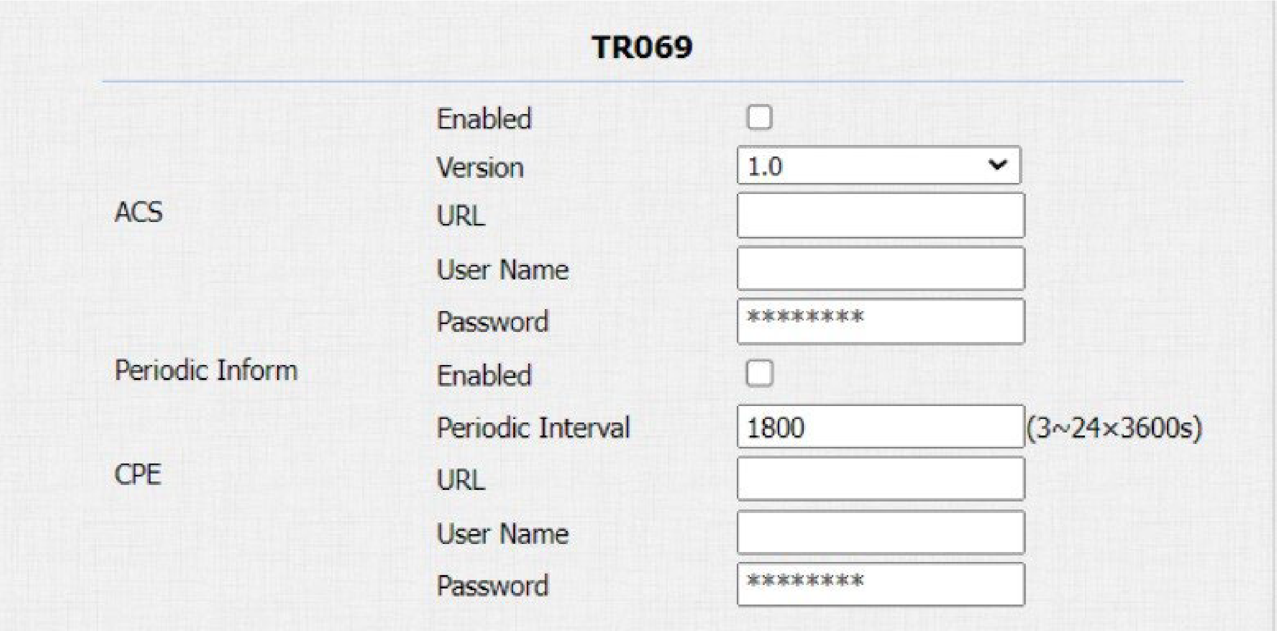
- **VID:** configure VLAN ID for designated port.
- **Priority:** select VLAN priority for designated port.

8.8 - TR069 configuration

Technical Report 069 (TR-069) provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes the safe auto configuration and the control of other CPE management functions within an integrated framework. The administrators can manage all door phones using a common TR-069 Platform. The devices can be configured easily and securely on the TR-069 platform to make mass deployment more efficient.

To configure the TR069 by the web interface:

Network > Advanced > TR069



TR069

ACS	Enabled	□
	Version	1.0
	URL	
	User Name	
	Password	********
Periodic Inform	Enabled	□
	Periodic Interval	1800 (3~24×3600s)
CPE	URL	
	User Name	
	Password	********

Table A9 - MyBell IP 1-button Station - TR069 configuration

Setting	Description
Version	Select the supported TR069 version (1.0 or 1.1).
ACS/CPE	• **ACS** – Auto Configuration Servers on the server side. • **CPE** – Customer-Premise Equipment on the client side devices.
URL	Configure URL address for ACS or CPE.
Periodic Inform	Tick this checkbox to enable periodic inform.
Periodic Interval	Configure the interval for periodic inform.

Note

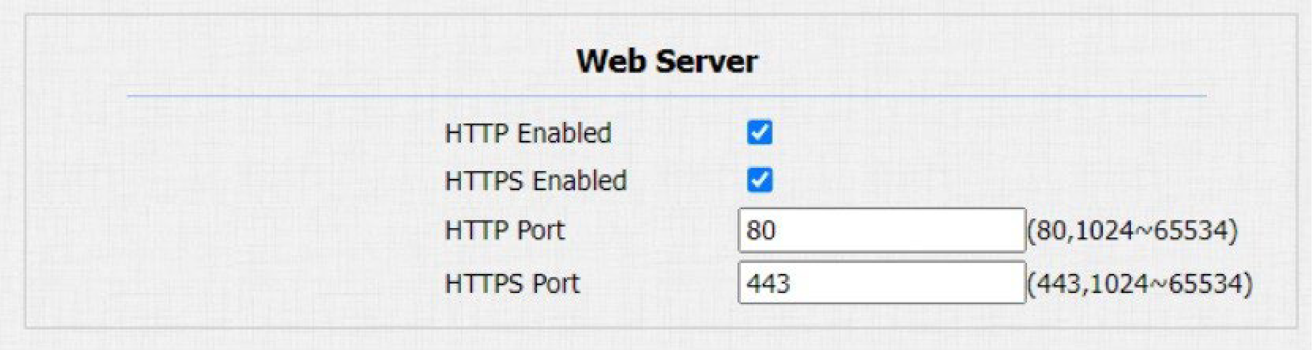
TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines the application layer protocol for remote management of end-user devices.

8.9 - 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)

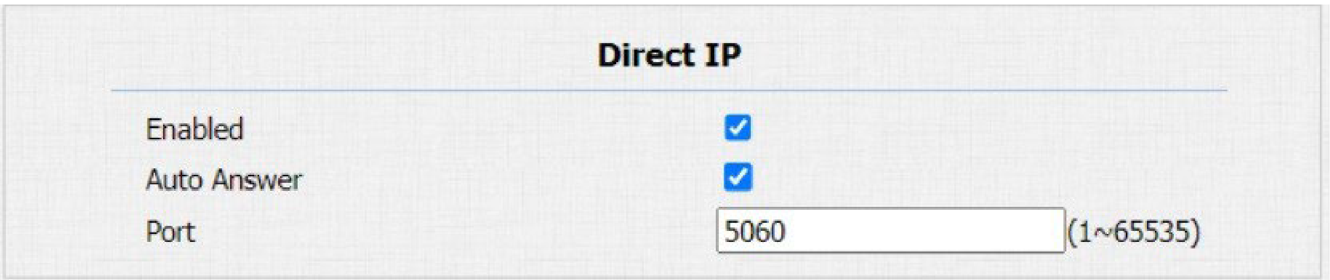
9 INTERCOM CALL CONFIGURATION

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:

Phone > Call Feature > Direct IP



Direct IP

Enabled ☑

Auto Answer ☑

Port 5060 (1~65535)

9.2 - SIP call and SIP call configuration

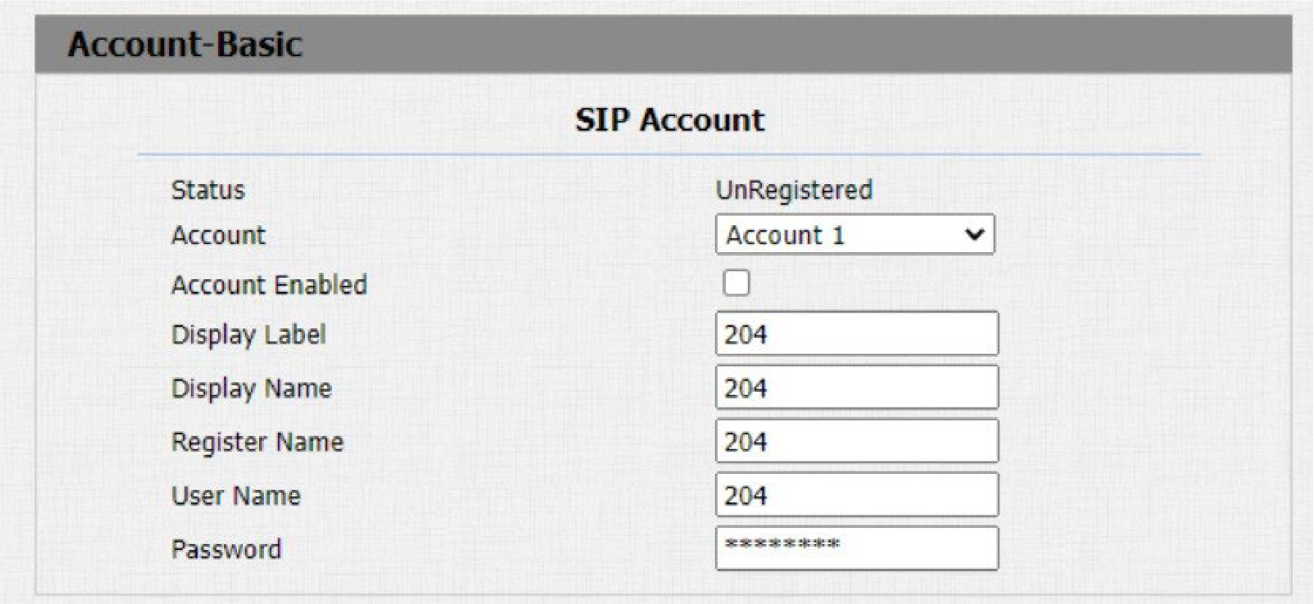
You can make a Session Initiation Protocol (SIP) call in the same way as you make the IP calls using the device. However, SIP call settings related to its account, server, and transport type need to be configured first.

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.

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 ********

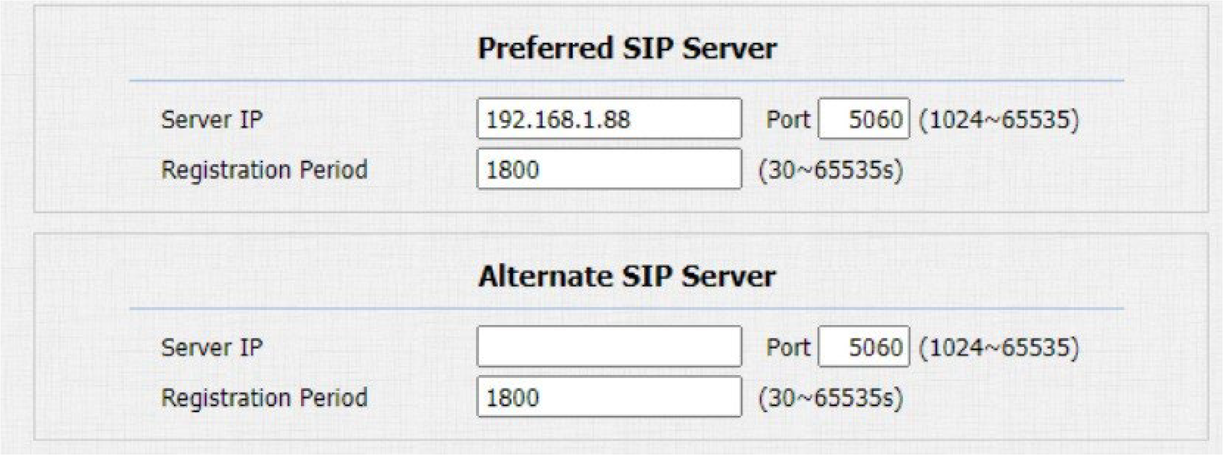
Table A10 - MyBell IP 1-button Station - SIP account registration	
Setting	**Description**
Display Label	Configure the device label to be shown on the device screen.
Display Name	Configure the name, for example, the device name to be shown on the device being called to.
Register Name	Enter the SIP account register name obtained from the SIP account administrator.
User Name	Enter the username obtained from the SIP account administrator.
Password	Enter the password obtained from the SIP server.

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 A11 - MyBell IP 1-button Station - SIP server configuration

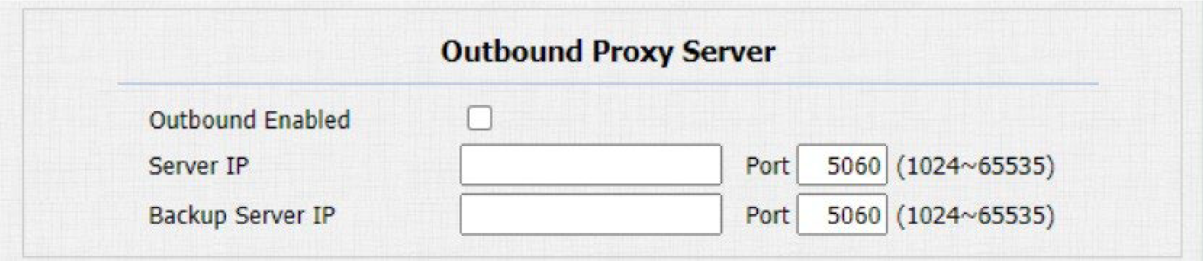
Setting	Description
Preferred SIP Server	Enter the primary SIP server IP address number or its URL.
Alternate SIP Server	Enter the backup SIP server IP address number or its URL.
Port	Set up the SIP server port for data transmission.
Registration Period	Set up the SIP account registration time span. 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)

9.4 - Data transmission type configuration

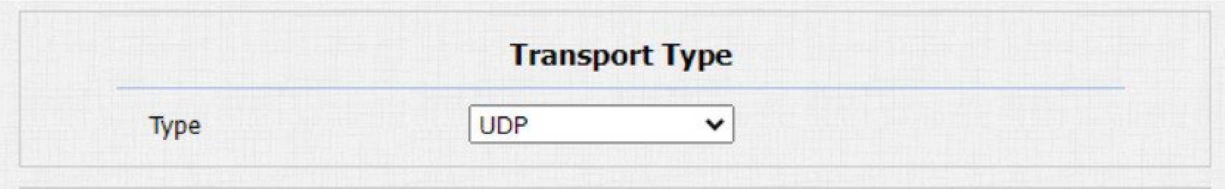
SIP messages can be transmitted in the following data transmission protocols:

- 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 A12 - MyBell IP 1-button Station - Data transmission type configuration

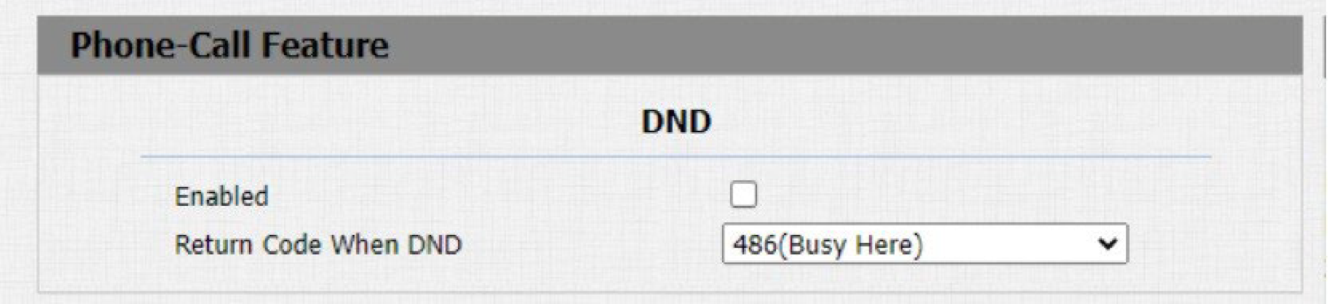
Setting	Description
UDP	Select **UDP** for unreliable but efficient transport layer protocol. UDP is the default transport protocol.
TCP	Select **TCP** for reliable but less-efficient transport layer protocol.
TLS	Select **TLS** for secure and reliable transport layer protocol.
DNS-SRV	Select **DNS-SRV** 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:

Phone > Call Feature



Phone-Call Feature

DND

Enabled □

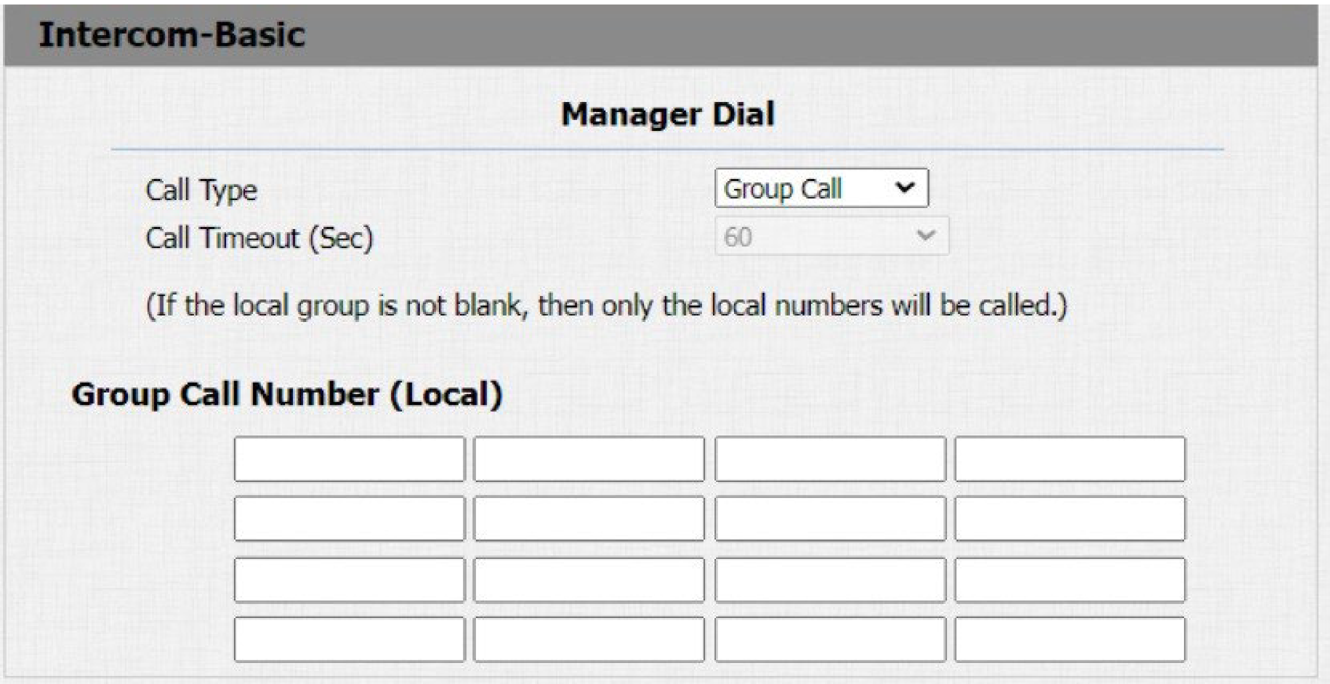
Return Code When DND: 486(Busy Here)

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. You can configure up to 10 numbers.

To configure the manager dial call by the web interface:

Intercom > Basic > Manager Dial



Intercom-Basic

Manager Dial

Call Type: Group Call

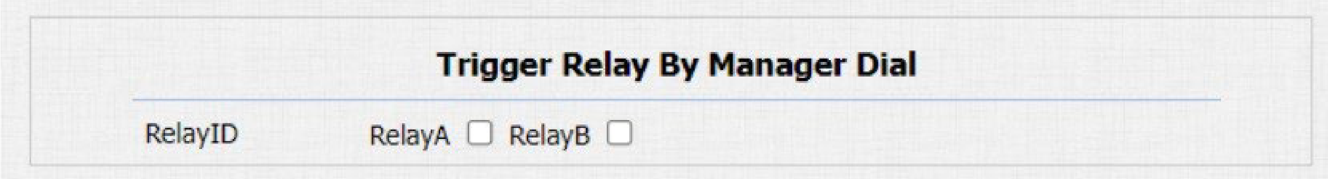
Call Timeout (Sec): 60

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

Group Call Number (Local)

Table A13 - MyBell IP 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 it's answered, the call 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.

After the manager dial is set up, on the same page you can set up relays to be triggered by the manager dial.



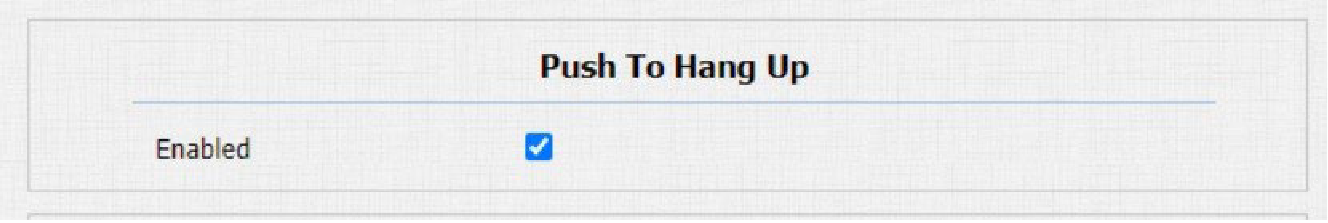
Trigger Relay By Manager Dial

RelayID: RelayA □ RelayB □

10.3 - Call hang up configuration

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

Intercom > Basic



Push To Hang Up

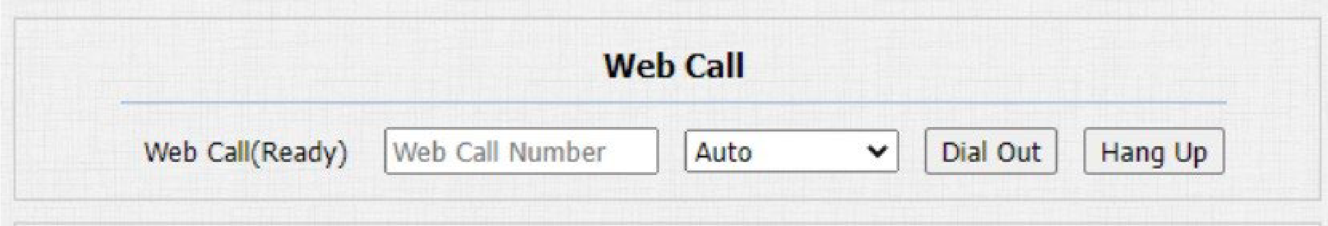
Enabled ☑

10.4 - Web call

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:

Intercom > Basic > 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

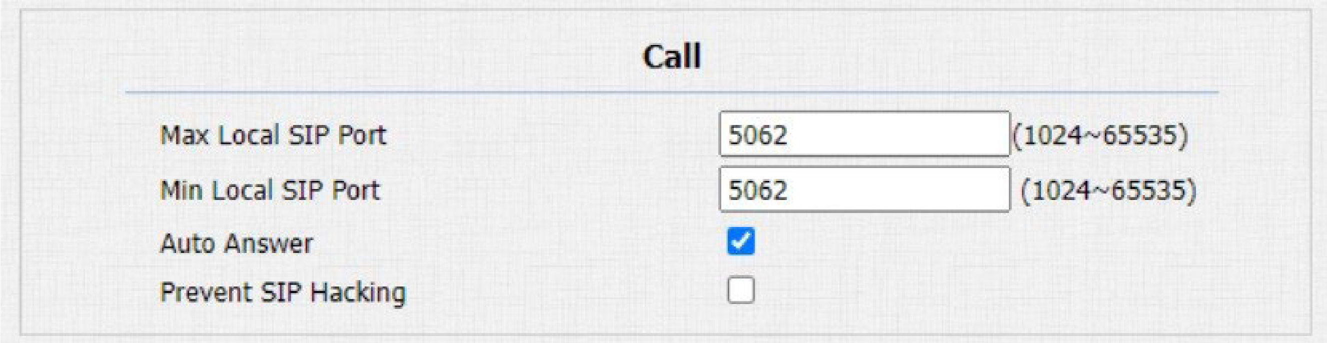
You can define the time of the door phone response for the incoming SIP/IP call automatically by setting up the time-related parameters. You can also define the mode in which the calls are answered (video or audio).

To enable the auto answer by the web interface:

Account > Advanced > Call

To configure the related parameters by the web interface:

Phone > Call Feature > Auto Answer



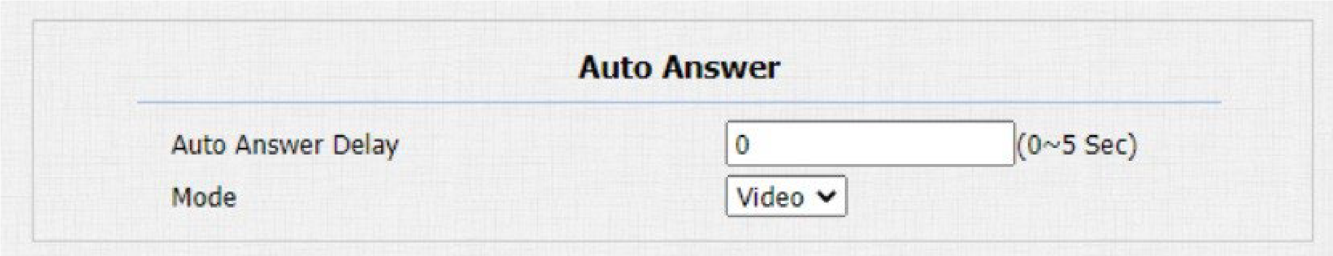
Call

Max Local SIP Port 5062 (1024~65535)

Min Local SIP Port 5062 (1024~65535)

Auto Answer ☑

Prevent SIP Hacking □



Auto Answer

Auto Answer Delay 0 (0~5 Sec)

Mode Video

Settings:

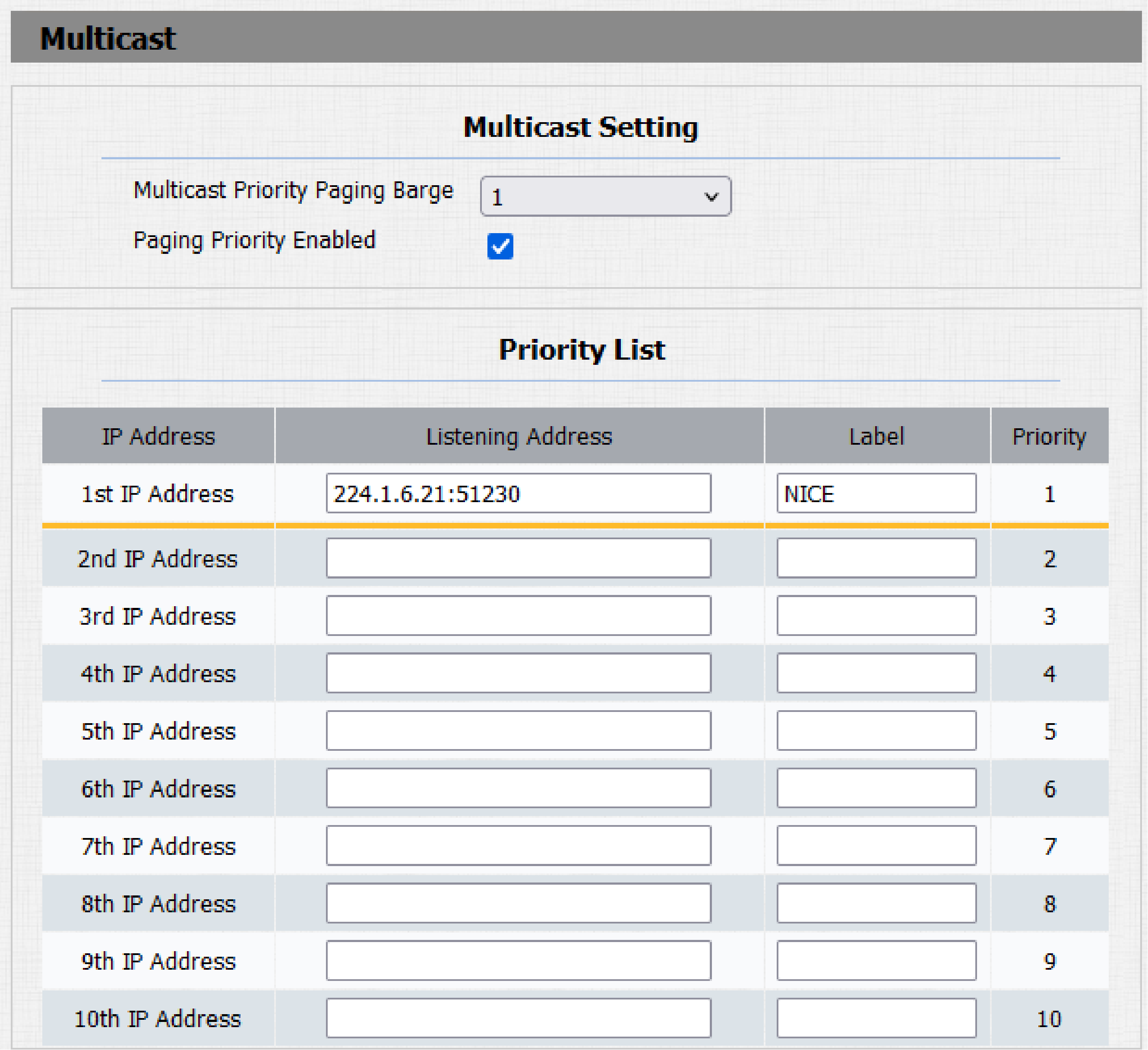
- **Auto Answer Delay:** set up the delay time (from 0 to 5 seconds) before the call is answered automatically. For example, if you set the delay time to 1 second, then the call is answered automatically in 1 second.
- **Mode:** set up the video or audio mode for answering the call automatically.

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:

Phone > 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 A14 - MyBell IP 1-button Station - Multicast configuration

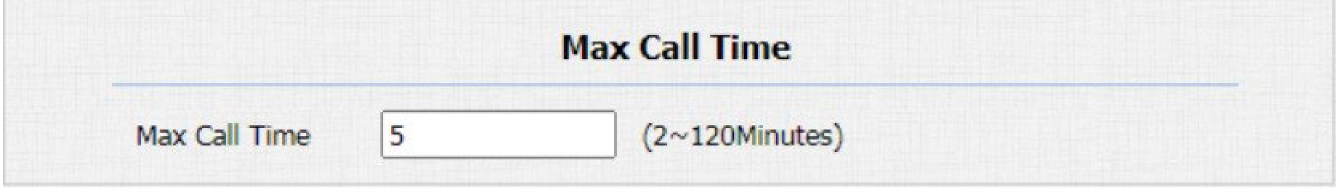
Setting	Description
Multicast Priority Paging Barge	Configure the amount of multicast calls with higher priority than an SIP call. If you disable Paging Priority by unticking the checkbox, the SIP call has higher priority than the multicast call.
Paging Priority Enabled	If enabled, multicast calls are 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 > Basic > Max Call Time



Max Call Time

Max Call Time: 5 (2~120Minutes)

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.

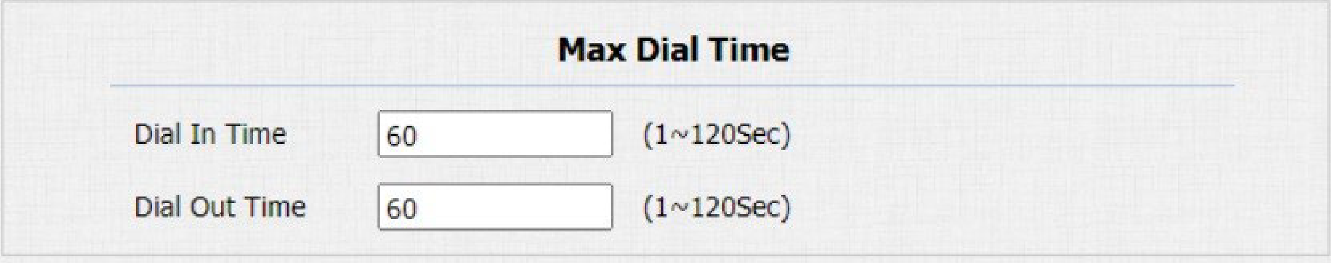
10.8 - Maximum dial duration configuration

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 > Basic > Max Dial Time



Max Dial Time

Dial In Time: 60 (1~120Sec)

Dial Out Time: 60 (1~120Sec)

Note

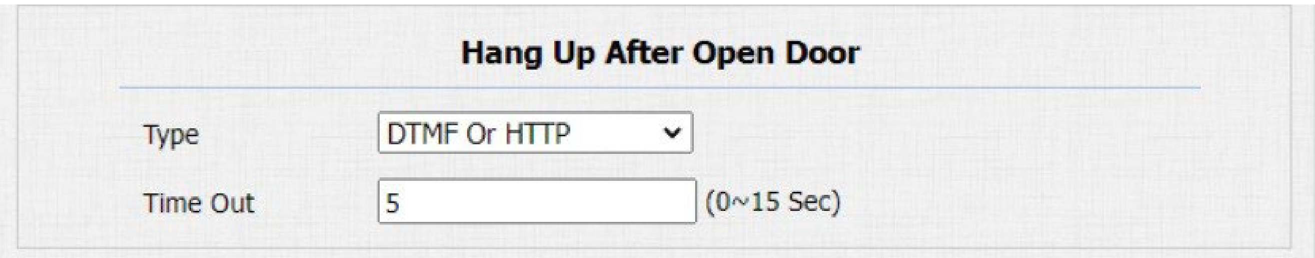
Maximum dial time for the device is related with maximum dial time for the SIP server. When using the SIP account to make a call, please pay attention to the maximum dial time for the SIP server. If it's shorter than the maximum dial time for the device, the shorter one applies.

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:

Intercom > Basic



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 call automatically ends within this set time after the door is opened.

11 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.

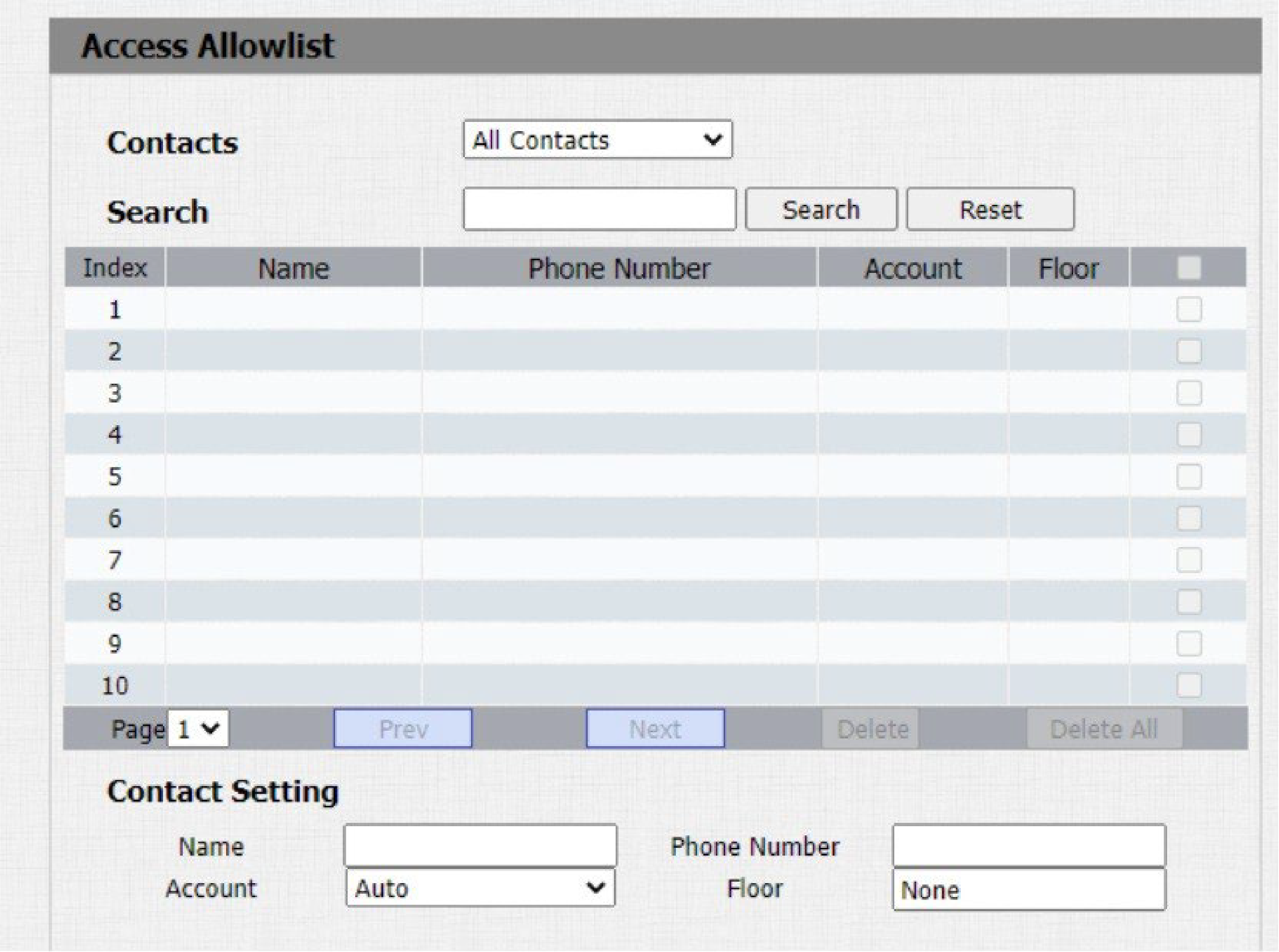
To configure the White List access feature by the web interface:

Contacts > Access Allowlist

11.1 - Managing contacts

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

Contacts > Access Allowlist



Access Allowlist

Contacts: All Contacts

Search: Search Reset

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

Page 1 Prev Next Delete Delete All

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.

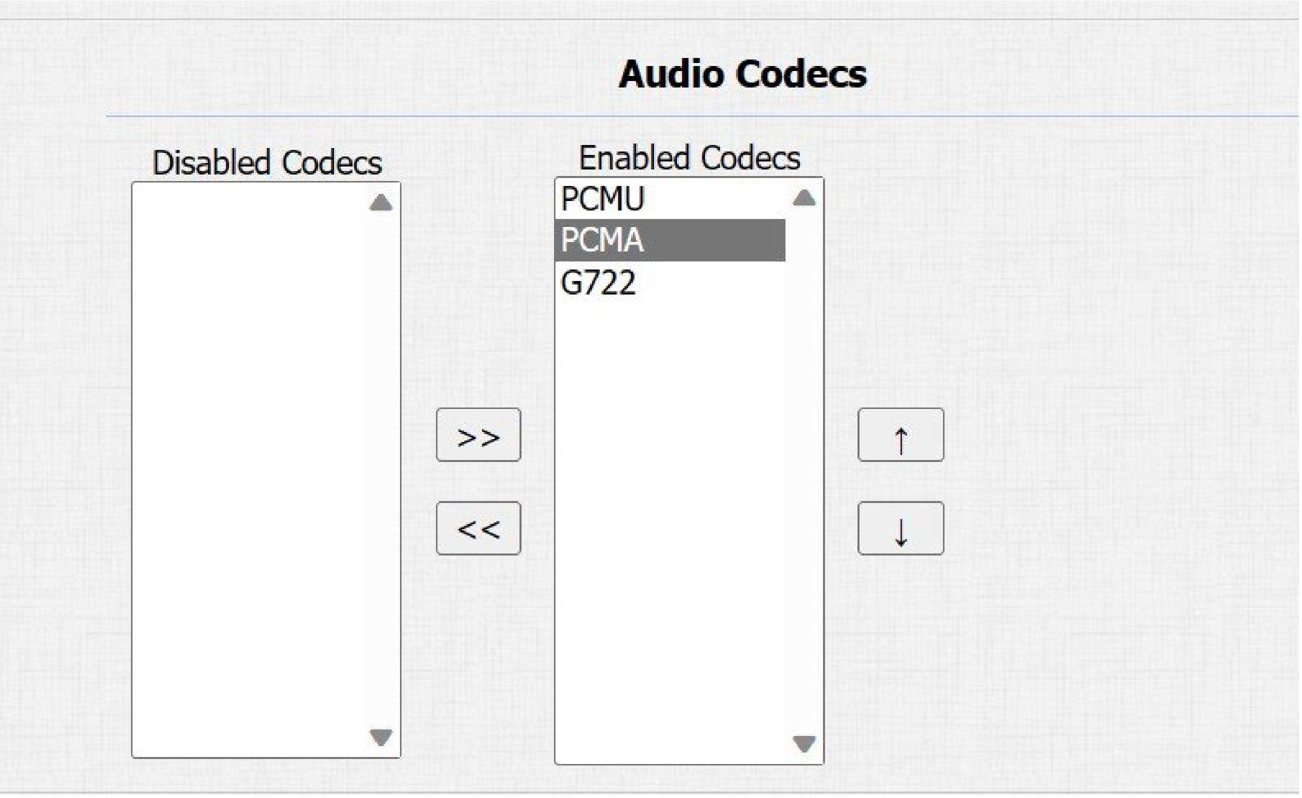
12 AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS

12.1 - Audio codec configuration

The door phone supports three 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



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 below:

Table A15 - MyBell IP 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

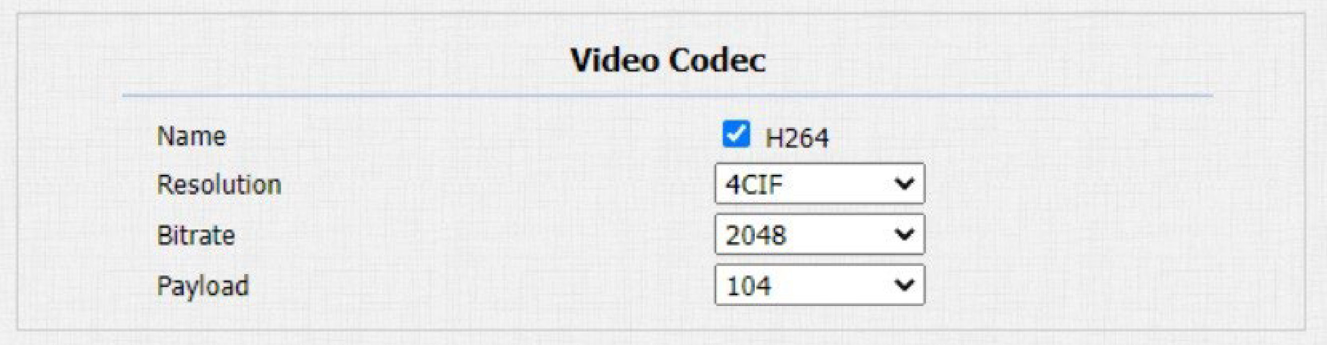
12.2 - Video codec configuration

You can choose the IP call video quality by selecting the proper codec resolution according to your network condition.

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

To configure the video codec by the web interface:

Account > Advanced



Video Codec

Name	☑ H264
Resolution	4CIF
Bitrate	2048
Payload	104

Table A16 - MyBell IP 1-button Station - Video codec configuration

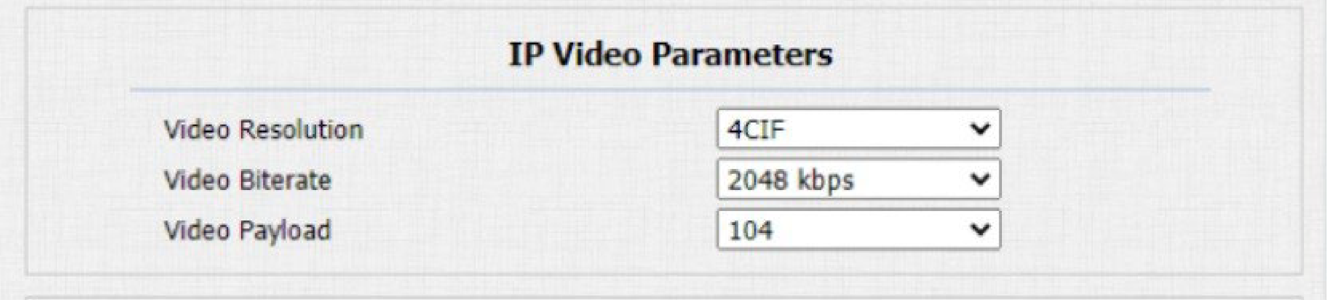
Setting	Description
Name	Check to select the H.264 video codec format for the door phone video stream. The default video codec is H.264.
Resolution	Select the codec resolution for the video quality from the following options: **CIF, VGA, 4CIF, 720P,** according to your network environment. The default 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 118) to set up the audio/video configuration file. The default payload is 104.

12.3 - 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:

Phone > Call Feature > IP Video Parameters



IP Video Parameters

Video Resolution: 4CIF

Video Biterate: 2048 kbps

Video Payload: 104

Table A17 - MyBell IP 1-button Station - Video codec configuration for IP direct calls

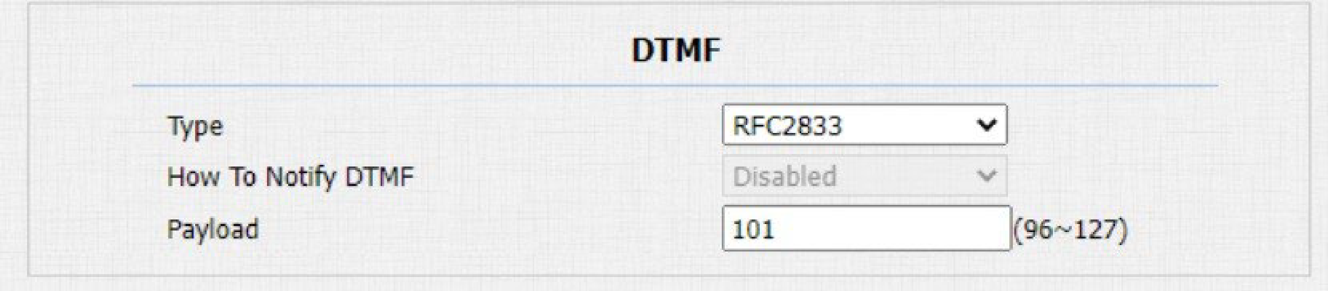
Setting	Description
Resolution	Select the codec resolution for the video quality from the following options: **CIF, VGA, 4CIF, 720P.** The default resolution is 4CIF.
Bitrate	Select the video stream bitrate form the following options: **64 kbps, 128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps,** according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

12.4 - 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

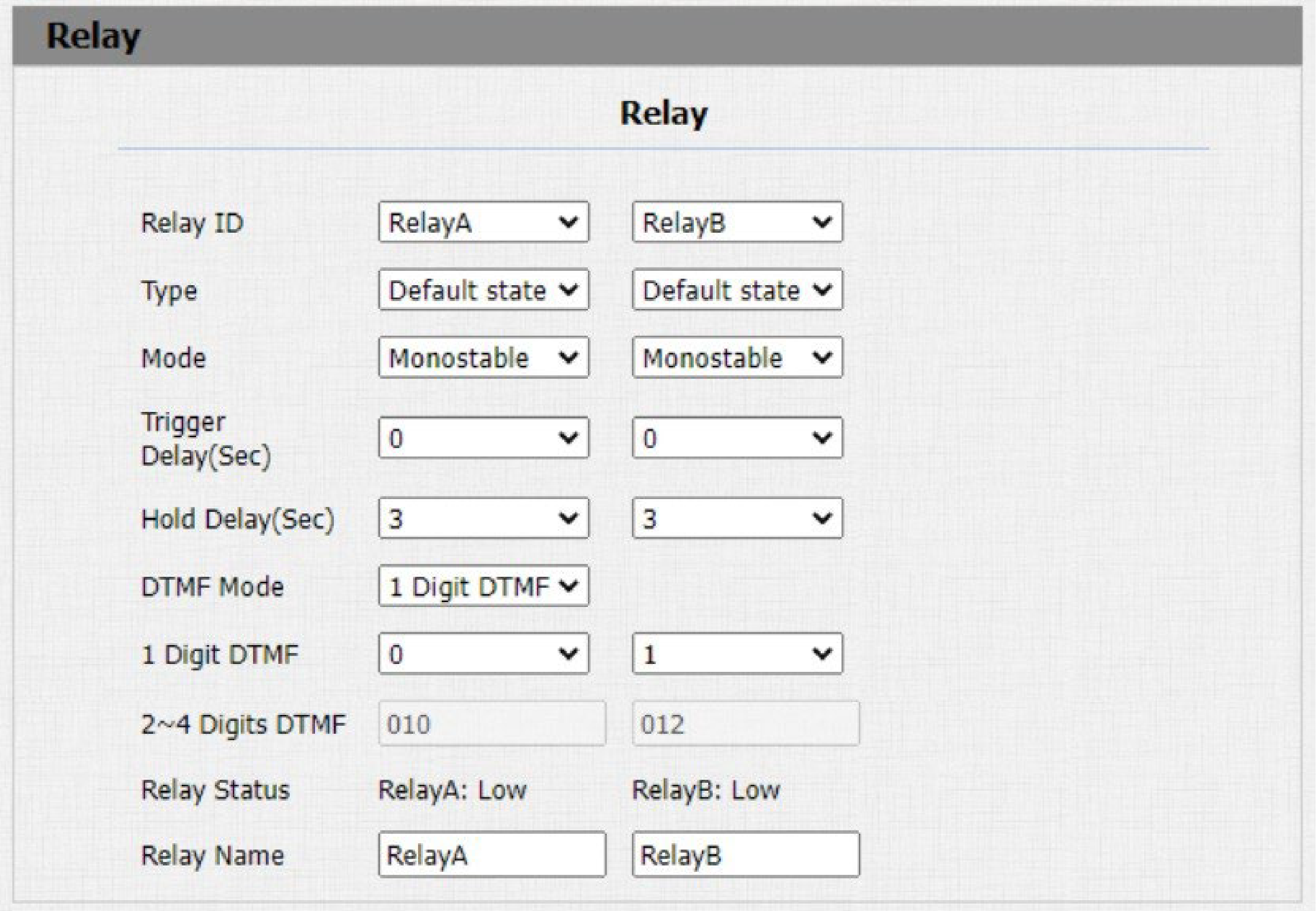
Payload: 101 (96~127)

Table A18 - MyBell IP 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.

13.1 - Relay switch configuration

To configure the relay switches and DTMF for the door access by the web interface:
Intercom > 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 A19 - MyBell IP 1-button Station - Relay switch configuration

Setting	Description
Relay ID	You can set up to three relay switches in total for the door access control.
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

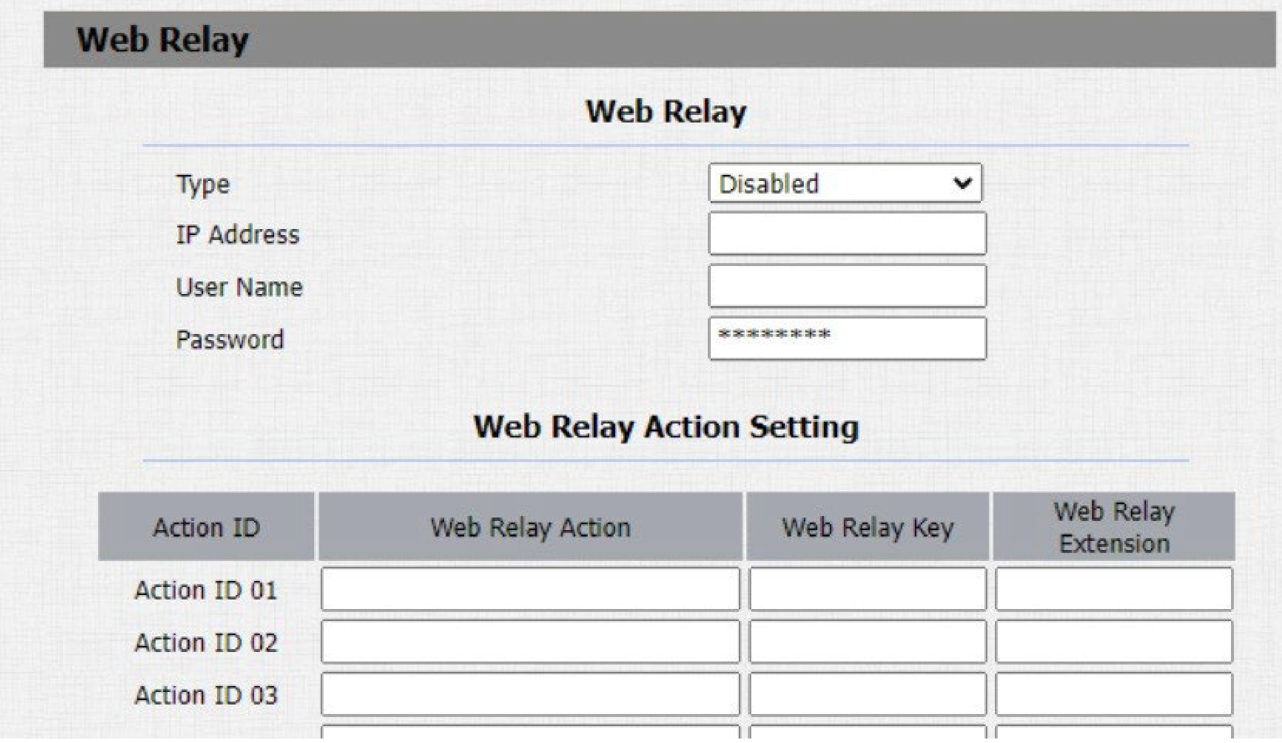
You can control the door access using the network-based web relay on the device and by the device web interface.

Web relay needs to be configured by the web interface.

To configure the web relay by the web interface:

Phone > 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 A20 - MyBell IP 1-button Station - Web relay configuration	
Setting	**Description**
Type	Select from the three options: • **Web relay** – enable the web relay. • **Disable** – 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 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

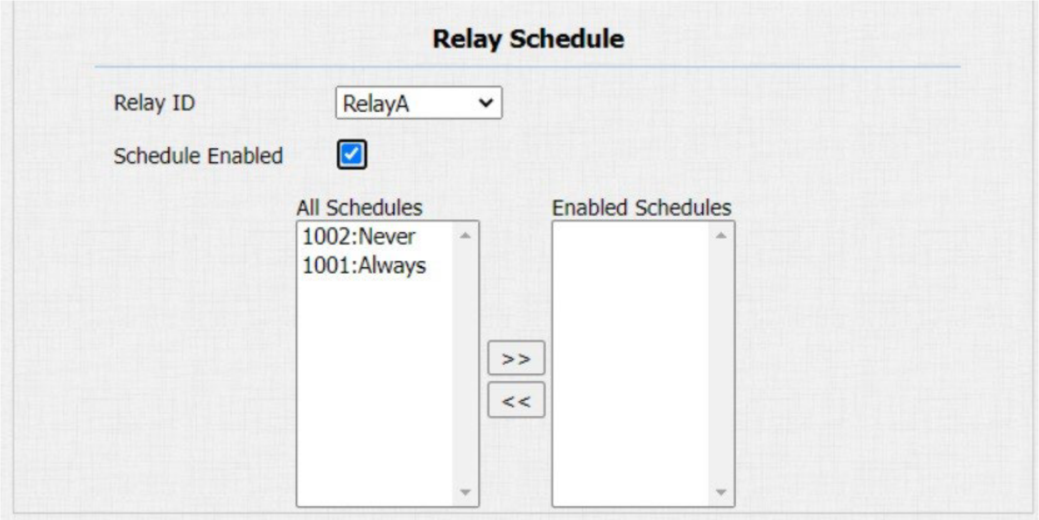
Configure and make a schedule for the user-based door access using RF card, Private PIN, and Facial recognition.

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:

Intercom > Relay > Relay Schedule



Relay Schedule

Relay ID: RelayA

Schedule Enabled ☑

All Schedules		Enabled Schedules
1002:Never 1001:Always	>> <<	

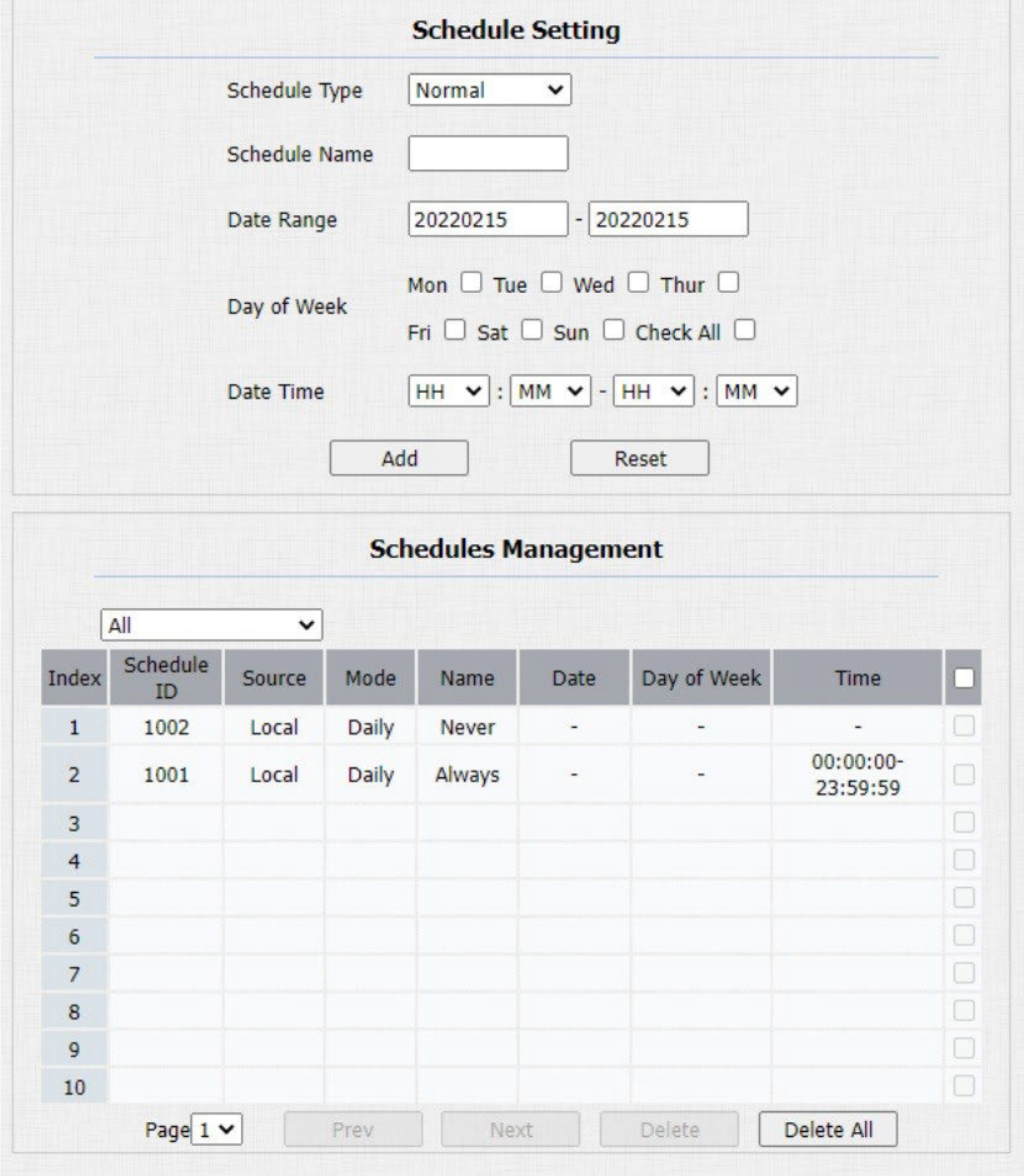
Setting:

- **Relay ID:** choose the relay to be set up.

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:

Intercom > 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

Add Reset

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								□

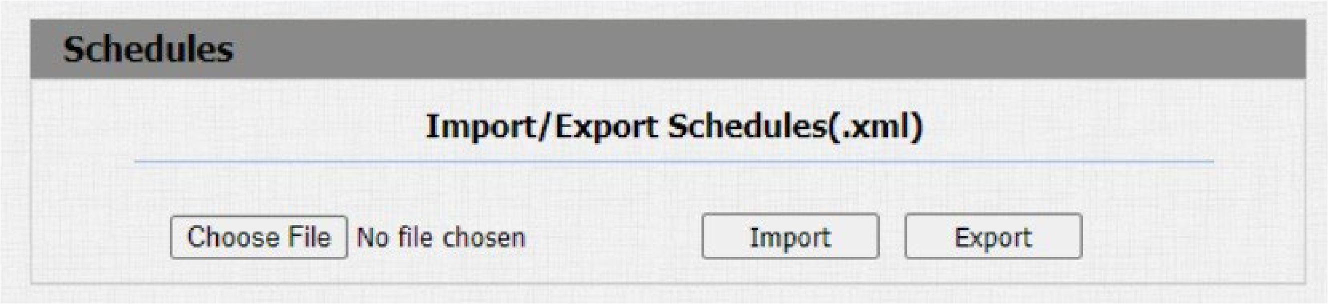
Page 1 Prev Next Delete Delete All

Settings:

- **Schedule Type:** choose from the three types: **Daily**, **Weekly**, and **Normal**. The default type is **Daily**.
- **Date Range:** set the corresponding date. This configuration is only displayed when the **Normal** type is selected.

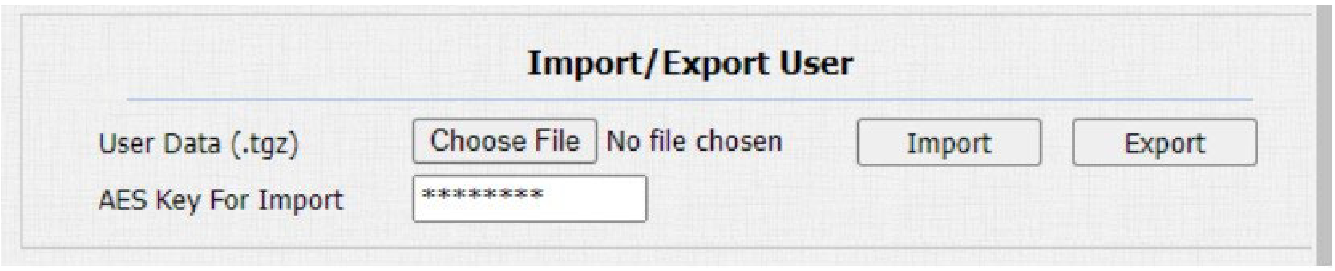
13.3.3 - Import and export door access schedule

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:
Intercom > Schedules > Import/Export Schedule(.xml)



13.4 - Import and export user

You can import or export the user in batch.
To import or export the user by the web interface:
Intercom > User



Setting:

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

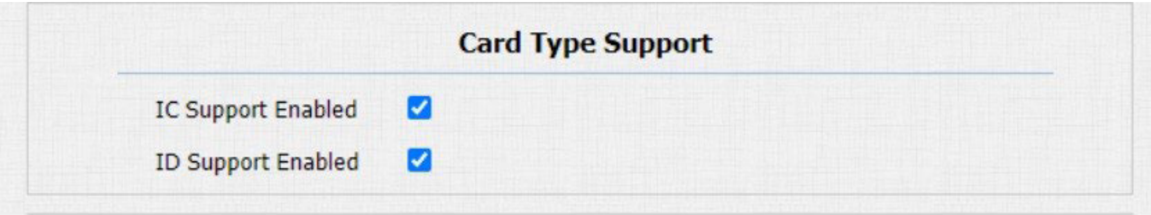
14 DOOR UNLOCK CONFIGURATION

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/ID card control configuration

To configure the IC/ID card control by the web interface:

Intercom > Card Setting > Card Type Support



Card Type Support

IC Support Enabled ☑

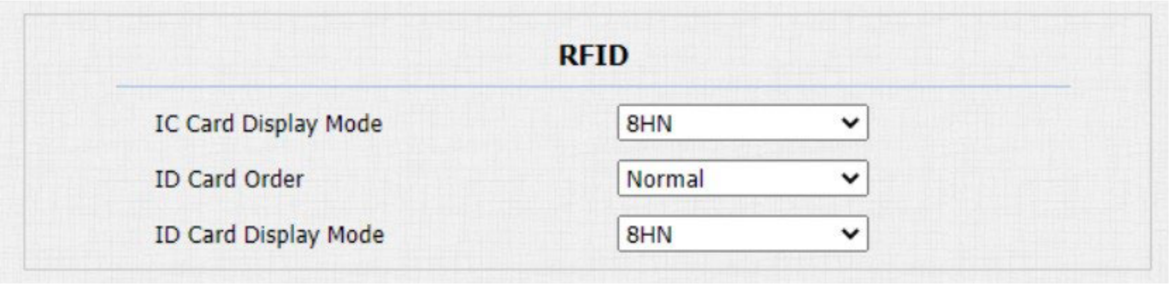
ID Support Enabled ☑

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

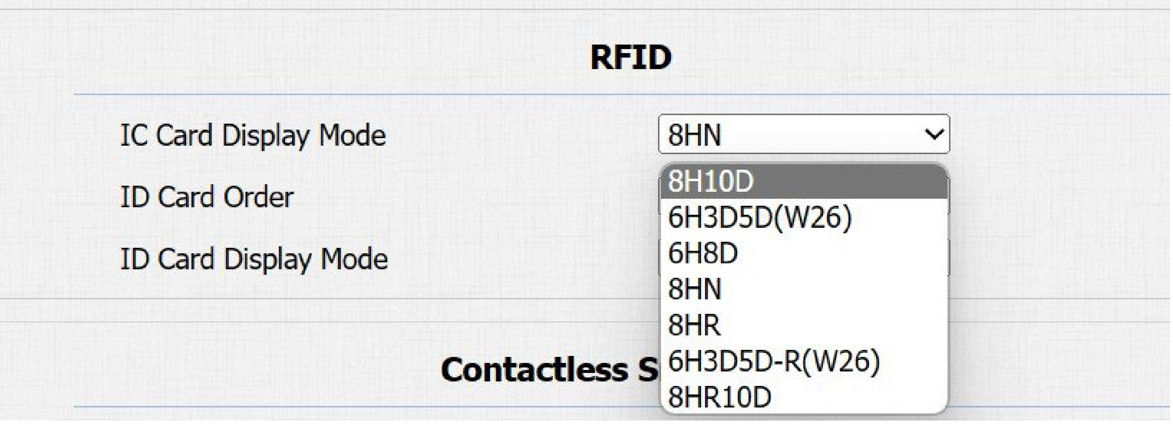


RFID

IC Card Display Mode: 8HN

ID Card Order: Normal

ID Card Display Mode: 8HN



RFID

IC Card Display Mode: 8HN

ID Card Order

ID Card Display Mode

Table A21 - MyBell IP 1-button Station - Access card format configuration

Setting	Description
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**.
ID Card Order	Select **Normal** or **Reversed** display order of the ID cards.
ID Card Display Mode	Select the card code format of the ID 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:

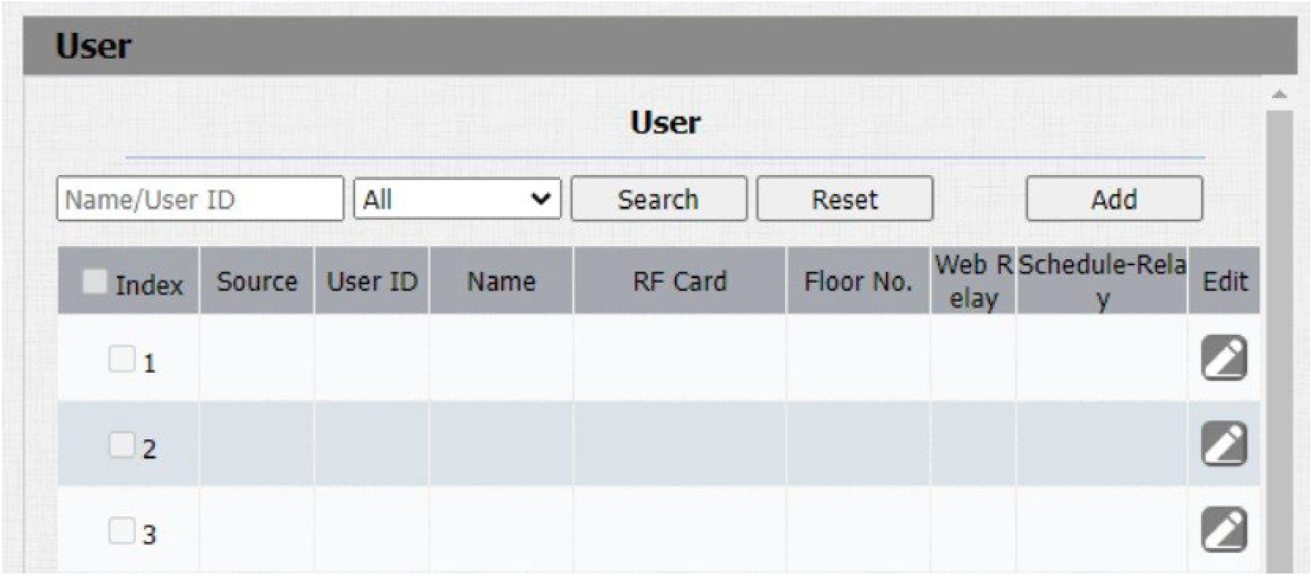
Intercom > Card Setting

14.4 - RF card configuration

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:

Intercom > User

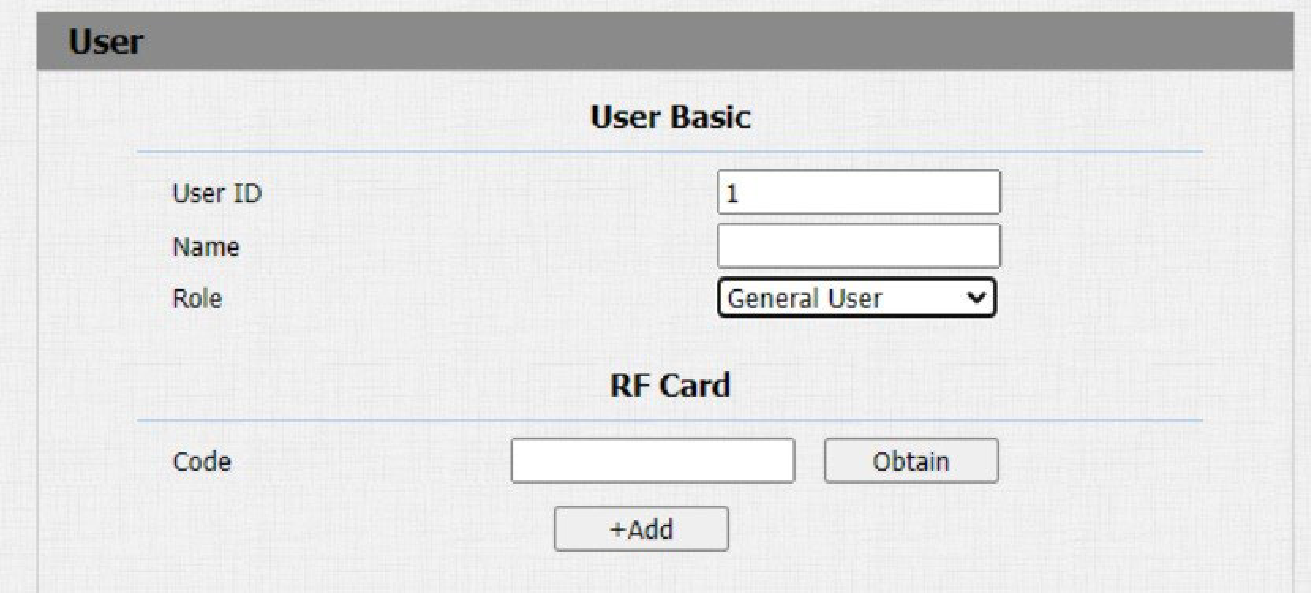


User

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

User Basic

User ID: 1

Name:

Role: General User

RF Card

Code: Obtain

+Add

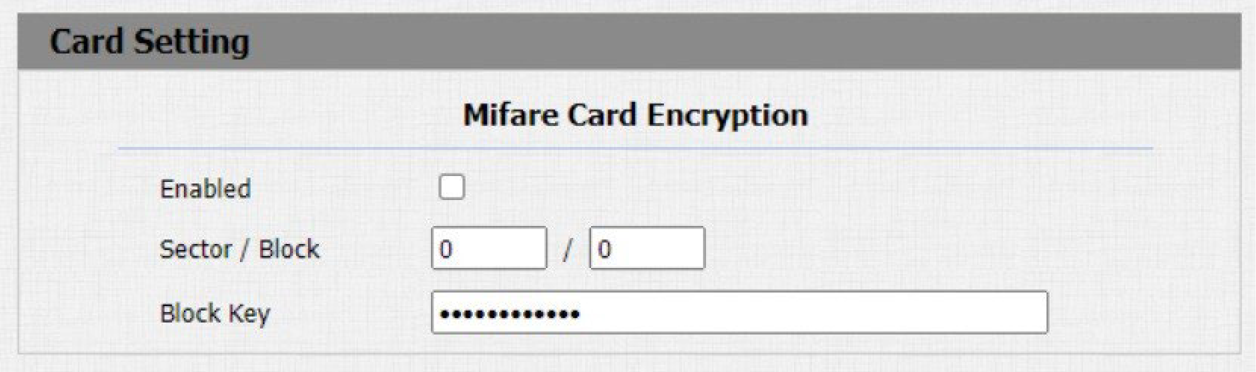
Table A22 - MyBell IP 1-button Station - RF card configuration	
Setting	**Description**
User ID	The **User ID** can be maximum 11 digits long and can't be reused for other users. The **User ID** can be generated automatically or manually.
Role	Select **General Users** for the residents and **Administrator** for the administrator.
Code	Tap the card on the reader area and click **Obtain**.

Note

- RF cards with 13.56 MHz and 125 KHz frequencies can be used for door access on the door phone.

14.5 - Mifare and Defare card encryption

Mifare and Defire cards can be encrypted for greater security.
To encrypt the Mifare or Defare card by the web interface:
Intercom > Card setting > Mifare/Defire Card Encryption



Card Setting

Mifare Card Encryption

Enabled: □

Sector / Block: 0 / 0

Block Key: ••••••••••••

Settings:

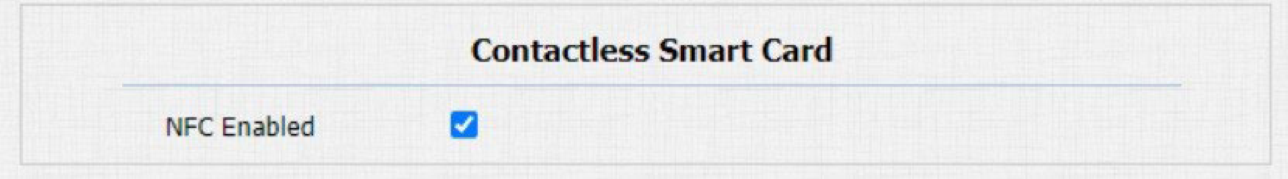
- **Sector/Block:** enter the sector and block that you want the card number to be written into for the Mifare/Defire card. For example, you can write the card number into sector 3 and block 3 in the card.
- **Block Key:** enter the block password for access.

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. The NFC function needs to be enabled before you use the NFC for contactless door access.

To configure the NFC card by the web interface:

Intercom > Card Setting



Contactless Smart Card

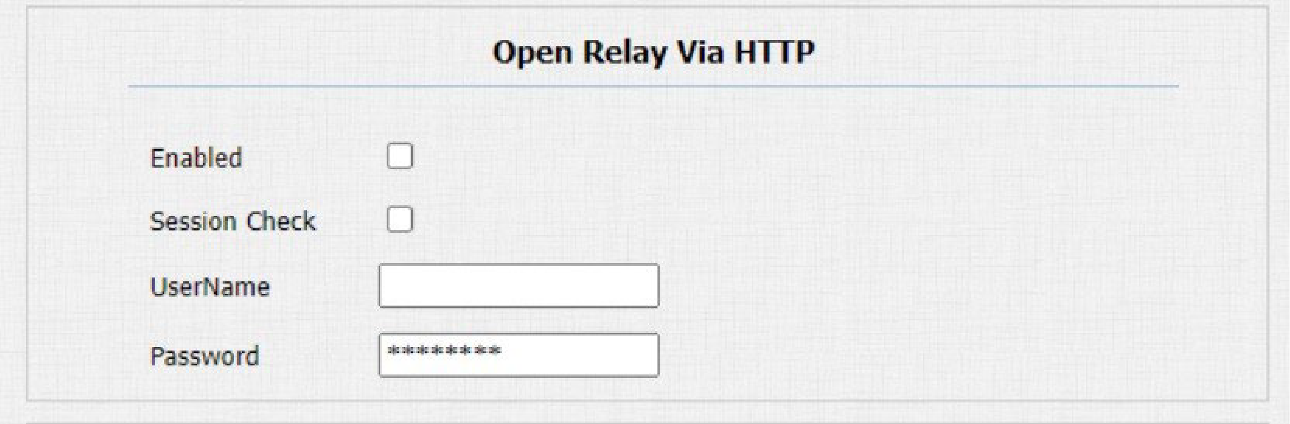
NFC Enabled ☑

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:

Intercom > Relay > Open Relay Via HTTP



Open Relay Via HTTP

Enabled □

Session Check □

UserName

Password *********

Table A23 - MyBell IP 1-button Station - Open relay configuration through HTTP for door access	
Setting	**Description**
Session Check	Enable to protect data transmission security.
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

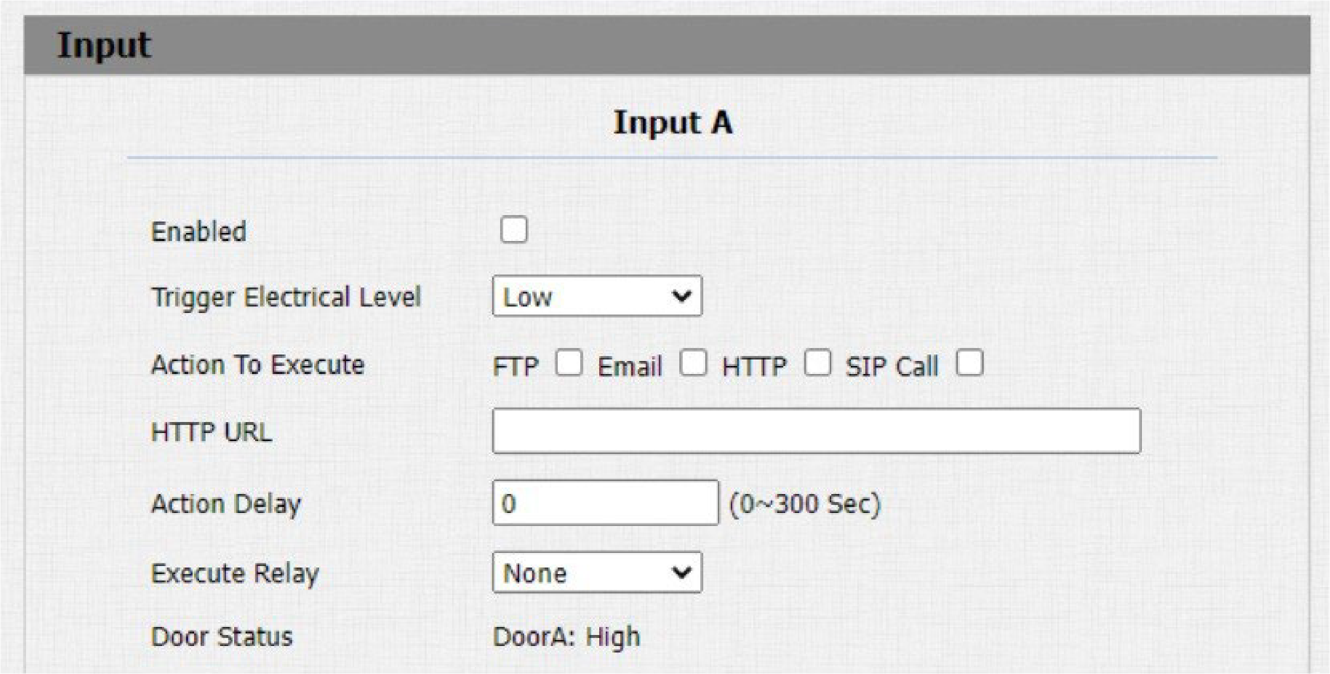
- **DoorNum** in the HTTP command above refers to the number of the relay to be triggered for the door access, in this case, relay 1.

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:

Intercom > Input



Input

Input A

Enabled □

Trigger Electrical Level: Low

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

HTTP URL:

Action Delay: 0 (0~300 Sec)

Execute Relay: None

Door Status: DoorA: High

Table A24 - MyBell IP 1-button Station - Exit button for door unlock configuration

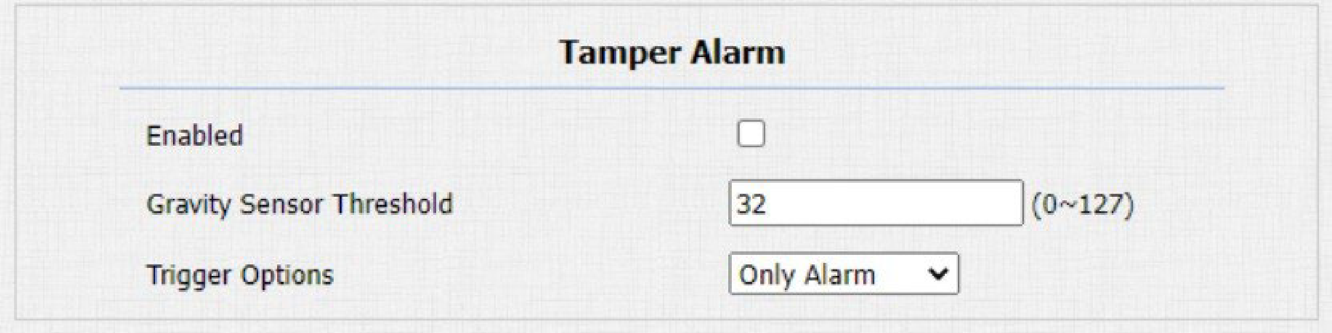
Setting	Description
Trigger Electrical Level	Select the **Trigger Electrical Level** option from **High** and **Low**, according to the operation on the exit button.
Action To Execute	Select the method to carry out the action from the following options: **FTP**, **Email, HTTP**, **TFTP**.
HTTP URL	If 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.
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:

- **Gravity Sensor Threshold:** set the threshold for the gravity sensory sensitivity. The lower the value, the higher the sensitivity. The default gravity sensor value is **32**.
- **Trigger Options:** select the options to be activated when the gravity sensor is triggered.

15.2 - Client certificate configuration

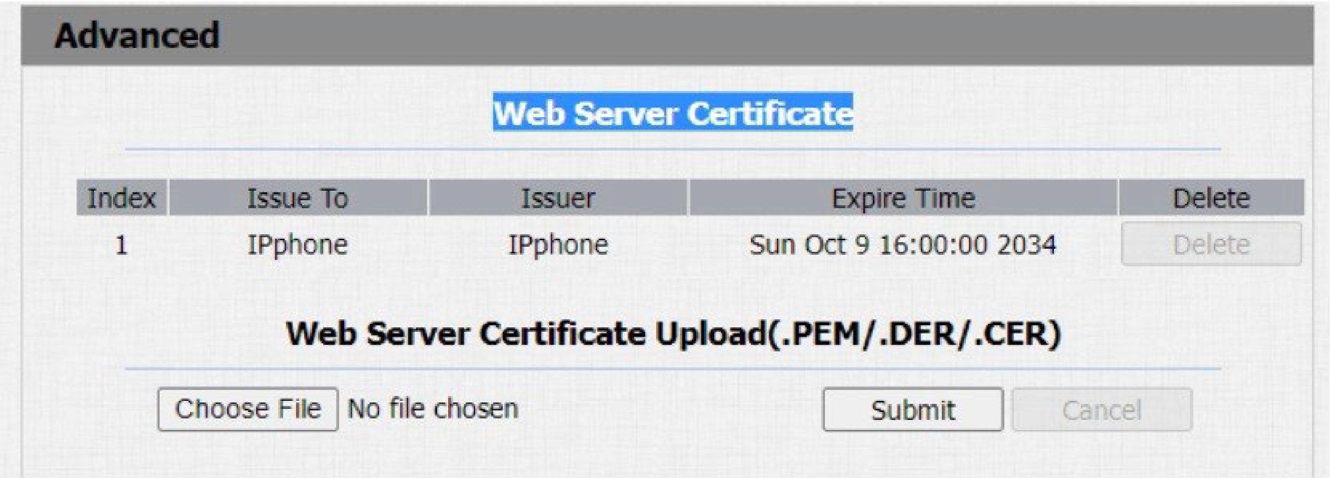
Certificates can ensure communication integrity and privacy when deploying the door phones. When the user needs to establish the SSL protocol, it is necessary to upload corresponding certificates for verification.

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)

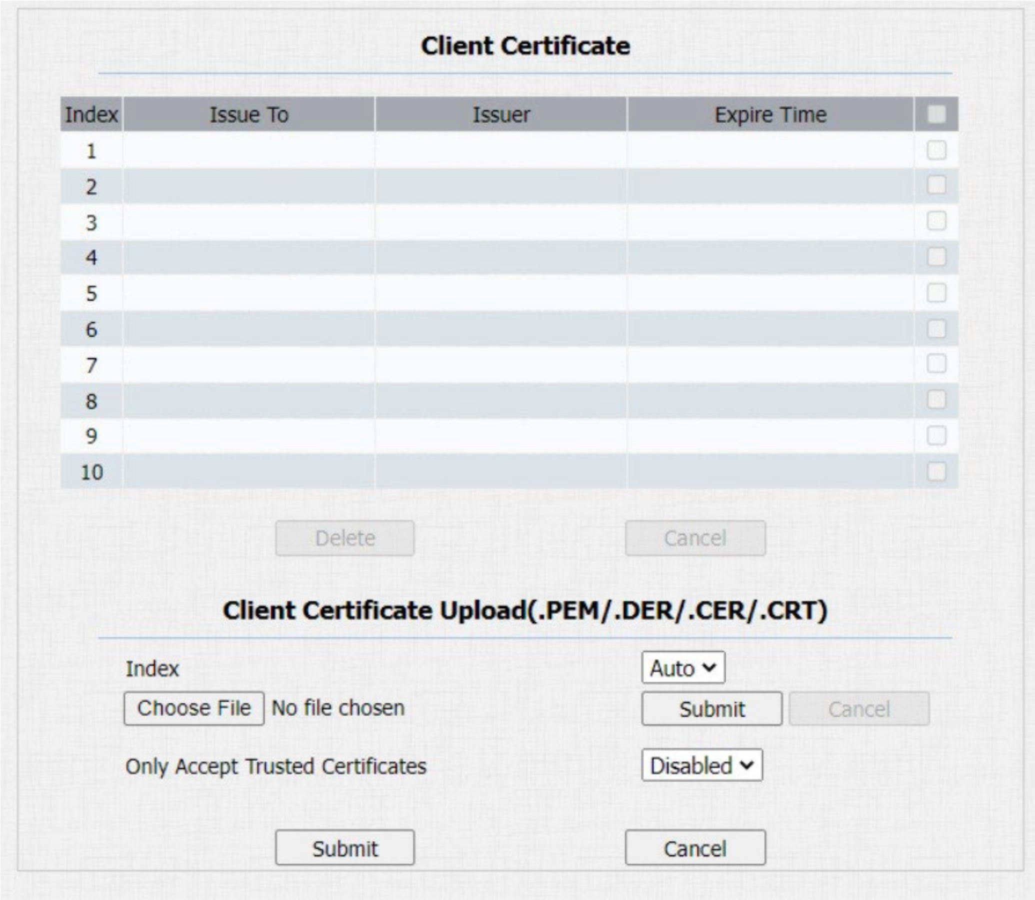
No file chosen

15.2.2 - Client certificate

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

No file chosen

Only Accept Trusted Certificates: Disabled

Table A25 - MyBell IP 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

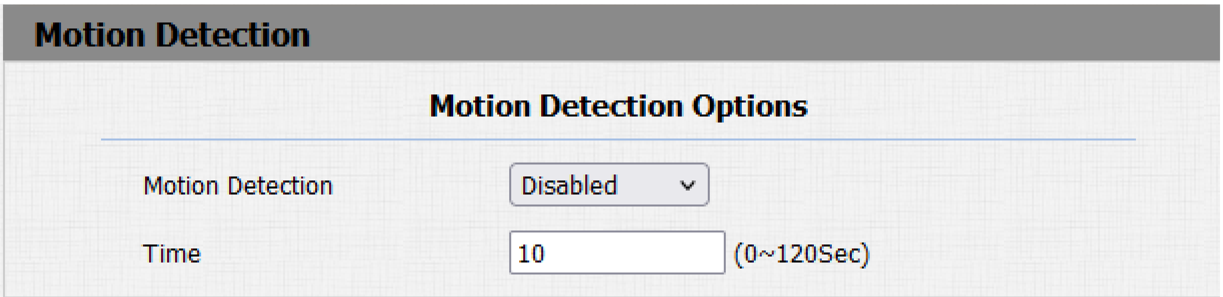
Motion detection is commonly used for unattended surveillance video and alarms. The CPU compares images collected by the camera at different frame rates using a specific algorithm. If there is a change in the picture, such as someone walking by or the lens moving, the calculation exceeds the threshold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

15.3.1 - Motion detection configuration

You can configure the time interval, motion detection sensitivity and notification type by the web interface, when the motion detection action is triggered.

To turn on and configure the motion detection and set up the motion detection interval by the web interface:

Intercom > Motion Detection

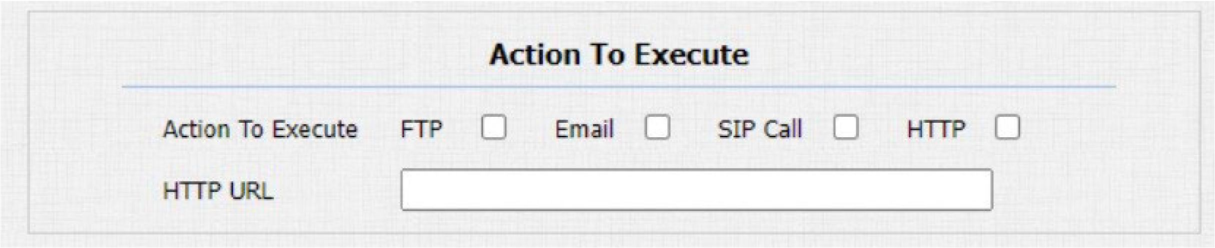


Motion Detection

Motion Detection Options

Motion Detection: Disabled

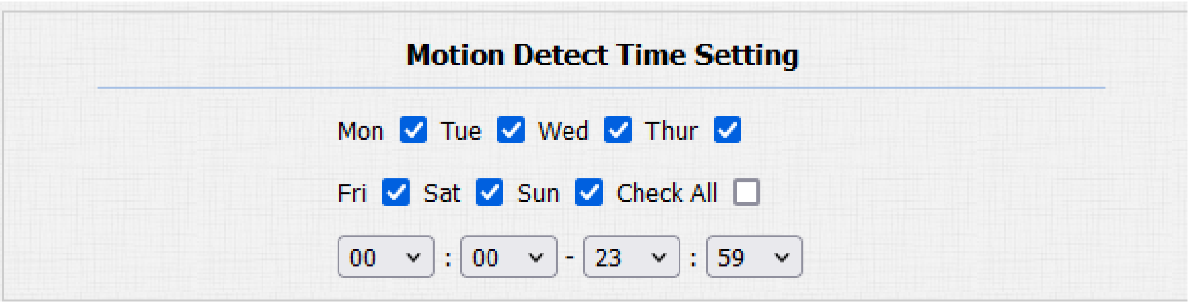
Time: 10 (0~120Sec)



Action To Execute

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

HTTP URL:



Motion Detect Time Setting

Mon ☑ Tue ☑ Wed ☑ Thur ☑

Fri ☑ Sat ☑ Sun ☑ Check All □

00 : 00 - 23 : 59

Setting:

- **Timing 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**.

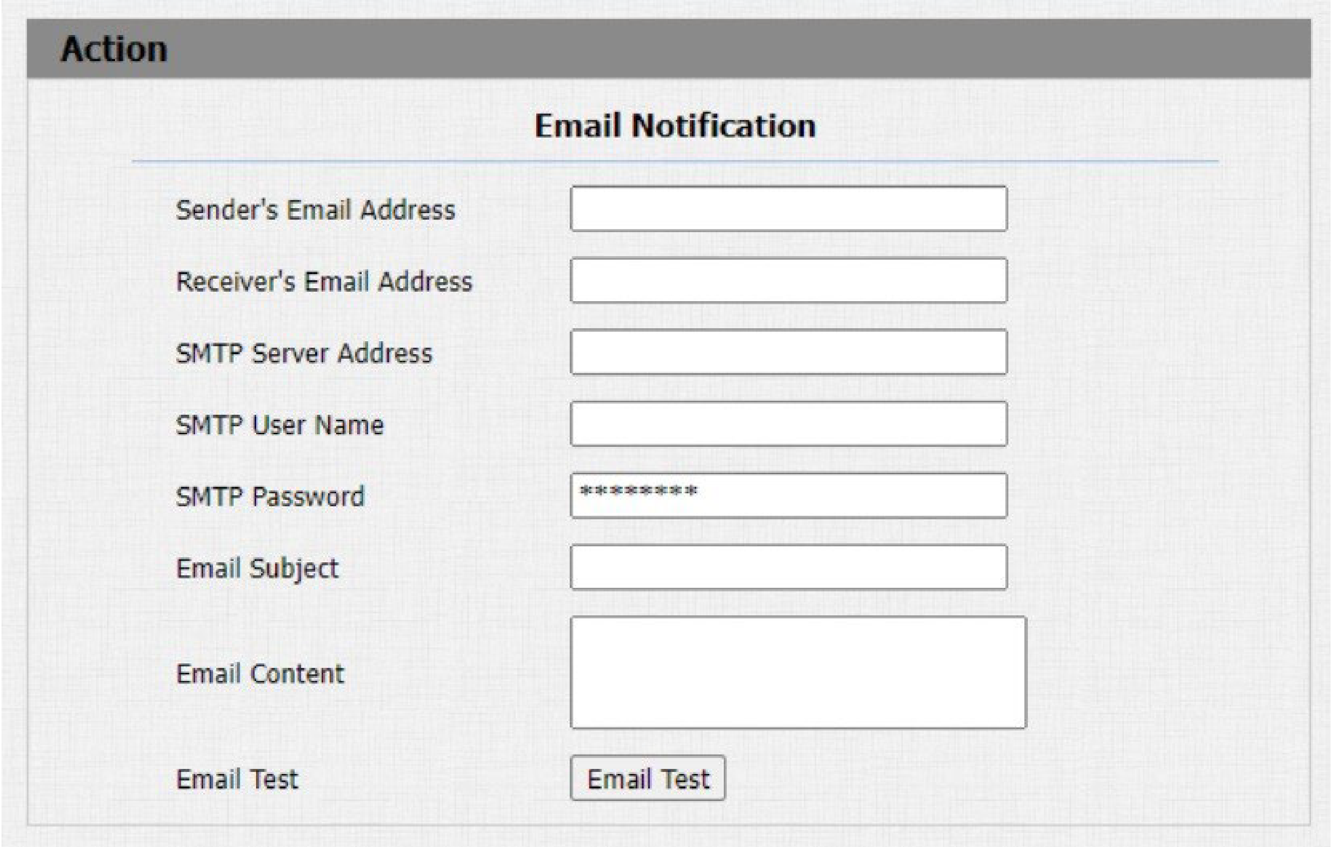
15.4 - Security notification configuration

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:

Intercom > 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

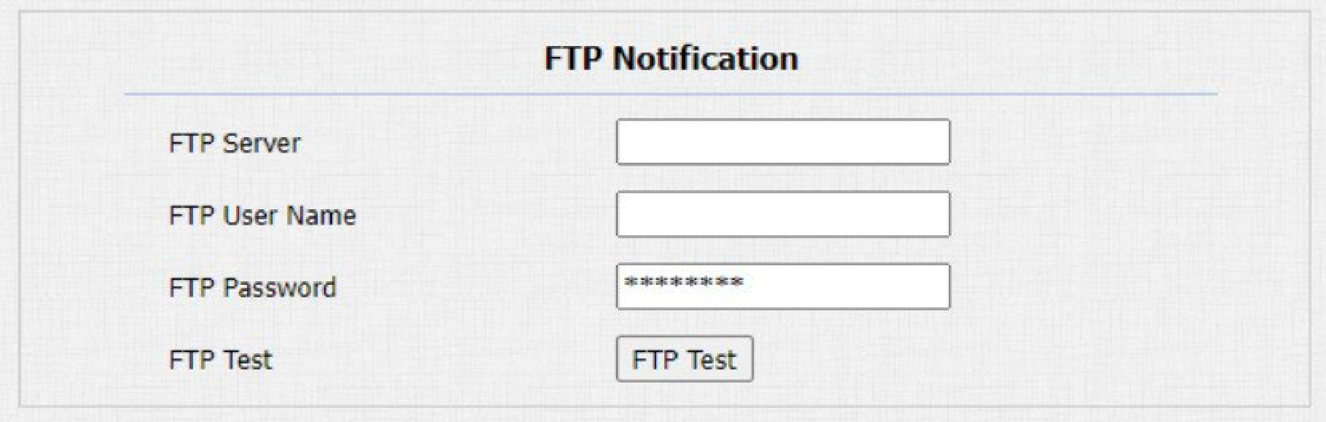
Email Test: Email Test

Table A26 - MyBell IP 1-button Station - Email notification configuration	
Setting	**Description**
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:

Intercom > Action > FTP Notification



FTP Notification

FTP Server

FTP User Name

FTP Password ********

FTP Test

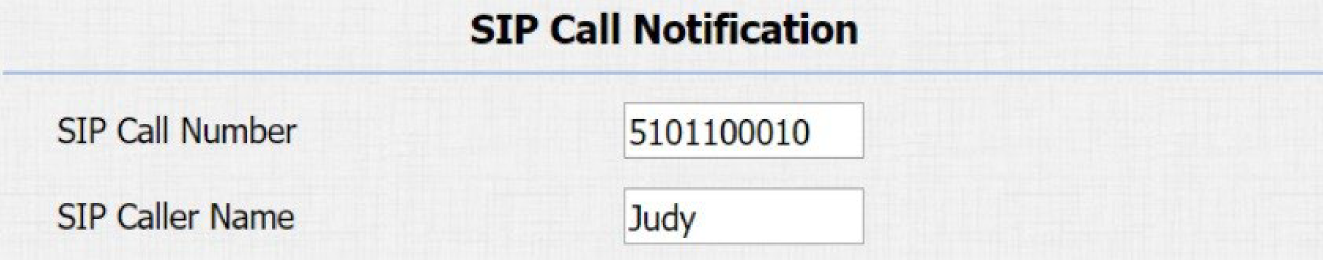
Settings:

- **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

To configure the SIP call notifications by the web interface:

Intercom > Action > SIP Call Notification



SIP Call Notification

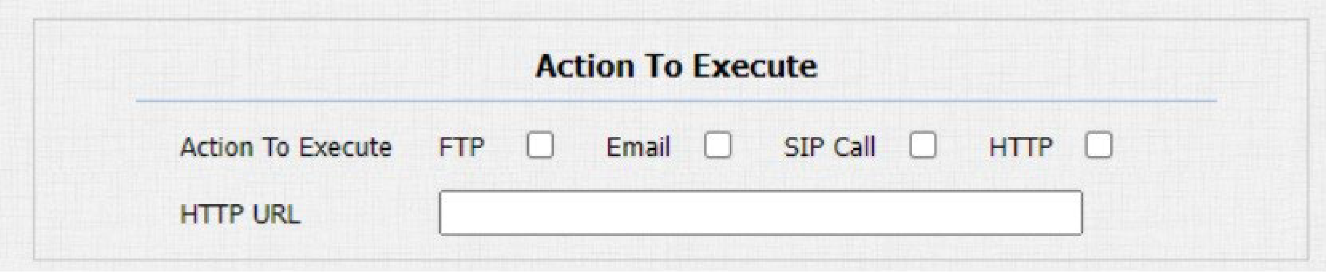
SIP Call Number 5101100010

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.
The URL format is: **http://http server IP address/any information**.
To configure the HTTP URL notification by the web interface:

Intercom > Motion > Action to Execute



Action To Execute

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

HTTP URL

Setting:

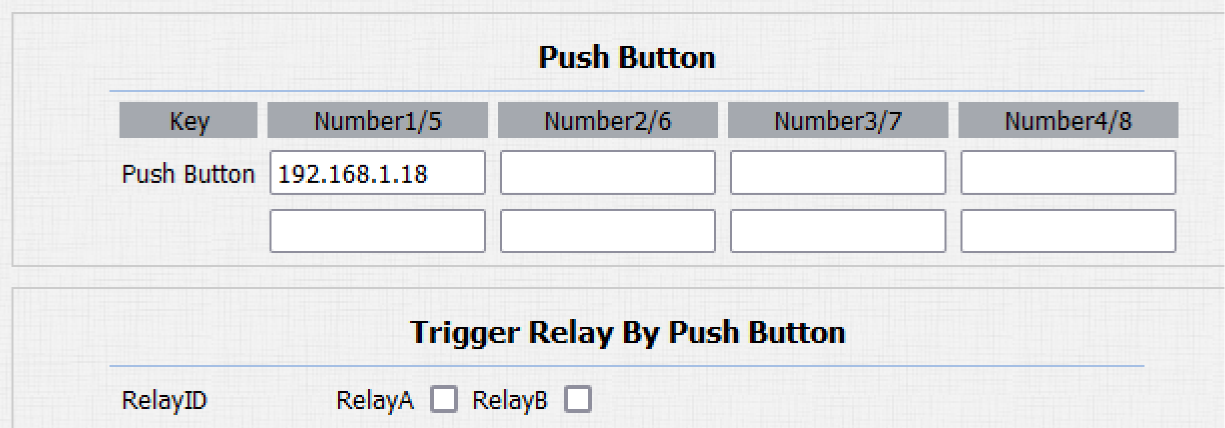
- **HTTP URL:** if you choose the HTTP mode, enter the URL in the following format: **http://http server IP address/any information**.

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

Key	Number1/5	Number2/6	Number3/7	Number4/8
Push Button	192.168.1.18			

Trigger Relay By Push Button

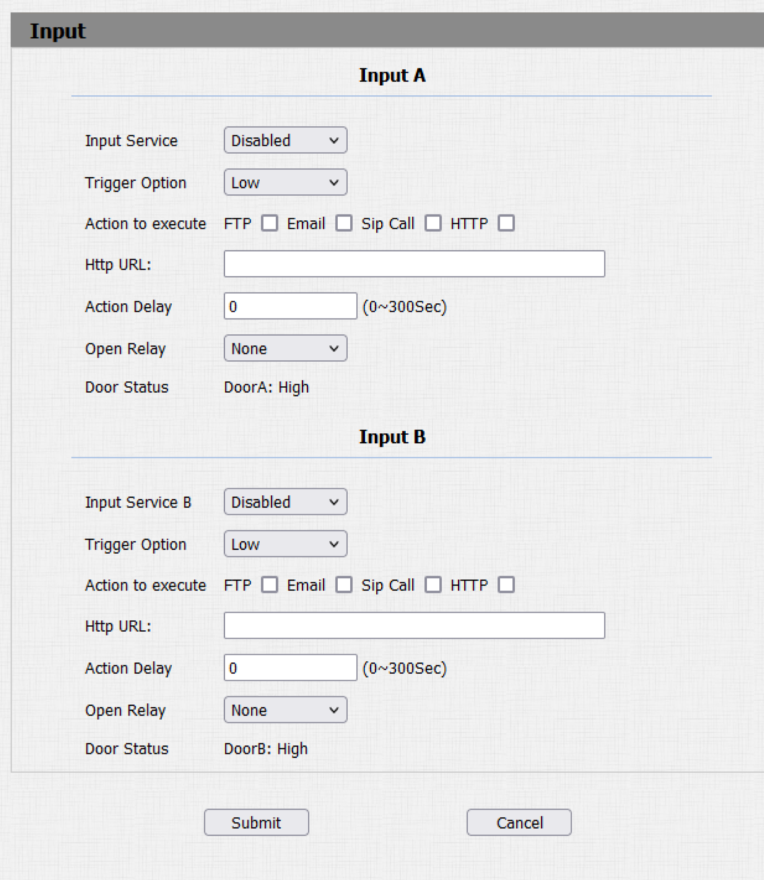
RelayID RelayA □ RelayB □

15.5.2 - Input action configuration

Working input interface can trigger an action.

To configure the input action by the web interface:

Intercom > Input



Input

Input A

Input Service: Disabled

Trigger Option: Low

Action to execute: FTP □ Email □ Sip Call □ HTTP □

Http URL:

Action Delay: 0 (0~300Sec)

Open Relay: None

Door Status: DoorA: High

Input B

Input Service B: Disabled

Trigger Option: Low

Action to execute: FTP □ Email □ Sip Call □ HTTP □

Http URL:

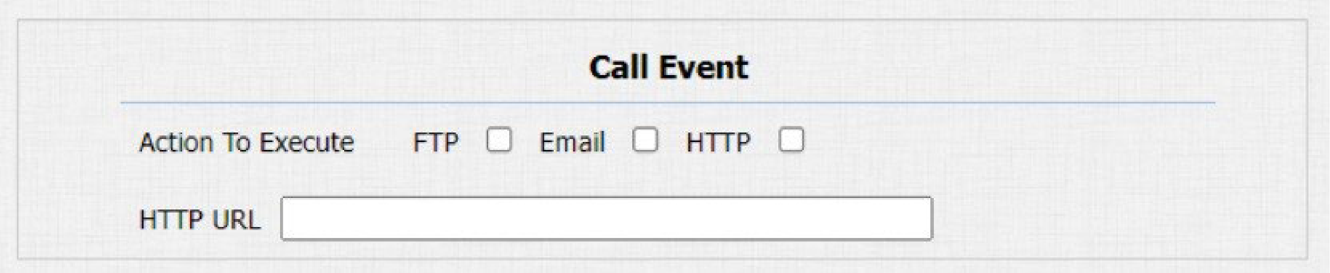
Action Delay: 0 (0~300Sec)

Open Relay: None

Door Status: DoorB: High

To configure notifications of the call events (such as call receiving, answering) by the web interface:

Intercom > Basic > Call Event



Call Event

Action To Execute: FTP □ Email □ HTTP □

HTTP URL:

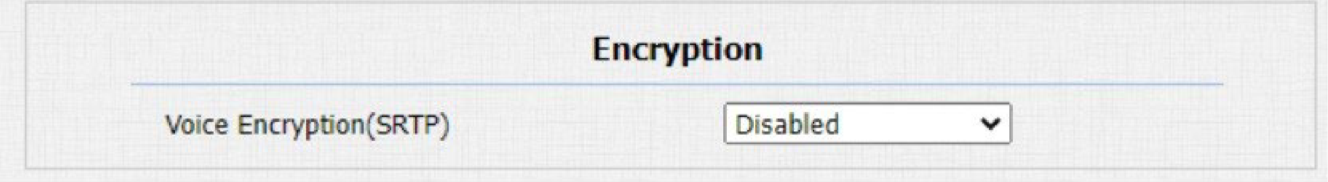
15.6 - Voice encryption

The encryption function provides greater security for the intercom call. The indoor monitor supports three modes of voice encryption: **SRTP (Compulsory), SRTP (Optional), ZRTP (Optional).**

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.

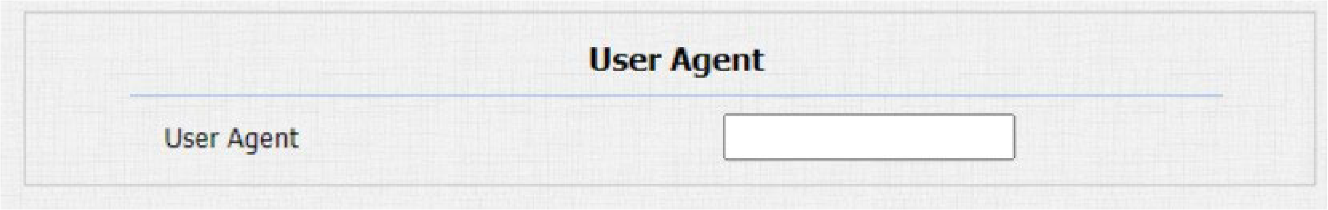
15.7 - User agent

User agent is used for the identification purpose during the analysis on the SIP data packet.

If the **User Agent** is set to a specific value, users can see the information from PCAP. If the **User Agent** is blank, by default users can see the company name, model number and firmware version from PCAP.

To configure the user agent by the web interface:

Account > Advanced > User Agent



User Agent

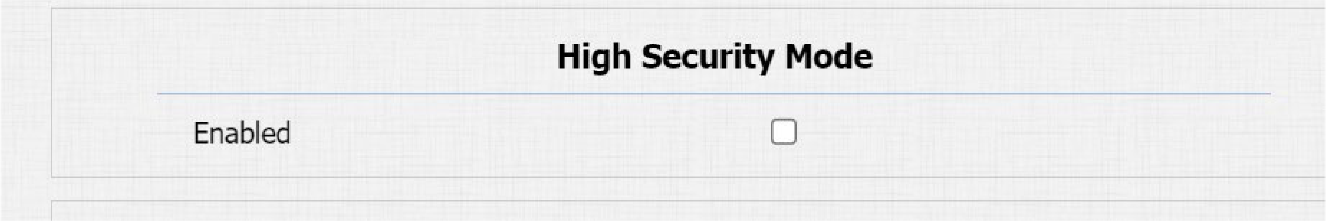
User Agent

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.

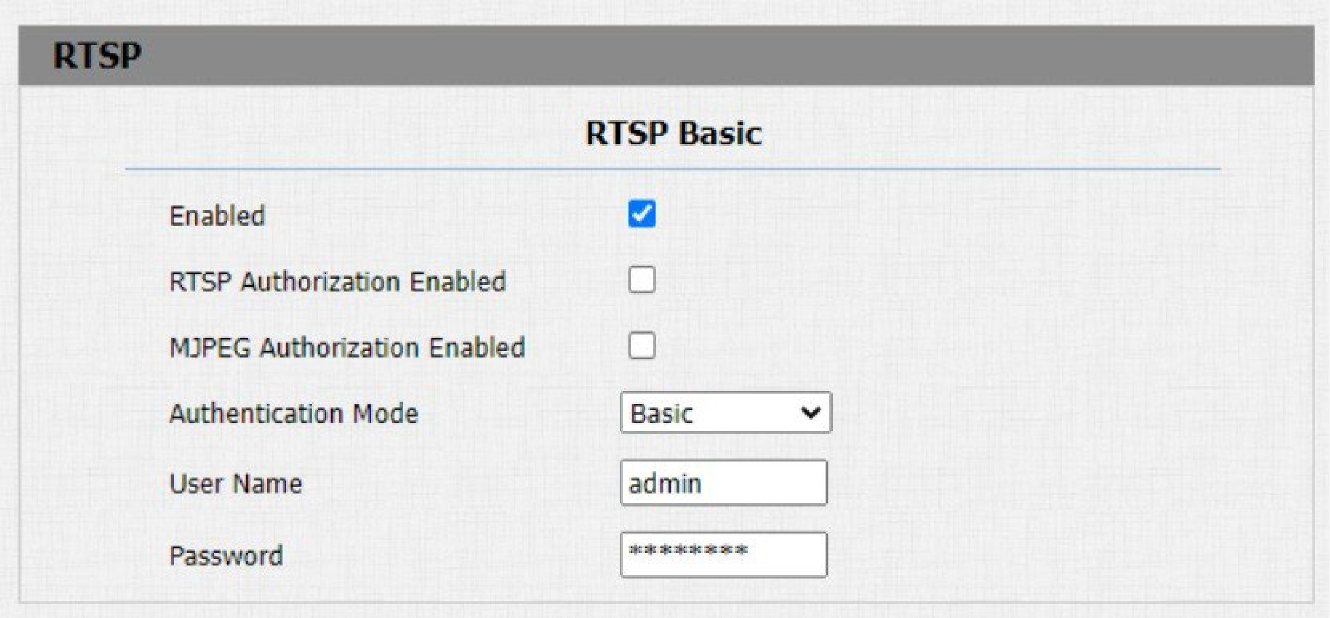
16.1 - RTSP stream monitoring

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

To configure the RTSP basic by the web interface:

Intercom > RTSP > RTSP Basic



RTSP

RTSP Basic

Enabled ☑

RTSP Authorization Enabled □

MJPEG Authorization Enabled □

Authentication Mode: Basic

User Name: admin

Password: ********

Settings:

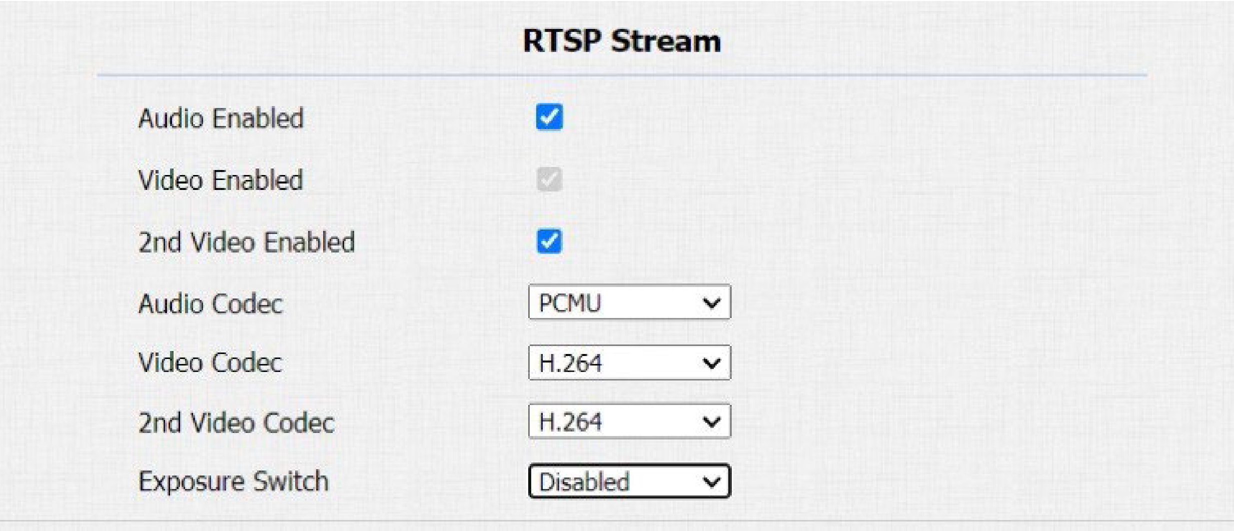
- **RTSP Authorization Enabled:** if enabled, you need to enter **RTSP Authentication Mode**, **RTSP User Name** and **RTSP Password** for authorization on the intercom device such as indoor monitor.
- **RTSP Authentication Mode:** select RTSP authentication mode from: **Basic** and **Digest**. The default 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:

Intercom > RTSP > RTSP stream



RTSP Stream

Audio Enabled ☑

Video Enabled ☑

2nd Video Enabled ☑

Audio Codec: PCMU

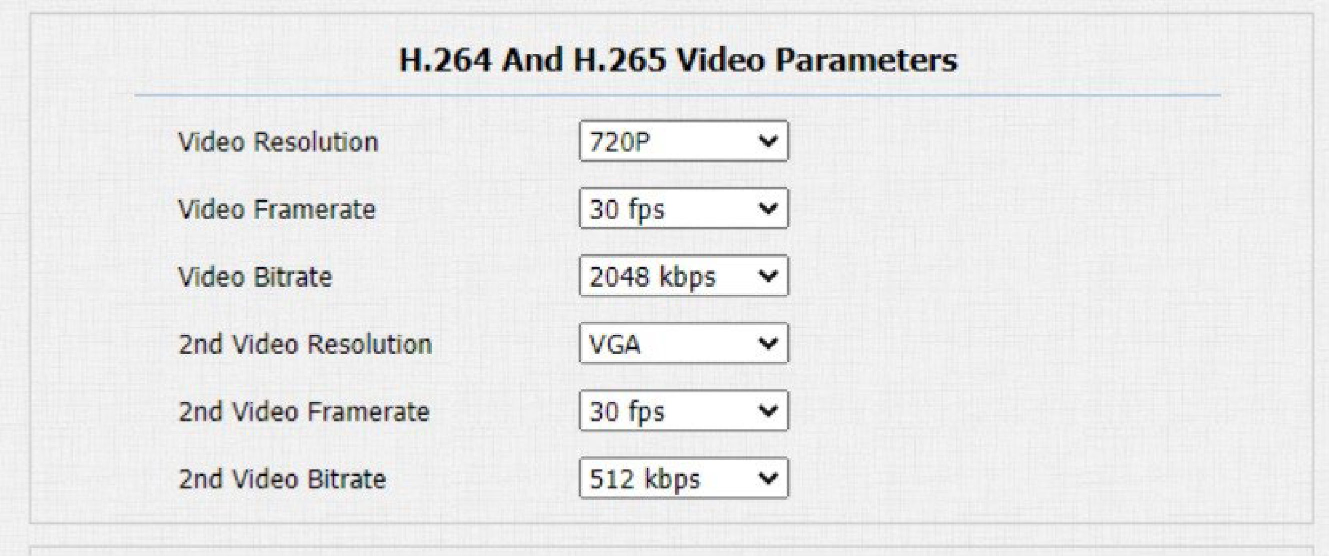
Video Codec: H.264

2nd Video Codec: H.264

Exposure Switch: Disabled

Table A27 - MyBell IP 1-button Station - RTSP stream configuration

Setting	Description
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.
Exposure Switch	Enable this function to optimize video quality under exposure.



H.264 And H.265 Video Parameters

Video Resolution: 720P

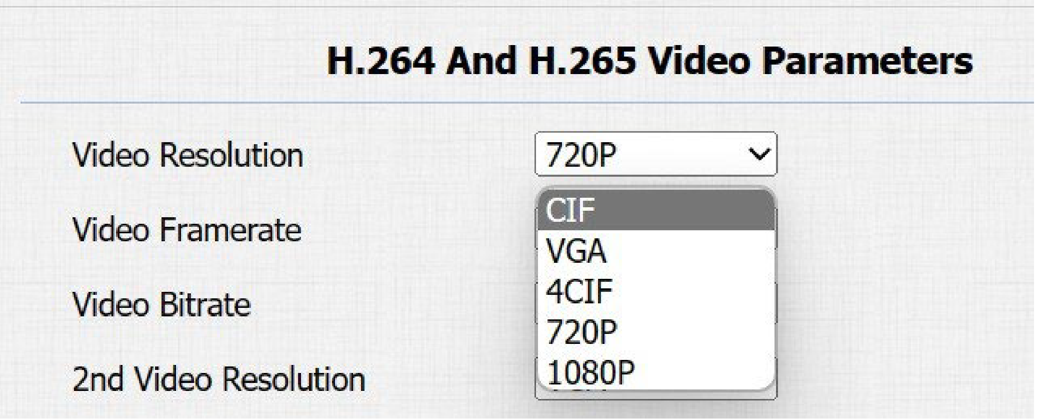
Video Framerate: 30 fps

Video Bitrate: 2048 kbps

2nd Video Resolution: VGA

2nd Video Framerate: 30 fps

2nd Video Bitrate: 512 kbps



H.264 And H.265 Video Parameters

Video Resolution: 720P

Video Framerate

Video Bitrate

2nd Video Resolution

Table A28 - MyBell IP 1-button Station - RTSP stream video parameters configuration

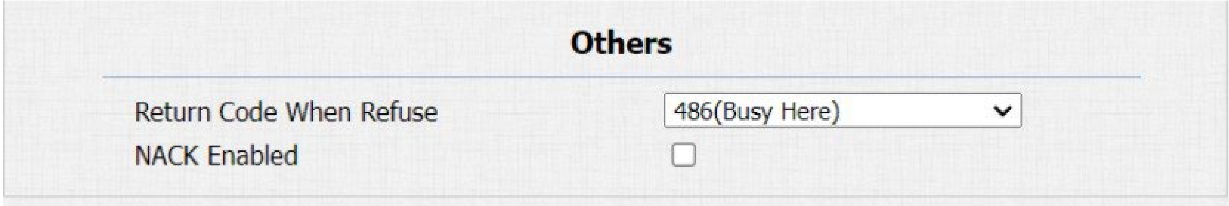
Setting	Description
Video Resolution	Select the video resolution from the following options: **CIF, VGA, 4CIF, 720P, 1080P.** The default video resolution is 4CIF. The video from the door phone can fail to be displayed on the indoor monitor if the resolution is set higher than 4CIF.
Video Framerate	The 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 30 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:

Phone > 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

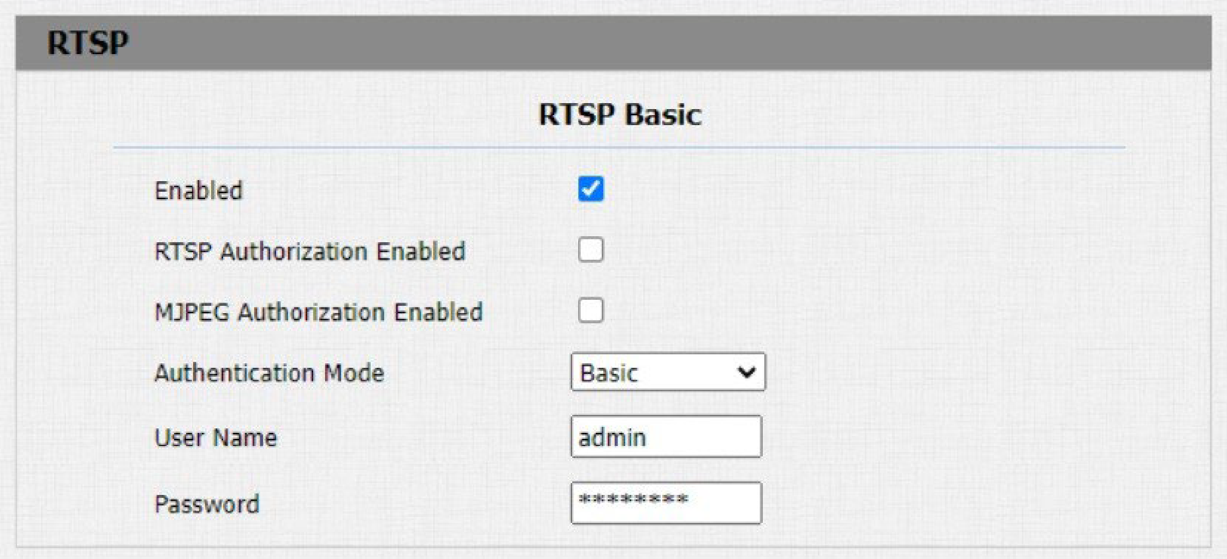
The door phone can capture the monitoring image in **MJPEG** format.

To enable the MJPEG function by the web interface:

Intercom > RTSP > RTSP Basic

To set the image quality by the web interface:

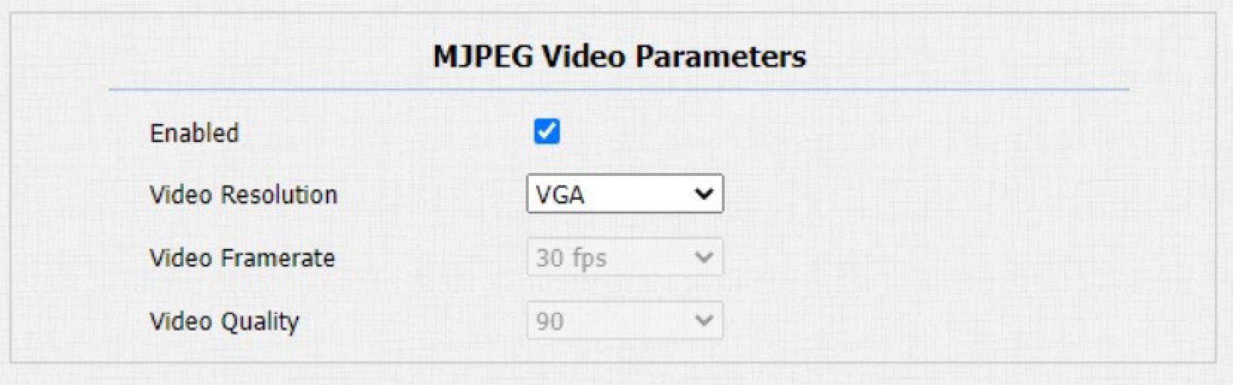
Intercom > RTSP > MJPEG Video Parameters



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 Framerate	30 fps
Video Quality	90

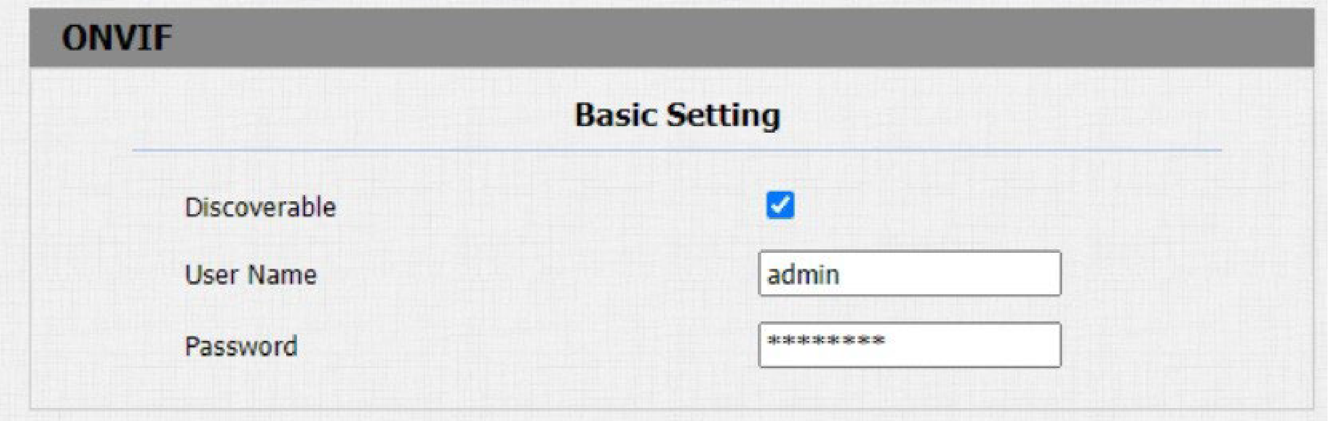
Table A29 - MyBell IP 1-button Station - MJPEG video configuration	
Setting	**Description**
Enabled	Tick this checkbox to access device video or real-time screenshots through a browser HTTP address such as: • http://device IP:8080/video.cgi (dynamic video). • http://device IP:8080/jpeg.cgi (static screenshot).
Video Resolution	Select the video resolutions from the following options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P.** 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 Quality	The video bitrate range is 50 to 90.

16.4 - ONVIF

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:

Intercom > ONVIF



ONVIF

Basic Setting

Discoverable ☑

User Name: admin

Password: ********

Settings:

- **Discoverable:** select to enable other devices to search the video from the door phone camera.
- **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.

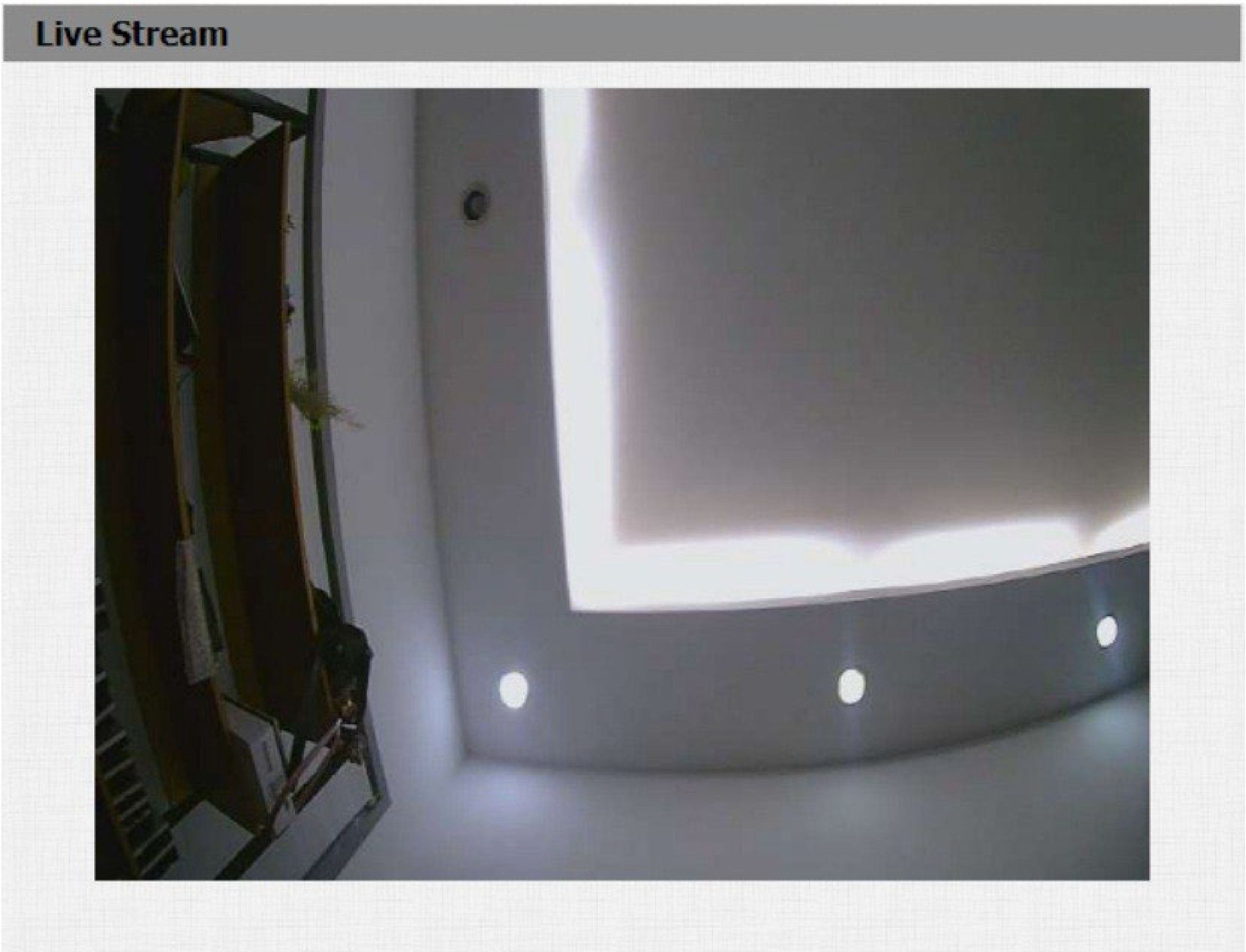
For example: **http://IP address:80/onvif/device_service**.

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:

Intercom > Live Stream



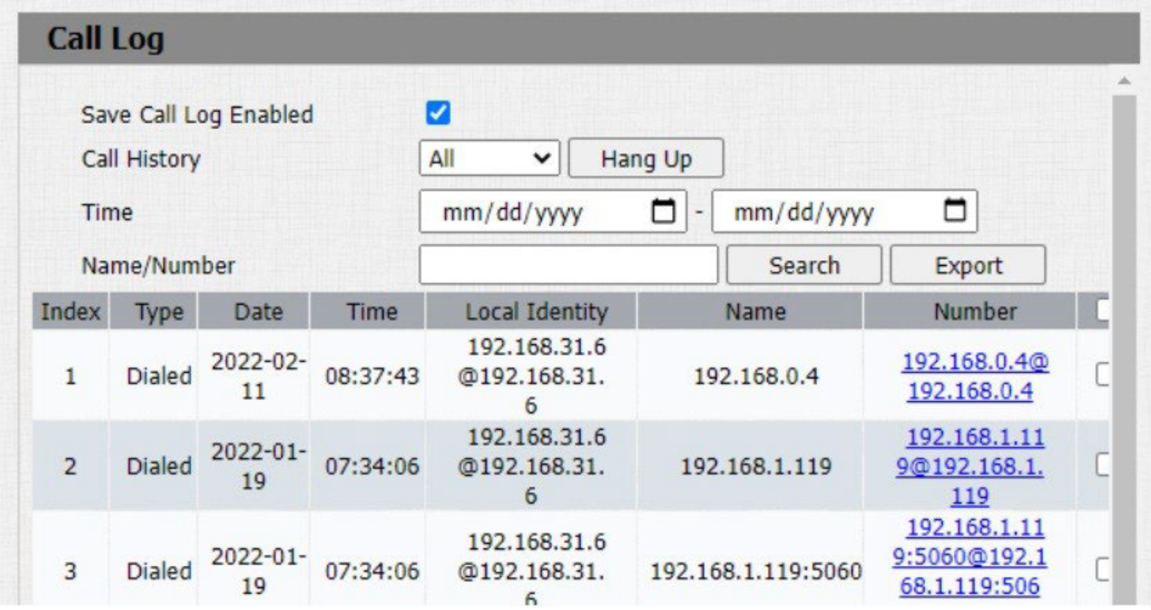
17 LOGS

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 by the device web interface and export the call log from the device.

To check the call logs by the web interface:

Phone > 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	□

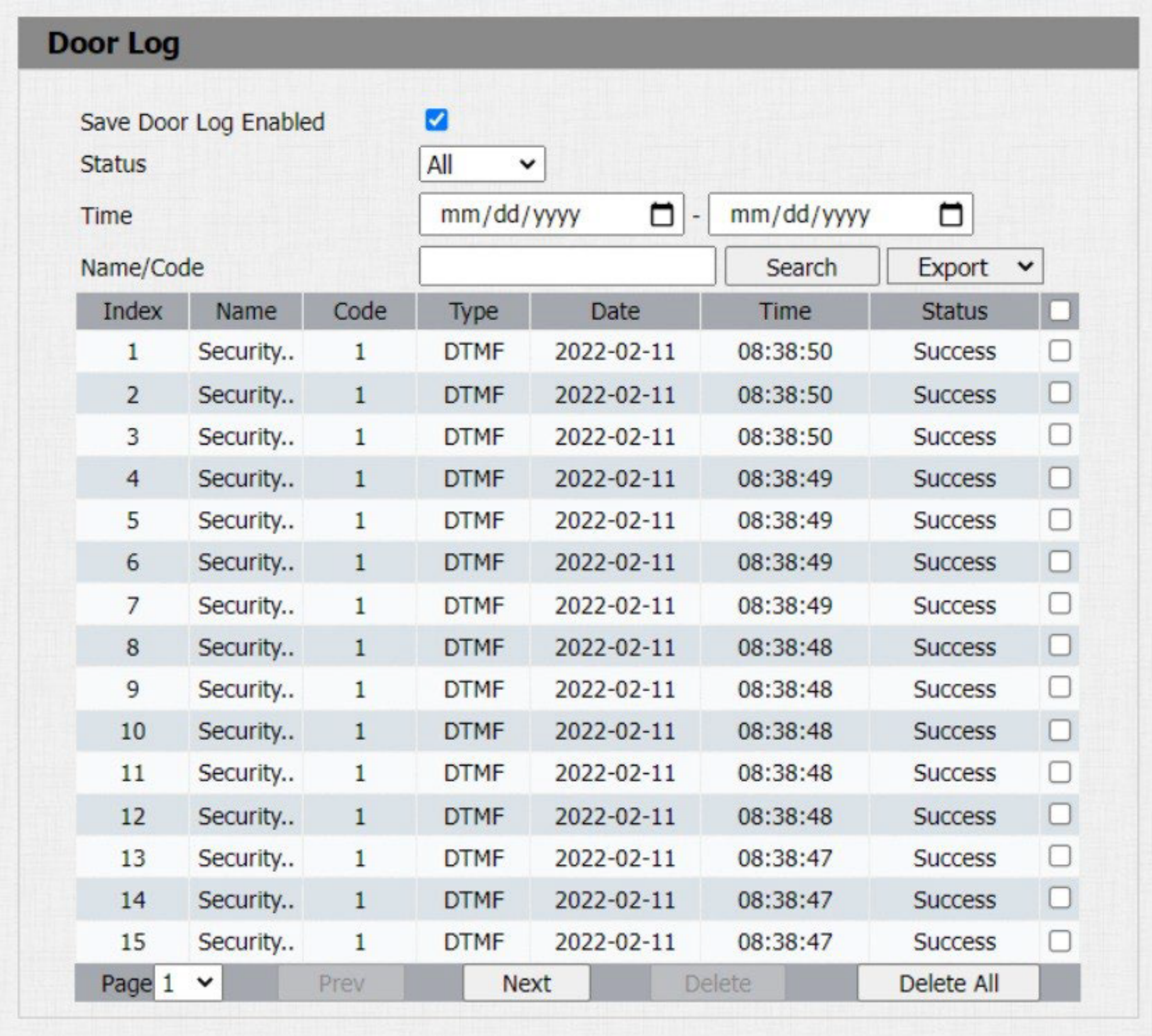
Setting:

- **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 call log by the web interface:

Phone > 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	□

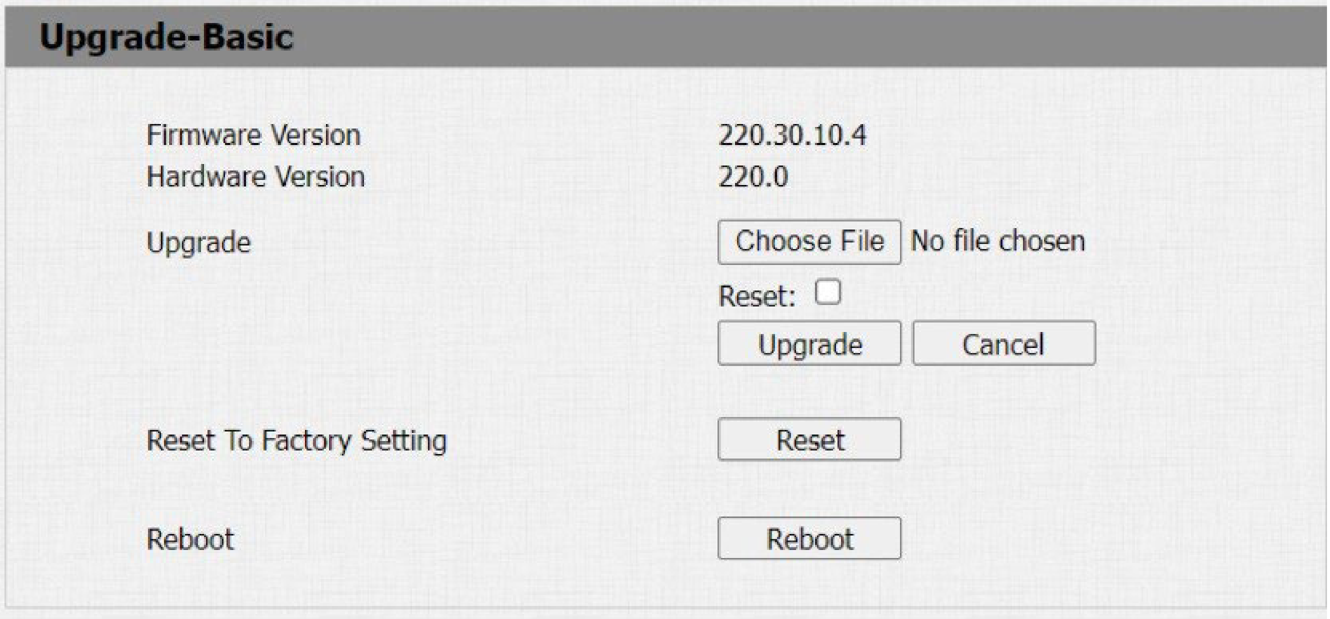
Settings:

- **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.

18 FIRMWARE UPGRADE

To upgrade the devices by the web interface:

Upgrade > Basic



Upgrade-Basic

Firmware Version	220.30.10.4
Hardware Version	220.0
Upgrade	Choose File No file chosen Reset: □ Upgrade Cancel
Reset To Factory Setting	Reset
Reboot	Reboot

Note

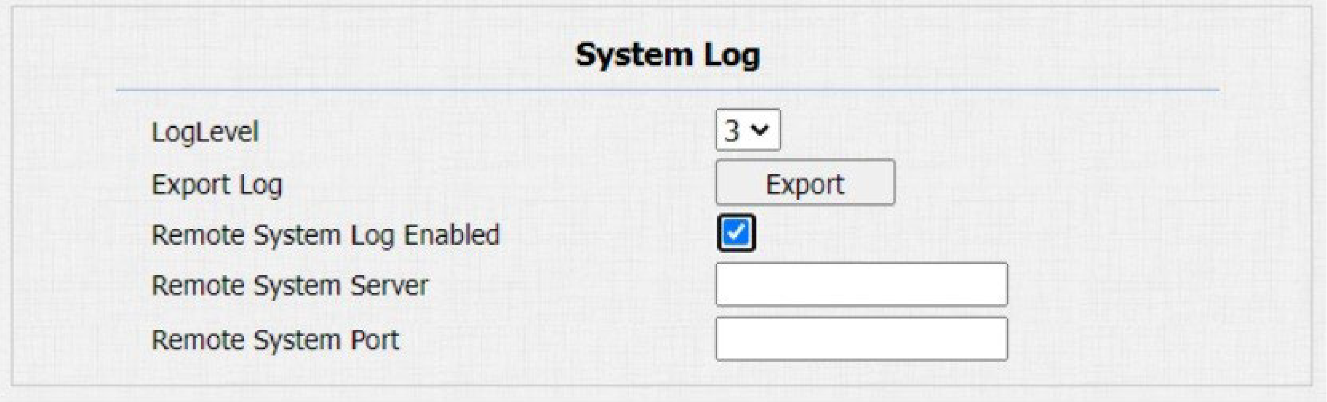
Don't disconnect the device from the internet and power supply when the firmware upgrade is in progress. It might cause upgrade failure or system breakdown.

19.1 - 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 > Advanced > System Log



System Log

LogLevel: 3

Export Log: Export

Remote System Log Enabled: ☑

Remote System Server:

Remote System Port:

Settings:

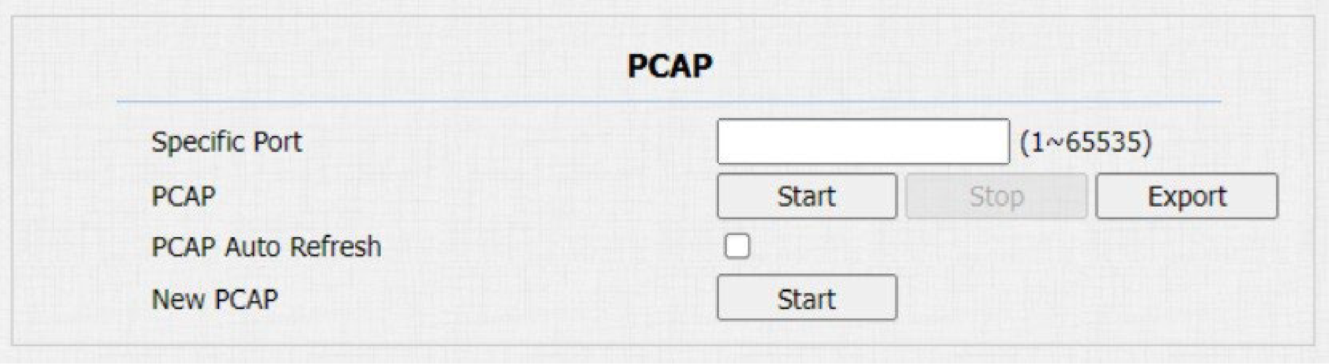
- **LogLevel:** select log level from 1 to 7. The technical staff instructs about the specific log level to be entered for debugging purpose. The default log level is **3**. The higher the level, the more complete the log.
- **Remote System Server:** enter the remote server address to receive the device log, the remote server address is provided by the technical support.

19.2 - PCAP

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 > Diagnosis > PCAP



PCAP

Specific Port: (1~65535)

PCAP: Start Stop Export

PCAP Auto Refresh: □

New PCAP: Start

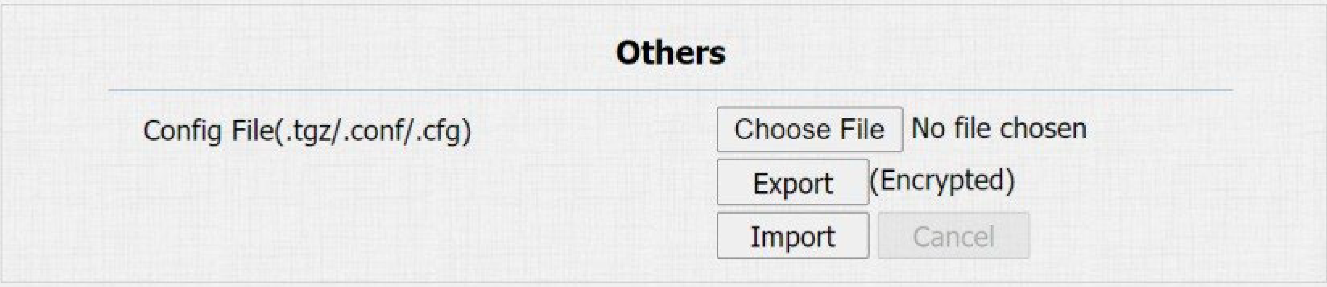
Table A30 - MyBell IP 1-button Station - PCAP configuration

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** tabs to capture a certain range of data packets before clicking the **Export** tab 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.

20 BACKUP

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

Upgrade > Advanced > Others



Others

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

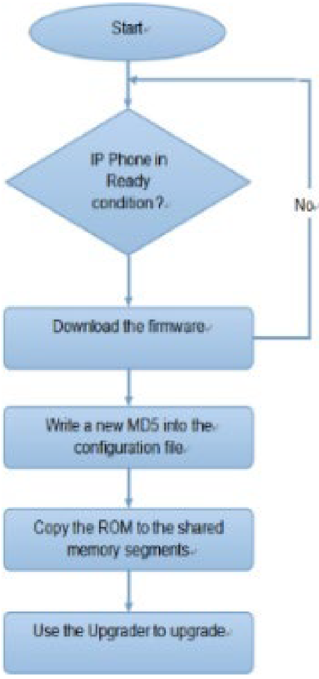
21 AUTO-PROVISIONING THROUGH CONFIGURATION FILE

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
Use the Upgrader to upgrade

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:

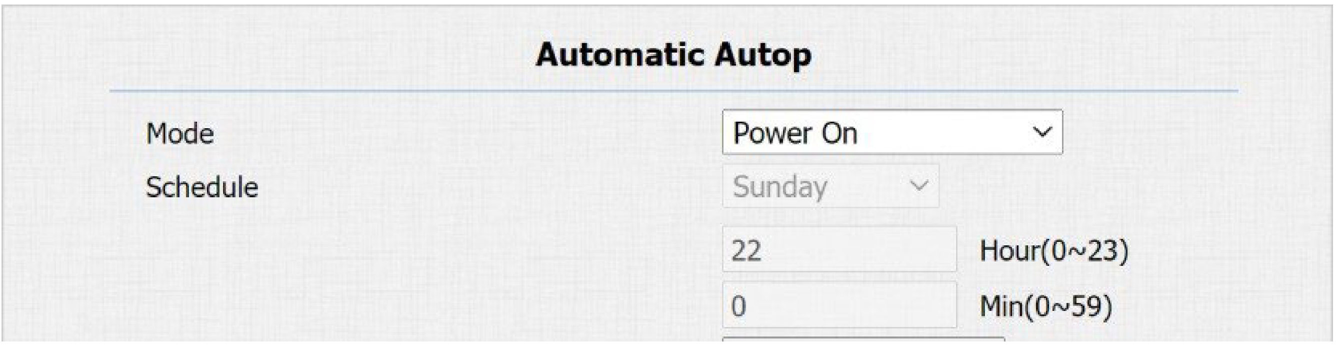
Upgrade > Advanced > Automatic Autop

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:

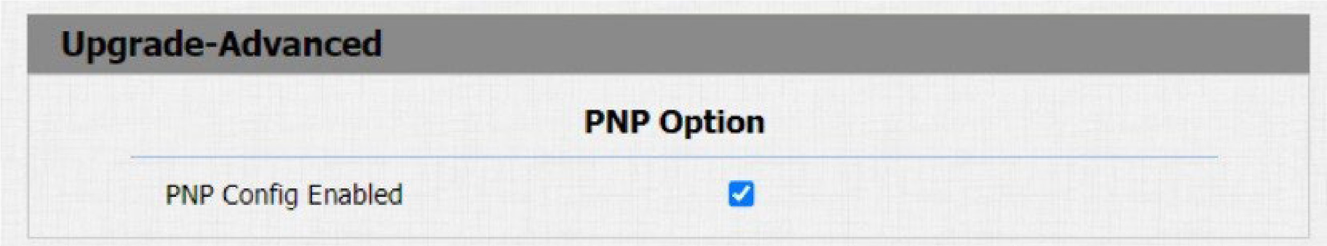
- **Mode:**
  - **Power on** – the device performs Autop every time it boots up.
  - **Repeatedly** – the device performs Autop according to the schedule you set up.
  - **Power On + Repeatedly** – combines the Power On Mode and the Repeatedly mode. It enables the device to perform Autop every time it 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

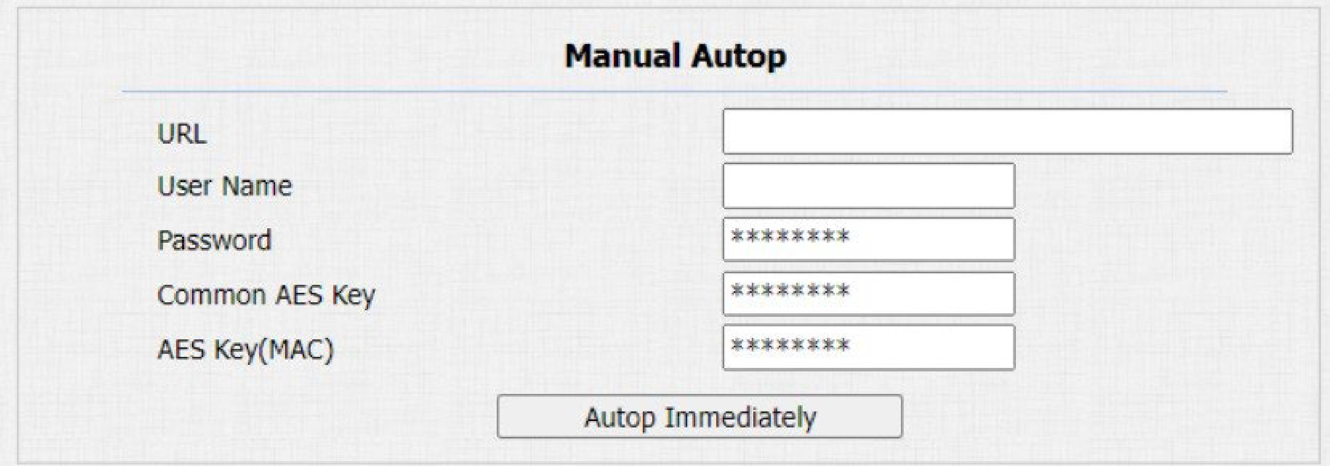
PNP Config Enabled ☑

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 A31 - MyBell IP 1-button Station - Static provisioning configuration

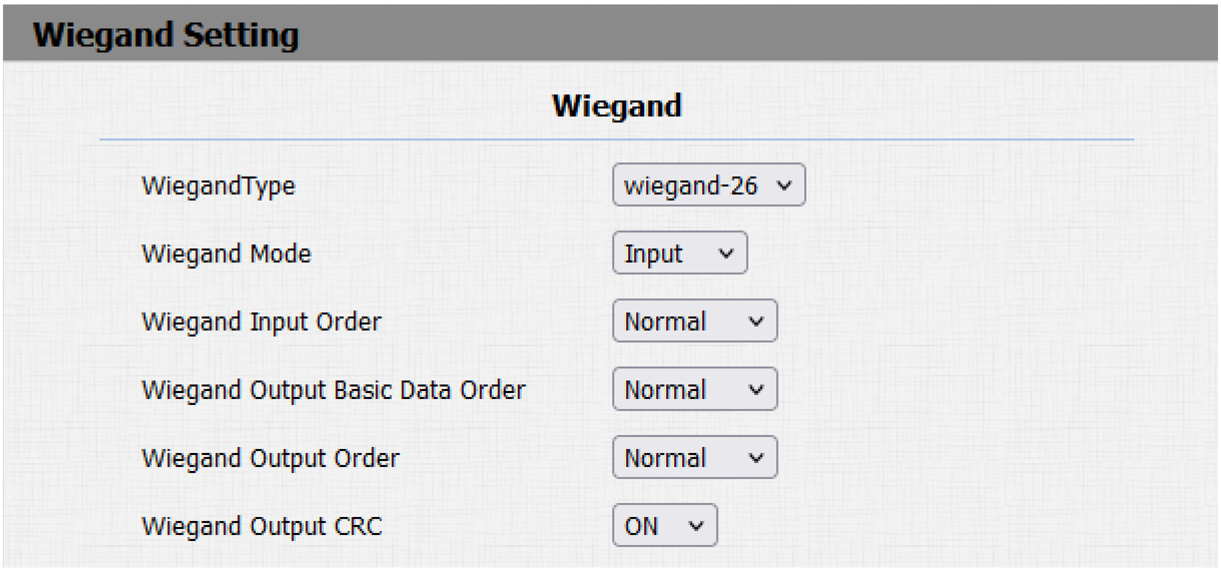
Setting	Description
URL	Set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
User Name	Set up a username if it is required to acces the server, otherwise leave it blank.
Password	Set up a password if it is required to acces the server, otherwise leave it blank.
Common AES Key	Set up 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.

22.1 - Wiegand integration

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



Wiegand Setting

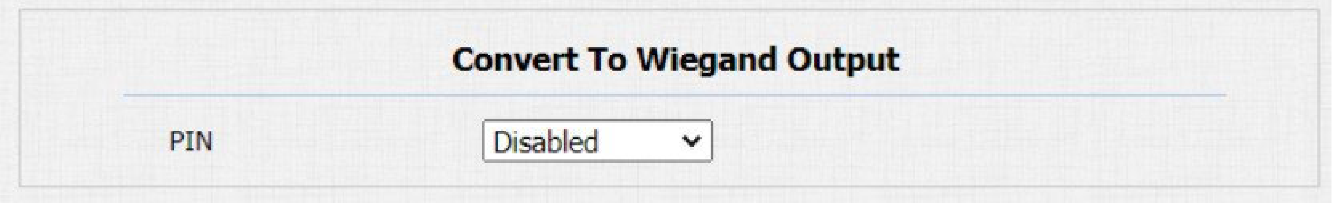
Wiegand

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

Table A32 - MyBell IP 1-button Station - Wiegand integration

Setting	Description
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. 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.

You can configure the Wiegand output mode. The output occurs when you press the PIN code on the device.



Convert To Wiegand Output

PIN	Disabled

Setting:

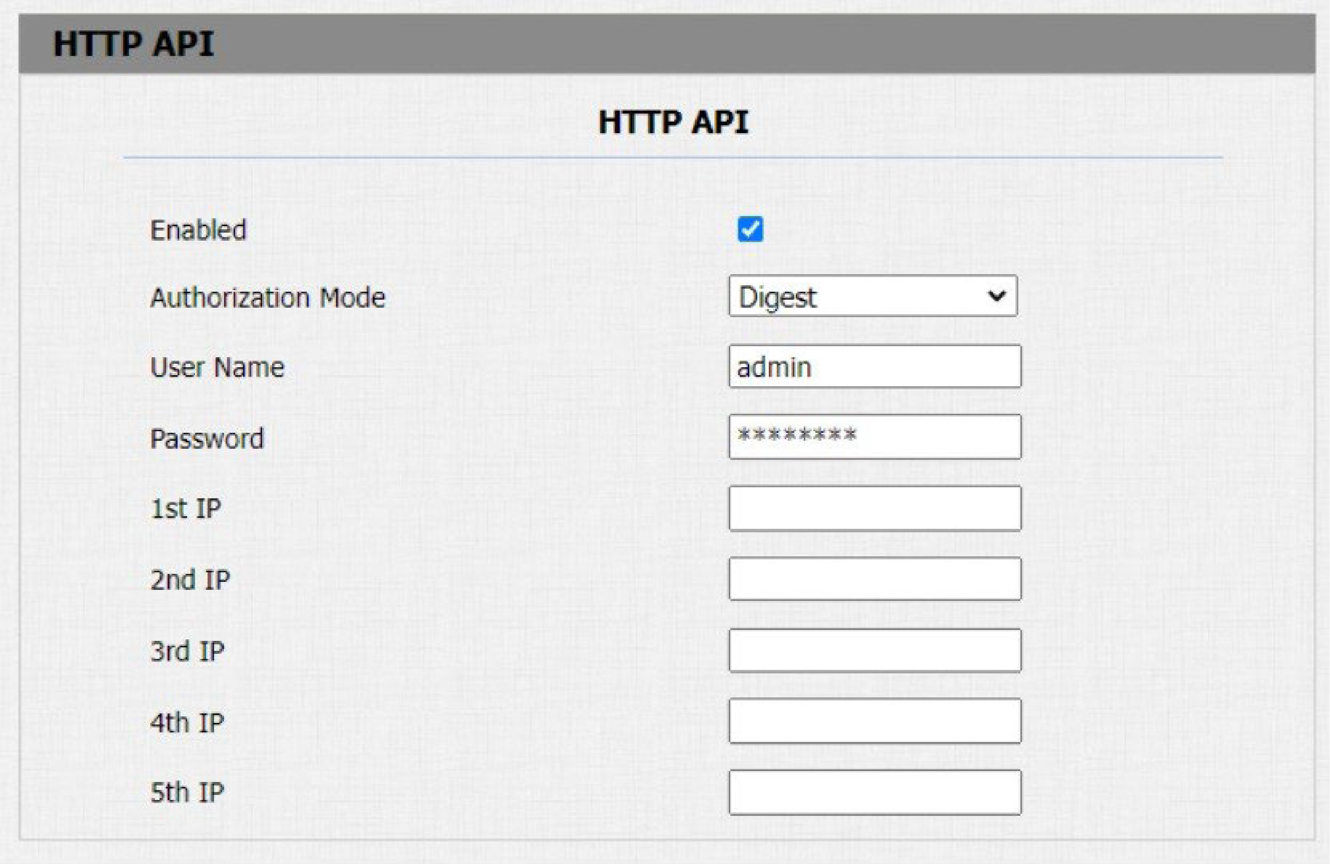
- **PIN**:
  - **Disabled** – the function is disabled.
  - **4 bits per digit** – output the PIN code by four continuous bits as a set.
  - **8 bits per digit** – output the PIN code by eight continuous bits as a set.

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:

Intercom > HTTP API



HTTP API

HTTP API

Enabled	☑
Authorization Mode	Digest
User Name	admin
Password	********
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

Table A33 - MyBell IP 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, WhiteList, 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 **WhiteList** authorization mode is selected.

Table A34 - MyBell IP 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.
WhiteList	You only need to enter the IP address of the third party device for authentication. The **WhiteList** 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.

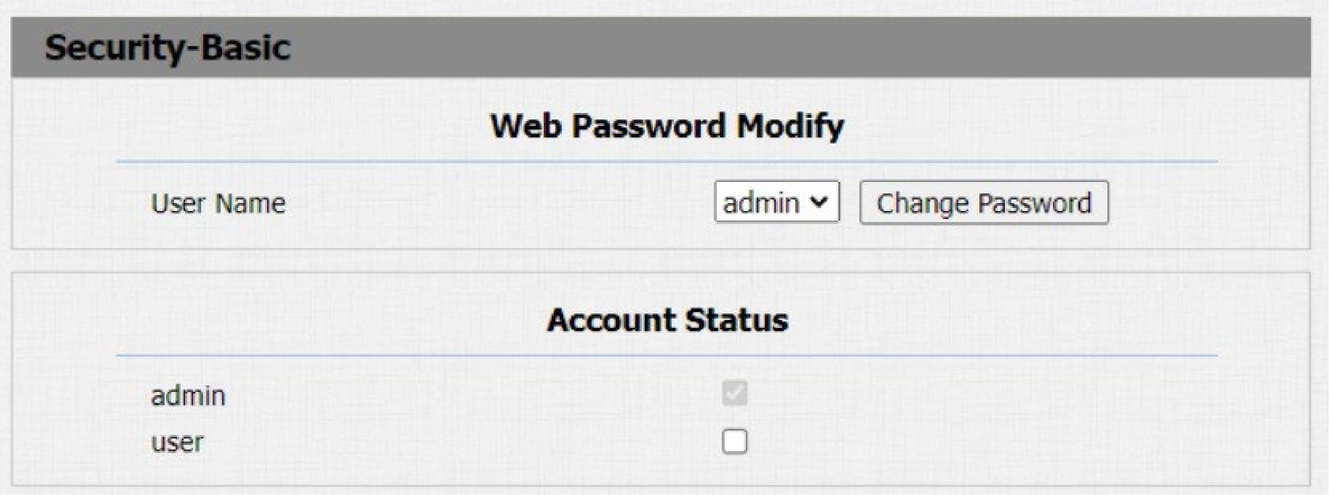
23 PASSWORD MODIFICATION

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.



Security-Basic

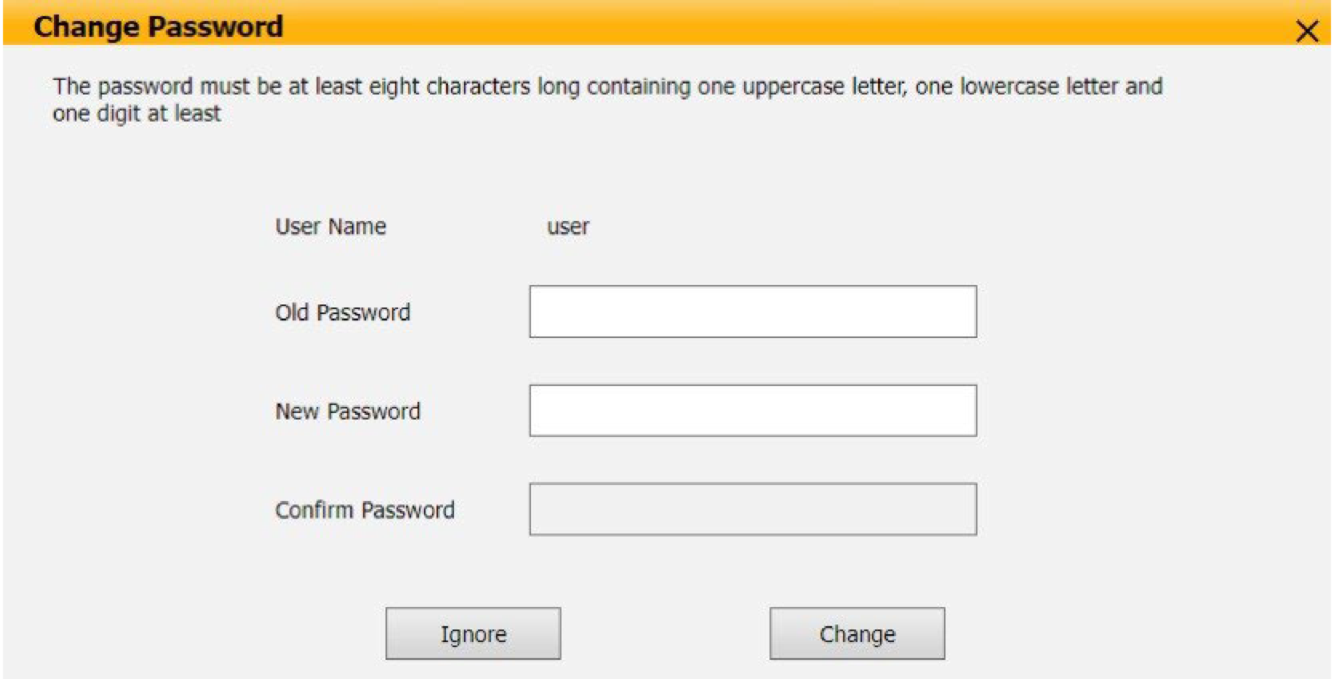
Web Password Modify

User Name admin Change Password

Account Status

admin ☑

user □



Change Password

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

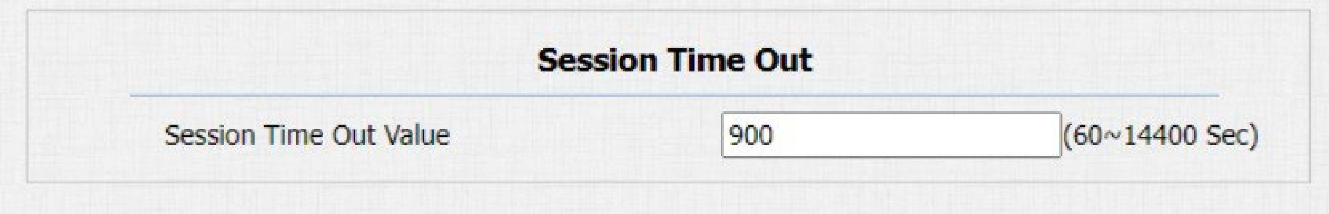
Ignore Change

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

Session Time Out Value 900 (60~14400 Sec)

Settings:

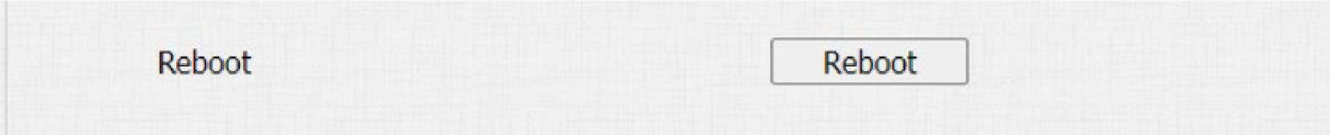
- **Session Time Out Value:** you can choose the session timeout between 60 and 14400 seconds. If there's no operation over the set time, you need to log in to the website again.

24 SYSTEM REBOOT AND RESET

24.1 - Reboot

To reboot the device system by the web interface:

Upgrade > Basic

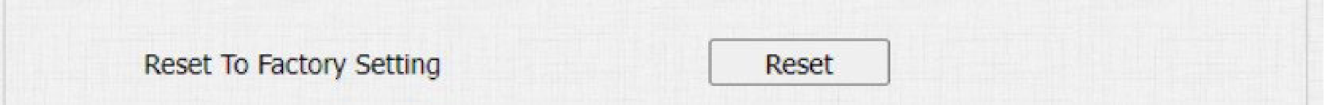


Reboot

Reboot

24.2 - Reset

Select **Reset To Factory Setting** to reset the device (deletes both configuration data and user data such as RF cards, face data, and so on).
Select **Reset Configuration to Default State (Except Data) Reset**, to reset the device (retains the user data).
To reset the device by the web interface:
Upgrade > Basic interface



Reset To Factory Setting

Reset

25 REGULATIONS

25.1 - 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.

25.2 - Declaration of conformity

Hereby, Nice S.p.A. declares that the device 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

25.3 - 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.

IS0931A00EN_08-11-2024

Nice

Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com