

MyBell

IP 1-button Kit

CE

EN - Instructions and warnings for installation and use

Part One

MyBell IP 1-button Station

1 - IMPORTANT SAFEGUARDS AND WARNINGS	7
2 - DEVICE DESCRIPTION	8
3 - CONFIGURATION MENU	10
4 - ACCESS TO DEVICE	11
4.1 - Obtain device IP address	11
4.2 - Access to device settings by web interface	11
5 - LANGUAGE AND TIME CONFIGURATION	12
5.1 - Language configuration	12
5.2 - Time configuration	12
5.2.1 - Manual time configuration	12
6 - LED CONFIGURATION	13
6.1 - LED display status	13
6.2 - LED display configuration from HTTP URL	13
6.3 - LED configuration on card reader area	14
7 - VOLUME AND TONE CONFIGURATION	15
7.1 - Volume configuration	15
7.2 - IP announcement configuration	15
7.3 - Open door tone configuration	15
7.4 - Uploading tone files	15
7.4.1 - Uploading ringback tone	15
7.4.2 - Uploading open door tone	16
8 - NETWORK CONFIGURATION	17
8.1 - Network status	17
8.2 - Device network configuration	17
8.3 - Device deployment in network	18
8.4 - Device local RTP configuration	18
8.5 - NAT configuration	19
8.6 - SNMP configuration	19
8.7 - VLAN configuration	19
8.8 - TR069 configuration	20
8.9 - Device web HTTP configuration	20
9 - INTERCOM CALL CONFIGURATION	21
9.1 - IP call and IP call configuration	21
9.2 - SIP call and SIP call configuration	21
9.2.1 - SIP account registration	21
9.2.2 - SIP server configuration	21
9.3 - Outbound proxy server configuration	22
9.4 - Data transmission type configuration	22
10 - CALLING FEATURE CONFIGURATION	23
10.1 - Do not disturb feature configuration	23
10.2 - Manager dial call configuration	23
10.3 - Call hang up configuration	24
10.4 - Web call	24
10.5 - Auto answer	24
10.6 - Multicast configuration	24
10.7 - Maximum call duration configuration	25
10.8 - Maximum dial duration configuration	26
10.9 - Hang up after open door	26
11 - ACCESS TO WHITE LIST CONFIGURATION	27
11.1 - Managing contacts	27
12 - AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS	28
12.1 - Audio codec configuration	28
12.2 - Video codec configuration	28

12.3 - Video codec configuration for IP direct calls	29
12.4 - DTMF data transmission configuration	29
13 - DOOR ACCESS CONFIGURATION	30
13.1 - Relay switch configuration	30
13.2 - Web relay configuration	31
13.3 - Door access schedule management	31
13.3.1 - Relay schedule configuration	31
13.3.2 - Creating door access schedule	32
13.3.3 - Import and export door access schedule	33
13.4 - Import and export user	33
14 - DOOR UNLOCK CONFIGURATION	34
14.1 - IC/ID card control configuration	34
14.2 - Access card format configuration	34
14.3 - RF card for door unlock configuration	34
14.4 - RF card configuration	34
14.5 - Mifare and Defare card encryption	35
14.6 - NFC function configuration	36
14.7 - Open relay configuration through HTTP for door access	36
14.8 - Exit button for door unlock configuration	36
15 - SECURITY	38
15.1 - Tamper alarm configuration	38
15.2 - Client certificate configuration	38
15.2.1 - Web Server certificate	38
15.2.2 - Client certificate	38
15.3 - Motion detection	39
15.3.1 - Motion detection configuration	39
15.4 - Security notification configuration	40
15.4.1 - Email notification configuration	40
15.4.2 - FTP notification configuration	41
15.4.3 - SIP call notification configuration	41
15.4.4 - HTTP URL notification configuration	41
15.5 - Security action configuration	41
15.5.1 - Pushbutton action configuration	41
15.5.2 - Input action configuration	42
15.6 - Voice encryption	42
15.7 - User agent	42
15.8 - High security mode	43
16 - MONITOR AND IMAGE	44
16.1 - RTSP stream monitoring	44
16.1.1 - RTSP basic configuration	44
16.1.2 - RTSP stream configuration	44
16.2 - NACK	45
16.3 - MJPEG image capturing	46
16.4 - ONVIF	46
16.5 - Live stream	47
17 - LOGS	48
17.1 - Call logs	48
17.2 - Door logs	48
18 - FIRMWARE UPGRADE	50
19 - DEBUG	51
19.1 - System log	51
19.2 - PCAP	51
20 - BACKUP	52
21 - AUTO-PROVISIONING THROUGH CONFIGURATION FILE	53
21.1 - Provisioning principle	53
21.2 - Configuration files for auto-provisioning	53
21.3 - Autop schedule	53
21.4 - PNP configuration	54
21.5 - Static provisioning configuration	54
22 - INTEGRATION WITH THIRD PARTY DEVICE	55
22.1 - Wiegand integration	55
22.2 - HTTP API integration	56

23 - PASSWORD MODIFICATION	57
23.1 - Device web interface password modification	57
23.2 - Web interface automatic logout configuration	57
24 - SYSTEM REBOOT AND RESET	58
24.1 - Reboot	58
24.2 - Reset	58

Part Two

MyBell IP Premium Indoor Monitor

1 - IMPORTANT SAFEGUARDS AND WARNINGS	59
2 - DEVICE DESCRIPTION	60
3 - INTRODUCTION TO CONFIGURATION MENU	62
3.1 - Configuration menu	62
3.2 - Mode selection	62
3.3 - Tool selection	62
4 - INDICATOR LIGHT STATUS	63
5 - ACCESS TO DEVICE	64
5.1 - Device start-up network selection	64
5.2 - Device home screen type selection	64
5.3 - Access to device settings on device	65
5.3.1 - Access to device basic settings	65
5.3.2 - Access to device advanced setting	65
5.4 - Access to device settings by web interface	66
6 - LANGUAGE AND TIME CONFIGURATION	67
6.1 - Language configuration	67
6.1.1 - Language configuration on device	67
6.1.2 - Language configuration by web interface	67
6.2 - Time configuration	67
6.2.1 - Time configuration on device	67
6.2.2 - Time configuration by device web interface	68
7 - SCREEN DISPLAY CONFIGURATION	69
7.1 - Screen display configuration on device	69
7.2 - Screen display configuration by web interface	70
7.2.1 - Uploading screen saver	70
7.2.2 - Uploading wallpaper	70
7.3 - Uploading device booting image	70
7.4 - Approach to wake up	71
7.5 - Icon screen display configuration	71
7.6 - Unlock Tab configuration	73
7.6.1 - Unlock Tab configuration on Talking Screen	73
7.6.2 - Unlock Tab configuration on Home and More Screen	73
7.6.3 - Unlock Tab configuration on Monitor Screen	73
7.6.4 - Unlock Tab configuration on Call Preview Screen	74
7.7 - Home screen display	74
8 - SOUND AND VOLUME CONFIGURATION	75
8.1 - Volume configuration	75
8.1.1 - Volume configuration on device	75
8.1.2 - Volume configuration by web interface	75
8.2 - Doorbell sound configuration	76
9 - PHONE BOOK CONFIGURATION	77
9.1 - Phone book configuration on device	77
9.1.1 - Adding contacts	77
9.1.2 - Editing contacts	78
9.1.3 - Blocklist setting on device	78

9.2 - Phone book configuration by web interface	78
9.2.1 - Adding, editing, deleting and searching local contacts	78
9.3 - Importing and exporting contacts	79
9.4 - Contact list display configuration	80
9.5 - Web call	80
10 - NETWORK CONFIGURATION AND OTHER CONNECTIONS	81
10.1 - Network connection configuration on device	81
10.2 - Network connection configuration by web interface	82
10.3 - Device deployment in network	83
10.4 - Device NAT configuration	83
10.5 - Device Bluetooth configuration	84
10.5.1 - Device Bluetooth pairing	84
10.5.2 - Device Bluetooth data transmission	84
10.6 - Device Wi-Fi configuration	85
11 - INTERCOM CALL CONFIGURATION	86
11.1 - IP call and IP call configuration	86
11.1.1 - Making IP calls	86
11.1.2 - IP configuration	87
11.2 - SIP call and SIP call configuration	87
11.2.1 - SIP account registration	87
11.2.2 - SIP server configuration	89
11.2.3 - Outbound proxy server configuration	89
11.3 - SIP Call DND and return code configuration	89
11.4 - Device local RTP configuration	90
11.5 - Data transmission type configuration	90
12 - CALL CONFIGURATION	91
12.1 - Auto-answer configuration	91
12.2 - Auto-answer Allow List configuration	91
12.3 - Live stream configuration	92
12.4 - Intercom call configuration (preview, mute)	92
12.5 - Voice changer	92
12.6 - Emergency call configuration	93
12.7 - Multicast configuration	94
12.8 - Call forwarding configuration	94
12.9 - Call forwarding configuration on device	94
12.10 - Call forwarding configuration by web interface	95
13 - INTERCOM MESSAGE CONFIGURATION	96
13.1 - Managing messages	96
14 - AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS	97
14.1 - Audio codec configuration	97
14.2 - Video codec configuration	97
15 - SECURITY	99
15.1 - Monitor configuration	99
15.2 - Video image capturing	100
15.3 - RTSP authentication	101
15.4 - Alarm and arming configuration	101
15.4.1 - Alarm and arming configuration on device	101
15.4.2 - Alarm and arming configuration by web interface	102
15.5 - Location-based alarm configuration	103
15.6 - Alarm text configuration	103
15.7 - Arming mode configuration	103
15.8 - Alarm ringtone configuration	104
15.9 - Alarm action configuration	104
15.9.1 - Select alarm action types	104
15.9.2 - Alarm action type configuration through HTTP command	105
15.9.3 - Alarm action configuration through SIP message	105
15.10 - Checking alarm log	106
15.11 - Screen unlock configuration	106
15.12 - Screen unlock by PIN code	107
15.13 - Voice encryption	107
15.14 - Remote control	107
15.15 - Location	107

15.16 - High security mode	108
16 - DOOR ACCESS CONTROL CONFIGURATION	109
16.1 - Relay switch configuration	109
16.1.1 - Local relay configuration	109
16.1.2 - Remote relay switch configuration	109
16.2 - Web relay configuration	109
16.3 - Door unlock configuration	110
16.3.1 - Door unlock by DTMF code	110
16.3.2 - Door unlock through HTTP command	110
17 - FIRMWARE UPGRADE	112
18 - BACKUP	112
19 - AUTO-PROVISIONING THROUGH CONFIGURATION FILE	113
19.1 - Provisioning principle	113
19.2 - Introduction to configuration files for auto-provisioning	113
19.3 - Autop	113
19.4 - DHCP provisioning configuration	114
19.5 - Static provisioning configuration	115
19.6 - Voice assistant	116
19.7 - Call log	119
20 - DEBUG	120
21.1 - System log for debugging	120
21.1.1 - Capturing system log for debugging	120
21.2 - PCAP for debugging	120
21.3 - User agent	121
21.4 - Screenshots	121
21 - DEVICE INTEGRATION WITH THIRD PARTY	122
21.1 - Entering applications screen	122
21.2 - Third-party app installation	123
21.3 - PBX feature	123
21.3.1 - PBX configuration on device	124
21.3.2 - Enabling PBX service	124
21.3.3 - PBX accounts management	125
21.3.4 - PBX groups management	126
21.3.5 - PBX configuration by web interface	126
22 - PASSWORD MODIFICATION	128
22.1 - Device basic setting password modification	128
22.2 - Device advanced setting password modification	128
22.3 - Device web interface password modification	129
22.4 - Browser password modification	129
23 - SYSTEM REBOOT AND RESET	130
23.1 - Reboot on device	130
23.2 - Reboot by web interface	130
23.3 - Reset on device	131
23.4 - Reset by web interface	131
24 - REGULATIONS	132
24.1 - Warranty	132
24.2 - Declaration of conformity	132
24.3 - WEEE Directive Compliance	132

Part One

MyBell IP 1-button Station

1 IMPORTANT SAFEGUARDS AND WARNINGS

- **⚠ CAUTION!** – Any use other than that specified herein or in environmental conditions other than those stated in this manual is to be considered improper and is strictly forbidden!
 - **⚠ CAUTION!** – Important instructions: keep this manual in a safe place to enable future product maintenance and disposal procedures.
 - **⚠ CAUTION!** – All installation and connection operations must be performed exclusively by suitably qualified and skilled personnel with the unit disconnected from the mains power supply.
 - **⚠ CAUTION!** – This manual contains important instructions and warnings for personal safety. Read carefully all parts of this manual. If in doubt, suspend installation immediately and contact Nice Technical Assistance.
-
- The product packaging materials must be disposed of in full compliance with local regulations.
 - Never apply modifications to any part of the device. Operations other than those specified can cause malfunctions. The manufacturer declines all liability for damage caused by makeshift modifications to the product.
 - Never place the device near the sources of heat or expose to naked flames. These actions can damage the product and cause malfunctions.
 - 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

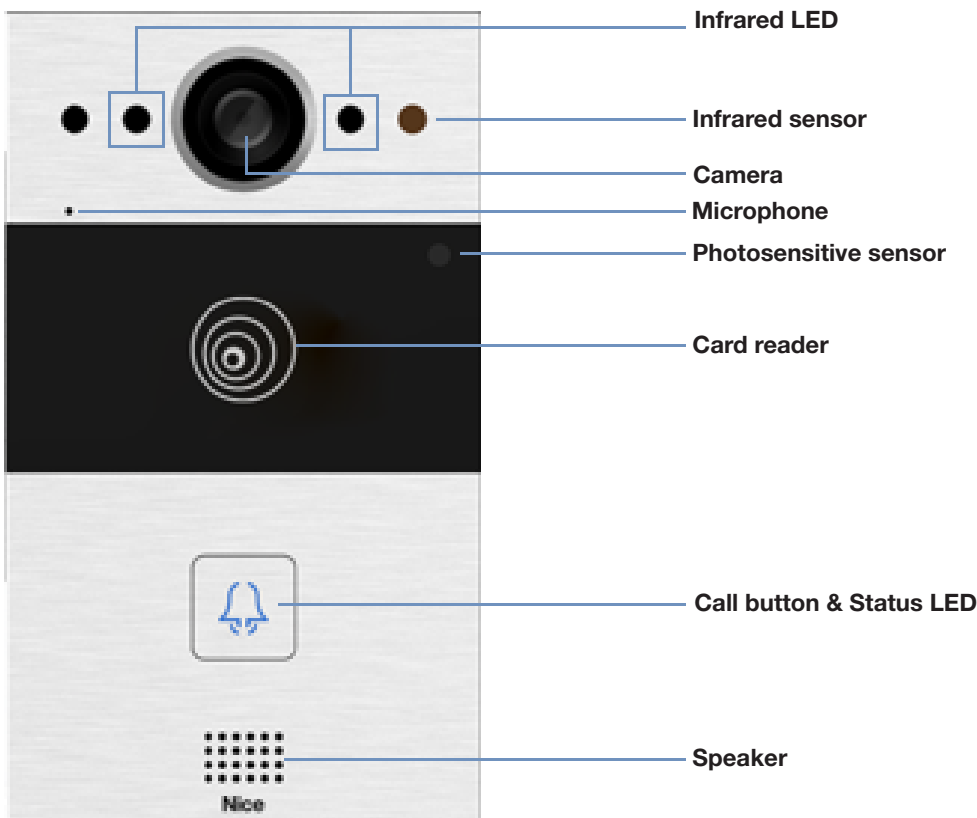
The device can be connected with indoor monitors for remote access control and communication. It enables audio and video calls with visitors and the door unlock function.

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	<ul style="list-style-type: none"> • 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.

Nice

▼ Status
Basic

▶ Account

▶ Network

▶ Intercom

▶ Surveillance

▶ Access Control

▶ Device

▶ Setting

▶ Upgrade

▶ Security

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:

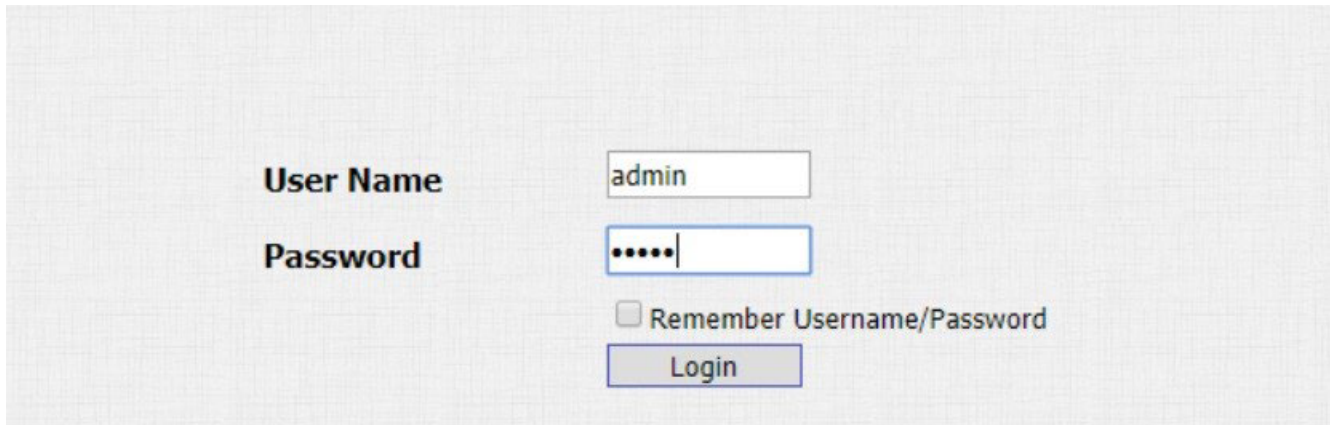
4 ACCESS TO DEVICE

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.



The image shows a login form on a web interface. It features two input fields: one for the 'User Name' containing the text 'admin', and one for the 'Password' containing five dots. Below the password field is a checkbox labeled 'Remember Username/Password' which is currently unchecked. At the bottom of the form is a 'Login' button.

User Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
	<input type="checkbox"/> Remember Username/Password
	<input type="button" value="Login"/>

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



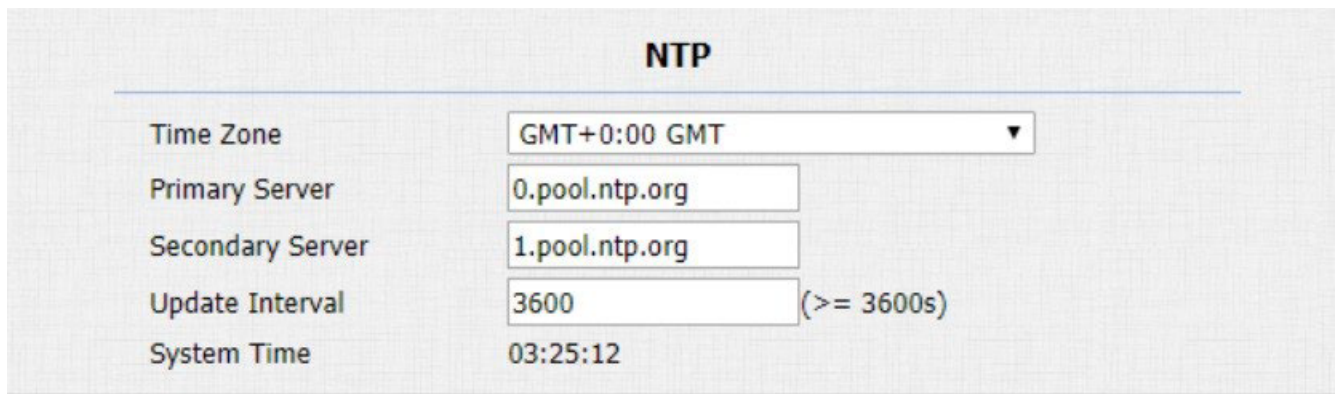
The screenshot shows a configuration page titled 'Time/Lang'. Under the 'Web Language' section, there is a 'Mode' label and a dropdown menu currently displaying 'English' with a downward arrow.

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



The screenshot shows an 'NTP' configuration page with the following settings:

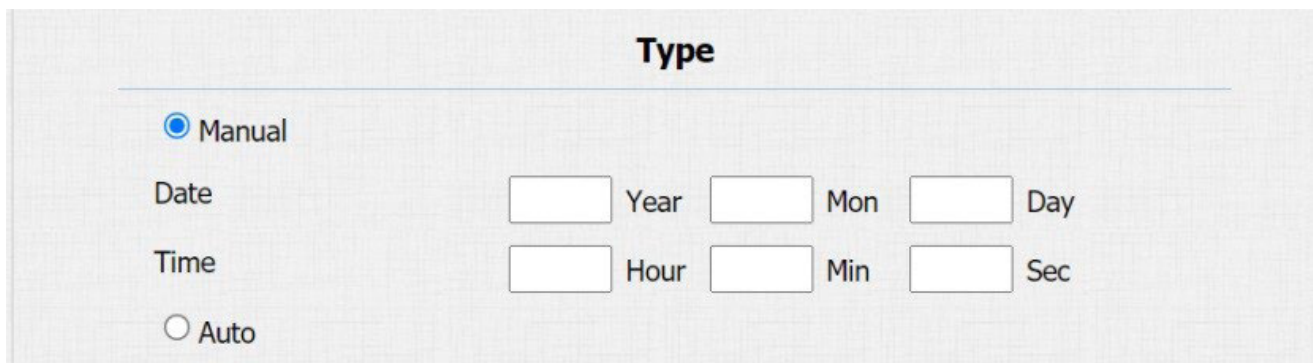
Time Zone	GMT+0:00 GMT
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	03:25:12

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.



The screenshot shows a 'Type' configuration page with the following options:

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

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	<input checked="" type="checkbox"/>
Card LED Enabled	<input type="checkbox"/>

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:

LED Control:

Card LED Enabled:

Time (H): - (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	<input type="text" value="8"/>	(1~15)
Mic Analog Gain	<input type="text" value="10"/>	(0~31)
Volume Level	<input type="text" value="1"/>	▼
Speaker Volume	<input type="text" value="15"/>	(1~15)
Tamper Alarm Volume	<input type="text" value="15"/>	(1~15)
Prompt Volume	<input type="text" value="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	<input type="text" value="0"/>	(0~180 sec)
Loop Times	<input type="text" value="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	<input checked="" type="checkbox"/>
Open Door Outside Tone	<input checked="" type="checkbox"/>
Open Door Failed Tone	<input checked="" type="checkbox"/>

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	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Succeeded Inside Warning	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Failed Warning	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Ringback	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Trigger Manager Dial Warning	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>

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	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Succeeded Inside Warning	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Failed Warning	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Ringback	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Trigger Manager Dial Warning	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>

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.

8.1 - 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

Submit
Cancel

Table A6 - MyBell IP 1-button Station - Network configuration

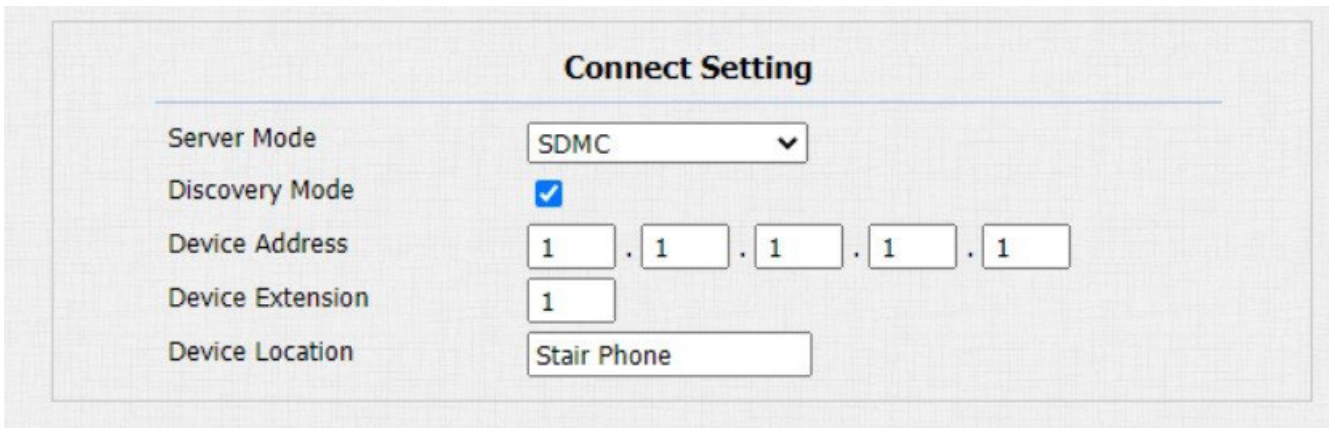
Setting	Description
DHCP	Select the DHCP mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, the door phone is assigned by the DHCP server with IP address, subnet mask, default gateway, and Domain Name Server (DNS) automatically.
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:

Discovery Mode:

Device Address:

Device Extension:

Device Location:

Table A7 - MyBell IP 1-button Station - Device deployment in network

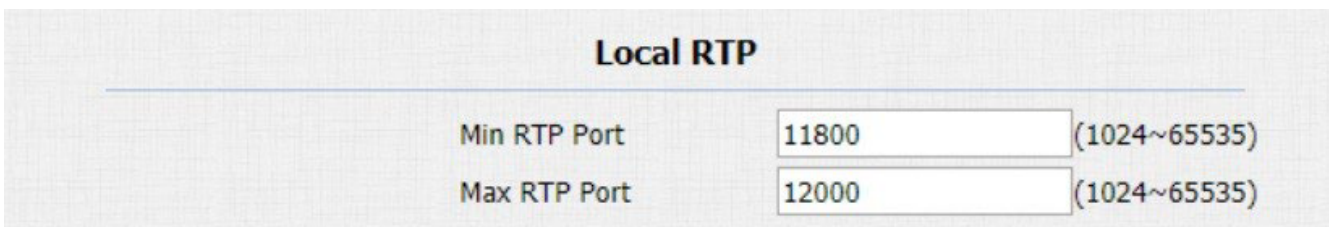
Setting	Description
Server Mode	It's set up automatically according to the device connection with a specific server in the network, such as SDMC or Cloud and None . None is the default factory setting indicating the device isn't in any server type and you can choose Cloud , SDMC in the discovery mode.
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: (1024~65535)

Max RTP Port: (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

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

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

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

	Enabled	<input type="checkbox"/>	
ACS	Version	<input type="text" value="1.0"/>	
	URL	<input type="text"/>	
	User Name	<input type="text"/>	
	Password	<input type="password" value="*****"/>	
Periodic Inform	Enabled	<input type="checkbox"/>	
	Periodic Interval	<input type="text" value="1800"/>	(3~24×3600s)
CPE	URL	<input type="text"/>	
	User Name	<input type="text"/>	
	Password	<input type="password" value="*****"/>	

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

Setting	Description
Version	Select the supported TR069 version (1.0 or 1.1).
ACS/CPE	<ul style="list-style-type: none"> • 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	<input checked="" type="checkbox"/>	
HTTPS Enabled	<input checked="" type="checkbox"/>	
HTTP Port	<input type="text" value="80"/>	(80,1024~65534)
HTTPS Port	<input type="text" value="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	<input checked="" type="checkbox"/>
Auto Answer	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1~65535)

9.2 - SIP call and SIP call configuration

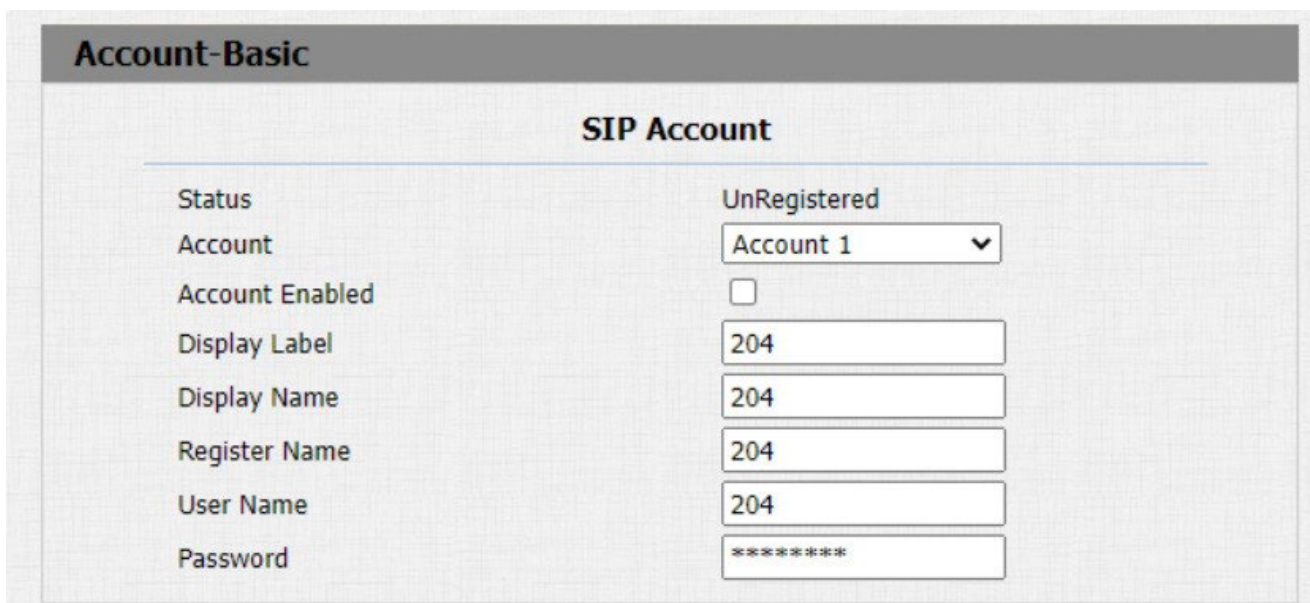
You can make a Session Initiation Protocol (SIP) call in the same way as you make the IP calls using the device. However, SIP call settings related to its account, server, and transport type need to be configured first.

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



SIP Account	
Status	UnRegistered
Account	Account 1
Account Enabled	<input type="checkbox"/>
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 Port (1024~65535)
 Registration Period (30~65535s)

Alternate SIP Server

Server IP Port (1024~65535)
 Registration Period (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 outbound proxy server by the web interface:

Account > Basic > Outbound Proxy Server

Outbound Proxy Server

Outbound Enabled
 Server IP Port (1024~65535)
 Backup Server IP Port (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 ▼

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 CALLING FEATURE CONFIGURATION

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

The screenshot shows the 'Phone-Call Feature' configuration page. Under the 'DND' section, there is an 'Enabled' checkbox which is currently unchecked. Below it, the 'Return Code When DND' is set to '486(Busy Here)' in a dropdown menu.

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

The screenshot shows the 'Intercom-Basic' configuration page. Under the 'Manager Dial' section, 'Call Type' is set to 'Group Call' and 'Call Timeout (Sec)' is set to '60'. A note below states: '(If the local group is not blank, then only the local numbers will be called.)'. Below this, there is a section titled 'Group Call Number (Local)' with a 4x4 grid of input fields for entering numbers.

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.

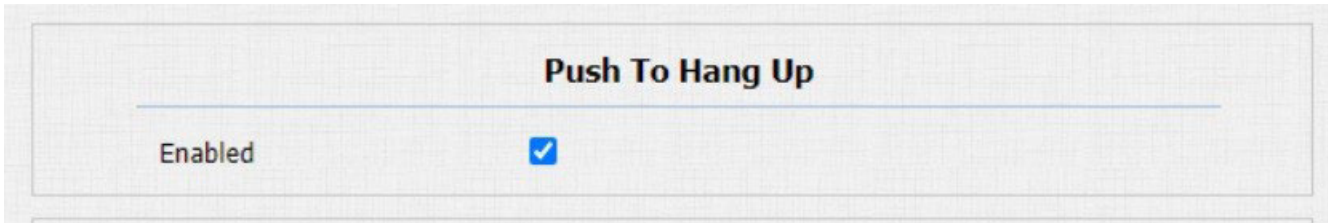
After the manager dial is set up, on the same page you can set up relays to be triggered by the manager dial.

The screenshot shows the 'Trigger Relay By Manager Dial' configuration page. It features a 'RelayID' label and two checkboxes for 'RelayA' and 'RelayB', both of which are currently unchecked.

10.3 - Call hang up configuration

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

Intercom > Basic

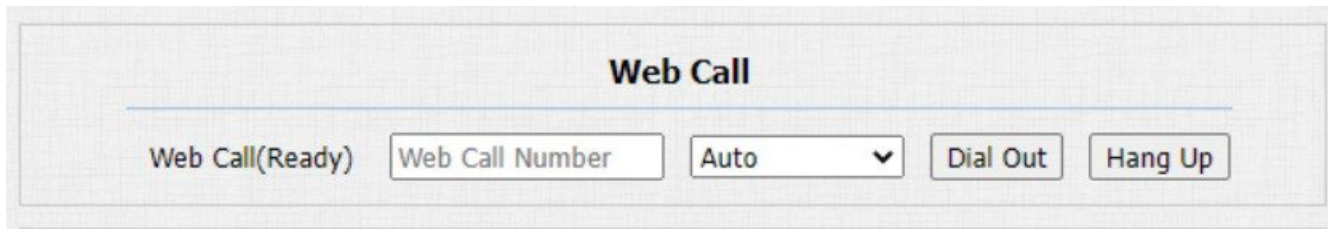


10.4 - Web call

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



Setting:

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

10.5 - Auto answer

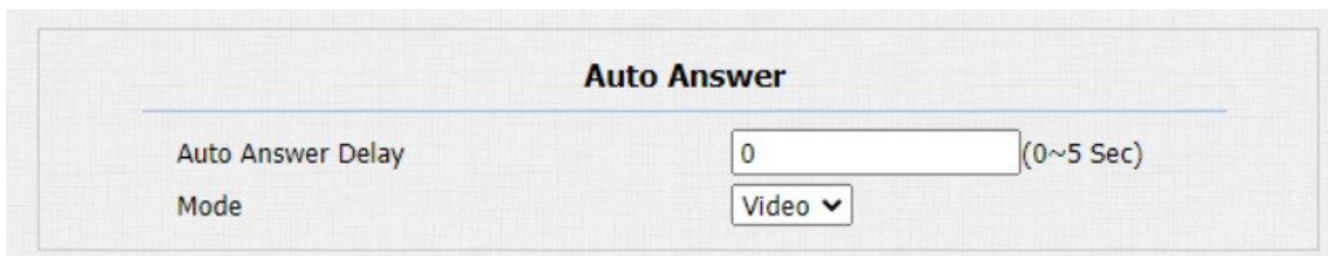
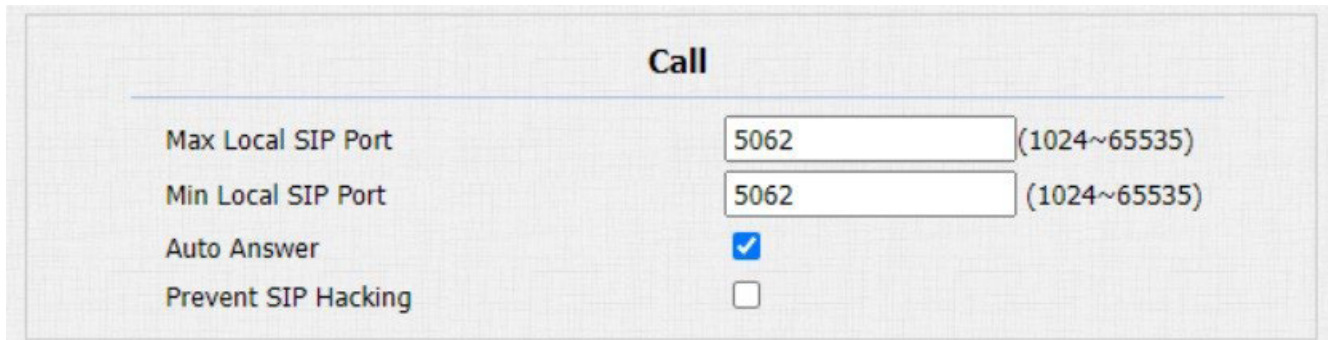
You can define the time of the door phone response for the incoming SIP/IP call automatically by setting up the time-related parameters. You can also define the mode in which the calls are answered (video or audio).

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



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

Paging Priority Enabled

Priority List

IP Address	Listening Address	Label	Priority
1st IP Address	<input type="text" value="224.1.6.21:51230"/>	<input type="text" value="NICE"/>	1
2nd IP Address	<input type="text"/>	<input type="text"/>	2
3rd IP Address	<input type="text"/>	<input type="text"/>	3
4th IP Address	<input type="text"/>	<input type="text"/>	4
5th IP Address	<input type="text"/>	<input type="text"/>	5
6th IP Address	<input type="text"/>	<input type="text"/>	6
7th IP Address	<input type="text"/>	<input type="text"/>	7
8th IP Address	<input type="text"/>	<input type="text"/>	8
9th IP Address	<input type="text"/>	<input type="text"/>	9
10th IP Address	<input type="text"/>	<input type="text"/>	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 performed 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 (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	<input type="text" value="60"/>	(1~120Sec)
Dial Out Time	<input type="text" value="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	<input type="text" value="DTMF Or HTTP"/>	▼
Time Out	<input type="text" value="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

The screenshot displays the 'Access Allowlist' web interface. At the top, there is a header 'Access Allowlist'. Below it, the 'Contacts' section includes a dropdown menu set to 'All Contacts'. A 'Search' section contains an input field, a 'Search' button, and a 'Reset' button. The main part of the interface is a table with the following columns: Index, Name, Phone Number, Account, Floor, and a checkbox. The table contains 10 rows, all of which are currently empty. Below the table is a navigation bar with 'Page 1' (dropdown), 'Prev', 'Next', 'Delete', and 'Delete All' buttons. At the bottom, the 'Contact Setting' section includes input fields for 'Name' and 'Phone Number', and dropdown menus for 'Account' (set to 'Auto') and 'Floor' (set to 'None').

Index	Name	Phone Number	Account	Floor	<input type="checkbox"/>
1					<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Contact Setting

Name:

Account:

Phone Number:

Floor:

Setting:

- **Account:** select the SIP account to be used to call out. This feature 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

The screenshot shows the 'Audio Codecs' configuration interface. It features two main columns: 'Disabled Codecs' on the left and 'Enabled Codecs' on the right. The 'Enabled Codecs' list contains three items: PCMU, PCMA (which is highlighted), and G722. Between the columns are two buttons: '>>' and '<<'. To the right of the 'Enabled Codecs' list are two buttons: an upward arrow and a downward arrow.

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

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

The screenshot shows the 'Video Codec' configuration interface. It includes a checked checkbox for 'H264'. Below this are three dropdown menus: 'Resolution' set to '4CIF', 'Bitrate' set to '2048', and 'Payload' set to '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

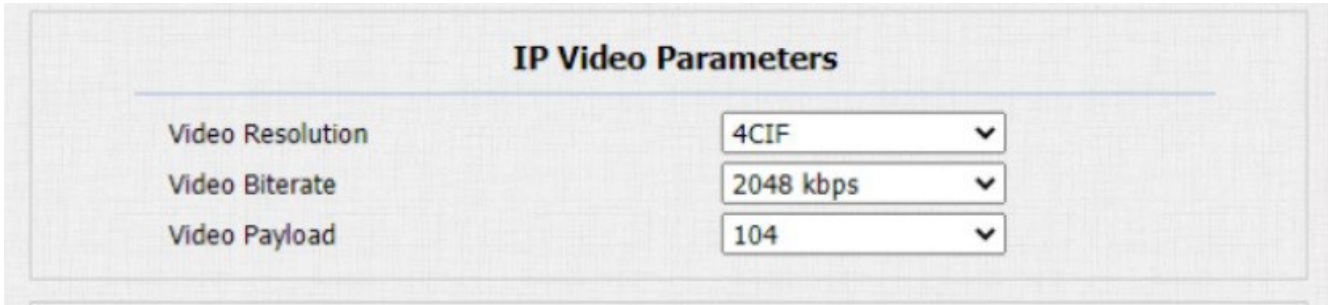


Table A17 - MyBell IP 1-button Station - Video codec configuration for IP direct calls

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 kbps.
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

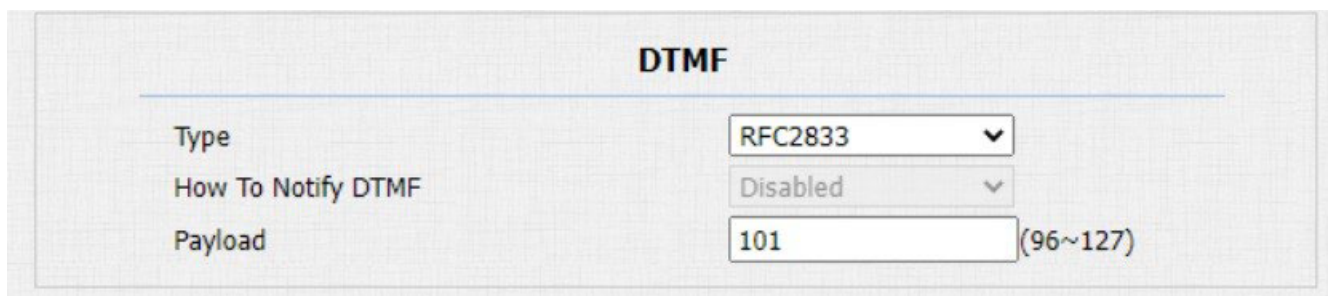


Table A18 - MyBell IP 1-button Station - DTMF data transmission configuration

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 needs 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 DOOR ACCESS CONFIGURATION

13.1 - Relay switch configuration

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

Intercom > Relay

Relay

Relay ID	<input type="text" value="RelayA"/>	<input type="text" value="RelayB"/>
Type	<input type="text" value="Default state"/>	<input type="text" value="Default state"/>
Mode	<input type="text" value="Monostable"/>	<input type="text" value="Monostable"/>
Trigger Delay(Sec)	<input type="text" value="0"/>	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="3"/>	<input type="text" value="3"/>
DTMF Mode	<input type="text" value="1 Digit DTMF"/>	
1 Digit DTMF	<input type="text" value="0"/>	<input type="text" value="1"/>
2~4 Digits DTMF	<input type="text" value="010"/>	<input type="text" value="012"/>
Relay Status	RelayA: Low	RelayB: Low
Relay Name	<input type="text" value="RelayA"/>	<input type="text" value="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	<ul style="list-style-type: none"> • Default State Relay Status: <ul style="list-style-type: none"> • Low – the door is closed. • High – the door is opened. • Invert State Relay Status: <ul style="list-style-type: none"> • High – the door is closed. • Low – the door is opened.
Mode	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• If you don't enter IP address in the IP Address field, enter the complete HTTP command, for exaple: <code>Http://admin:admin@192.168.1.2/state.xml?relayState=2.</code> (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: <code>state.xml?relayState=2.</code>
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

Schedule Enabled

All Schedules

- 1002:Never
- 1001:Always

>>
<<

Enabled Schedules

-

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 schedule by the web interface:

Intercom > Schedules

Schedule Setting

Schedule Type

Schedule Name

Date Range -

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

Date Time : - :

Schedules Management

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	<input type="checkbox"/>
1	1002	Local	Daily	Never	-	-	-	<input type="checkbox"/>
2	1001	Local	Daily	Always	-	-	00:00:00-23:59:59	<input type="checkbox"/>
3								<input type="checkbox"/>
4								<input type="checkbox"/>
5								<input type="checkbox"/>
6								<input type="checkbox"/>
7								<input type="checkbox"/>
8								<input type="checkbox"/>
9								<input type="checkbox"/>
10								<input type="checkbox"/>

Page

Settings:

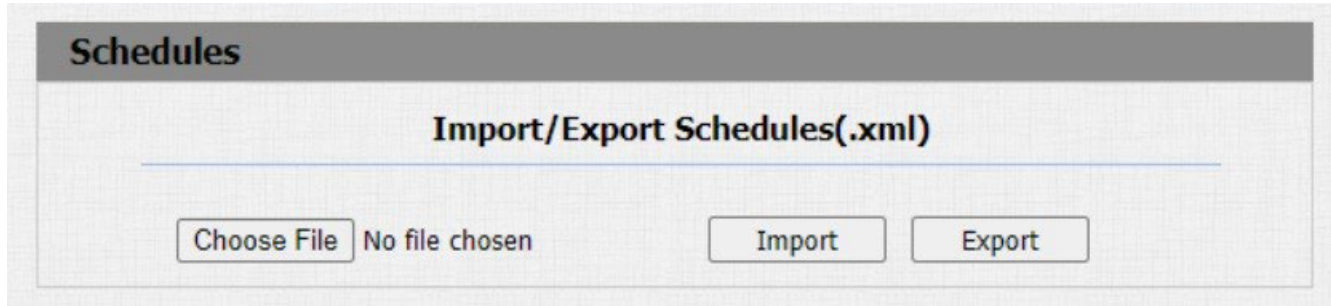
- **Schedule Type:** choose from the three types: **Daily**, **Weekly**, and **Normal**. The default type is **Daily**.
- **Date Range:** set the corresponding date. This configuration is only displayed when the **Normal** type is selected.

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 schedule by the web interface:

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



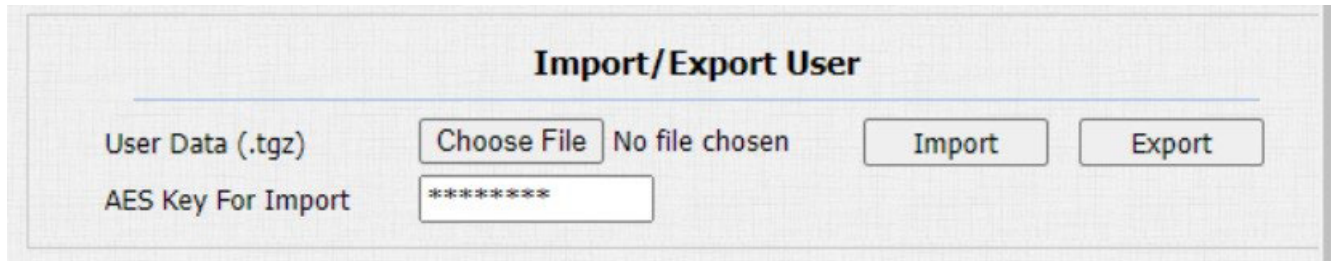
The screenshot shows a web interface titled "Schedules" with a sub-section "Import/Export Schedules(.xml)". Below the title, there is a "Choose File" button followed by the text "No file chosen". To the right of this are two buttons: "Import" and "Export".

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



The screenshot shows a web interface titled "User" with a sub-section "Import/Export User". Below the title, there is a "Choose File" button followed by the text "No file chosen". To the right of this are two buttons: "Import" and "Export". Below these are two labels: "User Data (.tgz)" and "AES Key For Import". The "AES Key For Import" label is followed by a text input field containing a series of asterisks (*****).

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: [dropdown]

ID Card Display Mode: [dropdown]

Contactless S

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

<input type="checkbox"/> Index	Source	User ID	Name	RF Card	Floor No.	Web R elay	Schedule-Rela y	Edit
<input type="checkbox"/> 1								
<input type="checkbox"/> 2								
<input type="checkbox"/> 3								

User

User Basic

User ID

Name

Role

RF Card

Code

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 Defare 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 /

Block Key

Settings:

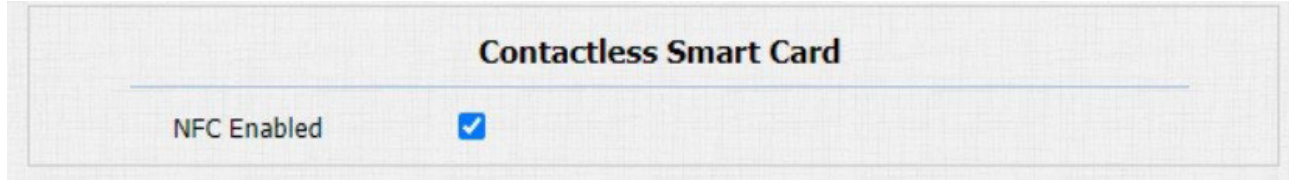
- **Sector/Block:** enter the sector and block that you want the card number to be written into for the Mifare/Defire card. For example, you can write the card number into sector 3 and block 3 in the card.
- **Block Key:** enter the block password for access.

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



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



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/cgi/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	<input type="checkbox"/>
Trigger Electrical Level	<input type="text" value="Low"/>
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call
HTTP URL	<input style="width: 100%;" type="text"/>
Action Delay	<input type="text" value="0"/> (0~300 Sec)
Execute Relay	<input type="text" value="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

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

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

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				<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

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. <ul style="list-style-type: none"> • Auto value – the uploaded certificate is displayed in numeric order. • Value from 1 to 10 – the uploaded certificate is displayed according to the selected value.
Select File	Click Choose file to browse the local drive, and locate the desired certificate (.pem files only).
Only Accept Trusted Certificates	<ul style="list-style-type: none"> • 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	<input style="width: 90%;" type="text"/>
Receiver's Email Address	<input style="width: 90%;" type="text"/>
SMTP Server Address	<input style="width: 90%;" type="text"/>
SMTP User Name	<input style="width: 90%;" type="text"/>
SMTP Password	<input style="width: 90%;" type="password" value="*****"/>
Email Subject	<input style="width: 90%;" type="text"/>
Email Content	<input style="width: 90%; height: 40px;" type="text"/>
Email Test	<input type="button" value="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

SIP Caller Name

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	<input type="text" value="192.168.1.18"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

The screenshot shows the 'Input' configuration page. It is divided into two sections: 'Input A' and 'Input B'. Each section has the following fields:

- Input Service:** A dropdown menu set to 'Disabled'.
- Trigger Option:** A dropdown menu set to 'Low'.
- Action to execute:** Radio buttons for FTP, Email, Sip Call, and HTTP, all of which are currently unchecked.
- Http URL:** An empty text input field.
- Action Delay:** A text input field containing '0', with '(0~300Sec)' written next to it.
- Open Relay:** A dropdown menu set to 'None'.
- Door Status:** A label indicating 'DoorA: High' for Input A and 'DoorB: High' for Input B.

At the bottom of the page, there are two buttons: 'Submit' and 'Cancel'.

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

Intercom > Basic > Call Event

The screenshot shows the 'Call Event' configuration page. It has the following fields:

- Action To Execute:** Radio buttons for FTP, Email, and HTTP, all of which are currently unchecked.
- HTTP URL:** An empty text input field.

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

The screenshot shows the 'Encryption' configuration page. It has the following field:

- Voice Encryption(SRTP):** A dropdown menu set to '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.

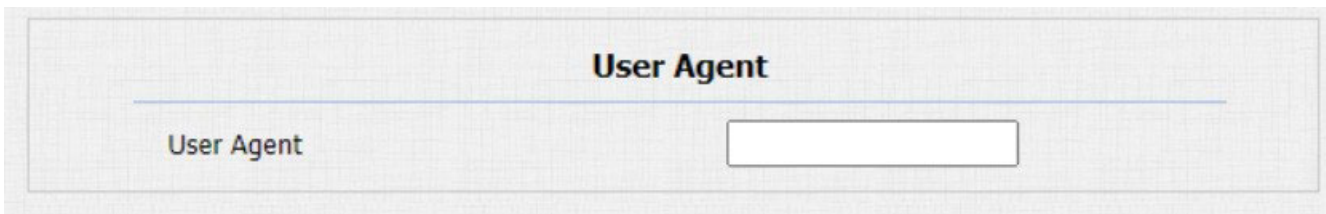
15.7 - User agent

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



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



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 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	CIF
Video Bitrate	VGA
2nd Video Resolution	4CIF
	720P
	1080P

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 kbps.
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 kbps.

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	<input type="checkbox"/>

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 occurs.

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

The image shows two screenshots of a web interface. The top screenshot is titled "RTSP" and "RTSP Basic". It contains the following settings: "Enabled" (checked), "RTSP Authorization Enabled" (unchecked), "MJPEG Authorization Enabled" (unchecked), "Authentication Mode" (Basic), "User Name" (admin), and "Password" (masked with asterisks). The bottom screenshot is titled "MJPEG Video Parameters" and contains the following settings: "Enabled" (checked), "Video Resolution" (VGA), "Video Framerate" (30 fps), and "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: <ul style="list-style-type: none">• 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	<input checked="" type="checkbox"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

Settings:

- **Discoverable:** select to enable other devices to search the video from the door phone camera.
- **Password:** enter the password. The default password is **admin**.

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

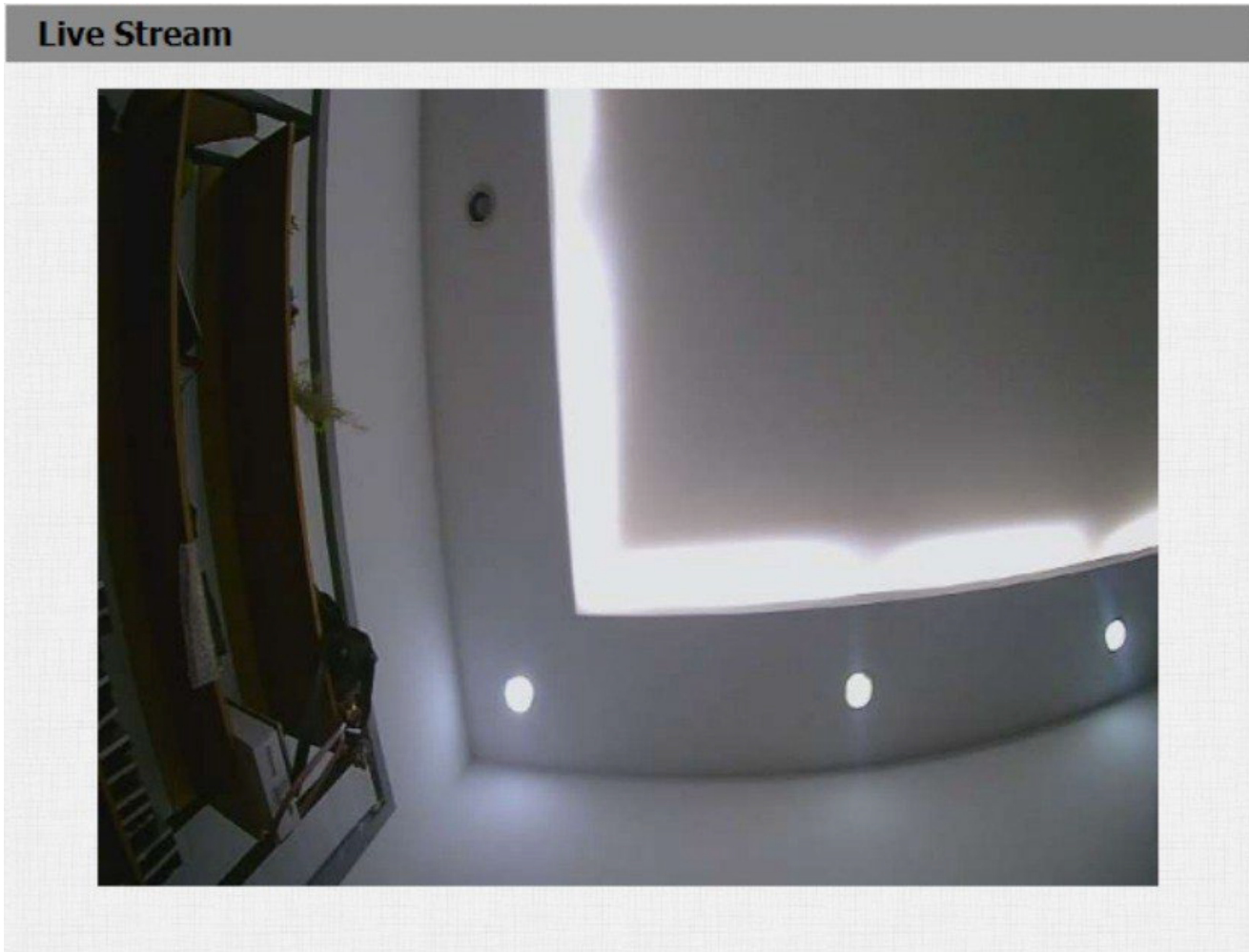
For example: **http://IP address:80/onvif/device_service**.

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, including 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 -

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@192.168.1.119:5060

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 -

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

Page 1 Prev Next Delete Delete All

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	<input type="button" value="Choose File"/> No file chosen
	Reset: <input type="checkbox"/>
	<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Reset"/>
Reboot	<input type="button" value="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

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

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.

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

Upgrade > Advanced > Others

Others

Config File(.tgz/.conf/.cfg)

Choose File	No file chosen
Export	(Encrypted)
Import	Cancel

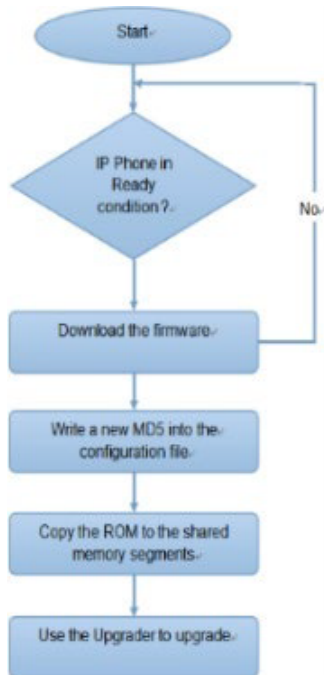
21 AUTO-PROVISIONING THROUGH CONFIGURATION FILE

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:



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.

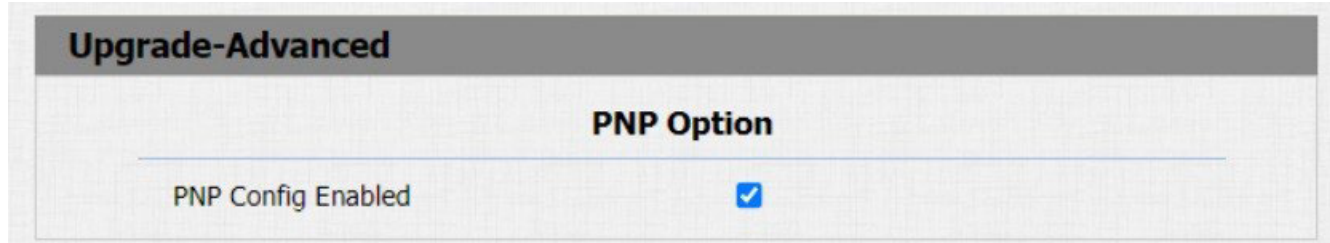
- **Schedule:** if the **Repeatedly** mode is selected, you can set up the time schedule for the Autop.

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

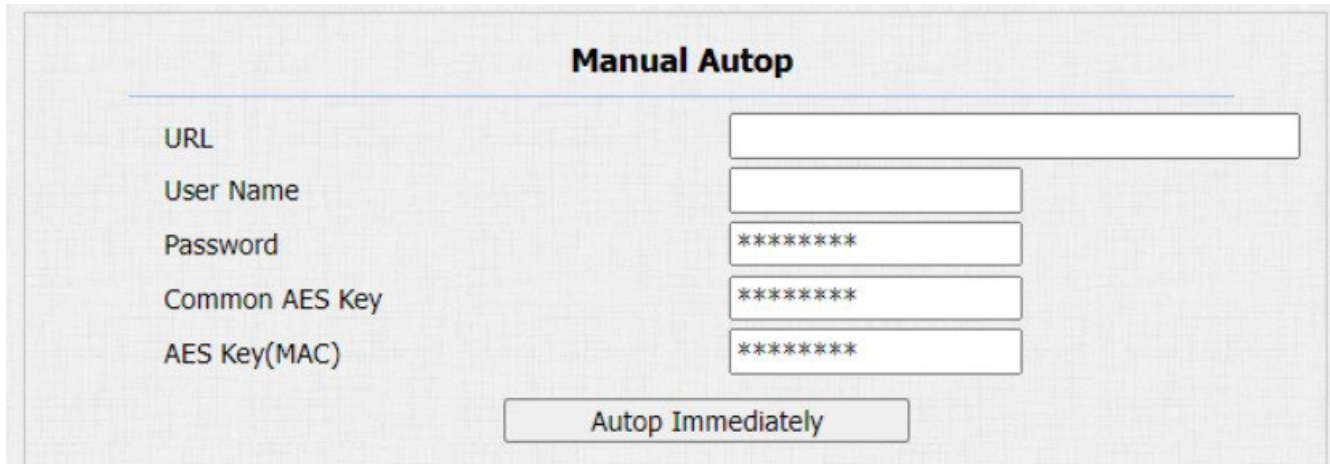
PNP Config Enabled

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)

Autop Immediately

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 access the server, otherwise leave it blank.
Password	Set up a password if it is required to access the server, otherwise leave it blank.
Common AES Key	Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
AES Key (MAC)	Set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

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

22 INTEGRATION WITH THIRD PARTY DEVICE

22.1 - Wiegand integration

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

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: <ul style="list-style-type: none">• Input – door phone is used as a receiver.• Output – Wiegand output is converted to card number before it is sent from the door phone to the receiver. 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	<input checked="" type="checkbox"/>
Authorization Mode	Digest ▼
User Name	admin
Password	*****
1st IP	<input type="text"/>
2nd IP	<input type="text"/>
3rd IP	<input type="text"/>
4th IP	<input type="text"/>
5th IP	<input type="text"/>

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="HTTAPAPI",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.

The screenshot shows the 'Security-Basic' web interface. At the top, there is a header 'Security-Basic'. Below it, the main title is 'Web Password Modify'. There is a 'User Name' dropdown menu currently set to 'admin' and a 'Change Password' button. Below this, there is a section titled 'Account Status' with a table listing 'admin' and 'user' accounts, each with a checkbox. The 'admin' checkbox is checked, and the 'user' checkbox is unchecked.

The screenshot shows a 'Change Password' dialog box with a yellow header and a close button (X). The text inside reads: 'The password must be at least eight characters long containing one uppercase letter, one lowercase letter and one digit at least'. Below this, there are four input fields: 'User Name' (set to 'user'), 'Old Password', 'New Password', and 'Confirm Password'. At the bottom, there are two buttons: 'Ignore' and 'Change'.

23.2 - Web interface automatic logout configuration

You can set up the web interface automatic log-out time. After this time re-logging 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

The screenshot shows the 'Session Time Out' configuration interface. It has a title 'Session Time Out' and a single input field for 'Session Time Out Value' set to '900', with a range '(60~14400 Sec)' indicated to the right.

Settings:

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

24 SYSTEM REBOOT AND RESET

24.1 - Reboot

To reboot the device system by the web interface:

Upgrade > Basic



24.2 - Reset

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



Part Two

MyBell IP Premium Indoor Monitor

1 IMPORTANT SAFEGUARDS AND WARNINGS

- **⚠ CAUTION!** – Any use other than that specified herein or in environmental conditions other than those stated in this manual is to be considered improper and is strictly forbidden!
 - **⚠ CAUTION!** – Important instructions: keep this manual in a safe place to enable future product maintenance and disposal procedures.
 - **⚠ CAUTION!** – All installation and connection operations must be performed exclusively by suitably qualified and skilled personnel with the unit disconnected from the mains power supply.
 - **⚠ CAUTION!** – This manual contains important instructions and warnings for personal safety. Read carefully all parts of this manual. If in doubt, suspend installation immediately and contact Nice Technical Assistance.
-
- The product packaging materials must be disposed of in full compliance with local regulations.
 - Never apply modifications to any part of the device. Operations other than those specified can cause malfunctions. The manufacturer declines all liability for damage caused by makeshift modifications to the product.
 - Never place the device near the sources of heat or expose to naked flames. These actions can damage the product and cause malfunctions.
 - This product isn't intended for use by people (including children) with reduced physical, sensory or mental capabilities or who lack experience and knowledge, unless they are supervised by a person responsible for their safety.
 - This product isn't a toy. Keep away from children and animals!
 - The device is designed to operate in an electrical home installation. Faulty connection or use can result in a fire or electric shock.
 - Even when the device is turned off, voltage can be present at its terminals. Any maintenance introducing changes to the configuration of connections or the load must be always performed with a disabled fuse.
 - Don't use in damp or wet locations, near a bathtub, sink, shower, swimming pool, or anywhere else where water or moisture are present.

2 DEVICE DESCRIPTION

The MyBell IP Premium Indoor Monitor with an Android 12 operating system, provides an unparalleled audio-visual intercom experience with four high level speakers. Automatically adjusts screen brightness through environment sensing, voice assistant and Voice Changer to bring convenience and safety to your home.

Table A1 - MyBell IP Premium Indoor Monitor - Device description

Feature	Description
CPU	CPU Quad Cortex-A55/1.8 GHz
Operation System	Android 12
Color	black
RAM	4 GB
ROM	16 GB
Front Panel	plastic
Wi-Fi	IEEE802.11 b/g/n/ax
Ethernet	1xRJ45, 10/100 Mbps, adaptive
Bluetooth	5.0
Power over Ethernet (PoE)	802.3af
Power Supply	12 V DC / 1.5 A
RS485 Port	1
Alarm Input	8
Relay Output	2 x relay out (NO/COM/NC)
Bell in	1
Microphone	dual microphone, -26 dB
Speaker	quad speakers, 8 Ω / 2 W
Installation	wall-mounted & desktop
Dimensions	278.51 x 165.11 x 22.8 mm
Working Humidity	10~90%
Working Temperature	-10°C ~ +45°C
Storage Temperature	-20°C ~ +70°C
Touch Screen Display Mode	normally black, transmissive
Display	10-inch (254 mm) IPS LCD
Screen	10-inch capacitive touch screen
Screen Resolution	1280 x 8000
Screen Contrast Ratio	900:1
Luminance	290 cd/m ²
Viewing Angle	80° left, 80° right, 80° upper, 80° lower
Audio	SIP v1 (RFC2543), SIP v2 (RFC3261)
Audio Codecs	iLBC_13_3, iLBC_15_2, L16, PCMU, PCMA, G729, G722
DTMF	in-band, out-of-band DTMF (RFC2833), SIP Info
Echo Cancellation	yes

Table A1 - MyBell IP Premium Indoor Monitor - Device description

Feature	Description
Voice Activation Detection	yes
Comfort Noise Generator	yes
Automatic Gain Control	yes
Video Streaming Formats	VP8, H.263, H.264, H.265
Supported Networking Protocols	DHCP, PNP, TFTP, FTP, HTTPS
Auto-Provisioning	yes
Web Management Portal	yes
Web-based Packet Dump	yes
Configuration Backup / Restore	yes
Firmware Upgrade	yes
System Logs (including door access logs)	yes
Tamper Resistant	support
Voice Pickup Distance	up to 5 metres
Voice Recognition Accuracy	up to 95%
Privacy Protection with Native Voice Data	yes
Support English	yes
Application Scenario	villas, apartment complexes, home automation systems, modern interiors



3 INTRODUCTION TO CONFIGURATION MENU

3.1 - Configuration menu

Section	Description
Status	Basic information such as product information, network information, and account information.
Account	SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, NAT and User Agent.
Network	DHCP & Static IP settings, RTP port setting, and device deployment.
Device	Settings of time, language, call feature, NTP, multicast, display, audio, multicast, relay, third- party APP, intercom, relay monitor.
Contacts	Configuration of the local contact list stored in the device and checking the logs.
Upgrade	Firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.
Security	Password modification, account status & session time out configuration, client certificate and service location switching.
Settings	RTSP setting, wake up the device and brightness adaptation functions.
Arming	Configuration including arming zone setting, arming mode, disarm code, and alarm action.
PBX	Creating SIP numbers and managing SIP account settings.

3.2 - Mode selection

Mode	Description
Discovery Mode	It's a plug and play configuration mode. MyBell devices configure themselves automatically when powered on and connected to the network. It saves time and reduces manual operations. No prior configurations are required.
Cloud Mode	Yubii Home is an all-in-one mobile management system. It enables audio, video, and remote access control between smartphones and MyBell intercoms. All configurations in the device are issued automatically from the cloud. If you decide to use Yubii Home, please contact technical support to help configure the related settings.
SDMC Mode	SDMC (SIP Device Management Controller) is a comprehensive software for building management. It provides topography for community and a graphic configuration interface for door access, intercom, monitoring, and alarm. It allows property managers to manage, operate, and maintain the community.

3.3 - Tool selection

The table below lists some common MyBell configuration tools. If needed, contact your administrator to get a tool.

Mode	Description
SDMC	Manage the devices in large communities, including access control, resident information and remote device control.
Upgrade	Upgrade the devices in batch on a LAN (Local Area Network).
PC Manager	Distribute all configuration items in batch on a LAN.
IP Scanner	Search the device IP addresses on a LAN.
FacePro	Manage face data in batch for the door phone on a LAN.

4 INDICATOR LIGHT STATUS

The indicator light is on the right side of the device. It shows the different status of the device.



Table A5 - MyBell IP Premium Indoor Monitor - Indicator light status

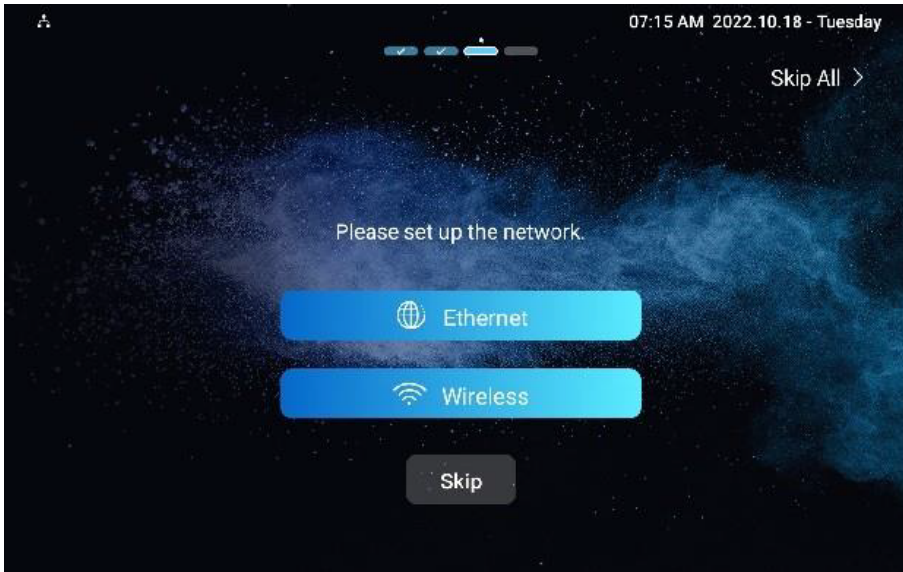
Indicator name	Color	Status	Description
Power	blue	ON	System is working.
		OFF	System isn't working.
System Status	blue	ON	System is working.
Device Booting	purple	ON	The device is powered on and booting.
Network	red	flashing	Failed to obtain IP address.
Incoming Call	blue	flashing	Receiving an incoming call.
Outgoing Call	blue	flashing	Making an outgoing call.
In a Call	blue	ON	During a call.
End a Call	blue	ON	End a call.
Miss a Call	purple	ON	Missed a call.
Message	purple	ON	There's an unread message.
Screen/System	N/A	OFF	<ul style="list-style-type: none"> Screen is turned off. Device is turned off.
Alarm	red	flashing	<ul style="list-style-type: none"> An alarm is triggered.
Voice Assistant	blue	ON	Waking up voice assistant.
Door Bell	blue	flashing	Door bell rings.
Device Upgrade	red	ON	Upgrading the device
Reset	red	ON	Resetting the device to factory setting.

5 ACCESS TO DEVICE

You can access the device system settings either on the device directly or by the device web interface.

5.1 - Device start-up network selection

When the device boots up initially, you need to select Ethernet or wireless network connection for the device.

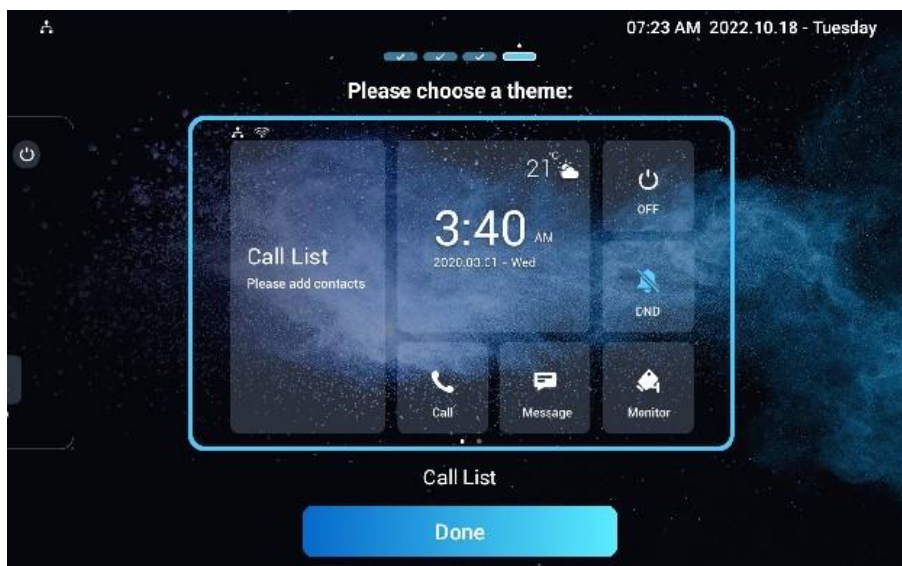
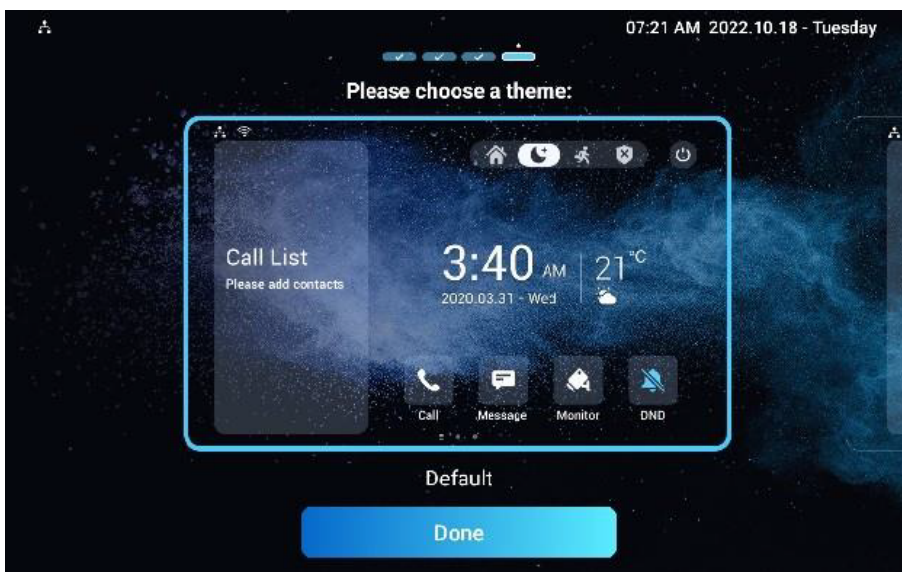


Note

Refer to the chapter on **Network Setting & Other connection** for the configuration of the Ethernet and wireless network connections.

5.2 - Device home screen type selection


The device supports two different home screen display modes: **Default** and **Call List**. Choose the mode suitable for your scenarios.

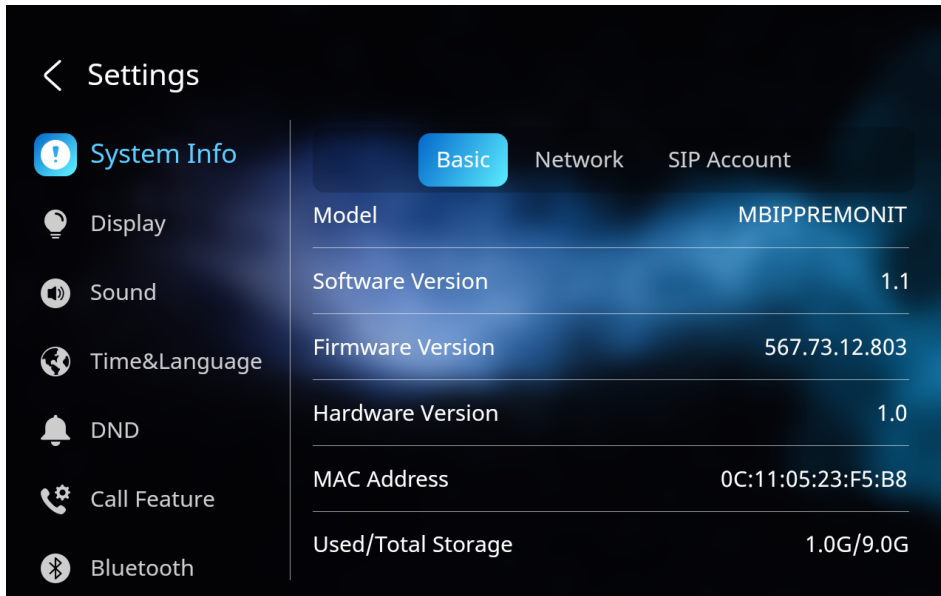


5.3 - Access to device settings on device

You can access the device basic setting and advanced setting to configure different types of functions as needed.

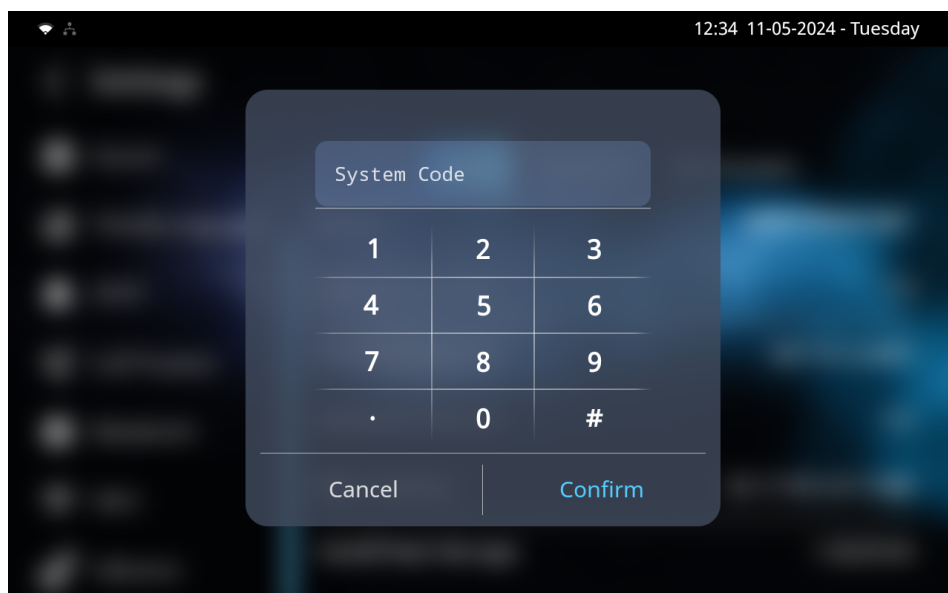
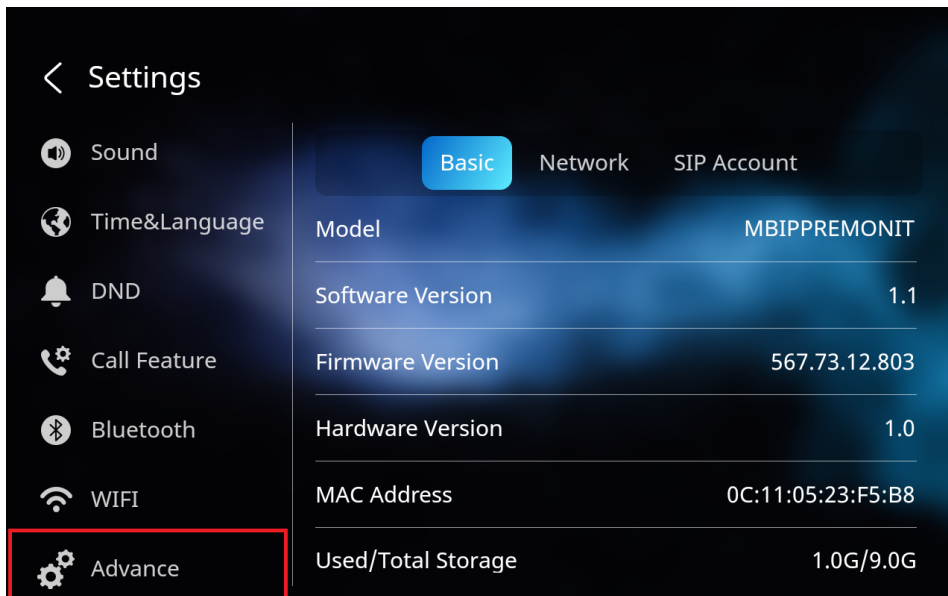
5.3.1 - Access to device basic settings

To access the device basic settings swipe your finger left on the home screen, then tap **Settings** icon . You can check basic information such as MAC and firmware.



5.3.2 - Access to device advanced settings

To access the device advanced settings, press **Settings**, then tap **Advanced Settings** icon and enter the password: **123456**.



5.4 - Access to device settings by web interface

You can enter the device IP address in the web browser to log into the device web interface and configure settings. The default username and password are **admin/admin**.

To check the IP address:

Settings > System Info > Network screen.

You can also search the device by IP scanner, it can search all the devices on the same LAN.

Note

- You can also obtain the device IP address using the IP scanner to log in the device web interface.
- Google Chrome browser is strongly recommended.
- The default username and password are **admin/admin**. Make sure to enter them in correct case.

6 LANGUAGE AND TIME CONFIGURATION

6.1 - Language configuration

When you first set up the device, you can choose the preferred language. That can be done directly on the device or by the device web interface. The language can later be changed.

6.1.1 - Language configuration on device

To choose the preferred language:

Settings > Time & Language.

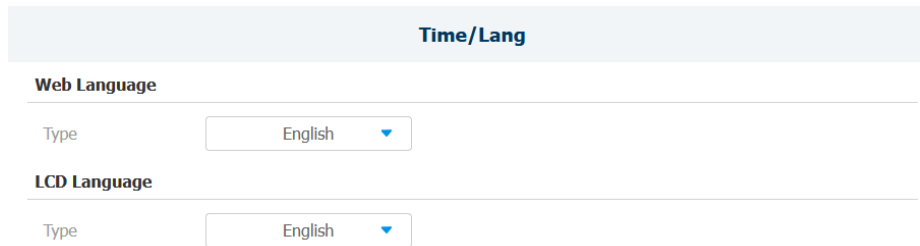


6.1.2 - Language configuration by web interface

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

To configure the language display by the web interface:

Device > Time/Lang.



6.2 - Time configuration

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

6.2.1 - Time configuration on device

To configure time on the device:

Settings > Time & Language.

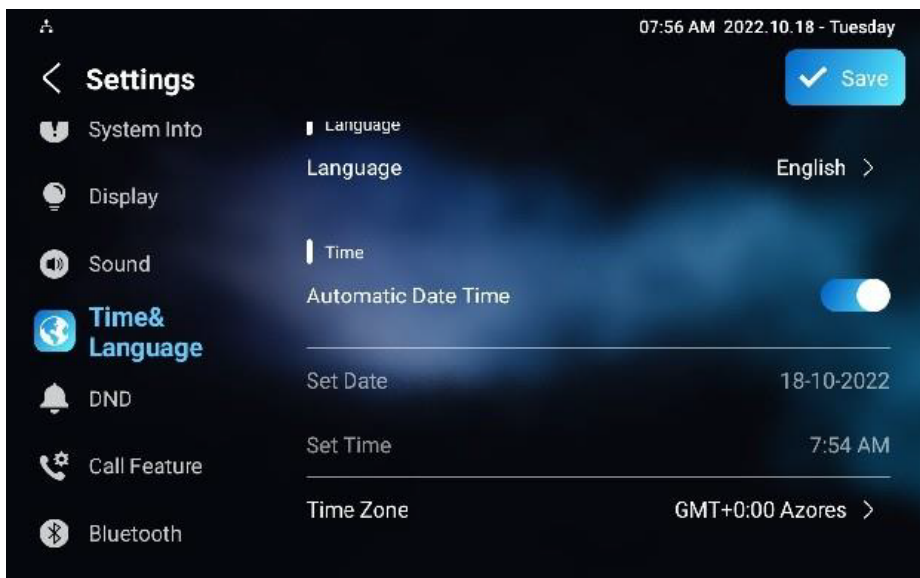


Table A6 - MyBell IP Premium Indoor Monitor - Time configuration on device

Setting	Description
Automatic Date & Time	Automatic date function is switched on by default, allowing the date and time to be automatically set and synchronized with the default time zone and the NTP server (Network Time Protocol). To set it up manually switch off the automatic date, then enter the date and time, and press the Save tab to save the setting.
Time Zone	Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
Date Format	Select the date format from the following options: Y-M-D , Y/M/D , D-M-Y , D/M/Y , M-D-Y , and M/D/Y .
Time Format	Select the 12-hour or 24-hour time format.
NTP Server	Enter the obtained NTP server in the NTP server field. NTP server 2 is the backup server.

6.2.2 - Time configuration by device web interface

To set the time by the device web interface:

Device > Time.

This option also allows you to set up the obtained NTP server address to automatically synchronize the time and date. When the time zone is selected, the device automatically notifies the NTP server and the NTP server can synchronize the time zone setting in the device.

Time Setting ?

Automatic Date&Time ?

Time Format ?

Date Format ?

Date ?

Time ?

Time Zone ?

NTP ?

Preferred Server ?

Secondary Server ?

Table A7 - MyBell IP Premium Indoor Monitor - Time configuration by web interface

Setting	Description
Preferred Server	Enter the obtained NTP server address in the NTP server field .
Secondary Server	Enter the back up server address. In case of the main NTP server failure, it changes to the back up server automatically.

7 SCREEN DISPLAY CONFIGURATION

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

7.1 - Screen display configuration on device

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

To configure screen display on the device:

Settings > Display.

Note

You can't adjust the screen brightness manually if the brightness adaptation is enabled.

Setting	Description
Brightness	Press the brightness setting and move the yellow dot to adjust the screen brightness. The default brightness is 145 .
Sleep Time	Set the sleep time based on the screen saver. The time range is from 15 seconds to 30 minutes. <ul style="list-style-type: none"> • If the screen saver is enabled, the sleep time is the screen saver start time. For example, if you set the sleep time to 1 minute, the screen saver starts automatically when there's no operation on the device for 1 min. • If the screen saver is disabled, the sleep time is the screen turn-off time. For example, if you set the sleep time to 1 minute, the screen is turned off automatically when there's no operation on the device for 1 min.
Screen Saver	Tick this checkbox to enable the screen saver function.
Screen Lock	Tick this checkbox to lock the screen after the screen is turned off (turn dark). You are required to enter the system code to unlock the screen or you can unlock the screen using facial recognition.
Screen Saver Type	Select screen saver type <ul style="list-style-type: none"> • Local Pictures: display picture uploaded to the indoor monitor as the screen saver. • Local Videos: display videos uploaded to the indoor monitor as the screen saver. • Clock: display the clock as the screen saver.
Screen Clean	Before you start wiping the screen clean press the Screen Clean feature to avoid unwanted changes in settings while wiping the screen.
Font Size	Select the font size from: Small, Normal, Large, and Huge.
Breathing Light	Move the toggle switch to enable the Breathing Light.
Wallpaper	Select the local wallpaper.
Brightness Adaptation	If enabled, the device adjusts screen brightness automatically to adapt to the ambient brightness.

To enable or disable the brightness adaptation function remotely by the web interface:

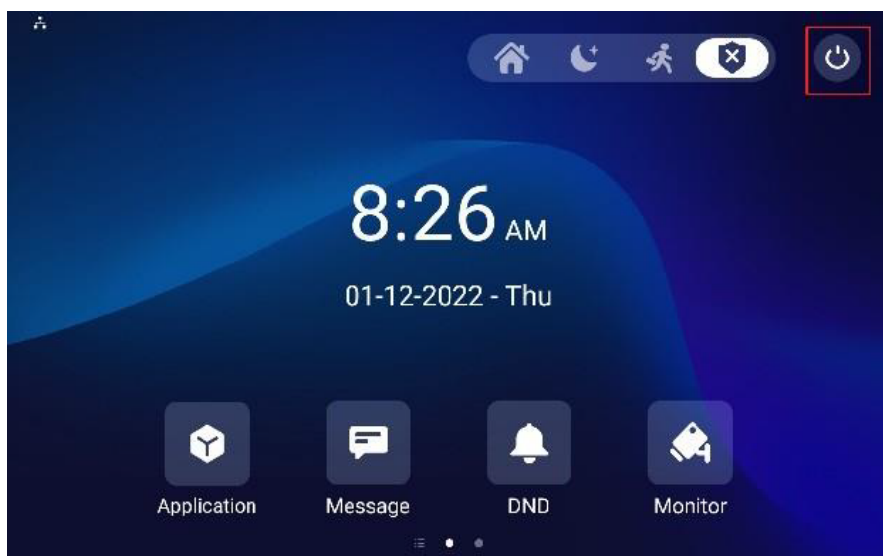
Settings > Basic > Brightness Adaptation.

Brightness Adaptation ?

Brightness Adaptation



You can also turn off the screen manually.



7.2 - Screen display configuration by web interface

7.2.1 - Uploading screen saver

To upload screen saver pictures separately or in batches to the device and the device web interface for public purpose or a greater visual experience:

Device > Display Setting > Screen Saver Setting

Screen Saver Setting ?

Screen Saver Pictures	<input type="button" value="Import"/> ?
Screen Saver Videos	<input type="button" value="Import"/> ?
Picture Files	<input type="text" value="Daydream1.jpg"/> <input type="button" value="Delete"/> ?
Video Files	<input type="text" value=""/> <input type="button" value="Delete"/> ?
Screen Saver Type	<input type="text" value="Local Pictures"/> ?

Note

- The uploaded pictures should be in **JPG, JPEG, or PNG** format, with the maximum size of 2 MB.
- The previous picture with a specific ID order is overwritten in case of repetitive designation of pictures to the same ID order.

7.2.2 - Uploading wallpaper

To customize screen background picture on the device web interface:

Device > Display Setting > Wallpaper.

Wallpaper ?

Wallpaper	<input type="button" value="Import"/> ?
Wallpaper Files	<input type="text" value="7.jpg"/> <input type="button" value="Delete"/> ?

Note

The uploaded pictures should be in **JPG, JPEG, or PNG** format, with the maximum size of 2 MB.

7.3 - Uploading device booting image

You can upload the booting logo, web logo and web homepage logo image. All three types of logos can be customised.

To upload the booting image:

Device > Display Setting > Boot Logo.

Boot Logo ?

Boot Logo	<input type="button" value="Import"/> <input type="button" value="Reset"/> ?
Web Logo	<input type="button" value="Import"/> <input type="button" value="Reset"/> ?
Web Homepage Logo	<input type="button" value="Import"/> <input type="button" value="Reset"/> ?

Table A9 - MyBell IP Premium Indoor Monitor - Booting image configuration

Setting	Description
Boot Logo	Upload the logo appearing on the screen when you reboot the device.
Web Logo	Upload the logo appearing in the upper left corner of the web interface.
Web Homepage Logo	Upload the logo appearing on the login page of the web interface.

Note

The uploaded pictures should be in **PNG** or **ZIP** format.

7.4 - Approach to wake up

You can wake up the device manually by tapping the screen, or automatically by walking up to the device within the preset distance.

To configure this function:

Settings > Basic > Wake Up Device.

Wake Up Device ?

Wake Up Mode	<input type="text" value="Auto"/> ?
Wake Up Distance	<input type="text" value="Short Distance"/> ?

Table A10 - MyBell IP Premium Indoor Monitor - Wake up function configuration

Setting	Description
Wake Up Mode	Select Manual for the manual wake up or Auto for the automatic wake up (approach to wake-up). The default setting is Auto.
Wake Up Distance	Select the approach to wake-up distance: <ul style="list-style-type: none"> • short distance – 50 cm. • long distance – 80 cm.

7.5 - Icon screen display configuration

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

To customize icon display:

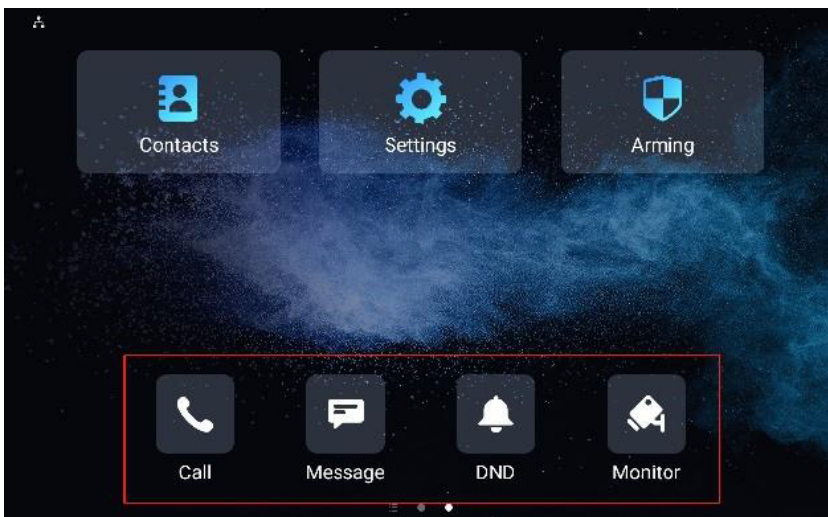
Device > Display Setting > Home Page Display.

Home Page Display ? Example

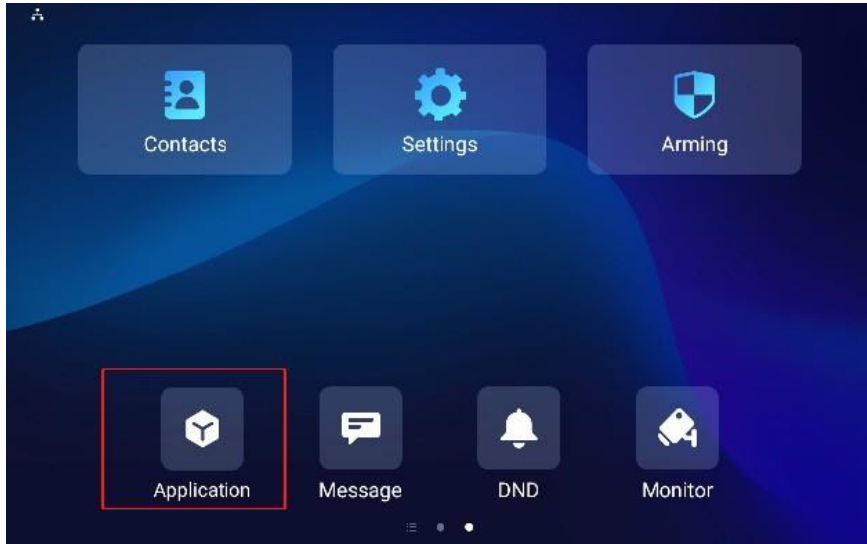
Area	Type	Value	Label	Icon(max size:100*100)
Area1	<input type="text" value="Call"/>	<input type="text"/>	<input type="text"/>	Not selected any files <input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area2	<input type="text" value="Message"/>	<input type="text"/>	<input type="text"/>	Not selected any files <input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area3	<input type="text" value="DND"/>	<input type="text"/>	<input type="text"/>	
Area4	<input type="text" value="Monitor"/>	<input type="text"/>	<input type="text"/>	Not selected any files <input type="button" value="Select File"/> <input type="button" value="Delete"/>

Table A11 - MyBell IP Premium Indoor Monitor - Icon screen display configuration

Setting	Description
Type	Select the functional icon you want to place on the home page (DND, Message, Contact, Call, System Info, Settings, Arming, SOS, Browser, Custom APK, Monitor, Relays, Unlock, All Calls, Unlock, Application).
Value	If you select the icon type, select the value. The value field for Custom APK fills in automatically if you have already installed a third-party app. If you select Browser , you are required to enter the URL of the browser before the browser icon is displayed.
Label	The icon can be renamed if needed. The DND can't be renamed.
Icons	Click to upload the icon picture. The maximum icon size is 100x100 . The picture format can be JPG, JPEG, and PNG . See the four icons on the home screen below.



To allow users to easily access the third-party App you installed, you can create an Application icon. Users can tap the icon to select and run the chosen app.



To configure the **More Icon Display** on **More Page Display** using the same interface, see the image below:

More Page Display Example

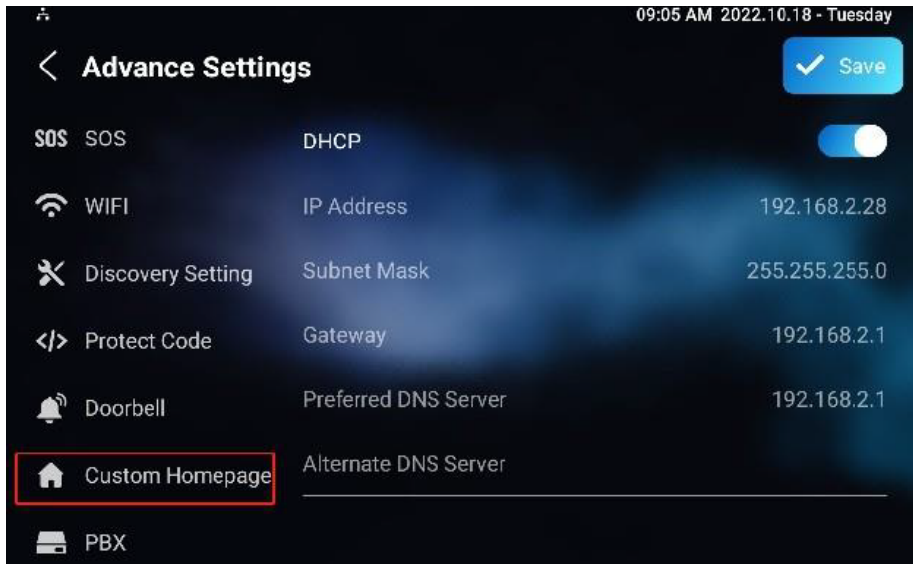
Area	Type	Value	Label	Icon(max size:100*100)
Area1	Contacts			Not selected any files Select File Delete
Area2	Settings			Not selected any files Select File Delete
Area3	Arming			Not selected any files Select File Delete
Area4	NA			Not selected any files Select File Delete
Area5	NA			Not selected any files Select File Delete
Area6	NA			Not selected any files Select File Delete

You can also customize the homepage display by selecting your favorite functions, which are displayed on the home screen.

To configure it:

Setting > Advanced Settings.

Then enter the default system code **123456**, tap **Custom Homepage**, then tap any icon before selecting your favorite function.



7.6 - Unlock Tab configuration

7.6.1 - Unlock Tab configuration on Talking Screen

You can customize your unlock tab on a different screen for door opening. You can also select the relay type for the door opening. To configure unlock tab on the Talking Screen:

Device > Relay > SoftKey In Talking Page.

SoftKey In Talking Page 

Key	Status	Display Name	Type
Key1	Enabled	Unlock1	Local Relay
Key2	Enabled	Unlock2	1
Key3	Enabled	Unlock3	Remote Relay DTMF1


Table A12 - MyBell IP Premium Indoor Monitor - Unlock Tab configuration on Talking Screen

Setting	Description
Status	Enable the unlock tabs on the talking screen. You can see the unlock tabs during a call.
Display Name	Name the unlock tab.
Type	Select the relay and the relay trigger type to be activated by the unlock tab (Local Relay, Remote Relay HTTP, Remote Relay DTMF, Web Relay Actions).

7.6.2 - Unlock Tab configuration on Home and More Screen

Scroll down to configure the **Unlock Tab** on the **Home Screen** and **More Screen**:

Device > Relay > SoftKey In Home or More Screen.

SoftKey In Home Or More Page 

Status	Display Name	Type
Enabled	Unlock	Remote Relay HTTP1

Table A13 - MyBell IP Premium Indoor Monitor - Unlock Tab configuration on Home and More Screen

Setting	Description
Status	Enable the unlock tabs on the screen. You can see the unlock tabs during a call.
Display Name	Name the unlock tab.
Type	Select the relay and the relay trigger type to be activated by the unlock tab (Remote Relay HTTP).

7.6.3 - Unlock Tab configuration on Monitor Screen

To configure the Unlock Tab on the Monitor Screen:

SoftKey In Monitor Page 

Status	Display Name	Type
Enabled	Unlock	Remote Relay HTTP

Table A14 - MyBell IP Premium Indoor Monitor - Unlock Tab configuration on Monitor Screen

Setting	Description
Status	Enable the unlock tabs on the screen. You can see the unlock tabs on the monitoring screen.
Display name	Name the unlock tab.
Type	Select the relay and the relay trigger type to be activated by the unlock tab (Remote Relay HTTP, Local Relay, Web Relay Action).

7.6.4 - Unlock Tab configuration on Call Preview Screen

To configure the **Unlock Tab** on the **Call Preview Screen**:

SoftKey In Call-Preview Page 

Status	Display Name	Type
Enabled 	Unlock	Remote Relay HTTP 


Table A15 - MyBell IP Premium Indoor Monitor - Unlock Tab configuration on Call Preview Screen



Setting	Description
Status	Enable the unlock tabs on the screen. You can see the unlock tabs on the call preview screen.
Display name	Name the unlock tab.
Type	Select the relay and the relay trigger type to be activated by the unlock tab (Remote Relay HTTP, Local Relay, Web Relay Action).

7.7 - Home screen display

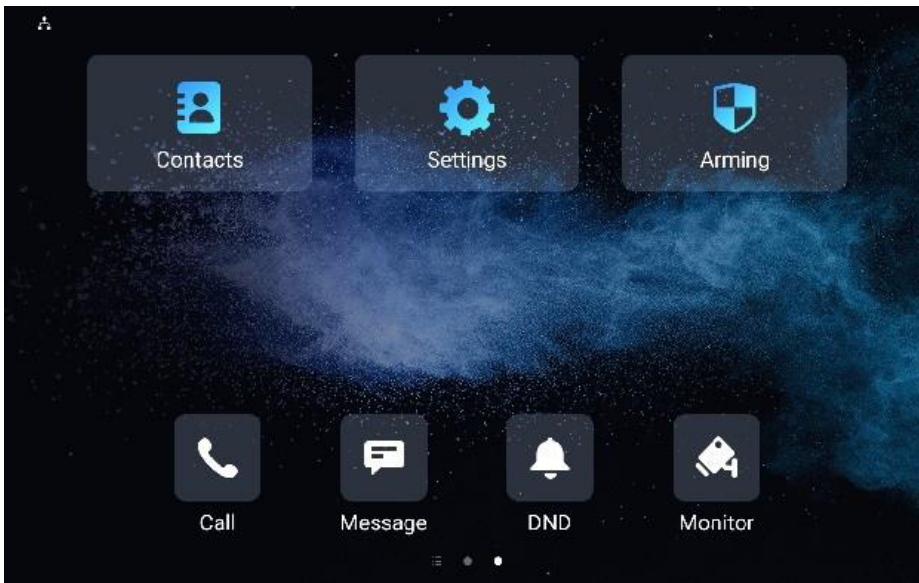
To select the default or call list home screen display:

Device > Display Setting > Theme.

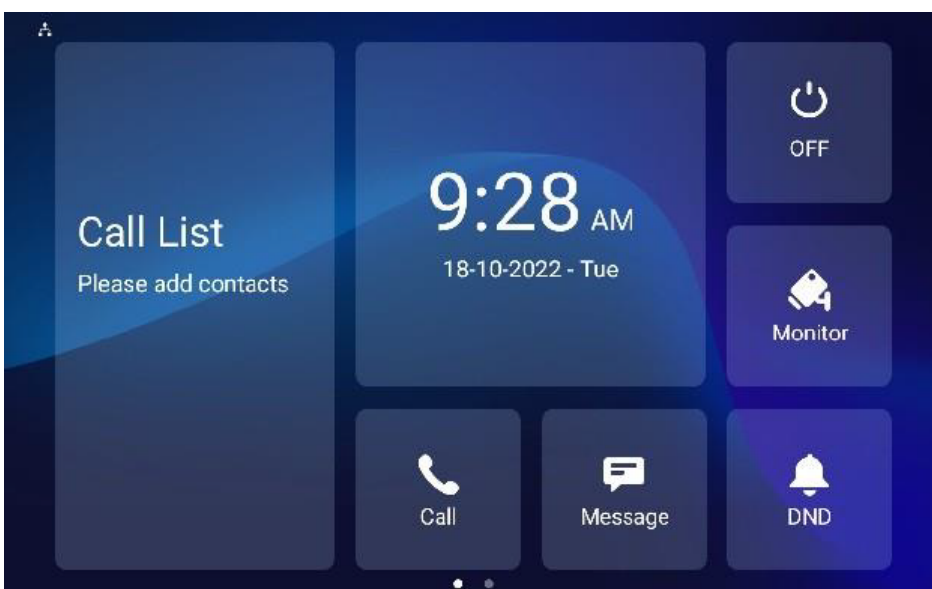
Theme 

Theme Default  

Default Home Screen:



Call List Home Screen:



8 SOUND AND VOLUME CONFIGURATION

8.1 - Volume configuration

8.1.1 - Volume configuration on device

To configure volume on the device:

Settings > Sound.



Table A16 - MyBell IP Premium Indoor Monitor - Volume configuration on device

Setting	Description
Ring Volume	Adjust the incoming call ringtone volume.
Call Volume	Adjust the speaker volume during a call.
Mic Volume	Adjust the microphone volume.
Media Volume	Adjust the video screen saver volume.
Touch Sound	Adjust the icon tapping sound.
Phone Ringtone	Select the incoming calls ringtone.
Notification Sound	Select the incoming messages ringtone.

8.1.2 - Volume configuration by web interface

To configure the volumes and tones and customize the doorbell sound and alarm ringtone by the device web interface:

Device > Audio > Volume Control.

Volume Control ?

Ring Volume	<input type="text" value="10"/>	(0-15) ?
Call Volume	<input type="text" value="10"/>	(1-15) ?
Mic Volume	<input type="text" value="1"/>	(1-15) ?
Media Volume	<input type="text" value="10"/>	(0-15) ?

Touch Sound ⓘ

Touch Sound Enabled ⓘ

Doorbell Sound Upload ⓘ

Doorbell Sound Upload ⓘ

Doorbell Sound ⓘ

Alarm Ringtone Upload ⓘ

Alarm Ringtone Upload ⓘ

Alarm Ringtone ⓘ

Note
 Doorbell sound files and Alarm Ringtone files must be in **WAV** or **MP3** format. There is no size limit for the file.

8.2 - Doorbell sound configuration

You can also configure the doorbell sound and select the local relay to be triggered along with the doorbell.



Table A17 - MyBell IP Premium Indoor Monitor - Doorbell sound configuration	
Setting	Description
Doorbell Sound	Select your doorbell sound.
Doorbell Timeout	Set doorbell duration (from 10 s to 5 min). Select the local relay you want to trigger along with the doorbell. You can select None if you don't want to trigger any relay.
Relay	Select the local relay you want to be triggered along with the doorbell. You can select None if you don't want to trigger any relay.

9.1 - Phone book configuration on device

To configure the contacts by adding and modifying contact groups or contacts on the device:

Contacts > Local Contacts.

9.1.1 - Adding contacts

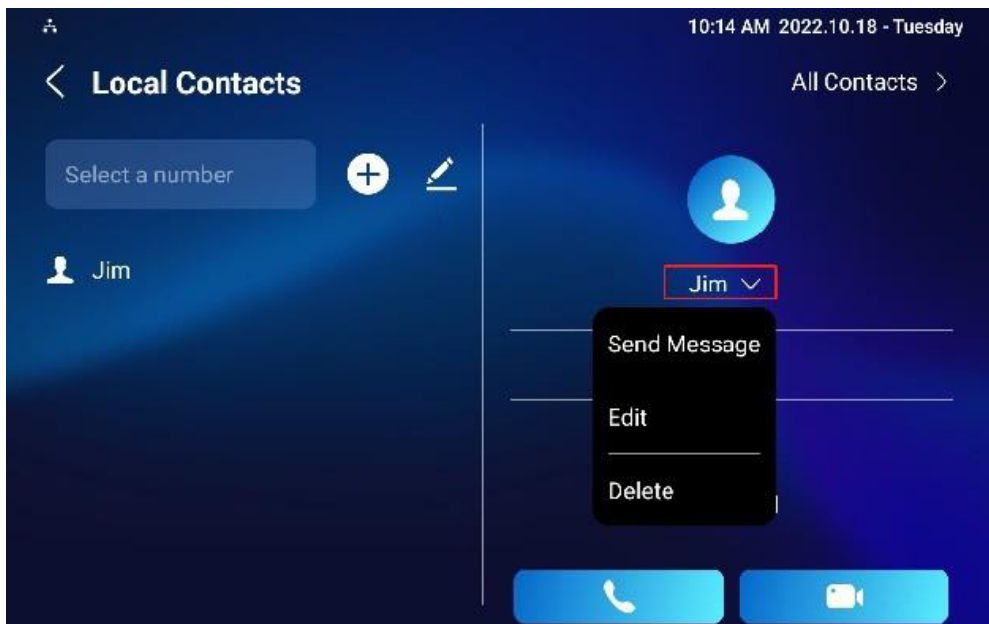
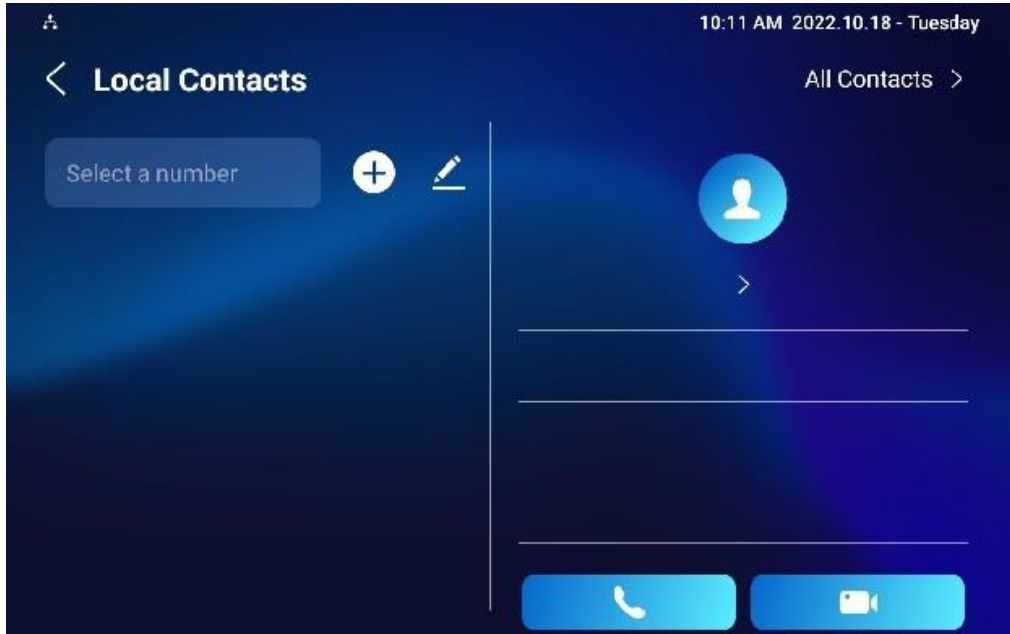


Table A18 - MyBell IP Premium Indoor Monitor - Adding contacts on device

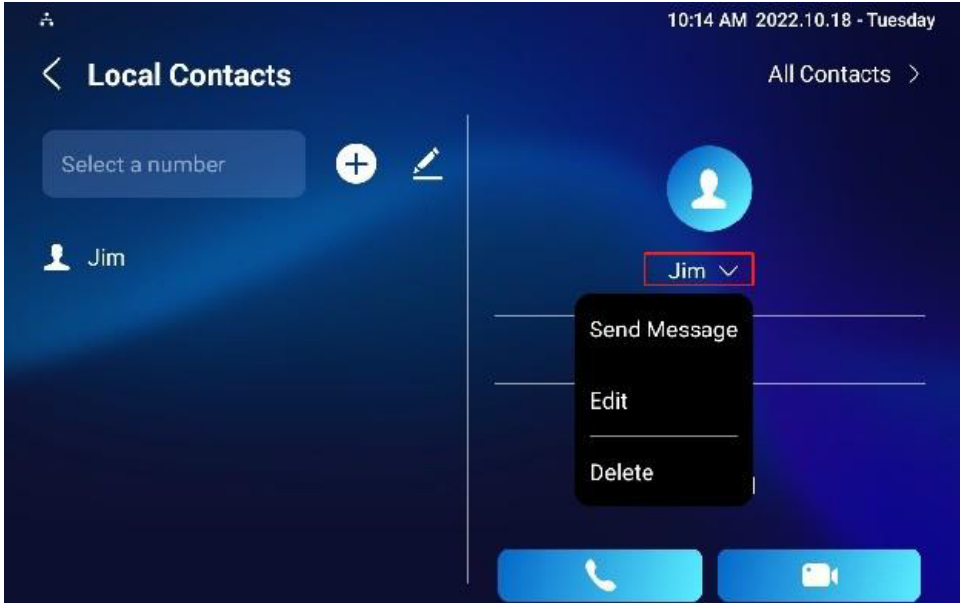
Field	Description
Account1	Select which account to use to dial out – Account 1 or Account 2.
New Contact Name	Enter the name to save.
Number	Enter the IP or SIP number to save.
CameraUrl	Enter the RTSP URL for video preview.
Auto Ringtone	Select the phone ringtone for incoming calls.

Note

The devices RTSP URL format is `rtsp://device IP/live/ch00_0`. If you use a third-party device, please confirm the URL format with their company.

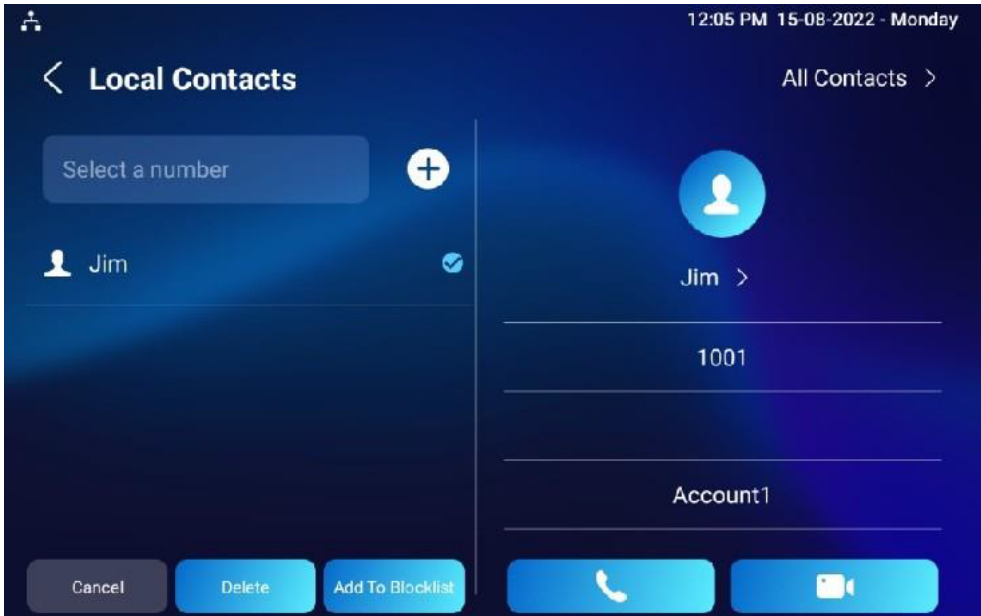
9.1.2 - Editing contacts

To check and edit the contacts in the phonebook list choose one contact and click **Edit** to modify.



9.1.3 - Blocklist setting on device

From the contact list you can choose the contact you want to add to the blocklist. Incoming calls from the contacts in the blocklist are rejected.



Note

You can delete contacts from the All Contacts screen and the Blocklist screen.

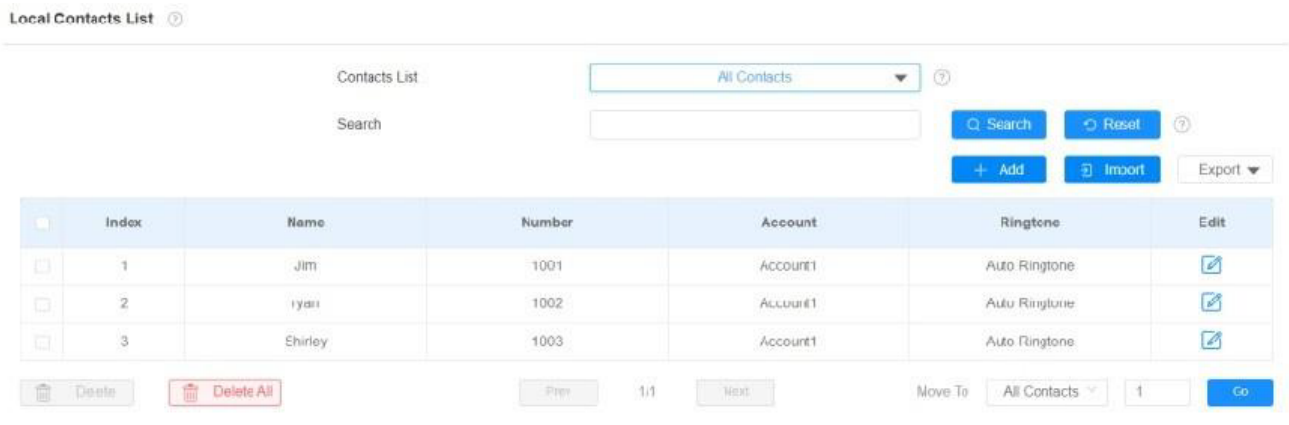
9.2 - Phone book configuration by web interface

9.2.1 - Adding, editing, deleting and searching local contacts

You can add, edit, delete and search local contacts by the web interface.

To add contacts:

Contacts > Local Contacts > Local Contacts List, then click **+ Add**.



Add Contact

X

Name	<input type="text"/>	?
Number	<input type="text"/>	?
Group	Default ▼	?
Dial Account	Account1 ▼	?
Ringtone	Auto Ringtone ▼	?

Cancel

Submit

Table A19 - MyBell IP Premium Indoor Monitor - Adding contacts by web interface

Field	Description
Contact List	Select All Contacts to display all contacts in the contact list. Select Blocklist to display the contacts in the blocklist.
Search	Search the contact by the contact number.
Name	Enter the contact name.
Number	Enter the contact SIP or IP number.
Group	Select Default for the local contact group. Select Blocklist to add the contact to the blocklist.
Dial Account	Select the account from which you want to call the contact.
Ringtone	Select the ringtone for the incoming call from the contact.

Note

To remove the contact from the blocklist by the web interface, change the group to **Default** when editing the contact.

9.3 - Importing and exporting contacts

To import and export contacts in batches:

Contacts > Local Contacts > Local Contacts List,

the file should be in **XML** or **CSV** format.

Local Contacts List ⓘ

Contacts List: ?

Search:

?

	Index	Name	Number	Account	Ringtone	Edit
<input type="checkbox"/>	1	Jim	1001	ACCOUNT1	Auto Ringtone	<input type="checkbox"/>
<input type="checkbox"/>	2	ryari	1002	ACCOUNT1	Auto Ringtone	<input type="checkbox"/>
<input type="checkbox"/>	3	Shirley	1003	Account1	Auto Ringtone	<input type="checkbox"/>

1/1

Move To:

9.4 - Contact list display configuration

To configure contacts by the web interface:

Contacts > Local Contacts > Contacts List Setting.

Contacts List Setting ⓘ

Contacts Sort By: ⓘ

Show Local Contacts Only: ⓘ

Local Contacts List ⓘ

Contacts List: ⓘ

Search: ⓘ

Index	Name	Number	Account	Ringtone	Edit
1	Jim	1001	Account1	Auto Ringtone	

1/1 Move To:

Table A20 - MyBell IP Premium Indoor Monitor - Contact list display configuration	
Setting	Description
Contact Sort By	If the local contacts are displayed before the contacts from SmartPlus, SDMC, etc., select ASCII Code to display contacts in alphabetical order. Select Created time to sort contacts by their creation time.
Show Local Contacts Only	If enabled, only the local contacts are displayed. If disabled, all contacts from SmartPlus cloud, SDMC, etc., are displayed.

9.5 - Web call

To make SIP calls or IP calls by the web interface enter the contact SIP or IP number and click **Dial**.

Dial Number ⓘ

ⓘ

10 NETWORK CONFIGURATION AND OTHER CONNECTIONS

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

10.1 - Network connection configuration on device

To check and configure the network connection on the device:

Settings > Advance Settings.



Table A21 - MyBell IP Premium Indoor Monitor - Network connection configuration on device

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. If you turn off the DHCP mode, the device switches to Static IP mode and the IP address, subnet mask, default gateway, and DNS server address 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.
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 actual network environment. The preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary address and the door phone connects to the alternate server when the preferred server is unavailable.

Note

- You can click on the **System Info** icon  and then click on the **Network** tab on the **Settings** screen to check the device network status.
- The default system code is **123456**.

10.2 - Network connection configuration by web interface

To check the network by the web interface:

Status > Network information.

Network Information ?

Network Type	LAN
LAN Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.2.47
Subnet Mask	255.255.255.0
GateWay	192.168.2.1
Preferred DNS	192.168.2.1
Alternate DNS	
Primary NTP	0.pool.ntp.org
Secondary NTP	1.pool.ntp.org

To check and configure network connection by the web interface:

Network > Basic > LAN Port.

LAN Port ?

Type	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP ?
IP Address	<input type="text" value="192.168.2.9"/> ?
Subnet Mask	<input type="text" value="255.255.255.0"/> ?
Default Gateway	<input type="text" value="192.168.2.1"/> ?
Preferred DNS Server	<input type="text" value="192.168.2.1"/> ?
Alternate DNS Server	<input type="text"/> ?

Table A22 - MyBell IP Premium Indoor Monitor - Network connection configuration by web interface	
Setting	Description
Type	<ul style="list-style-type: none"> If the DHCP mode is selected, the indoor monitor is assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically. If the Static IP mode is selected, the IP address, subnet mask, default gateway, and DNS server address 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 actual network environment. The preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary address and the door phone connects to the alternate server when the preferred server is unavailable.

10.3 - Device deployment in network

Indoor monitors need to be deployed before they are properly configured 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.

Table A23 - MyBell IP Premium Indoor Monitor - Device deployment in network

Setting	Description
Connect Mode	It's set up automatically according to the actual 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, therefore 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 Node	Specify the device address by entering device location information from the left to the right: Community, Unit, Stair, Floor, Room in sequence.
Device Extension	Enter the device extension number for the device you installed.
Device Location	Enter the location in which the device is installed and used.

10.4 - Device NAT configuration

Network Address Translation (NAT) enables hosts in an organization private intranet to connect transparently to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate an internal private network IP address into a legal network IP address technology.

To set up NAT by the web interface:

Account > Basic > NAT.

Table A24 - MyBell IP Premium Indoor Monitor - Device NAT configuration

Setting	Description
NAT	Enable the NAT function
Stun Server Address	Enter the SIP server in WAN.
Port	Enter the SIP server port.

Then go to **Account > Advanced > NAT interface.**

RPort: enable the RPort when the SIP server is in Wide Area Network (WAN) for the SIP account registration.

10.5 - Device Bluetooth configuration

10.5.1 - Device Bluetooth pairing

You need to enable the Bluetooth feature on the device before you can pair the indoor monitor with other Bluetooth-featured devices. To enable the Bluetooth feature:

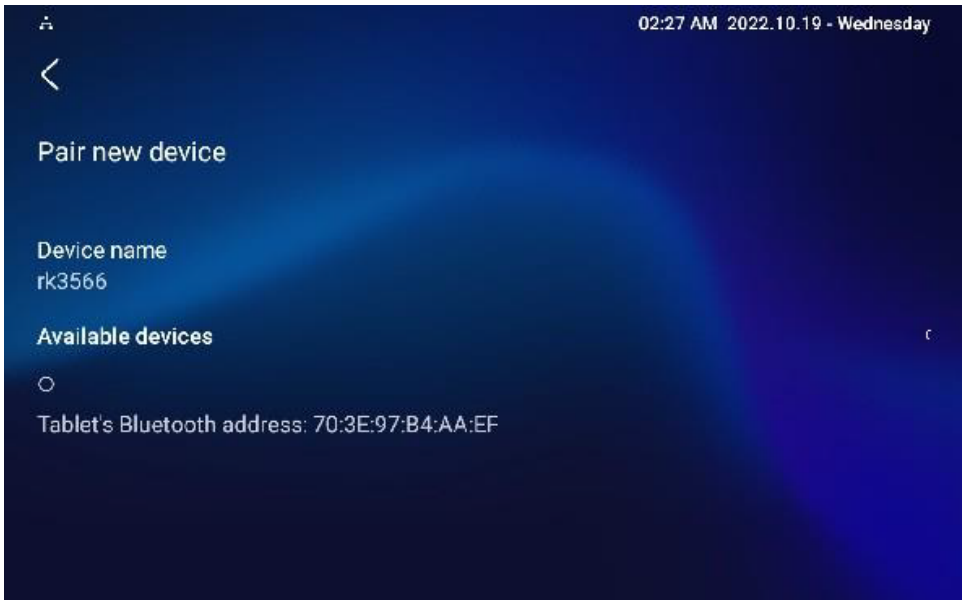
Settings > Bluetooth.

NAT 

NAT	<input checked="" type="checkbox"/>	
Stun Server Address	<input type="text"/>	
Port	<input type="text" value="3478"/>	(1024-65535) 

10.5.2 - Device Bluetooth data transmission

To transfer data via Bluetooth click **Pair new device**.



Note

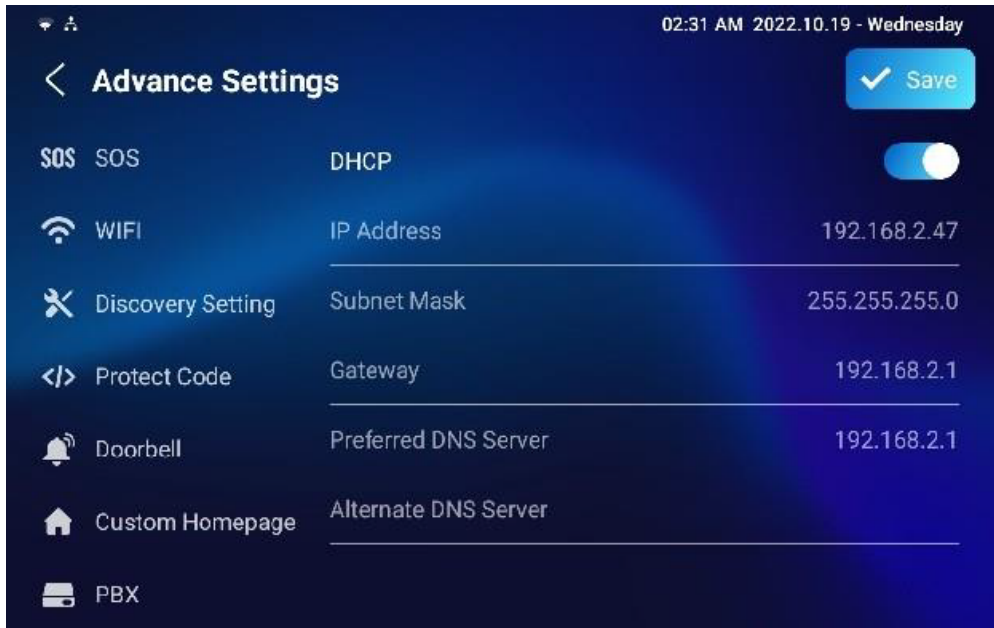
After successful Bluetooth pairing, data transmission can be carried out.

10.6 - Device Wi-Fi configuration

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

To configure Wi-Fi on the device:

Settings > Advance Setting.



11 INTERCOM CALL CONFIGURATION

11.1 - IP call and IP call configuration

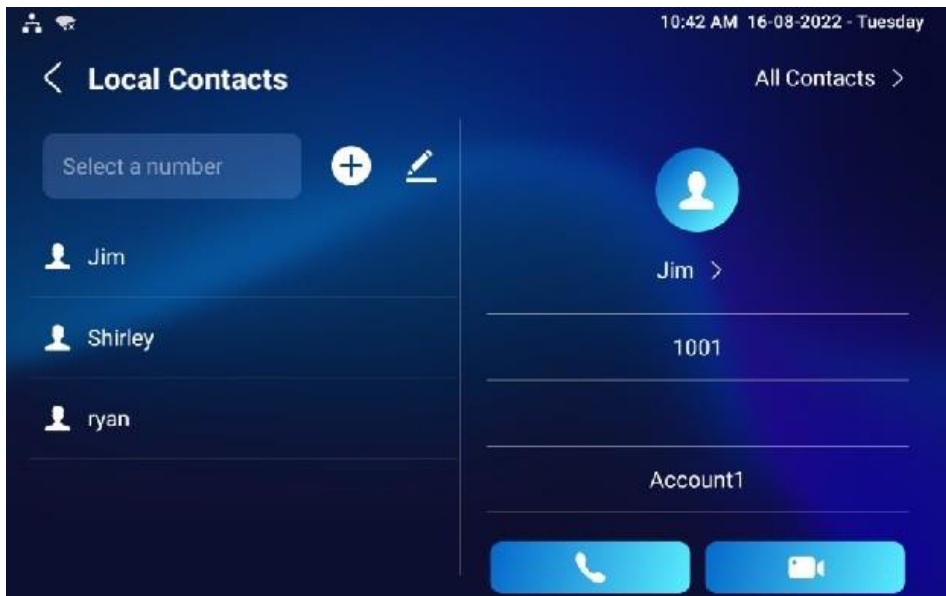
IP calls and SIP calls can be made directly on the intercom device by entering the IP number. You can also disable the direct IP calls so that no IP calls can be made.

11.1.1 - Making IP calls

To make a direct IP call on the device **Call** screen enter the IP address you wish to call on the soft keyboard and press **Audio** or **Video** tab to call out.



You can also make IP calls on the **Local Phonebook** on your device.



11.1.2 - IP configuration

To configure the IP call feature and port by the device web interface:

Device > Call Feature > Others.

Others ?

Return Code When Refuse	486(Busy Here) ▼ ?
Auto Answer Delay	0 (0-30Sec) ?
Answer Mode	Video ▼ ?
Answer Tone	Enabled ▼ ?
Busy Tone	<input checked="" type="checkbox"/> ?
Indoor Auto Answer	<input type="checkbox"/> ?
Direct IP Call	<input checked="" type="checkbox"/> ?
Direct IP Call Port	5060 (1-65535) ?

Table A25 - MyBell IP Premium Indoor Monitor - IP configuration

Setting	Description
Direct IP Call	Tick this checkbox to enable the direct IP call. If you don't allow direct IP calls to be made on the device, untick this checkbox.
Direct IP Call Port	The direct IP port is 5060 by default. The range for direct IP port is from 1 to 65535. If you enter any other values within the range other than 5060 , you need to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

11.2 - 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.

11.2.1 - SIP account registration

The indoor monitors support two SIP accounts that can be registered according to your applications and you can switch between them. The SIP account can be configured on the device or by the web interface.

To configure the SIP account on the device:

Settings > Advance Settings > Account.

10:55 AM 16-08-2022 - Tuesday

Advance Settings [Save]

- Network [Account1] Account2
- Monitor Active [Toggle]
- Account** Label
- Reset& Reboot Display Name
- Arming Register Name
- SOS SOS User Name
- WIFI Password

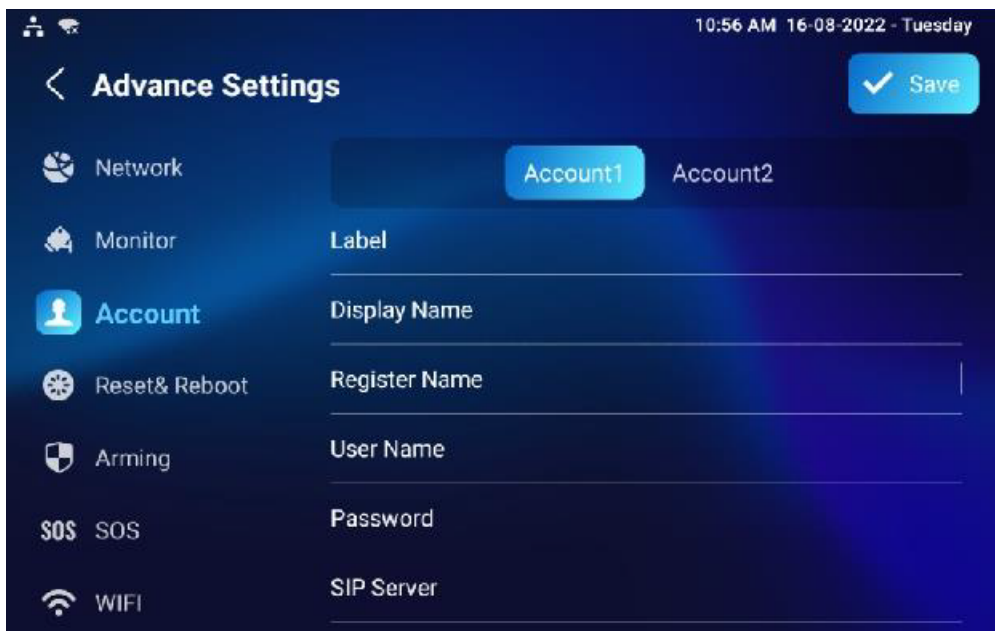


Table A26 - MyBell IP Premium Indoor Monitor - SIP account registration on device

Setting	Description
Account1/Account2	Select Account1 or Account2. The default SIP account is Account1.
SIP Port	Enter the SIP server port for communication. The default SIP port is 5060.

The parameter settings for SIP account registration can be configured on the Account setting screen and by the device web interface.

To configure these parameters by the web interface:

Account > Basic > SIP Account interface.

SIP Account ⓘ

Status	Disabled	ⓘ
Account	Account1	ⓘ
Account Enabled	<input type="checkbox"/>	ⓘ
Display Label	<input type="text"/>	ⓘ
Display Name	<input type="text"/>	ⓘ
Register Name	<input type="text"/>	ⓘ
Username	<input type="text"/>	ⓘ
Password	*****	ⓘ

Table A27 - MyBell IP Premium Indoor Monitor - SIP account registration by web interface

Setting	Description
Status	Check to see if the SIP account is registered.
Account	Select Account1 or Account2.
Account Enabled	Tick this checkbox to activate the registered SIP account.
Display Label	Configure the device label to be shown on the device screen.
Display Name	Configure the name, for example, the device name to be shown on the device being called to.
Register Name	Enter the SIP account register name obtained from the SIP account administrator.
Username	Enter the username obtained from the SIP account administrator.
Password	Enter the password obtained from the SIP server.

11.2.2 - SIP server configuration

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

To set the SIP account by the web interface:

Account > Basic > SIP Account.

Table A28 - MyBell IP Premium Indoor Monitor - SIP server configuration by web interface

Setting	Description
Server IP	Enter the server IP address number or its URL.
Port	Set up the SIP server port for data transmission.
Registration Period	Set up the SIP account registration time span. A SIP re-registration starts automatically if the account registration fails during the registration time span. The default registration period is 1800 and it can range from 30 to 65535 seconds.

11.2.3 - Outbound proxy server configuration

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

To configure the outbound proxy server by the web interface:

Account > Basic > Outbound Proxy Server.

Table A29 - MyBell IP Premium Indoor Monitor - Outbound proxy server configuration

Setting	Description
Outbound Enable	Tick or untick this checkbox to turn the outbound proxy server on or off.
Preferred Outbound Proxy Server	Enter the SIP address of the outbound proxy server.
Preferred Outbound Proxy Port	Enter the port number to establish call session through the outbound proxy server.
Alternate Outbound Proxy Server	Set up backup server IP for the backup outbound proxy server.
Alternate Outbound Proxy Port	Enter the port number to establish call session through the backup outbound proxy server.

11.3 - SIP Call DND and return code configuration

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

To configure DND by the web interface:

Device > Call Feature > DND.

Table A30 - MyBell IP Premium Indoor Monitor - DND configuration

Setting	Description
DND	Check the Whole Day or Schedule to enable the DND function. The DND function is disabled by default.
Return Code When DND	Select what code should be sent to the calling device through the SIP server: <ul style="list-style-type: none"> • 404 for Not found. • 480 for Temporary Unavailable. • 486 for Busy Here.
Return Code When Refuse	Select the code to be sent to the caller side via SIP server when you rejected the incoming call.

11.4 - Device local RTP configuration

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

To set up device local RTP by the web interface:

Network > Advanced > Local RTP.

Table A31 - MyBell IP Premium Indoor Monitor - Device local RTP configuration

Setting	Description
Starting RTP Port	Enter the port value to establish the start point for the exclusive data transmission range.
Max RTP Port	Enter the port value to establish the endpoint for the exclusive data transmission range.

11.5 - 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.

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

To set up data transmission type by the web interface:

Account > Basic > Transport Type.

Table A32 - MyBell IP Premium Indoor Monitor - Data transmission type configuration

Setting	Description
UDP	Select UDP for unreliable but very 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 a secured and reliable transport layer protocol.
DNS-SRV	Select DNS-SRV to obtain a DNS record for specifying the location of services. SRV records the server address and the server port. SRV can also be used to configure the priority and the weight of the server address.

12 CALL CONFIGURATION

12.1 - Auto-answer configuration

The device answers all incoming calls if call auto-answer is enabled and receives live stream if live stream is enabled.

To configure this function by the device web interface:

Account > Advanced > Call > Auto Answer,

and

Device > Call Feature > Others.

Call ?

Max Local SIP Port: 5032 (1024-65535) ?

Min Local SIP Port: 5032 (1024-65535) ?

PTime(ms): 20 ?

Auto Answer ?

Prevent SIP Hacking: ?

Others ?

Return Code When Refuse: 486(Busy Here) ?

Auto Answer Delay: 0 (0-30Sec) ?

Answer Mode: Video ?

Busy Tone: Video ?

Indoor Auto Answer: ?

Direct IP Call: ?

Direct IP Call Port: 5060 (1-65535) ?

Table A33 - MyBell IP Premium Indoor Monitor - Auto-answer configuration

Setting	Description
Auto Answer	Turn on the Auto Answer function by ticking the square box.
Auto Answer Delay	Set up the delay time (from 0 to 30 seconds) before the call can be answered automatically. For example, if you set the delay time to 1 second, the call is answered in 1 second automatically.
Answer Mode	Set up the video or audio mode for answering the call automatically.
Indoor Auto Answer	Enable it if you want to auto-answer the calls from the indoor monitors only.

12.2 - Auto-answer Allow List configuration

Auto-answer can only be applicable to the SIP or IP numbers that are already added in the auto-answer **Allow List** of your indoor monitor. Therefore, you are required to configure or edit the numbers in the **Allow List** by the web interface.

To configure a call-auto answer **Allow List** setting by the device web interface:

Device > Call Feature > Auto Answer AllowList.

Auto Answer AllowList ?

+ Add Import Export

Index	Device Location	SIP/IP	Edit
1	Gate	101	
2	Living	102	
3	Front Door	192.168.3.15	

Delete Delete All Prev 1/1 Next 1 Go

Add Auto Answer AllowList X

Device Location: ?

SIP/IP: ?

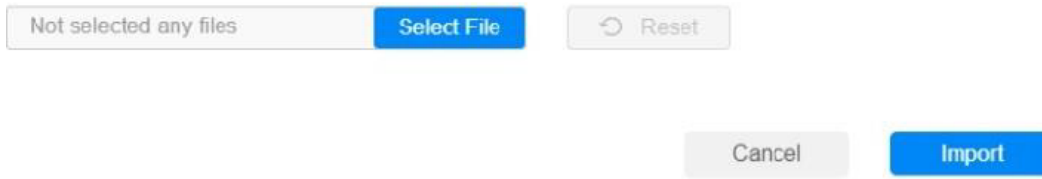
Cancel Submit

SIP/IP numbers can be imported to or exported out of the indoor monitor in batch.

To import to or export out SIP/IP by the device web interface:

Device > Call Feature > Import/Export.

Select Answer Allowlist File(xml or csv)



Note

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

12.3 - Live stream configuration

Receiving live stream on the indoor monitor allows you to see the video image (one-way video stream) from the calling device such as a door phone.

To configure this function by the web interface:

Device > Call Feature > Audio Call Settings.



If an audio call is received on the device, you can see the video image of the calling party.

12.4 - Intercom call configuration (preview, mute)

To see the image at the door station before answering the incoming call, enable the intercom preview function by the web interface:

Device > Intercom > Intercom.



Table A34 - MyBell IP Premium Indoor Monitor - Intercom call configuration	
Setting	Description
Intercom Active	Tick this checkbox to enable or disable the intercom function. It's enabled by default.
Intercom Mute	Tick this checkbox to mute the voice from the caller side and vice versa.
Intercom Preview	Tick this checkbox to enable the incoming call preview function. If intercom preview is enabled, the group call isn't available.

12.5 - Voice changer

Voice changer helps ensure users privacy and home security. Users (especially women and children) can protect themselves by changing their voices when talking to a stranger.

To configure the voice changer on device:

Settings > Call Feature.

12.6 - Emergency call configuration

Emergency call is used to call out three emergency contacts when you are in urgent status. It's especially useful for the elders and children.

To display the Emergency call softkey by the web interface:

Device > Display Setting > Home Page Display/More Page Display.

Home Page Display
Example

Area	Type	Value	Label	Icon(max size:50*50)
Area1	Call			Not selected any files Select File Delete
Area2	SOS		SOS	Not selected any files Select File Delete
Area3	DND			
Area4	Monitor			Not selected any files Select File Delete

More Page Display
Example

Area	Type	Value	Label	Icon(max size:50*50)
Area1	Contacts			Not selected any files Select File Delete
Area2	Settings			Not selected any files Select File Delete
Area3	Arming			Not selected any files Select File Delete

After setup on web, you also need to perform configuration on the device or by the device web interface.

To configure the Emergency call on the device:

Settings > Advance Settings > SOS screen.

Table A35 - MyBell IP Premium Indoor Monitor - Emergency call configuration

Setting	Description
Call Number	Set up 3 SOS numbers. Once the users press the SOS key on the home page (SOS display key needs to be set on the web manually), indoor monitors call out the numbers in order.
Call Timeout	Set up the timeout for each number. When one number is called out and the other side doesn't answer within the timeout, the device calls the next number.
Loop Times	Set up the call loop times.
Account	Select the account from which you want to make the SOS calls.

To configure the Emergency call by the web interface:

Device > Intercom > SOS.

SOS 

Account	<input type="text" value="Auto"/>	
Call Number 1	<input type="text"/>	
Call Number 2	<input type="text"/>	
Call Number 3	<input type="text"/>	
Call Timeout(Sec)	<input type="text" value="60"/>	
Loop Times	<input type="text" value="3"/>	

12.7 - Multicast configuration

The device allows conducting one-to-many broadcasting through the multicast function.

To configure multicast communication by the web interface:

Device > Multicast > Multicast List.

Multicast List 

Multicast Group	Multicast Address	Enabled
Multicast Group 1	<input type="text" value="224.1.6.11.51231"/>	<input checked="" type="checkbox"/>
Multicast Group 2	<input type="text"/>	<input type="checkbox"/>
Multicast Group 3	<input type="text"/>	<input type="checkbox"/>

Listen List 

Listen Group	Listen Address	Label
Listen Group 1	<input type="text" value="224.1.6.11.51230"/>	<input type="text" value="Test_1"/>
Listen Group 2	<input type="text"/>	<input type="text"/>
Listen Group 3	<input type="text"/>	<input type="text"/>

12.8 - Call forwarding configuration

Call Forward is a feature used to redirect an incoming call to a specific third party. Users can redirect the incoming call based on different scenarios. Typically, there are three **Call Forward** modes:

- Always Forward.
- No Answer Forward.
- Busy Forward.

12.9 - Call forwarding configuration on device

To configure call forwarding on the device:

Device > Call Feature.

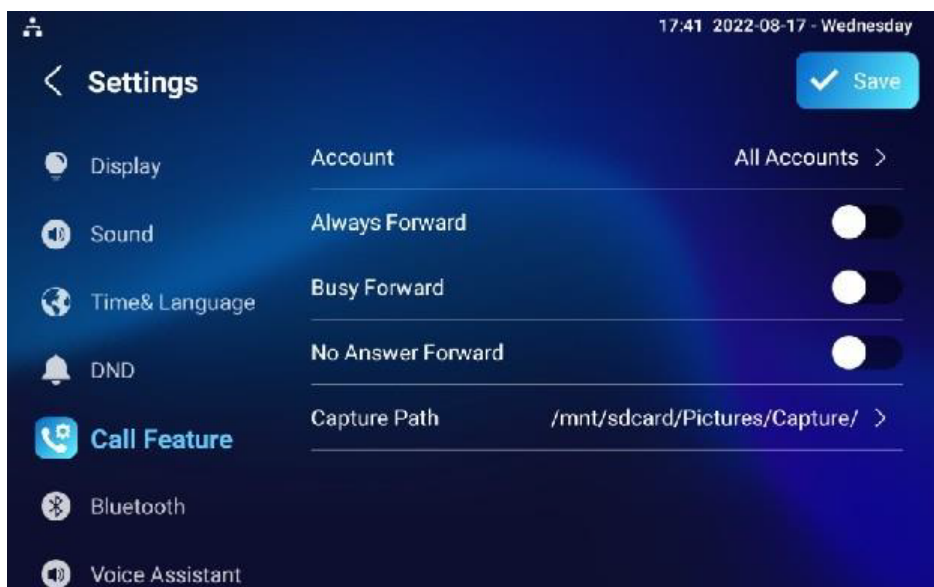


Table A36 - MyBell IP Premium Indoor Monitor - Call forwarding configuration on device

Setting	Description
Account	Choose which account shall implement the call forwarding feature.
Always Forward	If enabled, all incoming calls are automatically forwarded to a specific number.
Busy Forward	If enabled, incoming calls are forwarded to a specific number if the phone is busy.
No Answer Forward	If enabled, incoming calls are forwarded to a specific number if the phone isn't picked up within no answer ring time.
Target Number	Enter the specific forward number if the device enables always forward / busy forward / no answer forward modes.
Capture Path	Select the storage location for all the captured pictures.

12.10 - Call forwarding configuration by web interface

To configure call forwarding by the web interface:

Device > Call Feature > Call Forward.

Call Forward ?

Always Forward	Disabled	?
Target Number		?
Busy Forward	Disabled	?
Target Number		?
No Answer Forward	Disabled	?
Target Number		?
No Answer Ring Time (Sec)	30	?

Table A37 - MyBell IP Premium Indoor Monitor - Call forwarding configuration by web interface

Setting	Description
Always Forward	If enabled, all incoming calls are automatically forwarded to a specific number.
Target Number	Enter the specific forward number if the device enables always forward mode.
Busy Transfer	If enabled, incoming calls are forwarded to a specific number if the phone is busy.
Target Number	Enter the specific forward number if the device enables the busy forward mode.
No Answer Forward	If enabled, incoming calls are forwarded to a specific number if the phone isn't picked up within no answer ring time.
Target Number	Enter the specific forward number if the device enables no answer forward mode.
No Answer Ring Time (sec)	Set the no answer ring time interval from 0-120 seconds before the call is transferred to a designated number.

13 INTERCOM MESSAGE CONFIGURATION

13.1 - Managing messages

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



Table A38 - MyBell IP Premium Indoor Monitor - Managing messages

Setting	Description
Notification	Messages from property manager. This feature is only available when using SDMC or Yubii Home.
Text MSG	Send, receive or manage the text messages here.
Owner MSG	If enabled, when nobody answers the incoming call within the pre-configured ring time, the visitor hears the owner's audio message.
Visitor MSG	If enabled, when nobody answers the incoming call within the pre-configured ring time, it saves the visitor record.
Family MSG	Record audio messages for your family members.

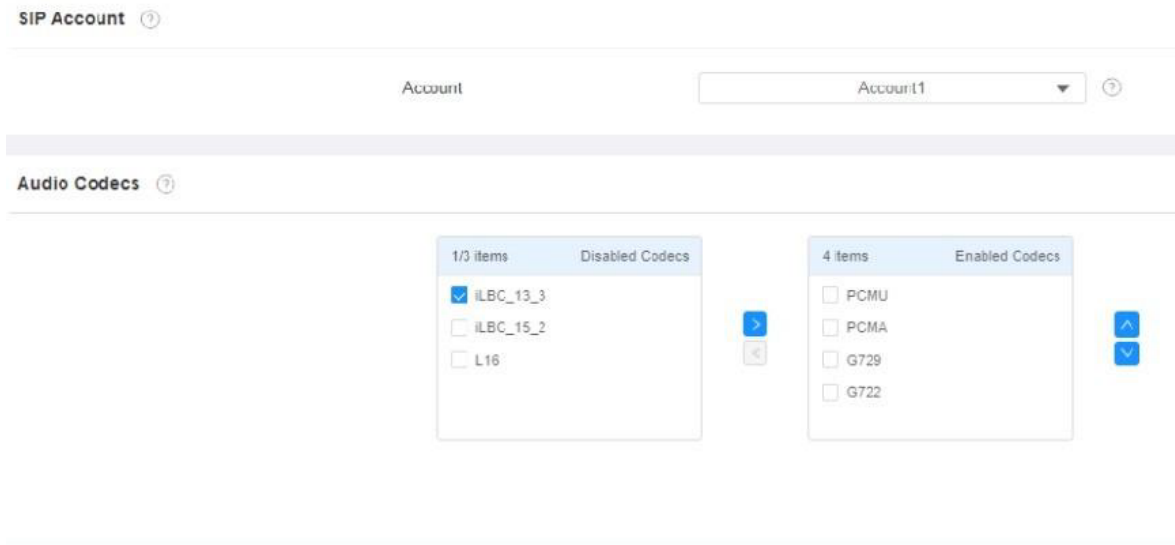
14 AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS

14.1 - Audio codec configuration

The indoor monitor supports seven types of Codec (iLBC_13_3, iLBC_15_2, L16, PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly, according to the actual network environment.

To configure audio codec by the web interface:

Account > Advanced > SIP Account.



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

Table A39 - MyBell IP Premium Indoor Monitor - Bandwidth consumption and sample rate for codecs types

Codec type	Bandwidth consumption	Sample rate
PCMA	64 kbit/s	8 kHz
PCMU	64 kbit/s	8 kHz
G729	8 kbit/s	8 kHz
G722	64 kbit/s	16 kHz
iLBC_13_3	8.16 kbit/s	13.3 kHz
iLBC_15_2	8.16 kbit/s	15.2 kHz
L16	128 kbit/s	15.2 kHz

14.2 - Video codec configuration

The indoor monitor supports the VP8, H263, H264, and H265 codecs that provide better video quality at a much lower bit rate with different video quality and payload.

To configure video codec by the web interface:

Account > Advanced > Video Codecs.

Choose an available video codec and set up the codec parameters.



Name	H263	?
Resolution	CIF	?
Bitrate	320	?
Payload	34	?
Name	H264	?
Resolution	CIF	?
Bitrate	320	?
Payload	104	?
Name	VP8	?
Resolution	CIF	?
Bitrate	320	?
Payload	96	?

Table A40 - MyBell IP Premium Indoor Monitor - Video codec configuration

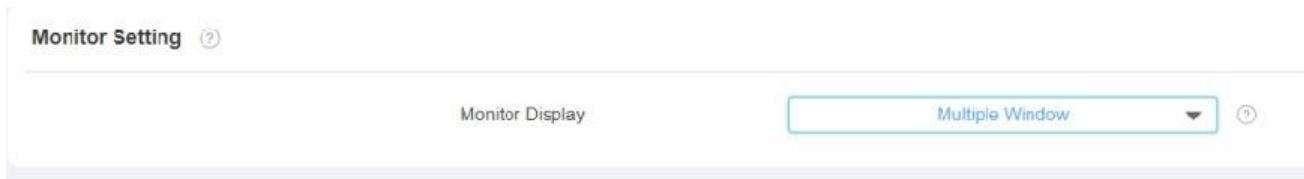
Setting	Description
Name	Check to select the H264 video codec format for the door phone video stream. The default video codec is H264.
Resolution	Select the codec resolution for the video quality from the following options: <ul style="list-style-type: none"> • QCIF, • CIF, • VGA, • 4CIF, • 720P, according to your network environment. The default code resolution is 4CIF.
Bitrate	Select the video stream bitrate (ranging from 320 to 2048). The bigger the bit rate, the bigger amount of 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.

15.1 - Monitor configuration

To configure the monitor setting by the web interface:

Device > Monitor.

Enter the IP/SIP number of the door phone in the device number field and fill in the device name. Then set up the RTSP address. The RTSP format of the door phone is `rtsp://deviceIP/live/ch00_0`. Enable or disable display in call. If it's enabled, the video is displayed when there's an incoming call.



Setting:

- **Monitor Display:** select **MultipleWindow** to display four video monitoring channels on the screen. Select **Single** to display only one video monitoring channel.

Note

You can import and export the monitored device setting using a template in **XML** format.

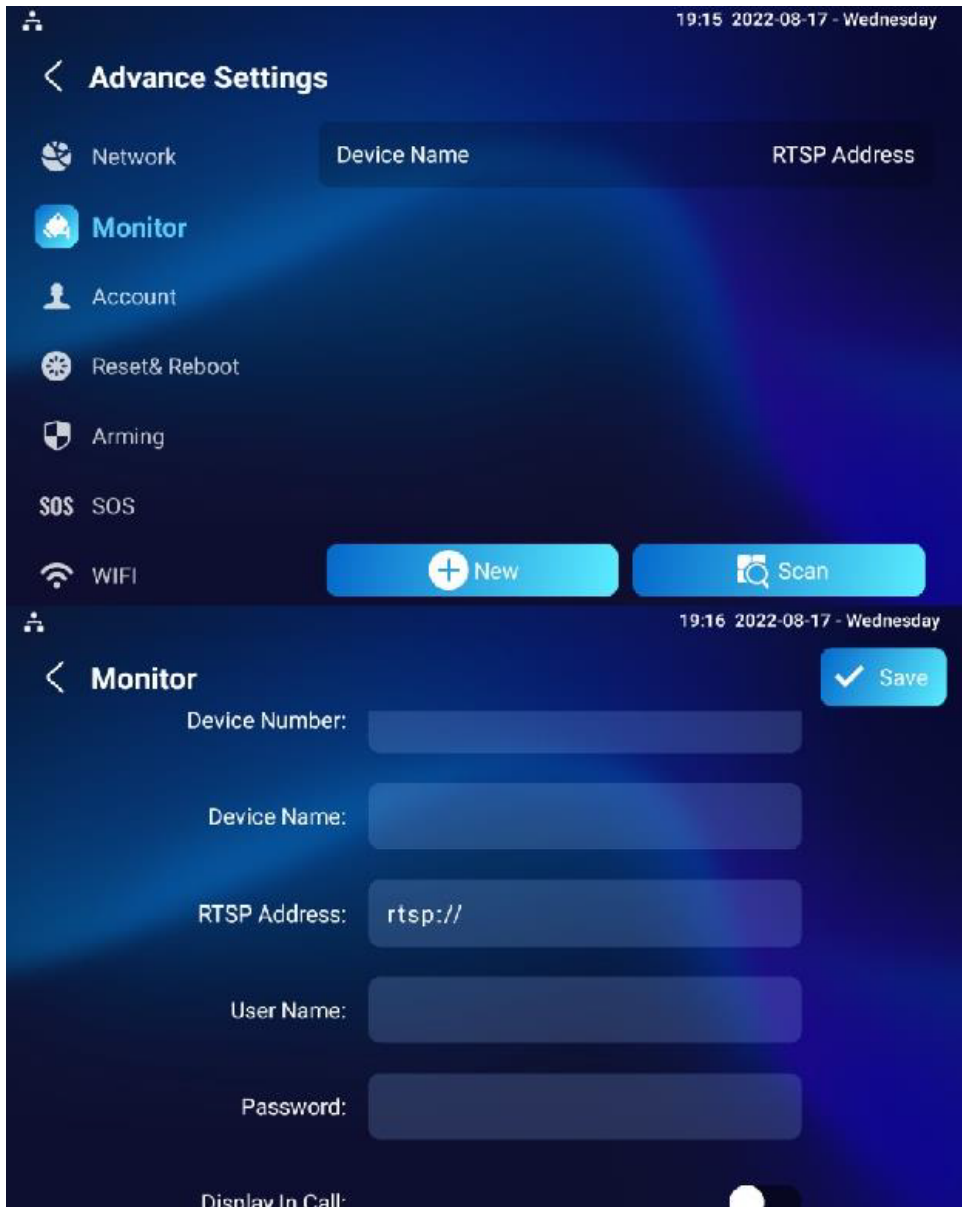


Add Monitor X

Device Number	<input type="text" value="157"/>	?
Device Name	<input type="text" value="R29"/>	?
RTSP Address	<input type="text" value="rtsp:// 192.168.13.157/live/ch00_0"/>	?
Username	<input type="text" value="admin"/>	?
Password	<input type="password" value="*****"/>	?
Display In Call	<input type="text" value="Disabled"/>	?

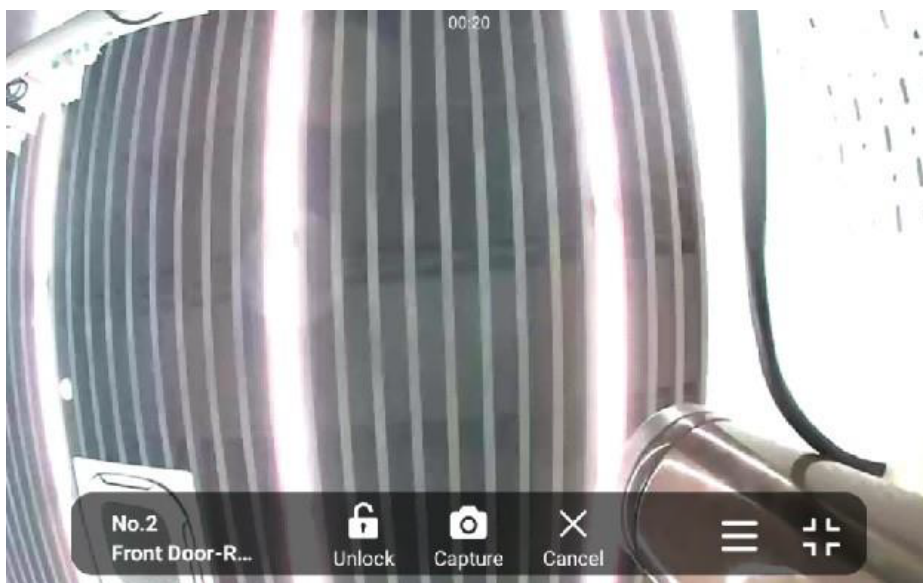
Table A41 - MyBell IP Premium Indoor Monitor - Monitor configuration	
Setting	Description
Device Number	Enter the monitored device number for identification
Device Name	Enter the monitored device name for identification.
RTSP Address	Enter the RTSP address of the monitored device. RSTP format: device IP address/live/ch00_0.
User Name	Enter the username of the monitored device for monitoring authentication.
Password	Enter the password of the monitored device for monitoring authentication.
Display in Call	Enable if you want to display the monitoring video when you are in the call.

You can also configure it on the device:



15.2 - Video image capturing

To capture video image click **Monitor > Capture** on the device screen.



15.3 - RTSP authentication

You can set the RTSP authentication to enable the indoor monitoring with RTSP audio stream. For example, you can monitor babies in their room using audio, to ensure their safety.

To configure RTSP authentication:

Setting > Basic > RTSP Setting.

RTSP Setting

RTSP Audio Enable	Disabled	?
Authorization Type	Basic	?
User Name	admin	?
Password	?

Table A42 - MyBell IP Premium Indoor Monitor - RTSP authentication

Setting	Description
RTSP Audio Enable	Enable it to monitor the device by RTSP audio stream.
Authorization Type	Select the authorization type (Basic or Digest). Select None if you allow all types of authorization for the RTSP audio stream.
User Name	Enter the username used for authentication.
Password	Enter the password used for authentication.

15.4 - Alarm and arming configuration

The alarm feature is used to connect some alarm detection devices to protect your home safety. The indoor monitors support 8 alarm connectors, which means you can connect 8 different alarm sensors in different rooms of your house. For example, by connecting a smoke sensor in your kitchen when the leaking gas is detected, the indoor monitor rings and sends the alarm message to the target, like community property.

15.4.1 - Alarm and arming configuration on device

To configure the arming and disarm codes on the device:

Arming > Arming/Disarm Code.

Change the current password and save it.

11:54 2022-08-19 - Friday

< Arming/Disarm Code Save

Please input current arming/disarm code:

Please input new arming/disarm code:

Please confirm new arming/disarm code:

1 2 3
4 5 6
7 8 9
0

To check the zone status:

Arming > Zone Status.

Zone	Location	Zone Type	Trigger	Status
Zone1	Bedroom	Infrared	NC	Disable
Zone2	Bedroom	Infrared	NC	Disable
Zone3	Bedroom	Infrared	NC	Disable
Zone4	Bedroom	Infrared	NC	Disable
Zone5	Bedroom	Infrared	NC	Disable
Zone6	Bedroom	Infrared	NC	Disable
Zone7	Bedroom	Infrared	NC	Disable

15.4.2 - Alarm and arming configuration by web interface

To configure a location-based alarm sensor by the device web interface:

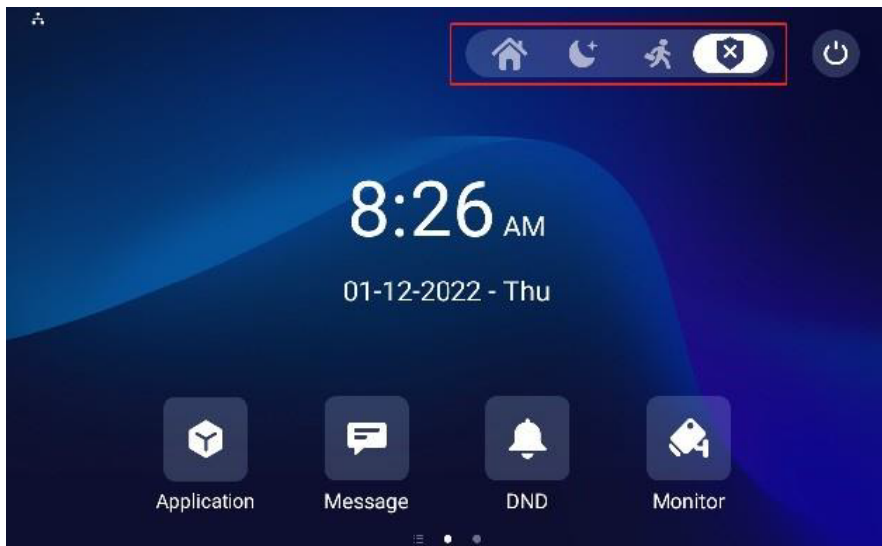
Arming > Zone Setting > Zone Setting.

Zone	Location	Zone Type	Trigger Mode	Status
Zone1	Bedroom	Infrared	NC	Enable
Zone2	Bedroom	Drmagnet	NC	Enable
Zone3	Bedroom	Smoke	NC	Disabled

Table A43 - MyBell IP Premium Indoor Monitor - Alarm and arming configuration

Setting	Description
Location	Set up the location according to where the alarm sensor is installed. You can select from the following location types: Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
Zone Type	Set up the alarm sensor types. You can select from the following sensor types: Infrared, Drmagnet, Smoke, Gas, and Urgency.
Trigger Mode	Set sensor trigger mode between NC and NO , as needed.
Status	Set the alarm sensor status to one of the three options: <ul style="list-style-type: none"> • Enable – enable the alarm, you need to set the alarm again after disarming. • Disable – disable the alarm. • 24H – keep the alarm sensor enabled for 24 hours without setting it up manually again after disarming.

If any of the zones are enabled or set to **24H**, the alarm-related icons are displayed on the home screen for quick access. If all zones are disabled, all the icons are displayed.



15.5 - Location-based alarm configuration

To configure the alarm sensor, follow the same steps as in configuration by the web interface.

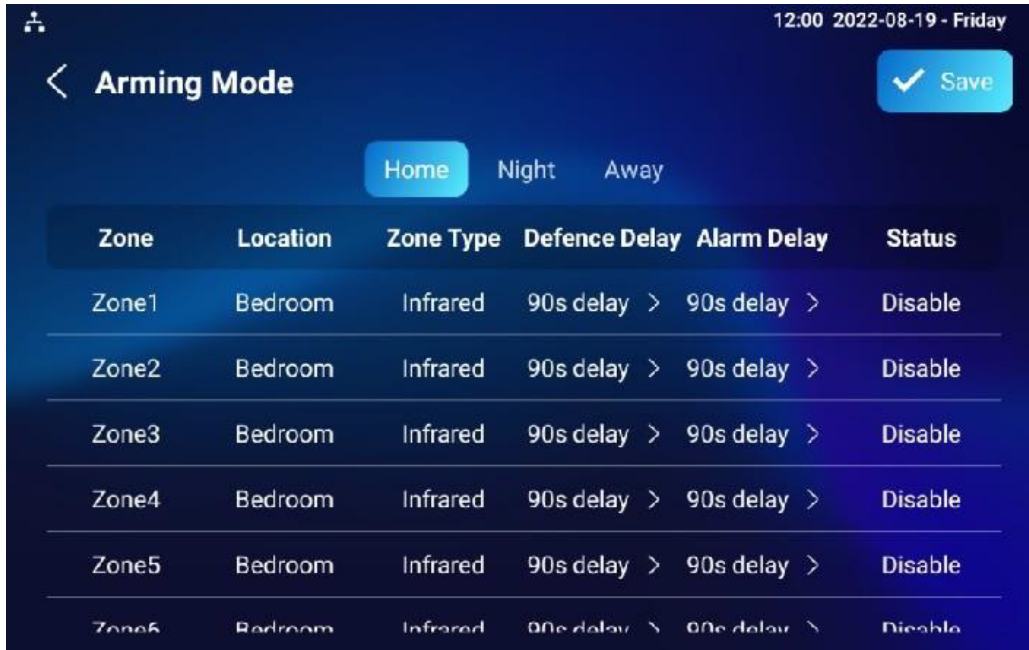


Table A44 - MyBell IP Premium Indoor Monitor - Location-based alarm configuration

Setting	Description
Location	Select the location of the detection device, including Bedroom, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
Zone type	Select the type of detection device, including Infrared, Drmagnet, Smoke, Gas, and Urgency.
Defence delay	When users switch to the arming mode from other modes, there's a 90-second delay before activation.
Alarm delay	When the sensor is triggered, there's a 90-second delay before announcing the notification.
Status	Enable or disable the Arming Mode for the corresponding Zone.

15.6 - Alarm text configuration

After the alarm sensor is set up, you can customize the alarm text shown on the screen when the alarm is triggered. Enter the alarm text for the alarm at each location according to your need.

To customize the text by the web interface:

Arming > Zone Setting > Zone Setting.

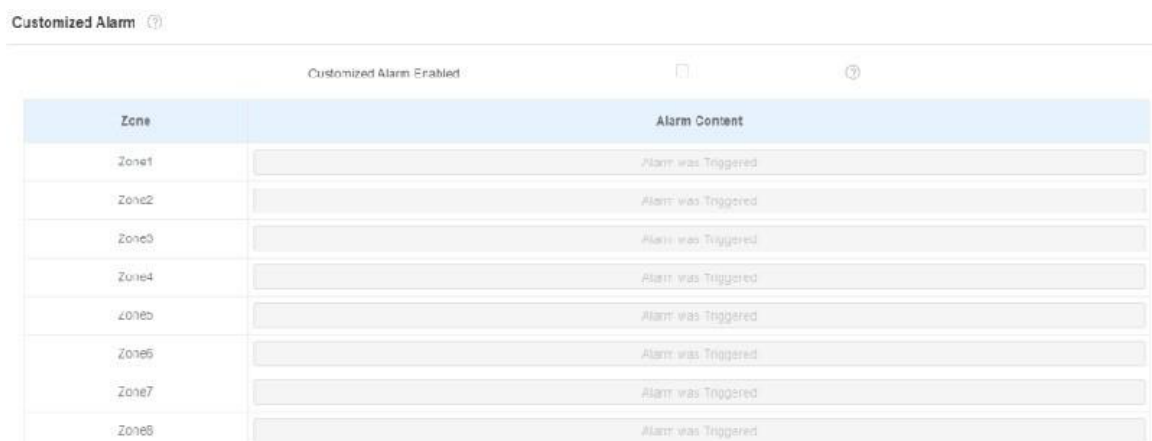
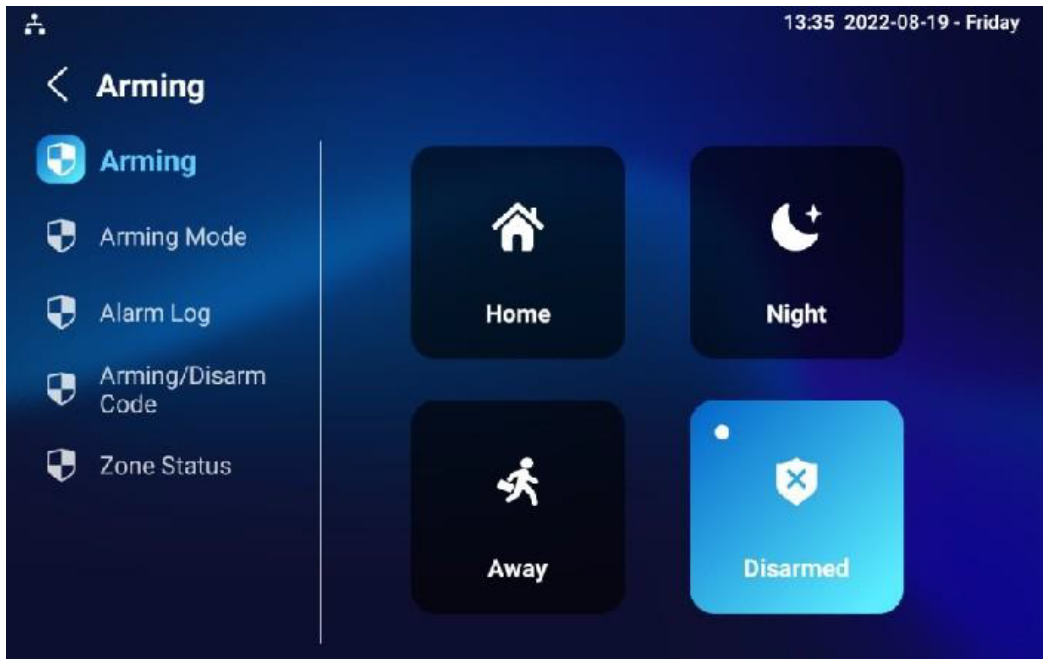


Table A45 - MyBell IP Premium Indoor Monitor - Alarm text configuration

Setting	Description
Customized Alarm Enable	Enable this feature before enetering the customized alarm text.
Alarm Context	Enter the alarm text in the specific arming zone. The alarm text is displayed when arming is triggered.

15.7 - Arming mode configuration

To switch to arming mode, disarm the alarm on **Arming** screen by pressing the respective icons. Press **Disarm** icon to clear the **Arming Mode**.



15.8 - Alarm ringtone configuration

To upload customized alarm ringtone by choosing the local audio file by web interface:

Device > Audio > Alarm Ringtone Upload.



Note

The file format of customised ringtone should be **WAV**.

15.9 - Alarm action configuration

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

15.9.1 - Select alarm action types

To select and set up actions by the web interface:

Arming > Alarm Action > Alarm Action.

Zone	Http Command	Send Http
Zone1	http://	Disabled
Zone2	http://	Disabled
Zone3	http://	Disabled
Zone4	http://	Disabled
Zone5	http://	Disabled
Zone6	http://	Disabled
Zone7	http://	Disabled
Zone8	http://	Disabled

Receiver Of SIP Setting ?

SIP Account

Zone	SIP Message	Send Sip Message
Zone1	<input type="text"/>	Disabled ▼
Zone2	<input type="text"/>	Disabled ▼
Zone3	<input type="text"/>	Disabled ▼
Zone4	<input type="text"/>	Disabled ▼
Zone5	<input type="text"/>	Disabled ▼
Zone6	<input type="text"/>	Disabled ▼
Zone7	<input type="text"/>	Disabled ▼
Zone8	<input type="text"/>	Disabled ▼

Call Setting ?

Call Number

Zone	Make Call Enable	Alarm Siren
Zone1	Disabled ▼	Enabled ▼
Zone2	Disabled ▼	Enabled ▼
Zone3	Disabled ▼	Enabled ▼
Zone4	Disabled ▼	Enabled ▼
Zone5	Disabled ▼	Enabled ▼
Zone6	Disabled ▼	Enabled ▼
Zone7	Disabled ▼	Enabled ▼

15.9.2 - Alarm action type configuration through HTTP command

To set up the HTTP Command action click **Enable** in the **Send HTTP** field to enable the actions for the alarm sensor installed in different locations. Then enter the HTTP command provided by the manufacturer of the device on which the action is to be carried out.

HTTP Command Setting ?

Zone	Http Command	Send Http
Zone1	http:// ▼	Disabled ▼
Zone2	http:// ▼	Disabled ▼
Zone3	http:// ▼	Disabled ▼
Zone4	http:// ▼	Disabled ▼
Zone5	http:// ▼	Disabled ▼
Zone6	http:// ▼	Disabled ▼
Zone7	http:// ▼	Disabled ▼
Zone8	http:// ▼	Disabled ▼

Table A46 - MyBell IP Premium Indoor Monitor - Alarm action type configuration through HTTP command

Setting	Description
Send HTTP	Enable it to implement the action on a designated third-party device.
HTTP Command	Enter the HTTP command provided by third-party device manufacturer.

15.9.3 - Alarm action configuration through SIP message

To set up the SIP message action receiver on the same web interface enter the SIP account to which you want to send the configured SIP message when the alarm is triggered.

SIP Account:

Zone	SIP Message	Send Sip Message
Zone1	<input type="text"/>	Disabled ▼
Zone2	<input type="text"/>	Disabled ▼
Zone3	<input type="text"/>	Disabled ▼
Zone4	<input type="text"/>	Disabled ▼
Zone5	<input type="text"/>	Disabled ▼
Zone6	<input type="text"/>	Disabled ▼
Zone7	<input type="text"/>	Disabled ▼
Zone8	<input type="text"/>	Disabled ▼

Table A47 - MyBell IP Premium Indoor Monitor - Alarm action configuration through SIP message

Setting	Description
Call Number	Enter the SIP number or IP number to receive the calls when the alarm is triggered.
Make Call Enable	Enable it so that a call goes to the designated SIP or IP number when the alarm is triggered.
Alarm Siren	Enable it to turn on alarm siren on the indoor monitor when the alarm is triggered.

15.10 - Checking alarm log

To check alarm log on device

Settings > Arming Log.



15.11 - Screen unlock configuration

The device screen is locked over sleep time. You are required to wake up the device through face recognition (Face ID).

To enable screen unlock on device:

Setting > Display.



15.12 - Screen unlock by PIN code

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

Note

The default unlock PIN is **123456**.

15.13 - Voice encryption

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

To configure voice encryption by the web interface:

Account > Advanced > Encryption.

Encryption ⓘ

Voice Encryption

Disabled ▼ ⓘ

Setting:

Voice Encryption: select encryption mode from the following four options:

- **Disable** – the call isn't encrypted.
- **RTP (Compulsory)** – all audio signals (RTP streams) are encrypted to improve security.
- **SRTP (Optional)** – voice from the called party is encrypted. If the called party enables SRTP, the voice signals are also encrypted.
- **ZRTP (Optional)** – the protocol that the two parties use to negotiate the SRTP session key.

15.14 - Remote control

Remote control function supports the configuration of a specific server to send HTTP commands or requests to the indoor monitor. It enables the monitor to perform some specific actions.

To configure this function by the web interface:

Device > Relay > Remote Control.

Remote Control ⓘ

Allowed Access IP List

Allowed Access IP List: set up the server IP address that can send the HTTP commands to the indoor monitor.

15.15 - Location

Select the level of protection for the location of the indoor monitor. For example, you can disable the location feature so that no app is allowed to obtain your device location.

To configure the location:

Security > Advanced > Service.

Service

Location

Only Device ▼

Table A48 - MyBell IP Premium Indoor Monitor - Location

Setting	Description
Disabled	No app can obtain your device location.
Only Device	The device location can be determined using GPS.
High Accuracy	The device location can be determined using WAN, Bluetooth or cellural networks.

15.16 - High security mode

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**

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

16 DOOR ACCESS CONTROL CONFIGURATION

16.1 - Relay switch configuration

16.1.1 - Local relay configuration

Local relays in the device can be used to trigger the relay for the door access and trigger a chime bell as needed in different scenarios. To configure a local relay by the device web interface:

Device > Relay > Relay Setting.

Relay Setting 

Local Relay1

Relay Delay (Sec) 

Relay Type 

Remote Control 

DTMF 

Table A49 - MyBell IP Premium Indoor Monitor - Local relay configuration

Setting	Description
Relay Delay	Set the relay delay time after the relay is triggered.
Relay Type	Set relay action type choosing one of the following options: <ul style="list-style-type: none"> • Chime bell – when there is a call, the chime bell rings. • Open door – when the unlock icon is pressed, the local relay opens.
Remote Control	Enable it to trigger local relay by DTMF and vice versa.
DTMF	Set the DTMF to trigger the local relay when Remote control is enabled.

16.1.2 - Remote relay switch configuration

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

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

Phone > Relay > Relay Setting > Remote Relay.

Remote Relay

DTMF1 Code 

DTMF2 Code 

DTMF3 Code 

Setting:

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

16.2 - Web relay configuration

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

To configure a web relay by the device web interface:

Device > Relay > Web Relay.

Web Relay 

IP Address 

Username 

Password 

Web Relay Action Setting

Action ID	IP	SIP	Web Relay Action
Action ID 1	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 2	<input type="text"/>	<input type="text"/>	<input type="text"/>

Table A50 - MyBell IP Premium Indoor Monitor - Web relay configuration

Setting	Description
IP address	Enter the web relay IP address.
Username	Enter the username provided by the web relay manufacturer.
Password	Enter the password provided by the web relay manufacturer. The passwords are authenticated with HTTP and you can define the passwords using HTTP get in Action.
Web Relay Action	Enter the specific web relay action command provided by the web manufacturer for different actions of the web relay.
IP/SIP	Enter the relay extension information, IP address or SIP account of an intercom device, such as an indoor monitor. It enables sending the specific action command when unlock is performed on the intercom device. This setting is optional. Please refer to the example below: http://admin:admin@192.168.1.2/state.xml?relayState=2.

16.3 - Door unlock configuration

16.3.1 - Door unlock by DTMF code

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

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

Account > Advanced > DTMF.

DTMF ⓘ

Type	RFC2833 ⓘ
DTMF Code Transport format	Disabled ⓘ
Payload	101 ⓘ (96-127) ⓘ

Table A51 - MyBell IP Premium Indoor Monitor - Door unlock by DTMF code configuration

Setting	Description
Type	Select a DTMF type from the following options: <ul style="list-style-type: none"> • Info. • RFC 2833. • Info+Inband. • Info+RFC 2833.
DTMF Code Transport Format	Select it only when the third-party device receiving the DTMF code adopts the Info transport format. Info transfers the DTMF code through signaling. Other transport format does it through RTP audio packet transmission. Select the DTMF transferring format according to the third-party device from the following options: <ul style="list-style-type: none"> • Disable. • DTMF. • DTMF-Relay. • Telephone-Event. For example, select Telephone-Event if the third-party device adopts the telephone-event.
Payload	Select the payload 96-127 for data transmission identification.

Note

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

16.3.2 - Door unlock through HTTP command

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

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

Intercom > Relay > Open Relay via HTTP.

Switch ⓘ

Username ⓘ

Password ⓘ

Remote Open Relay Via HTTP AllowList ⓘ

1st IP

2st IP

3st IP

4st IP

5st IP

Table A52 - MyBell IP Premium Indoor Monitor - Door unlock through HTTP command

Setting	Description
Switch	Enable it to allow the relay to be triggered remotely using HTTP command.
Username	Enter the device username to be used as a part of the HTTP command to trigger the local relay. For example, admin .
Password	Enter the device password to be used as part of the HTTP command to trigger the local relay. For example, 12345 . Please refer to the following example: http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1
Remote Open Relay Through HTTP Allowlist	Enable it and enter, for example, the IP address of the server that enables sending the HTTP command to the indoor monitor to trigger the local relay.

Note





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

17 FIRMWARE UPGRADE

To upgrade the device firmware for the indoor monitors by the device web interface:

Upgrade > Basic.

Basic ?

Firmware Version	5.67.30.1.209	?
Hardware Version	1.0	?
Upgrade	 Import	?
Factory Default	 Reset	?
Reset Config	 Reset	?
Reboot	 Reboot	?

Note


Firmware files should be in **ZIP** format for an upgrade.

18 BACKUP

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

Upgrade > Advanced > Others.

Others ?

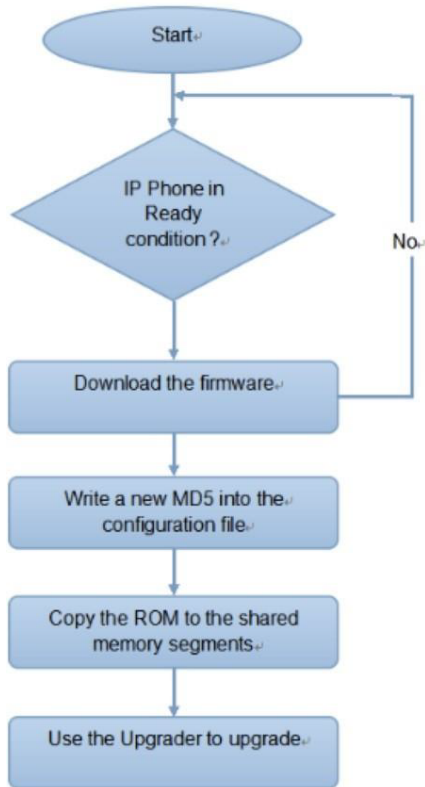
Config File  Import  Export (Encrypted) ?

19 AUTO-PROVISIONING THROUGH CONFIGURATION FILE

19.1 - 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 MyBell intercom devices to access the URL address of the third-party server which stores configuration files and firmware used to update the firmware and the corresponding settings on the device.

See the flow chart below:



19.2 - Introduction to configuration files for auto-provisioning

Configuration files have two following formats for auto-provisioning:

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

Note

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

19.3 - Autop

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

To set up the schedule by the device web interface:

Upgrade > Advanced > Automatic Autop.

The screenshot shows the 'Automatic Autop' configuration page. It features several settings:

- Mode:** A dropdown menu set to 'Repeatedly'.
- Schedule:** A dropdown menu set to 'Sunday'.
- Time:** A text input field containing '22' with a '(0-23Hour)' label.
- Minutes:** A text input field containing '0' with a '(0-59Min)' label.
- ExportAutop Template:** A blue button labeled 'Export'.
- Clear MDE:** A blue button labeled 'Clear'.

Table A53 - MyBell IP Premium Indoor Monitor - Autop configuration

Setting	Description
Power On	Select Power On if you want the device to perform Autop every time it boots up.
Repeatedly	Select Repeatedly if you want the device to perform autop according to the schedule you set up.
Power On + Repeatedly	Select Power On + Repeatedly if you want to combine Power On mode and Repeatedly mode, which enable the device to perform Autop every time it boots up or according to the schedule you set up.
Hourly Repeat	Select Hourly Repeat if you want the device to perform Autop every hour.

19.4 - DHCP provisioning configuration

Auto-provisioning URL can be obtained using DHCP option which enables the device to send a request to a DHCP server for a specific DHCP option code.

To use Custom Option as defined by users with option code (ranging from 128-255), configure DHCP Custom Option by the web interface:

Upgrade > Advanced > Automatic Autop.

Automatic Autop ?

Mode: ?

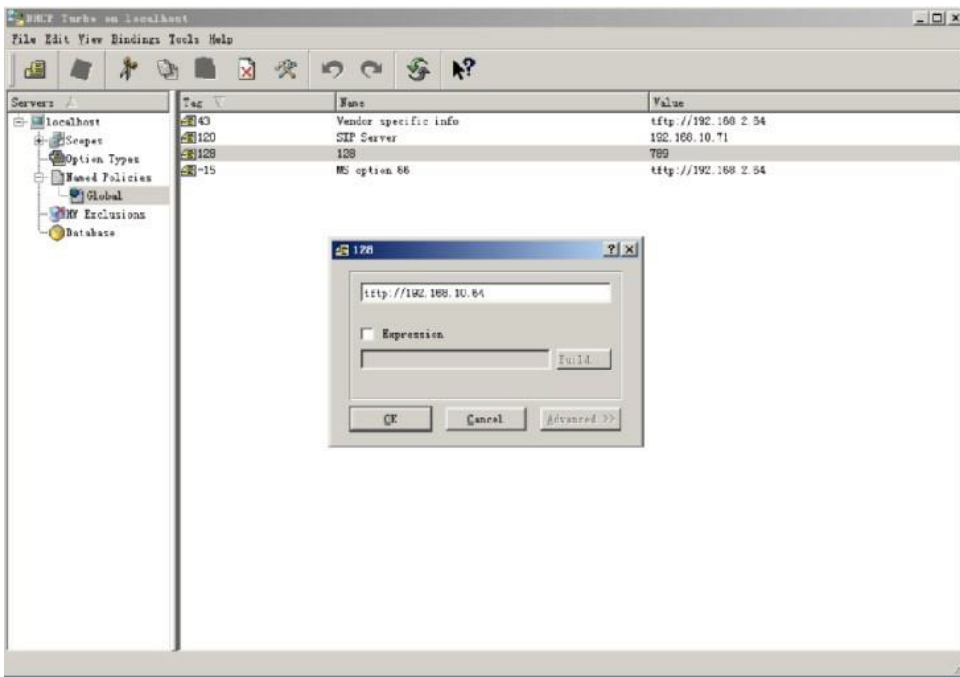
Schedule: ?

(0-23Hour)

(0-55Min)

Export Autop Template: ?

Clear MD5: ?



Note

The custom Option type must be a string. The value is the URL of the TFTP server.

DHCP Option ?

Custom Option: (128-254) ?

DHCP Option Enabled: Custom Option Option 43 Option 66 ?

Table A54 - MyBell IP Premium Indoor Monitor - DHCP provisioning configuration	
Setting	Description
Custom Option	Enter the DHCP code matched with corresponding URL so that device finds the configuration file server for the configuration or upgrading.
DHCP Option 66	If none of the above is set, the device automatically uses DHCP Option 66 for getting the upgrade of the server URL. This is done within the software and the user doesn't need to specify this. To make it work, configure the DHCP server for option 66 with the update of the server URL in it.
DHCP Option 43	If the device doesn't get an URL from DHCP Option 66, it automatically uses DHCP Option 43. This is done within the software and the user doesn't need to specify this. To make it work, configure the DHCP server for option 43 with the update of the server URL in it.

Note

The general configuration file for the in-batch provisioning is in the **CFG** format. For R29 it is r000000000029.cfg (10 zeros in total). The MAC-based configuration file for the specific device provisioning is in the **MAC_Address** format of the device.cfg, for example, 0C 110504AE5B.cfg.

19.5 - Static provisioning configuration

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

To configure static provisioning:

Upgrade > Advanced > Manual Autop.

Table A55 - MyBell IP Premium Indoor Monitor - Static provisioning configuration	
Setting	Description
URL	Set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
Username	Set up a username if it is required to access the server, otherwise leave it blank.
Password	Set up a password if it is required to access 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 does't provide user specified server.
- Please prepare the TFTP/FTP/HTTP/HTTPS servers by yourself.

19.6 - Voice assistant

The voice assistant **Albert** can be configured to perform a variety of functions related to intercom calls such as open-door or arming modes on the device. You can also set up the specific relay to be triggered by the voice assistant for the door access control.

To configure the voice assistant on device:

Settings > Voice Assistant.

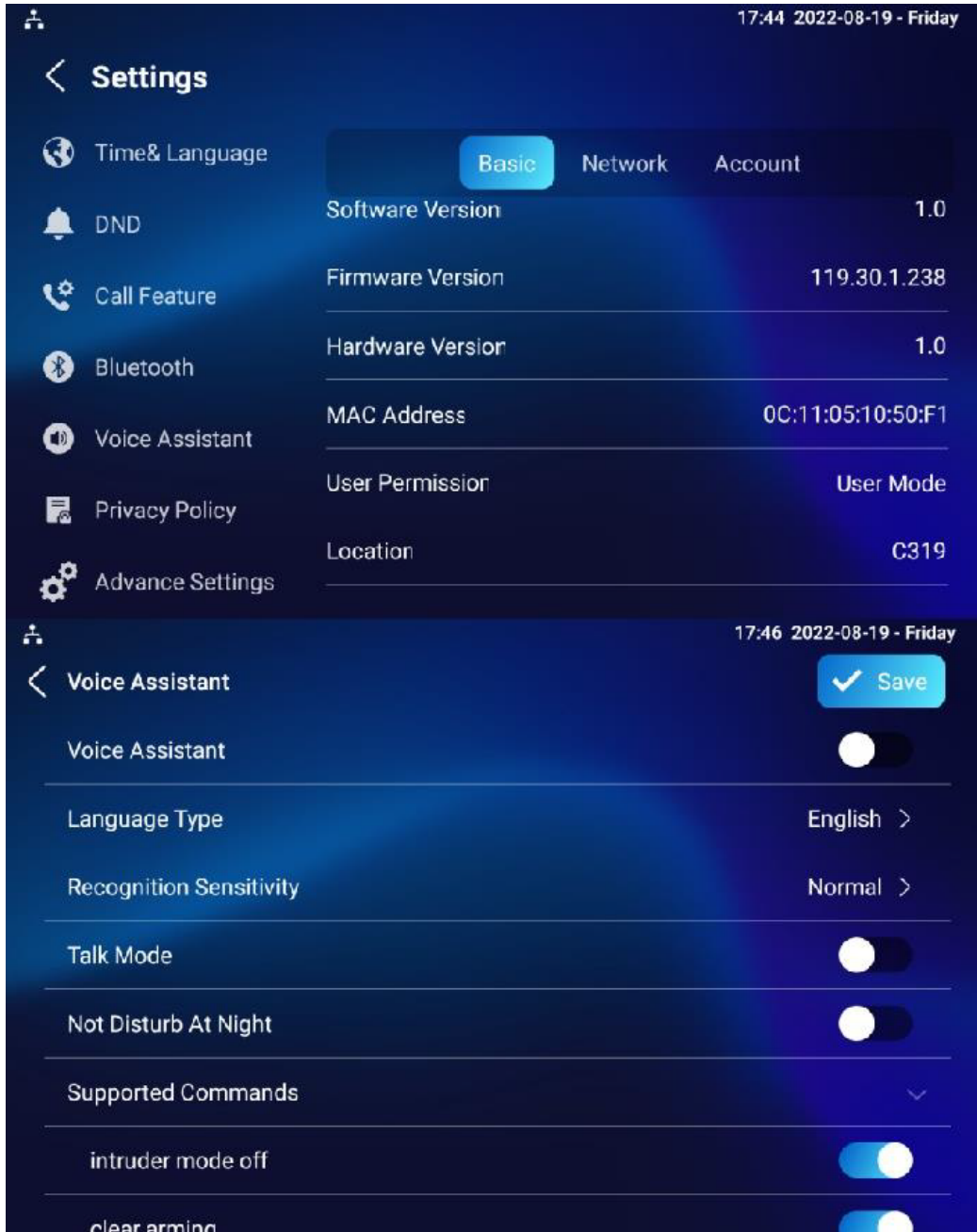


Table A56 - MyBell IP Premium Indoor Monitor - Voice assistant configuration

Setting	Description
Language Type	Select the language.
Recognition Sensitivity	Adjust the voice assistance recognition sensitivity, choose from the following options: <ul style="list-style-type: none"> • Low. • Normal. • High.
Talk Mode	Move the toggle switch to the right if you want to enable this mode. When the talk mode is enabled, the voice assistant stays on to receive your voice commands for 30 seconds, you don't need to call Albert again to wake up the voice assistant. If you disable it, the voice assistant wakes up again for each voice command.
Not Disturb At Night	Move the toggle switch to the left to enable this function. It is used when you want the voice assistant to stay silent while carrying out your voice commands.
Supported Command	Enable or disable the voice commands.

Table A57 - MyBell IP Premium Indoor Monitor - Voice commands

No.	Voice Command	Description	Voice Prompt
1.	Intruder mode off	Use it to clear the arming mode when the arming alarm is triggered. (You are required to enter the disarm password in the pop-out window initiated by the voice assistant.)	<ul style="list-style-type: none"> • Please input password.
2.	Clear arming	Use it to clear the arming mode when the arming alarm is triggered. (You are required to enter the disarm password in the pop-out window initiated by the voice assistant.)	<ul style="list-style-type: none"> • Please input password.
3.	Night mode	Use it to change the arming mode to night mode.	<ul style="list-style-type: none"> • Started it, sweet dreams! • Made it, good night. • Sure, sleep mode is on. • OK, start sleep mode, have a good night. • Alright, sleep mode is opened, have a nice dream.
4.	Sleep mode	Use it to change the arming mode to sleep mode.	<ul style="list-style-type: none"> • Sure, sleep mode is on. • OK, start sleep mode, have a good night. • Alright, sleep mode is opened, have a nice dream. • Made it, good night. • Started it, sweet dreams!
5.	Away mode	Use it to change the arming mode to away mode.	<ul style="list-style-type: none"> • Sure, away mode is on. • OK, start away mode. • Alright, away mode is opened. • Made it, have a good day. • Done, away mode is started.
6.	Home mode	Use it to change the arming mode to home mode.	<ul style="list-style-type: none"> • Sure, home mode is on. • OK, start home mode. • Alright, home mode is opened. • Made it. • Done, home mode is started.
7.	Open door	Use it to open the door.	<ul style="list-style-type: none"> • Sure, the door is open. • The door is open for you. • No problem, open the door. • Opened, always here for you. • Yep, door is opened now.
8.	Open the door	Use it to open the door.	<ul style="list-style-type: none"> • Sure, the door is open. • The door is open for you. • No problem, open the door. • Opened, always here for you. • Yep, door is opened now.
9.	Disable DND	Use it to disable the DND mode.	<ul style="list-style-type: none"> • Yes, closed it for you. • Welcome back, DND is off. • DND is closed, to mingle with the world. • Sure, DND is off.
10.	Enable DND	Use it to enable the DND mode.	<ul style="list-style-type: none"> • OK, DND is on. • Done, enjoy yourself. • DND is on, feel your inner peace. • Turn on it now.
11.	Emergency	Use it to dial SOS number.	<ul style="list-style-type: none"> • Got it, calling SOS as soon as possible. • Okay, be relaxed, making an emergency call now. • Calling ambulance now. • Calling SOS now, please hold on. • God bless you, calling emergency now. • Hold on please, calling emergency right now. • Take it easy, calling emergency right now.

Table A57 - MyBell IP Premium Indoor Monitor - Voice commands

No.	Voice Command	Description	Voice Prompt
12.	Help me	Use it to dial SOS number.	<ul style="list-style-type: none"> • Got it, calling SOS as soon as possible. • Okay, be relaxed, making an emergency call now. • Calling ambulance now. • Calling SOS now, please hold on. • God bless you, calling emergency now. • Hold on please, calling emergency right now. • Take it easy, calling emergency right now.
13.	Call manager	Use it to call manager you name set up in the phonebook.	<ul style="list-style-type: none"> • Please choose one for calling. • Sorry I didn't get that.
14.	Call staff	Use it to call staff you named and set up in the phonebook.	<ul style="list-style-type: none"> • Please choose one for calling. • Sorry I didn't get that.
15.	Call carer	Use it to call carer you named and set up in the phonebook.	<ul style="list-style-type: none"> • Please choose one for calling. • Sorry I didn't get that.
16.	Open message	Use it to check text messages.	<ul style="list-style-type: none"> • Got it, please check. • OK, message is opened, you can write some content to send. • Message is ready for you. • Already opened it for you.
17.	Open monitor	Use it to check monitor.	<ul style="list-style-type: none"> • Got it, please check.
18.	Homepage	Use it to go to the home screen.	<ul style="list-style-type: none"> • Home page is already for you. • Already got it for you.
19.	Enable mute	Use it to mute your voice on the indoor monitor so that the caller or callee can't hear you.	<ul style="list-style-type: none"> • OK, mute is on. • Done, enjoy yourself. • Mute is on, feel your inner peace. • Set it now.
20.	Disable mute	Use it to unmute your voice on the indoor monitor so that the caller or callee can hear you.	<ul style="list-style-type: none"> • Sure, mute is off. • Mute is closed, to mingle with the world. • Welcome back, mute is off. • Yes, closed it for you.
21.	Shut down/cancel	Use it to turn off the voice assistant function.	<ul style="list-style-type: none"> • See you. • See you later. • Bye. • Good bye. • See you next time. • Bye, best regards. • See you, have a great time.
22.	Answer Call Permission	Enable it to answer or reject the incoming call through voice assistant by replying Yes or No .	<ul style="list-style-type: none"> • The call is coming, do you want to accept it? Yes or No? • OK, here for you. • Sure, hung up now.
23.	Call Fuzzy Match	Enable it to allow the fuzzy match of the manager calls. For example, if you have multiple manager call contacts: manager1, and manager2, you are required to select the specific manager call contact when using Call manager voice command.	

To enable the voice assistant and set the voice assistant-controlled relay by the web interface:

Settings > Voice Assistant > Voice Assistant Setting.

Tick the checkbox to enable the voice assistant function. Then go to **Voice Command Setting** to select a specific relay to be triggered using voice assistant.



Setting:

- **Unlock type:** select the type of relay to be triggered by the voice assistant for the predefined action, for example, door opening.

19.7 - Call log

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

To check call logs by the device web interface:

Contacts > Call Log.

Call Logs ⓘ

Capture Delay (Sec) ⓘ

Upper Limit ⓘ

Call History Export Hang Up ⓘ

Index	Type	Date	Time	Local Identity	Name	Number
1	Missed	29-12-2020	7:19:33 AM	192.168.0.32@192.168.0.32	manager	192.168.0.31@192.168.0.31
2	Received	29-12-2020	1:55:27 AM	192.168.0.32@192.168.0.32	192.168.13.142	192.168.13.142@192.168.13.142
3	Dialed	29-12-2020	1:42:22 AM	192.168.0.32@192.168.0.32	192.168.13.157	192.168.13.157@192.168.13.157

Delete Delete All Prev 1/1 Next 1 Go

Cancel Submit

Table A58 - MyBell IP Premium Indoor Monitor - Call log

Setting	Description
Capture Delay	Set the image capturing starting time when the device goes into video preview.
Upper Limit	Set the maximum screenshot storage capacity, when the capacity is reached the previous screenshots are overwritten.
Call History	Select call history (All, Dialed, Received, Missed, Forwarded).
Local Identity	Display the door phone SIP account or IP number that receives incoming calls.
Name/Number	Select the Name and Number options to search call log by the name or by the SIP or IP number.

To check call log on the device:

Call > Call Logs.



20.1 - System log for debugging

20.1.1 - Capturing system log for debugging

System logs can be used for debugging purposes.

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

Upgrade > Diagnosis > System Log.

Table A59 - MyBell IP Premium Indoor Monitor - Debug

Setting	Description
LogLevel	Select log level from 1 to 7. The technical staff instructs about the specific log level to be entered for debugging purpose. The default log level is 3 . The higher the level, the more complete the log.
Export Log	Click the Export tab to export the temporary debug log file to a local PC.
Export Debug Log	Click the Export tab to export the debug log file to a local PC.
Remote System Log	Select Enable or Disable if you want to enable or disable the remote system log.
Remote System Server	Enter the remote server address to receive the system log, the remote server address is provided by the technical support.

20.2 - PCAP for debugging

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

To set up PCAP by the device web interface:

Upgrade > Diagnosis > PCAP.

Table A60 - MyBell IP Premium Indoor Monitor - PCAP configuration

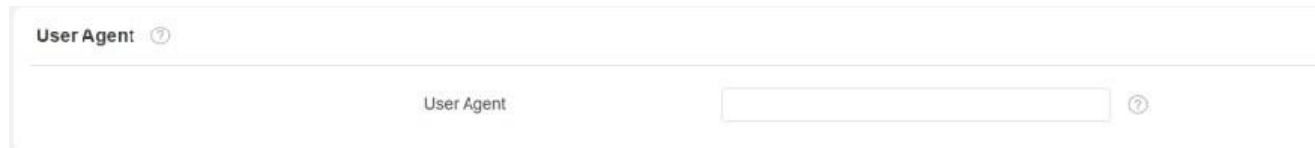
Setting	Description
Specific Port	Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
PCAP	Click the Start tab and Stop tab to capture a certain range of data packets before clicking Export tab to export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

20.3 - User agent

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

To configure the user agent by the web interface:

Account > Advanced.



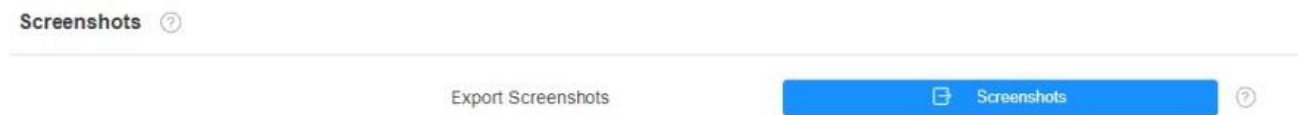
The screenshot shows a web interface for configuring the User Agent. At the top left, there is a header "User Agent" with a help icon (question mark in a circle). Below this, there is a label "User Agent" followed by an empty text input field and another help icon.

20.4 - Screenshots

You can take screenshots of specific device screens to help with the troubleshooting.

To take screenshots:

Upgrade > Diagnosis > Screenshots, then click **Screenshots**.



The screenshot shows a web interface for the Screenshots section. At the top left, there is a header "Screenshots" with a help icon. Below this, there are two buttons: "Export Screenshots" and "Screenshots". The "Screenshots" button is highlighted in blue and has a help icon to its right.

21 DEVICE INTEGRATION WITH THIRD PARTY

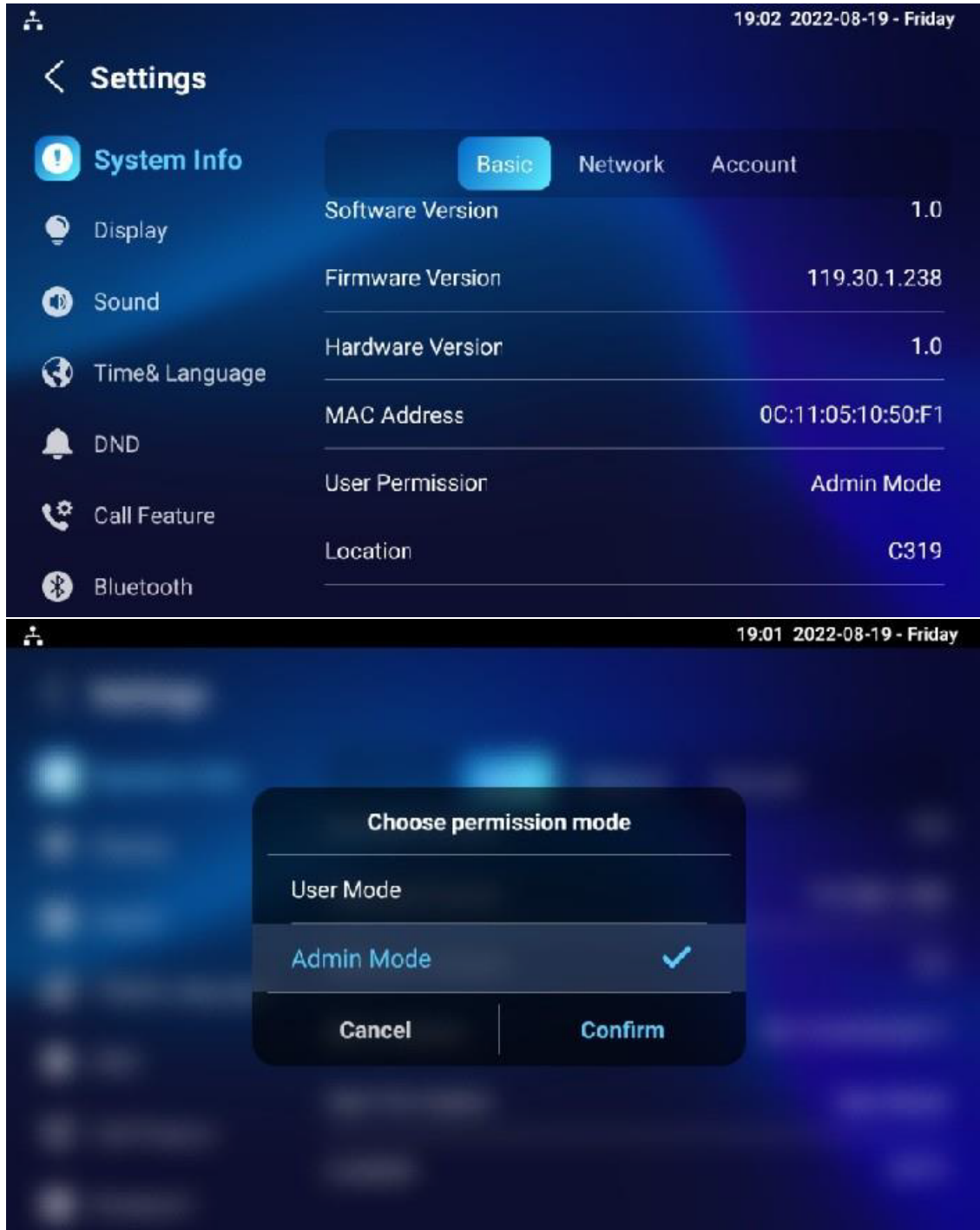
21.1 - Entering applications screen

You can enter the APK interface through hidden operations.

To configure this function on device:

Settings > System Info.

Press **User Mode** 10 times > **Admin Mode** > **Confirm.**



21.2 - Third-party app installation

To install the third-party App to your device by the device web interface:

Device > Third Party APK.

Choose a suitable **APK** file from PC to upload. To clear the **APK** file uploaded, click **Reset**.



To configure the installed third-party app, click **App Name** field to select the specific name of the installed **APK** files for configuration. Then tick the check boxes of the configuration you need.

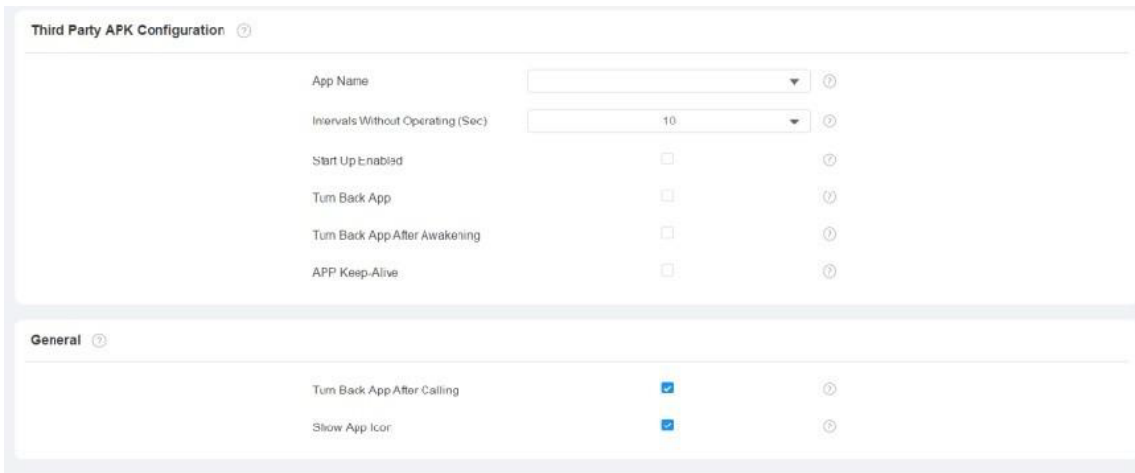


Table A61 - MyBell IP Premium Indoor Monitor - Third-party app configuration

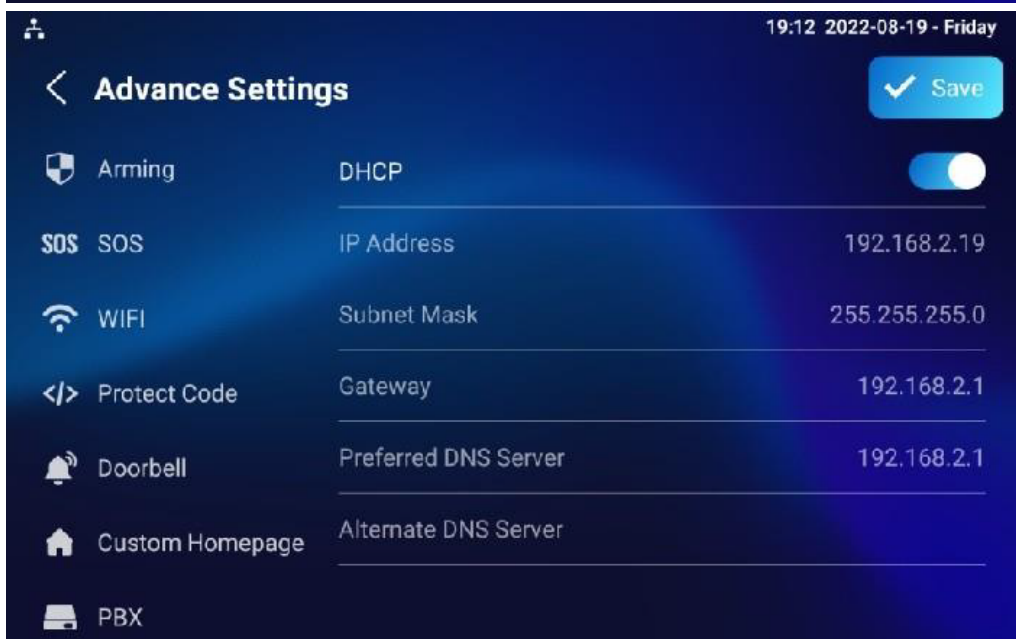
Setting	Description
App Name	Select the App Name to be configured.
Interval Without Operating (sec)	Tick this checkbox to set the app returning time-interval when there is no operation on the device.
Start Up Enable	Tick this checkbox to set the app to run automatically when the device is turned on.
Turn Back App After Awakening	Tick this checkbox to set the device to return to the app when the screen is awake.
APP Keep-Alive	Tick this checkbox to set the app to stay on.
Turn Back App After Calling	Tick this checkbox to set the app to return automatically after finishing a call (this feature applies to all apps).
Show App Icon	Tick this checkbox to set the app icon to be displayed on the screen.

21.3 - PBX feature

The Android indoor monitor has a built-in PBX server which allows the indoor monitor to serve as an intercom monitor and a SIP PBX. Users don't need to prepare extra SIP PBX. The PBX supports the features such as call, forward, transfer, conference and ring group. You can configure it on the device or by the web interface.

To configure it on the device:

Go to **Advanced Settings**.



21.3.1 - PBX configuration on device

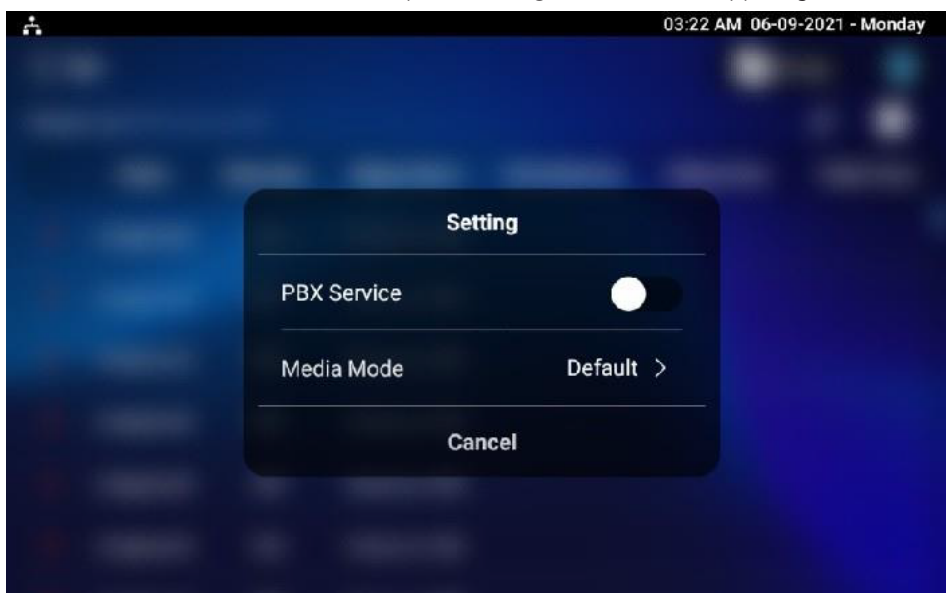
To check and manage SIP accounts, enable the PBX feature on the device.

To enable this feature:

Advance Settings > PBX.

21.3.2 - Enabling PBX service

To enable PBX, in the PBX interface, tap the **Settings** icon  in the upper right corner.



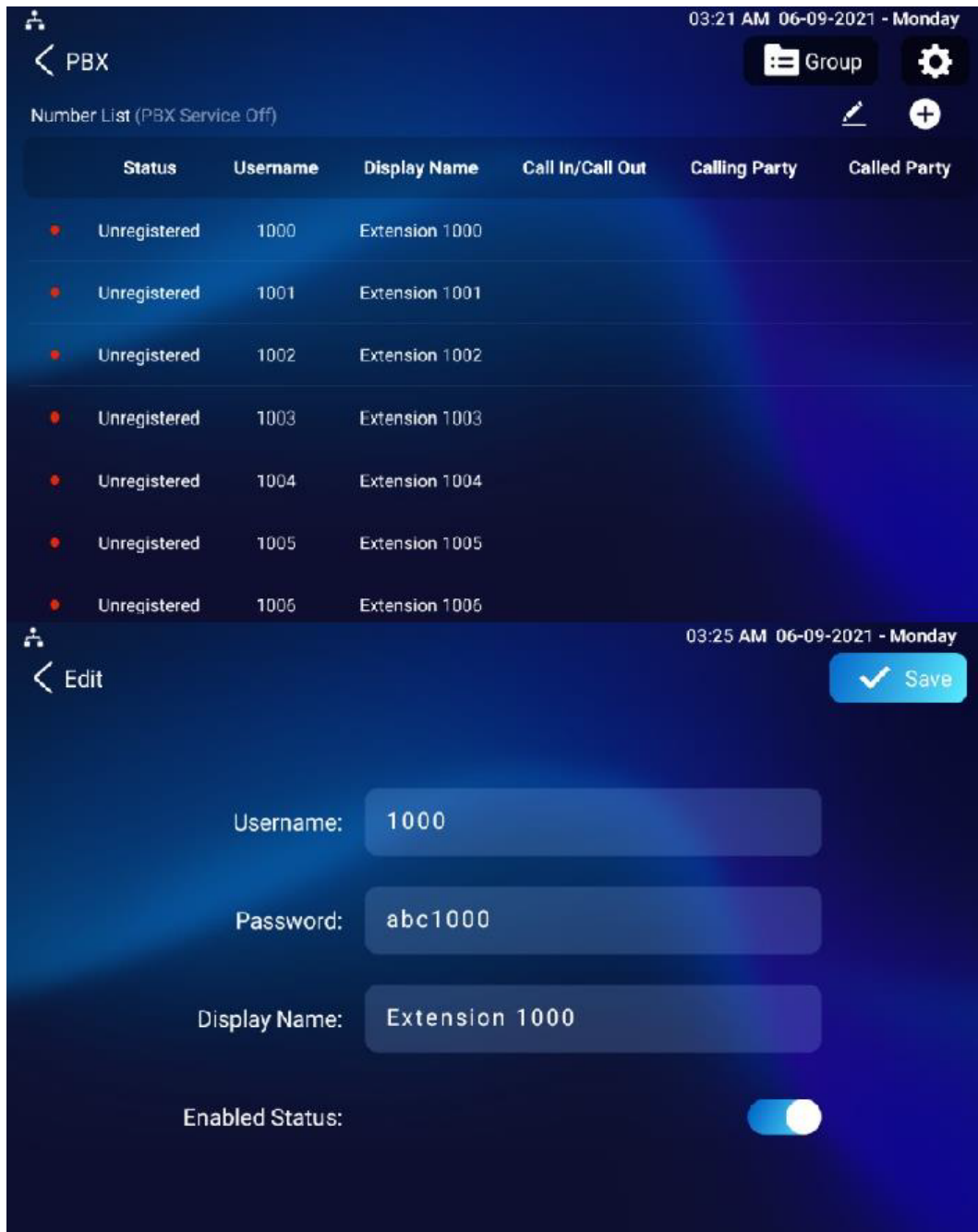
Setting:

• **Media mode:**

- **Default** if the intercom devices are deployed in the same LAN network.
- **Bypass** if the intercom devices are deployed in the different LAN networks where PBX serves as a bridge or a media for the network data transmission.

21.3.3 - PBX accounts management

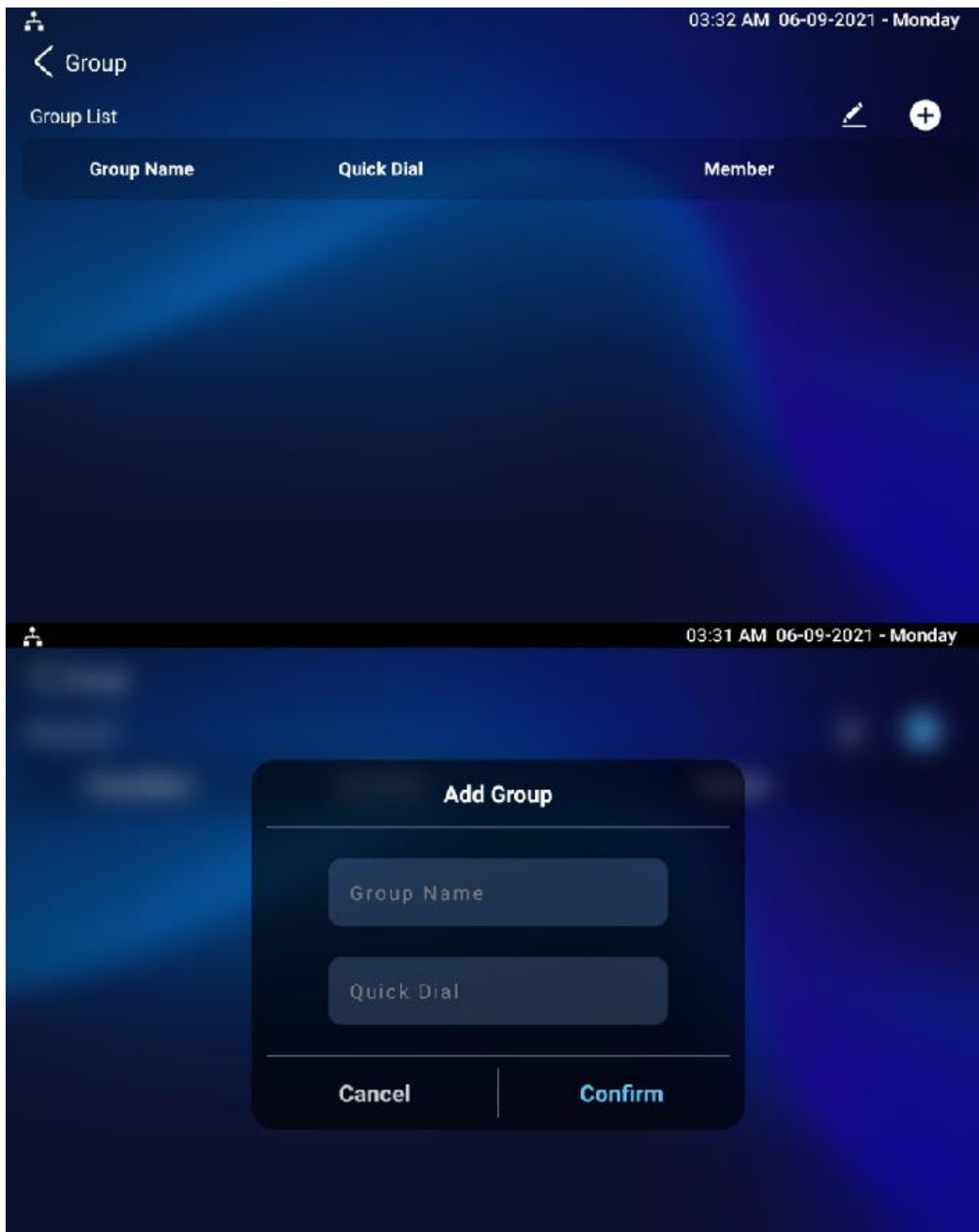
You can check the basic PBX information such as PBX server, port and accounts status.



Setting	Description
Status	Show whether the account is registered or not.
Username	Enter the extension number registered onto SIP server.
Display Name	Enter the display name of this account, it's shown on other devices when making calls.
Password	Enter the password of the corresponding users.
Enabled Status	Activate SIP account.
Call IN/Call Out	Shows the calling status of this account.
Calling Party	Shows the calling party number.
Caller Party	Shows the caller party number.

21.3.4 - PBX groups management

Click **Group** in the top right corner to add a new ring group or edit the existing group. One number can be added in different ring groups. Once receiving an incoming call, the numbers in one group ring up at the same time.



Setting:

- **Group Name:** the name of a ring group.
- **Quick Dial:** the number of this ring group.

21.3.5 - PBX configuration by web interface

To do the same configuration by the web interface:

PBX > Basic,

and

PBX > Ring Group.

PBX Basic

PBX Service Enabled

PBX Status: Stopped

Media Model: Default

PBX Port: 5070

+ Add

Index	Username	Password	Display Name	Status	Edit
1	1000	abc1000	Extension 1000	InRegistered	
2	1001	abc1001	Extension 1001	InRegistered	
3	1002	abc1002	Extension 1002	UnRegistered	
4	1003	abc1003	Extension 1003	UnRegistered	
5	1004	abc1004	Extension 1004	UnRegistered	
6	1005	abc1005	Extension 1005	UnRegistered	
7	1006	abc1006	Extension 1006	UnRegistered	
8	1007	abc1007	Extension 1007	UnRegistered	
9	1008	abc1008	Extension 1008	UnRegistered	
10	1009	abc1009	Extension 1009	UnRegistered	

Delete Delete All Prev 1/10 Next 1 Go

FBX » Ring Group

Group Setting

+ Add

Index	Group Name	Quick Dial	Member	Edit
 No Data				

Delete Delete All Prev 1/1 Next 1 Go

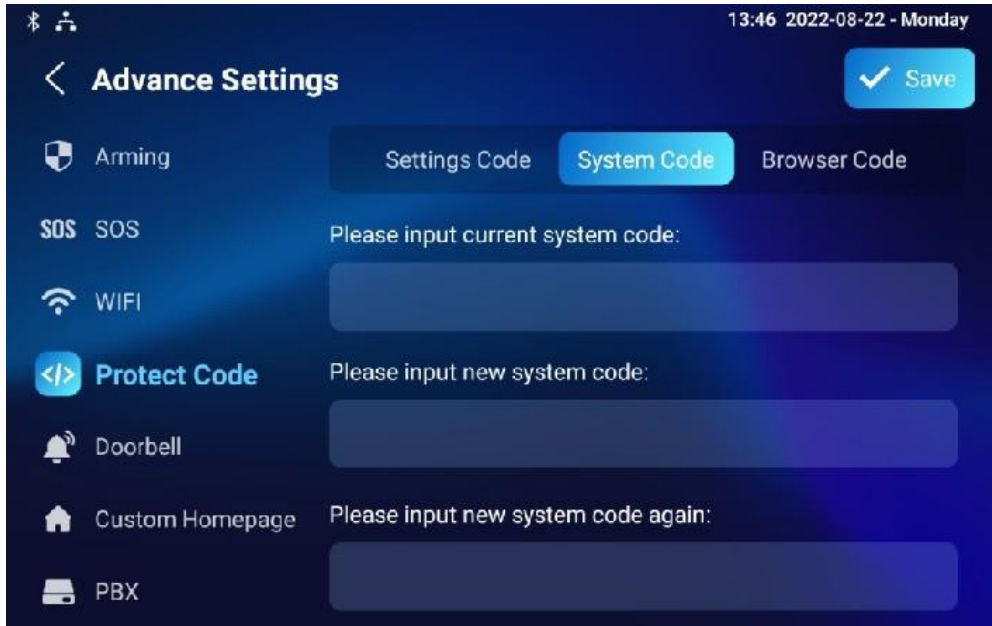
22 PASSWORD MODIFICATION

22.1 - Device basic setting password modification

To modify the basic setting password on device:

Settings > Advanced Settings > Protected Code.

Choose **System Code** to change a new password. The default password is **123456**.



The screenshot shows the 'Advance Settings' screen on a mobile device. At the top, there is a back arrow, the title 'Advance Settings', and a 'Save' button with a checkmark. Below the title, there are three tabs: 'Settings Code', 'System Code' (which is selected and highlighted in blue), and 'Browser Code'. The main content area lists several settings: 'Arming', 'SOS', 'WIFI', 'Protect Code', 'Doorbell', 'Custom Homepage', and 'PBX'. The 'Protect Code' section is expanded, showing three input fields: 'Please input current system code:', 'Please input new system code:', and 'Please input new system code again:'. Each input field is a dark blue rounded rectangle.

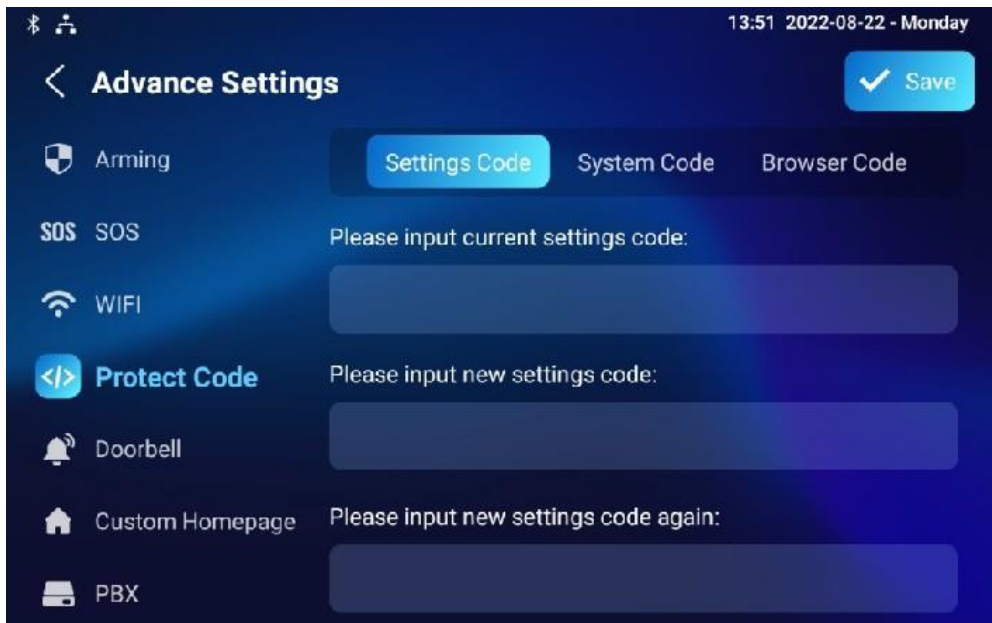
22.2 - Device advanced setting password modification

This password is used to enter the advanced settings of the device, such as password settings, account numbers, SOS numbers, network settings.

To modify the advanced setting password on device:

Settings > Advanced Settings > Protected Code > Setting Code.

The default password is **123456**.



The screenshot shows the 'Advance Settings' screen on a mobile device. At the top, there is a back arrow, the title 'Advance Settings', and a 'Save' button with a checkmark. Below the title, there are three tabs: 'Settings Code' (which is selected and highlighted in blue), 'System Code', and 'Browser Code'. The main content area lists several settings: 'Arming', 'SOS', 'WIFI', 'Protect Code', 'Doorbell', 'Custom Homepage', and 'PBX'. The 'Protect Code' section is expanded, showing three input fields: 'Please input current settings code:', 'Please input new settings code:', and 'Please input new settings code again:'. Each input field is a dark blue rounded rectangle.

22.3 - Device web interface password modification

To modify the password by the web interface:

Security > Basic > Web Password Modify.

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



Note

There are two accounts:

- **admin** - password: admin.
- **user** - password: user.

22.4 - Browser password modification

This password is used to lock the browser on the device in case someone uses the browser for any unwanted applications.

To modify the browser password on device:

Settings > Advanced Settings > Protected Code > Browser Code.

The default password is **123456**.

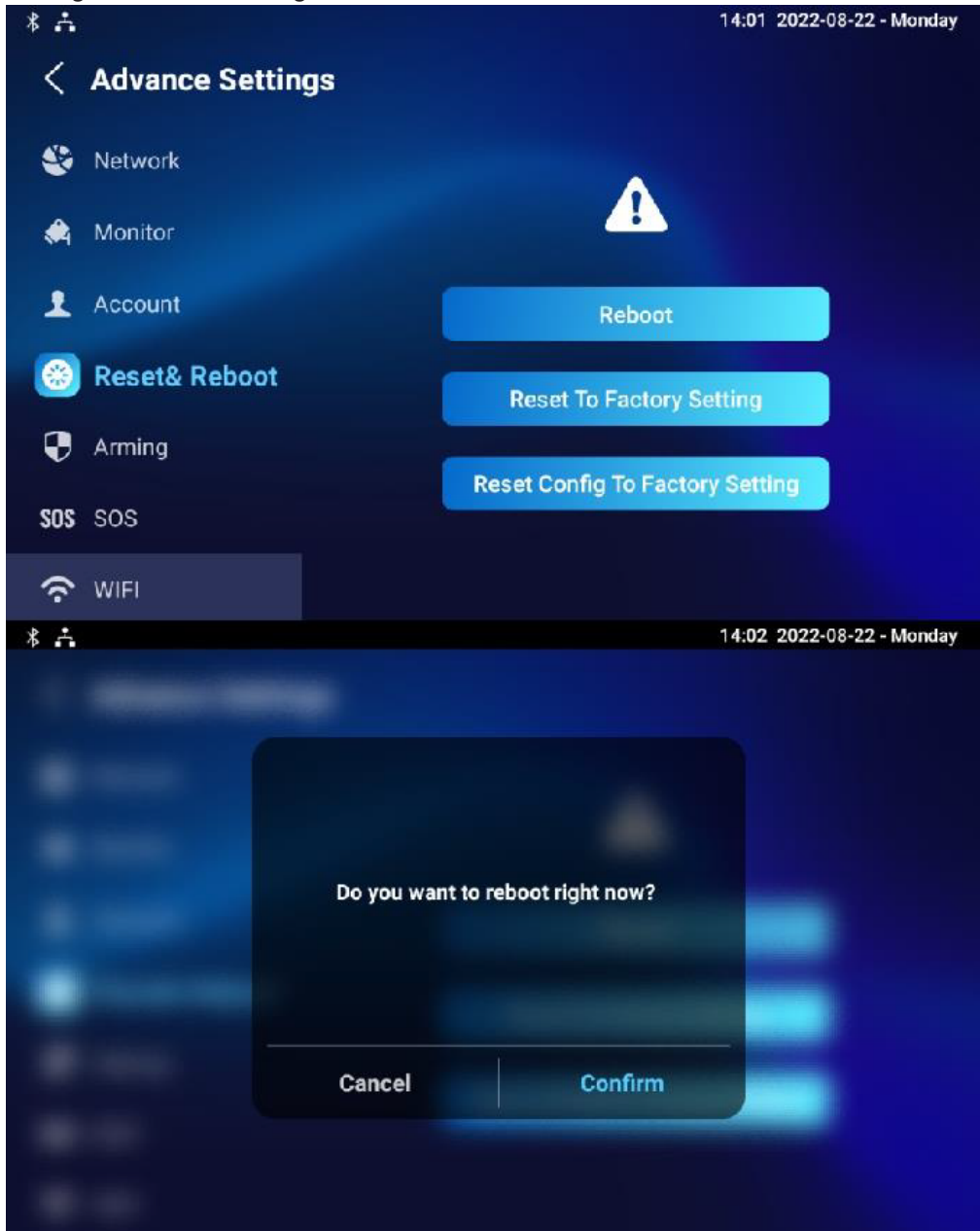


23 SYSTEM REBOOT AND RESET

23.1 - Reboot on device

If you want to restart the system setting of the device, you can operate it directly on the device setting screen or by the device web interface. To restart to the system setting on device:

Settings > Advance Settings > Reset&Reboot.



23.2 - Reboot by web interface

To reboot the system by the web interface:

Upgrade > Basic.

You can also set up a schedule for the device to be restarted.

Basic [?](#)

Firmware Version	567.30.1.209	?
Hardware Version	1.0	?
Upgrade	Import	?
Factory Default	Reset	?
Reset Config	Reset	?
Reboot	Reboot	?

To configure the device restart schedule by the web interface:

Upgrade > Advanced > Reboot Schedule.

Reboot Schedule ?

Switch ?

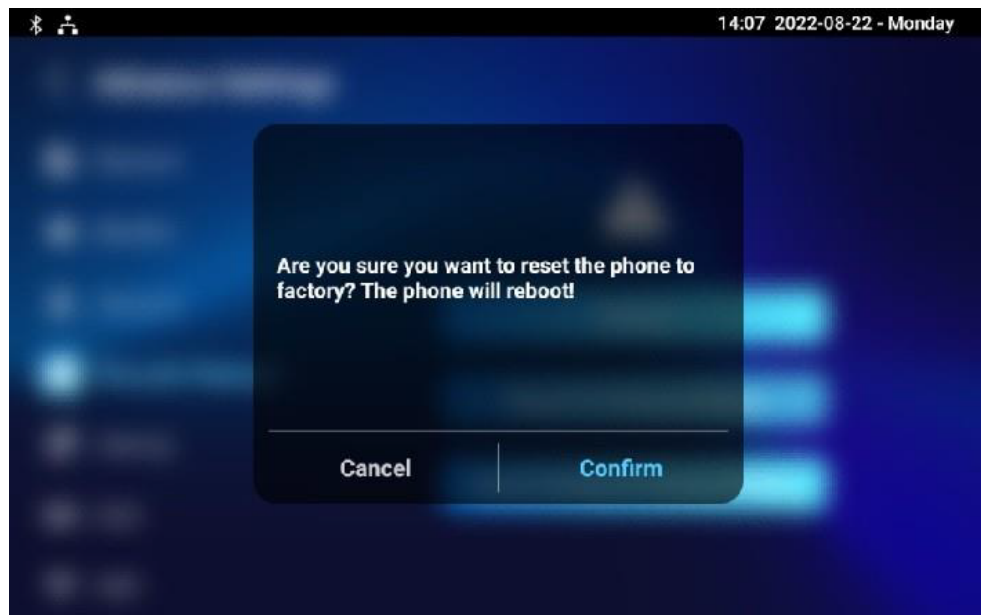
Schedule ?

(0-23Hour)

23.3 - Reset on device

To reset the whole device system to the factory setting:

Settings > Advance Settings > Reset&Reboot.



To reset only the configuration file to the factory setting, press **Reset Config To Factory Setting** tab.

23.4 - Reset by web interface

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

Upgrade > Basic

Basic ?

Firmware Version	567.30.1.209	?
Hardware Version	1.0	?
Upgrade	<input type="button" value="Import"/>	?
Factory Default	<input type="button" value="Reset"/>	?
Reset Config	<input type="button" value="Reset"/>	?
Reboot	<input type="button" value="Reboot"/>	?

To reset only the configuration file to the factory setting, click **Reset Config** on the same page.

24 REGULATIONS

24.1 - 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, ABNORMAL MECHANICAL 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.

24.2 - Declaration of conformity



Hereby, Nice-Polska Sp. z o.o. declares that MyBell IP 1-button Kit is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.manuals.fibaro.com

24.3 - 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.



Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com