

MyBell

IP Indoor Monitor

CE

EN - Instructions and warnings for installation and use

1 - IMPORTANT SAFEGUARDS AND WARNINGS	5
2 - DEVICE DESCRIPTION	6
3 - INTRODUCTION TO THE CONFIGURATION MENU	8
4 - ACCESS TO THE DEVICE	9
4.1 - Device home screen type selection	9
4.2 - Access to the device setting on the device	9
4.3.1 - Access to the device basic setting	9
4.3.2 - Access to the device advanced setting	9
4.4 - Access to the device setting by the web interface	10
5 - LANGUAGE AND TIME SETTING	11
5.1 - Language setting	11
5.1.1 - Language setting on the device	11
5.1.2 - Language setting by the web interface	11
5.2 - Time setting	11
5.2.1 - Time setting on the device	11
5.2.2 - Time setting by the device web interface	12
5.2.3 - Daylight saving time setting	12
6 - SCREEN DISPLAY CONFIGURATION	13
6.1 - Screen display setting on the device	13
6.2 - Screen display setting by the web interface	13
6.2.1 - Brightness and time setting by the device web interface	13
6.2.2 - Screen saver configuration	13
6.3 - Uploading a device booting image	14
6.4 - Icon screen display configuration	14
6.5 - Functional buttons display	15
7 - SOUND AND VOLUME CONFIGURATION	16
7.1 - Configuring volume on the device	16
7.2 - Configuring volume by the web interface	16
8 - NETWORK CONFIGURATION	17
8.1 - Configuring network connection on the device	17
8.2 - Configuring network connection by the web interface	17
8.3 - Device deployment in the network	18
8.4 - Device NAT setting	19
8.5 - VLAN setting	19
9 - PHONE BOOK CONFIGURATION	20
9.1 - Configuring the phone book on the device	20
9.1.1 - Adding a contact group on the device	20
9.1.2 - Adding contacts on the device	20
9.1.3 - Editing contacts on the device	21
9.1.4 - Blocklist setting on the device	22
9.2 - Phone book configuration by the web interface	20
9.2.1 - Contact group management by the web interface	20
9.2.2 - Blocklist setting by the web interface	23
9.2.3 - Contact display	23
9.2.4 - Contacts import and export by the web interface	23
10 - INTERCOM CALL CONFIGURATION	25
10.1 - IP call & IP call configuration	25
10.2 - SIP call & SIP call configuration	25
10.2.1 - SIP account registration	25
10.2.2 - SIP server configuration	26
10.2.3 - Outbound proxy server configuration	26
10.3 - DND	26
10.4 - Configuring the device local RTP	27
10.5 - Configuring a data transmission type	27
11 - DOOR ACCESS CONTROL CONFIGURATION	28
11.1 - Relay switch setting	28
11.1.1 - Local relay setting	28
11.1.2 - Remote relay switch setting	28

11.2 - Web relay setting	28
11.3 - Door unlock configuration	29
11.3.1 - Door unlock by the DTMF code	29
11.3.2 - Door unlock through a HTTP command	29
11.3.3 - Unlock by icon button	30
12 - CALL SETTING	31
12.1 - Call auto-answer configuration	31
12.2 - Auto-answer allow list setting	31
12.3 - Intercom preview setting	32
12.4 - SIP hacking protection	32
12.5 - Emergency call setting	32
12.5.1 - SOS icon display	32
12.5.2 - SOS number settings by the web interface	33
12.5.3 - SOS number settings on the device	33
12.6 - Multicast configuration	34
12.7 - Call forwarding setting	34
12.7.1 - Call forwarding configuration on the device	34
12.7.2 - Call Forwarding Configuration by the web interface	35
13 - INTERCOM MESSAGE SETTING	36
13.1 - Managing Text Messages	36
13.2 - Managing Voice Messages	36
14 - AUDIO & VIDEO CODEC CONFIGURATION FOR SIP CALLS	37
14.1 - Audio codec configuration	37
14.2 - Video codec configuration	37
15 - SECURITY	38
15.1 - Monitor setting	38
15.1.1 - Web camera setting by the web interface	39
15.1.2 - Web camera setting on the device	39
15.2 - Alarm and arming configuration	41
15.2.1 - Alarm and arming configuration on the device	41
15.2.2 - Alarm and arming configuration by the web interface	42
15.3 - Location-based alarm configuration	43
15.3.1 - Location-based alarm on the device	43
15.3.2 - Location-based alarm by the web interface	43
15.4 - Configuring the alarm text	44
15.5 - Configuring the arming mode	44
15.6 - Configuring alarm action	44
15.6.1 - Configuration of alarm action through HTTP command	45
15.6.2 - Configuration of alarm action through SIP message	45
15.6.3 - Configuring the alarm action through SIP message	46
15.7 - Checking alarm logs	46
15.8 - Screen unlock setting	46
15.9 - Screen unlock by PIN code	47
15.10 - Location-based alarm configuration	47
15.10.1 - Web server certificate	47
15.10.2 - Client certificate	47
15.11 - Power output setting	48
15.12 - High security mode	48
16 - FIRMWARE UPGRADE	49
17 - BACKUP	50
18 - AUTO-PROVISIONING	51
18.1 - Introduction to the configuration files for auto-provisioning	51
18.2 - Autop schedule	51
18.3 - Static provisioning configuration	52
18.4 - Call log	52
19 - DEBUG	54
19.1 - System Log for debugging	54
19.2 - PCAP for debugging	54
20 - PASSWORD MODIFICATION	55
20.1 - Modification of the device advanced setting password	55
20.2 - Modification of the device web interface password	55

21 - SYSTEM REBOOT & RESET	56
21.1 - Reboot on the device	56
21.2 - Reboot by the web interface	56
21.3 - Reset on the device	56
21.4 - Reset by the web interface	56
22 - REGULATIONS	57
22.1 - Warranty	57
22.2 - Declaration of conformity	57
22.3 - WEEE Directive Compliance	57

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

Table A1 - MyBell IP Indoor Monitor - Device description	
Feature	Description
Operation system	Linux
RAM	64MB
ROM	128MB
Front panel	plastic
Wi-Fi	no
Ethernet	2xRJ45, 10/100Mbps adaptive
Power over Ethernet (PoE)	802.3af Power-over-Ethernet
Power supply	PoE 48 V (IEEE802.3af) or 12V DC
RS485 port	supported
Alarm input	8
Relay output	1
Bell in	1
I/O	8
Microphone	-58dB
Speaker	4Ω / 2W
2-wire ports	2 pairs
Ethernet ports	1xRJ45, 10/100Mbps adaptive
Installation	wall-mounted & desktop
Dimension	200.2x132.2x27.2mm
Working humidity	10~90%
Working temperature	-10°C ~ +45°C
Storage temperature	-20°C ~ +70°C
Touch screen display mode	normally white, transmissive
Display	7-inch (176 mm) TFT LCD
Screen	7-inch capacitive touch screen
Screen resolution	800 x 480
Screen contrast ratio	500:1
Luminance	220 cd/m ²
Viewing angle	50° Left, 50° Right, 40° Upper, 50° Lower
Touch Screen	projected capacitive
Audio	SIP v1 (RFC2543), SIP v2 (RFC3261)
Narrowband audio codec	G.711a, G.711μ, G.729
Broadband audio codec	G.722
DTMF	Out-of-band DTMF (RFC2833), SIP Info
Echo cancellation	yes
Supported networking protocols	IPv4, HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, DHCP, ARP

Table A1 - MyBell IP Indoor Monitor - Device description

Feature	Description
Video streaming format	H.264
Auto-Provisioning	yes
Web management portal	yes
Web-based packet dump	yes
Configuration backup / restore	yes
Firmware upgrade	yes
System logs (including door access logs)	yes
Application scenario	Villas, Apartment complexes, Home automation systems, Modern interiors



3 INTRODUCTION TO THE CONFIGURATION MENU

Status ^	
Basic	Product Information
	Model
Account v	Firmware Version
	Location
Network v	
	Network Information
Phone v	Network Type
Contacts v	LAN Link Status
	LAN Subnet Mask
Upgrade v	LAN DNS1
Arming v	Primary NTP
Security v	Account Information
	Account1
DeviceSetting v	

Table A2 - MyBell IP Indoor Monitor - Configuration Menu

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

4 ACCESS TO THE DEVICE

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

4.1 - Device home screen type selection

The device supports two different home screen display modes:

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

To configure home page mode by the web interface:

Phone > Key/ Display

Choose one suitable mode for your scenarios.

Home Page Mode

Home Page Mode

Call list simple ▼

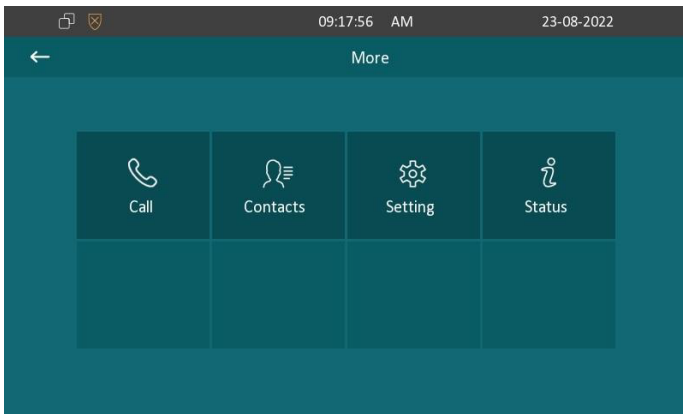
4.2 - Access to the device setting on the device

4.2.1 - Access to the device basic setting

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

To access the device basic setting:

More > Settings

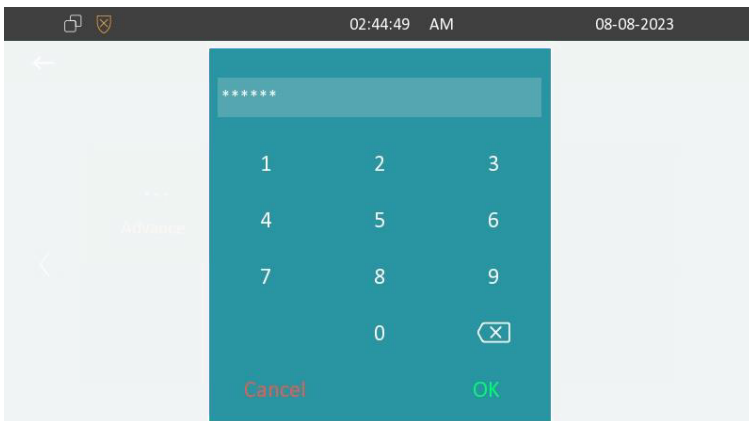


4.2.2 - Access to the device advanced setting

To access the device advanced basic setting:

More > Advance Settings

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



4.3 - Access to the device setting by the web interface

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

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

Login

The screenshot shows a mobile web interface with a dark teal background. At the top, there is a status bar with the time 06:51:03 AM and the date 10-05-2021. Below the status bar is a header with a back arrow and the word "Status". There are three tabs: "Basic", "Network" (which is selected and highlighted in orange), and "Account". The main content area displays network configuration details in a table-like format with horizontal lines separating rows.

Basic		Network		Account	
Type			DHCP		
IP Address			192.168.16.169		
Subnet Mask			255.255.255.0		
Gateway			192.168.16.1		
DNS1			8.8.8.8		

5 LANGUAGE AND TIME SETTING

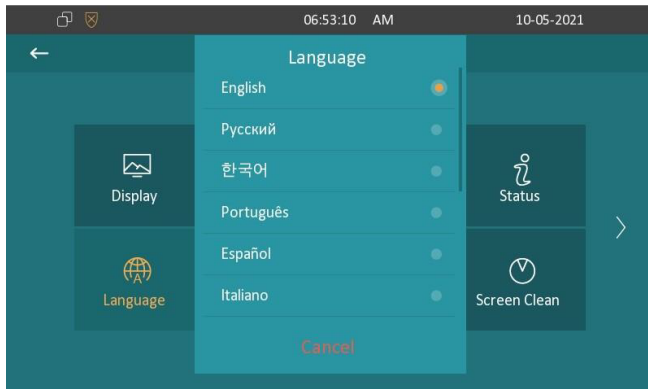
5.1 - Language setting

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

5.1.1 - Language setting on the device

To configure the language display on the device:

Settings > Language



5.1.2 - Language setting by the web interface

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

To configure the language display using the web interface:

Phone > Time/Lang

Web Language

Type English ▾

LCD Language

Type English ▾

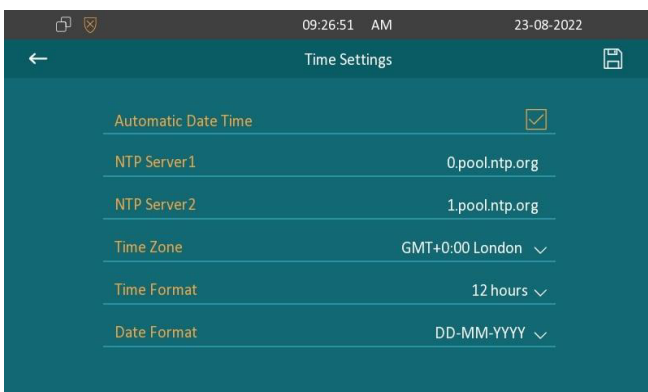
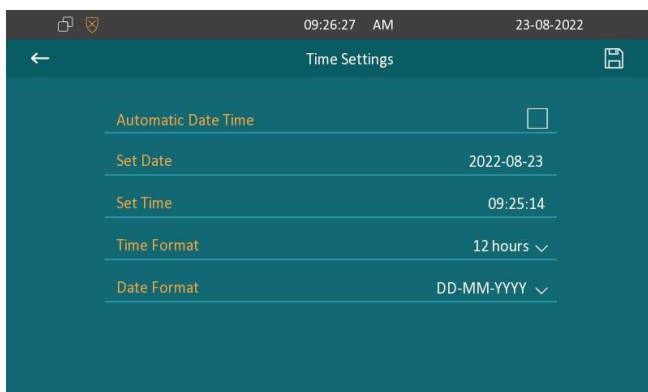
5.2 - Time setting

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

5.2.1 - Time setting on the device

To configure time on the device:

More > Setting > Time



Parameter Set-up

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

- **NTP Server1&2** - Enter the NTP server you obtained in the NTP server field.

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

5.2.2 - Time setting by the device web interface

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

To configure time by the device web interface:

Phone > Time/Lang

Format Setting

Time Format Date Format

Type

Manual Auto

Date Year Mon Day

Time Hour Min Sec

NTP

Time Zone Primary Server

Secondary Server

Update Interval (>= 3600s)

5.2.3 - Daylight saving time setting

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

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

Phone > Time/Lang

Daylight Saving Time

Active

Offset (-300~300Minutes)

By Date By Week

Start Time Mon Day Hour

End Time Mon Day Hour

Start Month Start Week Of Month

Start Day Of Week Start Hour (0~23)

End Month End Week Of Month

End Day Of Week End Hour (0~23)

Table A4 - MyBell IP Indoor Monitor - Configuration of the daylight saving time	
Setting	Description
Active	To enable or disable the daylight saving time. You can also configure it to make the device adjust the daylight saving time automatically.
Offset	To set the offset value. The default value is 60 minutes, which sets the clocks an hour ahead of the standard time.
By Date	To set the date schedule for the daylight saving time
By Week	To set the schedule for the daylight saving time according to the week and month

6 SCREEN DISPLAY CONFIGURATION

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

6.1 - Screen display setting on the device

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

To configure a screen display on the device:

More > Setting > Display

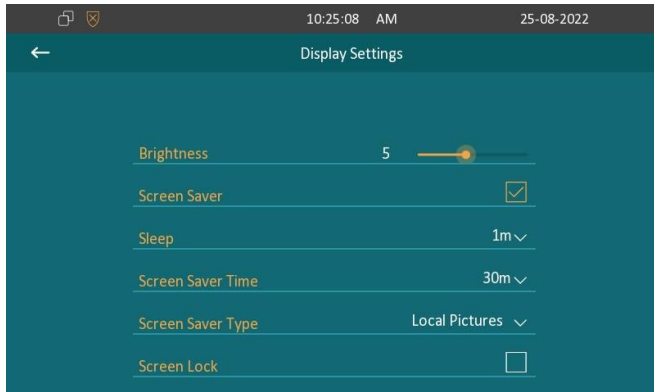


Table A5 - MyBell IP Indoor Monitor - Configuration of the daylight saving time

Setting	Description
Brightness	Press on the brightness setting and move the yellow dot to adjust the screen brightness. The default brightness is 5.
Sleep	Set the sleep timing based on the screen saver. The time range is from 15 second to 30 minutes. <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 timing to 1 minute, the screen saver starts automatically when the device has no operation for 1 min. If the screen saver is disabled, the sleep time is the screen turn-off time. For example, if you set the sleep timing to 1 minute, the screen is turned off automatically when the device has no operation for 1 min.
Screen Lock	Tick the screen lock if you want to lock the screen after the screen is turned off (turn dark). You are required to enter the system code to unlock the screen or you can unlock the screen by facial recognition.
Screen Saver Time	Set the screen saver duration. The time range is from 15 minutes to 2 hours.
Screen Saver Type	Select screen saver type <ul style="list-style-type: none"> Local Pictures: Display picture uploaded to the indoor monitor as the screen saver. Clock: Display the clock as the screen saver.

6.2 - Screen display setting by the web interface

6.2.1 - Brightness and time setting by the device web interface

To configure brightness and sleep by the device web interface:

Phone > Key/Display > Display

Display

Brightness Sleep

6.2.2 - Screen saver configuration

To upload a screen saver by the web interface:

Phone > Display Setting > Screen Saver Setting

Screen Saver Setting

Picture Files

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

Screen Saver Pictures

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

Screen Saver Type

Table A6 - MyBell IP Indoor Monitor - Configuration of the screen saver

Setting	Description
Picture File	Choose a picture file you want to use for the screen saver.
Screen Saver Pictures	Choose a picture from the PC and upload the picture to the indoor monitor.
Screen Saver Type	Select screen saver type <ul style="list-style-type: none"> • Local Pictures: Display picture uploaded to the indoor monitor as the screen saver. • Clock: Display the clock as the screen saver.

Note.

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

6.3 - Uploading a device booting image

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

To upload a booting image:

Phone > Logo > Boot Log

Boot Logo

Boot Logo

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

Note.

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

6.4 - Icon screen display configuration

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

To customize icon display:

Phone > Key/Display

Home Page Display

Example

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

Setting

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

6.5 - Functional buttons display

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

Phone > Key/Display > Softkey In Talking Page

Softkey In Talking Page

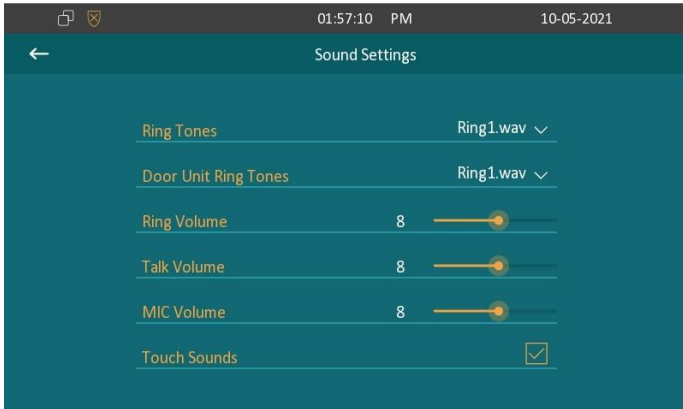
Key	Display	Label
Mute	Enabled ▼	
Hold	Enabled ▼	
New	Enabled ▼	
Capture	Enabled ▼	
Keyboard	Enabled ▼	

7 SOUND AND VOLUME CONFIGURATION

7.1 - Configuring volume on the device

To configure volume on the device:

More > Setting > Sound



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

7.2 - Configuring volume by the web interface

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

To configure volume by the web interface:

Phone > Audio

Ring Volume

Volume (0~15)

Talk Volume

Volume (1~15)

Mic Volume

Volume (1~15)

Touch Sound

Touch Sound Enabled

All Ringtones

Upload(Max Size: 25...

Ringtones

Door Unit Ring Tones

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

Note.

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

8 NETWORK CONFIGURATION

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

8.1 - Configuring network connection on the device

To check and configure the network connection on the device:

More > Setting > Advance > Network

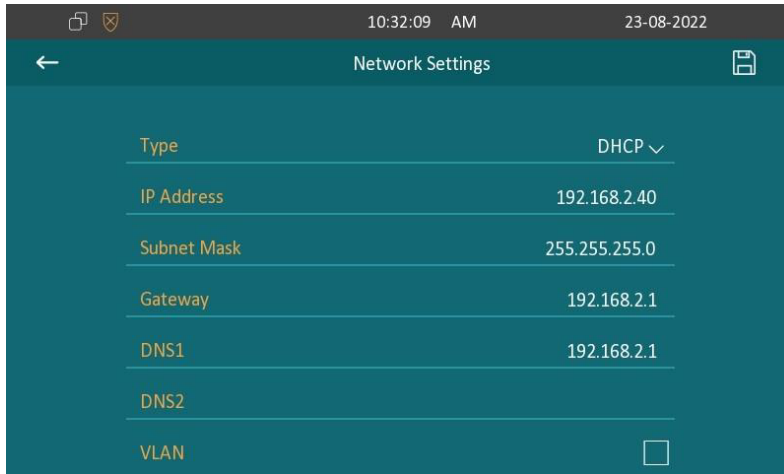


Table A7 - MyBell IP Indoor Monitor - Configuration of the network on the device

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

Note.

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

The default system code is **123456** .

8.2 - Configuring network connection by the web interface

To check the network connection by the web interface:

Status > Network Information

Network Information

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

To configure the network connection by the web interface:

Network > Basic

LAN Port

DHCP
 Static IP

IP Address Subnet Mask

Default Gateway LAN DNS1

LAN DNS2

Table A8 - MyBell IP Indoor Monitor - Configuration of the network by the web interface	
Setting	Description
DHCP	Select the DHCP mode by ticking the DHCP box. The DHCP mode is the default network connection. If the DHCP mode is selected, the indoor monitor is assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS address automatically.
Static IP	When the Static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS address have to be configured manually according to your actual network environment.
IP Address	Set up the IP Address if the Static IP mode is selected.
Subnet Mask	Set up the subnet mask according to your actual network environment.
Gateway	Set up the gateway according to the IP address.
LAN DNS 1/2	Set up a preferred or alternate Domain Name Server (DNS) according to your actual network environment. The preferred DNS is the primary DNS address while the alternate DNS is the secondary DNS address. The indoor monitor connects to the alternate server when the primary DNS server is unavailable.

8.3 - Device deployment in the network

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

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

Network > Advanced > Connect Setting

Connect Setting

Connect Type
 Discovery Mode

Cloud Server
 Cloud Port

Device Address

Device Extension (1-9)
 Device Location

Control4 Mode

Table A9 - MyBell IP Indoor Monitor - The device deployment in the network	
Setting	Description
Connect Type	It's set up automatically according to the actual device connection with a specific server in the network such as SDMC Cloud or None . None is the default factory setting indicating the device isn't in any server type, therefore you are allowed to choose Cloud, SDMC in the discovery mode.
Cloud Server	If you deploy your devices in a local cloud server, enter the local server RPS address. The device data redirects to the local server automatically.
Cloud Port	Enter the local cloud server port for the data transmission.
Discovery Mode	Turn on the discovery mode of the device so that it can be discovered by other devices in the network, and disable it if you want to conceal the device so as not to be discovered by other devices.
Device Address	Specify the device address by entering device location info from the left to the right: Community, Unit, Stair, Floor, Room in sequence.
Device Extension	Enter the device extension number for the device you installed.
Device Location	Enter the location in which the device is installed and used to distinguish the device from others.

8.4 - Device NAT setting

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

To set up NAT by the web interface:

Account > Advanced > NAT

NAT

RPort

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

8.5 - VLAN setting

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

To configure the VLAN function by the device web interface:

More > Setting > Advance > VLAN Setting

VLAN Setting

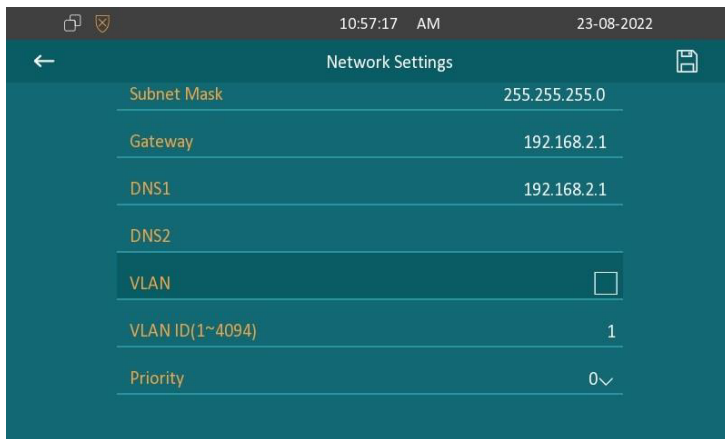
VLAN Priority
VLAN ID (1~4094)

Setting:

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

To configure the VLAN function on the device:

More > Setting > Advance > Network



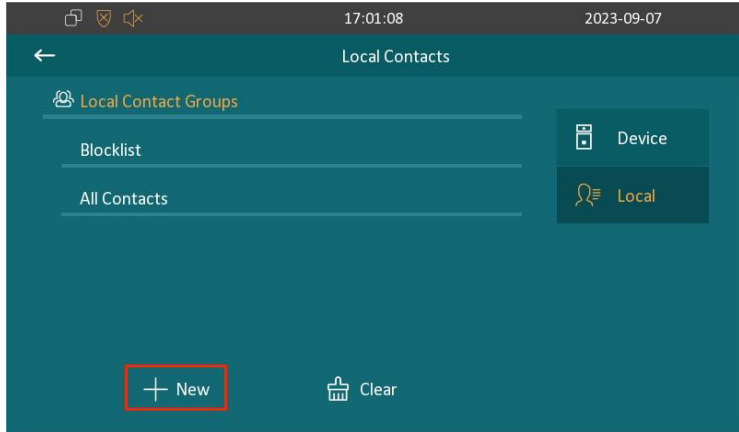
9.1 - Configuring the phone book on the device

You can create contacts and contact groups for users.

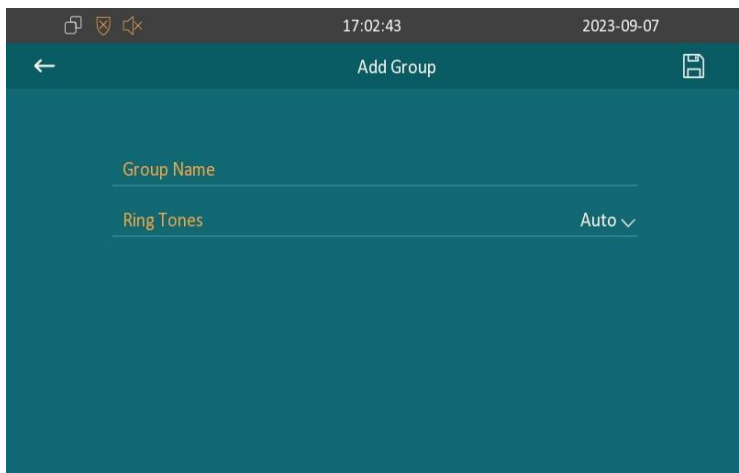
9.1.1 - Adding a contact group on the device

To add a contact group on the device screen:

More > Contacts > New



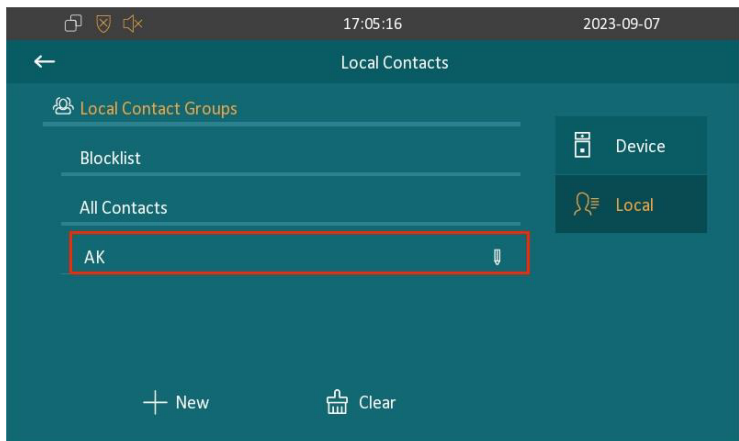
Enter a group name and press **Save** tab.

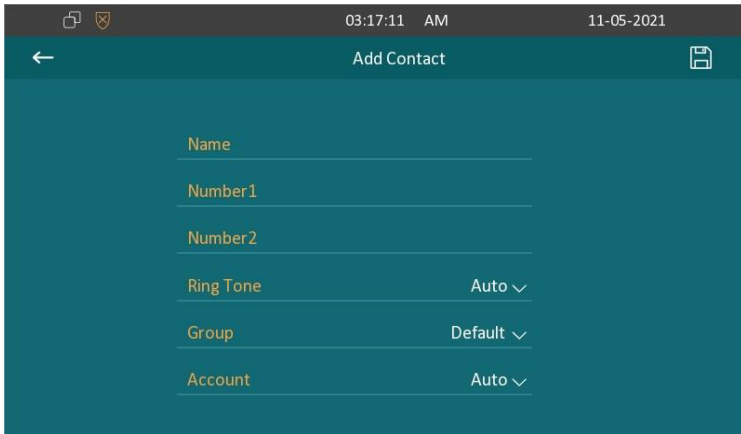
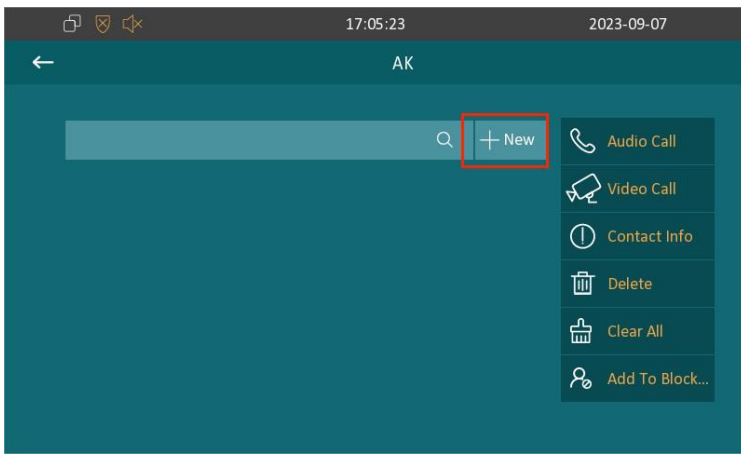


9.1.2 - Adding contacts on the device

To add a contact on the device screen:

More > Contacts > the desired group > New





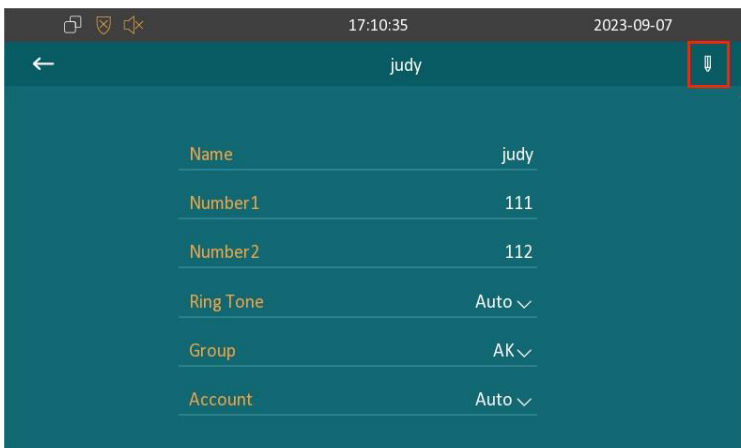
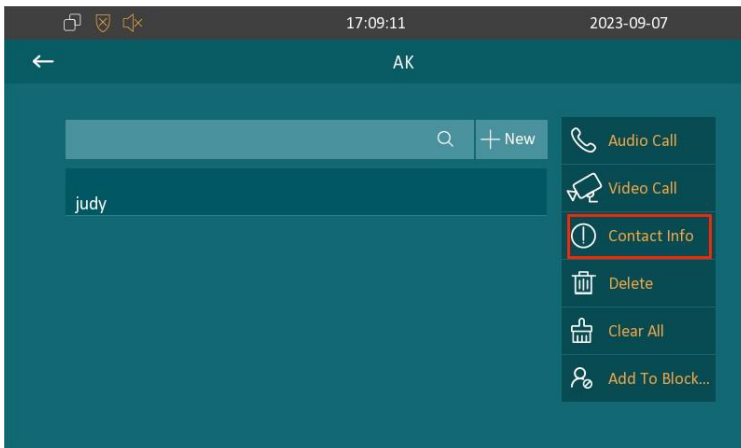
Setting:

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

9.1.3 - Editing contacts on the device

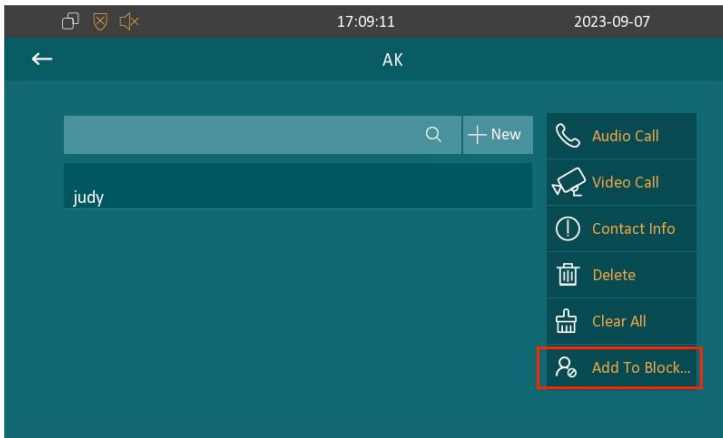
To edit a contact on the device screen:

The desired contact > Contact Info > Edit



9.1.4 - Blocklist setting on the device

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



Note.

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

9.2 - Phone book configuration by the web interface

9.2.1 - Contact group management by the web interface

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

Contacts > Local Contacts

Group

<input type="checkbox"/>	Index	Name	Ring	Description
<input type="checkbox"/>	1	AK	Auto	
<input type="checkbox"/>	2			
<input type="checkbox"/>	3			
<input type="checkbox"/>	4			
<input type="checkbox"/>	5			

Delete Delete All

Group Setting

Name Ring

Description

+ Add Edit X Cancel

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

<input type="checkbox"/>	Index	Name	Number 1	Number 2	Group	Ring	Account
<input type="checkbox"/>	1	Test	1234		Default	Auto	Auto
<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						

Delete Delete All Prev 1/1 Next MoveTo All Contacts 1 Page

Contact Setting

Name Number 1

Number 2 Group

Ring Account

+ Add Edit X Cancel

Table A10 - MyBell IP Indoor Monitor - Contact management by the web interface

Setting	Description
Number	Enter the contact number (SIP or IP number) to be saved.
Group	Select Default, a Blocklist group or a group created.
Account	Select Account 1 or Account 2.

You can dial out a number using the contact phone number.

To dial out a number:

Contacts > Local Contacts.

Dial

9.2.2 - Blocklist setting by the web interface

You can set the blocklist directly in the contact list by the web interface or set it when editing a contact.

To block a contact by the web interface:

Contacts > Local Contacts > Local Contacts List

<input type="checkbox"/> Index	Name	Number 1	Number 2	Group	Ring	Account
<input type="checkbox"/> 1	Test	1234		Default	Auto	Auto
<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						

1/1 MoveTo 1

Contact Setting

- All Contacts
- Blocklist

Note.

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

9.2.3 - Contact display

You can configure the contact display order and control whether to display the discovery device on the device.

To configure the contact display by the web interface:

Contacts > Local Contacts

Contacts List Setting

Contacts Sort By Show Local Contacts...

Setting:

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

9.2.4 - Contacts import and export by the web interface

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

To import and export contacts by the web interface:

Contacts > Local Contacts

Import/Export

Contacts(.XML/.CSV)	Not selected any files	Select File	Import	Export
				Cancel
Blocklist(.XML/.CSV)	Not selected any files	Select File	Import	Export
				Cancel

Note.

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

10 INTERCOM CALL CONFIGURATION

10.1 - IP call & IP call configuration

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

To configure IP calls:

Phone > Call Feature > Others

Others

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

Setting:

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

10.2 - SIP call & SIP call configuration

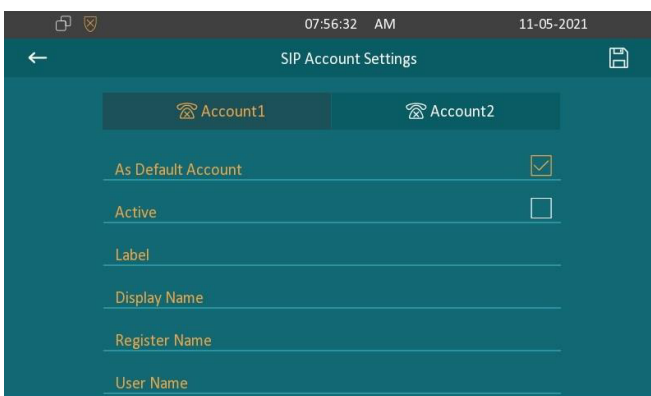
You can make a Session Initiation Protocol (SIP) call in the same way as you make the IP calls using the device. However, SIP call settings related to its account, server, and transport type need to be configured first

10.2.1 - SIP account registration

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

To configure the SIP account on the device screen:

More > Setting > Advance > SIP Account



To configure the SIP account by the web interface:

Account > Basic > SIP Account

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

SIP Account

Status	Disabled	Account	Account 1 ▼
Account Active	Disabled ▼	Display Label	
Display Name		Register Name	
User Name		Password

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

10.2.2 - SIP server configuration

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

To set the SIP account by the web interface:

Account > Basic > SIP Server

SIP Server 1

Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)	

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

10.2.3 - Outbound proxy server configuration

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

To configure the outbound proxy server by the web interface:

Account > Basic > Outbound Proxy Server

Outbound Proxy Server

Enable Outbound	<input type="text" value="Disabled"/>		
Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>
Backup Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>

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

10.3 - DND

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

To configure DND by the web interface:

Phone > Call Feature > DND

DND

Whole Day Return Code When ...

Schedule DND Start Time

DND End Time

Table A14 - MyBell IP Indoor Monitor - Configuration of DND

Setting	Description
DND	Check the Whole Day or Schedule to enable the DND function. The DND function is disabled by default.
Schedule	Enable the DND schedule for your indoor monitor. To configure a specific time to enable the DND feature. If you choose Schedule for DND, the whole day is checked on the device.
Return Code When DND	Select what code should be sent to the calling device through the SIP server: <ul style="list-style-type: none"> • 404 for Not found • 480 for Temporary Unavailable • 486 for Busy Here • 603 for Decline

10.4 - Configuring the device local RTP

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

To set up device local RTP by the web interface:

Network > Advanced > Local RTP

Local RTP

Starting RTP Port (1024~65535)

Max RTP Port (1024~65535)

Setting:

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

10.5 - Configuring a data transmission type

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

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

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

To set up data transmission type by the web interface:

Account > Basic > Transport Type

TransportType

TransportType

NAT

NAT

NAT

NAT

NAT

Stun Server Address Port

Table A15 - MyBell IP Indoor Monitor - Configuration of a data transport type

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

11 DOOR ACCESS CONTROL CONFIGURATION

11.1 - Relay switch setting

11.1.1 - Local relay setting

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

Phone > Relay > Relay Setting > Local Relay

Relay Setting

Local Relay

DTMF

#

Relay Interval

3s

Relay Type

Open Door

Table A16 - MyBell IP Indoor Monitor - Local relay setting

Setting	Description
DTMF	Set the DTMF code for the local relay.
Relay Interval	Set the relay delay time after the relay is triggered.
Relay Type	Set a relay action type choosing one of the following options: <ul style="list-style-type: none">• Chime Bell - when there is a call, a chime bell rings• Open Door - when press the unlock icon, the local relay opens• Other Switches (Reset By Event) - when the call is answered, the relay is reset

11.1.2 - Remote relay switch setting

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

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

Phone > Relay > Relay Setting > Remote Relay

Remote Relay

DTMF

#

DTMF Code1

#

DTMF Code2

#

DTMF Code3

#

Setting:

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

11.2 - Web relay setting

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

To configure a web relay by the device web interface:

Phone > Relay > Web Relay

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

WebRelay Setting

IP Address

UserName

Password

WebRelay Action

1

WebRelay Action Setting

ActionId	WebRelay Action
1	<input type="text"/>
2	<input type="text"/>

Setting:

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

11.3 - Door unlock configuration

11.3.1 - Door unlock by DTMF code

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

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

Account > Advanced > DTMF

DTMF

Type	<input type="text" value="RFC2833"/>	How to info DTMF	<input type="text" value="Disabled"/>
DTMF Payload	<input type="text" value="101"/>	(96~127)	

Table A17 - MyBell IP Indoor Monitor - Configuration of door unlock by DTMF code

Setting	Description
Type	Select a DTMF type from the following options: <ul style="list-style-type: none">• Info• RFC 2833• Info+RFC 2833
How to info DTMF	Select among the following options: <ul style="list-style-type: none">• Disable• DTMF• DTMF-Relay• Telephone-Event
DTMF Payload	Select the payload 96-127 for data transmission identification.

Note.

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

11.3.2 - Door unlock through the HTTP command

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

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

Phone > Relay > Remote Relay By HTTP or HTTPS

Remote Relay By HTTP or HTTPS

Index	IP/SIP	URL	UserName
<input type="checkbox"/> 1			
<input type="checkbox"/> 2			
<input type="checkbox"/> 3			
<input type="checkbox"/> 4			
<input type="checkbox"/> 5			

1/1

IP/SIP	<input type="text"/>	URL	<input type="text"/>
UserName	<input type="text"/>	Password	<input type="text" value="....."/>

Table A18 - MyBell IP Indoor Monitor - Configuration of door unlock by HTTP command

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

Note.

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

11.3.3 - Unlock by icon button

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

Phone > Relay > Key Setting

Key Setting

Softkey In Talking Page

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

Softkey In Call-Preview Page

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

Softkey In Homepage or More Page

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

Softkey In Monitor Page

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

12 CALL SETTING

12.1 - Call auto-answer configuration

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

Account > Advanced > Call > Auto Answer

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

Phone > Call Feature > Others

Call

Min Local SIP Port (1024~65535)

Max Local SIP Port (1024~65535)

Auto Answer Prevent SIP Hacking

Is escape non Ascii ...

Others

Return Code When ...

Auto Answer Delay (0~30s)

Busy Tone Indoor Auto Answer

Direct IP Direct IP Port

Answer Tone

Table A19 - MyBell IP Indoor Monitor - Configuration of call auto-answer

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

12.2 - Auto-answer allow list setting

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

To configure a call-auto answer allow list setting by the device web interface:

Phone > Call Feature > Auto Answer AllowList

Auto Answer Allowlist

Index	Device Location	SIP/IP
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

1/1

Device Location SIP

IP

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

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

Phone > Call Feature > Import/Export

Import/Export

Auto Answer AllowList(.XML/.CSV)

Not selected any files

Select File

Import

Export

Note.

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

12.3 - Intercom preview setting

If you want to see the image at the door station before answering the incoming call, you can enable the intercom preview function.

To enable the intercom preview function by the device web interface:

Phone > Intercom > Intercom Preview

Intercom Preview

Intercom Preview

Disabled

Note.

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

12.4 - SIP hacking protection

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

To enable the SIP hacking protection by the device web interface:

Account > Advanced > Call

Call

Min Local SIP Port

5062

(1024~65535)

Max Local SIP Port

5062

(1024~65535)

Auto Answer

Disabled

Prevent SIP Hacking

Disabled

Is escape non Ascii ...

Enabled

Setting:

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

12.5 - Emergency call setting

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

Press the SOS key, the indoor monitor initiates automatically the target SOS numbers.

12.5.1 - SOS icon display

To display SOS softkey by the device web interface:

Phone > Key/Display

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

Home Page Display

Example

Area	Type	Label
Area1	SOS	SOS
Area2	Setting	
Area3	Sound	

Area	Type	Label
Area1	SOS	SOS
Area2	Setting Sound	

12.5.2 - SOS number settings by the web interface

To set up SOS numbers by the device web interface:

Phone > Intercom

SOS

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

Table A20 - MyBell 2-Wire Indoor Monitor - Configuration of SOS numbers

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

12.5.3 - SOS number settings on the device

To set up SOS numbers on the device:

More > Setting > Advance > SOS

The screenshot shows the 'SOS Settings' screen with the following configuration:

- Call Number1
- Call Number2
- Call Number3
- Call Timeout: 60s
- Loop Times: 3
- Account: Auto

12.6 - Multicast configuration

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

To set up multicast communication on the device:

Phone > Multicast

Multicast Setting

Multicast Group

Multicast List

Multicast Group	Multicast Address
Multicast Group 1	<input type="text" value="224.1.6.11:51230"/>
Multicast Group 2	<input type="text" value="224.1.6.11:51231"/>
Multicast Group 3	<input type="text" value="224.1.6.11:51232"/>

Listen List

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

Table A21 - MyBell IP Indoor Monitor - Configuration of multicast

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

12.7 - Call forwarding setting

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

11.7.1 - Call forwarding configuration on the device

To set up call forwarding on the device:

More > Setting > Advance > Direct IP

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

12.7.2 - Call Forwarding Configuration by the web interface

To set up forward function using the device web interface:

Phone > Call Feature > Forward Transfer

Forward Transfer

Account	<input type="text" value="Account 1"/>		
Always Forward	<input type="text" value="Disabled"/>	Target Number	<input type="text"/>
Busy Forward	<input type="text" value="Disabled"/>	Target Number	<input type="text"/>
No Answer Forward	<input type="text" value="Disabled"/>	Target Number	<input type="text"/>
No Answer Ring Time	<input type="text" value="30"/>		

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

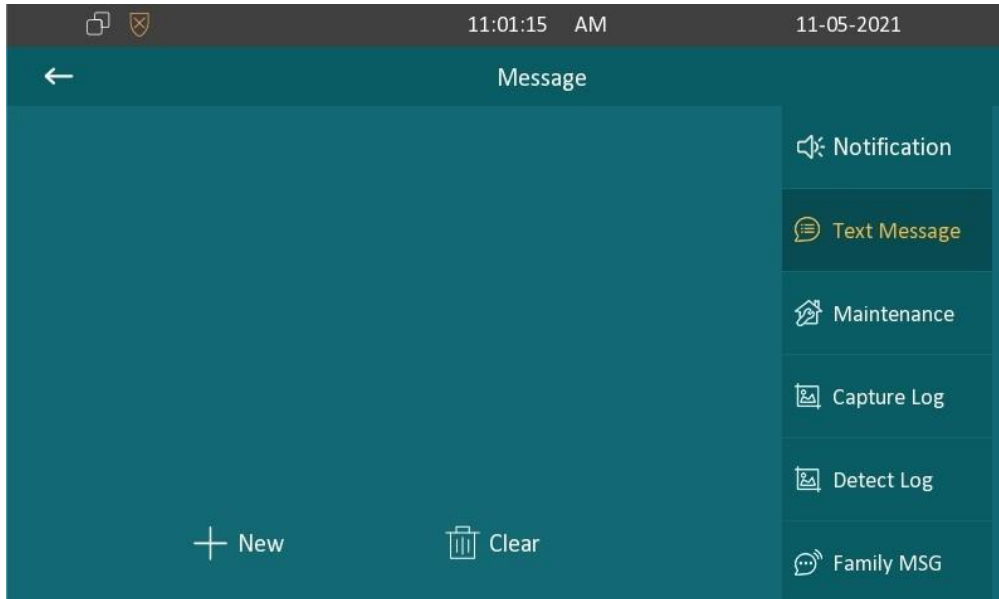
13 INTERCOM MESSAGE SETTING

13.1 - Managing Text Messages

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

To manage text messages on the device:

Message > Text Message

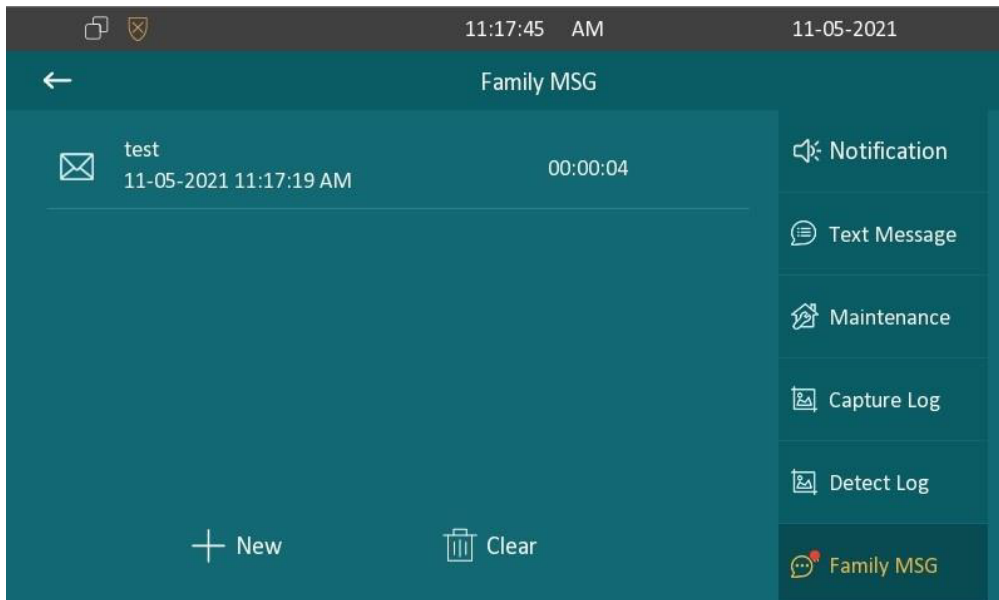


13.2 - Managing Voice Messages

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

To manage voice messages on the device:

Message > Family MSG



14 AUDIO & VIDEO CODEC CONFIGURATION FOR SIP CALLS

14.1 - Audio codec configuration

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

To configure audio codec by the web interface:

Account> Advanced > Audio Codecs

Audio Codecs



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

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

14.2 - Video codec configuration

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

To configure video codec by the web interface:

Account> Advanced > Video Codecs

Video Codecs



15.1 - Monitor setting

To configure the monitor setting by the web interface:

Phone > Monitor > Door Phone

Door Phone

<input type="checkbox"/>	Index	Number	Name	URL	User Name	Display
<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					

Delete
Delete All

Device Number	<input type="text"/>	Device Name	<input type="text"/>
RTSP Address	<input type="text"/>	User Name	<input type="text"/>
Password	<input type="password" value="....."/>	Display in Call	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px; border-radius: 3px; font-size: 0.9em; font-weight: normal; color: #333; text-decoration: none; width: 100%;" type="text" value="Disabled"/>

+ Add
↶ Edit
✕ Cancel

Table A24 - MyBell IP Indoor Monitor - Monitor setting

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

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

Monitor Import/Export

Import(.xml)

Not selected any files

Select File
 Import
✕ Cancel

Export
 Export

15.1.1 - Web camera setting by the web interface

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

Phone > Monitor > Web Camera

Web Camera

Index	Device Name	RTSP Address
<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	

1/1

Device Name RTSP Address

Setting:

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

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

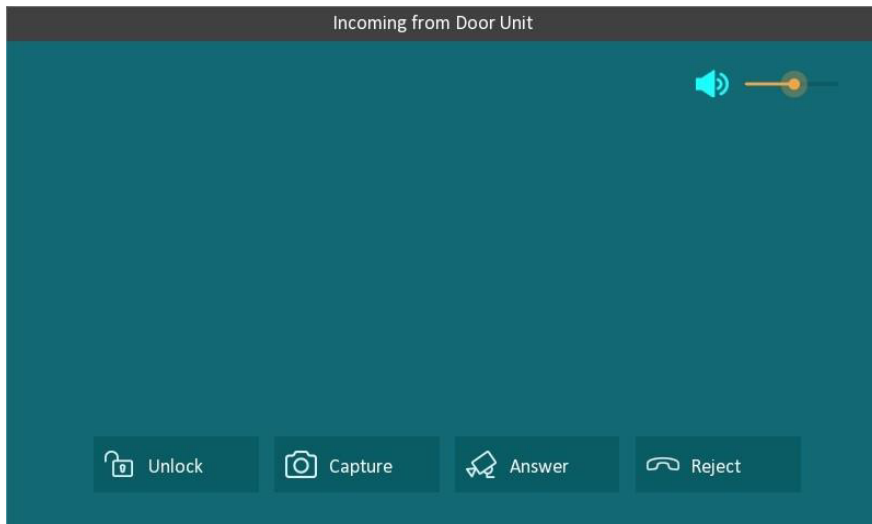
Web Camera Import/Export

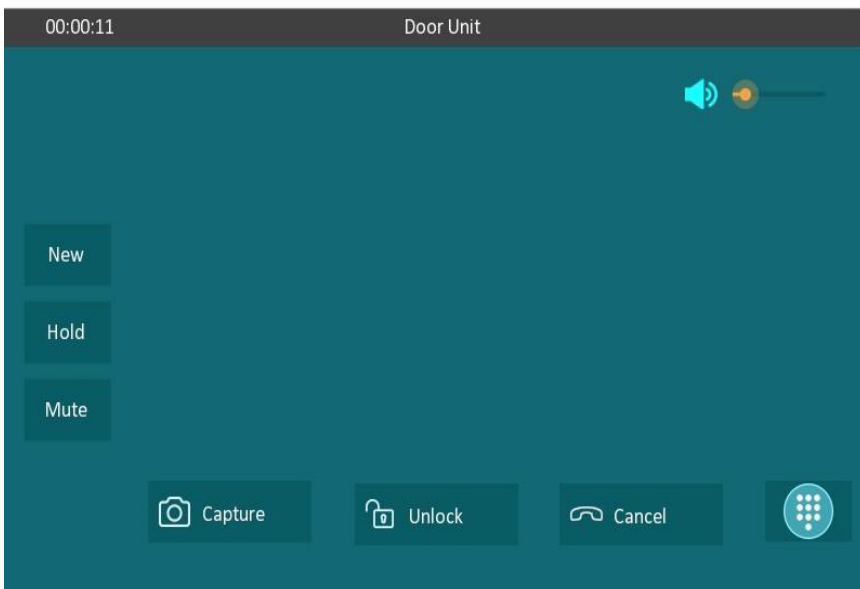
Import(.xml)

Export

15.1.2 - Web camera setting on the device

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





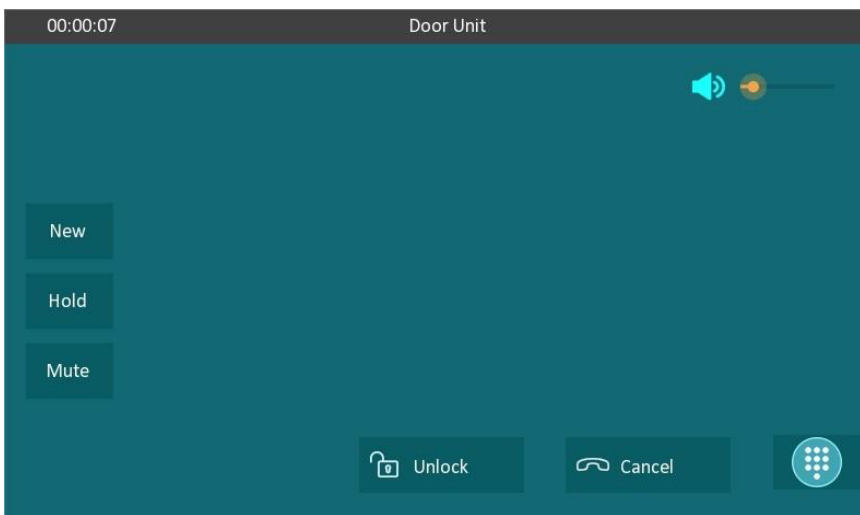
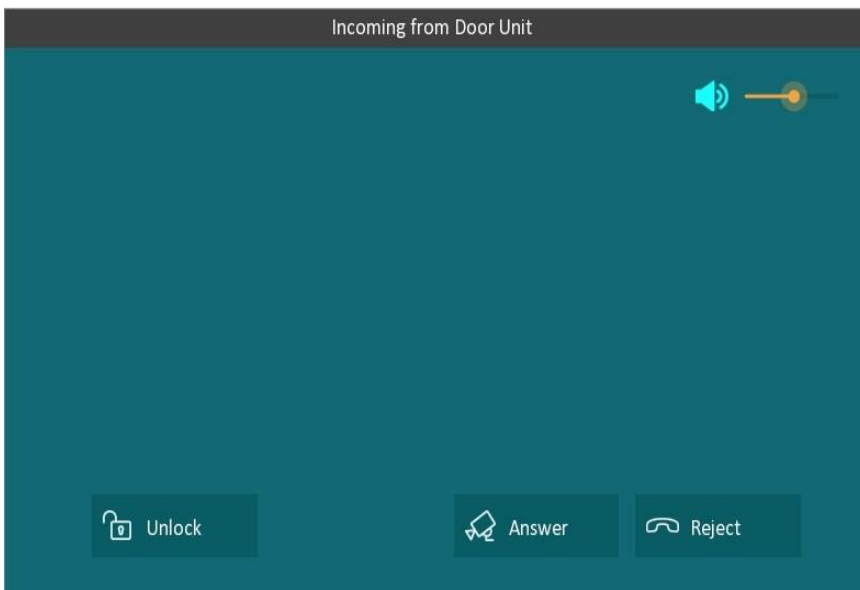
You can also disable the capture function on device web interface.

To disable the capture function by the web interface:

Phone > Key/Display > Softkey In Monitor Page

Softkey In Monitor Page

Key	Display	Label
Capture	Enabled	



15.2 - Alarm and arming configuration

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

To set up the **Arming icon**:

Phone > Key/Display

Home Page Display Example

Area	Type	Label
Area1	Arming	Arming
Area2	<div style="border: 1px solid gray; padding: 2px;"> Contacts Call Arming </div>	

More Page Display Example

Area	Type	Label
Area1	Arming	Arming
Area2	<div style="border: 1px solid gray; padding: 2px;"> Call Arming SOS </div>	

15.2.1 - Alarm and arming configuration on the device

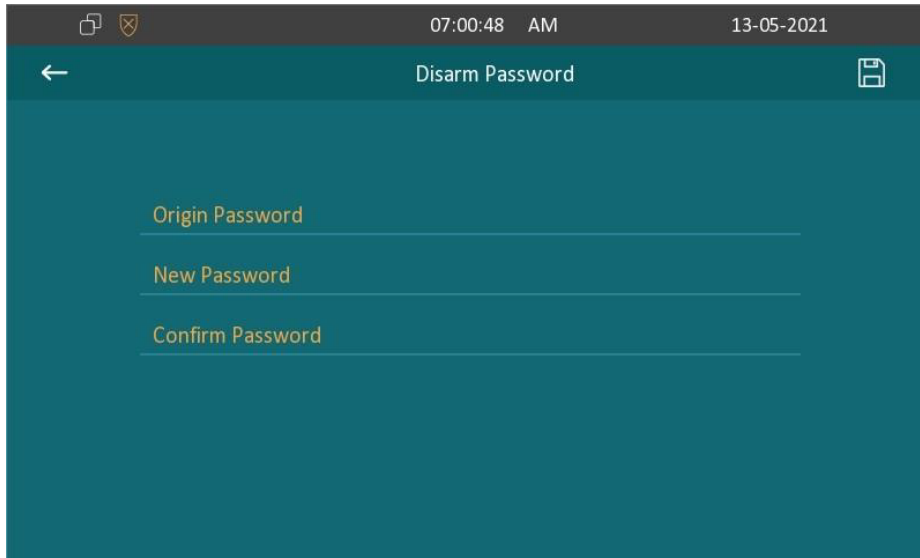
To set up a location-based alarm sensor on the device:

More > Setting > Advance > Arming > Zone Setting

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

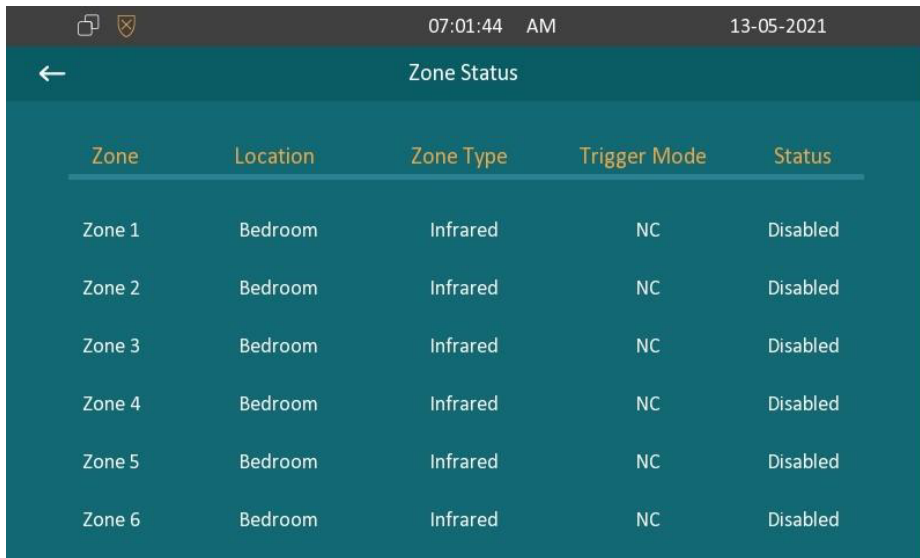
Setting	Description
Location	Set up the location according to where the alarm sensor is stalled. You can select among ten location types: Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
Zone Type	Set up the alarm sensor types. You can select among the following sensor types: Infrared, Drmagnet, Smoke, Gas, Urgency.
Trigger Mode	Set the sensor trigger mode between NC and NO according to your need.
Status	Set the alarm sensor status among three options: <ul style="list-style-type: none"> • Enable - if you want to enable the alarm, however, you are required to set the alarm again after an alarm is disarmed. • Disable - if you want to disable the alarm. • 24H - if you want the alarm sensor to stay enabled for 24 hours without the need to set up the alarm manually again after the alarm is disarmed.

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



To check the zone status on the device:

Arming > Zone Status



15.2.2 - Alarm and arming configuration by the web interface

To set up a location-based alarm sensor by the web interface:

Arming> Zone Setting > Zone Setting

Zone Setting

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

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

15.3 - Location-based alarm configuration

15.3.1 - Location-based alarm on the device

To configure the location-based alarm:

Arming > Arming Mode

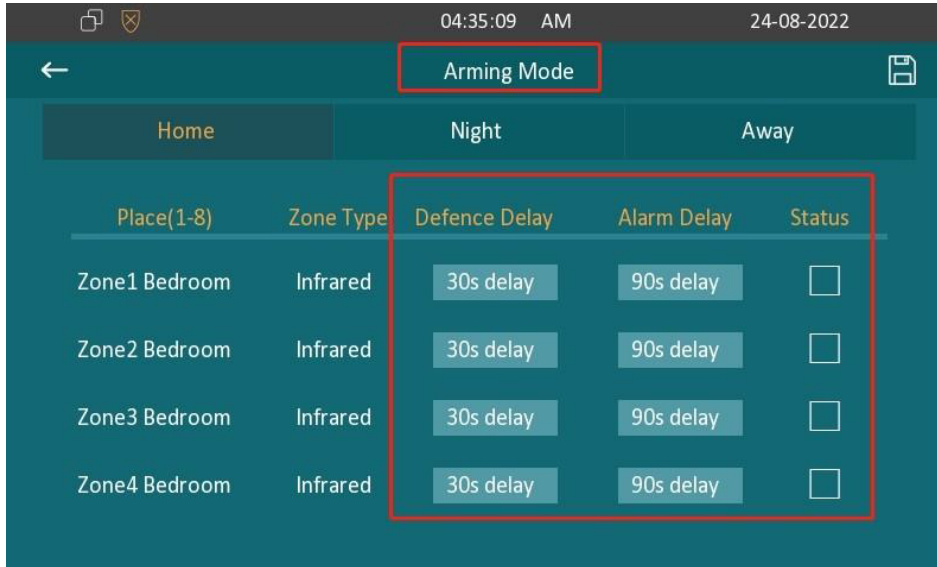


Table A26 - MyBell IP Indoor Monitor - Configuration of the arming mode

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

15.3.2 - Location-based alarm by the web interface

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

Arming > Arming Mode

Zone	Location	Zone Type	Defence Delay	Alarm Delay	Status
1	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
2	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
3	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
4	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
5	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
6	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
7	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>
8	Bedroom	Infrared	30s ▼	90s ▼	<input type="checkbox"/>

15.4 - Configuring the alarm text

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

To customize your alarm text alarm:

Arming > Zone Setting > Customized Alarm

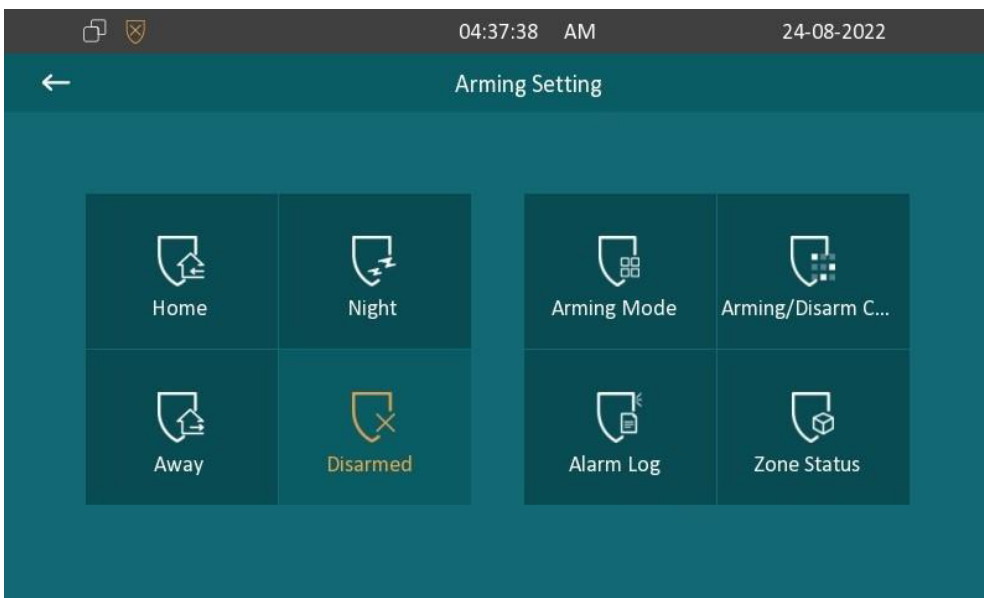
Customized Alarm

Customized Alarm Disabled

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

15.5 - Configuring the arming mode

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



15.6 - Configuring alarm action

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

To select and set up actions by the web interface:

Arming > Alarm Action

Action Type HTTP Command SIP Message Call Local Relay

15.6.1 - Configuration of alarm action through HTTP command

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

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

To set the HTTP Command up:

Arming > Alarm Action > HTTP Command Setting

HTTP Command Setting

Zone	HTTP Command	Send HTTP Enabled
Zone1	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone2	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone3	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone4	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone5	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone6	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone7	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼
Zone8	<input type="text" value="must start with http:// or https://"/>	<input type="button" value="Disabled"/> ▼

15.6.2 - Configuration of alarm action through SIP message

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

To set the SIP message action receiver:

Arming > Alarm Action > Receiver Of SIP Message

Receiver Of SIP Message

Receiver

SIP Message Setting

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

15.6.3 - Configuring the alarm action through SIP message

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

To set a call action:

Arming > Alarm Action > Call Setting

Call Setting

Call Number



15.7 - Checking alarm logs

To check alarm logs:

Arming > Alarm Log

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

12:12:47 PM 13-05-2021

Alarm Log 2/2  

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

15.8 - Screen unlock setting


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

To set screen unlock:


More > Setting > Display


04:53:27 AM 24-08-2022

Display Settings

Brightness 5 

Screen Saver

Sleep 1m 

Screen Saver Type Local Pictures 

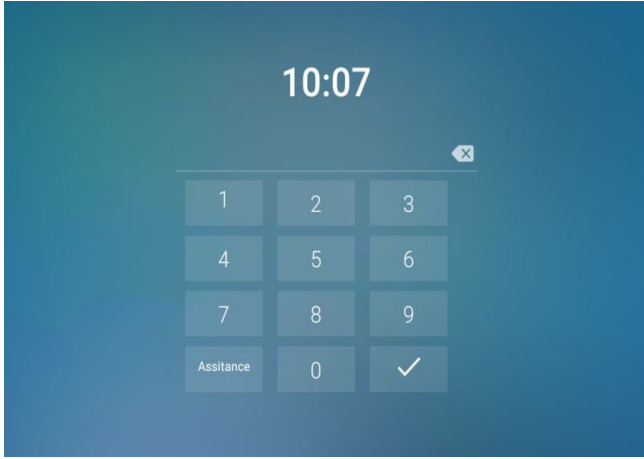
Screen Lock

15.9 - Screen unlock by PIN code

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

Note.

The default unlock PIN is **123456**.



15.10 - Location-based alarm configuration

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

15.10.1 - Web server certificate

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

To upload web server certificate to the device web interface:

Security > Advanced > Web Server Certificate

Web Server Certificate

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

Web Server Certifica...

15.10.2 - Client certificate

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

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

Security > Advanced > Client Certificate

Client Certificate

Index	Issue To	Issuer	Expire Time	
1				<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

Index

Only Accept Trusted...

Table A27 - MyBell IP Indoor Monitor - Configuration of the client certificate

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

15.11 - Power output setting

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

Device Setting > Basic > Power Output Setting

Power Output Setting

Power Output Enable

Note.

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

15.12 - High security mode

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

To configure the high security mode by the web interface

Security > Basic > High Security Mode

High Security Mode

Enable

Important notes.

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

To upgrade the device by the device web interface:

Upgrade > Basic

Firmware Version

213.30.10.33

Hardware Version

213.0.2.0.1.0.0.0

Upgrade

Not selected any files

Select File

Submit

Cancel

Note.

Firmware files should be .rom format for an upgrade.

17 BACKUP

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

Upgrade > Advanced > Others

Others

Config File(.tgz/.con...

Not selected any files

Select File

Export

(Encrypted)

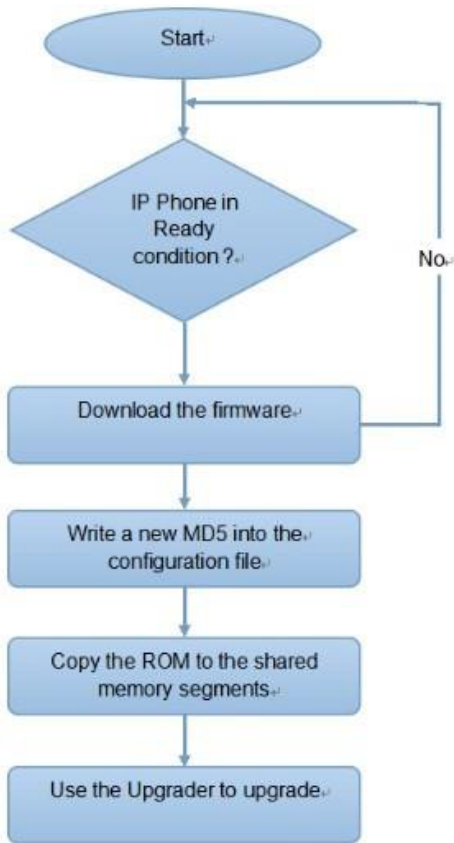
Import

Cancel

18 AUTO-PROVISIONING

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

See the flow chart below:



18.1 - Introduction to the configuration files for auto-provisioning

Configuration files have two following formats for auto-provisioning:

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

Note.

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

18.2 - Autop schedule

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

To set up the schedule by the device web interface:

Upgrade > Advanced > Automatic Autop

Automatic Autop

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> Hour(0~23) <input type="text" value="0"/> Min(0~59)
Clear MD5	<input type="button" value="Submit"/>
Export Autop Templ...	<input type="button" value="Export"/>
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Table A30 - MyBell IP Indoor Monitor - Configuration of the automatic autop

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

18.3 - Static provisioning configuration

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

To configure static provisioning:

Upgrade > Advanced > Manual Autop

Manual Autop

URL	<input type="text"/>	User Name	<input type="text"/>
Password	<input type="password"/>	Common AES Key	<input type="password"/>
AES Key(MAC)	<input type="password"/>		

[AutoP Immediately](#)

Table A31 - MyBell IP Indoor Monitor - Configuration of the static provisioning

Setting	Description
URL	Set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
Common AES Key	Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
AES Key (MAC)	Set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note.

- AES encryption should be configured only when the config file is encrypted with AES.
- User specified server isn't provided. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/ (allows anonymous login)
 - ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/ (use the default port 80)
 - http://192.168.0.19:8080/ (use other ports, such as 8080)
 - HTTPS: https://192.168.0.19/ (use the default port 443)
- The general configuration file for the in-batch provisioning is with the format cfg. For example, r000000000313.cfg (9 zeros in total). While the MAC-based configuration file for the specific device provisioning is with the format MAC_Address of the device.cfg, for example, 0C110504AE5B.cfg.

18.4 - Call log

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

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

To check call logs by the device web interface:

Contacts > Call Log

Capture Enable

Enabled ▼

Capture Delay

5s ▼

Call History

All ▼

 Export

<input type="checkbox"/>	Index	Type	Date	Time	Local Identity	Name	Number
<input type="checkbox"/>	1	Missed	1970-01-01	00:24:12	192.168.88.2 @192.168.88.2	Door Unit	192.168.0.7@ 192.168.0.7
<input type="checkbox"/>	2	Missed	1970-01-01	00:22:48	192.168.88.2 @192.168.88.2	Door Unit	192.168.0.7@ 192.168.0.7
<input type="checkbox"/>	3	Missed	1970-01-01	00:14:44	192.168.88.2 @192.168.88.2	Door Unit	192.168.0.2@ 192.168.0.2

Table A32 - MyBell IP Indoor Monitor - Configuration of the call log

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

19.1 - System Log for debugging

System logs can be used for debugging purposes.

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

Upgrade > Advanced > System Log

System Log

LogLevel

Export Log

Remote System Log Remote System Serv...

Setting:

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

19.2 - PCAP for debugging

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

To set up PCAP by the device web interface:

Upgrade > Advanced > PCAP

PCAP

Specific Port

PCAP

PCAP Auto Refresh

Table A33 - MyBell IP Indoor Monitor - Configuration of the PCAP

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

20 PASSWORD MODIFICATION

20.1 - Modification of the device advanced setting password

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

To modify the advanced setting password on the device screen:

More > Setting > Advance > Password



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

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

20.2 - Modification of the device web interface password

To modify the password by the web interface:

Security > Basic > Web Password Modify

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

Web Password Modify

User Name

Change Password

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

User Name

Old Password

New Password

Confirm Password

Note.

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

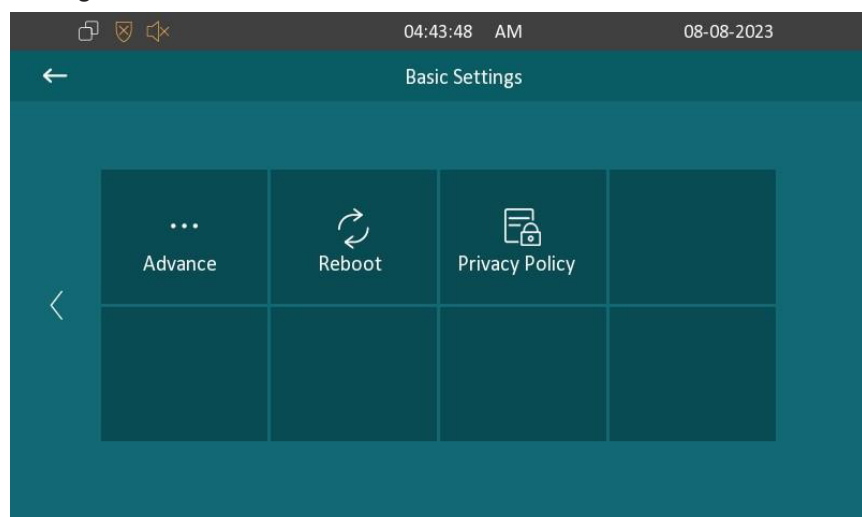
The default password for the user account is **user**.

21 SYSTEM REBOOT & RESET

21.1 - Reboot on the device

To reboot the system on the device screen:

Setting > Reboot



21.2 - Reboot by the web interface

To reboot the system by the web interface:

Upgrade > Basic

Reset Config To Factory Setting

Submit

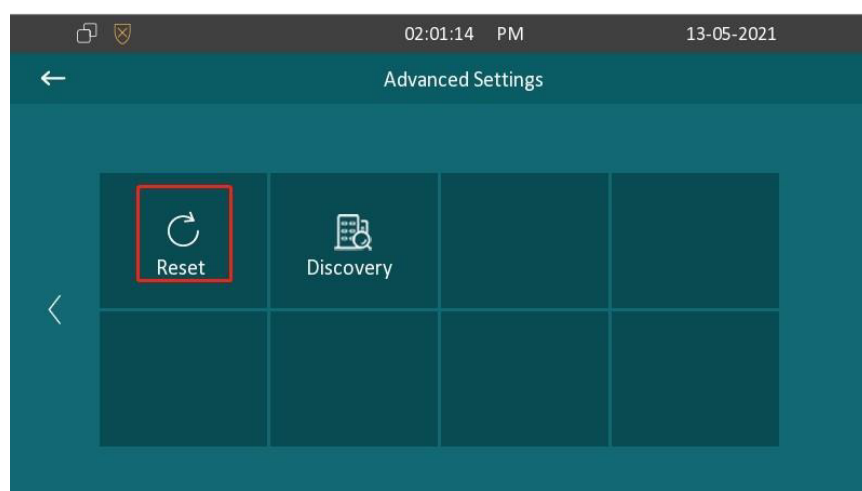
Reboot

Submit

21.3 - Reset on the device

To reset the whole device system to the factory setting:

More > Setting > Advance



21.4 - Reset by the web interface

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

Upgrade > Basic

Reset To Factory Setting

Submit

Reset Config To Factory Setting

Submit

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

22.1 - Warranty

We warrant this product to be free from defects in material and workmanship under normal and proper use for one year from the purchase date of the original purchaser. We will, at its option, either repair or replace any part of the products that prove defective due to improper workmanship or materials. THIS LIMITED WARRANTY DOES NOT COVER ANY DAMAGE TO THIS PRODUCT THAT RESULTS FROM IMPROPER INSTALLATION, ACCIDENT, ABUSE, MISUSE, NATURAL DISASTER, INSUFFICIENT OR EXCESSIVE ELECTRICAL SUPPLY, 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.

22.2 - Declaration of conformity



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

22.3 - WEEE Directive Compliance



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



Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com

IS093A00EN_17-05-2024