MyBell

IP Keypad Station

EN - Instructions and warnings for installation and use

v0.5

CONTENT

1 - IMPORTANT SAFEGUARDS AND WARNINGS 5
2 - DEVICE DESCRIPTION 6
3 - CONFIGURATION MENU 8
4 - ACCESS TO DEVICE 9
4.1 - Access to the device setting on the device 9
4.2 - Access to device settings by web interface 9
5 - LANGUAGE AND TIME CONFIGURATION 10
5.1 - Language configuration 10
5.2 - Time configuration 10
6 - LED CONFIGURATION 11
6.1 - Infrared LED configuration 11
6.2 - LED configuration in card reader area 11
6.3 - LED configuration on Keypad 11
6.4 - Screensaver configuration 12
6.5 - Screensaver uploading 12
6.6 - Adjusting screen backlight brightness 13
6.7 - LCD Heat Control 13
7 - VOLUME AND TONE CONFIGURATION 14
7.1 - Volume configuration 14
7.2 - Tone files uploading 14
8 - NETWORK CONFIGURATION 15
8.1 - Network status 15
8.2 - Device network configuration 15
8.3 - Device deployment in network 16
8.4 - Device local RTP configuration 16
8.5 - SNMP configuration 16
8.6 - VLAN configuration 17
8.7 - QoS configuration 17
8.8 - TR069 configuration 18
8.9 - Device web HTTP configuration 18
8.10 - NAT configuration 18
9 - INTERCOM CALL CONFIGURATION 19
9.1 - IP call and IP call configuration 19
9.2 - SIP call and SIP call configuration 19
9.2.1 - SIP account registration 19
9.2.2 - SIP server configuration 20
9.3 - Outbound proxy server configuration 20
9.4 - Data transmission type configuration 21
10 - CONTACTS CONFIGURATION 22
10.1 - Contact groups management 22
10.2 - Adding contacts 22
10.3 - Contact list display configuration 23
11 - CALL CONFIGURATION 24
11.1 - DND configuration 24
11.2 - Maximum call duration configuration 24
11.3 - Maximum dial duration configuration 24
11.4 - Auto answer configuration 25
11.5 - Hang up after open door 25
11.6 - SIP hacking protection 25
11.7 - Speed dial 26
11.7.1 - Group call 26
11.7.2 - Sequence call 26
11.8 - Web call 28
12 - AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS 29
12.1 - Audio codec configuration 29
12.2 - Video codec configuration 29
12.3 - Video codec configuration for IP direct calls 30
12.4 - DTMF data transmission configuration 30
13 - RELAY SETTING 31

14 - DOOR ACCESS SCHEDULE MANAGEMENT 32
14.1 - Creating door access schedule 32
14.2 - Editing door access schedule 33
14.3 - Import and export of door access schedule 33
15 - DOOR UNLOCK CONFIGURATION 34
15.1 - Configuration of PIN code for door unlock 34
15.1.1 - Public PIN cofiguration 34
15.1.2 - Private PIN cofiguration 34
15.2 - Configuration of RF card for door unlock 35
15.3 - Configuration of RF card code format 35
15.4 - Mifare card encryption 36
15.5 - NFC card configuration 37
15.6 - Open relay configuration using HTTP for door unlock 37
15.7 - Configuration of exit button for door unlock 37
15.9 - Configuration of open relay through DTMF for door unlock 38
15.10 - DTMF whitelist 39
16 - MONITOR AND IMAGE 40
16.1 - RTSP Stream Monitoring 40
16.1.1 - RTSP Stream Setting 40
16.2 - ONVIF 41
16.3 - MJPEG image capturing 42
16.4 - Live stream 42
17 - SECURITY 43
17.1 - Tamper alarm configuration 43
17.2 - Disarm Setting 43
17.3 - Virtual PIN 43
17.4 - Client certificate configuration 43
17.4.1 - Web Server certificate 43
17.4.2 - Client certificate 44
17.5 - Motion detection 44
17.6 - Security Notification Setting 45
17.6.1 - Email Notification Setting 45
17.6.2 - FTP notification configuration 46
17.6.3 - SIP call notification configuration 46
17.6.4 - Action URL 46
17.7 - Web interface automatic log-out 47
17.8 - Low power mode 47
18 - LOGS 48
18.1 - Call logs 48
18.2 - Door access logs 48
19 - BACKUP 49
20 - DEBUG 50
20.1 - Capturing system log for debugging 50
20.2 - Remote debug server 50
20.3 - PCAP for debugging 50
20.4 - Ping 51
21 - FIRMWARE UPGRADE 52
22 - AUTO-PROVISIONING THROUGH CONFIGURATION FILE 53
22.1 - Provisioning principle 53
22.2 - Introduction to configuration files for auto-provisioning 53
22.3 - Autop schedule 53
22.4 - Static provisioning configuration 54
22.5 - DHCP provisioning configuration 55
22.6 - PNP Configuration 56
23 - DEVICE INTEGRATION WITH THIRD PARTY 57
23.1 - Wiegand integration 57
23.2 - HTTP API integration 57
23.3 - Power output control 58
23.4 - Integration with Milestone 58

24 - PASSWORD MODIFICATION **59**
24.1 - Accounts Management 59
24.2 - Device web interface password modification 59
24.3 - System password modification 59
24.4 - Setting password modification 59
25 - SYSTEM REBOOT AND RESET **60**
25.1 - Reboot 60
25.2 - Reset 60
25.2.1 - Reset by web interface 60
25.2.2 - Reset on the Device 60
26 - REGULATIONS **61**
26.1 - Warranty 61
26.2 - Declaration of conformity 61
26.3 - WEEE Directive Compliance 61

1 IMPORTANT SAFEGUARDS AND WARNINGS

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

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

2 DEVICE DESCRIPTION

MyBell IP Keypad Station incorporates a wide-angle camera to provide comprehensive visual coverage. The device enables keyless access. It has notable IP and IK rating ensuring durability and security for the building.

Table A1 - MyBell IP Keypad Station - Device description

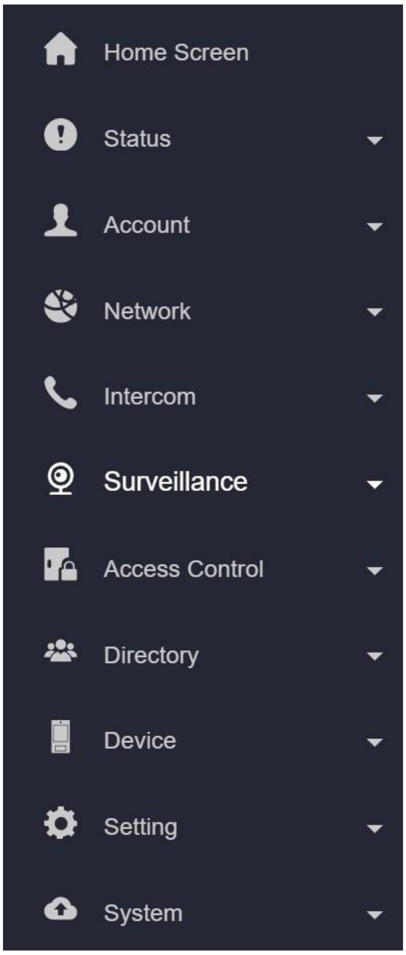
Feature	Description
Operation System	Linux
Size	310 x 106 x 37.8 mm
Camera	2M pixels, automatic lighting
Front Panel	aluminium
IR LEDs	yes
Card Reader	yes
Touch Screen	yes
Ethernet	x 1, PoE+(802.3at)
Power over Ethernet (PoE)	802.3af
Ethernet ports	1 x RJ45, 10/100 Mbps adaptive
TF Card Slot	1
Power In	x 1, 12V/2A
Analog Audio	optional
Analog Video	optional
RS485 Port	1
Relay	2
Input	4
Line Out	1
Microphone	1
Speaker	1
BLE	yes
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	IP66
IK Rating	IK08
Audio	SIP v1 (RFC2543), SIP v2 (RFC3261)
Narrowband Audio Codec	G.711a, G.711µ
Wideband Audio Codec	G.722

Table A1 - MyBell IP Keypad Station - Device description

Feature	Description
DTMF	in-band, out-of-band DTMF (RFC2833), SIP Info
Echo Cancellation	yes
Voice Activation Detection	yes
Comfort Noise Generator	yes
Video Sensor	1/2.8", CMOS
Pixels	CIF, VGA, 4CIF, 720p, 1080 p
Video codec	H.264
Video resolution	up to 1920 x 1080
Maximum image transfer rate	1080p – 30 fps
Viewing angle	110°(H) / 58°(V)
High intensity IR LEDs for picture lightning during dark hours with internal light sensor	yes
Compatible with 3rd party video components, such as NVRs	yes
Relays controlled individually by DTMF tones	yes
Camera permanently operational	yes
Auto night mode with LED illumination	yes
White balance	auto
Minimum illuminaton	0.1 LUX
Supported Networking Protocols	IPv4, HTTP, HTTPS, FTP, DNS, NTP, RTSP, RTP, TCP, UDP, TLS, ICMP, DHCP, ARP
Auto-Provisioning	yes
Web Management Portal	yes
Web-based Packet Dump	yes
Configuration Backup / Restore	yes
Entry log export	yes
Access table export / import	yes
Firmware Upgrade	yes
System Logs (including door access logs)	yes
Application Scenario	• office door phone with on-site or hosted IP-PBX • remote site entry over Internet • apartment/flat intercom with door access control

Table A2 - MyBell IP Keypad Station - Configuration menu

Section	Description
Status	Basic information such as product information, network information, and account information.
Account	Including SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF
Network	Including DHCP & static IP setting, RTP port setting, device deployment
Intercom	Including LCD setting, call features, multicast
Surveillance	Including motion detection, RTSP setting, ONVIF setting
Access Control	Including relay setting, card setting, PIN setting
Directory	Section for user management
Device	LCD, light, wiegand, audio, and lift control settings
Setting	Time and language, action, schedule and HTTP API settings
System	Including upgrading, maintenance, auto-provisioning



4 ACCESS TO DEVICE

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

4.1 - Access to the device setting on the device

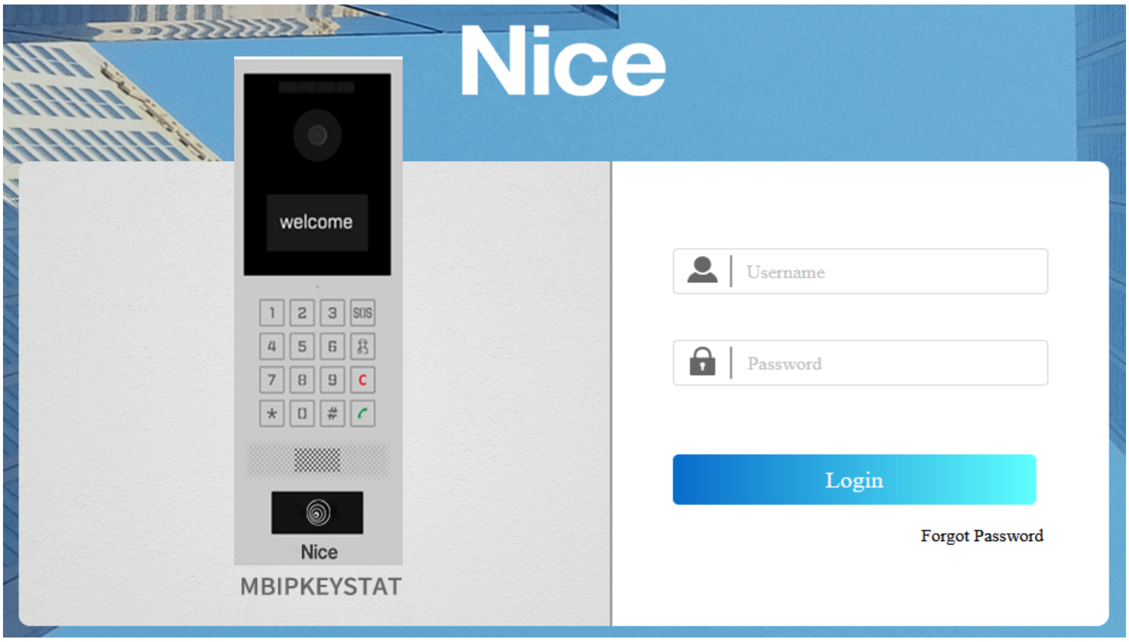
To enter the advanced setting screen press ***2396#.**

The advanced settings enable you to edit network, and resetting configuration, as well as modify admin password for sections such as System Information, Admin Setting, and System Setting.

4.2 - 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 where you can configure settings.
You can check the IP address on the device **System Information** screen or you can search the device IP by the IP scanner in the same LAN network.

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



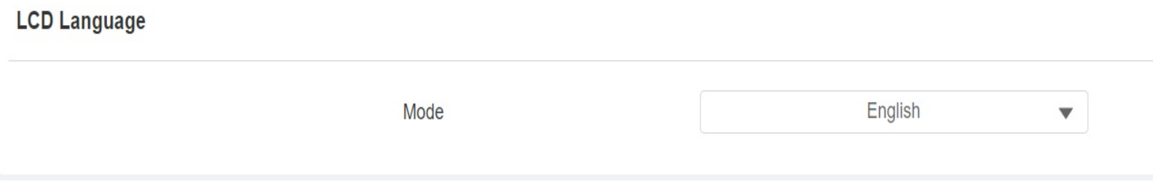
5 LANGUAGE AND TIME CONFIGURATION

5.1 - Language configuration

To configure language:

Setting > Time/Lang

Currently, only English is supported.



LCD Language

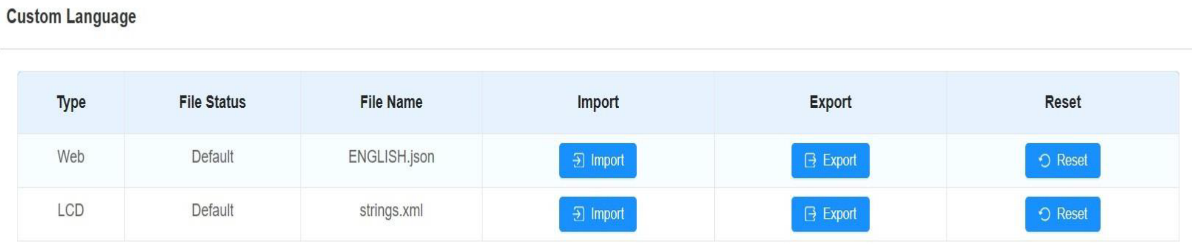
Mode	English ▼

You can select the web language in the upper right corner.

You can customize the web and device language by exporting the file and importing it after modification.

To customize the language:

Setting > Time/Lang



Custom Language

Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	Import	Export	Reset
LCD	Default	strings.xml	Import	Export	Reset

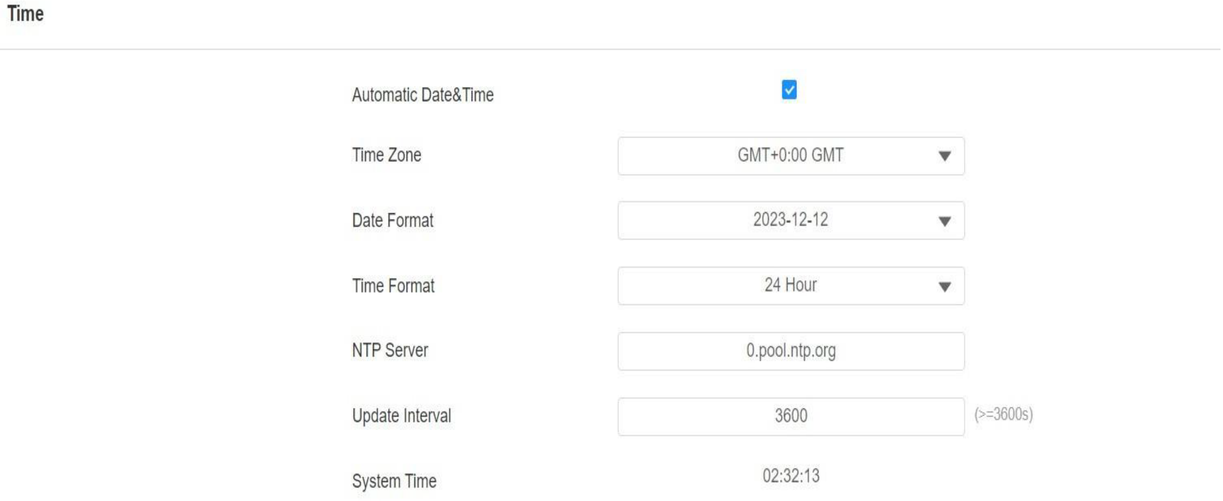
Note

- The uploaded file for customizing **web language** should be in **.json** format.
- The uploaded file for customizing **LCD language** should be in **.xml** format.

5.2 - Time configuration

To configure time:

Setting > Time/Lang



Time

Automatic Date&Time	☑	
Time Zone	GMT+0:00 GMT ▼	
Date Format	2023-12-12 ▼	
Time Format	24 Hour ▼	
NTP Server	0.pool.ntp.org	
Update Interval	3600	(>=3600s)
System Time	02:32:13	

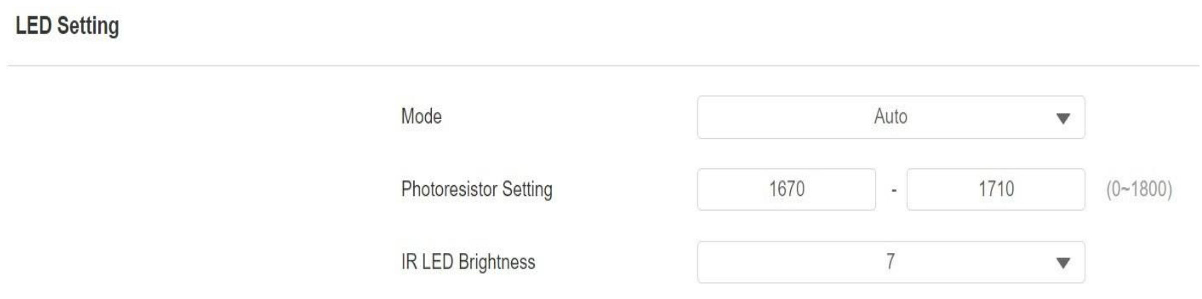
Settings:

- When a time zone is selected, the device notifies automatically **Network Time Protocol (NTP) server** of the time zone so that the **NTP server** can synchronize the time zone setting in your device.
- If enabled, **Automatic Date & Time** enables synchronization of time and data with the **NTP server** and default time zone.
- **Update Interval** sets the intervals between consecutive NTP requests.

6 LED & LCD CONFIGURATION

6.1 - Infrared LED configuration

Infrared LED is mainly designed to reinforce the light for facial recognition at night or in a dark environment.
To configure the infrared LED:
Device > Light > LED Setting



LED Setting

Mode: Auto

Photoresistor Setting: 1670 - 1710 (0~1800)

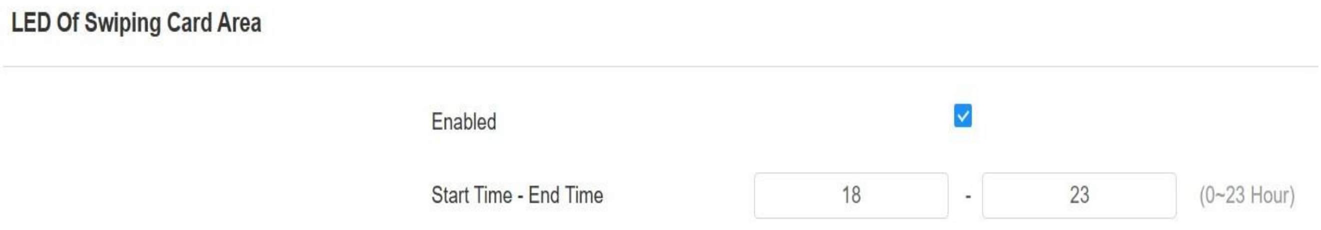
IR LED Brightness: 7

Table A3 - MyBell IP Keypad Station - Infrared LED configuration

Setting	Description
Mode	Select from **Auto, Always ON, Always OFF,** and **Schedule.**
Photoresistor Setting	Set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the ON-OFF of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off.
IR LED Brightness	Adjust the IR LED brightness from level 0 to 10.

6.2 - LED configuration in card reader area

You can enable or disable the LED lighting in the card reader area using web interface. You can also set the time after which the Led light is turned off to reduce power consumption.
To configure the LED light in the card reader area:
Device > Light > LED of Swiping Card Area



LED Of Swiping Card Area

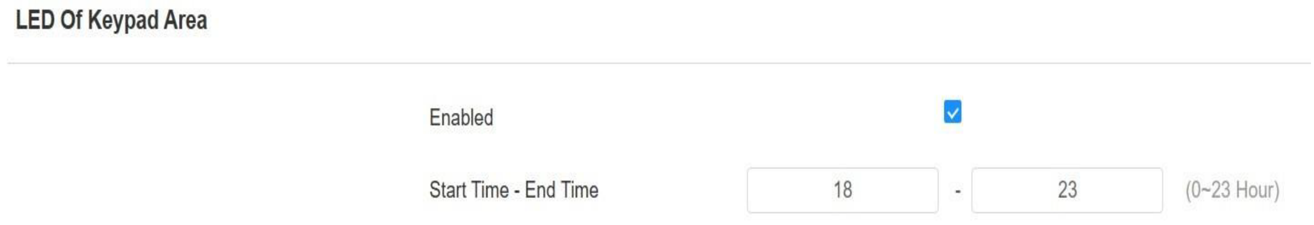
Enabled ☑

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

Start Time- End Time - you can set the time when the LED lighting in the card area turns on.

6.3 - LED configuration on Keypad

You can enable or disable the LED lighting in the card reader area using web interface. You can also set the time after which the Led light is turned off to reduce power consumption.
To configure the LED light in the keypad area:
Device > Light > LED of Keypad Area



LED Of Keypad Area

Enabled ☑

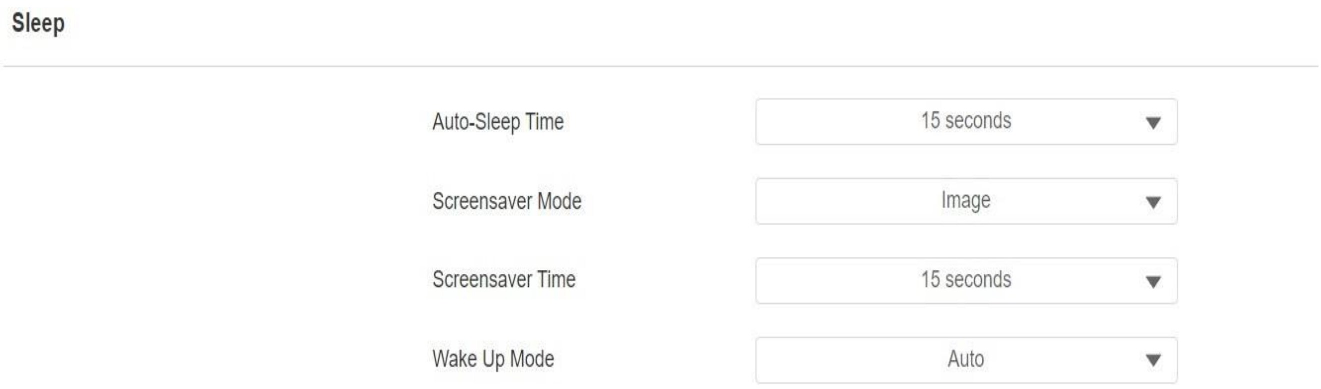
Start Time - End Time: 18 - 23 (0~23 Hour)

Start Time- End Time - you can set the time when the LED lighting in the card area turns on.

6.4 - Screensaver configuration

You can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction.
To configure LED on card reader area:

Device > LCD



Sleep

Auto-Sleep Time: 15 seconds

Screensaver Mode: Image

Screensaver Time: 15 seconds

Wake Up Mode: Auto

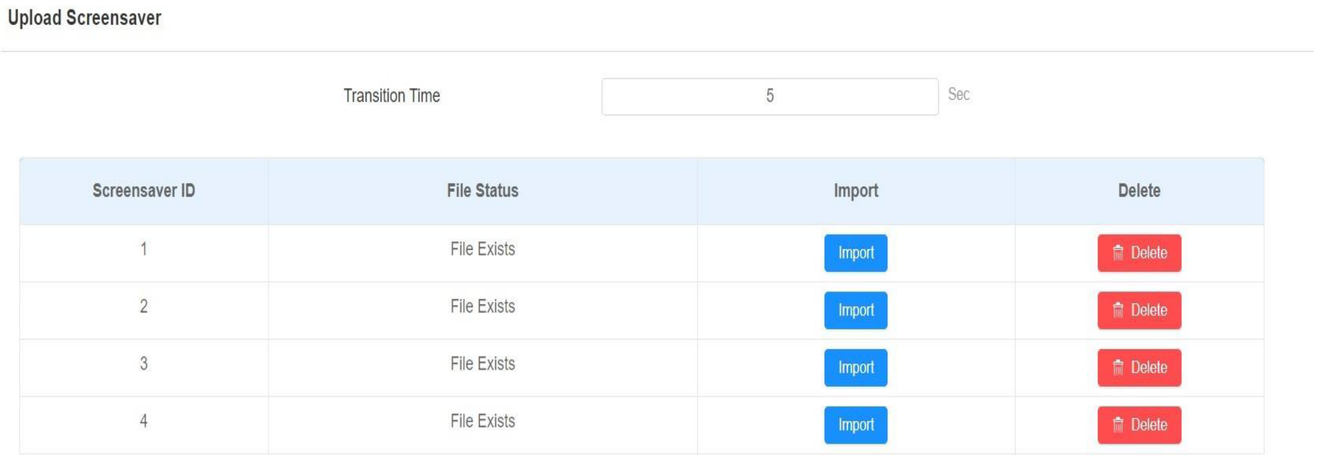
Table A4 - MyBell IP Keypad Station - Screensaver configuration

Setting	Description
Auto-Sleep Time	It ranges from 5 seconds to 30 minutes and determines the time after which the screen saver mode turns on if there is no operation on the device or no one is detected approaching.
Screensaver Mode	Image displays the default picture or the picture uploaded.
Screensaver Time	The screensaver duration after which the device goes into the sleep mode. Screensaver duration ranges from 5 seconds to 30 minutes. The default is 15 seconds.
Wake Up Mode	• **Auto** - the screen awakes when someone approches without touching the screen • **Manual** - the screen needs to be touched to wake up

6.5 - Screensaver uploading

To upload screensaver pictures to the device:

Device > LCD



Upload Screensaver

Transition Time: 5 Sec

Screensaver ID	File Status	Import	Delete
1	File Exists	Import	Delete
2	File Exists	Import	Delete
3	File Exists	Import	Delete
4	File Exists	Import	Delete

- **Transition Time** - the time after which the pictures changes for the next one

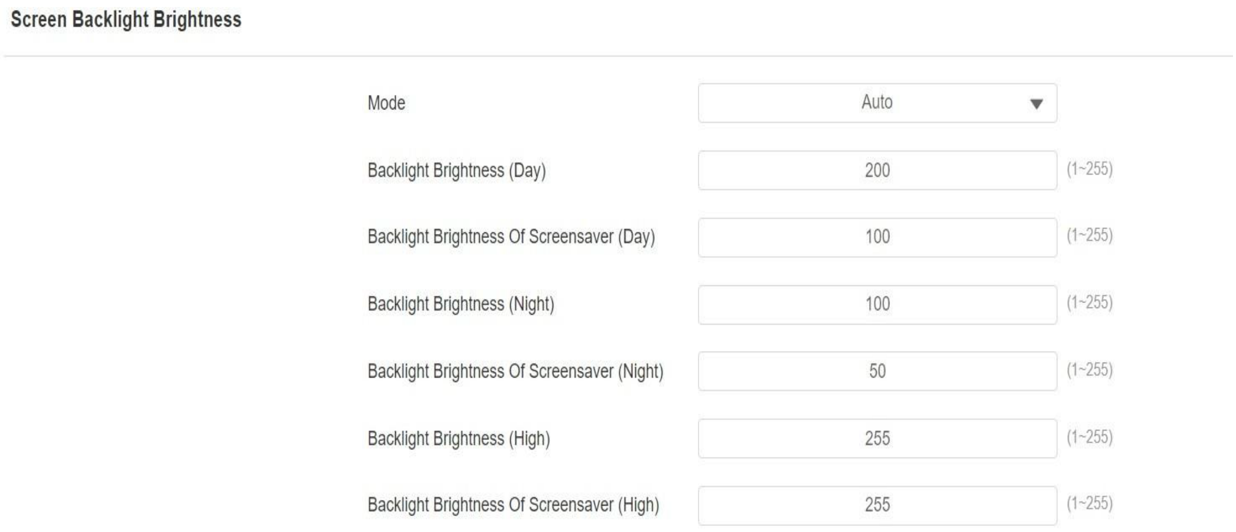
Note

The file should be in .jpg format with a 1M max size.

6.6 - Adjusting screen backlight brightness

To adjust the backlight brightness:

Device > LCD



Screen Backlight Brightness

Mode: Auto

Backlight Brightness (Day): 200 (1~255)

Backlight Brightness Of Screensaver (Day): 100 (1~255)

Backlight Brightness (Night): 100 (1~255)

Backlight Brightness Of Screensaver (Night): 50 (1~255)

Backlight Brightness (High): 255 (1~255)

Backlight Brightness Of Screensaver (High): 255 (1~255)

The backlight brightness has three modes, Day, Night, and High. They are determined by the photoresistor:

- If the current photoresistor is lower than the preset minimum photoresistor, the device is in High mode.
- If the current value is between the minimum and maximum photoresistor, the device is in Day mode.
- If the current value is higher than the maximum photoresistor, the device is in Night mode.

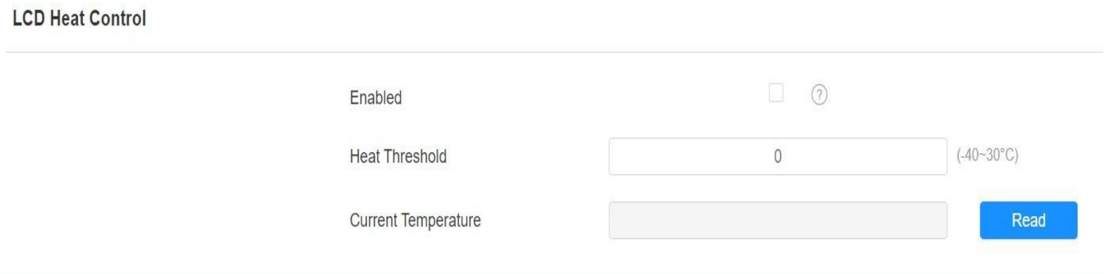
Table A5 - MyBell IP Keypad Station - Screen backlight brightness configuration

Setting	Description
Backlight Brightness (Day)	The brightness value ranges from 1 to 255. The default is 200. The larger the value, the brighter the screen.
Backlight Brightness Of Screensaver (Day)	The backlight for the screensaver in the daytime with the value ranging from 1 to 255
Backlight Brightness (Night)	The backlight at night with a value ranging from 1 to 255
Backlight Brightness Of Screensaver (Night)	The backlight for the screensaver at night with the value ranging from 1 to 255
Backlight Brightness (High)	The backlight with a value ranging from 1 to 255
Backlight Brightness Of Screensaver (High)	The backlight for the screensaver with a value ranging from 1 to 255.

6.7 - LCD Heat Control

To ensure normal operation of the door phone in low temperature, you can heat up the device LCD screen according to your heat control setting. To configure heat control:

Intercom > Basic



LCD Heat Control

Enabled: □

Heat Threshold: 0 (-40~30°C)

Current Temperature:

Table A6 - MyBell IP Keypad Station - Screensaver configuration

Setting	Description
Enabled	This function cannot be used in Low Power Mode. You need to use POE+ to ensure a sufficient power supply.
Threshold	When the device temperature reaches the threshold, the device starts heating up.
Current Temperature	Click **Read** to acquire the device's current temperature.

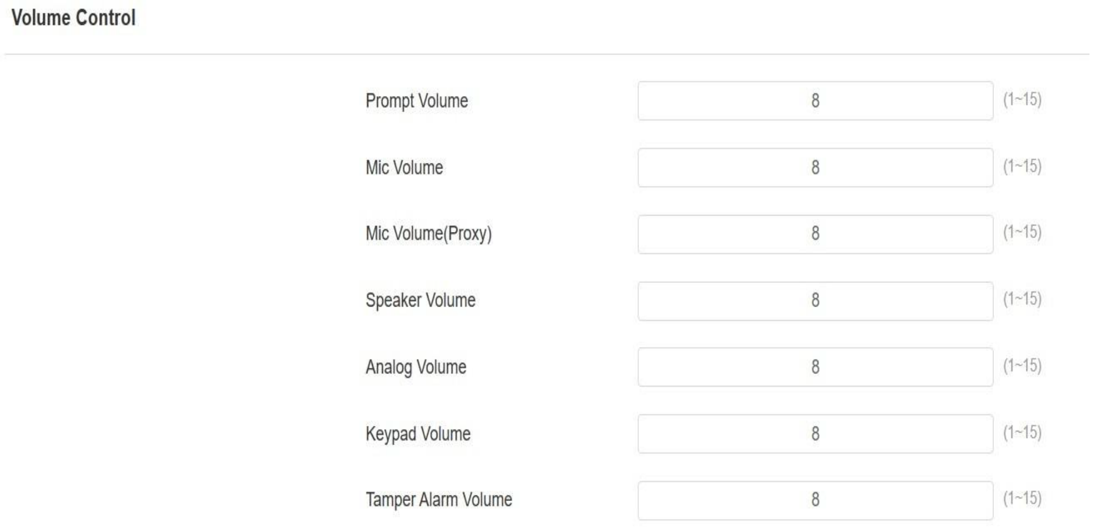
7 VOLUME AND TONE CONFIGURATION

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 volume by the web interface:

Phone > Audio > Volume Control



Volume Control

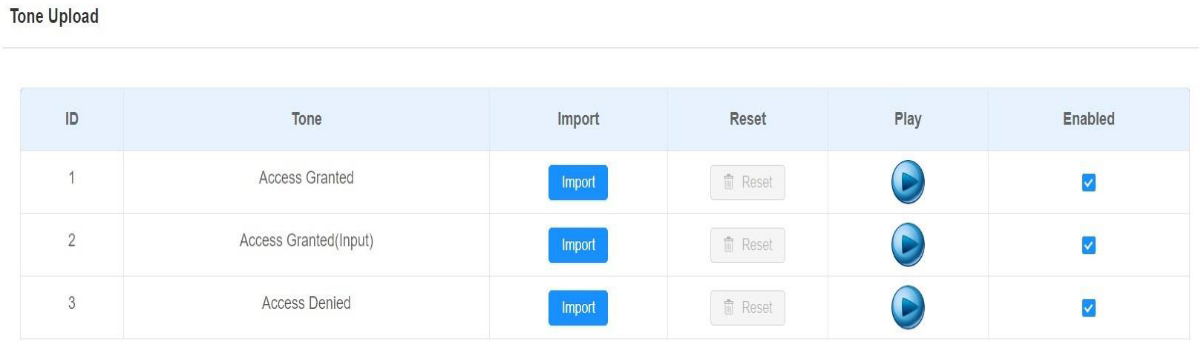
Prompt Volume	8	(1~15)
Mic Volume	8	(1~15)
Mic Volume(Proxy)	8	(1~15)
Speaker Volume	8	(1~15)
Analog Volume	8	(1~15)
Keypad Volume	8	(1~15)
Tamper Alarm Volume	8	(1~15)

- **Mic Volume (Proxy)** - the mic volume of the analog switch
- **Analog Volume -** the volume of the analog switch during a call

7.2 - Tone files uploading

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

Device > Audio



Tone Upload

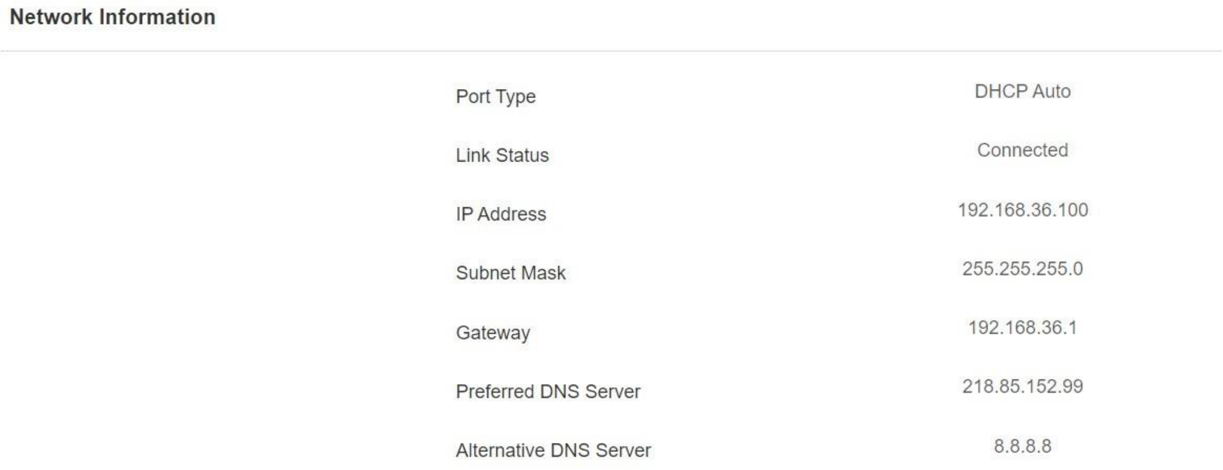
ID	Tone	Import	Reset	Play	Enabled
1	Access Granted	Import	Reset	▶	☑
2	Access Granted(Input)	Import	Reset	▶	☑
3	Access Denied	Import	Reset	▶	☑

8 NETWORK CONFIGURATION

8.1 - Network status

To check the network status by the web interface:

Status > Info > Network Information.



Network Information

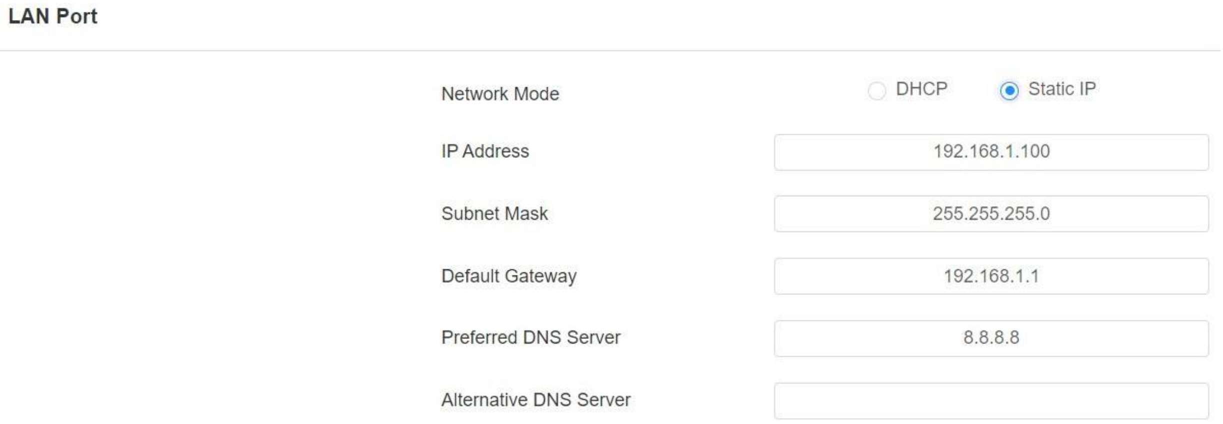
Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.100
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternative DNS Server	8.8.8.8

8.2 - Device network configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the Dynamic Host Configuration Protocol (DHCP) server.

To configure the device network by the web interface:

Network > Basic



LAN Port

Network Mode	○ 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
Alternative DNS Server	

Table A7 - MyBell IP Keypad Station - Screen backlight brightness configuration

Setting	Description
DHCP	DHCP mode is the default network connection. If selected, the DHCP server assigns the device with an IP address, subnet mask, default gateway, and DNS server address automatically.
Static IP	If selected, the IP address, subnet mask, default gateway, and DNS server address(es) needs to be configured manually according to the actual network environment.
IP Address	Needs to be type in if the static IP mode is selected
Subnet Mask	Needs to be set according to the actual network environment
Default Gateway	Needs to be set according to the IP address
Preferred/Alternate DNS	The preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary one. The door phone connects to the alternate server when the primary server is unavailable.

You can also configure the network on the device.

To enter the network setting screen press:

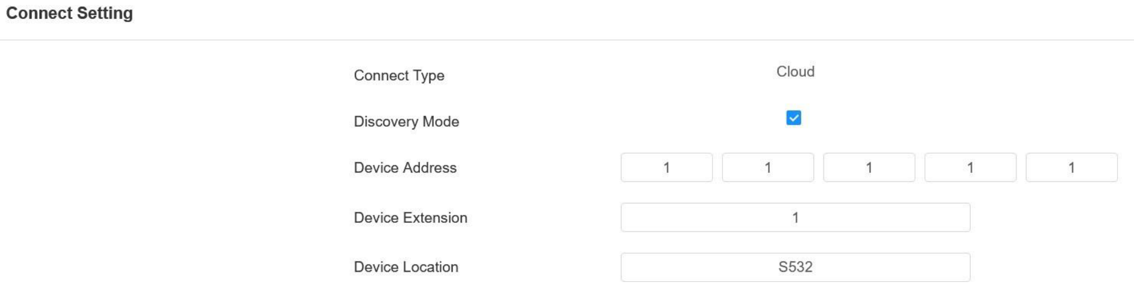
***2396#** > **3** > **1**

8.3 - Device deployment in network

You can configure the device with details such as location, operation mode, address, and extension numbers to facilitate device control and management.

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

Network > Advanced



Connect Setting

Connect Type: Cloud

Discovery Mode: ☑

Device Address: 1 1 1 1 1

Device Extension: 1

Device Location: S532

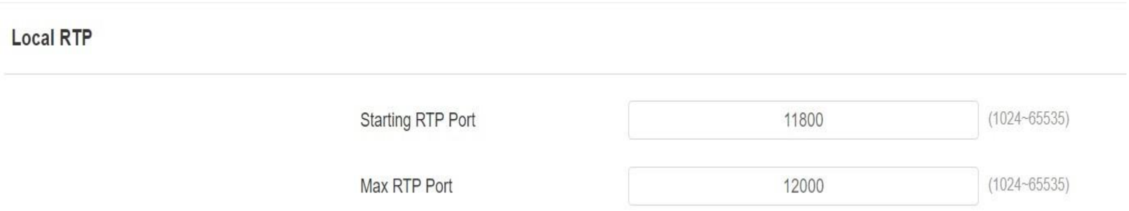
Table A8 - MyBell IP Keypad Station - Device deployment in network	
Setting	**Description**
Server Mode	It's set up automatically according to the actual device connection with a specific server in the network such as **SDMC** or **Cloud** and **None**. **None** is the default factory setting indicating the device isn't in any server type.
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 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.

8.4 - Device local RTP configuration

You need to set a range of Real-time Transport Protocol (RTP) ports on your device and router to avoid network interference and improve audio and video quality.

To configure the device local RTP by the web interface:

Network > Advanced > Local RTP



Local RTP

Starting RTP Port: 11800 (1024~65535)

Max RTP Port: 12000 (1024~65535)

Setting:

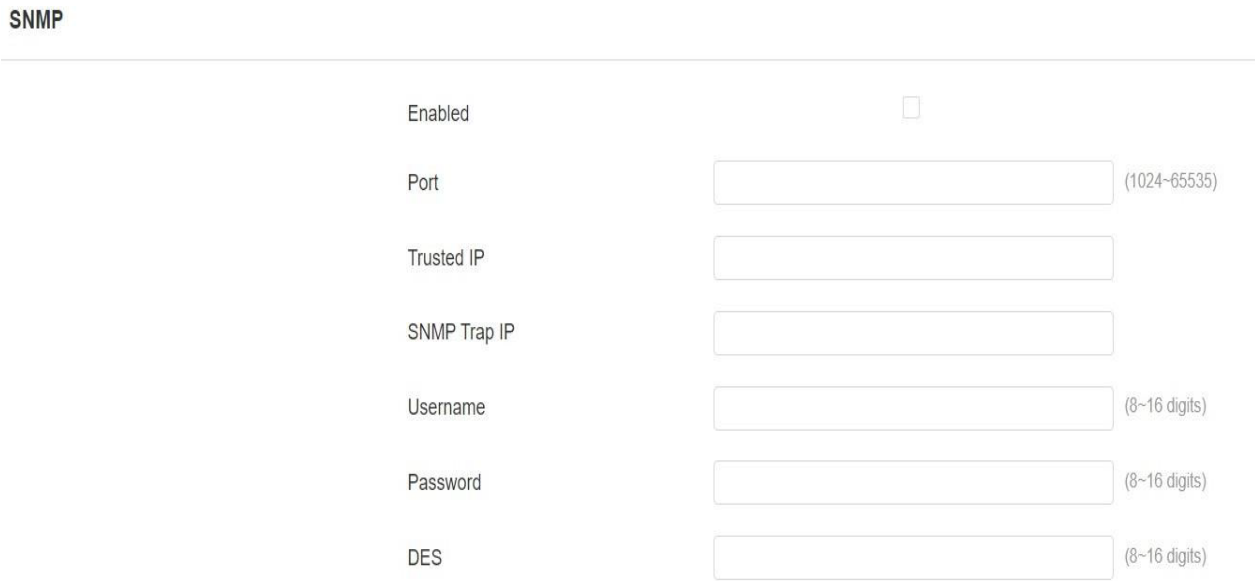
- **Starting RTP Port** - the port value for establishing the start point for the exclusive data transmission range
- **Max RTP Port** - the port value for establishing the endpoint for the exclusive data transmission range

8.5 - SNMP configuration

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

To configure the SNMP by the web interface:

Network > Advanced > SNMP



SNMP

Enabled □

Port (1024~65535)

Trusted IP

SNMP Trap IP

Username (8~16 digits)

Password (8~16 digits)

DES (8~16 digits)

Setting:

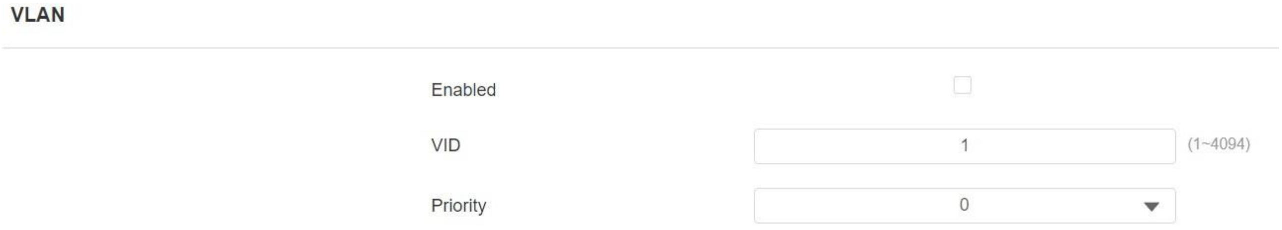
- **Port** - the SNMP server port
- **Trusted IP** - the allowed SNMP server address. It can be an IP address or any valid URL domain name

8.6 - 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 VLAN by the web interface:

Network > Advanced > VLAN



VLAN

Enabled □

VID 1 (1~4094)

Priority 0

Settings:

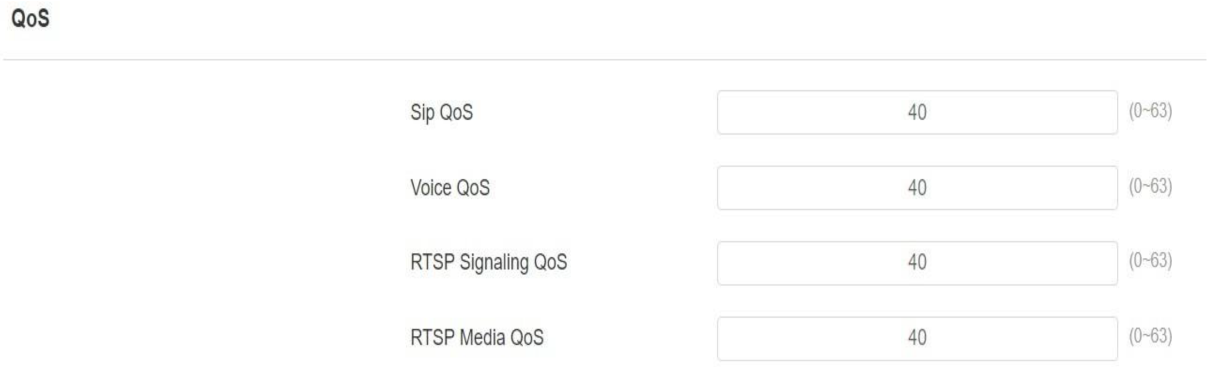
- **VID -** configure VLAN ID for designated port.
- **Priority -** select VLAN priority for designated port.

8.7 - QoS configuration

Quality of Service (QoS) is a network ability to provide better service for specific network communications by utilizing various technologies. It serves as a security mechanism in networks, addressing issues like network latency and congestion. Ensuring QoS is crucial for networks with limited capacity, particularly for multimedia applications such as VoIP and IPTV. These applications often require a consistent transmission rate and are sensitive to delays.

To configure QoS by the web interface:

Network > Advanced > QoS



QoS

Sip QoS 40 (0~63)

Voice QoS 40 (0~63)

RTSP Signaling QoS 40 (0~63)

RTSP Media QoS 40 (0~63)

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 TR069 by the web interface:

Network > Advanced > TR069.

Table A9 - MyBell IP Keypad Station - TR069 configuration

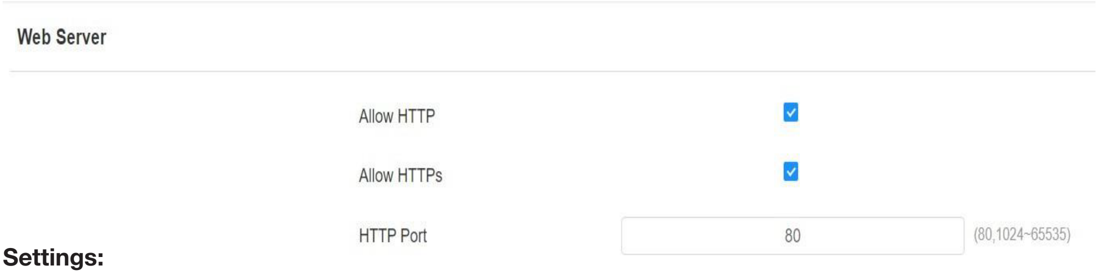
Setting	Description
Version	Select the supported TR069 version (1.0 or 1.1).
ACS/CPE URL	The URL address for auto-configuration servers (ACS) or customer-premise equipment (CPE).
Periodic Inform	Tick this checkbox to enable periodic inform.
Periodic Interval	Configure the interval for periodic inform.

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 web HTTP by the web interface:

Network > Advanced > Web Server.



Web Server

Allow HTTP ☑

Allow HTTPs ☑

HTTP Port 80 (80,1024~65535)

Settings:

- **HTTP Port - 80** is the default HTTP port.

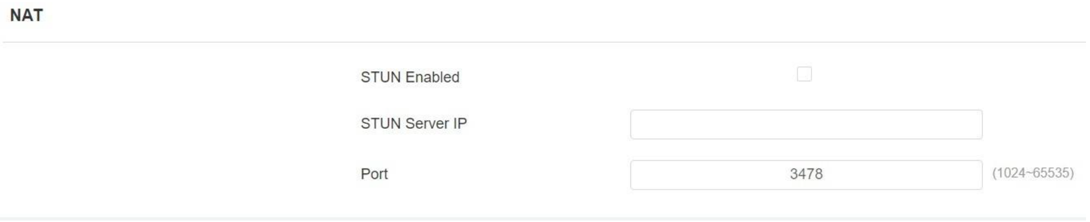
8.10 - NAT configuration

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's a way to translate an internal private network IP address into a legal network IP address technology.

To configure NAT by the web interface:

Account > Advanced > NAT.



NAT

STUN Enabled □

STUN Server IP

Port 3478 (1024~65535)

Settings:

- **Port - 3478** is the default port.

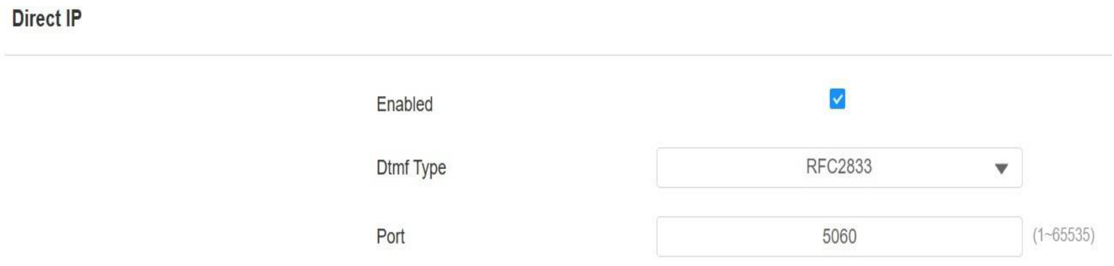
9 INTERCOM CALL CONFIGURATION

9.1 - IP call and IP call configuration

An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are in the same network.

To configure IP calls:

Phone > Call Feature > Direct IP.



Direct IP

Enabled ☑

Dtmf Type RFC2833

Port 5060 (1~65535)

Port - set the port for direct IP calls. The default port is **5060**, with a range from 1 to 65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

9.2 - SIP call & SIP call configuration

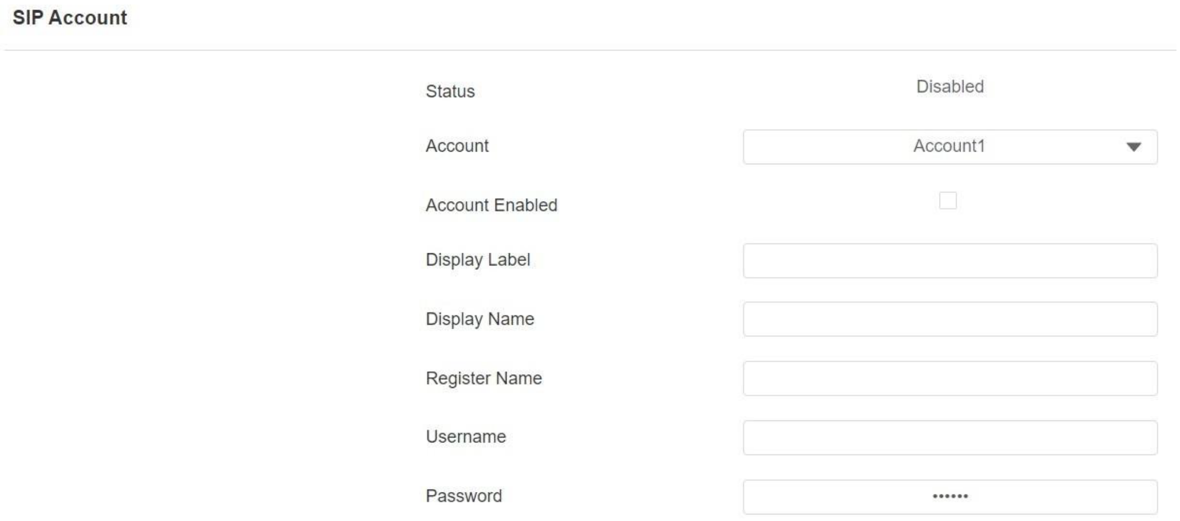
Session Initiation Protocol (SIP) is a signaling transmission protocol used for initiating, maintaining, and terminating calls. A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

9.2.1 - SIP account registration

The device supports the configuration of two SIP accounts, which can be registered under two independent servers.

To configure the SIP account by the web interface:

Web Account > Basic > SIP Account.



SIP Account

Status Disabled

Account Account1

Account Enabled □

Display Label

Display Name

Register Name

Username

Password ••••••

Table A10 - MyBell IP Keypad Station - SIP account registration

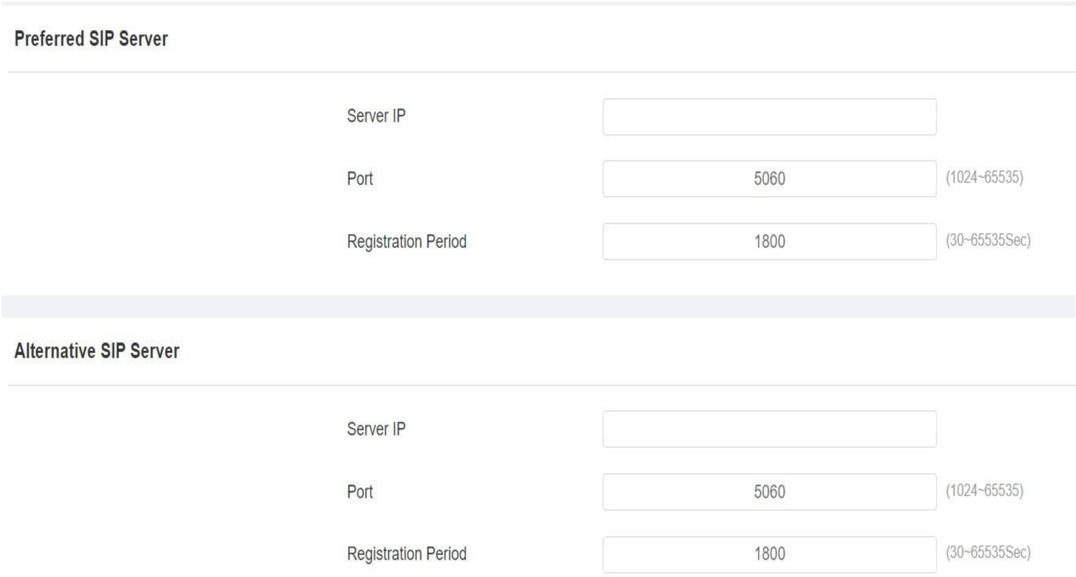
Setting	Description
Status	Displays whether the SIP account is registered
Account	**Account 1/Account 2** - the door phone supports 2 SIP accounts. **Account 1** is the default account for call processing. The system switches to **Account 2** if **Account 1** isn't registered. To designate the account to be used for outgoing calls, select the account number for contacts or dial plan prefixes in their settings.
Account Enabled	Check to activate the registered SIP account
Display Label	The device label to be shown on the device screen
Display Name	The device name to be shown on the device being called to
Username	The same as the username from the private branch exchange (PBX) server for authentication
Password	The same as the password from the PBX server for authentication

9.2.2 - SIP server configuration

SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX MyBell indoor monitor.

To configure the SIP server by the web interface:

Account > Basic > SIP Server.



Preferred SIP Server

Server IP

Port 5060 (1024~65535)

Registration Period 1800 (30~65535Sec)

Alternative SIP Server

Server IP

Port 5060 (1024~65535)

Registration Period 1800 (30~65535Sec)

Table A11 - MyBell IP Keypad Station - SIP server conifguration

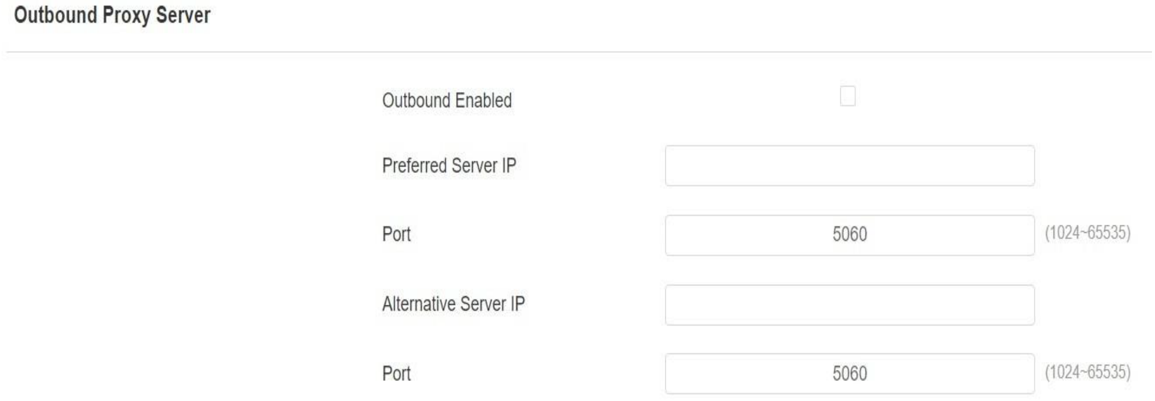
Setting	Description
Server IP	Enter the server IP address or its domain name
Port	Set up the SIP server port for data transmission.
Registration Period	Set up the SIP account registration time span. A SIP re-registration starts automatically if the account registration fails during the registration time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

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. It's an optional configuration, but if set up, all SIP requests get sent there in the first instance.

To configure the outboubound proxy server by the web interface:

Account > Basic > Outbound Proxy Server.



Outbound Proxy Server

Outbound Enabled □

Preferred Server IP

Port 5060 (1024~65535)

Alternative Server IP

Port 5060 (1024~65535)

Table A12 - MyBell IP Keypad Station - Conifguration of outbound proxy server

Setting	Description
Preferred Server IP	Enter the SIP proxy IP address.
Port	Set the port for establishing a call session through the outbound proxy server.
Alternative Server IP	Enter the SIP proxy IP address to be used when the main proxy malfunctions.
Port	Set the proxy port for establishing a call session through the backup outbound proxy server.

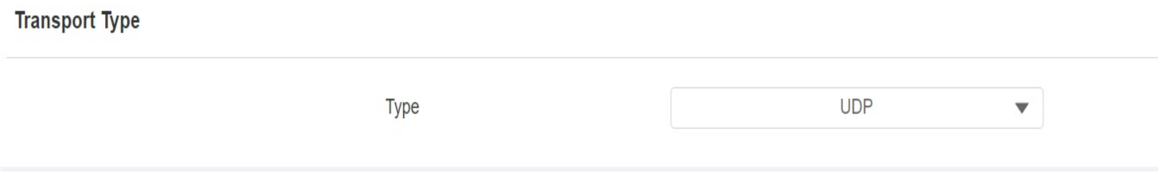
9.4 - Data transmission type configuration

The device supports the following data transmission protocols:

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

To configure data transmission type by the web interface:

Account > Basic > Transport Type.



Transport Type

Type: UDP

Table A13 - MyBell IP Keypad Station - Data transmission type conifguration	
Setting	**Description**
UDP	An unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
TCP	A reliable but less-efficient transport layer protocol.
TLS	A secured and reliable transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.
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.

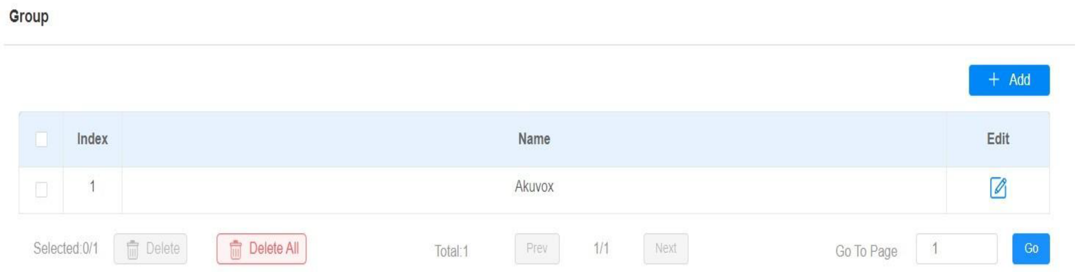
10 CONTACTS CONFIGURATION

10.1 - Contact groups management

To create and edit a contact group by the web interface:

Directory > User > Group

Click **+Add** to add a group. The device supports adding up to 1000 groups.



Group

+ Add

□	Index	Name	Edit
□	1	Akuvox	✎

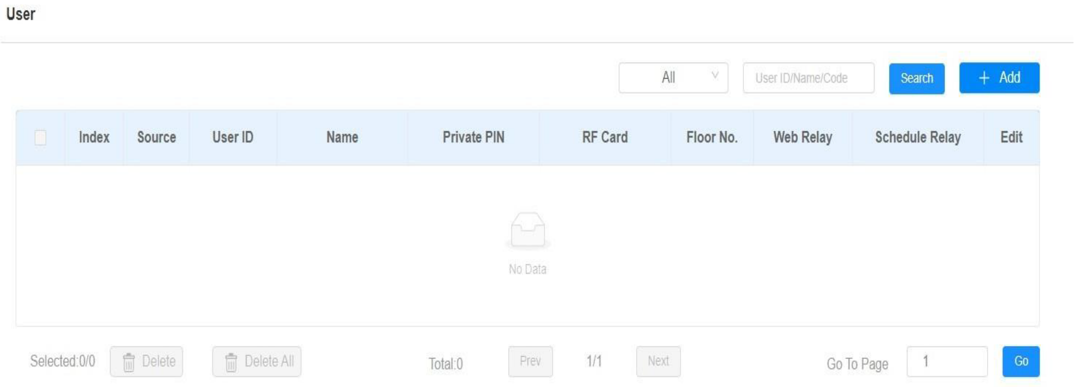
Selected:0/1 Delete Delete All Total:1 Prev 1/1 Next Go To Page 1 Go

10.2 - Adding contacts

To add a user by the web interface:

Directory > User

Click **+Add** to add a user. The device supports adding up to 1000 users.



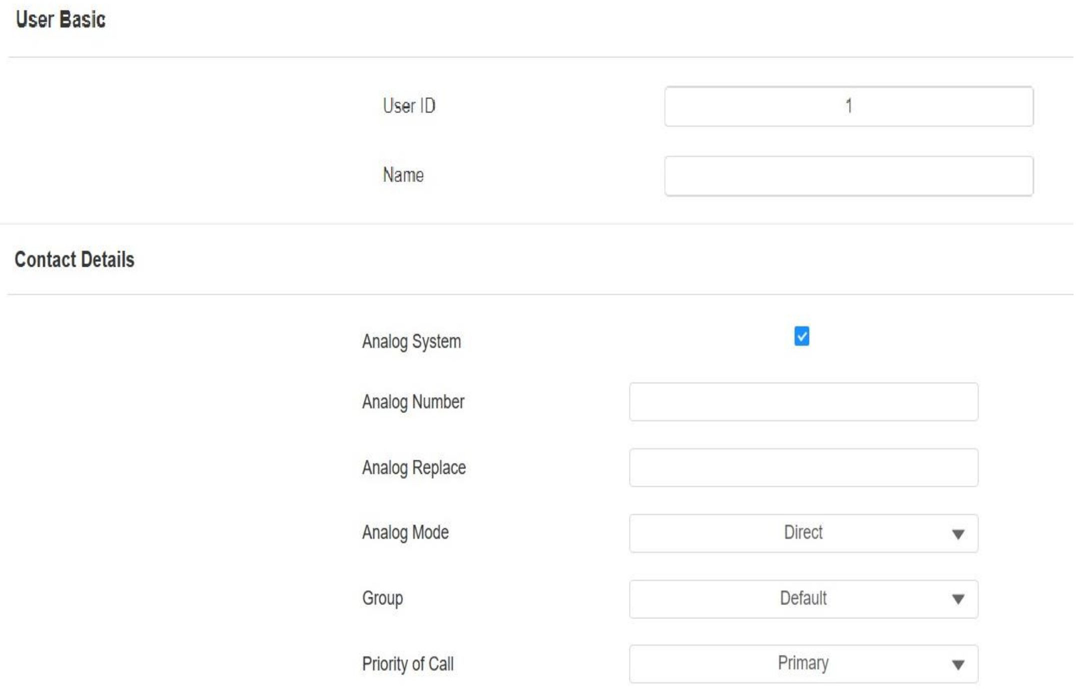
User

All User ID/Name/Code Search + Add

□	Index	Source	User ID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule Relay	Edit

No Data

Selected:0/0 Delete Delete All Total:0 Prev 1/1 Next Go To Page 1 Go



User Basic

User ID	1
Name	

Contact Details

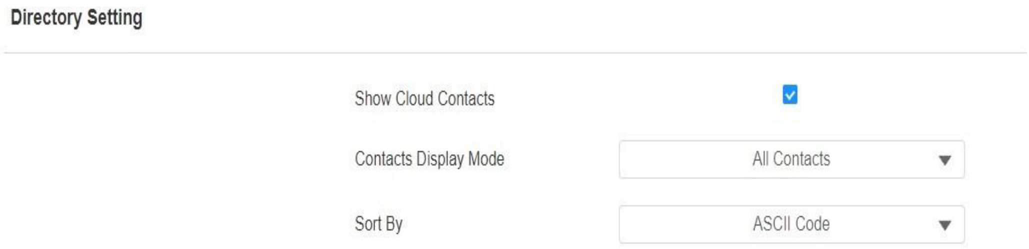
Analog System	☑
Analog Number	
Analog Replace	
Analog Mode	Direct ▼
Group	Default ▼
Priority of Call	Primary ▼

Table A14 - MyBell IP Keypad Station - SIP account registration	
Setting	**Description**
Analog System	If enabled, configure the analog number for users to call the analog switch.
Analog Number	The number of the analog switch
Analog Replace	Optional configuration. The short number replaces the analog number. Users can call the analog switch by entering the short number on the door phone keypad.
Analog Mode	• **Direct** - the analog switch is connected to the door phone through wires • **Proxy** - the analog switch isn't connected to the door phone through wires. When this option is selected, the analog proxy address needs to be filled in.
Analog Proxy Address	The proxy IP address
Group	Put the user in the desired contact group.
Priority of Call	You can set the priority coosing one of three options: **Primary, Secondary**, and **Tertiary.** If you marked one of the contacts as Primary it's the first to be called in its group when you press on the contact group to make a call.

10.3 - Contact list display configuration

To customize the contact list display:

Directory > Directory Setting



Directory Setting

Show Cloud Contacts ☑

Contacts Display Mode: All Contacts ▼

Sort By: ASCII Code ▼

Table A15 - MyBell IP Keypad Station - Contact list display configuration	
Setting	**Description**
Show Cloud Contacts	The contacts synchronized from the SmartPlus cloud can be displayed.
Contacts Display Mode	• **All Contacts** - displays all the contacts • **Groups Only** - displays contact groups. Press the desired group on the device screen to make a group call. • **Contact Display by Group** - displays contacts by groups. Press the group and users can see the contacts in it.
Sort By	• **ASCII Code** lists the tenants by their names in the sequence of the ASC I code. • **Room No.** lists the tenants according to their room numbers. • **Import** lists the tenants according to their order in the imported file.

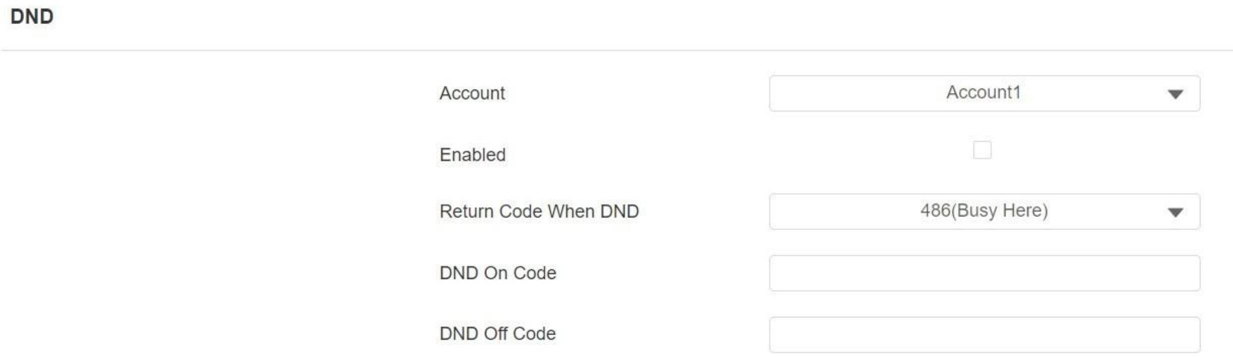
11 CALL CONFIGURATION

11.1 - DND 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:

Intercom > Call Feature



DND

Account: Account1

Enabled: □

Return Code When DND: 486(Busy Here)

DND On Code:

DND Off Code:

Table A16 - MyBell IP Keypad Station - Conifguration of DND

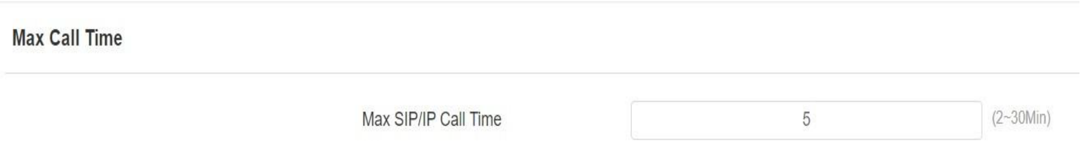
Setting	Description
Account	The account to apply the DND feature.
Return Code When DND	Specify the code sent to the caller through the SIP server when rejecting an incoming call in DND mode
DND On Code	The code used to turn on DND in the SIP server
DND Off Code	The code used to turn off DND in the SIP server

11.2 - 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:

Intercom > Call Feature > Max Call Time



Max Call Time

Max SIP/IP Call Time: 5 (2~30Min)

Setting:

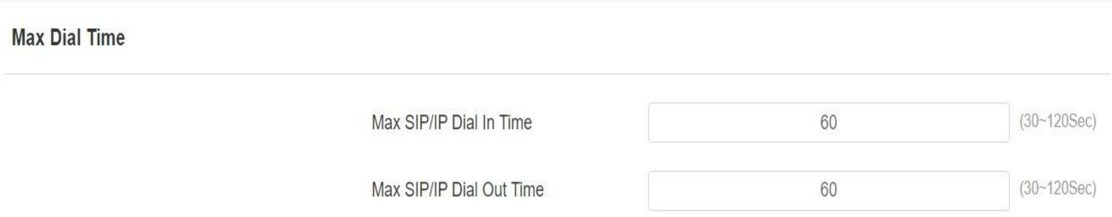
- **Max SIP/IP Call Time -** specify the maximum duration of all calls.

11.3 - Maximum dial duration configuration

Maximum Dial Duration is the time limit for incoming and outgoing calls on the door phone. If configured, the door phone automatically terminates the call if no one answers the call within the set time.

To configure the maximum dial duration:

Intercom > Call Feature > Max Dial Time.



Max Dial Time

Max SIP/IP Dial In Time: 60 (30~120Sec)

Max SIP/IP Dial Out Time: 60 (30~120Sec)

Setting:

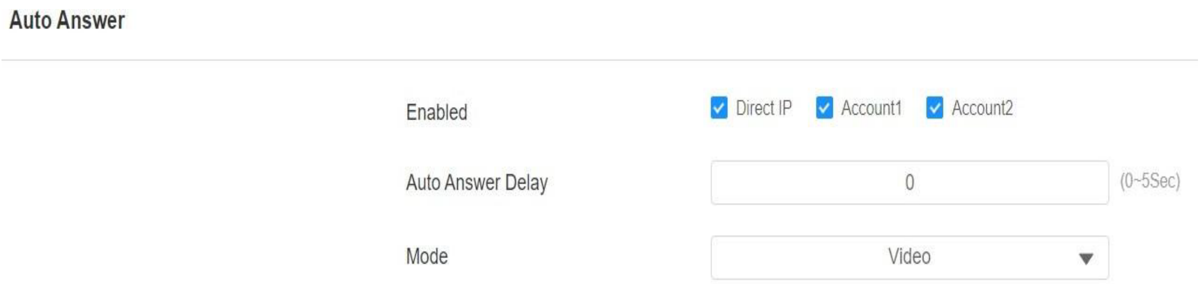
- **Max SIP/IP Dial In Time -** specify the maximum duration of an incoming call.
- **Max SIP/IP Dial Out Time** - specify the maximum duration of an outgoing call

11.4 - Auto answer configuration

Auto-answer feature enables the device to pick up automatically incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To configure the auto answer by the web interface:

Intercom > Call Feature > Auto Answer



Auto Answer

Enabled ☑ Direct IP ☑ Account1 ☑ Account2

Auto Answer Delay: 0 (0~5Sec)

Mode: Video ▼

Settings:

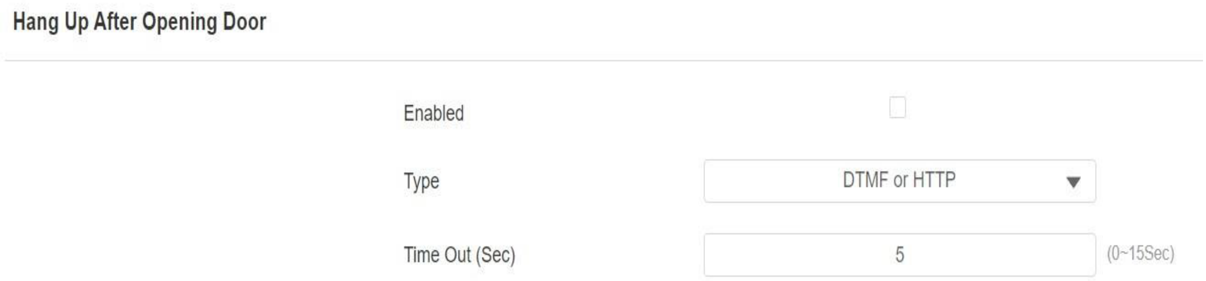
- **Auto Answer Delay:** set up the delay time (from 0 to 5 seconds) before the call can be answered automatically. For example, if you set the delay time to 1 second, then the call is answered automatically in 1 second.
- **Mode:** set up the video or audio mode for answering the call automatically.

11.5 - 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 door opening:

Intercom > Call Feature > Hang Up After Opening Door



Hang Up After Opening Door

Enabled □

Type: DTMF or HTTP ▼

Time Out (Sec): 5 (0~15Sec)

Setting:

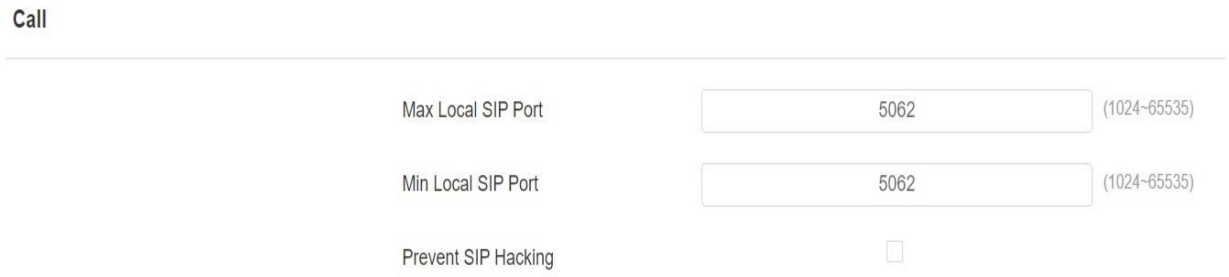
- **Type** - specifies the door unlock method. If the door is opened during a call, the door phone ends the call when the set hang-up time is reached.
- **Time Out (Sec)** - specifies the hang-up time limit. The door phone terminates automatically the call when the set time is reached after the door is opened.

11.6 - SIP hacking protection

Internet phone eavesdropping is a network attack enabling unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls from being compromised on the Internet.

To configure SIP hacking protection:

Account > Advanced > Call



Call

Max Local SIP Port: 5062 (1024~65535)

Min Local SIP Port: 5062 (1024~65535)

Prevent SIP Hacking □

Setting:

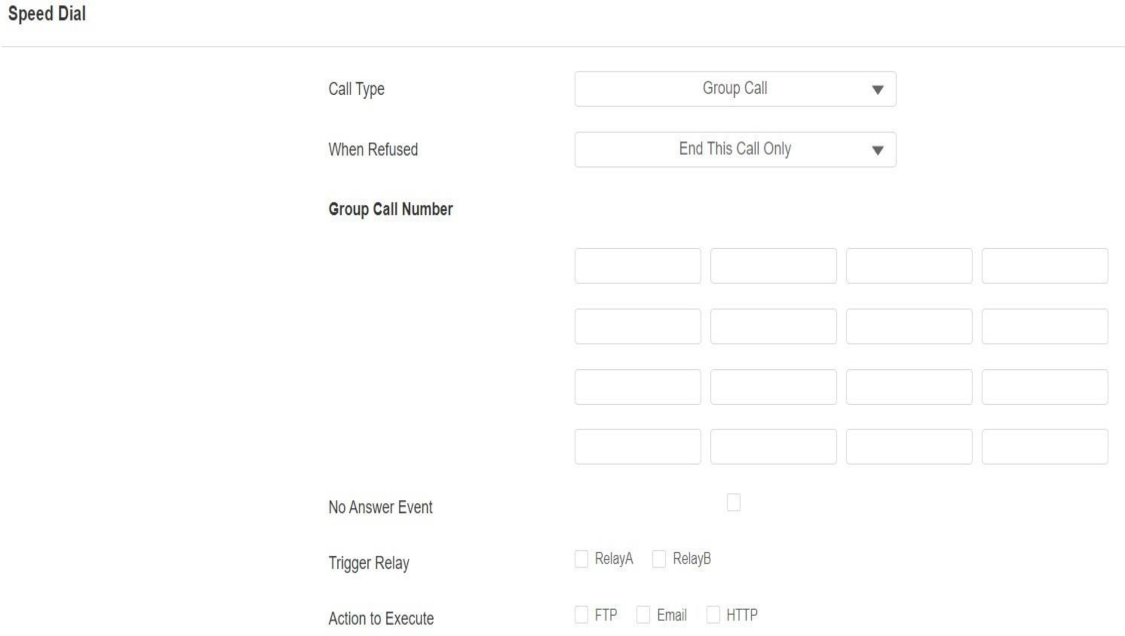
- **Prevent SIP Hacking** - Activate this feature to receive calls only from contacts in the whitelist. This protects users private and secret information from potential hackers during SIP calls.

11.7 - Speed dial

11.7.1 - Group call

Group call is used to quickly initiate the pre-configured numbers by pressing the Dial key. You can create up to 16 group call numbers.
To configure the group call:

Intercom > Basic > Speed Dial



Speed Dial

Call Type: Group Call

When Refused: End This Call Only

Group Call Number

No Answer Event □

Trigger Relay □ RelayA □ RelayB

Action to Execute □ FTP □ Email □ HTTP

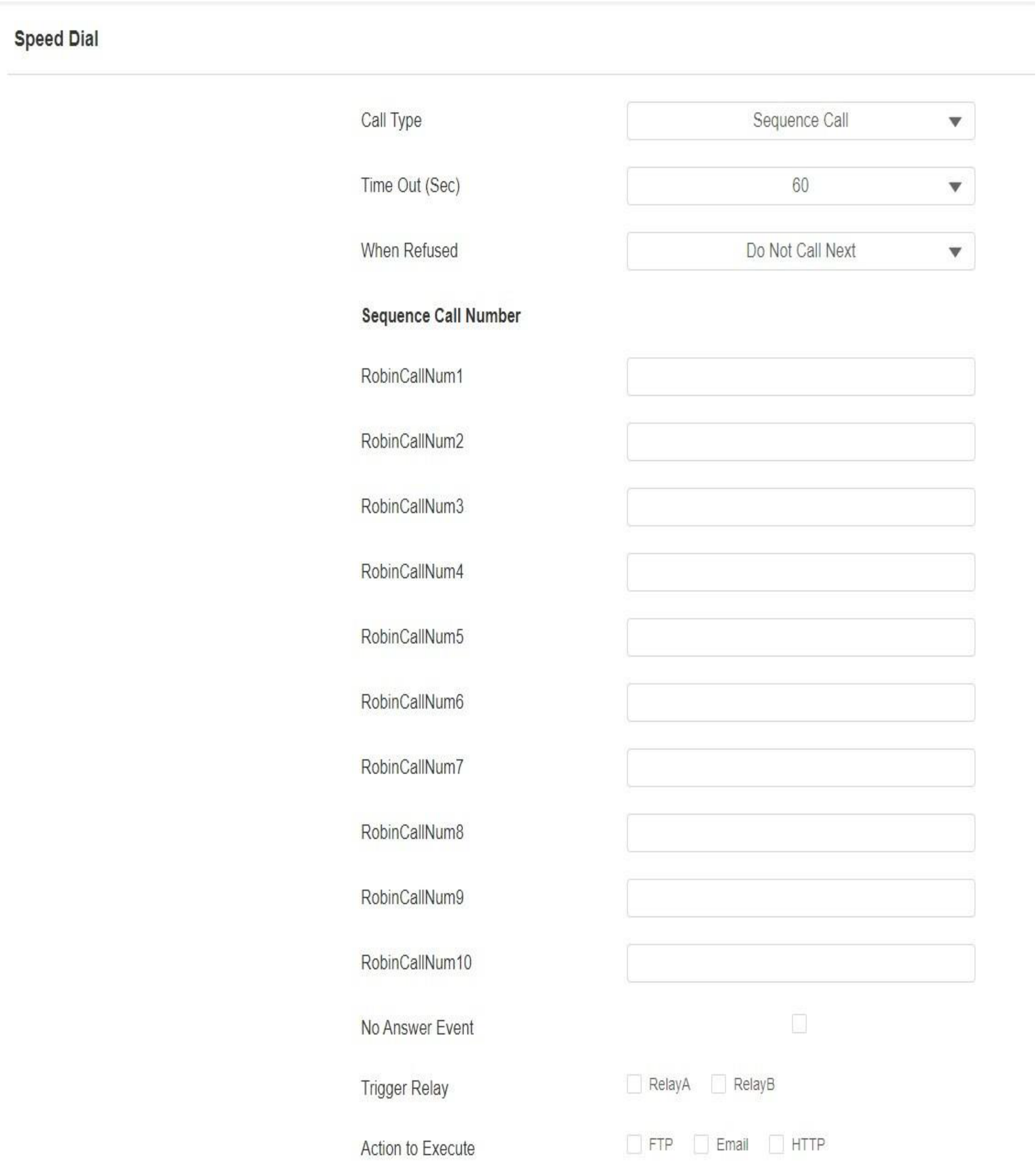
Table A17 - MyBell IP Keypad Station - Speed dial configuration

Setting	Description
Call Type	**Group Call** or **Sequence Call**
When Refused	• **End This Call Only** - The call made to the refusing party is terminated. • **End All Calls** - all calls are terminated
Group Call Number	If fill in, the local group number is called instead of the SmartPlus group call number.
No Answer Event	When the call isn't answered, actions are triggered
Trigger Relay	Relay to be triggered when the call isn't answered.
Action to Execute	Action to be triggered when the call isn't answered

11.7.2 - Sequence call

Sequence call enables you to dial a group of numbers in a predefined order until one of them answers.
To configure the sequence call:

Intercom > Basic > Speed Dial



Speed Dial

Call Type: Sequence Call ▼

Time Out (Sec): 60 ▼

When Refused: Do Not Call Next ▼

Sequence Call Number

RobinCallNum1

RobinCallNum2

RobinCallNum3

RobinCallNum4

RobinCallNum5

RobinCallNum6

RobinCallNum7

RobinCallNum8

RobinCallNum9

RobinCallNum10

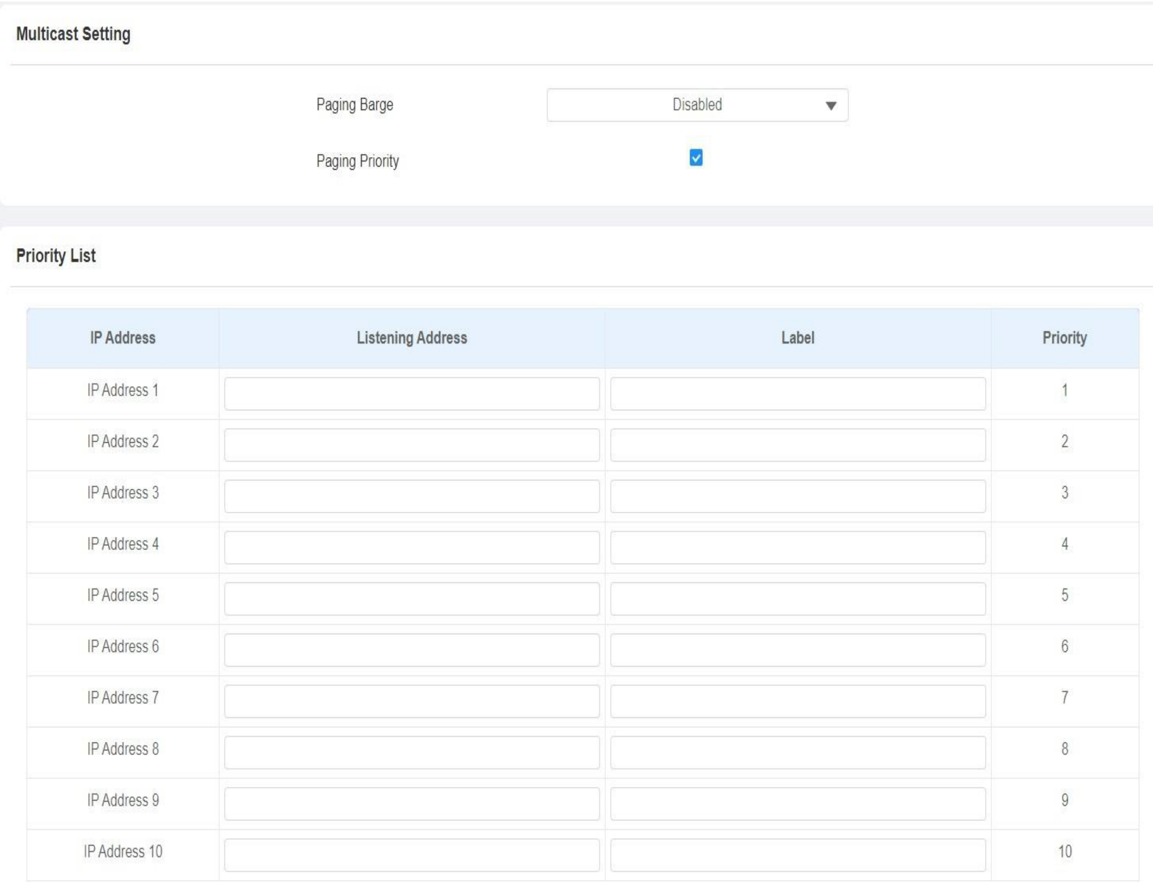
No Answer Event ☐

Trigger Relay ☐ RelayA ☐ RelayB

Action to Execute ☐ FTP ☐ Email ☐ HTTP

Table A18 - MyBell IP Keypad Station - Sequence call configuration

Setting	Description
Call Type	**Group Call** or **Sequence Call**
Time Out (Sec)	Set the call timeout before calling the next party when there is no answer from the first called party.
When Refused	• **Do Not Call Next** - The sequence call is terminated if the call is rejected by the called party. • **Call Next** - The sequence call is continued to the next called party if it's rejected by the called party
No Answer Event	When the call isn't answered, actions are triggered
Trigger Relay	Relay to be triggered when the call isn't answered.
Action to Execute	Action to be triggered when the call isn't answered



Multicast Setting

Paging Barge: Disabled ▾

Paging Priority: ☑

Priority List

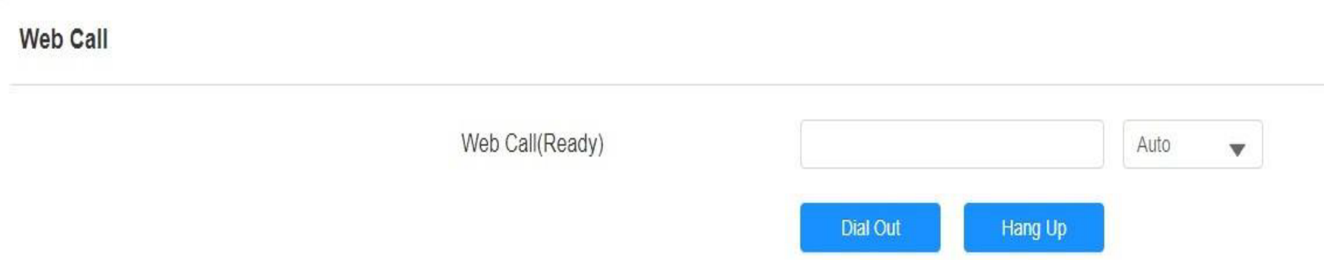
IP Address	Listening Address	Label	Priority
IP Address 1			1
IP Address 2			2
IP Address 3			3
IP Address 4			4
IP Address 5			5
IP Address 6			6
IP Address 7			7
IP Address 8			8
IP Address 9			9
IP Address 10			10

Table A19 - MyBell IP Keypad Station - Multicast configuration

Setting	Description
Paging Barge	Configure the amount of multicast calls having higher priority than an SIP call. If you disable Paging Priority by unticking the checkbox, the SIP call has higher priority than the multicast call.
Paging Priority Enabled	If enabled, multicast calls are perfomed in order of priority.
Listening Address	Enter the multicast IP address from which you want to listen 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.

11.8 - Web call

You can also make a call by the device web interface without approaching the device physically, for example, for testing purposes.
To make the call by the web interface:
System > Maintenance > Web Call



Web Call

Web Call(Ready)

Setting:

- **Web Call (Ready)** - Select the target SIP/IP number to make the web call.

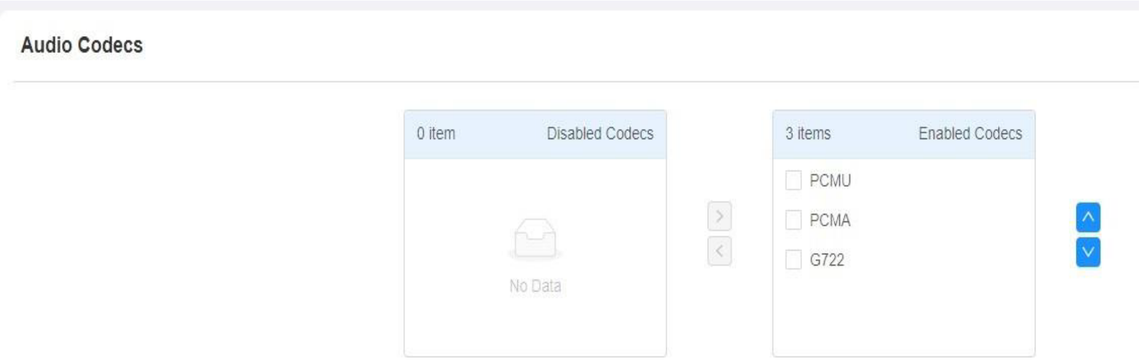
12 AUDIO AND VIDEO CODEC CONFIGURATION FOR SIP CALLS

12.1 - Audio codec configuration

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

To configure the audio codec by the web interface:

Account > Advanced.



Audio Codecs

0 item Disabled Codecs

No Data

3 items Enabled Codecs

□ PCMU
□ PCMA
□ G722

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

Table A20 - MyBell IP Keypad Station - Bandwidth consumption and sample rate for codecs types

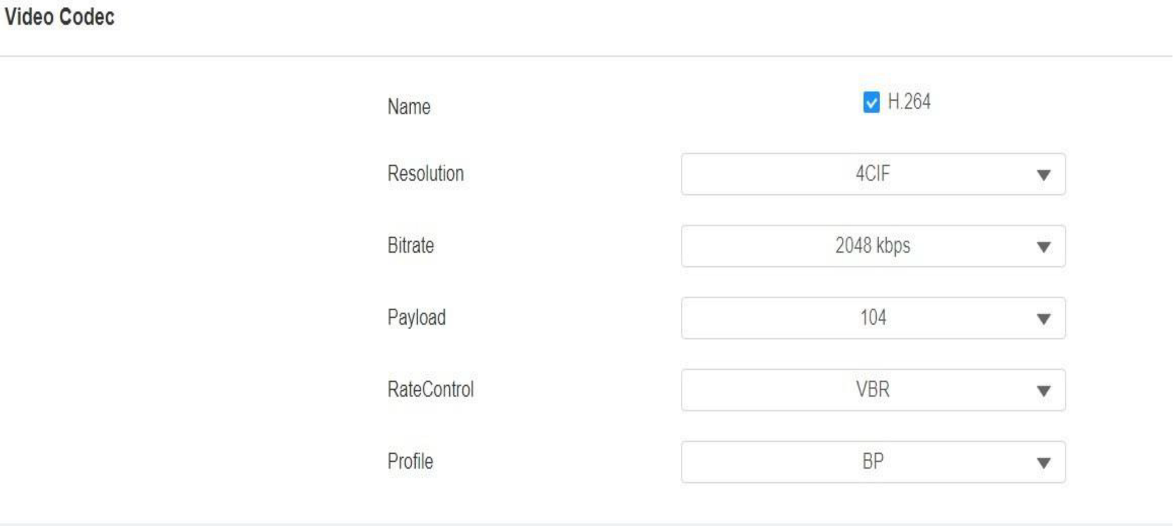
Codec type	Bandwidth consumption	Sample rate
PCMA	64 kbit/s	8 kHZ
PCMU	64 kbit/s	8 kHZ
G722	64 kbit/s	16 kHZ

12.2 - Video codec configuration

Thw door phone supports the H264 codec that provides better video quality at a much lower bit rate.

To configure the video codec by the web interface:

Account > Advanced



Video Codec

Name ☑ H.264

Resolution 4CIF

Bitrate 2048 kbps

Payload 104

RateControl VBR

Profile BP

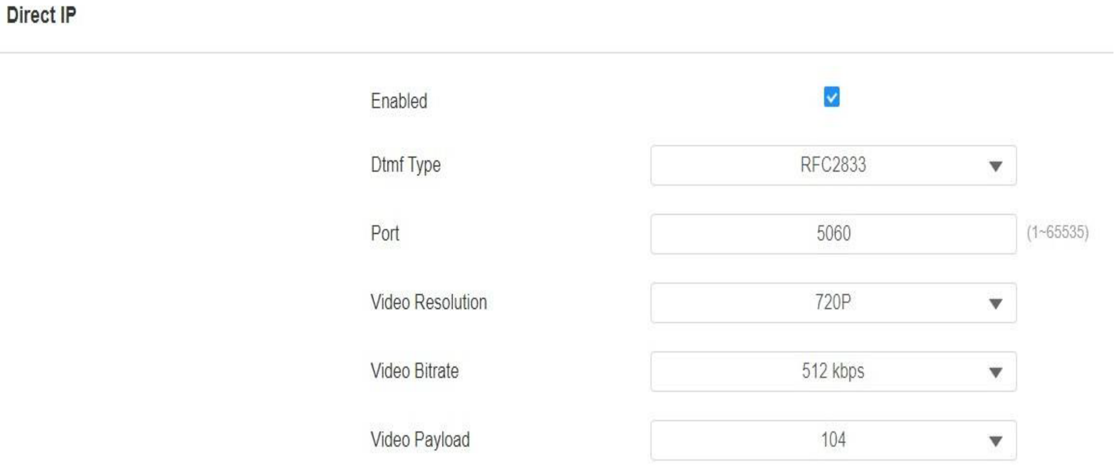
Table A21 - MyBell IP Keypad Station - Video codec configuration

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: **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.

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:

Intercome > Call Feature > IP Video Parameters.



Direct IP

Enabled ☑

Dtmf Type: RFC2833

Port: 5060 (1~65535)

Video Resolution: 720P

Video Bitrate: 512 kbps

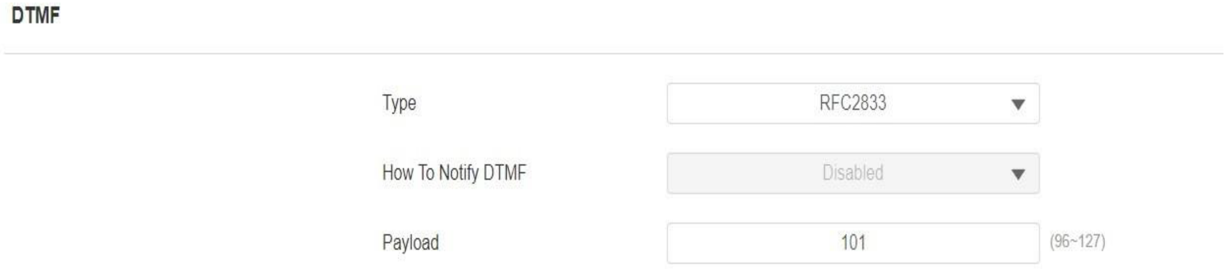
Video Payload: 104

Table A22 - MyBell IP Keypad Station - Video codec configuration for IP direct calls	
Setting	**Description**
Video Resolution	Select the codec resolution for the video quality from the following options: **CIF, VGA, 4CIF, 720P, 1080P** The default code resolution is **720P.**
Video Bitrate	The video stream bitrate ranges from 128 to 2048 kbps. The default code bitrate is 2048.
Video Payload	Select the payload type (ranging from 90 to 118) to set up the audio/video configuration file. The default payload is 104.

12.4 - DTMF data transmission configuration

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

Account > Advanced > DTMF



DTMF

Type: RFC2833

How To Notify DTMF: Disabled

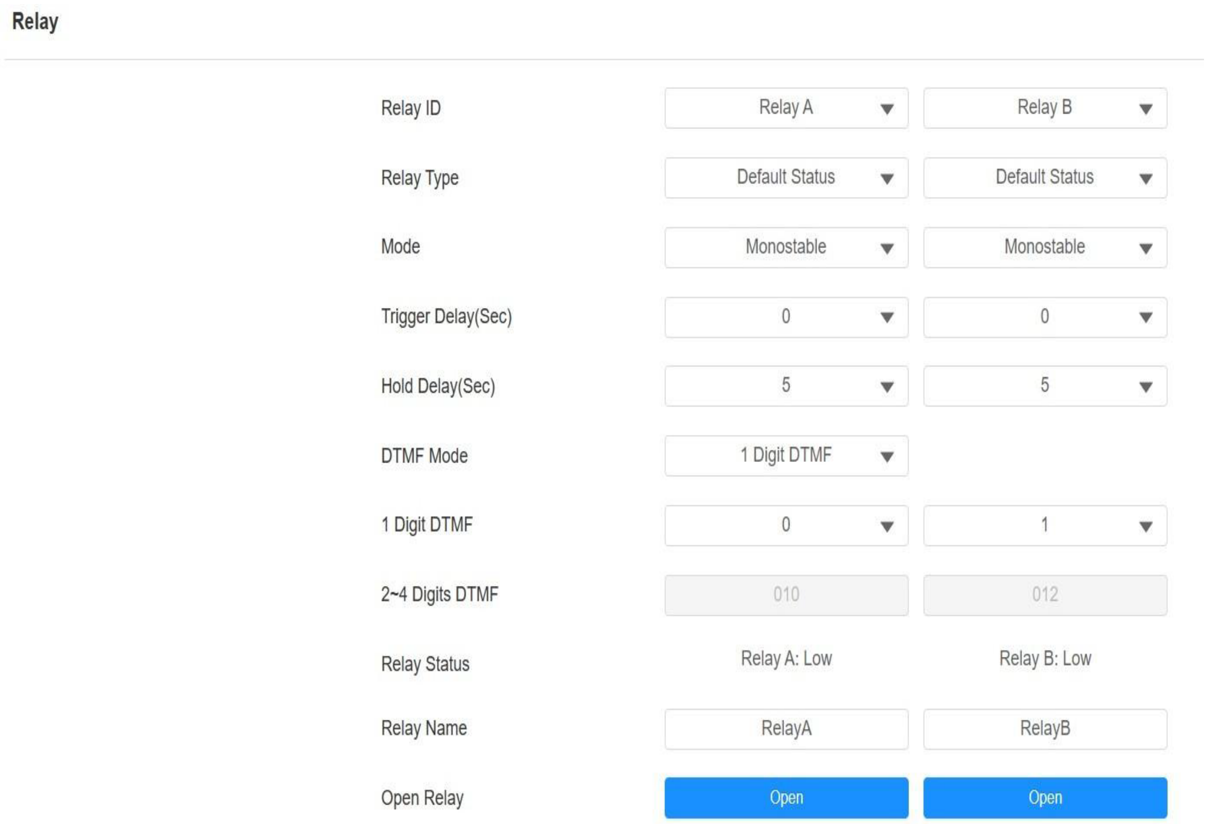
Payload: 101 (96~127)

Table A23 - MyBell IP Keypad 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.
How To Notifying DTMF	Select from the following types: **Disable, DTMF, DTMF-Relay, Telephone-Event.** It neeeds to be matched with the type adopted by the third party device. You need to set it up only when the third party device adopts the **Info** mode.
Payload	Set the payload according to the data transmission payload agreed on between the sender and receiver during the data transmission.

13 RELAY SETTING

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

Access Control > Relay



Relay

Relay ID	Relay A	Relay B
Relay Type	Default Status	Default Status
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	0	1
2~4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	RelayA	RelayB
Open Relay	Open	Open

Table A24 - MyBell IP Keypad Station - Relay switch configuration

Setting	Description
Relay ID	The specific relay for door access
Relay Type	Determine the interpretation of the Relay Status regarding the state of the door: • **Default State Relay Status:** • **Low** – the door is closed. • **High** – the door is opened. • **Invert State Relay Status:** • **High** – the door is closed. • **Low** – the door is opened.
Mode	• **Monostable** – the relay status is reset automatically within the relay delay time after the relay is triggered. • **Bistable** – relay status is reset after the relay is triggered again.
Trigger Delay (Sec)	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 (Sec)	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-digt DTMF code. Choose characters from: **0-9** and *****, **#**.
2~4 Digit DTMF	Set the DTMF code according to the **DMTF Mode** setting. Example: you need to set the 3-digit DTMF code if the **DTMF Mode** is set as **3 Digit**.
Relay Status	• **Low** (default) – normally closed (NC). • **High** – normally open (NO).
Relay Name	Name the relay switch as needed, for example, based on its location.

Note

External devices connected to the relay require separate power adapter.

14 DOOR ACCESS SCHEDULE MANAGEMENT

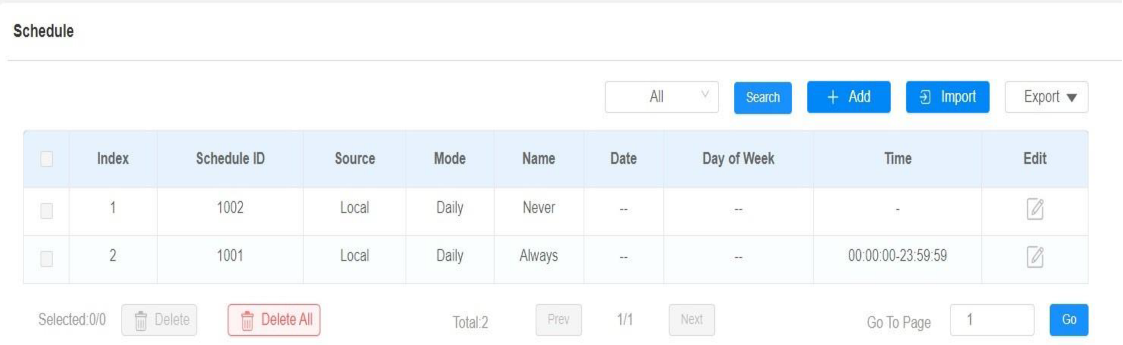
A door access schedule enables you to decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

14.1 - Creating door access schedule

You can create door access schedules for daily, weekly, or custom time periods.

To create a schedule:

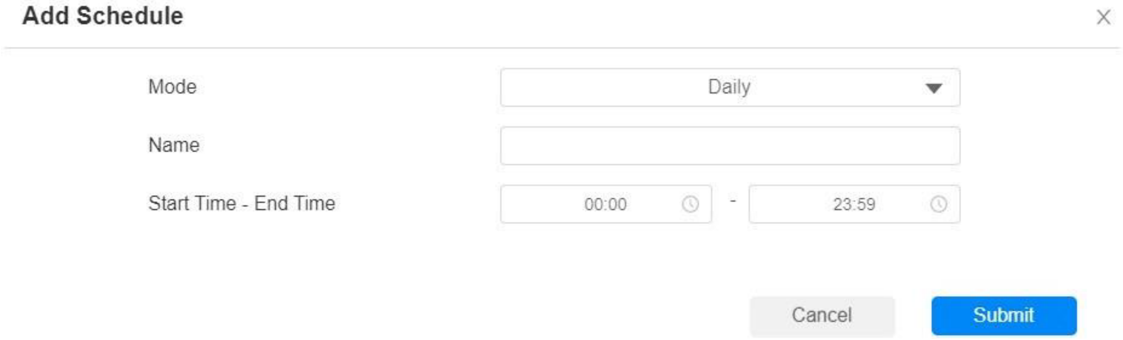
Setting > Schedule > +Add


Schedule

☐	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
☐	1	1002	Local	Daily	Never	--	--	-	✎
☐	2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	✎

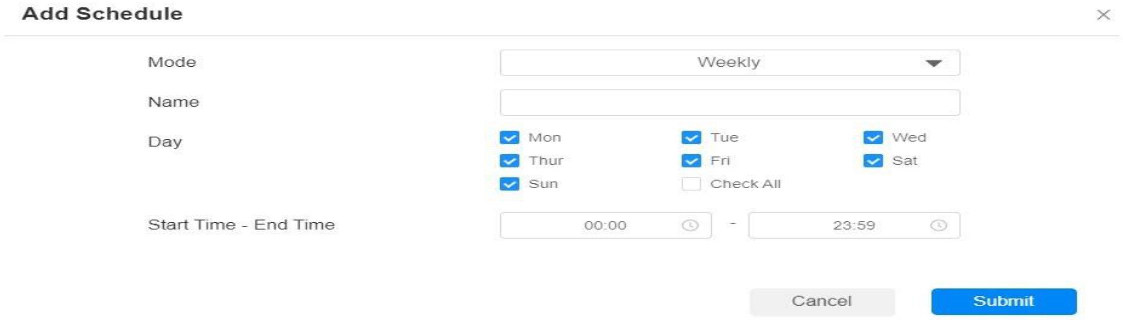
Selected:0/0 Total:2 1/1 Go To Page 1

To create a daily schedule:


Add Schedule

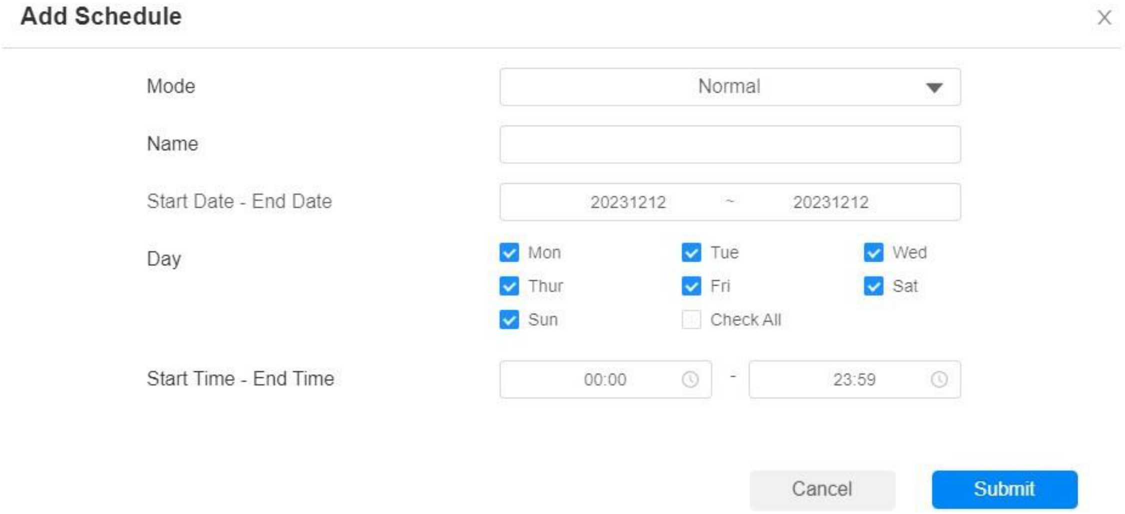
Mode	Daily
Name	
Start Time - End Time	00:00 - 23:59

To create a weekly schedule:


Add Schedule

Mode	Weekly
Name	
Day	☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun ☐ Check All
Start Time - End Time	00:00 - 23:59

To create a longer period schedule:

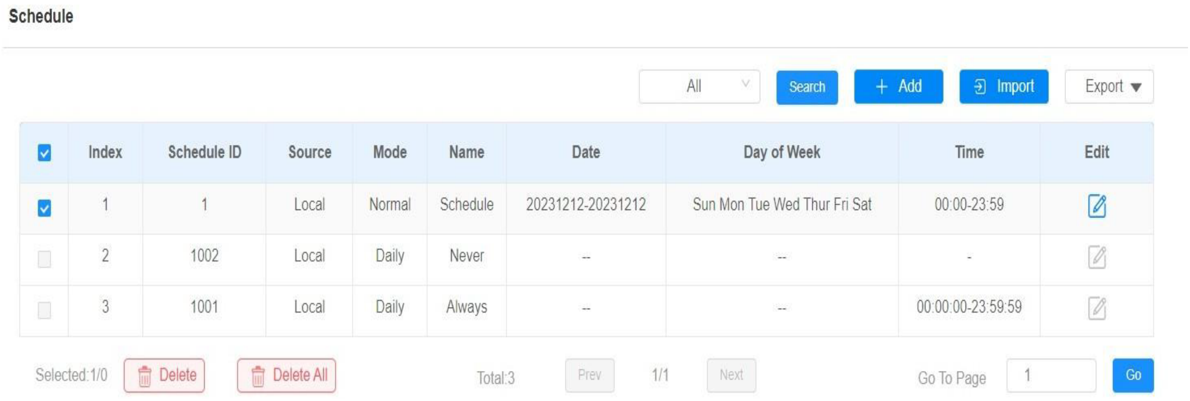

Add Schedule

Mode	Normal
Name	
Start Date - End Date	20231212 ~ 20231212
Day	☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun ☐ Check All
Start Time - End Time	00:00 - 23:59

14.2 - Editing door access schedule

To configure door access schedule:

Setting > Schedule > Tick the box of the local schedule to edit or delete



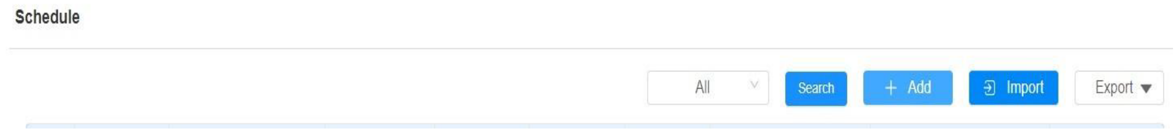
☑	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
☑	1	1	Local	Normal	Schedule	20231212-20231212	Sun Mon Tue Wed Thur Fri Sat	00:00-23:59	✎
□	2	1002	Local	Daily	Never	--	--	-	✎
□	3	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	✎

14.3 - Import and export of door access schedule

You can create door access schedules one by one or in bulk. You can export the current schedule file, edit it or add more schedules following the format, and import the new file to the desired devices. This helps you manage your door access schedules easily.

To import or export a door access schedule:

Setting > Schedule



Note

Only a **.xml** format file for importing and exporting the schedule is supported.

15 DOOR UNLOCK CONFIGURATION

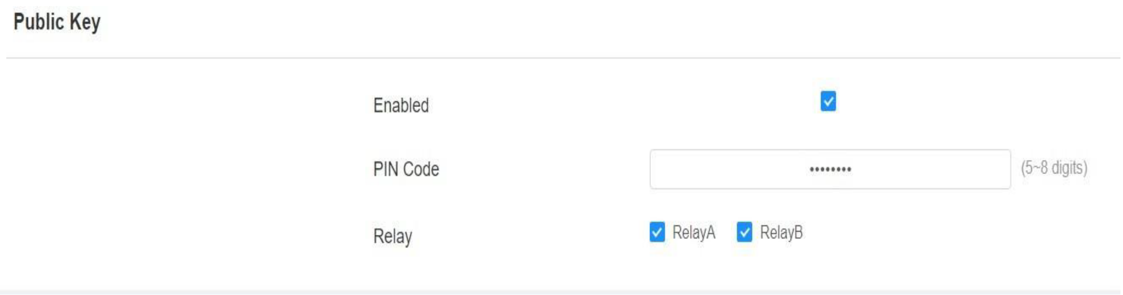
15.1 - Configuration of PIN code for door unlock

There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex.

15.1.1 - Public PIN cofiguration

To create or modify a public PIN:

Access Control > PIN Setting



Public Key

Enabled	☑
PIN Code	•••••••• (5~8 digits)
Relay	☑ RelayA ☑ RelayB

Setting:

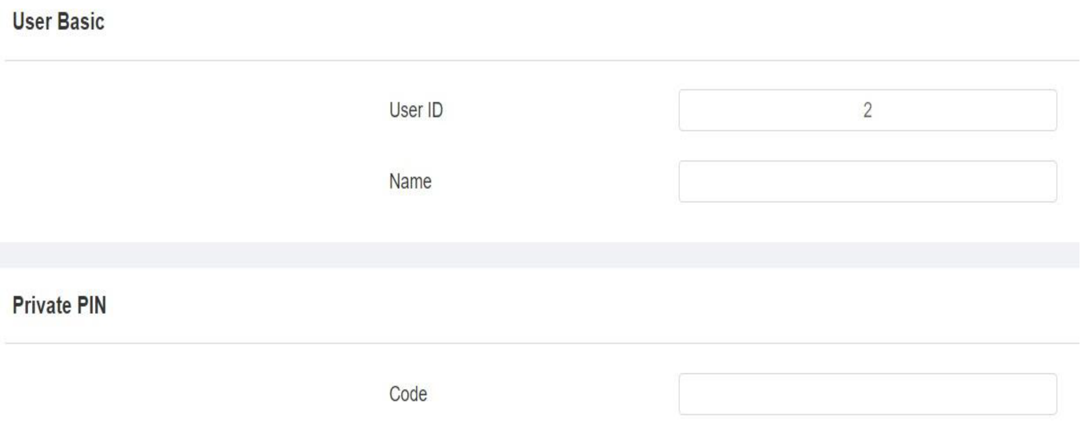
- **PIN Code** - Select a 3 - 8 digits PIN code accessible for universal use.
- **Relay** - The relay to be triggered

15.1.2 - Private PIN cofiguration

Using the web interface, you can create the PIN code and customize additional settings, such as defining the door access schedule to determine when the code is valid and which relay to open.

To create or modify a public PIN:

Directory > User > Add



User Basic

User ID	2
Name	

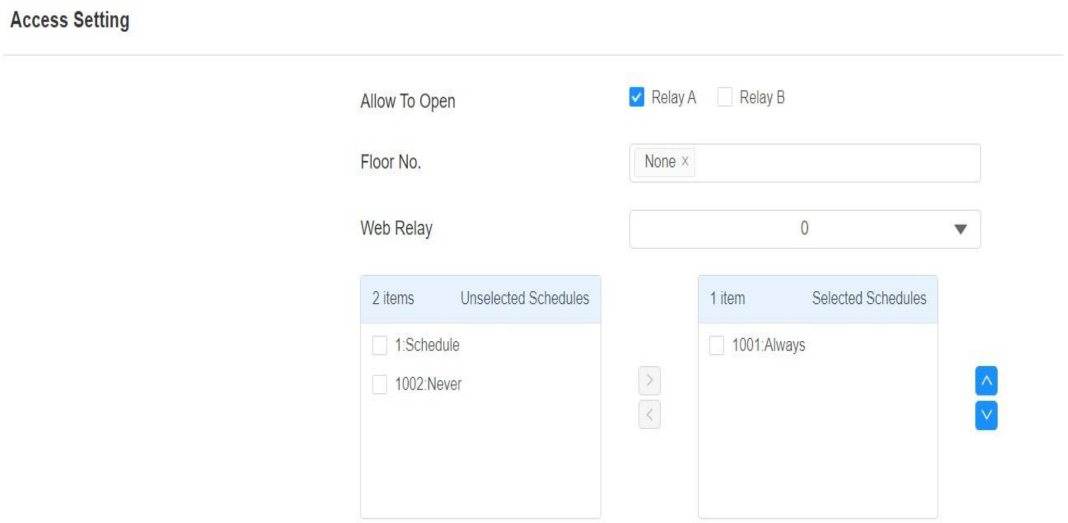
Private PIN

Code	

Setting:

- **User ID** - the unique identification number assigned to the user
- **Code** - Set a 2 - 8 digit PIN code solely for the use of this user. Each user can only be assigned a single PIN code.

Scroll down and select the door access schedule for private PIN code door access.



Access Setting

Allow To Open	☑ Relay A □ Relay B
Floor No.	None ×
Web Relay	0 ▼

2 items Unselected Schedules
□ 1:Schedule
□ 1002:Never

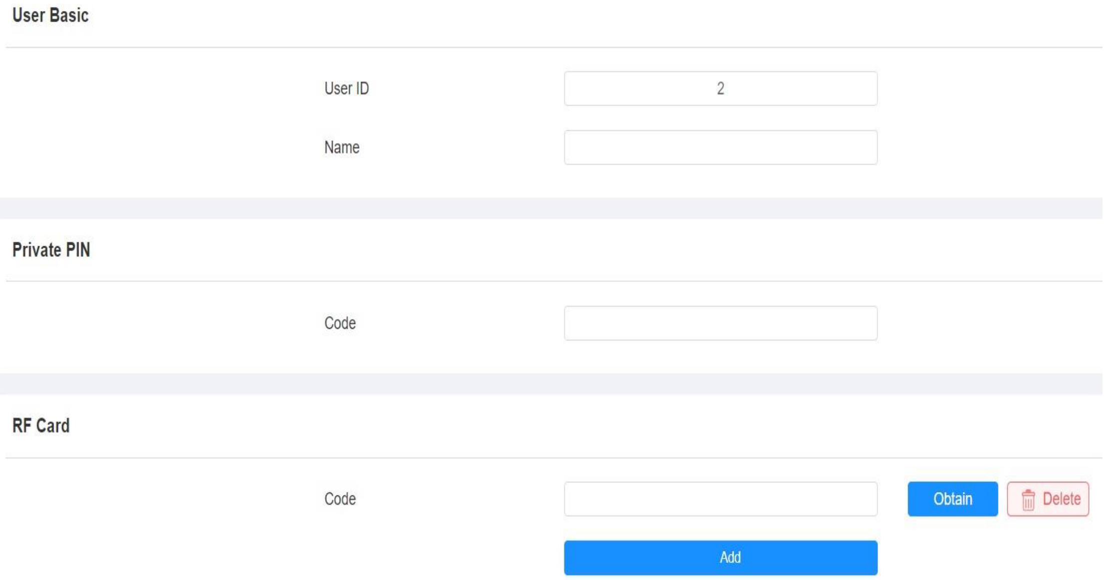
1 item Selected Schedules
□ 1001:Always

Table A25 - MyBell IP Keypad Station - Private PIN configuration	
Setting	**Description**
Allow To Open	Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
Floor NO.	Specify the accessible floor(s) to the user through the elevator.
Web Relay	Specify the ID of web relay action commands that you can configure using the Web Relay interface. A default value of **0** indicates that the web relay isn't triggered.
Schedule	By relocating the desired schedule(s) from the right box to the left one, you grant the user the possibility to open the chosen door during the set periods. Besides custom schedules, there are 2 default options: • **Always** - allows door opening without limitations • **Never** - prohibits door opening **Note** This step applies to door access by RF card and facial recognition as they are identical in configuration.

15.2 - Configuration of RF card for door unlock

To add a RF card:

Directory > User > Add > Place the card on the card reader area and click **Obtain**



User Basic

User ID: 2

Name:

Private PIN

Code:

RF Card

Code:

Setting:

- **Code** - the card ID that the card reader reads

Note

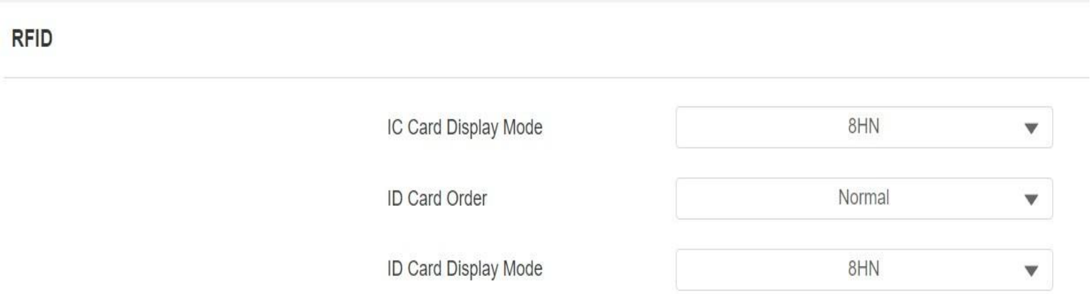
- RF cards with 13.56 MHz and 125 KHz can be applied for the door access.
- Each user can have a maximum of 5 cards added.
- The device allows to add up to 10000 users.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the door phone.
- You can also add admin cards on the device. Press ***2396#** on the keypad. Then, press **2** and **1** to enter the card setting screen where you can add or delete an RF card.

15.3 - Configuration of RF card code format

To integrate the RF card door access with the third-party intercom system, you need to match the RF card code format with the one used by the third-party system.

To configure the RF card code:

Access Control > Card Setting > RFID



RFID

IC Card Display Mode: 8HN

ID Card Order: Normal

ID Card Display Mode: 8HN

Setting:

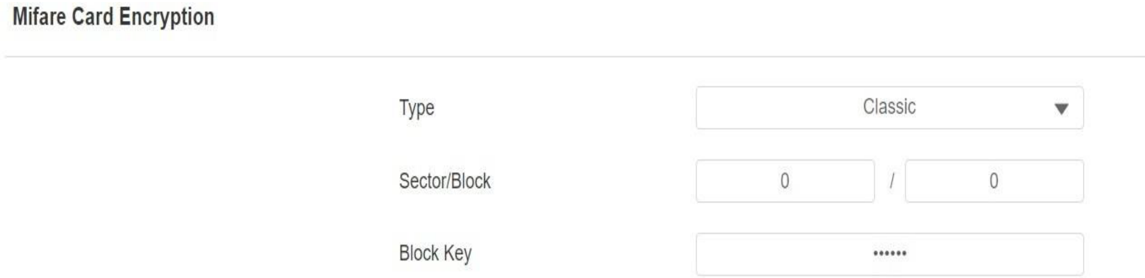
- **IC/ID Card Display Mode** - Set the card number format from available options. The default format in the door phone is **8HN**.
- **ID Card Order -** Select normal or reversed display of ID card number.

15.4 - Mifare card encryption

The door phone can encrypt Mifare cards for greater security. When this feature is enabled, it reads the data in the card designated sectors and blocks.

To configure the Mifare card:

Access Control > Card Setting > Mifare Card Encryption



Mifare Card Encryption

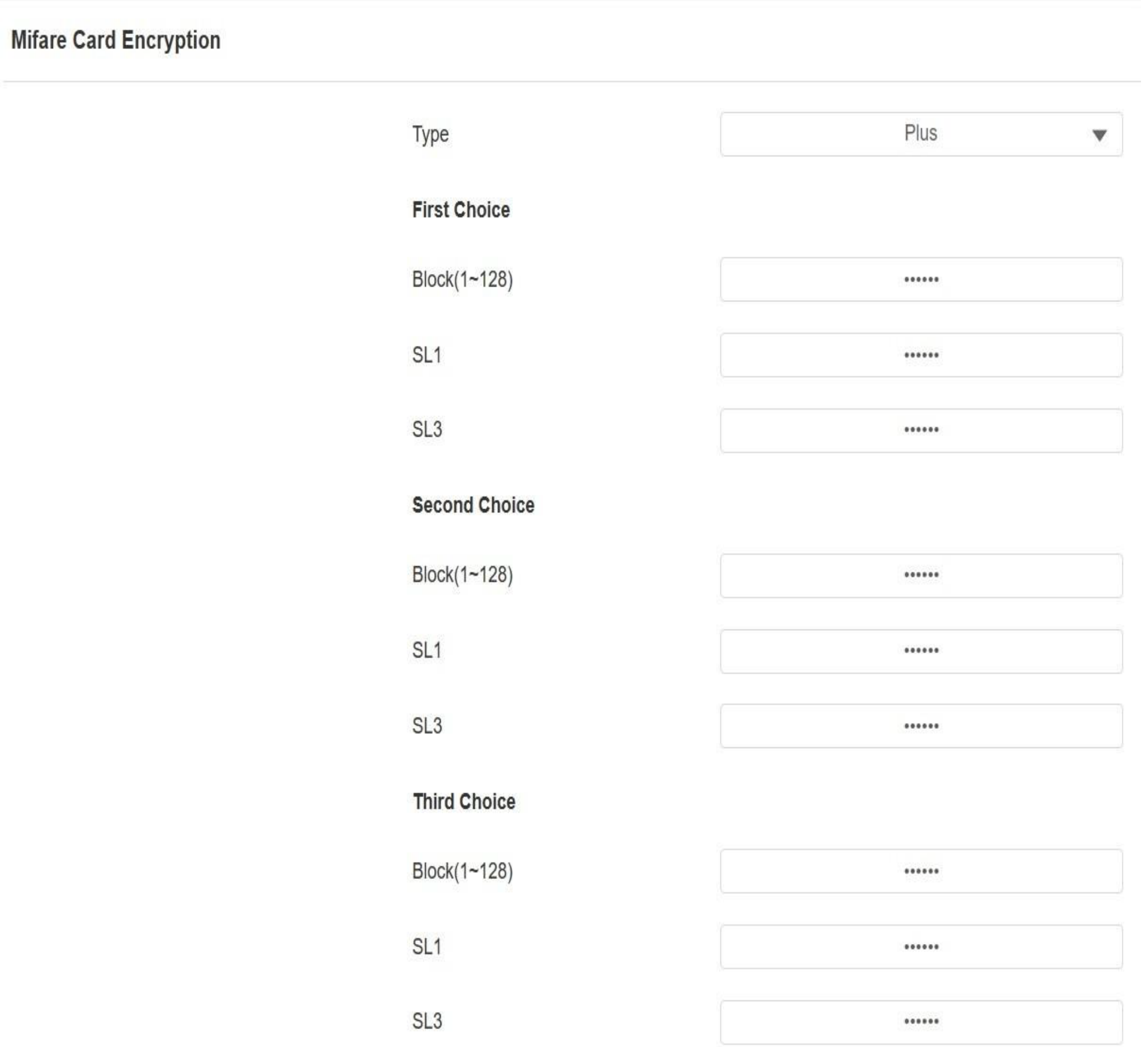
Type	Classic
Sector/Block	0 / 0
Block Key	••••••

Setting:

Type - There are three options, None, Classic , and Plus

If you choose the **Classic** Type, you need to configure the following settings:

- **Sector/Block** - Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
- **Block Key** - Set a password to access the data stored in the predefined sector/block.



Mifare Card Encryption

Type	Plus
First Choice	
Block(1~128)	••••••
SL1	••••••
SL3	••••••
Second Choice	
Block(1~128)	••••••
SL1	••••••
SL3	••••••
Third Choice	
Block(1~128)	••••••
SL1	••••••
SL3	••••••

Setting:

If you choose the **Plus** Type, there are three block choices. The device can read the encrypted data in SL1 and SL3.

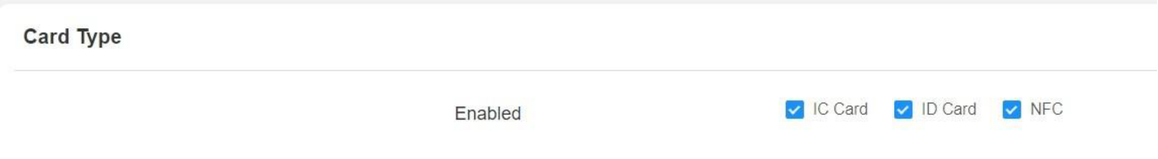
- **Block** - the block number where the encrypted data is located
- **SL1** - the key number within 24 bits
- **SL3** - the key number within 32 bits

15.5 - NFC card configuration

NFC (Near Field Communication) is a way for door access, which uses radio waves for data transmission interaction. The device can be unlocked by NFC. You can put a mobile phone close to the device for door access.

To configure NFC:

Access Control > Card Setting > Card Type



Card Type

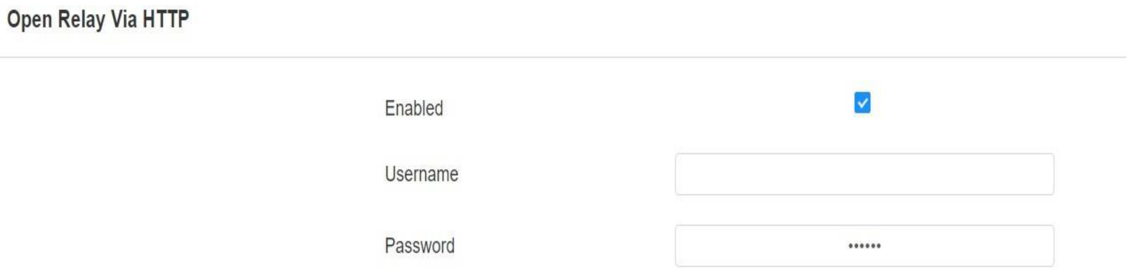
Enabled ☑ IC Card ☑ ID Card ☑ NFC

15.6 - Open relay configuration using HTTP for door unlock

You can unlock the door remotely by typing in the created HTTP command (URL) in the web browser to trigger the relay.

To configure the open relay:

Access Control > Relay > Open Relay Via HTTP



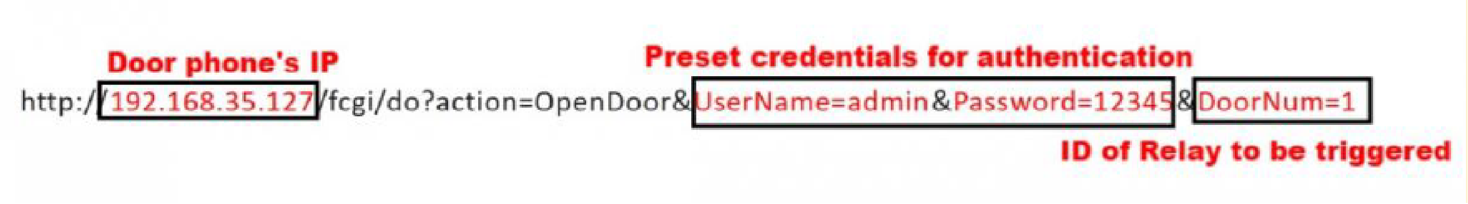
Open Relay Via HTTP

Enabled	☑
Username	
Password	••••••

Setting:

- **Username** - Set a username for authentication in HTTP command URLs.
- **Password** - Set a password for authentication in HTTP command URLs.

Example of HTTP command:



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

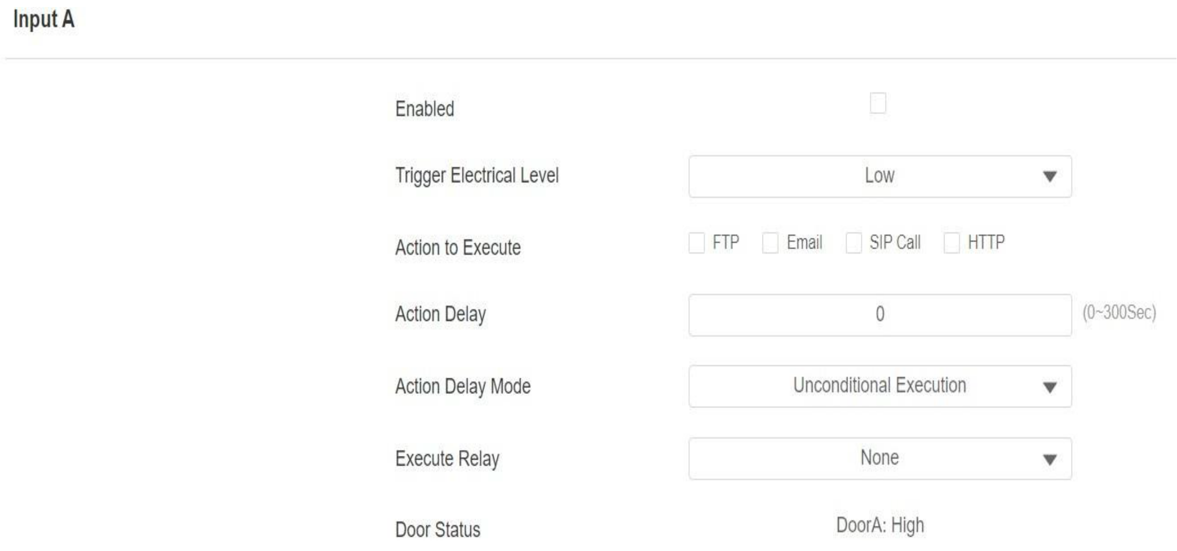
Door phone's IP
Preset credentials for authentication
ID of Relay to be triggered

15.7 - Configuration of exit button for door unlock

When users need to open the door from inside by pressing the exit button, you need to set up the Input terminal that matches the exit button to activate the relay for the door access.

To configure the exit button:

Access Control > Input



Input A

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

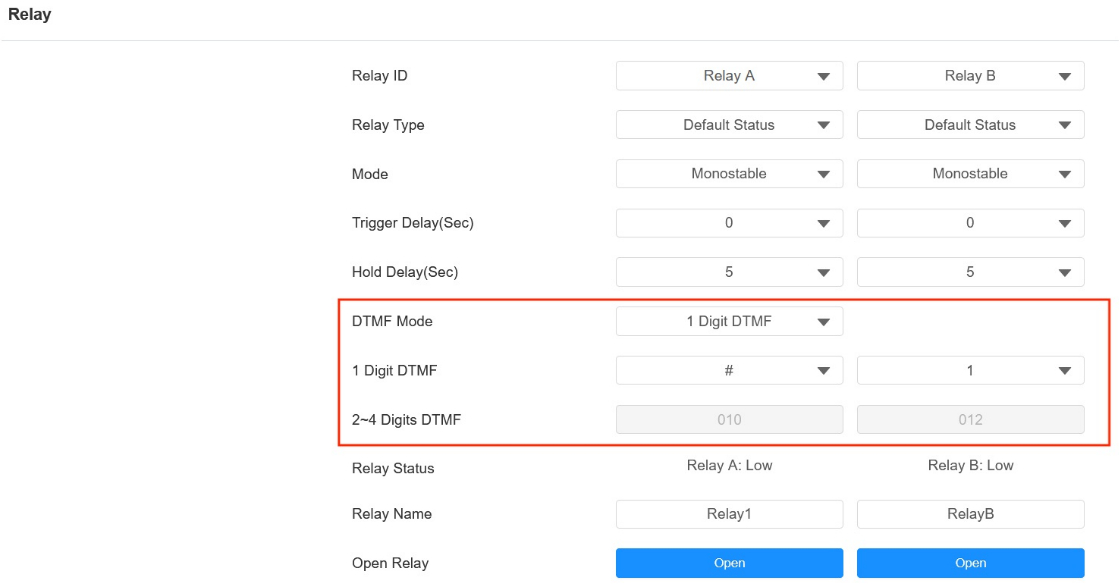
Table A26 - MyBell IP Keypad Station - Configuration of exit button for door unlock	
Setting	**Description**
Enabled	To use a specific input interface
Trigger Electrical Level	Select the **Trigger Electrical Level** option from **High** and **Low**, according to the operation on the exit button.
Action To Execute	Select the method to carry out the action from the following options: • **FTP -** Send a screenshot to the preconfigured FTP server. • **Email** - Send a screenshot to the preconfigured Email address • **SIP Call -** Call the preset number upon the trigger. • **HTTP -** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP and enter the URL.
HTTP URL	Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
Action Delay	Specify whether the relay can be triggered at any time or only within a scheduled period: • **Unconditional Execution** - The action is carried out when the input is triggered. • **Execute If Input Still Triggered -** The action is carried out when the input stays triggered. For example, if the door stays open after triggering input, an email is sent to notify the receiver.
Execute Relay	Set up the relays to be triggered by the actions.

15.8 - Configuration of open relay through DTMF for door unlock

Dual-tone multi-frequency signaling (DTMF) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad, or tapping the unlock tab with the DTMF code on the screen.

To configure the DTMF codes:

Access Control > Relay



Relay

Relay ID	Relay A	Relay B
Relay Type	Default Status	Default Status
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	#	1
2~4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	Relay1	RelayB
Open Relay	Open	Open

Table A27 - MyBell IP Keypad Station - Configuration of open relay through DTMF for door unlock	
Setting	**Description**
DTMF Mode	Set the number of digits for the DTMF code.
1 Digit DTMF	Define the 1-digit DTMF code within the range (0-9 and *,#) when the DTMF Mode is set to 1-digit.
2-4 Digit DTMF	Set the DTMF code based on the number of digits selected in the DTMF Mode.

Note

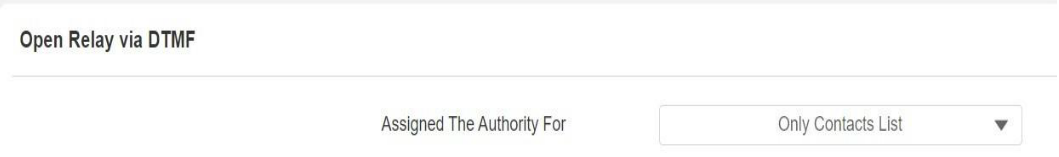
To open the door with DTMF, the intercom devices that send and receive the unlock command need to use the same mode and code. Otherwise, the DTMF unlock can fail.

15.9 - DTMF whitelist

Dual-tone multi-frequency signaling (DTMF) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad, or tapping the unlock tab with the DTMF code on the screen.

To configure the DTMF codes:

Access Control > Relay > Open Relay via DTMF



Open Relay via DTMF

Assigned The Authority For: Only Contacts List ▼

Setting:

Assigned The Authority For - specify the contacts authorized to open doors using DTMF:

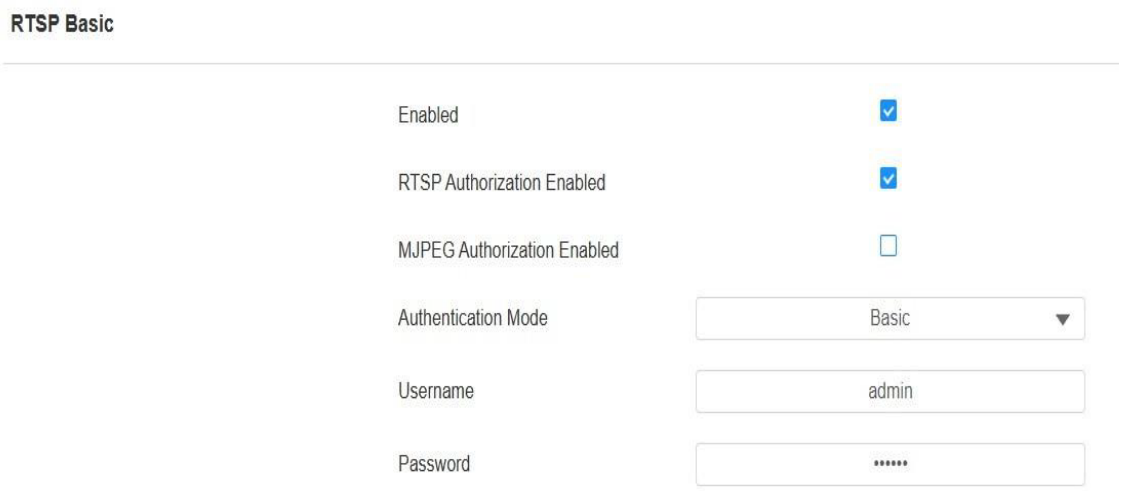
- **None** - No numbers can unlock doors using DTMF.
- Only Contacts List - Only numbers added to the door phone contact list can unlock using DTMF
- All Numbers - Any numbers can unlock using DTMF.

16.1 - RTSP Stream Monitoring

RTSP (Real Time Streaming Protocol) can be used to stream video and audio from the third-party cameras to the device. You can add a camera stream by adding its URL.

To configure the RTSP stream:

Surveillance > RTSP > RTSP Basic



RTSP Basic

Enabled ☑

RTSP Authorization Enabled ☑

MJPEG Authorization Enabled □

Authentication Mode: Basic

Username: admin

Password: ••••••

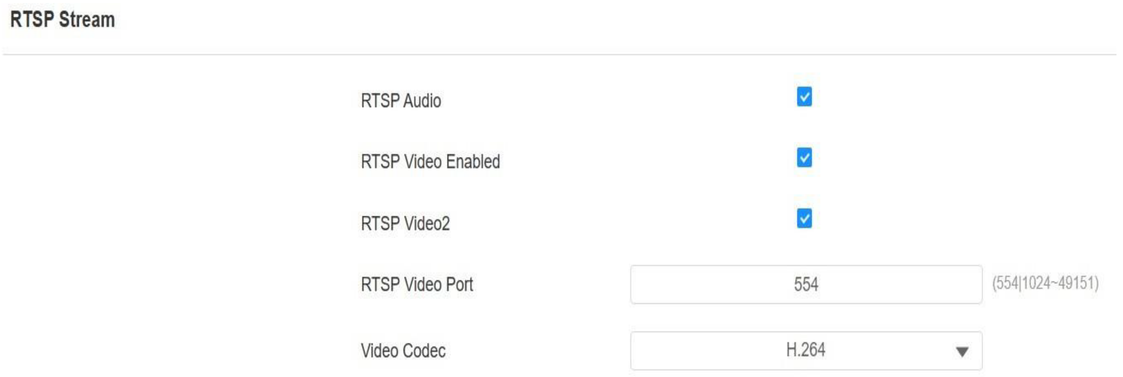
Table A28 - MyBell IP Keypad Station - Configuration of RTSP	
Setting	**Description**
RTSP Authorization Enabled	If enabled, you need to configure RTSP Authentication Mode, RTSP Username, and Password for authorization.
Authentication Mode	Choose one of the two options: **Basic** (default) or **Digest.**
Username	Set the username for authentication.
Password	Set the password for authentication.

16.1.1 - RTSP Stream Setting

The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

To configure the RTSP:

Surveillance > RTSP > RTSP Stream



RTSP Stream

RTSP Audio ☑

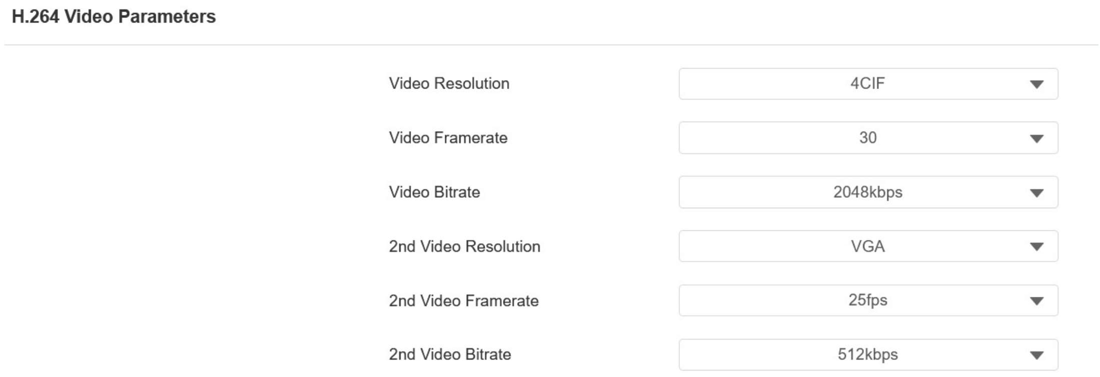
RTSP Video Enabled ☑

RTSP Video2 ☑

RTSP Video Port: 554 (554|1024~49151)

Video Codec: H.264

Table A29 - MyBell IP Keypad Station - Configuration of RTSP stream	
Setting	**Description**
RTSP Audio	Allows the door phone to send audio information to the monitor by RTSP
RTSP Video Enabled	The door phone can send the video information to the monitor. After enabling the RTSP feature, the video RTSP is enabled by default and can't be modified.
RTSP Video 2	Two RTSP streams are supported. Tick this box to enable the second one.
RTSP Video Port	Choose a suitable audio codec for RTSP audio.
Video Codec	Choose a suitable video codec for RTSP video.



H.264 Video Parameters

Video Resolution: 4CIF

Video Framerate: 30

Video Bitrate: 2048kbps

2nd Video Resolution: VGA

2nd Video Framerate: 25fps

2nd Video Bitrate: 512kbps

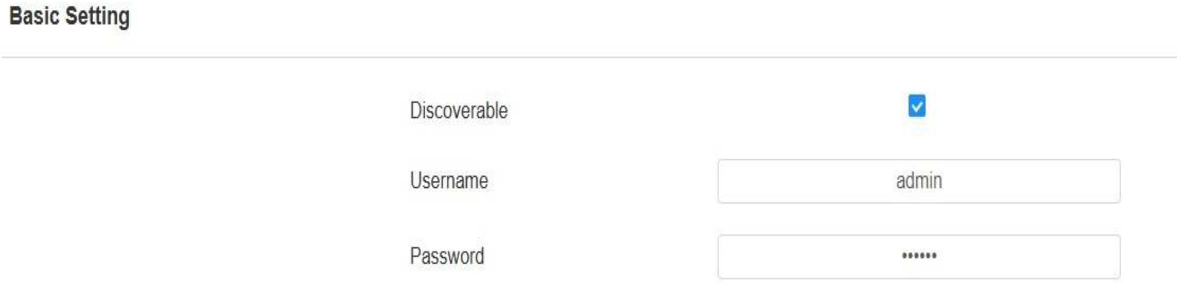
Table A30 - MyBell IP Keypad Station - Configuration of H.264 Video Parameters	
Setting	**Description**
Video Resolution	There are the following options, **QVGA, CIF, VGA, 4CIF, 720P,** and **1080P.** The default video resolution is **720P.** The video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than 720P.
Video Framerate	30 fps is the video frame rate by default.
Video Bitrate	There are the following options, **128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps,** and **4096 kbps**. Select it according to the network environment. The default video bitrate is **2048 kbps.**
2nd Video Resolution	The video resolution for the second video stream channel. The default video solution is **VGA.**
2nd Video Framerate	The video framerate for the second video stream channel. 25 fps is by default for the second video stream channel.
2nd Video Bitrat	There are the following options: **128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps**, and **4096 kbps** for the second video stream channel. The second video stream channel is **512 kbps** by default.

16.2 - ONVIF

ONVIF (Open Network Video Interface Forum) enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format. When ONVIF is enabled the device makes its video available to be visible on other divices.

To configure ONVIF:

Surveillance > ONVIF > Basic Setting



Basic Setting

Discoverable: ☑

Username: admin

Password: ••••••

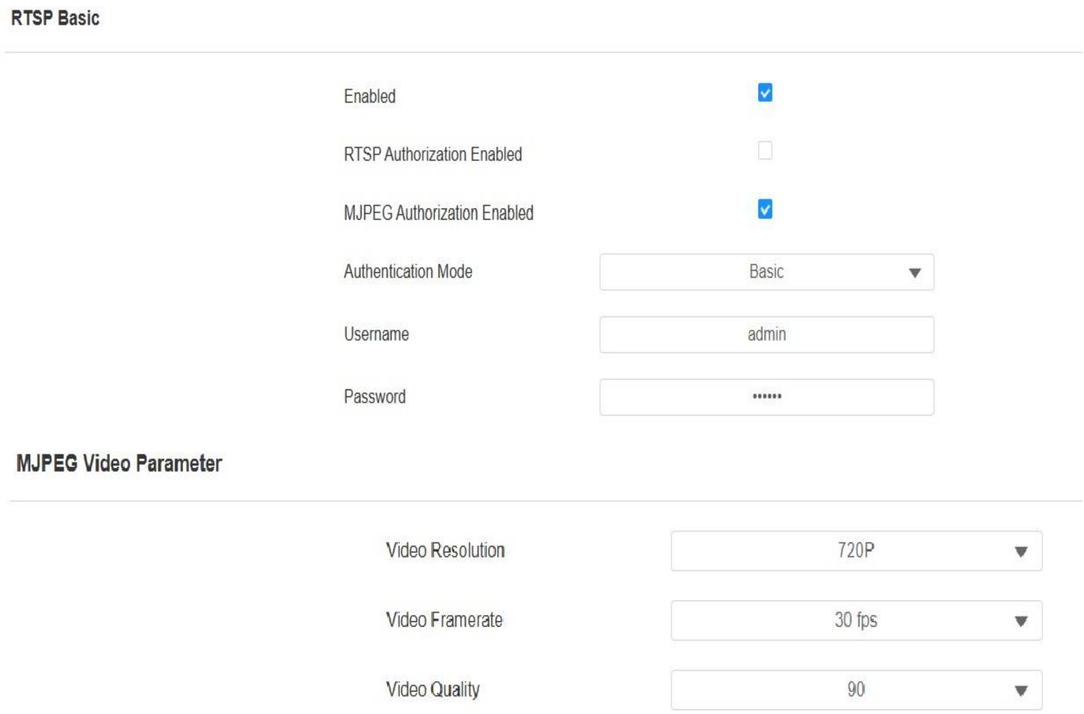
Table A31 - MyBell IP Keypad Station - Configuration of RTSP	
Setting	**Description**
Discoverable	If enabled, the video from the door phone camera can be searched by other devices.
Username	Set the username for authentication. The default username is **admin**.
Password	Set the password for authentication. The default password is **admin**.

16.3 - MJPEG image capturing

Motion JPEG (MJPEG) is a video compression format that uses JPEG images for each video frame. MyBell devices display live streams using the web interface and capture monitoring screenshots in MJPEG format. Settings related to MJPEG determine video quality and the on/off status of the live stream function.

To enable MJPEG image capturing:

Surveillance > RTSP > RTSP Setting



RTSP Basic

Enabled ☑

RTSP Authorization Enabled □

MJPEG Authorization Enabled ☑

Authentication Mode: Basic

Username: admin

Password: ••••••

MJPEG Video Parameter

Video Resolution: 720P

Video Framerate: 30 fps

Video Quality: 90

Table A32 - MyBell IP Keypad Station - MJPEG image capturing configuration	
Setting	**Description**
MJPEG Authorization Enabled	If enabled, configure the Authentication Mode, RTSP Username, and Password for authorization.
Username	Set the username for authentication.
Password	Set the password for authentication.
Authentication Mode	Choose one of the two options: **Basic** (default) or **Digest.**
Video Resolution	There are the following options, **QVGA, CIF, VGA, 4CIF, 720P,** and **1080P.** The default video resolution is **720P.** The video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than 720P.
Video Framerate	There are three options, 10 fps, 15 fps, and 30 fps. 30 fps is the default video frame rate.
Video Quality	It ranges from 50 to 90.

You can capture the image from the door phone using the following three types of URL formats:

- http:// deviceip:8080/picture.cgi
- http://deviceip:8080/picture.jpg
- http://deviceip:8080/jpeg.cgi

16.4 - Live stream

You can check the real-time video using the device web interface or entering the URL in the web browser to access the video.

To view the real-time video:

Surveillance > Live Stream

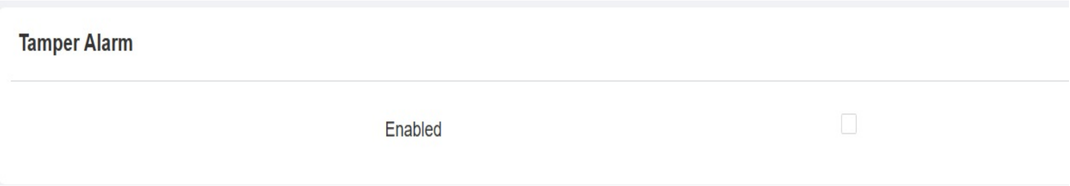
17 SECURITY

17.1 - 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:

System > Security > Tamper Alarm



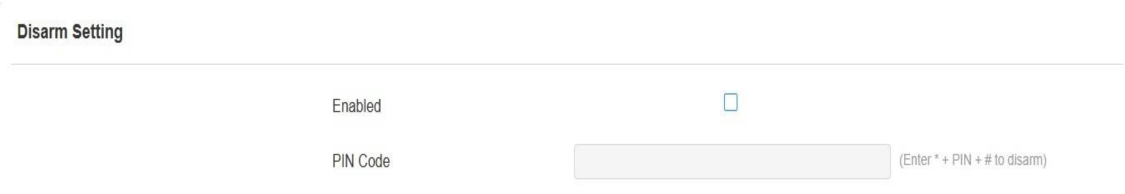
Tamper Alarm

Enabled □

17.2 - Disarm Setting

To set the disarm code by the web interface:

System > Security > Disarm Setting



Disarm Setting

Enabled □

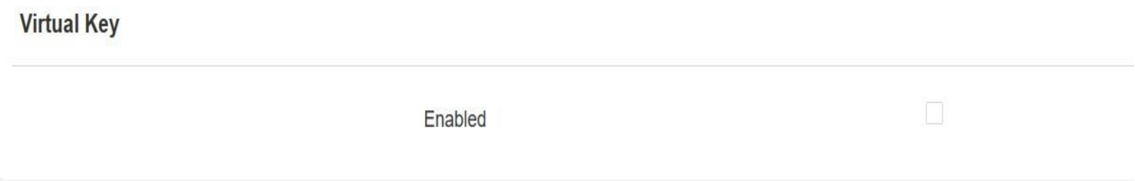
PIN Code (Enter * + PIN + # to disarm)

17.3 - Virtual PIN

The virtual PIN enables you to protect your PIN code from being discoved by the third parties.

To configure the virtual PIN:

Access Control > PIN Setting > Virtual Key



Virtual Key

Enabled □

If **enabled**, you can put fake numbers on both sides of the PIN code for PIN code protection. For example, if your password is 1234567 you can put 99 and 88 on both sides (99123456788). The virtual password is matched to the users by the number of matched digits. If user A has a greater number of digits that are matched with the virtual password entered than user B, then it is regarded as user A's password. However, when the double authentication is applied, then the virtual password is matched with the users who pass the first level of authentication, for example, Face + PIN.

Note

This feature isn't used for Public PIN and Apartment+PIN.

17.4 - Client certificate configuration

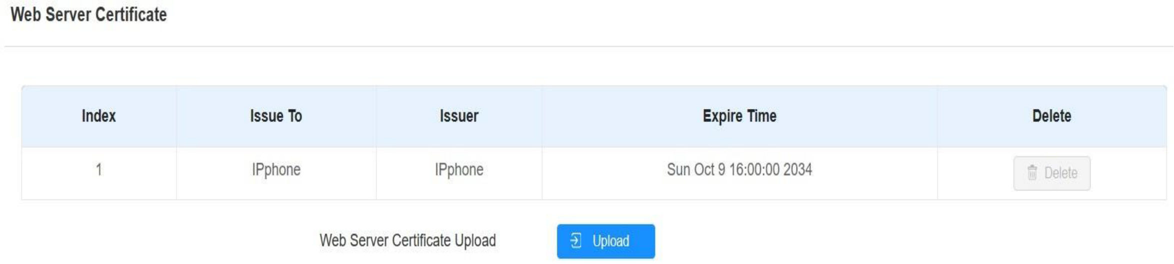
Certificates can ensure communication integrity and privacy when deploying the door phones. When the user needs to establish the SSL protocol, it is necessary to upload corresponding certificates for verification.

17.4.1 - Web Server certificate

This certificate is sent to the client for authentication when the client requires an SSL connection with the door phone. Please upload the certificates in accepted formats.

To upload the Web Server certificate by the web interface:

System > Certificate > Web Server Certificate



Web Server Certificate

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

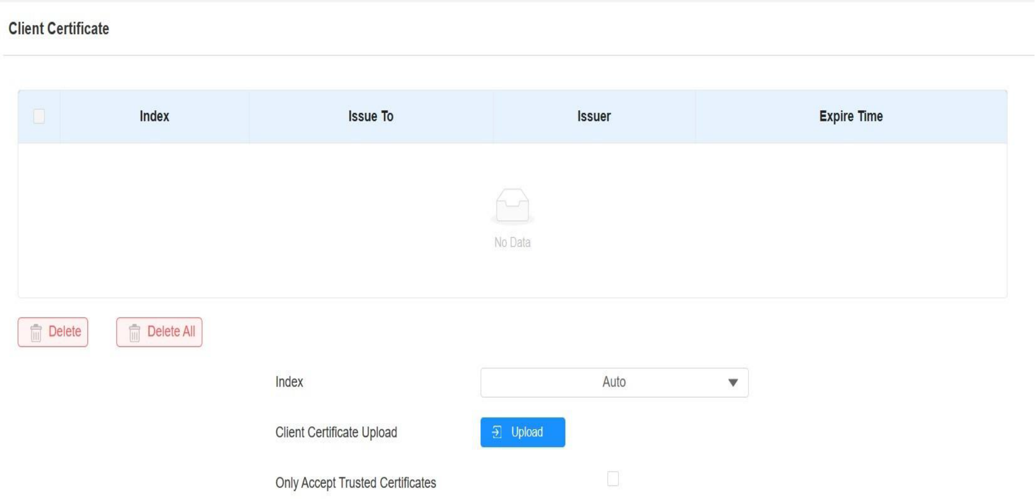
Web Server Certificate Upload

17.4.2 - 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 the client certificates by the web interface:

System > Certificate > Client Certificate



Client Certificate

□	Index	Issue To	Issuer	Expire Time

No Data

Index: Auto

Client Certificate Upload: Upload

Only Accept Trusted Certificates: □

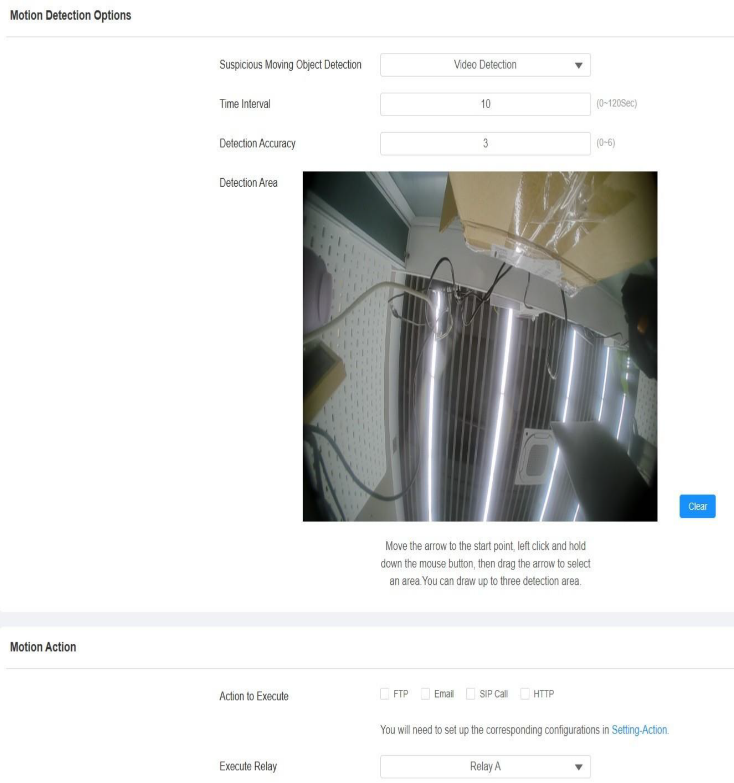
Table A33 - MyBell IP Keypad Station - Client certificate configuration	
Setting	**Description**
Index	Select the desired value from the drop-down Index list: • **Auto value** – the uploaded certificate is displayed in numeric order. • **Value from 1 to 10** – the uploaded certificate is displayed according to the seleced value.
Select File	Click **Choose file** to browse the local drive, and locate the desired certificate (**.pem** files only).
Only Accept Trusted Certificates	• **Enabled** – if the authentication is successful, the phone verifies the server certificate based on the client certificate list. • **Disabled** – the phone doesn't verify the server certificate, whether the certificate is valid or not.

17.5 - Motion detection

Motion detection is commonly used for unattended surveillance video and alarms. Images collected by the camera at different frame rates are compared 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.

To configure motion detection:

Surveillance > Motion > Motion Detection Options



Motion Detection Options

Suspicious Moving Object Detection: Video Detection

Time Interval: 10 (0~120Sec)

Detection Accuracy: 3 (0~6)

Detection Area

Move the arrow to the start point, left click and hold down the mouse button, then drag the arrow to select an area.You can draw up to three detection area.

Motion Action

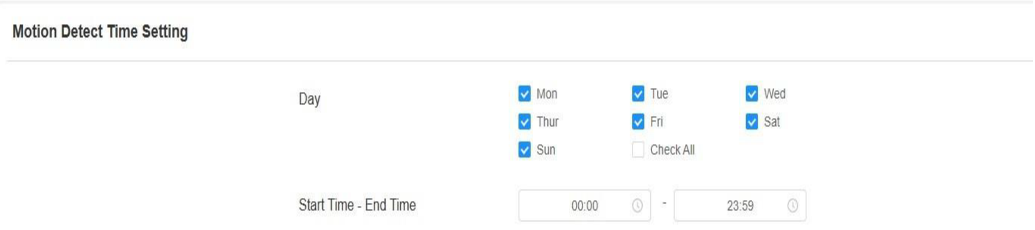
Action to Execute: □ FTP □ Email □ SIP Call □ HTTP

You will need to set up the corresponding configurations in Setting-Action.

Execute Relay: Relay A

Table A34 - MyBell IP Keypad Station - Motion detection configuration	
Setting	**Description**
Suspicious Moving Object Detection	Select from the following options: • **Disabled** • **Video Detection** – focuses on analyzing visual information captured through cameras • **Radar Detection** – offers longer-ranged and better detection in poor visibility conditions • **Video + Radar**
Detection Range	If radar detection is enabled, you can select the detection range: 1, 2, or 3 meters.
Time Interval	The absolute triggering interval is 3 seconds. if you select 3 seconds, then the alarm is triggered when a moving object is detected once within 3 seconds. If you select a number greater than 3 seconds, then it requires a second triggering interval to trigger the alarm. For example, if you select 5 seconds, the alarm isn't triggered until a moving object is detected for the second time within 3 to 5 seconds. The default interval is 10 seconds.
Detection Accuracy	The higher the value, the greater the sensitivity. The default detection accuracy value is 3.
Detection Area	Click and hold the mouse button to select up to three detection areas.
Action to Execute	The notification types include: • **FTP -** the notification is sent to the designated server • **Email** - the email is sent to the pre-configured email address • **SIP Call -** a call is made to the pre-configured number • **HTTP -** the notification is sent to the designated server
Execute Relay	The relay to be triggered

Scroll down to set the motion detection schedule:



Motion Detect Time Setting

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

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

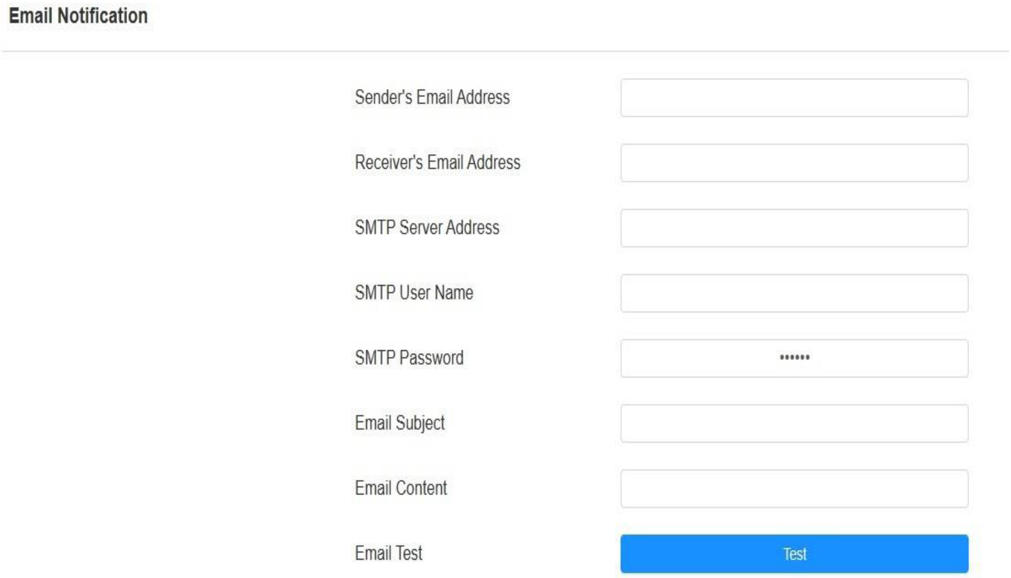
17.6 - Security Notification Setting

A security notification informs users or security personnel of any breach or threat that the door phone detects. If the door phone detects something unusual, the system sends a notification to users or security through email, phone call, or other methods.

17.6.1 - Email Notification Setting

To configure email notification with screenshots of unusual motion from the door phone:

Setting > Action > Email Notification



Email Notification

Sender's Email Address

Receiver's Email Address

SMTP Server Address

SMTP User Name

SMTP Password ••••••

Email Subject

Email Content

Email Test [Test]

Setting:

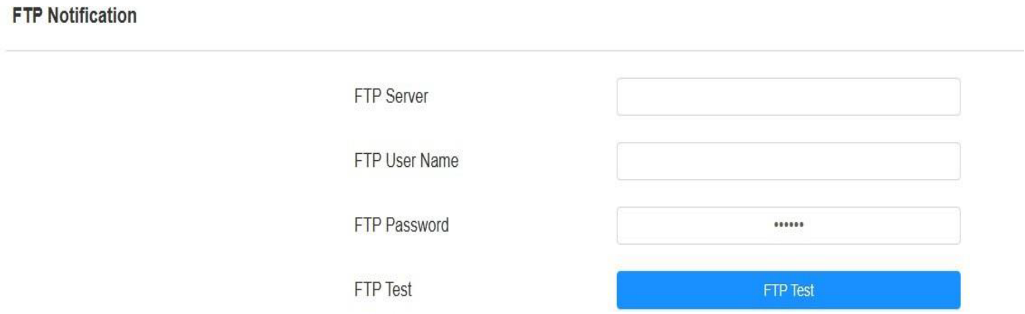
- **SMTP User Name** - usually the same as the sender’s email address
- **SMTP Password** - the same as the sender’s email address

17.6.2 - FTP notification configuration

You can receive the security notifications through FTP server. The door phone uploads a screenshot to the specified FTP folder if it senses any unusual motion.

To configure the FTP notifications by the web interface:

Setting > Action > FTP Notification



FTP Notification

FTP Server

FTP User Name

FTP Password ••••••

FTP Test [FTP Test]

Setting:

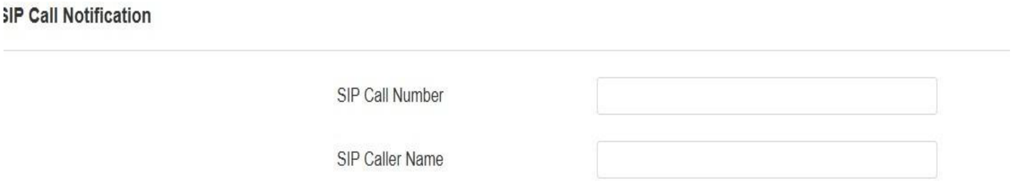
- **FTP Path** - the folder name you created in the FTP server

17.6.3 - SIP call notification configuration

You can enter the SIP number to receive the notification.

To configure the SIP call notifications by the web interface:

Setting > Action > SIP Call Notification



SIP Call Notification

SIP Call Number

SIP Caller Name

17.6.4 - Action URL

You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions is triggered when the relay status, input status, PIN code, or RF card access changes.

Table A35 - MyBell IP Keypad Station - URL actions

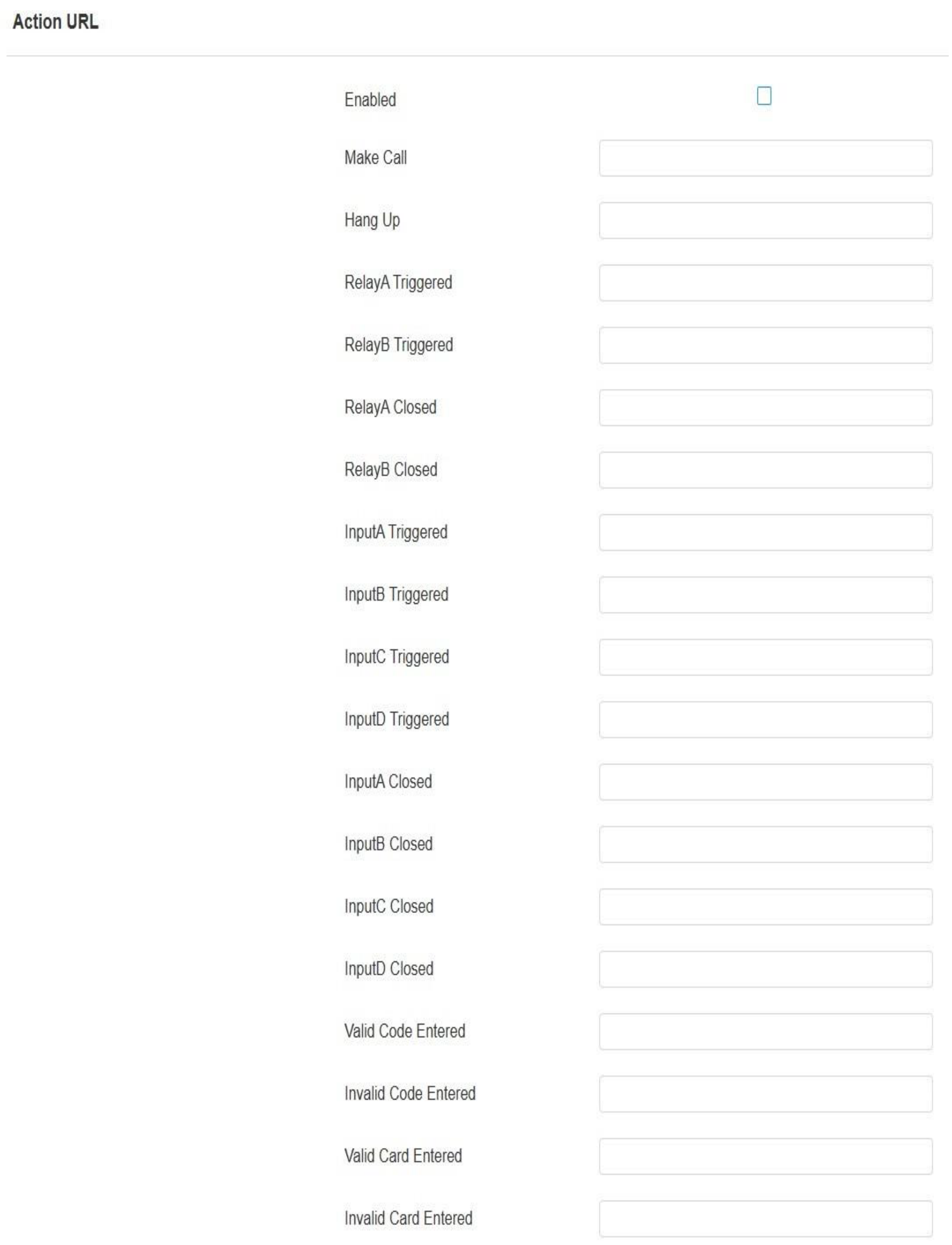
No.	Event	Parameter format	Example
1	**Make Call**	$remote	http://server ip/callnumber=$remote
2	**Hang Up**	$remote	http://server ip/callnumber=$remote
3	**Relay triggered**	$relay1status	http://server ip/relaytrigger=$relay1status
4	**Relay Closed**	$relay1status	http://server ip/ relayclose=$relay1status
5	**Input Triggered**	$input1status	http://server ip/ inputtrigger=$input1status
6	**Input Closed**	$input1status	http://server ip/ inputclose=$input1status
7	**Valid Code Entered**	$code	http://server ip/ validcode=$code
8	**Invalid Code Entered**	$code	http://server ip/ invalidcode=$code
9	**Valid Card Entered**	$card_sn	Http://server ip/ validcard=$card_sn
10	**Invalid Card Entered**	$card_sn	http://server ip/ invalidcard=$card_sn
11	**Tamper Alarm Triggered**	$alarm status	Http://server ip/tampertrigger=$alarm status

Example:

http://192.168.16.118/help.xml? mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

To configure the SIP call notifications by the web interface:

Setting > Action > Action URL



Action URL

Enabled □

Make Call

Hang Up

RelayA Triggered

RelayB Triggered

RelayA Closed

RelayB Closed

InputA Triggered

InputB Triggered

InputC Triggered

InputD Triggered

InputA Closed

InputB Closed

InputC Closed

InputD Closed

Valid Code Entered

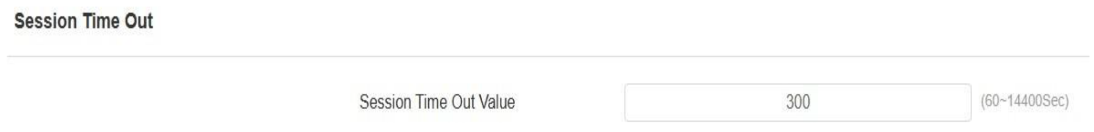
Invalid Code Entered

Valid Card Entered

Invalid Card Entered

17.7 - Web interface automatic log-out

You can set up the web interface automatic log-out timing, requiring re-login by entering the user name and the passwords.
To configure the web interface automatic log-out timing:
System > Security > Session Time Out



Session Time Out

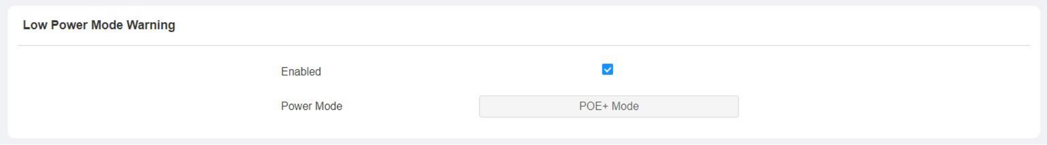
Session Time Out Value: 300 (60~14400Sec)

Setting:

- **Session Time Out Value** - The automatic web interface log-out time ranges from 60 seconds to 14400 seconds. The default value is 300.

17.8 - Low power mode

It displays the device power mode. When the device is powered by POE, it displays POE+Mode. When it's powered by the 12-volt power supply, it displays Low Power Mode.
To see the power mode:
System > Security > Low Power Mode Warning



Low Power Mode Warning

Enabled ☑

Power Mode: POE+ Mode

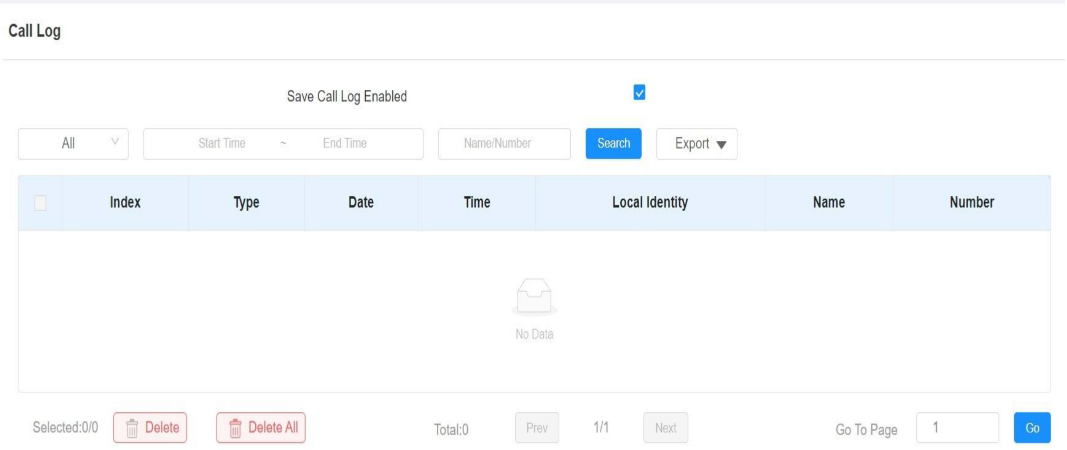
18 LOGS

18.1 - Call logs

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

To check the call logs by the web interface:

Status > Call Log



Call Log

Save Call Log Enabled ☑

☐	Index	Type	Date	Time	Local Identity	Name	Number

No Data

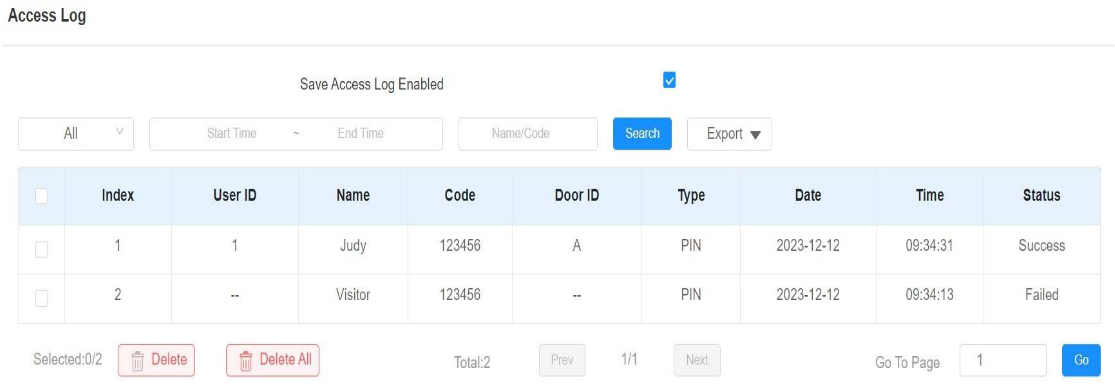
Selected:0/0 | Delete | Delete All | Total:0 | Prev | 1/1 | Next | Go To Page | 1 | Go

Table A36 - MyBell IP Keypad Station - Call logs configuaration	
Setting	**Description**
All	Four types of call history are available: **All, Dialed, Received**, and **Missed**
Start Time - End Time	The specific time of the call logs you want to search, check, or export
Name/ Number	Search the call log by the name or by the SIP or IP number.
Export	Call logs can be exported in **.csv** format.

18.2 - Door access logs

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

Status > Access Log



Access Log

Save Access Log Enabled ☑

☐	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status
☐	1	1	Judy	123456	A	PIN	2023-12-12	09:34:31	Success
☐	2	--	Visitor	123456	--	PIN	2023-12-12	09:34:13	Failed

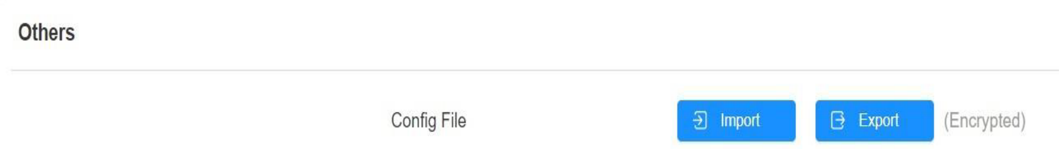
Selected:0/2 | Delete | Delete All | Total:2 | Prev | 1/1 | Next | Go To Page | 1 | Go

Table A37 - MyBell IP Keypad Station - Access logs configuration	
Setting	**Description**
All	Three types of access logs are available, **All, Success**, and **Failed.**
Start Time - End Time	The specific time of the access logs you want to search, check, or export
Name/ Number	Search the access log by the name or by the SIP or IP number.
Export	Access logs can be exported in **.csv** format.

19 BACKUP

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

System > Maintenance > Others



Others

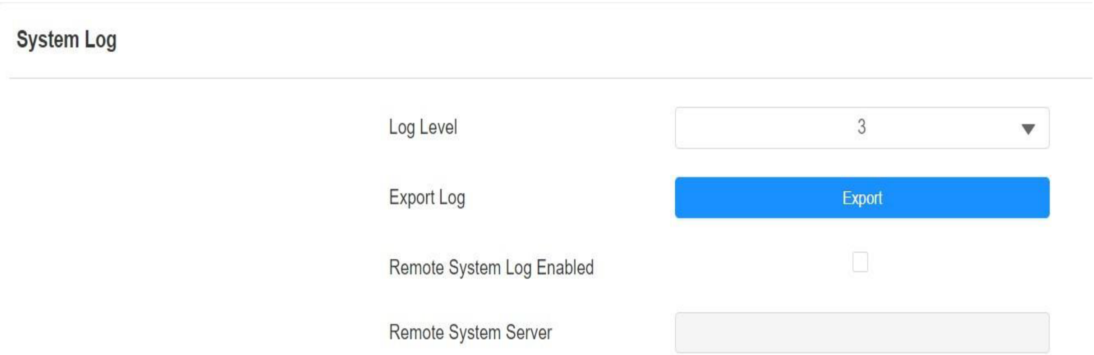
Config File

(Encrypted)

20 DEBUG

20.1 - 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:
System > Maintenance > System Log



System Log

Log Level: 3

Export Log: Export

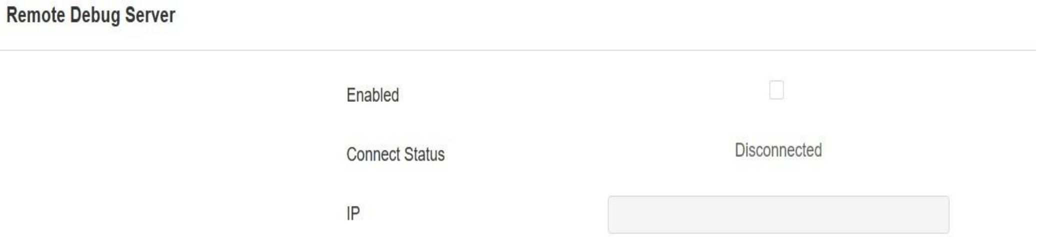
Remote System Log Enabled: □

Remote System Server:

Table A38 - MyBell IP Keypad Station - 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.
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 - Remote debug server

When the device has a problem, you can use the remote debug server to access the device log.
To access the log remotely:
System > Maintenance > Remote Debug Server



Remote Debug Server

Enabled: □

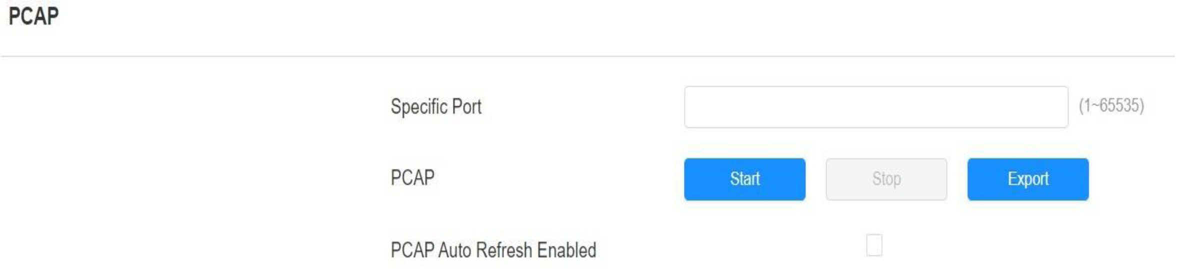
Connect Status: Disconnected

IP:

Setting:
- **IP** - The remote debug server IP

20.3 - PCAP for debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.
To configure PCAP:
System > Maintenance > PCAP



PCAP

Specific Port: (1~65535)

PCAP: Start | Stop | Export

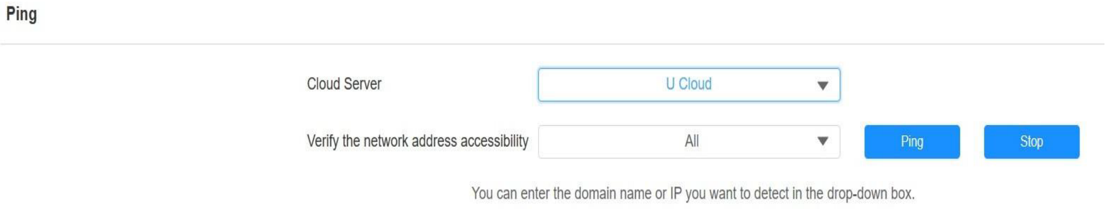
PCAP Auto Refresh Enabled: □

Table A39 - MyBell IP Keypad 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.

20.4 - Ping

To verify the accessibility of the target server:

System > Maintenance > Ping



Cloud Server: U Cloud

Verify the network address accessibility: All

You can enter the domain name or IP you want to detect in the drop-down box.

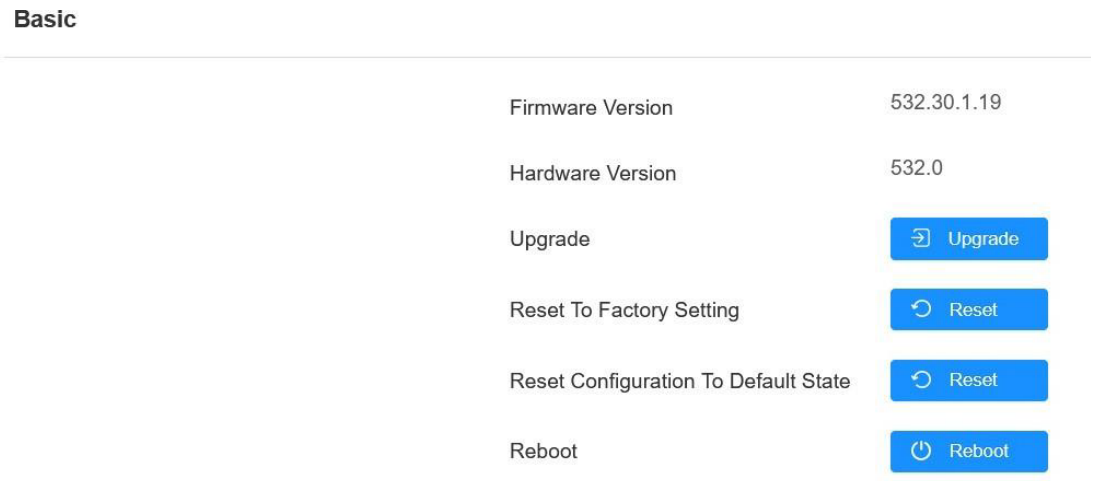
Setting:

- **Cloud Server** - the server to be verified
- **Verify the network address accessibility** - the service type

21 FIRMWARE UPGRADE

To upgrade the devices by the web interface:

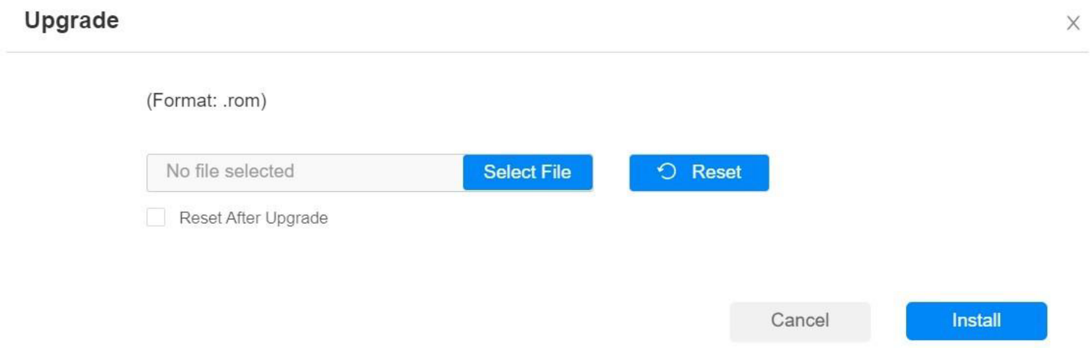
System > Upgrade > Basic



Basic

Firmware Version 532.30.1.19

Hardware Version 532.0



Upgrade

(Format: .rom)

No file selected

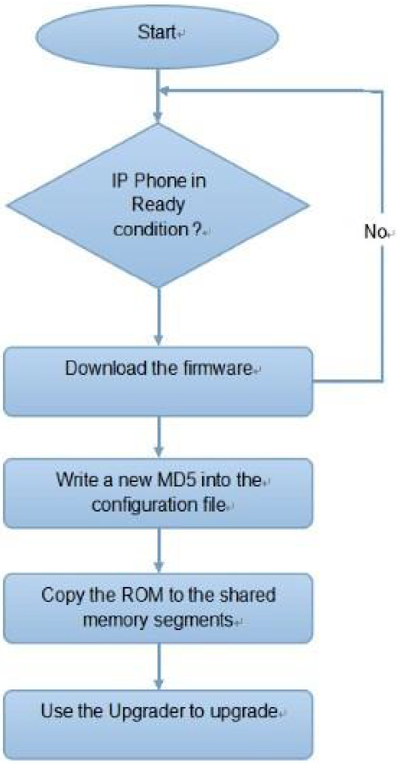
Note

Firmware files should be in **.rom** format for upgrade.

22 AUTO-PROVISIONING THROUGH CONFIGURATION FILE

22.1 - 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 devices to access the URL address of the third-party server which stores configuration files and firmware used to update the firmware and the corresponding settings on the device.
See the flow chart below:


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

22.2 - 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.
- **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 before being downloaded for provisioning on the specific device.

Note

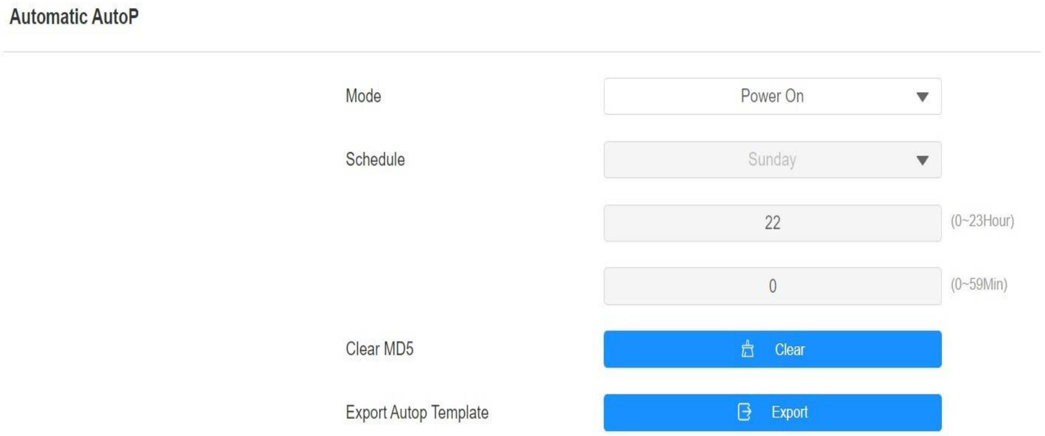
- The configuration file should be in **.cfg** format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has two types of configuration files, then IP devices first access the general configuration files before accessing the MAC-based configuration files.

22.3 - AutoP schedule

The device provides you with AutoP methods that enable the device to perform provisioning at a specific time according to your schedule.

To set up the schedule by the device web interface:

System > Auto Provisioning > Automatic AutoP



Automatic AutoP

Mode: Power On ▼

Schedule: Sunday ▼

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

Table A40 - MyBell IP Keypad Station - Autop configuration	
Setting	**Description**
Mode	• **Power On** - The device performs Autop every time it boots up. • **Repeatedly** - The device performs Autop according to the schedule. • **Power On + Repeatedly** - Combine Power On and Repeatedly modes. The device to perform Autop every time it boots up or according to the schedule. • **Hourly Repeat -** The device performs Autop every hour.
Schedule	When **Power On + Repeatedly** mode is selected, you can select the specific day and time for the Autop.
Clear MD 5	Enables comparison of the existing autop file with the autop file in the server. If the files are the same, the provisioning is stopped, thus avoiding unnecessary auto-provisioning.

22.4 - Static provisioning configuration

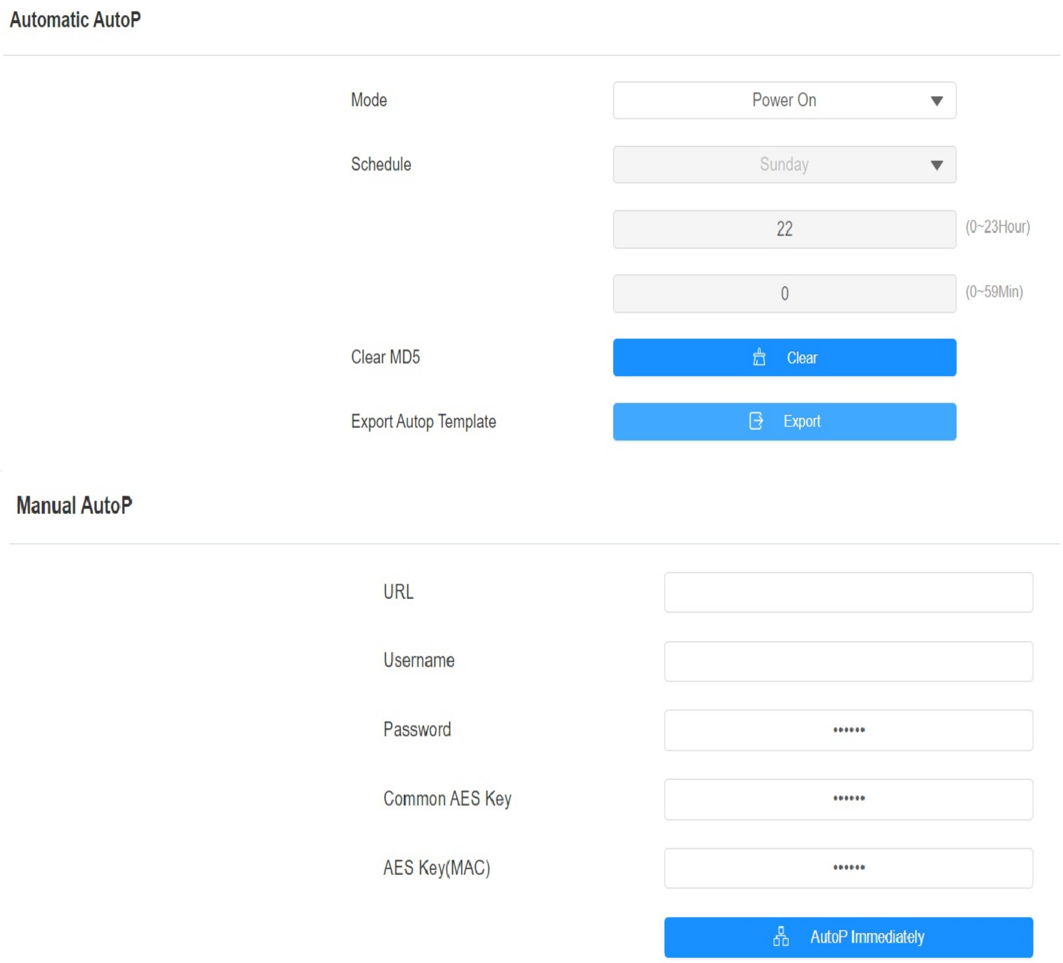
You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the device performs the auto-provisioning at a specific time according to the autop schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS protocols can be used for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

To download the AutoP template:

System > Auto Provisioning > Automatic AutoP

To set up the AutoP server:

System > Auto Provisioning > Manual AutoP



Automatic AutoP

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

Manual AutoP

URL:

Username:

Password: ••••••

Common AES Key: ••••••

AES Key(MAC): ••••••

AutoP Immediately

Table A41 - MyBell IP Keypad Station - Static provisioning configuration	
Setting	**Description**
URL	The TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
Username	Set up a username if it's required to acces the server, otherwise leave it blank.
Password	Set up a password if it's required to acces the server, otherwise leave it blank.
Common AES Key	Set up AES code for the intercom to decipher the general auto-provisioning configuration file.
AES Key (MAC)	Set up AES code for the intercom to decipher the MAC-based auto-provisioning configuration file.

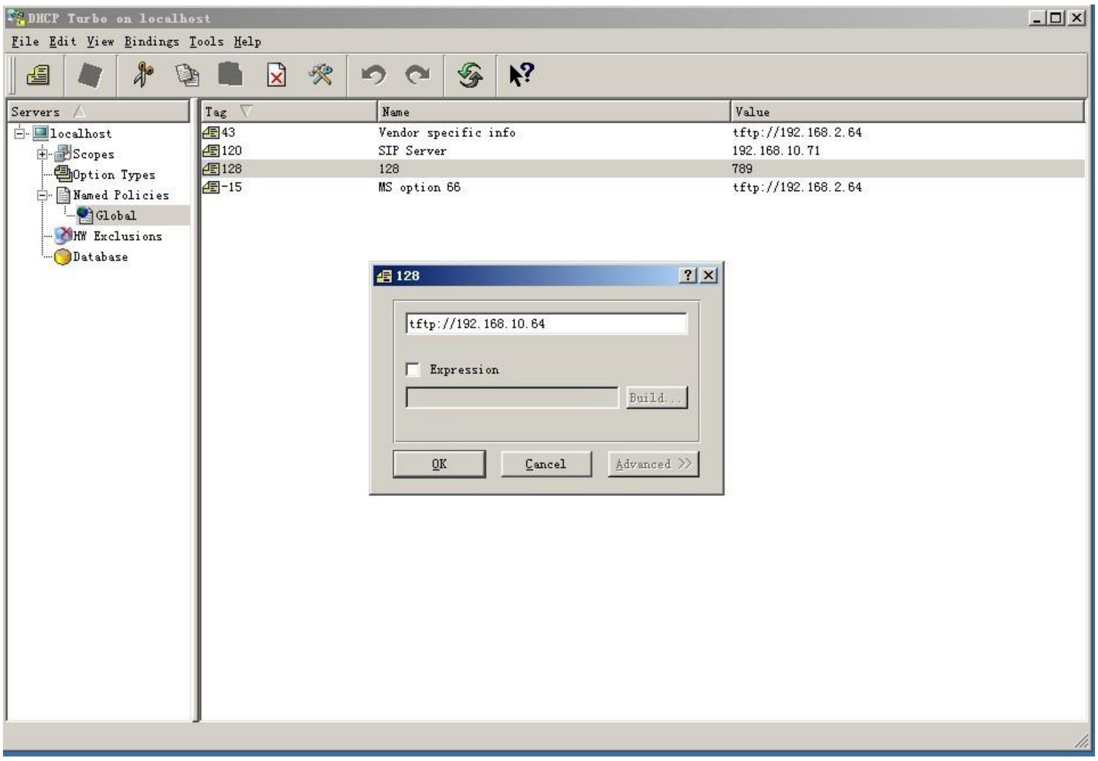
Note

- AES encryption should be configured only when the config file is encrypted with AES.
- 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 manufacturer does't provide user with a specified server. Please prepare the TFTP/FTP/HTTP/HTTPS servers by yourself.

22.5 - 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 to 255), you need to configure DHCP Custom Option by the web interface.



Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

128

tftp://192.168.10.64

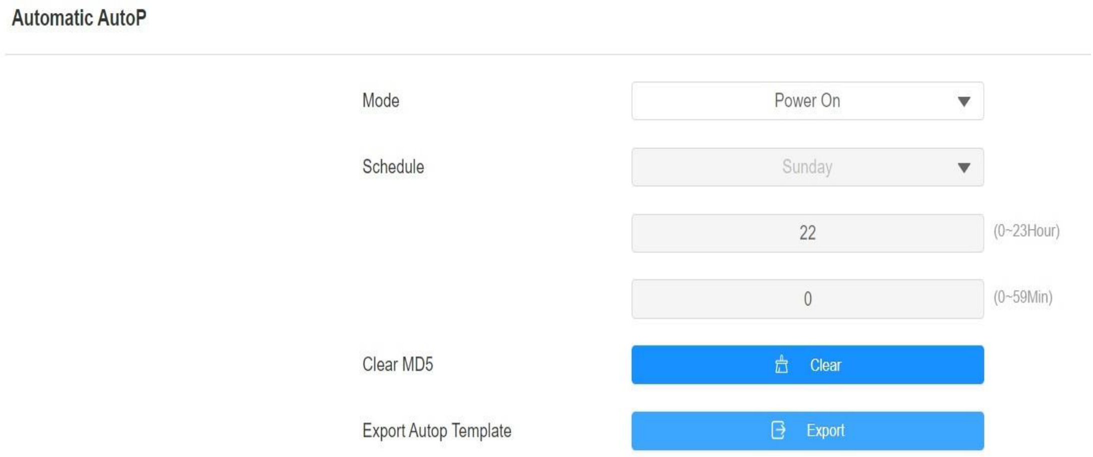
□ Expression

Note

The Custom Option type needs to be a string. The value is the URL of TFTP server.

To set up DHCP AutoP with Power On mode and export AutoP Template so that you can edit the configuration on the same interface:

System > Auto Provisioning > Automatic AutoP


Automatic AutoP

Mode: Power On

Schedule: Sunday

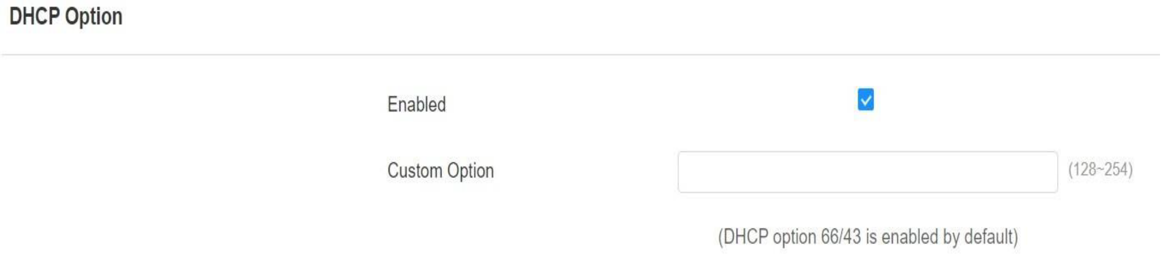
22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

Then, set up the DHCP Option.



DHCP Option

Enabled ☑

Custom Option (128~254)

(DHCP option 66/43 is enabled by default)

Table A42 - MyBell IP Keypad Station - 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

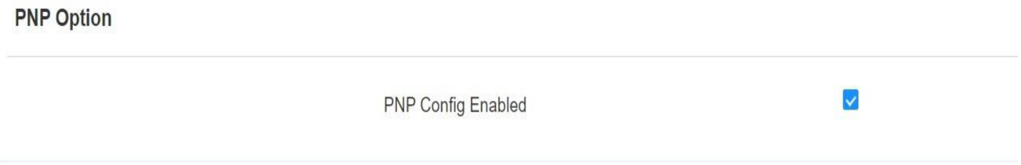
The general configuration file for the in-batch provisioning is in the **.cfg** format. For R29 it's r000000000029.cfg (10 zeros in total). The MAC-based configuration file for the specific device provisioning is in the **MAC_Address** format of the device.cfg, for example, 0C 110504AE5B.cfg.

22.6 - PNP Configuration

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

To configure PNP:

System > Auto Provisioning > PNP Option



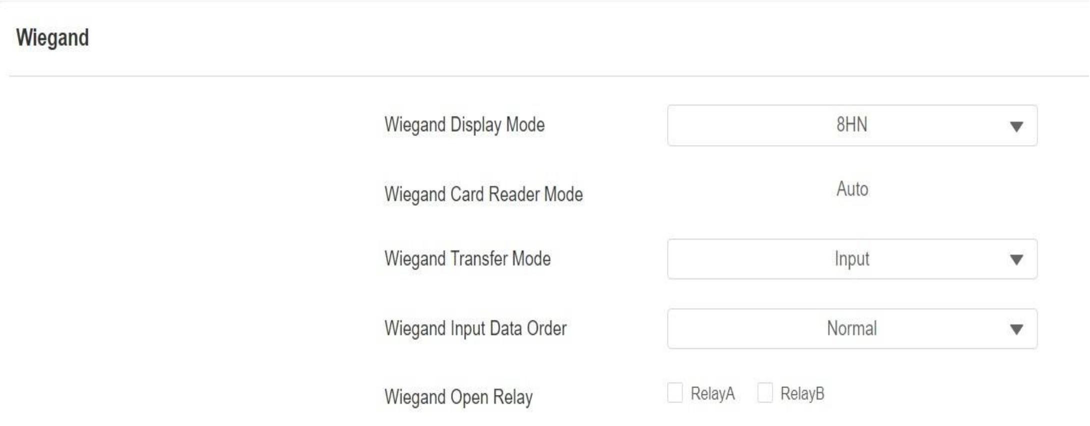
PNP Option

PNP Config Enabled ☑

23.1 - Wiegand integration

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

Device > Wiegand



Wiegand

Wiegand Display Mode: 8HN

Wiegand Card Reader Mode: Auto

Wiegand Transfer Mode: Input

Wiegand Input Data Order: Normal

Wiegand Open Relay: □ RelayA □ RelayB

Table A43 - MyBell IP Keypad Station - Wiegand integration

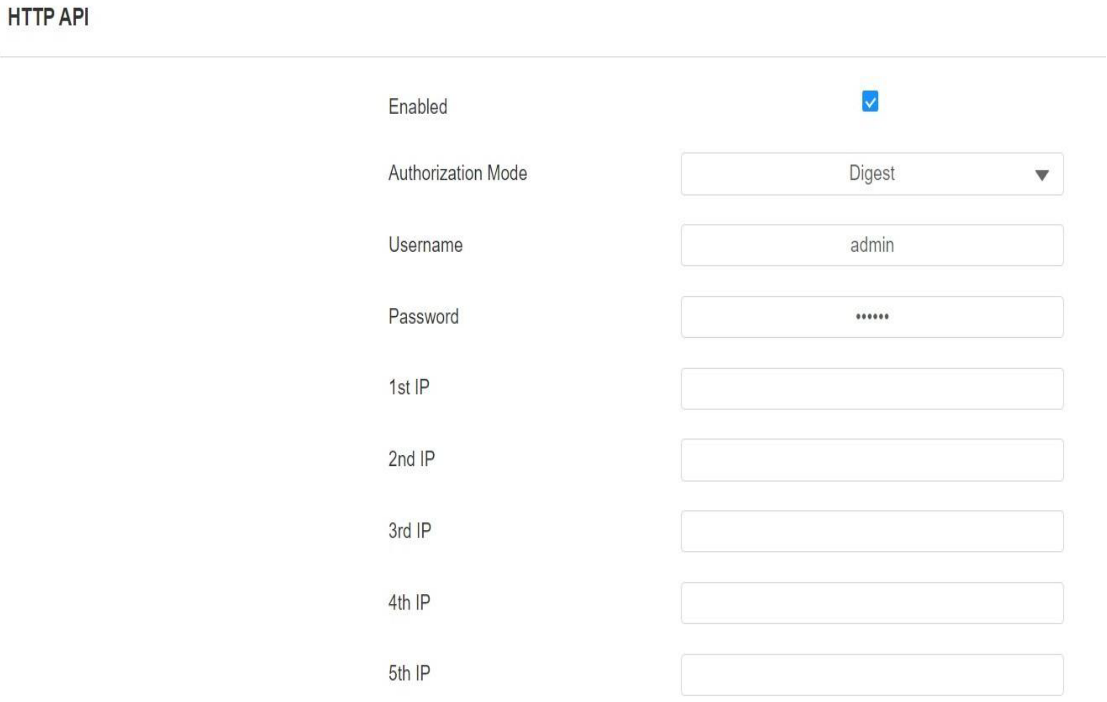
Setting	Description
Wiegand Display Mode	Select Wiegand Card code format from the following options: **8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26), 8HR10D, RAW.**
Wiegand Card Reader Mode	The transmission format needs to be the same for the door phone and the device to be integrated with. It's configured automatically.
Wiegand Transfer Mode	Select the transfer mode from the following options: **Input** – door phone is used as a reciever. **Output** – door phone is used as a sender. **Convert to Card No.OutputWiegand** - Wiegand output is converted to a card number before sending it from the door phone to a receiver.
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 Open Relay	The relay to be triggered.

23.2 - HTTP API integration

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

To perform the HTTP API integration by the web interface:

Setting > HTTP API



HTTP API

Enabled: ☑

Authorization Mode: Digest

Username: admin

Password: ••••••

1st IP:

2nd IP:

3rd IP:

4th IP:

5th IP:

Table A44 - MyBell IP Keypad Station - HTTP API integration	
Setting	**Description**
Enabled	If disabled, any request to initiate the integration is denied and HTTP 403 forbidden status is returned.
Authorization Mode	Select the authorisation type from the following options: **None, Normal, Allowlist, Basic, Digest** or **Token.** The options are explained in detail in Table A46 below.
User Name	Enter the user name when **Basic** or **Digest** authorization mode is selected. The default user name 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 the **Allowlist** authorization mode is selected.

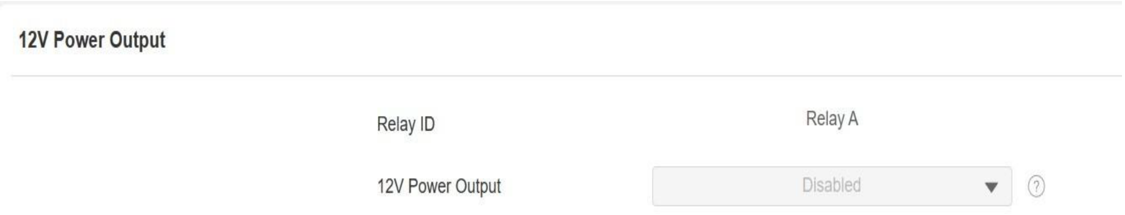
Table A45 - MyBell IP Keypad Station- Authorization modes	
Authorization Mode	**Description**
None	No authentication is required for HTTP API as it's only used for demo testing.
Normal	This mode is used by the developers only.
Allowlist	You only need to enter the IP address of the third party device for authentication. The **Allowlist** is suitable for operation on the LAN.
Basic	You need to enter the **User Name** and the **Password** for authentication. In the **Authorization** field of the HTTP request header use **Base64** encode method to encode the **User Name** and **Password**.
Digest	Password encryption method only supports the Message-Digest Algorithm (MD5). MD5 in the **Authorization** field of the HTTP request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
Token	This mode is used by the developers only.

23.3 - Power output control

The device can serve as a power supply for the external relays.

To configure the device as a power supply for the external relays:

Access Control > Relay > 12VPower Output



12V Power Output

Relay ID: Relay A

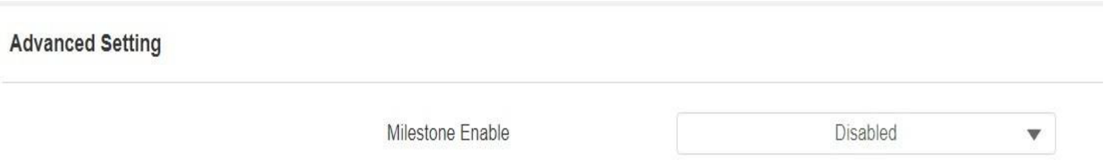
12V Power Output: Disabled

23.4 - Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature.

To configure integration with Milestone:

Surveillance > ONVIF > Advanced Setting



Advanced Setting

Milestone Enable: Disabled

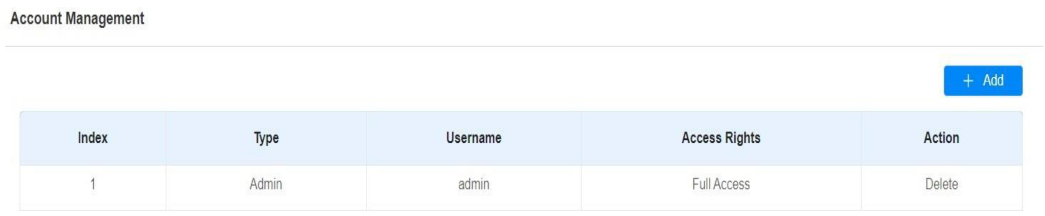
24 PASSWORD MODIFICATION

24.1 - Accounts Management

You can add administrator and user accounts and configure their passwords for logging into the device web interface.

To create an account:

System > Security > Account Management > +Add



Account Management

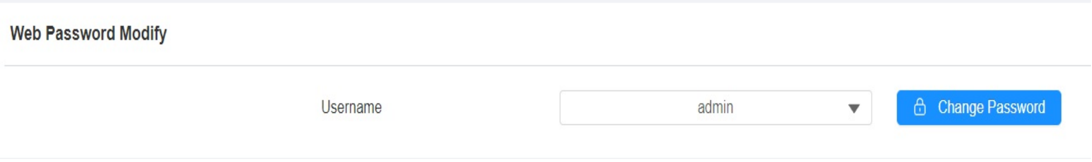
Index	Type	Username	Access Rights	Action
1	Admin	admin	Full Access	Delete

24.2 - Device web interface password modification

To change the password by the web interface:

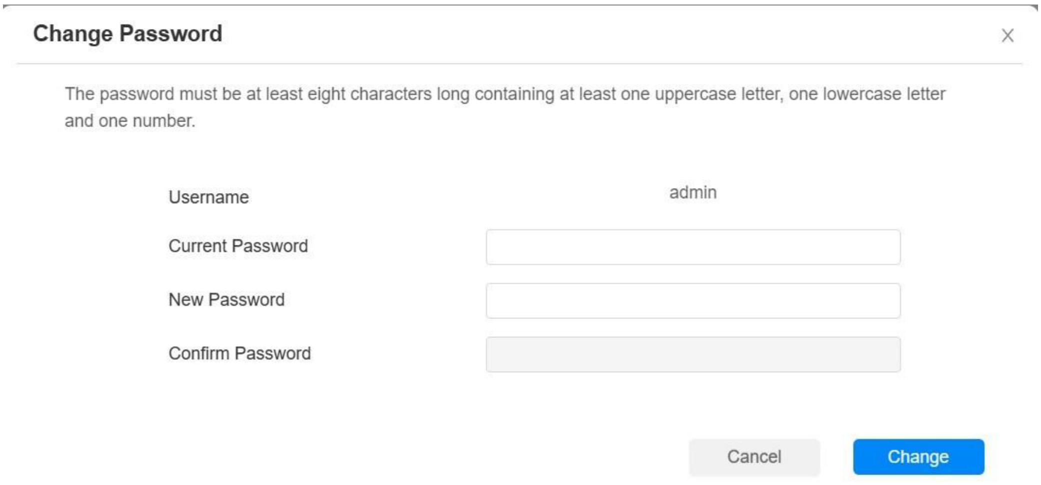
System > Security > Web Password Modify

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



Web Password Modify

Username: admin



Change Password

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

Username: admin

Current Password

New Password

Confirm Password

24.3 - System password modification

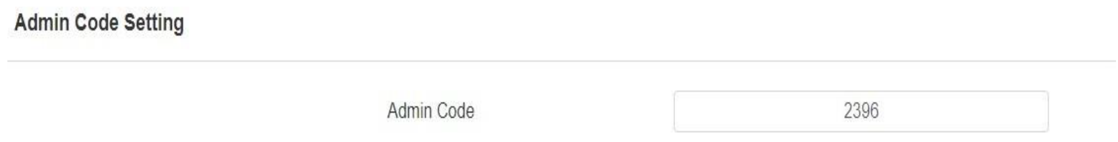
The system PIN code is used to access the device system. You can modify the system PIN code on the device and web interface.

Press ***2396#** on the device keypad and then **2** to enter the Admin Code Setting screen.

To modify the system password by the web interface:

System > Security > Admin Code Setting

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



Admin Code Setting

Admin Code: 2396

24.4 - Setting password modification

The setting PIN code is used to access the settings that include public PIN, private PIN, and user card code modification. You can modify the setting PIN code on the device.

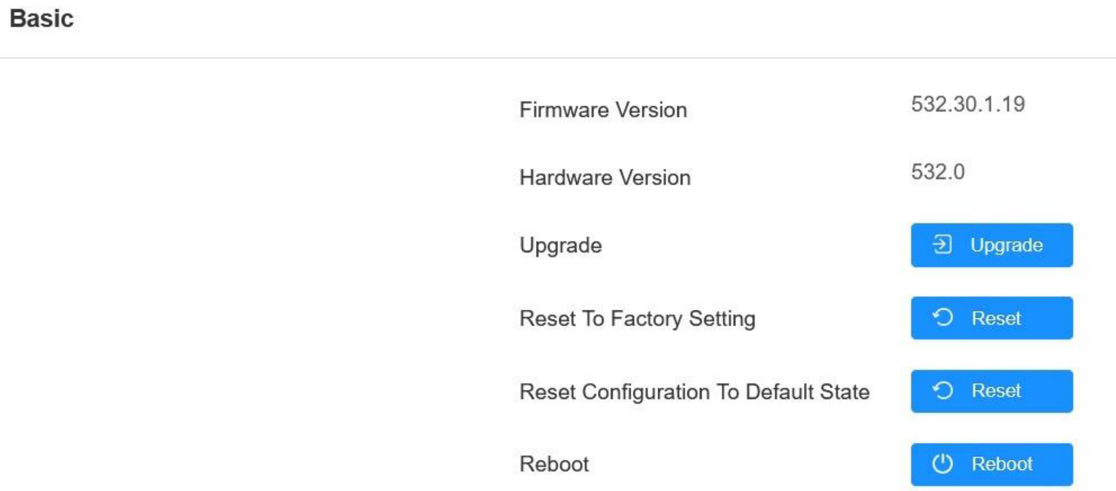
Press ***2396#** on the device keypad, then **2** and **3** to enter the Service Code Setting screen.

25 SYSTEM REBOOT AND RESET

25.1 - Reboot

To reboot the device by the web interface:

System > Upgrade > Basic



Basic

Firmware Version 532.30.1.19

Hardware Version 532.0

Upgrade

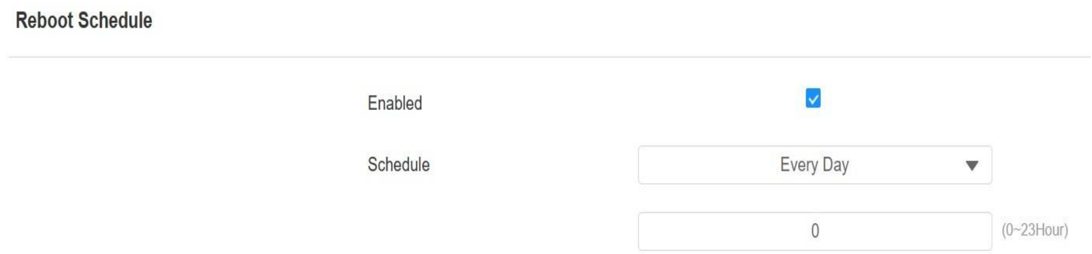
Reset To Factory Setting

Reset Configuration To Default State

Reboot

To set up the reboot schedule by the web interface:

System > Auto Provisioning > Reboot Schedule



Reboot Schedule

Enabled ☑

Schedule Every Day ▼

0 (0~23Hour)

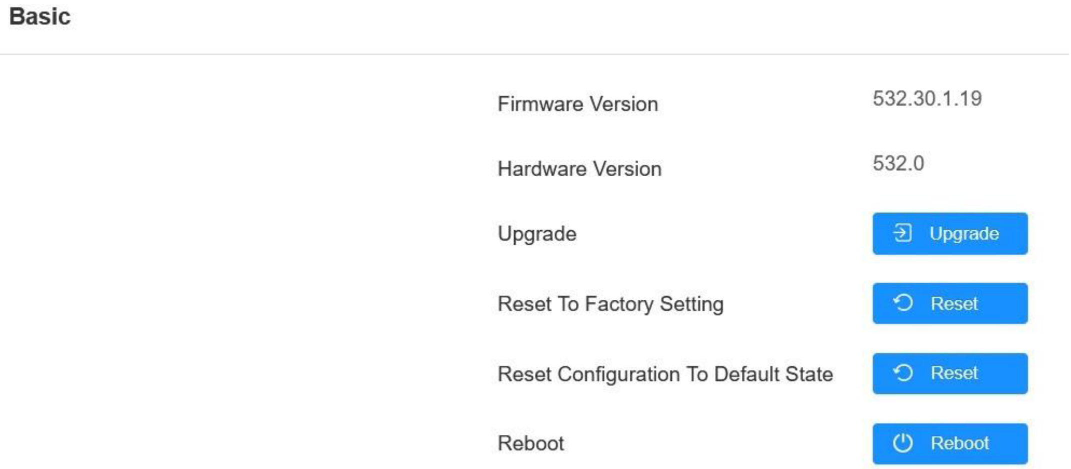
25.2 - Reset

25.2.1 - Reset by web interface

You can select **Reset To Factory Setting** if you want to reset the device deleting both configuration data and user data such as RF cards, face data. You can also select **Reset Configuration to Default State**, if you want to reset the device retaining the user data.

To reset the device by the web interface:

System > Upgrade > Basic



Basic

Firmware Version 532.30.1.19

Hardware Version 532.0

Upgrade

Reset To Factory Setting

Reset Configuration To Default State

Reboot

25.2.2 - Reset on the Device

Press ***2396#** on the device keypad and then **3** and **2** to enter the restore screen. Nextly, swipe the admin card or enter the admin code to reset the device. The default code is **2396**.

26 REGULATIONS

26.1 - Warranty

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

26.2 - Declaration of conformity

Hereby, Nice S.p.A. declares that MyBell IP Keypad Station 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

26.3 - 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.

IS0932A00 EN_08-11-2024

Nice SpA
Oderzo TV Italia
info@niceforyou.com

www.niceforyou.com