About This Manual

Thank you for choosing Akuvox R28 series door phones. This manual is intended for the administrators who need to properly configure the door phone. This manual is written based on the 28.30.10.3 version, and it provides all the configurations for the functions and features of the Akuvox door phone. Please visit Akuvox web or consult technical support for any new information or the latest firmware.

Product Overview

The security that comes with being able to control who comes into your building along with the ability to verbally and visually confirm their identity is immeasurable. Akuvox R28A is a SIP-compliant, hands-free, and video(optional) door phone. It can be connected with Akuvox indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. The door phone enables you to easily monitor an entrance door or gate and gives you peace of mind knowing that your facility is more secure.

Change Log

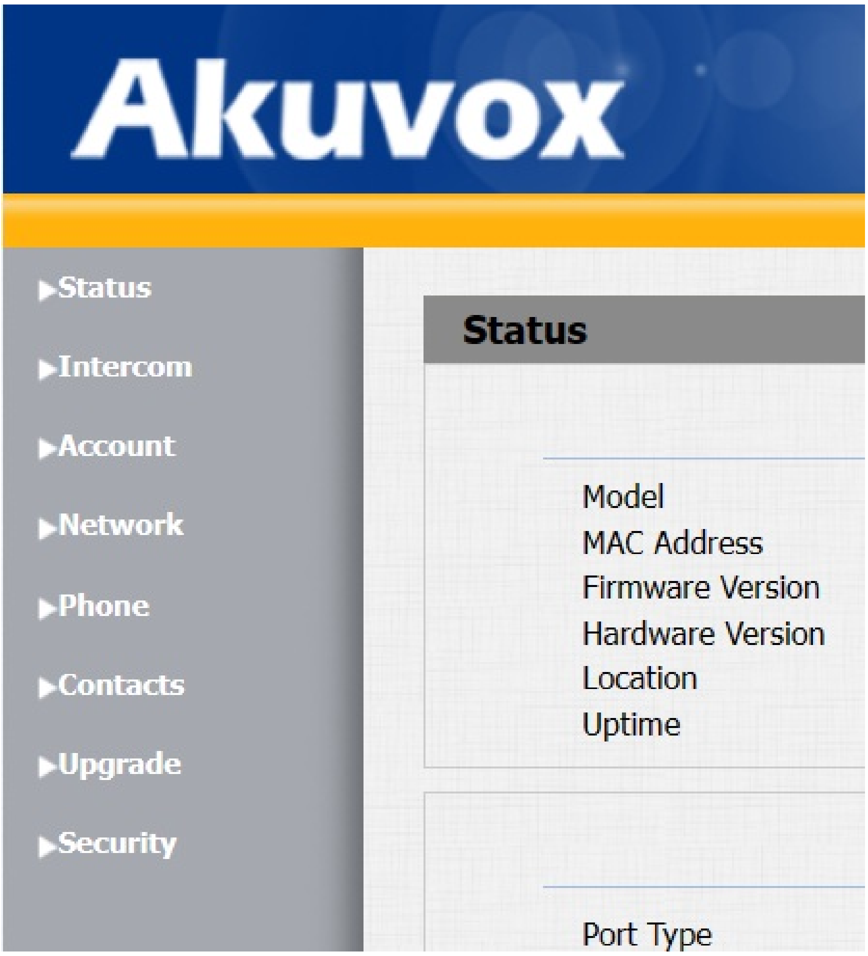
Add High Security Mode.

Model Specification

Model	R28A
Camera	2 Megapixels, automatic lighting
Relay In	3
Relay Out	3
RS485	✔
Card Reader	✔

Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, network information, and account information, etc.
- **Intercom**: this section cover intercom call setting, user, access schedule, Input control, Relay, Card settings, PIN Code, Wiegand connection, ONVIF, RTSP, and Mjpeg monitoring, lift control, motion detection, HTTP API, etc.
- **Account**: this section concerns the SIP account, SIP server, NAT, proxy server, transport protocol type, audio&video codec.
- **Network**: this section mainly deals with DHCP&Static IP setting, RTP port setting, device deployment, SNMP, VLAN, and TR069 Web server.
- **Phone**: this section covers time, language, call feature, audio, dial plan multicast, door logs, call logs, web relay, etc.
- **Contacts**: this section covers contact settings.
- **Upgrade**: this section covers firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault diagnosis.
- **Security**: this section is for password modification and server certificates.



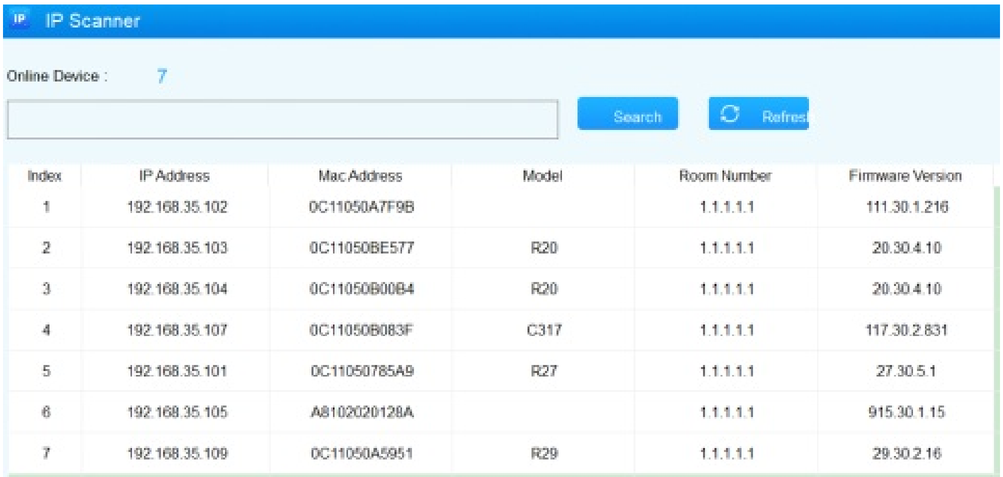
Access the Device

Access the Device

Door phones' system settings can be either accessed on the device directly or on the device web interface.

Obtain Device IP Address

Searching the device IP by the IP scanner in the same LAN network. Just click the **Scan** tab in the IP scanner to check the device IP. Or checking the device IP address from the device setting screen.



Online Device : 7

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

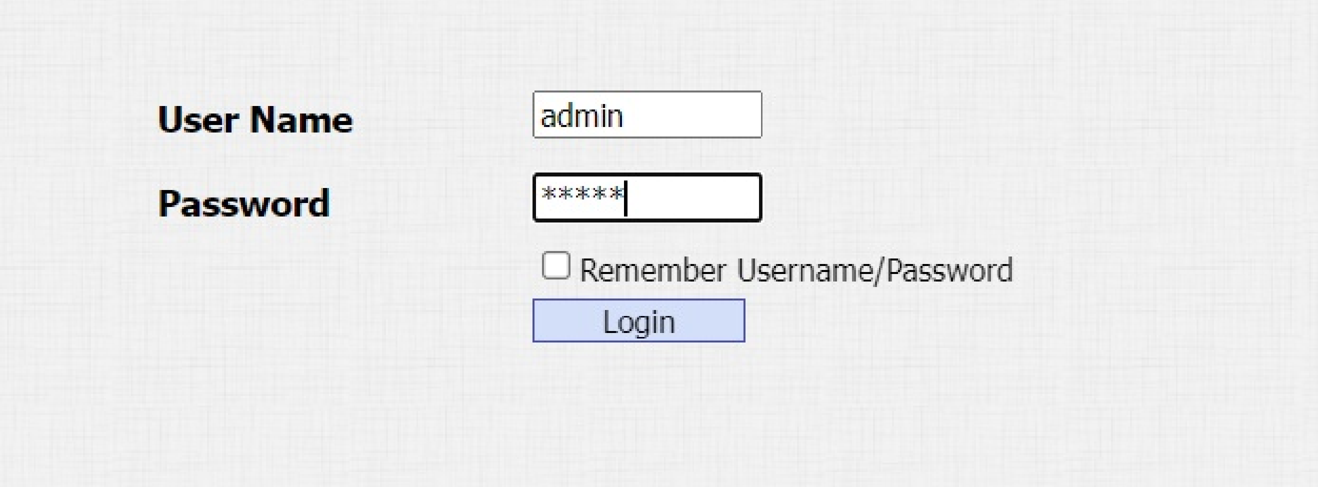
Access the Device Setting on the Device

To access the device setting, press “***2396#**” to enter the advanced setting screen. It provides some advanced permissions like editing network, reset, and admin password modification to administrators, including **System Information**, **Admin Access**, and **System Settings**.

Access the Device Setting on the Web Interface

You can also enter the device IP address on the web browser in order to log in to the device web interface where you can configure and adjust parameters, etc.

The initial user name and password are all **admin**, and please be case-sensitive to the user names and passwords entered.



User Name admin

Password *****

Note

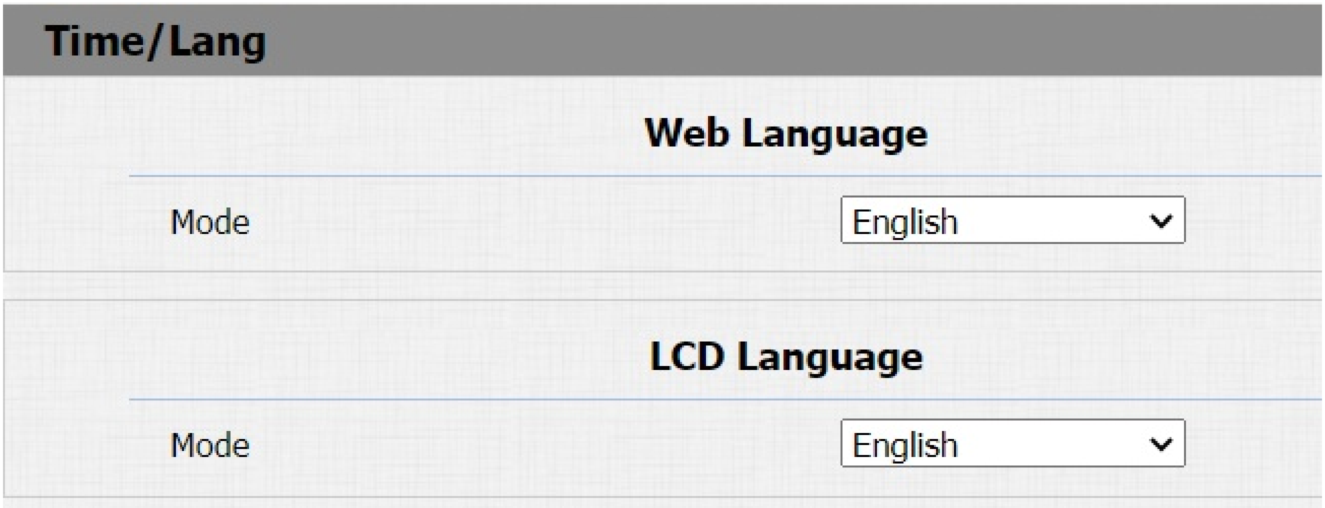
- You can obtain the device IP address using the Akuvox IP scanner to log in to the device web interface.
- To download: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.

Language and Time Setting

Language Setting

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

To set up the language you need, go to **Phone** > **Time/Lang**.



Time/Lang

Web Language

Mode: English

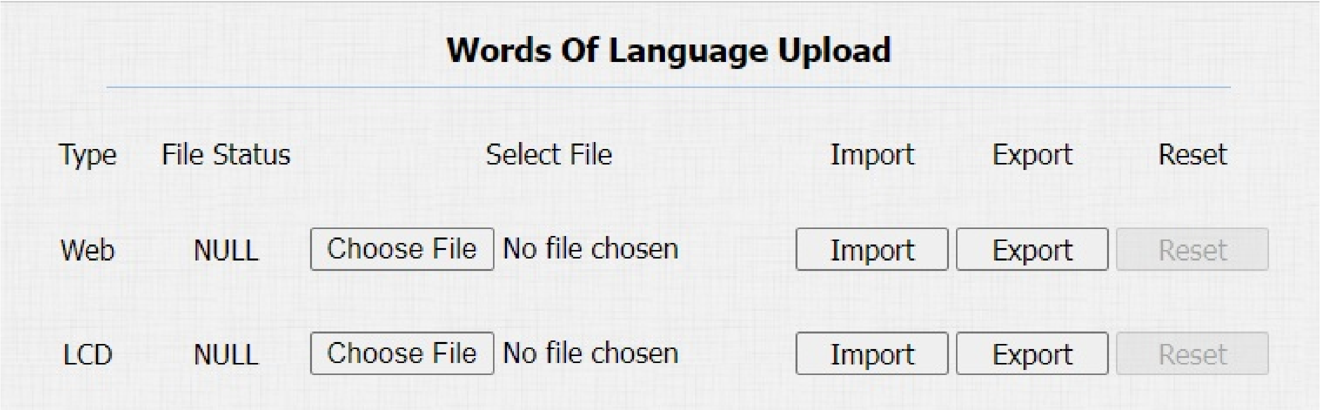
LCD Language

Mode: English

Parameter Set-up:

- **Type**: choose a suitable web language. Normally, English is the default web and LCD language.

To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device **Phone** > **Time/Lang** > **Words Of Language Upload**.



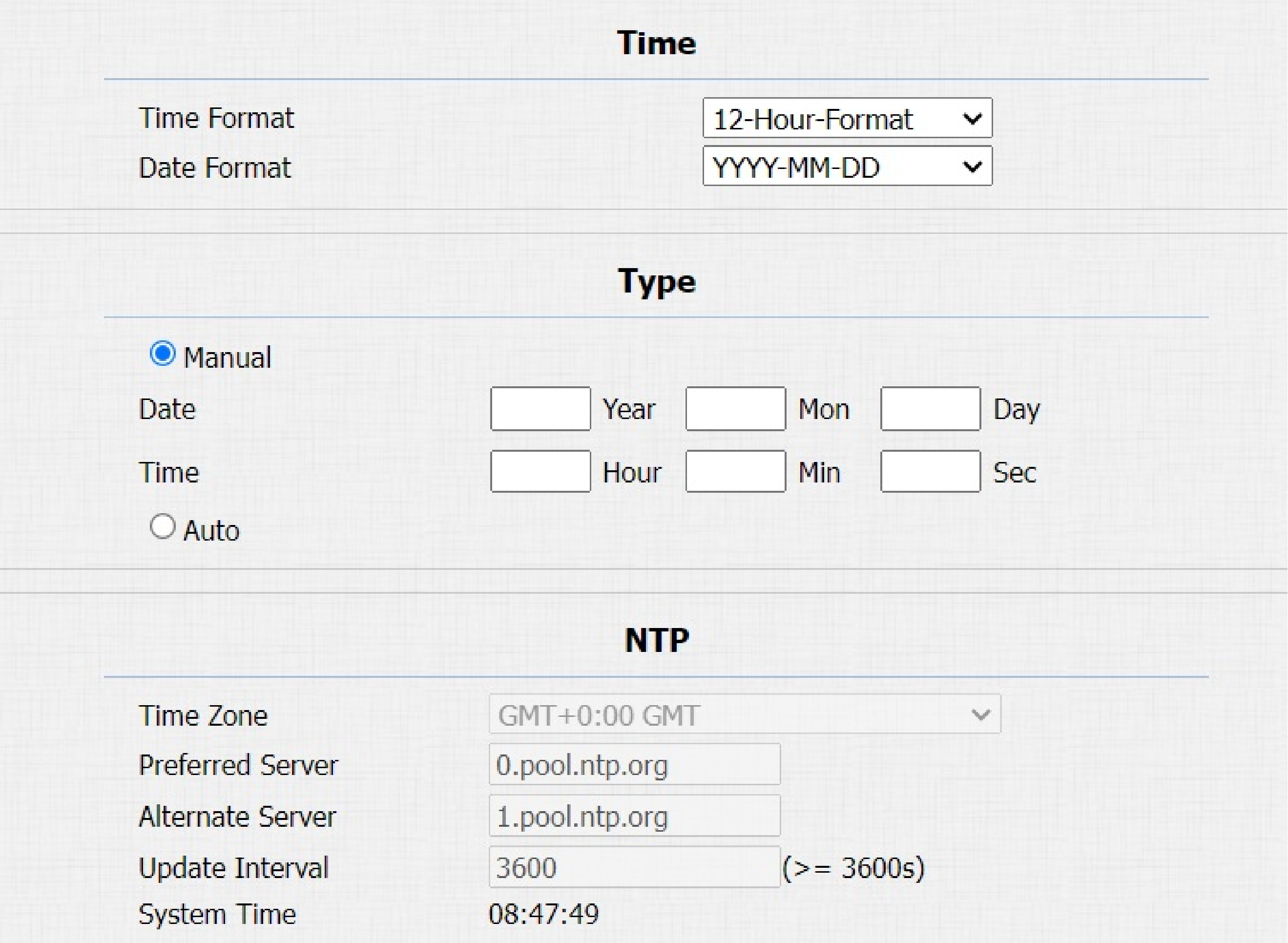
Words Of Language Upload

Type	File Status	Select File	Import	Export	Reset
Web	NULL	Choose File No file chosen	Import	Export	Reset
LCD	NULL	Choose File No file chosen	Import	Export	Reset

Time Setting

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

To set up the device time, go to **Phone > Time/Lang> Time**.



Time

Time Format	12-Hour-Format
Date Format	YYYY-MM-DD

Type

● Manual

Date Year Mon Day

Time Hour Min Sec

○ Auto

NTP

Time Zone	GMT+0:00 GMT
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	08:47:49

Parameter Set-up:

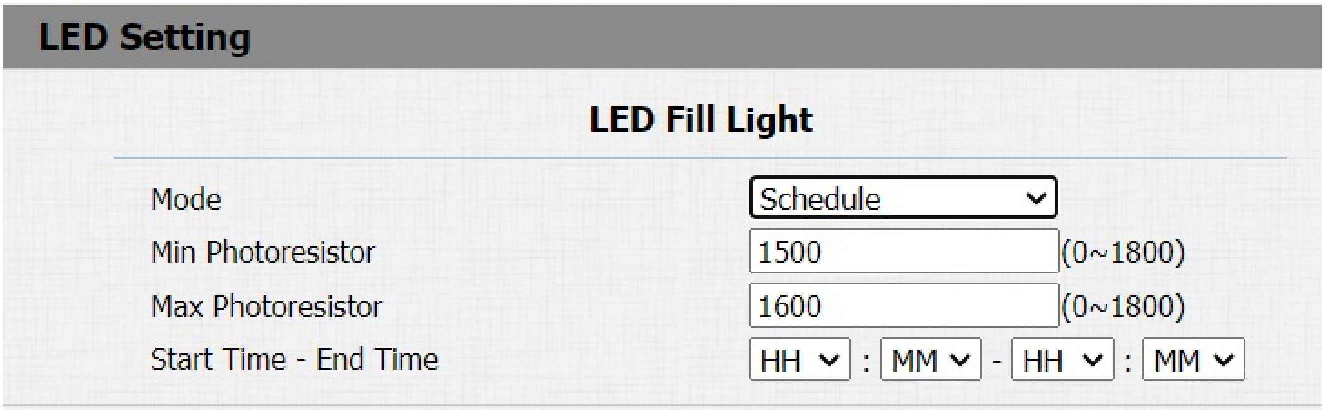
- **Time Zone**: it is available when you choose **Auto**. Select the specific time zone depending on where the device is used and then click **Submit**. The default time zone is **GMT GMT+0.00**.
- **Preferred Server/Alternate Server**: it is available when you choose **Auto**. The time zone server normally will automatically obtain the time when connecting to the network. The secondary server will take effect when the primary server is invalid.
- **Update Interval**: it is available when you choose **Auto**. To configure the interval between two consecutive NTP requests.

Screen Display and LED Setting

Infrared LED Setting

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

You can set up it on the device web **Intercom > LED Setting > LED Fill Light**.



LED Setting

LED Fill Light

Mode	Schedule
Min Photoresistor	1500 (0~1800)
Max Photoresistor	1600 (0~1800)
Start Time - End Time	HH : MM - HH : MM

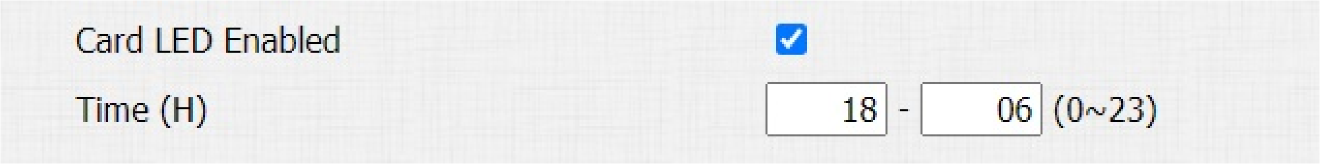
Parameter Set-up:

- **Mode**: select infrared LED mode.
  - If you select **Auto**, then the infrared LED will be turned on automatically based on the photoresistor setting below.
  - If you select **Always On**, then the infrared LED will stay on.
  - If you select **Always Off**, then the infrared LED will stay off.
  - If you select **Schedule**, then the infrared LED will be turned on based on the photoresistor setting according to your schedule.
- **Photoresistor Setting**: set the triggering points for disabling the infrared LED and enabling the infrared LED. For example, if you set the triggering points at 1500-1600, the infrared LED will be enabled when the photoresistor value gets higher than 1600 (the video image you see from the door phone will become black and white) and if the value gets lower than 1500, then the infrared light will be disabled (the video image you see will have color).

LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce electrical power consumption.

To do this configuration, go to **Intercom > LED Setting > LED Control**.



Card LED Enabled ☑

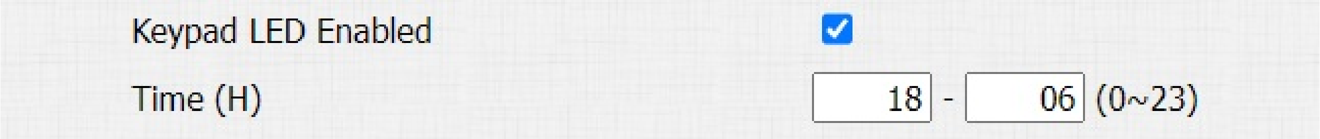
Time (H) 18 - 06 (0~23)

Parameter Set-up:

- **Time (H)**: set the time interval for the light to stay on. enter the time interval for the LED light to be turned on, e.g., if the time interval is set from **8-0 (Start time- End time)** it means the LED light will stay on during the time span from **8:00** am to **12:00** pm during one day (24 hours). This setting cannot be set up when you disable the LED light.

LED Settings on Keypad

You can enable or disable the LED lighting of the keypad as needed on the web interface. Meanwhile, if you prefer not to have the LED light of the keypad stay on, you can also set the timing for the exact time span during which the LED light can be enabled in order to reduce the electrical power consumption, etc. To do this configuration, go to **Intercom > LED Setting > LED Control** interface.



Keypad LED Enabled ☑

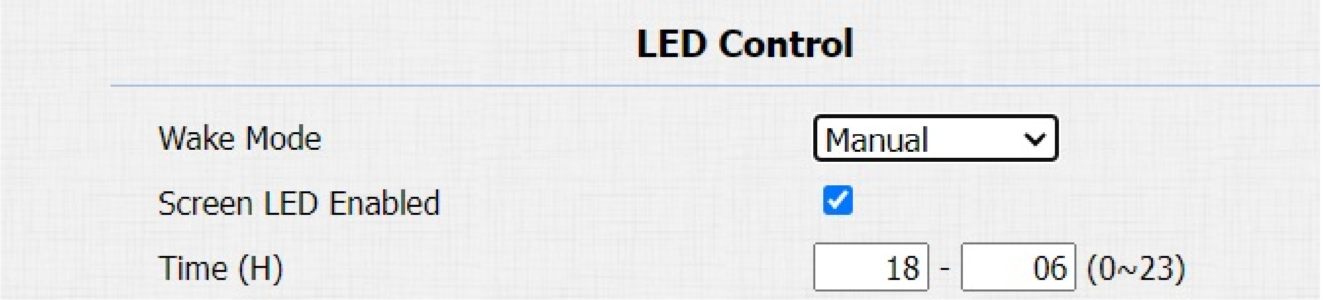
Time (H) 18 - 06 (0~23)

Parameter Set-up:

- **Time (H)**: enter the time span for the LED lighting to be valid. E.g. If the time span is from **18-22** it means LED light will stay on during the time span from **6:00** pm to **22:00** pm during a day.

LED Settings on Screen

You can enable or disable the LED lighting of the screen as needed on the web interface. Meanwhile, if you prefer not to have the LED light on the screen stay on, you can also set the timing for the exact time span during which the LED light can be enabled in order to reduce the electrical power consumption, etc. To do this configuration, go to **Intercom > LED Setting > LED Control**.



LED Control

Wake Mode: Manual

Screen LED Enabled: ☑

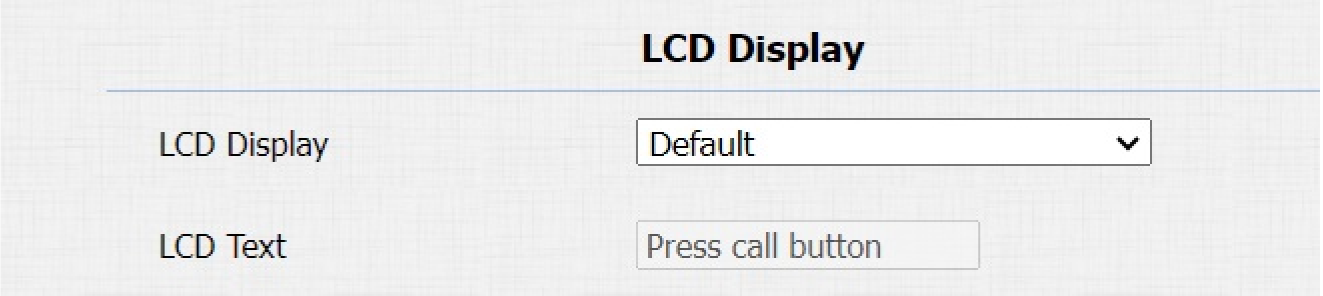
Time (H): 18 - 06 (0~23)

Parameter Set-up:

- **Wake Mode**: there are two modes: **Auto** and **Manual** for waking up the device when idle. If you select **Auto** mode, then the screen will be awakened when someone approaches, and the IR sensor will be triggered. And if **Manual** mode is selected, then you have to press the keypad.
- **Time(H)**: enter the time span for the LED lighting to be valid. For example, if the time span is from **18-22**, it means LED light will stay on during the time span from **6:00** pm to **22:00** pm during a day.

LCD Screen Display

You can customize the LCD display. You can do this configuration on the web **Intercom > Advanced** interface.



LCD Display

LCD Display: Default

LCD Text: Press call button

Parameter Set-up:

- **LCD Display**: select the LCD display.
  - **Default**: if you select it, then Call, Contacts, PIN Entry, and Security Center will be displayed on the home screen.
  - **Hide Contacts**: if you select it, then Contacts will be hidden on the home screen.
  - **Text Only**: if you select it, then only the text will be displayed on the home screen.

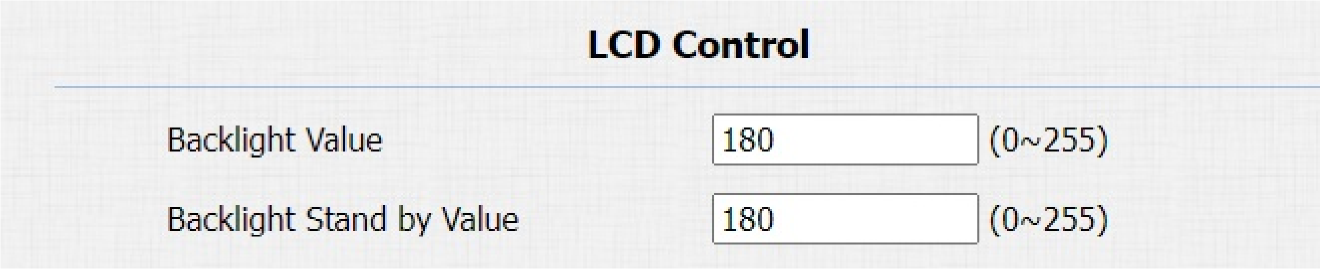
You can customize the text if needed.

  - **Contacts Only**: if you select it, then only the Contacts will be displayed on the home screen.
  - **Hide Contacts & Room Number**: if you select it, then Contacts and room number will be hidden on the home screen. It only displays PIN Entry and Security.

- **LCD Text**: it is available when you choose **Text Only.** Enter the display content you need.

Backlight Setting

If you want to brighten up the screen in order to see the screen at greater ease in an environment with higher light intensity, you need to set up the related parameters in web **Intercom > LED Setting > LED Control** interface.



LCD Control

Backlight Value	180	(0~255)
Backlight Stand by Value	180	(0~255)

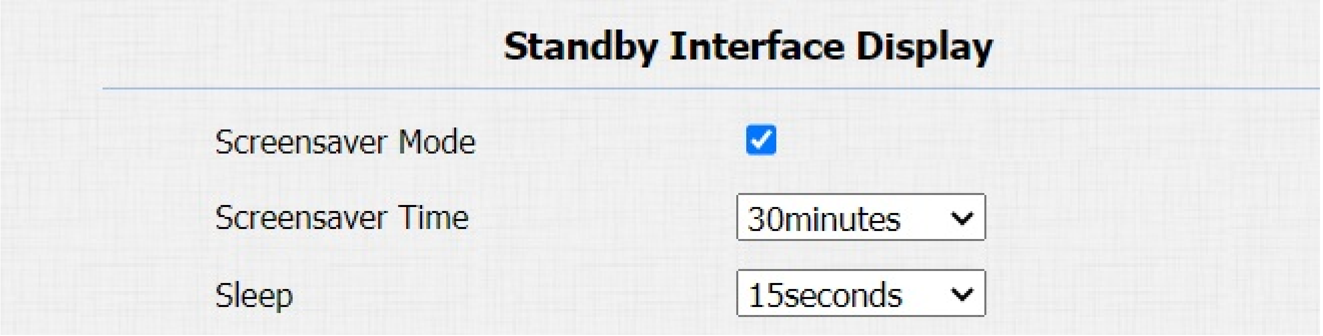
Parameter Set-up:

- **Backlight value**: set the backlight value when the device is working with a value ranging from 0-255.
- **Backlight Standby Value**: adjust the backlight for the screen in standby mode with the value ranging from 0-255.

Screen Saver Setting

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 do this configuration on the web **Intercom > LED Setting > Standby Interface Display.**



Standby Interface Display

Screensaver Mode	☑
Screensaver Time	30minutes
Sleep	15seconds

Parameter Set-up:

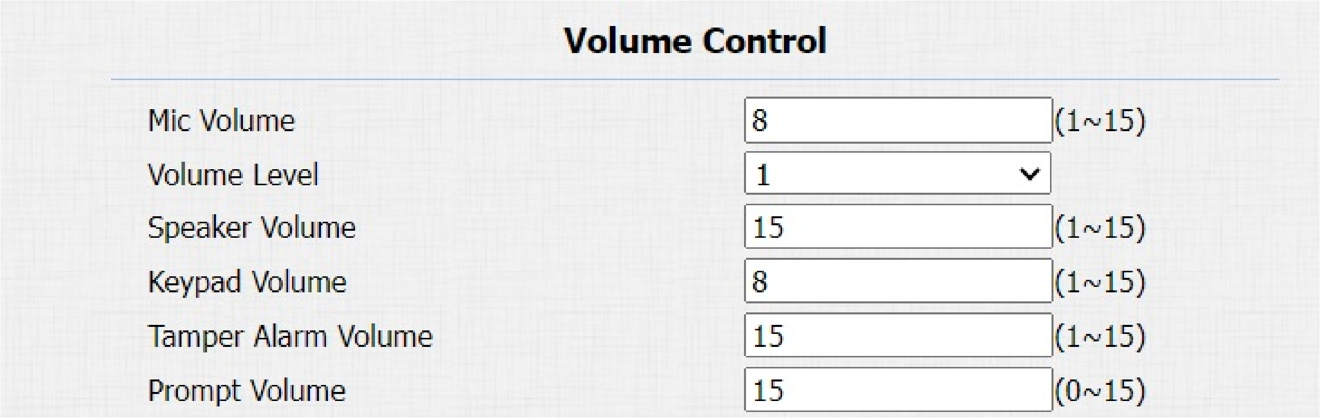
- **Screensaver Time (Sec)**: Set the screen saver start time. For example, if you set the start time as 5 minutes, then the screen saver will start if there is no operation on the device or no one is approaching the device during the five minutes interval.
- **Sleep**: set how long you expect the screen saver to last before turning off the device's screen.

Volume and Tone Configuration

Volume and tone configuration include microphone volume, the AD volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

Volume Configuration

To set up the volumes, you can set them up on the device web **Phone > Audio > Volume Control** interface.



Volume Control

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

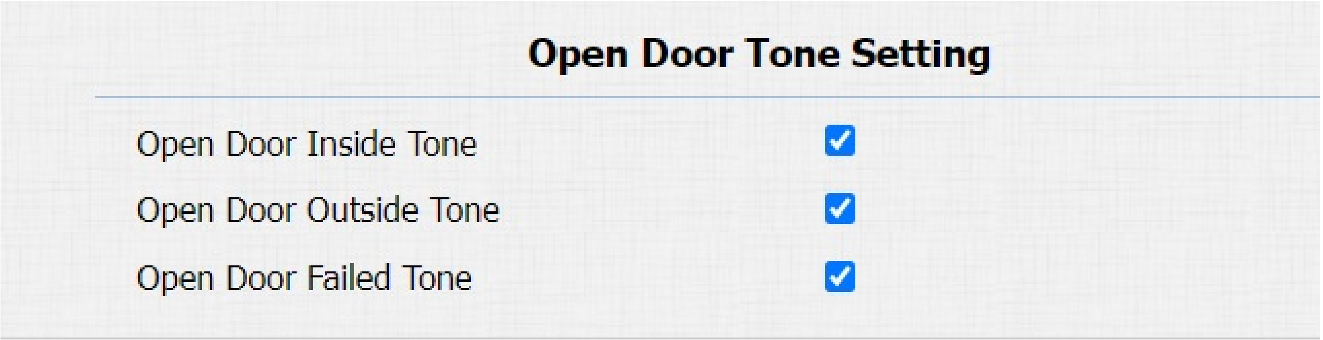
Parameters Set-up:

- **Volume Level**: control the volume of all speakers. The default is 1, the first level of volume, the volume range is roughly 80-95, and 2 is the second level of volume, the volume range is roughly 95-109.
- **Prompt Volume**: adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound, etc.

Open Door Tone Configuration

You can upload the tone for open door failure and success on the device web interface.

Go to **Phone** > **Audio** > **Open Door Tone Setting** interface.



Open Door Tone Setting

Open Door Inside Tone ☑

Open Door Outside Tone ☑

Open Door Failed Tone ☑

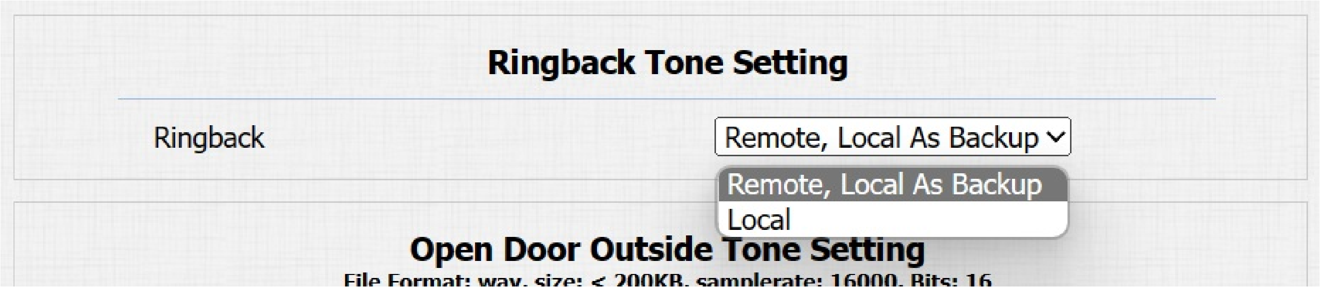
Parameters Set-up:

- **Open Door Inside Tone**: enable it so that you can hear the open door tone when you open the door by pressing the exit button.
- **Open Door Outside Tone**: enable it so that you can hear the open door tone when you open the door using the access method on the door phone.
- **Open Door Failed Tone**: enable it so that you can hear the open door failure tone following the open door failure.

Ringback Tone Setting

You can also configure ringback tone on the **Phone** > **Audio** > **Ringback Tone Setting** interface.

You can hear the ringback tone whether **Remote, Local As Backup** or **Local** is selected. The differences lie in what the callee can see.



Ringback Tone Setting

Ringback: Remote, Local As Backup

Open Door Outside Tone Setting

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

Parameter Set-up:

- **Remote, Local As Backup**:
  - If selected, when the door phone calls another device, for example, Akuvox indoor monitor and the SIP server returns 183, the callee will see the video preview without voice.
  - If the SIP server returns non-183, the callee will not have the intercom preview.

- **Local**: whether the SIP server returns 183 or not, the callee will not have the intercom preview.

Upload Tone Files

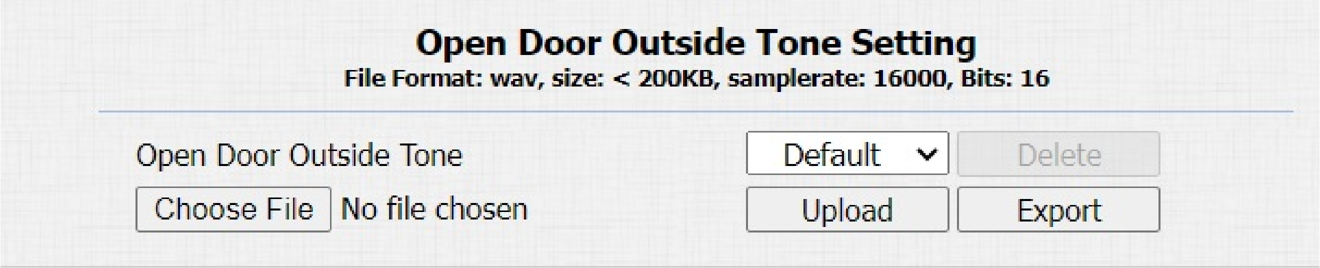
You can configure the door phone ringback tone and other tones related to the door opening.

Upload Open Door Tone

You can upload the tone for open door failure and success on the device web interface.

The outside tone is heard when you open the door via card, DTMF or PIN code. The inside tone is heard when you open the door via a triggered input interface. Please follow the file size and format.

On the web, navigate to **Phone > Audio**.



Open Door Outside Tone Setting

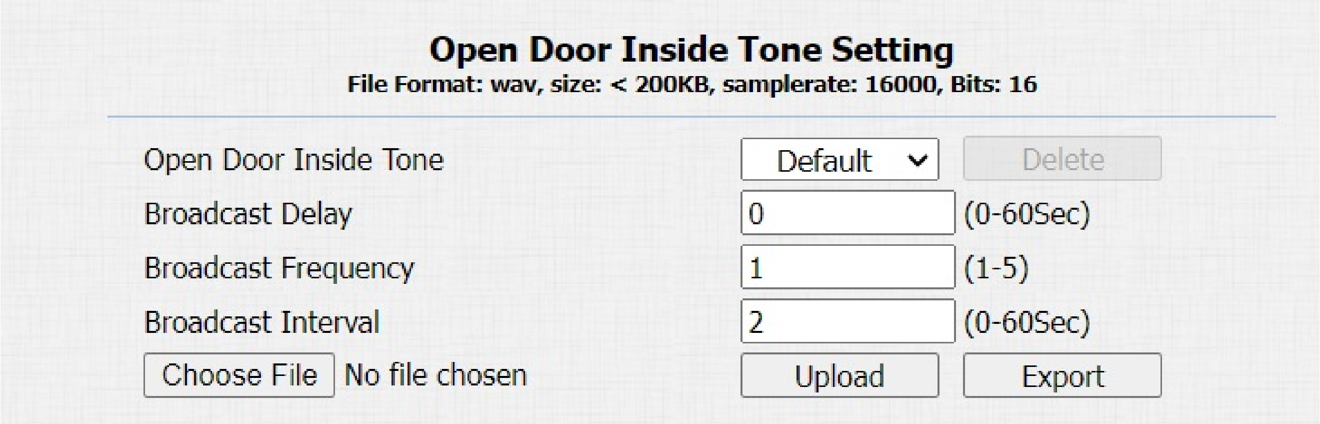
File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

Open Door Outside Tone: Default

No file chosen

Parameter Set-up:

- **Open Door Outside Tone Setting**: upload the open door success tone which you can hear when you open the door using the access method on the door phone.



Open Door Inside Tone Setting

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

Open Door Inside Tone: Default

Broadcast Delay: 0 (0-60Sec)

Broadcast Frequency: 1 (1-5)

Broadcast Interval: 2 (0-60Sec)

No file chosen

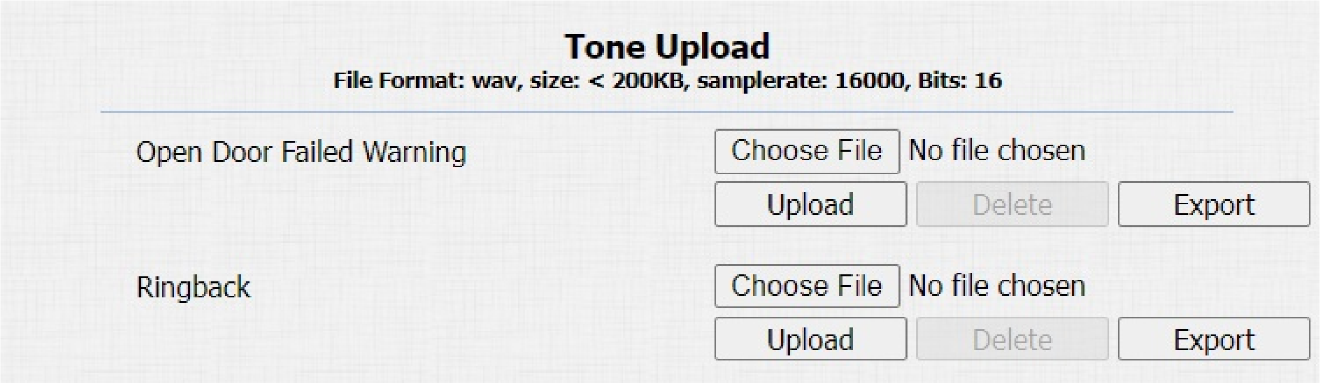
Parameter Set-up:

- **Open Door Inside Warning**: upload the open door tone when you open the door by pressing the exit button.
- **Broadcast Delay**: select open door tone waiting time after door opening success. For example, if you set it at 2 seconds, then the tone will go on 2 seconds after the door opens.
- **Broadcast Frequency**: select the number of open door tones. For example, if you select

1, then the tone will be played only once after the door opening.

- **Broadcast Interval**: select the time interval between every two open door tones. For example, if you select 2, then the interval between two open door tones will be two seconds. The number of open door tones should be 2 minimum if in this application.

Upload Door Failed Tone and Ringback Tone



Tone Upload

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

Open Door Failed Warning

Ringback

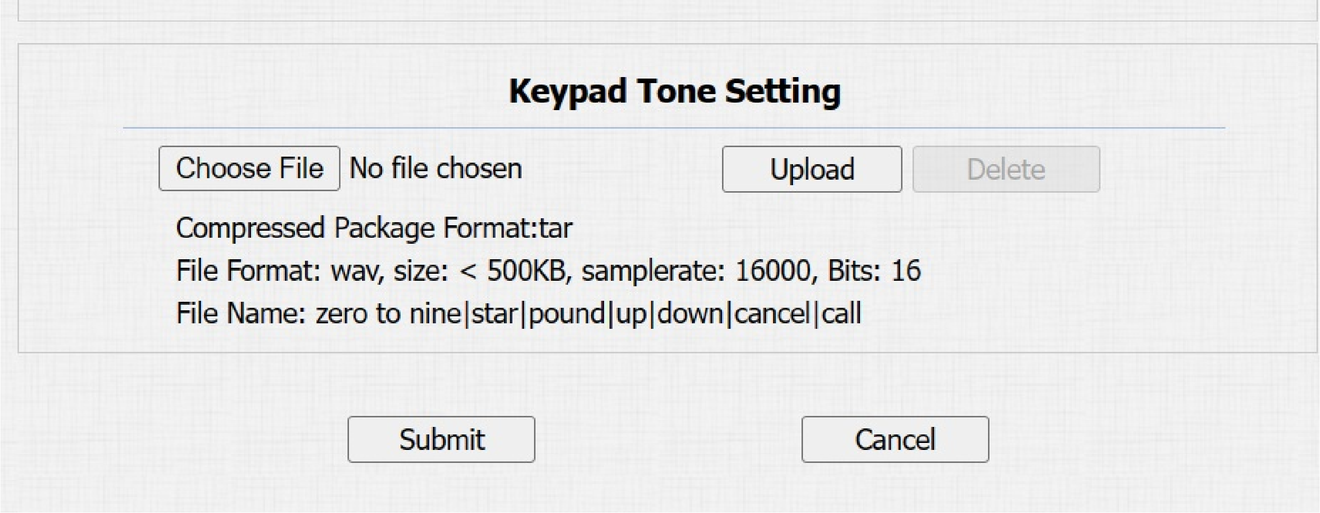
Parameter Set-up:

- **Open Door Failed Warning**: upload the open door failure tone.

- **Ringback**: upload the ringback tone.

Upload Keypad Tone

You can upload keypad tone for each key. When pressing any key, corresponding tone can be heard so that you can distinguish the key from others.



Keypad Tone Setting

Compressed Package Format:tar

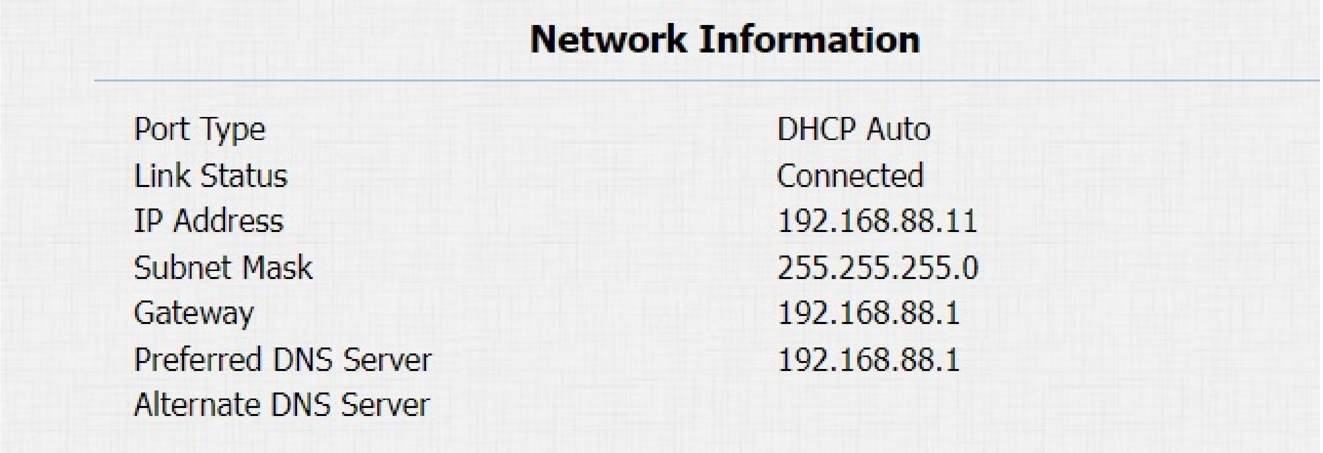
File Format: wav, size: < 500KB, samplerate: 16000, Bits: 16

File Name: zero to nine|star|pound|up|down|cancel|call

Network Setting

Network Status

To check the network status on the web **Status** > **Network Information** interface.



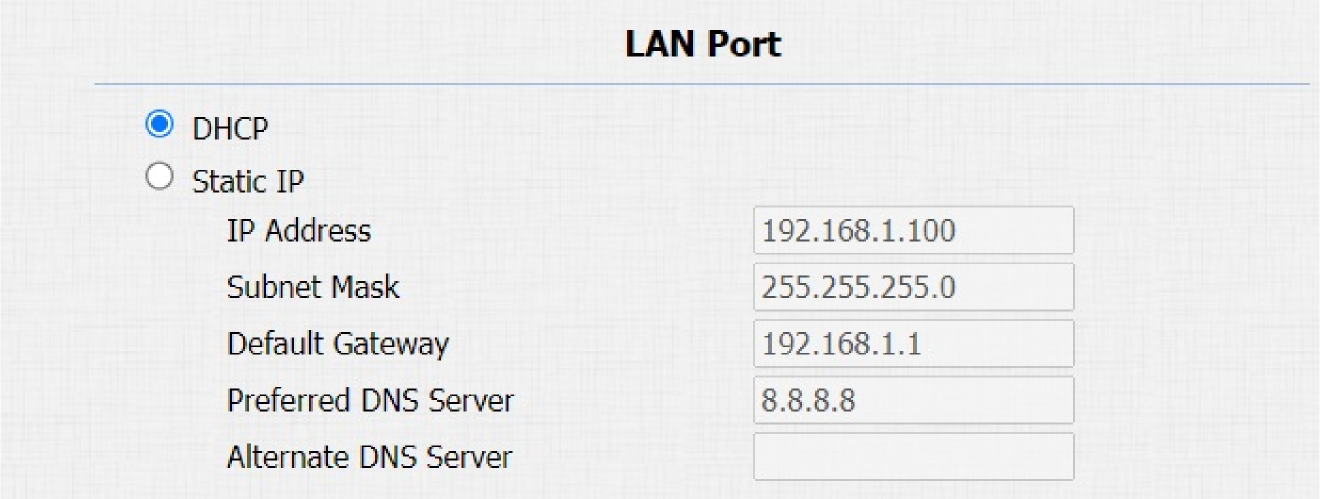
Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.88.11
Subnet Mask	255.255.255.0
Gateway	192.168.88.1
Preferred DNS Server	192.168.88.1
Alternate DNS Server	

Device Network Configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the DHCP server.

Go to **Network** > **Basic** interface.



LAN Port

● DHCP

○ Static IP

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

Parameter Set-up:

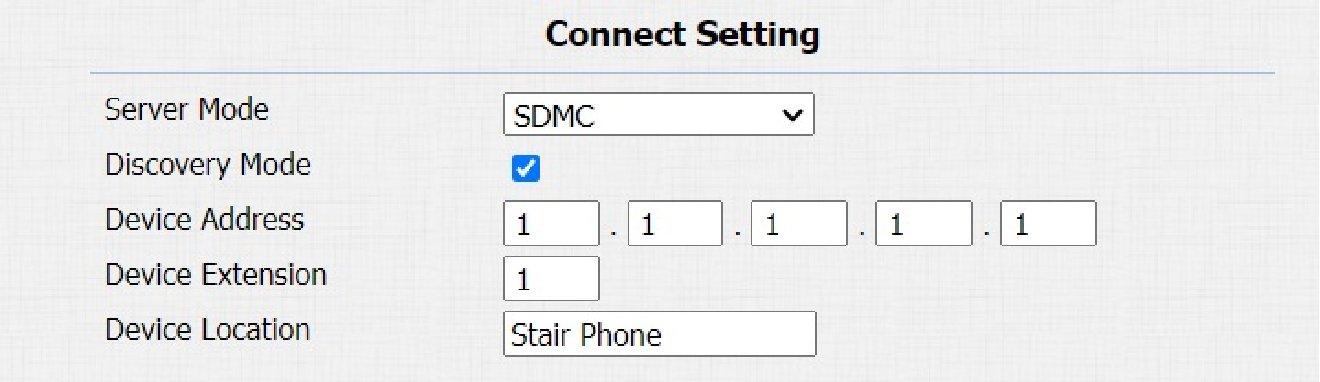
- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.

- **Static IP**: When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to your actual network environment.
- **IP Address**: set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **LAN DNS1/2**: set up a preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address and the door phone will connect to the alternate server when the primary DNS server is unavailable.

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

So, you can do it on web **Network > Advanced > Connect Setting** interface.



Connect Setting

Server Mode	SDMC
Discovery Mode	☑
Device Address	1 . 1 . 1 . 1 . 1
Device Extension	1
Device Location	Stair Phone

Parameter Set-up:

- **Server Type**: it is automatically set up 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 is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **Discovery Mode**: click **Enable** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click Disable 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.

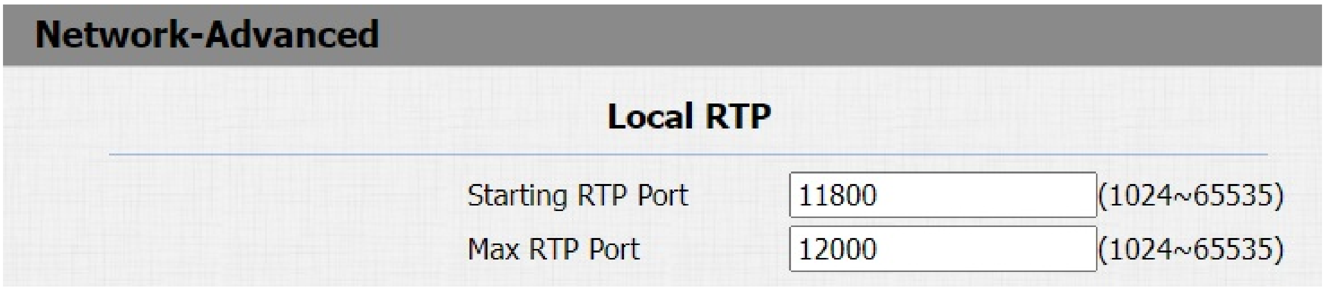
- **Device Extension**: enter the device extension number for the device you installed.
- **Device Location**: enter the location in which the device is installed and used.

Device Local RTP Configuration

Real-time Transport Protocol(**RTP**) lets devices stream audio and video data over a network in real time.

To use RTP, devices need a range of ports. A port is like a channel for data on a network. By setting up RTP ports on your device and router, you can avoid network interference and improve audio and video quality.

Path: **Network** > **Advanced** > **Local RTP** interface.



Network-Advanced

Local RTP

Starting RTP Port: 11800 (1024~65535)

Max RTP Port: 12000 (1024~65535)

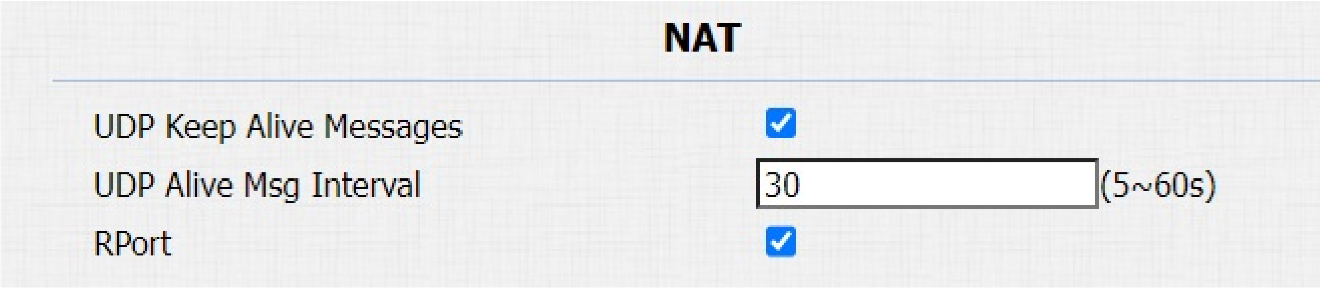
Parameter Set-up:

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

NAT Setting

Network Address Translation(**NAT**) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

To do this configuration on web **Account** > **Advanced** > **NAT** interface.



NAT

UDP Keep Alive Messages ☑

UDP Alive Msg Interval 30 (5~60s)

RPort ☑

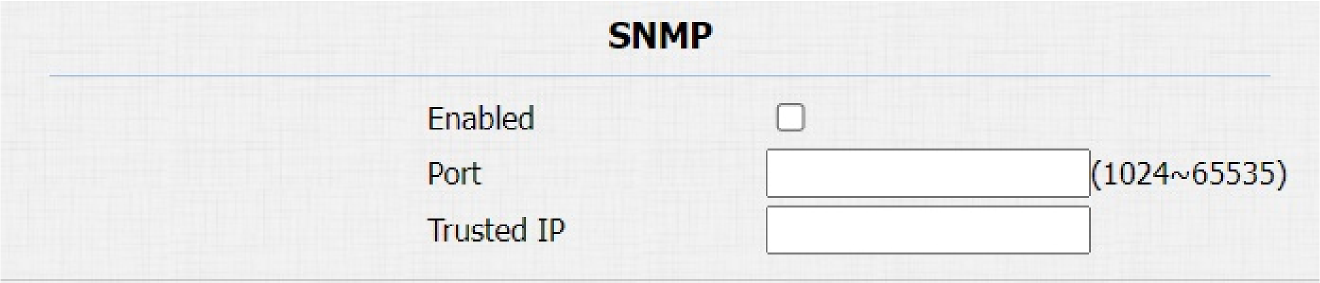
Parameter Set-up:

- **UDP Keep Alive Messages**: if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Messages Interval**: set the message sending time interval from 5-60 seconds, the default is 30 seconds.
- **RPort**: enable the RPort when the SIP server is in WAN (**Wide Area Network**).

SNMP Setting

Simple Network Management Protocol(**SNMP**) is a protocol for managing IP network devices. It allows 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 do the configuration on the web **Network** > **Advanced** > **SNMP** interface.



SNMP

Enabled □

Port (1024~65535)

Trusted IP

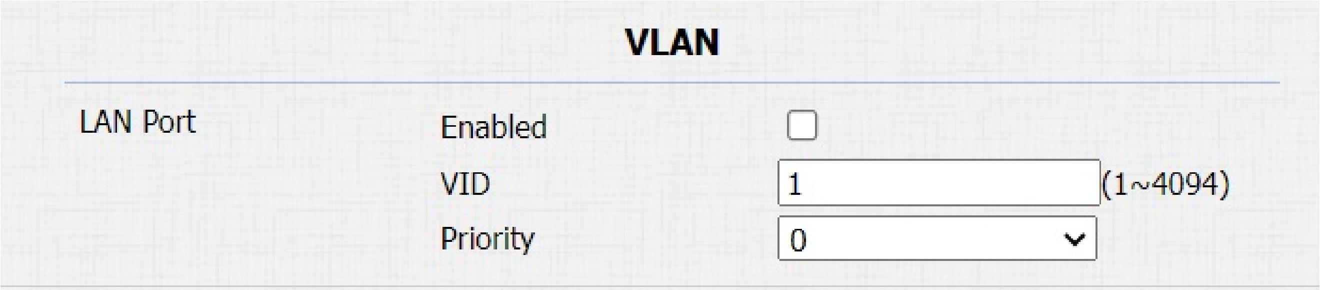
Parameter Set-up:

- **Port**: to configure the SNMP server’s port.
- **Trusted IP**: to configure allowed SNMP server address. It could be an IP address or any valid URL domain name.

VLAN Setting

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

To do the configuration on the web **Network > Advanced > VLAN** interface.



VLAN

LAN Port

Enabled □

VID 1 (1~4094)

Priority 0

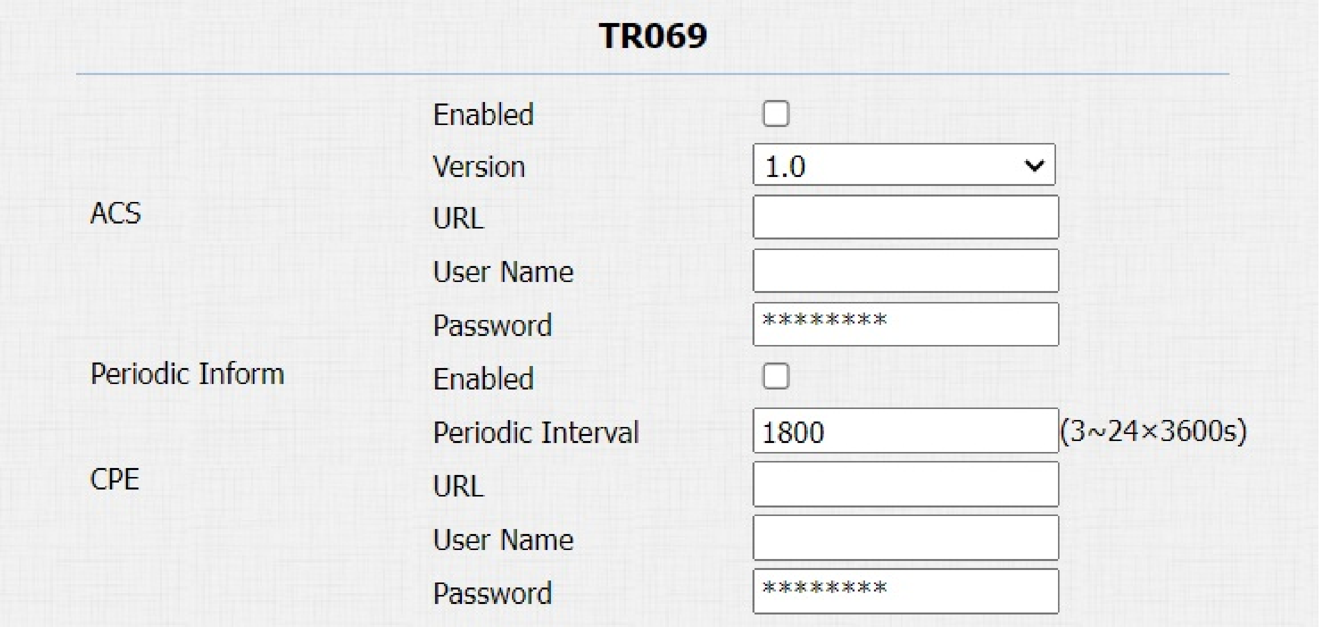
Parameter Set-up:

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

TR069 Setting

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

To do the configuration on the web **Network** > **Advanced** > **TR069** interface.



TR069

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

Parameter Set-up:

- **Version**: select supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE**: ACS is short for auto-configuration servers on the server side, and CPE is short for customer-premise equipment as client-side devices.
- **URL**: to configure URL address for ACS or CPE.
- **Periodic Interval**: to configure the interval for periodic notifications.

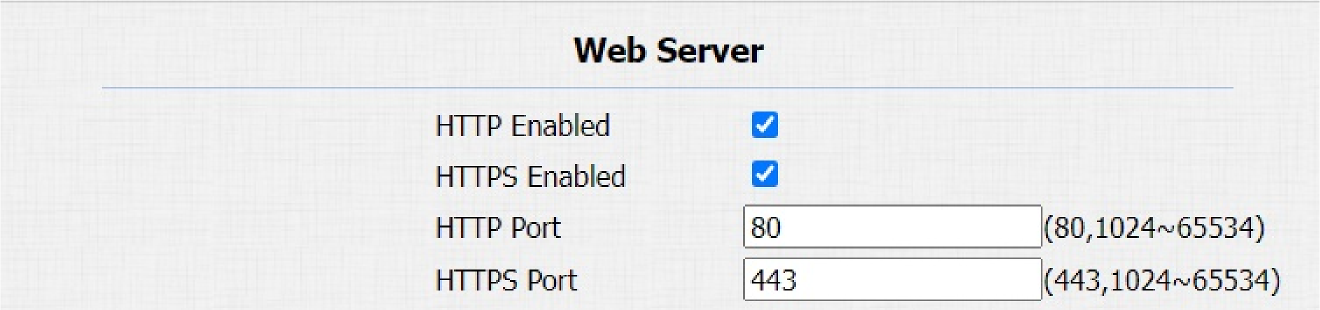
Note:

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

Device Web HTTP Setting

This function manages device website access. The door phone supports two remote access methods: HTTP and HTTPS (encryption).

To do this configuration on the web **Network > Advanced > Web Server** interface.



Web Server

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

Parameters Set-up:

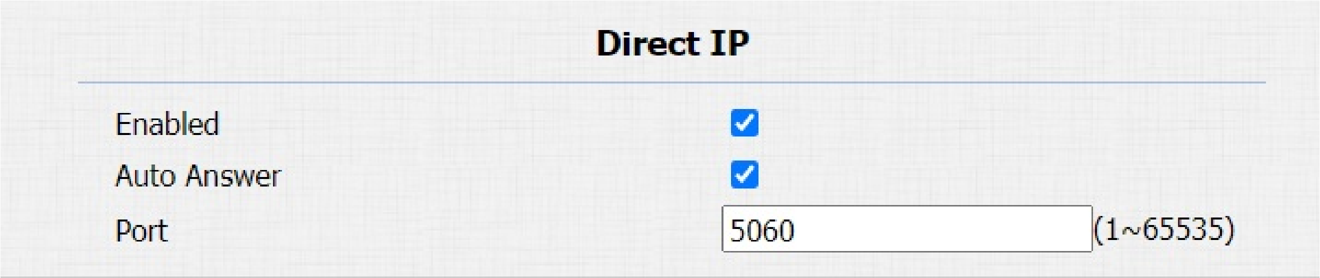
- **HTTP Port**: set up the port for HTTP access method. 80 is the default port.
- **HTTPS Port**: set up the port for HTTPS access method. 443 is the default port.

Intercom Call Configuration

IP Call & 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 on the same network.

To do this configuration on web **Phone > Call Feature > Direct IP** interface.



Direct IP

Enabled ☑

Auto Answer ☑

Port 5060 (1~65535)

Parameters Set-up:

- **Port**: set up the IP direct call port, 5060 is the default port.

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.

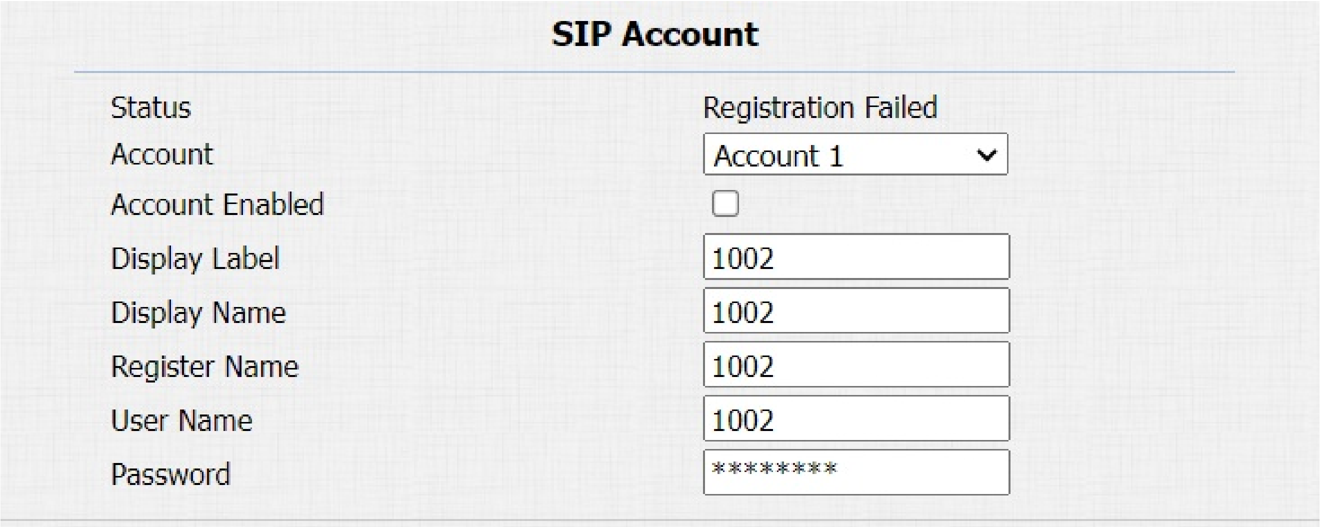
SIP Account Registration

Each device needs a SIP account to make and receive SIP calls.

Akuvox intercom devices support the configuration of two SIP accounts, which can be registered under two independent servers.

Configure SIP Account Configuration

To perform the SIP account setting on the Web **Account > Basic > SIP Account** Interface. The **User Name, Register Name**, and **Password** are provided from the SIP account administrator.



SIP Account

Status	Registration Failed
Account	Account 1
Account Enabled	□
Display Label	1002
Display Name	1002
Register Name	1002
User Name	1002
Password	********

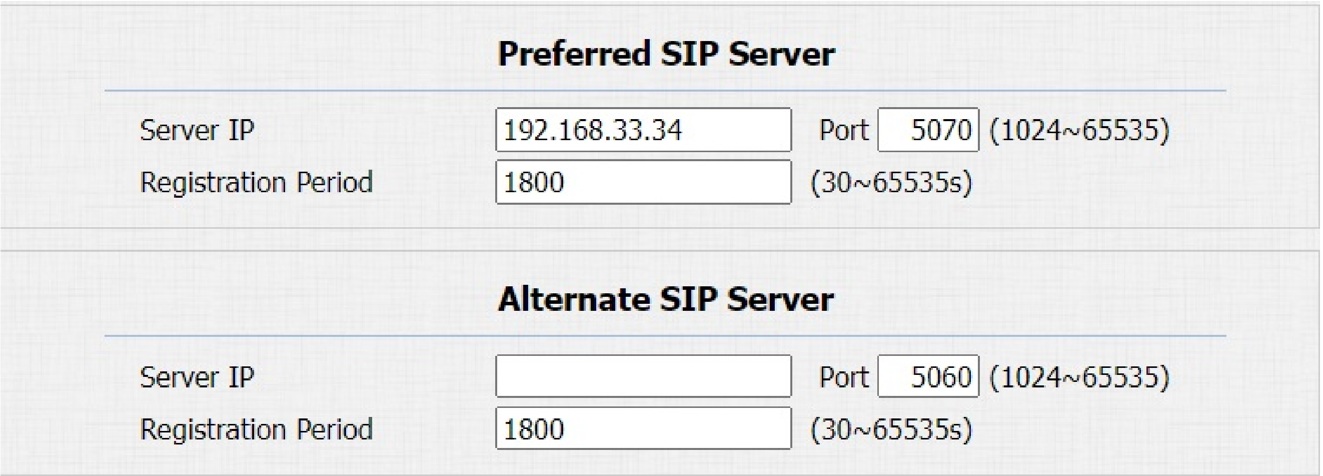
Parameter Set-up:

- **Status**: check to see if the SIP account is registered or not.
- **Display Name**: configure the name, for example, the device's name to be shown on the device being called to.
- **Account**: select the exact account (Account 1&2) to be configured.
- **Display Label**: configure the device label to be shown on the device screen.

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 in Akuvox indoor monitor.

To do this configuration also on web **Account > Basic > SIP Server** interface.



Preferred SIP Server

Server IP	192.168.33.34	Port	5070	(1024~65535)
Registration Period	1800	(30~65535s)		

Alternate SIP Server

Server IP		Port	5060	(1024~65535)
Registration Period	1800	(30~65535s)		

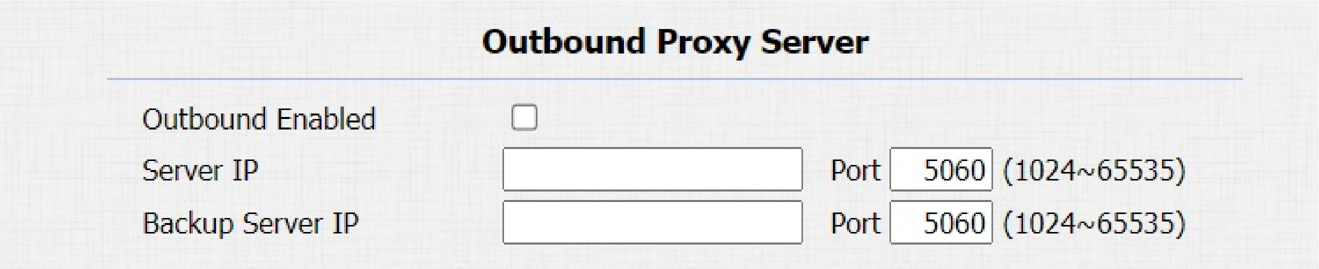
Parameter Set-up:

- **Server IP**: enter the primary server IP address number or its URL.
- **Server IP**: enter the backup SIP server IP address or its URL.
- **Port**: set up SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is **1800**, ranging from **30-65535s.**

Configure Outbound Proxy Server

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

To set it up on the device web **Account > Basic > Outbound Proxy Server** Interface.



Outbound Proxy Server

Outbound Enabled	☐			
Server IP		Port	5060	(1024~65535)
Backup Server IP		Port	5060	(1024~65535)

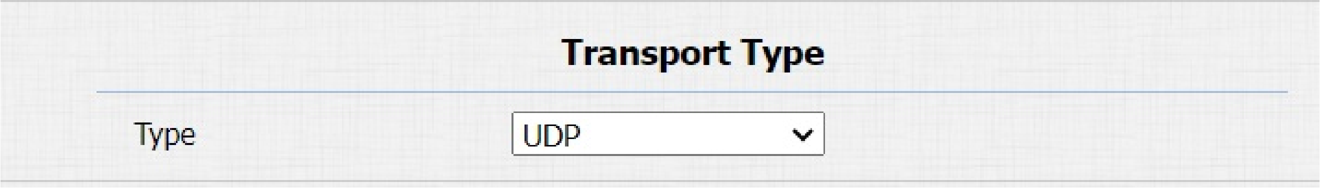
Parameter Set-up:

- **Server IP**: enter the SIP address of the primary outbound proxy server.
- **Port**: enter the Port number to establish a call session via the primary outbound proxy server.
- **Backup Server IP**: set up Backup Server IP for the backup outbound proxy server.
- **Port**: enter the port number for establishing call sessions via the backup outbound proxy server.

Configure Data Transmission Type

Akuvox intercom devices support four data transmission protocols: **User Datagram Protocol(UDP)**, **Transmission Control Protocol(TCP)**, **Transport Layer Security(TLS)**, and **DNS-SRV**.

To do this configuration on web **Account** > **Basic** > **Transport Type** interface.



Transport Type

Type: UDP

Parameter Set-up:

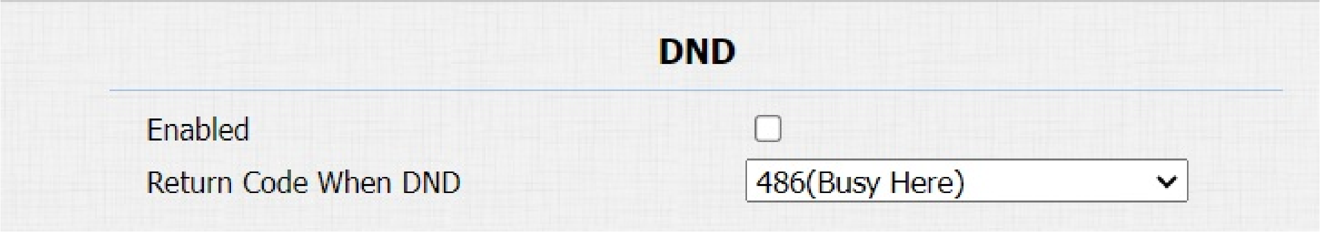
- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for a reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for secured and Reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain a DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

Configure Calling Feature

DND

The Do Not Disturb(**DND**) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

Go to **Phone** > **Call Feature** > **DND** interface.



DND

Enabled ☐

Return Code When DND: 486(Busy Here)

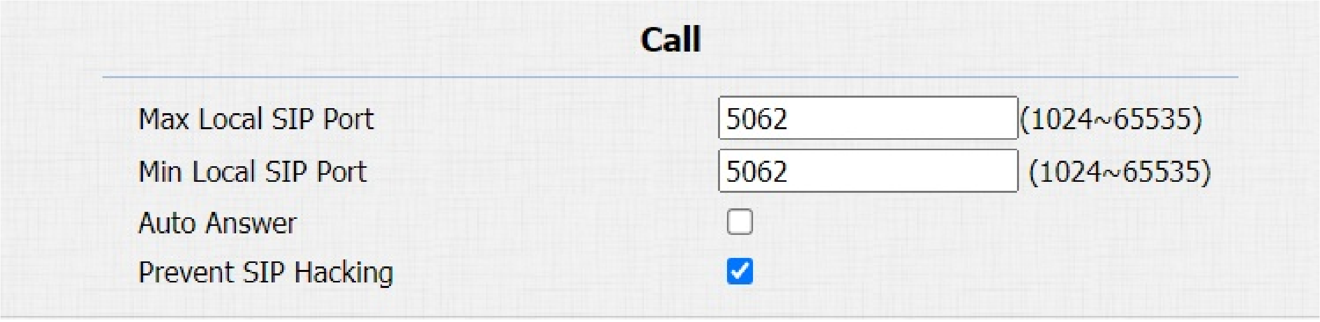
Parameter Set-up:

- **Return Code When DND**: select what code should be sent to the calling device via the SIP server. **404 for not found; 480 for temporary unavailable; 486 for busy here; 603 for decline.**

Enable Prevent SIP Hacking

Internet phone eavesdropping is a network attack that allows 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.

You can enable **Prevent SIP Hacking** if you only want to receive the calls made by the callers in your contact list. To enable it, go to **Account > Advanced > Call**.

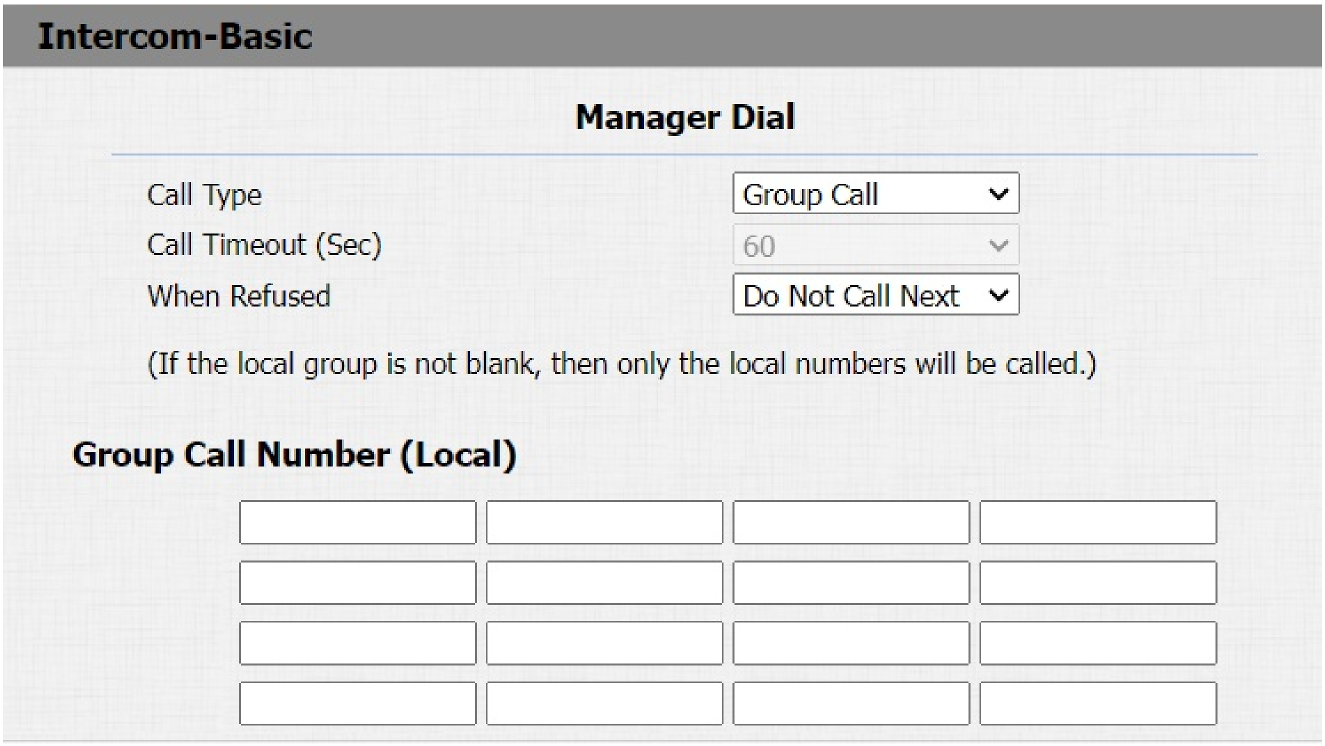


Call

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

Group Call

You can make calls to a group of numbers by pressing the on the device dial pad. To set the group call, go to **Intercom > Basic > Manager Dial**.



Intercom-Basic

Manager Dial

Call Type	Group Call
Call Timeout (Sec)	60
When Refused	Do Not Call Next

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

Group Call Number (Local)

Parameter Set-up:

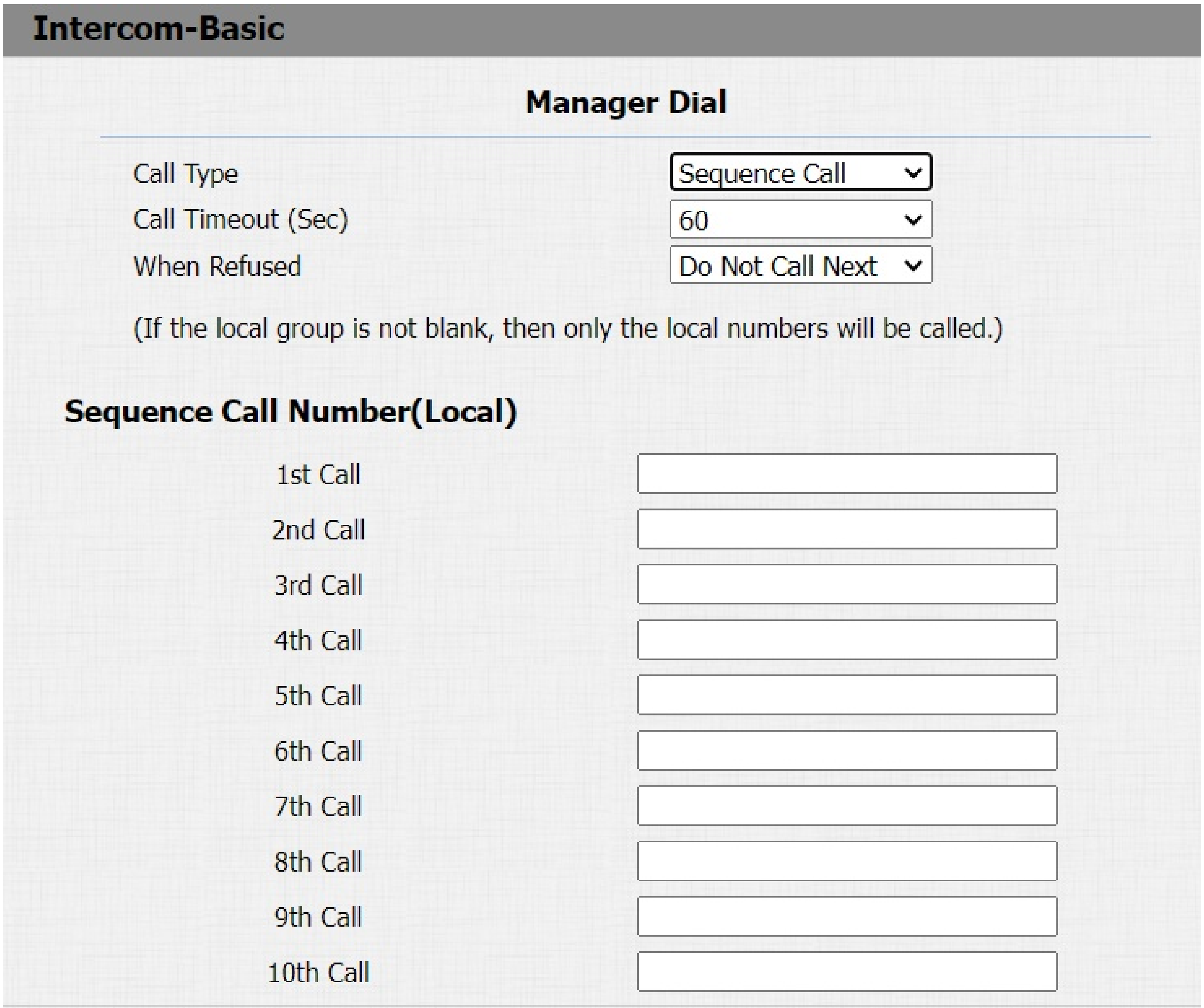
- **Call type**: select **Group Call**.
- **Group Call Number (Local)**: enter the group call number. If you fill in the local group call number, then the local group number will be called instead of the SmartPlus group call

number.

Sequence Call

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application.

To do the configuration on the web **Intercom > Basic > Manager Dial** interface.



Intercom-Basic

Manager Dial

Call Type	Sequence Call
Call Timeout (Sec)	60
When Refused	Do Not Call Next

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

Sequence Call Number(Local)

1st Call	
2nd Call	
3rd Call	
4th Call	
5th Call	
6th Call	
7th Call	
8th Call	
9th Call	
10th Call	

Parameters Set-up:

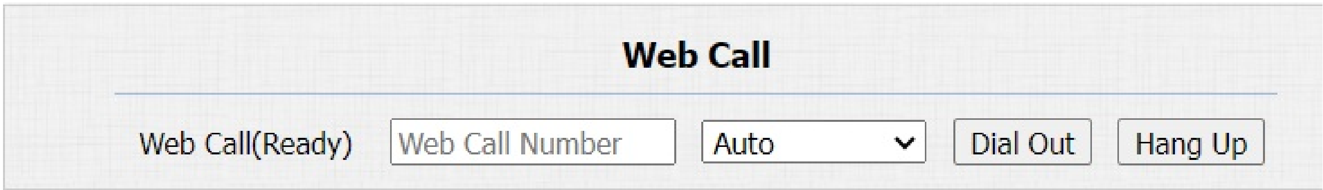
- **Call Type**: select **Sequence Call.**
- **Call Timeout (Sec)**: set the call timeout before calling the next called party when the first called party does not receive the call within the timeout.
- **When Refused**: if you select **Do Not Call Next**, then the sequence call will be terminated

if the call is rejected by the called party. If you select **Call Next**, then the sequence call will be continued to the next called party if it is rejected by the first called party.

Web Call

The web call feature allows for making calls via the device’s web interface, commonly used for remote call testing purposes.

To do the configuration on the web **Intercom** > **Basic** > **Web Call** interface.



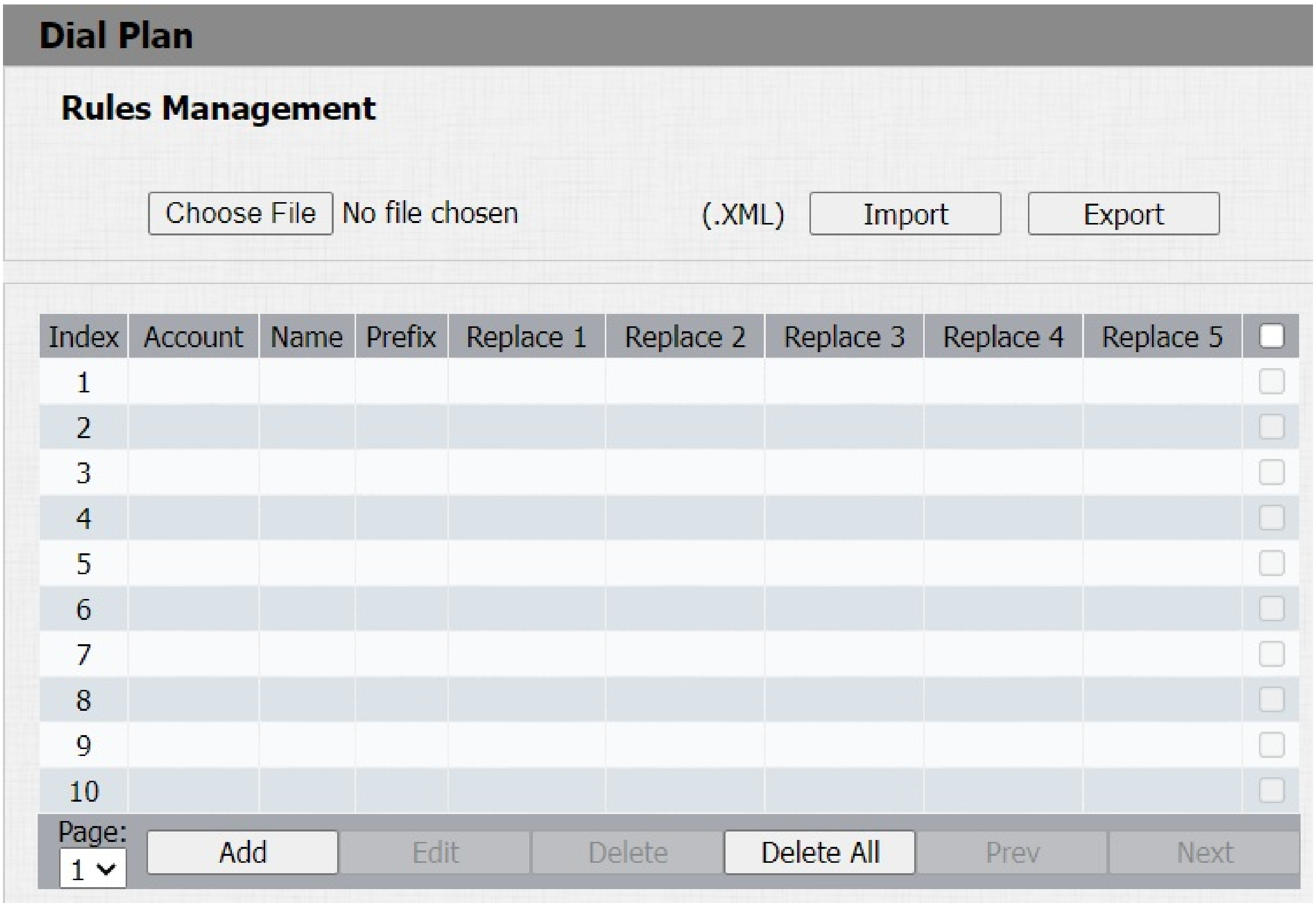
Parameters Set-up:

- **Auto/Account1/Account2**: to choose a suitable SIP account to make a web call. If you call using an IP address, account selection is not needed here.

Dial Plan

The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

To configure the number replacement on the device, navigate to **Phone > Dial Plan**, then click **Add**. To replace the number in batch, you can import the .xml file to the door phone. And the file from the door phone can be exported out before importing them to other door phones.



Dial Plan

Rules Management

Choose File No file chosen (.XML) Import Export

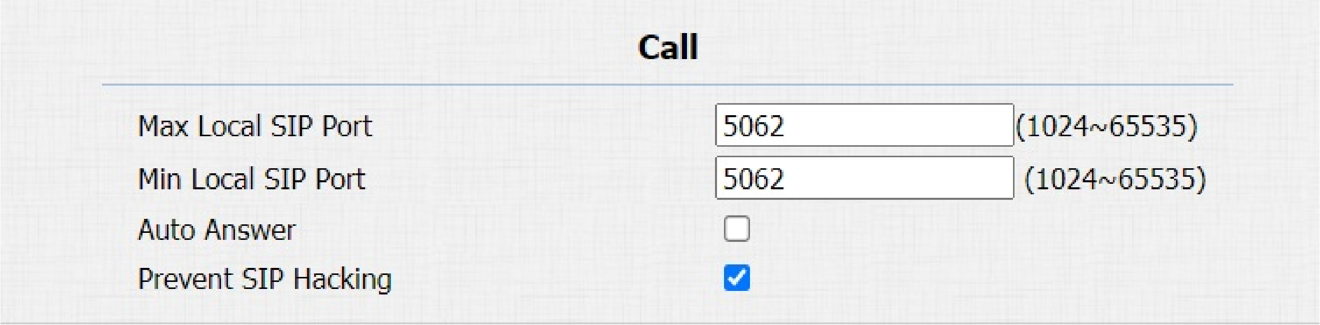
Index	Account	Name	Prefix	Replace 1	Replace 2	Replace 3	Replace 4	Replace 5	☐
1									☐
2									☐
3									☐
4									☐
5									☐
6									☐
7									☐
8									☐
9									☐
10									☐

Page: 1 Add Edit Delete Delete All Prev Next

Auto Answer

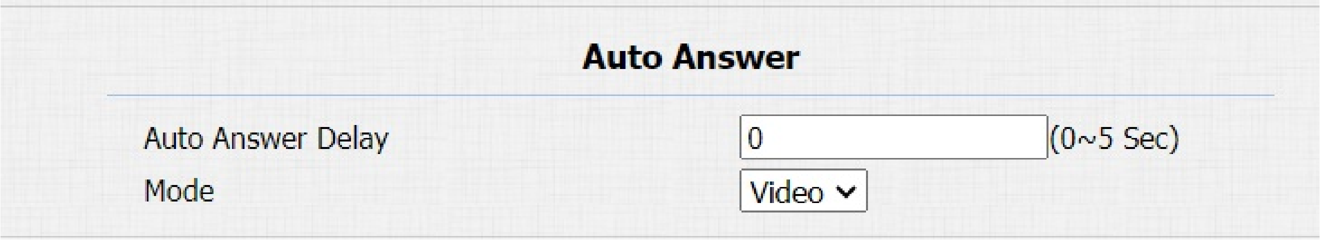
Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To enable this feature on web **Account > Advanced > Call** interface, you can set up the related parameters on web **Phone > Call Feature> Auto Answer**.



Call

Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)
Auto Answer	☐	
Prevent SIP Hacking	☑	



Auto Answer

Auto Answer Delay: 0 (0~5 Sec)

Mode: Video

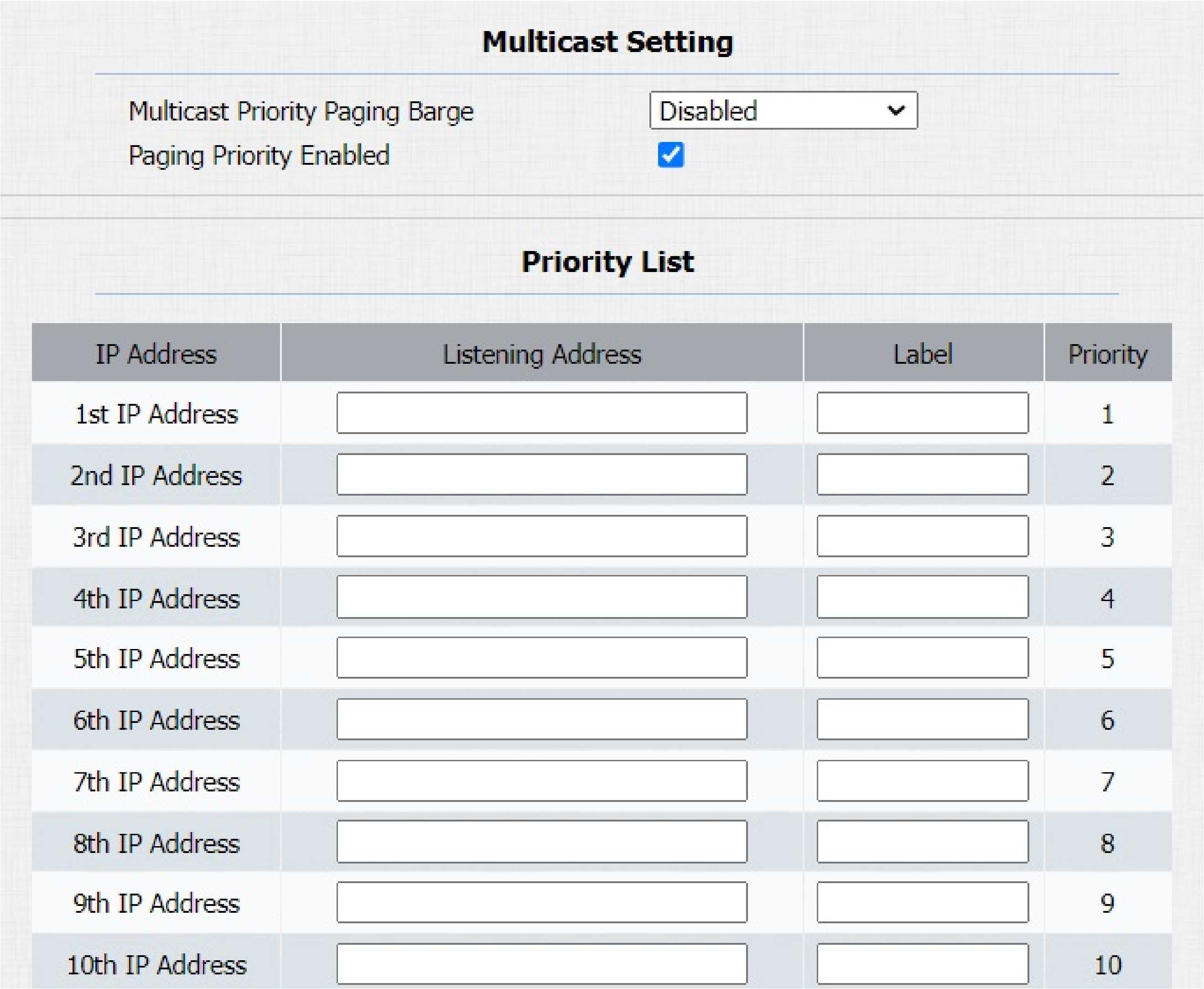
Parameters Set-up:

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

Multicast

The Multicast function allows one-to-many broadcasting for different purposes. For example, it enables the indoor monitor to announce messages from the kitchen to other rooms, or to broadcast notifications from the management office to multiple locations. In these scenarios, indoor monitors can either listen to or send audio broadcasts.

To do the configuration on the web **Phone > Multicast** interface.



Multicast Setting

Multicast Priority Paging Barge: Disabled

Paging Priority Enabled: ☑

Priority List

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

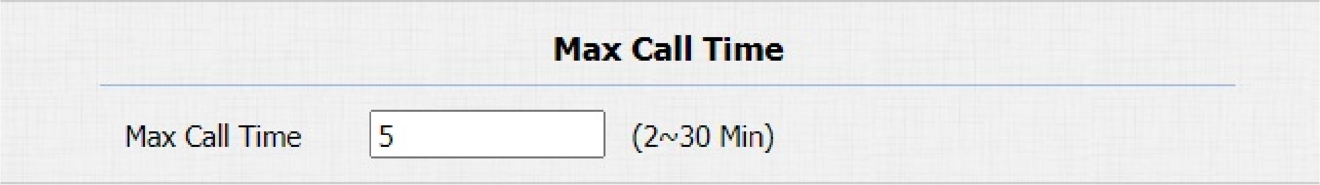
Parameters Set-up:

- **Multicast Priority Paging Barge**: multicast or how many multicast calls are higher priority than SIP calls, if you disable Paging Priority Active, SIP calls will have high priority.
- **Paging Priority Enabled**: multicast calls are called in order of priority or not.
- **Listening Address**: enter the multicast IP address you want to listen to. The multicast IP address needs to be the same as the listened part and the multicast port can not be the same for each IP address. Multicast IP address is from 224.0.0.0 to 239.255.255.255.
- **Label**: enter the label for each listening address.

Configure Maximum Call Duration

The door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the call automatically.

To do this configuration on the web **Intercom > Basic > Max Call Time** interface.



Max Call Time

Max Call Time: 5 (2~30 Min)

Parameters Set-up:

- **Max Call Time**: enter the call time duration according to your need (ranging from 0-120 min). The default call time duration is 5 min.

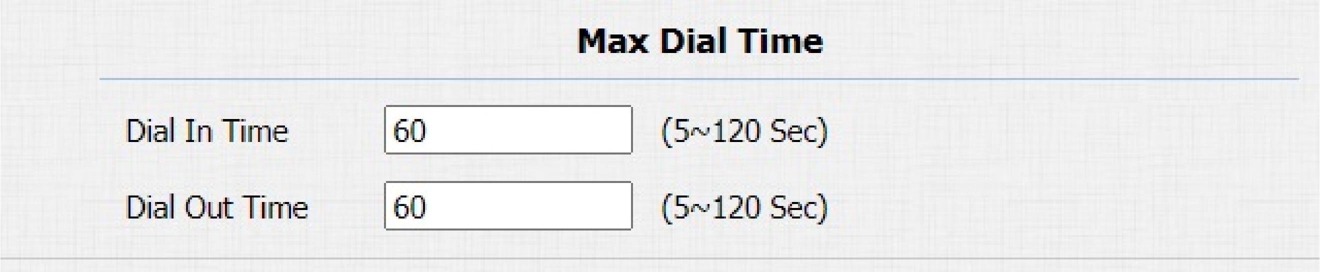
Note:

- Max call time of the device is also related to the max call time of the SIP If using a SIP account to make a call, please pay attention to the max call time of the SIP server. If the max call time of the SIP server is shorter than the max call time of the device, the shorter one is available.

Maximum Dial Duration

Maximum Dial Duration is the time limit for incoming- and/or outgoing calls on the door phone. If configured, the door phone will automatically terminate the call if no one answers the call within the preset time, whether it is incoming or outgoing.

To do this configuration, go to **Intercom > Basic > Max Dial Time** interface.



Max Dial Time

Dial In Time: 60 (5~120 Sec)

Dial Out Time: 60 (5~120 Sec)

Parameters Set-up:

- **Dial in Time**: enter the dial-in time duration for your door phone (ranging from 5-120 sec). For example, if you set the dial-in time duration as 60 seconds on your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial-in time duration by default.

- **Dial out Time**: enter the dial-in time duration for your door phone (ranging from 5-120 sec). For example, if you set the dial-out time duration as 60 seconds on your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answered by the device being called.

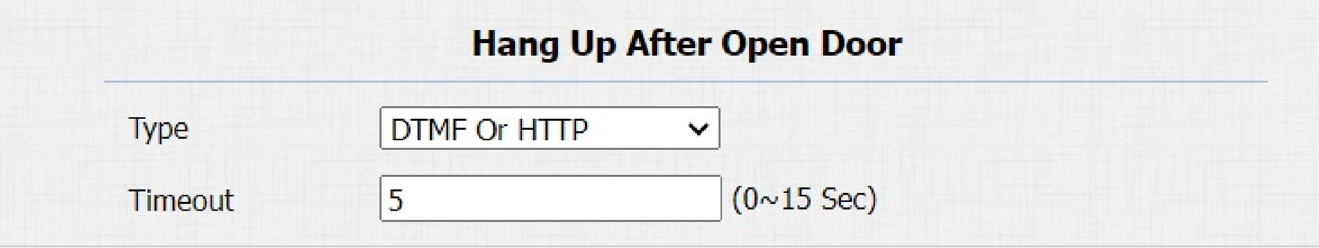
Note

- Max dial time of device is also related with max dial time of SIP server. If using SIP account to make a call, please pay attention to the max dial time of SIP server. If the max dial time of SIP server is shorter than the max dial time of device, the shorter one is available.

Hang Up After Open Door

This feature automatically ends the call once the door is released, allowing for the seamless reception of subsequent calls.

To do this configuration on the web **Intercom > Basic> Hang Up After Open Door.**



Hang Up After Open Door

Type: DTMF Or HTTP

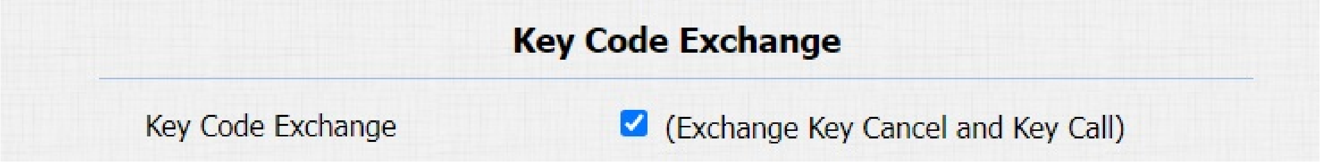
Timeout: 5 (0~15 Sec)

Parameter Set-up:

- **Type**: select the open door type. The door can be unlocked via the **DTMF, HTTP Command, DTMF or HTTP**, and **Input, DTMF, or HTTP**.
- **Timeout**: set up from 1 second to 15 seconds. 5 seconds is the default. If you set it 5 seconds, then the call will be hung up 5 seconds after the door is opened. If you want to disable the feature, set the timeout as 0.

Switch Cancel Key &Dial Key

On R28 door phones, the **Cancel** Keys and **Dial** keys can be different in their positions functionally and physically. Either the **Cancel** key is right on the top of the **Dial** key or the other way round. You can reverse their functional positions on the web to match their physical position on the keypad. On the web, navigate to **Intercom** > **Advanced** > **Key Code Exchange**.



Key Code Exchange

Key Code Exchange ☑ (Exchange Key Cancel and Key Call)

Parameter Set-up:

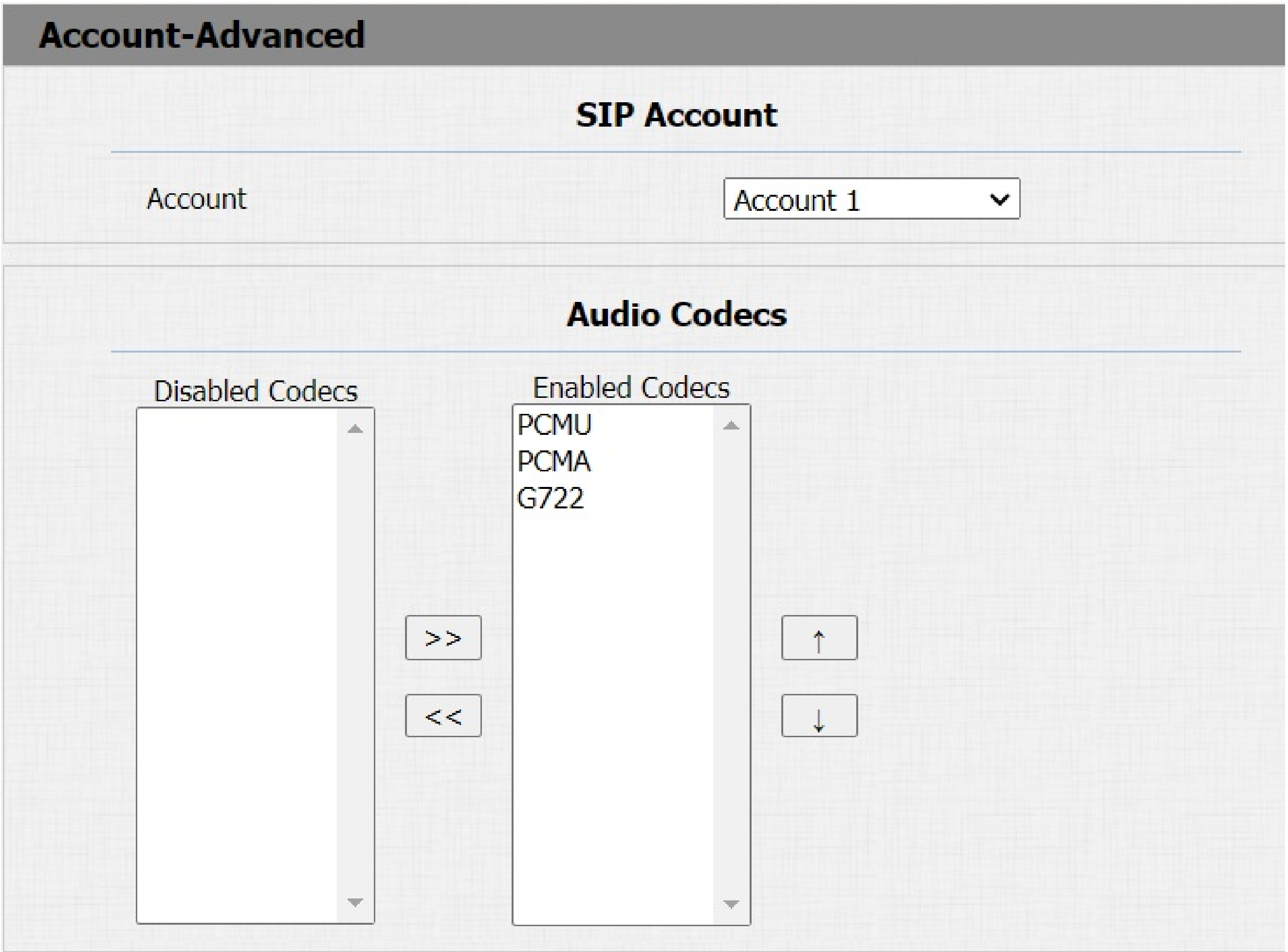
- **Key Code Exchange**: if enabled, the **Cancel** function will be placed right on the top of the **Dial** function in their functional location. If disabled, their functional location will be functionally reversed.

Audio & Video Codec Configuration

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 actual network environment.

To do the configuration on device web **Account** > **Advanced** interface.



Account-Advanced

SIP Account

Account: Account 1

Audio Codecs

Disabled Codecs

Enabled Codecs
PCMU
PCMA
G722

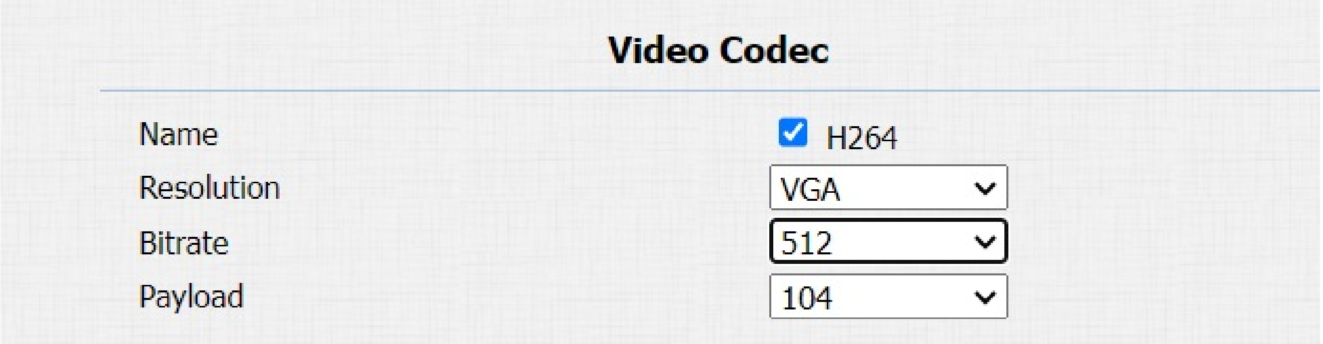
Please refer to the bandwidth consumption and sample rate for the four codecs types below:

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

Video Codec Configuration

The door phone supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

To set up video codec on web **Account** > **Advanced** interface.



Video Codec

Name ☑ H264

Resolution VGA

Bitrate 512

Payload 104

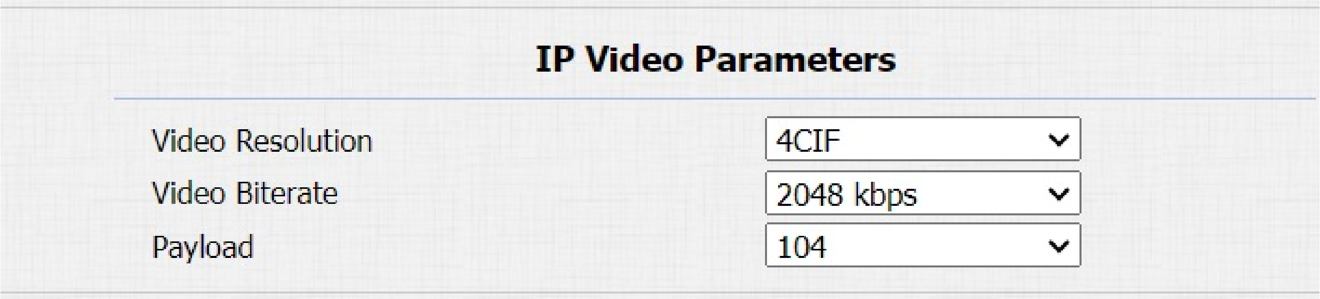
Parameter Set-up:

- **Name**: check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Resolution**: select the code resolution for the video quality among four options: **CIF, VGA, 4CIF, and 720P** according to your actual network environment. The default code resolution is **4CIF**.
- **Bitrate**: select the video stream bit rate (ranging from **128-2048**). The greater the bit rate is, the larger the data transmitted every second in amount. Therefore the video will be clearer. While the default code bit rate is 2048.
- **Payload**: select the payload type (ranging from **90-119**) to configure the audio/video configuration file. The default payload is 104.

Video Codec Configuration for IP Direct Calls

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

To do so, you can go to **Phone** > **Call Feature** > **IP Video Parameters**.



IP Video Parameters

Video Resolution	4CIF
Video Biterate	2048 kbps
Payload	104

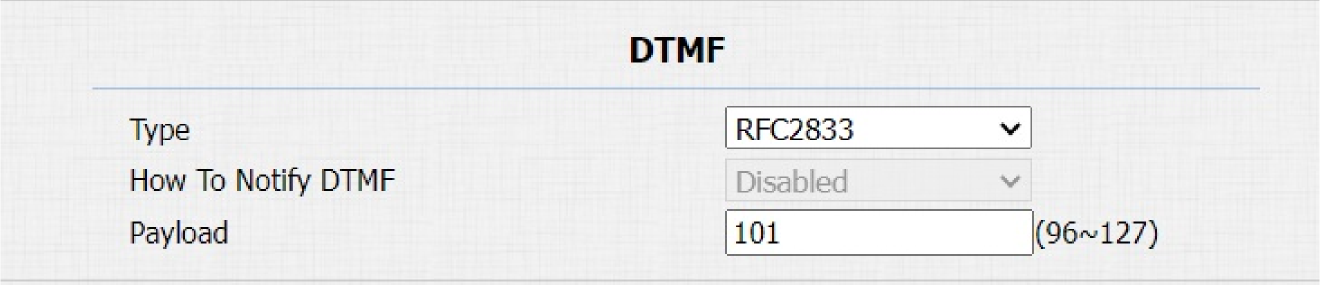
Parameter Set-up:

- **Video Resolution**: select the code resolution for the video quality among four options: **CIF, VGA, 4CIF**, and **720P**. The default code resolution is 4CIF.
- **Video Bitrate**: select video bit rate among six options: **64 kbps, 128kbps, 256kbps, 512 kbps, 1024 kbps, and 2048 kbps** according to your network environment. The default video bit rate is **2048 kpbs**.
- **Video Payload**: select the payload type (ranging from **90-119**) to configure the audio/ video configuration file. The default payload is 104.

Configure DTMF Data Transmission

In order to achieve door access via DTMF code or some other applications, you are required to properly configure DTMF in order to establish a DTMF-based data transmission between the door phone and other intercom devices for third-party integration.

Go to **Account** > **Advanced** > **DTMF** interface.



DTMF

Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)

Parameter Set-up:

- **Type**: select DTMF mode among six options: **Inband, RFC2833, Info+Inband, Info, Info+Inband+RFC2833**, and **Info+RFC2833** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: select among four types: **Disable, DTMF, DTMF-Relay**, and **Telephone-Event** according to the specific type adopted by the third party device. You

are required to set it up only when the third party device is to be matched with adopts such modes: **Info, Info+Inband, Info+RFC2833**, and **Info +Inband + RFC2833.**

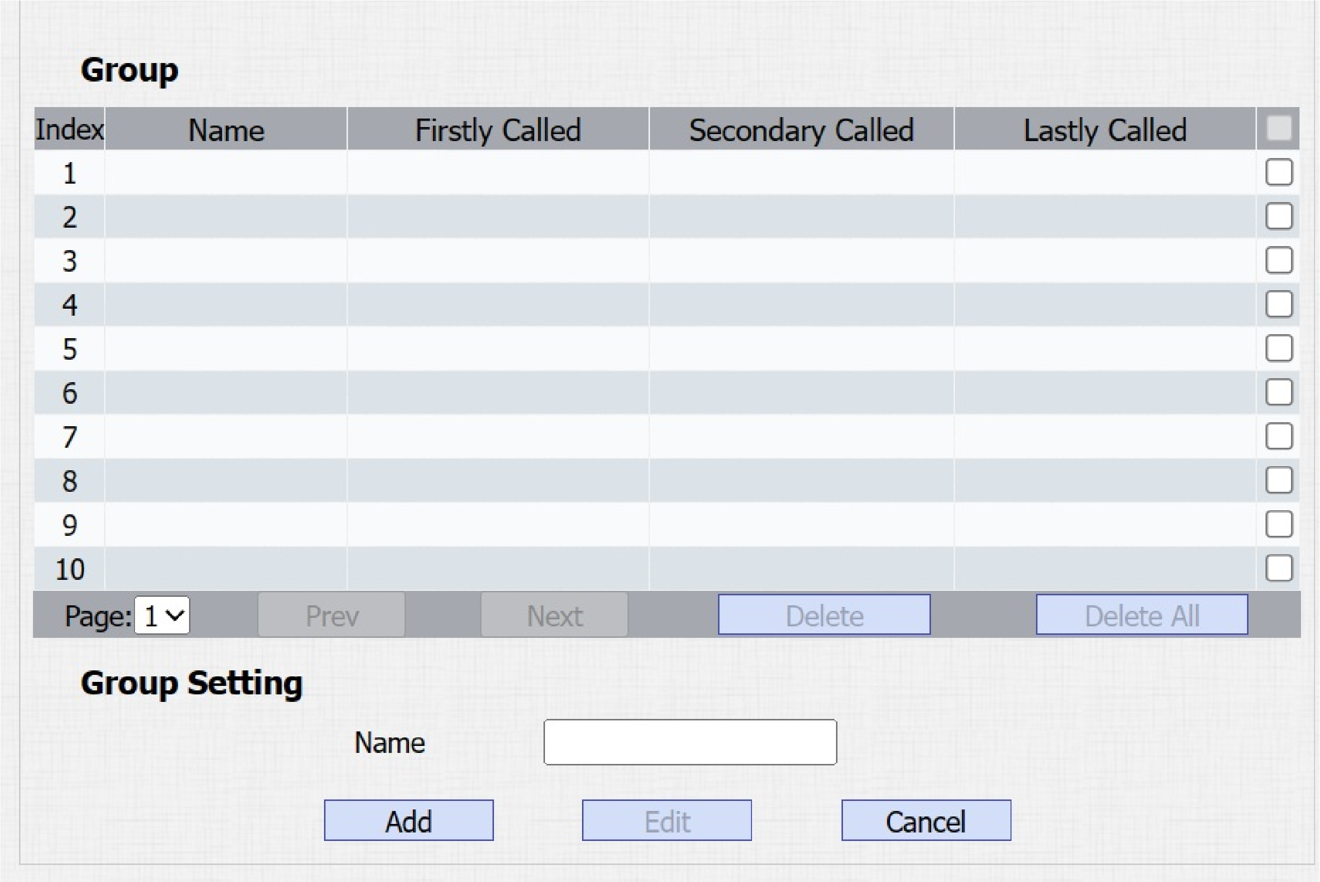
- **DTMF Payload**: set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

Contact List Configuration

Managing Contact Group

You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

Navigate to **Contacts > Contacts List > Group**.



Group

Index	Name	Firstly Called	Secondary Called	Lastly Called	□
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□
9					□
10					□

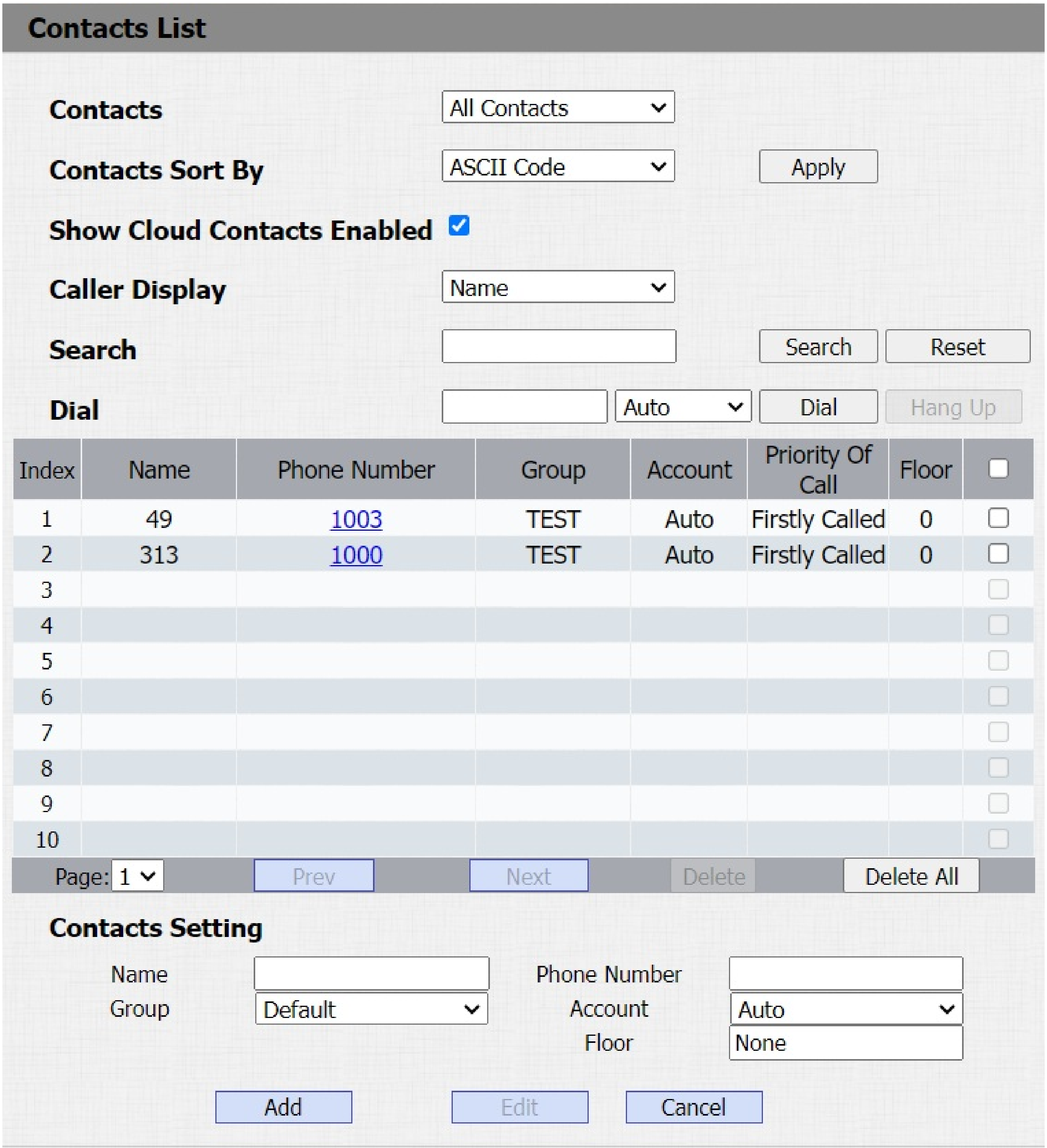
Page: 1

Group Setting

Name

Managing Contacts

You can search, create, display, edit and delete the contacts in your phone book. **Contacts > Contact List.**



Contacts List

Contacts	All Contacts	
Contacts Sort By	ASCII Code	
Show Cloud Contacts Enabled	☑	
Caller Display	Name	
Search		
Dial		Auto

Index	Name	Phone Number	Group	Account	Priority Of Call	Floor	□
1	49	1003	TEST	Auto	Firstly Called	0	□
2	313	1000	TEST	Auto	Firstly Called	0	□
3							□
4							□
5							□
6							□
7							□
8							□
9							□
10							□

Page: 1

Contacts Setting

Name		Phone Number	
Group	Default	Account	Auto
		Floor	None

Parameters Set-up:

- **Contact**: you can choose to show all contact information or one group's contact information.
- **Contacts Short By**: there are three options **ASCII Code, Room Number**, and **Import**. If **ASCII Code** is selected, sort in ascending ASCII order, for example, 0-9, a-z, numbers take precedence over letters. Not case sensitive, but the same letter, lowercase

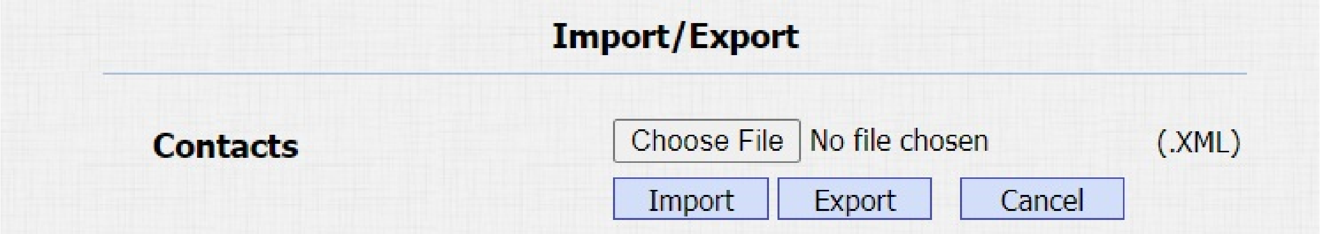
is sorted before uppercase. If **Room Number** is selected, sort by room name. If there is no room name, the room number is taken as the room name by default. The room number is available after enabling Cloud contact. If **Import** is selected, sort by contacts in the imported file.

- **Search**: enter the key number or key letter of the name to quickly search the contact.
- **Dial**: enter a phone number, then click **Dial** to initiate the call from the web.
- **Group**: select the group name you have created. You cannot select the group name if no group name has been created.
- **Account**: select which SIP account will be used to call out. If using IP direct call, it is not available.
- **Priority of Call**: up to 3 numbers in one group and set up the call sequence for these numbers.

Export/Import Contacts

When the contact becomes so many that you cannot afford to manage each contact one by one manually, you can import and export the contacts in batch on the device web.

You can go to **Contacts > Contacts List > Import/Export**.



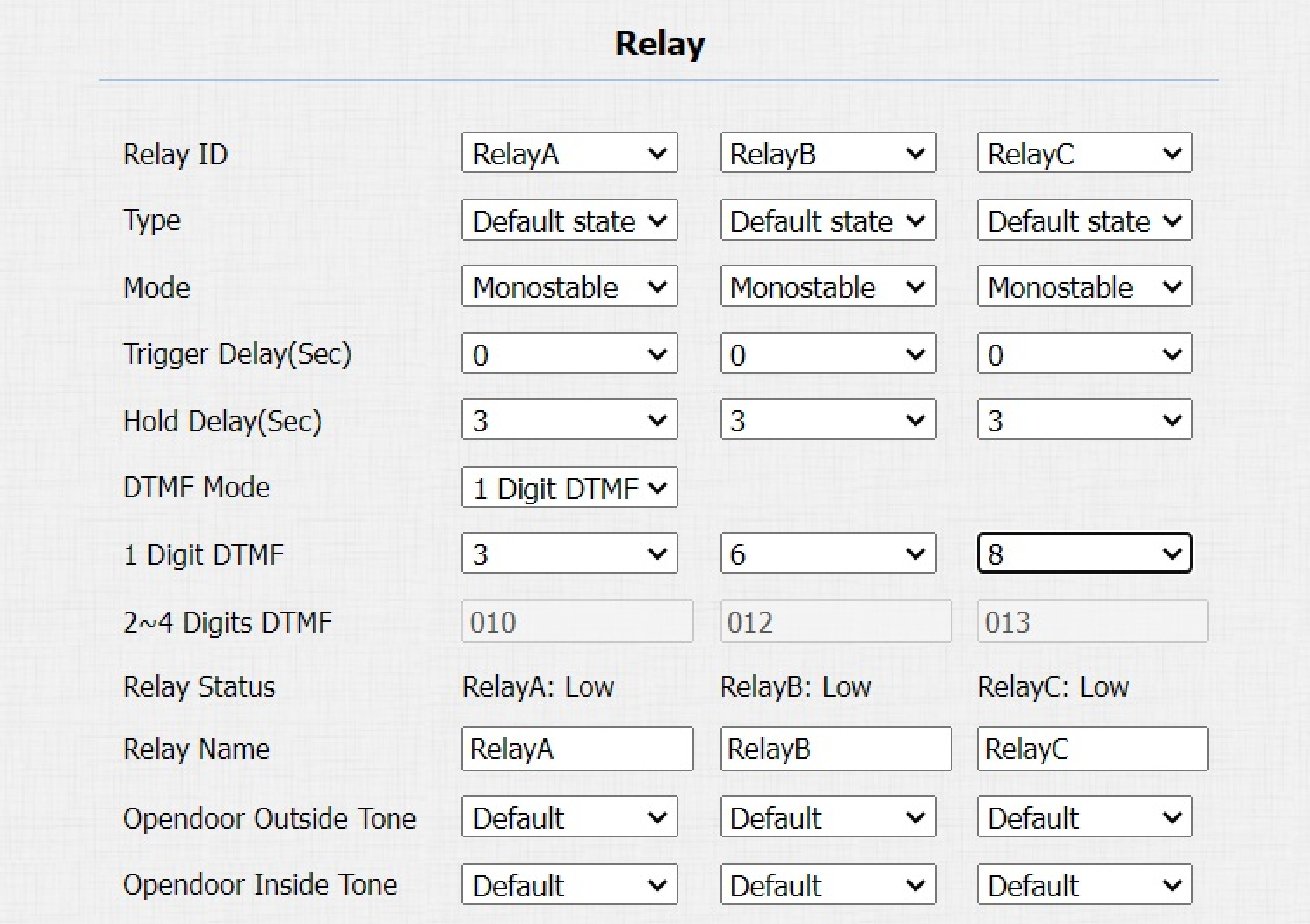
Import/Export

Contacts Choose File No file chosen (.XML)

Relay Setting

Relay Switch Setting

You can configure the relay switch(es) and DTMF for the door access on the web **Intercom > Relay** interface.



Relay

Relay ID	RelayA	RelayB	RelayC
Type	Default state	Default state	Default state
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	3	3	3
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	3	6	8
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	RelayA	RelayB	RelayC
Opendoor Outside Tone	Default	Default	Default
Opendoor Inside Tone	Default	Default	Default

Parameter Set-up:

- **Trigger Delay (Sec)**: set the relay trigger delay timing (ranging from 1-10 Sec). For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press **unlock** tab.
- **Hold Delay (Sec)**: set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. then the relay will stay triggered for 5 seconds after the door is opened. It means the door will stay open for 5 seconds.
- **DTMF Mode**: select the number of DTMF digits for the door access control (ranging from 1-4 digits). For example, you can select a 1-digit DTMF code or 2-digit DTMF code, etc., according to your need.

- **1-digt DTMF**: set the 1-digt DTMF code within range from (**0-9 and *, #**).
- **2~4 Digits DTMF**: set the DTMF code according to the **DMTP Option** For example, you are required to set the 3-digits DTMF code if DTMP Mode is set as 3-digits.
- **Relay Status**: relay status is low by default which means **Normally Closed** (NC). If the relay status is high, then it is in **Normally Open** status (NO).
- **Relay Name**: name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note:

- Only the external devices connected to the relay switch need to be powered by power adapters as the relay switch does not supply power.

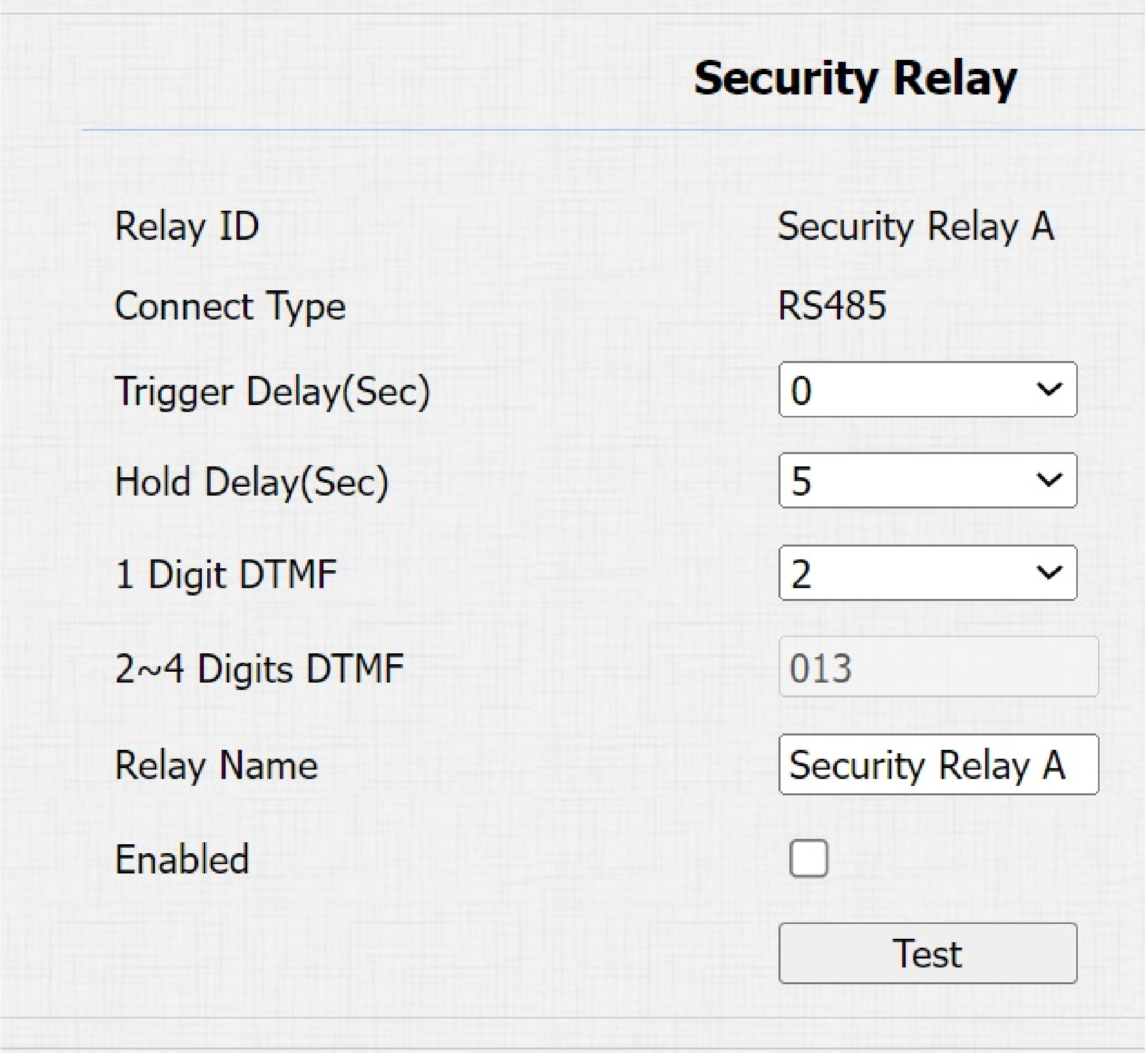
Note:

- If DTMF mode is set as **1 Digit DTMF**, you cannot edit DTMF code in 2~4 Digits DTMF. And if you set DTMF mode from 2-4 in the **2~4 Digits DTMF** field, you can not edit the DTMF code in the **1 Digit DTMF** field.

Security Relay Setting

The Security Relay, known as Akuvox SR01, is a product designed to bolster access security by preventing unauthorized forced entry attempts. Installed inside the door, it directly governs the door opening mechanism, ensuring that the door remains secure even in the event of damage to the device.

To set up the security relay, navigate to **Intercom > Relay > Security Relay.**



Security Relay

Relay ID	Security Relay A
Connect Type	RS485
Trigger Delay(Sec)	0
Hold Delay(Sec)	5
1 Digit DTMF	2
2~4 Digits DTMF	013
Relay Name	Security Relay A
Enabled	□

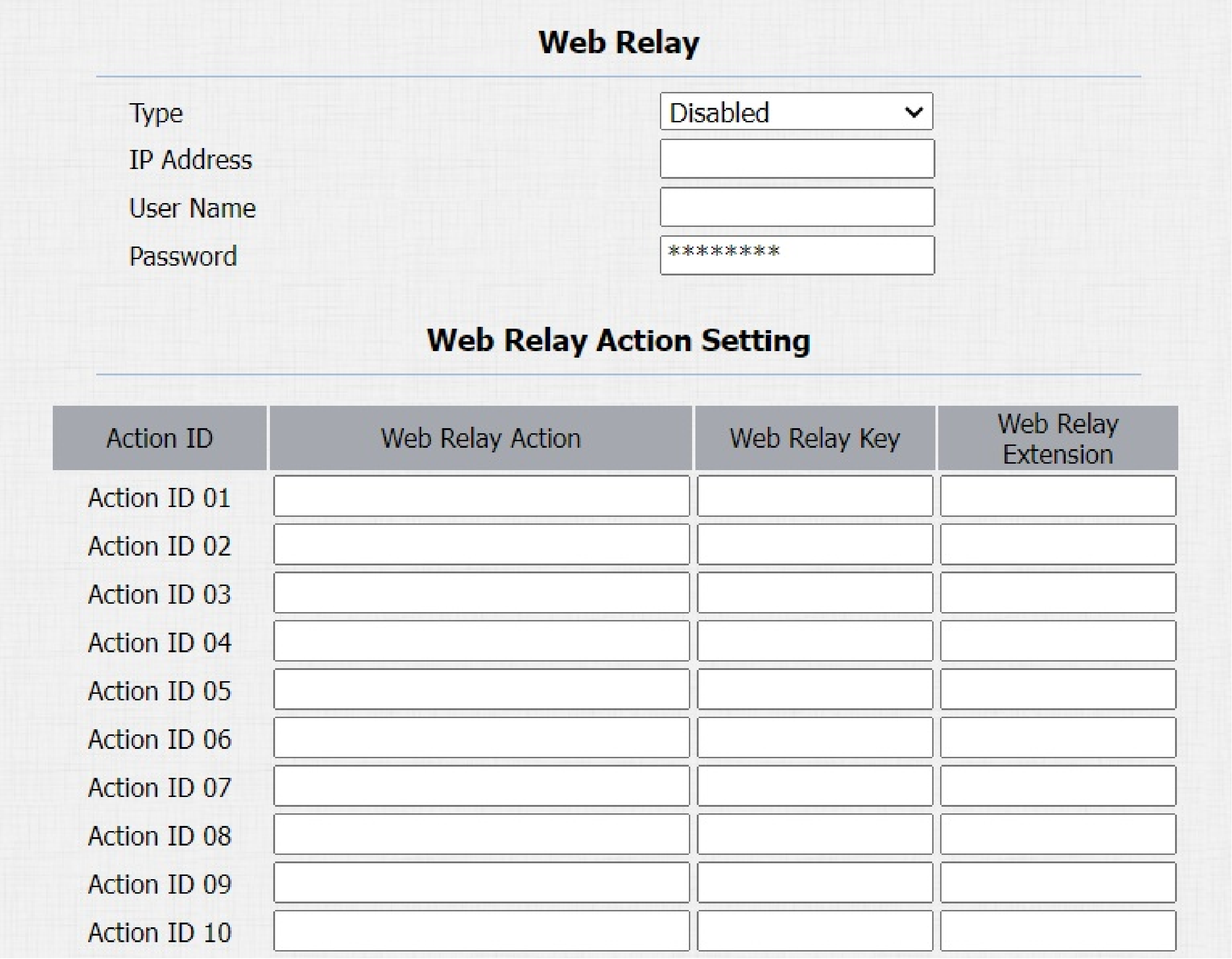
Parameter Set-up:

- **Connect Type**: select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Trigger Delay (Sec)**: set the relay trigger delay timing (ranging from 1-10 Sec.) For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press Unlock tab. The default is 0 meaning triggering relay right after you press the unlock tab.
- **Hold Delay (Sec)**: set the relay hold delay timing (ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. then the relay will be delayed for 5 after the door is unlocked.
- **1 Digit DTMF**: set the 1 digit DTMF code within range from (0-9 and *,#).
- **2~4 Digits DTMF**: set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digit DTMF code if DTMP Mode is set as 3- digits.
- **Relay Name**: give a name to the relay if needed. And relay name can be edited on the SmartPlus cloud and SDMC.

Web Relay Setting

A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.

Web relay needs to be set up on the web **Phone > Web Relay** interface. IP address, Username, and Password are provided by the web relay manufacturer.



Web Relay

Type	Disabled
IP Address	
User Name	
Password	*********

Web Relay Action Setting

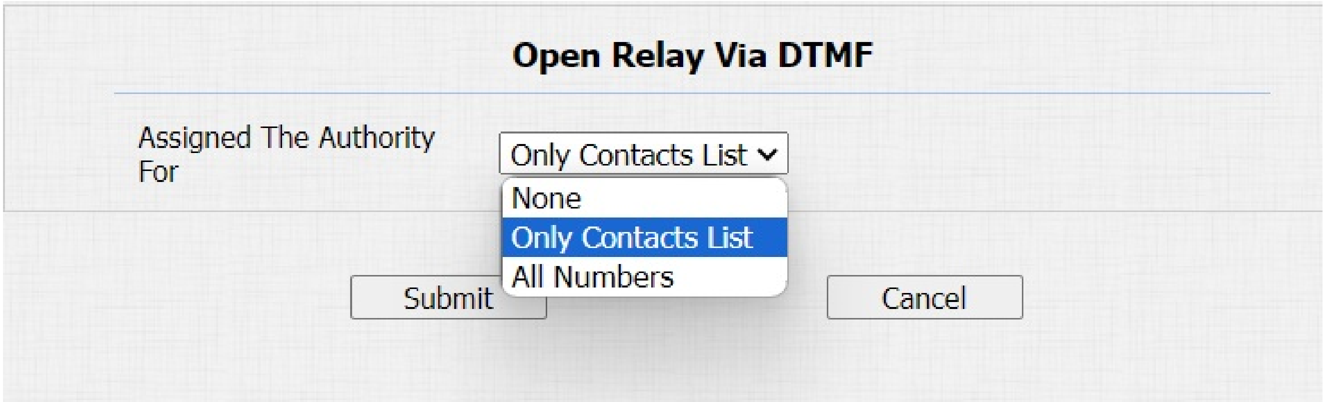
Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01			
Action ID 02			
Action ID 03			
Action ID 04			
Action ID 05			
Action ID 06			
Action ID 07			
Action ID 08			
Action ID 09			
Action ID 10			

Parameter Set-up:

- **Type**: select among three options **Disabled, Web Relay**, and **Both**. Select **Web relay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.
- **Password**: The passwords are authenticated via HTTP and you can define the passwords using http get in Action.
- **Web Relay Action**: enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without adding IP, username, pwd, you can fill in the HTTP command in the web relay action, so you can configure multiple web relays.
- **Web Relay Key**: it can be null or enter the configured DTMF code, when the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.

Configure White List for Door Relay

In order to secure the door access via DTMF codes, you can set up the DTMF whitelist on the device web **Intercom > Relay > Open Relay Via DTMF** interface so that only the caller numbers you designated in the door phone can use the DTMF code to gain door access.



Open Relay Via DTMF

Assigned The Authority For: Only Contacts List

Parameter Set-up:

- **Assigned The Authority For**: select **All numbers** to allow all numbers for the DTMF door unlock; select **None** to deny all numbers for the DTMF door unlock; select **Only Contact List** to only allow the contact number in your door phone.

Door Access Schedule Management

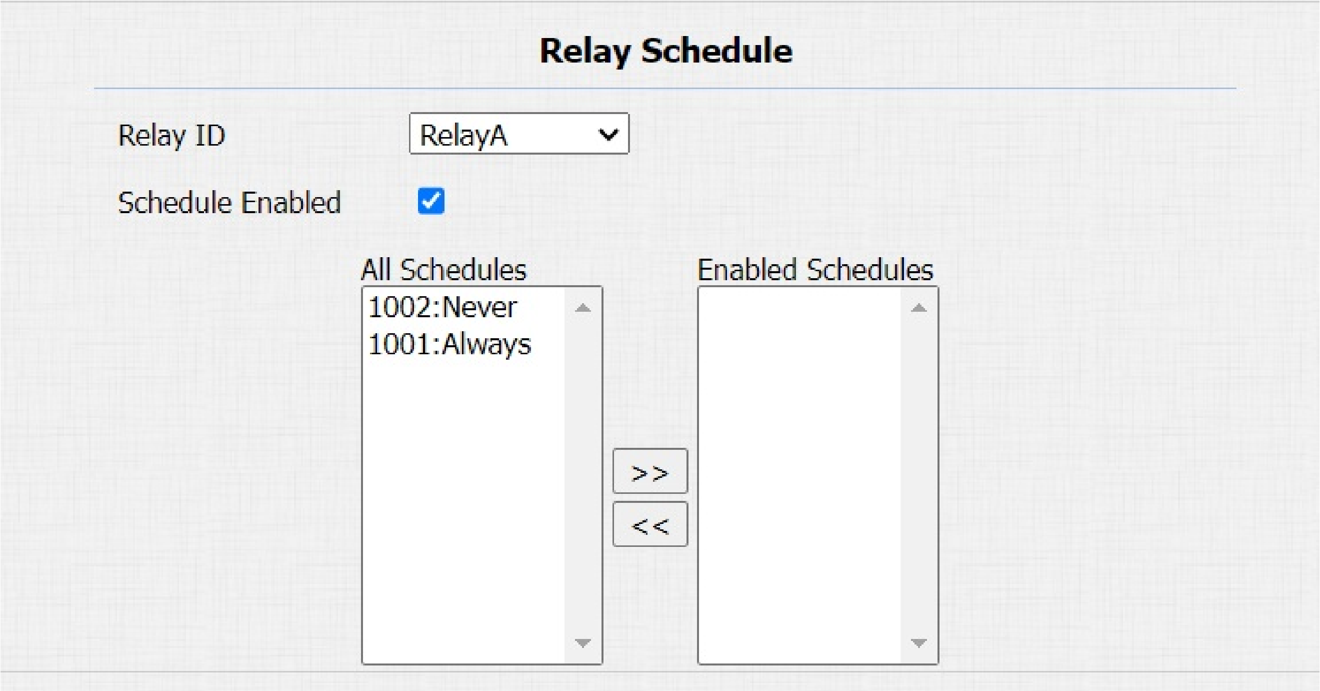
Configure Door Access Schedule

A door access schedule lets you 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.

Manage Relay Schedule

The relay schedule allows you to set a specific relay to always open at a certain time. This is helpful for situations like keeping the gate open after school or keeping the door open during work hours.

To do the configuration on the web **Intercom** > **Relay** > **Relay Schedule** interface.



Relay Schedule

Relay ID: RelayA

Schedule Enabled: ☑

All Schedules:
1002:Never
1001:Always

Enabled Schedules:

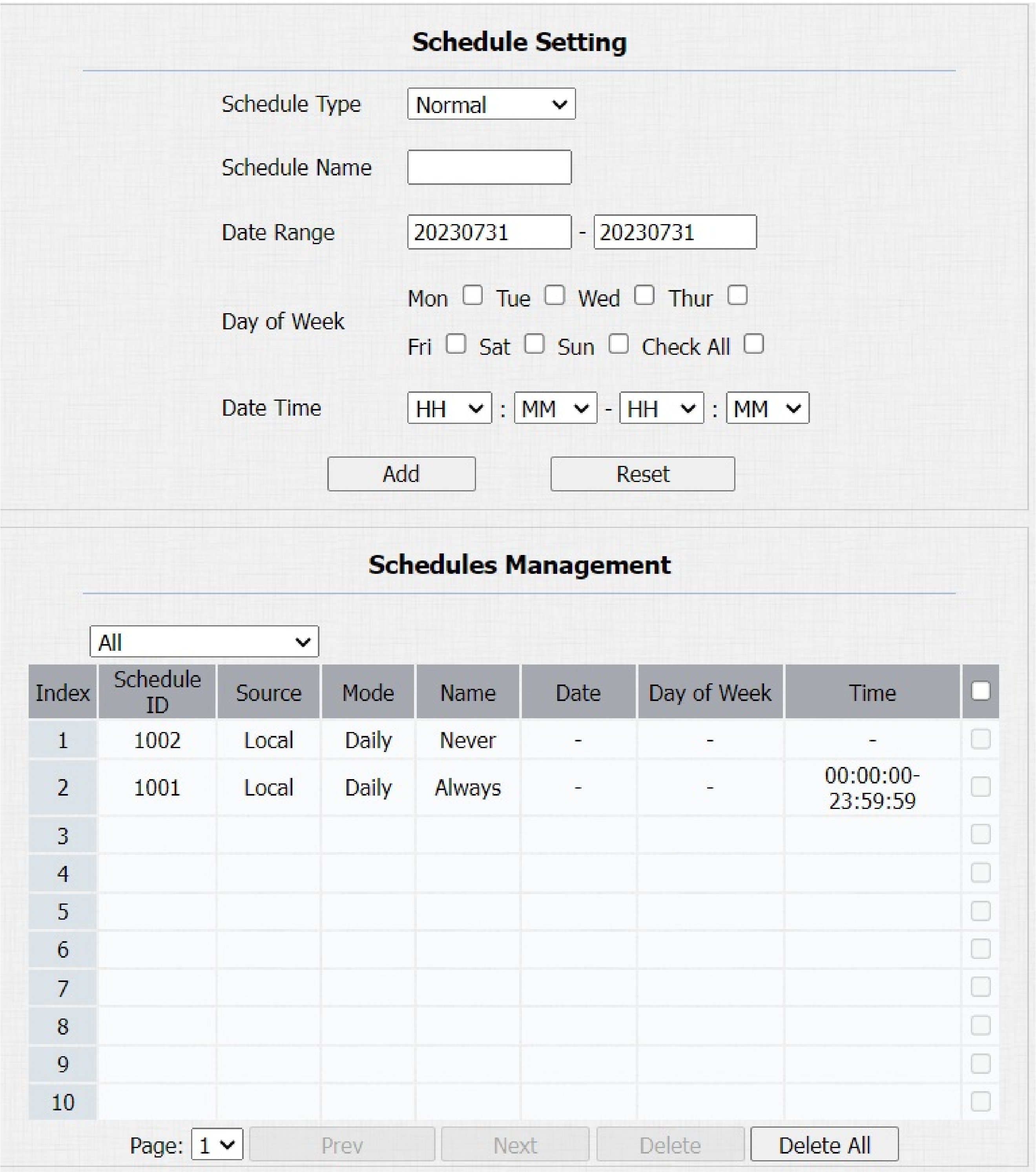
Parameter Set-up:

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

Create Door Access Schedule

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

To do this configuration on web **Intercom** > **Schedule** interface.



Schedule Setting

Schedule Type	Normal
Schedule Name	
Date Range	20230731 - 20230731
Day of Week	Mon □ Tue □ Wed □ Thur □ Fri □ Sat □ Sun □ Check All □
Date Time	HH : MM - HH : MM

Schedules Management

All

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

Page: 1

Parameters Set-up:

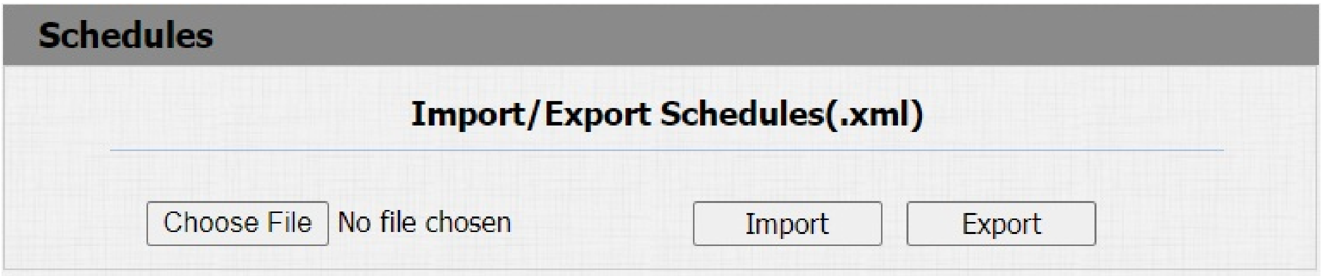
- **Schedule Type**: set the type of time period. There are three types to choose from: **Daily, Weekly**, and **Normal.** The default is **Normal.**
- **Day of Week**: select the corresponding day of the week. This field will only be displayed when the **Weekly** and **Normal** types are selected.

- **Date Range**: set the corresponding date. This field will only be displayed when the **Normal** type is selected.

Import and Export 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.

Path: **Intercom > Schedule > Import/Export Schedule(.xml).**



Note:

- It only supports .xml format files for importing and exporting the schedule.

Door Unlock Configuration

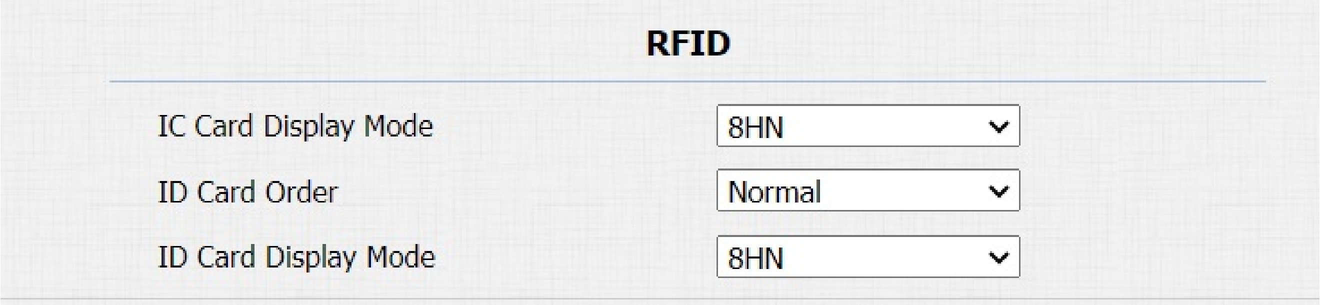
Door Unlock Configuration

Akuvox door phone offers you two types of door access via PIN code and RF card. You can configure them on the device and web interface. Moreover, you can import or export the configured files to maximize your RF card configuration efficiency.

Configure Access Card Format

If you want to integrate with the third-party intercom system in terms of RF card door access, you can change the RF card code format to be identical to that applied in the third- party system.

You can do this configuration on web **Intercom** > **Card Setting** interface.



RFID

IC Card Display Mode: 8HN

ID Card Order: Normal

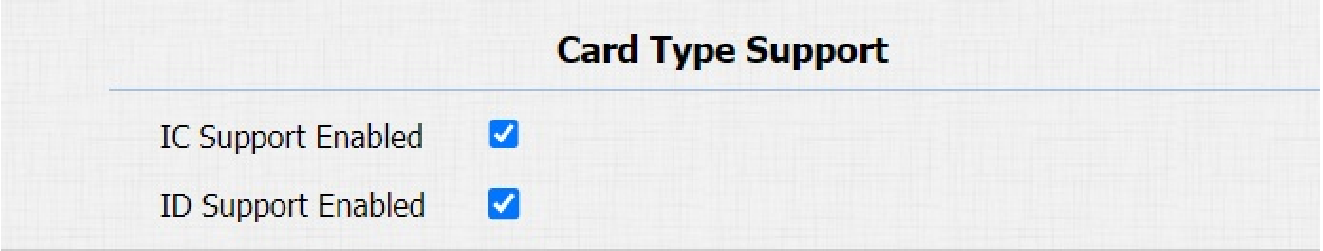
ID Card Display Mode: 8HN

Parameters Set-up:

- **IC CARD Display Mode**: select the card code format for the **IC card** for the door access among seven format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D**. The card code format is **8HN** by default in the door phone.
- **ID Card Order**: select normal or reversed display of ID card.
- **ID Card Display Mode**: select the card format for the **ID Card** for the door access among seven format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D**. The card code format is **8HN** by default in the door phone.

IC/ID Card Control

You can enable or disable the IC and ID card function if needed. You can navigate to **Intercom > Card Setting > Card Type Support**.



Card Type Support

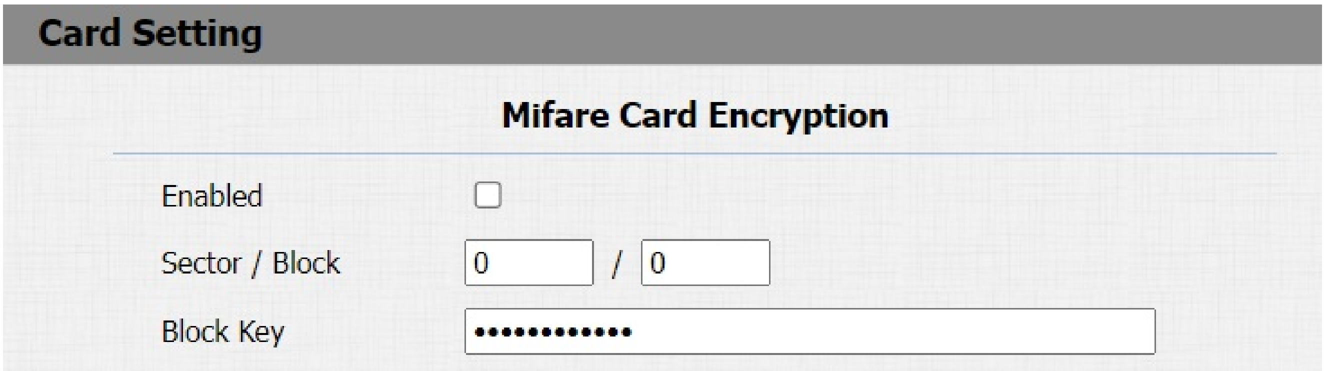
IC Support Enabled ☑

ID Support Enabled ☑

Mifare Card Encryption

The door phone can encrypt Mifare cards for greater security. When this feature is enabled, it reads the data in the cards' designated sectors and blocks, not the UID.

To do so, you can navigate to **Intercom > Card setting > Mifare Card Encryption.**



Card Setting

Mifare Card Encryption

Enabled □

Sector / Block 0 / 0

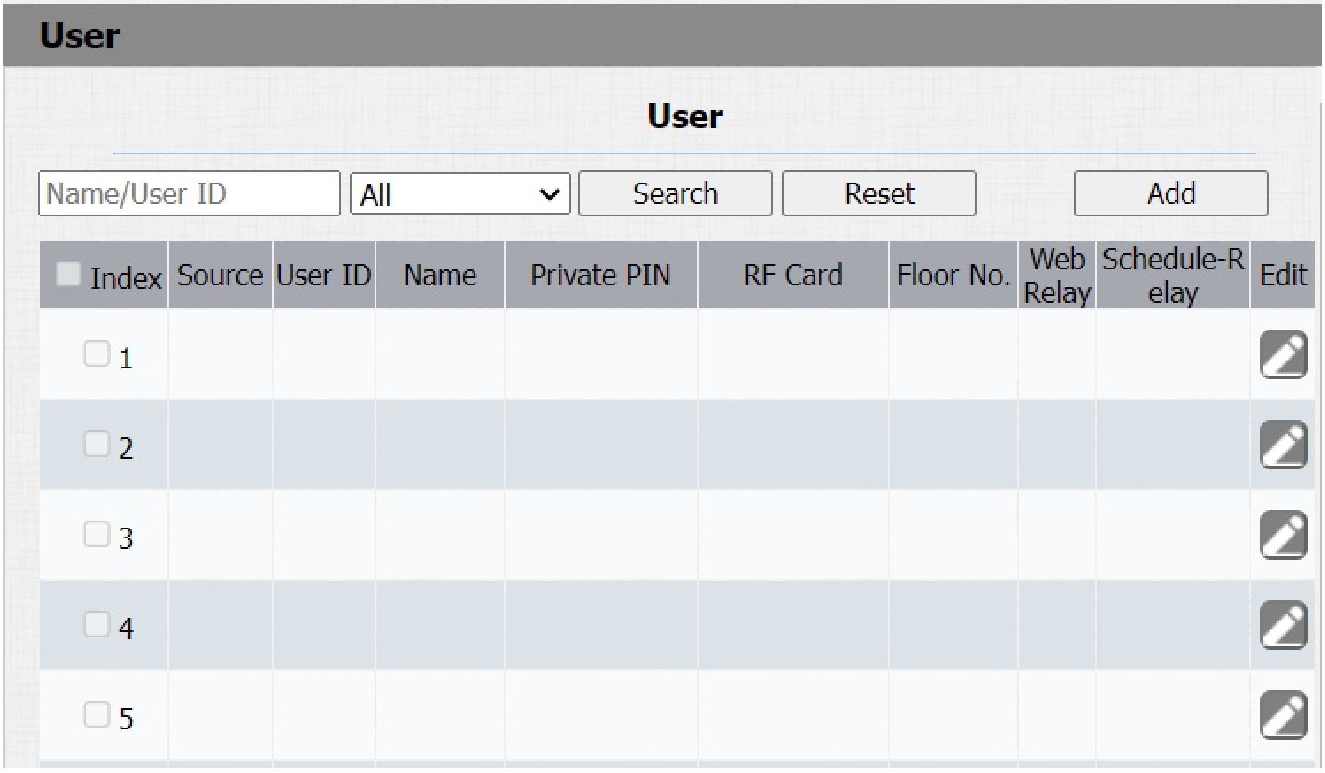
Block Key ••••••••••••

Parameter Set-up:

- **Sector/Block**: enter the sector and block in which the card number is located in the Mifare/Defire Card. For example, the card number can be in sector 3 and block 3 in the card.
- **Block Key**: enter the block password for access.

Configure RF Card for Door Unlock

You can tap the RF card on the reader and click **obtain** to add an RF card for the user. Path: **Intercom > User**. Click **Add** to see the screenshot below.

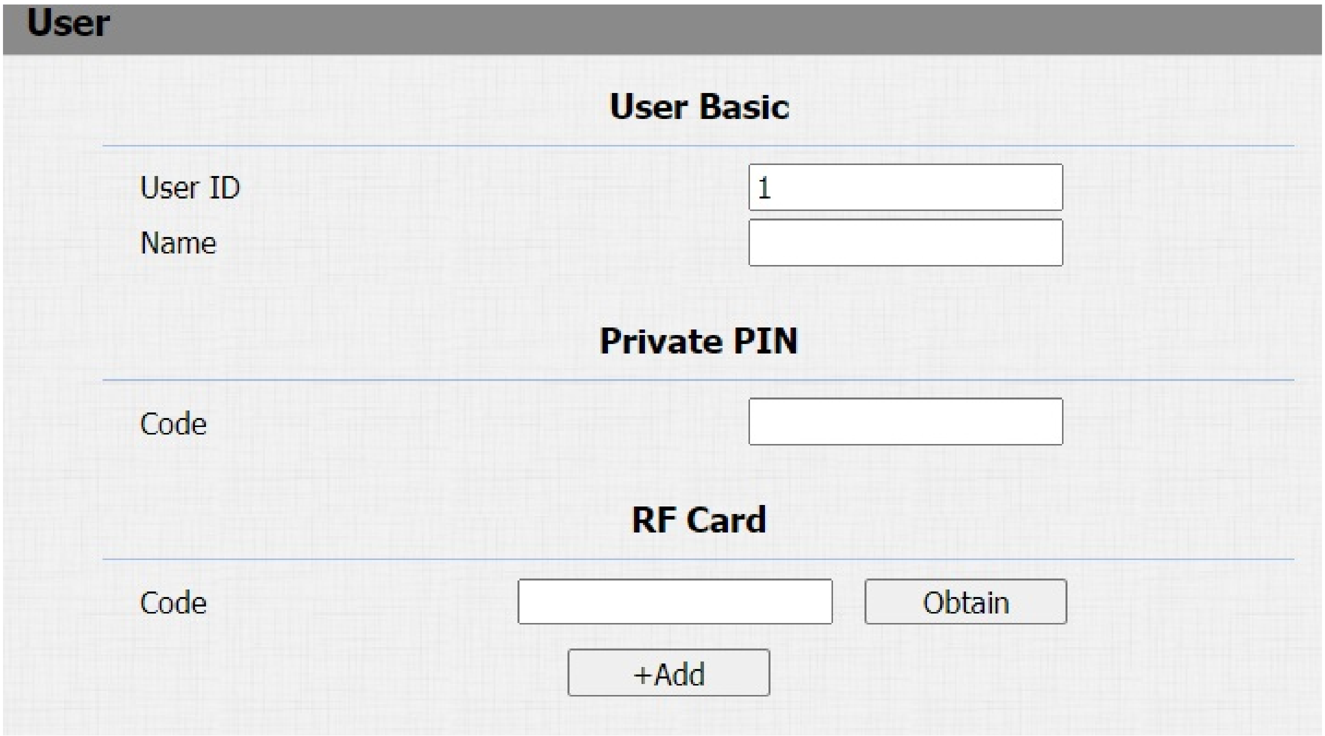


User

User

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

□ Index	Source	User ID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
□ 1									✎
□ 2									✎
□ 3									✎
□ 4									✎
□ 5									✎



User

User Basic

User ID: 1

Name:

Private PIN

Code:

RF Card

Code: Obtain

+Add

Parameter Set-up:

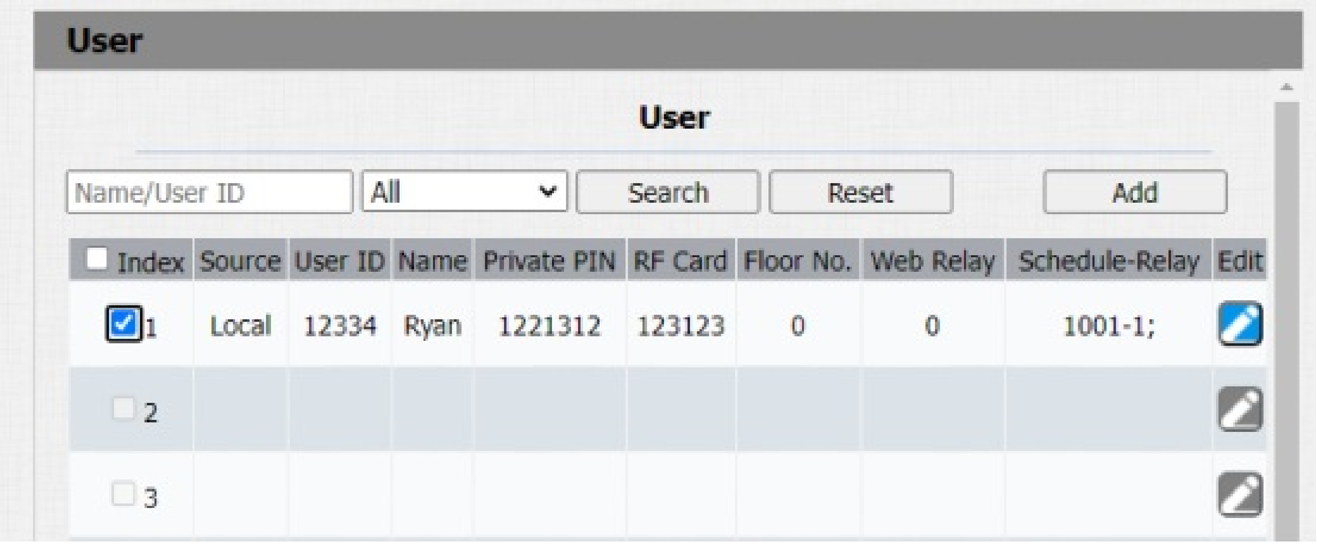
- **User ID**: enter the user ID. The user ID is 11 digits maximum in length and cannot be reused for other users. The User ID can be generated automatically or manually.
- **Code**: place the card on the device card reader area and click **Obtain**.

Note:

- RF card with 13.56 MHz and 125 kHz can be applicable to the door phone for door access.

Edit the User-specific Door Access Data

You can search user(s)-specific door access and edit the door access data on the web **Intercom > User** interface.



User

User

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

☐ Index	Source	User ID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
☑ 1	Local	12334	Ryan	1221312	123123	0	0	1001-1;	✎
☐ 2									✎
☐ 3									✎

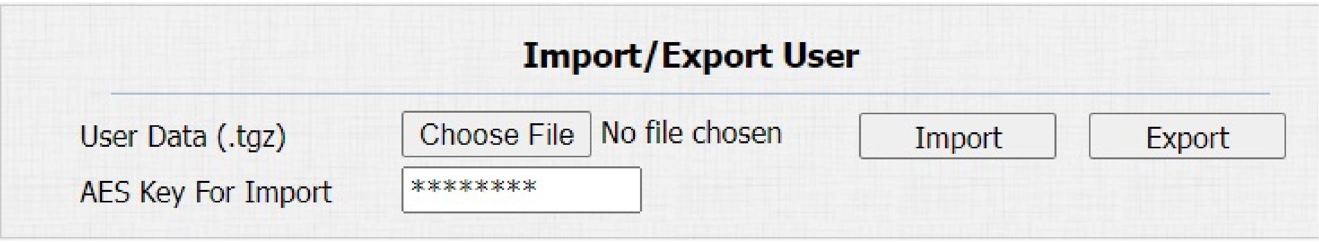
Note:

- Users synchronized from the SmartPlus cannot be edited or deleted.

Import and Export User Data of Access Control

The door phone supports user data of access control to be shared among Akuvox door phones through import and export, and then import it to a third-party device.

To configure the configuration on the web **Intercom > User > Import/Export User** interface.



Import/Export User

User Data (.tgz) | Choose File | No file chosen | Import | Export

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

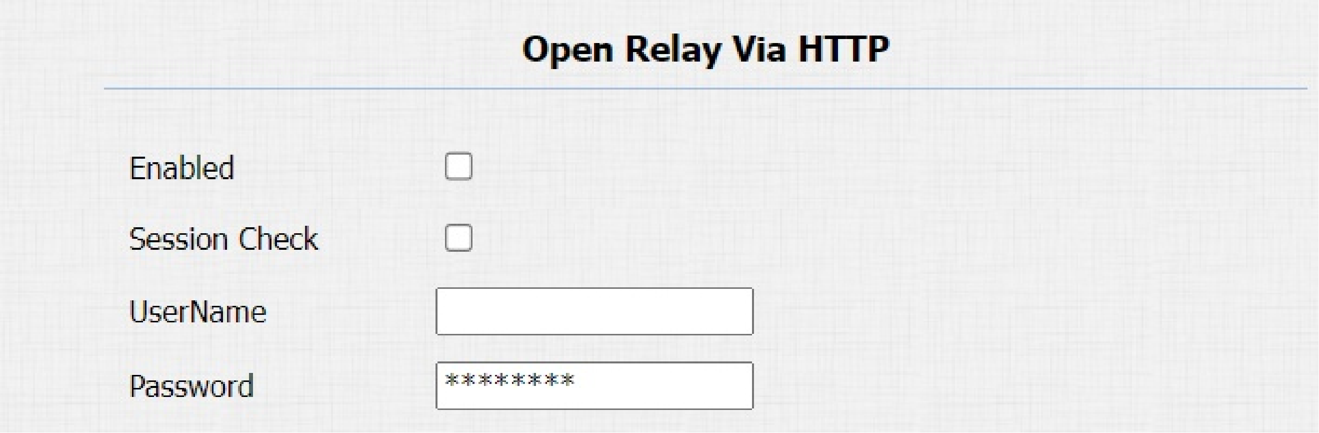
Parameter Set-up:

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

Configure Open Relay via HTTP for Door Unlock

You can unlock the door remotely without approaching the device physically for door entry by typing in the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for door entry.

To configure it, go to **Intercom > Relay > Open Relay Via HTTP**.



Open Relay Via HTTP

Enabled □

Session Check □

UserName

Password ********

Parameter Set-up:

- **Session Check**: this feature is for some network security limitations, if you enable it, the door may not be unlocked in this way.
- **User Name**: enter the user name of the device's web interface, for example, **admin**.
- **Password**: enter the password for the HTTP command. For example, **12345**.

Please refer to the following example:

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

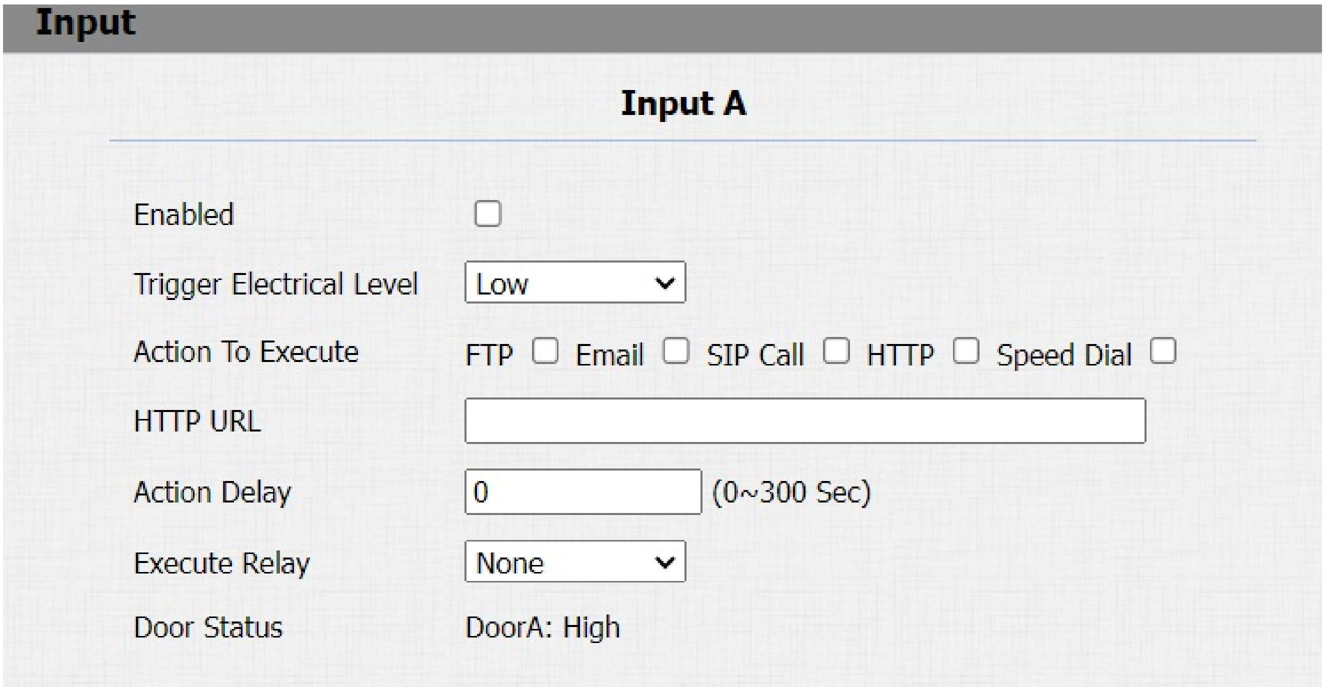
Note:

- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

Configure 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.

Navigate to **Intercom** > **Input** interface.



Input

Input A

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

Parameter Set-up:

- **Trigger Electrical Level**: select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action to Execute**: select the method to carry out the action: **FTP, Email, HTTP, TFTP, Speed Dial.**
- **HTTP URL**: enter the URL if you select the HTTP to carry out the action.
- **Action Delay**: set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 seconds after you press the button.
- **Execute Relay**: set up relays to be triggered by the input.
- **Door Status**: display the status of the input signal.

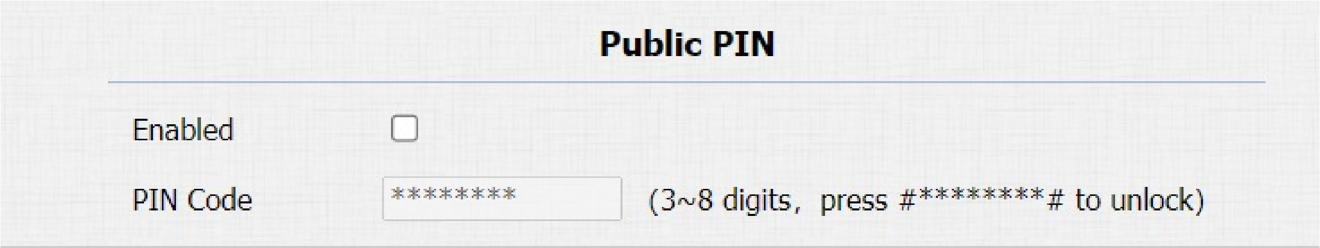
Configure PIN Code for Door Unlock

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. You can create and modify both the public and private PIN codes.

Configure Public Code for Door Unlock

The device supports public pin codes for administrators or cleaners to open the door.

To do this configuration on the web **Intercom > PIN Setting > Public PIN** interface.



Public PIN

Enabled	□
PIN Code	********* (3~8 digits， press #*********# to unlock)

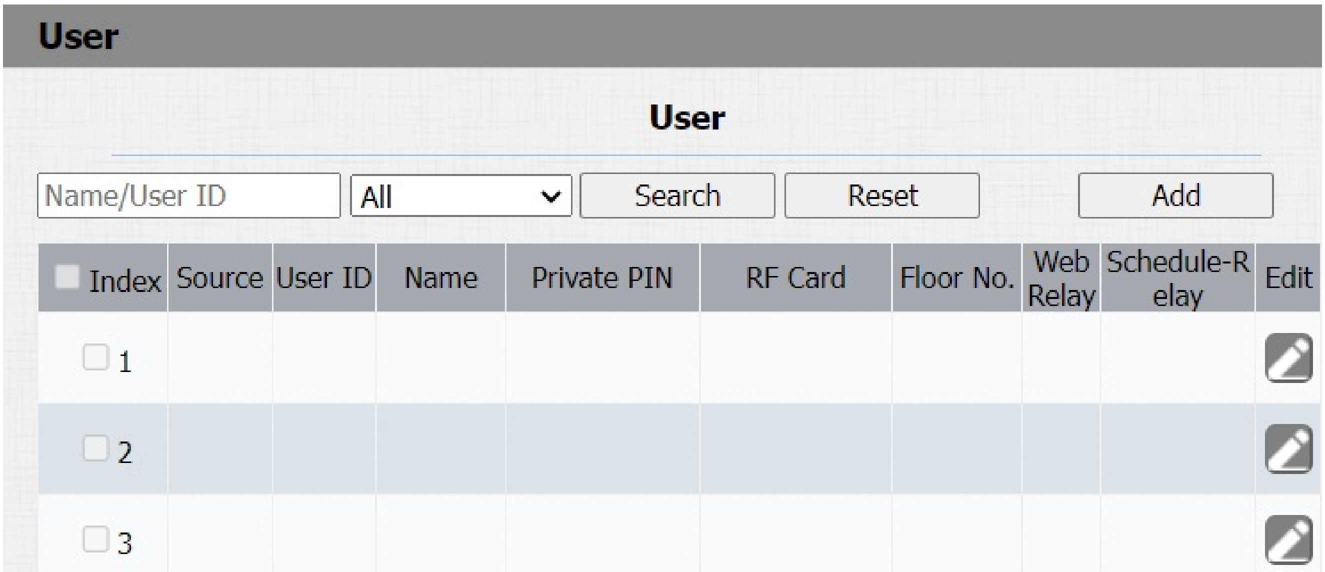
Parameter Set-up:

- **PIN Code**: customize 3-8 digit numbers for the public key value.

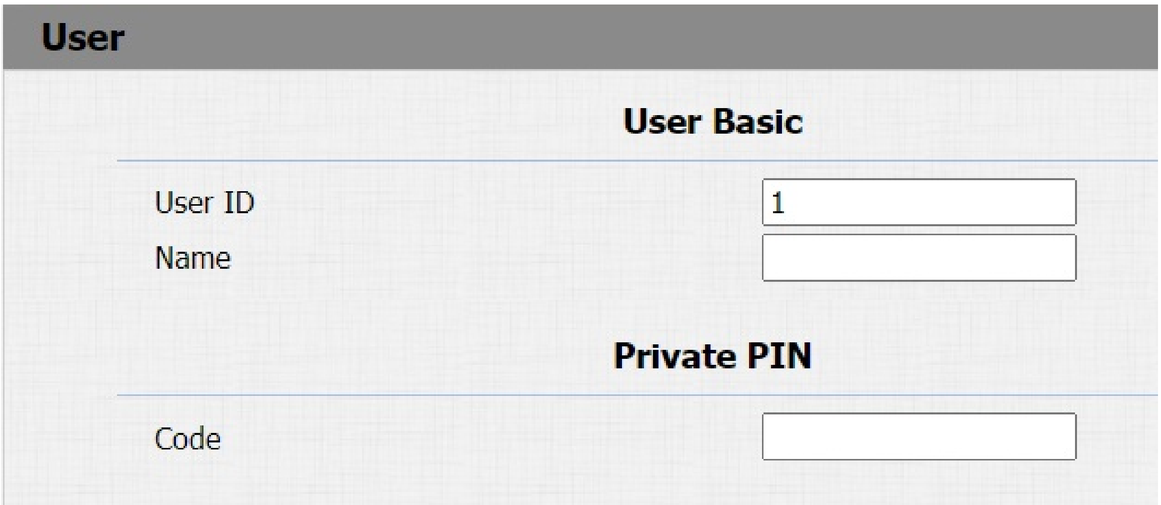
Configure Private PIN Code on the Web Interface

On 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 specifying which relay to open.

Path: **Intercom > User**.



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



User

User Basic

User ID	1
Name	

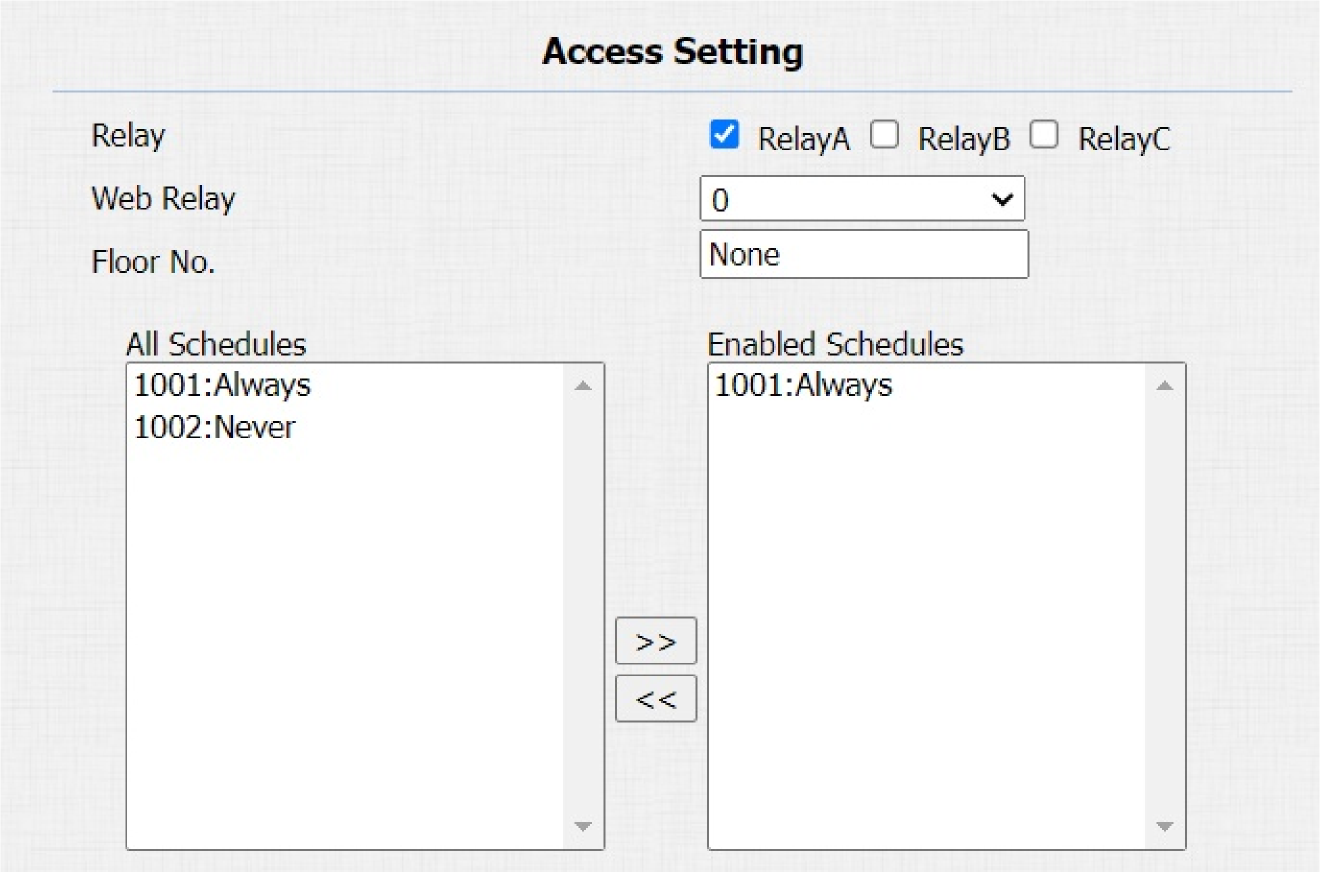
Private PIN

Code	

Parameter Set-up:

- **Code**: enter the user’s private PIN.

After user information and PIN code are entered, you can scroll down to **Access Setting** and configure private PIN code access control.



Access Setting

Relay	☑ RelayA ☐ RelayB ☐ RelayC
Web Relay	0
Floor No.	None

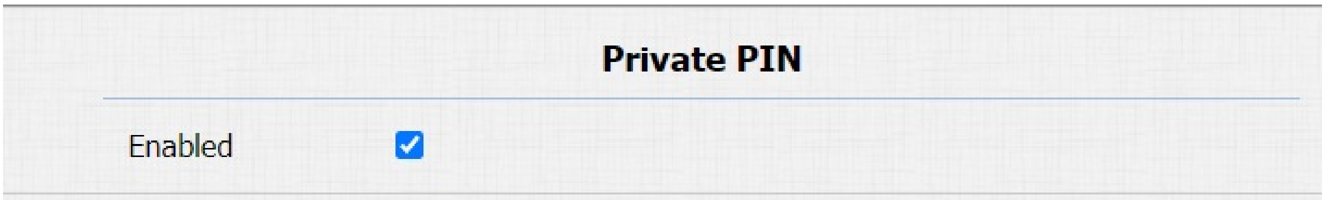
All Schedules	Enabled Schedules
1001:Always 1002:Never	1001:Always

Parameter Set-up:

- **Relay**: select the relay(s) that you want to apply the private PIN code for the door unlock.
- **Web relay**: select the specific number of web relay action commands you have set up on the web interface.

- **Schedule**: select from the created door access schedule on the right box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

You are required to enable the PIN code before you can get door access via private PIN code, you can navigate to **Intercom > PIN setting > Private PIN.**



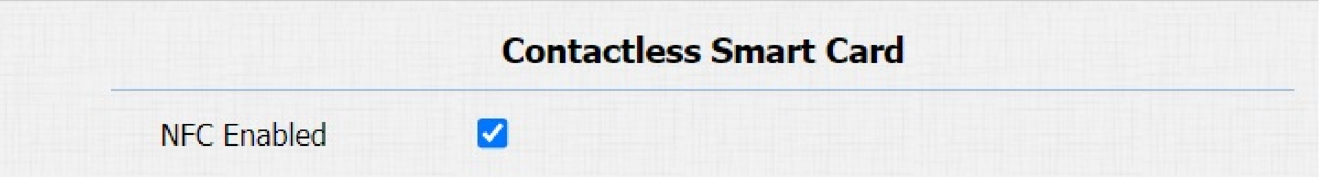
Private PIN

Enabled ☑

Configure NFC for Unlock

NFC (Near Field Communication) is a popular way for door access. It uses radio waves for data transmission interaction. The device can be unlocked by NFC. You can keep the mobile phone closer to the device for door access.

To enable the NFC feature, go to **Intercom > Card Setting > Contactless Smart Card.**



Contactless Smart Card

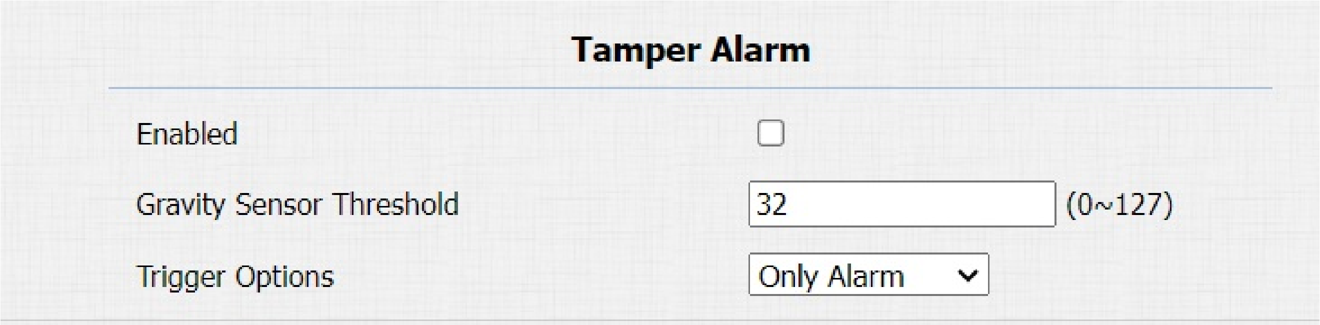
NFC Enabled ☑

Security

Tamper Alarm Setting

The tamper alarm function prevents anyone from removing the devices without permission. It does this by setting off the tamper alarm and making calls to a designated location when the device detects a change in its gravity value from the original one.

To do this configuration on the web **Security > Basic > Tamper Alarm**.



Tamper Alarm

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

Parameter Set-up:

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

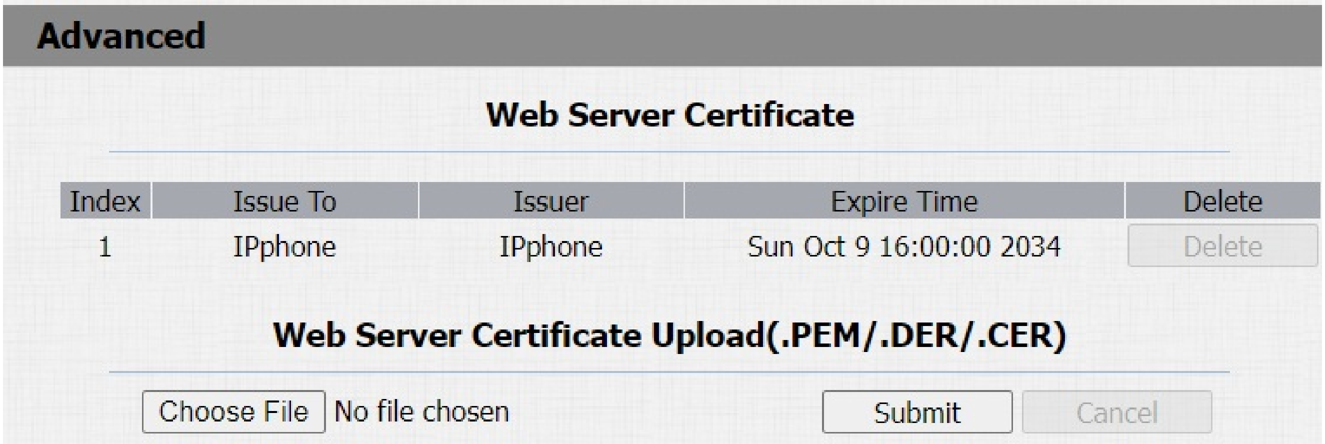
Client Certificate Setting

Certificates ensure communication integrity and privacy. To use the SSL protocol, you need to upload the right certificates for verification.

Web Server Certificate

It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

To upload Web Server certificate on the device web interface **Security > Advanced > Web Server Certificate.**



Advanced

Web Server Certificate

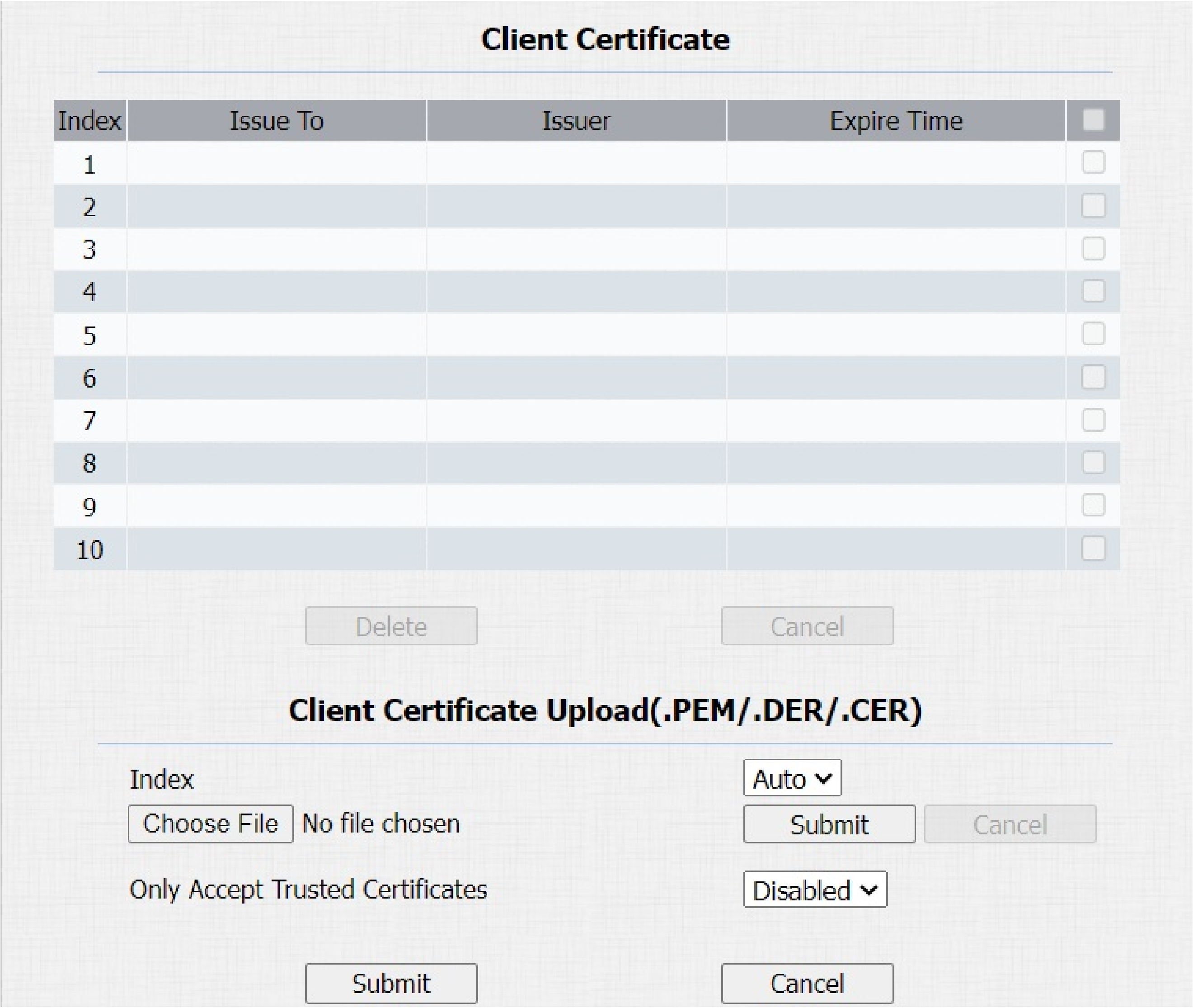
Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

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

Client Certificate

This certificate verifies the server to the Akuvox door phone when they want to connect using SSL. The door phone verifies the server's certificate against its client certificate list.

To upload and configure client certificates on the same page.



Client Certificate

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

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

Index: Auto

Choose File No file chosen

Only Accept Trusted Certificates: Disabled

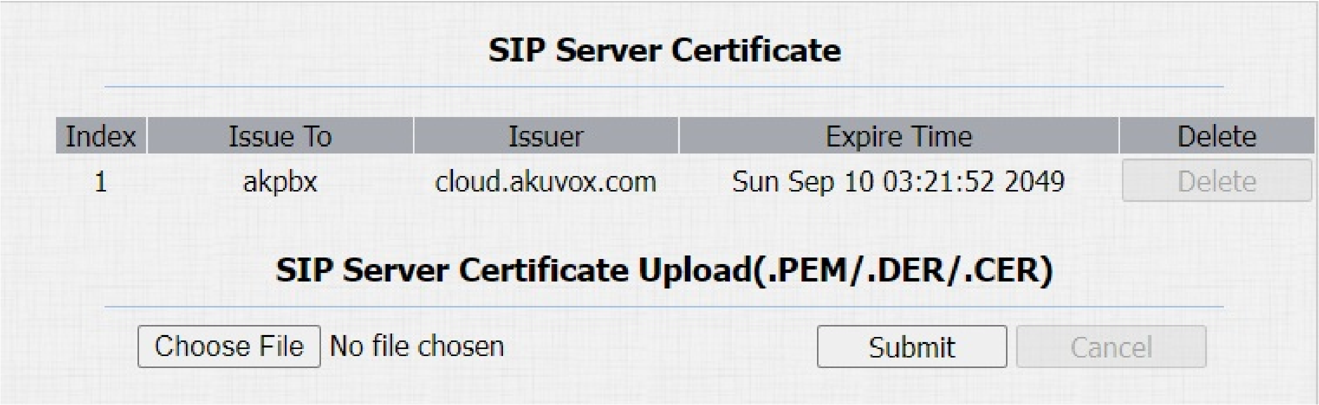
Parameter Set-up:

- **Index**: select the desired value from the drop-down list of Index. If you select **Auto** value, the uploaded certificate will be displayed in numeric order. If you select values from **1** to **10**, the uploaded certificate will be displayed according to the value that the user selected.
- **Select File**: click **Choose File** browse the local drive, and locate the desired certificate (*.pem only).
- **Only Accept Trusted certificates**: if you select **Enabled**, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If you select **Disabled**, the phone will not verify the server certificate no matter whether the certificate is valid or not.

Upload TLS Certificate for SIP Account Registration

Before applying for a SIP account from a SIP or a DNS server using the TLS protocol, you'll need to upload a TLS certificate. This certificate is essential for server authentication.

To upload the TLS certificate, go to **Security > Advanced > SIP Server Certificate.**



SIP Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	akpbx	cloud.akuvox.com	Sun Sep 10 03:21:52 2049	Delete

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

Parameter Set-up:

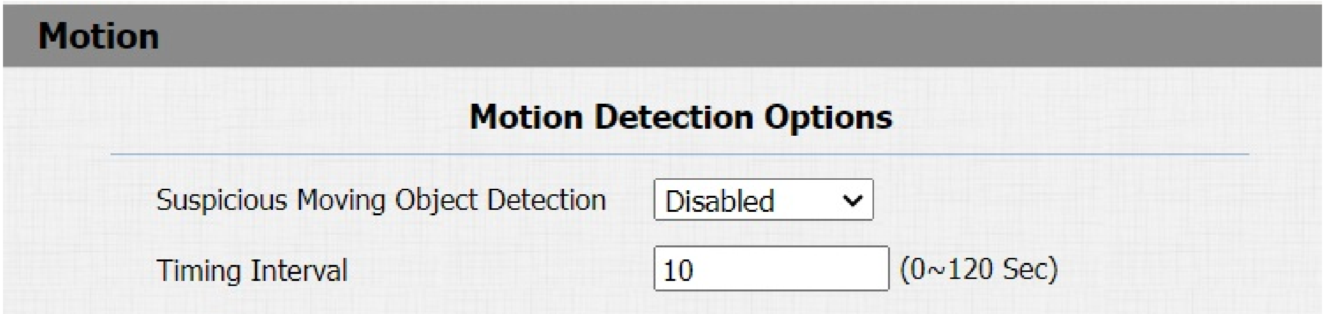
- **Choose file**: upload the certificate file. You can only upload the certificate file in .PEM, .DER, and CER format.

Motion Detection

Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved, and activates the system to perform the appropriate action.

Configure Motion Detection

You can turn on the motion detection and set up the motion detection interval on the web **Intercom > Motion** interface.



Motion

Motion Detection Options

Suspicious Moving Object Detection: Disabled

Timing Interval: 10 (0~120 Sec)

Parameter Set-up:

- **Suspicious Moving Object Detection**: select **Disable** to disable the motion detection. Select **IR detection** to enable the IR sensor-based motion detection. And select **Video**

detection to enable the video-based motion detection during the monitoring of the suspicious moving object.

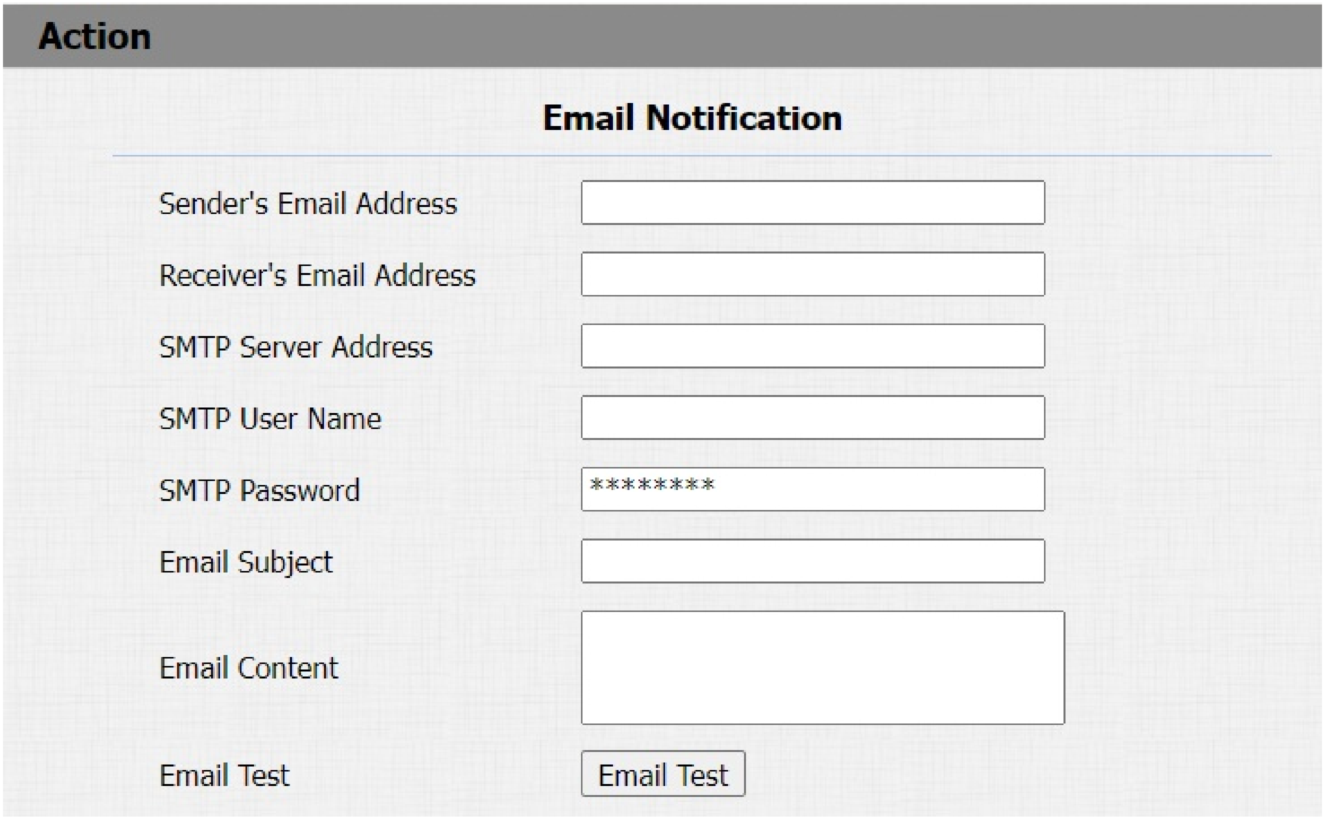
- **Detection Accuracy**: set the detection accuracy for the detection sensitivity. The higher the value is, the greater the sensitivity is. The default detection accuracy value is 3.
- **Time Interval**: the absolute triggering interval is 3 seconds. If you select a number greater than 3 seconds, then it requires a second triggering interval to trigger the alarm. For example, if you select 3 seconds, then the alarm will be triggered when a moving object is detected one time from 0 to 3 seconds (triggered any time from 0 to 3 seconds). However, for example, if you select 5 seconds (greater than 3), then the alarm will not be triggered until a moving object is detected for the second time from 3 to 5 seconds (triggered any time from 3 to 5 seconds). The default interval is 10 seconds.
- **The Width of Detected Area/The Height of Detected Area**: The full size of the detection area is calculated by percentage (100%) from left to right. Pick the horizontal detection range anywhere from 0% to 100%, and pick the vertical detection range anywhere from 0% to 100%. After that, you will be able to get the exact detection area you want.

Security Notification Setting

Email Notification Setting

Set up email notification to receive screenshots of unusual motion from the door phone.

Go to **Intercom > Action > Email Notification** interface. The email notification will show as the captures.



Action

Email Notification

Sender's Email Address	
Receiver's Email Address	
SMTP Server Address	
SMTP User Name	
SMTP Password	********
Email Subject	
Email Content	
Email Test	Email Test

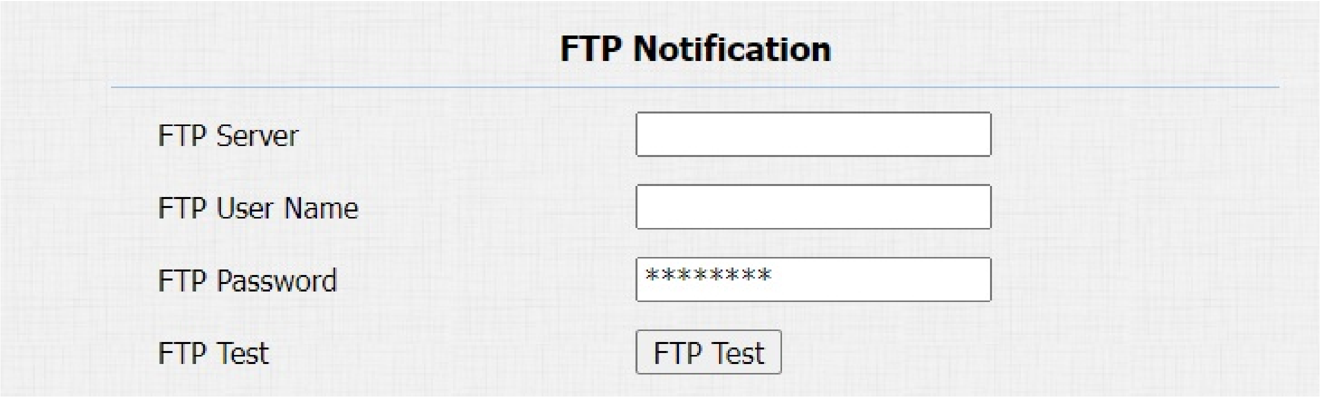
Parameter Set-up:

- **SMTP Server Address**: enter the SMTP server address of the sender.
- **SMTP User Name**: enter the SMTP user name, which is usually the same as the sender’s email address.
- **SMTP Password**: configure the password of the SMTP service, which is the same as the sender’s email address.
- **Email Test**: click to test if the email can be sent and received.

FTP Notification Setting

To get notifications through FTP server, you need to set up the FTP settings. The door phone will upload a screenshot to the specified FTP folder if it senses any unusual motion.

Go to **Intercom > Action > FTP Notification.**



FTP Notification

FTP Server

FTP User Name

FTP Password: ********

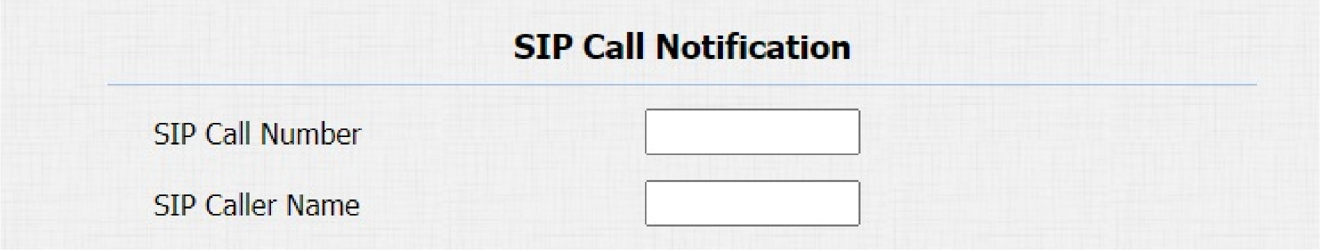
FTP Test: FTP Test

Parameter Set-up:

- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP Test**: click **FTP Test**, then a triggered event snapshot will be sent to the FTP server for testing purposes.

SIP Call Notification Setting

In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered. To configure a SIP call notification on web **Intercom > Action > SIP Call Notification** interface.



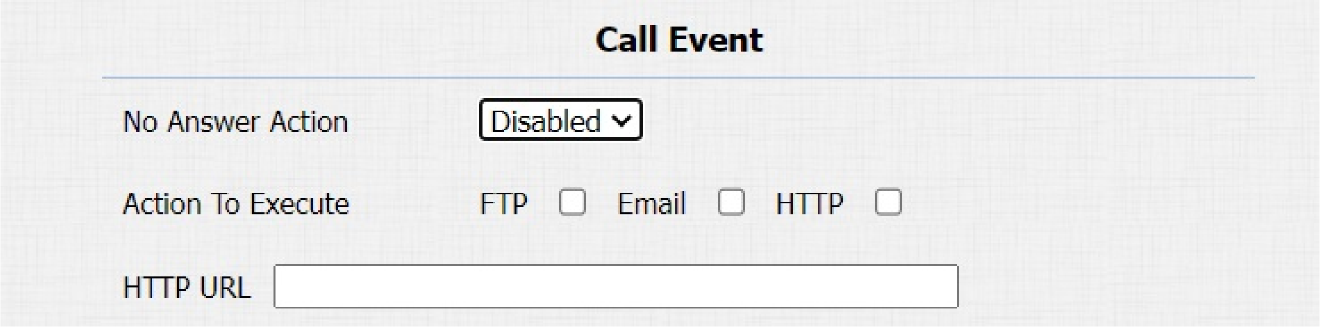
SIP Call Notification

SIP Call Number

SIP Caller Name

Call Event Notification

Enable this feature if you want to be notified when any outgoing calls from the door phone are not answered. The notification is made via FTP, Email, and HTTP. On the web, navigate to **Intercom > Basic > Call Event**.



Call Event

No Answer Action: Disabled

Action To Execute: FTP □ Email □ HTTP □

HTTP URL

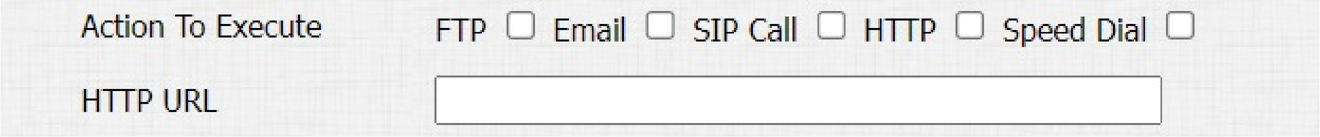
Parameter Set-up:

- **Action To Execute**: select FTP, Email or HTTP method for the notification. If FTP is selected, a screenshot of the caller will be sent via as notification. If Email is selected, the Emails containing a screenshot of the caller will be sent. If HTTP is selected, you can add the event message to the HTTP URL before sending.
- **Http URL**: enter the HTTP URL that will be sent to the Http server. For example:http//192.168.31.6/door phone#1. HTTP URL format: **http://http server IP address/any information**

Security Action Configuration

Configure Action of Input

When the Input interface is working, it can also trigger an action. You can do this configuration on web **Intercom > Input** interface.



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

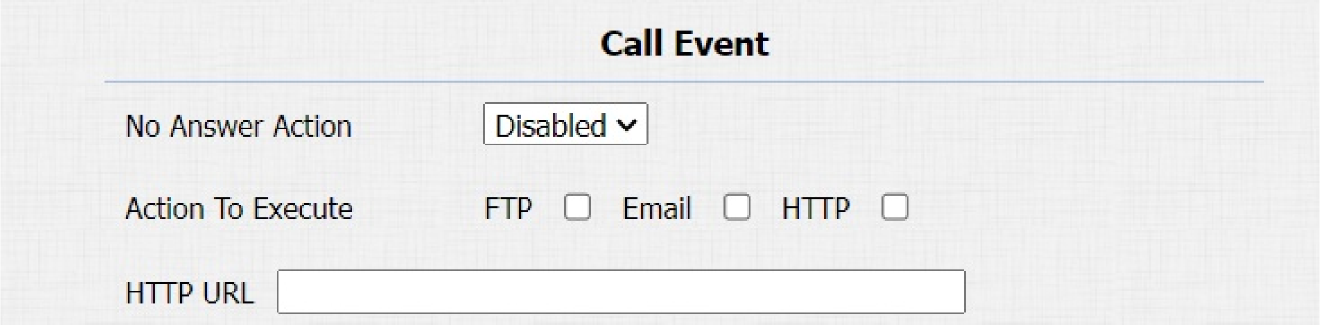
HTTP URL

Parameter Set-up:

- **Action To Execute**: to choose which action to execute after triggering.

Configure Action of Call

When pressing the push button, the door phone will trigger the pre-configured action type, the notification can be sent out by Email, FTP notification, or SIP call. To do this configuration on web **Intercom > Basic** interface.



Call Event

No Answer Action: Disabled

Action To Execute FTP □ Email □ HTTP □

HTTP URL

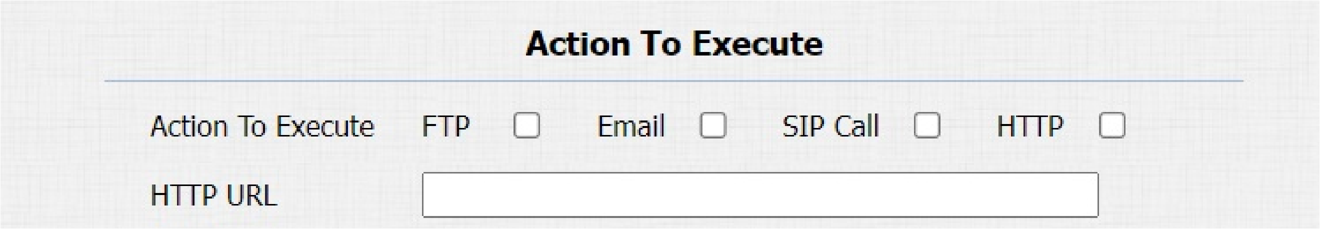
Parameter Set-up:

- **No Answer Action**: if the call will not be answered, it still triggers the action event after enabling this feature.

- **Action to execute**: to choose which action to be executed after triggering.

Configure Action of Motion

When the motion detection feature is working, you can make it trigger an action. To do this configuration on web **Intercom** > **Motion** interface.



Action To Execute

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

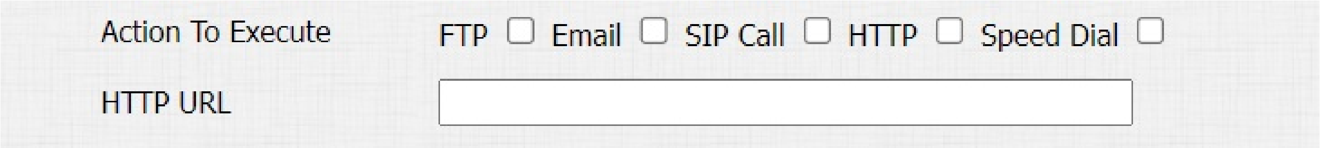
HTTP URL

Parameter Set-up:

- **Action to execute**: to choose which action to be executed after triggering.

Configure Action of Input

When the Input interface is working, it can also trigger an action. You can do this configuration on web **Intercom** > **Input** interface.



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

HTTP URL

Parameter Set-up:

- **Action to execute**: To choose which action to be executed after triggering.

Action URL

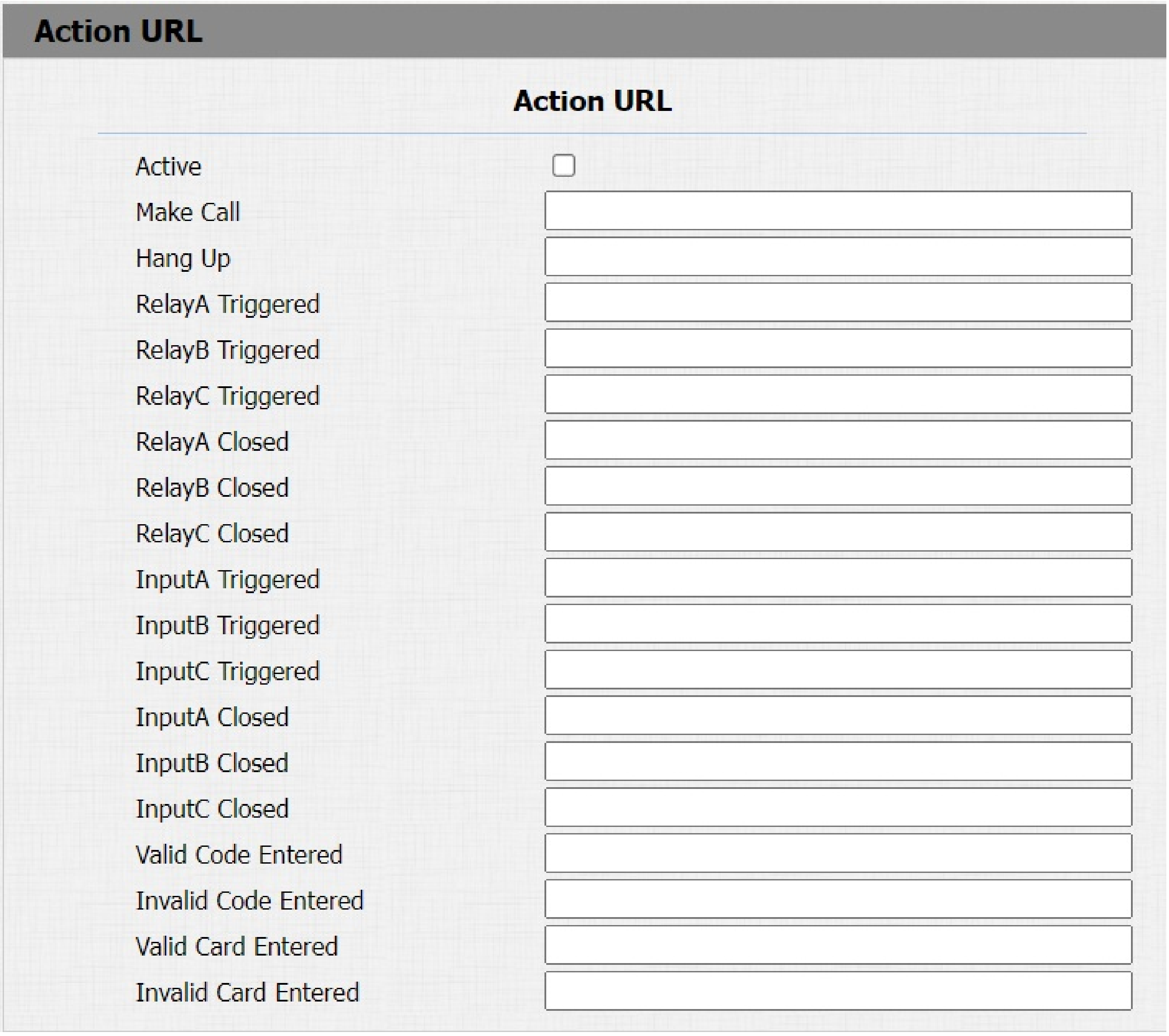
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

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

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

Path: **Phone > Action URL**.



Action URL

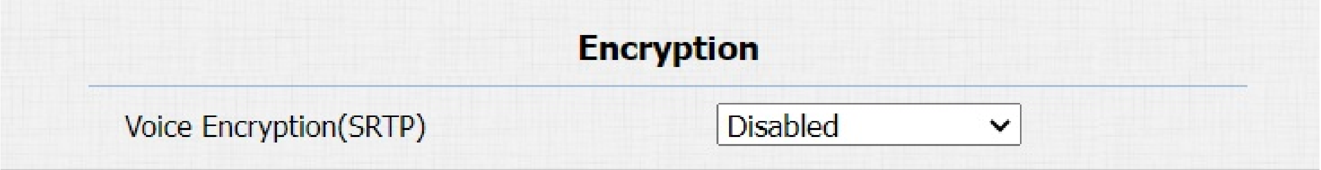
Action URL

Active	□
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayC Triggered	
RelayA Closed	
RelayB Closed	
RelayC Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	
InputA Closed	
InputB Closed	
InputC Closed	
Valid Code Entered	
Invalid Code Entered	
Valid Card Entered	
Invalid Card Entered	

Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the Real-time Transport Protocol (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance, and replay protection.

To configure this feature on web **Account > Advanced > Encryption** interface.



Encryption

Voice Encryption(SRTP)	Disabled

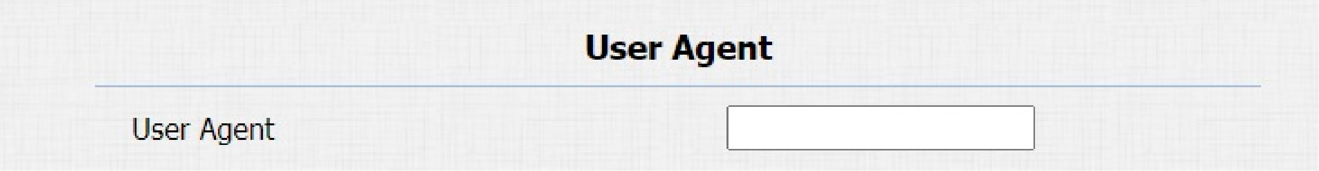
Parameter Set-up:

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

User Agent

User agent is used for identification purpose when you are analyzing the SIP data packet.

To do this configuration on the web **Account > Advanced > User Agent** interface.



User Agent

User Agent

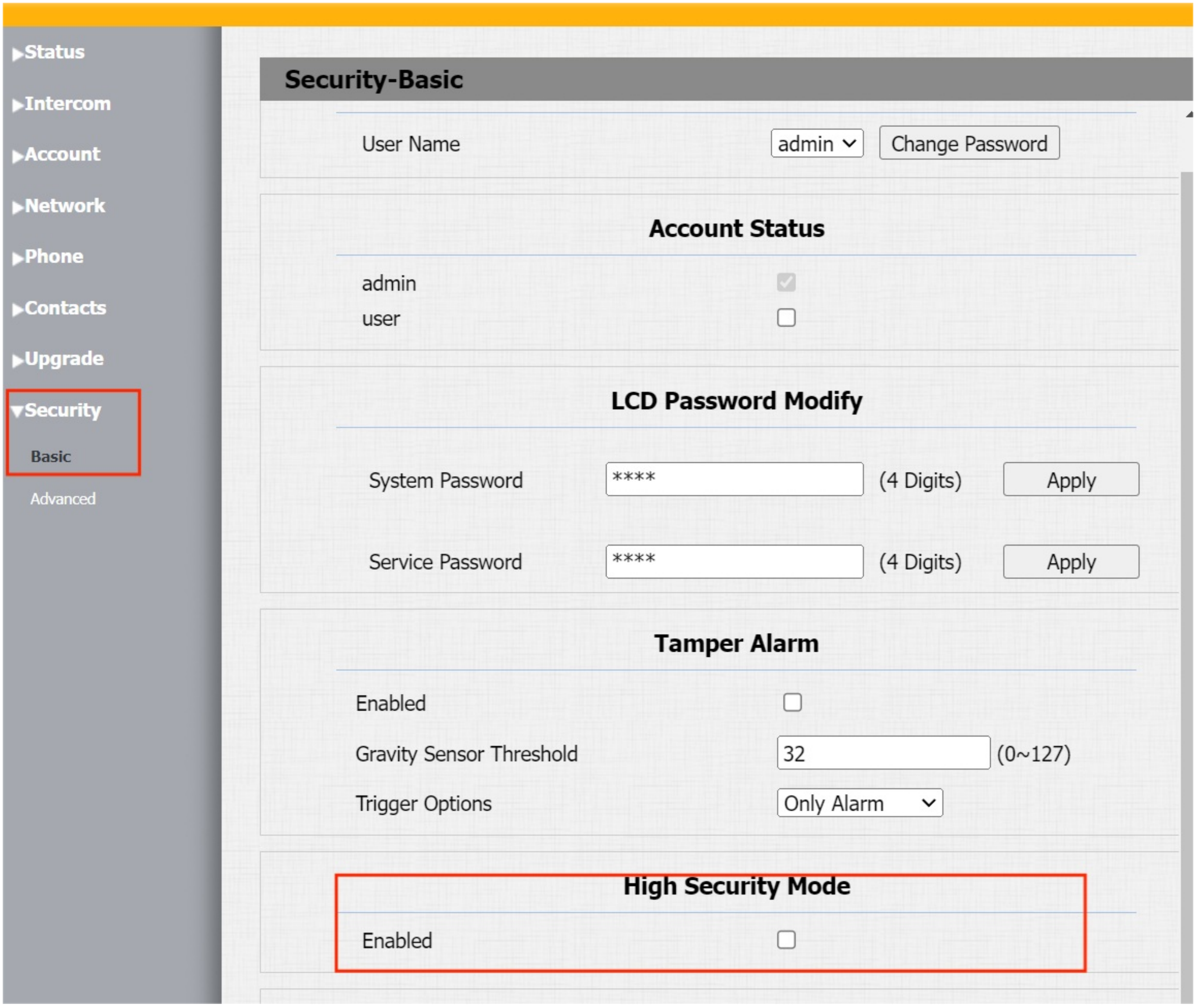
Parameter Set-up:

- **User Agent**: support to enter another specific value, it is "Akuvox" by default.

High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods, and more.

To configure this feature on the web: **Security>Basic>High Security Mode.**



Security-Basic

User Name: admin [Change Password]

Account Status

admin ☑

user □

LCD Password Modify

System Password: **** (4 Digits) [Apply]

Service Password: **** (4 Digits) [Apply]

Tamper Alarm

Enabled □

Gravity Sensor Threshold: 32 (0~127)

Trigger Options: Only Alarm

High Security Mode

Enabled □

Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.

2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

3. The supported HTTP format for relay triggering varies depending on whether high secure mode is enabled or disabled.

If the mode is on, the device only accepts the new HTTP formats below for door opening.

- l http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- l http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is off, the device can use both the new formats above and the old format below:

- l http://deviceIP/fcgi/do?
  action=OpenDoor&UserName=username&Password=password&DoorNum=1

4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Monitor and Image

MJPEG and RTSP are the primary monitoring stream types discussed in this chapter.

MJPEG, or Motion JPEG, is a video compression format that uses JPEG images for each video frame. Akuvox devices display live streams on 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.

RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

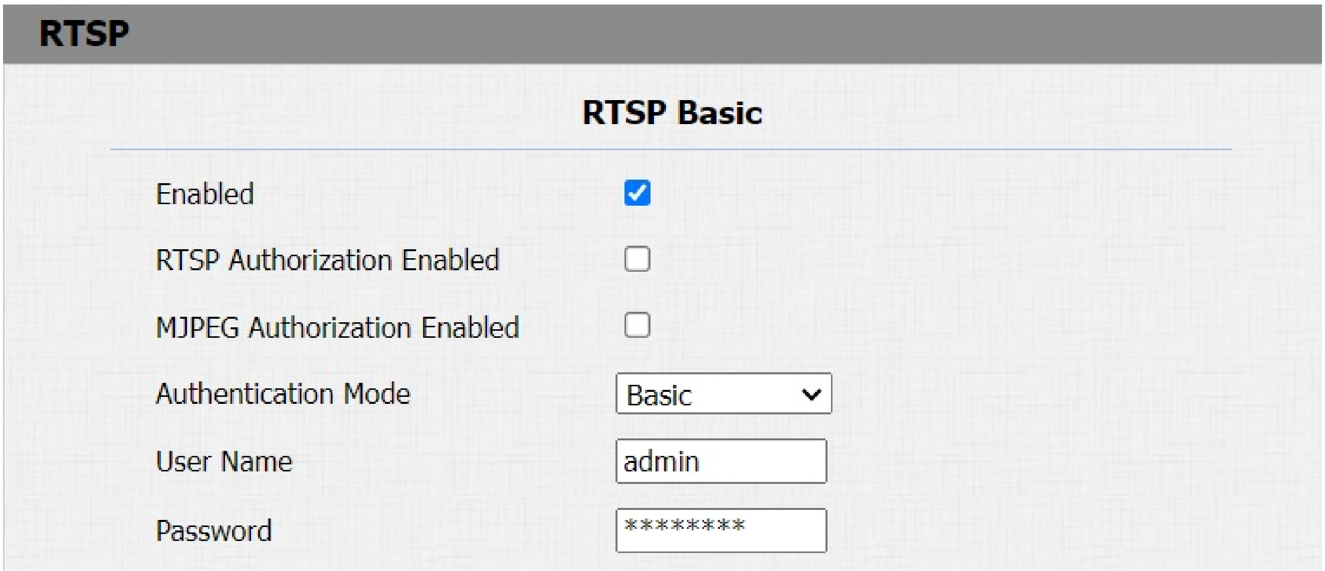
ONVIF is an Open Network Video Interface Forum. It enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

You are required to set up the RTSP function on the device web **Intercom** > **RTSP** > **RTSP Basic** interface in terms of RTSP authorization, authentication, and password, etc. before you are able to use the function.



RTSP

RTSP Basic

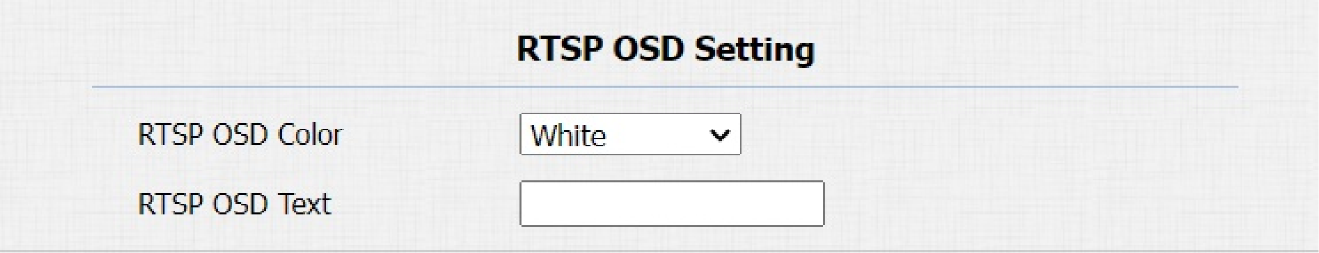
Enabled	☑
RTSP Authorization Enabled	□
MJPEG Authorization Enabled	□
Authentication Mode	Basic
User Name	admin
Password	*********

Parameter Set-up:

- **RTSP Authorization Enabled**: enable or disable the RTSP authorization. If you enable the **RTSP Authorization**, you are required to enter **RTSP Authentication Type, RTSP Username, and RTSP Password** on the intercom device such as an indoor monitor for authorization.
- **Authentication Mode**: select RTSP authentication type between **Basic** and **Digest.** Basic is the default authentication type.

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture. To protect the owner of the video or image. To do this configuration on the web **Intercom** > **RTSP** > **RTSP OSD Setting** interface.



RTSP OSD Setting

RTSP OSD Color	White
RTSP OSD Text	

Parameter Set-up:

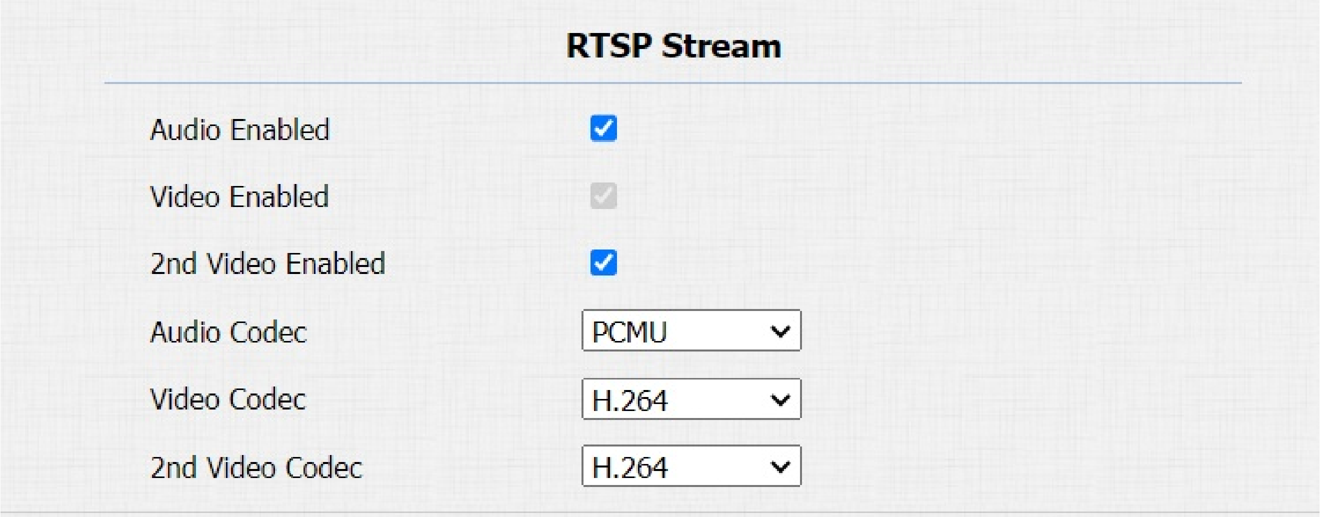
- **RTSP OSD Color**: there are five color options - **White, Black, Red, Green, and Blue** for RTSP watermark text.

- **RTSP OSD Text**: enter the customized text you want to show for the watermark.

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.

Navigate to **Intercom > RTSP > RTSP Stream** interface.

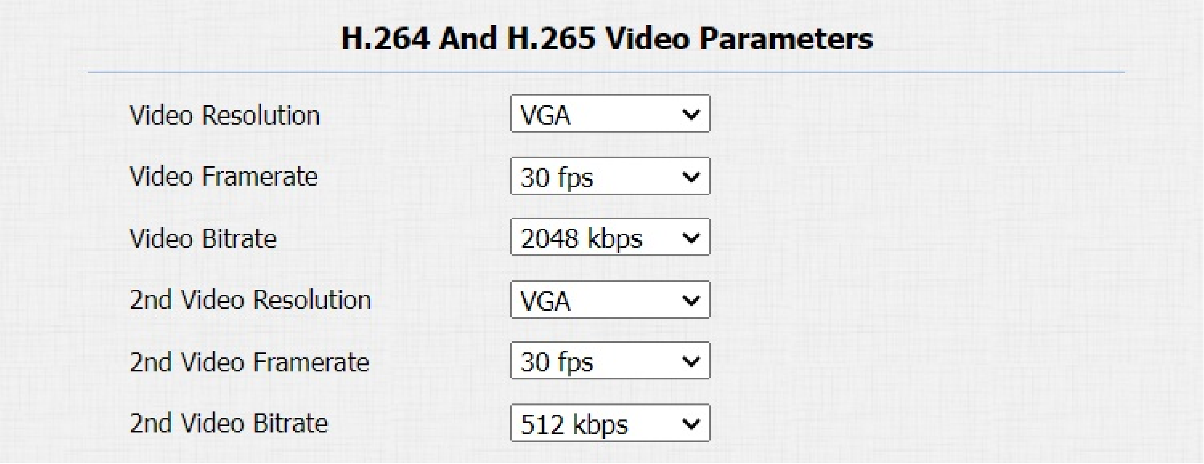


RTSP Stream

Audio Enabled	☑
Video Enabled	☑
2nd Video Enabled	☑
Audio Codec	PCMU
Video Codec	H.264
2nd Video Codec	H.264

Parameter Set-up:

- **Audio Enabled**: tick to enable RTSP audio which means, the door phone can also send audio information to the monitor by RTSP.
- **Video Enabled**: the door phone can send video information to the monitor. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **2nd Video Enabled**: Akuvox door phones support 2 RTSP streams, you can enable the second one.
- **Audio Codec**: choose a suitable audio codec for RTSP audio.
- **Video/2nd Video Codec**: choose a suitable video codec for RTSP video.



H.264 And H.265 Video Parameters

Video Resolution	VGA
Video Framerate	30 fps
Video Bitrate	2048 kbps
2nd Video Resolution	VGA
2nd Video Framerate	30 fps
2nd Video Bitrate	512 kbps

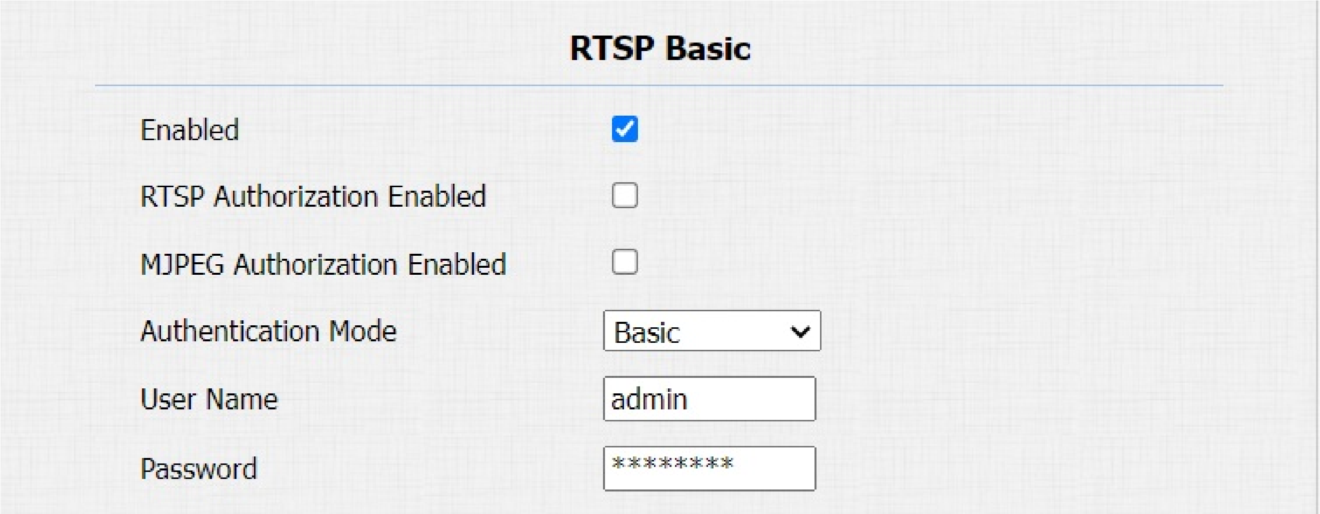
Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: **QVGA, CIF, VGA, 4CIF, 720P**, and **1080P**. The default video resolution is **720P**. and 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**: **30fps** is the video frame rate by default.
- **Video Bitrate**: select video bit-rate among six options: **64kbps, 128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps** according to your network environment. The default video bit rate is **2048 kpbs**.
- **2nd Video Resolution**: select video resolution for the second video stream channel. While the default video solution is **VGA**.
- **2nd Video Framerate**: select the video framerate for the second video stream channel. **25fps** is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate**: select the video bit rate for the second video stream channel. While the second video stream channel is **512 kbps** by default.

MJPEG Image Capturing

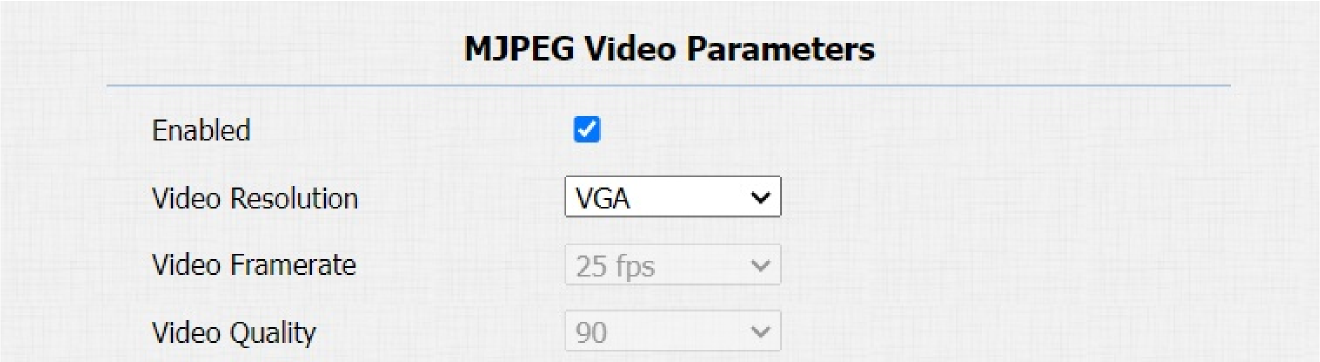
You can take a monitoring image in Mjpeg format with the device. To do this, you need to turn on the Mjpeg function and choose the image quality.

Go to **Intercom > RTSP > RTSP Basic** and **Intercom > RTSP > MJPEG Video Parameters** interface.



RTSP Basic

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



MJPEG Video Parameters

Enabled	☑
Video Resolution	VGA
Video Framerate	25 fps
Video Quality	90

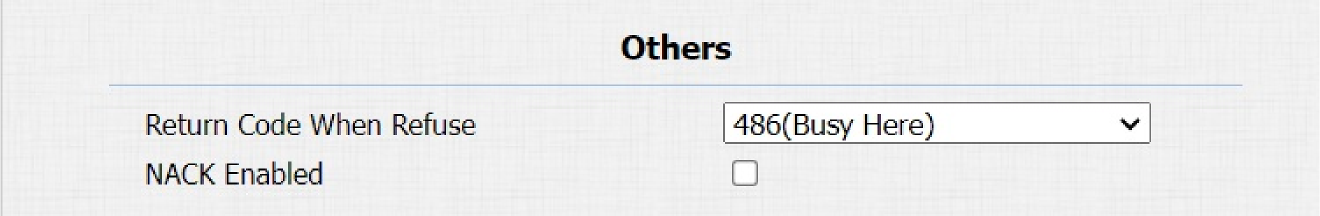
Parameter Set-up:

- **MJPEG Authorization**: tick it to access device video or real-time screenshots through a browser (http address such as: http://device IP:8080/video.cgi (dynamic video), http://device IP:8080/jpeg.cgi (static screenshot)).
- **Video Resolution**: select video resolutions among seven options: **CIF, VGA, 4CIF, 720P**, and **1080P.** The default video resolution is **VGA.** And the video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than **VGA.**
- **Video Framerate**: **25fps** is the video frame rate by default.
- **Video Quality**: the video bit rate is from 50 to 90.

NACK

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

To enable NACK, navigate to **Phone > Call Feature > Others.**



Others

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

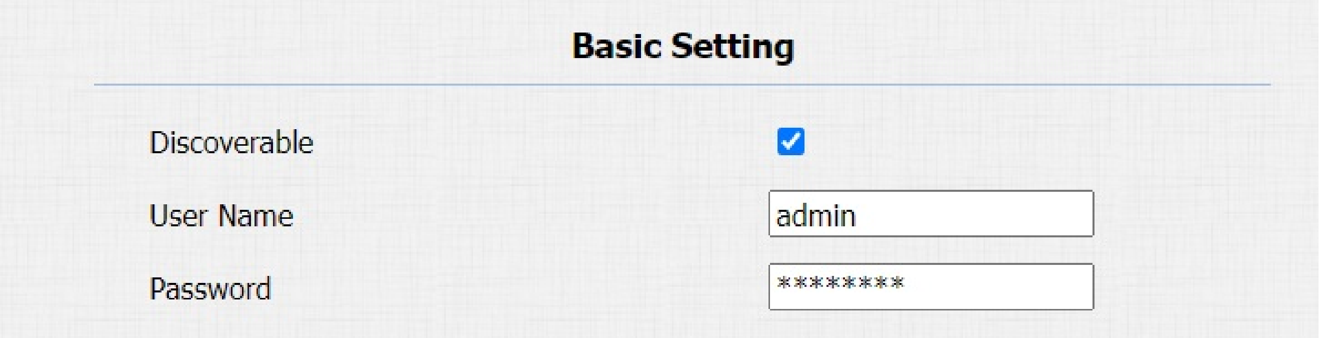
Parameter Set-up:

- **NACK Enabled**: enable the NACK. It can be used to prevent losing data packets in the weak network environment when discontinued and mosaic video images occurred.

ONVIF

You can access the real-time video from the device's camera using the Akuvox indoor monitor or other third-party devices like Network Video Recorder(**NVR**). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

You can configure the ONVIF function on the web **Intercom > ONVIF** interface so that other devices will be able to see the video from the door phone.



Basic Setting

Discoverable	☑
User Name	admin
Password	*********

Parameter Set-up:

- **Discoverable**: tick the check box to enable the **Discoverable** ONVIF mode. If you select Discoverable then the video from the door phone camera can be searched by other devices.
- **User Name**: enter the user name. The user name is **admin** by default.
- **Password**: enter the password. The password is **admin** by default.
  After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream.
  For example: http://IP address:80/onvif/device_service

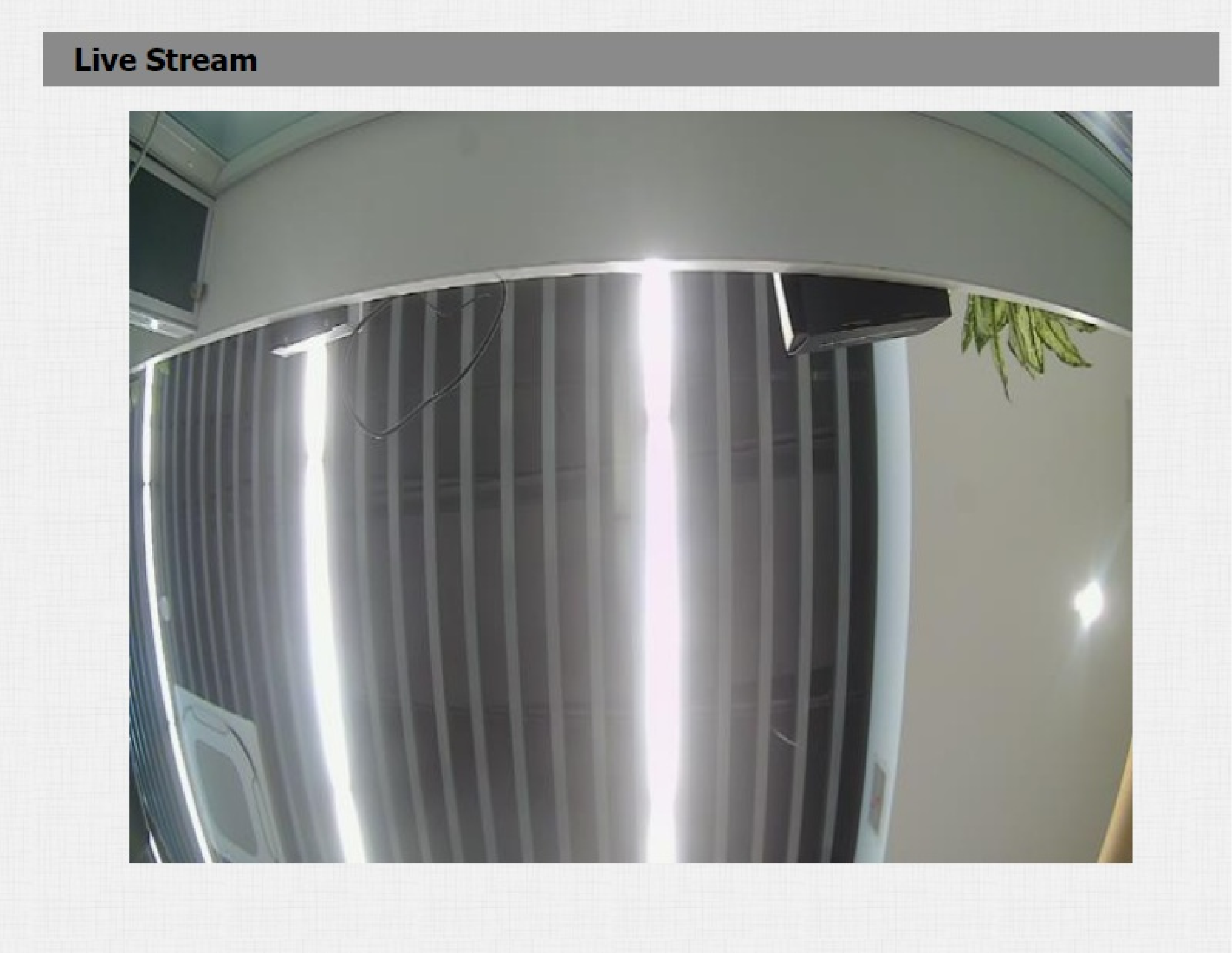
Note:

- Fill in the specific IP address of the door phone in the URL.

Live Stream

There are two ways to check the real-time video from the device. One is to go to the device web interface and view the video there. The other is to enter the correct URL on the web browser and access the video directly.

Go to the device web **Intercom > Live Stream** interface.



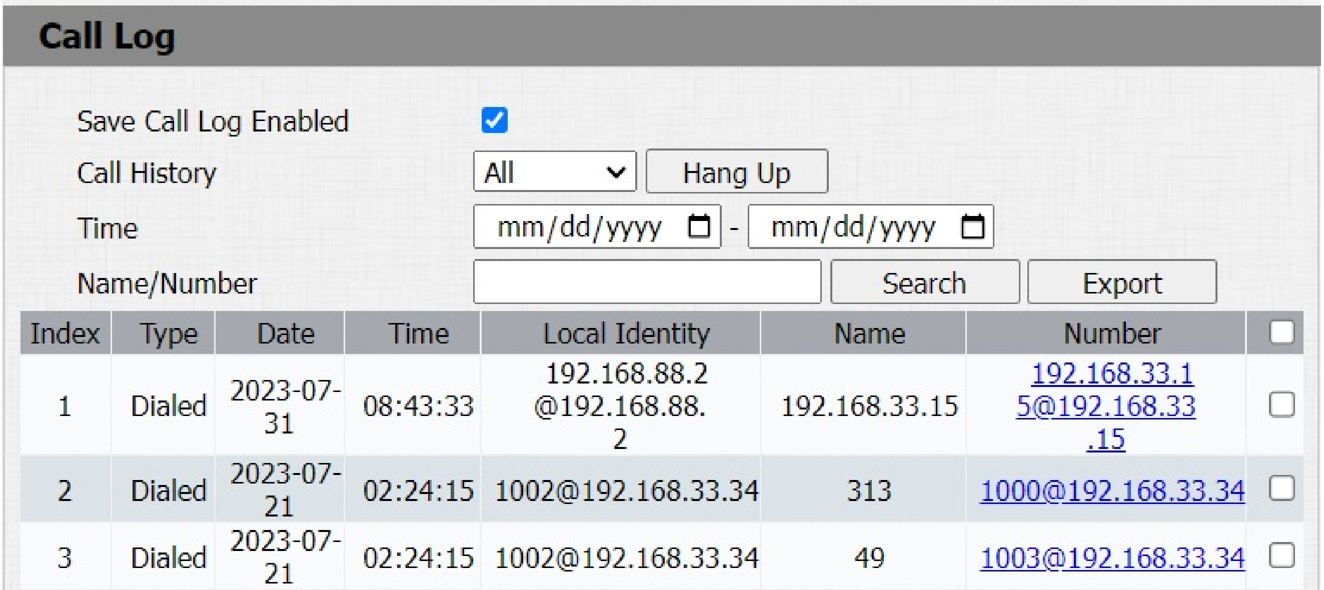
Live Stream

Logs

Call Logs

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

Go to **Phone** > **Call Log** interface.



Call Log

Save Call Log Enabled	☑
Call History	All ⌄ [Hang Up]
Time	mm/dd/yyyy - mm/dd/yyyy
Name/Number	[Search] [Export]

Index	Type	Date	Time	Local Identity	Name	Number	□
1	Dialed	2023-07-31	08:43:33	192.168.88.2@192.168.88.2	192.168.33.15	192.168.33.15@192.168.33.15	□
2	Dialed	2023-07-21	02:24:15	1002@192.168.33.34	313	1000@192.168.33.34	□
3	Dialed	2023-07-21	02:24:15	1002@192.168.33.34	49	1003@192.168.33.34	□

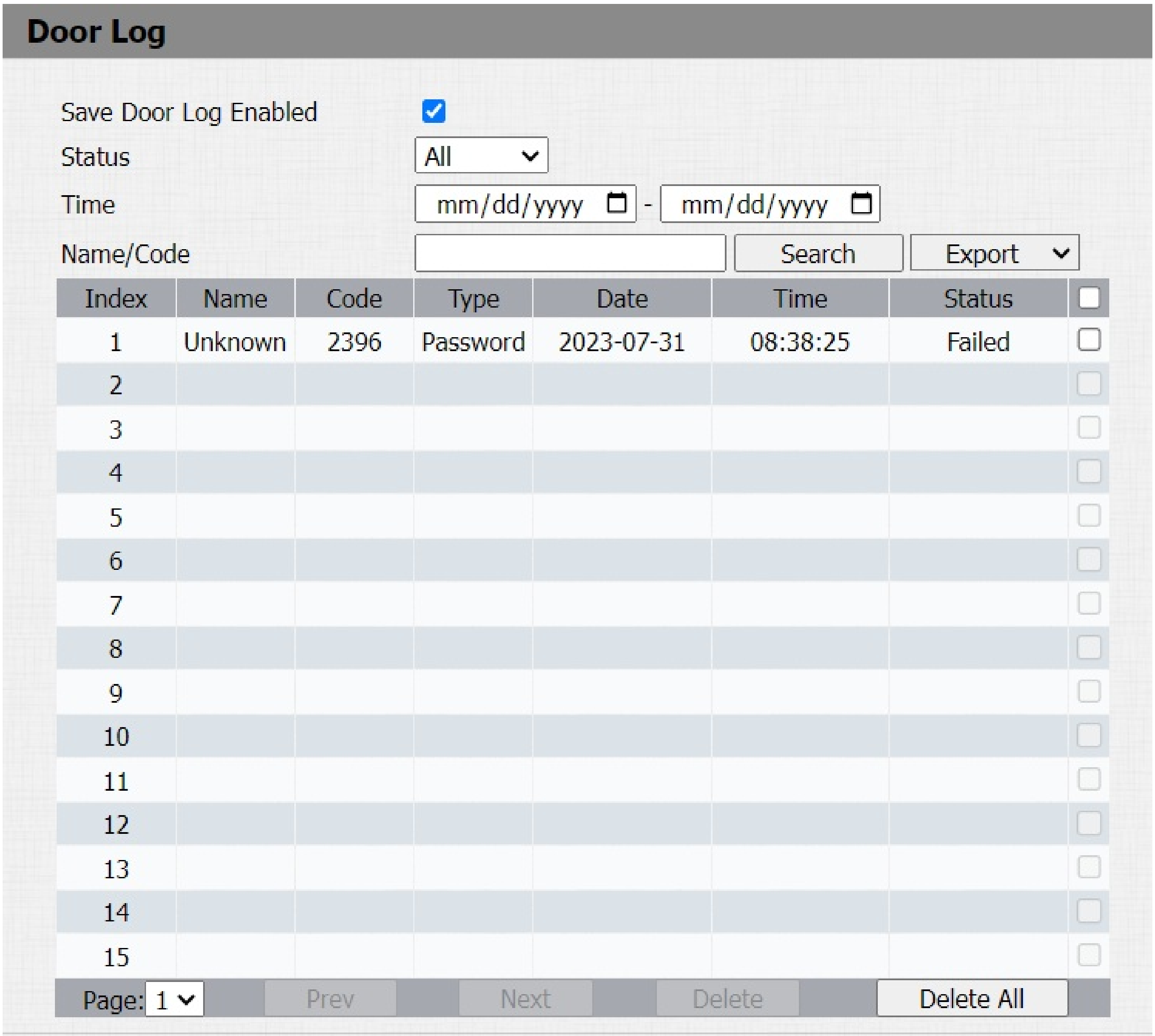
Parameter Set-up:

- **Call History**: select call history among four options: **All, Dialed, Received**, and **Missed** for the specific type of call log to be displayed.
- **Time**: select the specific time span of the call logs you want to search, check, or export.
- **Local Identity**: displays the door phone's SIP account or IP number that receives incoming calls.
- **Name/Number**: select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

Door Logs

If you want to search and check on the various types of door access history, you can search and check the door logs on the device's web.

Go to **Phone** > **Door Log** interface.



Door Log

Save Door Log Enabled	☑
Status	All
Time	mm/dd/yyyy - mm/dd/yyyy
Name/Code	[Search] [Export]

Index	Name	Code	Type	Date	Time	Status	□
1	Unknown	2396	Password	2023-07-31	08:38:25	Failed	□
2							□
3							□
4							□
5							□
6							□
7							□
8							□
9							□
10							□
11							□
12							□
13							□
14							□
15							□

Page: 1 [Prev] [Next] [Delete] [Delete All]

Parameter Set-up:

- **Status**: select between **Success** and **Failed** options to search for successful door accesses or Failed door accesses.
- **Time**: select the specific time span of the door logs you want to search, check, or export.
- **Name/Code**: select the **Name** and **Code** options to search door log by the name or by the PIN code.
- **Index**: the order of the call logs.
- **Name**: if it is a locally added key or card, the corresponding added name will be displayed. If it is an unknown key or card, it will display **Unknown**.
- **Code**: if opening the door via PIN code, the corresponding PIN code will be displayed. If opening the door via RF cards, the corresponding card number will be displayed, and if the door is opened by an HTTP command, it will be empty.

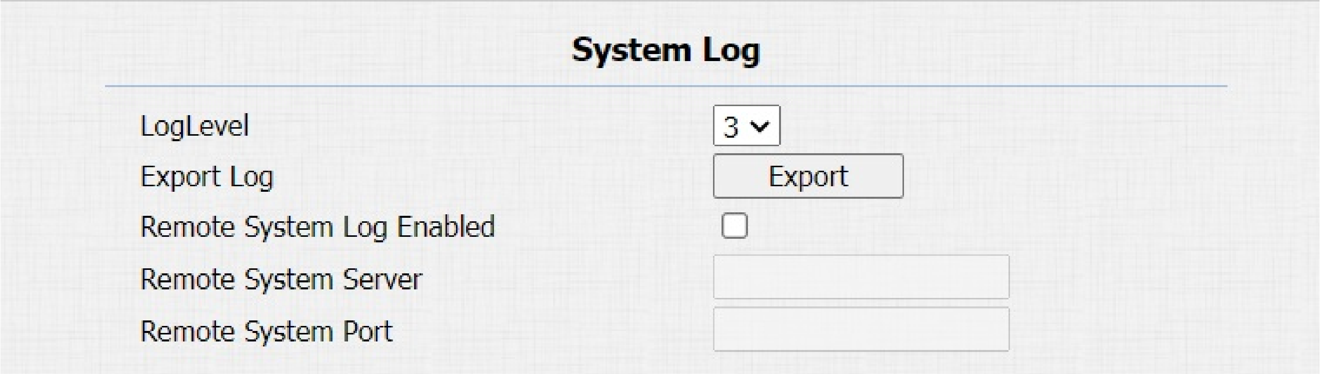
- **Type**: if opening the door via PIN code, **Password** will be displayed. If opening the door via RF cards, **Card** will be displayed, and if the door is opened by HTTP command, **Http** will be displayed.

Debug

System Log

System logs can be used for debugging purposes.

You can set up the function on the web **Upgrade > Advanced > System Log** interface.



System Log

LogLevel	3
Export Log	Export
Remote System Log Enabled	□
Remote System Server	
Remote System Port	

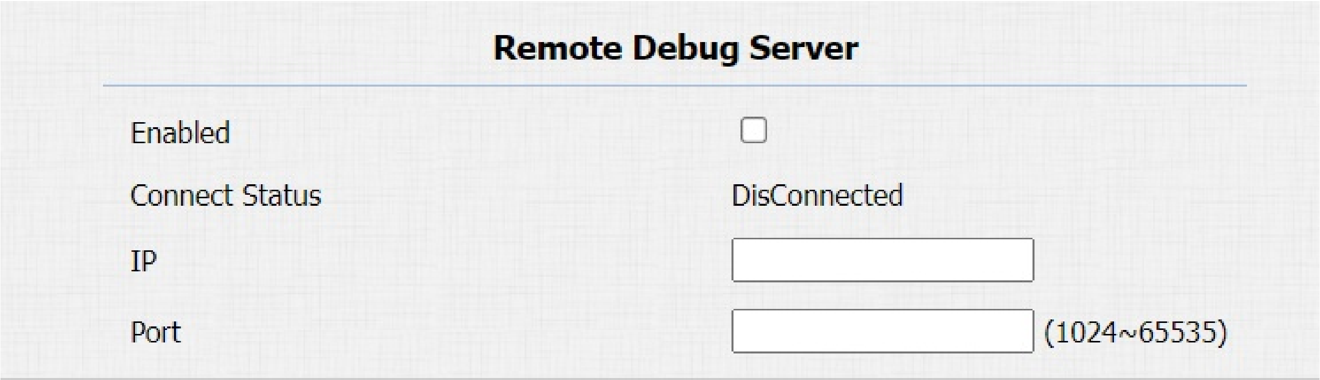
Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is **3**, the higher level is **5**, and the more complete log is **7**.
- **Export Log**: click the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Server**: enter the remote server address to receive the device log. And the remote server address will be provided by Akuvox technical support.
- **Remote System Port**: enter the remote system server port for the data transmission.

Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

On the web, Navigate to **Upgrade > Advanced > Remote Debug Server**.



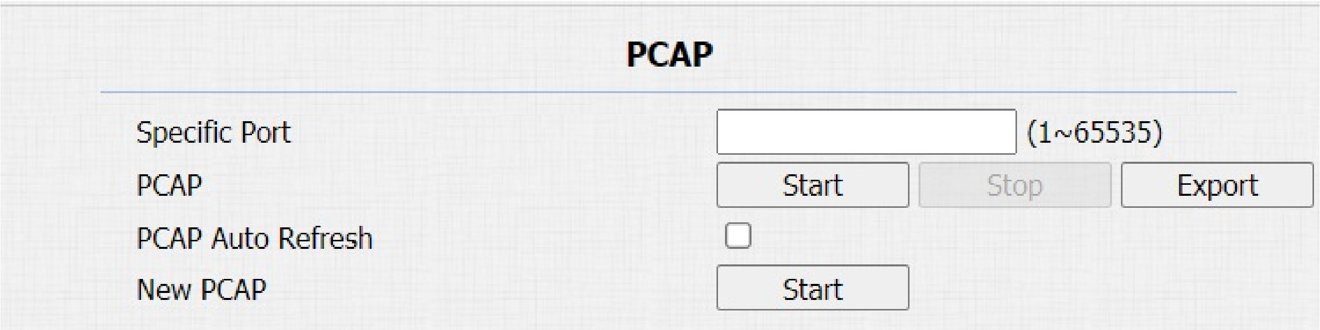
Remote Debug Server

Enabled	□
Connect Status	DisConnected
IP	
Port	(1024~65535)

PCAP

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

You can set up the PCAP on the device web **Upgrade > Advanced > PCAP** interface properly before using it.



PCAP

Specific Port	(1~65535)		
PCAP	Start	Stop	Export
PCAP Auto Refresh	□		
New PCAP	Start		

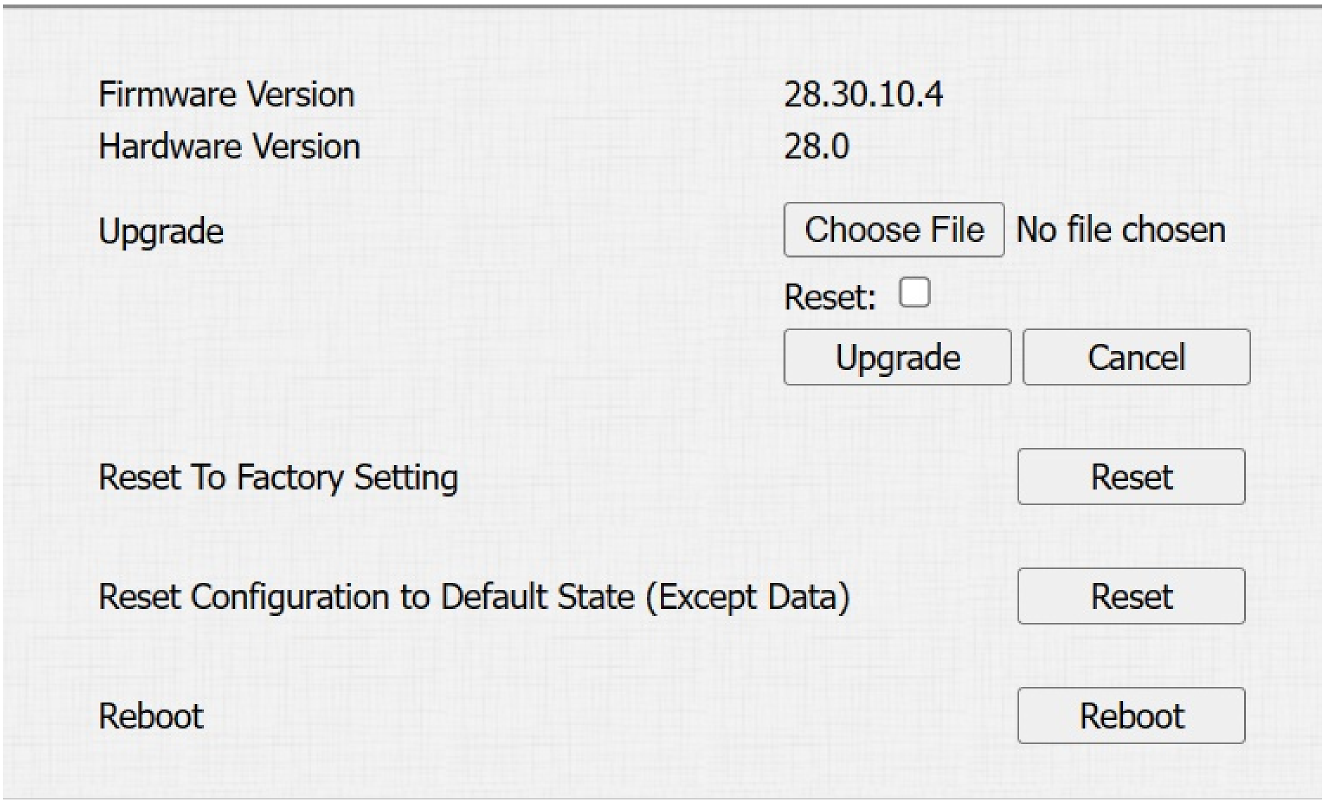
Parameter Set-up:

- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: select **Enable** or **Disable** to turn on or turn off the PCAP auto fresh function. If you set it as Enable then the PCAP will continue to capture data packets even after the data packets reached their 1M maximum in capacity. If you set it as **Disable** the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.
- **New PCAP**: click **Start** to capture a bigger data package.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Go to **Upgrade > Basic** interface.



Firmware Version	28.30.10.4
Hardware Version	28.0
Upgrade	Choose File No file chosen Reset: □ Upgrade Cancel
Reset To Factory Setting	Reset
Reset Configuration to Default State (Except Data)	Reset
Reboot	Reboot

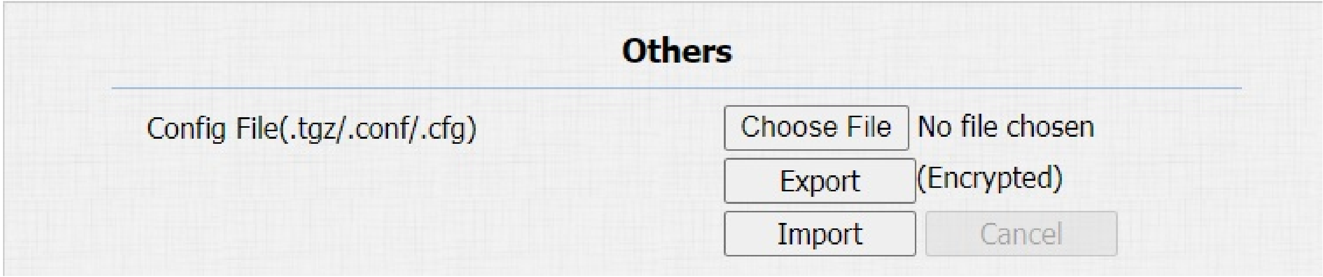
Parameter Set-up:

- **Upgrade**: choose .rom firmware from your PC, then click **Upgrade** to update. If you want to upgrade the firmware and reset the device to the factory setting, tick the **Reset** check box.

Backup

You can import or export encrypted configuration files to your Local PC.

Go to **Upgrade > Advanced > Others** interface if needed.



Others

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

Parameter Set-up:

- **Choose File**: to choose the config file in your PC.
- **Export/Import**: to export the current config file (Encrypted) or import a new config file.

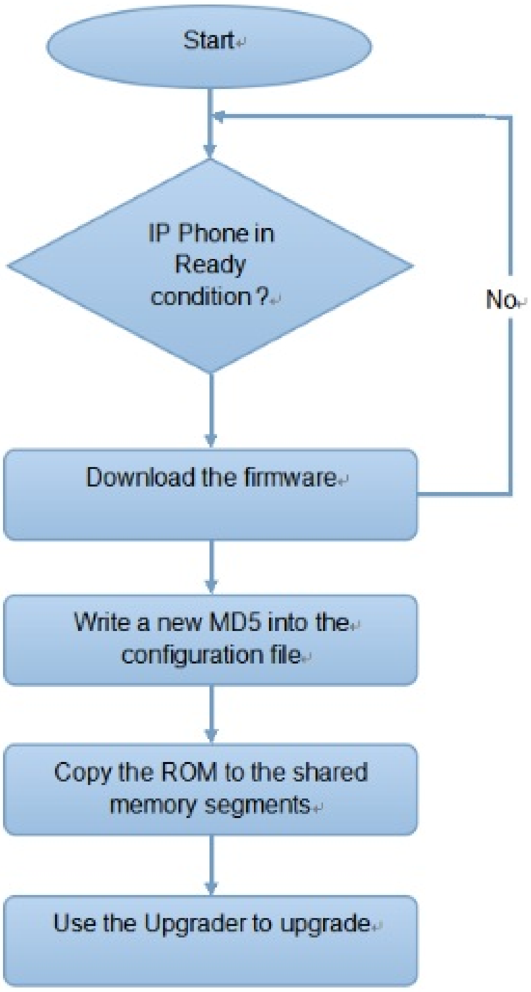
Auto-provisioning

Configurations and upgrading on the device can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the access control terminal.

Provisioning Principle

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

Please 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

Configuration Files for Auto-provisioning

Configuration files have two formats for auto-provisioning. One is the general configuration files used for the general provisioning and the other one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown below:

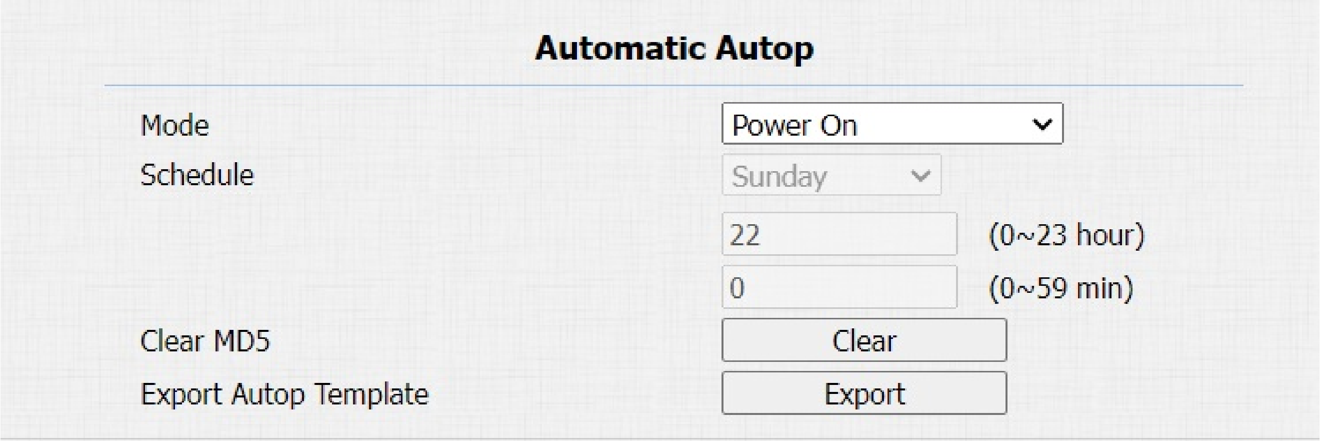
- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used for auto-provisioning on a specific device, as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number 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 these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

You may click here to see the detailed format and steps.

To get the Autop configuration file template on **Upgrade** > **Advanced** > **Automatic Autop** interface.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23 hour)

0 (0~59 min)

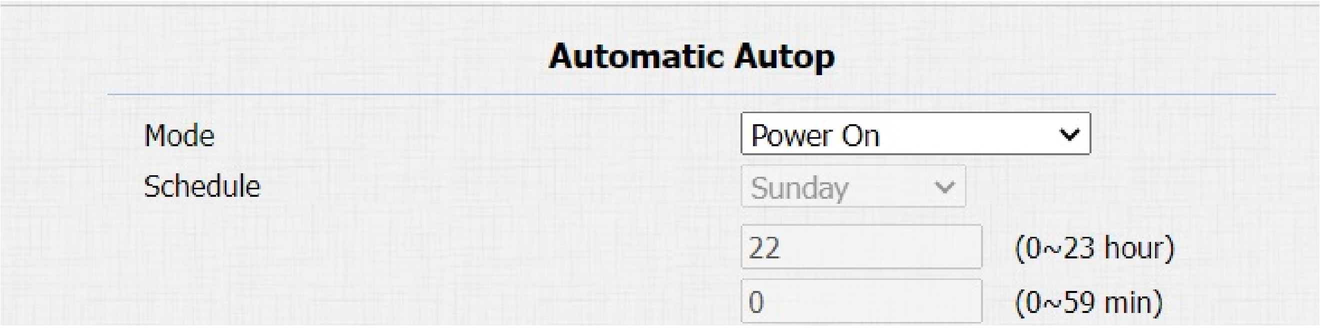
Clear MD5

Export Autop Template

AutoP Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself according to the schedule.

Navigate to **Upgrade > Advanced > Automatic Autop**.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23 hour)

0 (0~59 min)

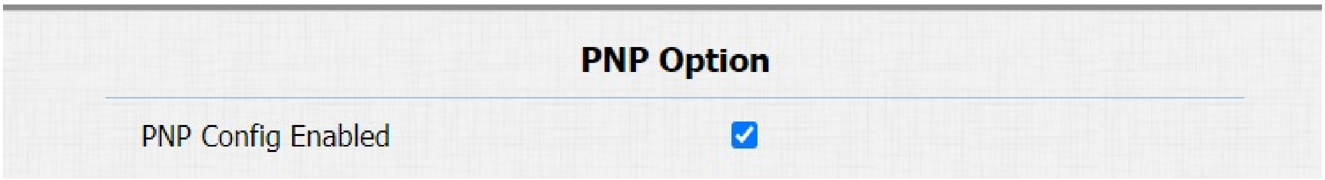
Parameter Set-up:

- **Mode**: select **Power on, Repeatedly, Power On + Repeatedly, Hourly Repeat** as your Autop schedule.
    - Select **Power on**, if you want the device to perform Autop every time it boots up.
    - Select **Repeatedly**, if you want the device to perform Autop according to the schedule you set up.
    - Select **Power On + Repeatedly**, if you want to combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
    - Select **Hourly Repeat**, if you want the device to perform Autop every hour.

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 do this configuration on web **Upgrade > Advanced > PNP Option** interface.



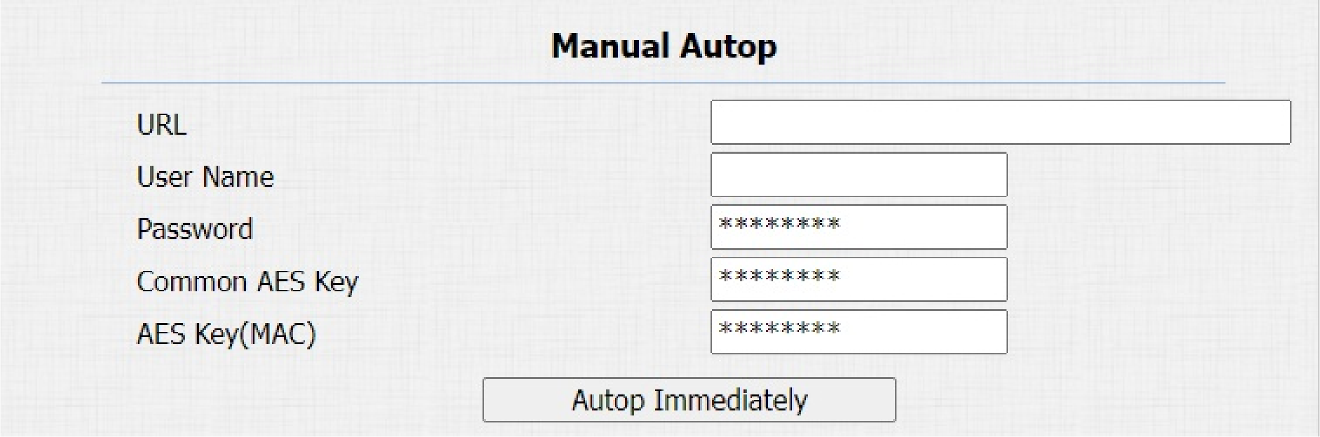
PNP Option

PNP Config Enabled ☑

Static Provisioning Configuration

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

Navigate to **Upgrade** > **Advanced** > **Manual Autop** interface.



Manual Autop

URL	
User Name	
Password	*********
Common AES Key	*********
AES Key(MAC)	*********

Parameter Set-up:

- **URL**: set up **TFTP, HTTP, HTTPS, and FTP** server addresses for the provisioning
- **User Name**: set up a user name if the server needs a user name to be accessed otherwise leave it blank.
- **Password**: set up a password if the server needs a password to be accessed otherwise leave it blank.
- **Common AES Key**: set up AES code for the intercom to decipher the general Auto Provisioning configuration files.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

- AES as one type of 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)

Tip

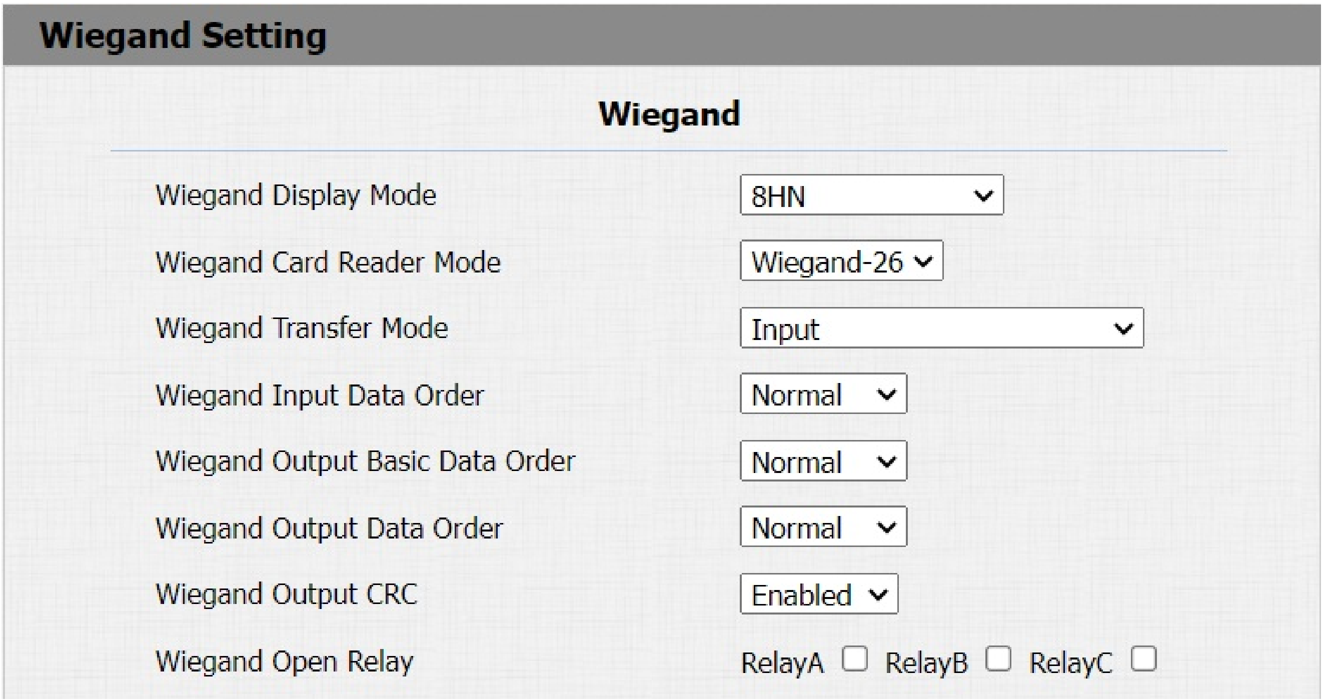
- Akuvox do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Integration with Third Party Device

Integration via Wiegand

The Wiegand feature enables Akuvox door phone to act as a controller or a card reader.

you can configure the Wiegand on the web **Intercom > Wiegand** interface.



Wiegand Setting

Wiegand

Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Wiegand-26
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output CRC	Enabled
Wiegand Open Relay	RelayA □ RelayB □ RelayC □

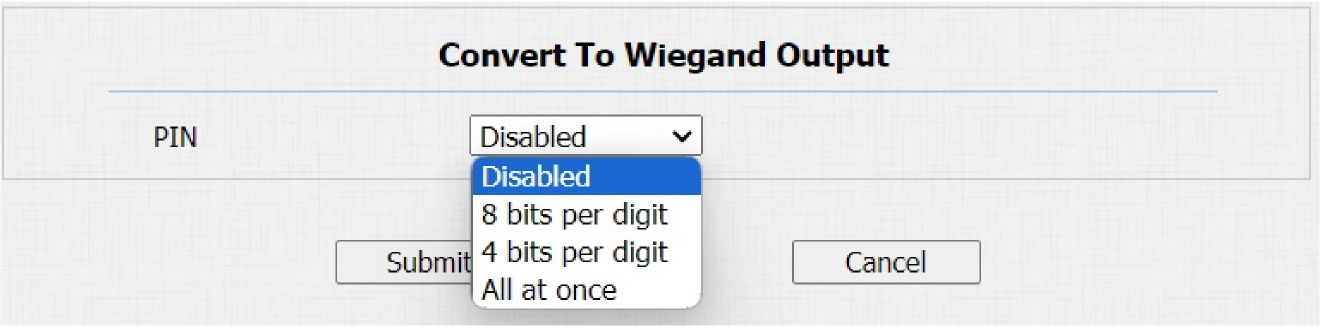
Parameter Set-up:

- **Wiegand Display Mode**: select Wiegand Card code format among **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.**
- **Wiegand Card Reader Mode**: set the Wiegand data transmission format among three options: **Wiegand 26, Wiegand 34, Wiegand 58.** The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode**: select **Input, Output, Convert to Card No. Output Wiegand.** If the door phone is used as a receiver, then set it as **Input** for the door phone. Select **Output** if you want Wiegand output to be 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 between **Normal** and **Reversed.** If you select **Reversed** then the input card number will be reversed and vice versa.

-
    - **Wiegand Output Basic Data Order**: set the Wiegand output data sequence between **Normal** and **Reversed**.

- **Wiegand Output Data Order**: set the Wiegand output data sequence between **Normal** and **Reversed**.
- **Wiegand Output CRC**: tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.

When integrating with third-party devices, you need to set up the Wiegand PIN code output based on the Wiegand output format of the third-party device.



Convert To Wiegand Output

PIN: Disabled

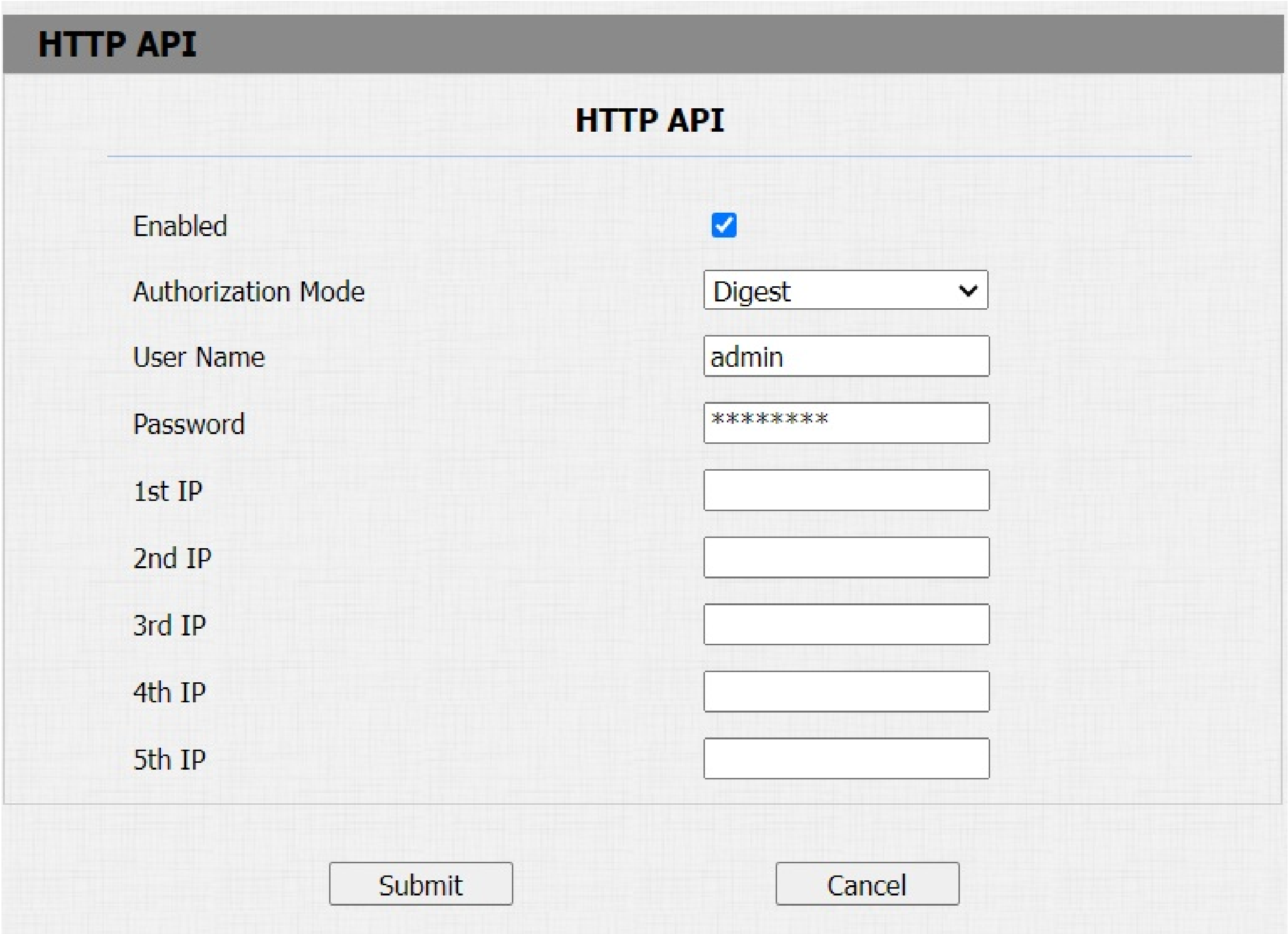
Parameter Set-up:

- **PIN**: enable or disable the Wiegand PIN code output based on your need. Select the Wiegand PIN code output format when you enable it.
- **8 bits per digit**: select it if the third-party device adopts 8 bits per digit format. The PIN code is transferred separately by a digit (one digit consists of 8 bits).
- **4 bits per digit**: select it if the third-party device adopts 4 bits per digit format. The PIN code is transferred separately by a digit (one digit consists of 4 bits).
- **All at once**: select it if the third-party device adopts All at once format. When it is selected, the PIN code will not be transferred until you enter the whole PIN code.

Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device and the Akuvox device.

You can configure the HTTP API function on the web **Intercom** > **HTTP API** interface for the integration.



HTTP API

HTTP API

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

Parameter Set-up:

- **HTTP API**: select **Enable** or **Disable** to enable or disable the HTTP API function for the third-party integration. For example, if the function is disabled, any request to initiate the integration will be denied and HTTP 403 forbidden status will be returned.
- **Auth Mode**: select among four options: **None, Normal, Allowlist, Basic, Basic, Digest** and **Token** for authorization type, which will be explained in detail in the following chart.
- **User Name**: enter the user name when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **Password**: enter the password when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **IP01-IP05**: enter the IP address of the third-party devices when the WhiteList authorization is selected for the integration.

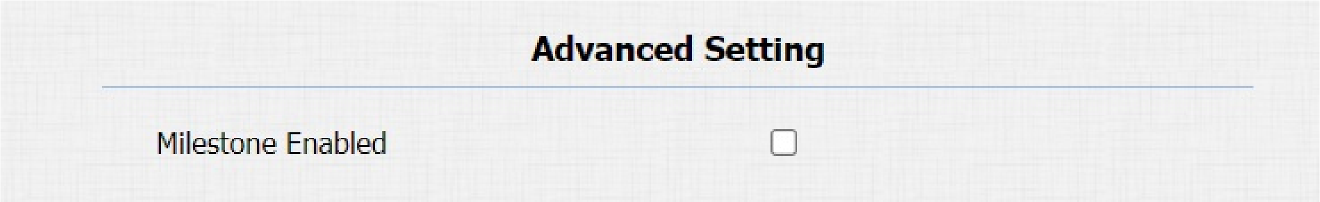
Please refer to the following description for the Authentication mode

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication. The whitelist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the user name and the password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode the username and password.
5	Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of the HTTP request header: WWW-Authenticate: Digest realm="HTTP API",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

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 do so, go to **Intercom > ONVIF**.



Advanced Setting

Milestone Enabled □

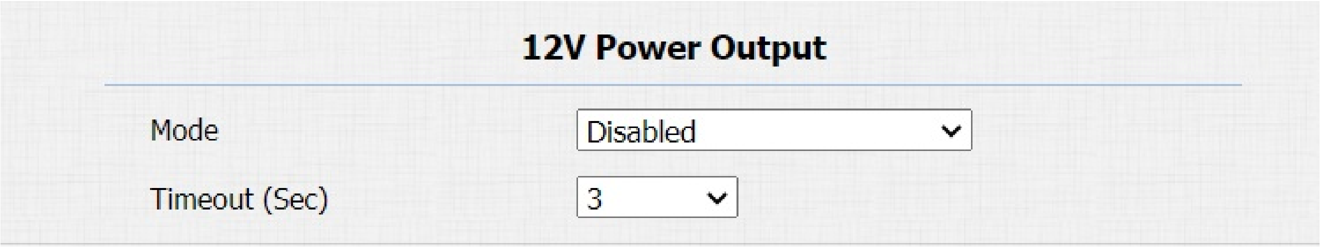
Parameter Set-up:

- **Milestone Enabled**: enable integration with the Milestone system. It is disabled by default.

Power Output Control

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

Path: **Intercom > Advanced >12V Power Output.**



12V Power Output

Mode: Disabled

Timeout (Sec): 3

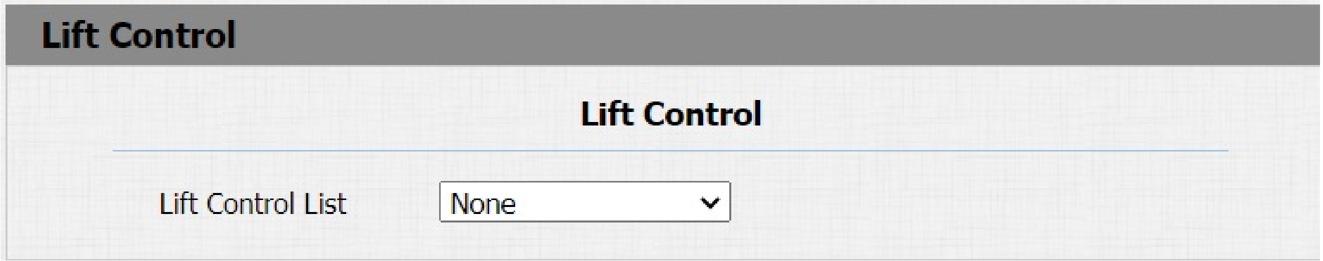
Parameter Set-up:

- **12V Power Output**: select **Disabled** to disable the power output function; select **Always** to enable the access controller to provide continuous power to the third-party device. Select **Triggered By Open Relay** if you want the R27 to provide power to the third party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.
- **Time Out (Sec)**: select the power supply time duration after the relay is triggered. Three options: **3, 5, 10.** It is 3 seconds by default. The power output is 12V, and the maximum output amperage is 0.8A.

Integration with Lift Control

The door phones can be connected to the Akuvox lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through various types of access methods on the door phone.

To set up the lift control, go to **Intercom > Lift Control** interface.



Lift Control

Lift Control

Lift Control List: None

Parameter Set-up:

- **Lift Control List**: select integration mode among seven Options: **None, Chiyu, KeyKing, ZKT, Akuvox EC32.** The detail for the options will be provided in the following chart.

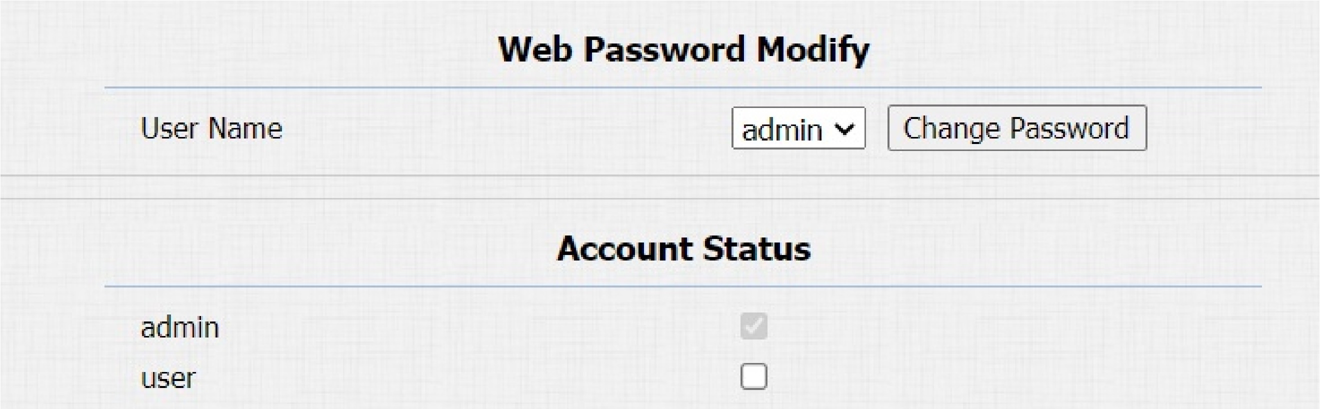
NO.	Integration Mode	Description
1	None	If you select None then the RS485 integration will be disabled.
2	Chiyu	Select Chiyu if you want to integrate with the Chiyu lift controller.
3	KeyKing	Select Keyking if you want to integrate with the KeKing lift controller.
4	ZKT	Select ZKT if you want to integrate with the ZKTeco lift controller.
5	Akuvox EC32	Select Akuvox EC32 if you want to connect the device with the Akuvox EC32 lift controller.

Password Modification

Modifying Device Web Interface Password

To change the default web password on web **Security** > **Basic** interface.

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



Web Password Modify

User Name: admin ▾ | Change Password

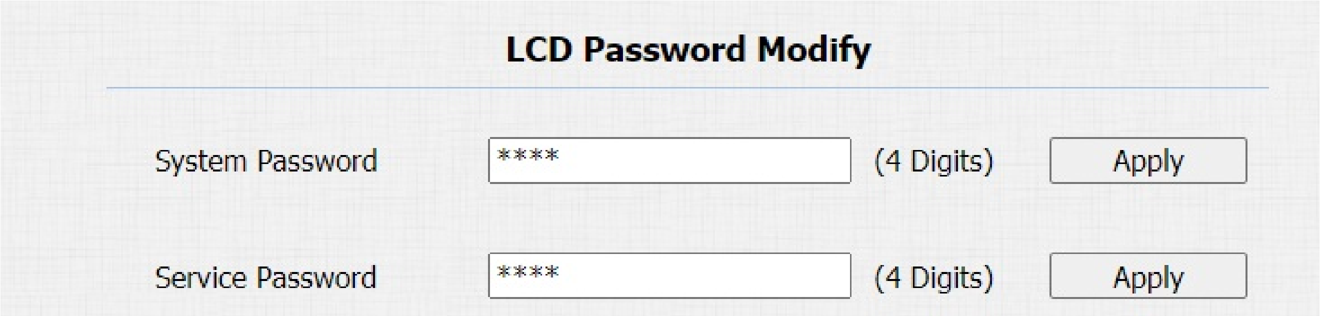
Account Status

admin ☑

user □

Modifying Device System Password

You can modify both device system password and service (setting) password on the web or on the device. On the web, navigate to **Security** > **Basic** > **LCD Password Modify**, and change the passwords if needed. The default system password is *2396#, and the default **service (setting)** password is **3888**.



LCD Password Modify

System Password: **** (4 Digits) | Apply

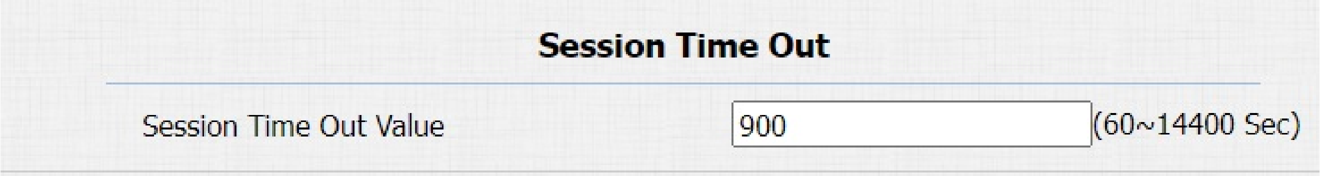
Service Password: **** (4 Digits) | Apply

To set or modify the system and service passwords on the device, press the system password (which is *2396# by default), select **Admin Access**, and select **Set Admin Password**, then set the system password. Select **Set Service Password**, then set the service password. You can delete the passwords if needed.

Configure Web Interface Automatic Logout

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation.

To do the configuration on the web **Security > Basic > Session Time Out** interface.



Session Time Out

Session Time Out Value: 900 (60~14400 Sec)

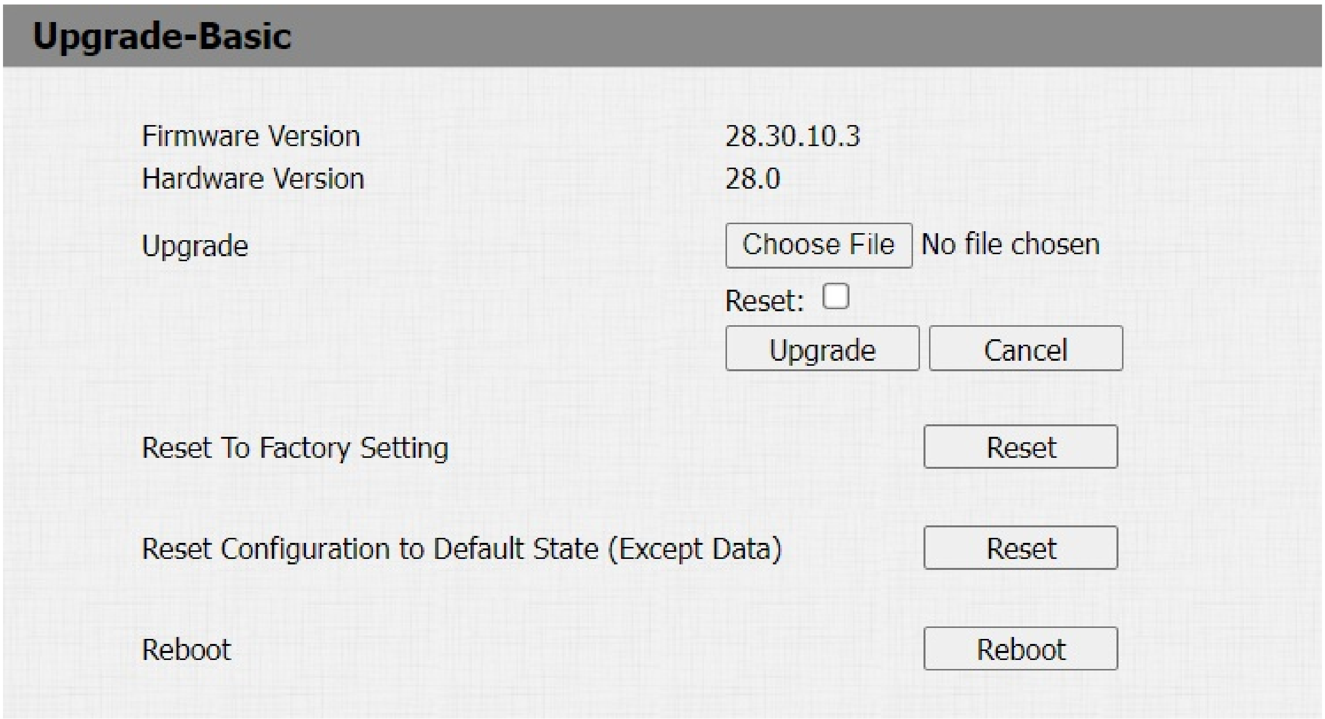
Parameters Set-up:

- **Session Time Out Value**: the range from 60 to 14400 sec. If there is no operation over time, you need to log in to the website again.

System Reboot&Reset

Reboot

If you want to restart the device system, you can operate it on the device **Upgrade > Basic** web interface as well.



Upgrade-Basic

Firmware Version 28.30.10.3

Hardware Version 28.0

Upgrade

Reset: □

Reset To Factory Setting

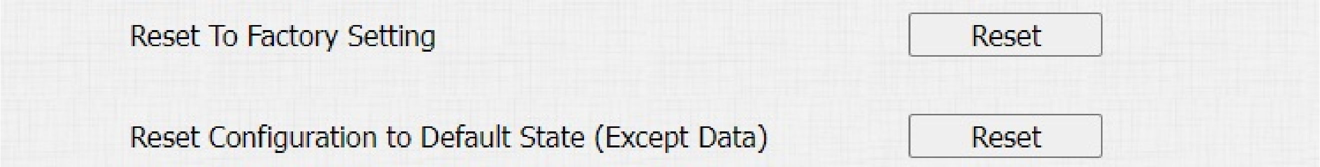
Reset Configuration to Default State (Except Data)

Reboot

Reset

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, and so on). Or, select **Reset Configuration to Default State (Except Data) Reset**, if you want to reset the device (retaining the user data).

To reset the device, go to **Upgrade > Basic**.



Reset To Factory Setting

Reset Configuration to Default State (Except Data)