About This Manual

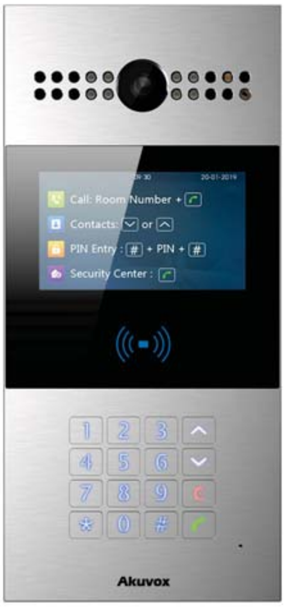
Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX R28A SERIES
DOOR PHONE
Administrator Guide

Thank you for choosing Akuvox R28A 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 228.30.10.116 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



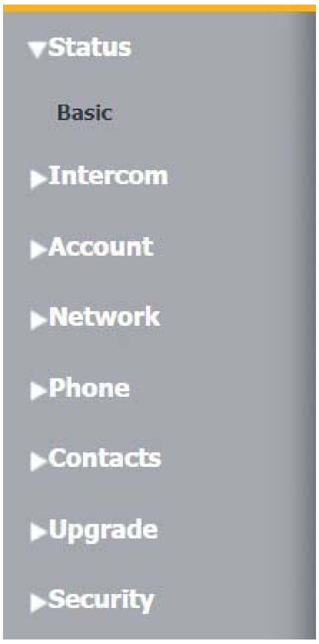
The ability to control access to your building and verify identities is invaluable. The Akuvox R28A is a SIP-compliant, hands-free door phone with optional video capabilities. It connects to Akuvox indoor monitors for remote access control and monitoring. Users can communicate with visitors through audio and video calls and unlock the door as needed. This door phone simplifies monitoring of entrances, providing peace of mind and enhanced security for your facility.

Model Specification

Model	R28A
Camera	2 Megapixels, automatic lighting
Light Sensor	✔
Motion Sensor	✔
Wiegand Port	✔
Relay In	x3
Relay Out	x3
RS485	✔
Card Reader	13.56MHz&130kHz,NFC
Microphone	x1
Speaker	x1
Power Out	12V/400mA(Max.)
Tamper Alarm	✔
Power Supply	802.3af Power-over-Ethernet or 12V power adapter

Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, account information, etc.
- **Intercom**: This section covers intercom call setting, user management, access schedule, input control, relay management, card settings, 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 and video codec setup, etc.
- **Network**: This section mainly deals with DHCP and Static IP settings, RTP port settings, device deployment, SNMP, VLAN, TR069, and web server setup.
- **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 and reboot, configuration file auto-provisioning, fault diagnosis, etc.
- **Security**: This section is for password modification and server certificate upload.

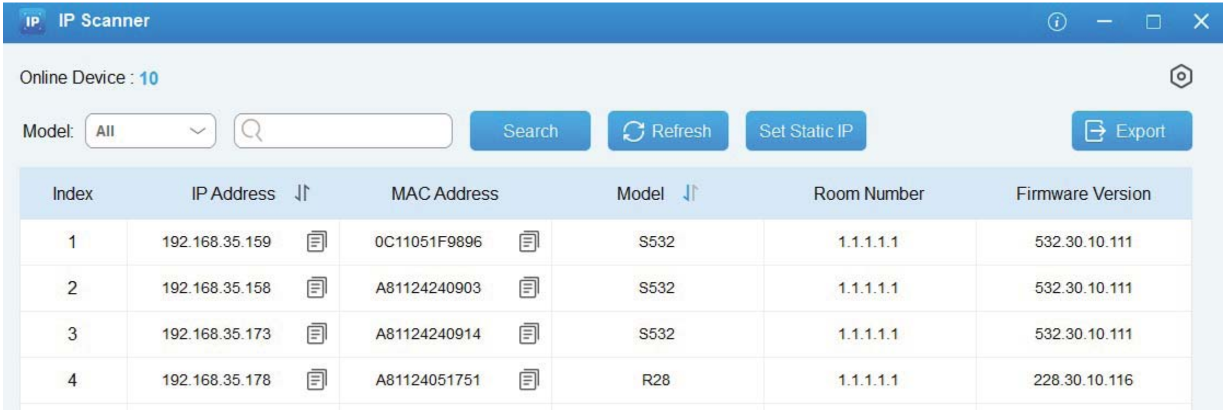


Access the Device

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

Obtain Device IP Address

Search for the device IP using the IP scanner in the same LAN network. Click **Refresh** to update the list.



Online Device : 10

Model: All

Index	IP Address	MAC Address	Model	Room Number	Firmware Version
1	192.168.35.159	0C11051F9896	S532	1.1.1.1.1	532.30.10.111
2	192.168.35.158	A81124240903	S532	1.1.1.1.1	532.30.10.111
3	192.168.35.173	A81124240914	S532	1.1.1.1.1	532.30.10.111
4	192.168.35.178	A81124051751	R28	1.1.1.1.1	228.30.10.116

Access the Device Setting

Press “*2396#” to access the device’s admin settings including:

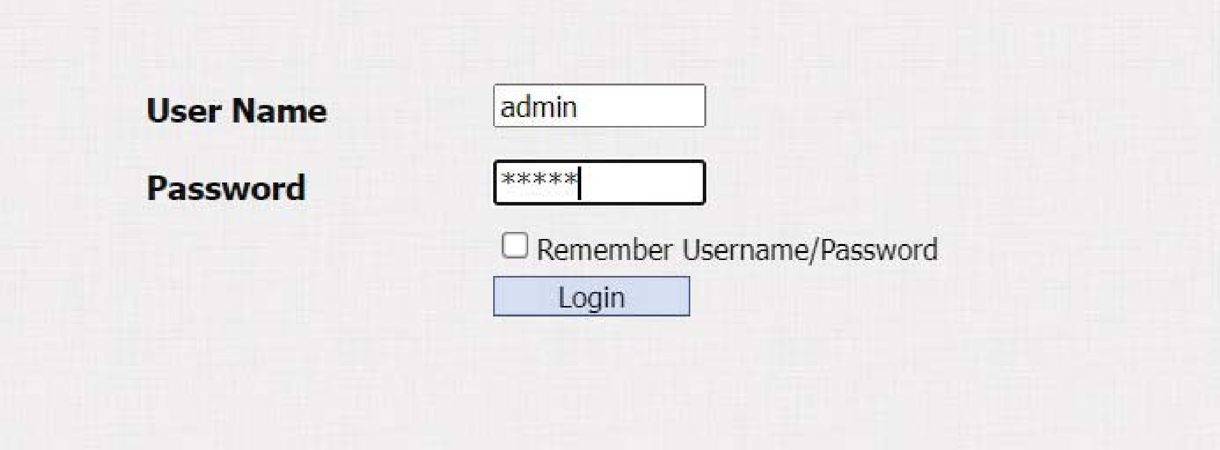
- system information;
- admin password and admin card management;
- system network settings;
- system reset.

You can check the device’s IP, MAC, and firmware version on the System Information screen.

Access Device’s Web Settings

You can enter the device IP address in a browser and log into the device web interface where you can configure and adjust parameters.

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



User Name admin

Password *****

□ Remember Username/Password

Note

- Download the IP Scanner: 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

Language

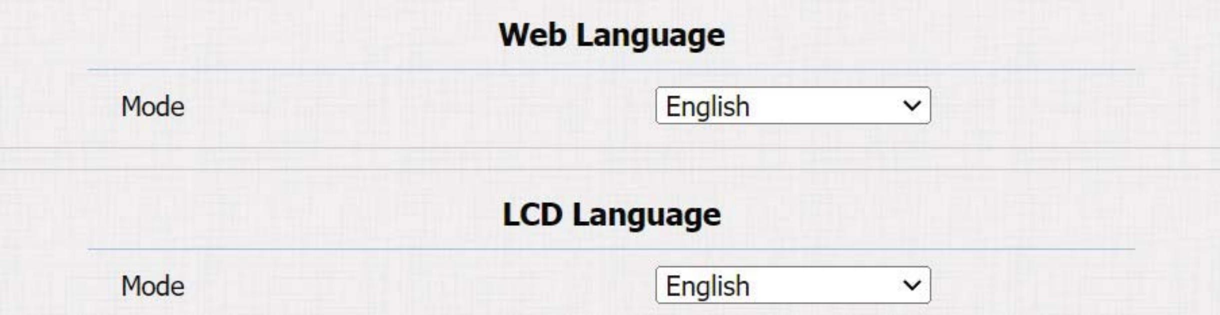
You can select the device's LCD and web language on the **Phone > Time/Lang** interface.

The device web supports the following languages:

- English, Traditional Chinese, Dutch, French, German, and Japanese.

The device LCD supports the following languages:

- English, Russian, Portuguese, Spanish, Italian, Dutch, French, German, Hebrew, Polish, Turkish, Czech, Norwegian, Montenegrin, and Ukrainian.



Web Language

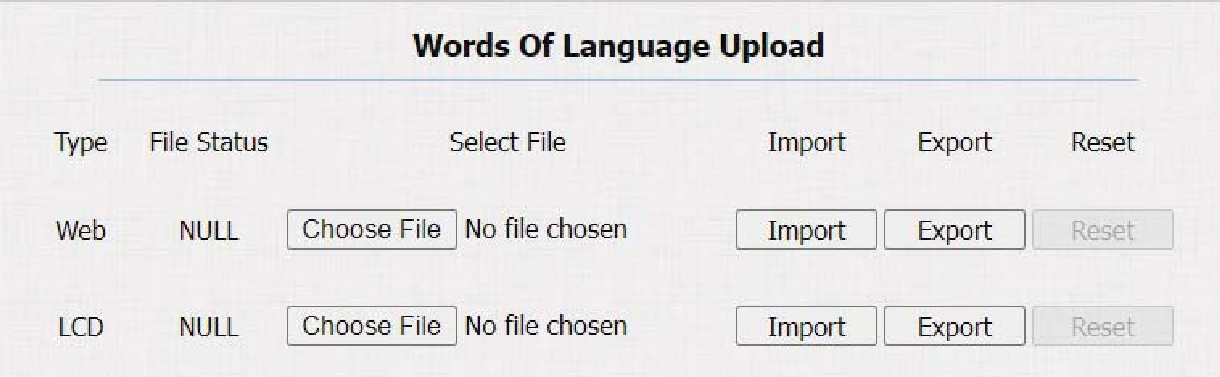
Mode: English

LCD Language

Mode: English

To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device.

Set it up on the **Phone > Time/Lang > Words of Language Upload** interface.



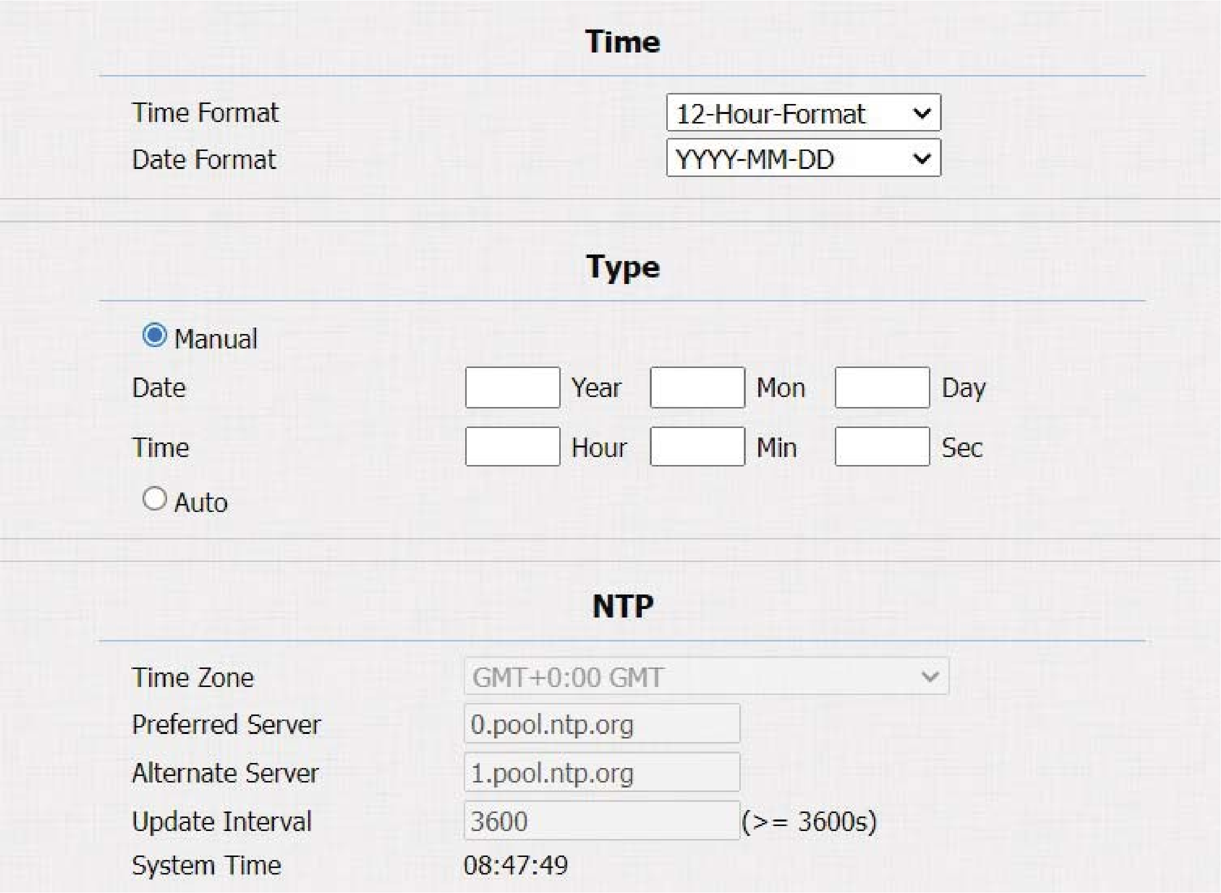
Words Of Language Upload

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

The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on 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

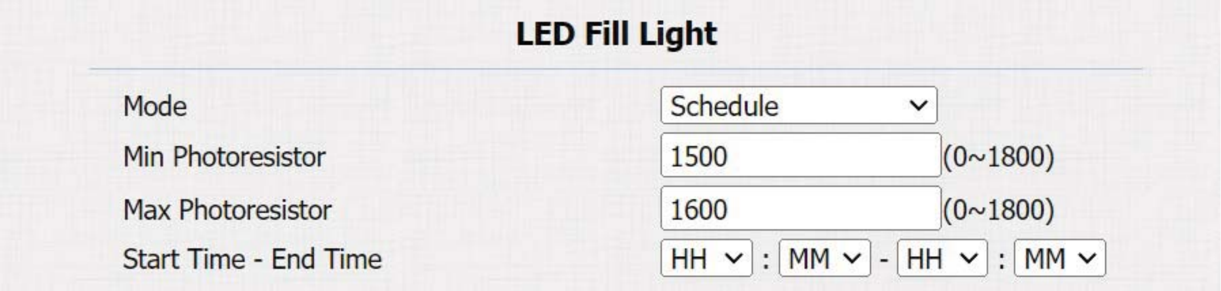
- **Time Format**: Select the 12-hour format or the 24-hour format.
- **Type**: You can set up the time manually by selecting **Manual**.
- **Preferred/Alternate Server**: The NTP server address. The alternate server will take effect when the primary server is invalid.
- **Update Interval**: The interval between two consecutive NTP requests.

Screen Display and LED Setting

Infrared LED Setting

Infrared LED is mainly designed to reinforce the light at night or in a dark environment.

Set it up on the web **Intercom > LED Setting > LED Fill Light**.



LED Fill Light

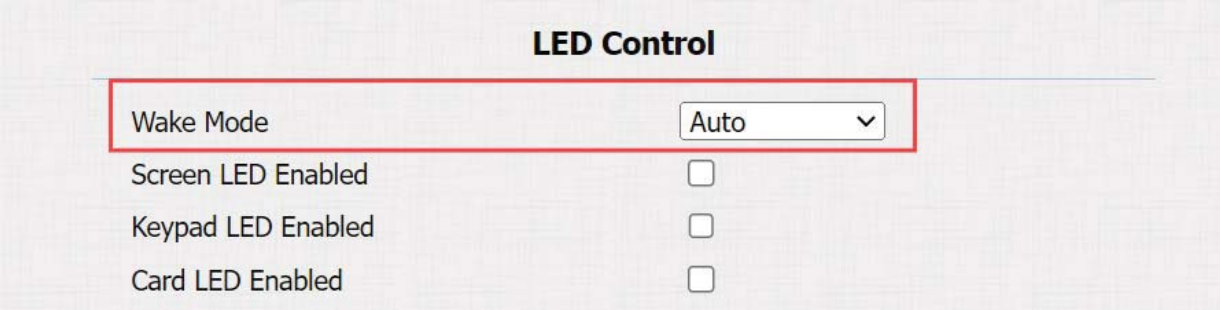
Mode	Schedule
Min Photoresistor	1500 (0~1800)
Max Photoresistor	1600 (0~1800)
Start Time - End Time	HH : MM - HH : MM

- **Mode**:
  - **Auto:** Turn on the LED light automatically based on the minimum and maximum photoresistor value.
  - **Always On:** Enable the LED light.
  - **Always Off:** Disable the LED light.
  - **Schedule:** Turn on the LED light based on the schedule. Specify the Start Time and End Time when this option is selected.
- **Min/Max Photoresistor**: Set the minimum and maximum photoresistor value to automatically control the ON-OFF of the LED light. If the photoresistor value is less than the minimum threshold, turn off the LED. If the photoresistor value is greater than the maximum threshold, turn on the LED.

LED Wakeup Mode

You can set the card reader light to be controlled by infrared detection.

To set it up, go to **Intercom > LED Setting > LED Control** interface.



LED Control

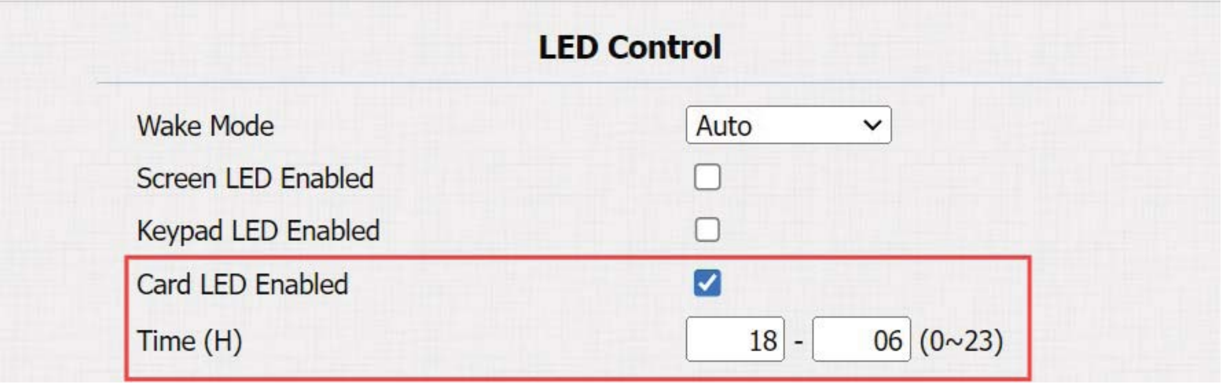
Wake Mode	Auto
Screen LED Enabled	□
Keypad LED Enabled	□
Card LED Enabled	□

- **Wake Mode**:
  - **Auto**: When the infrared detection is triggered, the card reader light will be on.
  - **Manual**: The LED is not controlled by infrared detection.

Card Reader LED Control

You can enable or disable the LED lighting on the card reader area. You can also set a specific time to turn on the light.

To set it up, go to **Intercom > LED Setting > LED Control** interface.



LED Control

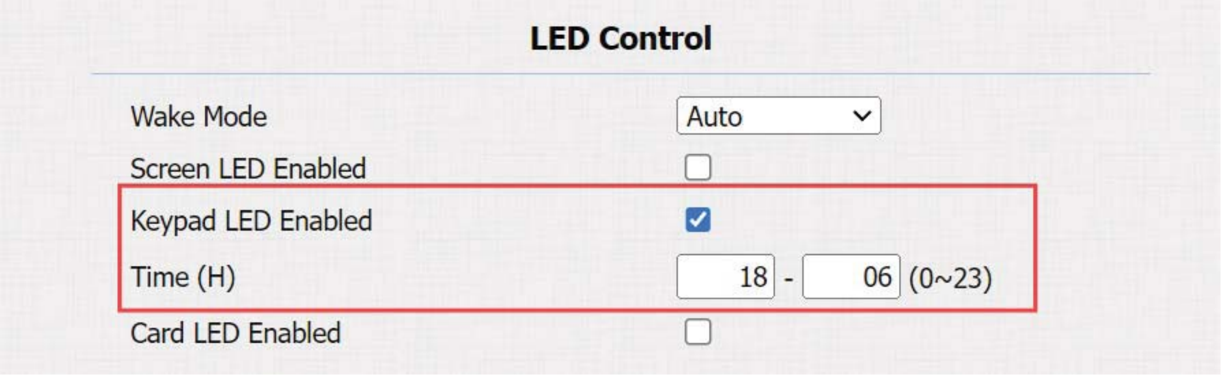
Wake Mode	Auto
Screen LED Enabled	□
Keypad LED Enabled	□
Card LED Enabled	☑
Time (H)	18 - 06 (0~23)

- **Card LED Enabled**: When enabled, specify the period when the light is on.

Keypad LED Control

You can enable or disable the LED lighting of the keypad. You can also set a specific time to turn on the light.

To set it up, go to **Intercom > LED Setting > LED Control** interface.



LED Control

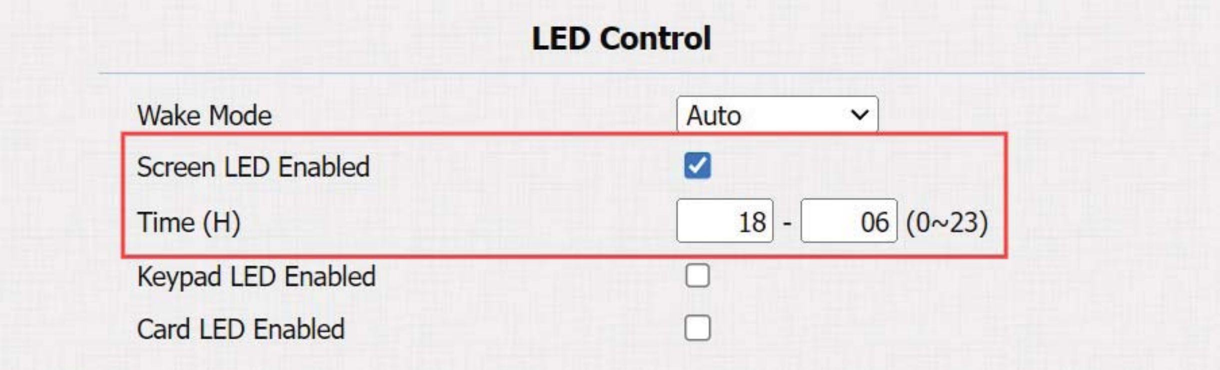
Wake Mode	Auto
Screen LED Enabled	□
Keypad LED Enabled	☑
Time (H)	18 - 06 (0~23)
Card LED Enabled	□

- **Keypad LED Enabled**: When enabled, specify the period when the light is on.

LED Settings on Screen

You can enable or disable the LED lighting of the screen and set a specific time to turn on the light.

To set it up, go to **Intercom > LED Setting > LED Control.**



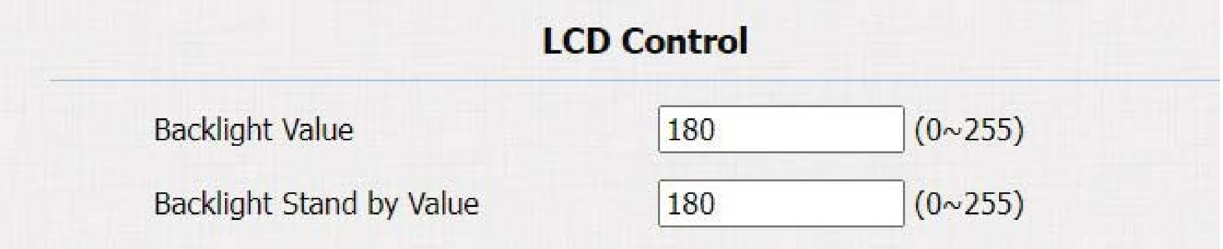
LED Control

Wake Mode	Auto
Screen LED Enabled	☑
Time (H)	18 - 06 (0~23)
Keypad LED Enabled	□
Card LED Enabled	□

- **Screen LED Enabled:** When enabled, specify the period when the light is on.

Backlight Setting

If you want to brighten up the screen to see the screen with ease in an environment with higher light intensity, you can set up the backlight on the **Intercom > LED Setting > LCD Control** interface.



LCD Control

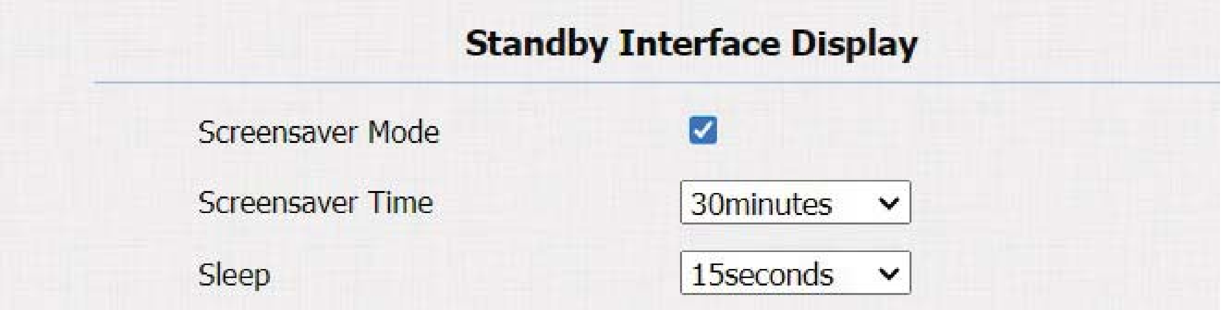
Backlight Value	180 (0~255)
Backlight Stand by Value	180 (0~255)

- **Backlight Value**: Set the backlight value when the device is working from 0-255.
- **Backlight Standby Value**: Adjust the backlight for the screen in standby mode 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 set it up, go to **Intercom > LED Setting > Standby Interface Display** interface.



Standby Interface Display

Screensaver Mode	☑
Screensaver Time	30minutes
Sleep	15seconds

- **Screensaver Mode:** Enable or disable the user of screen saver. If disabled, the device screen will directly turn dark when it is in standby mode.
- **Screensaver Time**: Set the screen saver duration time(5 seconds to 2 hours).

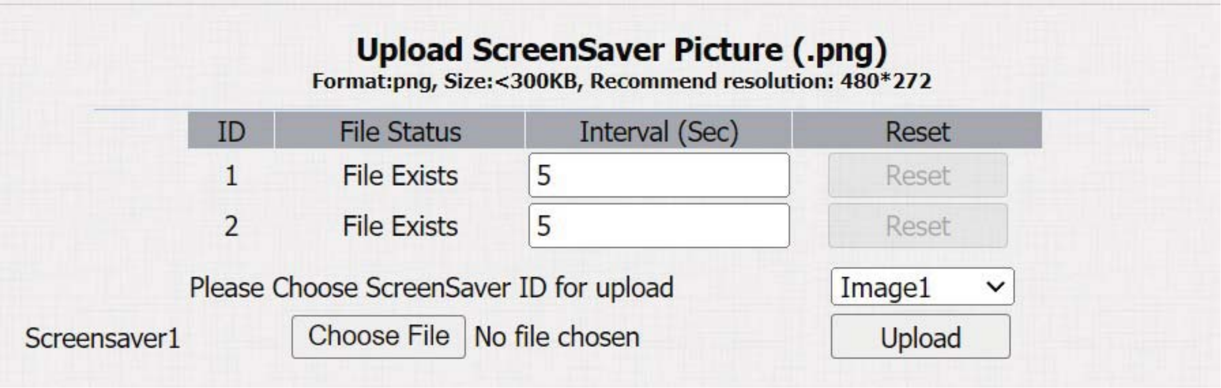
- **Sleep**: The time to start the screen saver mode(5 seconds to 30 minutes). For example, if it is set to 15 seconds, the device will go into screen saver mode when the device detects no operation or no approaching object for the consecutive 15 seconds. When screen saver mode is disabled, the device screen will be turned off directly in 15 seconds.

Upload Screen Savers

You can upload screen-saver images individually or in batches to the device via the web interface, enhancing visual experience or serving publicity purposes.

To set it up, go to **Intercom > LED Setting > Upload Screensaver Picture** interface.

- Click **Choose File** to select a file from your computer and click **Upload**.
- Click **Reset** to remove the existing picture.



Upload ScreenSaver Picture (.png)

Format:png, Size:<300KB, Recommend resolution: 480*272

ID	File Status	Interval (Sec)	Reset
1	File Exists	5	Reset
2	File Exists	5	Reset

Please Choose ScreenSaver ID for upload: Image1

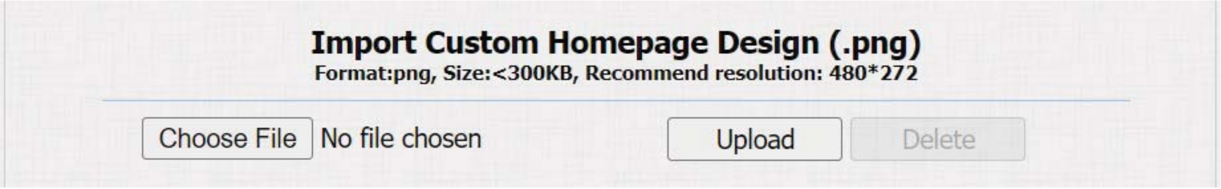
Screensaver1 — Choose File — No file chosen — Upload

> **Note**
>
> - File Format: PNG; Size: <300KB; Recommended Resolution: 480×272.
> - If the uploaded image duplicates an existing image ID, the existing image will be overwritten.

Homepage Display

You can customize the homepage display picture on the **Intercom > LED Setting > Import Custom Homepage Design** interface.

- Click **Choose File** to select a file from your computer and click **Upload** to import it.
- Click **Delete** to remove the existing picture.



Import Custom Homepage Design (.png)

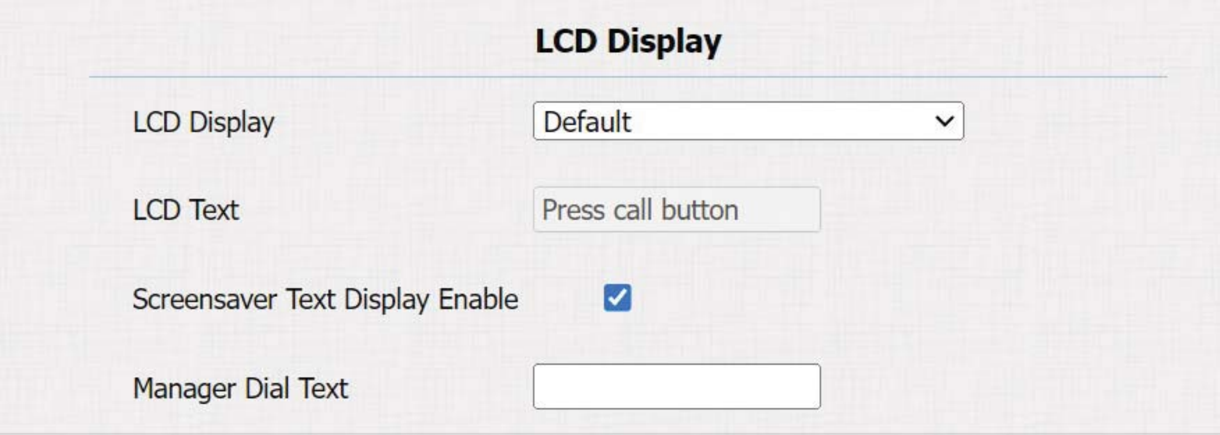
Format:png, Size:<300KB, Recommend resolution: 480*272

Choose File — No file chosen — Upload — Delete

> **Note**
>
> - File Format: PNG; Size: <300KB; Recommended Resolution: 480×272.
> - If the uploaded image duplicates an existing image ID, the existing image will be overwritten.

LCD Display

You can set what to be displayed on the device screen on the **Intercom** > **Advanced** > **LCD Display** interface.



LCD Display

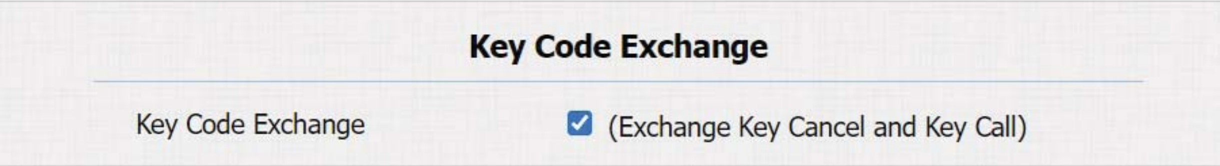
LCD Display	Default
LCD Text	Press call button
Screensaver Text Display Enable	☑
Manager Dial Text	

- **LCD Display**:
  - **Default**: Display Call, Contacts, PIN Entry, and Security Center instructions on the home screen.
  - **Hidden Contacts**: Display Call, PIN Entry, and Security Center instructions but hide the Contacts.
  - **Text Only**: Only display the content you enter in the LCD Text box.
    - **LCD Text**: Customize the text to be displayed on the home screen.
  - **Contacts Only**: Only display contacts.
  - **Hide Contacts & Room Number**: Display PIN Entry and Security Center instructions.
- **Manager Dial Text**: Name the Manager Dial key(Press the Call key to call). Its default name is Security Center.

Key Code Exchange

This feature exchanges the function of the **Call** and **Cancel** Keys.

To set it up, go to the **Intercom** > **Advanced** > **Key Code Exchange** interface.



Key Code Exchange

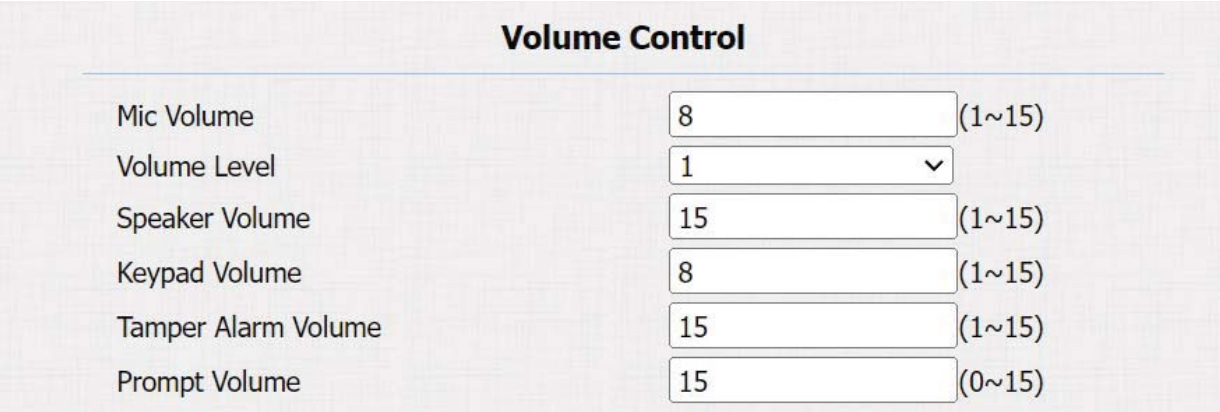
Key Code Exchange	☑ (Exchange Key Cancel and Key Call)

- **Key Code Exchange**: When enabled, the Cancel function will be linked to the Cancel key right on top of the Call key on the keypad. When disabled, the function of the Cancel and the Call key will be reversed.

Volume and Tone

Volume Control

You can set up various volumes on the **Phone** > **Audio** > **Volume Control** interface.



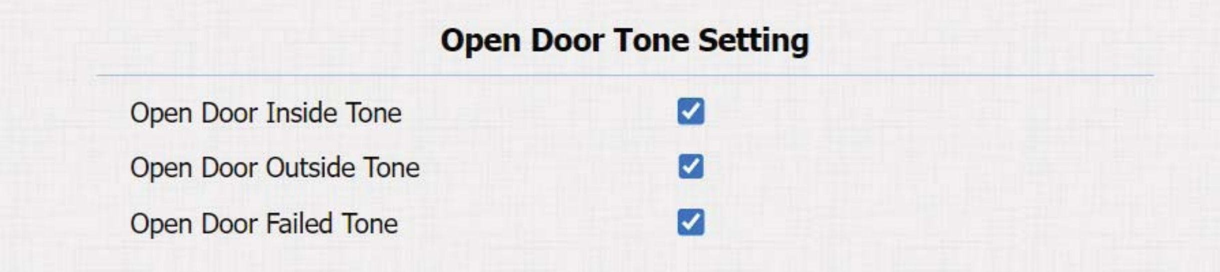
Volume Control

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)

- **Volume Level**: Set the overall volume. Level 1 volume range is roughly 80-95, and 2 is 95-109.
- **Tamper Alarm Volume**: Set the volume when the tamper alarm is triggered.
- **Prompt Volume**: Various prompts including door-opening success and failure prompts.

Door-opening Tones

You can enable or disable the door-opening tones on the **Phone** > **Audio** interface.



Open Door Tone Setting

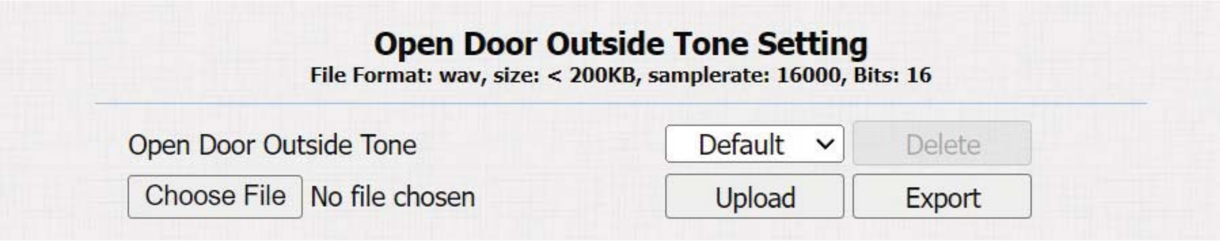
Open Door Inside Tone	☑
Open Door Outside Tone	☑
Open Door Failed Tone	☑

- **Open Door Inside Tone**: The input-triggered tone. The door-opening tone can be heard when users open doors by pressing an exit button.
- **Open Door Outside Tone**: The relay-triggered tone. The door-opening tone can be heard when users open doors by the device-supported access methods except for the exit button.

Open Door Outside Tone Setting

You can customize the open door outside tone on the **Open Door Outside Tone Setting** section.

- Click **Choose File** and then **Upload** to import the tone.
- Click **Export** to download the existing tone.



Open Door Outside Tone Setting

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

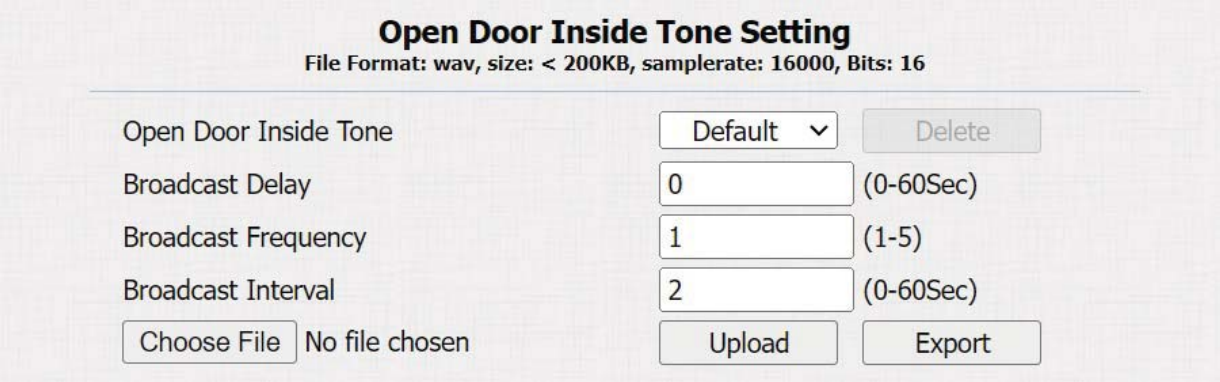
Open Door Outside Tone: Default

> **Note**
>
> File Format: WAV; Size: <200KB; Sample Rate: 16K; Bits: 16.

Open Door Inside Tone Setting

You can customize the open door inside tone on the **Open Door Inside Tone Setting** section.

- Click **Choose File** and then **Upload** to import the tone.
- Click **Export** to download the existing tone.



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)

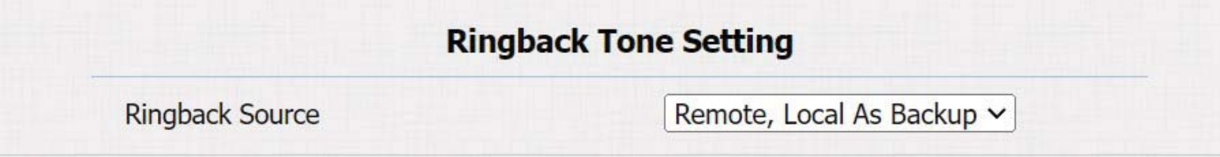
- **Broadcast Delay**: Set the delay to ring the tone when the door is opened. For example, if you set 3 seconds, the tone will ring 3 seconds after the door opens.
- **Broadcast Frequency**: Set the times of ringing the tone.
- **Broadcast Interval**: Set the interval between each ringing of the tone.

> **Note**
>
> File Format: WAV; Size: <200KB; Sample Rate: 16K; Bits: 16.

Ringback Tone Setting

The ringback tone setting prioritizes the playing of local ringtones and determines what kinds of previews the callee can receive.

To set it up, go to the **Phone > Audio > Ringback Tone Setting** interface.



Ringback Tone Setting

Ringback Source: Remote, Local As Backup

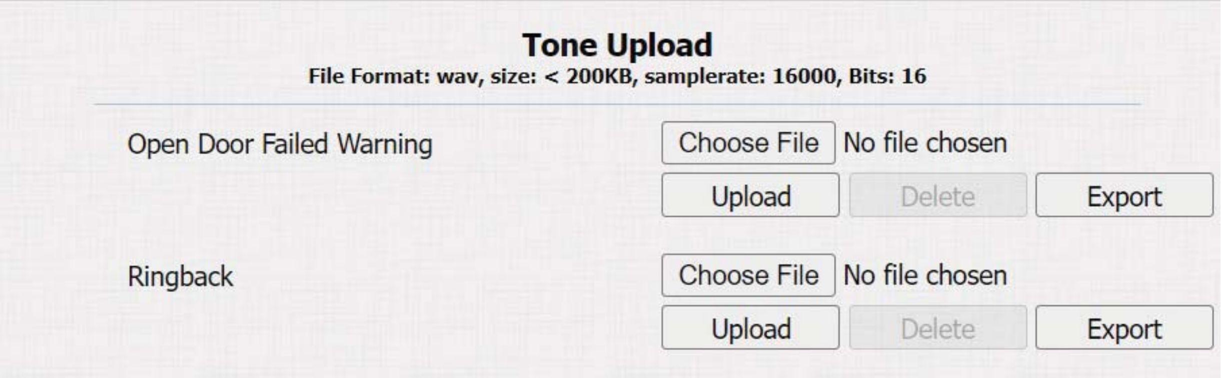
- **Ringback Source**:
  - **Remote, Local As Backup**: The local ringtone will be played.
    - When the door phone calls another device, for example, an Akuvox indoor monitor, and the SIP server returns non-183, the indoor monitor will not have any intercom preview.
    - If the SIP server returns 183, the indoor monitor will receive the video preview without voice.
  - **Local**: The local ringtone will be played. Whether the SIP server returns 183 or not, the callee will not have any intercom preview.
  - **Remote**:
    - If the SIP server returns non-183, the local ringtone will be played and the callee will not have any intercom preview.
    - If the SIP server returns 183, the SIP server's ringtone will be played and the callee will receive the video preview without voice.

Upload Tones

Apart from the open door inside and outside tones, you can also upload door-opening failure, ringback, and keypad pressing tones.

Upload tones on the **Phone** > **Audio** > **Tone Upload** interface.

- Click **Choose File** and then **Upload** to import the tone.
- Click **Export** to download the existing file.



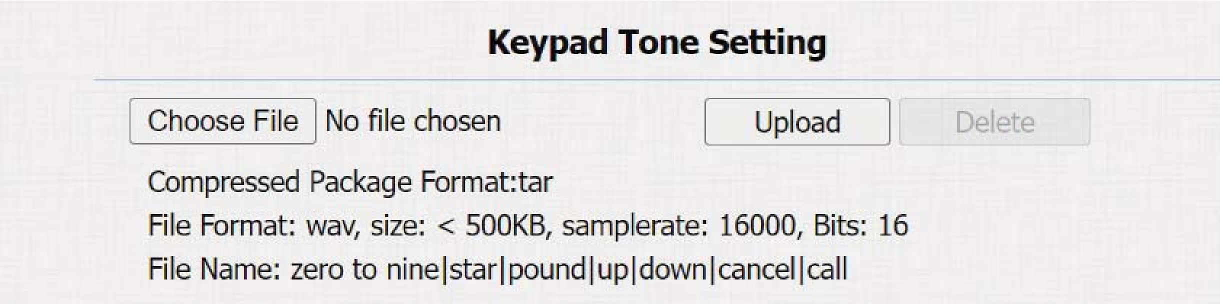
Tone Upload
File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

Open Door Failed Warning

Ringback

> **Note**
>
> File Format: WAV; Size: <200KB; Sample Rate: 16K; Bits: 16.

Upload the keypad tone on the **Keypad Tone Setting** section. You can upload a keypad tone for each key. When pressing any key, the 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

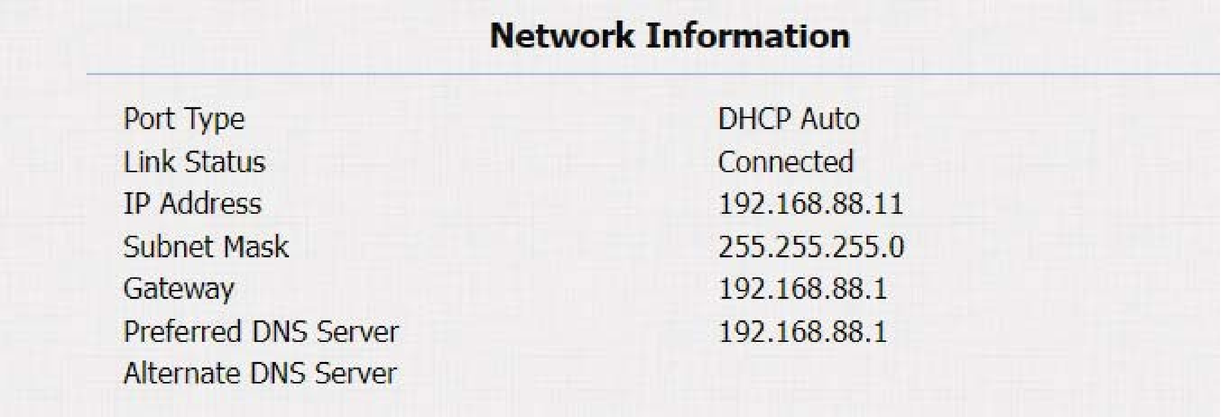
Note

File Format: WAV; Size: <500KB; Sample Rate: 16K; Bits: 16.

Network Setting

Network Status

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



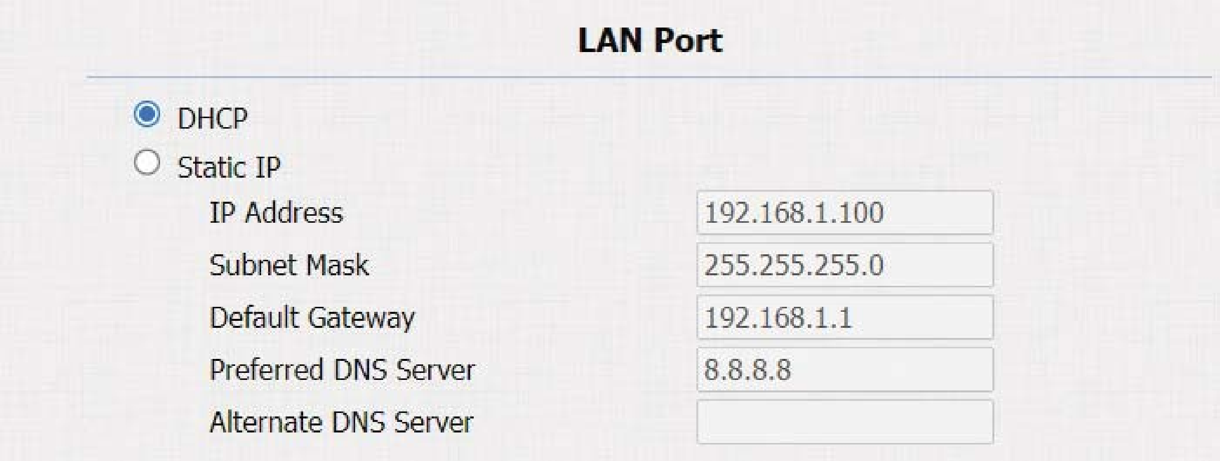
Network Information

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.

Set up the network on the **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	

- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, the device will automatically be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address.
- **Static IP**: The IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **IP Address**: Specify the IP address when the static IP mode is selected.
- **Subnet Mask**: The subnet mask should be set up according to the actual network environment.
- **Default Gateway**: The gateway should be set up according to the IP address.

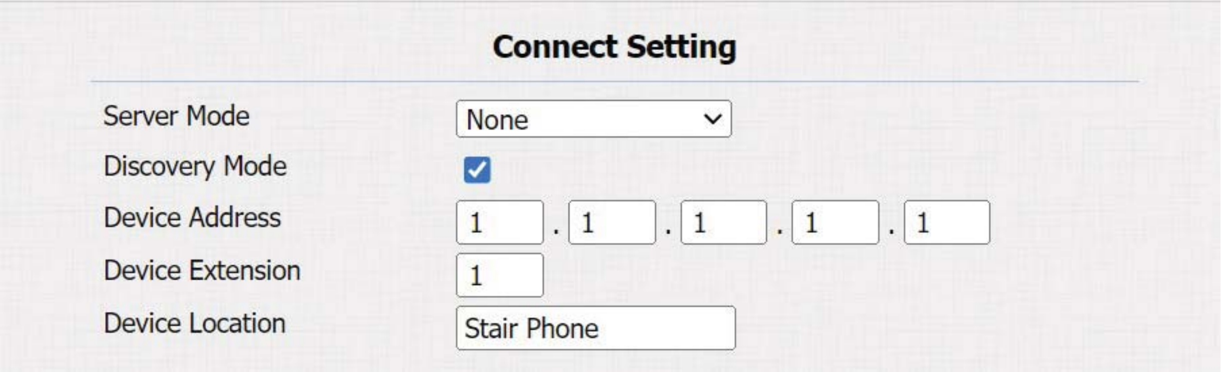
- **Preferred & Alternate DNS Server**: The preferred and alternate Domain Name Server(DNS). The preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.

> **Tip**
>
> 1. You can also set the network on the device by pressing “*2396#”.
> 2. Press “3” to enter the System Setting.
> 3. Select Network Settings to set up the device’s network.

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.

To set it up, go to the **Network > Advanced > Connect Setting** interface.



Connect Setting

Server Mode: None
Discovery Mode: ☑
Device Address: 1 . 1 . 1 . 1 . 1
Device Extension: 1
Device Location: Stair Phone

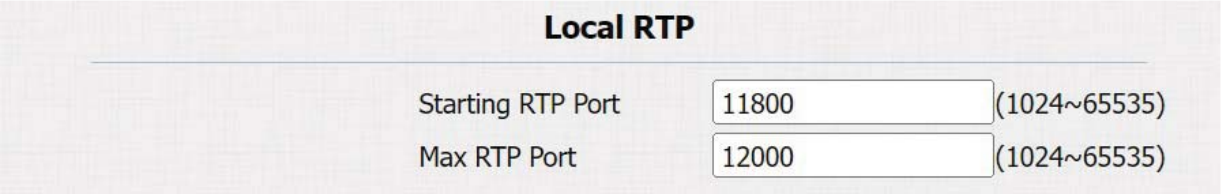
- **Server Mode**: It is automatically set up according to the actual device connection with a specific server in the network such as SDMC, Cloud, or None. None is the default factory setting indicating the device is not in any server type.
- **Discovery Mode**: With discovery mode enabled, the device can be discovered by other devices in the network. Uncheck the box if you want to conceal the device.
- **Device Address**: Specify the device address by entering device location info from the left to the right: Community, Unit, Stair, Floor, and Room in sequence.
- **Device Extension**: The device extension number.
- **Device Location**: The location where 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.

To set it up, go to the **Network** > **Advanced** > **Local RTP** interface.



Local RTP

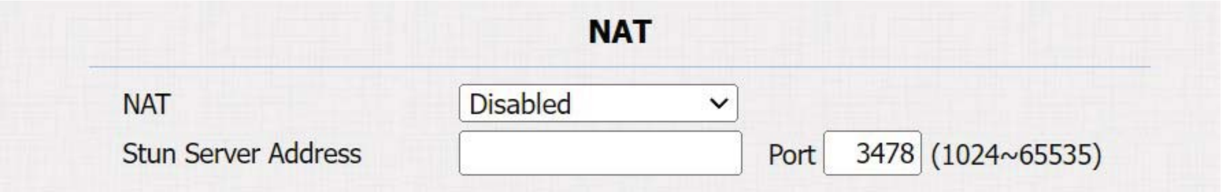
Starting RTP Port	11800	(1024~65535)
Max RTP Port	12000	(1024~65535)

- **Starting RTP Port**: The port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: The port value 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 set up NAT, navigate to the **Account** > **Basic** > **NAT** interface.

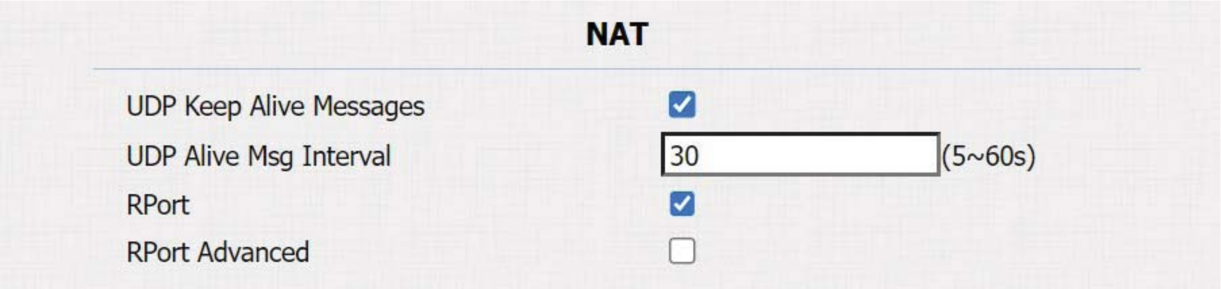


NAT

NAT	Disabled			
Stun Server Address		Port	3478	(1024~65535)

- **Stun Server Address**: Set the SIP server address in the Wide Area Network(WAN).
- **Port**: Set the SIP server port.

Then set up NAT on the **Account** > **Advanced** > **NAT** interface.



NAT

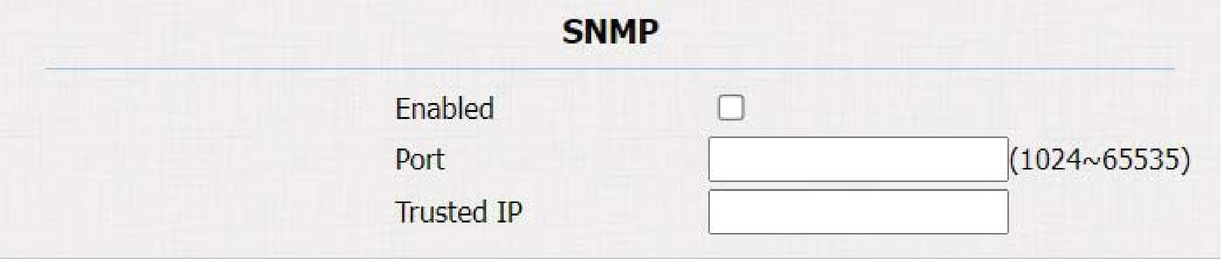
UDP Keep Alive Messages	☑	
UDP Alive Msg Interval	30	(5~60s)
RPort	☑	
RPort Advanced	□	

- **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 Msg Interval**: The message-sending time interval ranges from 5 to 60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when the SIP server is in WAN.
- **RPort Advanced**: Further stabilize the network based on RPort.

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 set it up, go to the **Network** > **Advanced** > **SNMP** interface.



SNMP

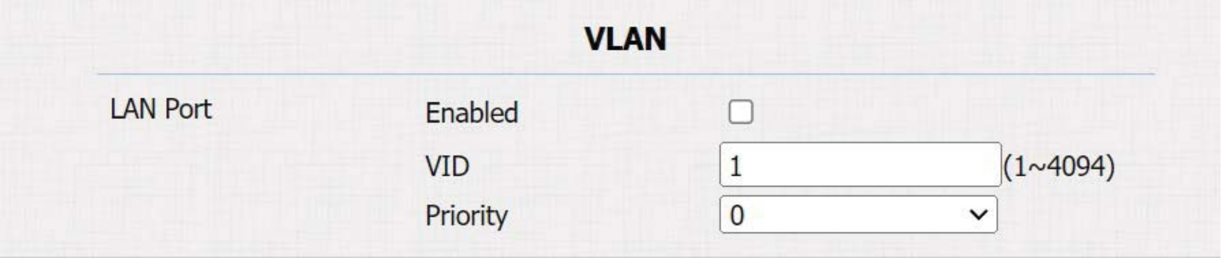
Enabled □
Port (1024~65535)
Trusted IP

- **Port**: Enter the SNMP server's port.
- **Trusted IP**: The allowed SNMP server address. It can 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 set it up, go to the **Network** > **Advanced** > **VLAN** interface.



VLAN

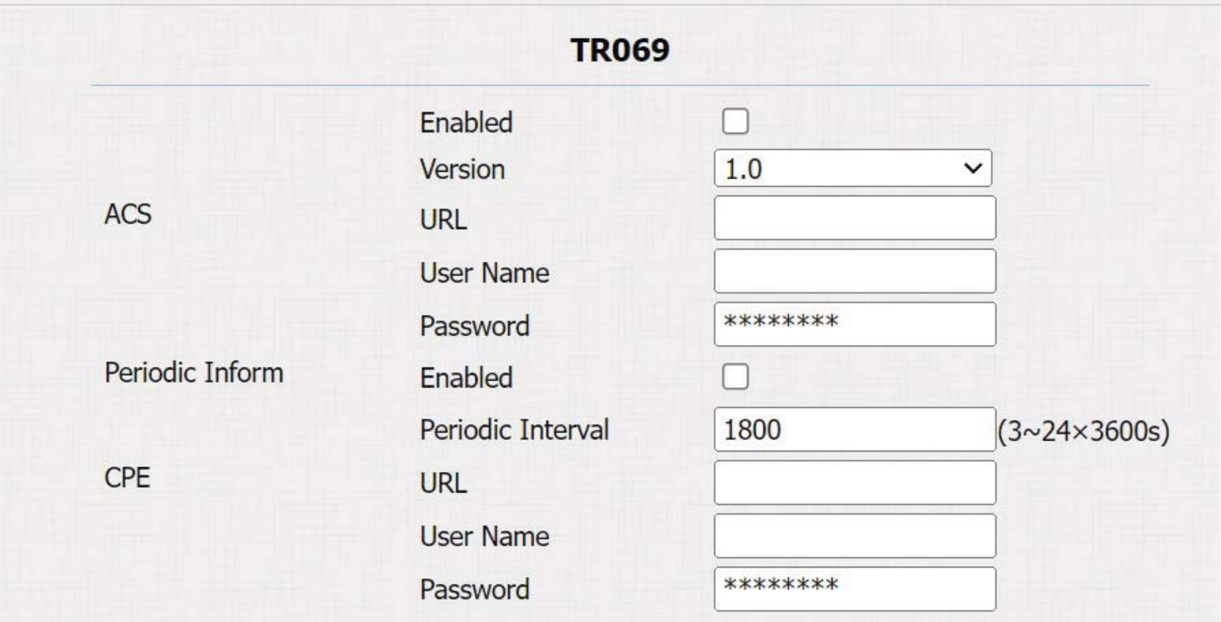
LAN Port
Enabled □
VID 1 (1~4094)
Priority 0

- **VID**: The VLAN ID for the designated port.
- **Priority**: The 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 set it up, go to the **Network** > **Advanced** > **TR069** interface.



TR069

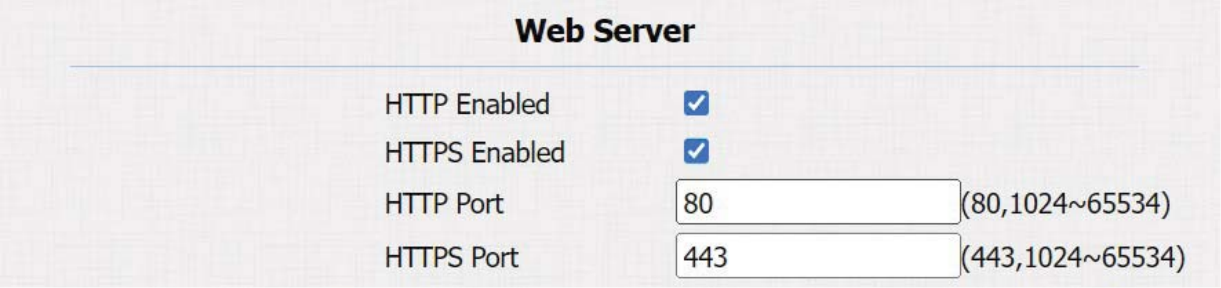
ACS	Enabled	□	
	Version	1.0	
	URL		
	User Name		
	Password	********	
Periodic Inform	Enabled	□	
	Periodic Interval	1800	(3~24×3600s)
CPE	URL		
	User Name		
	Password	********	

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

Device Web HTTP Setting

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

To set it up, go to the **Network** > **Advanced** > **Web Server** interface.



Web Server

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

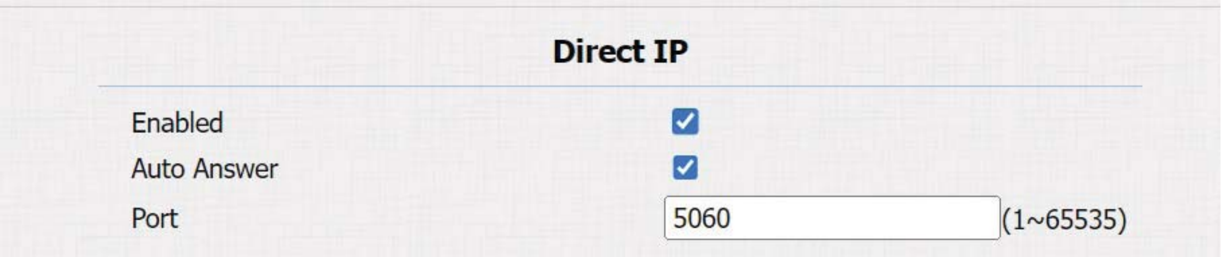
- **HTTP/HTTPS Enabled**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

Intercom Call Configuration

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.

Enable or disable the direct IP call function on the **Phone > Call Feature > Direct IP** interface.



Direct IP

Enabled	☑
Auto Answer	☑
Port	5060 (1~65535)

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

SIP Call Configuration

Session Initiation Protocol(SIP) is a signaling transmission protocol used for initiating, maintaining, and terminating calls.

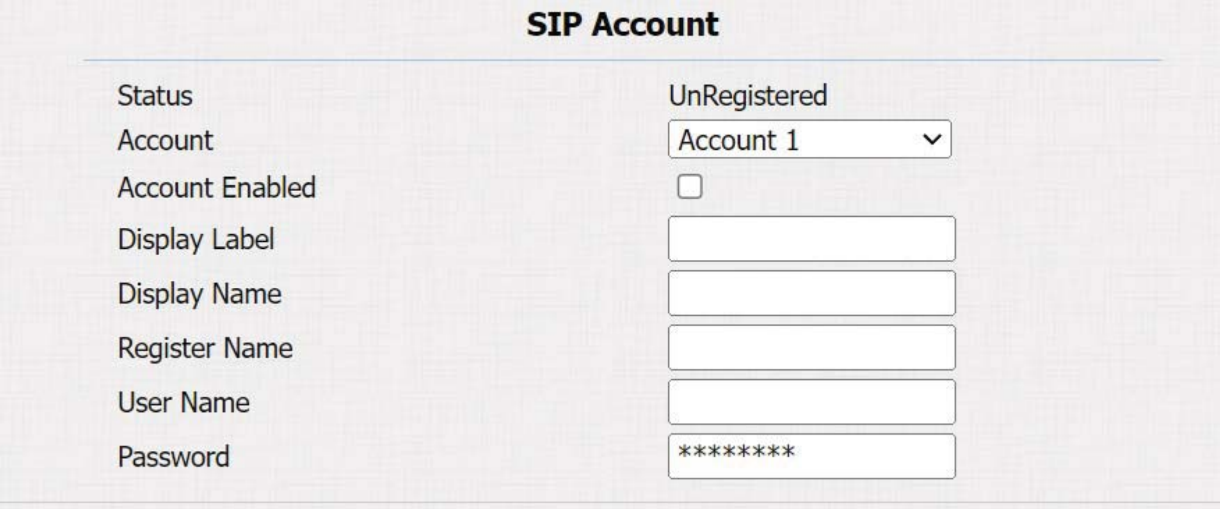
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

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.

Register the SIP account on the **Account > Basic** interface.



SIP Account

Status	UnRegistered
Account	Account 1
Account Enabled	□
Display Label	
Display Name	
Register Name	
User Name	
Password	********

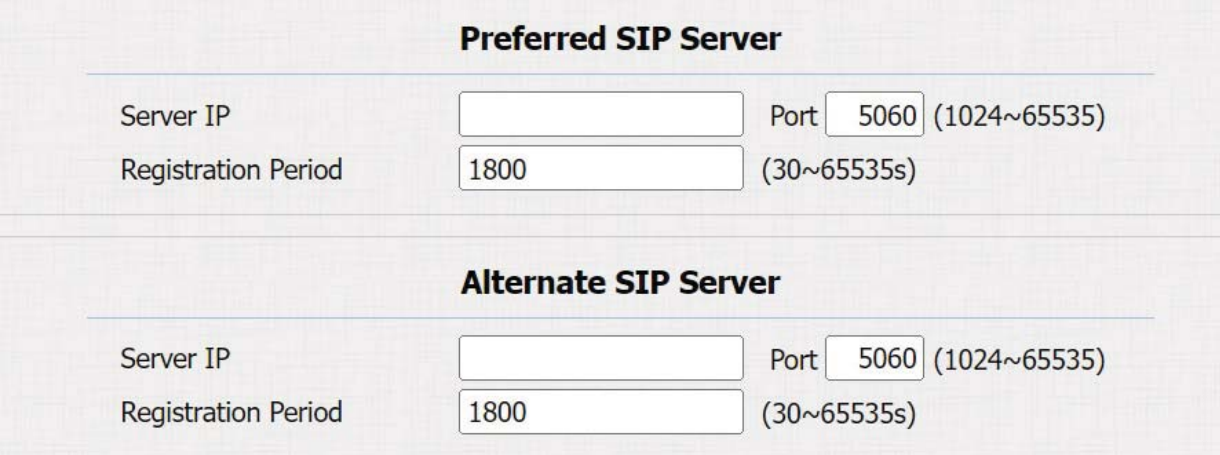
- **Status:** Indicate whether the SIP account is registered or not.
- **Account 1/Account 2:** The door phone supports 2 SIP accounts.
  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.
  - The system switches to Account 2 if Account 1 is not registered.

- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 is to be shown on the calling device’s screen.
- **Register Name:** Same as the username from the PBX server.
- **User Name:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

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 set it up, go to the **Account > Basic** interface.



Preferred SIP Server

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

Alternate SIP Server

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

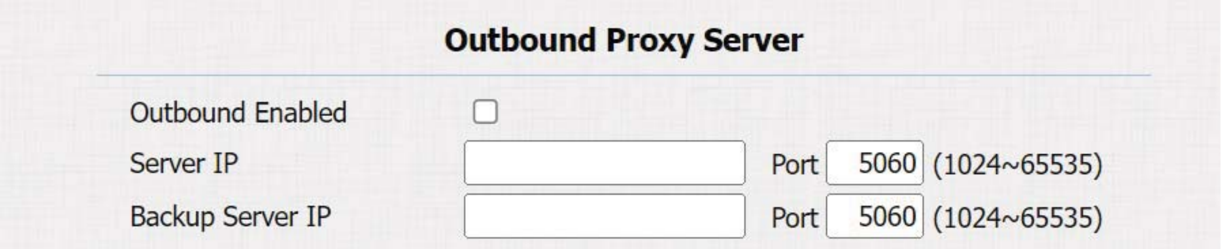
- **Server IP:** Enter the server’s IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.

- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified period.

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, go to the **Account** > **Basic** > **Outbound Proxy Server** interface..



Outbound Proxy Server

Outbound Enabled ☐

Server IP [ ] Port 5060 (1024~65535)

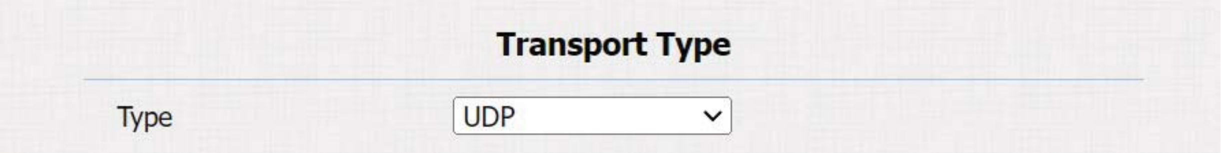
Backup Server IP [ ] Port 5060 (1024~65535)

- **Server IP:** Enter the SIP proxy server's IP address.
- **Port:** Set the port for establishing a call session via the outbound proxy server.
- **Backup Server IP:** Enter the SIP proxy IP address to be used when the main proxy server malfunctions.
- **Port:** Set the proxy port for establishing a call session via the backup outbound proxy server.

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**.

Select the data transmission type on the **Account** > **Basic** > **Transport Type** interface.



Transport Type

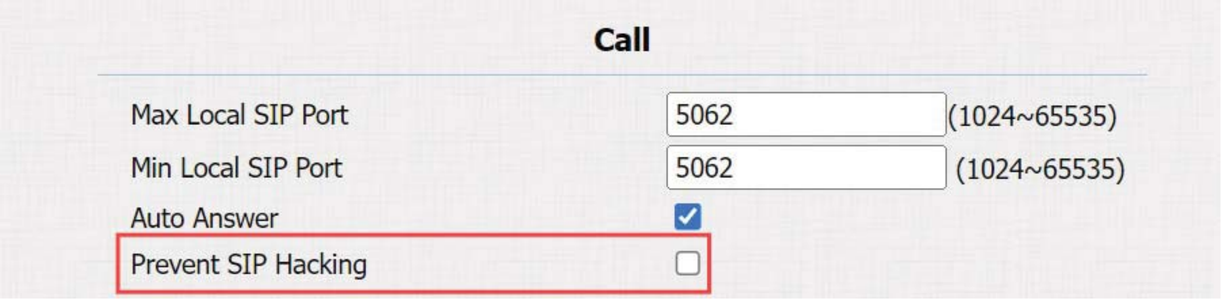
Type UDP

- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.
- **DNS-SRV:** A DNS service record defines the location of servers. This record includes the hostname and port number of the server, as well as the priority and weight values that determine the order and frequency of using the server.

SIP Hacking Prevention

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.

Enable SIP hacking prevention on the **Account** > **Advanced** > **Call** interface.



Call

Max Local SIP Port 5062 (1024~65535)

Min Local SIP Port 5062 (1024~65535)

Auto Answer ☑

Prevent SIP Hacking □

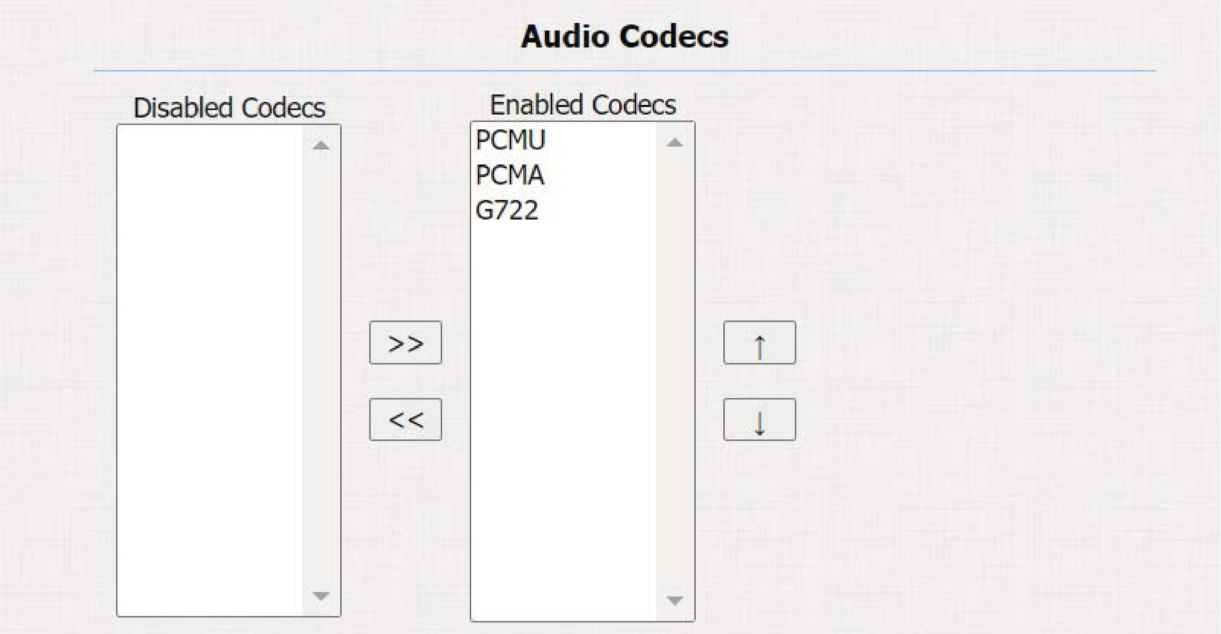
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Audio and Video Codec Configuration

Audio Codec

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 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 set it up, go to the **Account** > **Advanced** interface.



Audio Codecs

Disabled Codecs

Enabled Codecs
PCMU
PCMA
G722

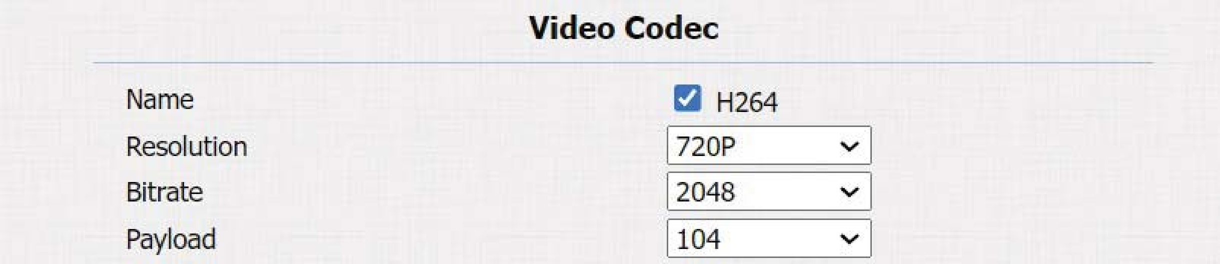
Please refer to the bandwidth consumption and sample rate for the codec types below:

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

Video Codec

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

Set it up on the **Account** > **Advanced** interface.



Video Codec

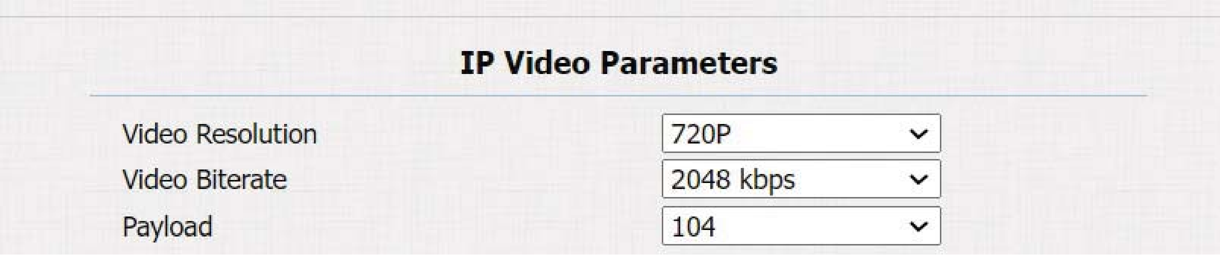
Name	☑ H264
Resolution	720P
Bitrate	2048
Payload	104

- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options.
- **Bitrate**: The video stream bitrate ranges from 64 to 2048 kbps. The greater the bitrate, the more data transmitted every second and the clearer the video will be. The default code bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec Configuration for Direct IP Calls

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

Set it up on the **Phone** > **Call Feature** > **IP Video Parameters**.



IP Video Parameters

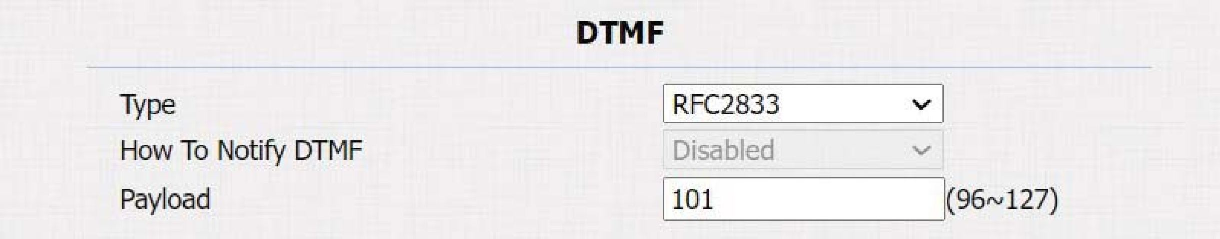
Video Resolution	720P
Video Biterate	2048 kbps
Payload	104

- **Video Resolution**: Select the resolution from the provided options.
- **Video Bitrate**: The video stream bitrate ranges from 64 to 2048 kbps. The default bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

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.

Set it up on the **Account** > **Advanced** > **DTMF** interface.



DTMF

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

- **Type:** Select from the following options: **Inband, RFC2833, Info, Info+Inband, Info+RFC2833,** or **Info+Inband+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 **Disabled, DTMF, DTMF-Relay**, or **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 to be matched with adopts **Info** mode.
- **Payload**: Set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

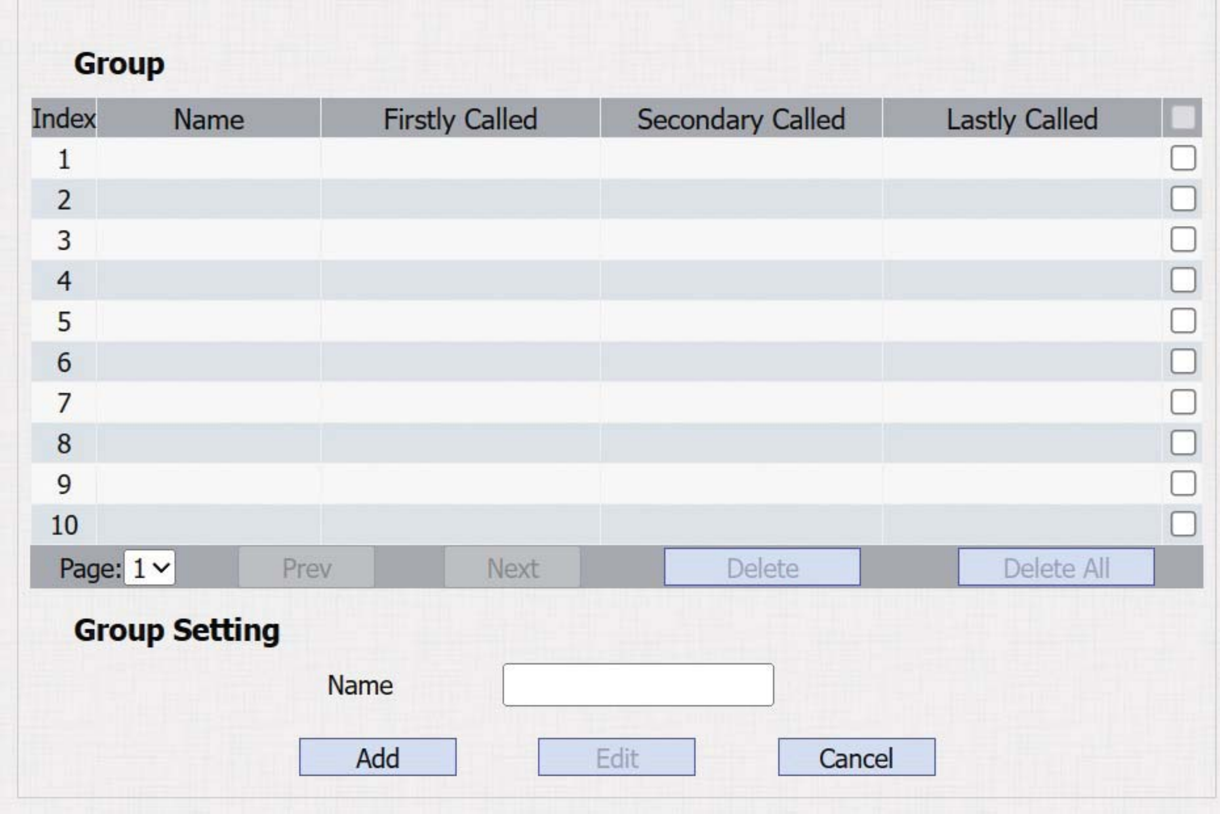
Contact List Configuration

Manage 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.

Set it up on the **Contacts** > **Contacts List** > **Group** interface.

Enter the group name and click **Add** to add a group.



Group

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

Page: 1

Group Setting

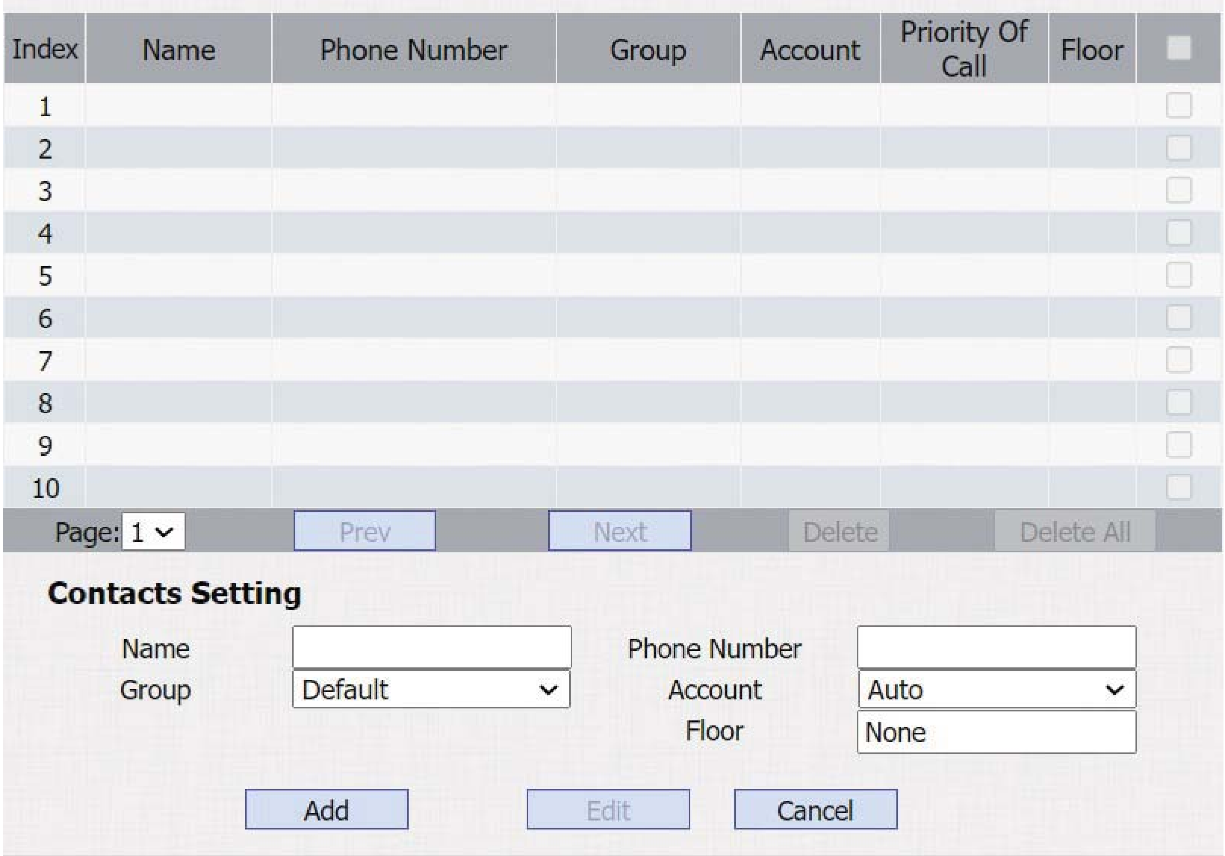
Name

Manage Contacts

You can search, create, display, edit, and delete the contacts.

Add Contacts

Add contacts on the **Contacts** > **Contacts List** interface. Find the **Contacts Setting** part.



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

Page: 1

Contacts Setting

Name		Phone Number	
Group	Default	Account	Auto
		Floor	None

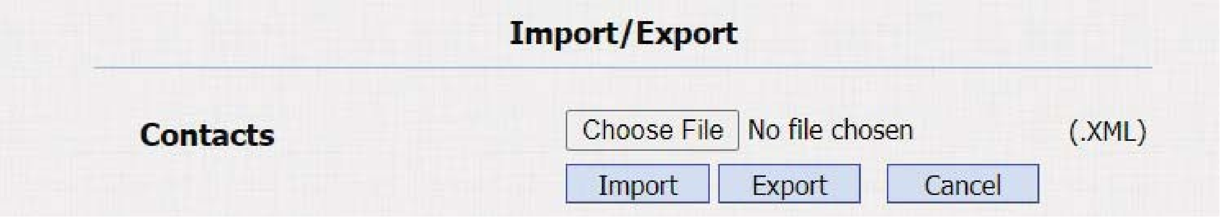
- **Name**: Enter the contact’s name.
- **Phone Number**: Enter the contact’s IP or SIP number.
- **Group**: Assign the contact to the default or a self-created group.
- **Account**: The account is used when making calls to the contact.
- **Floor**: Specify the accessible floor(s) to the contact via the elevator.

Export/Import Contacts

You can easily import and export contacts for quick management.

Go to the **Contacts** > **Contacts List** > **Import/Export** interface.

The import and export file is in XML format.



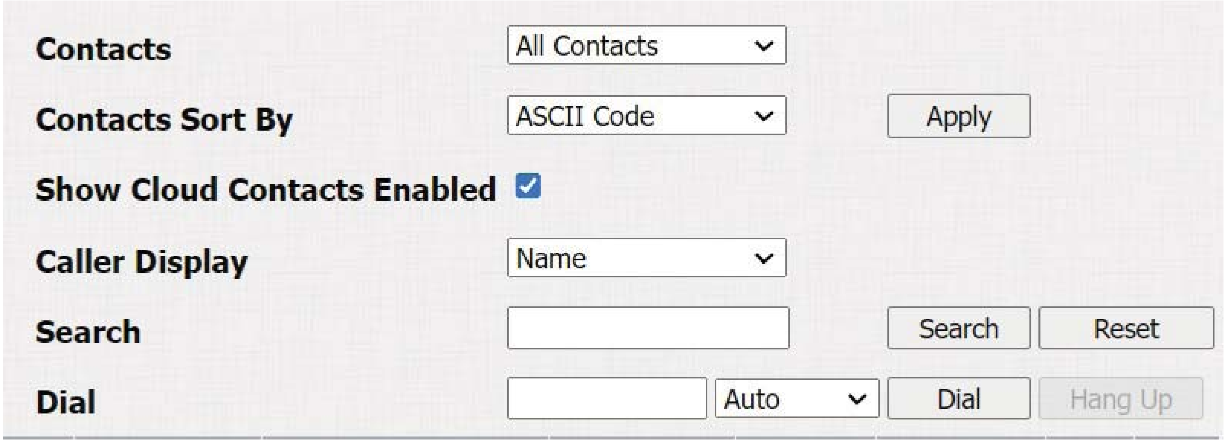
Import/Export

Contacts: No file chosen (.XML)

Contact List Display

You can customize the contact list display to cater to users' operational and visual preferences.

Set it up on the **Contacts** > **Contacts List** interface.



Contacts	All Contacts ⌄		
Contacts Sort By	ASCII Code ⌄	Apply	
Show Cloud Contacts Enabled	☑		
Caller Display	Name ⌄		
Search		Search	Reset
Dial	Auto ⌄	Dial	Hang Up

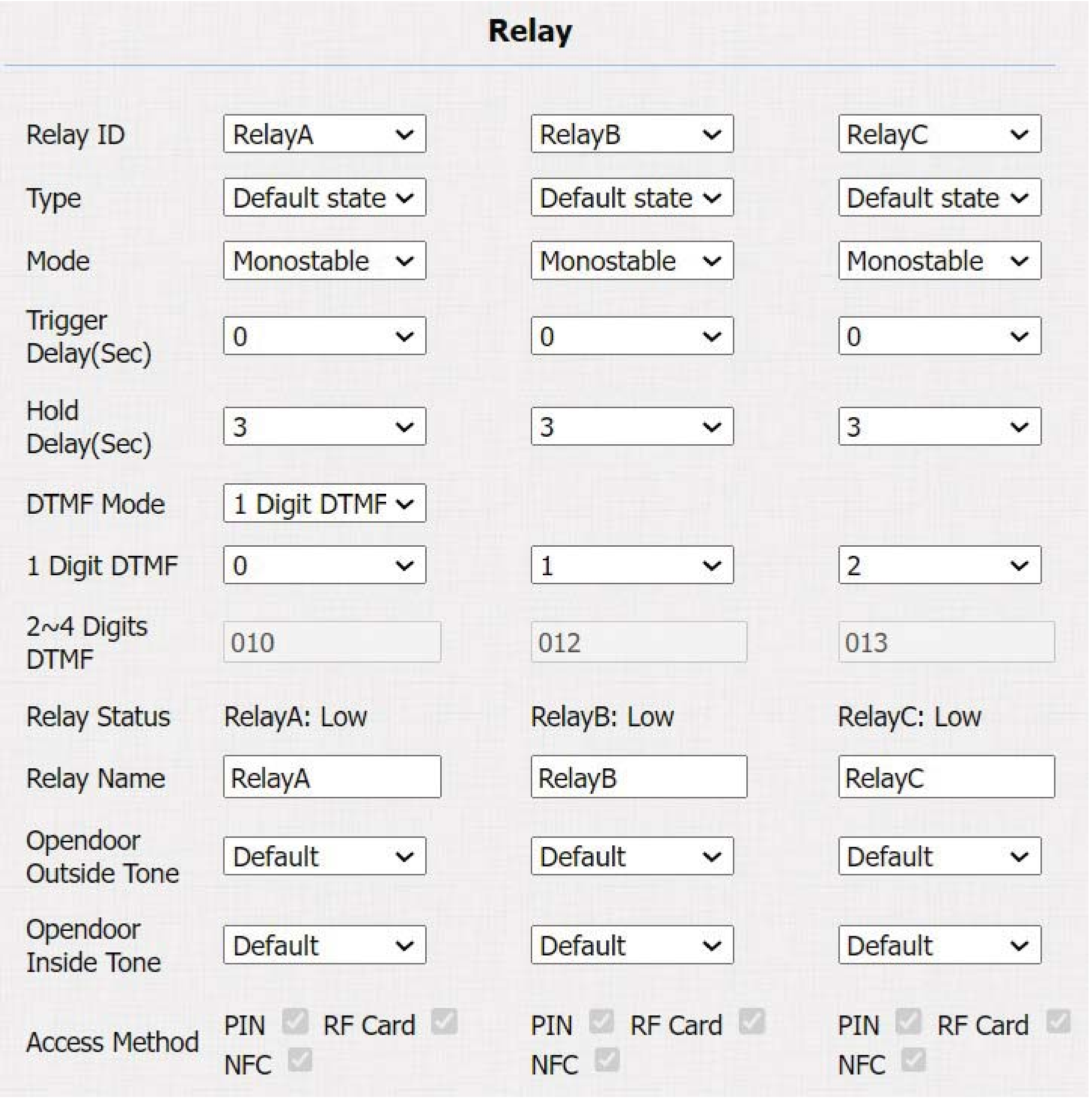
- **Contacts**: Select to display all contacts or contacts in a specific group.
- **Contacts Sort By**:
  - **ASCII Code**: List the contacts by their names in the sequence of the ASCII code.
  - **Room Number**: List the contacts according to their room number. This feature works with SmartPlus Cloud.
  - **Import**: List the contacts based on their order in the import file.
- **Show Cloud Contacts Enabled**: When enabled, The contacts synchronized from the SmartPlus Cloud can be displayed.
- **Caller Display**: Choose what to be displayed on the device screen when receiving calls from contacts.
  - **Name**: Display the contact name.
  - **Group**: Display the group the contact belongs to.
- **Search**: Enter the contact name to search for a specific contact. Click Reset to clear the box.
- **Dial**: You can directly call a contact by checking it and selecting the account on the web interface. Click Dial to make the call.

Relay Setting

Local Relay

A local relay is an external unit that is physically nearby and directly connected to the intercom device. It allows the intercom system to trigger actions, such as unlocking a door, based on user input or authorization.

Set it up on the **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	0	1	2
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
Access Method	PIN ☑ RF Card ☑ NFC ☑	PIN ☑ RF Card ☑ NFC ☑	PIN ☑ RF Card ☑ NFC ☑

- **Type**: Determine the interpretation of the Relay Status regarding the state of the door:
  - **Default State**: A "Low" status in the Relay Status field indicates that the door is closed, while "High" indicates that it is opened.
  - **Invert State**: A "Low" status in the Relay Status field indicates an opened door, while "High" indicates a closed one.

- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.

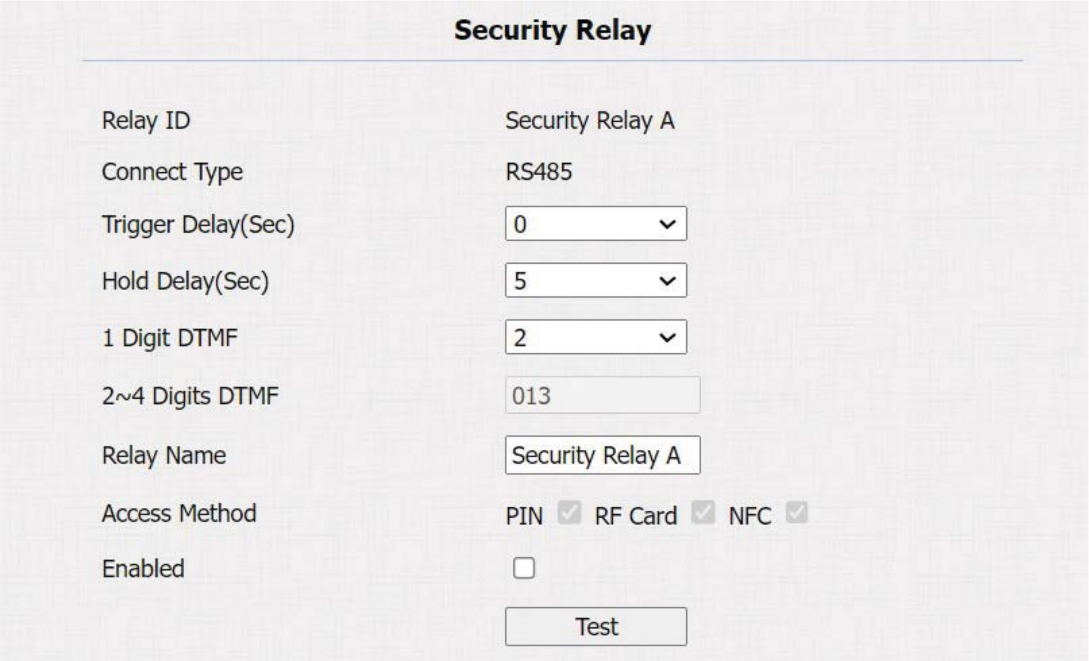
  - **Bistable:** The relay status resets upon triggering the relay again.

- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Open Door Outside Tone**: Select the tone to be heard when the relay is triggered by the device-supported access methods except for pressing the exit button.
- **Open Door Inside Tone**: Select the tone to be heard when the door is opened by triggering the input(pressing the exit button).
- **Access Method**: Display the access methods that can unlock the relay and cannot be changed.

Security Relay

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.

Set it up on the **Intercom** > **Relay** > **Security Relay** interface.



Security Relay

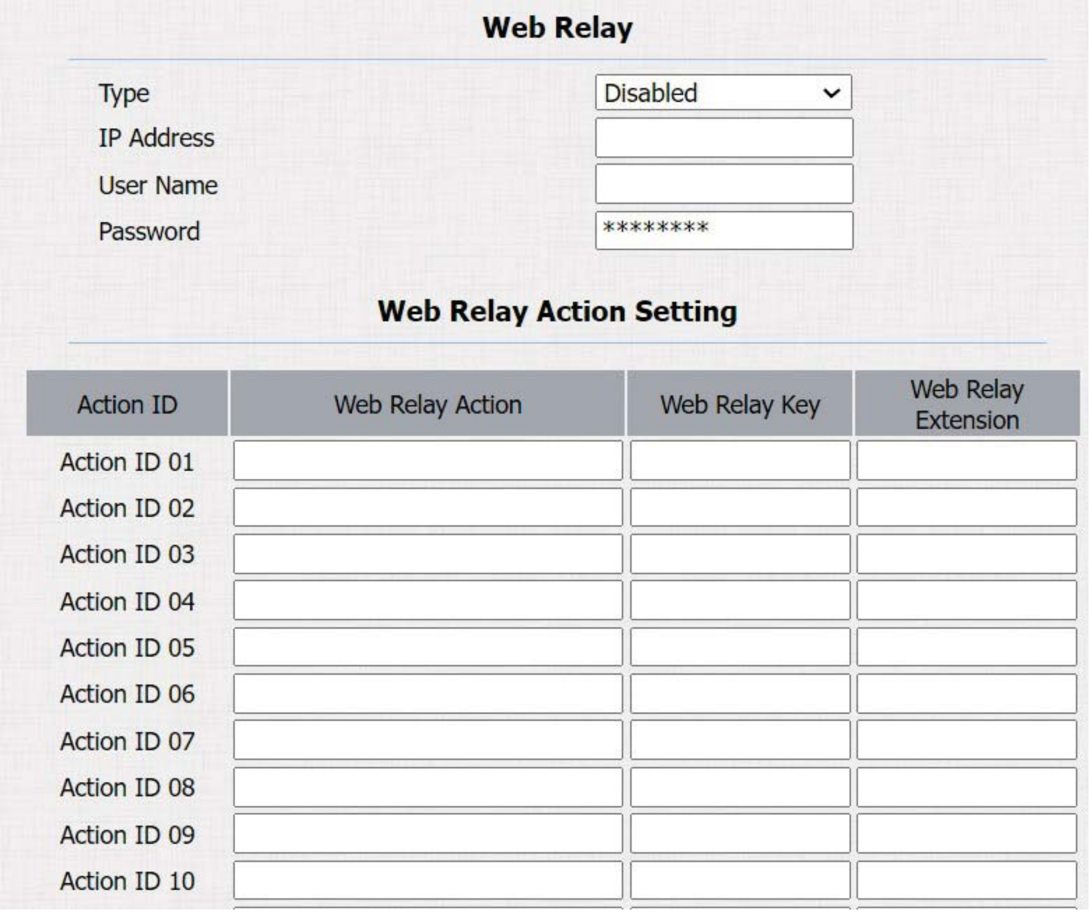
Relay ID	Security Relay A
Connect Type	RS485
Trigger Delay(Sec)	0
Hold Delay(Sec)	5
1 Digit DTMF	2
2~4 Digits DTMF	013
Relay Name	Security Relay A
Access Method	PIN ☑ RF Card ☑ NFC ☑
Enabled	☐
	Test

- **Connect Type**: The connection type is RS485 by default.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name**: Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method**: Display the access methods that can unlock the security relay and cannot be changed.
- **Enabled**: Enable or disable the use of the security relay.
- **Test**: Click to send the signal to the SR01. When the door phone and SR01 are pairing, click Test to finish the matching.

Web Relay

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.

To set it up, go to **Phone** > **Web Relay** interface.



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			

- **Type**: Determine the type of relay activated when employing door access methods for entry.
  - **Disabled**: Only activate the local relay.
  - **Web Relay**: Only activate the web relay.
  - **Both**: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **User Name**: The user name provided by the web relay manufacturer.

- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.
- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

> NOTE
>
> If the URL includes full HTTP content (e.g., http://admin:admin@192.168.1.2/state.xml?relayState=2), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., state.xml?relayState=2), the relay uses the entered IP address.

- **Web Relay Key**: Determine the methods to activate the web relay based on whether the DTMF code is filled.

- Filling with the configured DTMF code restricts activation to card swiping and DTMF.

- Leaving it blank enables all door-opening methods.

- **Web Relay Extension**: Specify the intercom device and the methods it can use to activate the web relay during calls.

- When an intercom device’s IP/SIP is specified, only that device can trigger the web relay (except for via card swiping or DTMF) during calls.

- If left blank, all devices can trigger the relay during calls.

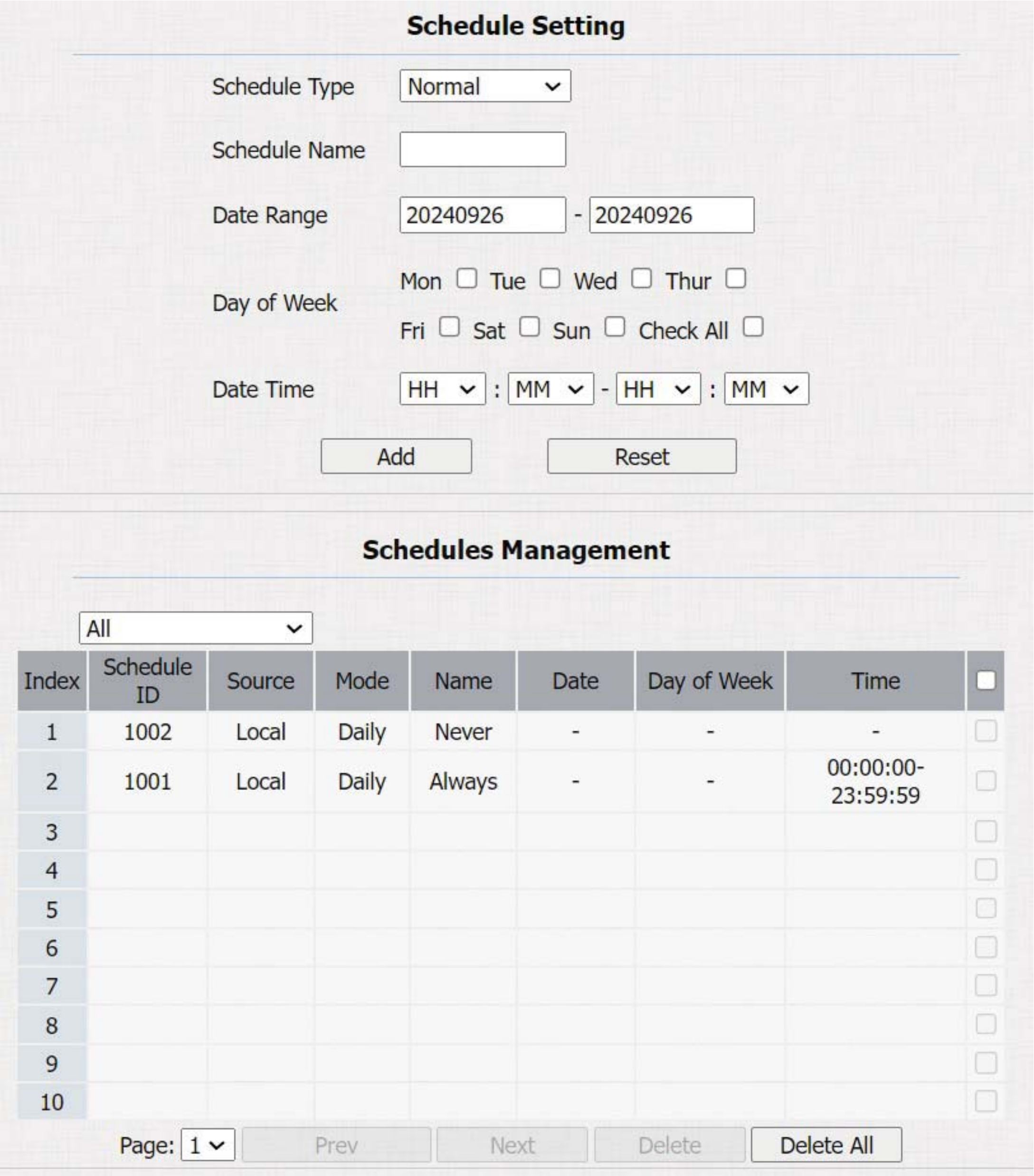
Door Access Schedule Management

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.

Create a Door Access Schedule

You can create the door access schedule on a daily or monthly basis, and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis.

Set it up on the web **Intercom** > **Schedule** interface.



Schedule Setting

Schedule Type	Normal
Schedule Name	
Date Range	20240926 - 20240926
Day of Week	Mon □ Tue □ Wed □ Thur □ Fri □ Sat □ Sun □ Check All □
Date Time	HH : MM - HH : MM

Schedules Management

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								□

- **Mode**:

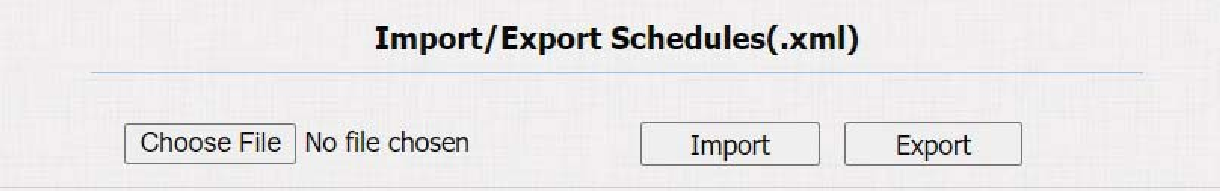
- **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
- **Weekly**: Set the schedule based on the week.
- **Daily**: Set the schedule based on 24 hours a day.

- **Name**: Name the schedule.

Import and Export Door Access Schedule

In addition to creating door access a schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency.

To set it up, go to the **Intercom > Schedule** interface. The export file is in **TGZ** format. The import file should be in **XML** format.



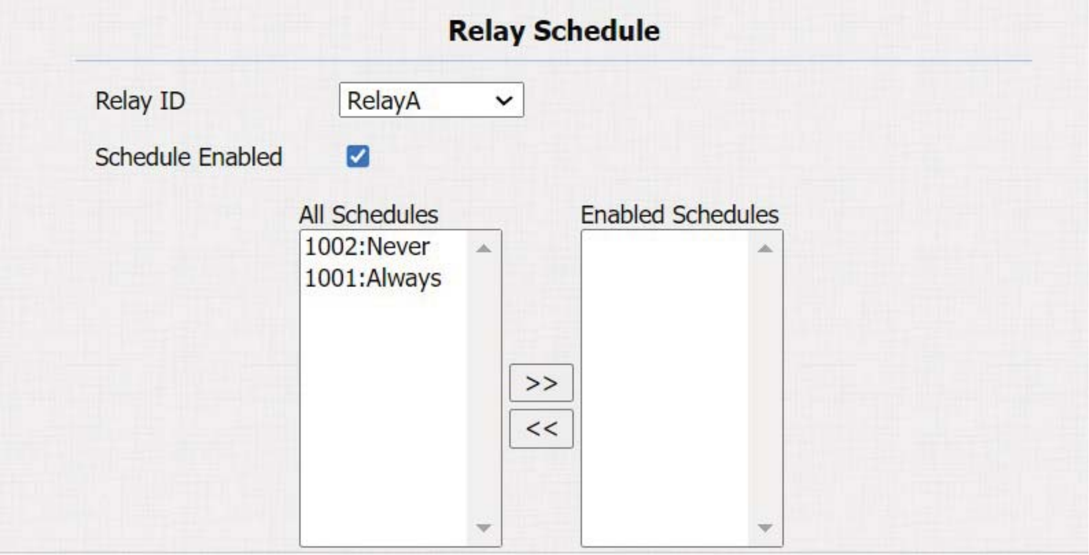
Import/Export Schedules(.xml)

No file chosen

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 set up a relay schedule, go to the **Intercom > Relay > Relay Schedule** interface.



Relay Schedule

Relay ID: RelayA

Schedule Enabled: ☑

All Schedules:
1002:Never
1001:Always

Enabled Schedules:

- **Relay ID**: Apply the schedule to the specific relay.
- **Schedule Enabled**: Assign particular door access schedules to the chosen relay. Simply move them to the Enabled Schedules box.

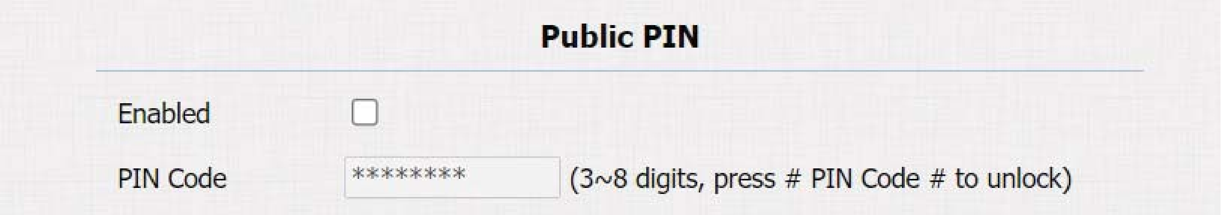
For instructions on creating schedules, kindly consult the Create Door Access Schedule section.

Door Opening Configuration

Public 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.

To set up the public PIN code, go to **Intercom** > **PIN Setting** > **Public PIN** interface.



Public PIN

Enabled □

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

- **PIN Code**: Specify the public PIN code when enabling this feature. The code should be within 3-8 digits. The default is 33333333.

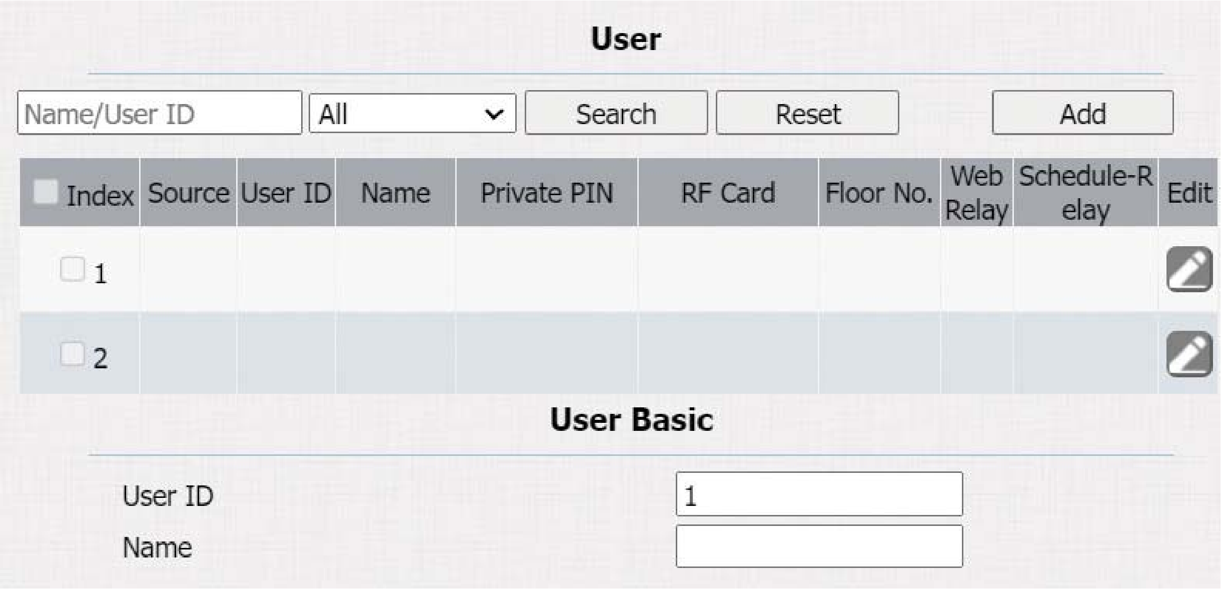
> **Tip**
>
> You can also modify the Public PIN on the device by pressing “*3888#” on the keypad to enter the Access Method Settings screen.

User-specific Access Methods

The private PIN code and RF card should be assigned to a particular user for door opening.

When adding a user, you can also customize settings such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

To add a user, go to **Intercom** > **User** interface and Click **+Add**.



User

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

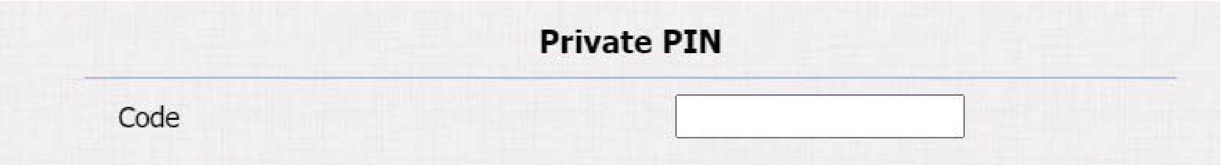
User Basic

User ID	1
Name	

- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.

Unlock by Private PIN Code

On the **Intercom** > **User** > **Add** interface, find the **Private PIN** part.



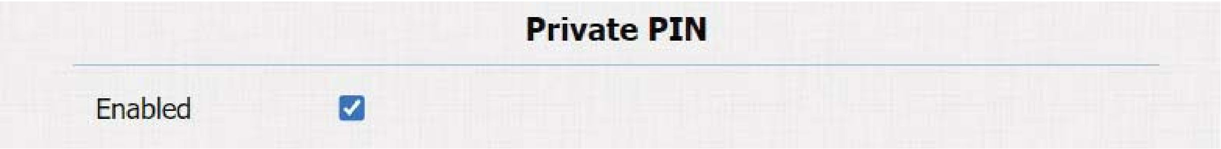
Private PIN

Code	

- **Code**: Set a 2-8 digit PIN code solely for the use of this user. A user can have multiple codes. Separate each code by “;”.

> **Tip**
>
> 1. You can also modify the Private PIN on the device by pressing “*3888#” on the keypad to enter the Access Method Settings screen.
> 2. Then, enter the Admin Code “2396” to enter the Private PIN Adding and Deleting screen.

You can also disable the use of private PIN unlock. Go to the **Intercom** > **PIN Setting** > **Private PIN** interface.

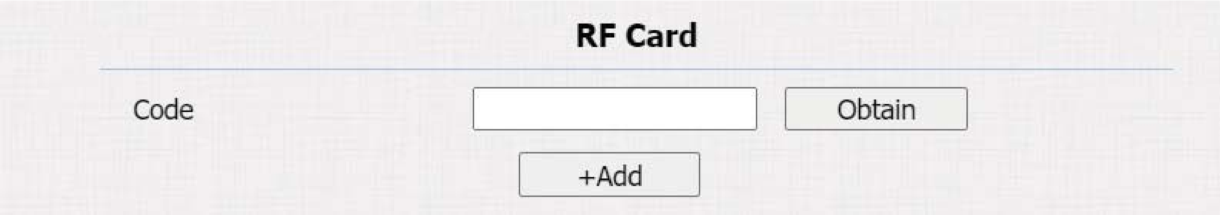


Private PIN

Enabled ☑

Unlock by RF Card

On the **Intercom** > **User** > **Add** interface, find the **RF Card** part.



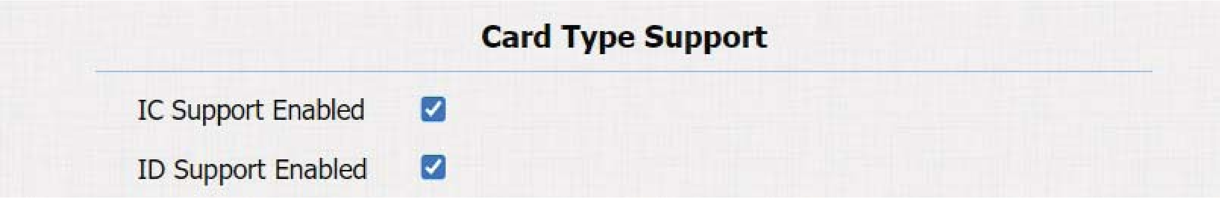
RF Card

Code

- **Code**: The card number that the card reader reads.

> **Note**
>
> - Each user can have a maximum of 5 cards added.
> - The device allows to add 5,000 users.
> - RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device for access.

You can enable and disable the use of RF cards on the **Intercom > Card Setting** interface.



Card Type Support

IC Support Enabled ☑

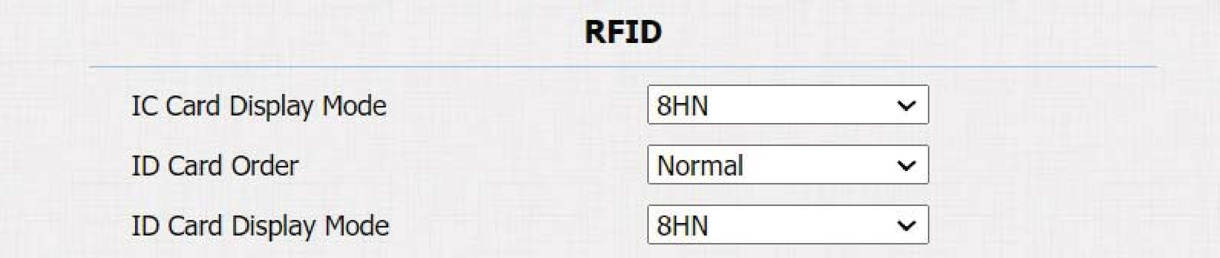
ID Support Enabled ☑

> **Tip**
>
> 1. You can also modify the user card on the device by pressing “*3888#” on the keypad to enter the Access Method Settings screen.
> 2. Then, enter the Admin Code “2396” to enter the User Card Adding and Deleting screen.

RF Card Code Format

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

To set it up, go to **Intercom > Card Setting > RFID** interface.



RFID

IC Card Display Mode: 8HN

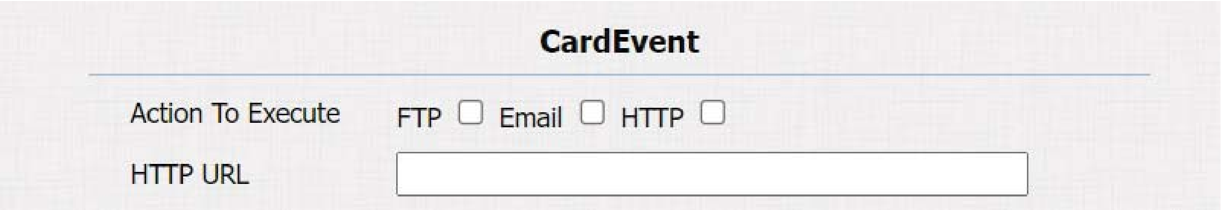
ID Card Order: Normal

ID Card Display Mode: 8HN

- **IC/ID Card Display Mode**: Set the card number format from the provided options.
- **ID Card Order**: Set the ID card reading mode between Normal and Reversed.

Actions Triggered by Swiping Cards

You can set actions triggered by swiping cards on the **Intercom > Card Setting > Card Event** interface.



CardEvent

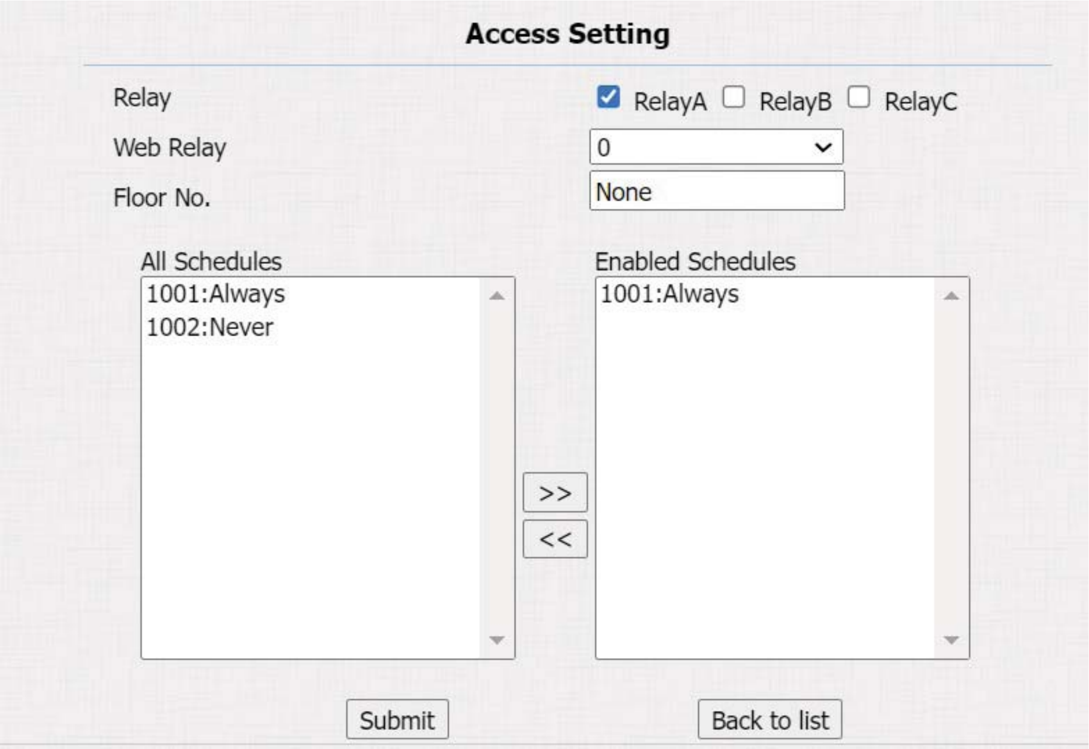
Action To Execute	FTP □ Email □ HTTP □
HTTP URL	

- **Action to Execute**:
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

Access Setting

You can customize access settings such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

On the **Intercom > User > Add** interface, scroll to the **Access Setting** section.



Access Setting

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

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

- **Relay**: Specify the relay(s) to be unlocked using the door opening methods assigned to the user.

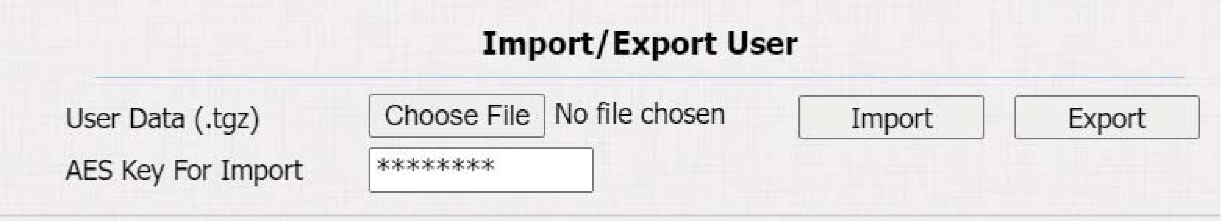
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **Floor No.** : Specify the accessible floor(s) to the user via the elevator.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
    - **Always**: Allows door opening without limitations on door open counts during the valid period.
    - **Never**: Prohibits door opening.

Import/Export User Data

The door phone supports User Data of access control to be shared among Akuvox door phones through import and export while you can also export the facial data out of the door phone and then import it to a third-party device.

To set it up, go to the **Intercom** > **User** > **Import/Export User** interface.

The import/export file should be in TGZ format.



Import/Export User

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

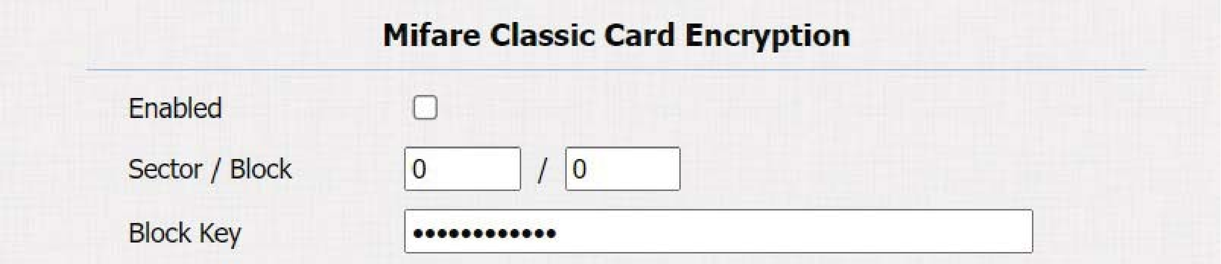
AES Key For Import ********

- **AES Key For Import**: When the imported file is encrypted, enter its password here.

Mifare Card

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 set it up, go to **Intercom** > **Card Setting** > **Mifare Classic Card Encryption** interface.



Mifare Classic Card Encryption

Enabled □

Sector / Block 0 / 0

Block Key ••••••••••••

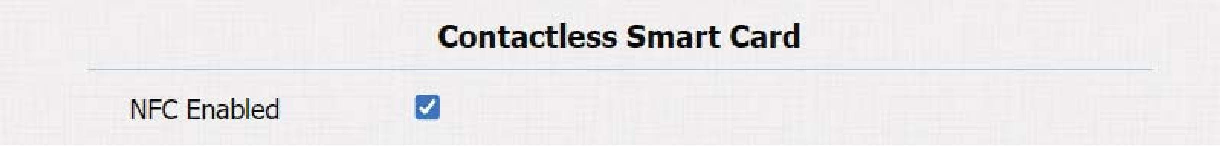
- **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).

- **Block Key**: Set a password to access the data stored in the predefined sector/block.

Unlock by NFC

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.

Enable or disable the NFC feature on the **Intercom** > **Card Setting** > **Contactless Smart Card** interface.



Contactless Smart Card

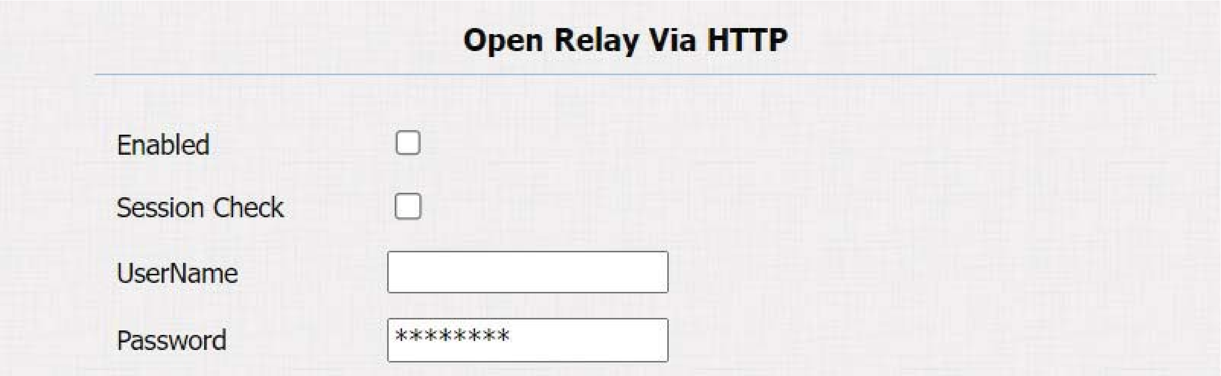
NFC Enabled ☑

> **Note**
>
> - The NFC feature is not available on iPhones.
> - Please refer to Open the Door via NFC for detailed configuration.

Unlock by HTTP Command

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 set it up, go to **Intercom** > **Relay** > **Open Relay Via HTTP** interface.



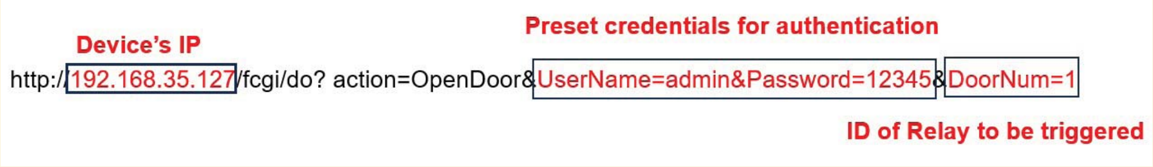
Open Relay Via HTTP

Enabled	□
Session Check	□
UserName	
Password	********

- **Session Check**: When enabled, the HTTP unlock requires logging into the device’s web interface. Or, the door opening may fail.
- **Username**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a password for authentication in HTTP command URLs.

Tip

Here is an HTTP command URL example for relay triggering.



Device's IP

Preset credentials for authentication

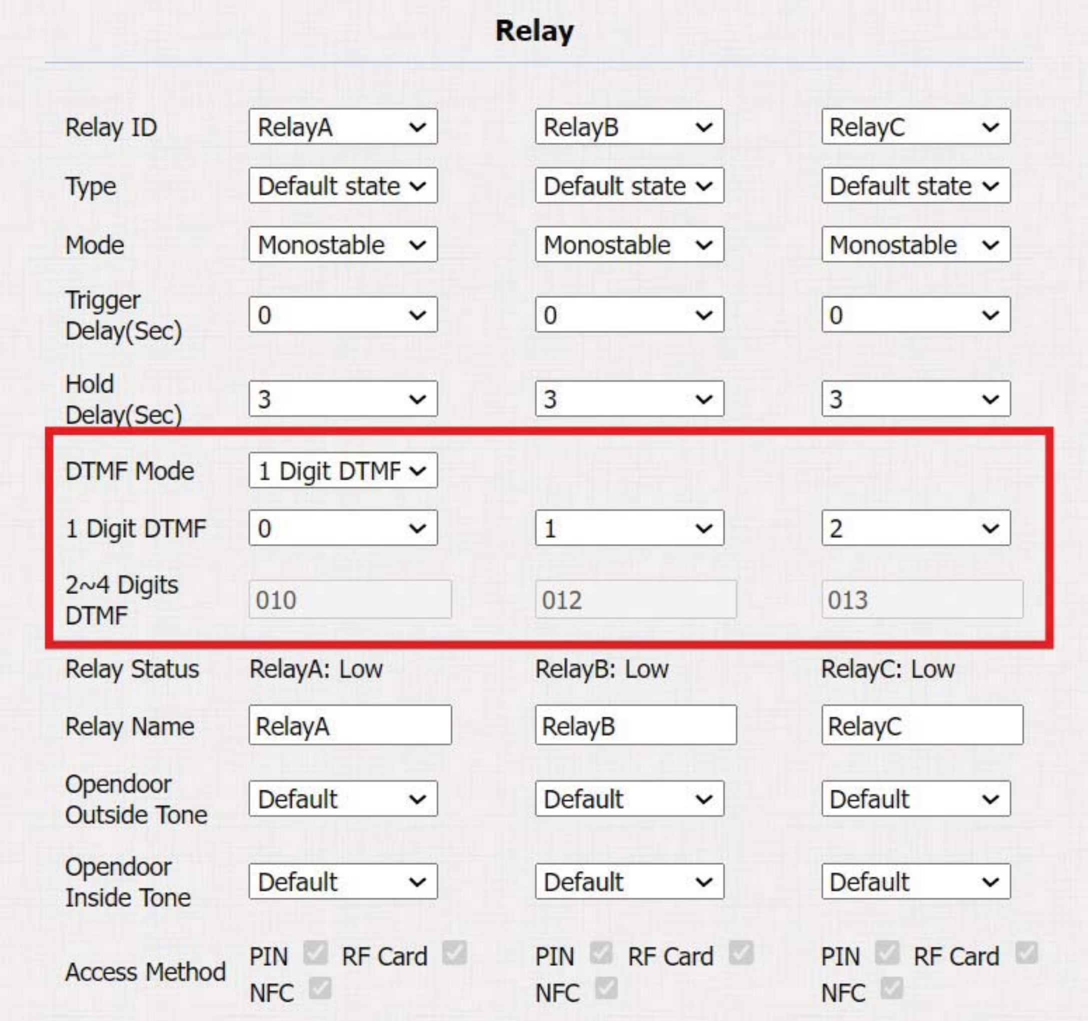
http://192.168.35.127/fcgi/do? action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

ID of Relay to be triggered

Unlock by DTMF Code

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

To configure DTMF codes, go to **Intercom** > **Relay** interface.



Relay

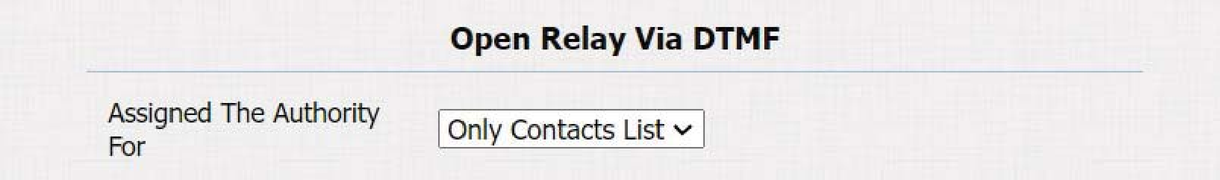
Relay ID	RelayA	RelayB	RelayC
Type	Default state	Default state	Default state
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	3	3	3
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	0	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	RelayA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

- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

> **Note**
>
> To open the door with DTMF, the intercom devices that send and receive the unlock command must use the same mode and code. Otherwise, the DTMF unlock may fail. See here for the detailed DTMF configuration steps.

DTMF White List

To secure 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

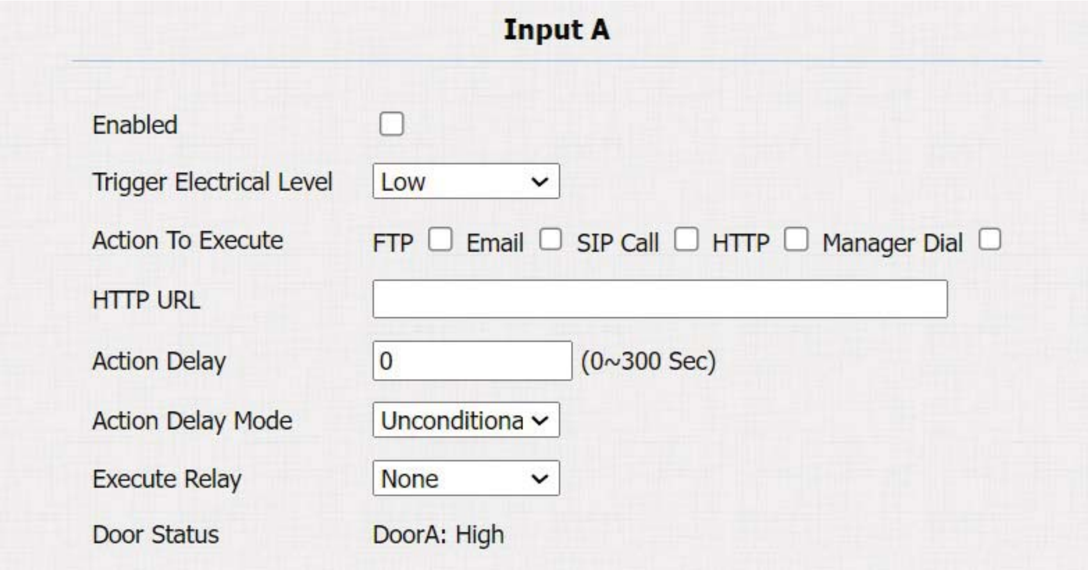
Assigned The Authority For	Only Contacts List ⌄

- **Assigned The Authority For**: Specify the contacts authorized to open doors via DTMF:
  - **None**: No numbers can unlock doors using DTMF.
  - **Only Contacts List**: Doors can be opened by numbers added to the door phone's contact list.
  - **All Numbers**: Any numbers can unlock using DTMF.

Unlock by Exit Button

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

To set it up, navigate to the **Intercom** > **Input** interface.



Input A

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

- **Enabled**: To use a specific input interface.

- **Trigger Electrical Level**: Set the input interface to trigger at a low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - SIP Call: Call the preset number upon the trigger.
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
  - Manager Dial: When the input is triggered, a call will be made to the number(s) set on the **Intercom** > **Basic** > Manager Dial interface.

- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode**:
  - Unconditional Execution: The action will be carried out when the input is triggered.
  - Execute If Input Still Triggered: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.

- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Door Status**: Display the status of the input signal.

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.

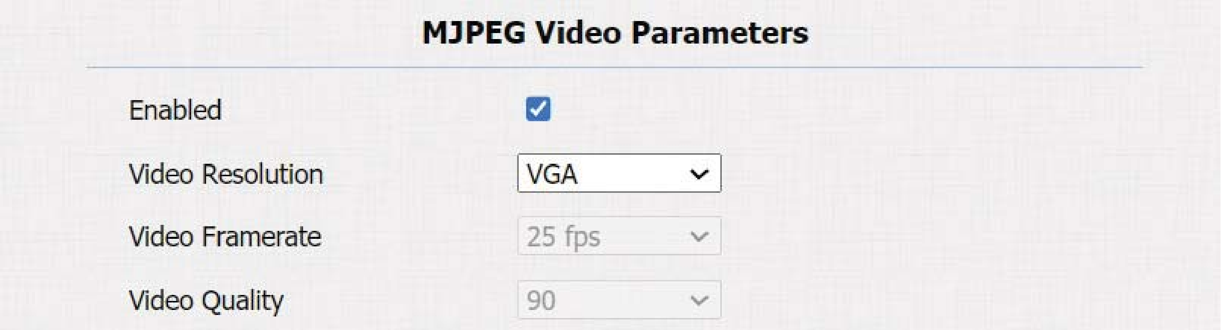
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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.

MJPEG Video Stream

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

To set it up, go to the **Intercom > RTSP > MJPEG Video Parameters** interface.



MJPEG Video Parameters

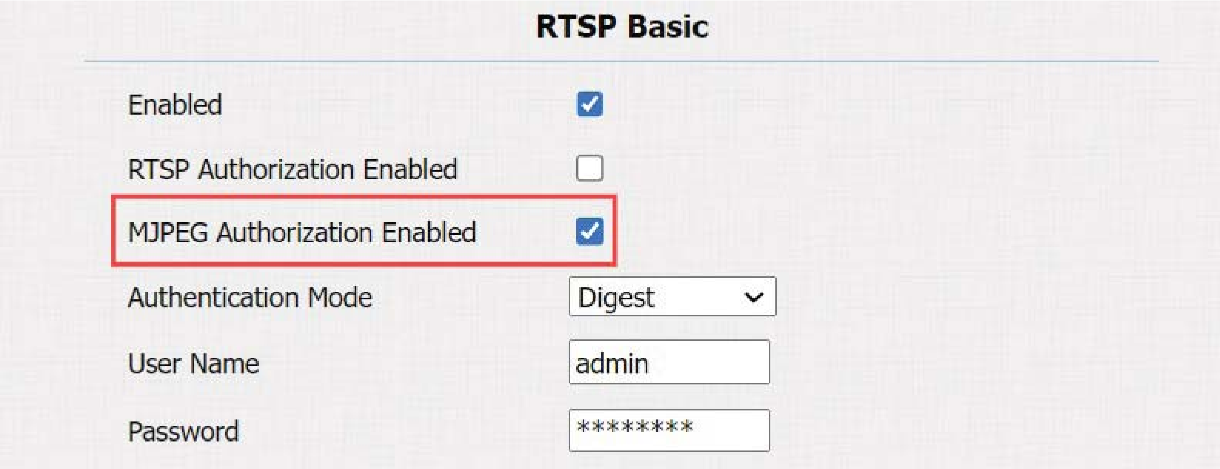
Enabled	☑
Video Resolution	VGA
Video Framerate	25 fps
Video Quality	90

- **Video Resolution**: Specify the video resolution from the lowest CIF(352×288 pixels) to the highest 1080P(1920×1080 pixels).
- **Video Framerate**: It is 25 fps by default.
- **Video Quality**: It is 90 by default.

MJPEG Authorization

You can enable MJPEG authorization to limit access to the MJPEG images and videos.

To set it up, go to the **Intercom > RTSP > RTSP Basic** interface.



RTSP Basic

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

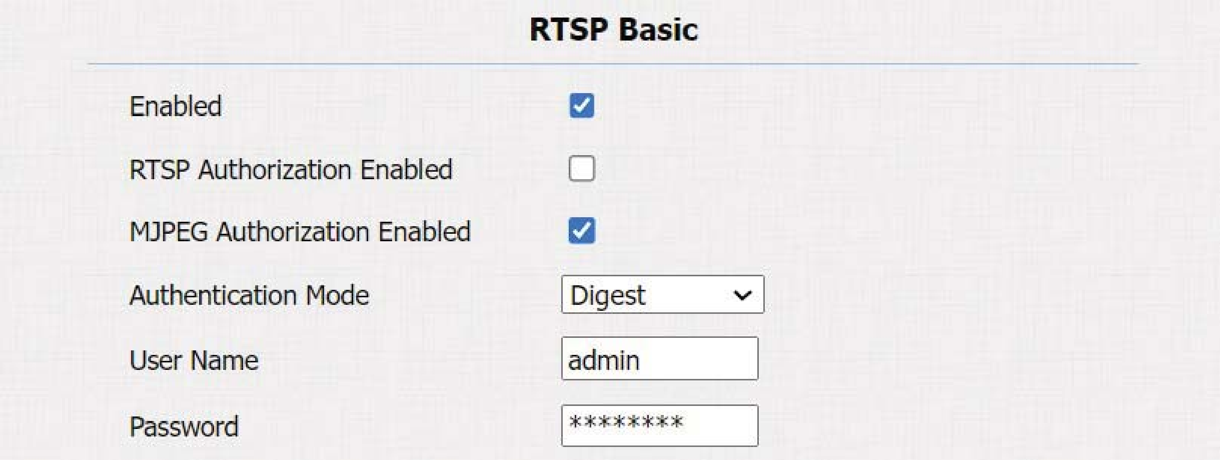
- **MJPEG Authorization Enabled**: Once enabled, accessing the door phone's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username, and RTSP Password.

> **Tip**
>
> - To view a dynamic stream, use the URL http://device_IP:8080/video.cgi.
> - For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
>   - http://device_IP:8080/picture.cgi
>   - http://device_IP:8080/picture.jpg
>   - http://device_IP:8080/jpeg.cgi
> - For example, if you want to capture the jpg format image of the door phone with the IP address 192.168.1.104, you can enter http://192.168.1.104:8080/picture.jpg on the web browser.

RTSP Stream Monitoring

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

To set it up, go to the **Intercom > RTSP > RTSP Basic** interface.



RTSP Basic

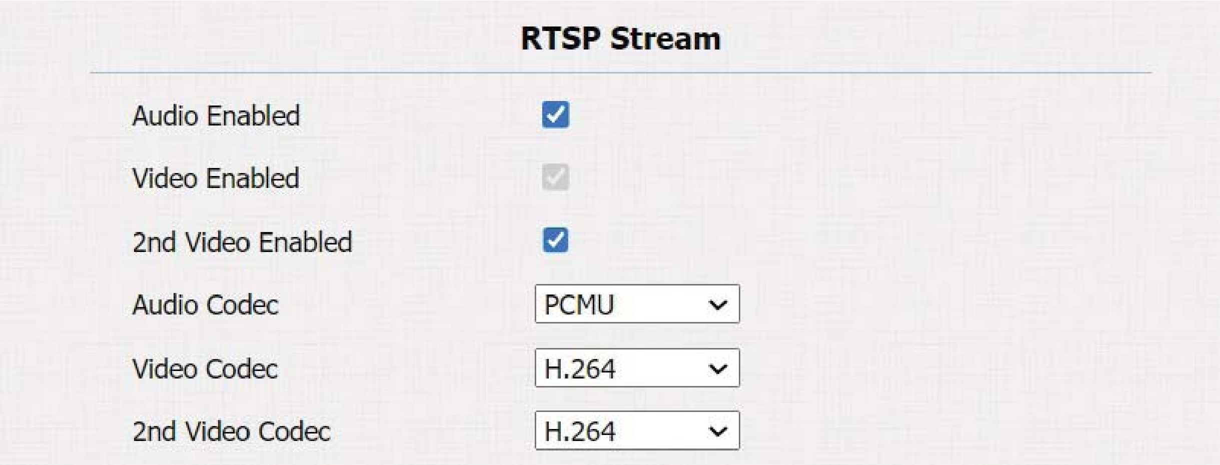
Enabled	☑
RTSP Authorization Enabled	□
MJPEG Authorization Enabled	☑
Authentication Mode	Digest
User Name	admin
Password	********

- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: It is Digest by default that uses hashing instead of the easily reversible Base64 encoding. A token is used for verification.
- **User Name**: Set the username for authorization.
- **Password**: Set the password for authorization.

RTSP Basic Setting

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

To set it up, go to the **Intercom > RTSP > RTSP Stream** interface.



RTSP Stream

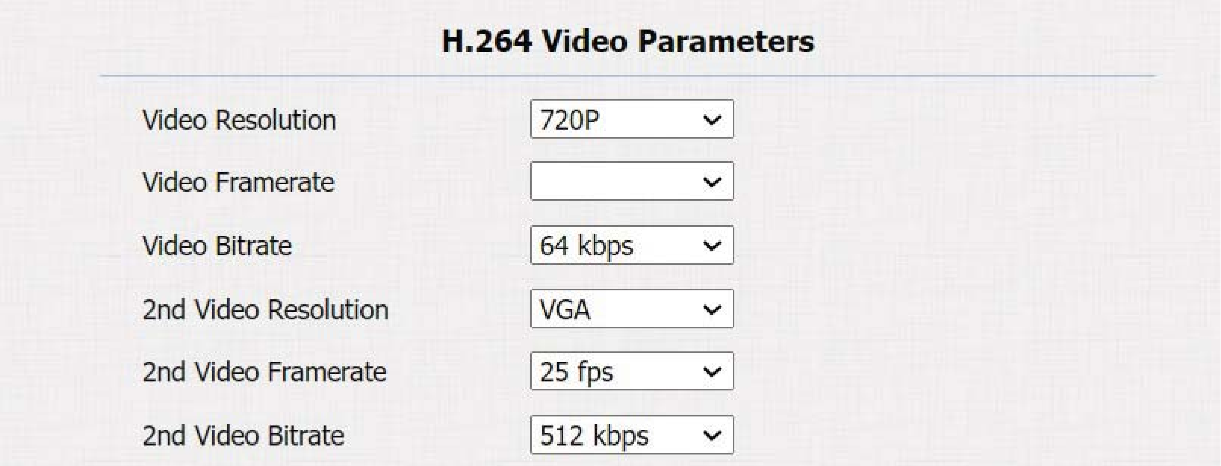
Audio Enabled	☑
Video Enabled	☑
2nd Video Enabled	☑
Audio Codec	PCMU
Video Codec	H.264
2nd Video Codec	H.264

- **Audio Enabled**: When enabled, the device will send the audio stream with the video to the monitor via RTSP.
- **Video Enabled**: It is enabled by default.
- **2nd Video Enabled**: The device supports two video stream channels. You can enable the second one.
- **Audio Codec**: Select the audio codec from the available options.
- **Video Codec**: Select the video codec between H.264 and MJPEG.
- **2nd Video Codec**: Select the video codec for the second video stream.

> **Tip**
>
> To view the audio and video stream using RTSP:
>
> - First channel: rtsp://Device’s IP/live/ch00_0
> - Second channel: rtsp://Device’s IP/live/ch00_1

H.264 Video Parameters Setup

Set up the H.264 video parameters for the RTSP video stream on the **Intercom > RTSP > H.264 Video Parameters** interface.



H.264 Video Parameters

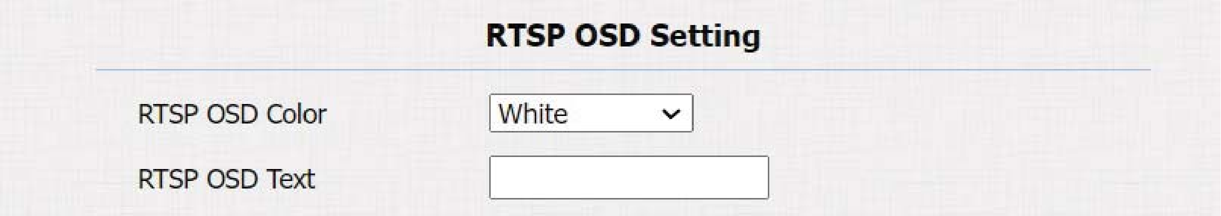
Video Resolution	720P
Video Framerate	
Video Bitrate	64 kbps
2nd Video Resolution	VGA
2nd Video Framerate	25 fps
2nd Video Bitrate	512 kbps

- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video.
- **Video Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth.
- **2nd Video Resolution**: Specify the image resolution for the second video stream channel.
- **2nd Framerate**: Set the frame rate for the second video stream channel.
- **2nd Video Bitrate**: Set the bit rate for the second video stream channel. The default is 512 kbps.

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 set it up, go to the **Intercom > RTSP > RTSP OSD Setting** interface.



RTSP OSD Setting

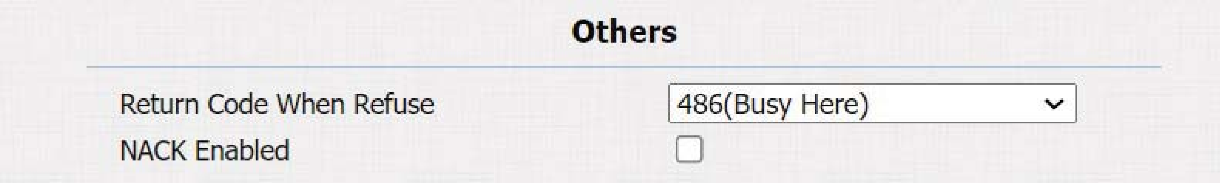
RTSP OSD Color	White
RTSP OSD Text	

- **RTSP OSD Color**: Select color from White, Black, Red, Green, and Blue.
- **RTSP OSD Text**: Customize the OSD content.

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** interface.



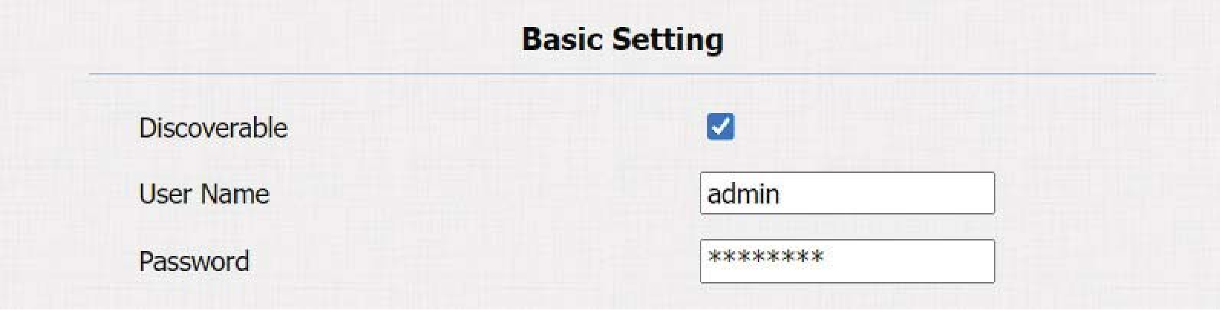
Others

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

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.

To set it up, go to the **Intercom > ONVIF** interface.



Basic Setting

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

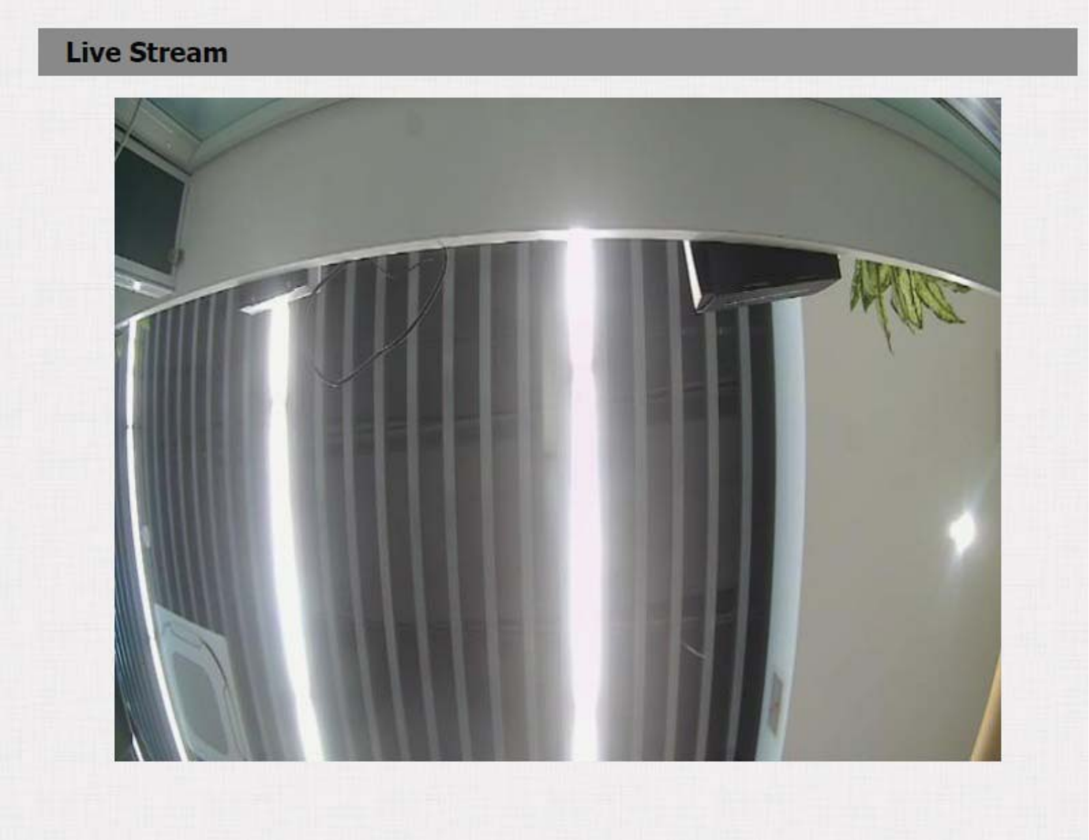
- **Discoverable**: When enabled, the video from the door phone camera to be searched by other devices.
- **User Name**: Set the username required for accessing the door phone's video stream on other devices. It is admin by default.
- **Password**: Set the password required for accessing the door phone's video stream on other devices. It is admin by default.

> **Tip**
>
> Once the settings are configured, to access the video stream on the third-party device, simply enter the ONVIF URL: http://Device’s IP:80/onvif/device_service.

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.

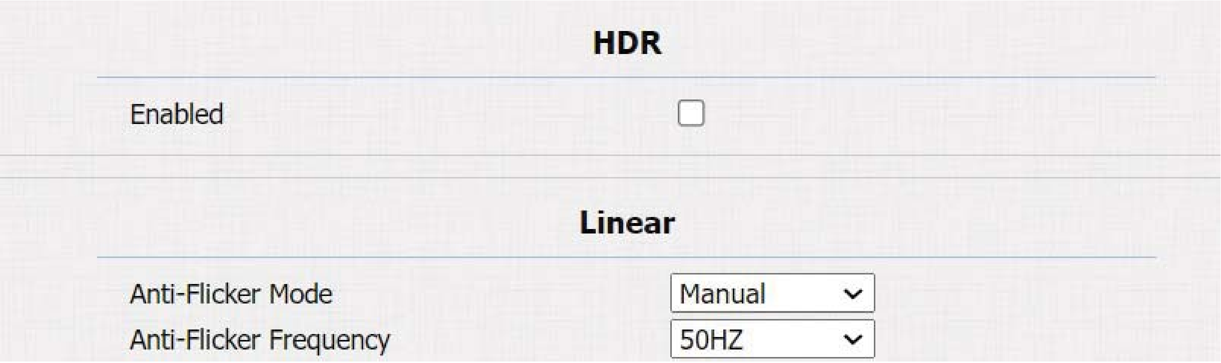
View the video stream on the **Intercom > Live Stream** interface. If you have enabled RTSP authorization, you need to enter the user name and password set in the RTSP Basic section for viewing the stream.



Camera Mode

- High Dynamic Range (HDR) is a technology used in photography, videography, and display devices to enhance image quality by capturing a wider range of brightness and color.
- Linear refers to a straightforward representation of brightness in images. Linear images are commonly used in controlled lighting environments, such as indoor scenes, where consistent brightness is present.

You can set the camera mode between HDR and Linear on the **Phone > Camera** interface. When you disable HDR, the device will adopt the Linear mode.



HDR

Enabled ☐

Linear

Anti-Flicker Mode: Manual

Anti-Flicker Frequency: 50HZ

- **Anti-Flicker Mode**: The anti-flicker feature reduces or eliminates flickering in images or videos caused by varying light sources.

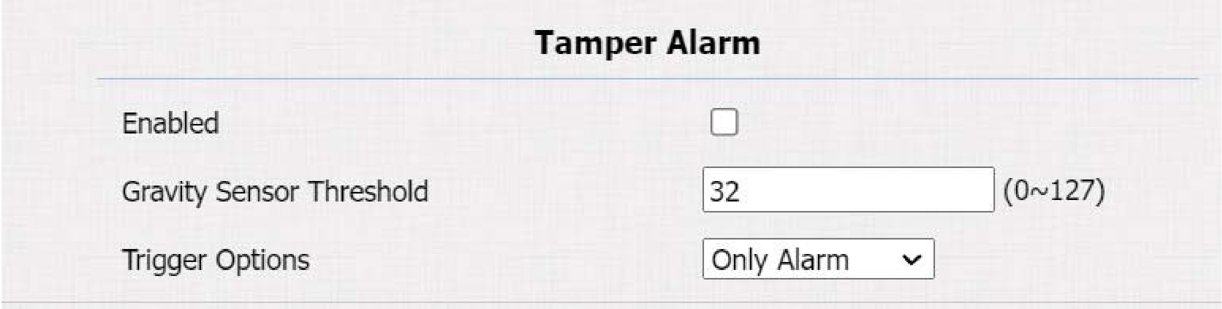
- Auto: The device will switch automatically between 50HZ and 60HZ anti-flicker frequency.
- Manual: Select the anti-flicker frequency manually between 50HZ and 60HZ.
- Off: Disable the anti-flicker function.

Security

Tamper Alarm

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 set it up, go to the **Security** > **Basic** > **Tamper Alarm** interface.



Tamper Alarm

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

- **Gravity Sensor Threshold**: The threshold for the gravity sensor sensitivity. The lower the value is, the easier the tamper alarm will be triggered. It is 32 by default.
- **Trigger Options**: Select what can be triggered when the gravity sensor is triggered.

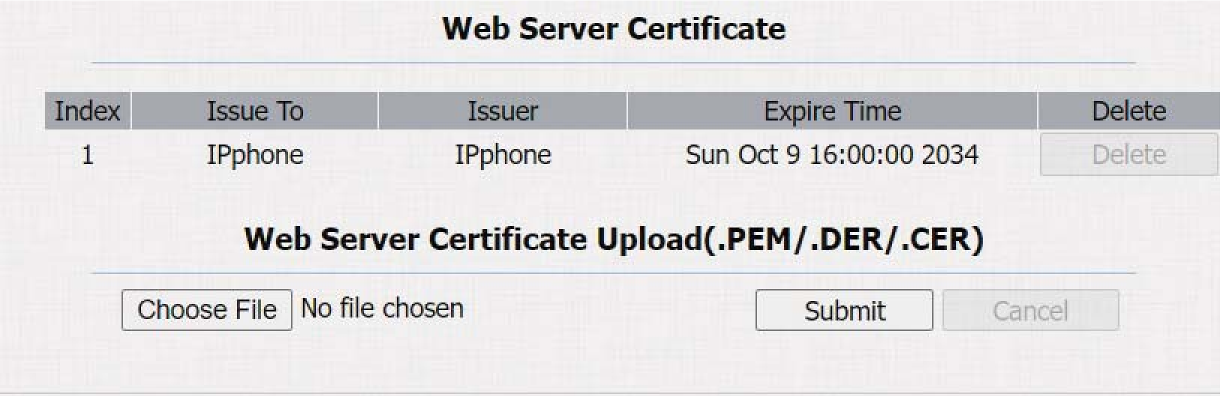
Client Certificate Setting

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.

Upload the Web Server Certificate on the **Security** > **Advanced** interface.



Web Server Certificate

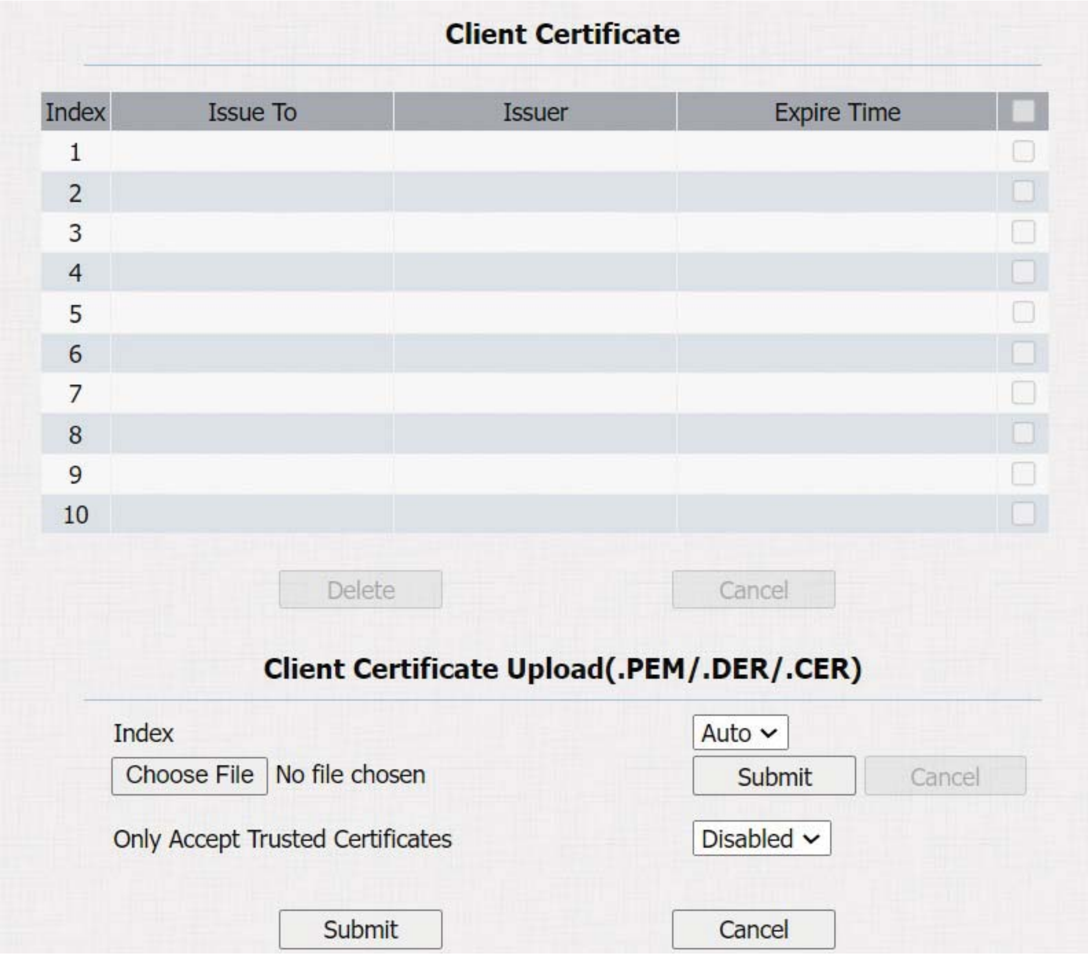
Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

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.

Upload the Client Certification on the **Security** > **Advanced** interface.



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

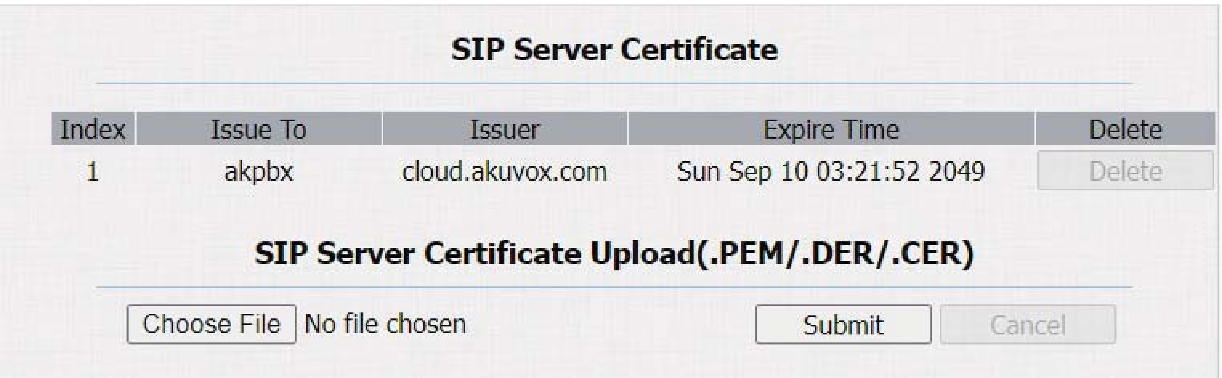
Only Accept Trusted Certificates: Disabled

- **Index:**
  - Auto: The uploaded certificate will be displayed in numeric order.
  - 1 to 10: the uploaded certificate will be displayed according to the value selected.
- **Upload:** Click Choose File to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, as long as the authentication succeeds, the doorphone will verify the server certificate based on the client certificate list. If select Disabled, the doorphone 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 certificate. This certificate is essential for server authentication.

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



SIP Server Certificate

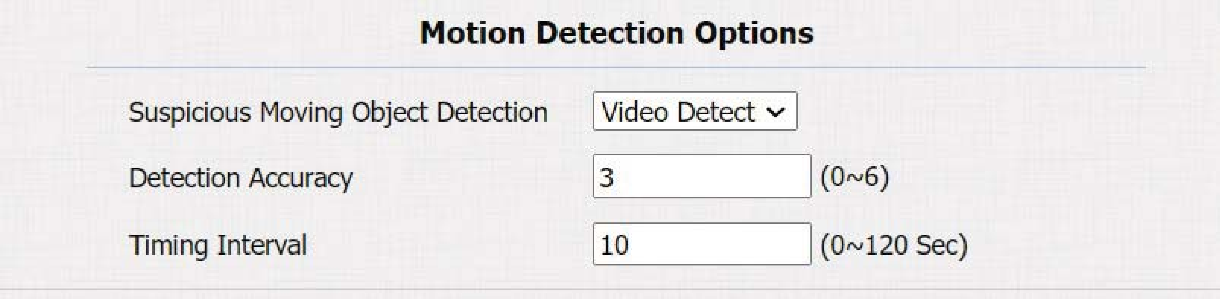
Index	Issue To	Issuer	Expire Time	Delete
1	akpbx	cloud.akuvox.com	Sun Sep 10 03:21:52 2049	Delete

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

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.

Set up motion detection on the **Intercom** > **Motion** interface.



Motion Detection Options

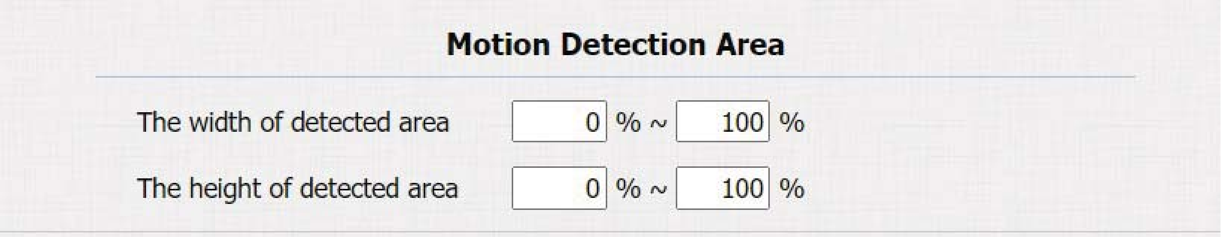
Suspicious Moving Object Detection	Video Detect	
Detection Accuracy	3	(0~6)
Timing Interval	10	(0~120 Sec)

- **Suspicious Moving Object Detection**:
  - Disabled: Turn off the motion detection function.
  - IR Detection: When the infrared sensor detects moving objects, preset actions will be triggered.
  - Video Detection: When the video camera detects moving objects, preset actions will be triggered.

- **Detection Accuracy**: The detection sensitivity. Specify this option when selecting **Video Detection**. The greater the value is, the more accurate the detection is. The default value is 3.
- **Timing Interval**: If you set the default time interval as 10 sec, the motion detection period will be 10 seconds. Assuming that we set the time interval as 10, and the first movement captured can be seen as the start point of the motion detection, and if the movement continues through 7 seconds of the 10 seconds interval, the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) anywhere between 7-10 seconds once the movement is detected. A 10-second interval is a complete cycle of motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the Time interval minus three.

When selecting **Video Detection**, you can scroll down to specify the motion detection 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%.



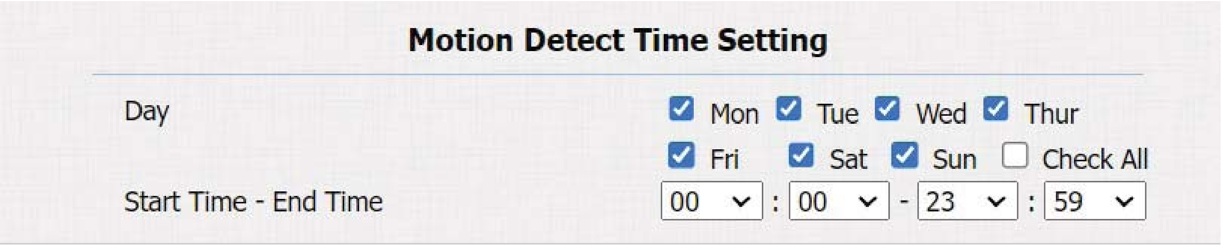
Motion Detection Area

The width of detected area	0 % ~ 100 %
The height of detected area	0 % ~ 100 %

Motion Detection Schedule

When motion detection is enabled, you can set a specific time for the feature to be effective.

Set it up on the **Intercom > Motion > Motion Detect Time Setting** interface.



Motion Detect Time Setting

Day	☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun □ Check All
Start Time - End Time	00 : 00 - 23 : 59

Security Notification

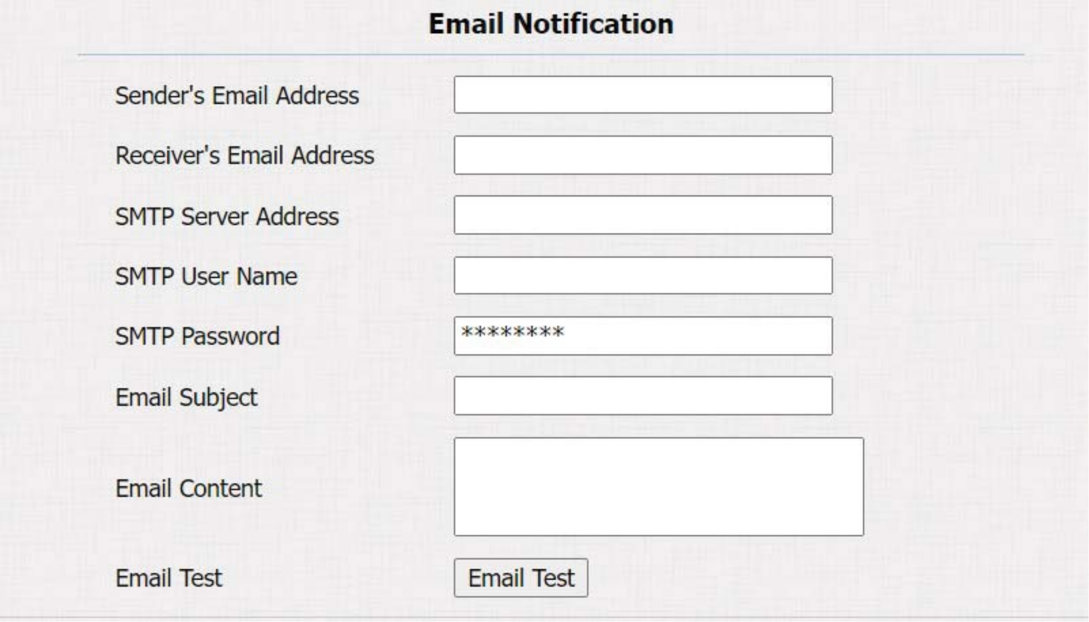
A security notification informs users or security personnel of any breach or threat that the door phone detects. For example, if the door phone detects something unusual, the system sends a notification to users or security through email, phone call, or other methods.

To set up security notifications, go to **Intercom > Action** interface.

Email Notification

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

Set it up in the **Email Notification** section.



Email Notification

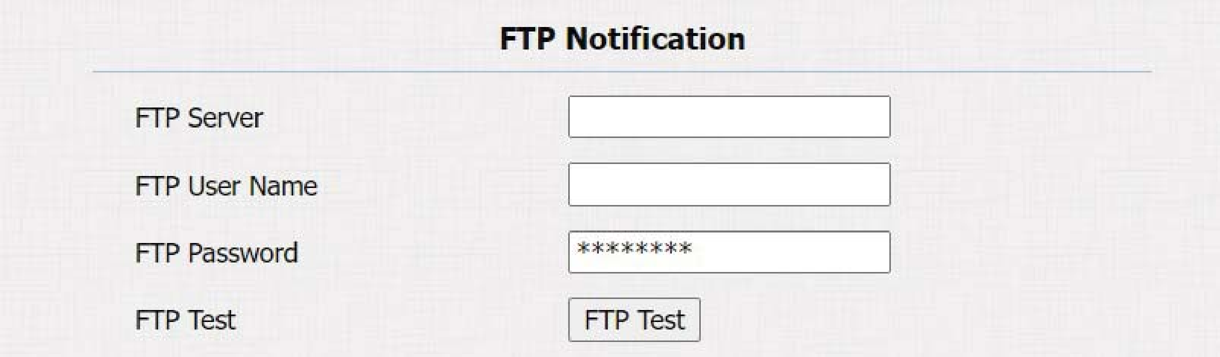
Sender's Email Address	
Receiver's Email Address	
SMTP Server Address	
SMTP User Name	
SMTP Password	********
Email Subject	
Email Content	
Email Test	Email Test

- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

FTP Notification

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.

Set it up in the **FTP Notification** section.



FTP Notification

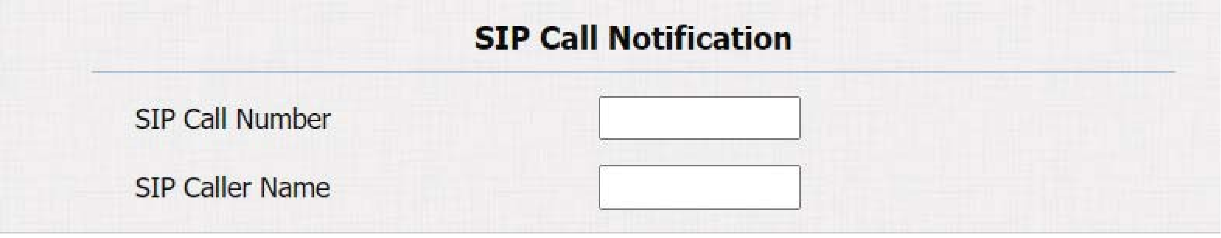
FTP Server	
FTP User Name	
FTP Password	********
FTP Test	FTP Test

- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

SIP Call Notification

In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered.

Set it up in the **SIP Call Notification** section.



SIP Call Notification

SIP Call Number

SIP Caller Name

Action URL

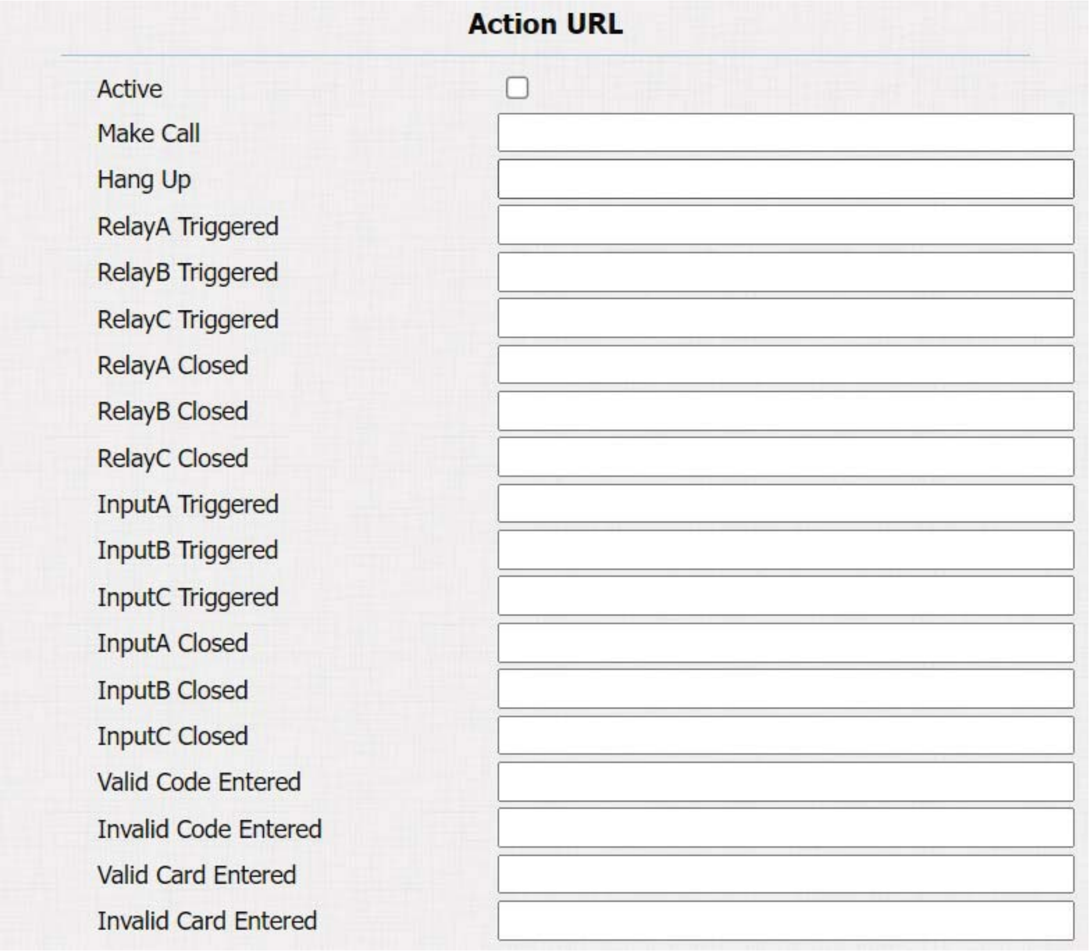
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

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

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

To set it up, go to the **Phone** > **Action URL** interface.



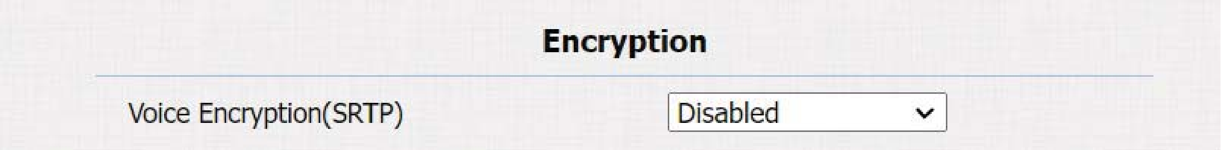
Action URL

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.

Set it up on the **Account** > **Advanced** > **Encryption** interface.



Encryption

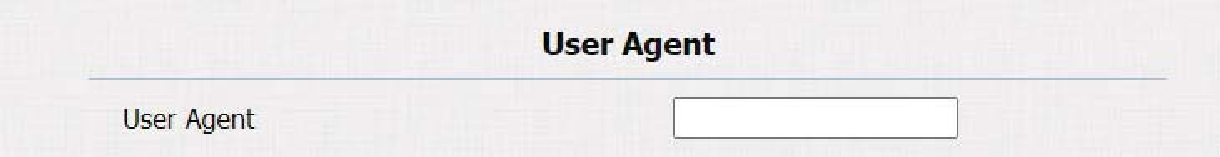
Voice Encryption(SRTP): Disabled

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

User Agent

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

To set it up, go to the **Account** > **Advanced** > **User Agent** interface.



User Agent

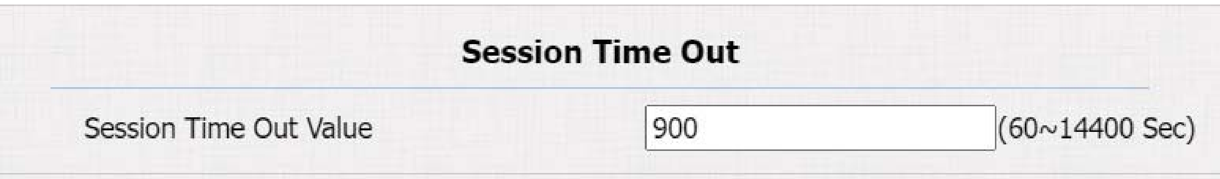
User Agent

- **User Agent:** Akuvox is by default.

Web Interface Automatic Log-out

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 set it up, go to **Security** > **Basic** > **Session Time Out** interface.



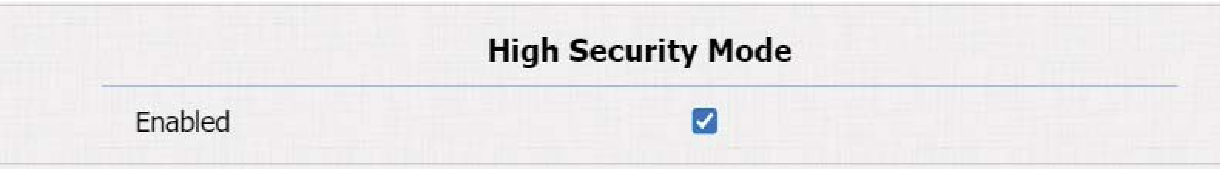
Session Time Out

Session Time Out Value 900 (60~14400 Sec)

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.

Enable or disable High Security Mode on the **Security** > **Basic** > **High Security Mode** interface.



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.

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

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

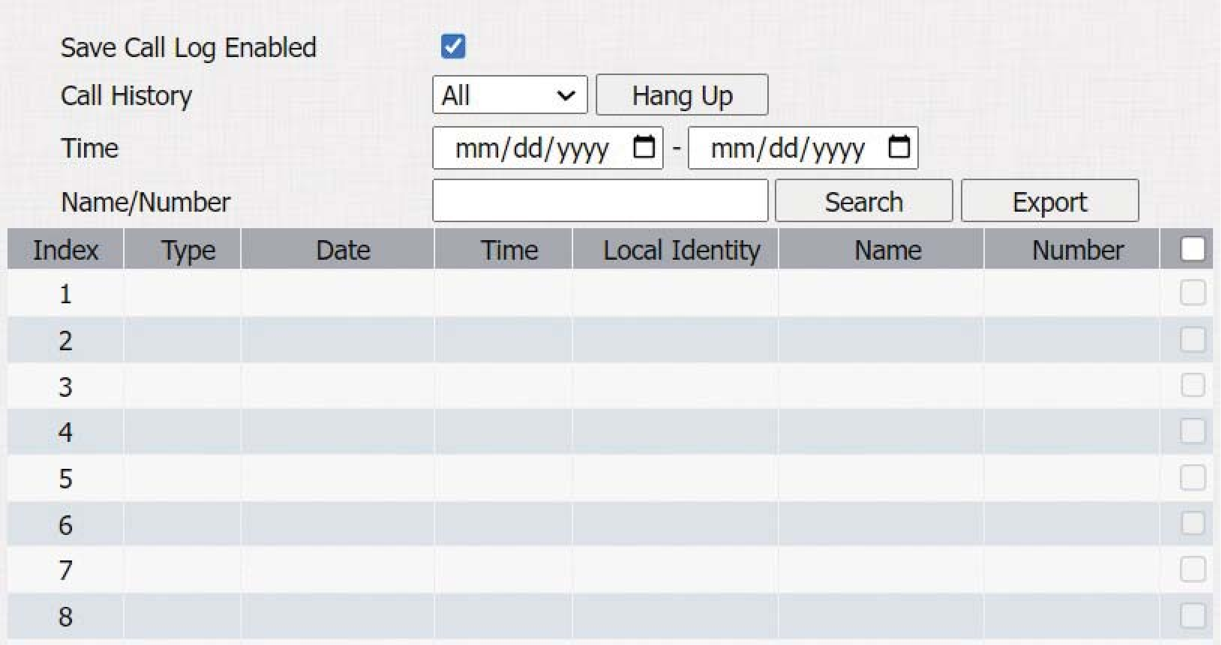
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

To check calls—including dial-out, received, and missed calls—within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

Check call logs on the **Phone** > **Call Log** interface.



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

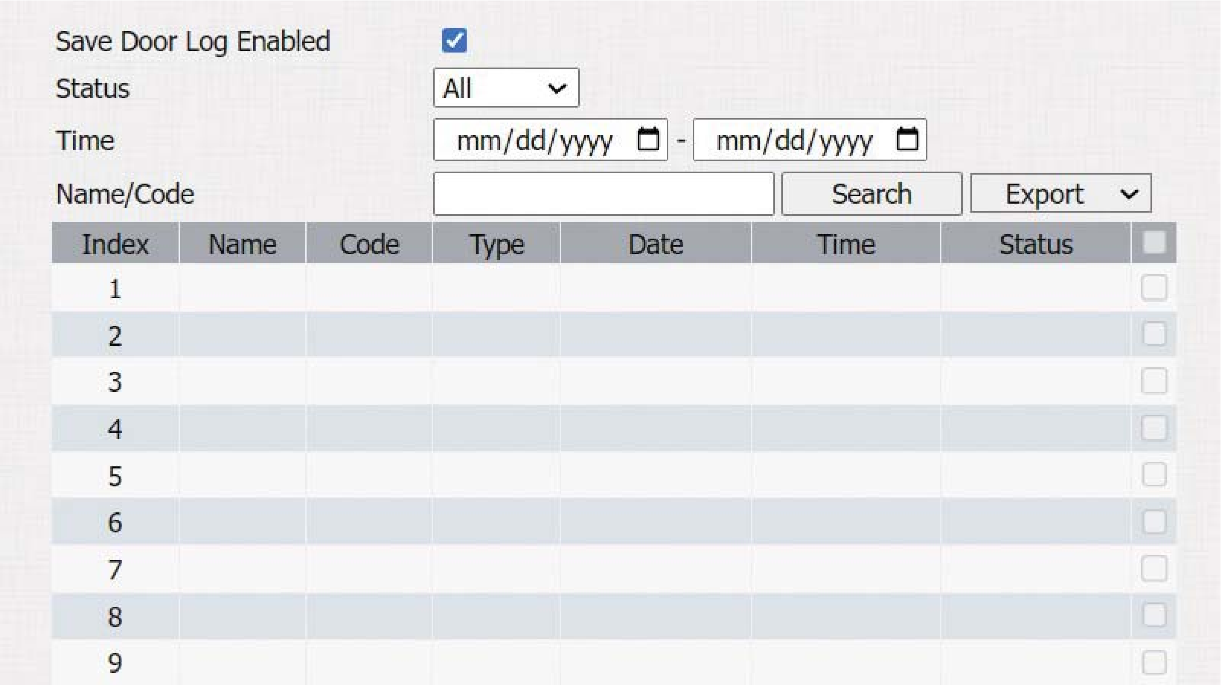
Index	Type	Date	Time	Local Identity	Name	Number	□
1							□
2							□
3							□
4							□
5							□
6							□
7							□
8							□

- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.

Door Logs

To search and review various types of door access history, simply check the door logs on the device's web interface.

Check door logs on the **Phone** > **Door Log** interface. You can click Export to export door logs in XML or CSV files.



Save Door Log Enabled	☑
Status	All
Time	mm/dd/yyyy - mm/dd/yyyy
Name/Code	

Index	Name	Code	Type	Date	Time	Status	☐
1							☐
2							☐
3							☐
4							☐
5							☐
6							☐
7							☐
8							☐
9							☐

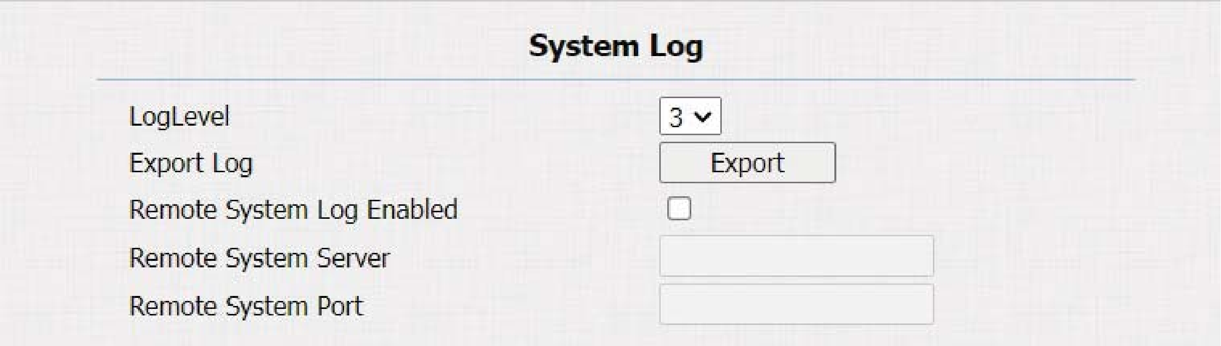
- **Status:** Display, All, Successful, or Failed door-opening records.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card code will be displayed. If the door is opened by an HTTP command, it will be empty.
- **Type:** Display the access methods.

Debug

System Log

System logs can be used for debugging purposes.

To set it up, go to the **Upgrade** > **Advanced** > **System Log** interface.



System Log

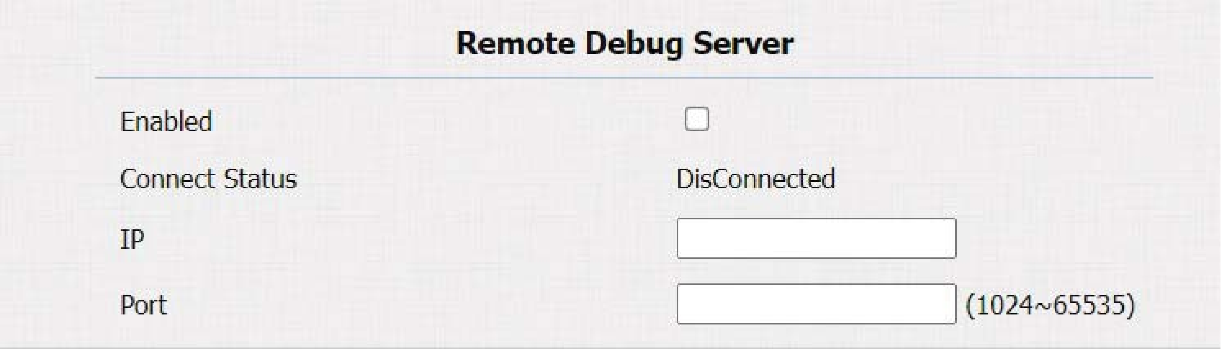
LogLevel	3
Export Log	Export
Remote System Log Enabled	□
Remote System Server	
Remote System Port	

- **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 the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export a temporary debug log file to a local PC.
- **Remote System Server:** Set the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.
- **Remote System Port**: Set the remote system server's port.

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.

To set it up, go to the **Upgrade** > **Advanced** > **Remote Debug Server** interface.



Remote Debug Server

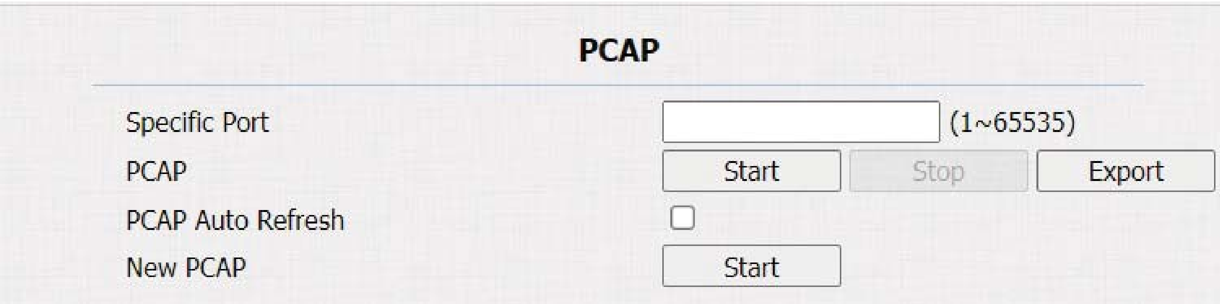
Enabled	□
Connect Status	DisConnected
IP	
Port	(1024~65535)

- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.
- **Port**: Enter the port of the server.

PCAP for Debugging

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

To set it up, go to the **Upgrade** > **Advanced** > **PCAP** interface.



PCAP

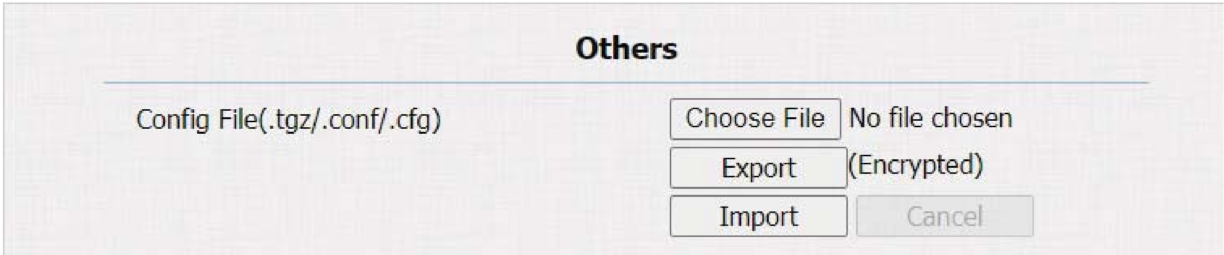
Specific Port	(1~65535)
PCAP	Start Stop Export
PCAP Auto Refresh	□
New PCAP	Start

- **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:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum in capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.
- **New PCAP:** Click Start to capture a bigger data package.

Backup

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

Export the file on the **Upgrade** > **Advanced** > **Others** interface.



Others

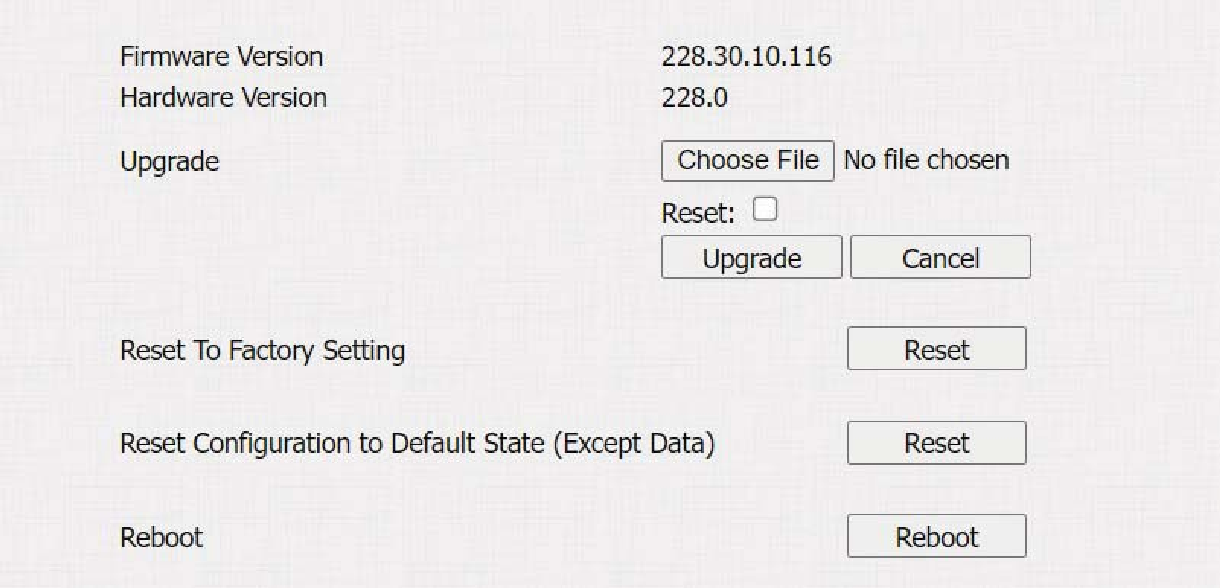
Config File(.tgz/.conf/.cfg)

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Upgrade the device on the **Upgrade > Basic** interface. Click Choose File to upload the firmware.

If you want to reset the device to the factory setting after the upgrade, you can check **Reset**.



Firmware Version 228.30.10.116

Hardware Version 228.0

Upgrade

Reset: □

Reset To Factory Setting

Reset Configuration to Default State (Except Data)

Reboot

> **Note**
>
> Firmware files should be .rom format for upgrade.

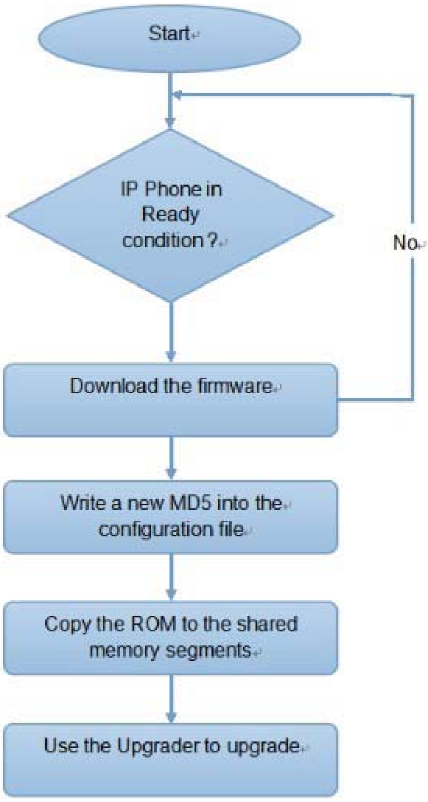
Auto-provisioning

You can configure and upgrade the device through the web interface using one-time or scheduled auto-provisioning with configuration files. This eliminates the need to set up configurations manually, saving you time and effort.

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 for auto-provisioning come in two formats: general configuration files and MAC-based configuration files.

Differences:

- **General Configuration Provisioning**:

A general configuration file is stored on a server, allowing all related devices to download the same file to update parameters.

- **MAC-Based Configuration Provisioning**:

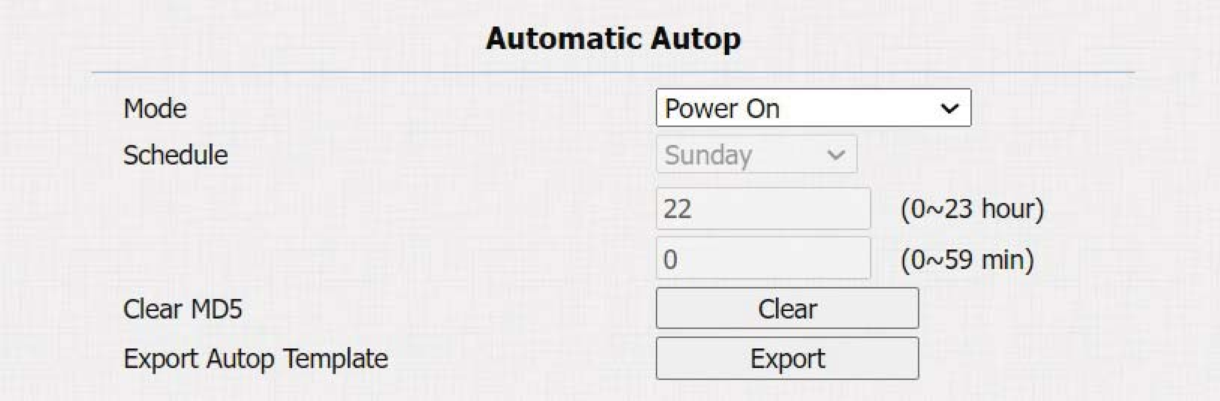
MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

> **Note**
>
> - Configuration files must be in CFG format.
> - The name of the general configuration file for batch provisioning varies by model.
> - The MAC-based configuration file is named after its MAC address.
> - Devices will first access general configuration files before the MAC-based ones if both types are available.
>
> You may click here to see the detailed format and steps.

AutoP Schedule

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

To set it up, go to the **Upgrade** > **Advanced** > **Automatic Autop** interface.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23 hour)

0 (0~59 min)

Clear MD5: Clear

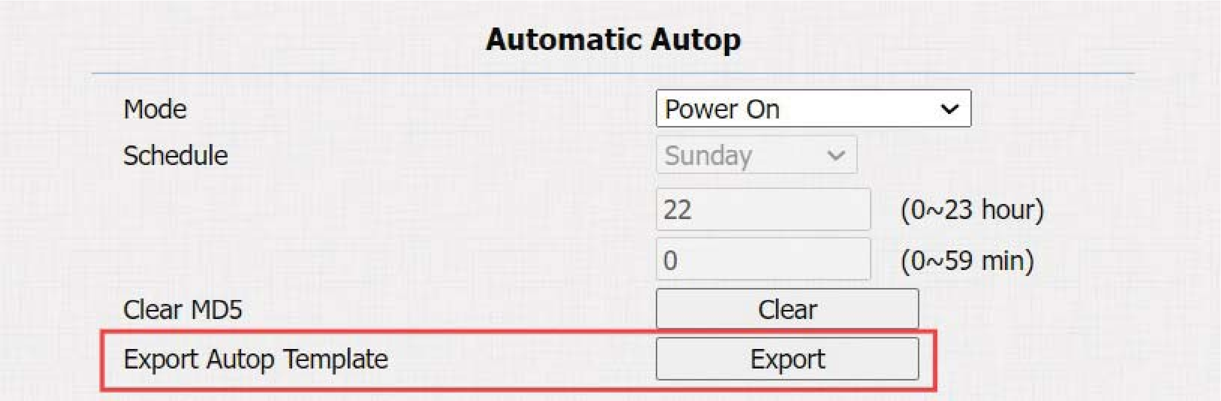
Export Autop Template: Export

- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: 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.
  - **Hourly Repeat**: The device will perform Autop every hour.

Static Provisioning

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.

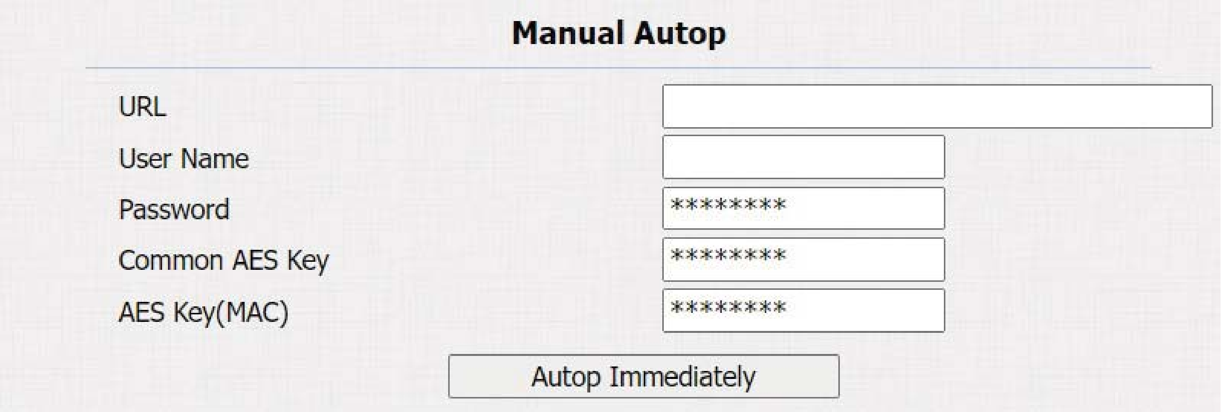
To set it up, download the template on **Upgrade > Advanced > Automatic Autop** interface first.



Automatic Autop

Mode	Power On	
Schedule	Sunday	
	22	(0~23 hour)
	0	(0~59 min)
Clear MD5	Clear	
Export Autop Template	Export	

Set up the Autop server in the **Manual Autop** section.



Manual Autop

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

Autop Immediately

- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server needs a username to be accessed.
- **Password**: Enter the password if the server needs a password to be accessed.
- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop 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)

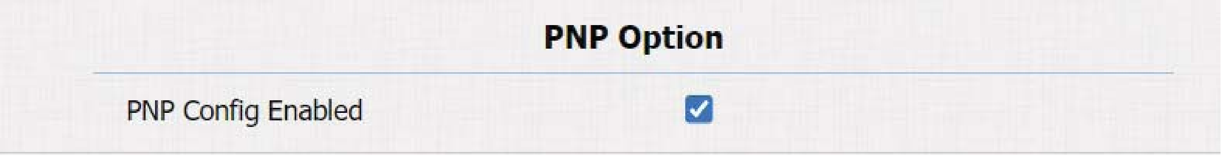
Tip

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

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.

Set it up on the web **Upgrade** > **Advanced** > **PNP Option** interface.

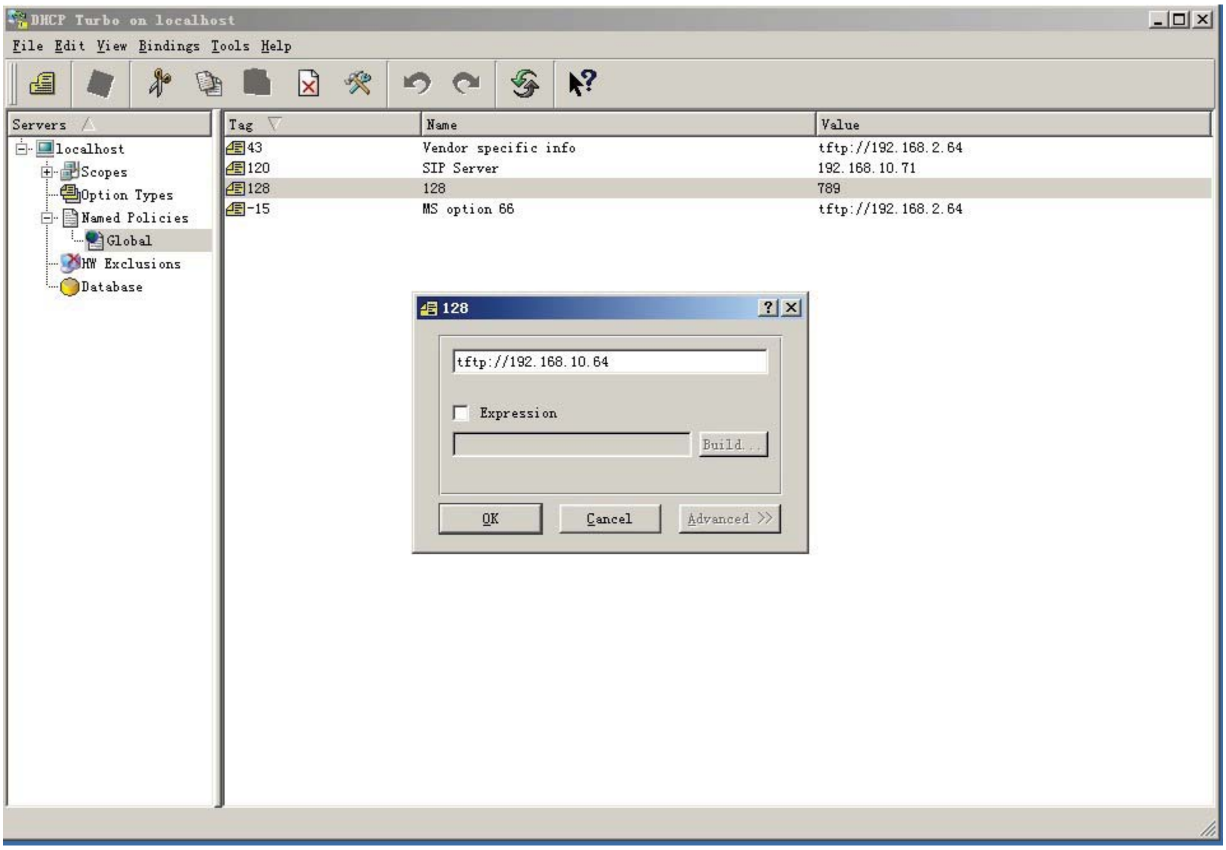


PNP Option

PNP Config Enabled ☑

DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.



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

128

tftp://192.168.10.64

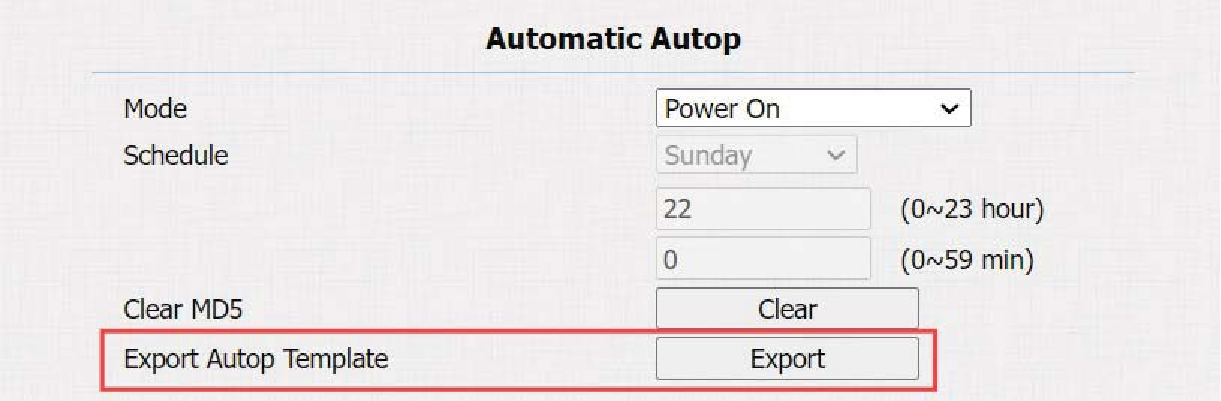
□ Expression

Note

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

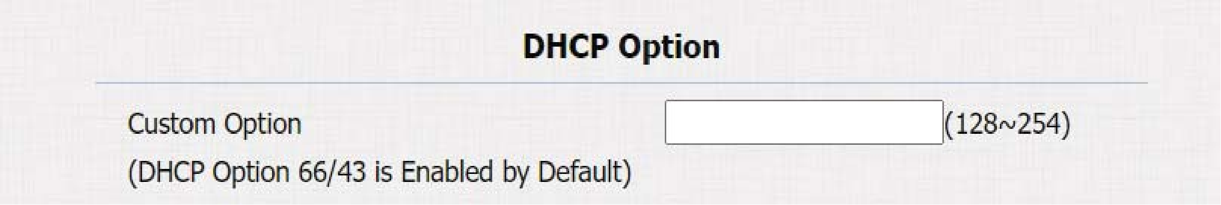
Set up DHCP Autop with Power On mode and export Autop Template to edit the configuration.

Export the Autop template on the **Upgrade** > **Advanced** > **Automatic Autop** interface.


Automatic Autop

Mode	Power On	
Schedule	Sunday	
	22	(0~23 hour)
	0	(0~59 min)
Clear MD5	Clear	
Export Autop Template	Export	

To set up the DHCP Option, scroll to the **DHCP Option** section.


DHCP Option

Custom Option (128~254)

(DHCP Option 66/43 is Enabled by Default)

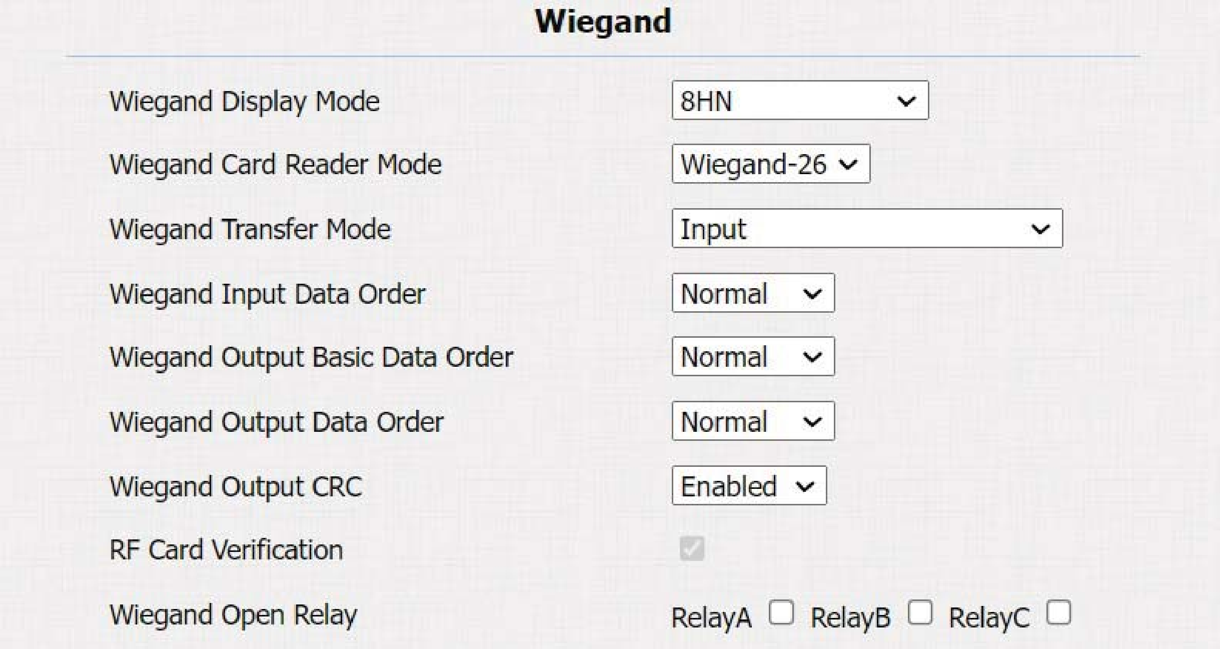
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the upgrade server URL in it.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the upgrade server URL in it.

Integration with Third Party Device

Integration via Wiegand

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

Set it up on the **Intercom** > **Wiegand** interface.



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
RF Card Verification: ☑
Wiegand Open Relay: RelayA □ RelayB □ RelayC □

- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the access control terminal and the third-party device. It is automatically configured.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender. If users can only open the door by swiping an RF card, select the Wiegand transfer mode as Output.
  - **Convert To Card No. Output**: The device serves as a sender. If users are assigned multiple door-opening methods, select the Wiegand transfer mode as Convert To Card No. Output.
- **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.
- **Wiegand Output Basic Data Order**: Set the sequence of the Wiegand output data.
  - **Normal**: The data is displayed as received.
  - **Reversed**: The order of the data bits is reversed.
- **Wiegand Output Data Order:** Determine the sequence of the card number.
  - **Normal**: The card number is displayed as received.

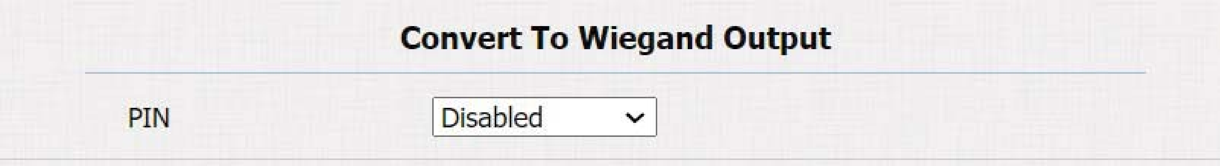
- **Reversed**: The order of the card number is reversed.

- **Wiegand Output CRC**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **RF Card Verification**: It is enabled by default. When the Wiegand Transfer Mode is Output, the device will check the validity of RF cards.
- **Wiegand Open Relay**: Check the relay to be triggered through Wiegand.

> **Note**
>
> Click here to see detailed configuration steps.

When the device is in Wiegand Output mode, you can set the Wiegand PIN code output format that determines how data are transmitted. The format should be consistent with that of the third-party device.

Set it up on the **Intercom > Wiegand > Convert To Wiegand Output** interface.



Convert To Wiegand Output

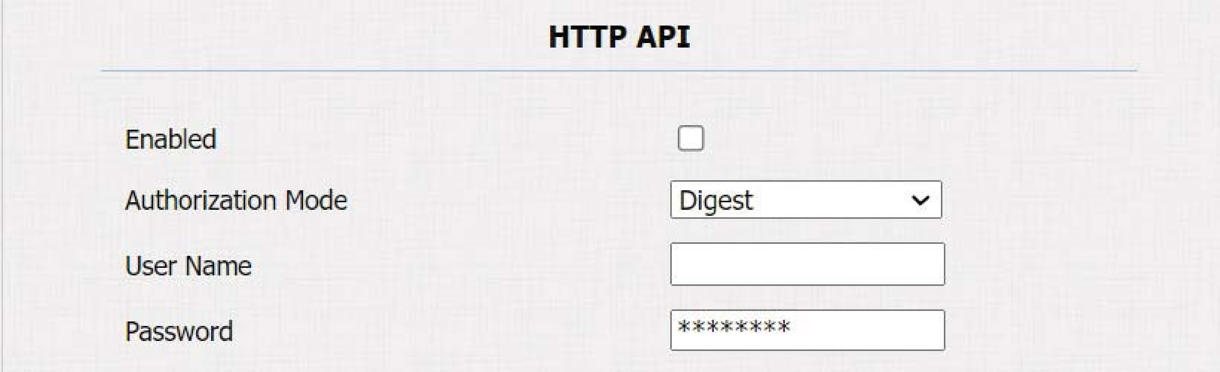
PIN: Disabled

- **8 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 8 bits "11100001".
- **4 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 4 bits "0001".
- **All at once**: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode.

Integration via HTTP API

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

Set it up on the **Intercom > HTTP API** interface.



HTTP API

Enabled: ☐

Authorization Mode: Digest

User Name:

Password: ********

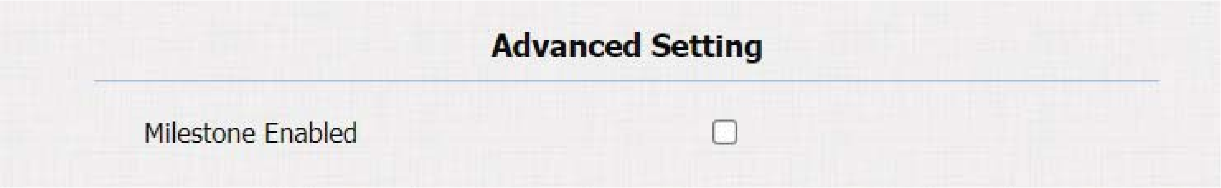
- **Enabled**: Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.

- **Authorization Mode**: It is Digest by default. You are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode the username and password.
- **User Name**: Enter the user name for authentication. The default is admin.
- **Password**: Enter the password for authentication. The default is admin.

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.

Enable it on the **Intercom > ONVIF** interface.



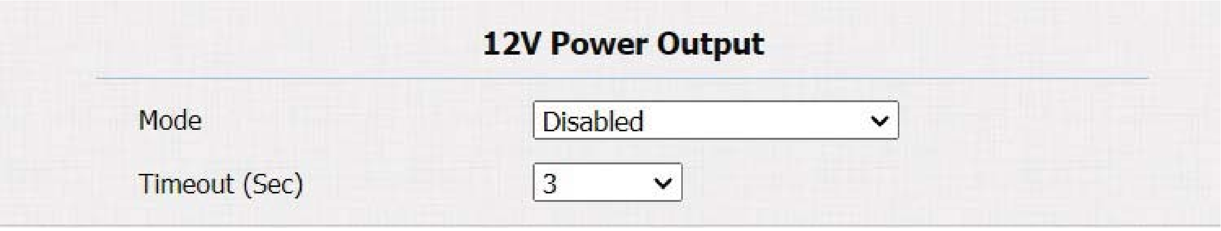
Advanced Setting

Milestone Enabled ☐

Power Output Control

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

To set up this feature, go to the **Intercom > Advanced >12V Power Output** interface.



12V Power Output

Mode: Disabled

Timeout (Sec): 3

- **Power Output Type**:
  - **Always**: Provide continuous power to the third-party device.
  - **Triggered by Open Relay**: 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.

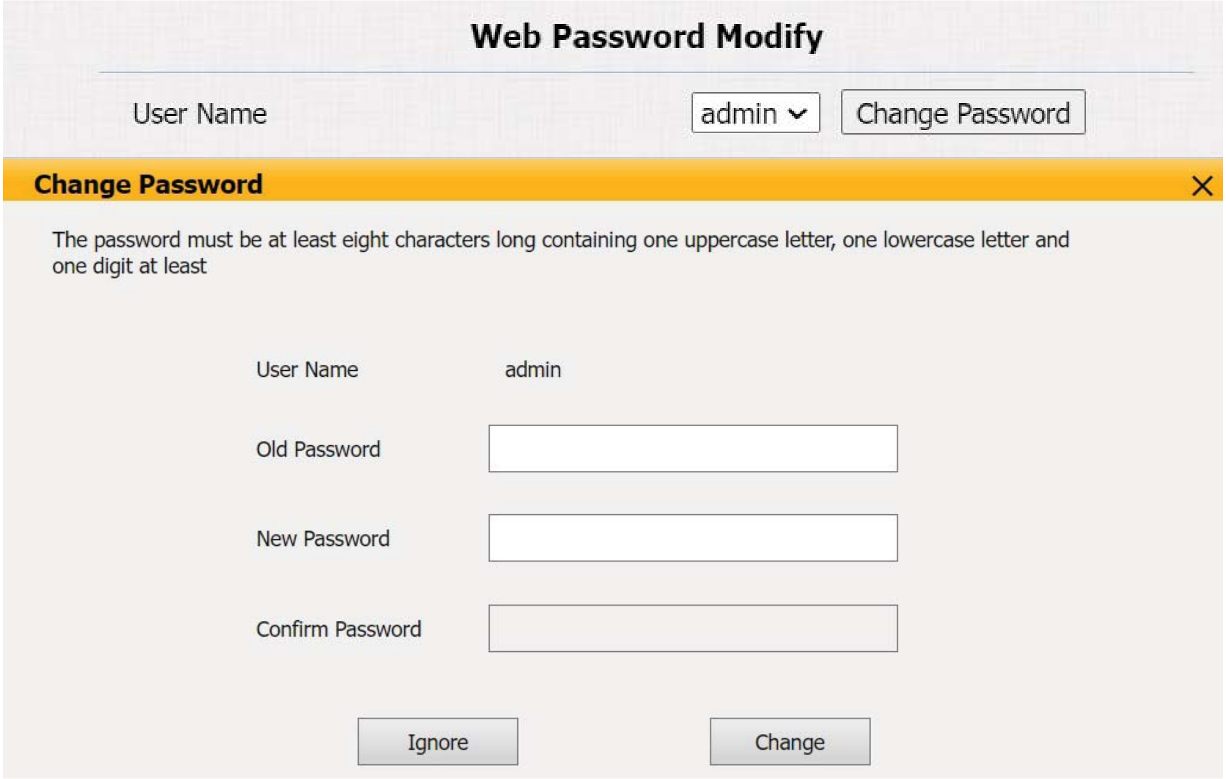
Password Modification

Modify Web Interface Password

You can modify the device web interface login password for both administrator and user accounts.

Go to the **Security** > **Basic** interface. Select admin for the administrator account and select user for the user account.

Click **Change Password** to modify the password.



Web Password Modify

User Name admin Change Password

Change Password

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

User Name admin

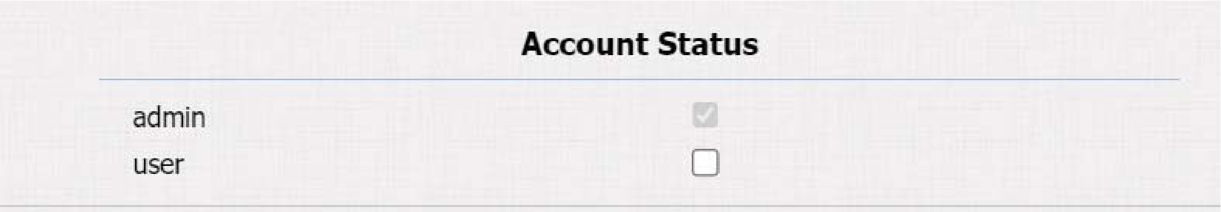
Old Password

New Password

Confirm Password

Ignore Change

Scroll to the **Account Status** section to enable or disable the use of the user account.



Account Status

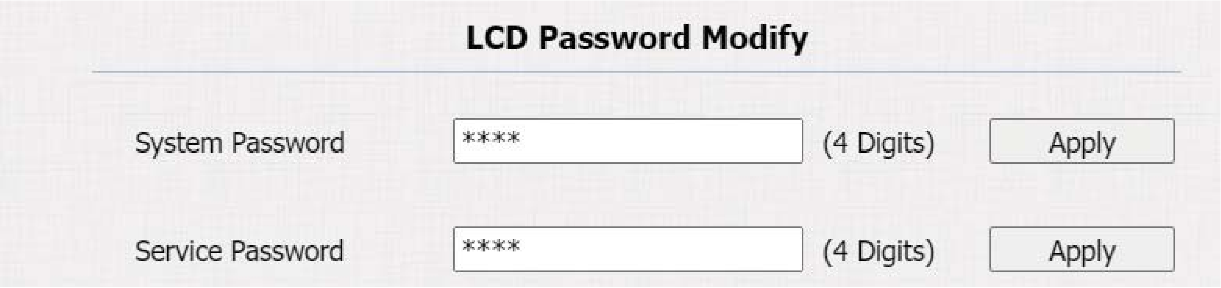
admin ☑

user □

Modify System Password

The system password is used to access the device's admin settings.

The default is 2396. You can change the password on the **Security** > **Basic** > **LCD Password Modify** interface.



LCD Password Modify

System Password	****	(4 Digits)	Apply
Service Password	****	(4 Digits)	Apply

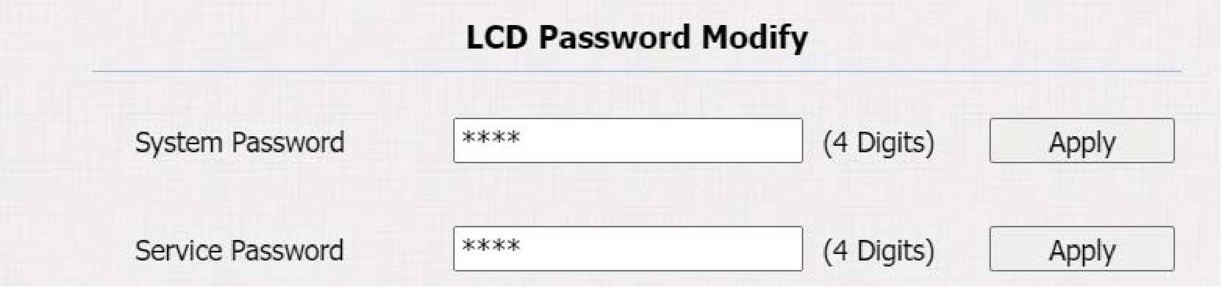
Tip

1. You can also change the system password directly on the device by pressing "*2396#".
2. Press "2" to enter the Admin Access screen.
3. Select Set Admin Password to change the system password.

Modify Service Password

The service password is used to quickly access the Access Methods Settings on the device.

The default is 3888. You can change the password on the **Security** > **Basic** > **LCD Password Modify** interface.



LCD Password Modify

System Password	****	(4 Digits)	Apply
Service Password	****	(4 Digits)	Apply

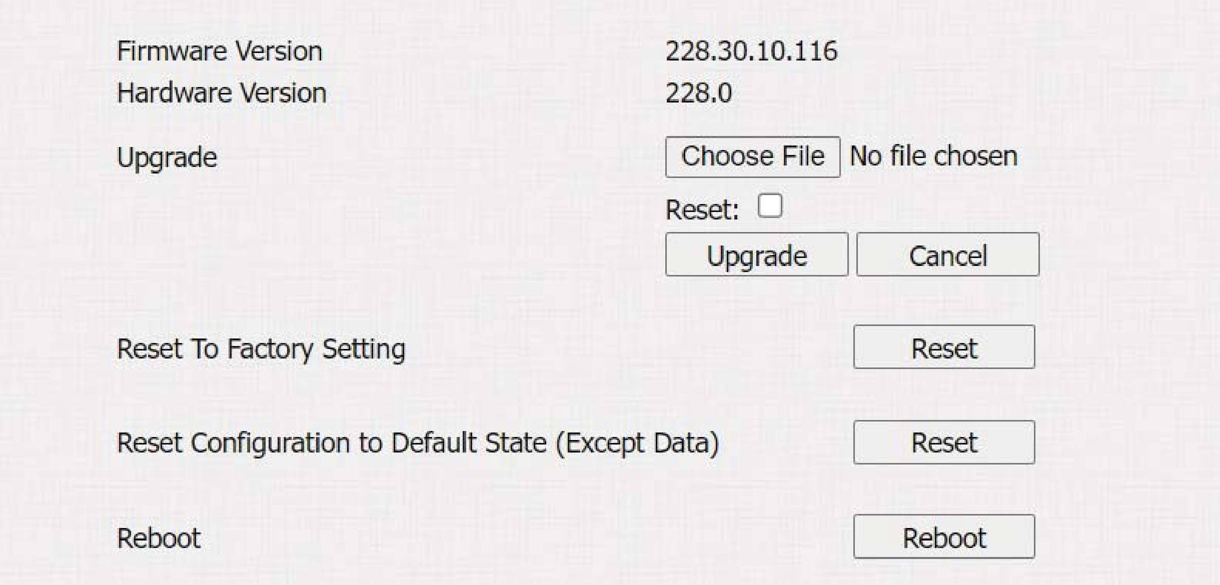
Tip

1. You can also change the service password directly on the device by pressing "*3888#".
2. Press "2" to enter the Admin Access screen.
3. Select Set Service Password to change the service password.

System Reboot&Reset

Reboot

You can reboot the device on the **Upgrade** > **Basic** interface.



Firmware Version 228.30.10.116

Hardware Version 228.0

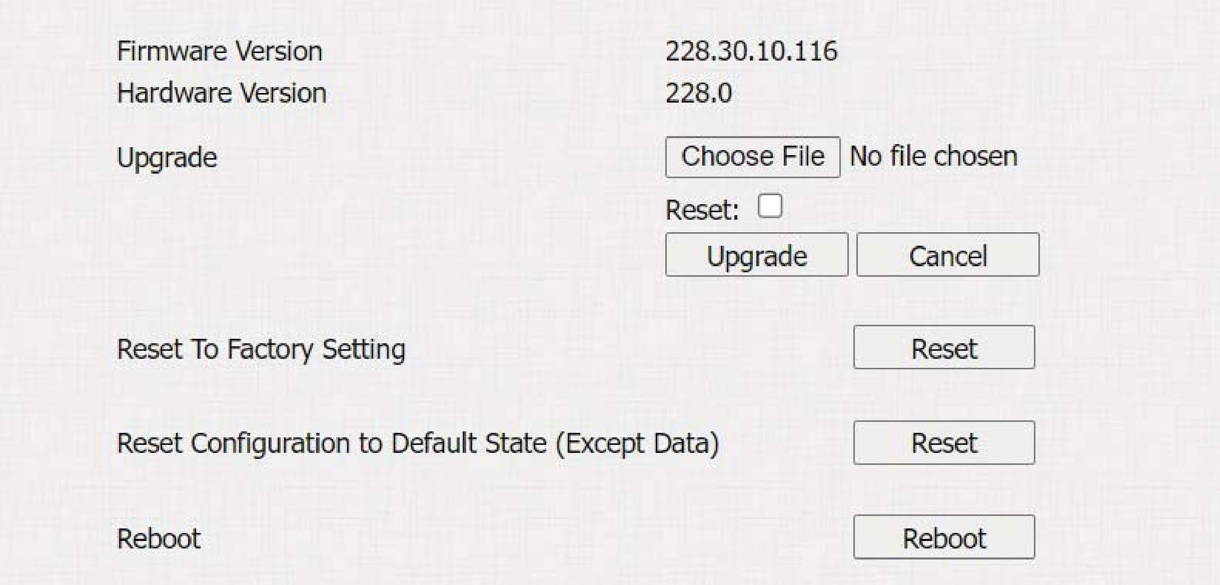
Upgrade Choose File No file chosen

Reset: □

Reset

Reset the device on the **Upgrade** > **Basic** interface.

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



Firmware Version 228.30.10.116

Hardware Version 228.0

Upgrade Choose File No file chosen

Reset: □

Tip

1. You can also reset the device directly by pressing “*2396#” on the keypad.
2. Press “3” to access the System Settings.
3. Select Restore Default to reset the device.

FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.