About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX R25A DOOR PHONE

Administrator Guide

Thank you for choosing the Akuvox R25A door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to 25.30.10.103 and provides all the configurations for the functions and features of the Akuvox door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox R25A door phone can be connected to indoor monitors for remote access control and communication. They allow audio calls with visitors, as well as opening the door. Featuring good video quality and wide view angle, it fits well in residential and commercial buildings.

Changelog

What's new in version 25.30.10.103:

- Support the video storage function.
- Support pedestrian detection.

Click here to view the device's changelog of previous versions.

Model Specification

Model	R25A
Camera	x1
Main Camera’s Sensor	4M pixels, CMOS
Main Camera’s Image Size	1/3.2"
Main Camera’s Resolution	Up to 2K
View Angle	150°(H), 150°(V)
Technology	WDR
LEDs	IR LEDs
Light Sensor	x1
Infrared Sensor	x1
G-Sensor	x1
IC Card Reader	✔, 13.56MHz & NFC
ID Card Reader	✔, 125KHz
Wiegand	x1
RS485	x1
Relays	x2
Inputs	x2
Power In	x1, 12V/1A
Ethernet	x1, with PoE
Microphone	x1
Speaker	x1

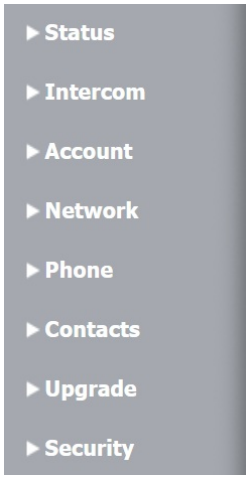
Supported Card Types

The device’s firmware should be 25.30.10.11 or higher:

- ID Card:
  - EM4100
  - EM4200
- IC Card:
  - Mifare Ultralight C/EV1
  - Mifare Classic Compatible Card
  - Mifare Plus-S 2K
  - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
  - NFC Type2 216
  - NFC Type2 215
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Akuvox Cards:
  - Mifare Classic 1K
  - Mifare S50-1K Card

Introduction to the Configuration Menu

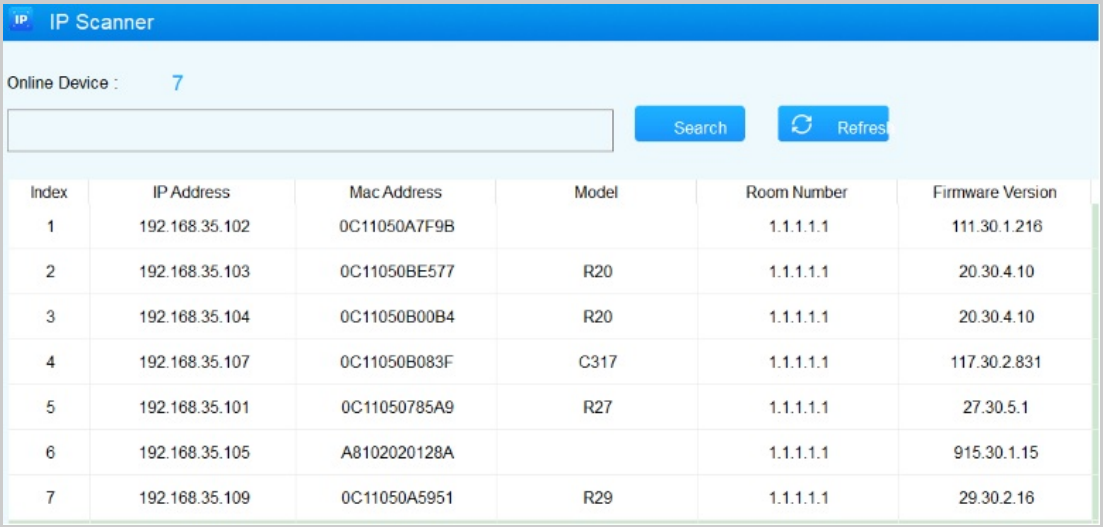
- **Status**: This section gives you basic information such as product information, network information, account information, etc.
- **Intercom**: This section covers intercom settings, relay, monitoring settings, etc.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, etc.
- **Network**: This section mainly deals with DHCP and static IP settings, RTP port settings, device deployment, etc.
- **Phone**: This section includes light settings, time and language, volume, tone settings, etc.
- **Contacts**: This section includes the setup of the access allowlist.
- **Upgrade**: This section covers firmware upgrade, device reset and reboot, configuration file auto-provisioning, and fault diagnosis.
- **Security**: This section is for password modification, certificate upload, etc.



Access the Device

Obtain Device IP Address

Check the device IP address by holding the push button for 5s. Or search the device IP by the IP scanner, an Akuvox software in the same network.

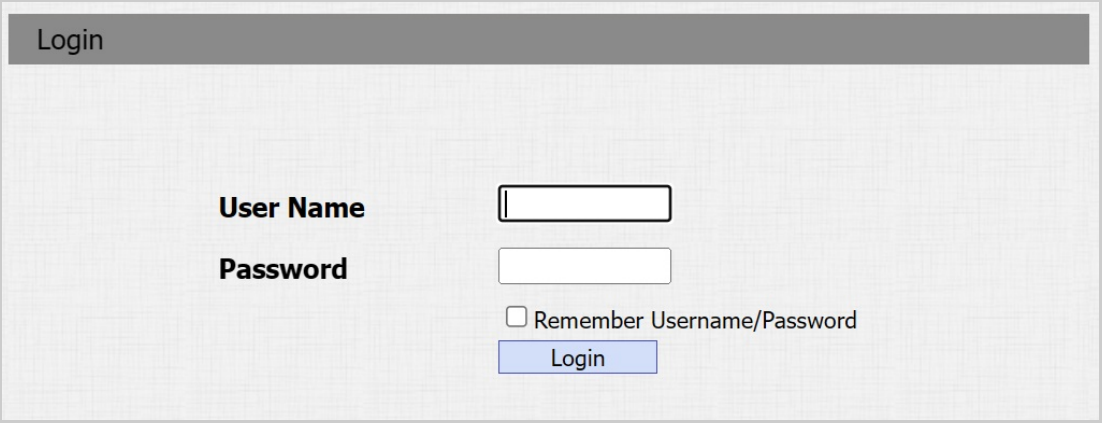


Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101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

Access the Device Setting

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 username and password entered.



Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See 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

Select the device's web language on the **Phone > Time/Lang** interface.

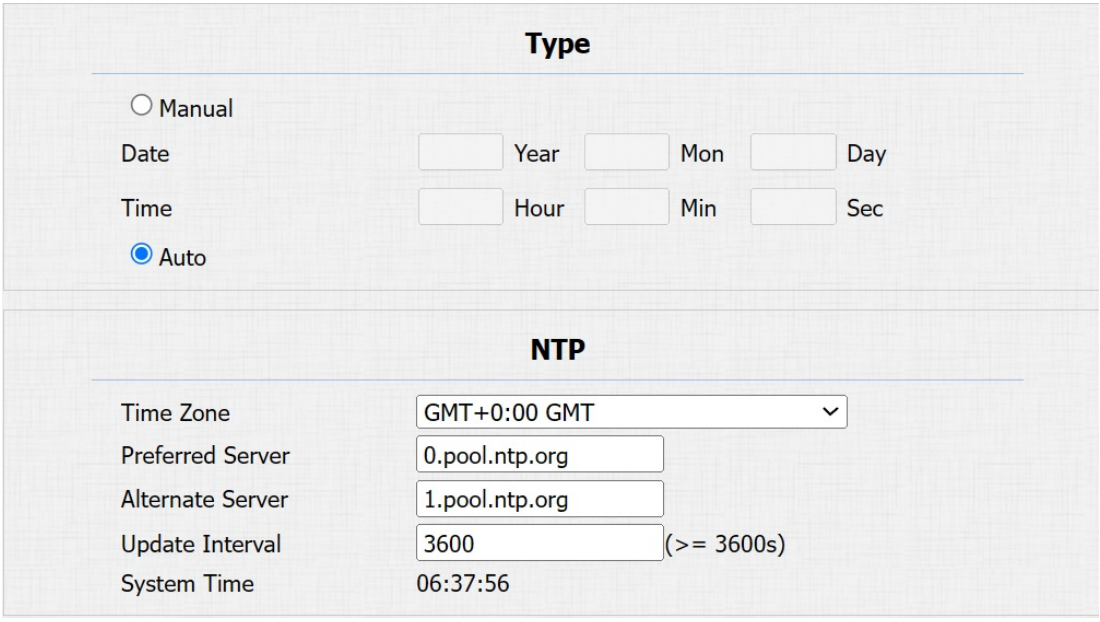
The following languages are supported:

- English, Russian, Spanish, Dutch, French, German, Polish, Japanese, and Hebrew.

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.

Set up time on the **Phone > Time/Lang** interface.



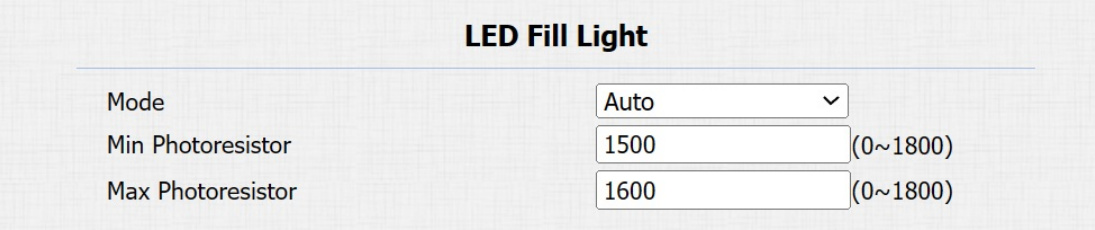
- **Type**:
  - **Manual**: Disable the NTP server, and enter the time and date manually.
  - **Auto**: Enable the NTP server and set up the relevant parameters in the NTP section.
- **Time Zone**: Select the time zone.
- **Preferred/Alternate Server**: The NTP server address. The alternate server will take effect when the primary server is invalid.
- **Update Interval**: The time interval between two consecutive NTP requests.
- **System Time**: Display the current time obtained by the device.

LED Setting

LED Fill Light

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

To set it up, navigate to the **Intercom > LED Setting > LED Fill Light** interface.

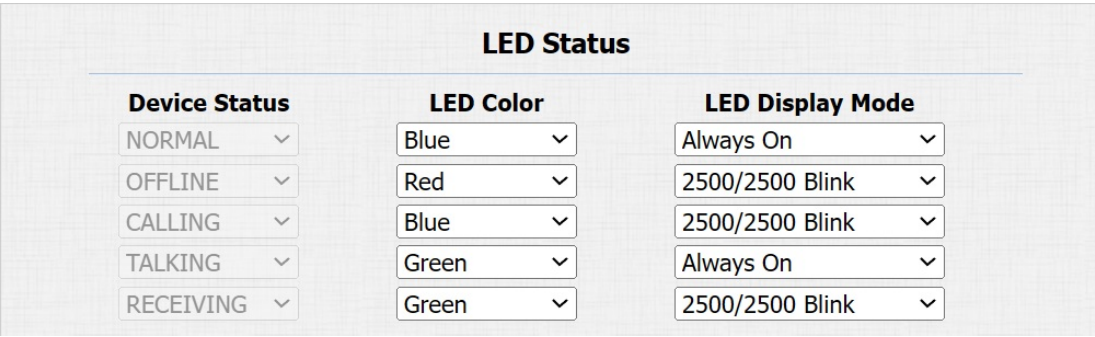


- **Mode**:
  - **Auto**: Turn on the LED light automatically based on the minimum and maximum photoresistor value.
  - **Always On**: Enable the LED light.
  - **Always Off**: Disable the LED light.
  - **Schedule**: Turn on the LED light based on the schedule. Specify the start time and end time when 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 Display Status

LED display adjustment is used to indicate the light changes of the call button in 5 statuses: normal (idle), offline, calling, talking, and receiving a call. The LED status allows users to verify the current mode of the device.

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

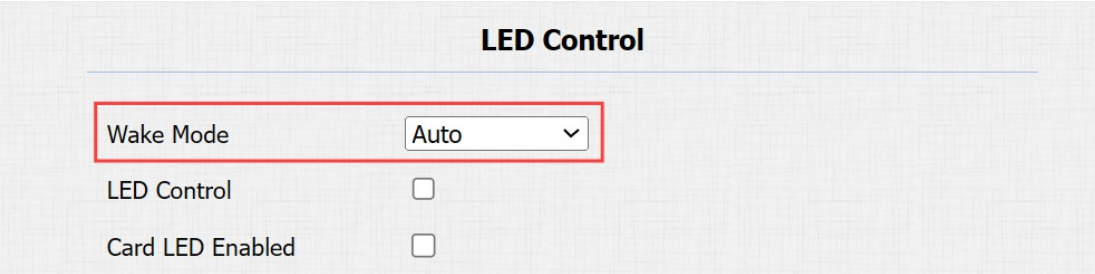


- **Device Status**: There are five statuses: Normal, Offline, Calling, Talking, and Receiving.
- **LED Color**: Three LED colors are available for each option: Blue, Red, and Green.
- **LED Display Mode**: Select the desired LED blinking frequency.

LED Wakeup Mode

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

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

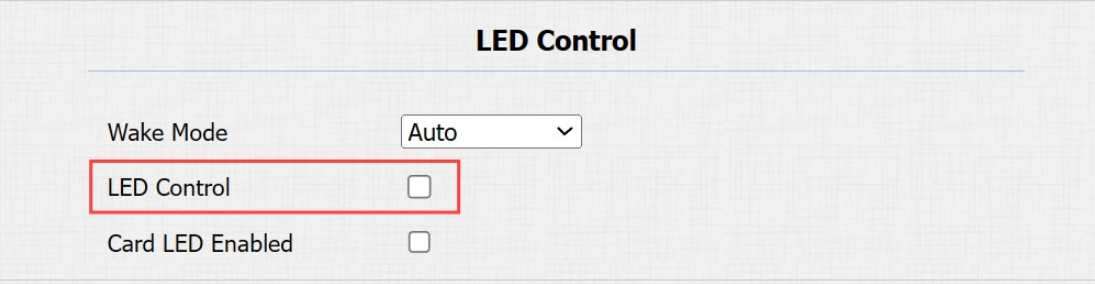


- **Wake Mode**:
  - **Auto**: When the infrared detection is triggered, the card reader light will be on.
  - **Manual**: The card reader light will not be controlled by infrared detection.

Control LED Display by HTTP URL

You can enter an HTTP URL in a browser to manage the LED color and frequency.

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



The HTTP URL format is http://device IP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500.

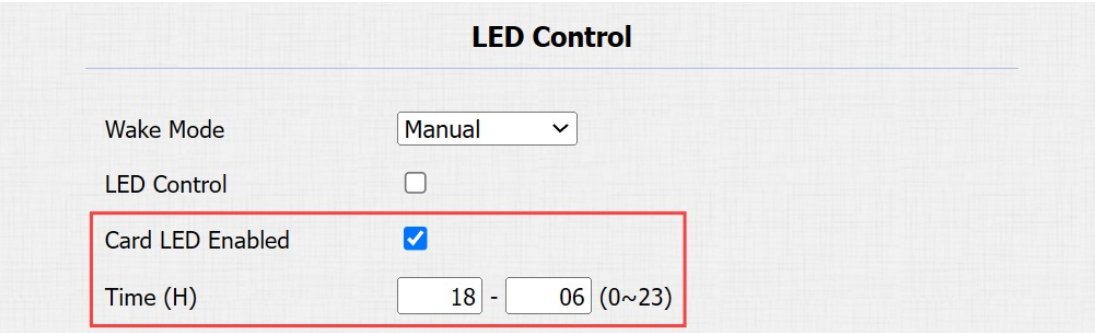
Replace the number in the format to change the LED to the desired status.

- State: 1=Normal ; 2=OffLine ; 3=Calling; 4=Talking; 5=Receiving;
- Color: 0=Red; 1=Green; 2=Blue;
- Mode: 0=Always On; 1=Always Off; 500/1000/1500/2000/2500/3000=Corresponding blinking frequency.

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 the **Intercom > LED Setting > LED Control** interface.

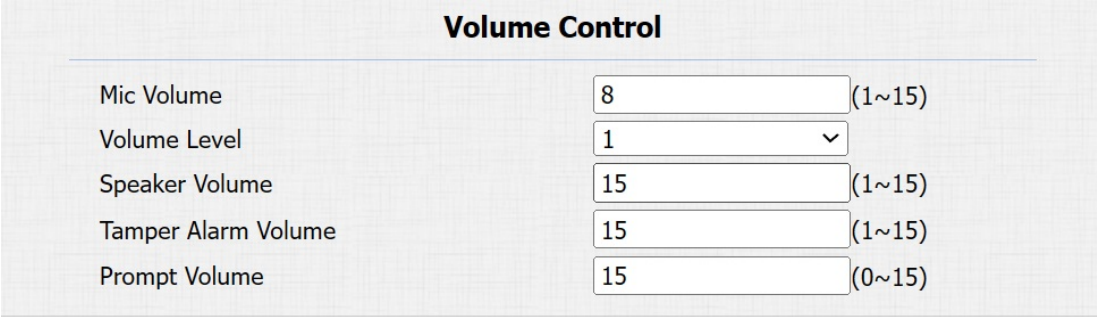


- **Card LED Enabled**: When enabled, specify the period when the light is on.

Volume and Tone

Volume Control

You can control the device volume on the **Phone > Audio** interface.

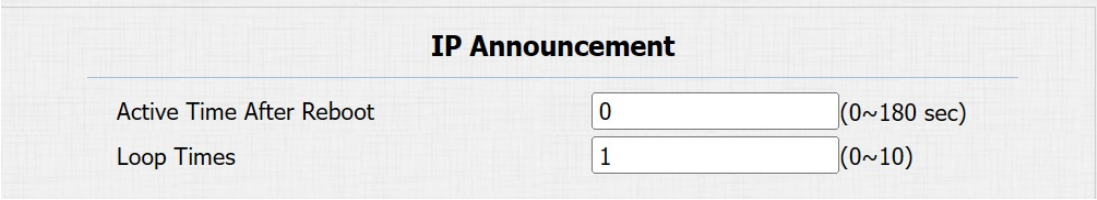


- **Volume Level**: Set the overall volume. Level 1 volume range is roughly 80-95, and 2 is 95-109.
- **Tamper Alarm Volume**: Set the volume when the tamper alarm is triggered.
- **Prompt Volume**: Various prompts including door-opening success and failure prompts.

IP Announcement

You can set when the device announces its IP after each reboot and the loop times.

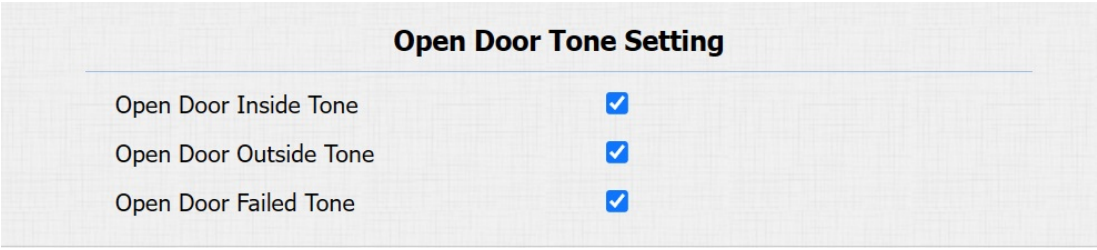
Set it up on the **Phone > Audio** interface.



- **Active Time After Reboot**: Set the time within which holding the push button to announce the IP address is valid. For example, if you set it as 30 seconds, you need to hold the button within 30 seconds after the device reboots. Otherwise, the device will not announce the IP. While 0 means you can hold the button for IP announcement any time after the device reboots.

Door-opening Tones

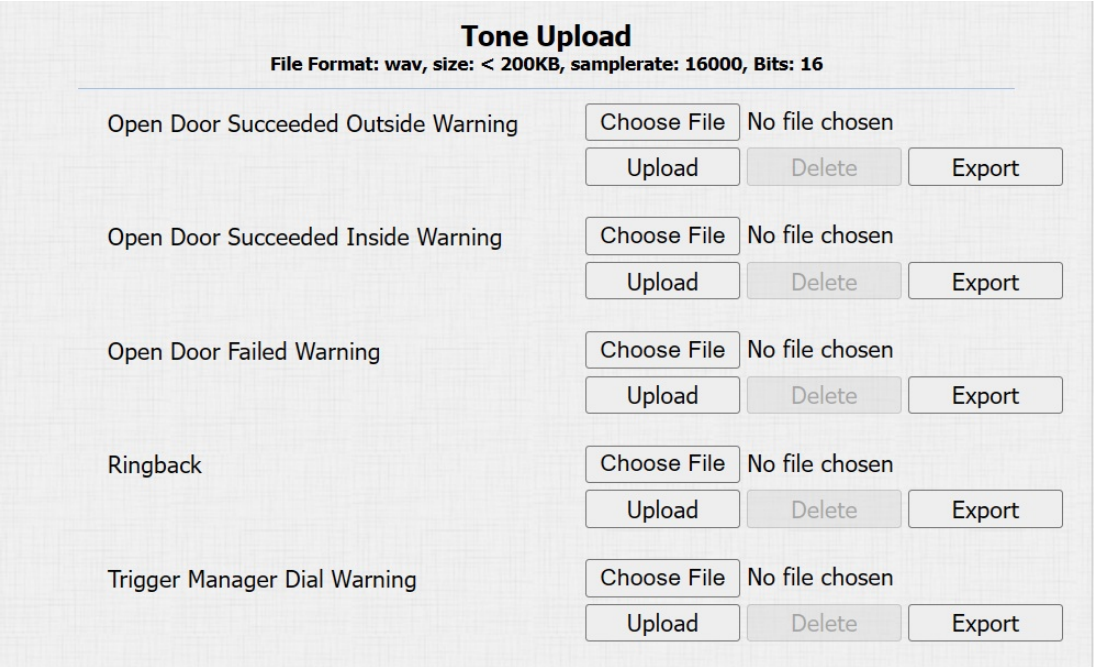
You can enable or disable the door-opening tones on the **Phone > Audio** interface.



- **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.

Upload Tones

You can upload various tones to enrich users' experience on the **Phone > Audio** interface. Click **Choose File** and then **Upload** to import the file.



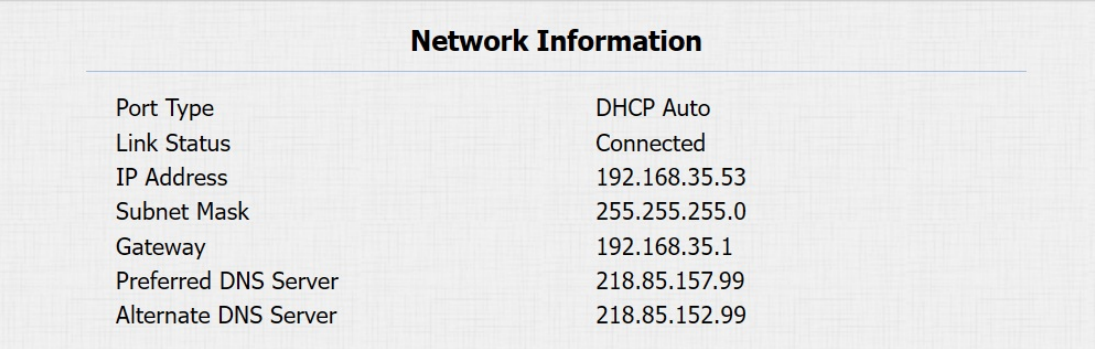
- **Open Door Succeeded Outside Warning**: The relay-triggered tone. The door-opening tone can be heard when users open doors by the device-supported access methods except for the exit button.
- **Open Door Succeeded Inside Warning**: The input-triggered tone. The door-opening tone can be heard when users open doors by pressing an exit button.
- **Open Door Failed Warning**: The tone can be heard when opening doors fails.
- **Ringback**: The ringback will play when someone calls the device.
- **Trigger Manager Dial Warning**: The tone can be heard when the push button is pressed.

> **Note**
> File Format: wav; Size: < 200KB; Sample Rate: 16000; Bits: 16.

Network Setting

Network Status

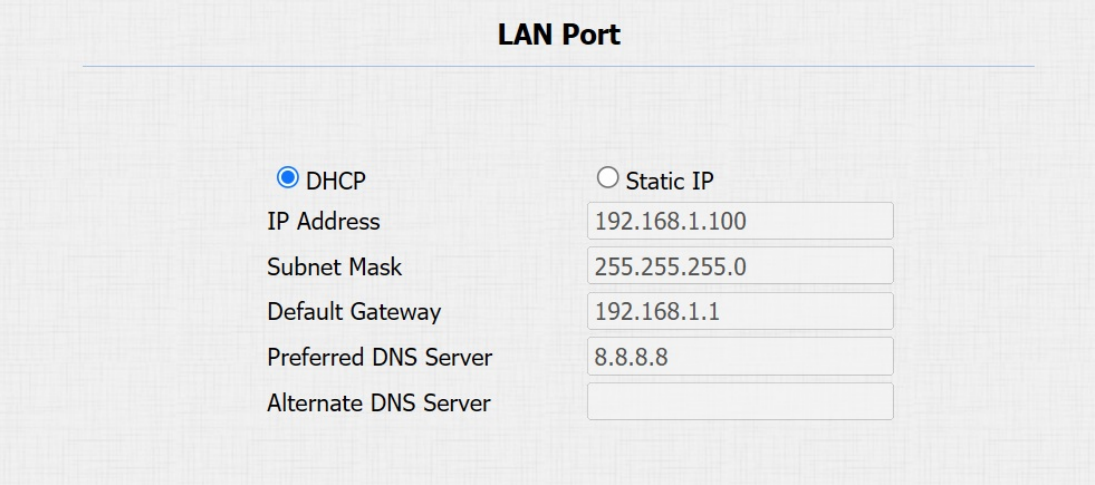
Check the network status on the web **Status > Basic > Network Information** interface.



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.

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

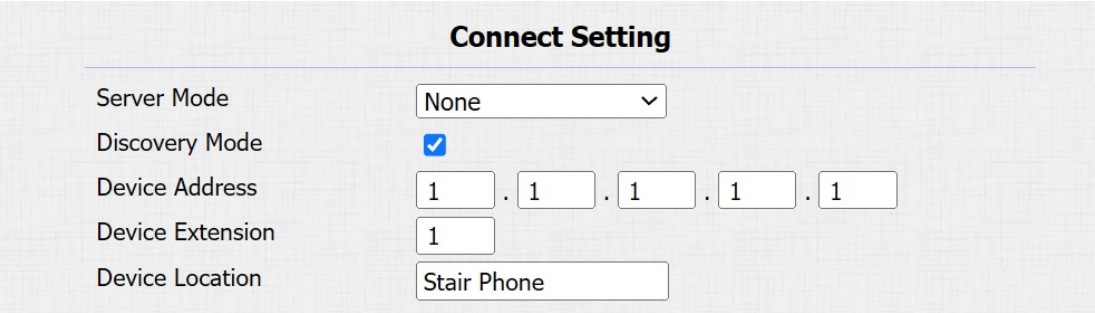


- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, the device will automatically be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address.
- **Static IP**: The IP address, subnet mask, default gateway, and DNS server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

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.



- **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.

- **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

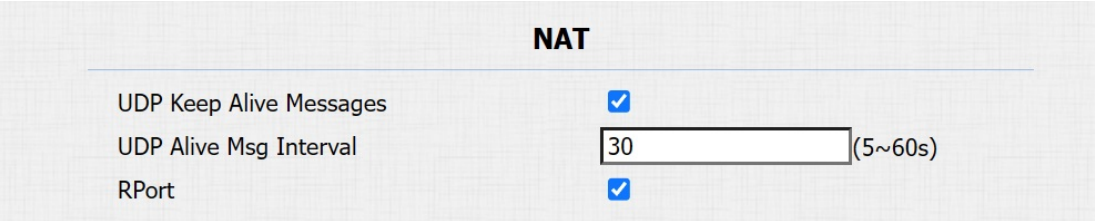
Network Address Translation(NAT) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses and hides the internal IP addresses and ports from the outside world.

To register SIP accounts on third-party servers in a Wide Area Network(WAN), you need to enable the RPort feature on the intercom devices to establish a stable connection.

To set up NAT, navigate to the **Account > Basic > NAT** interface.

- **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.

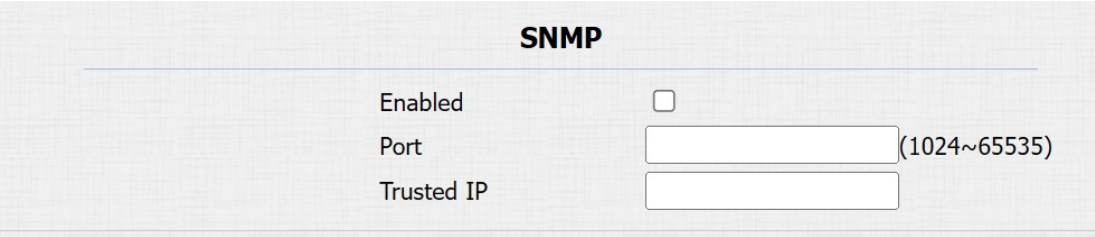


- **UDP Keep Alive Messages**: If enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Msg Interval**: The message-sending time interval ranges from 5 to 60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when the SIP server is in WAN.

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.

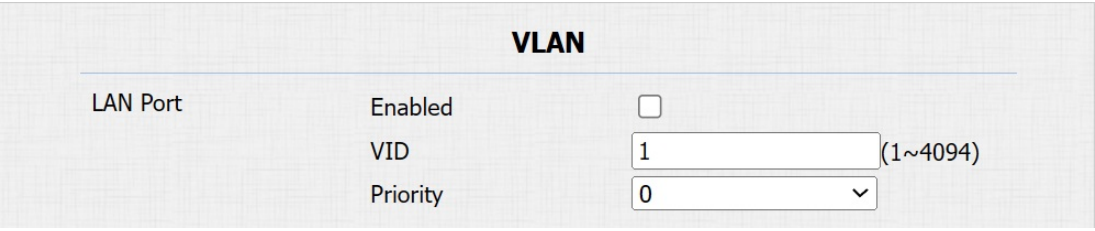


- **Trusted IP**: The allowed SNMP server address. It can be an IP address or any valid URL domain name.

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.

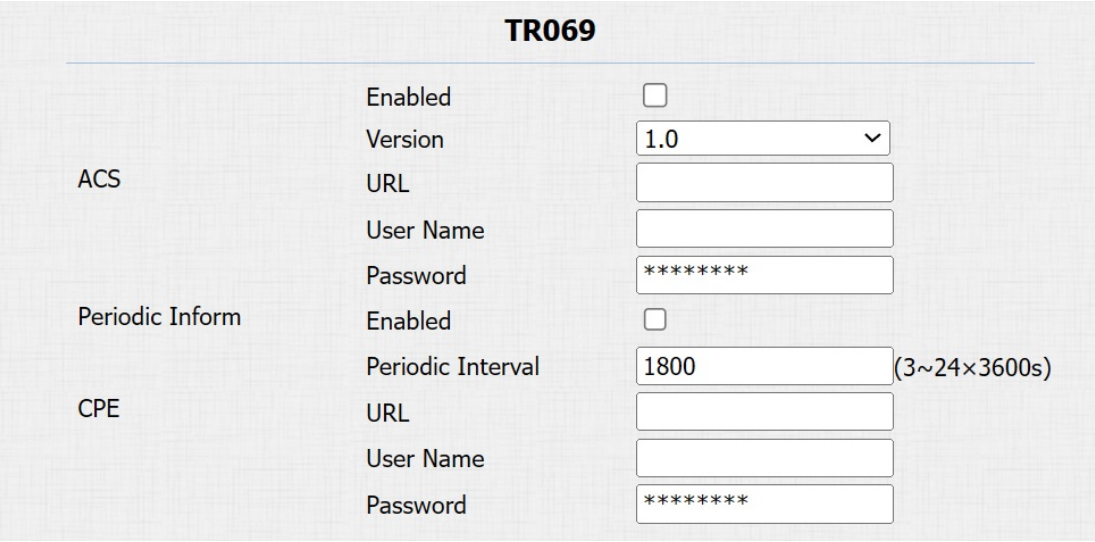


- **VID**: The VLAN ID for the designated port.
- **Priority**: The VLAN priority for the designated port.

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.

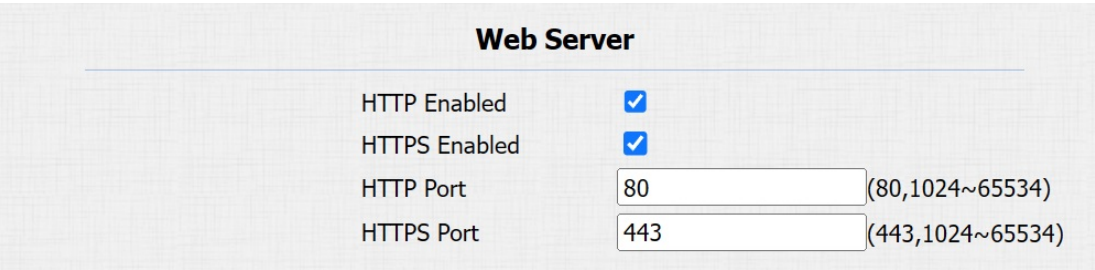


- **Version**: Select the supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE**: ACS is short for auto-configuration servers as server side, and CPE is short for customer-premise equipment as client-side devices.
- **URL**: The URL for ACS or CPE.
- **Periodic Interval**: The interval for periodic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



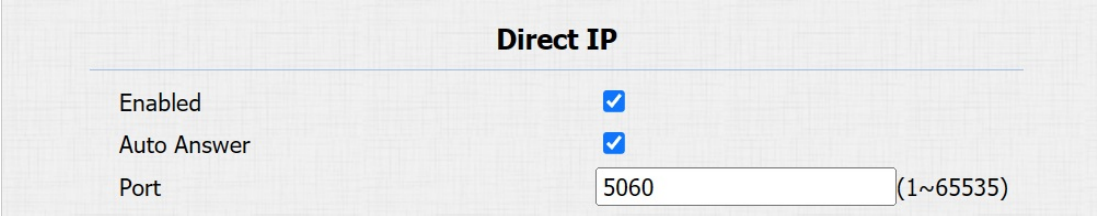
- **HTTP/HTTPS Enabled**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

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.



- **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.

Click here to view the SIP account registration example.

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

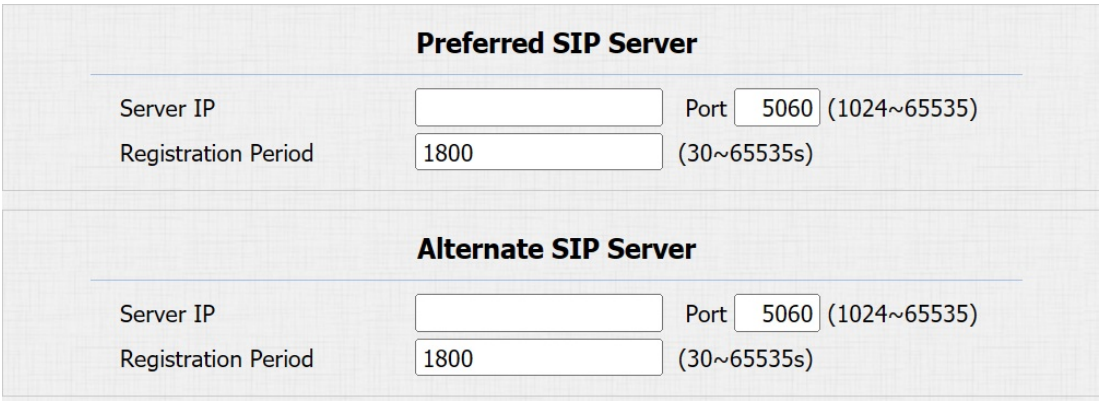
- **Status:** Indicate whether the SIP account is registered or not.
- **Account 1/Account 2:** The door phone supports 2 SIP accounts.
  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.
  - The system switches to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

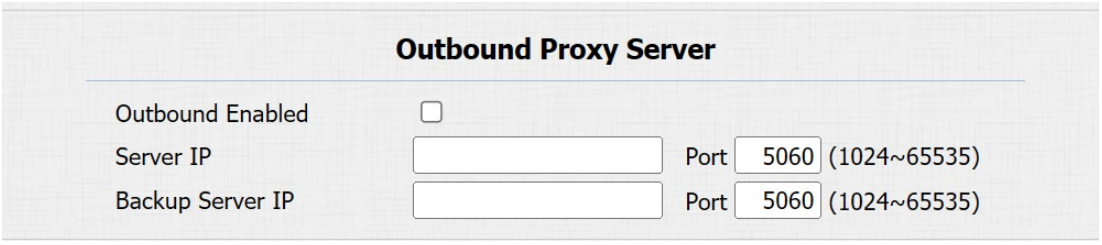


- **Server IP:** Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified period.

Outbound Proxy Server

An outbound proxy server receives and forwards all requests the designated server. It is an optional configuration, but if set it up, all future SIP requests get sent there in the first instance.

To set it up, go to the **Account > Basic > Outbound Proxy Server** interface.

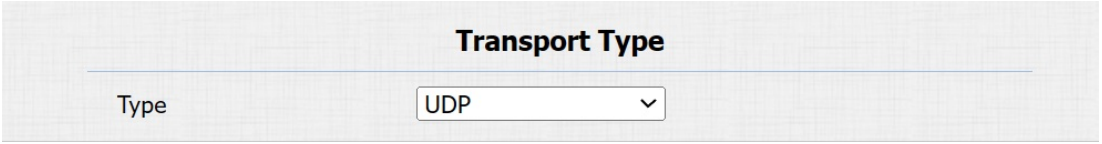


- **Server IP:** Enter the SIP proxy server's IP address.
- **Port:** Set the port for establishing a call session via the outbound proxy server.
- **Backup Server IP:** Enter the SIP proxy IP address to be used when the main proxy server malfunctions.
- **Port:** Set the proxy port for establishing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



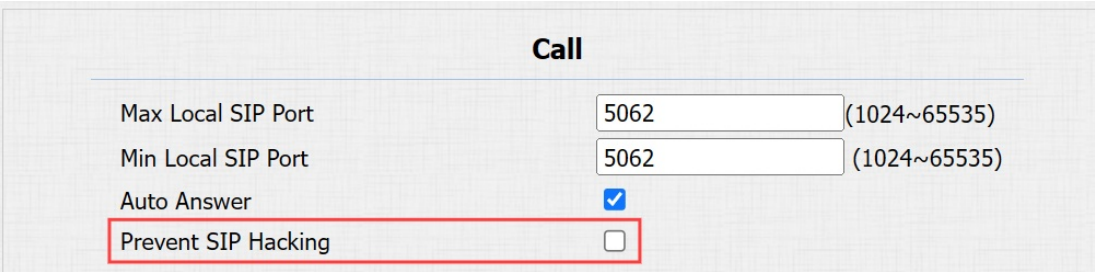
- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.

- **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.



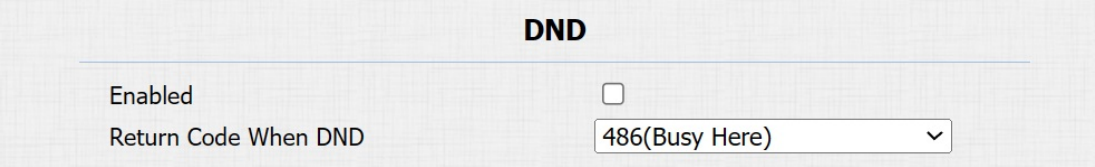
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Settings

Do Not Disturb

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

To set it up, go to the **Phone > Call Feature > DND** interface.

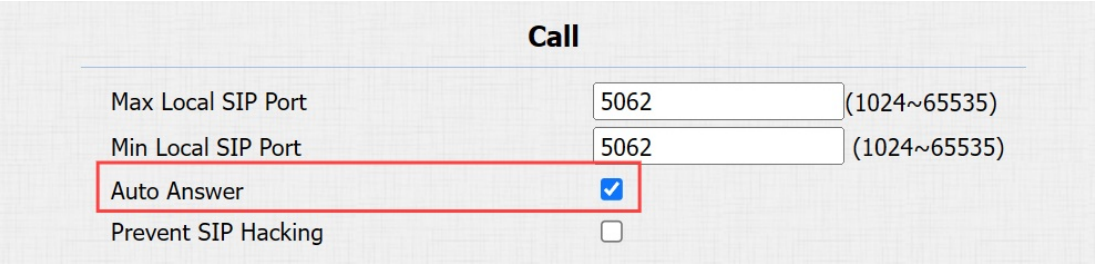


- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

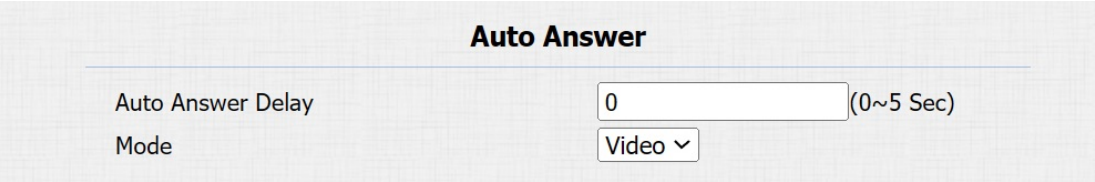
Call Auto-answer

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

To enable the call auto-answer feature, go to the **Account > Advanced > Call** interface.



To set it up, go to the **Intercom > Call Feature > Auto Answer** interface.

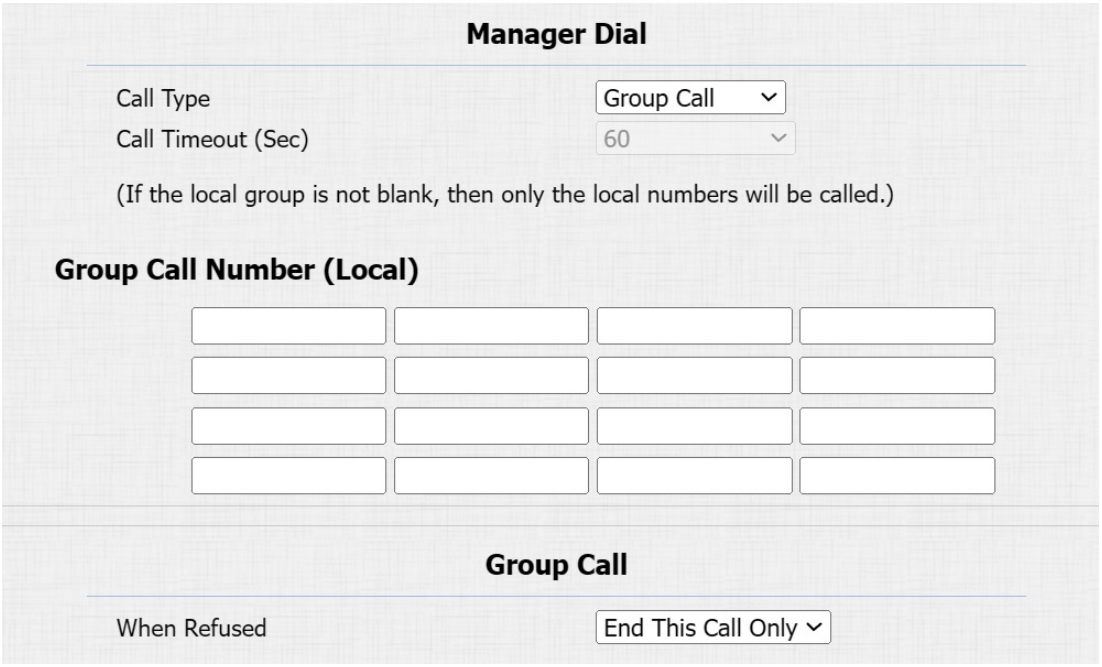


- **Auto Answer Delay**: Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode**: Determine whether to auto-answer the call as a video or audio call.

Group Call

This feature allows users to call a group of contacts by a single press. The device supports local and SmartPlus-featured group calls. To learn about the detailed configuration, please click here.

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

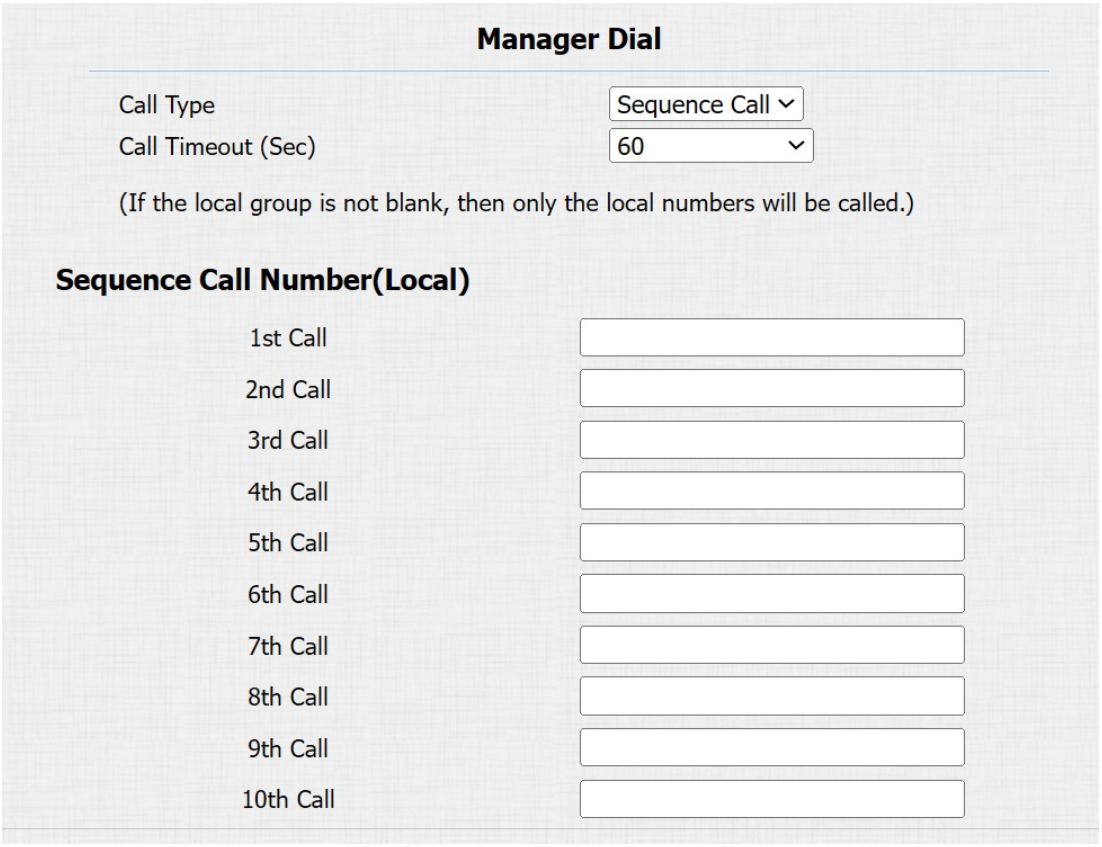


- **Call Type**: Select Group Call.
- **Group Call Number(Local)**: Enter the target numbers.
- **When Refused**:
  - **End All Calls:** The device will stop calling.
  - **End This Call Only**: The device will continue to call other numbers.

Sequence Call

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. You can set up local sequence call numbers, or connect the device to the Akuvox SmartPlus which provides a set of sequence call numbers for the application. Please click here for the detailed configuration.

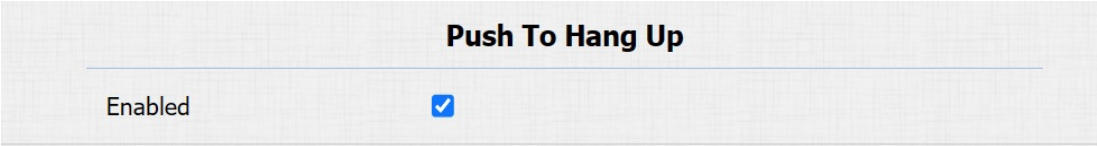
To set it up, go to the **Intercom > Basic** interface.



- **Call Type**: Select Sequence Call.
- **Call Timeout(Sec)**: Determine the duration before calling the next number when the previous call is not answered.
- **Sequence Call Number(Local)**: Enter the target numbers.

Call Hang up by Pressing the Push Button

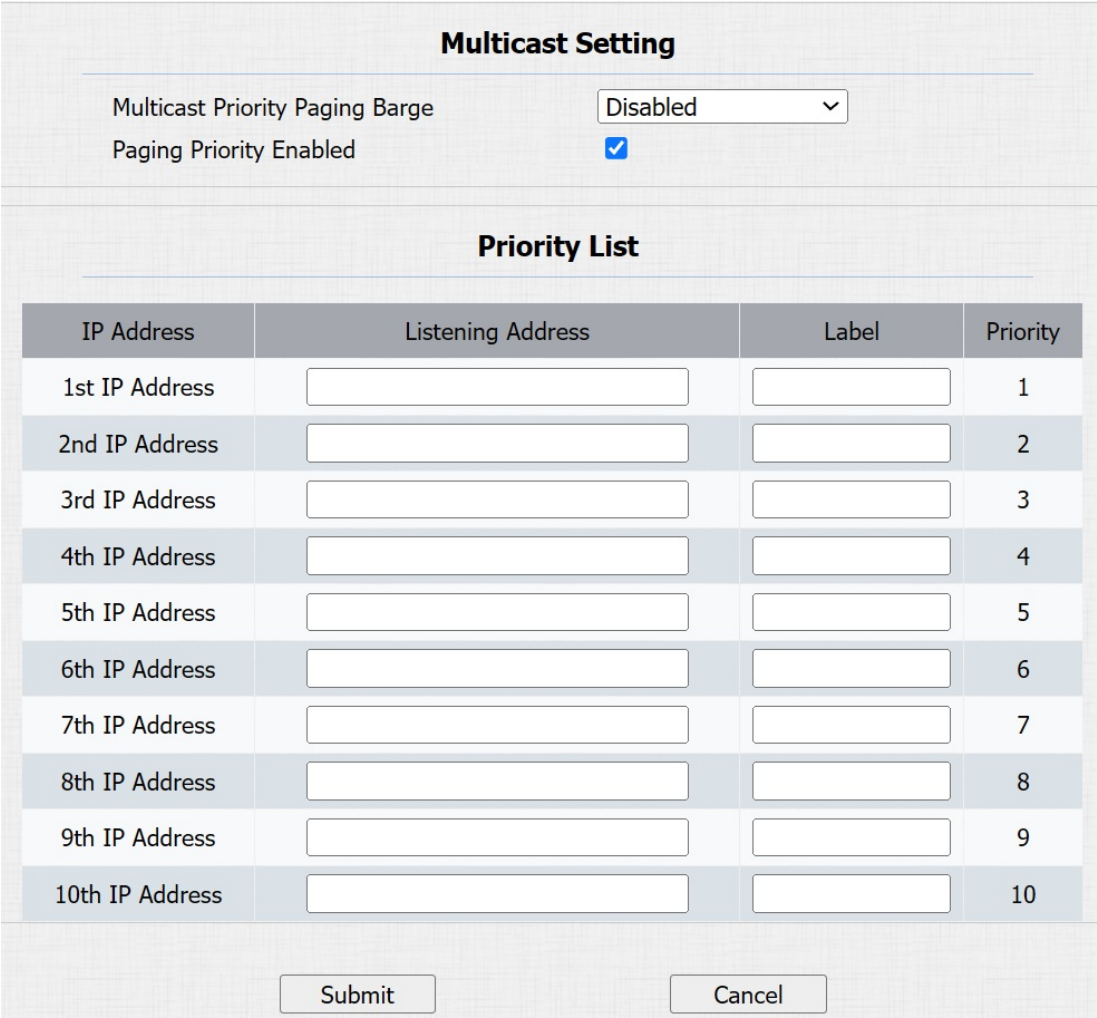
You can enable or disable pressing the push button to hang up a call on the **Intercom > Basic > Push to Hang Up** interface.



Multicast

The Multicast function allows one-to-many broadcasting for different purposes. For example, it enables the indoor monitor to announce messages from the kitchen to other rooms or to broadcast notifications from the management office to multiple locations. The door phone can only receive the multicast.

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



- **Multicast Priority Paging Barge:** Determine how many multicast groups have higher priority than SIP calls. If disabled, SIP calls will have higher priority.
- **Paging Priority Enabled:** Decide whether to make multicast in order of priority.
- **Listening Address:** Enter the IP address. The listen address should be the same as the multicast address. The listening port and the multicast port cannot be the same for each IP address. Multicast IP address is from 224.0.0.0 to 239.255.255.255.

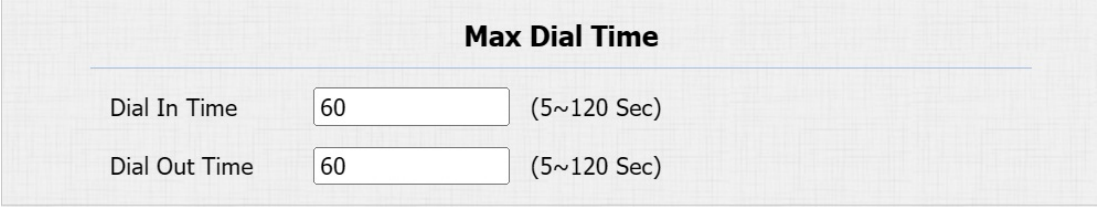
> **Note**
> Please contact Akuvox tech team for a valid multicast address.

- **Label**: Name the multicast group.

Maximum Dial Duration

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

To set it up, go to the **Intercom > Basic > Max Dial Time** interface.



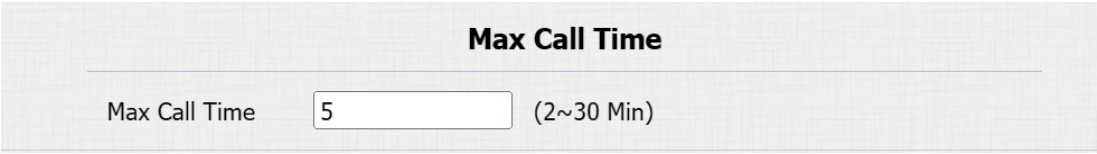
- **Dial In Time:** Specify the maximum duration of an incoming call. The door phone will automatically end the incoming call if it is not answered within the preset time.
- **Dial Out Time:** Specify the maximum duration of an outgoing call. The door phone will automatically end the call it dialed out if there is no answer from the recipient within the preset time.

> **Note**
> The max dial time is affected by the SIP server's max dial time when users make SIP calls. The max call time should not exceed the dial duration of SIP server.

Maximum Call Duration

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

To set it up, go to the **Intercom > Basic > Max Call Time** interface.

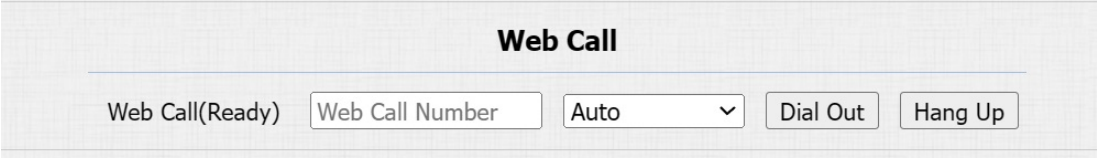


> **Note**
> The max call time is affected by the SIP server's max call time when users make SIP calls. The max call time should not exceed the call duration of SIP server.

Web Call

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

Make a web call on **Intercom > Basic > Web Call** interface.

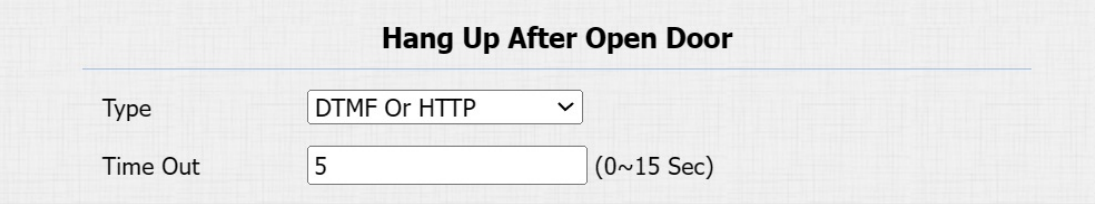


- **Web Call (Ready):** Enter the target IP/SIP number and select the account to dial out.

Hang up After Open Door

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

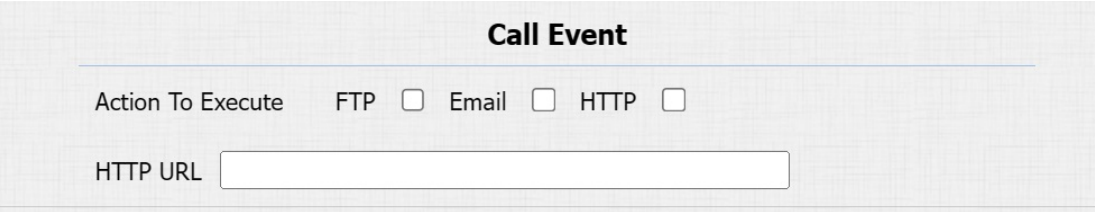
To set it up, go to the **Intercom > Basic > Hang Up After Open Door** interface.



- **Type:** Specify the door-opening method. If this specific method is used to release the door during a call, the door phone will end the call when the preset hang-up time is reached.
- **Time Out:** Specify the hang-up time limit. The door phone will automatically terminate the call when the specific time is reached after the door is opened.

Actions Triggered by Calling

You can set up actions triggered when the device is making a call on the **Intercom > Basic > Call Event** interface.



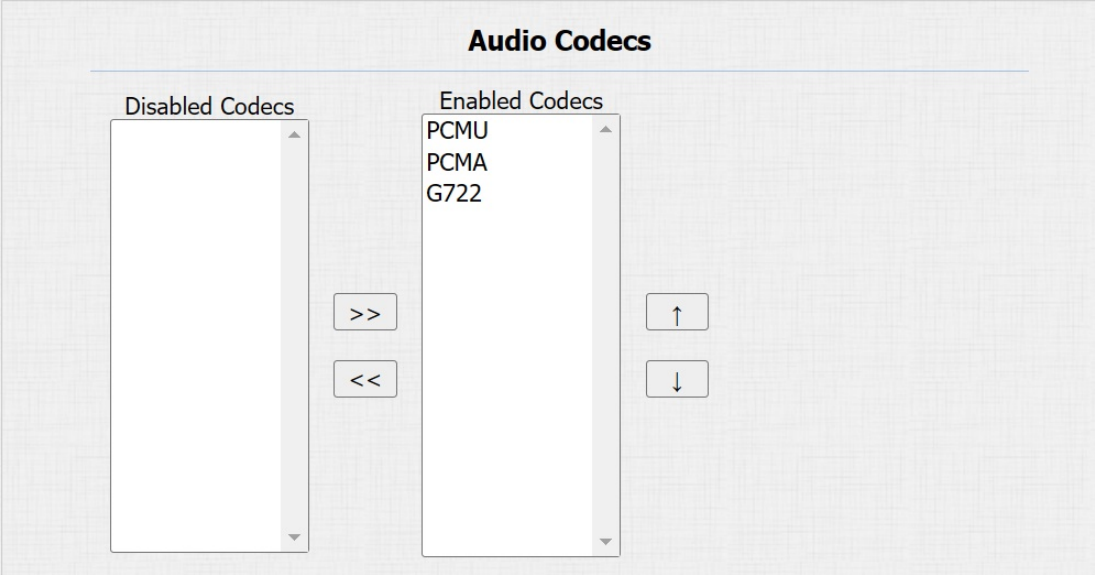
- **Action To Execute**:
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server 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.

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 codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

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



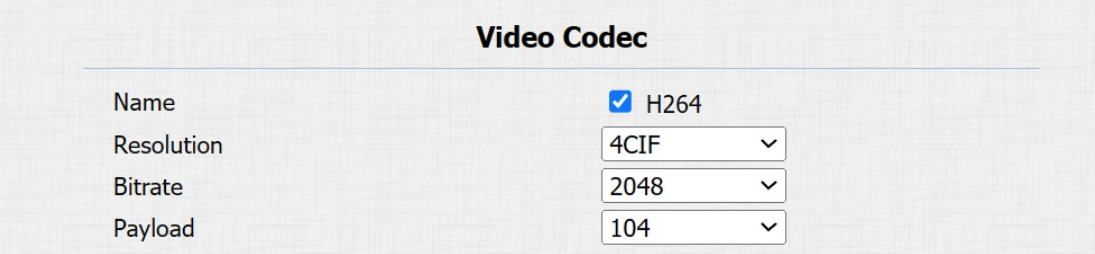
Please refer to the bandwidth consumption and sample rate for the three codec types below:

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 > Video Codec** interface.

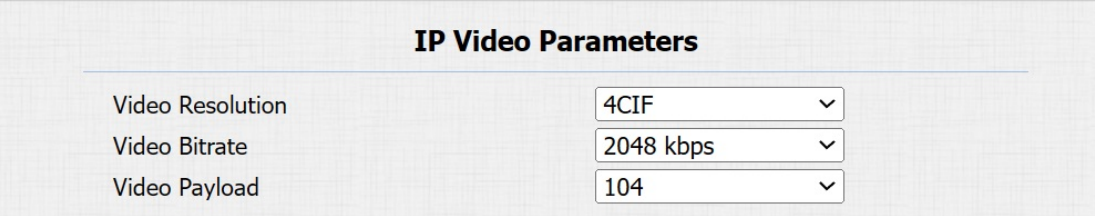


- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default code resolution is 4CIF.
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data 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 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** interface.



- **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.

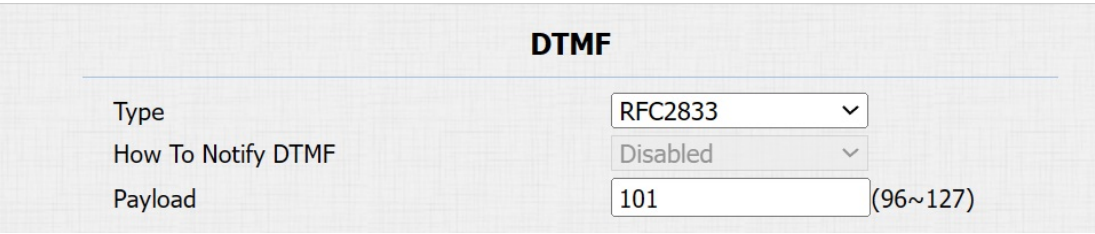
DTMF Data Transmission

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 device and other intercom devices.

DTMF Type Differences:

Inband	DTMF signals are transmitted within the same audio channel as voice data. Simple implementation but signal distortion may occur with highly compressed codecs (e.g., G.729).
RFC2833	Transmits DTMF as special event packets over RTP (Real-Time Transport Protocol), known as out-of-band transmission. Reliable and unaffected by codecs.
Info	Sends DTMF signals via SIP (Session Initiation Protocol) signaling channel. Separate from voice transmission, ensuring audio quality.
Info+Inband	Combines Info and Inband methods.
Info+RFC2833	Combines both Info and RFC2833 methods.
Info+Inband+RFC2833	All three methods are used simultaneously.

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



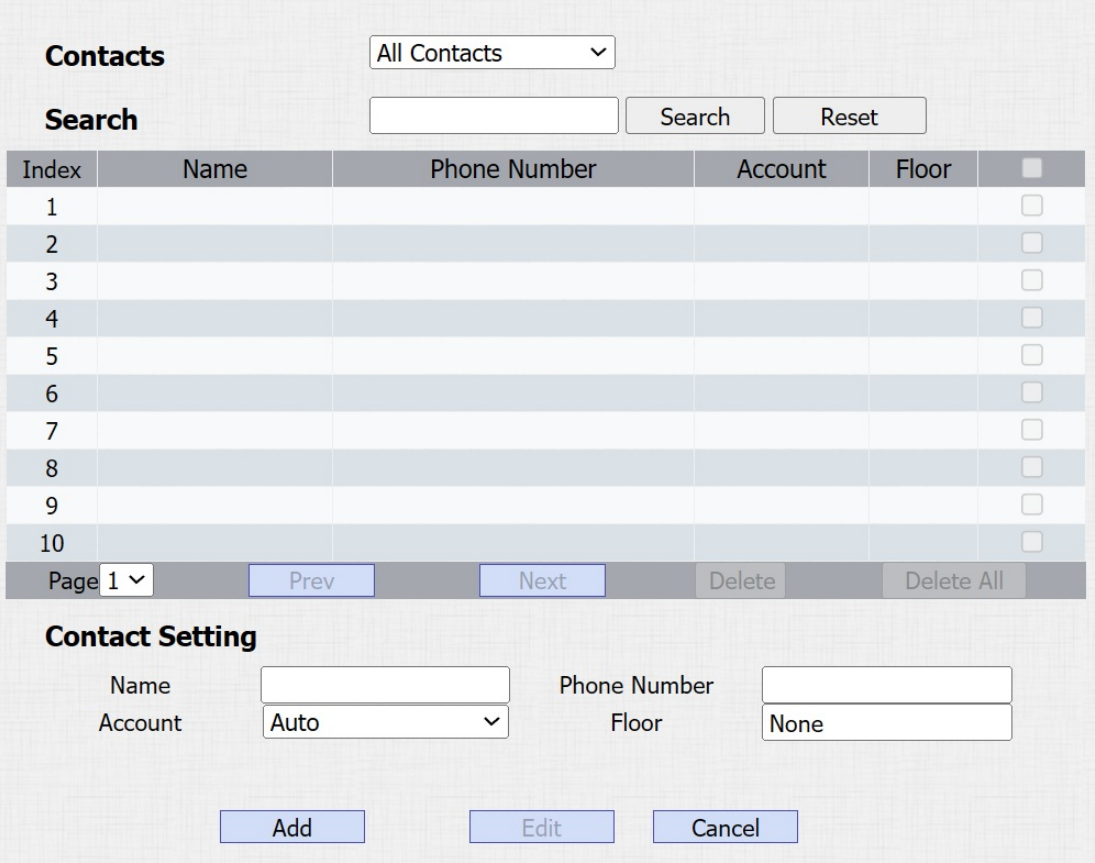
- **Type:** Select from the following options: **Inband, RFC2833, Info, Info+Inband,** or **Info+RFC2833** based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, 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.

Access Allowlist Configuration

The door phone can store up to 1000 contacts, giving access permission to indoor monitors or other devices.

You can search, create, edit, and delete the contacts in the allowlist.

Set it up on the **Contacts > Access Allowlist** interface.



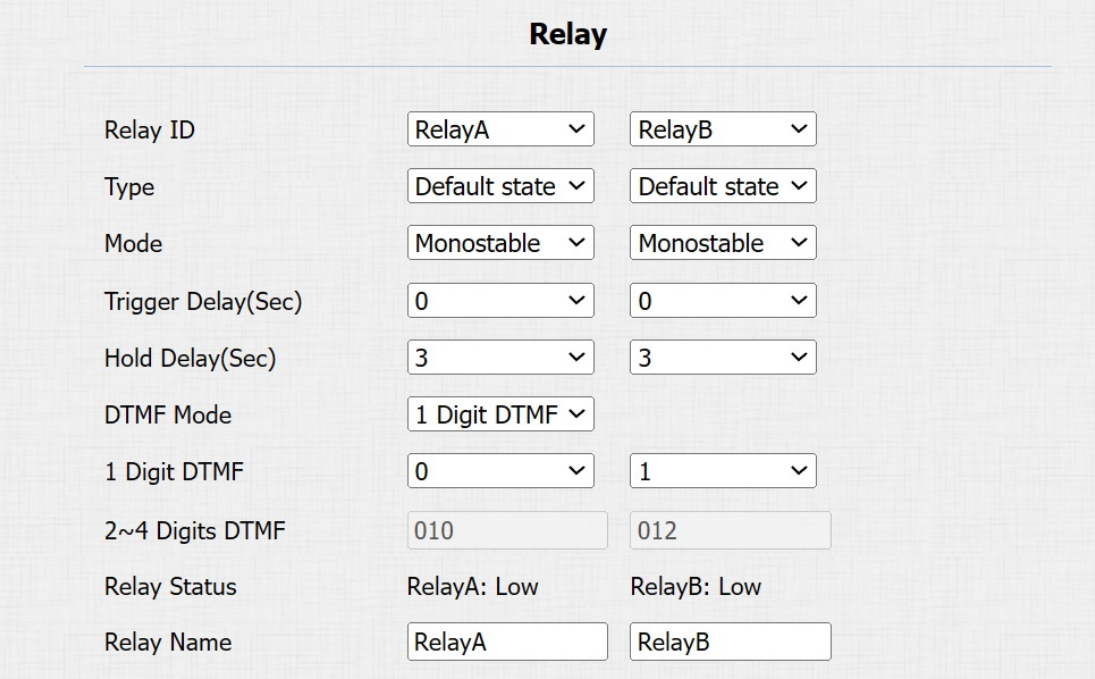
- **Name:** Name the contact.
- **Phone Number:** The phone number of the contact. It supports IP addresses and SIP numbers.
- **Account:** Select the account to receive the call from the contact.
- **Floor:** Specify the accessible floor(s) to the contact via the elevator.

Relay Setting

Relay Switch Setting

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.

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



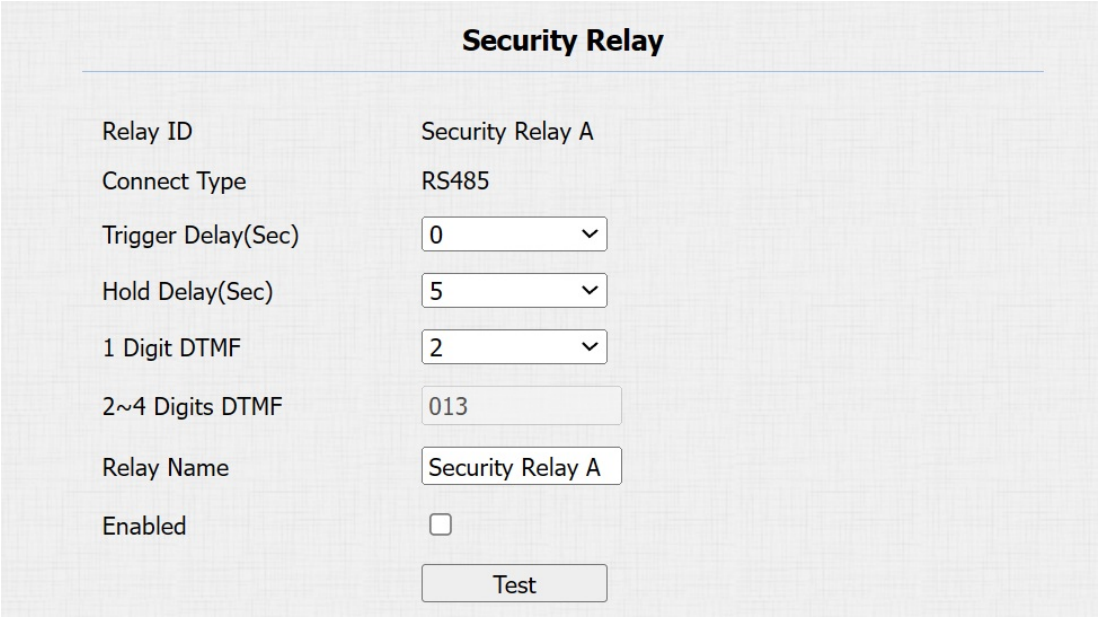
- **Type**: Determine the interpretation of the Relay Status regarding the state of the door:
  - **Default State**: A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.
  - **Invert State**: A “Low” status in the Relay Status field indicates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

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.

Click here to view how to set up the security relay.

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



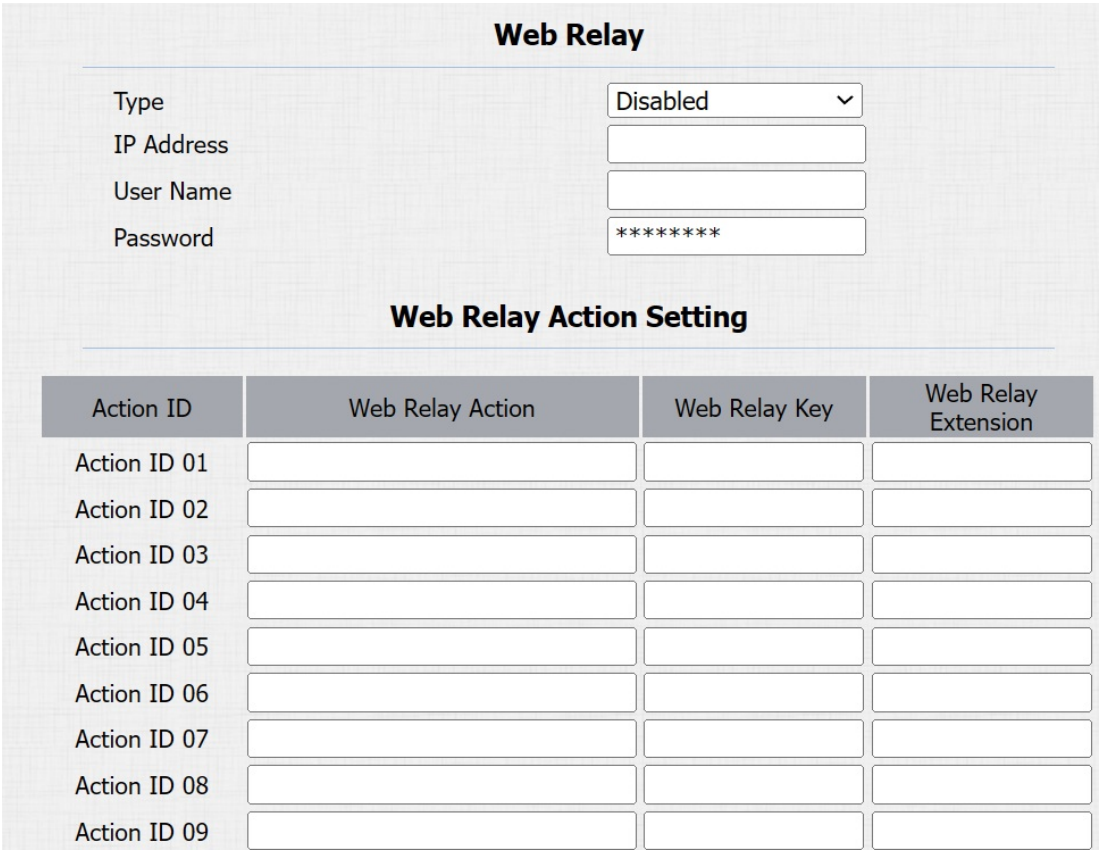
- **Connect Type**: The connection type is RS485 by default.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For 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.
- **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.

Click here to view how to set up web relay.

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



- **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.

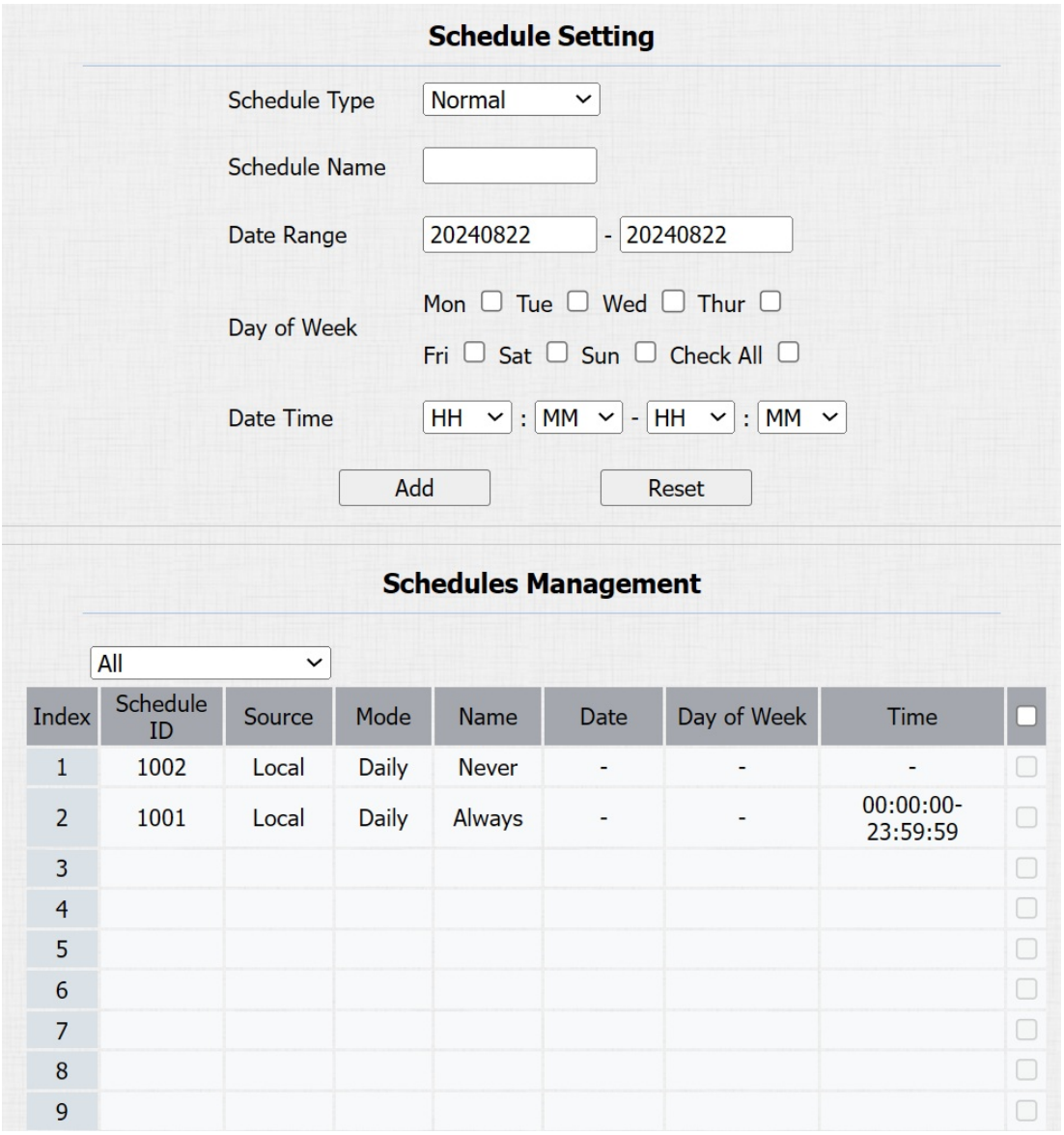
Door Access Schedule Management

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

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

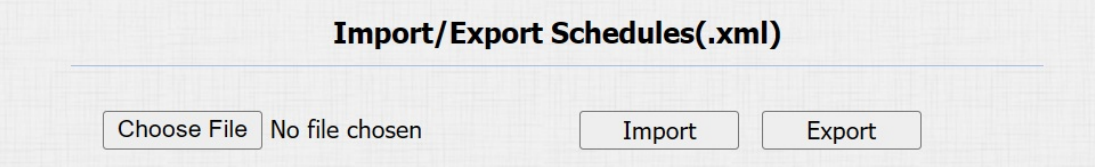


- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Name**: Name the schedule.

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.

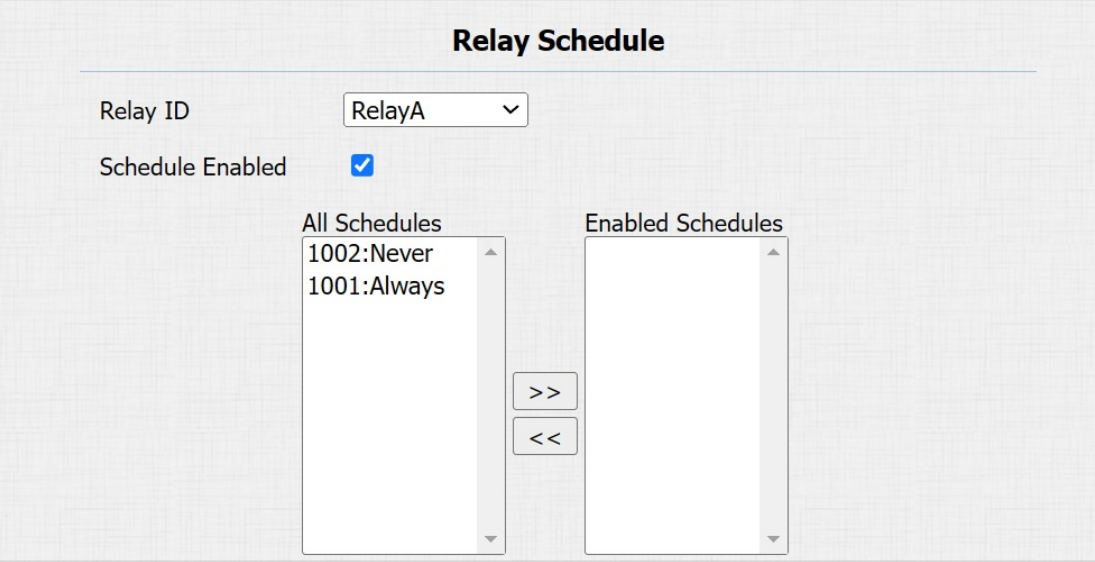
To set it up, go to the **Intercom > Schedule** interface. The export file is in **TGZ** format. The import file should be in **XML** format.



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 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.

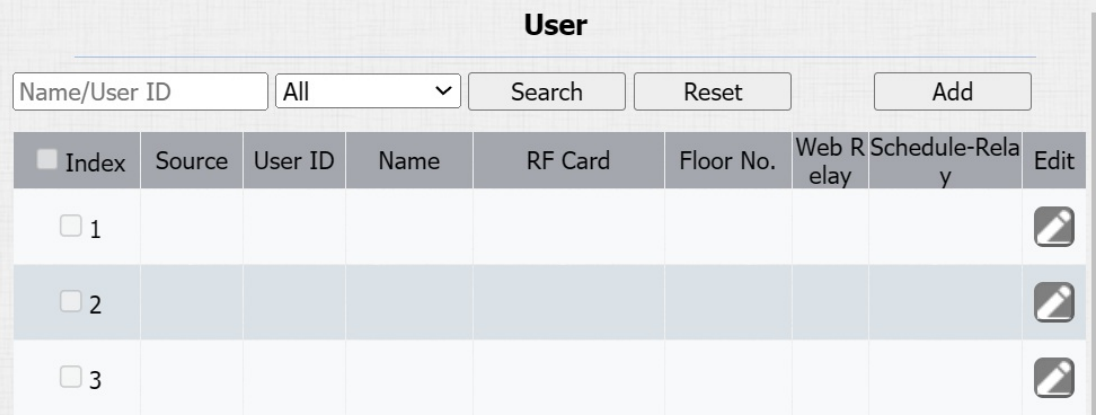
Door Opening Configuration

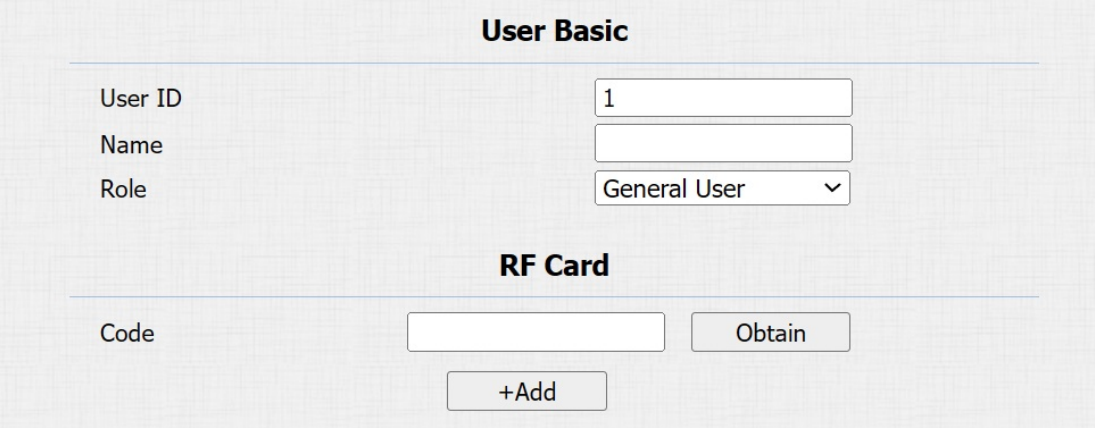
Unlock by RF Cards

The 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**.



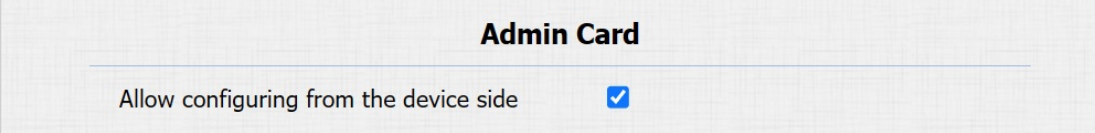


- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.
- **Role**: Define the user as a General User or an Administrator. The Admin card can be used to add a user card. Please refer to Configure Admin Cards and User Cards for detailed configuration.
- **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 125 KHz and 13.56 MHz frequencies are compatible with the door phone for access.

You can enable or disable the use of Admin Card on the **Intercom > Card Setting > Admin Card** interface.

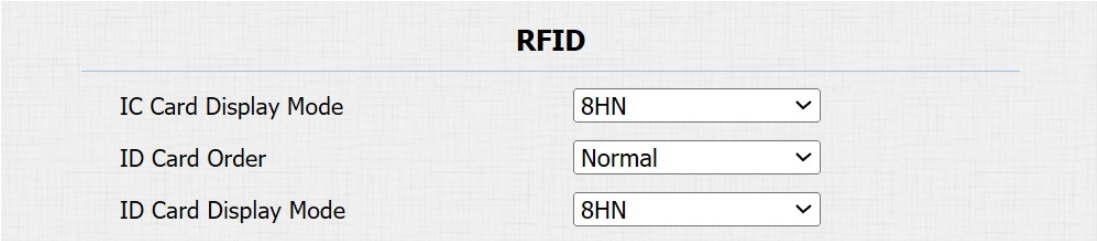


You can enable or disable the IC/ID card function on the **Intercom > Card Setting > Card Type Support** interface.

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.

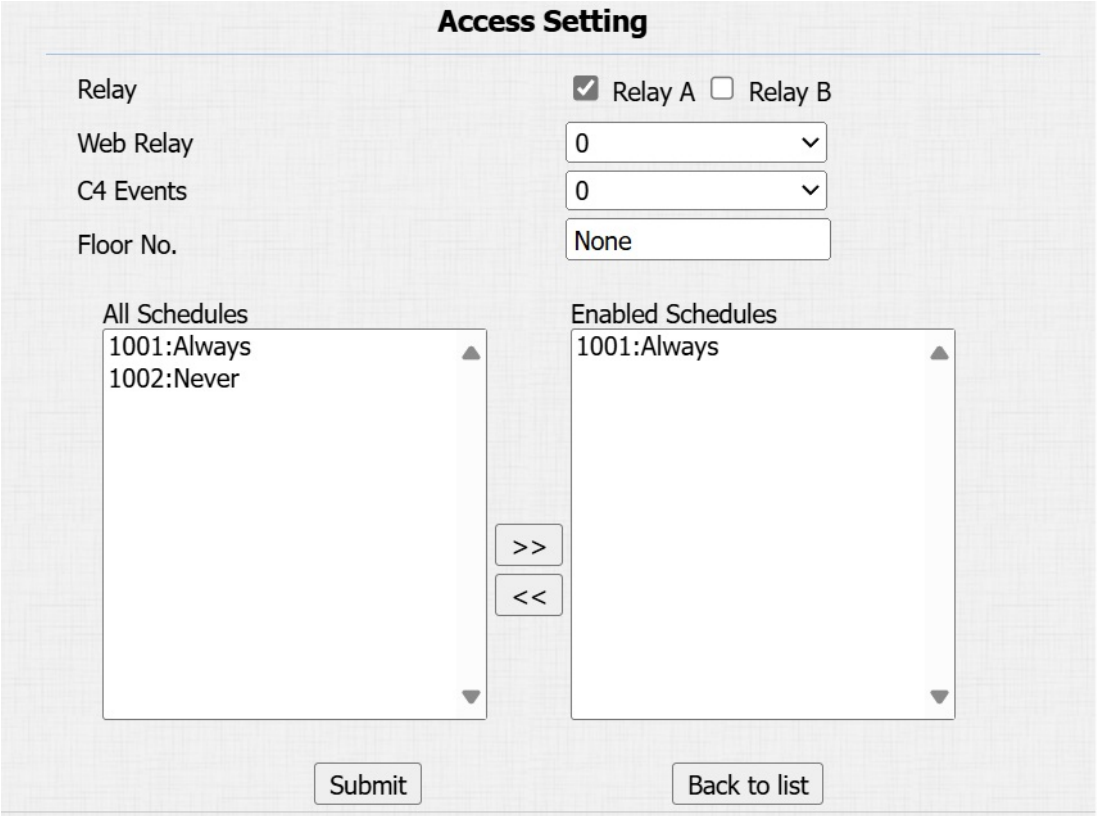
To set it up, go to the **Intercom > Card Setting > RFID** interface.



- **IC/ID Card Display Mode**: Set the card number format from the provided options. The default format in the device is 8HN.
- **ID Card Order**: Select **Normal** or **Reversed** ID card number reading order.

Access Settings

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



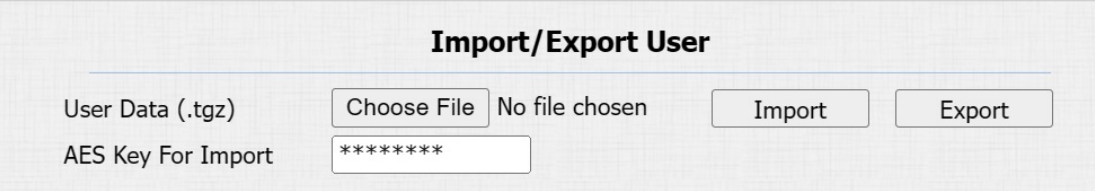
- **Relay**: The relay to be unlocked using the door-opening methods should be assigned to the user.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.

- **C4 Events**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **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

After adding users, you can export the user data and import it to another intercom device for quick management.

On the **Intercom > User** interface, scroll to the **Import/Export User** section. If the file is encrypted, enter the password in **AES Key For Import** box.

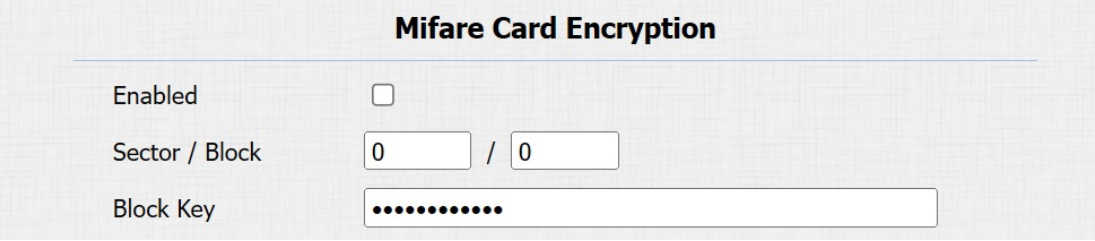


Mifare Card Encryption

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

Click here to view the details of encrypting and reading Mifare cards.

Set it up on the **Intercom > Card Setting > Mifare Card Encryption** interface.

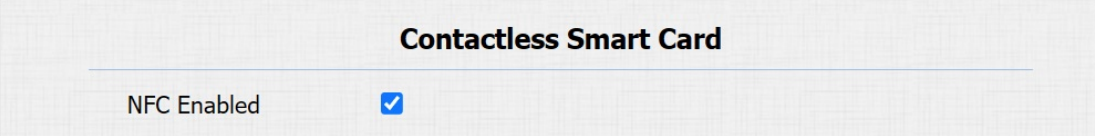


- **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
- **Block Key**: Set a password to access the data stored in the predefined sector/block.

NFC Card

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 the NFC function on the **Intercom > Card Setting > Contactless Smart Card** interface.

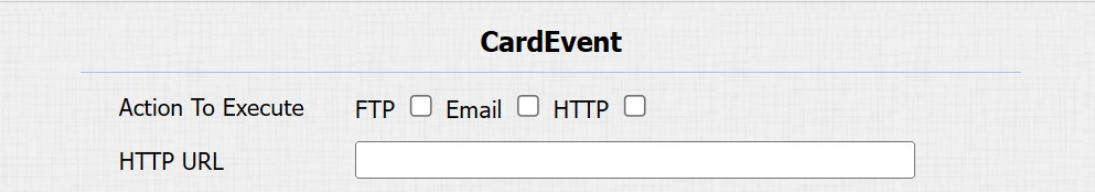


Note

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

Actions Triggered by Swiping Cards

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

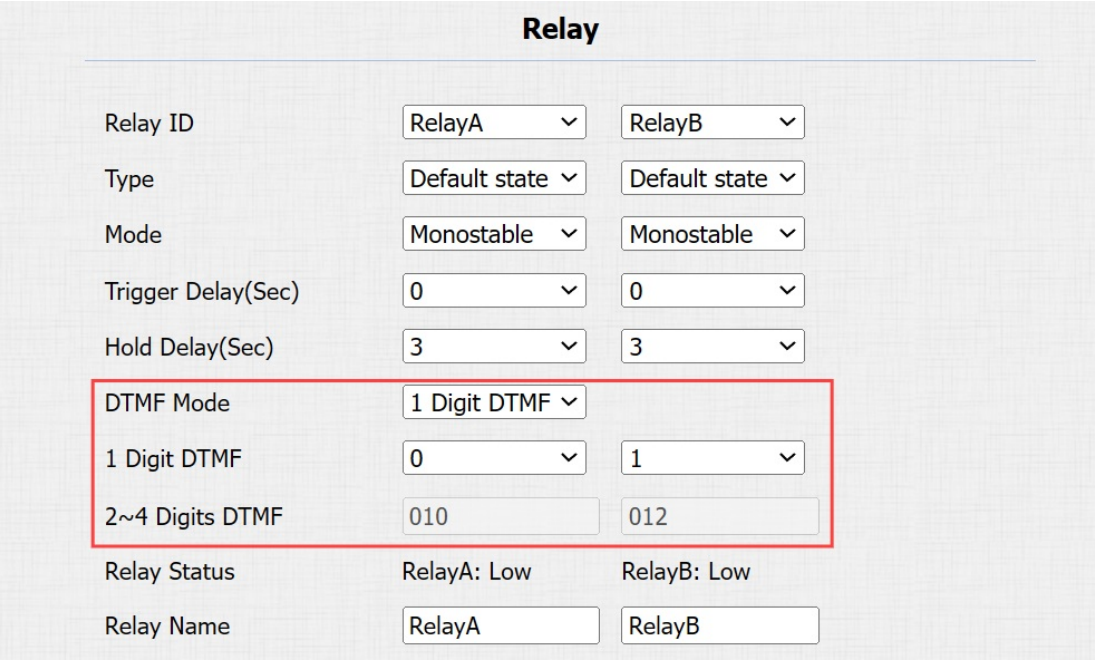


- **Action To Execute**:
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server 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.

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.

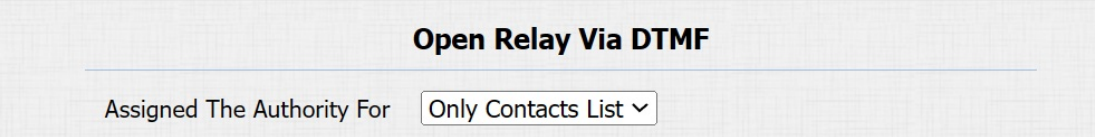


- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

> **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.

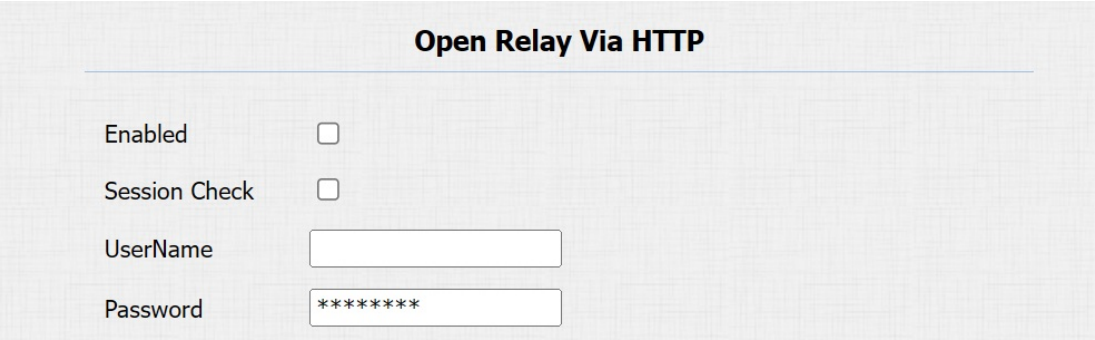


- **Assigned The Authority For** : Specify the contacts authorized to open doors via DTMF:
  - None: No numbers can open doors using DTMF.
  - Only Contacts List: Doors can be opened by numbers added to the door phone's contact list and pressing the push button.
  - All Numbers: Any numbers can unlock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

Unlock by HTTP Commands

The device supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the device. This will trigger the relay and open the door, even if the users are away from the device.

Set it up on the **Intercom > Relay > Open Relay Via HTTP** interface.



- **Session Check**: Enable to enhance data transmission security.
- **User Name**: 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.

Note

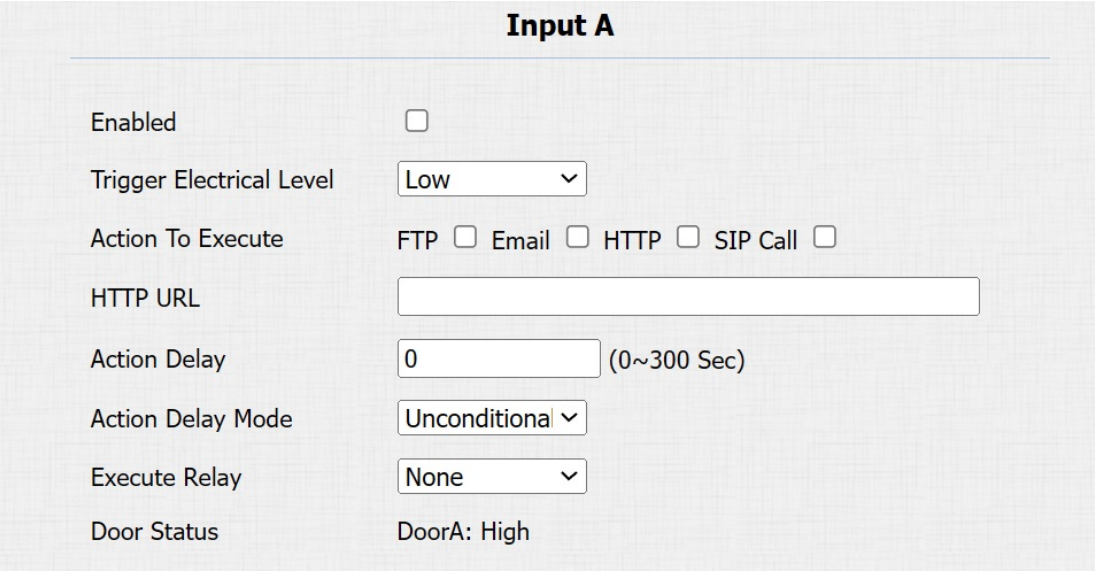
The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide **Opening the Door via HTTP Command** for more information.

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.

Click here to watch the instruction video.

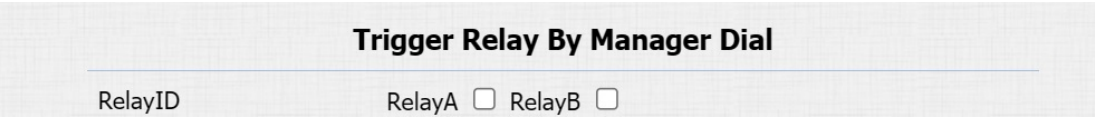
To set it up, go to the **Intercom > Input** interface.



- **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.
- **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.

Unlock by Pressing the Push Button

You can select the relay(s) to be triggered by pressing the push button on the **Intercom > Basic > Trigger Relay By Manager Dial** interface.



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.

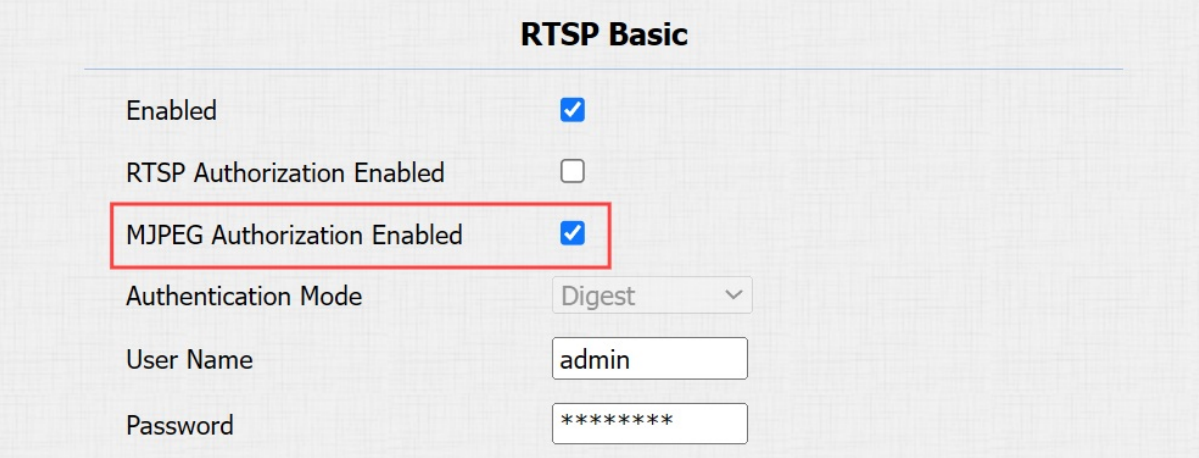
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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 Image Capturing

You can take a monitoring image or check the monitoring video in Mjpeg format with the device. To view the video stream, you need to turn on the Mjpeg video function and choose the image quality.

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



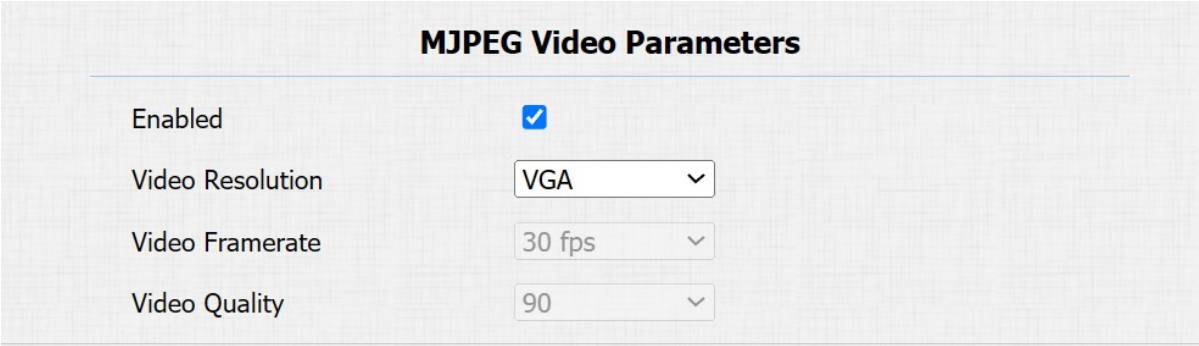
- **MJPEG Authorization Enabled**: Once enabled, accessing the door phone's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, User Name, and Password.

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.

You can set up the MJPEG video parameters in the **MJPEG Video Parameters** section.



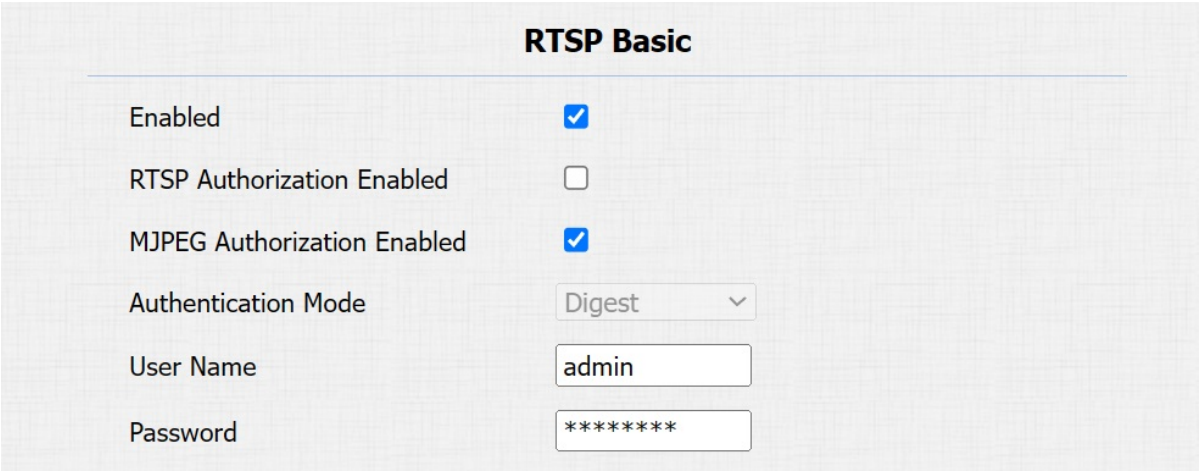
- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Video Quality**: The video bitrate ranges from 50 to 90.

RTSP Stream Monitoring

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

RTSP Basic Setting

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

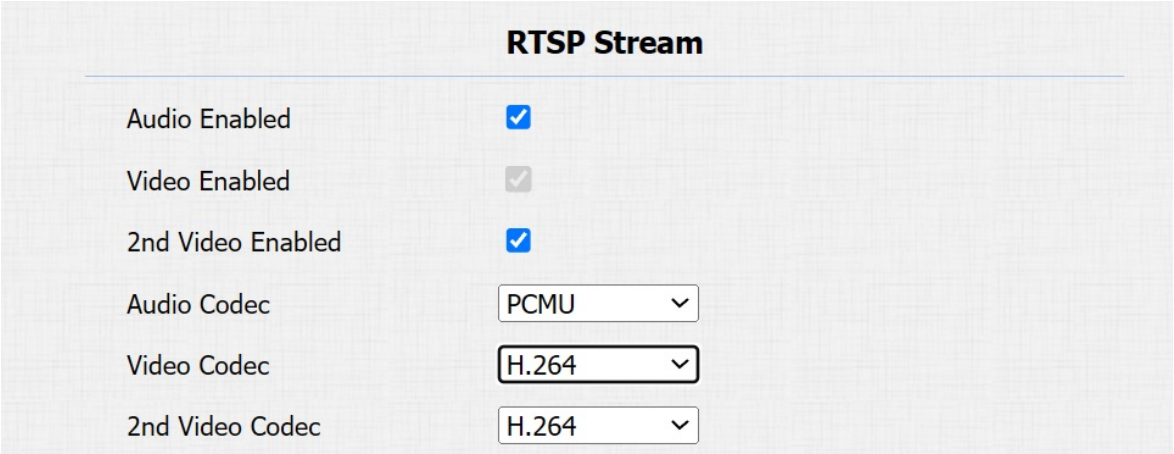


- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: The Digest mode uses hashing instead 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 Stream Setting

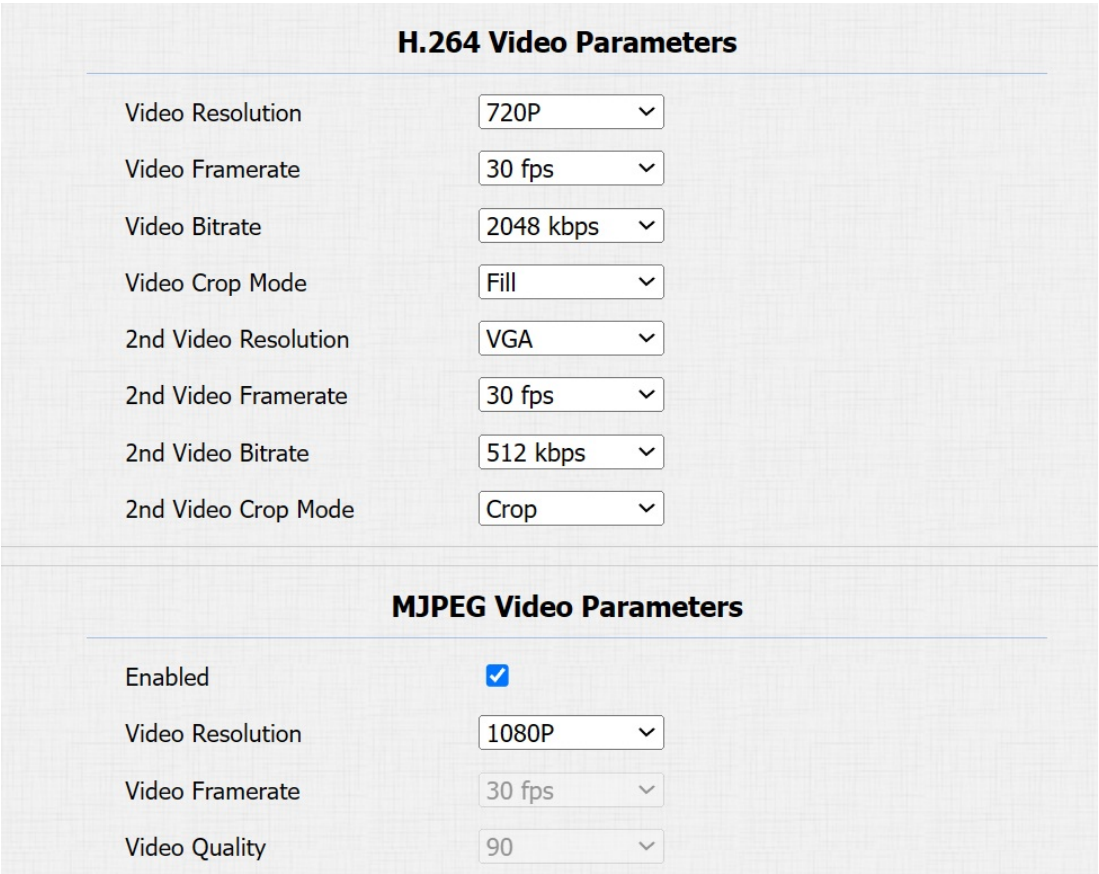
The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

Set it up on the **Intercom > RTSP > RTSP Stream** interface.



- **Audio Enabled:** Decide whether the RTSP stream has sound.
- **Video Enabled:** Decide whether the RTSP stream has video. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **2nd Video Enabled:** The device supports two RTSP streams.
- **Audio Codec:** Choose a suitable audio codec for RTSP audio.
- **Video Codec:** Specify the video compression formats.
  - H.264: Offer highly efficient compression but at a cost of higher latency and computational load.
  - MJEPG: Offer improved quality but inefficient compression.

You can set up the video parameters for H.264 and MJPEG in the **H.264** and **MJPEG Video Parameters** section.



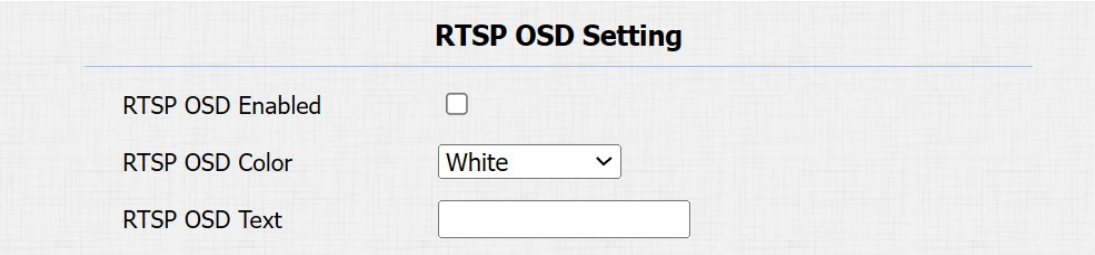
- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 2K(2560×1440 pixels).
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Video Bitrate**: The amount 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. The default is 2048 kbps.
- **Video Crop Mode**:
  - Scale: The original video frame is transmitted without cropping.

  - Crop: The transmitted video frame is cropped to eliminate vignettes.
  - Fill: The transmitted video frame fills the screen with an aspect ratio of 1:1.
- **2nd Video Resolution**: Specify the image resolution for the second video stream channel.
- **2nd Video 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.
- **2nd Video Crop Mode**: Set the crop mode for the second video stream.

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture.

Set it up on the web **Intercom > RTSP > RTSP OSD Setting** interface.

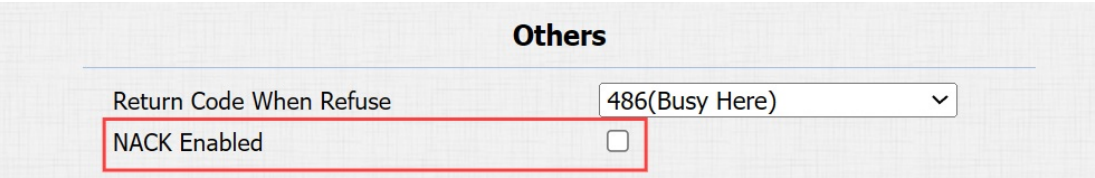


- **RTSP OSD Color**: There are five color options, White, Black, Red, Green, and Blue for RTSP watermark text.
- **RTSP OSD Text**: Customize the watermark text.

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 the **Phone > Call Feature > Others** interface.



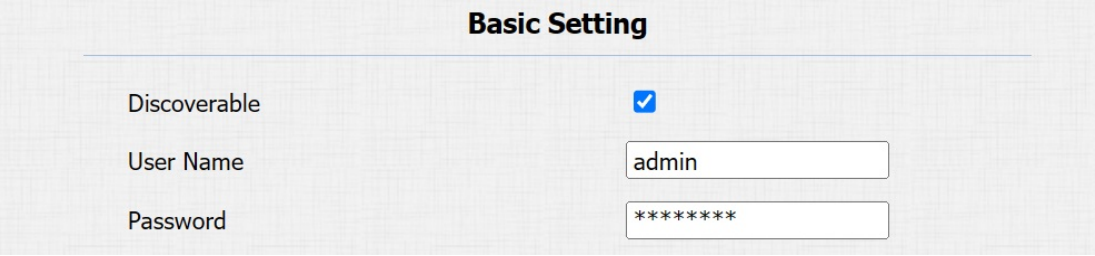
- **NACK Enabled:** It can be used to prevent losing data packets in the weak network environment when discontinued and mosaic video images occur.

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.

Click here to view an example of using the ONVIF feature: the integration with Uniview NVR System.

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



- **Discoverable**: When enabled, the video from the door phone camera can 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.

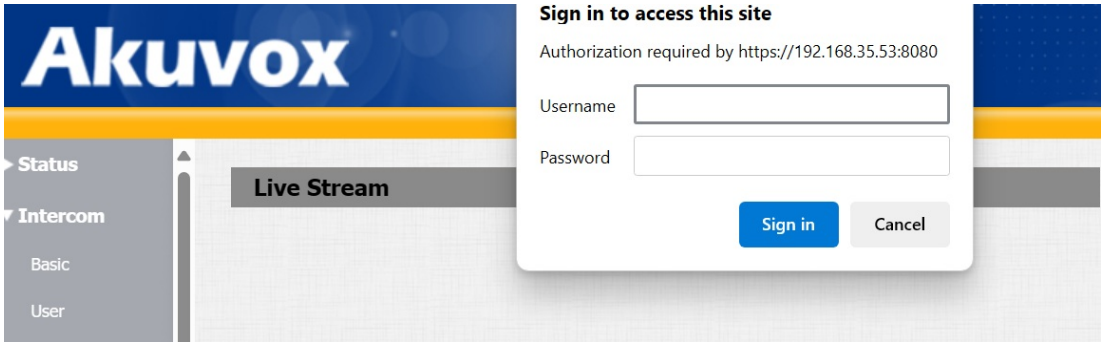
- **Password**: Set the password required for accessing the door phone's video stream on other devices. It is admin by default.

> **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.

See live stream on the device **Intercom > Live Stream** interface. Enter the authorization username and password set in the RTSP settings.

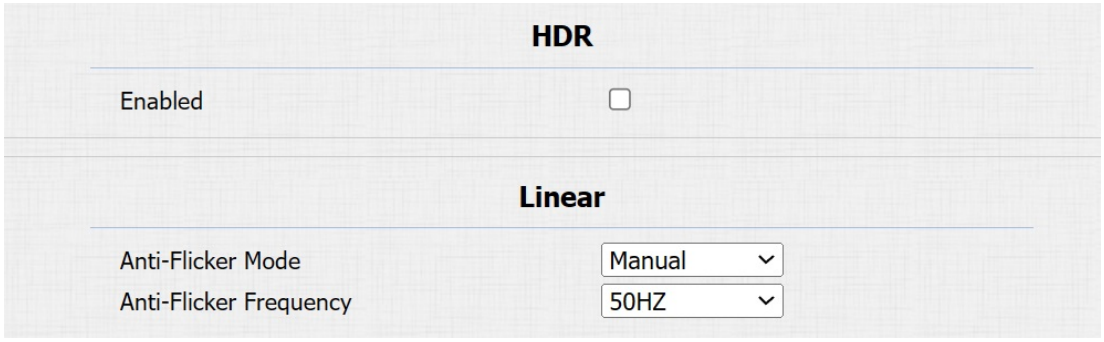


Camera Mode

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.



- **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.

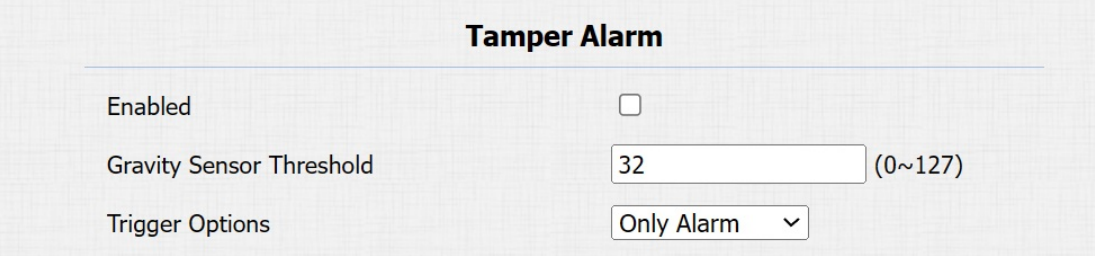
Security

Tamper Alarm

The tamper alarm function prevents anyone from removing the device without permission. Akuvox devices support two types of tamper proof: gravity detection and button status detection.

Click here to view which type is supported by the device and learn the function details.

Set it up on the **Security > Basic > Tamper Alarm** interface.



- **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

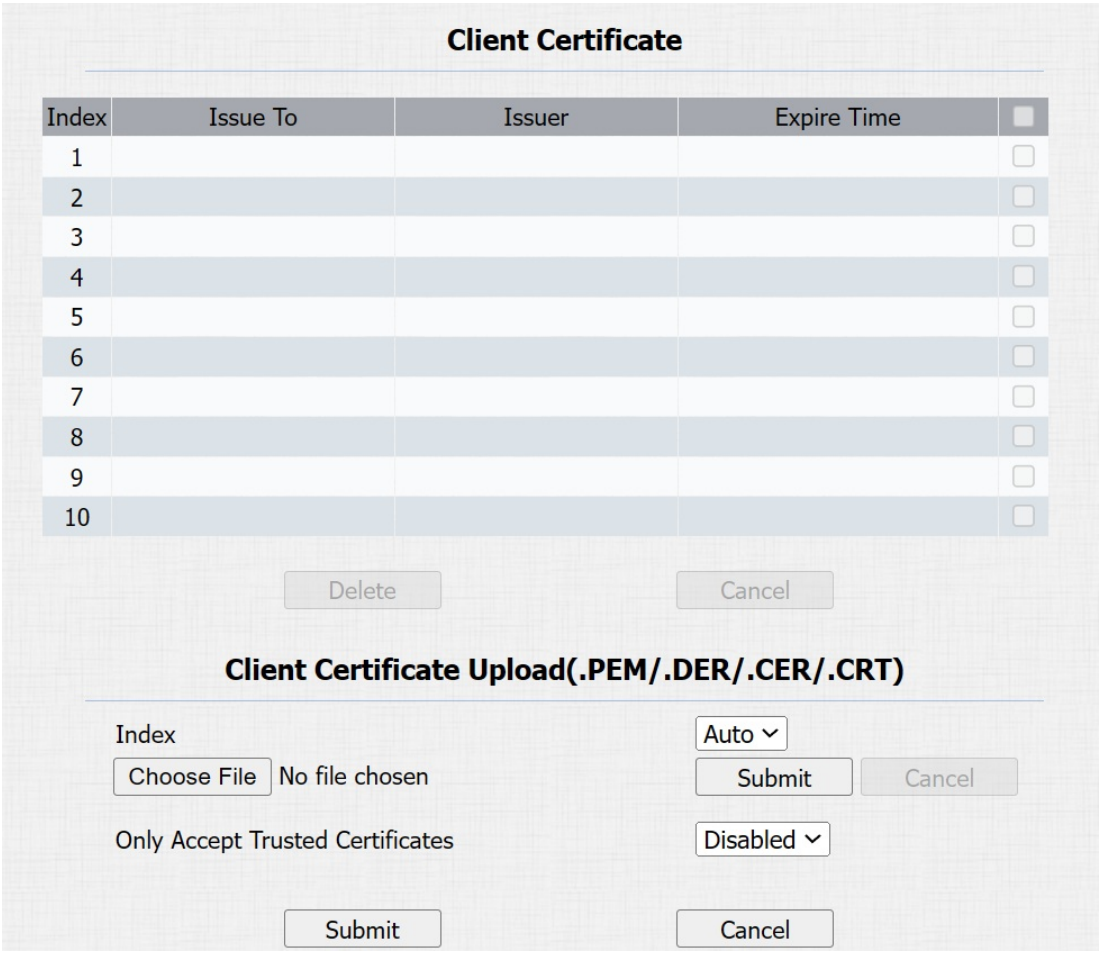
It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

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

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 and configure the Client Certificate on the **Security > Advanced > Client Certificate** interface.

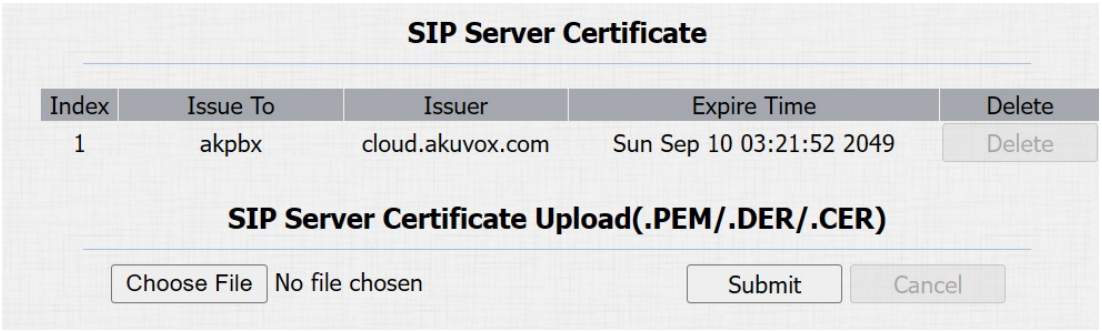


- **Index:**
  - Auto: The uploaded certificate will be displayed in numeric order.
  - 1 to 10: The uploaded certificate will be displayed according to the value selected.
- **Choose File:** Click Choose File to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, as long as the authentication succeeds, the door phone will verify the server certificate based on the client certificate list. If select Disabled, the door phone will not verify the server certificate no matter whether the certificate is valid or not.

Upload TLS Certificate for SIP Account Registration

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

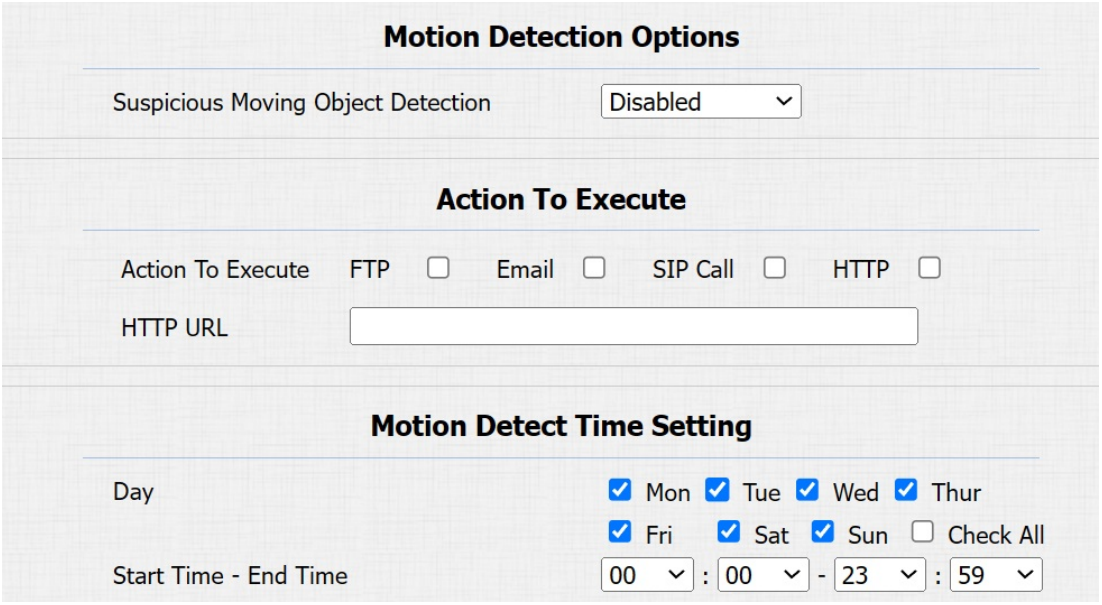
To set it up, go to **Security > Advanced** interface.



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.



- **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.
  - **Image Detection**: When the video camera detects moving objects, preset actions will be triggered.
  - **Pedestrian Detection**: When the device detects the upper body of the passersby, preset actions will be triggered.

When selecting Image Detection or Pedestrian Detection, you need to further set up the following options.

- **Detection Accuracy**: The detection sensitivity. The greater the value is, the more accurate the detection is. The default value is 3.
- **Detection Distance(M)**: This option is only available for Pedestrian Detection. Set the distance to detect the pedestrian. For example, if it is set to 5 meters, the pedestrian will only be detected when he/she is away from the device within 5 meters.
- **Timing Interval**: Determine how to delay and trigger motion detection.
  - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.
  - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
  - The default interval is 10 seconds.
- **Detection Area**: You can specify three detection areas by pressing the left mouse button and drawing boxes.
- **Action To Execute**: Set the desired actions that occur when suspicious movement is detected.
  - 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 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.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Motion Detect Time Setting**: Specify the time when the motion detection setting is effective.

Security Notification

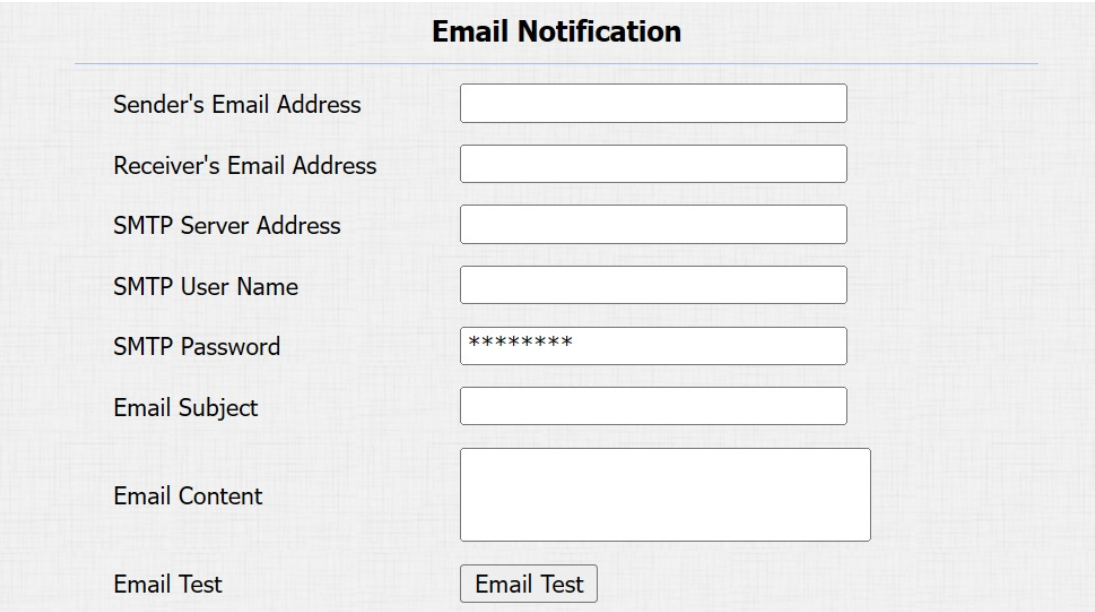
A security notification informs users or security personnel of any breach or threat that the device detects. For example, if the device detects something unusual, the system sends a notification to users or security through email, phone calls, or other methods.

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

Email Notification

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

Click here to view how to set this feature up.

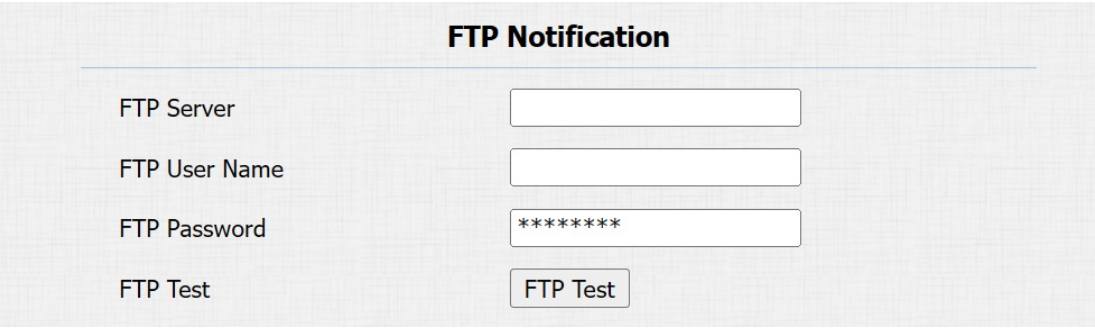


- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.
- **Email Test**: Used to test whether the email can be sent and received.

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.

Click here to view the configuration steps.

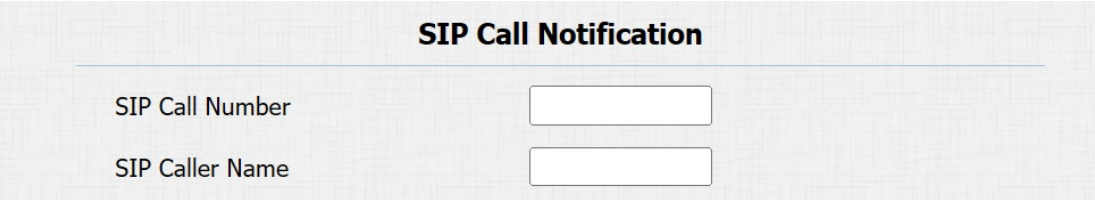


- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.
- **FTP Test:** Used for testing whether the FTP notification can be sent and received by the FTP server.

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.



Action URL

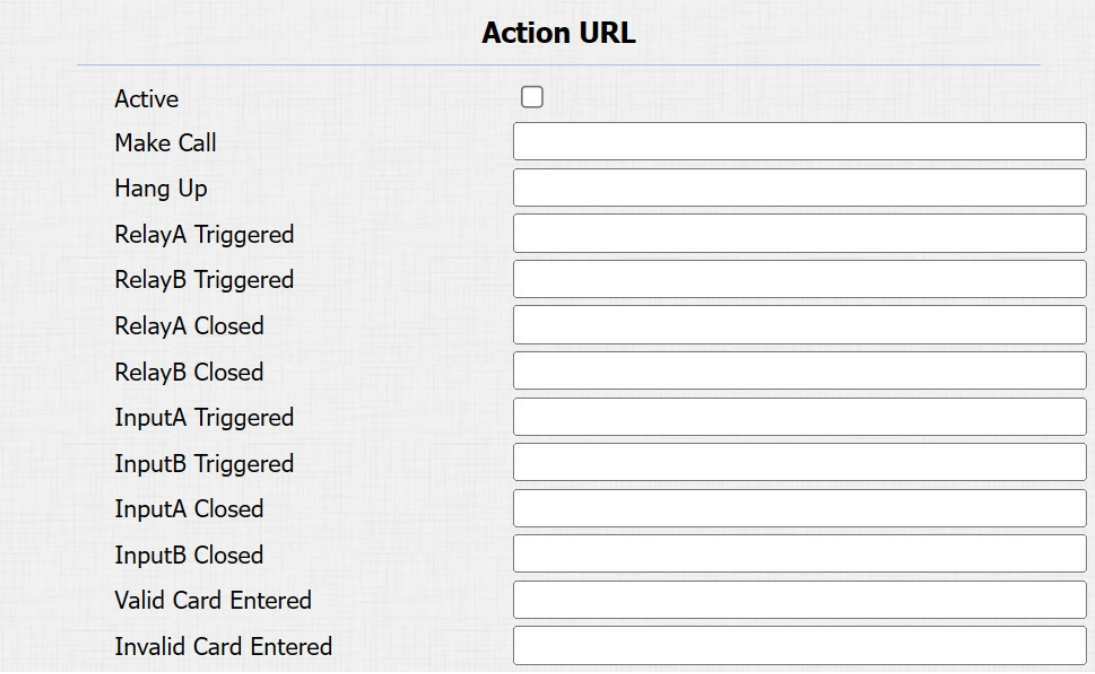
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, or RF card access changes.

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 Card Entered	$card_sn	Http://server ip/validcard=$card_sn
8	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.



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.

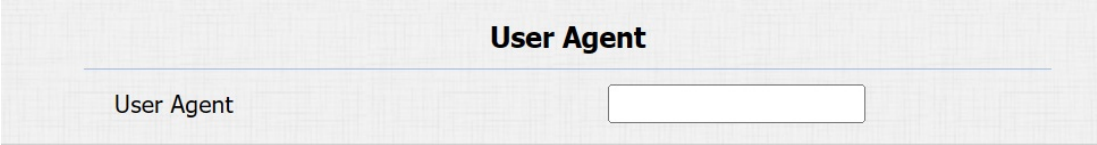
Set it up on the **Account > Advanced > Encryption** interface.

- **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.

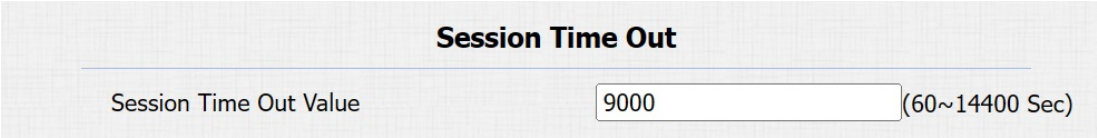
To set it up, go to the **Account > Advanced > User Agent** interface.



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.



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 it on the **Security > Basic > High Security Mode** interface.

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.

Emergency Action

This feature works with Akuvox SmartPlus Cloud. It keeps the door open when an emergency happens. You need to specify the Input that applies the feature.

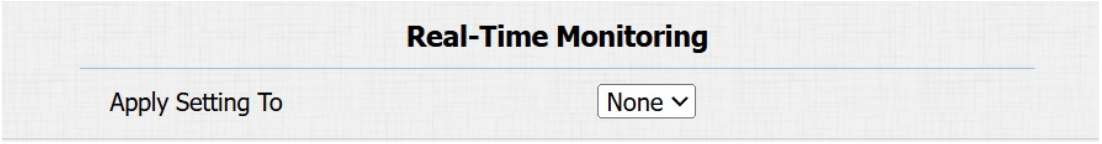
Click here to view the detailed configuration of this feature.

Set it up on the **Security > Basic > Emergency Action** interface.

Real-time Monitoring

This feature displays the door status when the device is connected to the SmartPlus Cloud. Property managers and end users can check the door status respectively on the SmartPlus Property Manager platform and SmartPlus App.You need to specify the relay(s) or input(s) that apply this feature. Click here to see the detailed configuration.

Set it up on the **Security > Basic > Real-time Monitoring** interface.



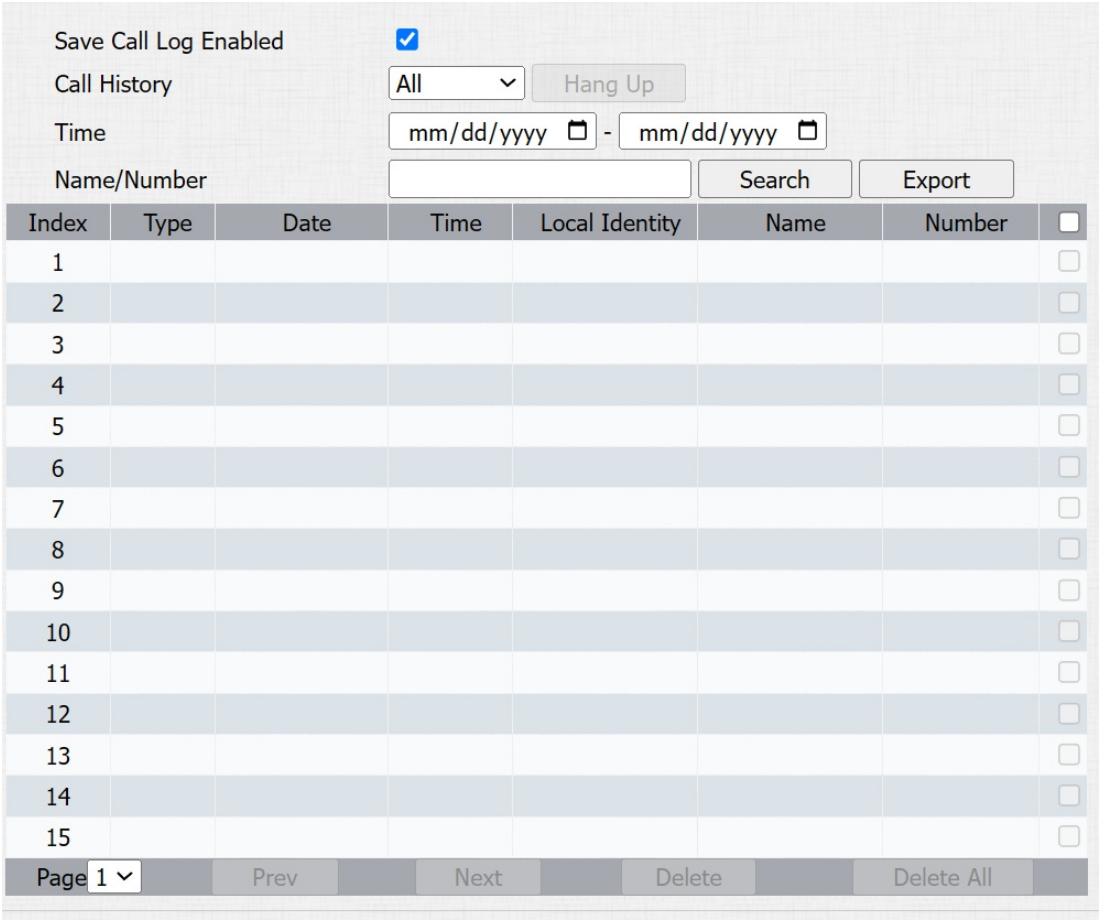
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: the door is opened by triggering input.
  - **Relay**: the door is opened by triggering the relay.

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

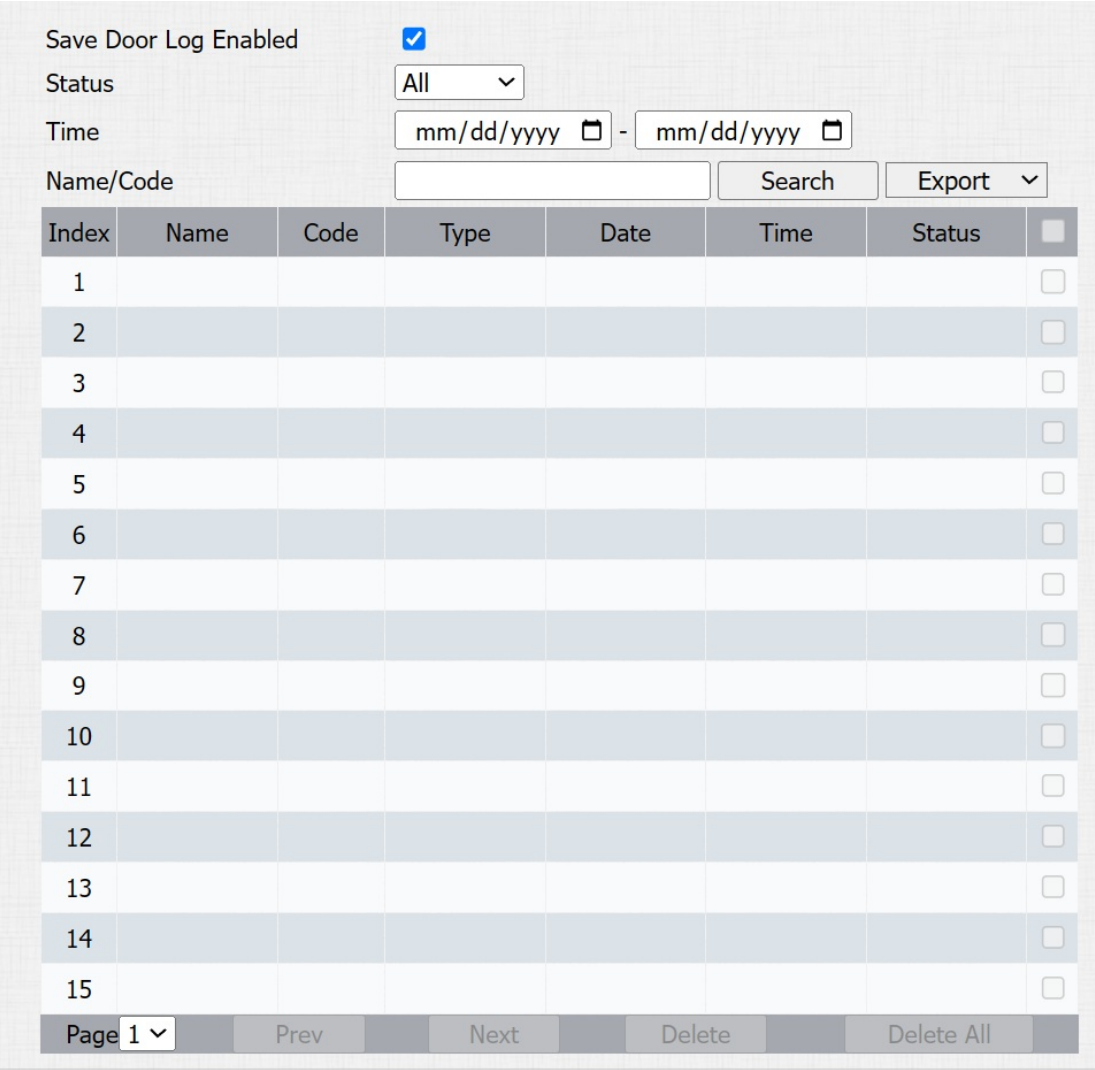


- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.

Door Logs

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

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



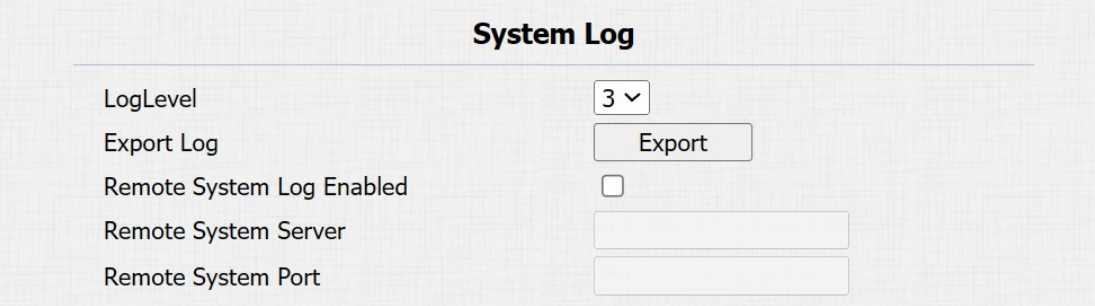
- **Status:** Display All, Successful, and Failed door-opening records.
- **Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card code will be displayed.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

Set the system log on the **Upgrade > Advanced > System Log** interface.

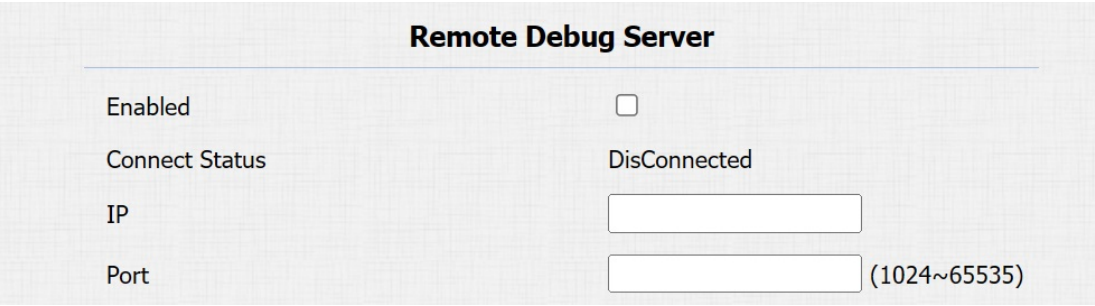


- **Log Level:** Select log levels from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export 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.

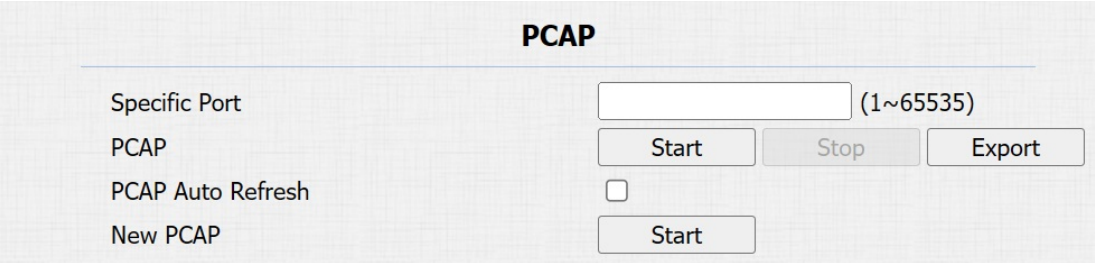


- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.
- **Port**: Enter the port of the server.

PCAP

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

Set up the PCAP on the web **Upgrade > Advanced > PCAP** interface.

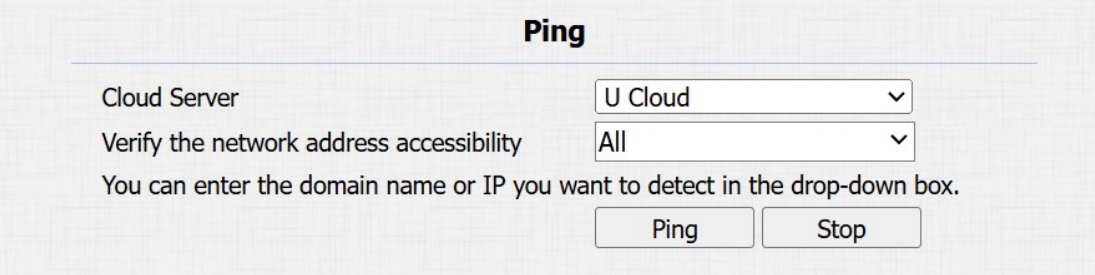


- **Specific Port:** Select the specific port from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the 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.

Ping

The device allows you to verify the accessibility of the target server.

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

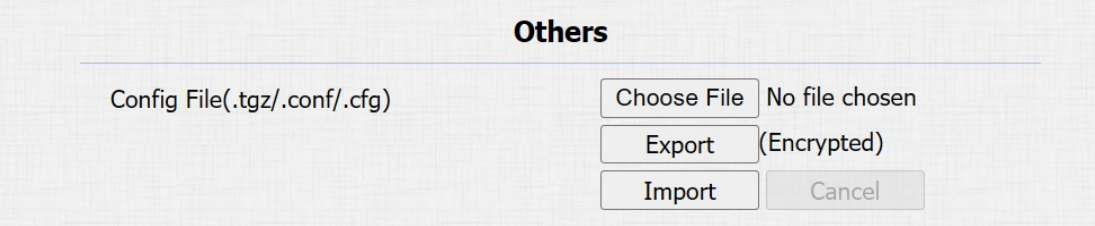


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Backup

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

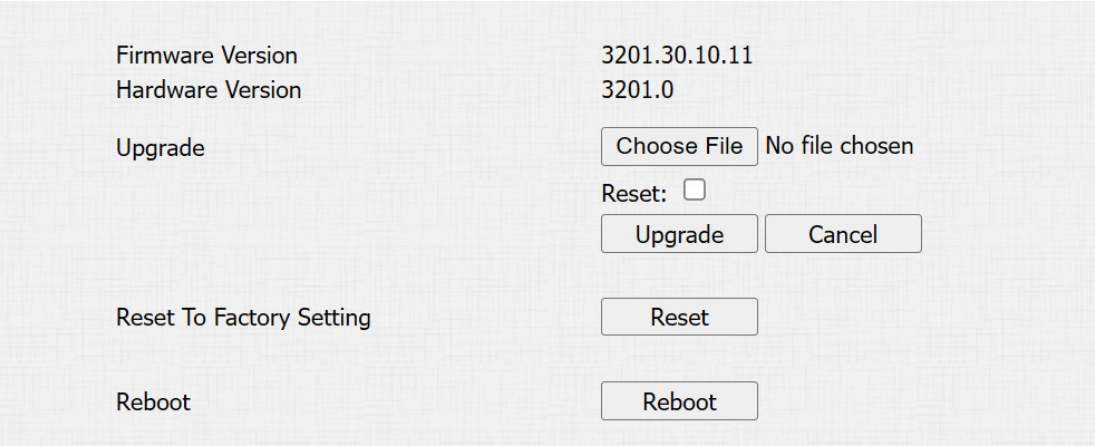
Export the file on the **Upgrade > Advanced > Others** interface.



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.



Note

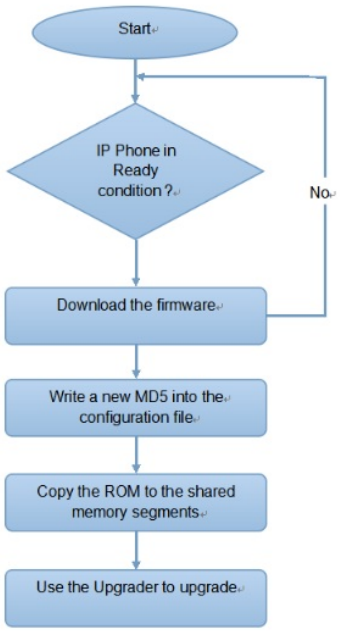
The upgrade file should be in .rom format.

Auto-provisioning via Configuration File

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:



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

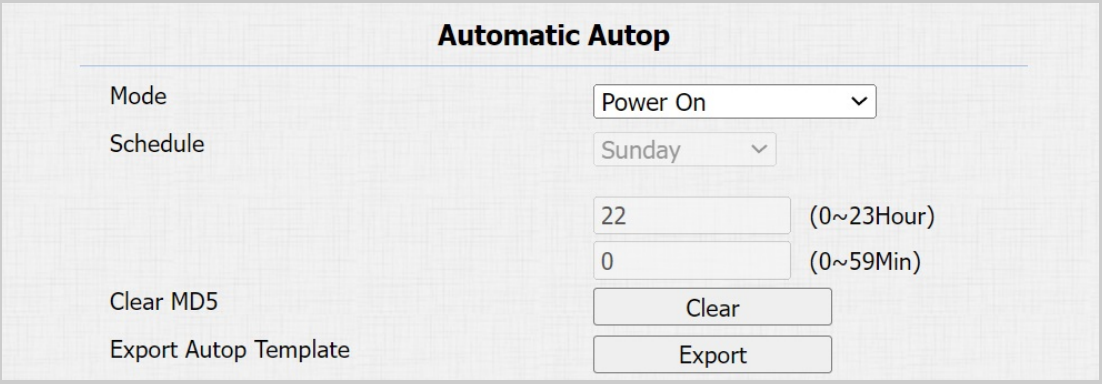
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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 **Upgrade > Advanced > Automatic Autop** interface.

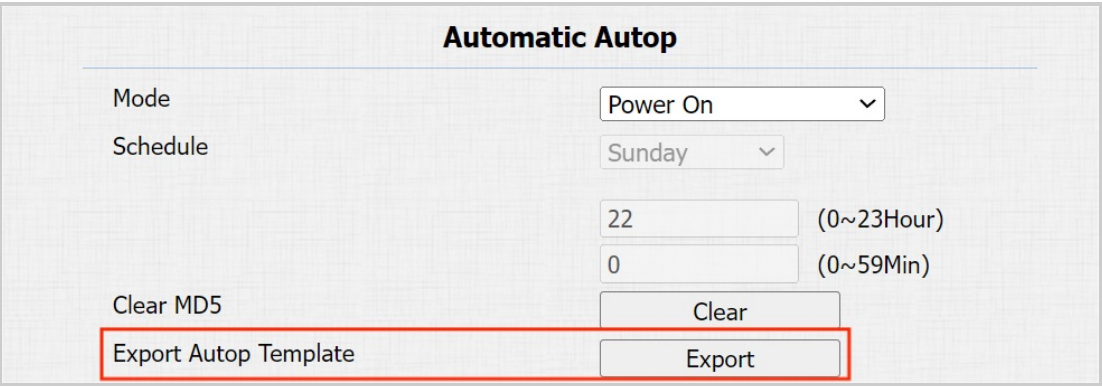


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every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

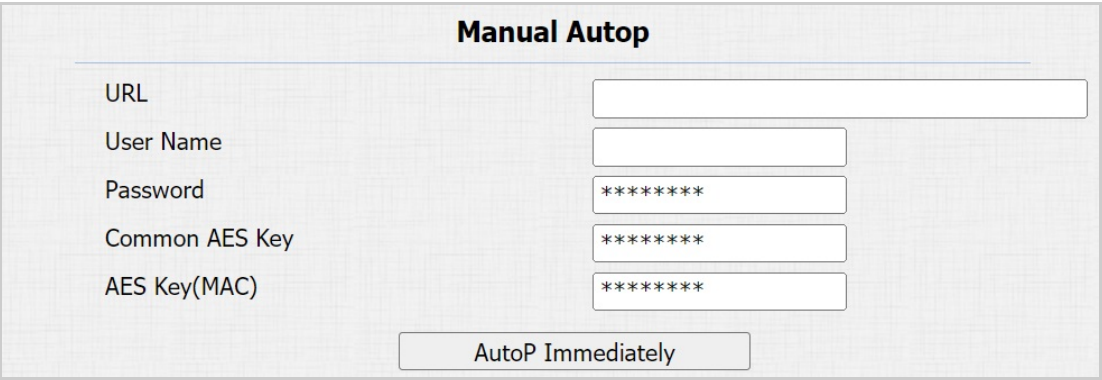
Static Provisioning

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.



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



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **User Name**: 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

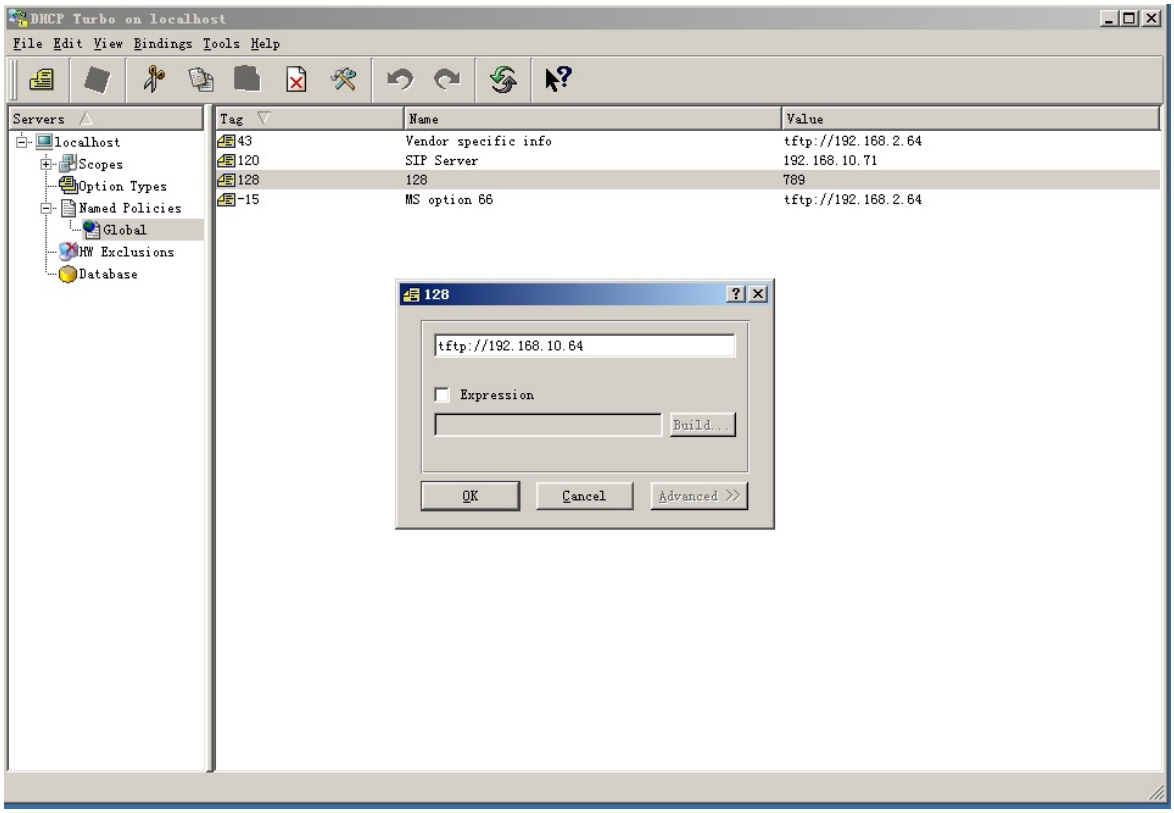
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use 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.

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.

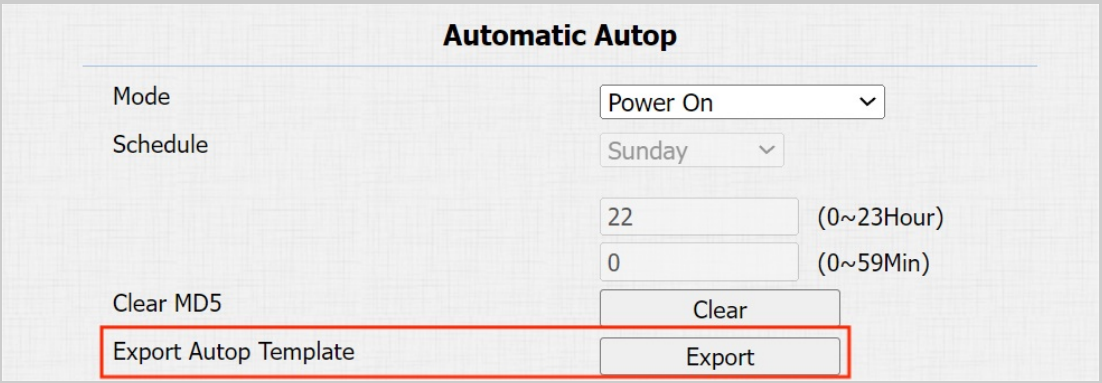


Note

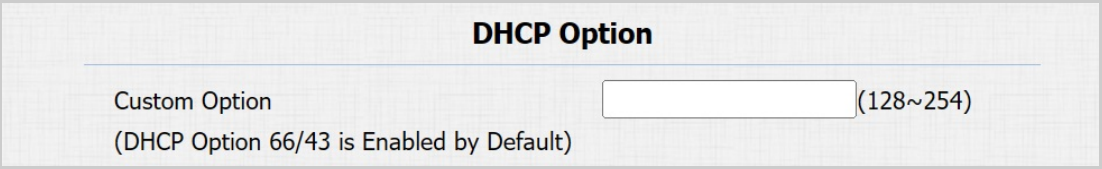
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

Go to **Upgrade > Advanced > Automatic Autop** interface.



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



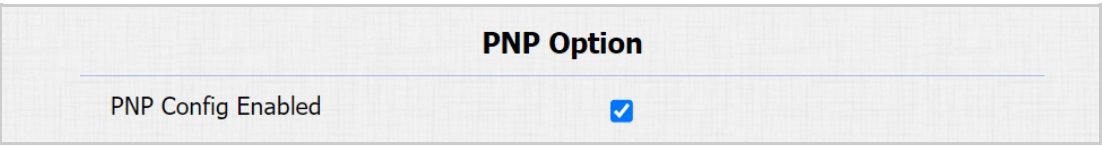
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done 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.

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.

Click here to watch the configuration video.

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

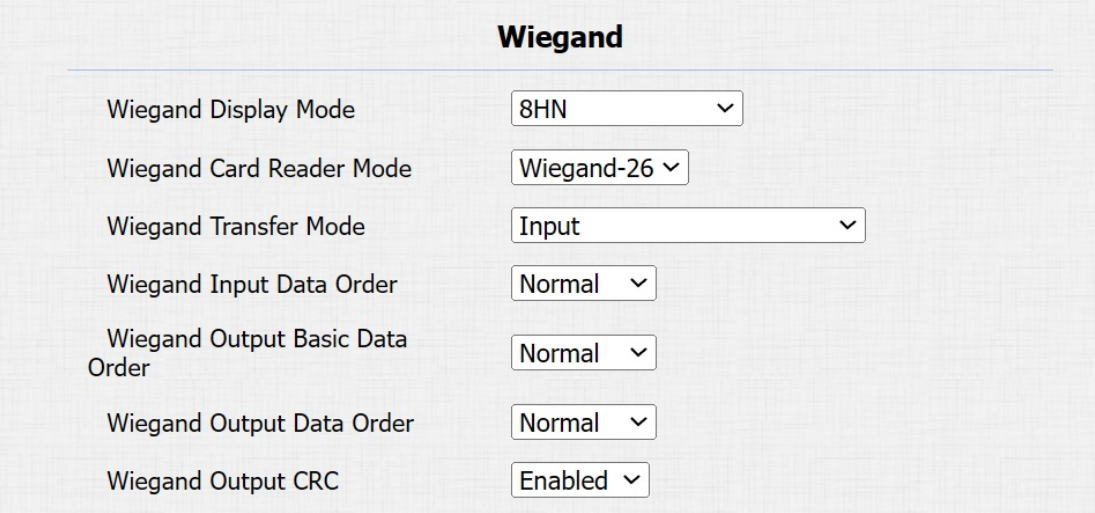


Integration with Third Party Device

Integration via Wiegand

The device can be integrated with third-party devices via Wiegand.

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



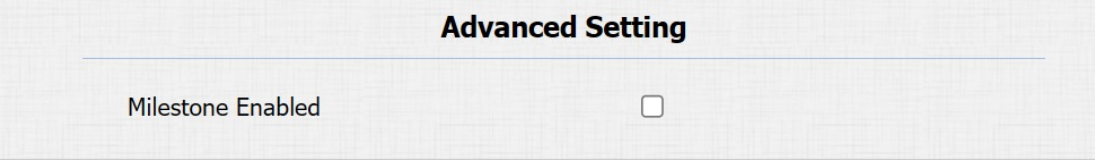
- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the access control terminal and the third-party device.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender, sending the card data to a third-party device for door access.
  - **Convert To Card No. Output**: The device serves as a sender. The access data including DTMF and RF card code will be converted to card numbers for door access.
- **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.

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

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 > Advanced Setting** interface.



Integration via HTTP API

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

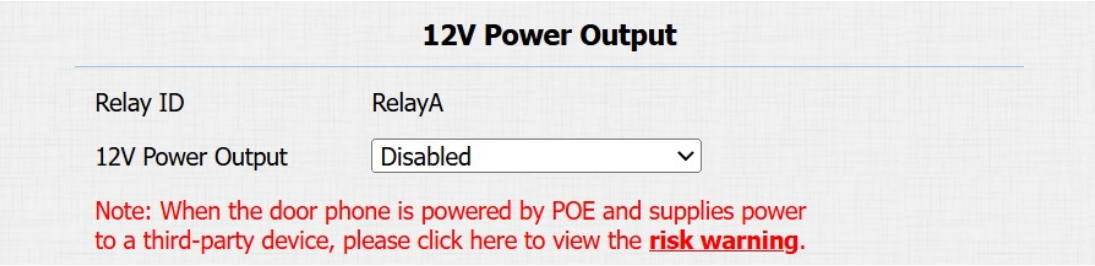
Set it up on the web **Intercom > HTTP API** interface.

- **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.

Power Output Control

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

To set it up, go to the **Intercom > Relay > 12V Power Output** interface.



- **12V Power Output**: This function can only be used when the device is powered by a 12V power adapter.
  - **Disabled**: Turn off the function.
  - **Always**: Provide continuous power.
  - **Triggered by Open Relay**: Provide power to the third-party device when Relay A is triggered via its NO and GND ports. Stop providing the power when Relay A is reset.
    - Timeout(Sec): Set the time(3, 5, or 10 seconds) to provide power when **Triggered by Open Relay** is selected.

Note

The door phone's **volume adjustment** affects external power supply.

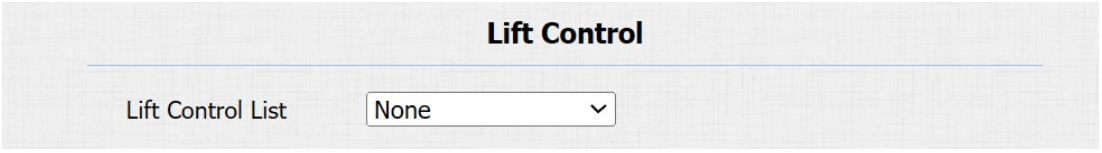
- If the third-party device operates at 12V and ≤0.2A, the door phone supports both Level 1 and 2 volume.
- If the device operates at 12V and 0.2A–0.4A, only Level 1 is supported; Level 2 may cause a shutdown.
- If the device exceeds 0.4A at 12V, it will shut down due to insufficient power.

Lift Control

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

Click here to watch a demonstration video of configuring the lift control feature.

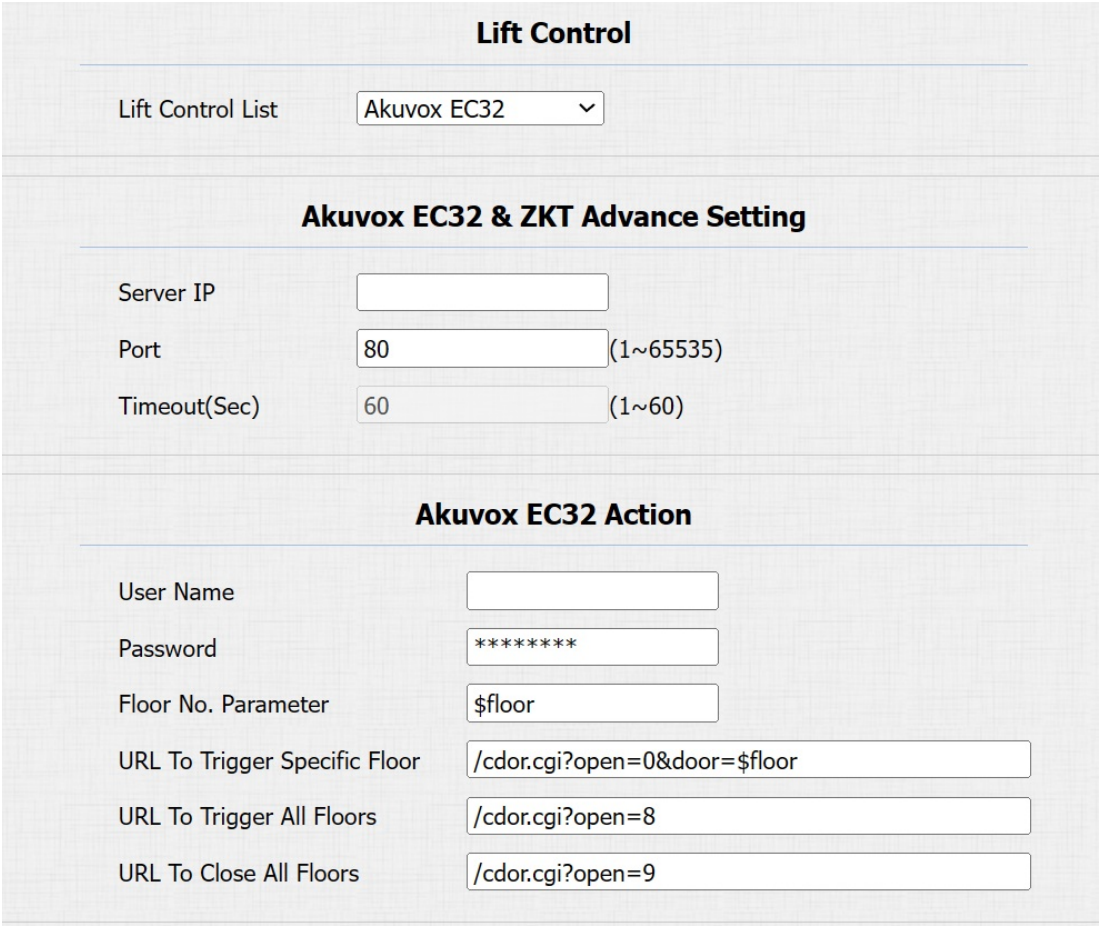
To set it up, go to the **Intercom > Lift Control** interface.



- **Lift Control List:** Select the lift controller brand.
  - None: The integration will be disabled.
  - Chiyu: Integrate with Chiyu lift controller.
  - KeyKing: Integrate with KeyKing lift controller.
  - Akuvox EC32: Connect the device with the Akuvox EC33 lift controller.
  - ZKT: Integrate with ZKTeco lift controller.

Akuvox Lift Controller

After selecting Akuvox EC32 in the Lift Control List, you need to set up relevant parameters.

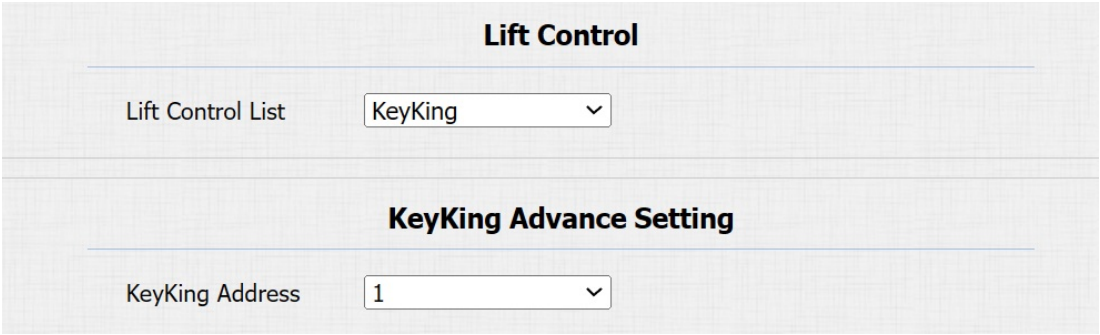


- **Server IP:** Enter the IP address of the Akuvox lift controller.
- **Port:** Enter the port of the Akuvox lift controller.
- **Timeout(Sec):** Decide the time limit within which users should press the lift button of their desired floors.
- **User Name:** Enter the user name set in the lift controller.

- **Password:** Enter the password set in the lift controller.
- **Floor NO. Parameter:** The floor number parameter is provided by Akuvox. The default is **$floor**. You can define your parameter string.
- **URL To Trigger Specific Floor:** The Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string $floor at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors:** The Akuvox URL for triggering all floors.
- **URL To Close All Floors:** The Akuvox URL for closing all floors.

KeyKing Lift Controller

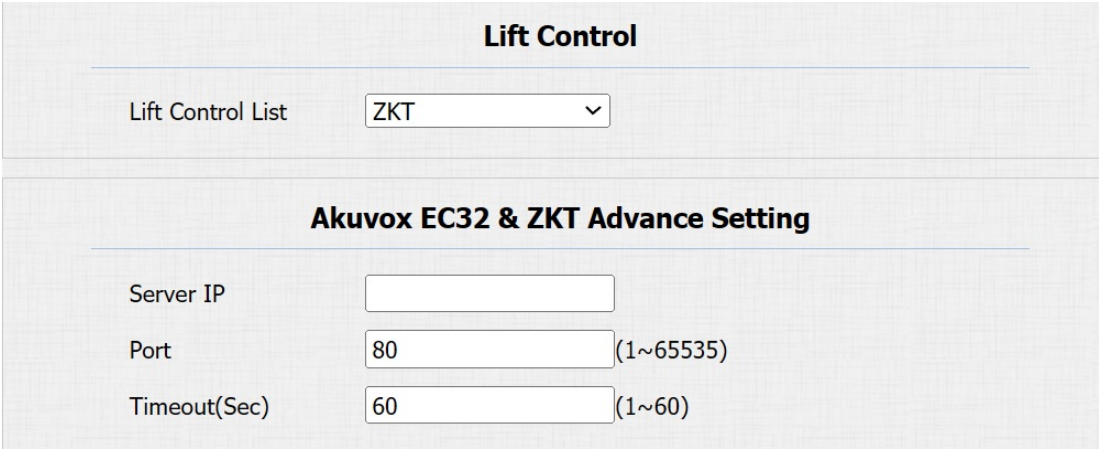
After selecting KeyKing, you need to set the KeyKing address.



- **KeyKing Address**: Select the number from 0 to 126. The binary number converted from the address number corresponds to the dip switch on the lift board. For example, if you select 5, set the dip switch to 101000.

ZKT Lift Controller

After selecting ZKT, you need to set up relevant parameters.

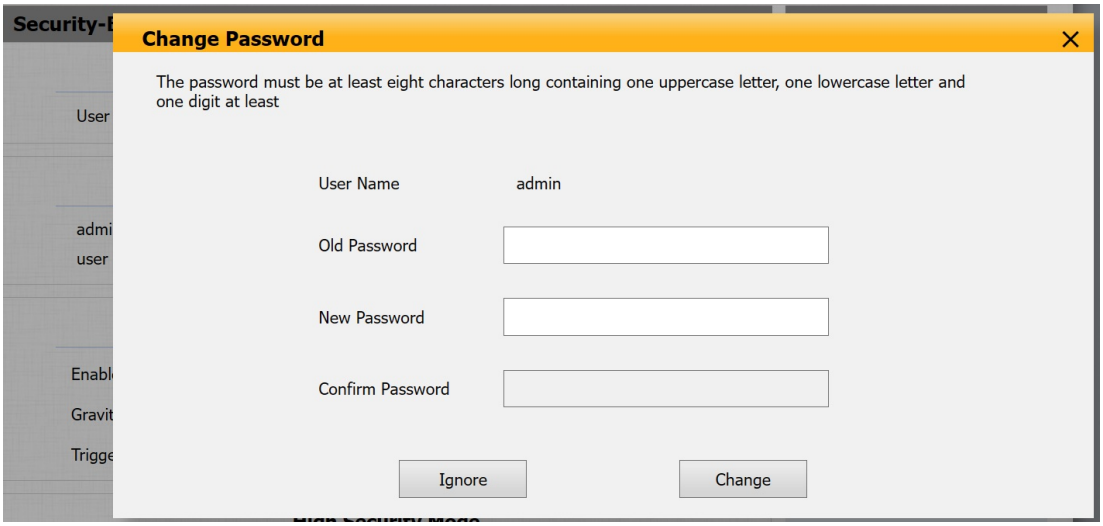


- **Server IP:** Enter the IP address of the controller server.
- **Port:** Enter the port of the controller server.
- **Timeout(Sec):** Decide the time limit within which users should press the lift button of their desired floors.

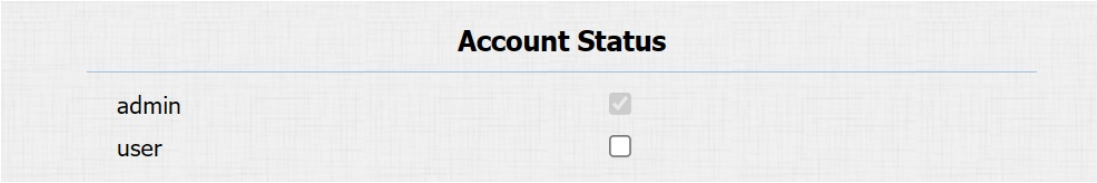
Password Modification

You can modify the device web password for both the administrator account and the user account.

To set it up, go to **Security > Basic > Web Password Modify** interface. Click **Change Password**.



To enable or disable the user account, scroll to the **Account Status** section.

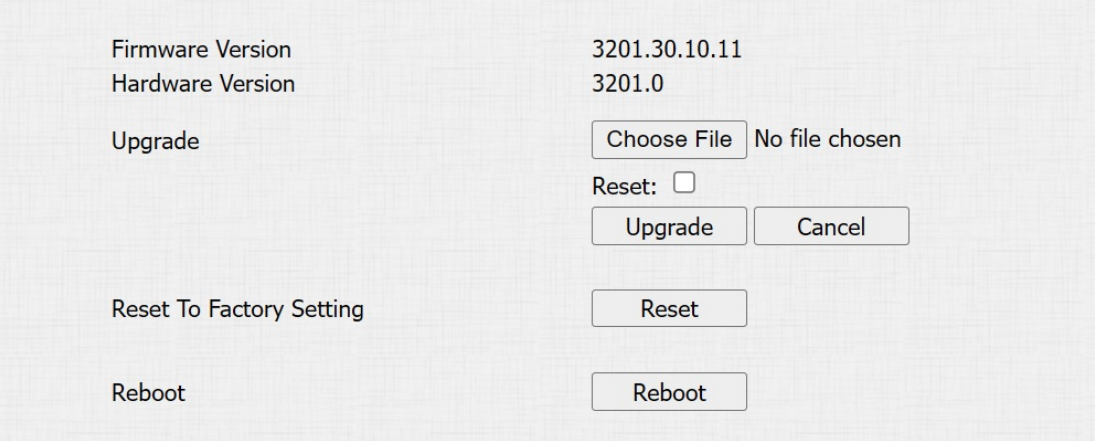


System Reboot and Reset

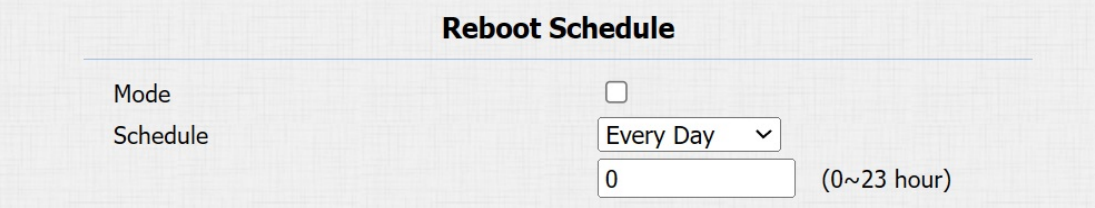
Reboot

If you want to restart the device system, you can operate it on the device web. Moreover, you can set up a schedule for the device to be restarted.

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



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



Reset

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