About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX R20A DOOR PHONE

Administrator Guide

Thank you for choosing Akuvox R20A series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 320.30.10.9 and it provides all the configurations for the functions and features of Akuvox door phone. Please visit Akuvox forum or consult technical support for any new information or latest firmware.

Product Overview

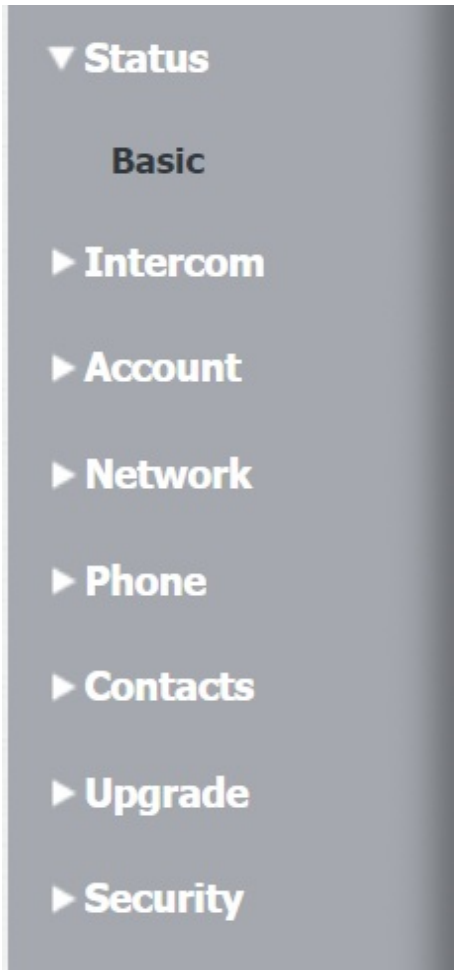
Akuvox R20A series can be connected with indoor monitors for remote access control and communication. They allow audio and video calls with visitors, as well as unlocking the door if necessary.

Model Specification

R20A	
Camera	2 Mega pixels, automatic lighting
Relay In	2
Relay Out	2
RS485	√
WiFi	X
Card Reader	√

Introduction to Configuration Menu

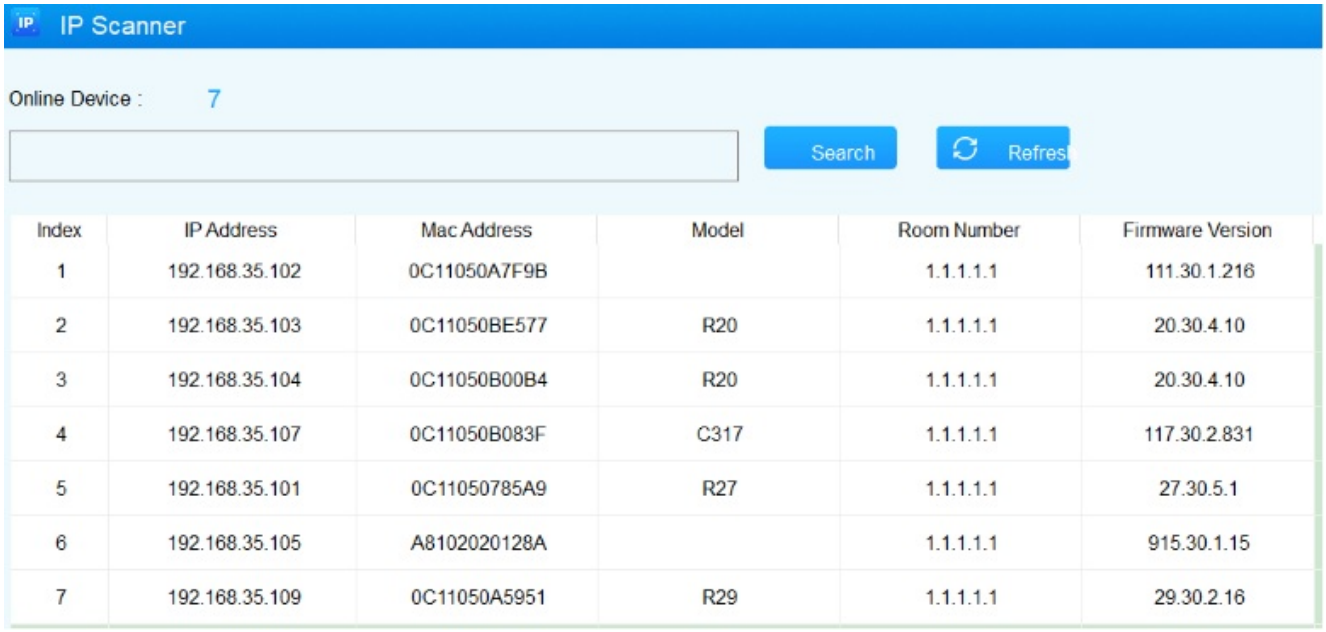
- **Status**: this section gives you basic information such as product information, network information, account information, etc.
- **Intercom**: this section covers intercom settings, call log, etc.
- **Account**: this section concerns SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, etc.
- **Network**: this section mainly deals with DHCP & static IP setting, RTP port setting, device deployment, etc.
- **Phone**: this section includes light settings, tab & button display, LCD settings and voice settings.
- **Contacts**: this section includes group and contact setting.
- **Upgrade**: this section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and fault diagnosis.
- **Security**: this section is for password modification.


Status
Basic
Intercom
Account
Network
Phone
Contacts
Upgrade
Security

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 in the same LAN network. Just click **Scan** tab in the IP scanner to check the device IP.

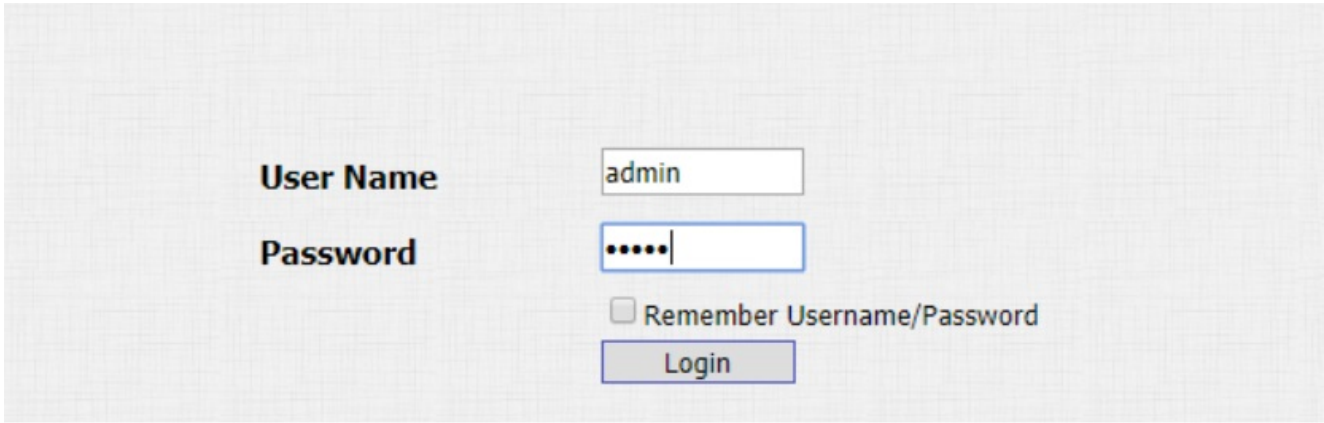


Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101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

Access the Device Setting on the Web Interface

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

The initial user name and password are 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.

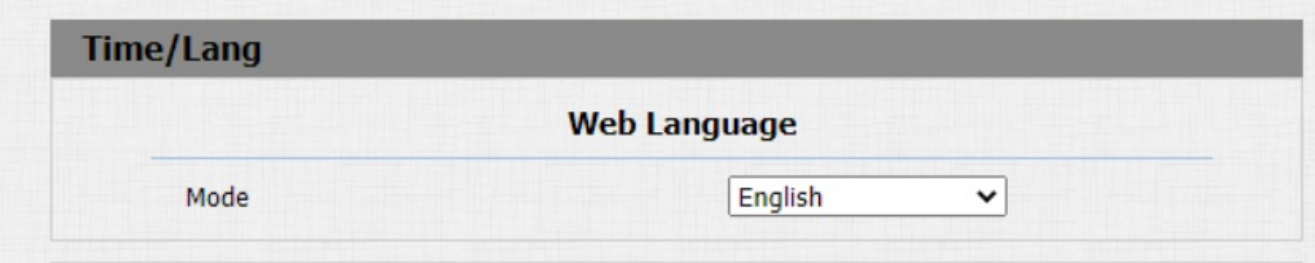
Language and Time Setting

Language Setting

The device supports the following web languages:

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

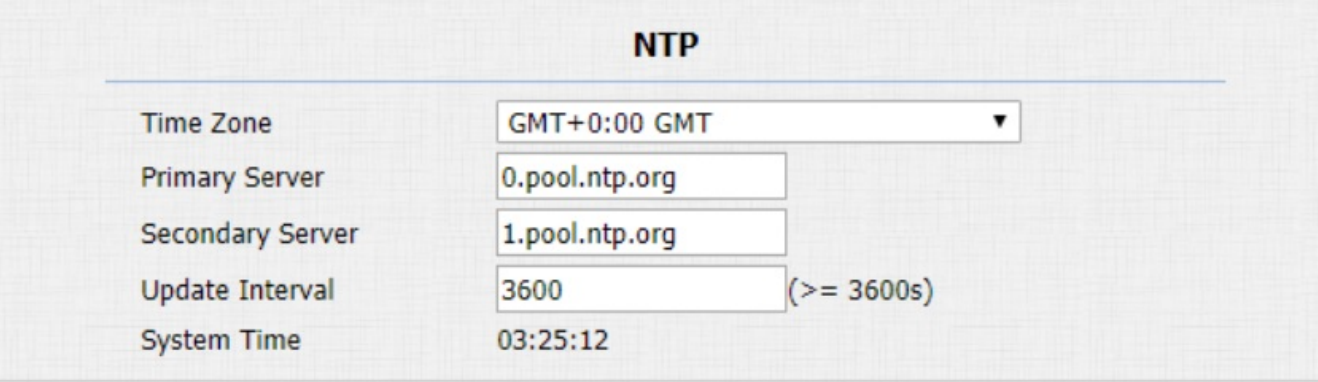
Navigate to the web **Phone > Time/Lang > Web Language** interface.



Time Setting

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

Navigate to the web **Phone > Time/Lang > NTP** interface.

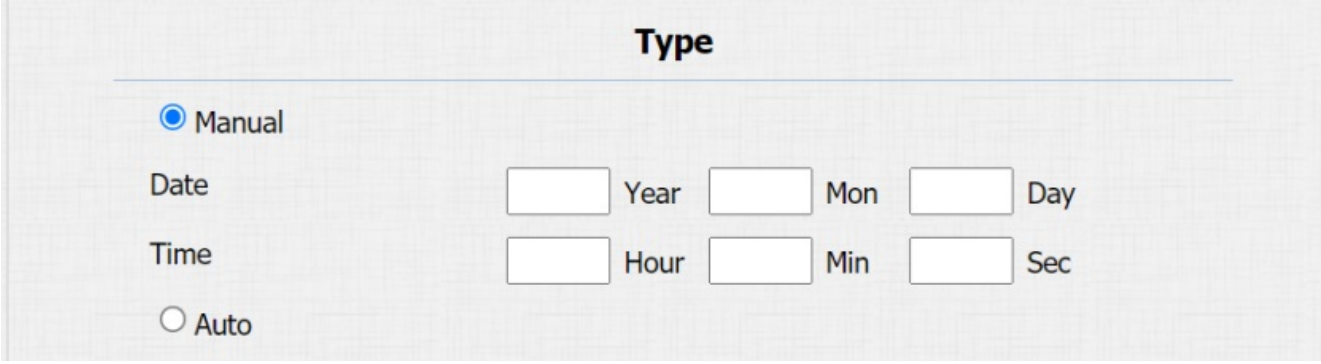


Parameter Set-up:

- **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.

You can also set up time manually, select the **Manual** checkbox, and input time data.

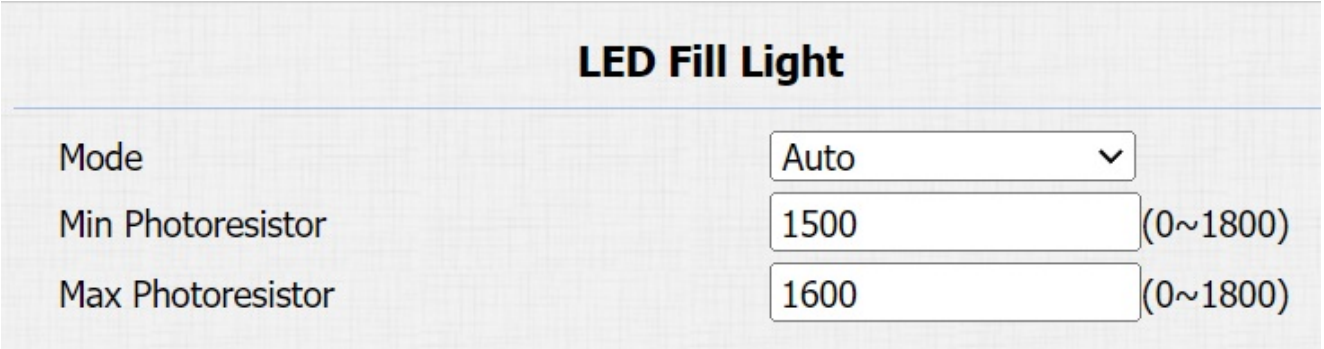


LED Setting

LED Fill Light

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

Navigate to the web **Intercom > LED Setting > LED Fill Light** interface.



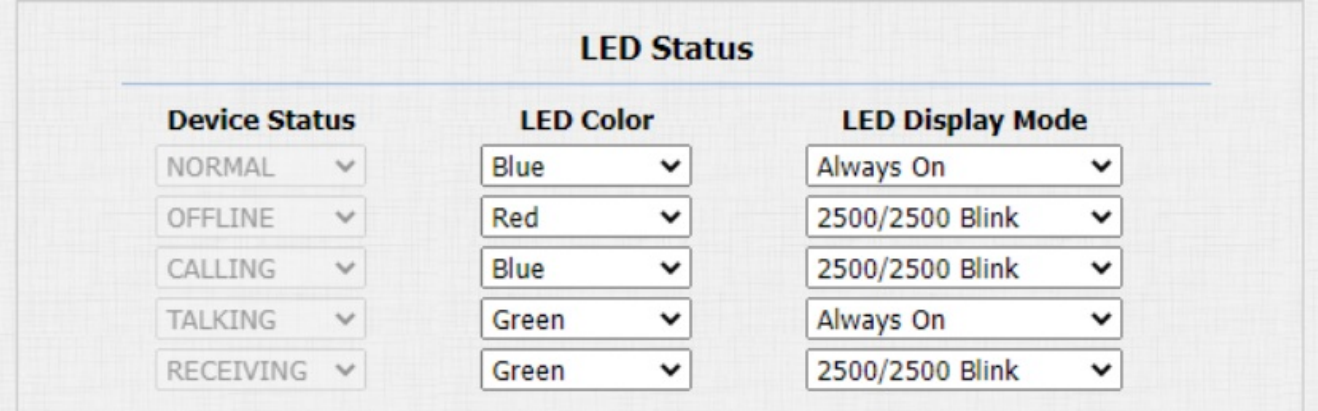
Parameter Set-up:

- **Mode**: **Auto** enables the LED light to be turned on automatically. **Schedule** turns on the LED according to the time schedule.
- **Min/Max Photoresistor**: set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the ON-OFF of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. The minimum and maximum photoresistor value are from 0 to 1800 respectively.

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 on the web **Intercom > LED Setting > LED Status** interface.



The default LED Display Status:

LED Status		Description	
Blue	Always on	Normal status	
	Flashing	Calling	
Red	Flashing	Network is unavailable	
Green	Always on	Talking on a call	
	Flashing	Receiving a call	
Pink	Flashing	Upgrading	

Parameters Set-up:

- **State**: there are five states: **Normal, Offline, Calling, Talking** and **Receiving**.
- **LED Color**: it can support three colors: **Red, Green, Blue**.
- **LED Display Mode**: the different blink frequencies.

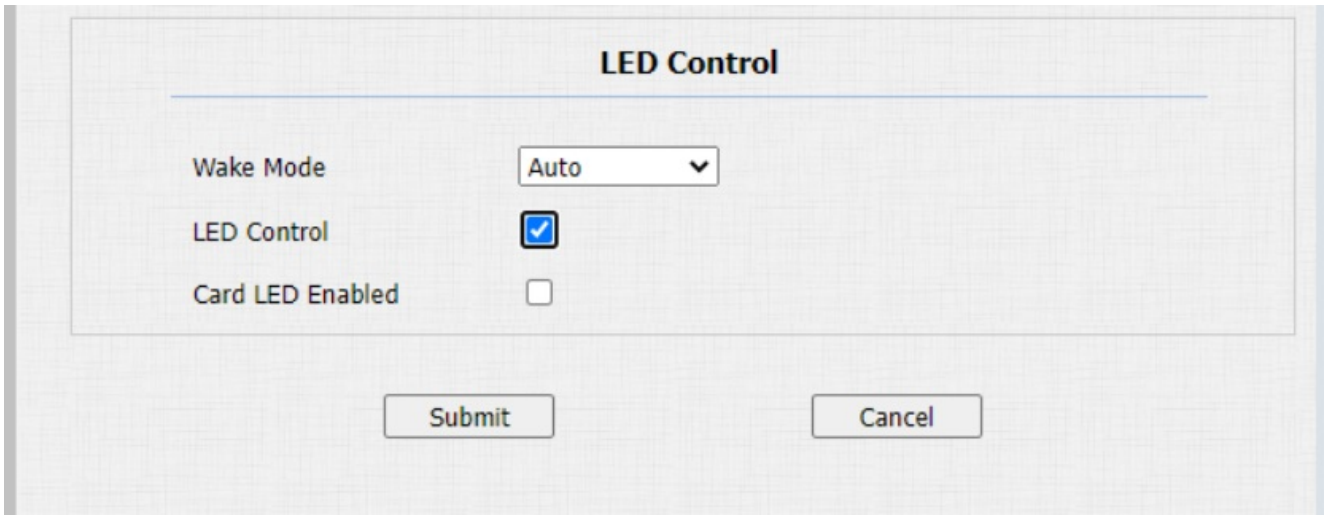
Note:

- The Status and Color of item cannot be changed.
- The LED of upgrading mode cannot be adjusted.

Set up LED Display from HTTP URL

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

Navigate to the web **Intercom > LED Setting > LED Control** to enable the function.



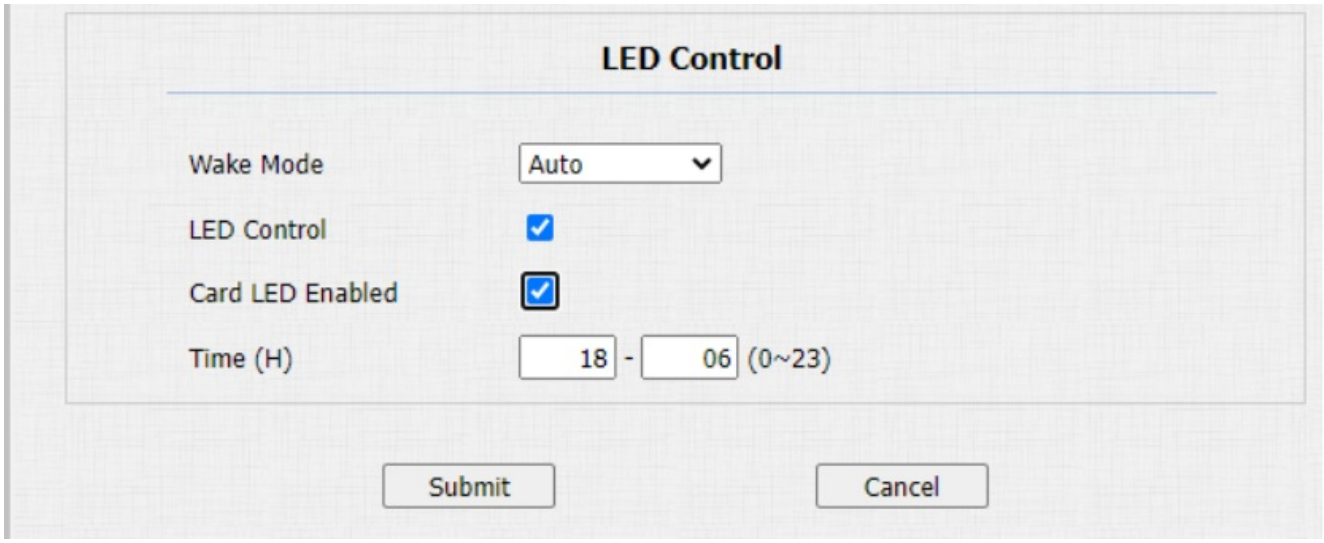
The HTTP URL format is: **http://PhoneIP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500**

- **Status**: 1=Idle; 2=OffLine; 3=Calling; 4=Talking; 5=Receiving; Color: 1=Green; 2=Blue; 3=Red; Mode: 0=Always On; 1=Always Off; 500/1000/1500/2000/25000/3000

LED Setting on Card Reader Area

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

Navigate to the web **Intercom > LED Setting > LED Control** interface.



Parameters Set-up:

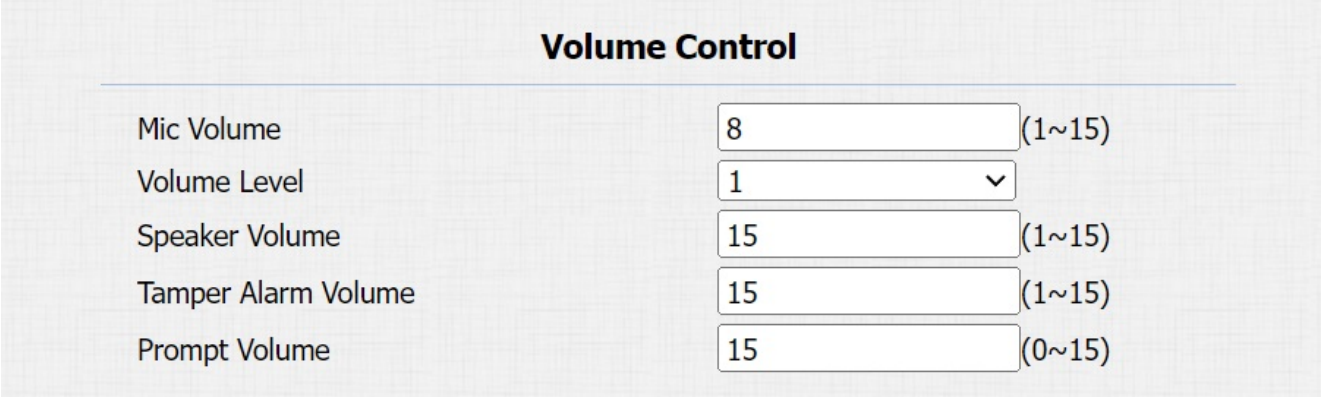
- **Time (H)**: the time span for the LED lighting to be valid. If the time span is set from **8-0 (Sart time- End time)**, it means LED light will stay on during the time span from **8:00** am to **12:00** pm during one day (24 hours).

Volume and Tone Configuration

Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

Navigate to the web **Phone > Audio > Volume Control** interface.

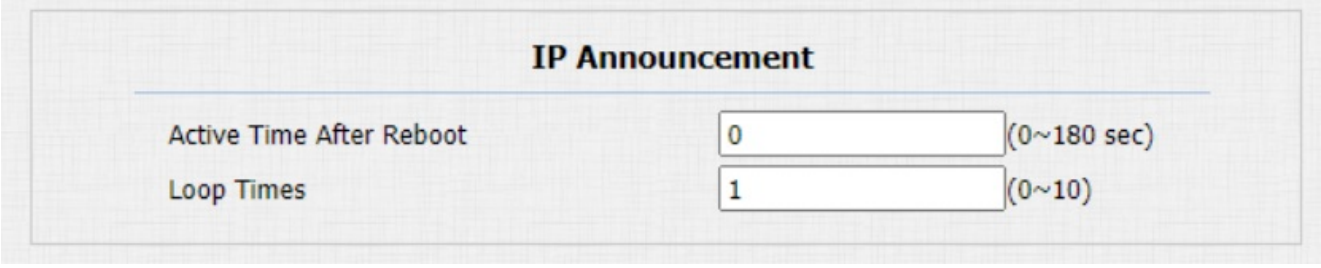


Parameter Set-up:

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

IP Announcement

Navigate to the web **Phone > Audio > IP announcement** interface.

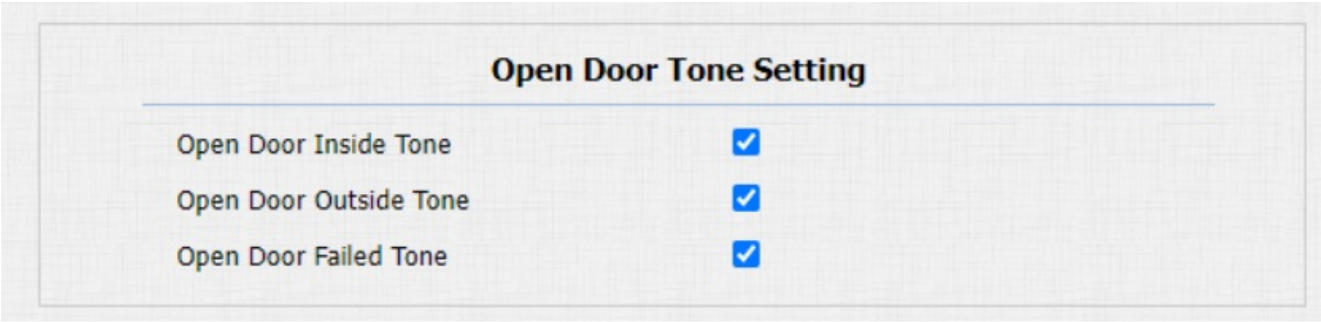


Parameter Set-up:

- **Active Time After Reboot**: the IP announcement time after the device reboot. If you set it as 30 seconds, then you must press the call button within 30 seconds for the IP announcement after the device is rebooted, otherwise, the IP announcement will expire. If you set it as 0 seconds, then you can press the call button any time after the reboot for the IP announcement.

Open Door Tone Configuration

You can control the prompt words that accompanies the tone on the web **Phone > Audio > Open Door Tone Setting** interface.



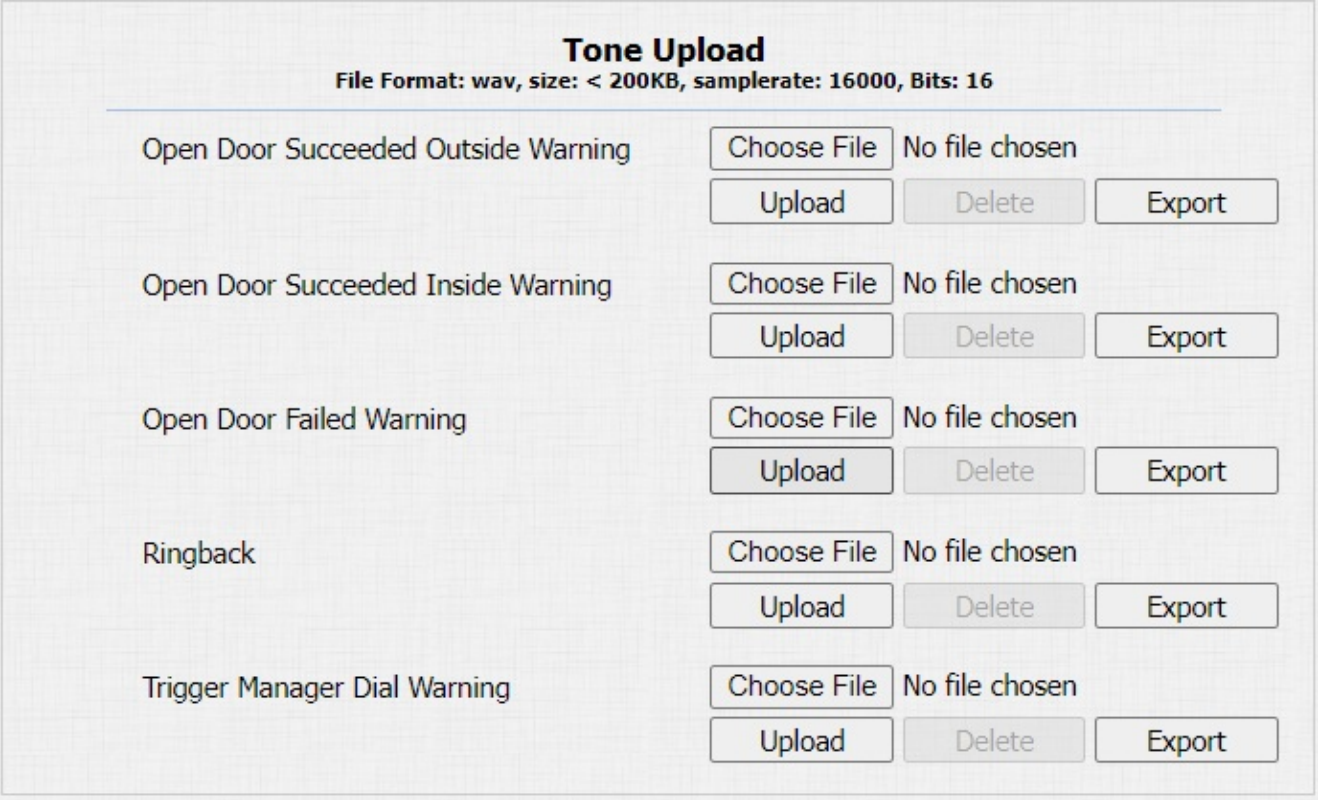
Parameter Set-up:

- **Open Door Inside Tone**: allows users to hear the open door tone when they open the door by pressing the exit button.
- **Open Door Outside Tone**: allows users to hear the open door tone when they open the door using the access methods supported by the door phone.

Upload Tone Files

Upload Ringback Tone

Navigate to the web **Phone > Audio > Tone Upload** interface.

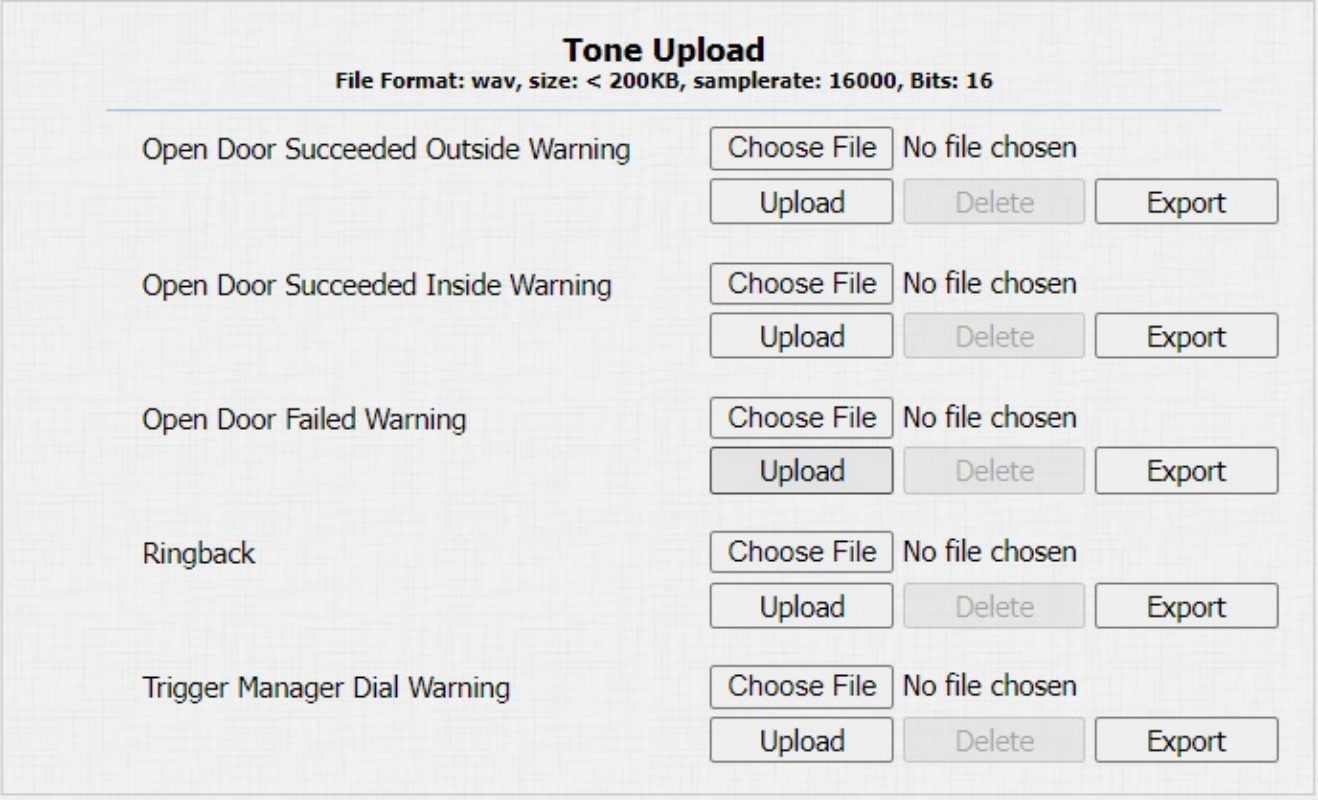


Upload Open Door Tone

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

The outside tone is heard when users open doors via card or DTMF. The inside tone is heard when users open doors via triggered input interface. Please follow the prompt about the file size and format.

Navigate to the web **Phone > Audio > Tone Upload** interface.



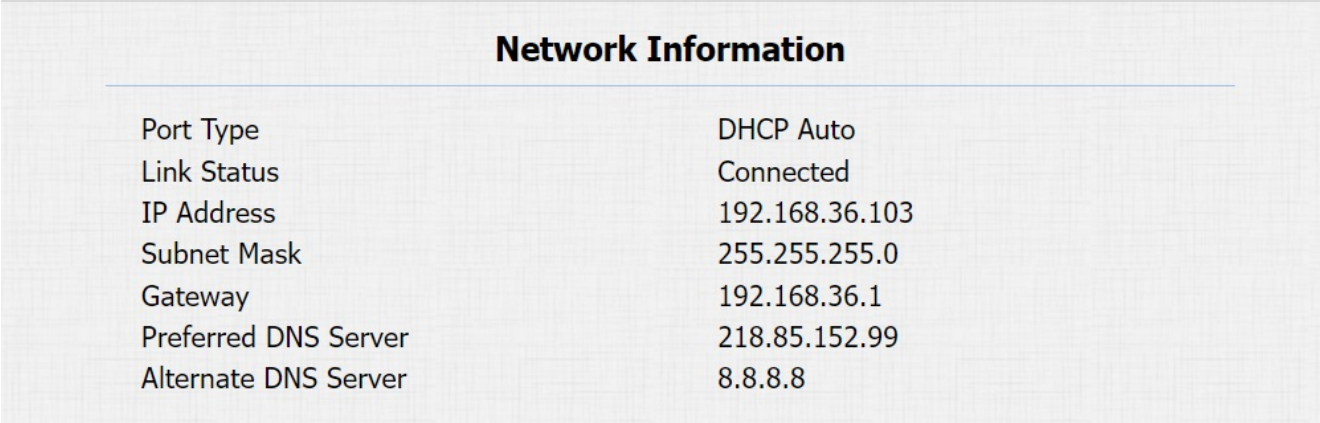
Parameter Set-up:

- **Open Door Succeeded Outside Warning**: warning tone that will go off when users open the door by pressing the exit button.
- **Open Door Succeeded Inside Warning**: warning tone that will go off when they open the door using the access methods supported by the door phone.
- **Trigger Manager Dial Warning**: warning tone that will go off when users press the push button to make group call or sequence call.

Network Setting

Network Status

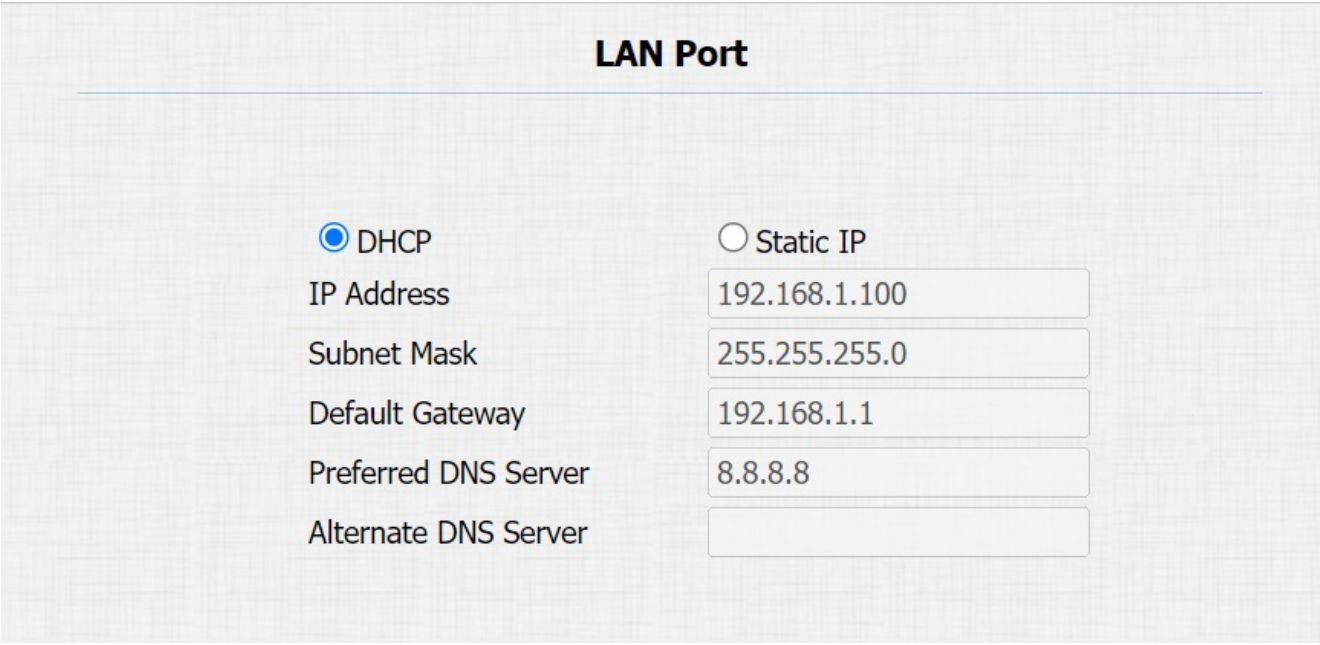
To check the network status on the web **Status > Basic > Network Information** interface.



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.

Navigate to the web **Network > Basic** interface



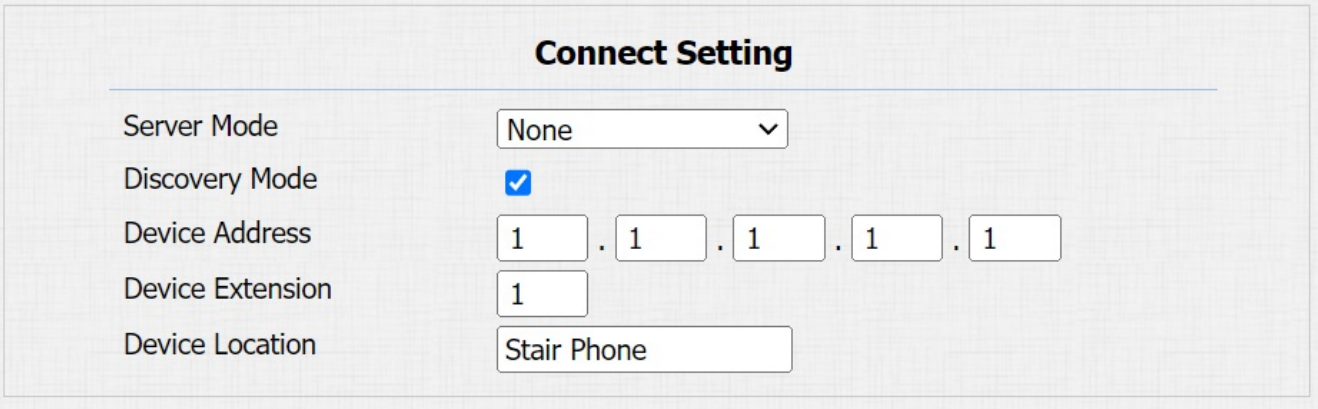
Parameter Set-up:

- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway and DNS server address automatically.
- **Static IP**: when static IP mode is selected, the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to the actual network environment.
- **IP Address**: enter the IP address when the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to the actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **Preferred/Alternate DNS Server**: preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary one. The door phone will connect to the alternate server when the primary one 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.

Navigate to the web **Network > Advanced > Connect Setting** interface.



Parameter Set-up:

- **Server Mode**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type, therefore, you are allowed to choose Cloud or SMDC in discovery mode.

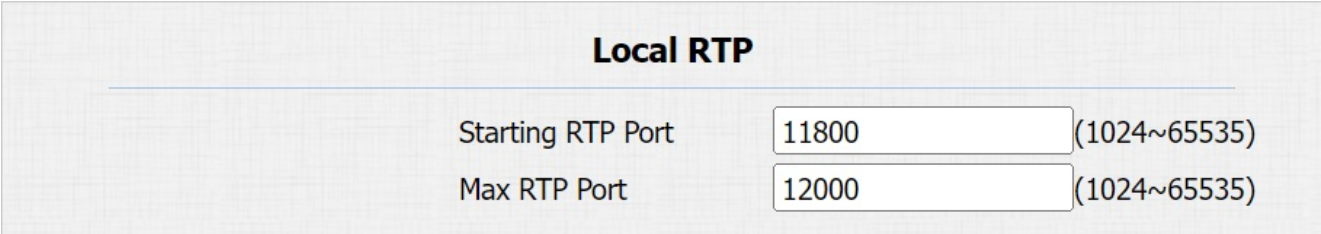
- **Discovery Mode**: allows the device to be discovered by other devices in the network. By disabling it, the device will be concealed and not to be discovered by other devices.
- **Device Address**: specifies the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
- **Device Extension**: the device extension number for the device you installed.
- **Device Location**: the location in which the device is installed and used.

Device Local RTP configuration

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

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

Navigate to the web **Network > Advanced > Local RTP** interface.



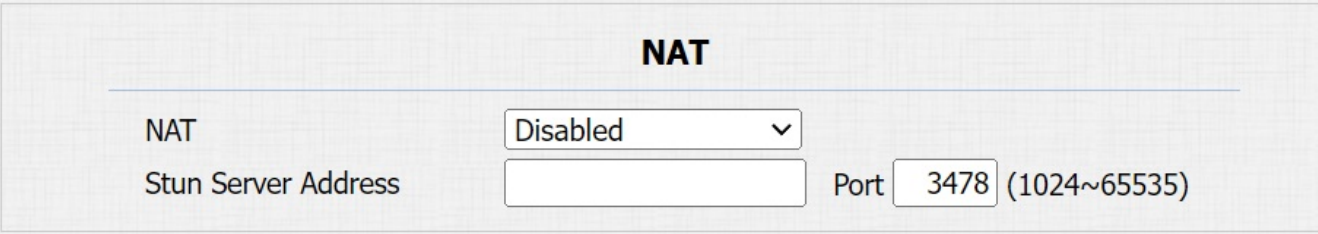
Parameter Set-up:

- **Min 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 end point for the exclusive data transmission range.

NAT Setting

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

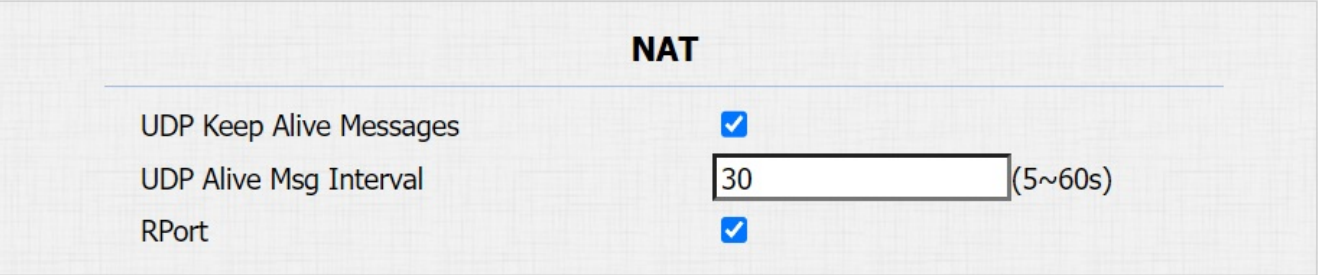
To set up NAT, navigate to the web **Account > Basic > NAT** interface.



Parameter Set-up:

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

Then go to the web **Account > Advanced > NAT** interface.



Parameter Set-up:

- **UDP Keep Alive Messages**: if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive 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).

Navigate to the web **Network > Advanced > SNMP** interface.

Parameter Set-up:

- **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.

Navigate to the web **Network > Advanced > VLAN** interface.

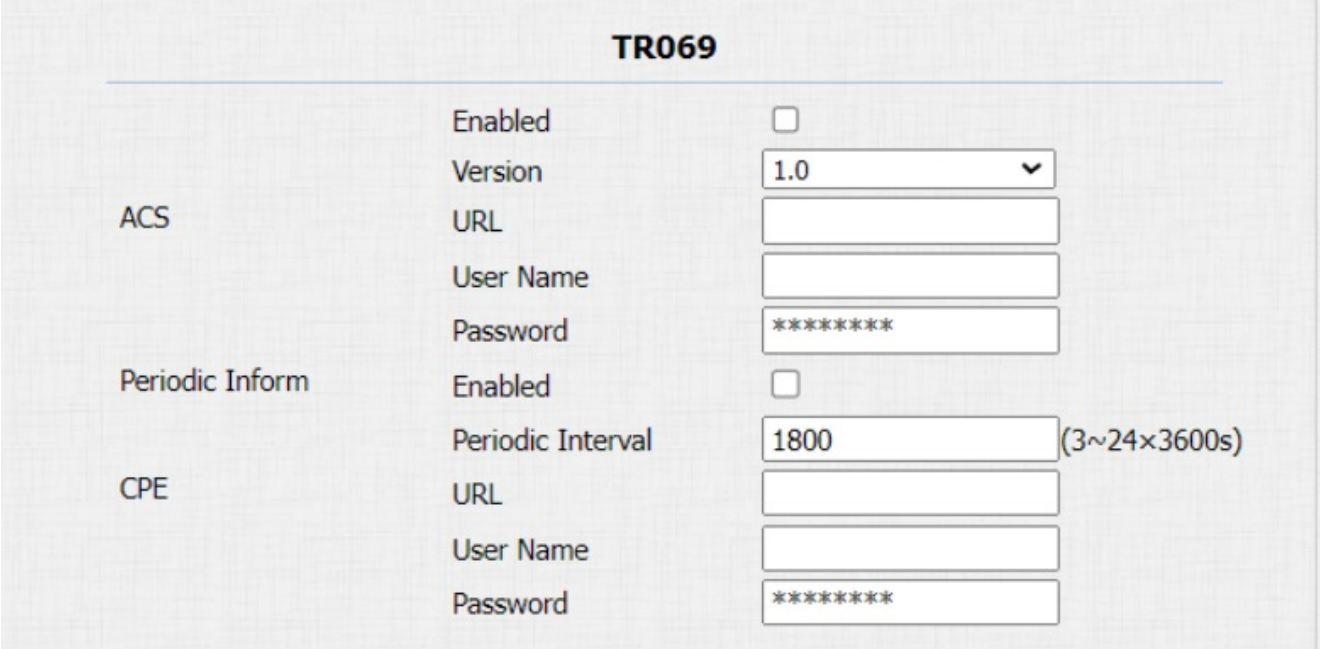
Parameter Set-up:

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

Navigate to the web **Network > Advanced > TR069** interface.



Parameter Set-up:

- **Version**: to select 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 address for ACS or CPE.
- **Periodic Interval**: the interval for periodic inform.

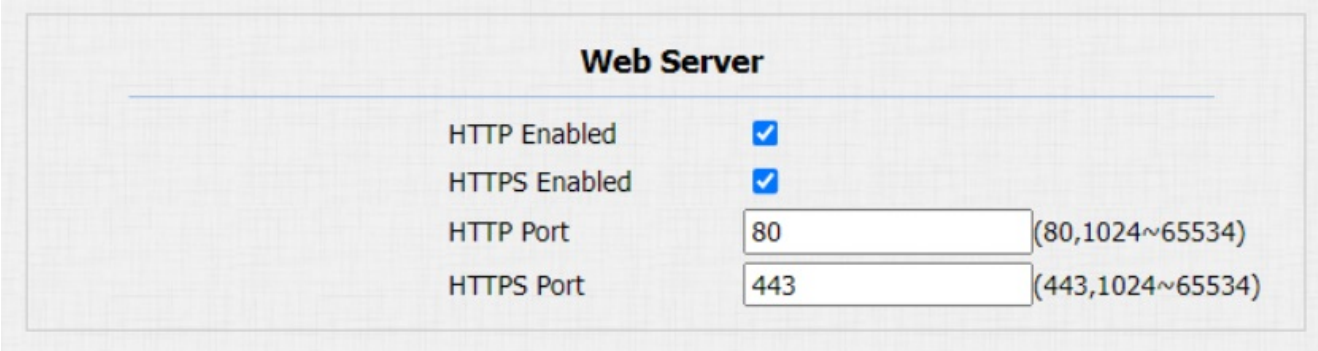
Note

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

Device Web HTTP Setting

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

Navigate to the web **Network > Advanced > Web Server** interface.



Intercom Call Configuration

IP Call & IP Call Configuration

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

Navigate to the web **Phone > Call Feature > Direct IP** interface.

SIP Call & SIP Call Configuration

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

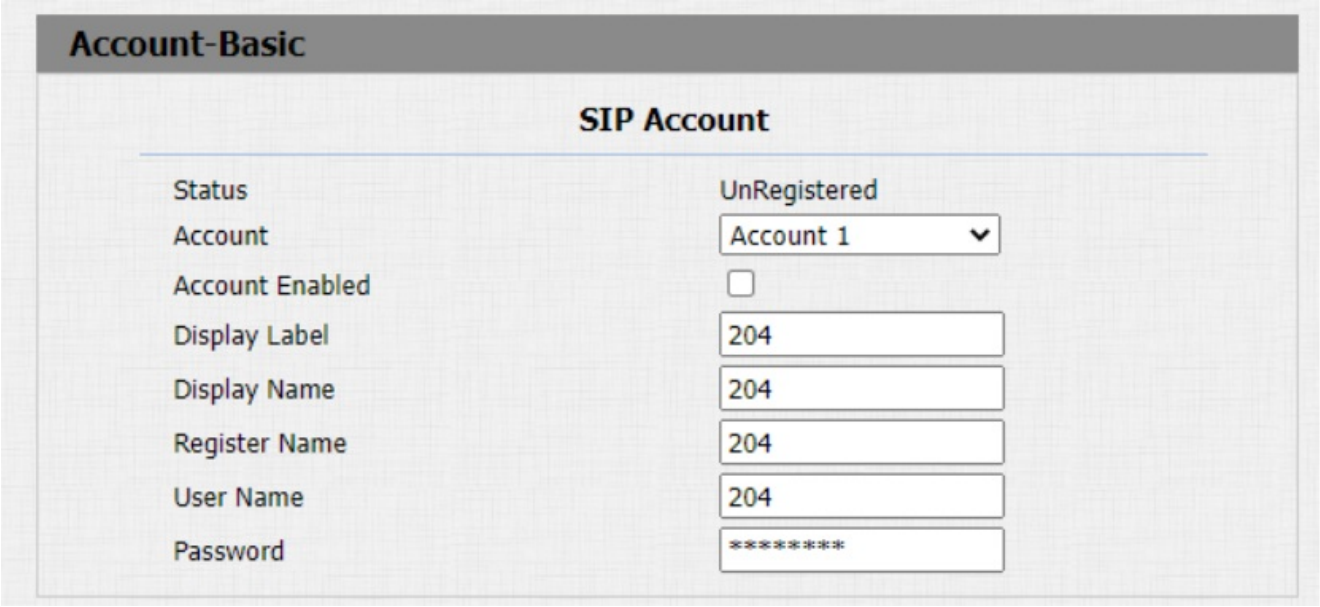
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Account Registration

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

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

Navigate to the web **Account > Basic > SIP Account** Interface.



Parameter Set-up:

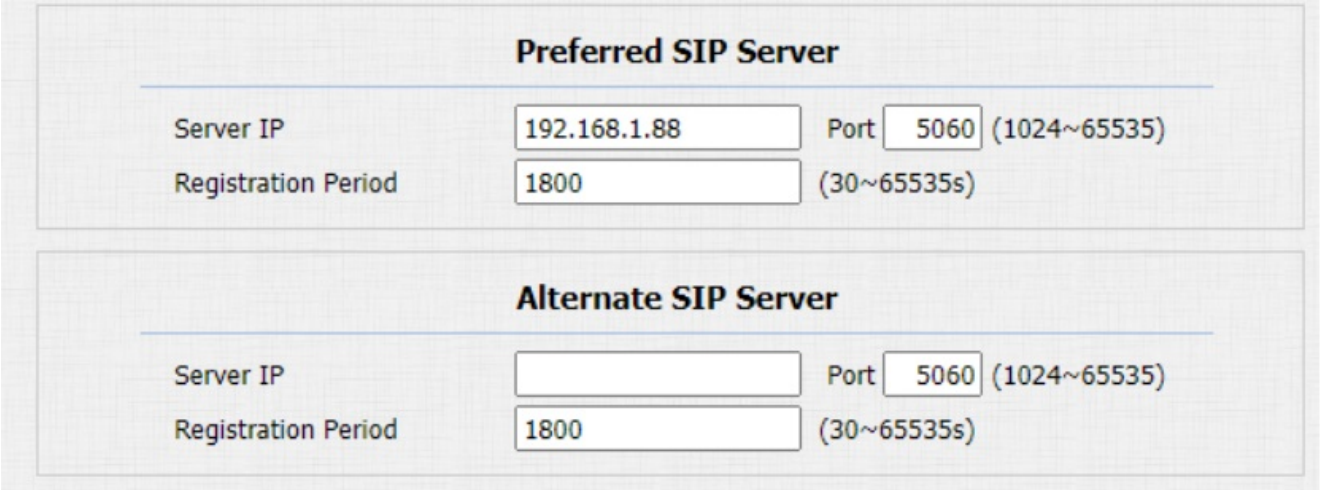
- **Display Label**: the device label to be shown on the device screen.
- **Display Name**: the device's name to be shown on the device being called to.

a. To register SIP account for Akuvox indoor monitors, obtain Register Name, Username, and Password from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain Register Name, Username, and Password from third-party service provider.

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.

Navigate to the web **Account > Basic > SIP Server** interface.



a. To register SIP account for Akuvox indoor monitors, obtain Server IP and Server Port from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain Server IP and Server Port from third-party service provider.

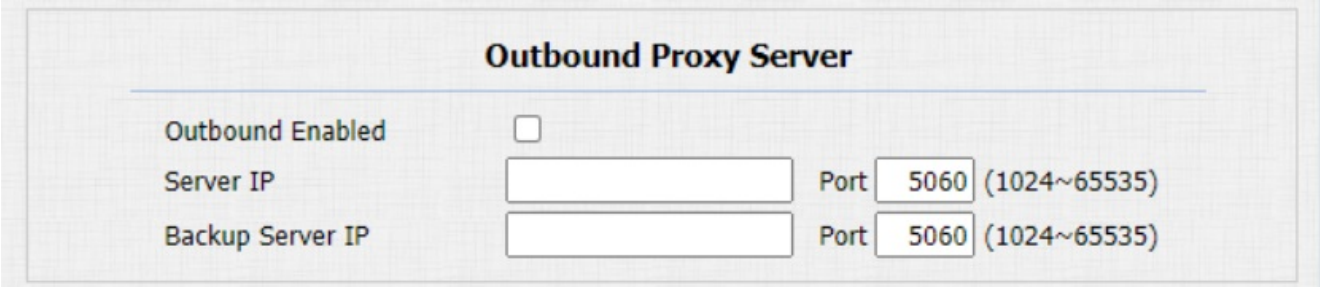
Parameter Set-up:

- **Preferred SIP Server**: the primary server IP address or its URL.
- **Alternate SIP Server**: the backup SIP server IP address or its URL.
- **Port**: the SIP server port for data transmission.
- **Registration Period**: the SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The registration period ranges **30-65535s** with **1800** default.

Configure Outbound Proxy Server

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

Navigate to the web **Account > Basic > Outbound Proxy Server** Interface.



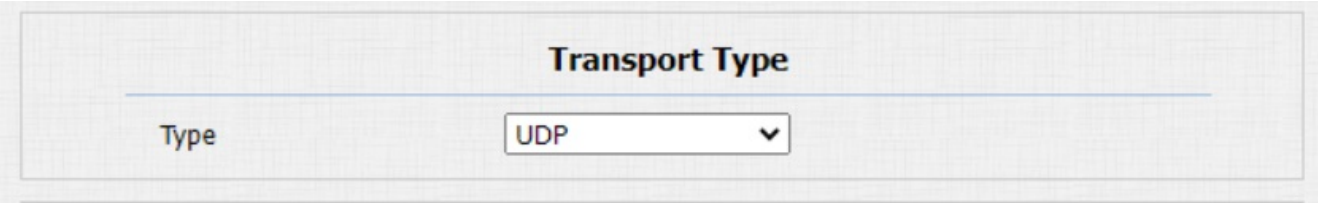
Parameter Set-up:

- **Server IP**: the SIP address of the outbound proxy server.
- **Port**: the Port number for establishing a call session via the outbound proxy server.

Configure Data Transmission Type

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

Navigate to the web **Account > Basic > Transport Type** interface.



Parameter Set-up:

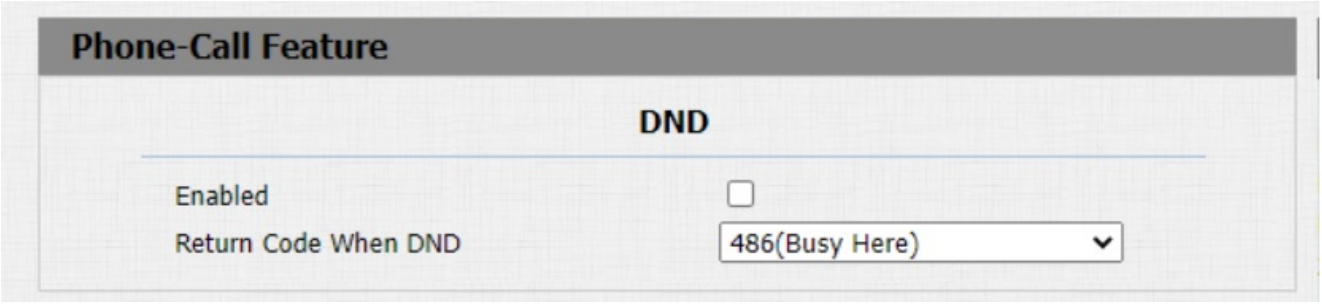
- **UDP**: an unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: a reliable but less-efficient transport layer protocol.
- **TLS**: a secured and reliable transport layer protocol.
- **DNS-SRV**: obtains DNS record for specifying the location of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

Call Settings

DND

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

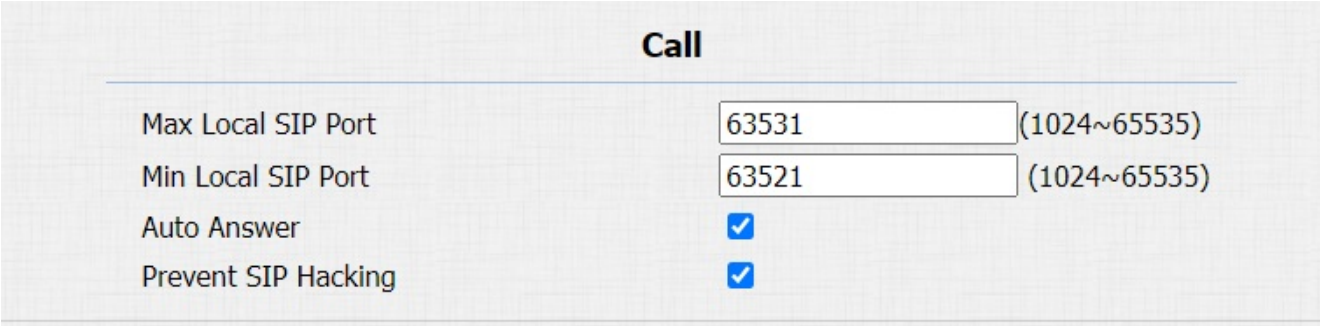
Navigate to the web **Phone > Call Feature** interface



Prevent SIP Hacking

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

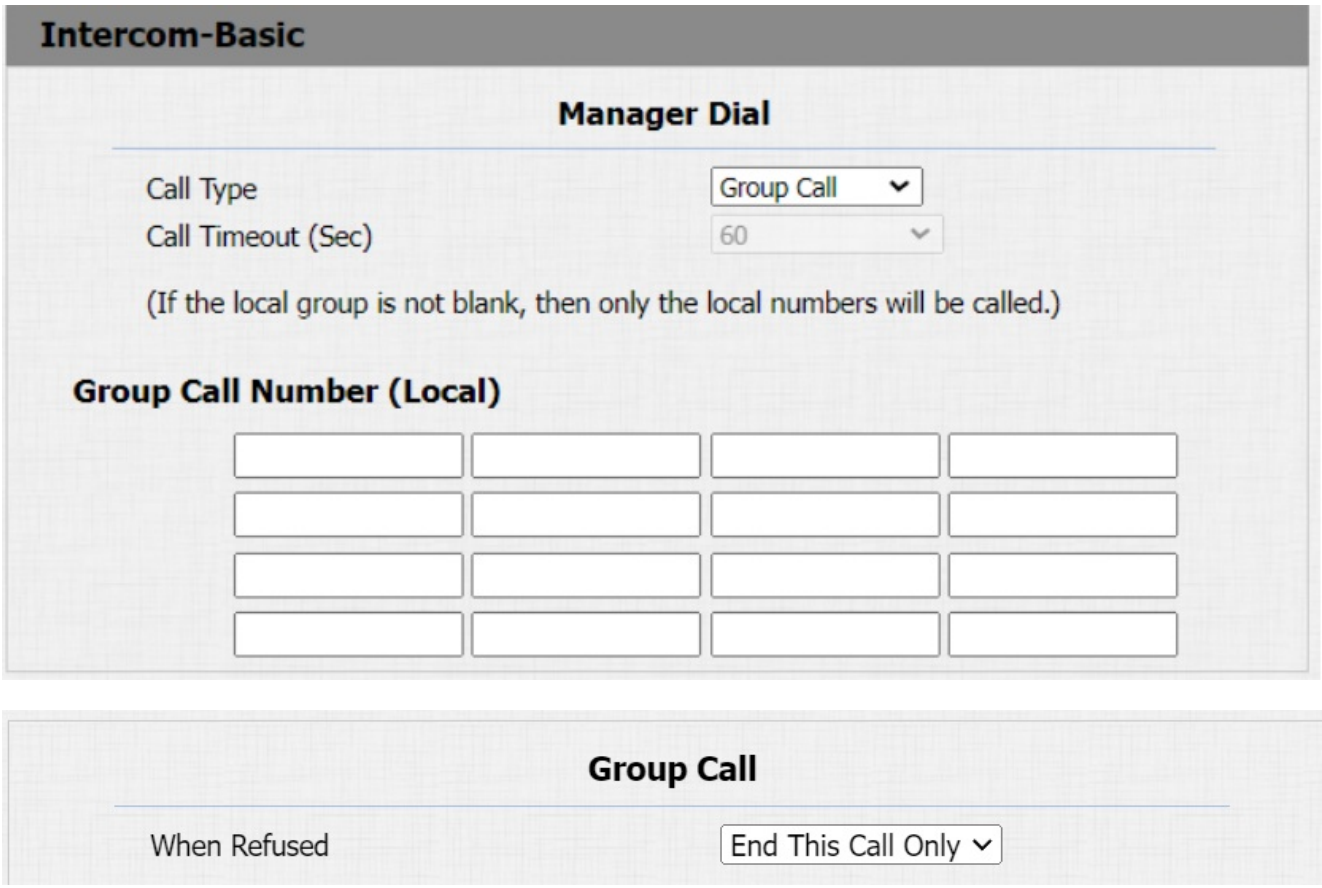
Navigate to the web **Account > Advanced > Call** interface.



Manager Dial Call

Manager Dial Call includes two types of calls: Sequence call and group call. It allows quick initiation of pre-configured numbers by pressing the Management key on the door phone.

Navigate to the web **Intercom > Basic > Manager Dial** interface.



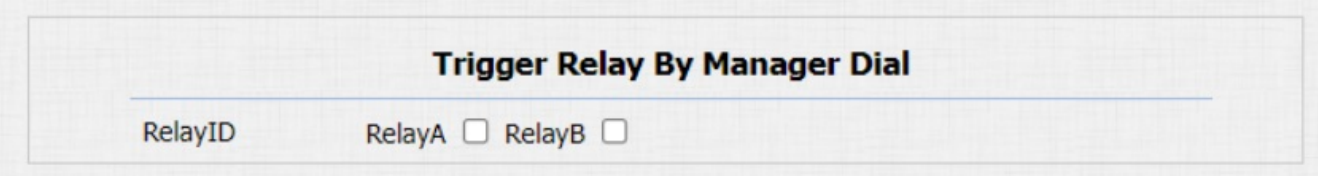
Parameter Set-up:

- **Call Type**: select the group call or sequence call (Robin call) for the manager dial call.
- **Sequence Call**: sequence call is used to initiate multiple numbers when your press the manager dial button. If the previous callee does not answer within the sequence call timeout, the call will be transferred to the next one. If the call is answered by one of the callees, the call will not be transferred.
- **When Refused**: if you select **End All Calls**, the sequence call will be terminated if the call is rejected by the called party. If you select **End This Call Only**, the sequence call will be continued to the next called party if it is rejected by the first called party.
- **Group Call**: group call is used to initiate calls to multiple numbers at the same when you press the manager dial button.

> **Note**
>
> Sequence call works with SmartPlus Cloud.

After the manager dial is set up, you can set up relays to be triggered by pressing the manager dial key.

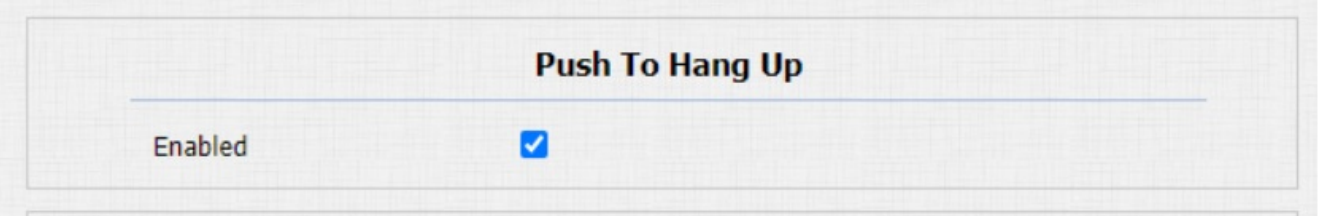
Scroll down to the **Trigger Relay By Manager Dial** section.



Call Hang-up

Press the push button to hang up a call.

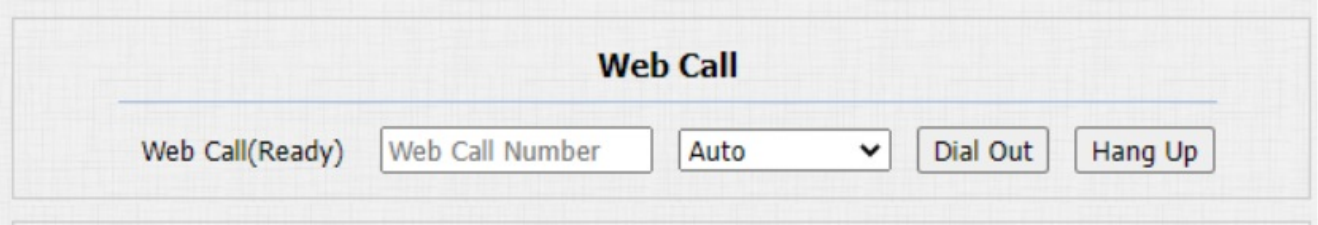
Navigate to the web **Intercom > Basic > Push To Hang Up** interface.



Web Call

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

Navigate to web **Intercom > Basic > Web Call** interface.



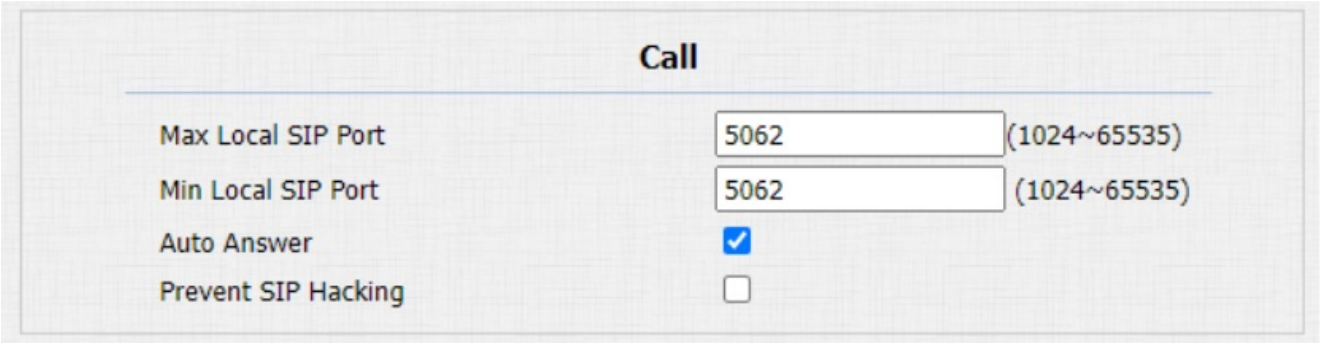
Parameters Set-up:

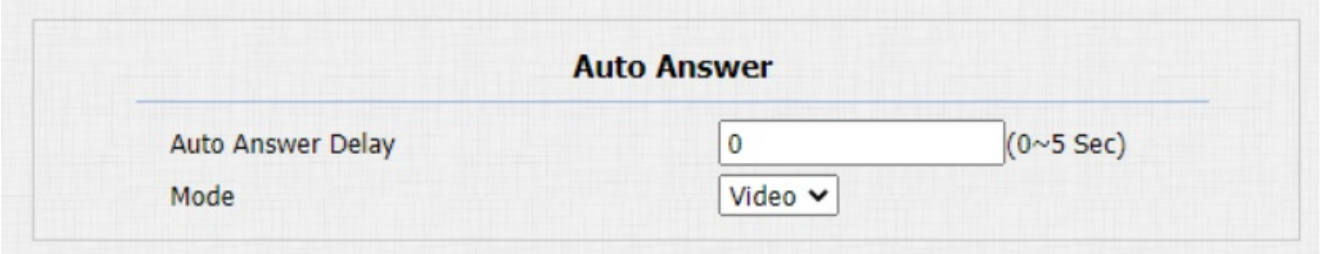
Web Call (Ready): the called IP/SIP number.

Auto Answer

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

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





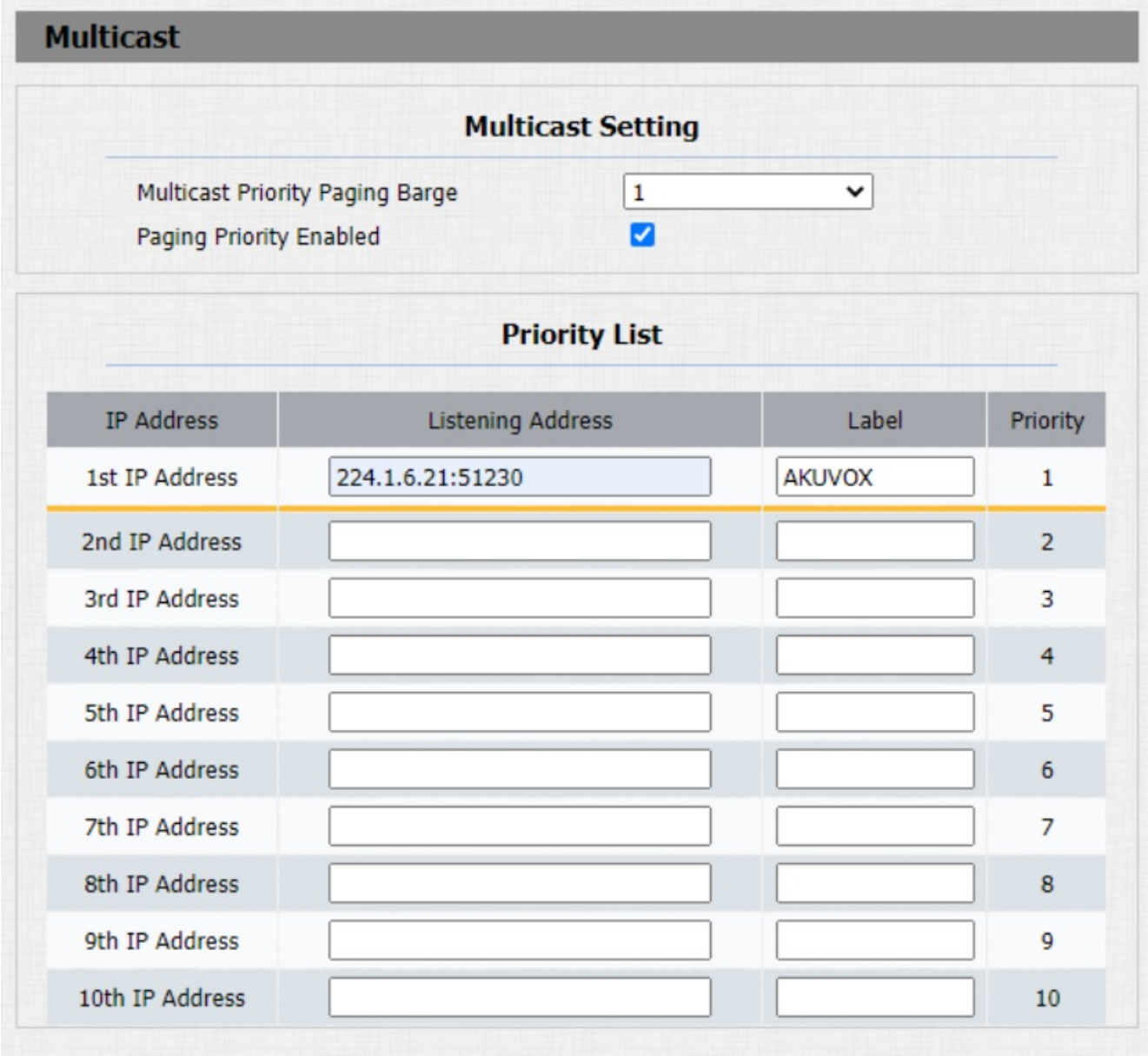
Parameters Set-up:

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

Multicast

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

Navigate to the web **Phone > Multicast** interface.



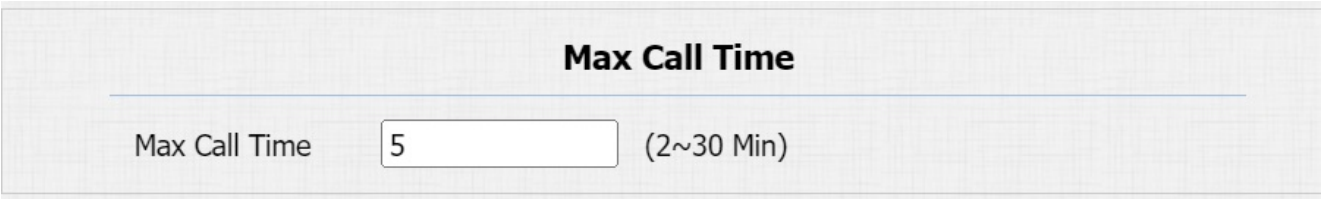
Parameters Set-up:

- **Multicast Priority Paging Barge**: multicast or how many multicast calls are higher priority than SIP call, if you disable Paging Priority Active, SIP call will have high priority.
- **Paging Priority enabled**: multicast calls are called in order of priority or not.
- **Listening Address**: the multicast IP address to be listened. The multicast IP address needs to be the same as the listened part 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.

Configure Maximum Call Duration

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

Navigate to the web **Intercom > Basic > Max Call Time** interface.



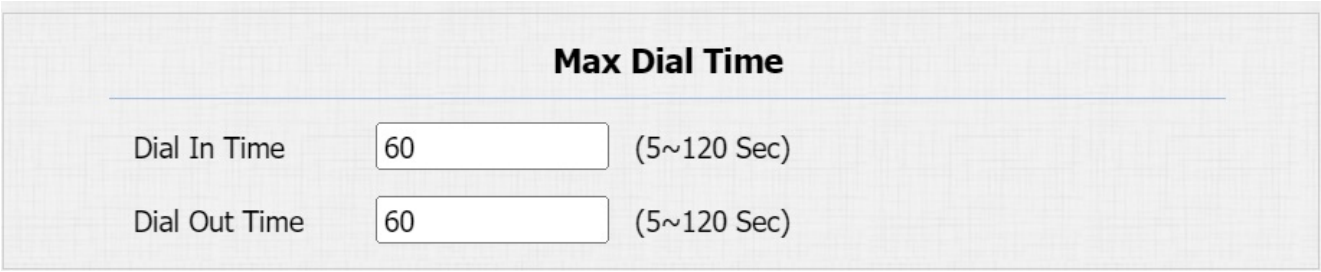
Note

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

Maximum Dial Duration

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

Navigate to the web **Intercom > Basic > Max Dial Time** interface.



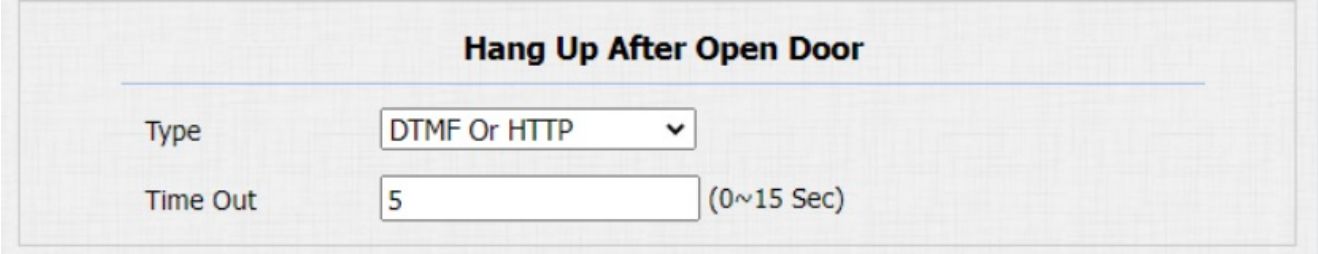
Note

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

Hang Up After Open Door

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

Navigate to the web **Intercom > Basic > Hang Up After Open Door** interface.



Parameter Set-up:

- **Type**: the door can be opened via **DTMF, HTTP Command, DTMF Or HTTP**, and **Input, DTMF Or HTTP**.
- **Timeout**: the call will be automatically hang up within this value after the door is opened.

Contacts Configuration

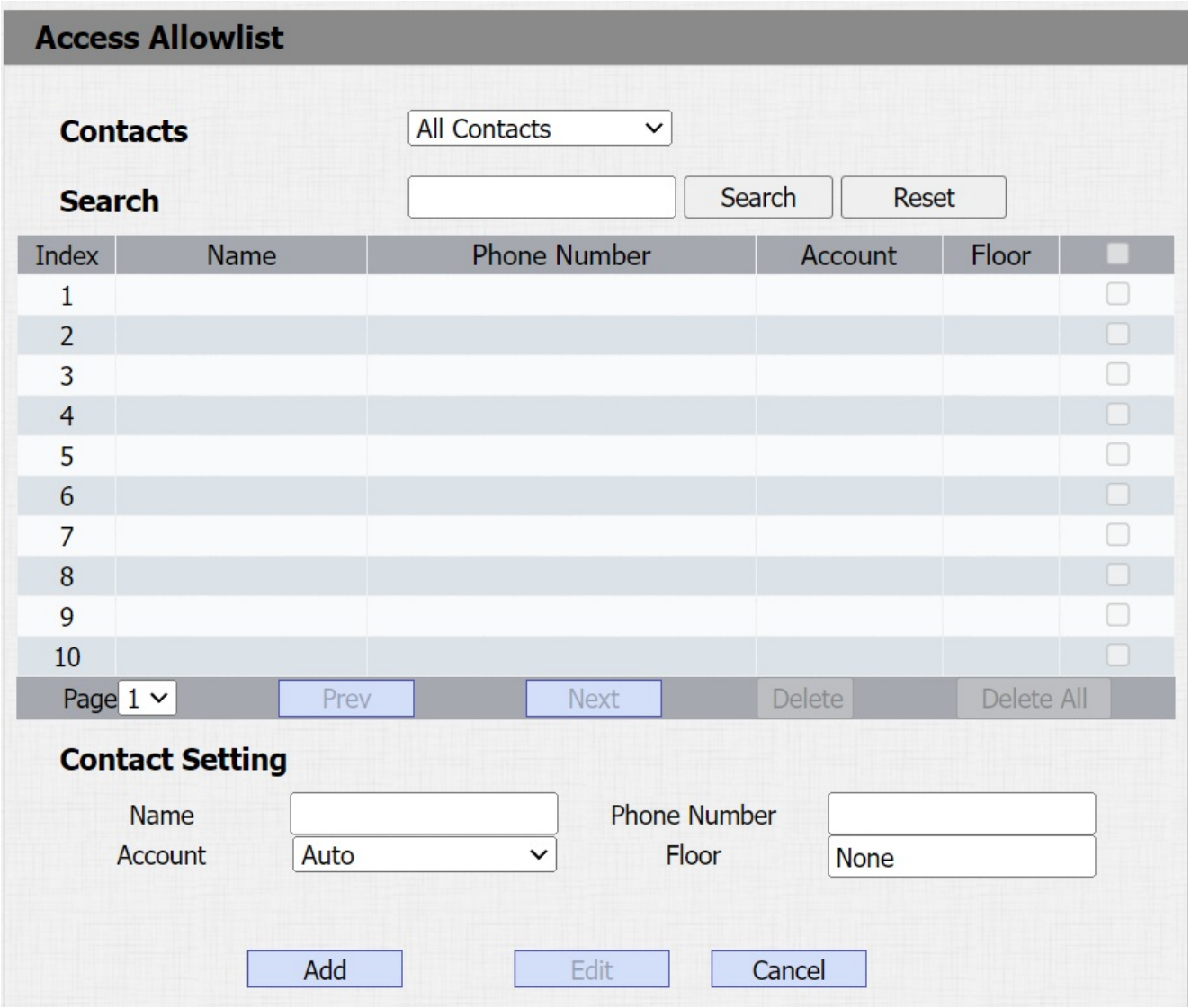
The contacts list is for granting access or calling permission to the indoor monitor or other devices.

To set it up on the web **Contacts > Access Allowlist** interface.

Manage Contacts

You can search, display, edit, and delete the contacts in your contacts list on the web.

Navigate to the web **Contacts > Access Allowlist**.



Parameters Set-up:

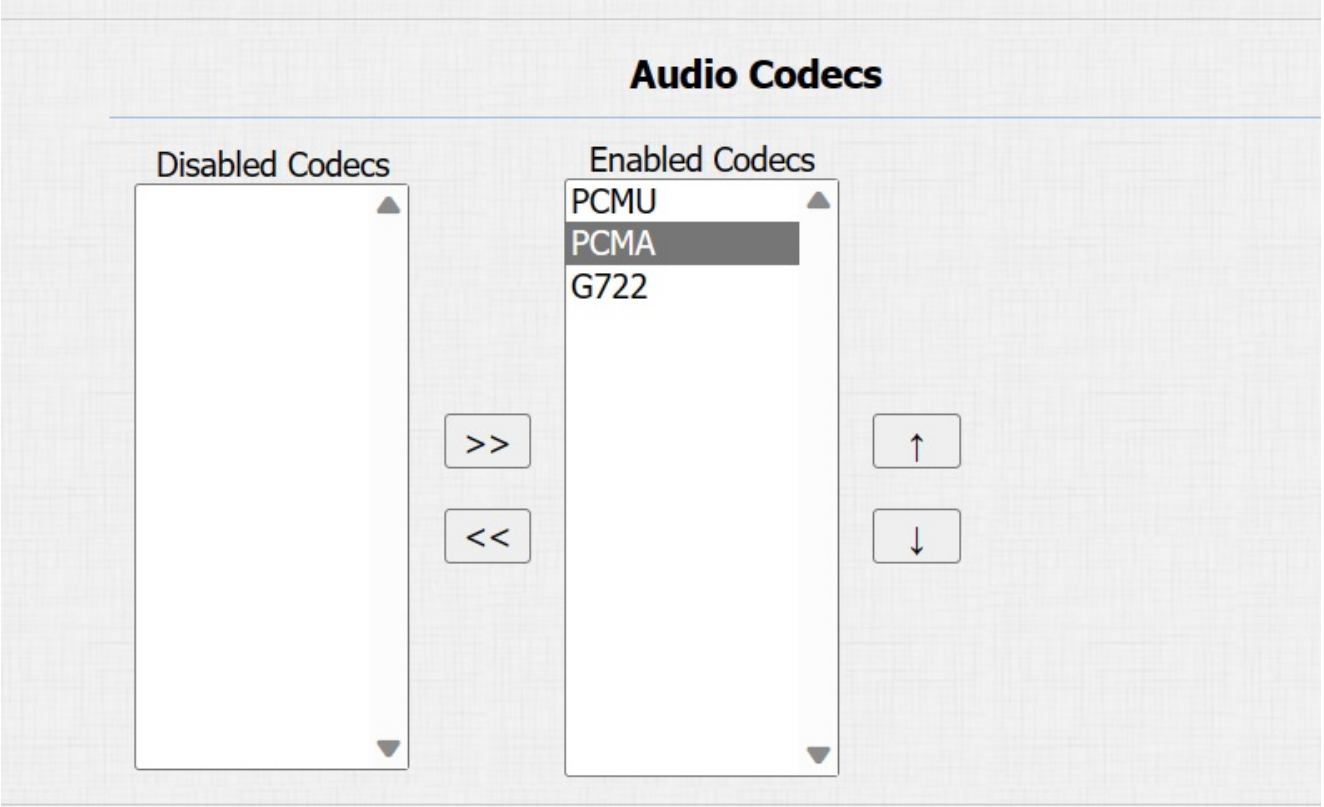
- **Account**: the registered SIP account to make a call. If using IP direct call, it is not available.
- **Floor**: the floor number that the contact is allowed to access.

Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

The door phone supports three types of Codec (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each 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.

Navigate to the web **Account > Advanced** interface.



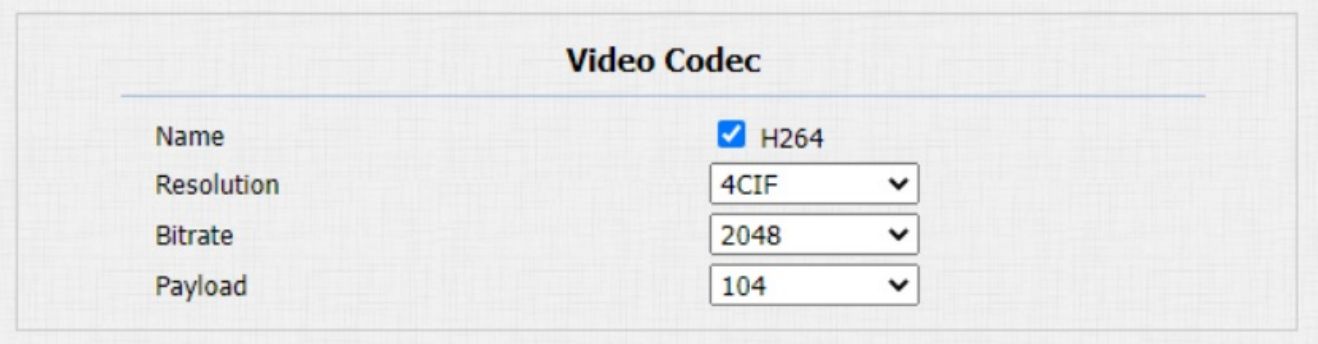
Please refers to the bandwidth consumption and sample rate for the three codecs types below:

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

Video Codec Configuration

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

Navigate to the web **Account > Advanced** interface.



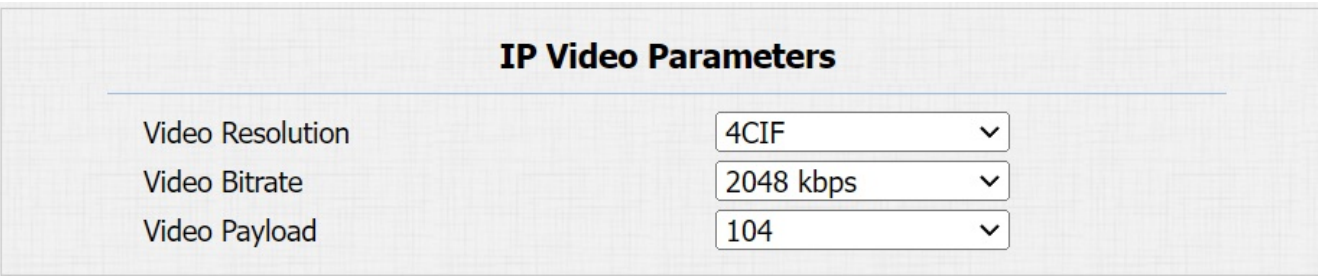
Parameter Set-up:

- **Name**: check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Resolution**: the video quality resolution has four option, **CIF, VGA, 4CIF** and **720P** according to the actual network environment. The default resolution is **4CIF**.
- **Bitrate**: the video stream bitrate ranges from 128 to 2048. The greater the bitrate, the data transmitted in every second is greater in amount, therefore, the clearer the video will be. The default code bitrate is 2048.
- **Payload**: the payload ranges from 90 to 119 for configuring the audio/video configuration file. The default payload is 104.

Video Codec Configuration for IP Direct Calls

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

Navigate to the web **Phone > Call Feature > IP Video Parameters** interface.



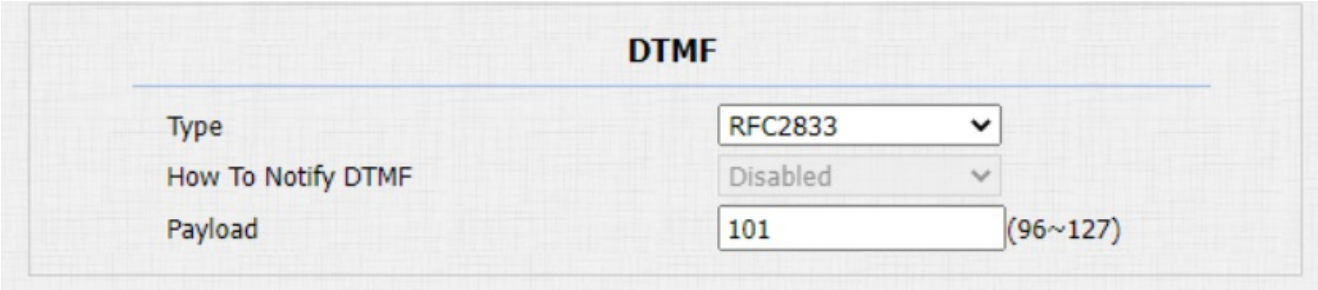
Parameter Set-up:

- **Video Resolution**: the video quality resolution has four option, **CIF, VGA, 4CIF** and **720P** according to the actual network environment. The default resolution is **4CIF**.
- **Video Bitrate**: the video stream bitrate ranges from 64 to 2048 kbps. The greater the bitrate, the data transmitted in every second is greater in amount, therefore, the clearer the video will be. The default code bitrate is 2048.
- **Video Payload**: the payload ranges from 90 to 119 for configuring the audio/video configuration file. The default payload is 104.

Configure DTMF Data Transmission

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

Navigate to the web **Account > Advanced > DTMF** interface.



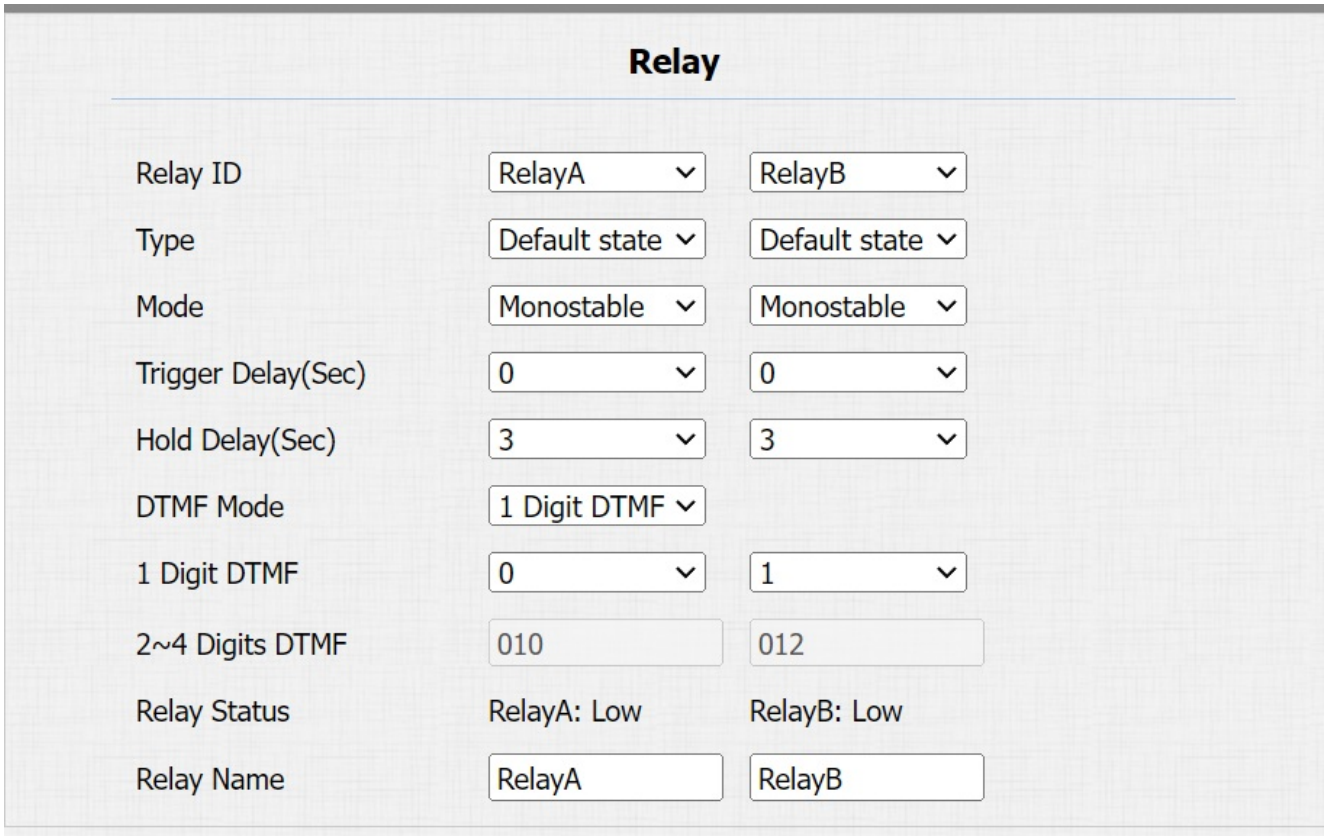
Parameter Set-up:

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

Relay Setting

Relay Switch Setting

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



Parameter Set-up:

- **Type**: when Default state is selected, the Relay Status shows Low which means the door is closed and the Relay Status shows High which means the door is opened. If Invert State is selected, the Relay Status shows High which means the door is closed and Low means the door is opened.
- **Mode**: there are two modes Monostable and Bistable. If Monostable is selected, the relay status will be automatically reset within the relay delay time after the relay is triggered. If Bistable is selected, relay status will be reset after the relay is triggered again.

- **Trigger Delay (Sec)**: the relay trigger delay time ranges from 1-10 seconds. If you set the delay time as 5 seconds, the relay will not be triggered until 5 seconds after you press the unlock tab.
- **Hold Delay (Sec)**: the relay hold delay time ranges from 1-10 seconds. If you set the hold delay time as 5 seconds, the relay will resume the initial state after maintaining the triggered state for 5s.
- **DTMF Mode**: the number of DTMF digits for the door access control (Ranging from 1-4 digits).
- **1 Digit DTMF**: select the code from *0-9 and ,# if the DTMF Option is set as 1 digit.
- **2~4 Digits DTMF**: set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMP Option** is set as 3-digits.
- **Relay Status**: relay status is low by default which means normally closed(NC). If the relay status is high, then it is in normally open status(NO).
- **Relay Name**: name the relay switch to distinguish it from others. You can name the relay switch according to where it is located for convenience.

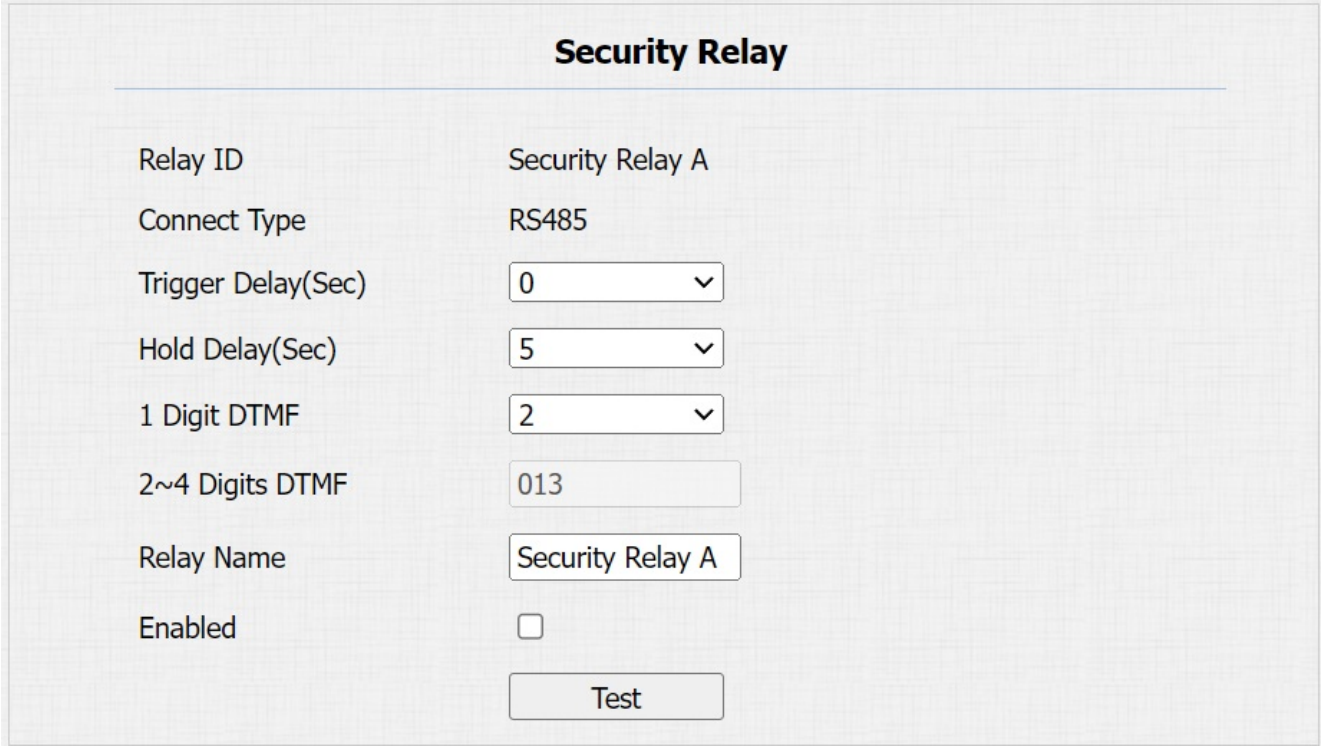
Tip

- Only the external devices connected to the relay switch need to be powered by power adapters as relay switch does not supply power.
- It is suggested to connect the door lock to **Relay B**.

Security Relay Setting

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

Navigate to the web **Intercom > Relay > Security Relay** interface.



Parameter Set-up:

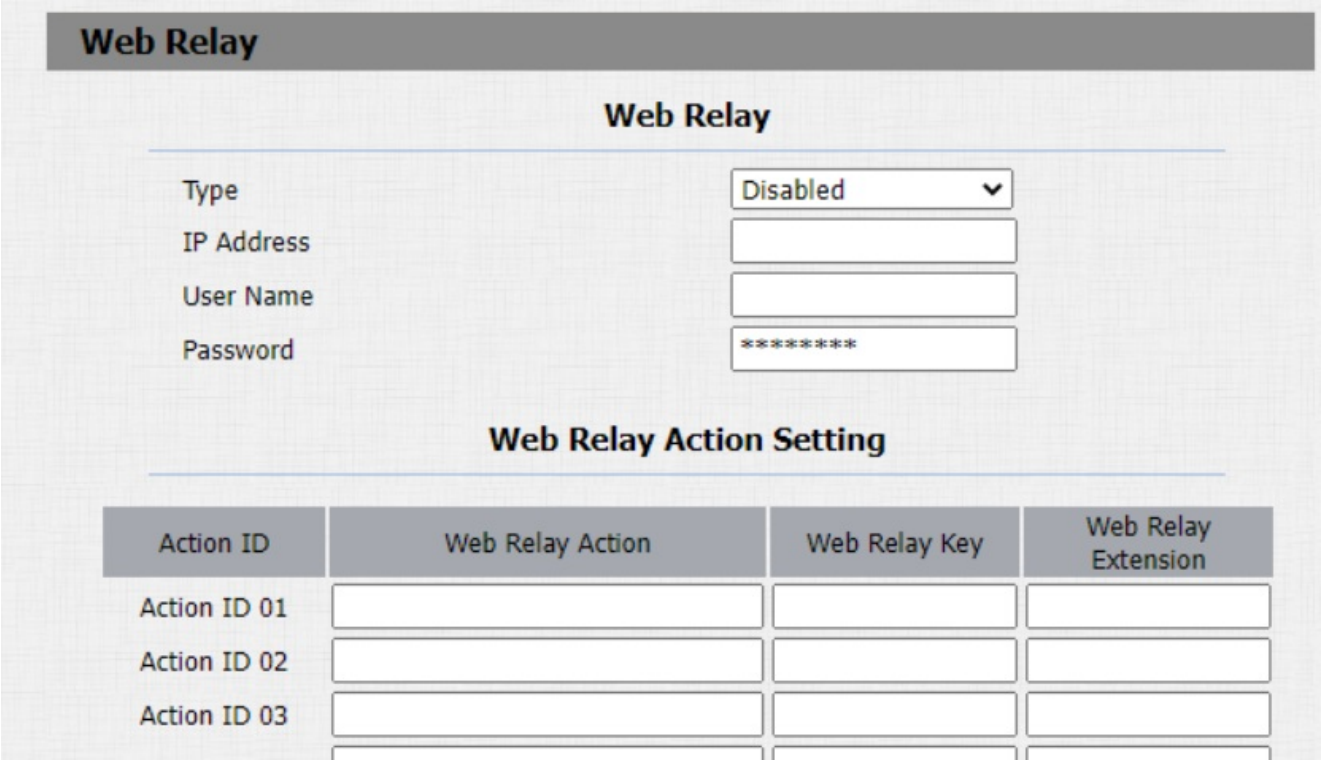
- **Connect Type**: the connection type between the security relay and the door phone.
- **Trigger Delay(Sec)**: the relay trigger delay time ranges from 0 to 10 seconds. If you set the delay time as 5 seconds, the relay will not be triggered until 5 seconds after you press the unlock tab. The default is 0 meaning triggering relay right after you press the unlock tab.
- **Hold Delay(Sec)**: the relay hold delay time ranges from 1 to 60 seconds. If you set the hold delay time as 5 seconds, the relay will be delayed for 5 seconds after the door is opened.
- **1 Digit DTMF**: set the 1 digit DTMF code from 0-9 and *, #.
- **2~4 Digits DTMF**: set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digit DTMF code if DTMP Mode is set as 3-digits.

- **Relay Name**: name the relay to distinguish it from others. It can be edited on the SmartPlus cloud and SDMC.

Web Relay Setting

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

Navigate to the web **Phone > Web Relay** interface. **IP Address**, **User Name**, and **Password** are provided by the web relay manufacturer.



Parameter Set-up:

- **Type**: **Web Relay** enables the feature. **Both** enables both local relay and web relay. The local relay has a higher priority.
- **Password**: the password is authenticated via HTTP and you can define the passwords using **http get** in Action.
- **Web Relay Action**: enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without adding IP, username, password, you can enter multiple HTTP commands in the web relay action field. See the HTTP command example below:

a. If you do not enter the IP address in the IP Address Field above, fill in a complete HTTP command.
For example, **http://admin:admin@192.168.1.2/state.xml?relayState=2**. (HTTP://@IP address>/state.xml?relayState=2)
b. If you have already entered the IP address above, fill in the omitted HTTP command, for example, **state.xml?relayState=2**.

- **Web Relay Key**: optional setting. When entering the configured DTMF code, the door can only be opened via DTMF code and RF cards.

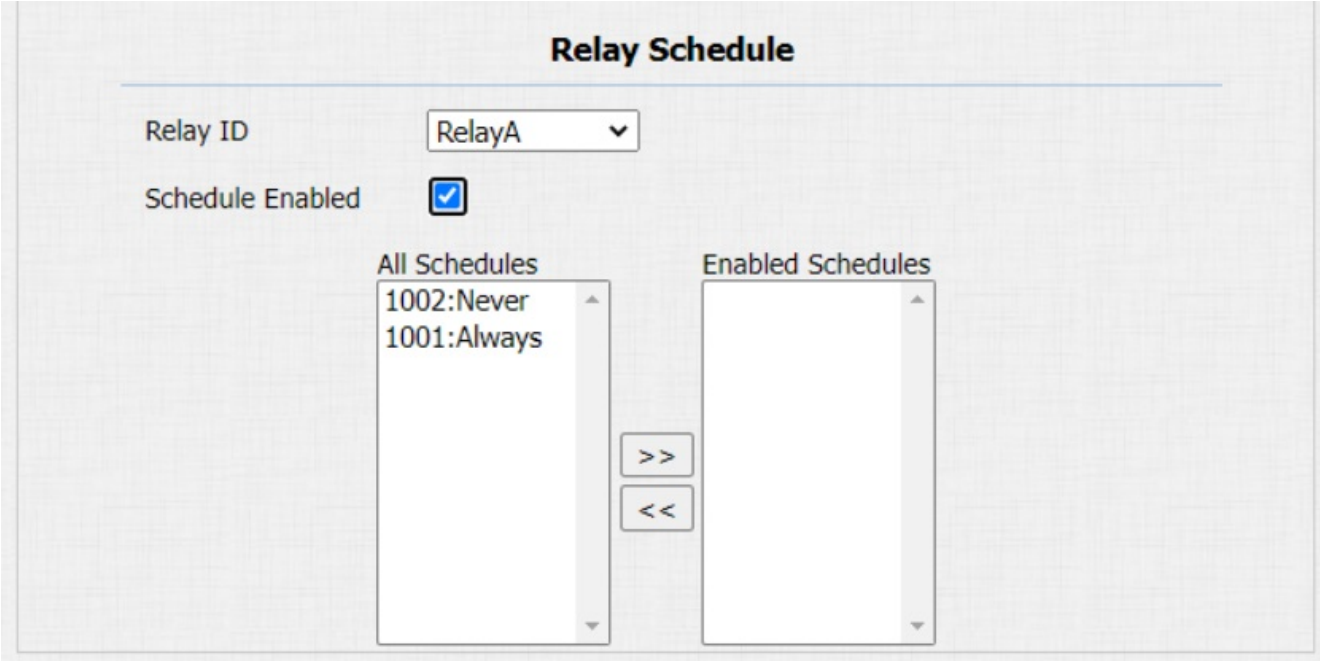
- **Web Relay Extension**: optional setting. When entering the SIP or IP number of an intercom device such as an indoor monitor, only the device can receive the web relay action command and trigger the web relay via DTMF code.

Door Access Schedule Management

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.

Navigate to the web **Intercom** > **Relay** > **Relay Schedule** interface.



Parameter Set-up:

- **Relay ID**: the relay to be set up.

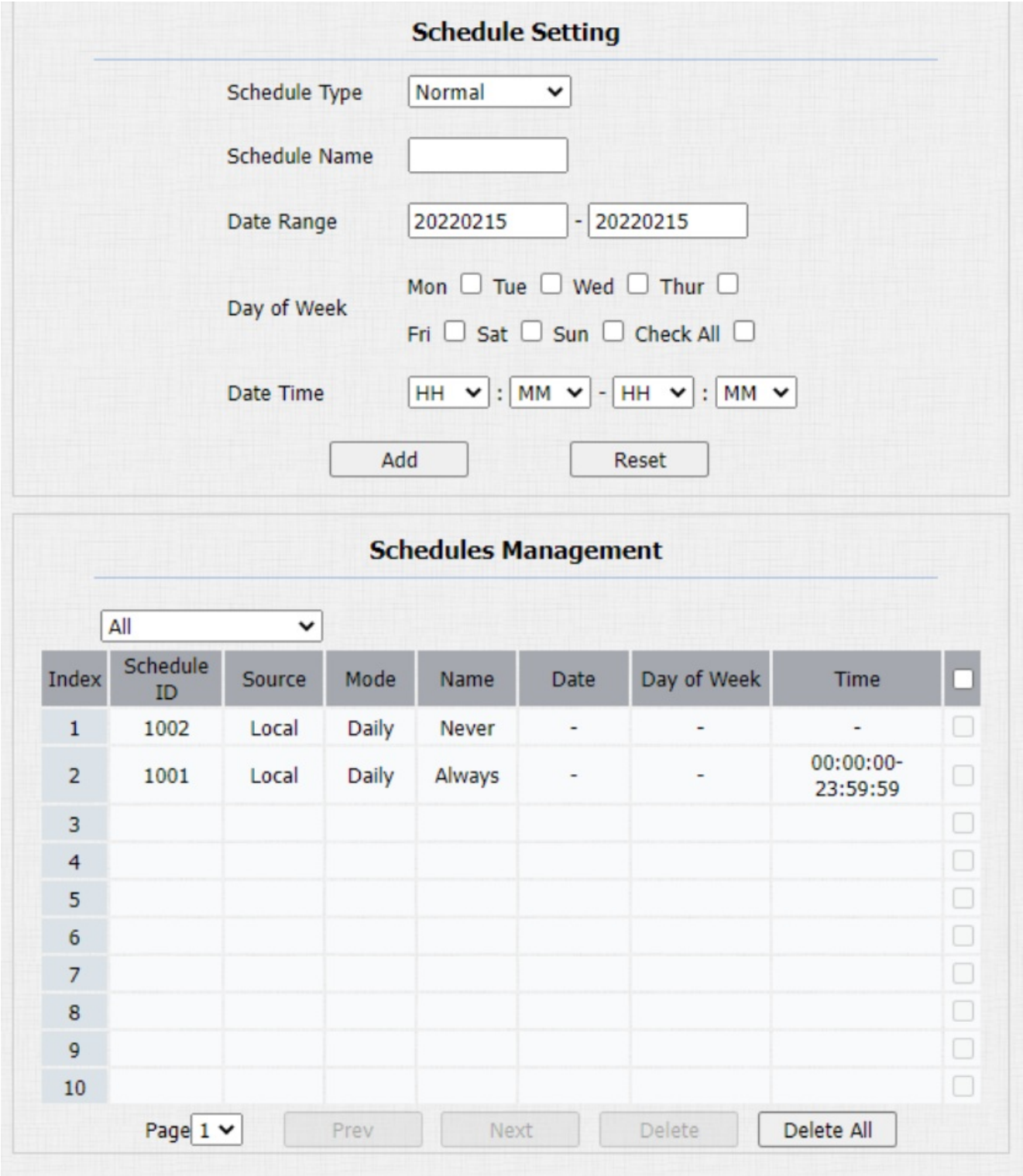
Configure Door Access Schedule

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

Create Door Access Schedule

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

Navigate to the web **Intercom > Schedule** interface.



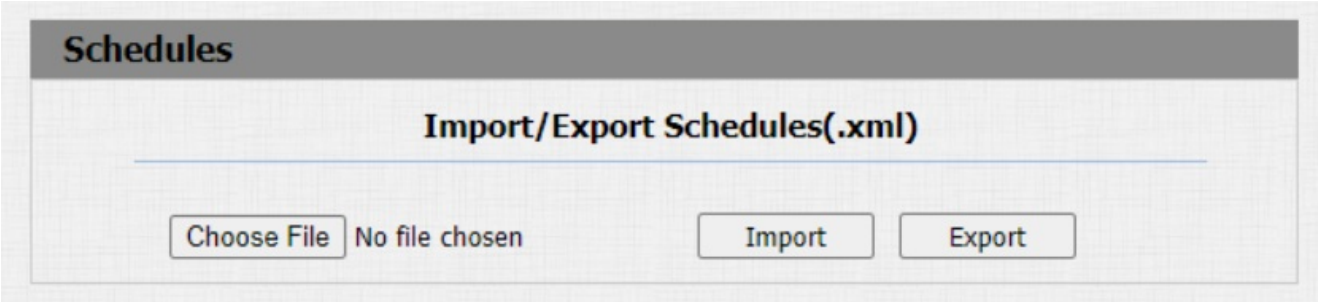
Parameters Set-up:

- **Schedule Type**: there are three types to choose from: **Daily, Weekly**, and **Normal**.
- **Date Range**: this field will only be displayed when the **Normal** type is selected.

Import and Export Door Access Schedule

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

Navigate to the web **Intercom > Schedule > Import/Export Schedule(.xml)** interface.



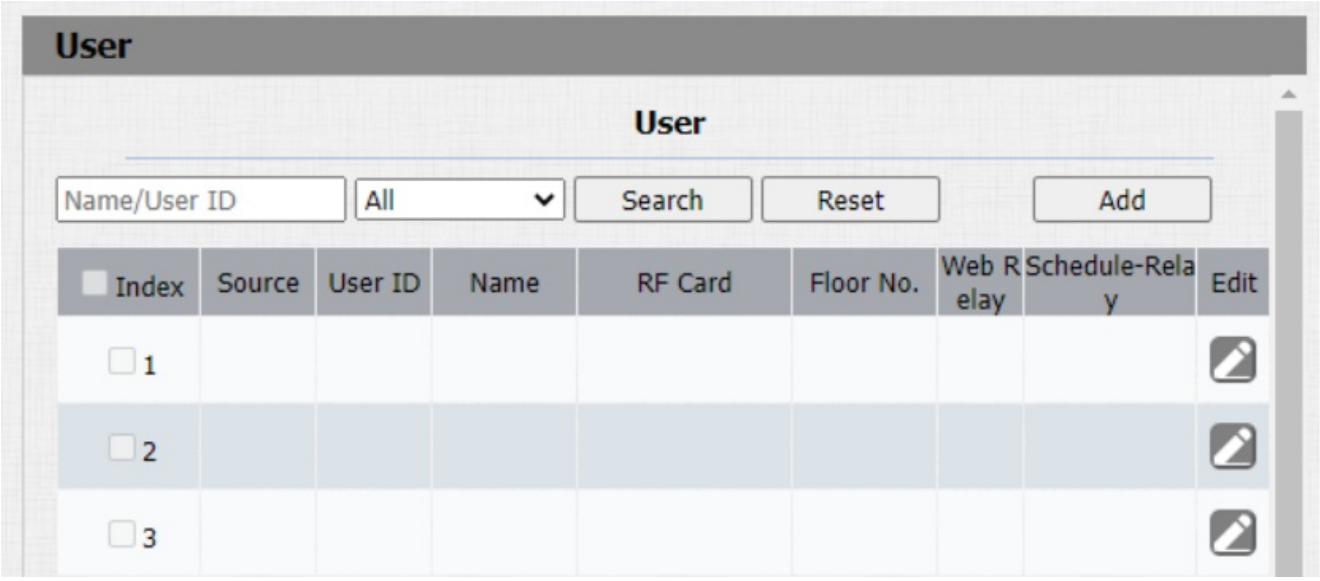
Door Unlock Configuration

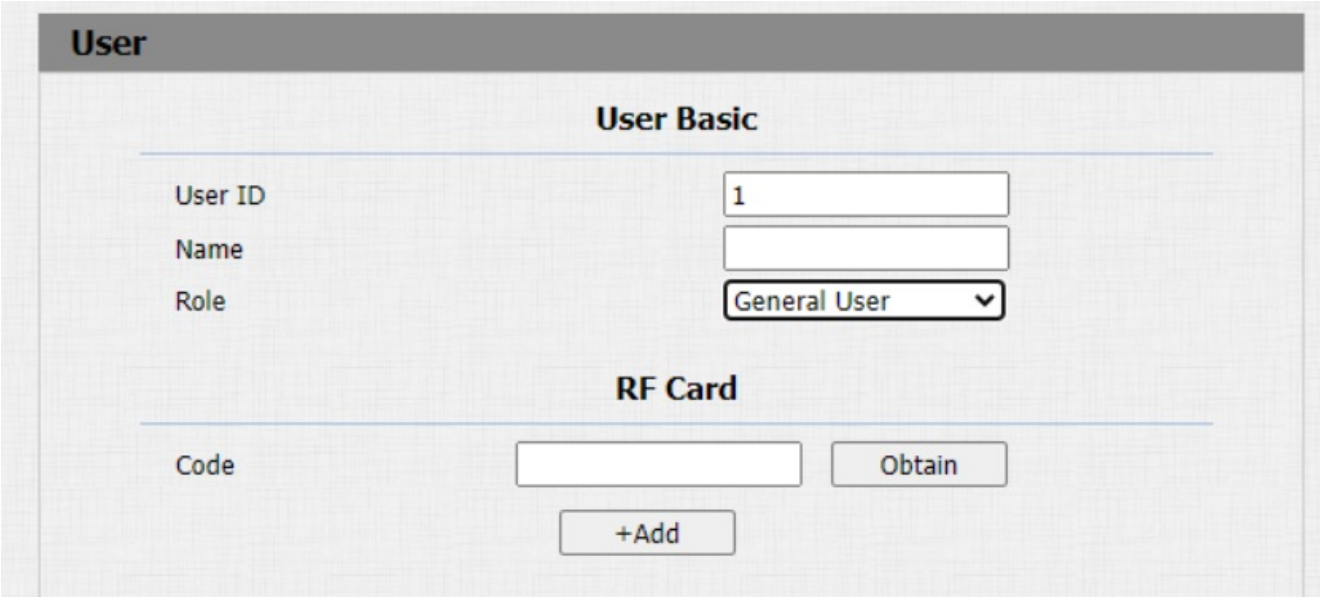
Configure RF Card for Door Unlock

Users can swipe RF cards to open doors. Before they can do so, you need to set up related parameters.

Assign RF Cards to Users

Navigate to the web **Intercom > User** interface. Click **Add**.





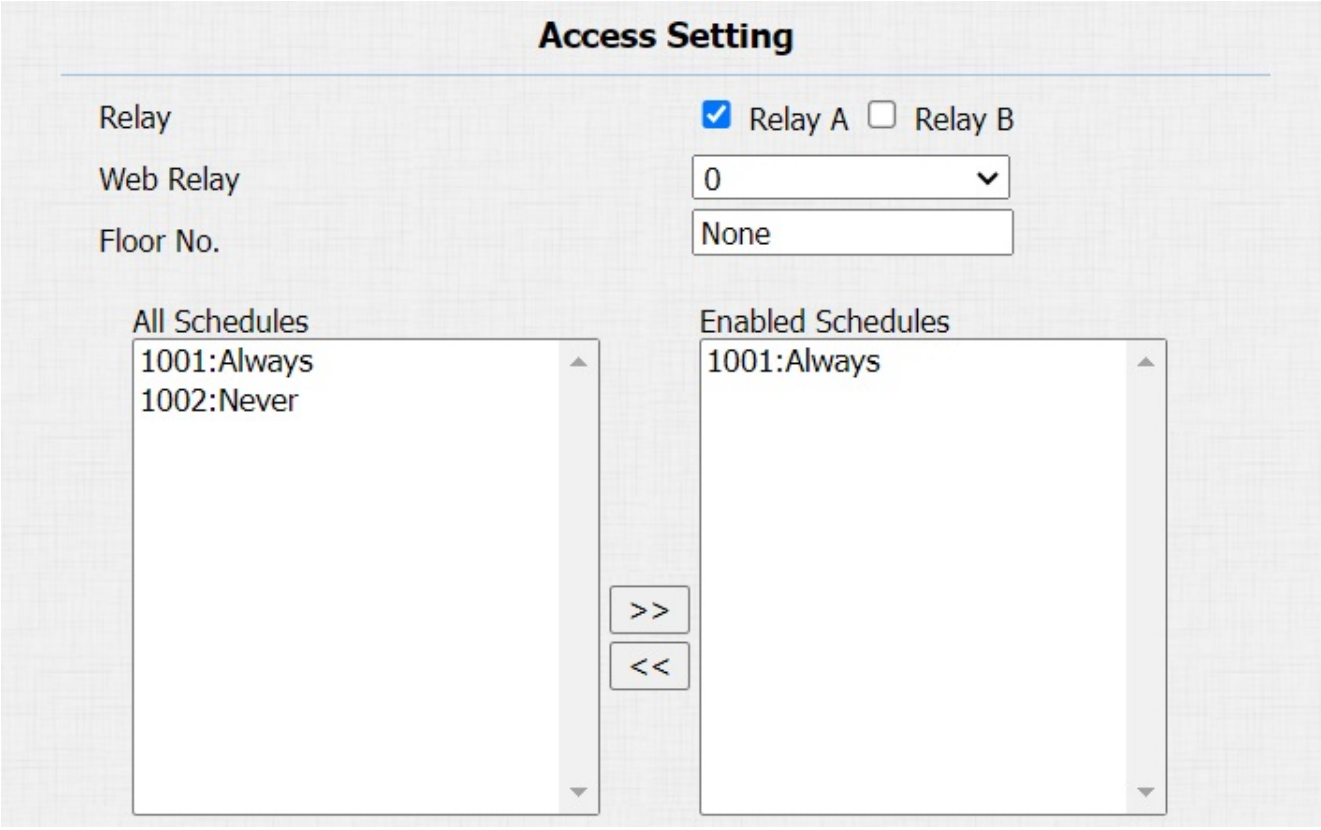
Parameter Set-up:

- **User ID**: the user ID is 11 digits maximum in length and cannot be reused for other users. The user ID can be generated automatically or manually.
- **Role**: select General User for residents and Admin for the administrator.
- **Code**: place the card on the device's card reader area and click **Obtain** to acquire the card code.

Note

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

After the user information and RF card are configured, you can configure the access control on the **Access Setting** section.



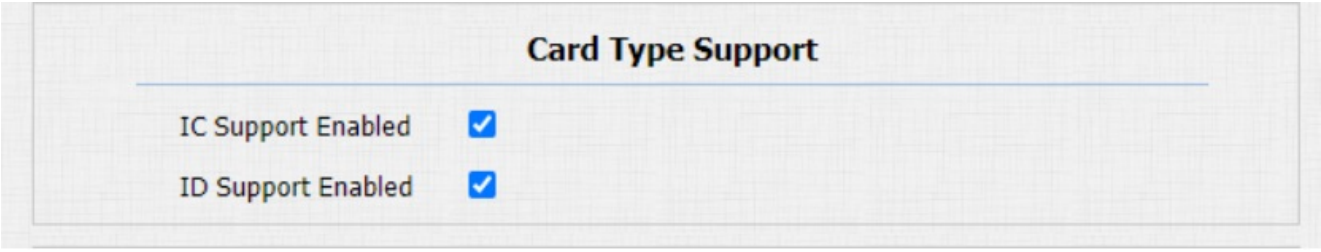
Parameter Set-up:

- **Relay**: select the relay(s) that you want to apply the private PIN code for the door unlock.
- **Web relay**: select the specific number of web relay action commands you have set up on the web interface.
- **Schedule**: select from the created door access schedule on the right box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

IC/ID Card Control

Enable or disable the device-supporting card type.

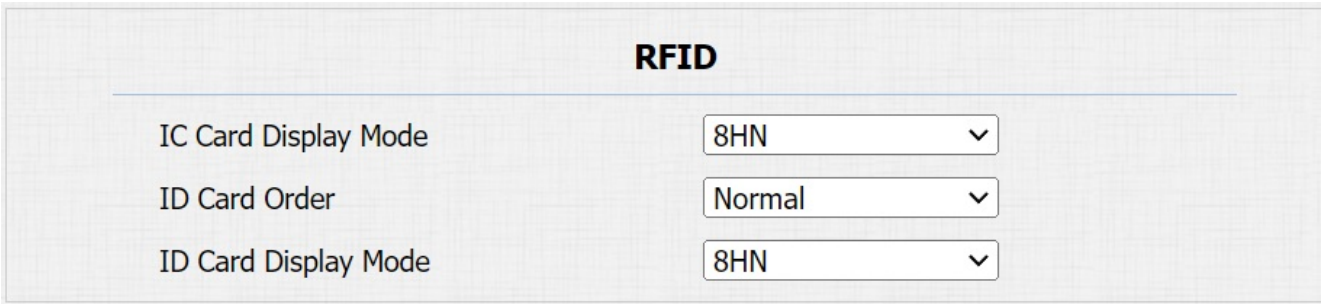
Navigate to the web **Intercom > Card Setting > Card Type Support** interface.



Configure 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.

Navigate to the web **Intercom > Card Setting > RFID** interface.



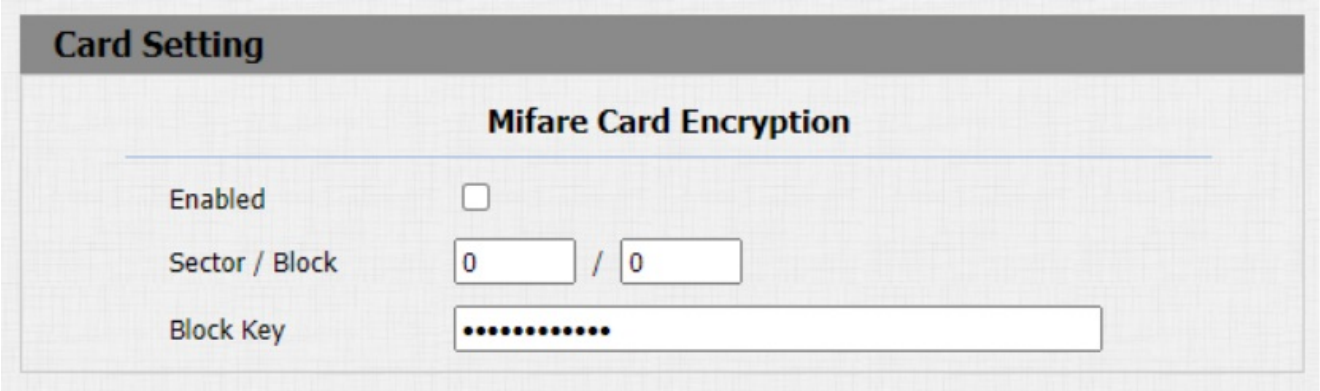
Parameters Set-up:

- **IC Card Display Mode**: select the card code format for the **IC Card** for the door access among seven format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D**. The card code format is 8HN by default in the door phone.
- **ID Card Order**: select ID card reading in normal order or reversed order. You might need to select card orders for third-party integration (eg. third-party access control). and you can also reverse the card number for card protection.
- **ID Card Display Mode**: select the card format for the **ID Card** for the door access among seven format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D**. The card code format is 8HN by default in the door phone.

Mifare Card Encryption

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

Navigate to the web **Intercom > Card Setting > Mifare Card Encryption** interface.



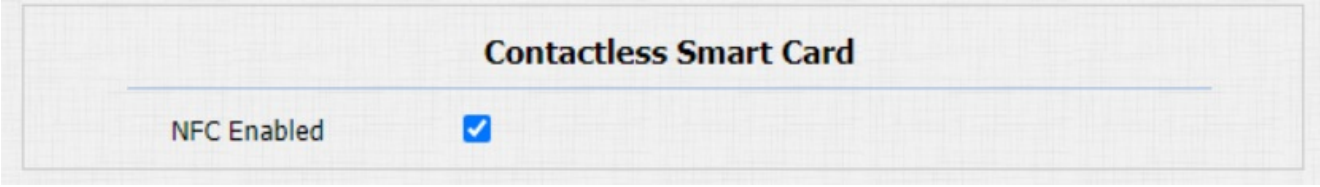
Parameter Set-up:

- **Sector/Block**: the sector and block that you want the card number to be written into the Mifare Card. For example, you can write the card number into sector 3 and block 3 in the card.
- **Block Key**: the block password for access.

NFC Card Setting

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

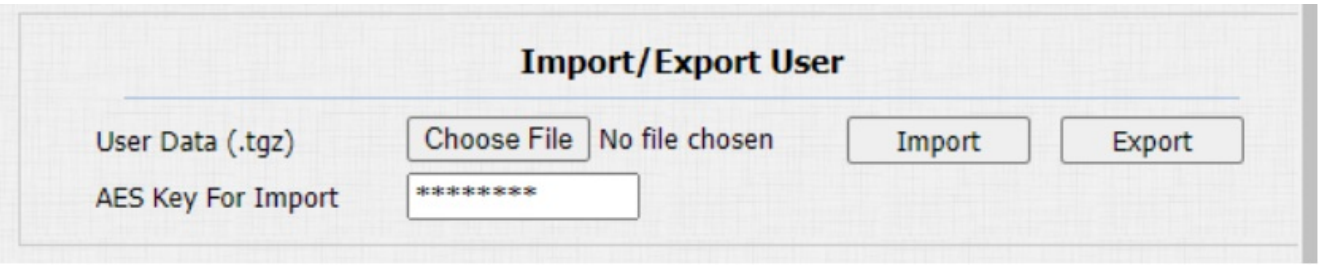
To enable it on the web **Intercom > Card Setting > Contactless Smart Card** interface.



Import and Export User Data

You can export the user data in batch to modify such information as RF card codes. Then, import it to other devices for efficiently managing users.

Navigate to the web **Intercom > User** interface.



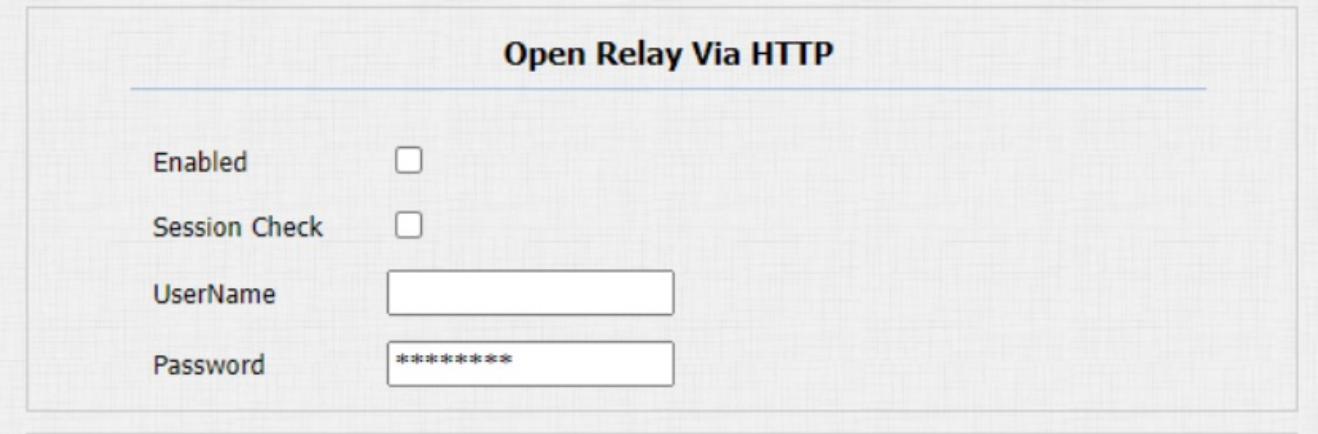
Parameter Set-up:

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

Configure Open Relay via HTTP for Door Unlock

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

Navigate to the web **Intercom > Relay > Open Relay Via HTTP** interface.



Parameter Set-up:

- **Session Check**: enable it to protect data transmission security.
- **User Name**: customize the username as part of the HTTP command, for example, **admin**.
- **Password**: customize the password as part of the HTTP command. For example: **12345**.

Please refer to the following example:

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

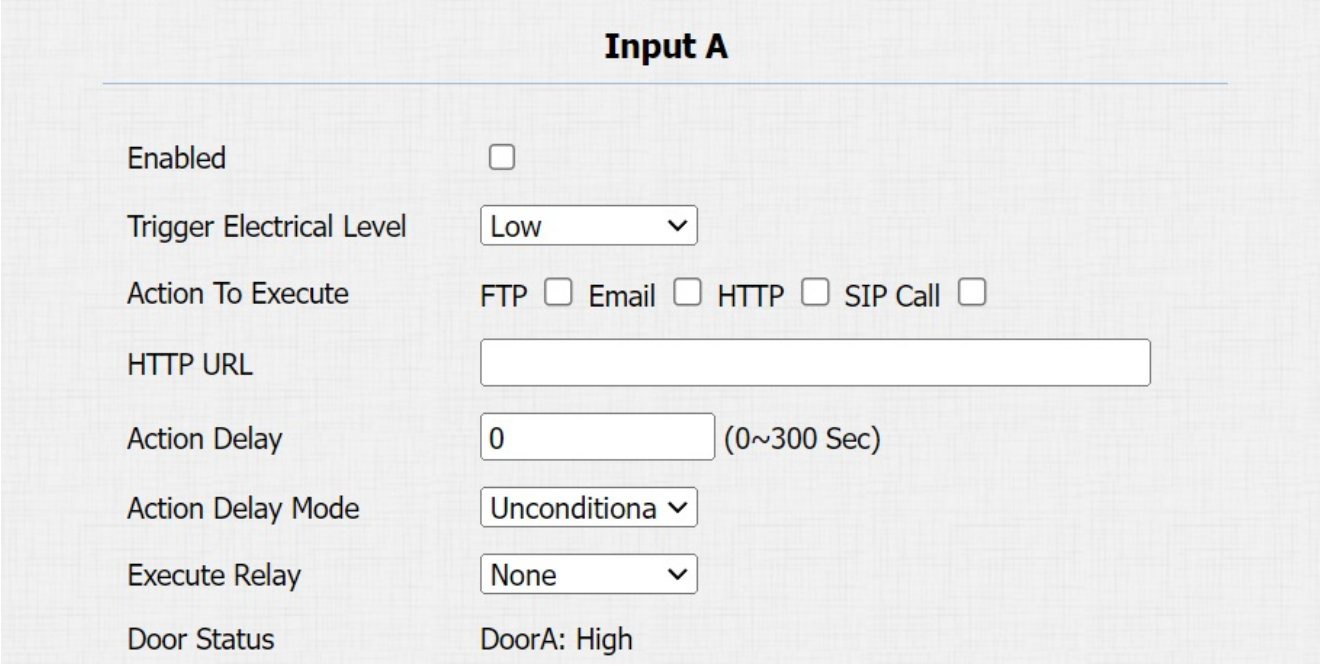
Note:

- DoorNum in the HTTP command above refers to the relay number #1 to be triggered for the door access.
- The device with high security mode enabled only supports the new HTTP formats. Please refer to **Security**.

Configure Exit Button for Door Unlock

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

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



Parameter set-up:

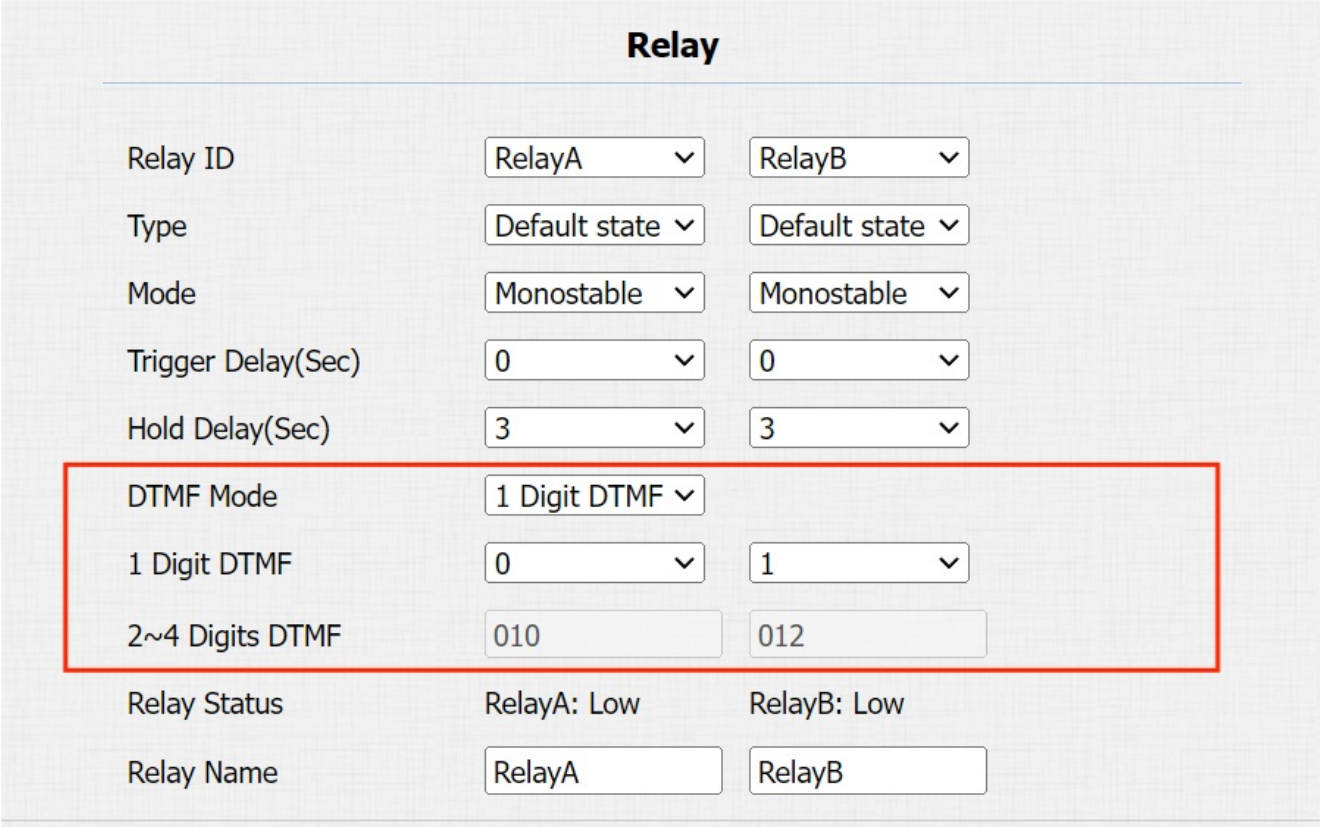
- **Trigger Electrical Level**: select the trigger electrical level options between High and Low according to the actual operation of the exit button.
- **Action To Execute**: select the method to carry out the action among four options: FTP, Email, HTTP, and SIP Call.

- **HTTP URL**: enter the URL if you select the HTTP to carry out the action.
- **Action Delay**: set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 seconds after your press the button.
- **Action Delay Mode**: if you select **Unconditional Execution**, the action will be carried out when the input is triggered. If you select **Execute If Input Still Triggered**, then 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**: set up relays to be triggered by the actions.

Configure DTMF for Door Unlock

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

Navigate to the web **Intercom > Relay > Open Relay Via DTMF** interface.



Parameter Set-up:

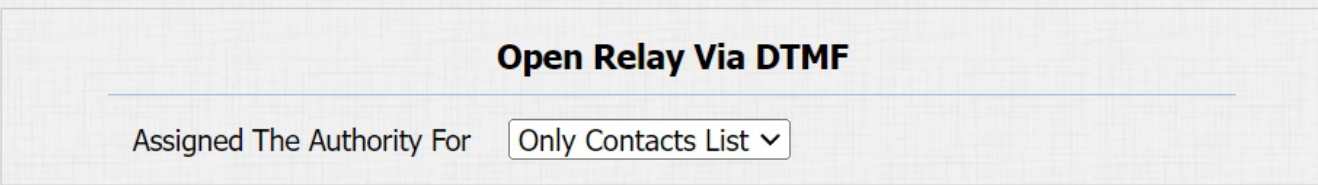
- **DTMF Mode**: the number of DTMF digits for the door access control(Ranging from 1-4 digits).
- **1 Digit DTMF**: select the code from **0-9 and ,#* if the DTMF Option is set as 1 digit.
- **2~4 Digits DTMF**: set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMP Option** is set as 3-digits.

Note

Intercom devices involved must be consistent in the DTMF type, otherwise DTMF code cannot be applied.

DTMF White List

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



Parameter Set-up:

- **Assigned The Authority For**: **All Numbers** allows all numbers for the DTMF door unlock; **None** denies all numbers for the DTMF door unlock; **Only Contacts List** allows the contact numbers in your door phone.

Monitor and Image

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

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

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

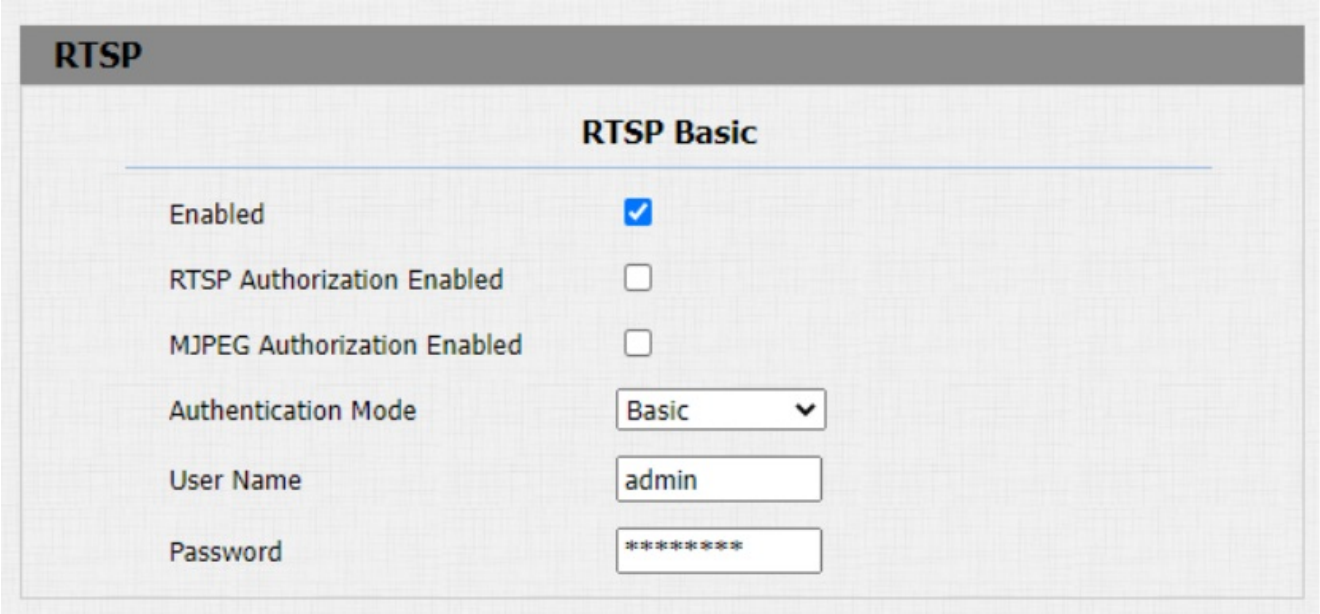
ONVIF is an Open Network Video Interface Forum. It enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

RTSP Stream Monitoring

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

RTSP Basic Setting

Navigate to the web **Intercom > RTSP > RTSP Basic** interface.



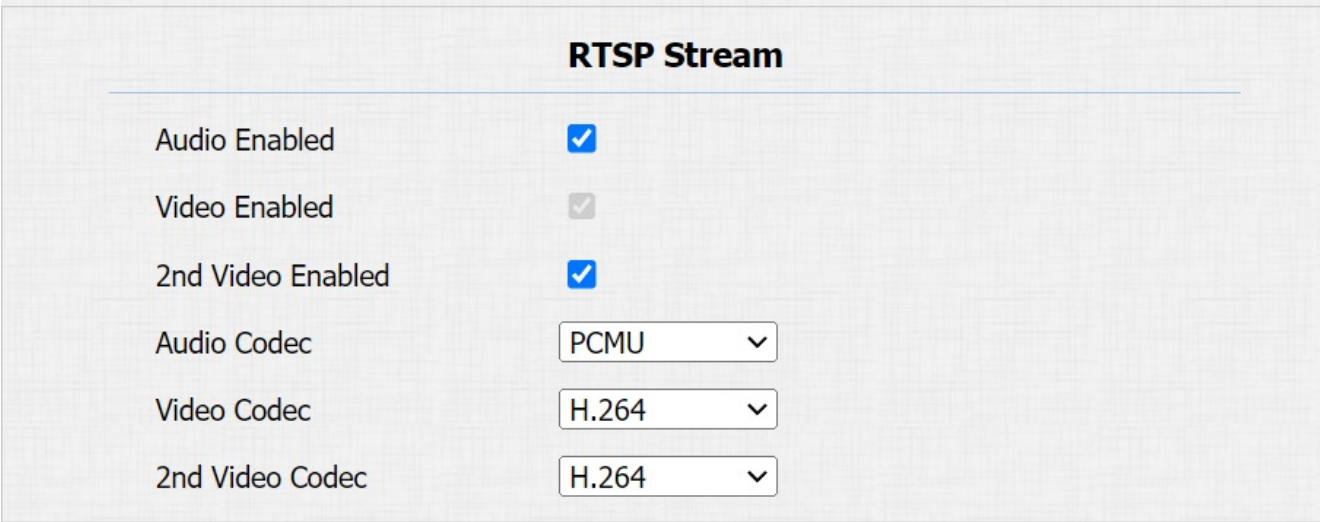
Parameter Set-up:

- **RTSP Authorization Enabled**: when enabled, you are required to select RTSP Authentication Mode and enter RTSP username and password for authentication.
- **RTSP Authentication Mode**: select RTSP authentication type between **Basic** and **Digest**.

RTSP Stream Setting

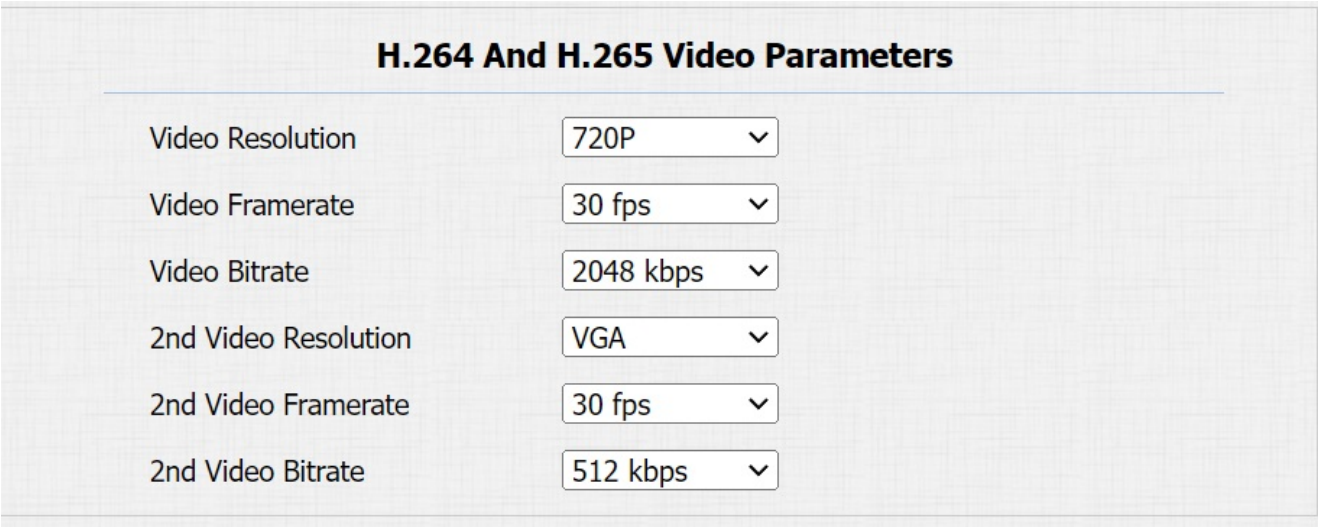
The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

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



Parameter Set-up:

- **Video Enabled**: After enabling RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **2nd Video Enabled**: Akuvox door phones support 2 RTSP streams, you can enable the second one.



Parameter Set-up:

- **Video Resolution**: select video resolutions among five options: **CIF, VGA, 4CIF, 720P, 1080P**. The default video resolution is **720P**, and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than **720P**.
- **Video Framerate**: **30fps** is the default video frame rate.
- **Video Bitrate**: select video bitrate among six options: **64 kbps**, **128kbps**, **256kbps**, **512 kbps**, **1024 kbps**, **2048 kbps** according to the network environment. The default video bitrate is **2048 kpbs**.
- **2nd Video Resolution**: select the video resolution for the second video stream channel. The default is **VGA**.
- **2nd Video Framerate**: select the video framerate for the second video stream channel. The default is **30 fps**.
- **2nd Video Bitrate**: select video bitrate among six options: **64 kbps**, **128kbps**, **256kbps**, **512 kbps**, **1024 kbps**, **2048 kbps** according to the network environment. The default video bitrate is **512 kpbs**.

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

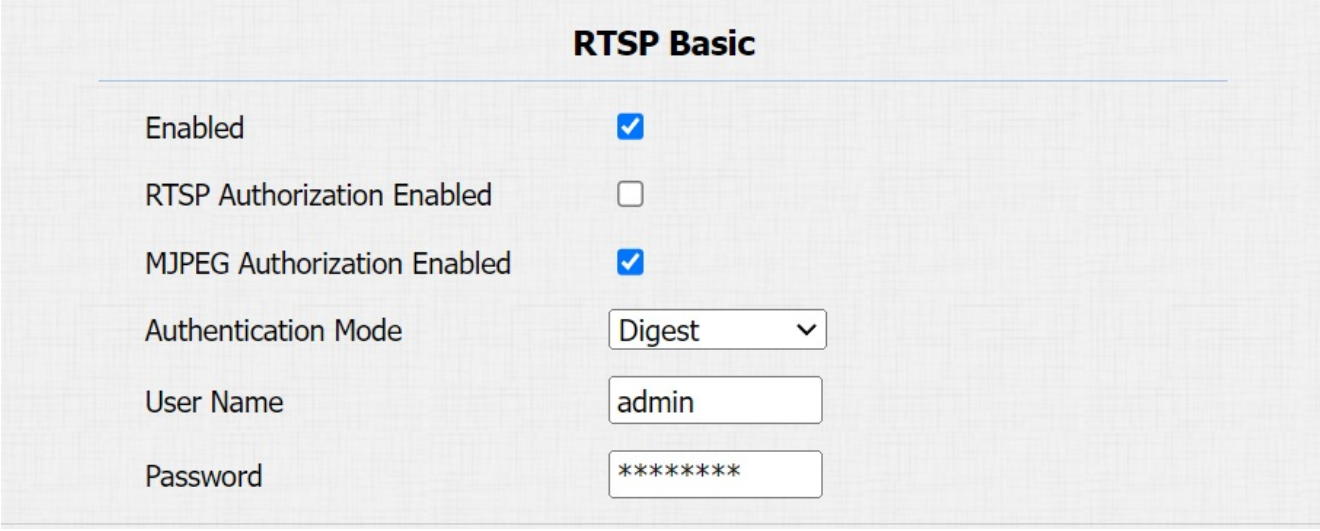
Parameter Set-up:

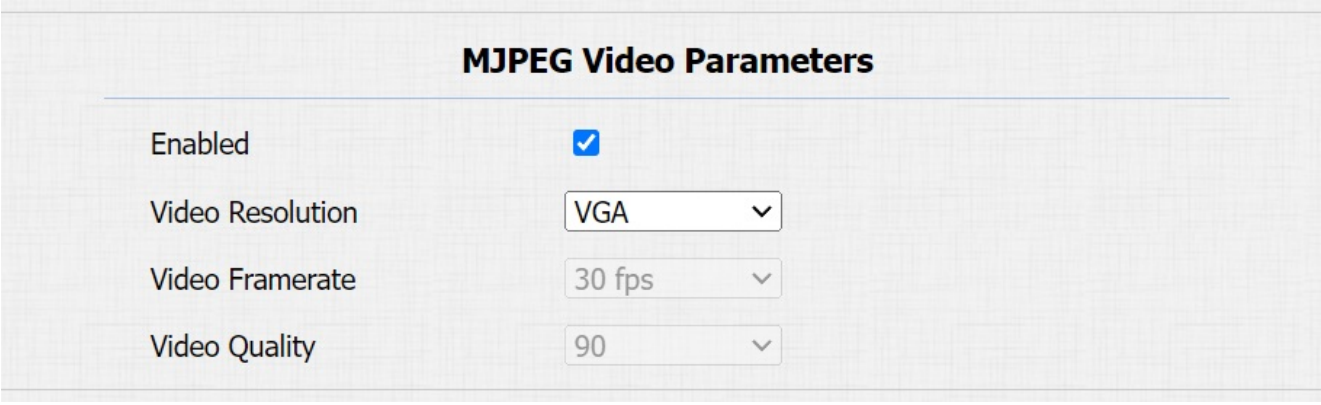
- **NACK Enabled**: It can be used to prevent losing data packet in the weak network environment when discontinued and mosaic video image occurred.

MJPEG Image Capturing

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

You can enable the Mjpeg function on the **Intercom > RTSP > RTSP Basic** and set the image quality on the web **Intercom > RTSP > MJPEG Video Parameters** interface.





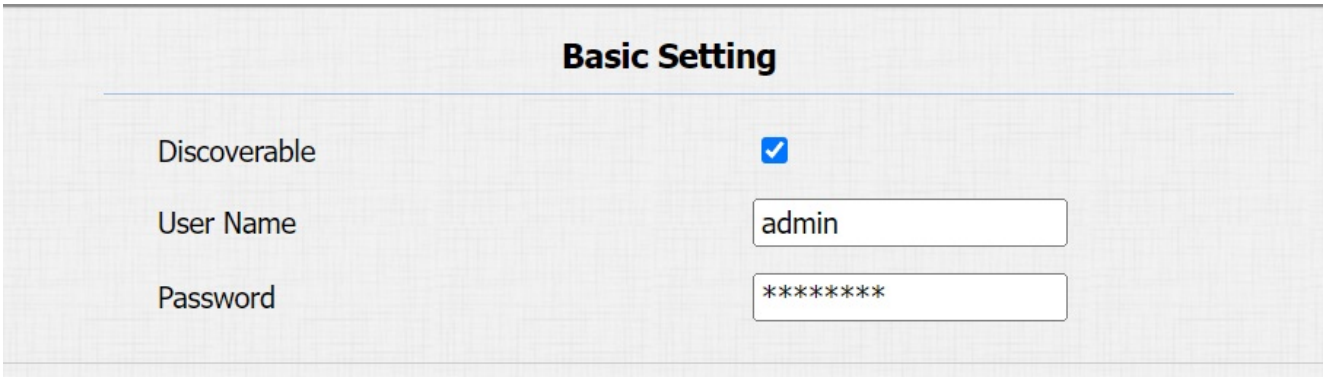
Parameter Set-up:

- **Video Resolution**: select video resolutions among five options: **CIF, VGA, 4CIF, 720P, 1080P**. The default video resolution is **VGA**, and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than **VGA**.

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.

Navigate to the web **Intercom > ONVIF** interface.



Parameter Set-up:

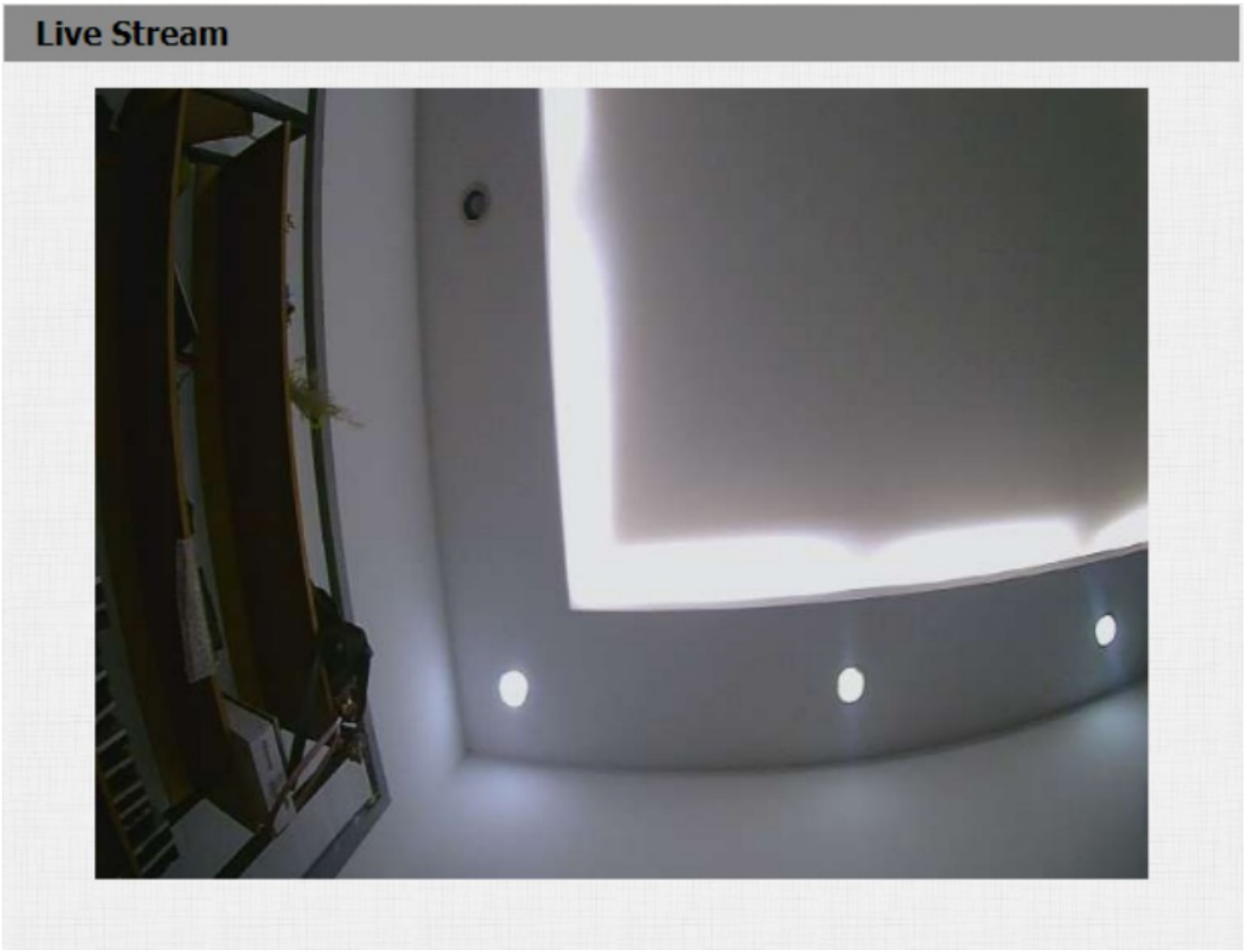
- **Discoverable**: when enabled, the video from the door phone camera can be searched by other devices.
- **Password**: customize the password for authentication. The default is **admin**.

After the setting is complete, you can enter the ONVIF URL on the third party device to view the video stream.
The example format is: **http://IP address: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.

Navigate to the web **Intercom > Live Stream** interface.

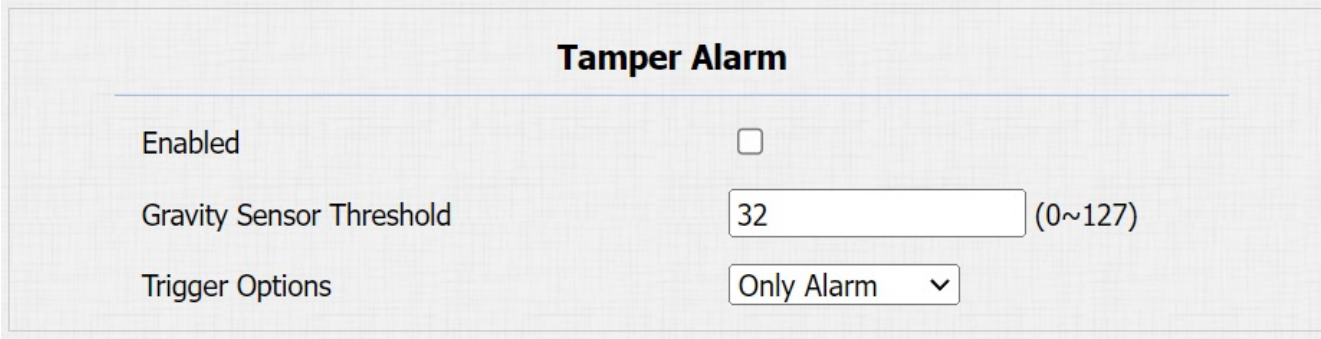


Security

Tamper Alarm Setting

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

Navigate to the web **Security > Basic > Tamper Alarm** interface.



Parameter Set-up:

- **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**: decides what can be triggered when the gravity sensor is triggered.

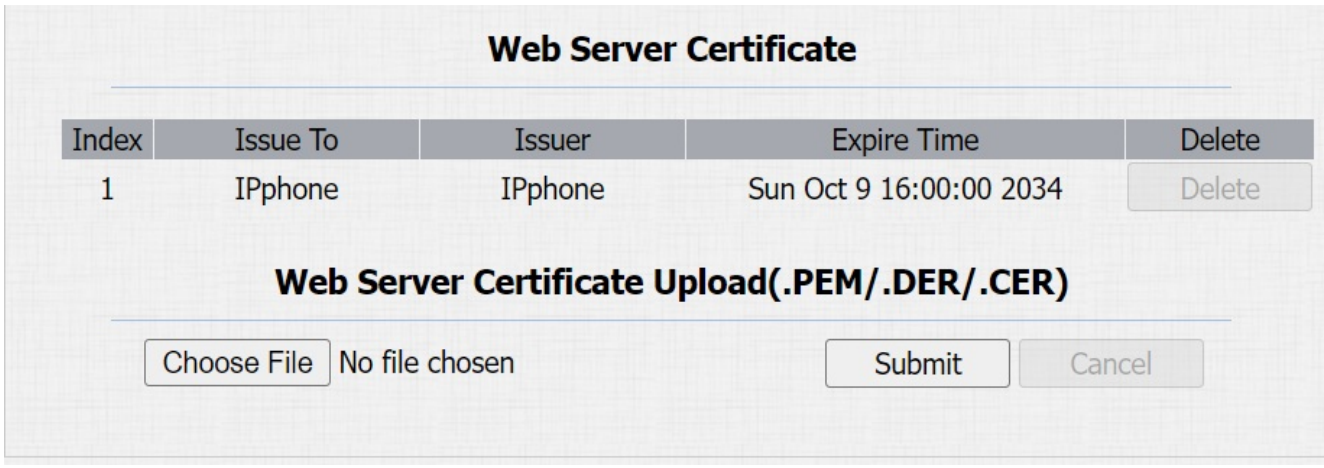
Client Certificate Setting

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

Web Server Certificate

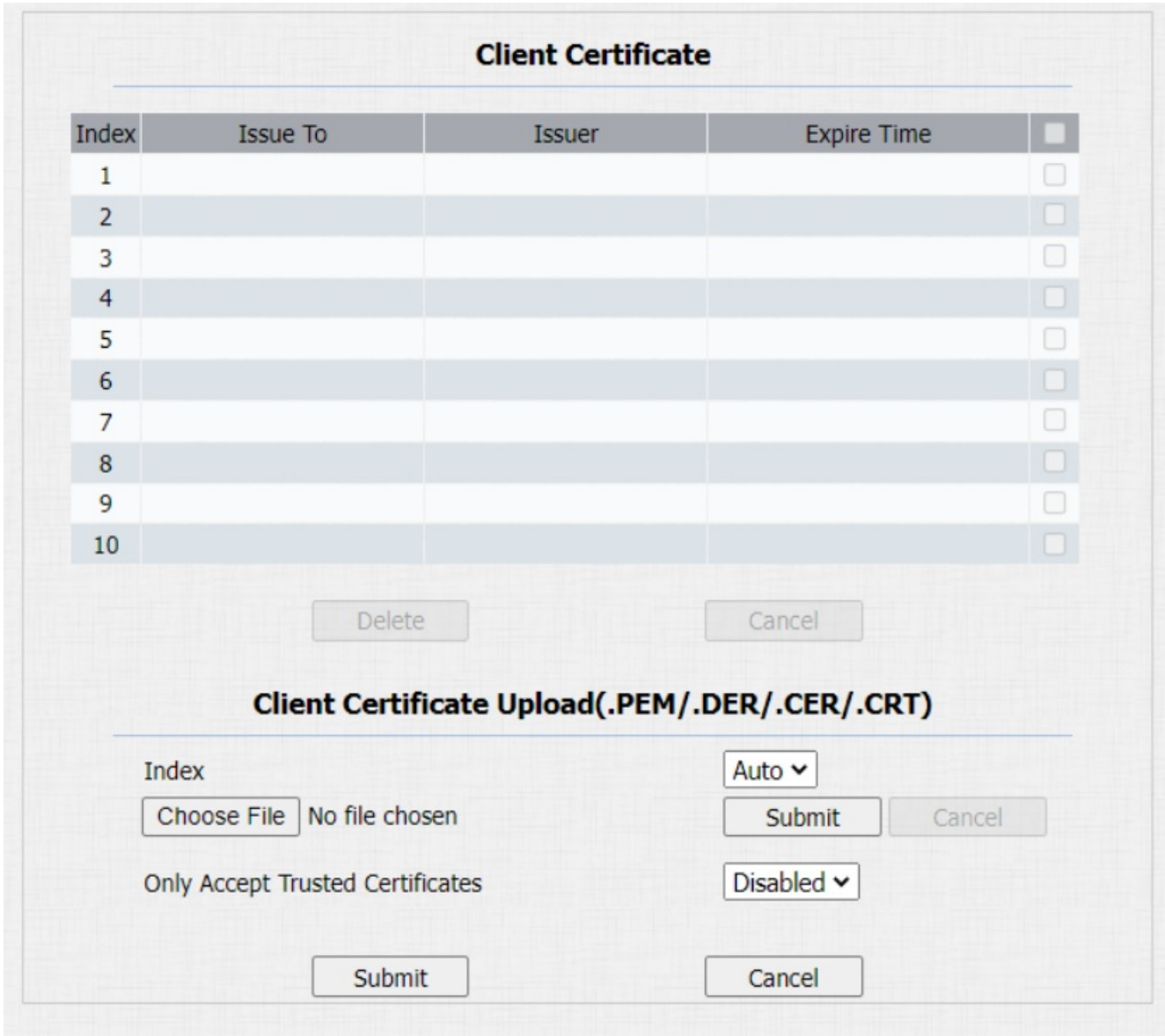
It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

Navigate to the web **Security > Advanced > Web Server Certificate** interface.



Client Certificate

Navigate to the web **Security > Advanced > Web Server Certificate** interface.



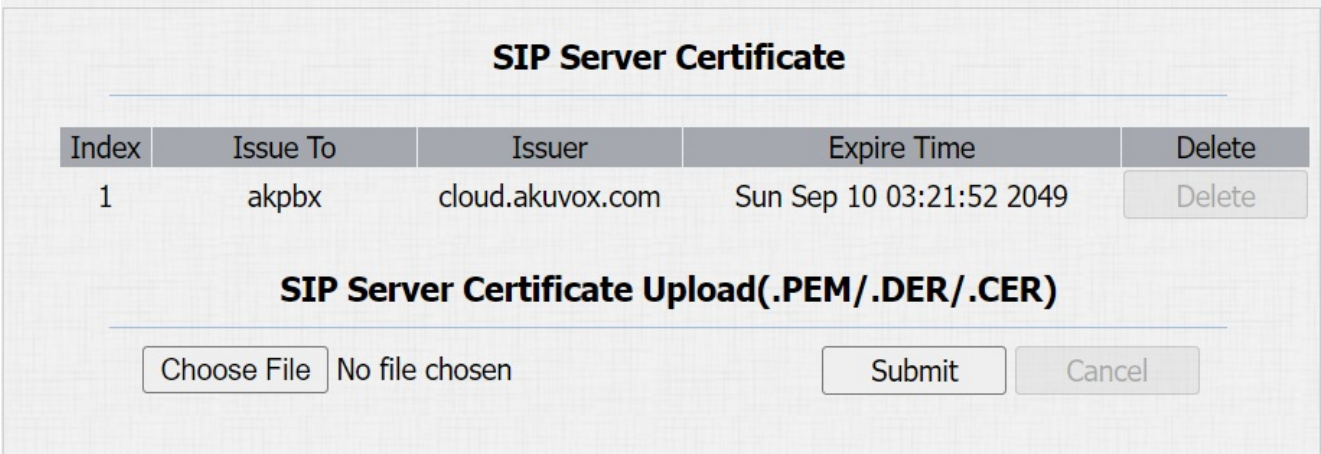
Parameter Set-up:

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

Upload TLS Certificate for SIP Account Registration

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

Navigate to the web **Security > Advanced > Web Server Certificate** interface.

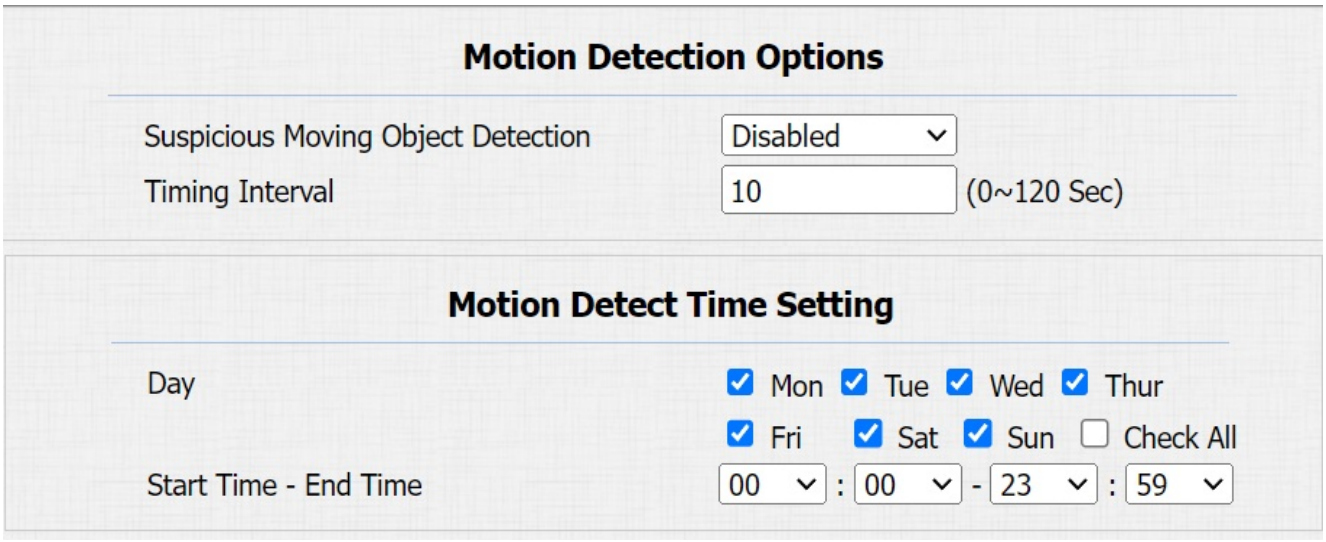


Motion Detection

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.

Configure Motion Detection

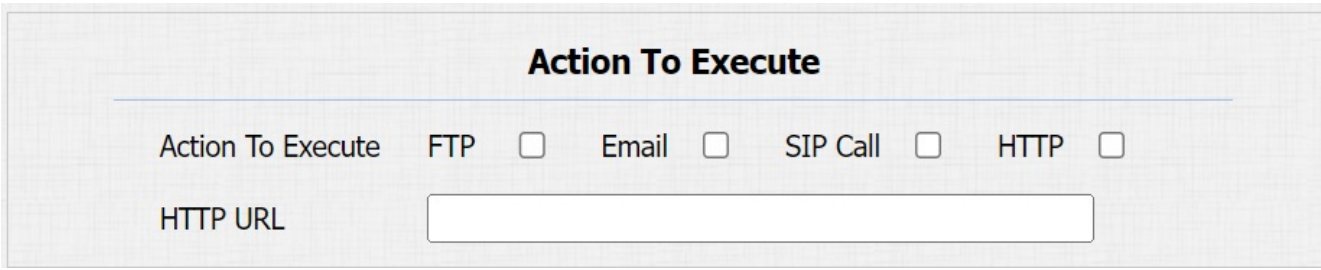
Navigate to the web **Intercom > Motion > Motion Detection Options** interface.



Parameter Set-up:

- **Suspicious Moving Object Detection**: select **Disable** to disable the motion detection. Select **IR Detection** to enable the IR sensor-based motion detection. And select **Video Detection** to enable the video-based motion detection during the monitoring of the suspicious moving object.
- **Time Interval**: the time interval for the motion detection. If you set the default time interval as **10** Sec, then the motion detection time span will be 10 seconds. Assuming that we set the time interval as **10** then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 seconds interval, then the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) anywhere between **7-10** seconds once the movement is detected.“10” Sec interval is a complete cycle of the motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the **Time interval minus three**.

You can set up the actions triggered by motion detection on the same interface.

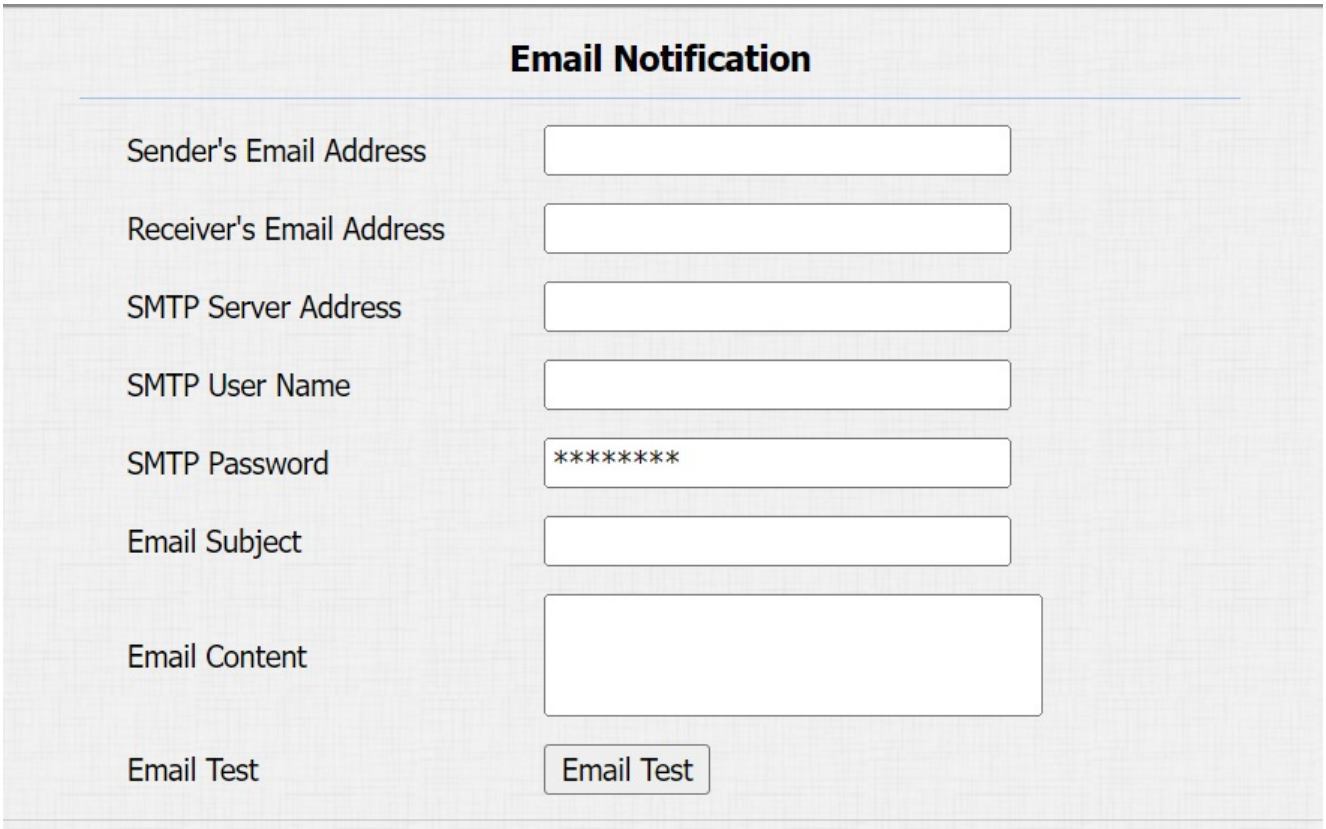


Security Notification Setting

Email Notification Setting

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

Navigate to the web **Intercom > Action > Email Notification** interface. The email notification will show the captured image.



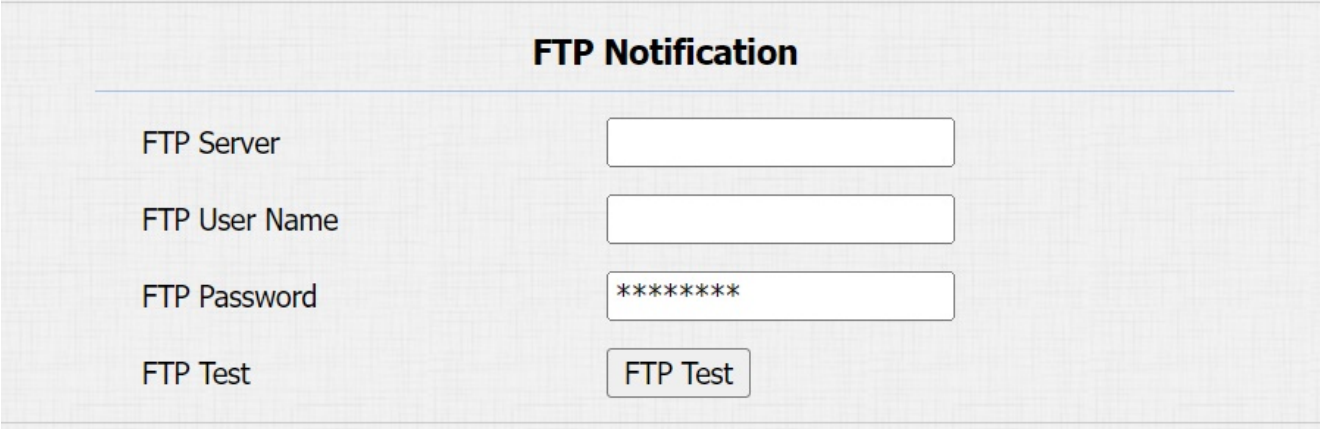
Parameter Set-up:

- **SMTP User Name**: the SMTP user name is usually the same as the sender's email address.
- **SMTP Password**: the password of SMTP server is usually the same as the sender's email address.
- **Email Test**: click Email Test to check whether the feature functions normally.

FTP Notification Setting

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

Navigate to the web **Intercom > Action > FTP Notification** interface.

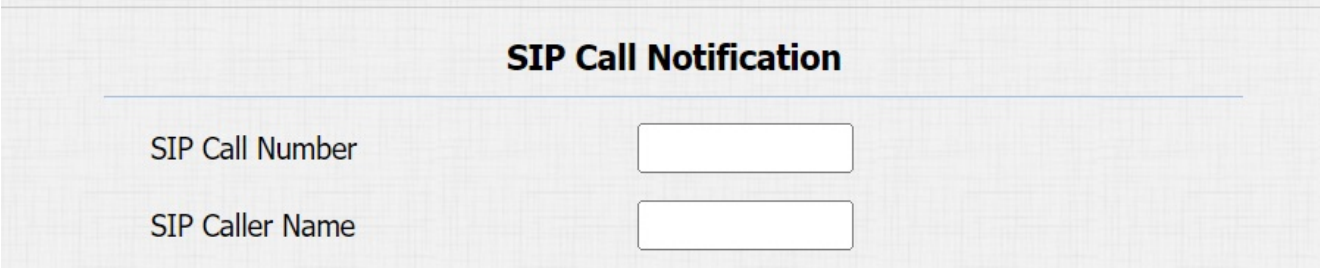


Parameter Set-up:

- **FTP Server**: the address(URL) of the FTP server.
- **FTP Test**: run the test to see if FTP notification can be sent and received by the FTP server.

SIP Call Notification Setting

Navigate to the **Intercom > Action > SIP Call Notification** interface.

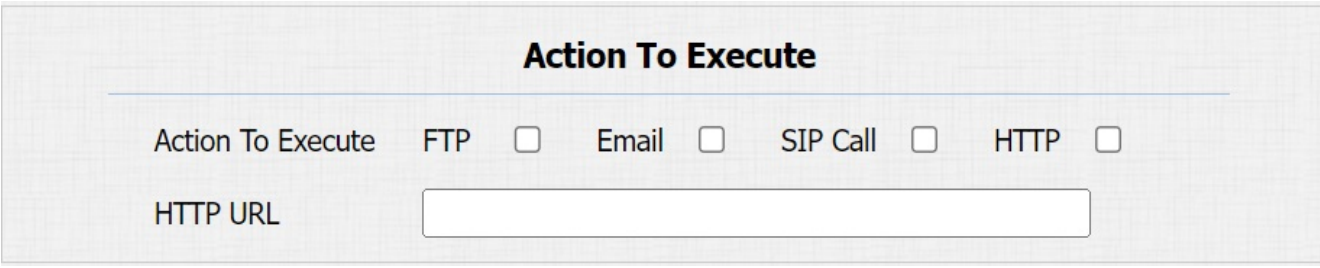


Security Action Configuration

Configure Motion Action

You can set up the action triggered by motion detection.

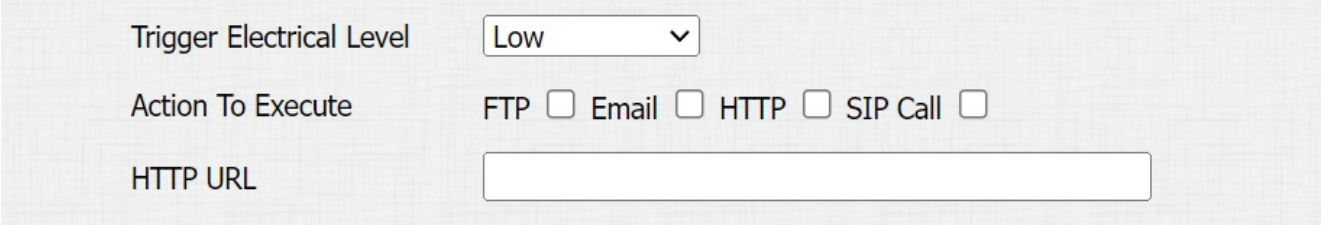
Navigate to the web **Intercom > Motion** interface.



Configure Input Action

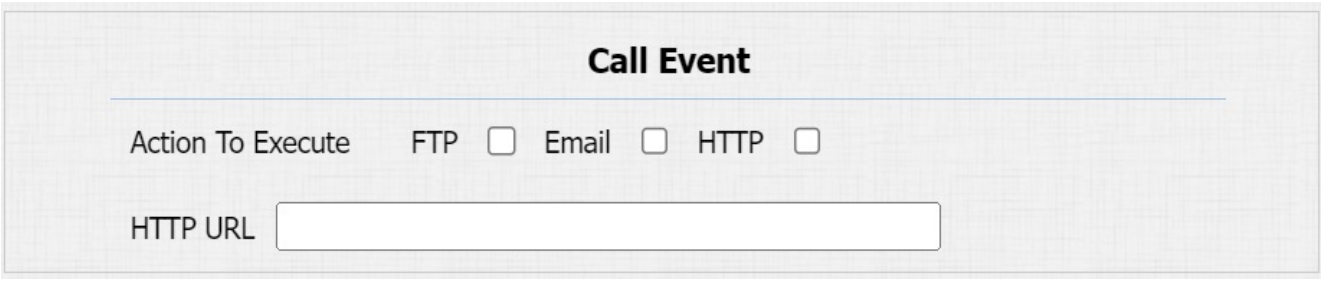
When Input interface is working , it can also trigger an action.

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



Call Event Notification

If you want to be notified of the call event (call receiving, answering, etc.), navigate to the web **Intercom > Basic > Call Event** interface.



Action URL

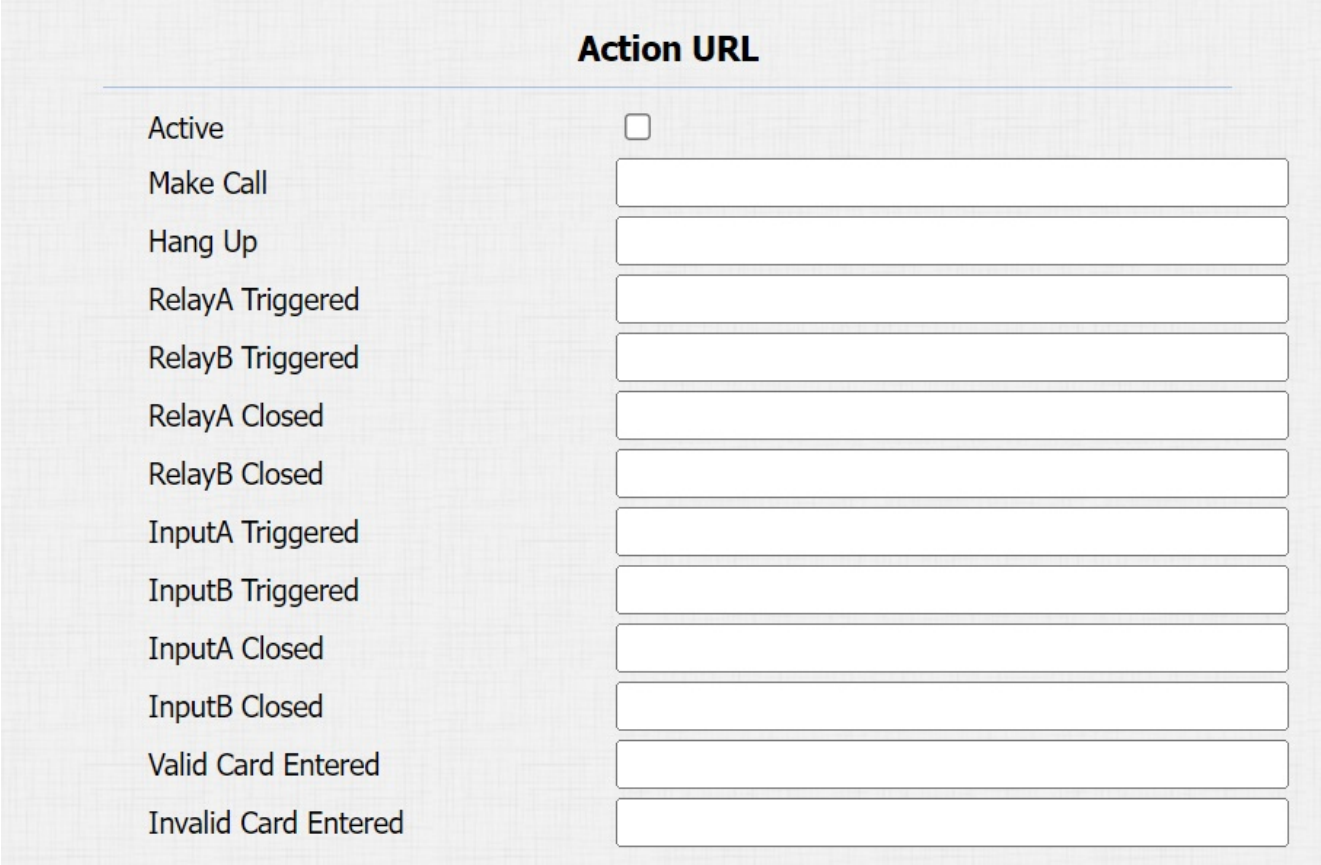
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

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

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

Navigate to the web **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.

Navigate to the web **Account > Advanced > Encryption** interface.

Parameter Set-up:

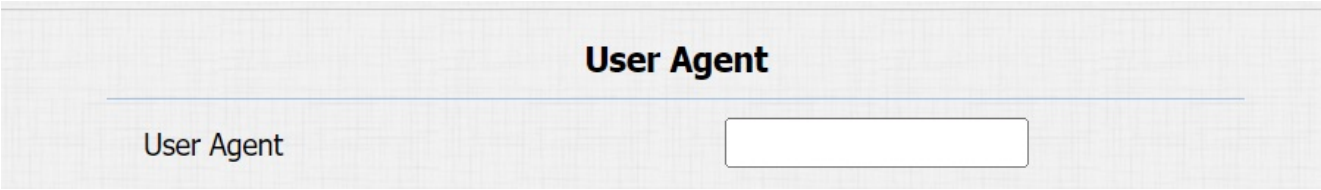
- **Voice Encryption(SRTP)**: choose **Disabled, Optional** or **Compulsory** for SRTP. If it is **Optional** or **Compulsory**, the voice during the call is encrypted, and you can grab the RTP packet to view.

User Agent

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

If user agent is set to a specific value, users can see the information from PCAP. If user agent is blank, by default, users can see the company name Akuvox, model number and firmware version from PCAP.

Navigate to the web **Account > Advanced > User Agent** interface.



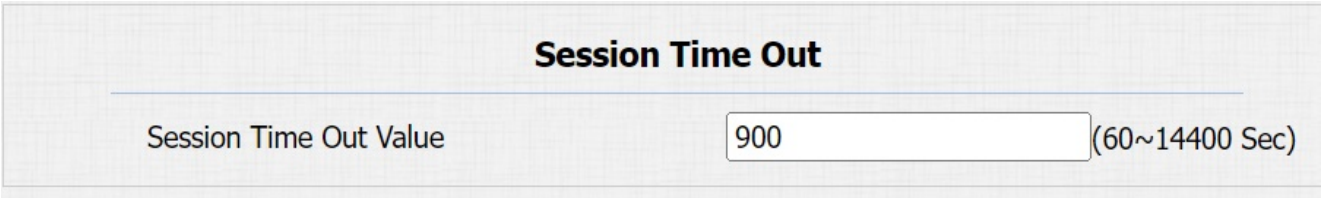
Parameter Set-up:

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

Web Interface Automatic Log-out

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

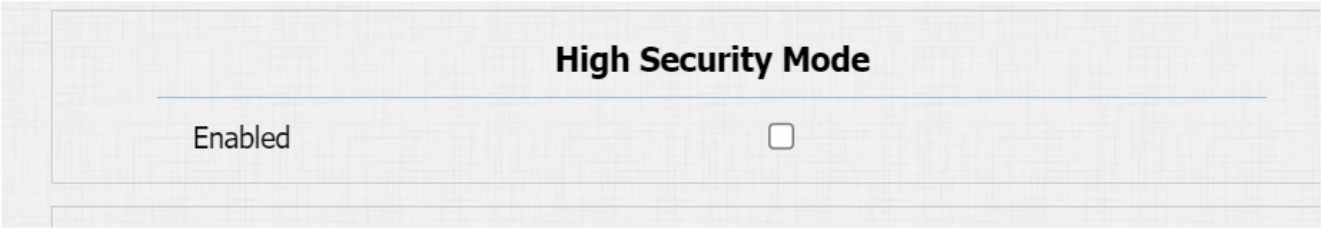
Navigate to the web **Security > Basic > Session Time Out** interface.



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.

Navigate to the web **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.

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

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

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

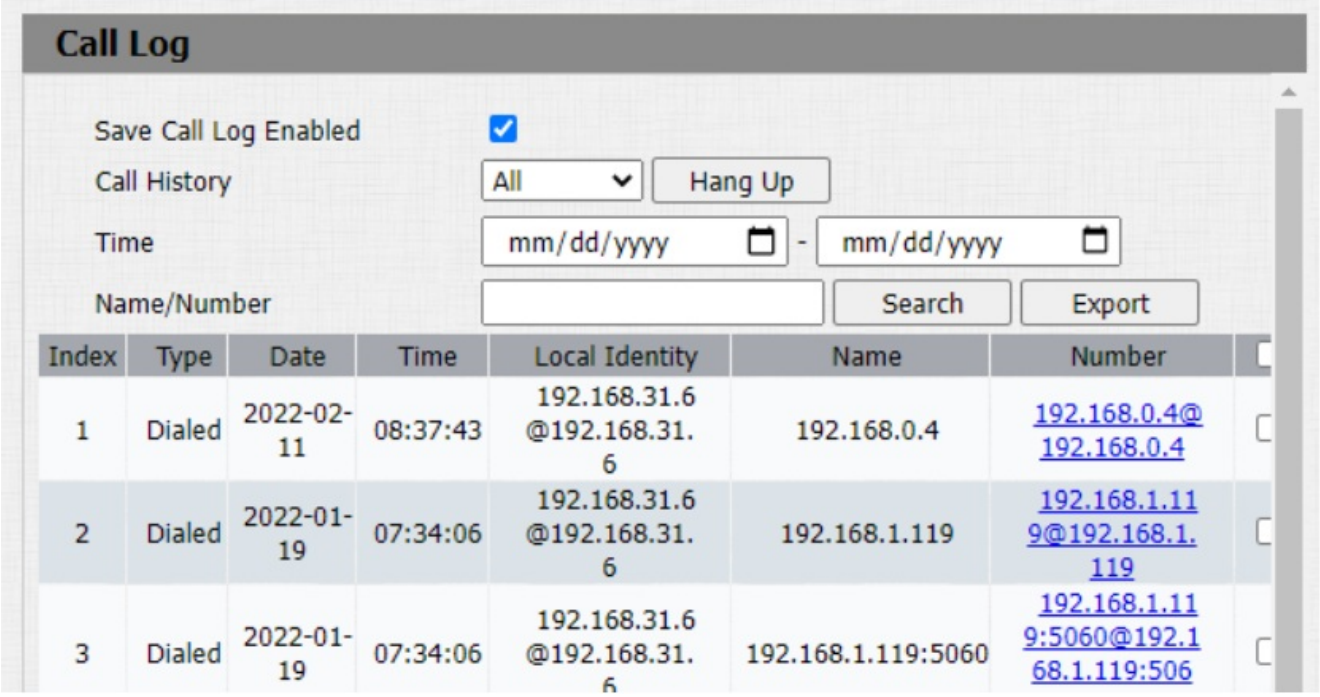
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

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

Navigate to the web **Phone > Call Log** interface.



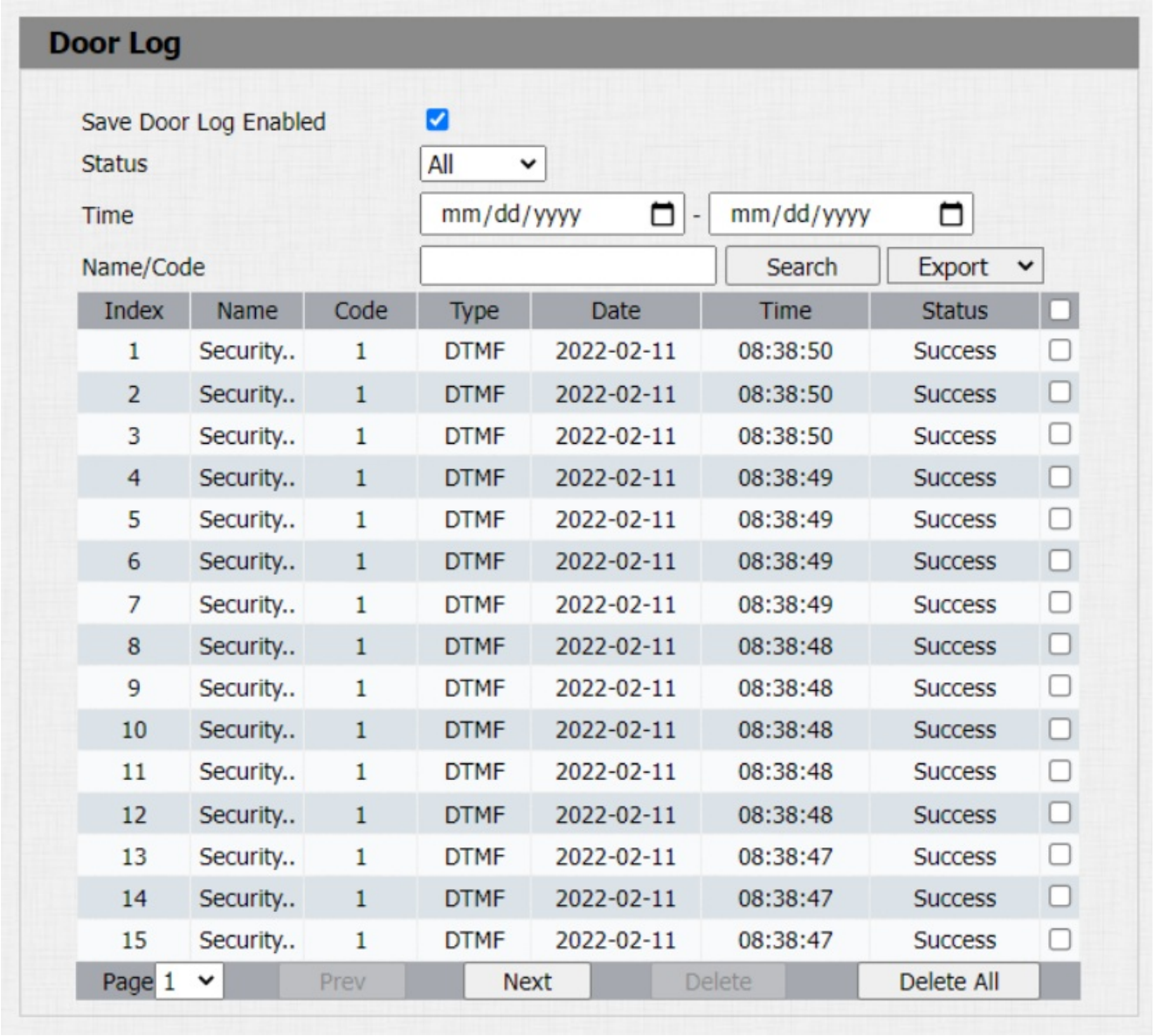
Parameter Set-up:

- **Name/Number**: search the call log by the name or by the SIP or IP number.

Door Logs

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

Navigate to the web **Phone > Door Log** interface.



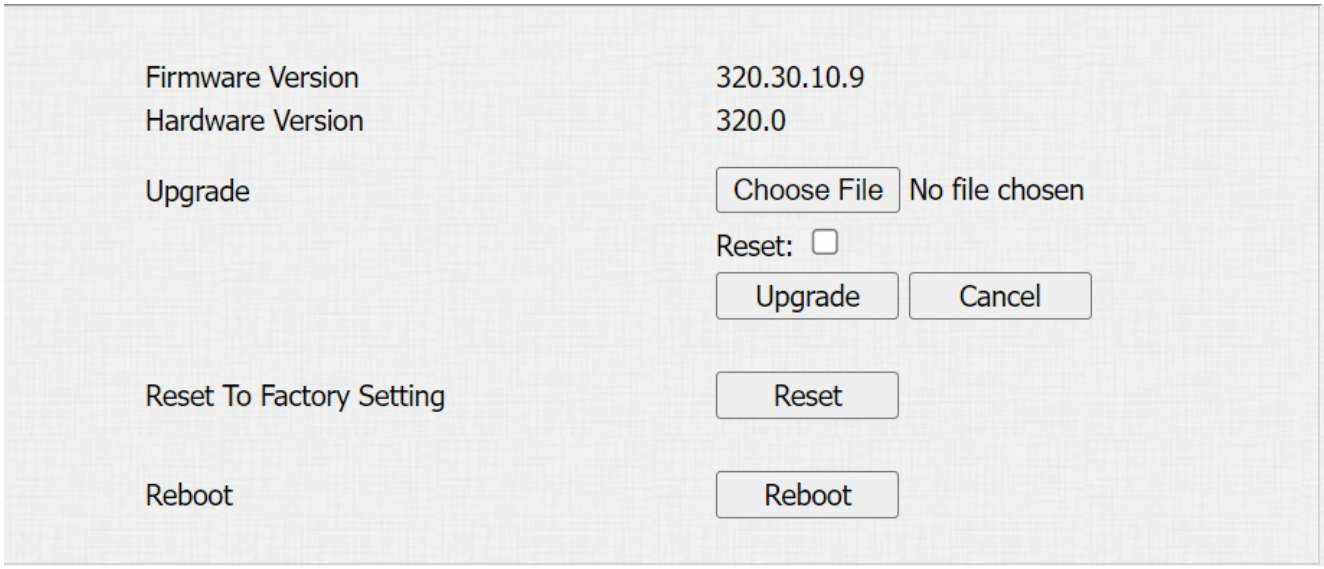
Parameter Set-up:

- **Name**: if it is a locally added key or card, the corresponding added name will be displayed. If it is an unknown key or card, it will display Unknown.
- **Code**: if opening the door via PIN code, the corresponding PIN code will be displayed. If opening the door via RF cards, the corresponding card number will be displayed. If the door is opened by HTTP command, it will be empty.
- **Export**: you can export the door logs in .xml or .csv format.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Navigate to the web **Upgrade > Basic** interface.



Note

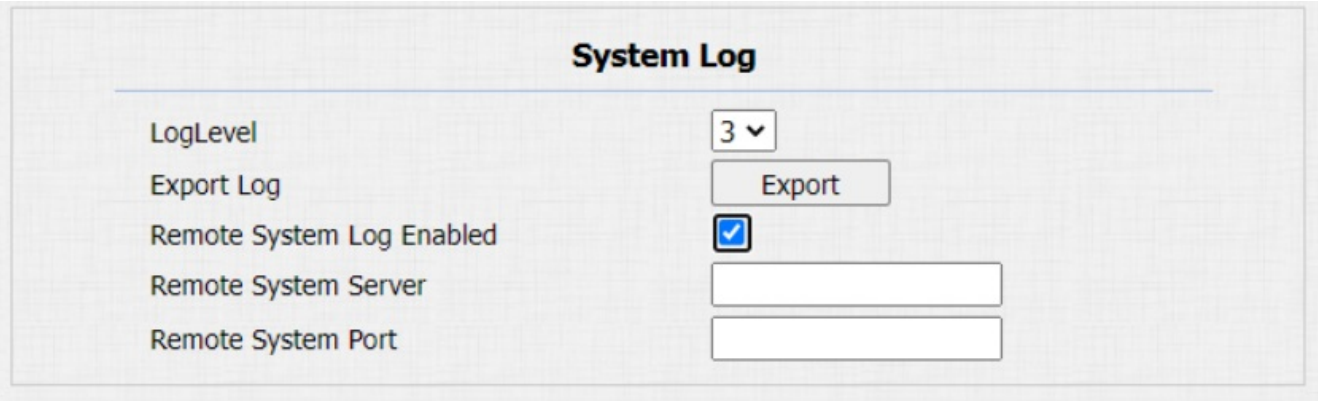
- The upgrade file is .rom format.
- Do not disconnect the device from internet and power supply when the firmware upgrade is in progress, otherwise, it might cause upgrade failure or system breakdown.

Debug

System Log

System logs can be used for debugging purposes.

Navigate to the web **Upgrade > Advanced > System Log** interface.



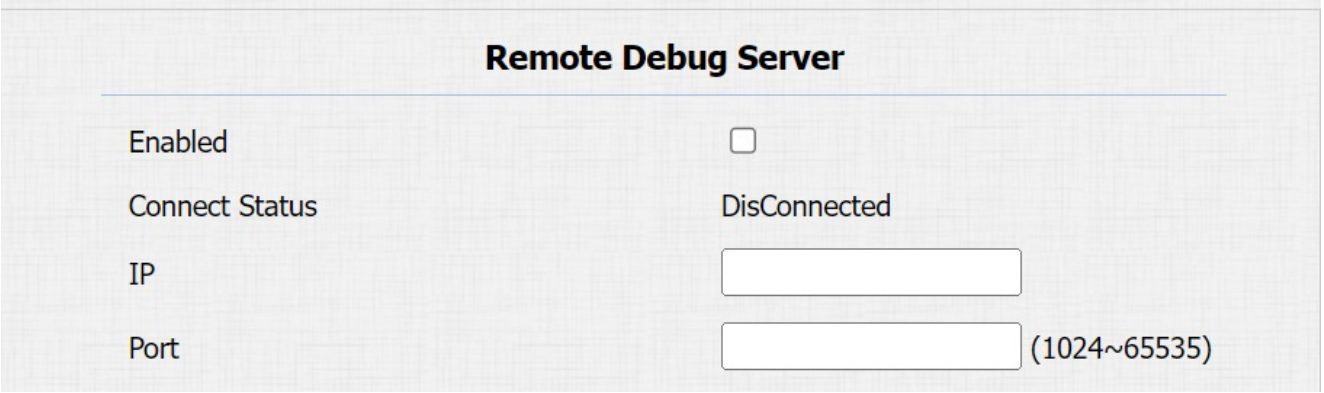
Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is **3**. The higher the level is, the more complete the log is.
- **Remote System Server**: the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.

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.

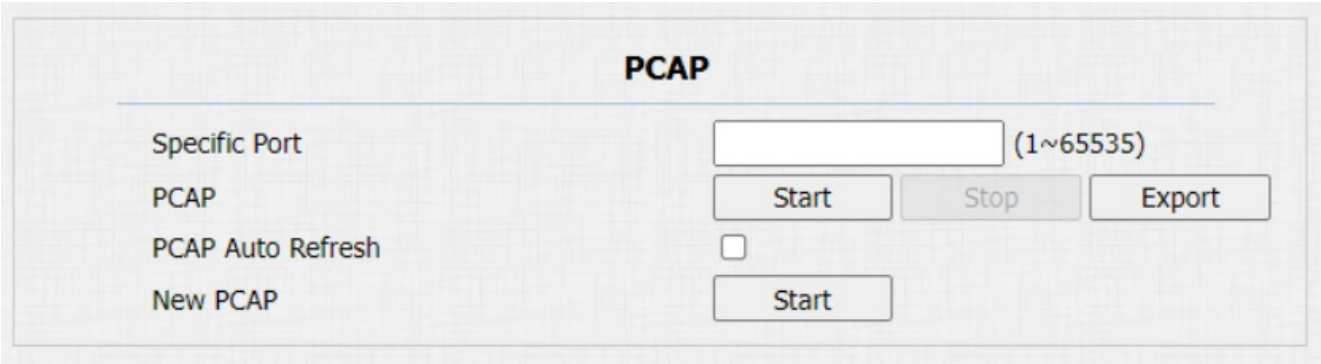
Navigate to the web **Upgrade > Advanced > Remote Debug Server** interface.



PCAP

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

Navigate to the web **Upgrade > Advanced > PCAP** interface.



Parameter Set-up:

- **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 **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: when enabled, the PCAP will continue to capture data packets even after the data packets reached their 1M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.
- **New PCAP**: click **Start** to capture bigger data package.

Backup

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

Navigate to the web **Upgrade > Advanced > Others** interface.

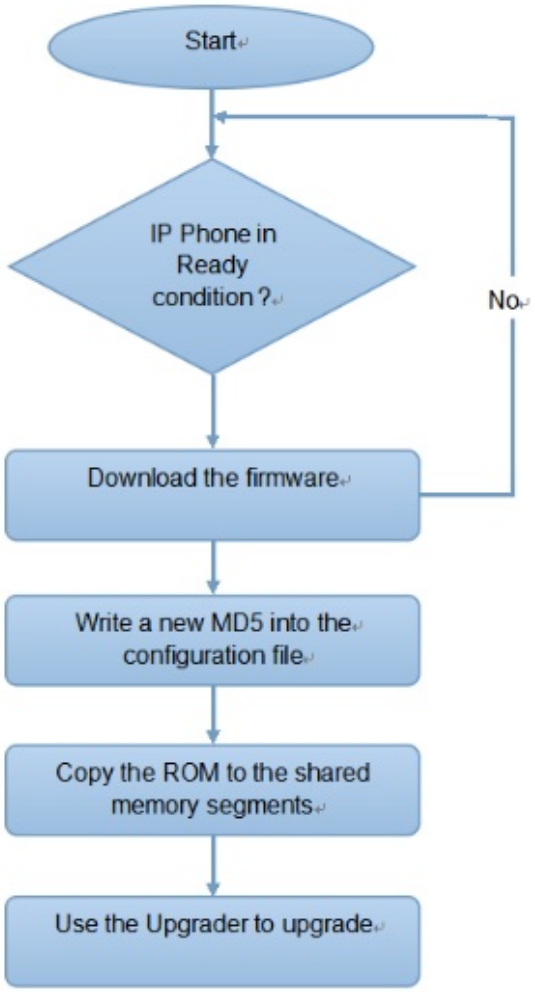
Auto-provisioning via Configuration File

You can configure and upgrade the door phone on the web interface via one-time auto- provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

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

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

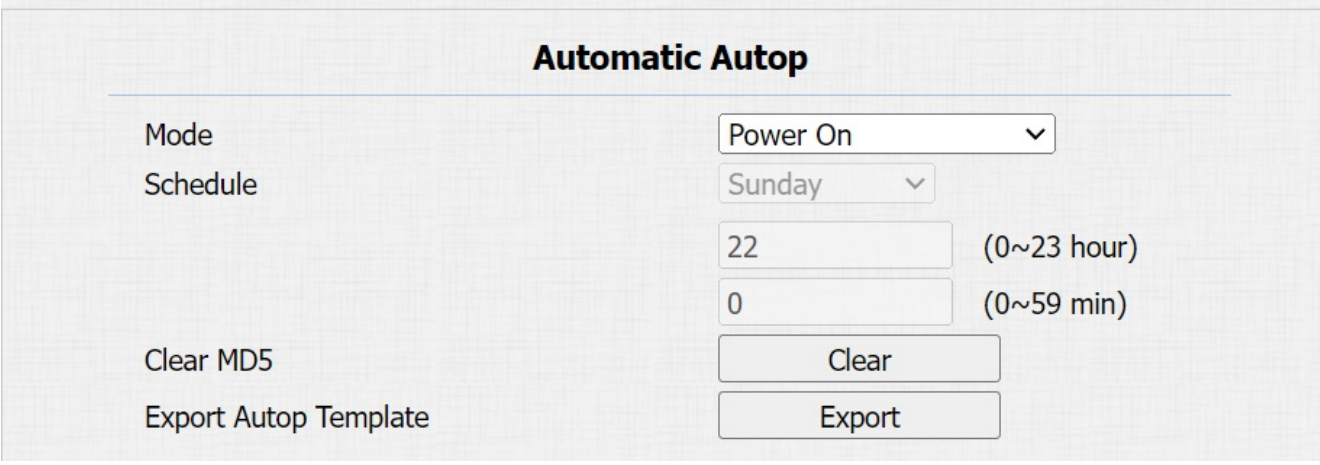
- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used for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

Note

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

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

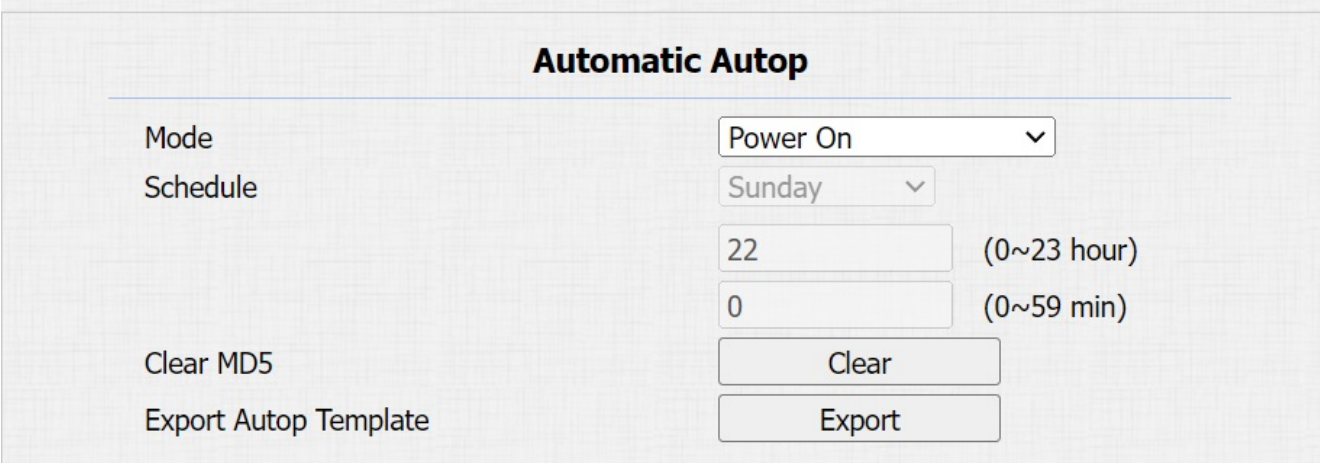
To get the Autop configuration file template on the **Upgrade > Advanced > Automatic Autop** interface.



AutoP Schedule

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

Navigate to the web **Upgrade > Advanced > Automatic Autop** interface.

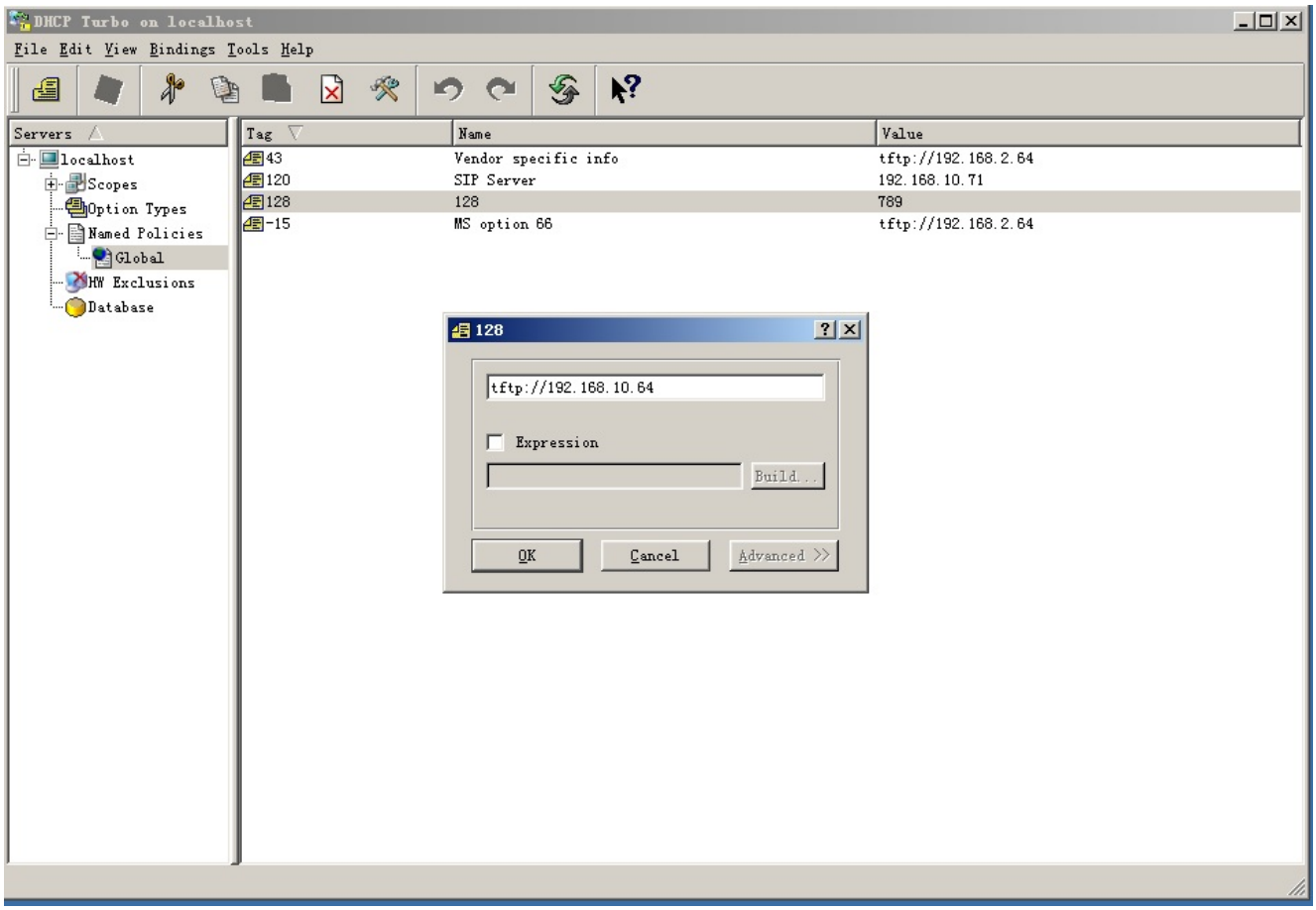


Parameter Set-up:

- **Mode**:
    - **Power on** allows the device to perform Autop every time it boots up.
    - **Repeatedly** allows the device to perform autop according to the schedule that is set up.
    - **Power On + Repeatedly** combines **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule.
    - **Hourly Repeat** allows the device to perform Autop every hour.
- **Schedule**: when **Repeatedly** is selected, you can set up the Autop schedule.

DHCP Provisioning Configuration

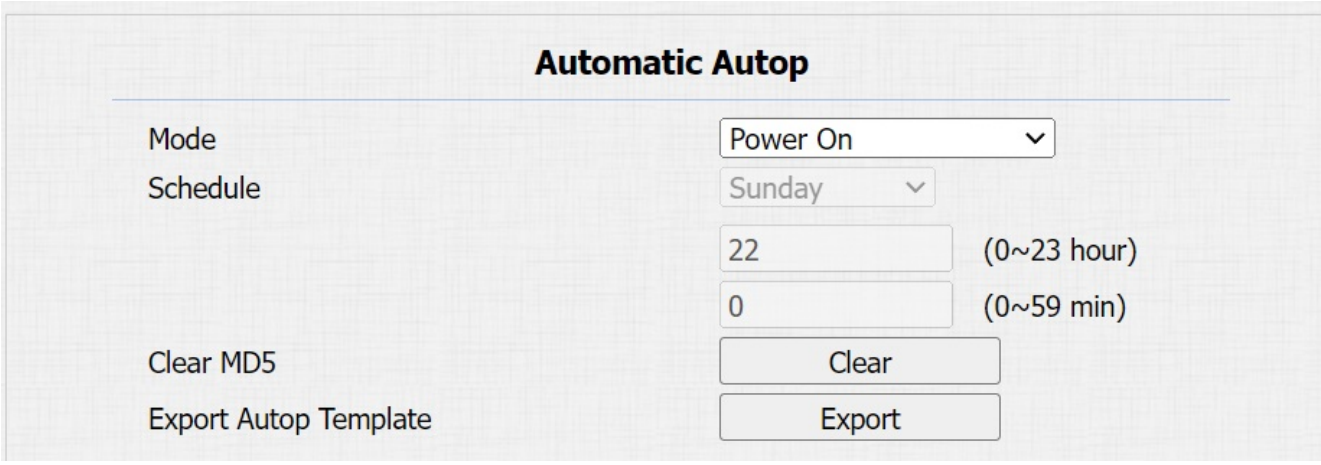
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option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



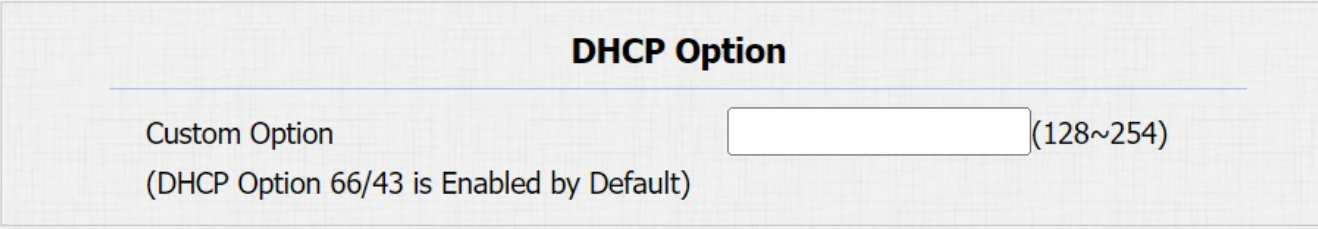
Note

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

To set up DHCP Autop with Power On mode and export Autop Template to edit the configuration. Navigate to the web **Upgrade > Advanced > Automatic Autop** interface.



Then set up DHCP Option on **Upgrade > Advanced > DHCP Option** interface.



Parameter Set-up:

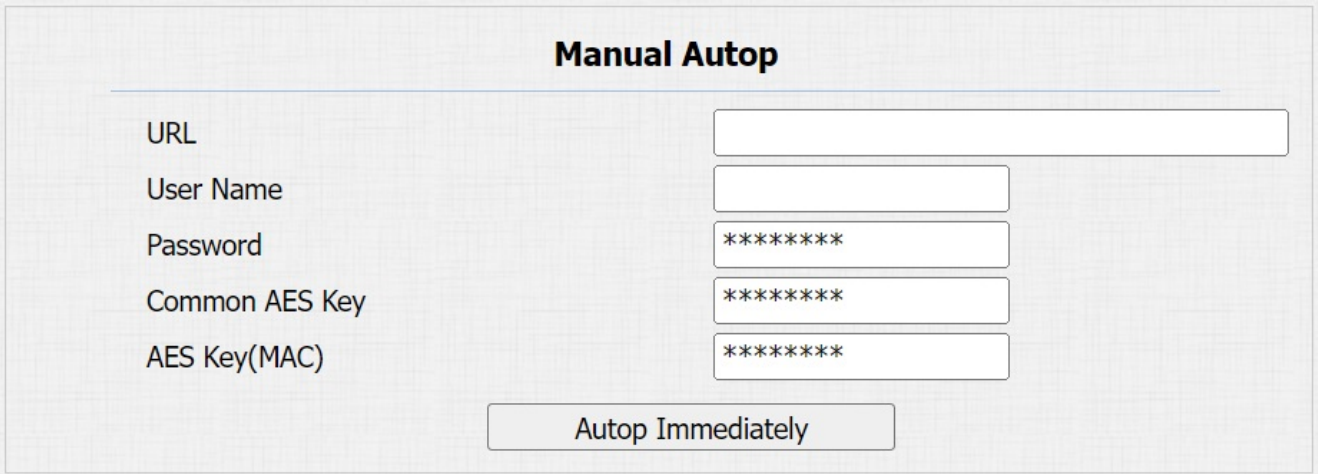
- **Custom Option**: enter the DHCP code that matched the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server 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 updated server URL in it.
- **DHCP Option 43**: if the device does not get an 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 updated server URL in it.

Note

- The general configuration file for the in-batch provisioning is in the format **r0000000000xx.cfg**. Taking X915 as an example r000000000915.cfg (**10 zeros** in total while the MAC-based configuration file for the specific device provisioning is with the format MAC Address of the device.cfg, for example, **0C110504AE5B.cfg**).
- You can upload the screen saver by Auto-provisioning.

Static Provisioning Configuration

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



Parameter Set-up:

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

Note

- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use the default port 80) http://192.168.0.19:8080/(use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/(use the default port 443)

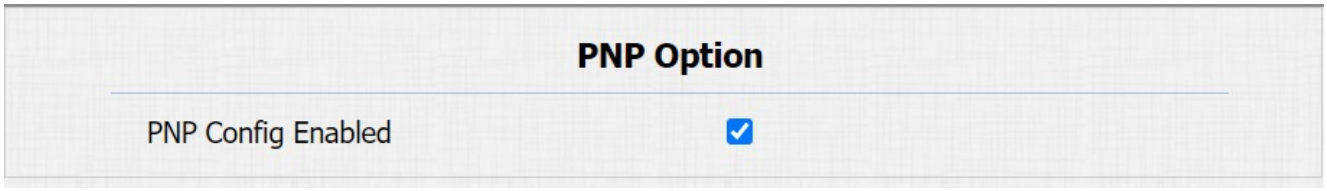
Tip

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

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.

Navigate to the web **Upgrade > Advanced > PNP Option** interface.

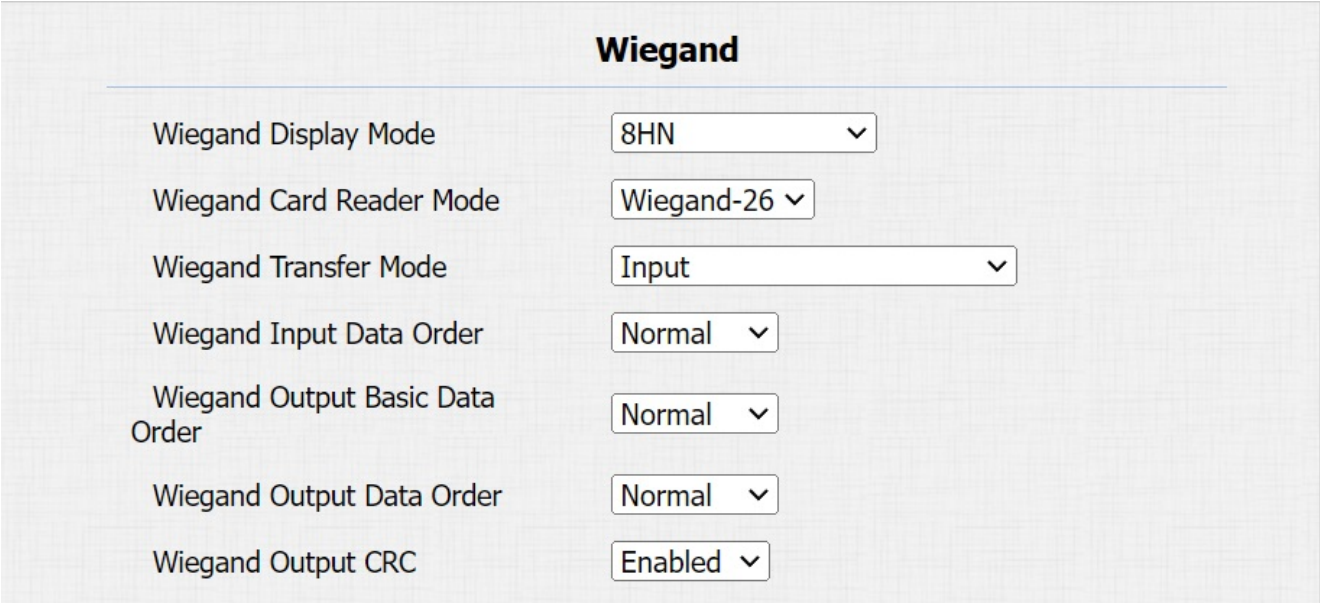


Integration with Third Party Device

Integration via Wiegand

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

Navigate to the web **Intercom > Wiegand** interface.



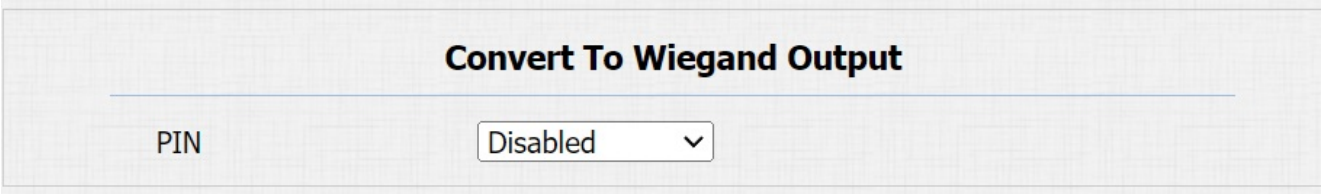
Parameter Set-up:

- **Wiegand Display Mode**: select Wiegand Card code format among 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.
- **Wiegand Card Reader Mode**: set the Wiegand data transmission format among three options: Wiegand 26, Wiegand 34, and Wiegand 58. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode**:
    - **Input**: when the door phone acts as a controller, users can swipe the RF card on the third-party card reader to open the door.
    - **Output**: users can only open the door by entering a PIN code or swiping an RF card.

  - **Convert To Card No. Output**: when users are assigned by multiple door-opening methods, data needs to be converted to the card number that the third-party device can verify.

- **Wiegand Input Data Order**: when **Normal** is selected, the card number is displayed as received. When **Reversed** is selected, the order of the card number is reversed.
- **Wiegand Output Data Order**: determines the sequence of the Wiegand output data. When **Normal** is selected, the data is displayed as received. When **Reversed** is selected, the order of the data bits 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.

When the door phone is in Wiegand output mode, you can configure the Wiegand PIN code output format that determines how data are transmitted. The format should be the same as that of the third-party device.



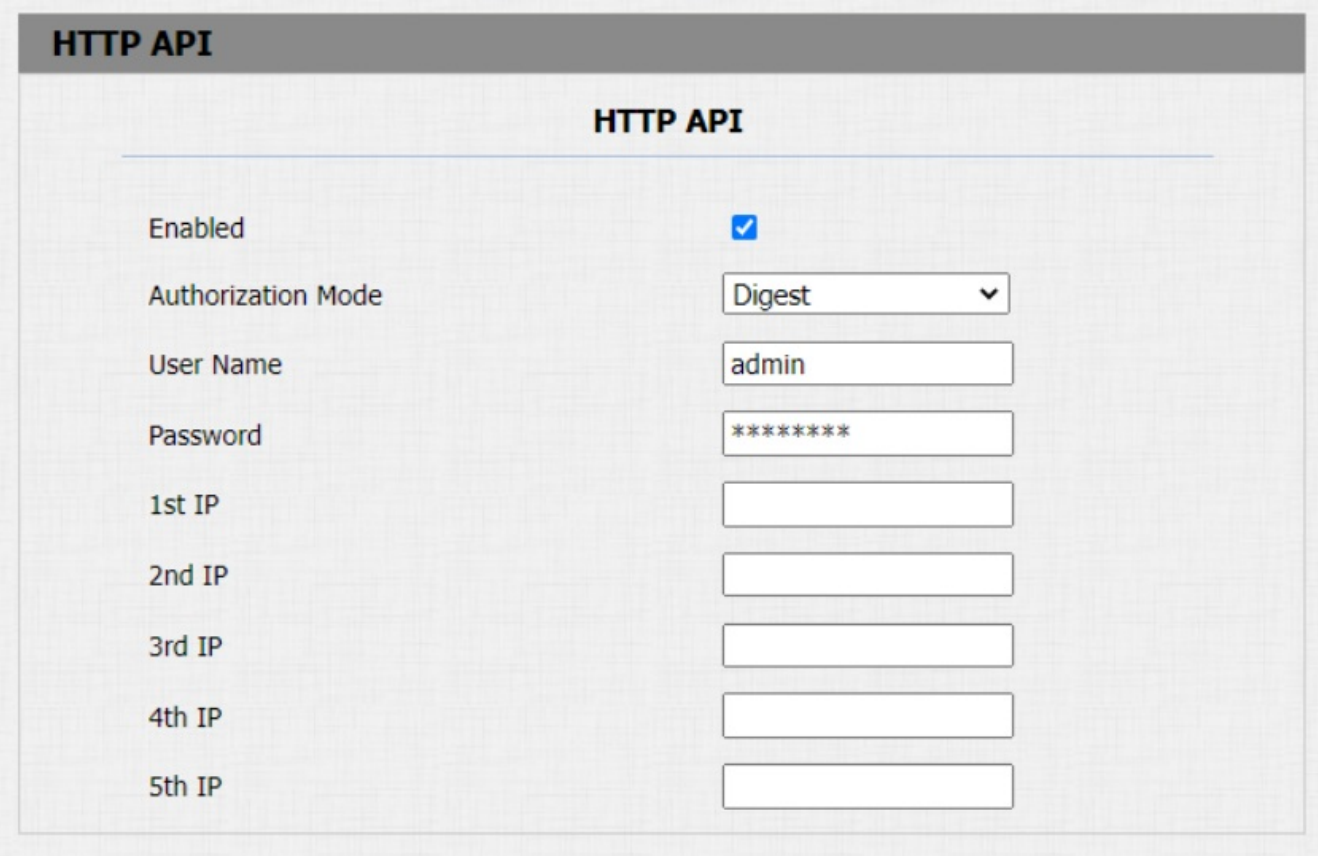
Parameter Set-up:

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

Integration via HTTP API

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

Navigate to the web **Intercom > HTTP API** interface.



Parameter Set-up:

- **Enabled**: if the function is disabled, any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Authorization Mode**: select from **None**, **Normal**, **Allowlist**, **Basic**, **Digest** and **Token** for authorization type, which will be explained in the following chart.
- **User Name**: enter the user name when **Basic** and **Digest** authorization mode is selected. The default is **admin**.
- **Password**: enter the password when **Basic** and **Digest** authorization mode is selected. The default is **admin**.
- **1st IP-5th IP**: enter the IP address of the third party devices when the **Allowlist** authorization is selected for the integration.

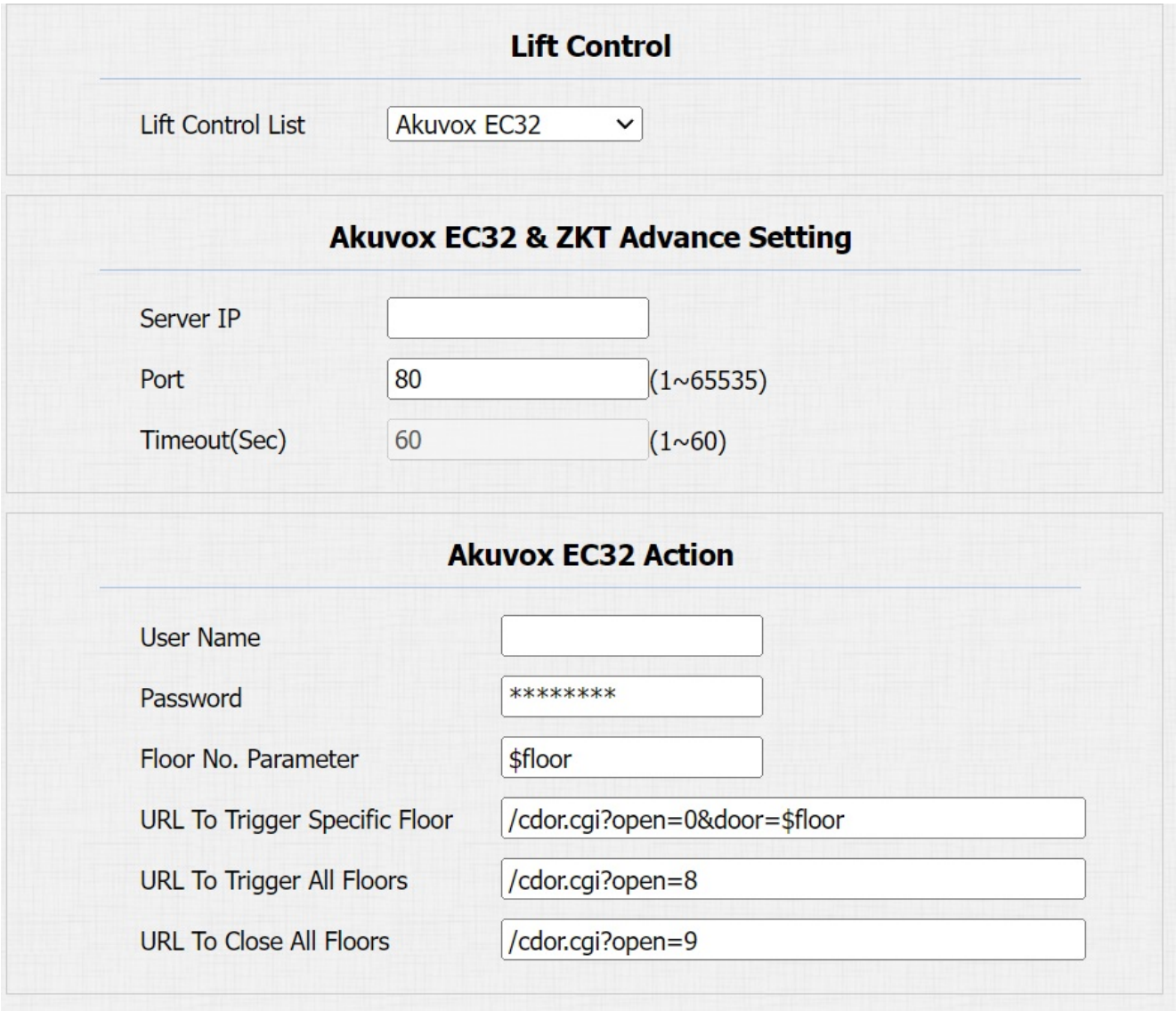
Please refer to the following description for the Authentication mode:

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

Lift Control Configuration

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

Navigate to the web **Intercom > Lift Control** interface.



Parameter Set-up:

- **Life Control List** : select the lift controller brand.

NO.	header	header
1	None	If you select **None**, then the RS485 integration will be disabled.
2	Akuvox EC32	Select **Akuvox EC32** if you want to connect the device with Akuvox EC33 lift controller.
3	KEKING	Select **KEYKING** if you want to integrate with KEYKING lift controller.
4	ZKT	Select **ZKT** if you want to integrate with **ZKTeco** lift controller
5	Chiyu	Select **Chiyu** if you want to integrate with **Chiyu** lift controller

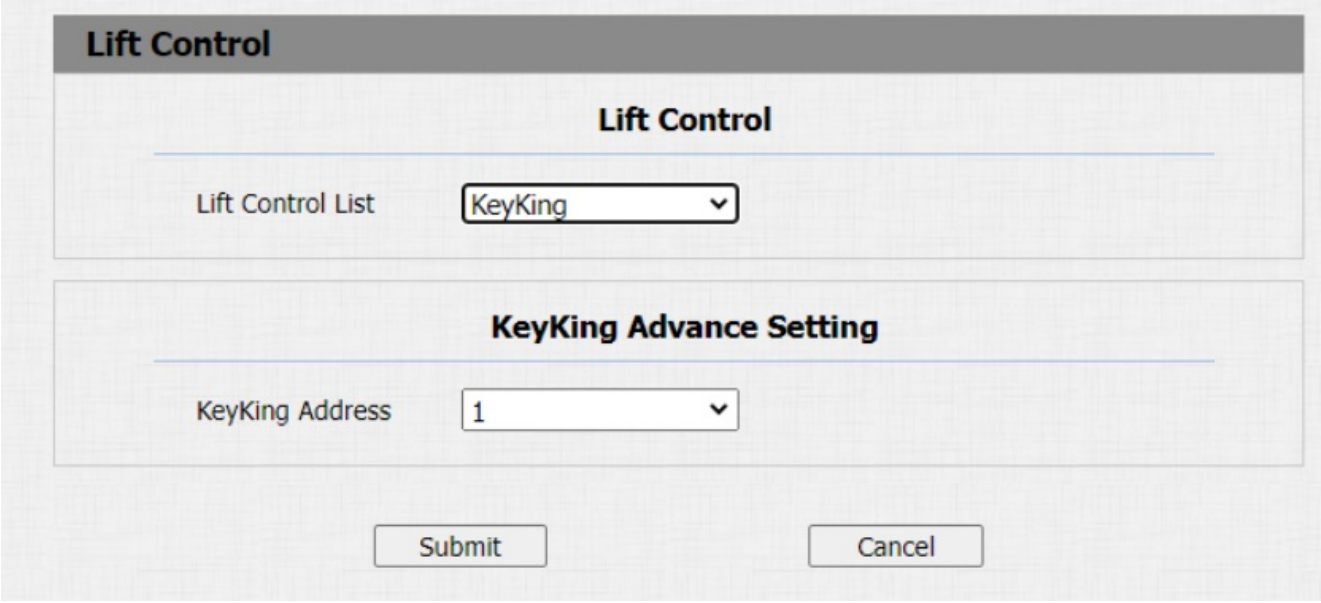
Note

- Please consult with Akuvox technical support if you have any inquiries on the integration mode of any OEM lift controller integration project.

KeyKing Setting

To integrate KeyKing lift controller, you are required to set up the KeyKing address obtained from your solution provider.

Navigate to the web **Intercom > Lift Control** interface and select KeyKing.

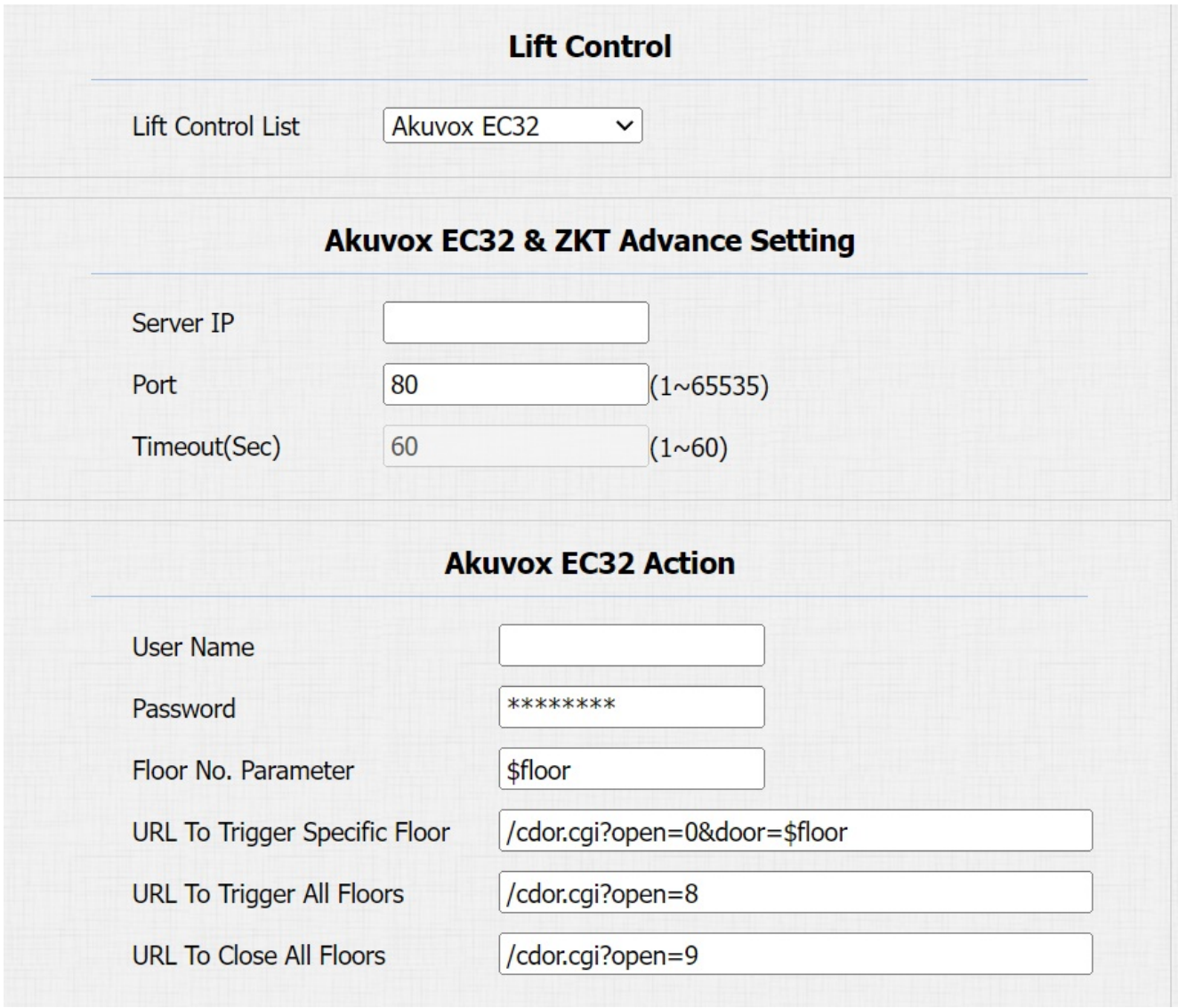


Parameter Set-up:

- **KeyKing Address**: enter the KeyKing address provided by your solution provider. The address number must be identical with the address number on the lift controller board.

Akuvox EC32 Lift Controller

Navigate to the web **Intercom > Lift Control** interface and select **Akuvox EC32**.



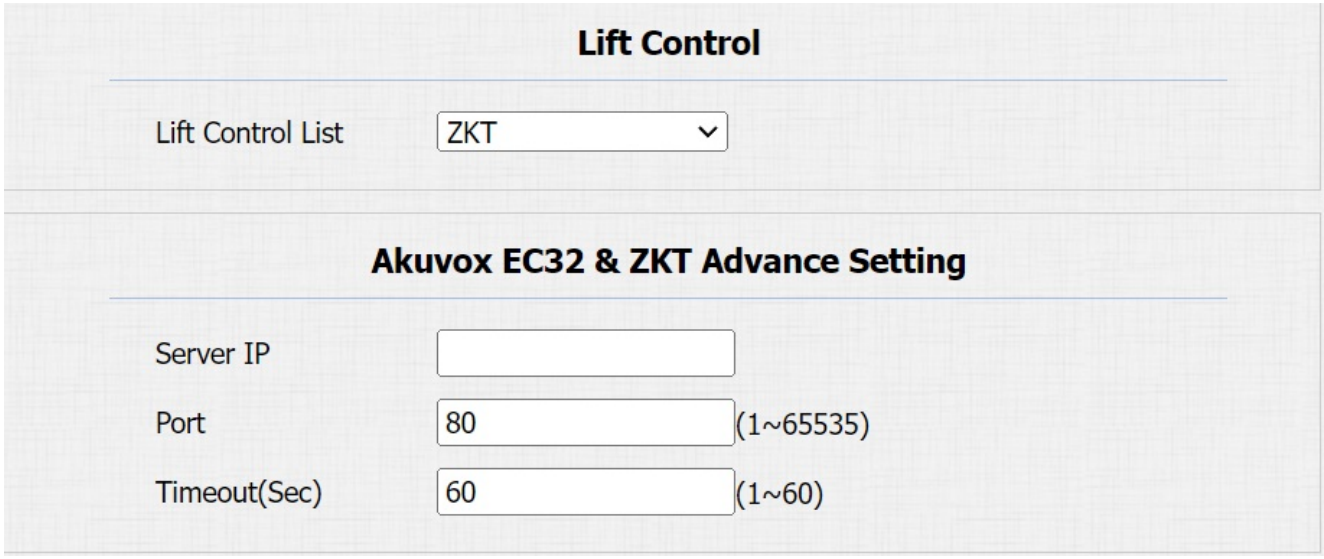
Parameter Set-up:

- **Timeout (Sec)**: enter the lift controller timeout. For example, if you set the timeout as 30 seconds, users have to press the lift button corresponding to the floor they are going to within 30 seconds, otherwise, the button will be locked again, and users have to go out of the lift and do it all over again.
- **User Name**: enter the user name of the lift controller for the authentication.
- **Password**: enter the password of the lift controller for the authentication.
- **Floor NO. Parameter**: enter the Floor number parameter provided by Akuvox. The default parameter string is "**$floor**". You can define your own parameter string if needed.

- **URL To Trigger Specific Floor**: enter the Akuvox life 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 with the parameter string you defined.

ZKT Lift Controller

Navigate to the web **Intercom > Lift Control** interface and select **ZKT**.

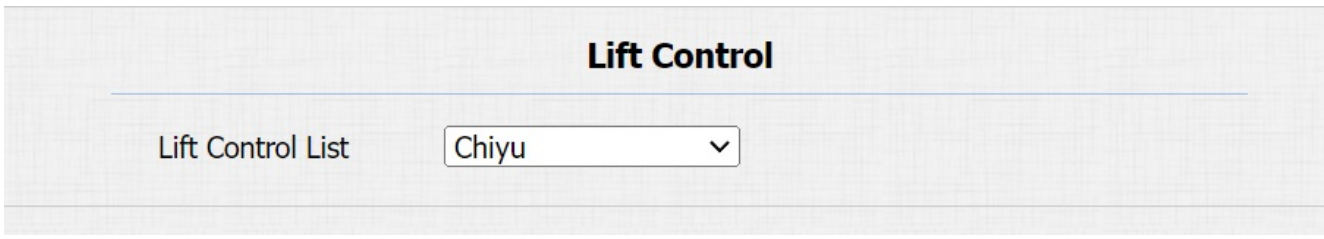


Parameter Set-up:

- **Timeout (Sec)**: enter the lift controller timeout. For example, if you set the timeout as 30 seconds, users have to press the lift button corresponding to the floor they are going to within 30 seconds, otherwise, the button will be locked again, and users have to go out of the lift and do it all over again.

Chiyu Lift Controller

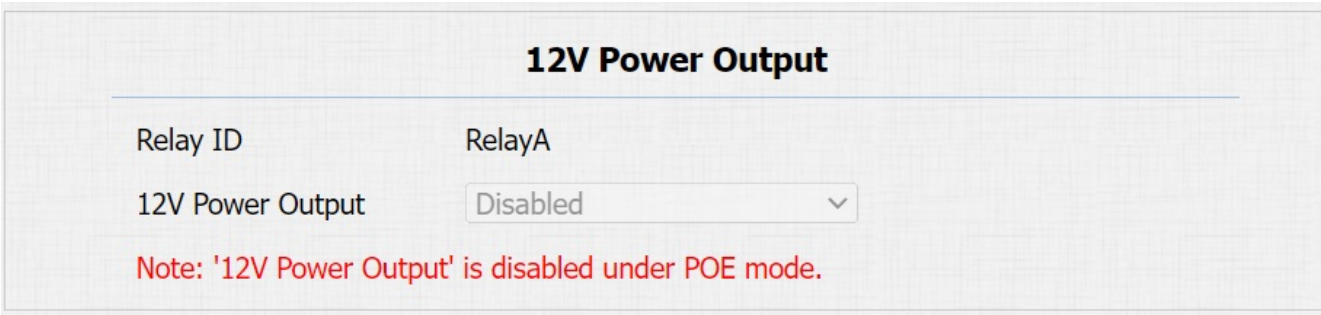
Navigate to **Intercom > Lift Control** and select **Chiyu**.



Power Output Control

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

Navigate to the web **Intercom > Relay > 12V Power Output** interface.



Parameter Set-up:

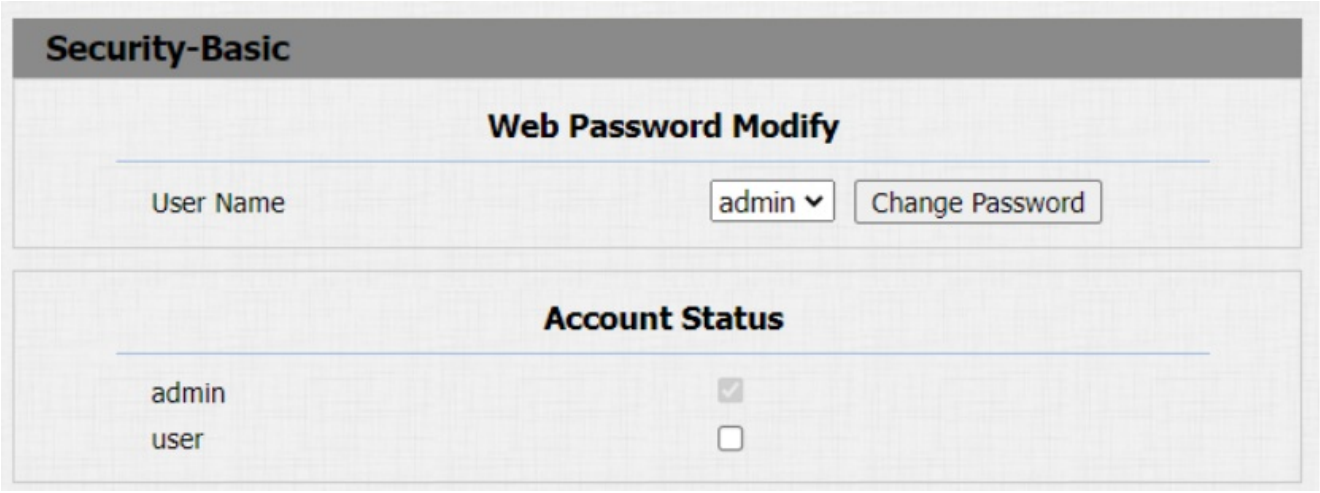
- **12V Power Output**: select Disabled to disable the power output function; select Always to enable the access controller to provide continuous power to the third-party device. Select Triggered By Open Relay if you want the door phone to provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high. Select Security Relay A to power security relay.

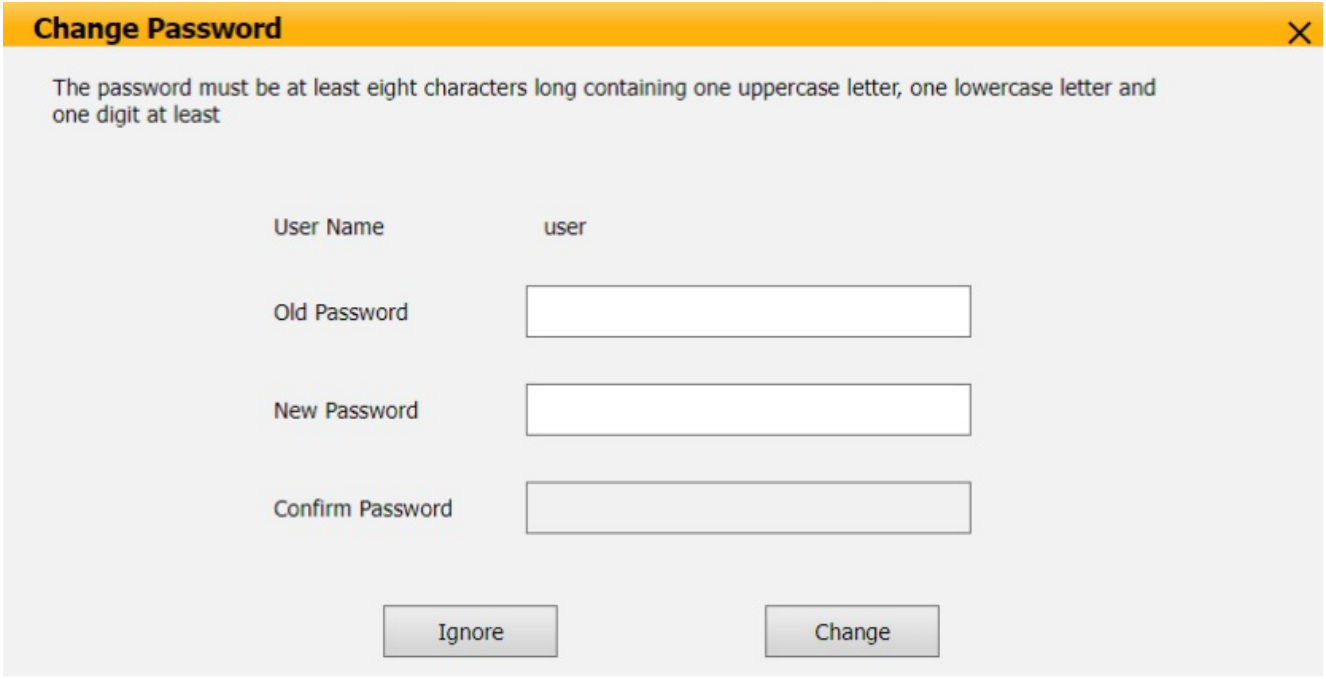
Password Modification

Modify Device Web Interface Password

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

Navigate to the web **Security > Basic** interface.





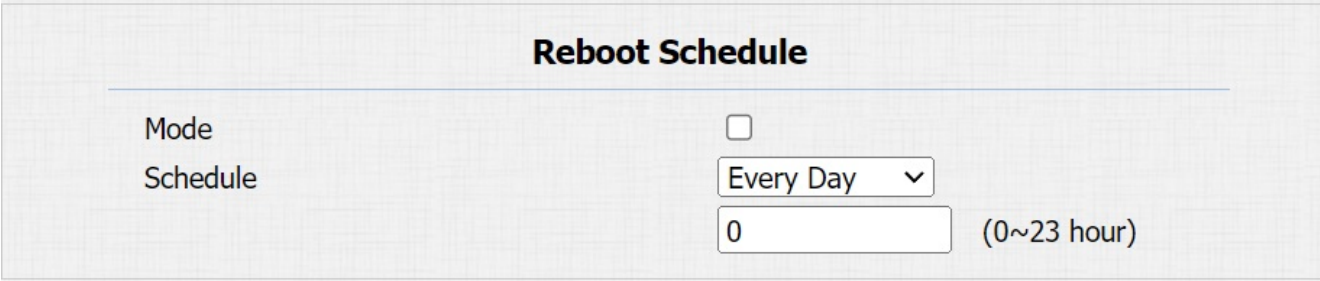
System Reboot&Reset

Reboot

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

Navigate to the web **Upgrade > Basic** interface.

To set up the schedule, navigate to the web **Upgrade > Advanced > Reboot Schedule** interface.



Reset

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

Navigate to the web **Upgrade > Basic** interface.