About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

E12 SERIES DOOR PHONE

Administrator Guide

Thank you for choosing the Akuvox E12 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to firmware version 312.30.10.18 and it provides all the configurations for the functions and features of the E12 and E12S-2 door phones. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

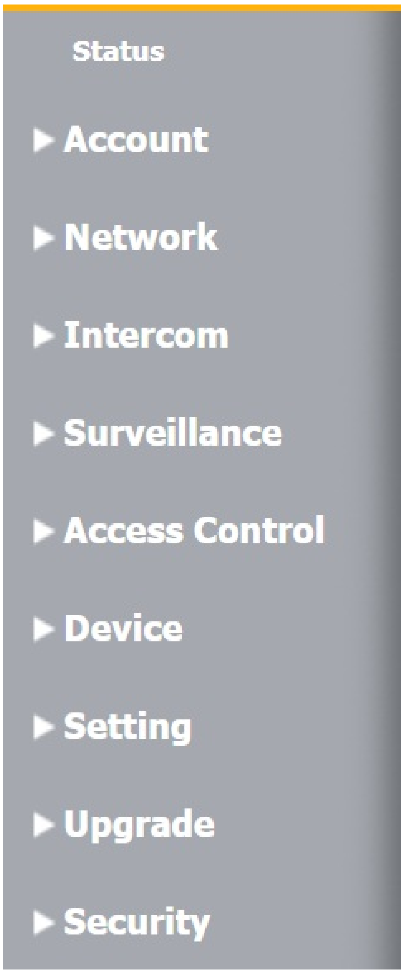
The security provided by controlling access to your building, and verifying identities verbally and visually, is invaluable. Akuvox E12 series door phones, SIP-compliant, can connect with Akuvox indoor monitors for remote access control and monitoring. Users can interact with visitors through audio and video calls, granting access. This door phone allows effortless monitoring of entry points, ensuring enhanced facility security and peace of mind.

Model Specification and Differences

Model	E12W	E12S
Camera	2M pixels, automatic lighting	2M pixels, automatic lighting
Relay In	2	2
Relay Out	1	1
RS485	X	X
WiFi	✔	X
Card Reader	✔	✔
Microphone	1	1
Speaker	1	1
Bluetooth	✔	✔
TF Card Slot	1	1
Wiegand Port	✔	✔
Tamper Alarm	✔	✔
Power Supply	802.3af Power-over-Ethernet 12V DC Connector(If not using PoE)	802.3af Power-over-Ethernet 12V DC Connector(If not using PoE)

Introduction to Configuration Menu

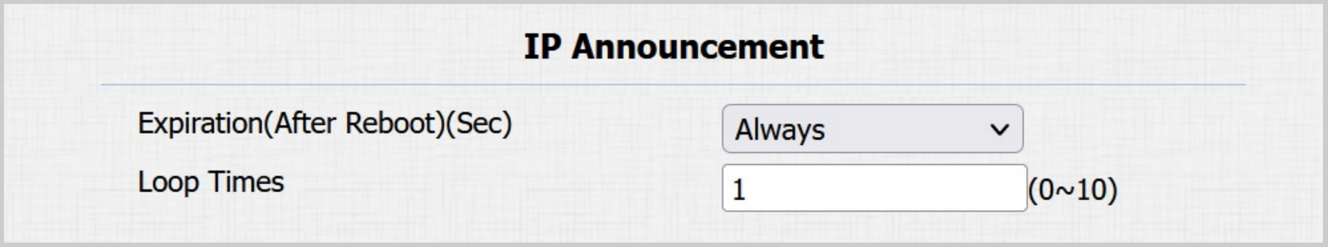
- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, etc.
- **Network:** This section mainly deals with DHCP & static IP settings, RTP port settings, device deployment, etc.
- **Intercom:** This section covers intercom settings, call logs, etc.
- **Surveillance:** This section covers motion detection, RTSP, MJPEG, ONVIF, and live streaming.
- **Access Control:** This section covers input control, relay, card settings, private PIN code, Wiegand connection, etc.
- **Device:** This section includes LED, audio, and SD card settings.
- **Setting:** This section includes time & language, action settings, door settings, and schedule for access control.
- **Upgrade:** This section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and fault diagnosis.
- **Security:** This section covers high-security mode configuration, password modification, tamper alarm, HTTP API settings, etc.


Status
▶ Account
▶ Network
▶ Intercom
▶ Surveillance
▶ Access Control
▶ Device
▶ Setting
▶ Upgrade
▶ Security

Access the Device

Obtain Device IP Address

Check the Device IP address by holding the push button. You can set up the IP announcement loop times on the **Device** > **Audio** interface.



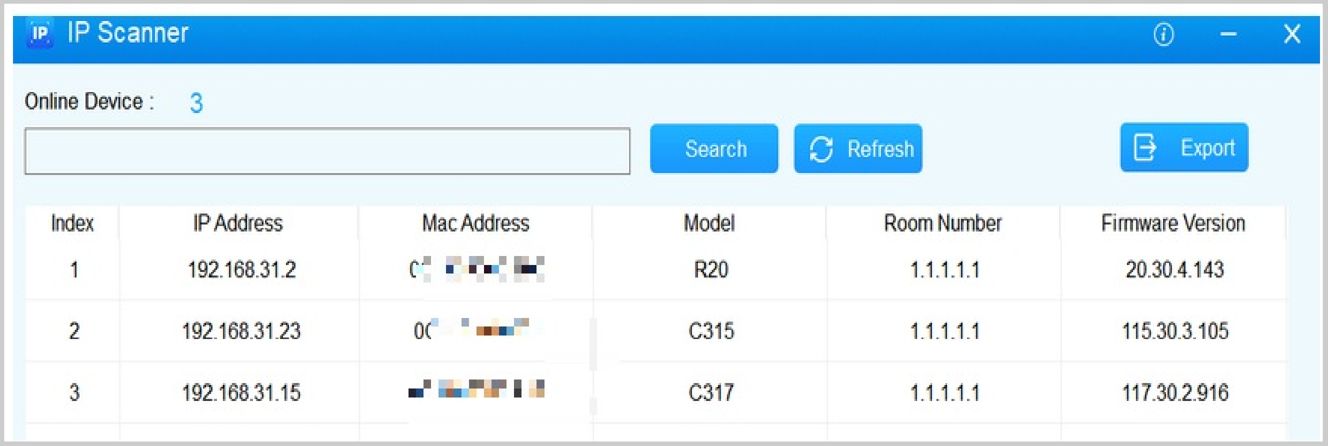
IP Announcement

Expiration(After Reboot)(Sec)	Always
Loop Times	1 (0~10)

- **Expiration(After Reboot)**
  (Sec): Set the time limit within which users should hold the call button to sound the IP announcement after the device
  reboot. If you select Always, users can hold the call button anytime for IP announcement afte r the device reboot.

- **Loop Times:** Set the IP announcement loop times.

Or search the device IP by the IP scanner in the same LAN network. Click **Refresh** to update the list.



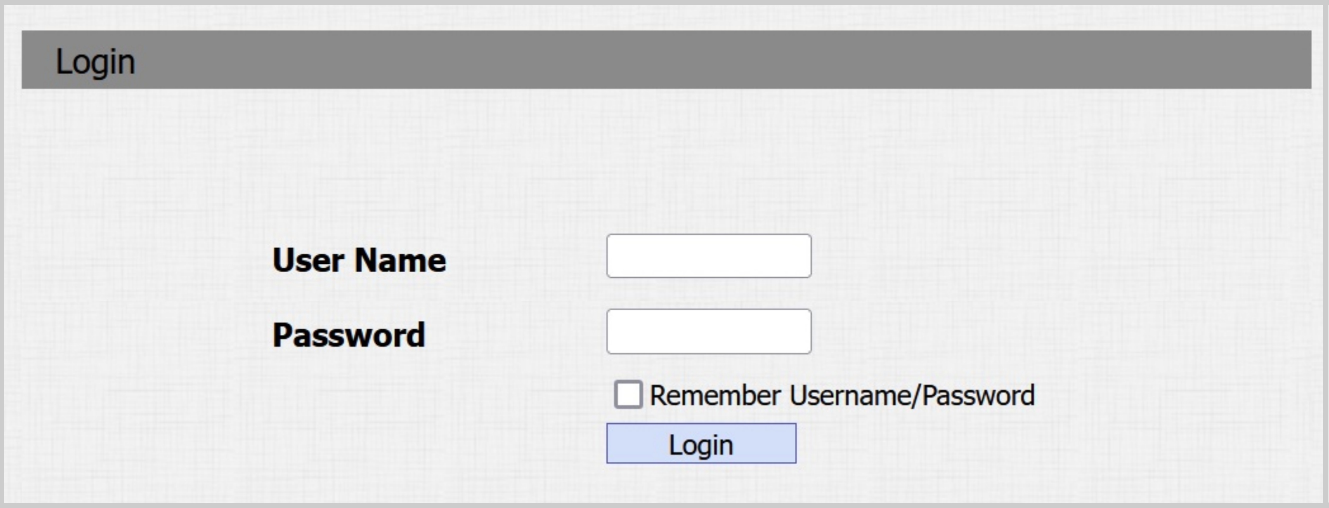
Online Device : 3

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.31.2	[redacted]	R20	1.1.1.1.1	20.30.4.143
2	192.168.31.23	[redacted]	C315	1.1.1.1.1	115.30.3.105
3	192.168.31.15	[redacted]	C317	1.1.1.1.1	117.30.2.916

Access the Device Setting

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 username and password are **admin** and please be case-sensitive to the usernames and passwords entered.



Login

User Name

Password

□ Remember Username/Password

Login

Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See the detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.

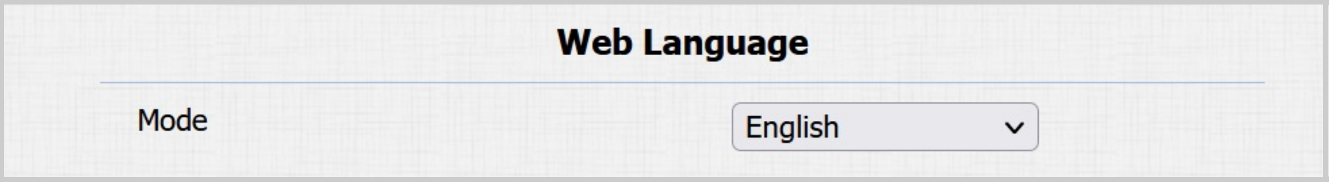
Language and Time Setting

Language Setting

You can set up the device web language on the device web **Setting** > **Time/Lang** > **Web Language** interface.

The device supports the following web languages:

English, Russian, Portuguese, Spanish, Italian, Dutch, French, German, and Turkish.



Web Language

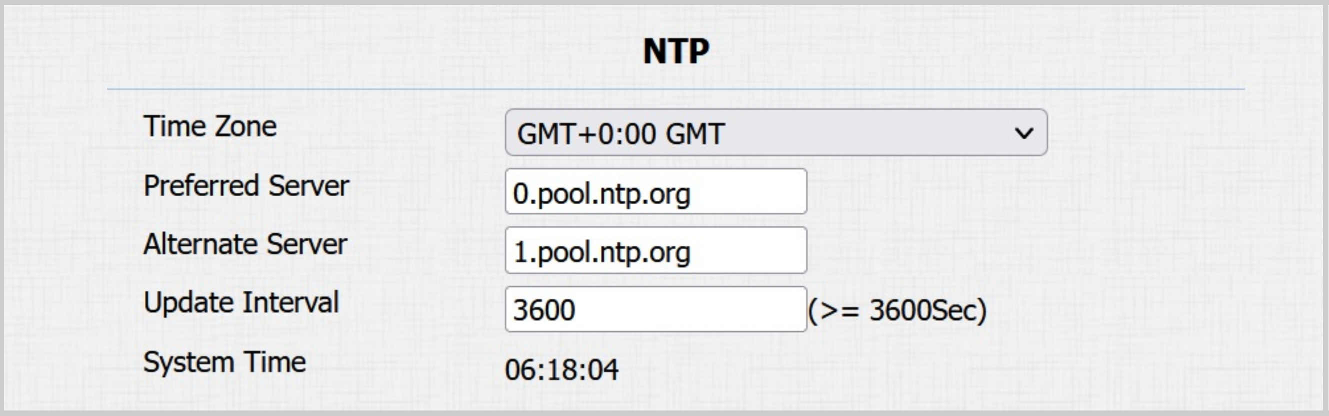
Mode: English

- **Mode:** English is the default web language.

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.

Set it up on the **Setting** > **Time/Lang** > **NTP** interface.



NTP

Time Zone: GMT+0:00 GMT

Preferred Server: 0.pool.ntp.org

Alternate Server: 1.pool.ntp.org

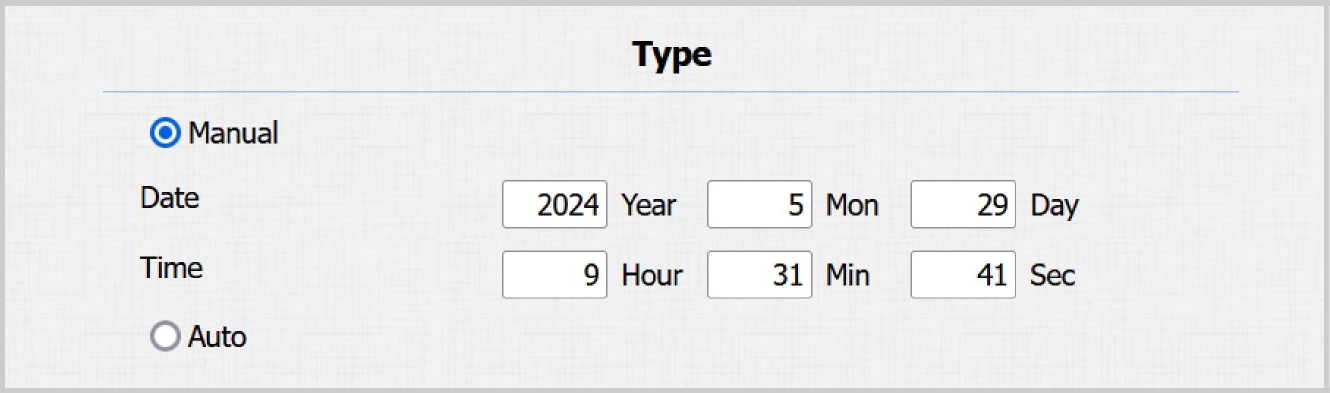
Update Interval: 3600 (>= 3600Sec)

System Time: 06:18:04

- **Time Zone**: Select the specific time zone based on where the device is used. The default time zone is GMT+0:00.

- **Preferred Server**: Enter the primary NTP server address for updating the time. The default NTP server address is 0.pool.ntp.org.
- **Alternate Server**: Enter the backup NPT server address when the primary one fails.
- **Update Interval**: Set the time update interval. For example, if you set it as 3600s, the device will send a request to the NPT server for the time update every 3600 seconds.
- **System Time**: Display the current device time.

You can also set up the time manually. Select **Manual,** and enter the date and time.



Type

● Manual

Date	2024	Year	5	Mon	29	Day
Time	9	Hour	31	Min	41	Sec

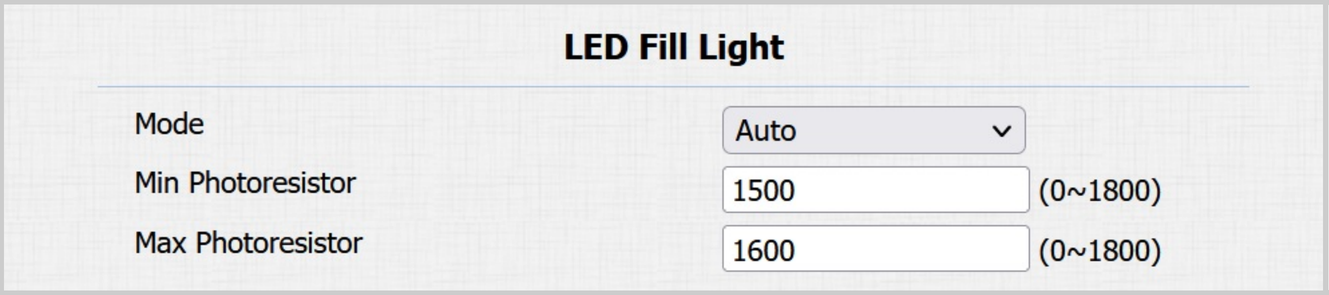
○ Auto

LED Setting

LED Light Setting

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

Set it up on the **Device > LED Setting > LED Fill Light** interface.



LED Fill Light

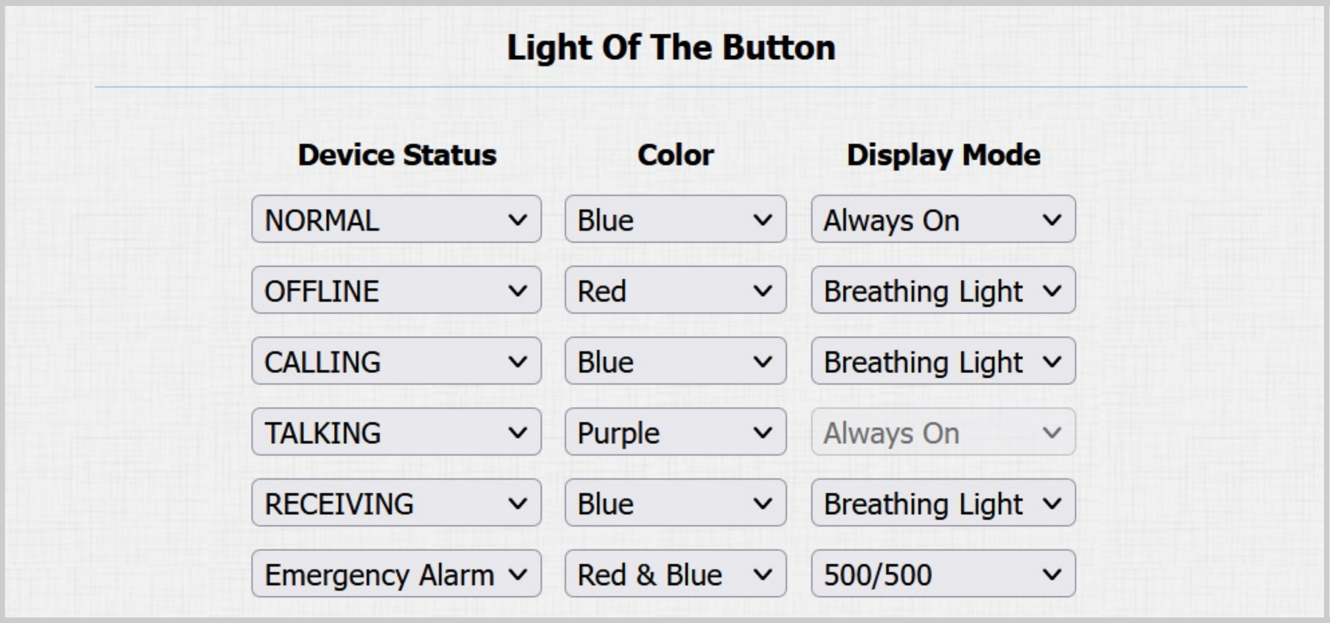
Mode	Auto	
Min Photoresistor	1500	(0~1800)
Max Photoresistor	1600	(0~1800)

- **Mode:**
  - **Auto** turns on the LED light automatically.
  - **Aways OFF** turns off the LED light.
  - **Specific Time** turns on the LED according to the 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 LED to be turned on and the minimum value for it to be turned off.

LED Light Status

LED display adjustment is used to indicate the light changes of the call button in different states. The LED status allows users to verify the current mode of the device.

Set it up on the web **Device > LED Setting > Light of The Button** interface.



Light Of The Button

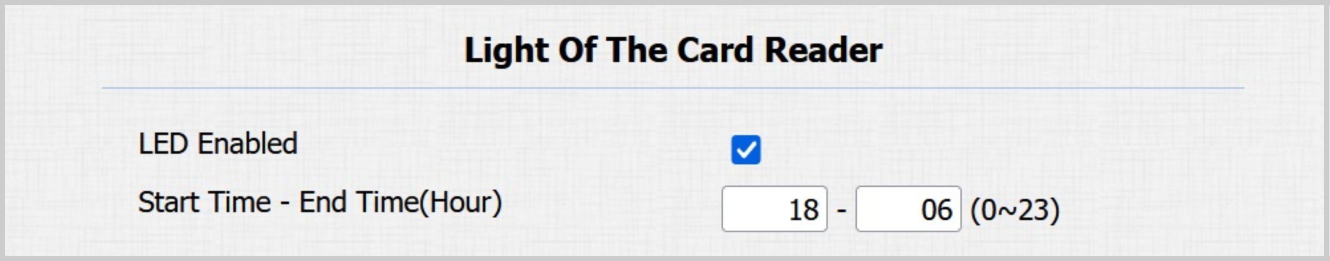
Device Status	Color	Display Mode
NORMAL	Blue	Always On
OFFLINE	Red	Breathing Light
CALLING	Blue	Breathing Light
TALKING	Purple	Always On
RECEIVING	Blue	Breathing Light
Emergency Alarm	Red & Blue	500/500

- **Device Status:** There are six statuses, Normal, Offline, Calling, Talking, Receiving, and Emergency Alarm. The status cannot be changed.
- **Color:** Select from Blue, Red, and Purple. You can select Red & Blue(flashing red and blue alternately) for Emergency Alarm status.
- **Display Mode:** Set the different flashing frequencies.

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.

Set it up on the **Device > LED Setting > Light of The Card Reader** interface.



Light Of The Card Reader

LED Enabled ☑

Start Time - End Time(Hour) 18 - 06 (0~23)

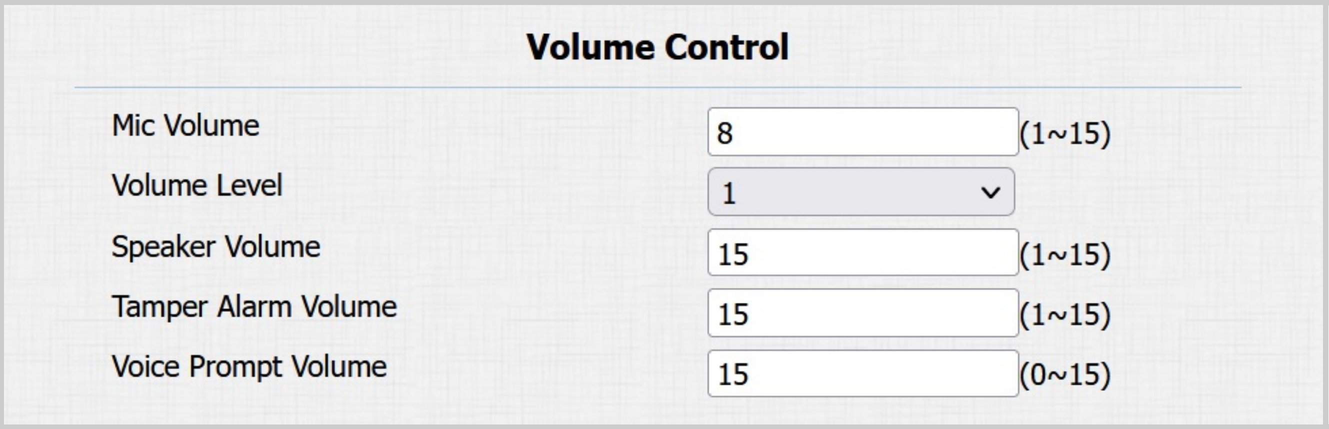
- **Start Time - End Time(Hour):** Set the LED light valid time. If the time is set from 8-0(Sart time- End time), the LED light will stay on from 8:00 a.m. to 12:00 p.m. for one day(24 hours).

Volume and Tone Configuration

Volume and tone configuration include various volume controls. Moreover, you can upload tones to enrich the user experience.

Volumes

To set up volumes, go to the web **Device > Audio** interface.



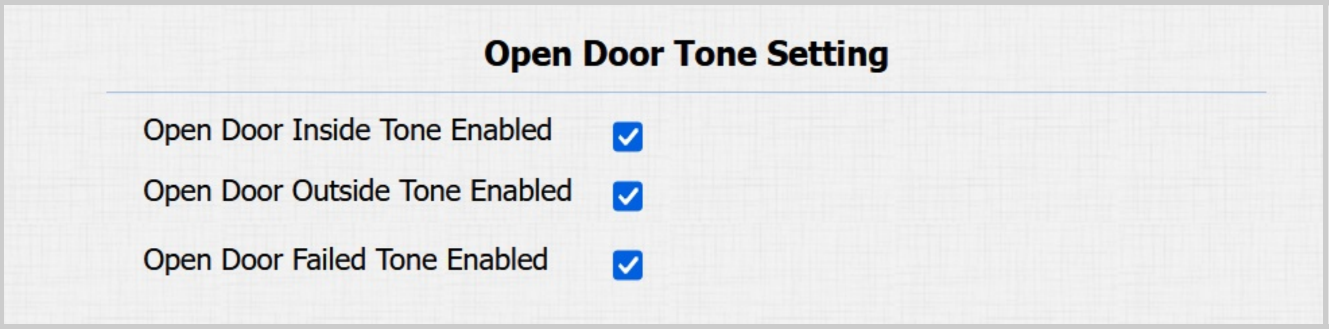
Volume Control

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

- **Tamper Alarm Volume**: Set the volume when the tamper alarm is triggered.
- **Voice Prompt Volume**: Set the voice prompt volume.

Open Door Tones

You can enable or disable the door-opening tones on the web **Device > Audio > Open Door Tone Setting** interface.



Open Door Tone Setting

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

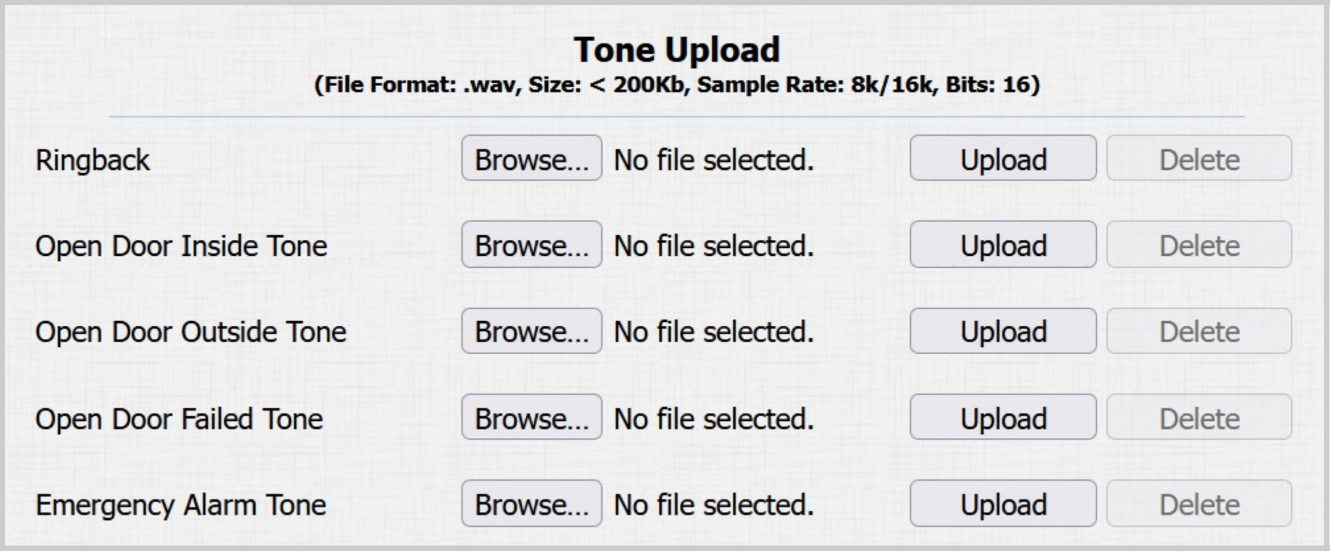
- **Open Door Inside Tone Enabled:** The tone sounds when users open the door by pressing the Exit Button.
- **Open Door Outside Tone Enabled:** The tone sounds when users open doors via various device-supported access methods.

- **Open Door Failed Tone Enabled**: The tone sounds when opening the door fails.

Upload Tone Files

You can customize ringback, door-opening, and emergency alarm tones.

Upload files on the **Device** > **Audio** > **Tone Upload** interface.



Tone Upload

(File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16)

Ringback	Browse...	No file selected.	Upload	Delete
Open Door Inside Tone	Browse...	No file selected.	Upload	Delete
Open Door Outside Tone	Browse...	No file selected.	Upload	Delete
Open Door Failed Tone	Browse...	No file selected.	Upload	Delete
Emergency Alarm Tone	Browse...	No file selected.	Upload	Delete

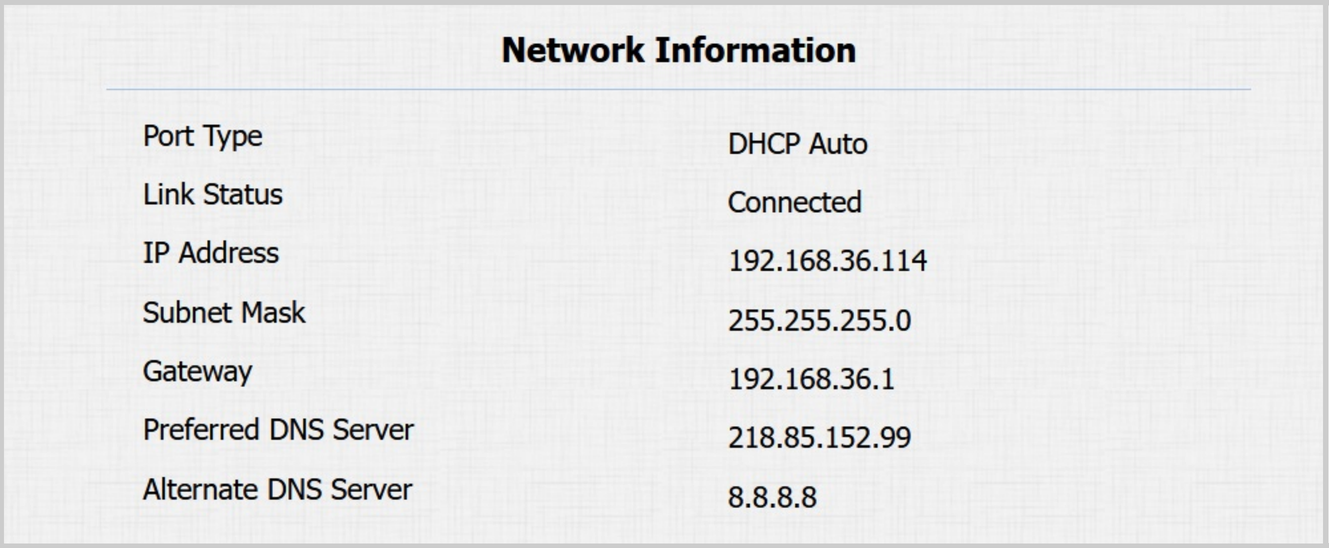
- **Ringback:** The tone is heard by the users who call the device.
- **Open Door Inside Tone:** The tone sounds when users open the door by pressing the Exit button.
- **Open Door Outside Tone:** The tone sounds when users open doors via various device-supported access methods.
- **Open Door Failed Tone:** The tone sounds when the door opening fails.
- **Emergency Alarm Tone:** The tone sounds when the emergency alarm is triggered.

> **Note**
>
> File Format: .wav, Size: < 200Kb, Sample Rate: 8k/16k, Bits: 16.

Network Setting

Network Status

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



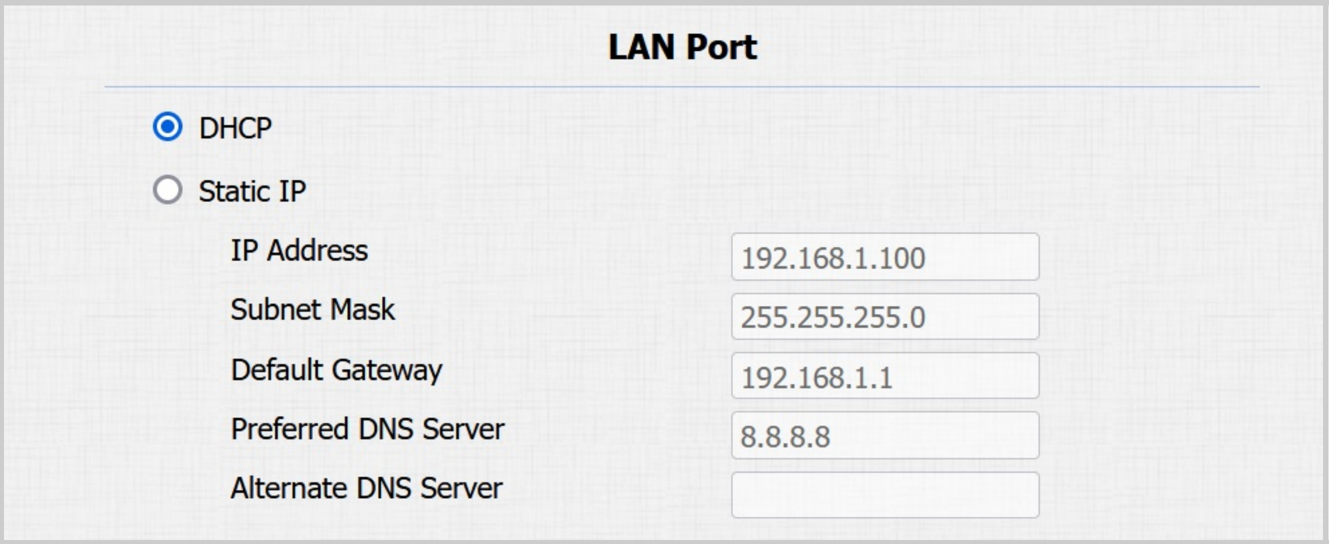
Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.114
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8

Device Network Configuration

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

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



LAN Port

● DHCP

○ Static IP

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

- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the device 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 server address should be configured according to the network environment.

- **IP Address**: Set up the IP address when the static IP mode is selected.

- **Subnet Mask**: Set up the subnet mask according to the actual network environment.

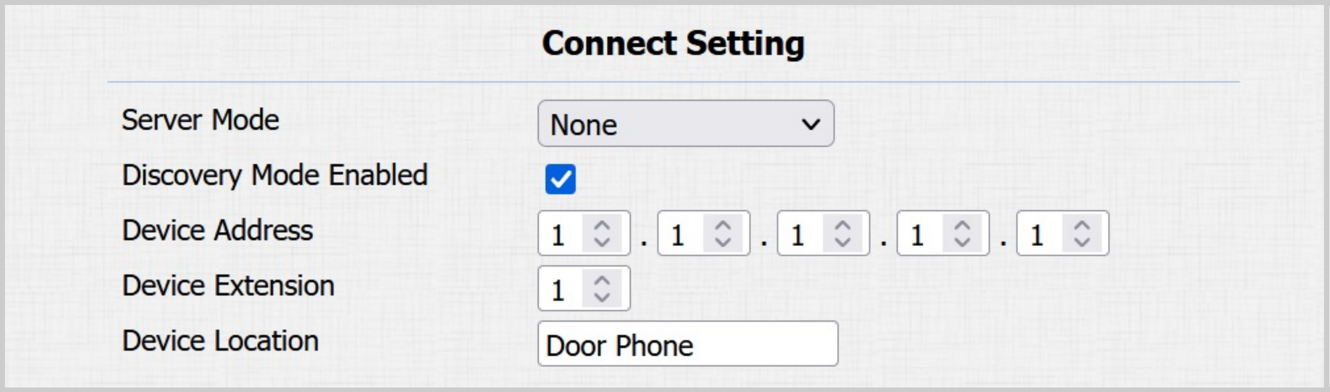
- **Default Gateway**: Set up the correct gateway according to the IP address.

- **Preferred/Alternate DNS Server**: Set up the preferred or alternate Domain Name Server(DNS) server according to the actual network environment. The preferred DNS server is the primary server while the alternate DNS server is the secondary one. The secondary server is for backup.

Device Deployment in Network

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

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



Connect Setting

Server Mode	None
Discovery Mode Enabled	☑
Device Address	1 . 1 . 1 . 1 . 1
Device Extension	1
Device Location	Door Phone

- **Server Mode**: It is automatically set up according to the device connection with a specific server in the network such as SDMC, Cloud, or None. **None** is the default factory setting indicating the device is not in any server type.

- **Discovery Mode Enabled**: When enabled, the device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.

- **Device Address**: Specify the device address by entering device location information from the left to the right: Community, Unit, Stair, Floor, and Room in sequence.

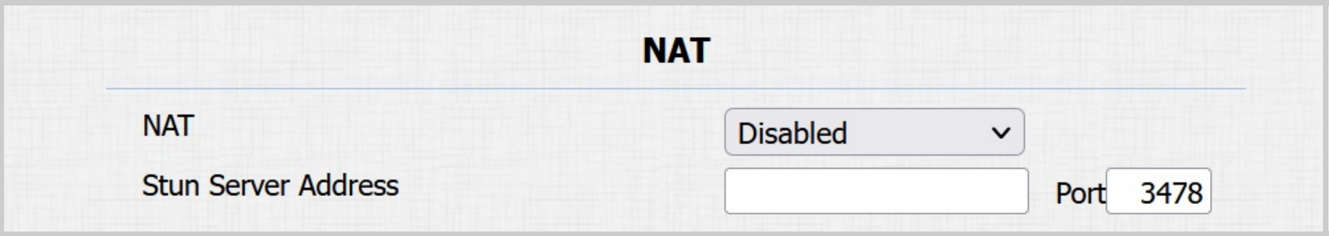
- **Device Extension**: The device extension number.

- **Device Location**: The location in which the device is installed and used.

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 enable NAT, go to **Account > Basic > NAT** interface.



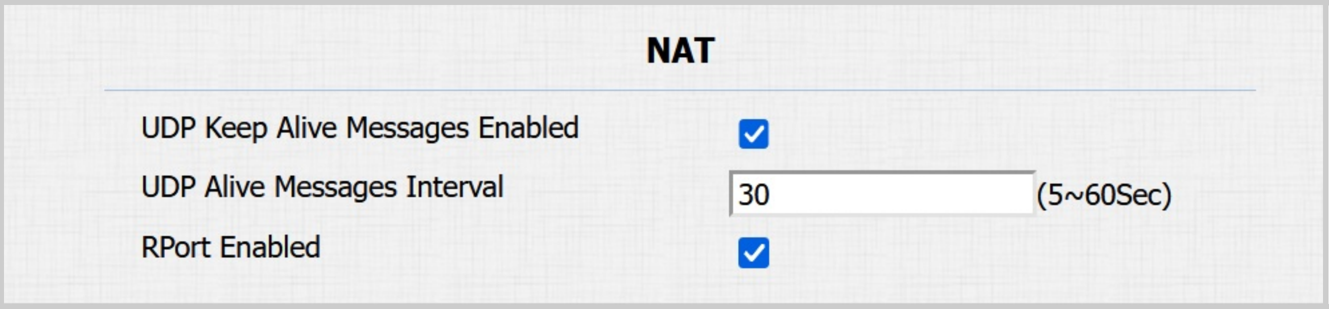
NAT

NAT	Disabled ⌄		
Stun Server Address		Port	3478

- **Stun Server Address**: Enter the server address when the device is in a Wide Area Network(WAN).

- **Port**: The server port.

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



NAT

UDP Keep Alive Messages Enabled	☑	
UDP Alive Messages Interval	30	(5~60Sec)
RPort Enabled	☑	

- **UDP Keep Alive Messages Enabled:** If enabled, the device will send the message to the SIP server which will recognize whether the device is online.

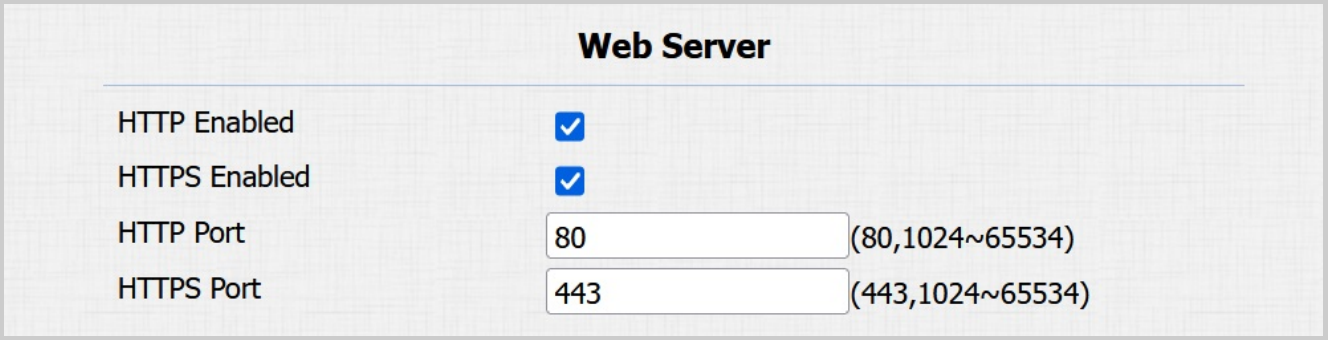
- **UDP Alive Messages Interval:** Set the message-sending interval from 5-60 seconds. The default is 30 seconds.

- **RPort**: Enable the RPort when the SIP server is in a WAN.

Device Web HTTP Setting

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

Set it up on the **Network** > **Advanced** > **Web Server** interface.



Web Server

HTTP Enabled ☑

HTTPS Enabled ☑

HTTP Port 80 (80,1024~65534)

HTTPS Port 443 (443,1024~65534)

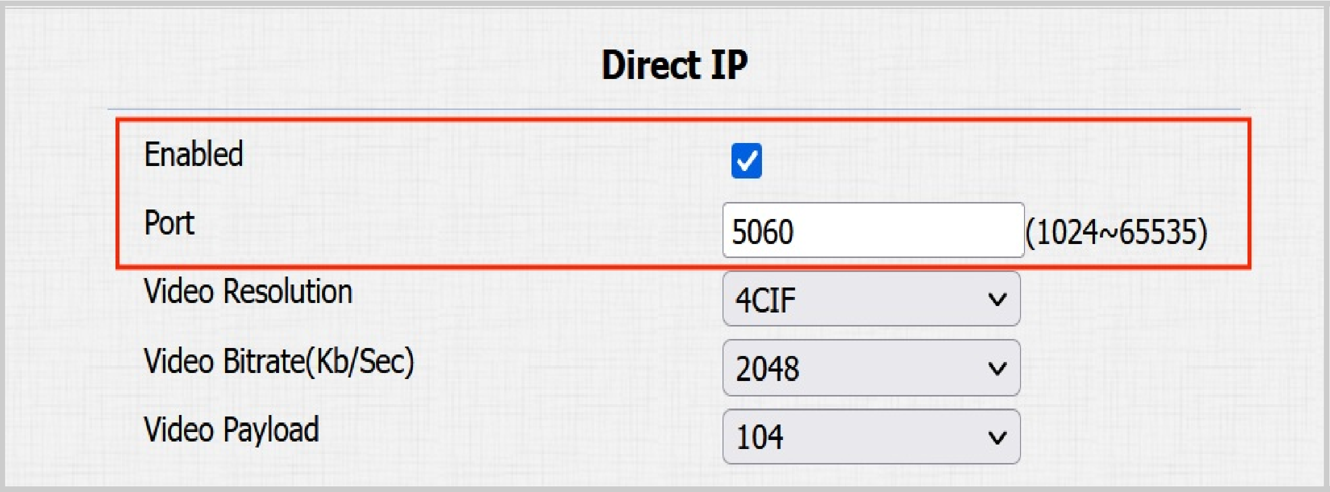
- **HTTP/HTTPS Enabled**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

Intercom Call Configuration

IP Call Configuration

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

Enable Direct IP on the **Intercom** > **Basic** > **Direct IP** interface.



Direct IP

Enabled	☑
Port	5060 (1024~65535)
Video Resolution	4CIF
Video Bitrate(Kb/Sec)	2048
Video Payload	104

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

SIP Call Configuration

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

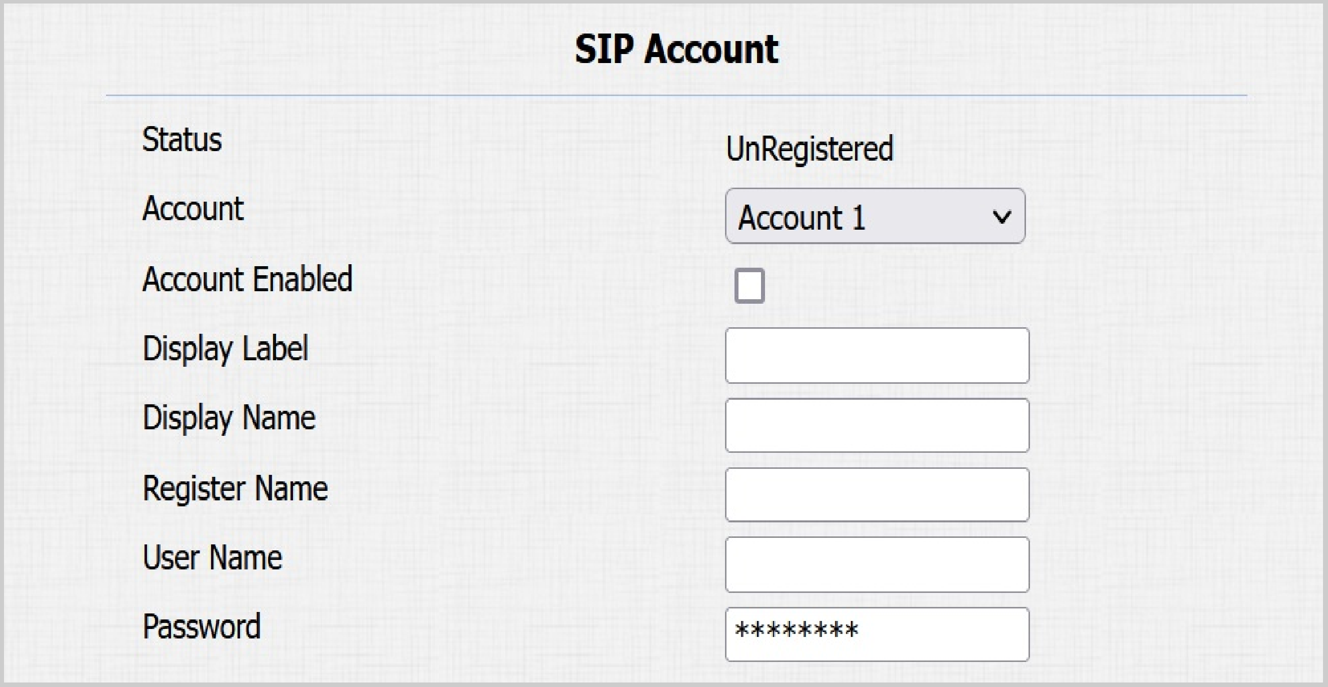
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Account Registration

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

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

To set it up, navigate to the web **Account > Basic > SIP Account** Interface.



SIP Account

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

- **Status:** Indicate whether the SIP account is registered or not.
- **Account 1/Account 2:** The door phone supports 2 SIP accounts.

  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.

  - The system switches to Account 2 if Account 1 is not registered.

  - To designate the account to be used for outgoing calls, select the account number for contacts or dial plan prefixes in their settings.

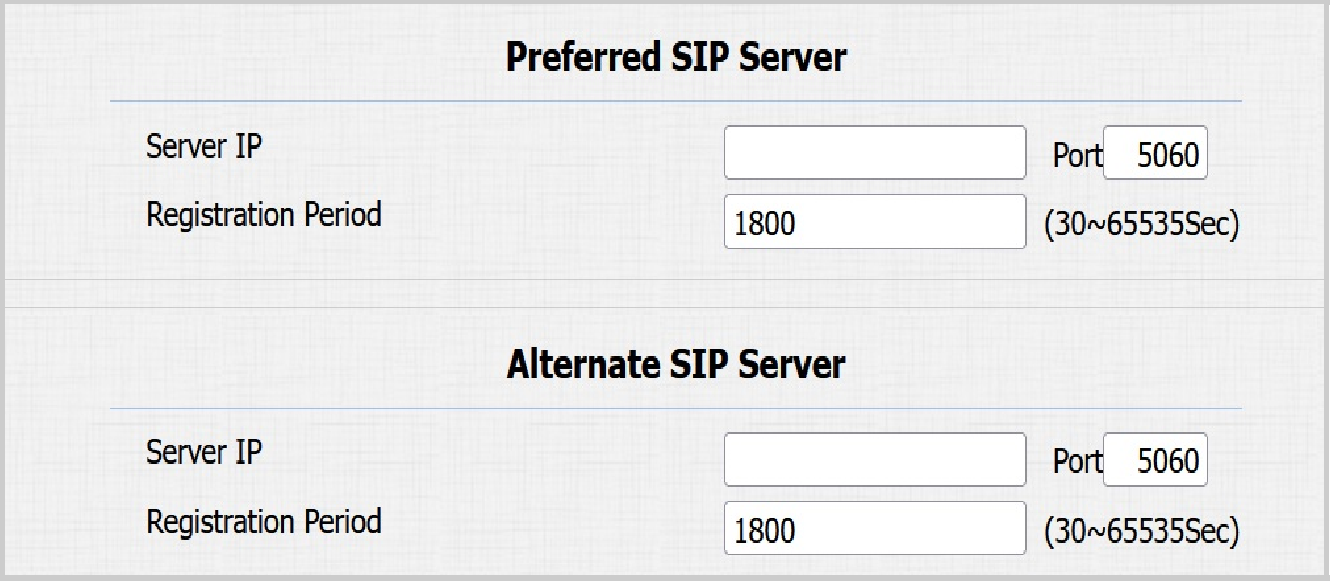
> Tip
> For configuring contact call and dial plan, see here.

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

SIP Server Configuration

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

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



Preferred SIP Server

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

Alternate SIP Server

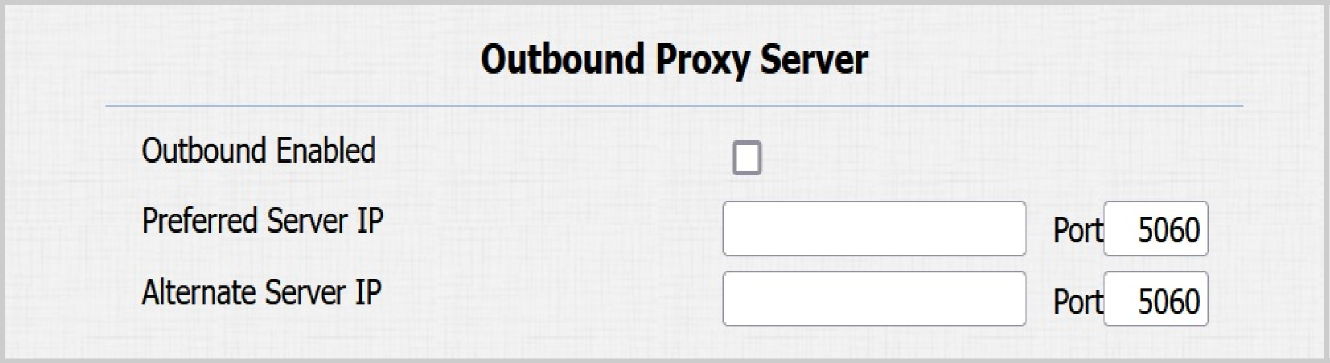
Server IP		Port	5060
Registration Period	1800	(30~65535Sec)	

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

Outbound Proxy Server

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

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



Outbound Proxy Server

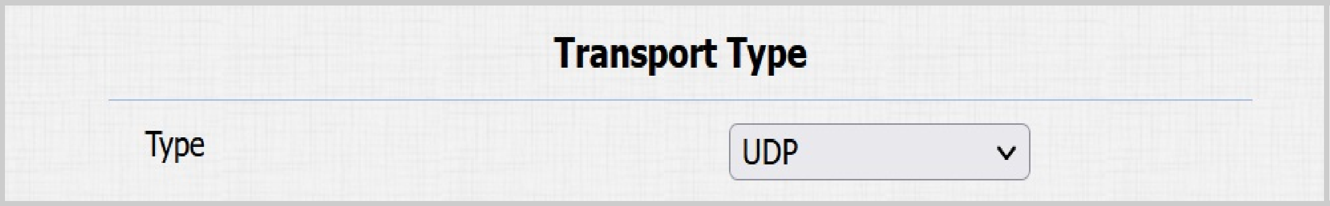
Outbound Enabled	□		
Preferred Server IP		Port	5060
Alternate Server IP		Port	5060

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

Data Transmission Type

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

To set it up, go to the web **Account > Basic > Transport Type** interface.



Transport Type

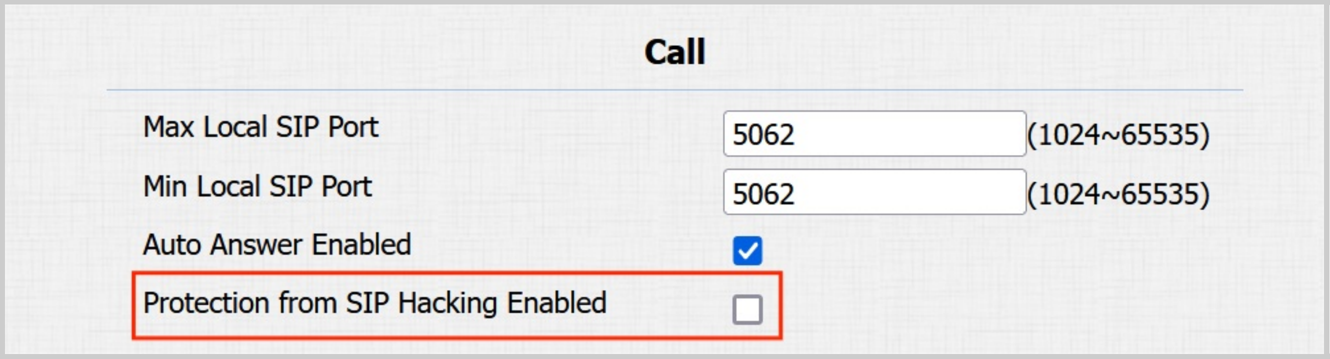
Type: UDP

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

SIP Hacking Protection

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.

To enable it, go to **Account > Advanced > Call** interface.



Call

Max Local SIP Port 5062 (1024~65535)

Min Local SIP Port 5062 (1024~65535)

Auto Answer Enabled ☑

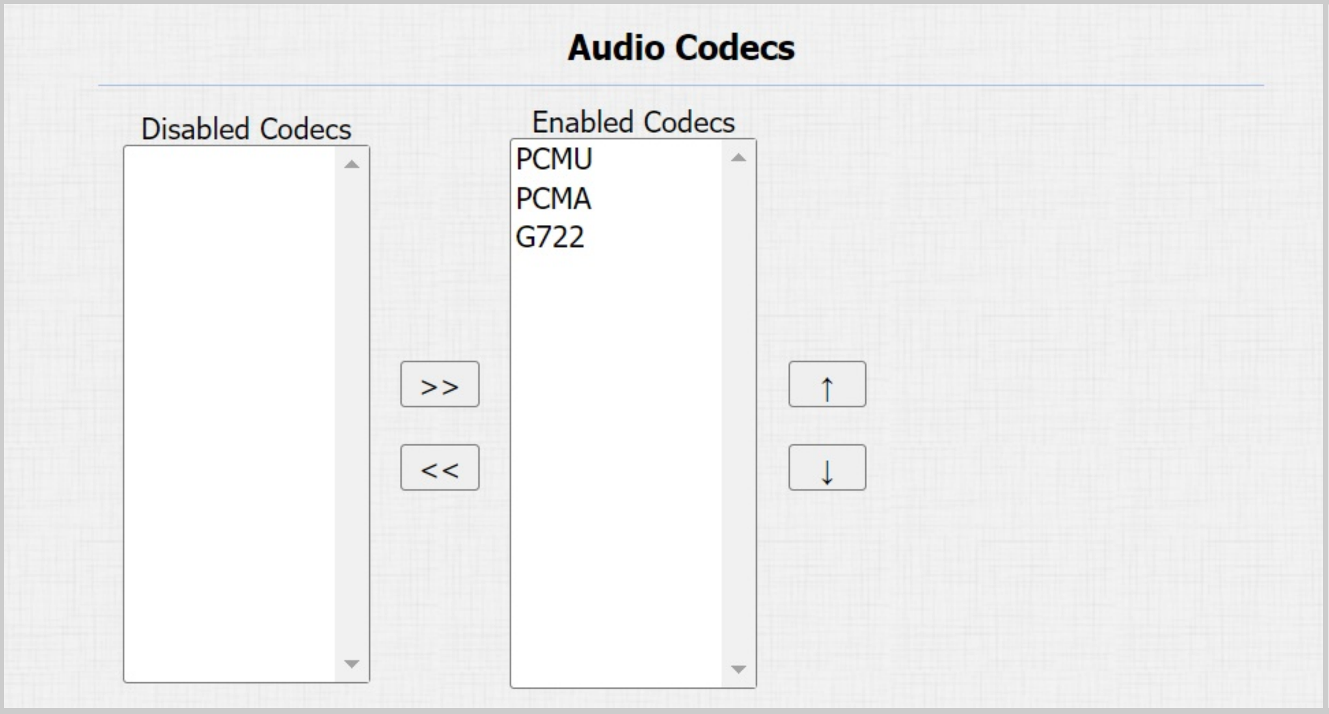
Protection from SIP Hacking Enabled □

Audio & Video Codec Configuration

Audio Codec

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

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



Audio Codecs

Disabled Codecs

Enabled Codecs
PCMU
PCMA
G722

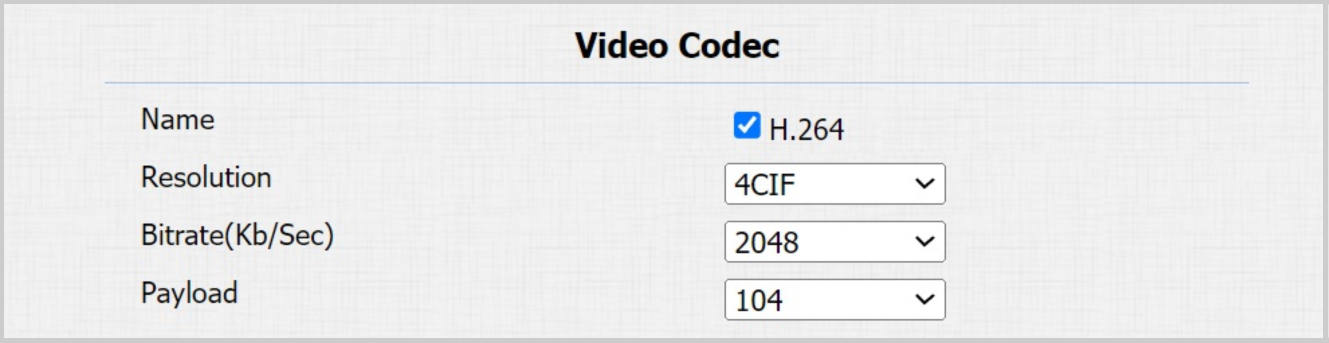
Please refer to the bandwidth consumption and sample rate for the three codec types below:

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

Video Codec

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

To set it up, go to the web **Account > Advanced > Video Codec** interface.



Video Codec

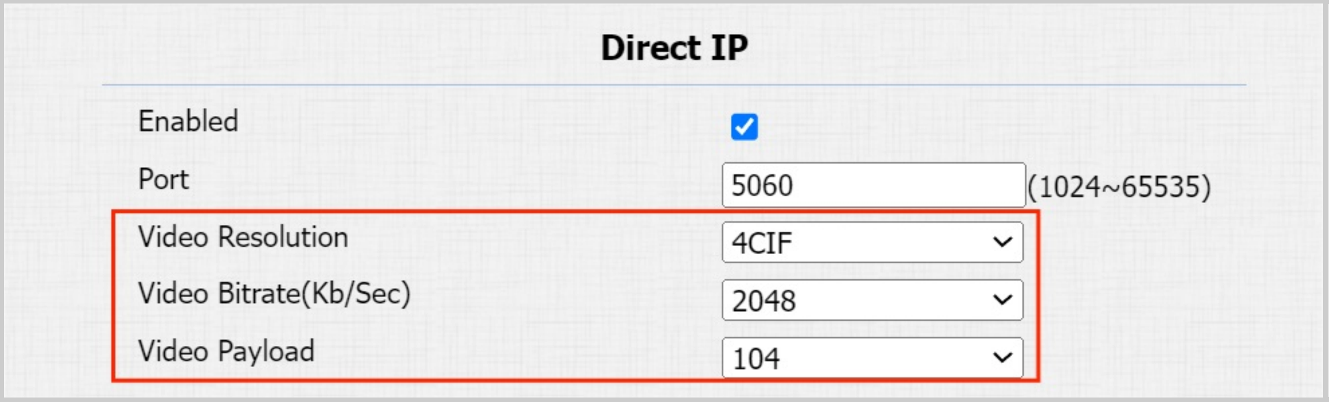
Name	☑ H.264
Resolution	4CIF
Bitrate(Kb/Sec)	2048
Payload	104

- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default code resolution is 4CIF.
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data transmitted every second and the clearer the video will be. The default code bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for IP Direct Calls

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

To set it up, navigate to the **Intercom > Basic > Direct IP** interface.



Direct IP

Enabled	☑
Port	5060 (1024~65535)
Video Resolution	4CIF
Video Bitrate(Kb/Sec)	2048
Video Payload	104

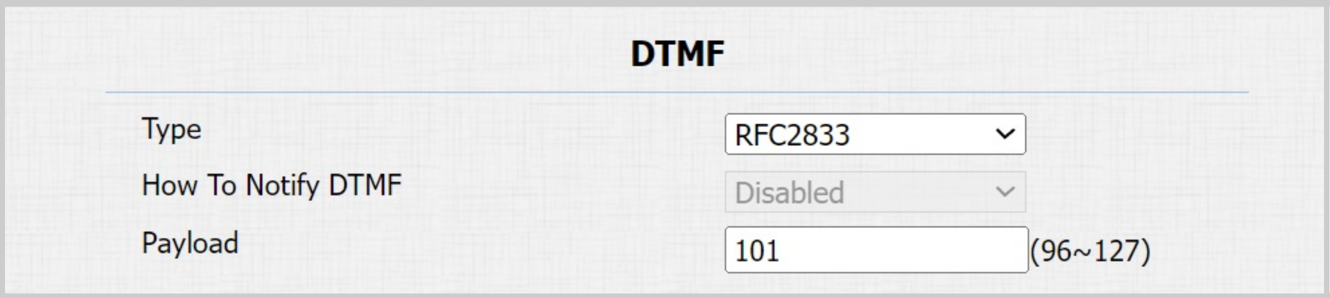
- **Video Resolution**: Select the resolution from the provided options.

- **Video Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The default bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

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.

To set it up, navigate to the **Account** > **Advanced** > **DTMF** interface.



DTMF

Type: RFC2833

How To Notify DTMF: Disabled

Payload: 101 (96~127)

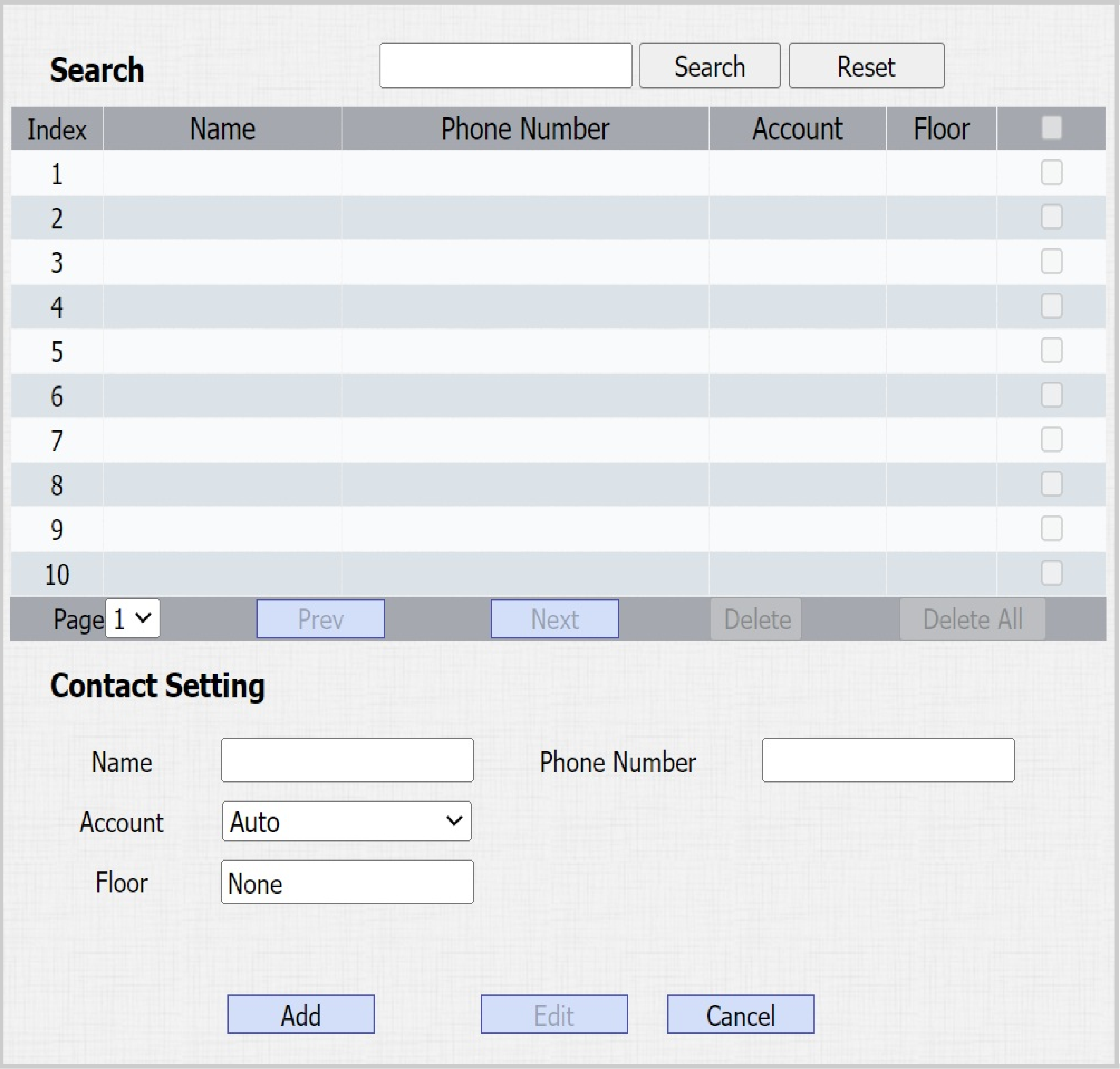
- **Type:** Select from the following options: **Inband, RFC2833, Info, Info+Inband, Info+RFC2833** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, or **Telephone-Event** according to the specific type adopted by the third-party device. You are required to set it up only when the third-party device to be matched with adopts **Info** mode.
- **Payload**: Set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

Access Allowlist Configuration

The door phone can store up to 500 contacts, giving access permission to indoor monitors or other devices.

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

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



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

Contact Setting

Name

Phone Number

Account: Auto

Floor: None

- **Name:** Name the contact.

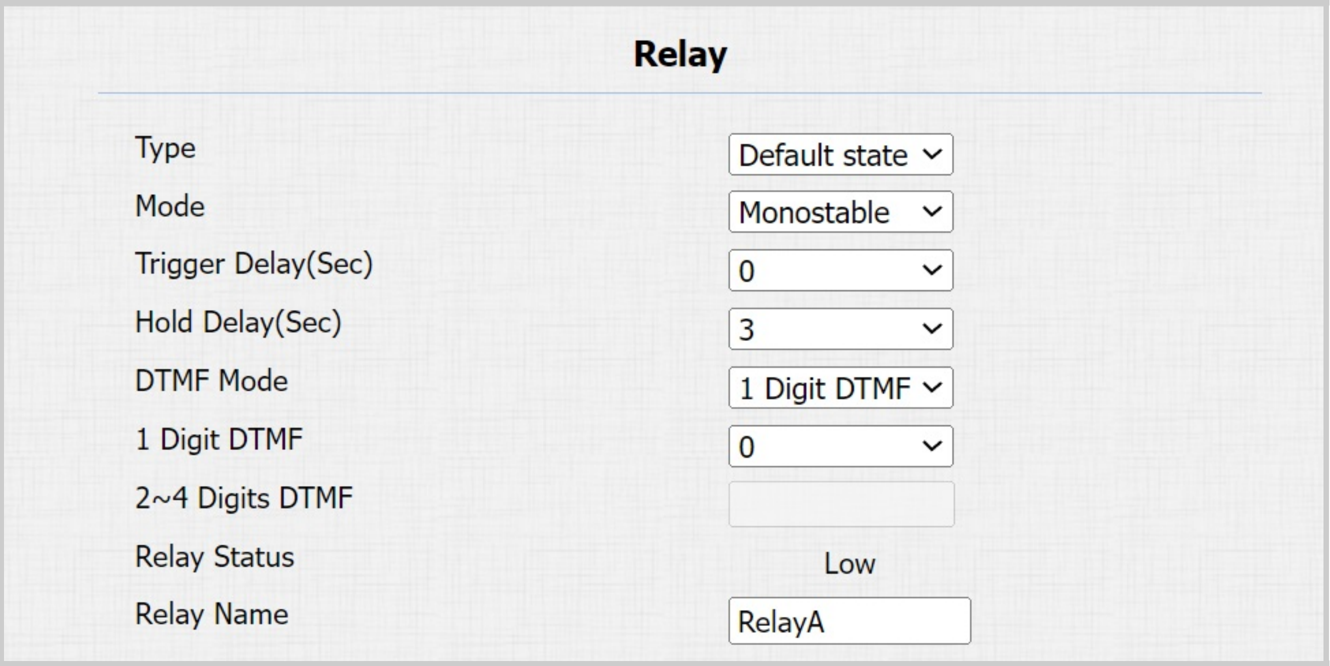
- **Phone Number:** The phone number of the contact. It supports IP addresses and SIP numbers.

- **Account:** Select the account to make the call.
- **Floor:** Specify the accessible floor(s) to the contact via the elevator.

Relay Setting

Relay Switch Setting

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



Relay

Type	Default state
Mode	Monostable
Trigger Delay(Sec)	0
Hold Delay(Sec)	3
DTMF Mode	1 Digit DTMF
1 Digit DTMF	0
2~4 Digits DTMF	
Relay Status	Low
Relay Name	RelayA

- **Type**: Determine the interpretation of the Relay Status regarding the state of the door:
    - **Default Status**: A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.
    - **Invert Status**: A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.
- **Mode**: Specify the conditions for automatically resetting the relay status.
    - **Monostable**: The relay status resets automatically within the relay delay time after activation.
    - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.

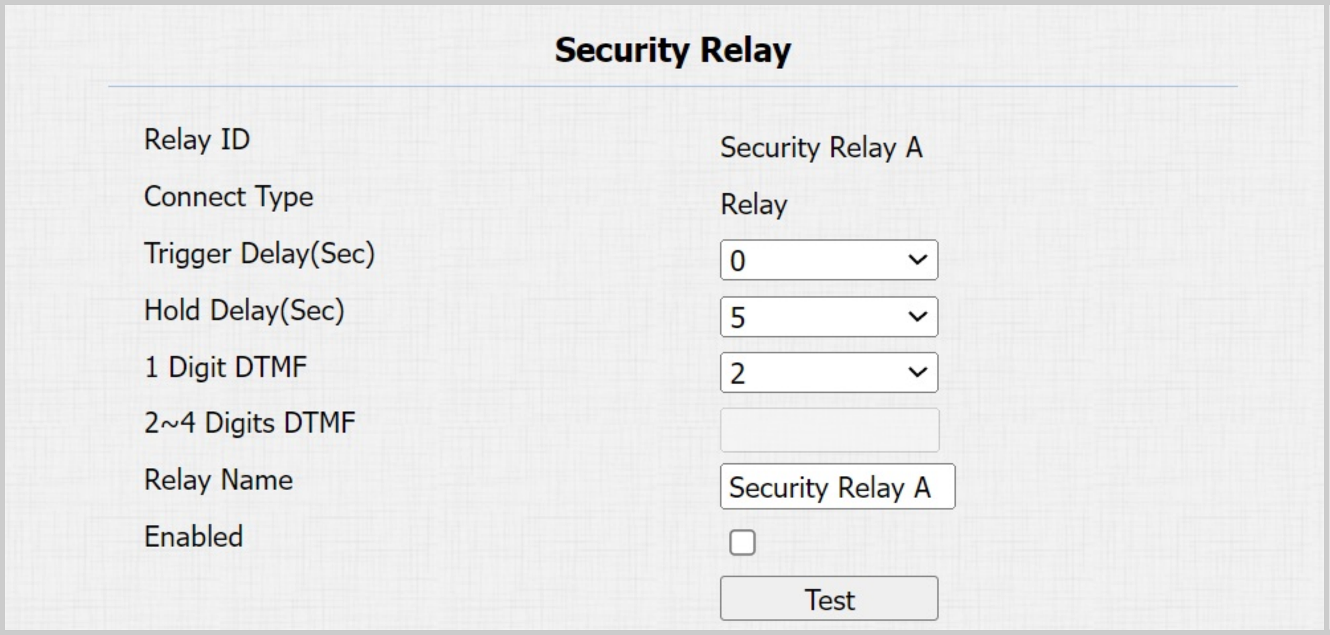
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.

> **Note**
>
> External devices connected to the relay require separate power adapter.

Security Relay Setting

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

To set up the security relay, navigate to **Access Control > Relay > Security Relay** interface.



Security Relay

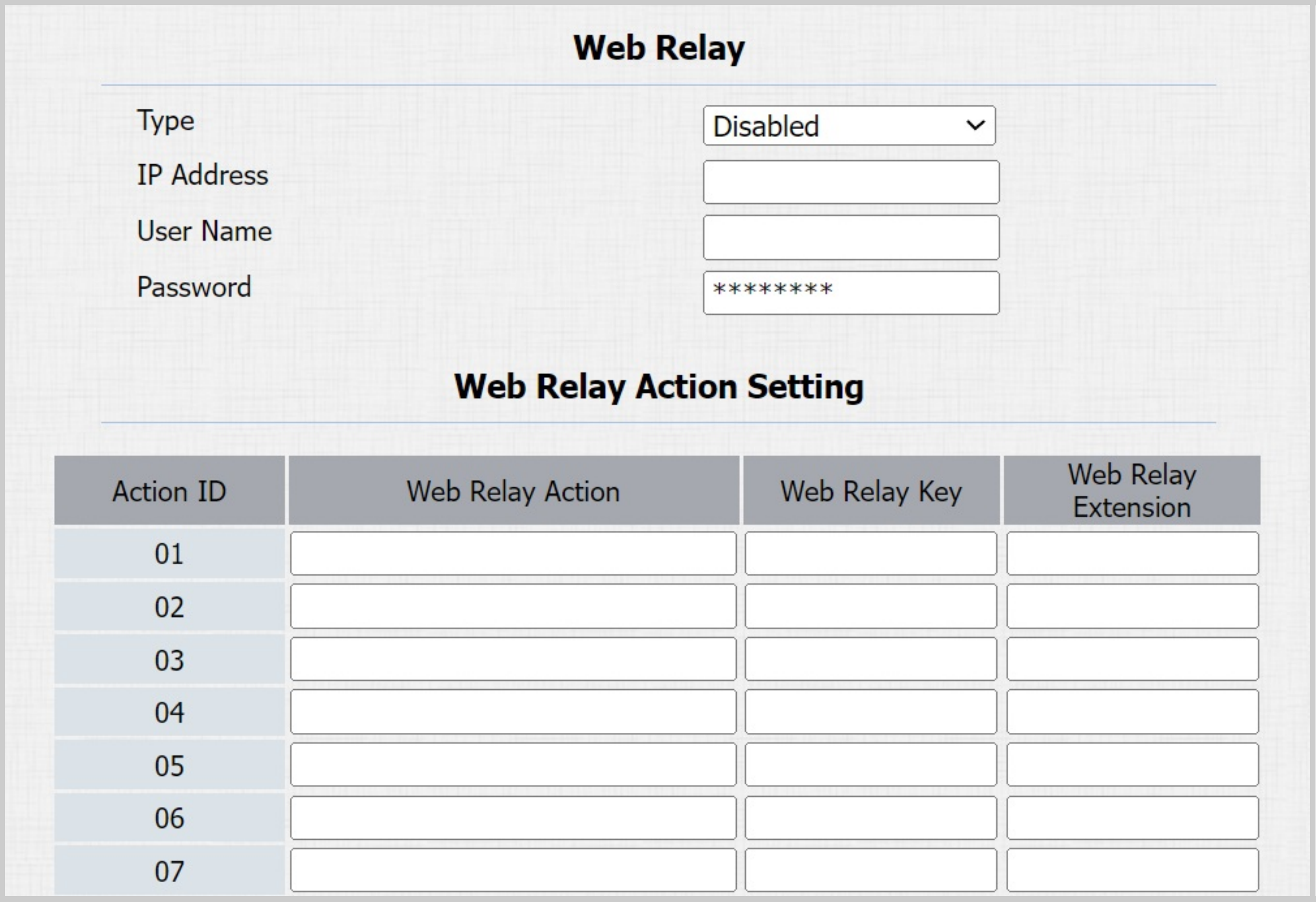
Relay ID	Security Relay A
Connect Type	Relay
Trigger Delay(Sec)	0
Hold Delay(Sec)	5
1 Digit DTMF	2
2~4 Digits DTMF	
Relay Name	Security Relay A
Enabled	☐

- **Connect Type**: Indicate the connection type between the security relay and the door phone.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name**: Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Test**: Click to send the signal to the SR01. When the door phone and SR01 are pairing, click Test to finish the matching.

Web Relay 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.

To set it up, navigate to **Access Control > Web Relay** interface.



Web Relay

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

Web Relay Action Setting

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

- **Type**: Determine the type of relay activated when employing door access methods for entry.
    - **Disabled**: Only activate the local relay.
    - **WebRelay**: Only activate the web relay.

  - **Both**: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.

- **IP Address**: The web relay IP address provided by the web relay manufacturer.

- **User Name**: The user name provided by the web relay manufacturer.

- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.

- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

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

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

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

- Leaving it blank enables all door-opening methods.

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

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

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

Door Access Schedule Management

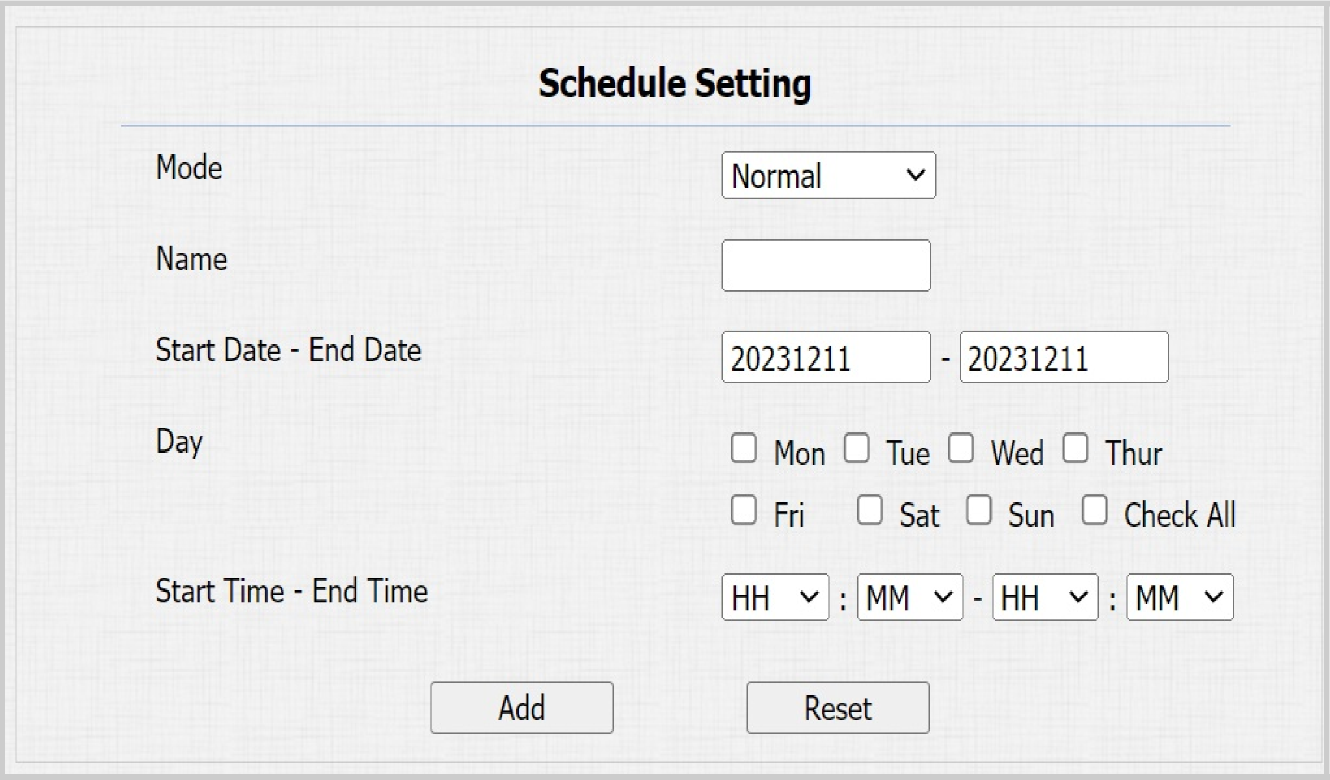
Configure Door Access Schedule

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.

To set it up, navigate to the web **Setting** > **Schedule** interface.



Schedule Setting

Mode	Normal
Name	
Start Date - End Date	20231211 - 20231211
Day	□ Mon □ Tue □ Wed □ Thur □ Fri □ Sat □ Sun □ Check All
Start Time - End Time	HH : MM - HH : MM

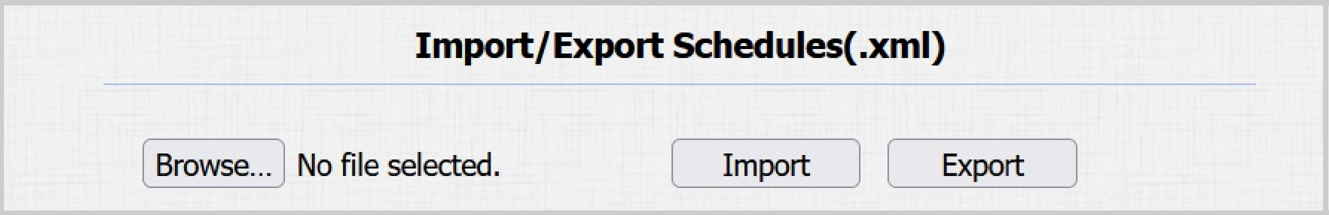
- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.

- **Name**: Name the schedule.

Import and Export Door Access Schedule

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

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

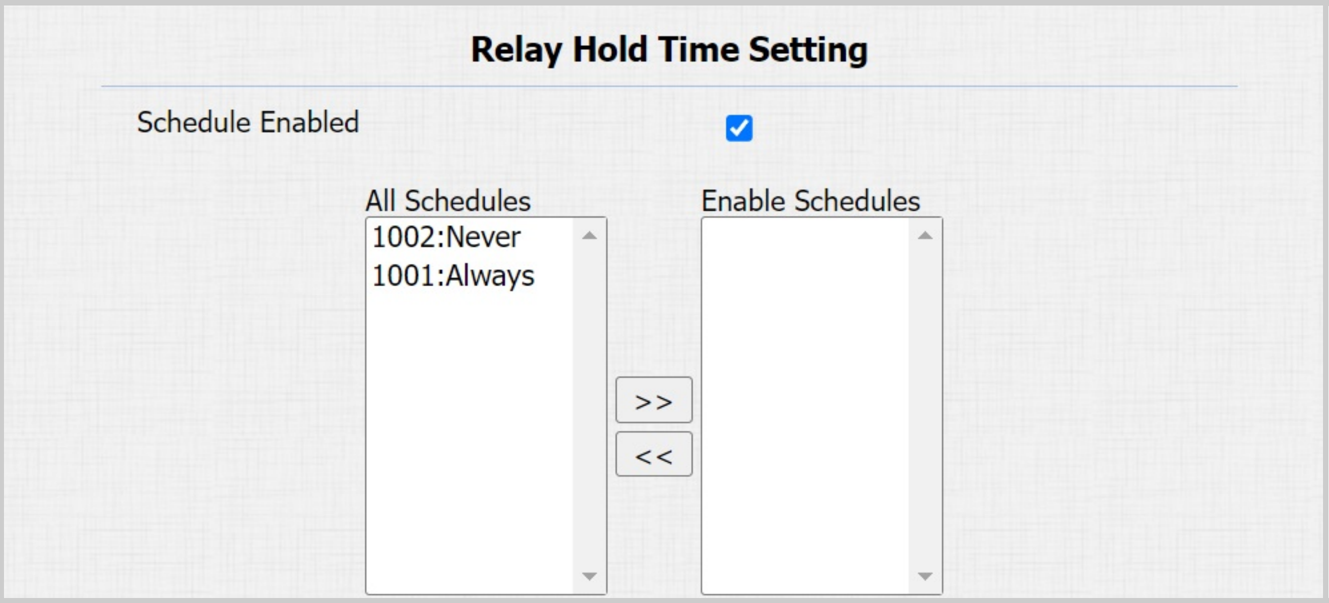


Import/Export Schedules(.xml)

Relay Schedule

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

To set up a relay schedule, navigate to the **Access Control > Relay > Relay Hold Time Setting** interface.



Relay Hold Time Setting

Schedule Enabled ☑

All Schedules: 1002:Never, 1001:Always

Enable Schedules:

- **Schedule Enabled**: Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

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

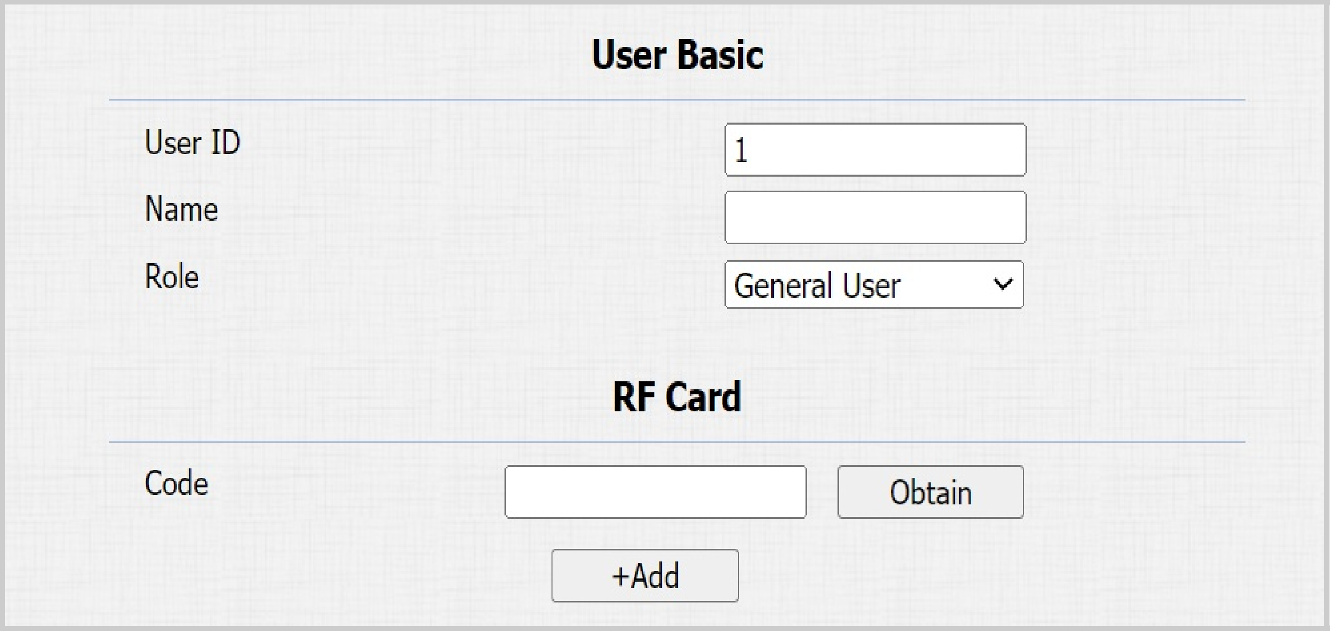
Door Unlock Configuration

Unlock by RF Cards

The RF card should be assigned to a particular user for door opening.

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

To add a user, go to **Access Control > User** interface and click **Add**.



User Basic

User ID: 1

Name:

Role: General User

RF Card

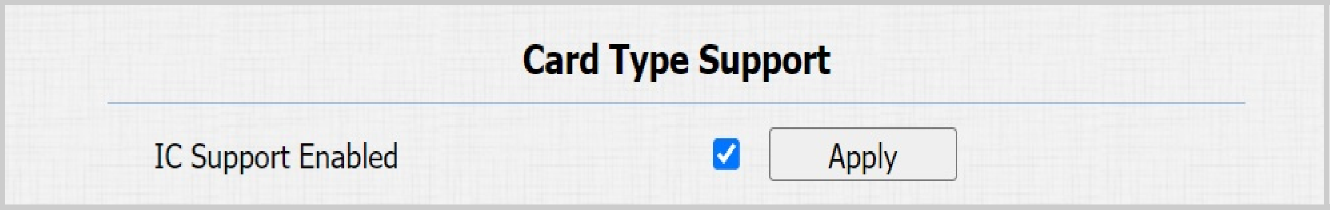
Code:

- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.
- **Role**: Define the user as a General User or an Administrator. The Admin card can be used to add a user card. Please refer to Configure Admin Cards and User Cards for detailed configuration.
- **Code**: The card number that the card reader reads.

Note:

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

To enable the IC card function, navigate to the **Access Control** > **Card Setting** > **Card Type Support** interface.

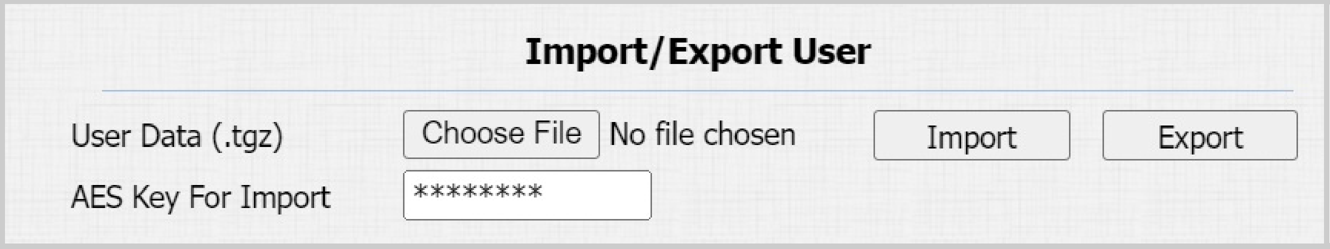


Card Type Support

IC Support Enabled ☑

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

On the **Access Control** > **User** interface, scroll to the **Import/Export User** section.



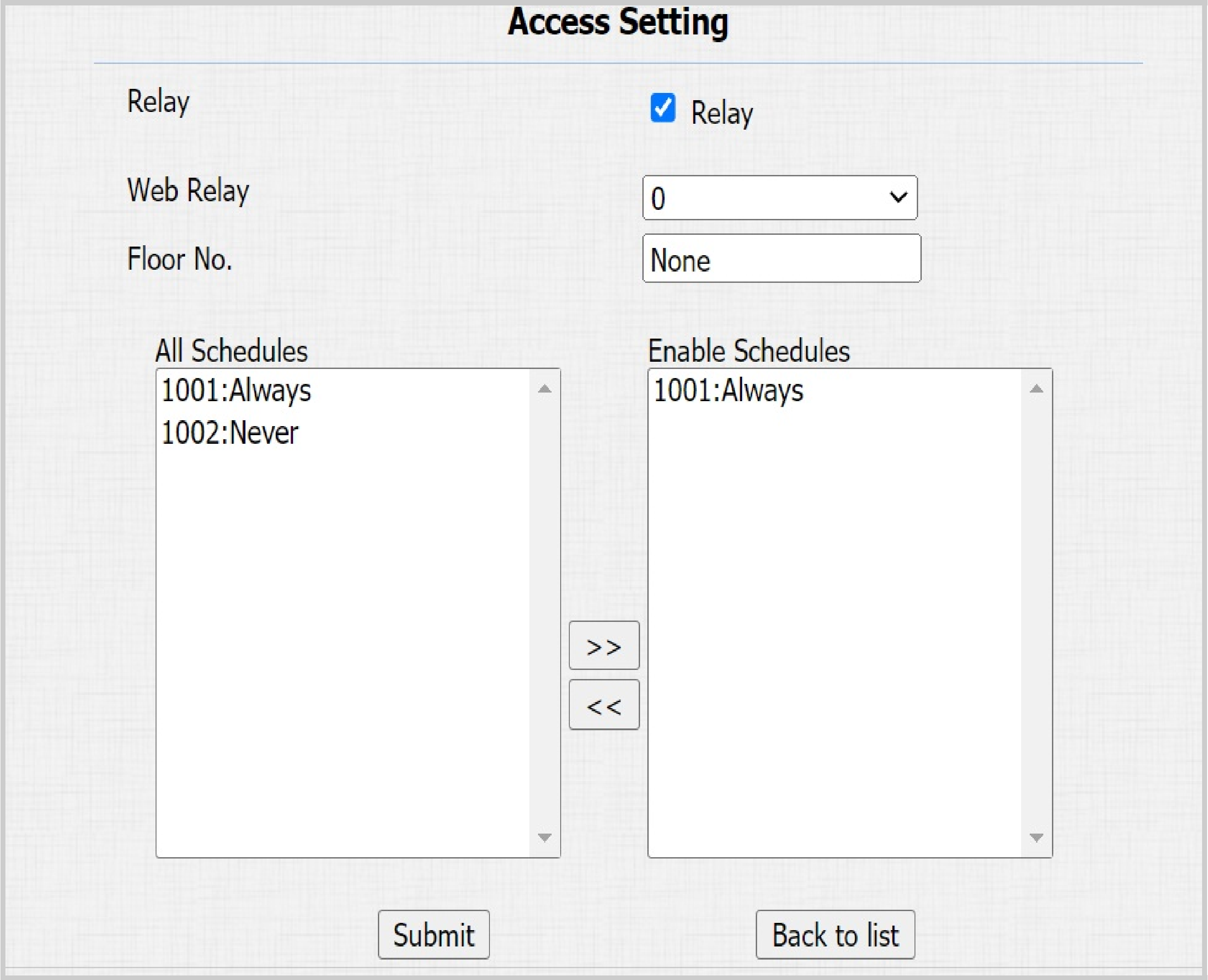
Import/Export User

User Data (.tgz) No file chosen

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

Access Settings

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



Access Setting

Relay	☑ Relay
Web Relay	0
Floor No.	None

All Schedules	Enable Schedules
1001:Always 1002:Never	1001:Always

- **Relay**: The relay to be unlocked using the door-opening methods should be assigned to the user.

- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.

- **Floor No.**: Specify the accessible floor(s) to the user via the elevator.

- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:

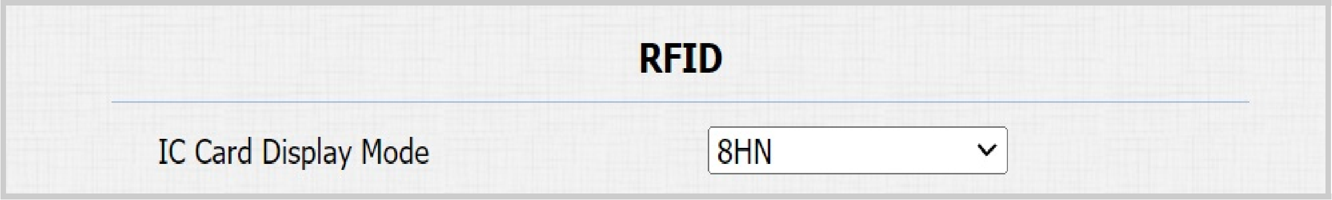
  - Always: Allows door opening without limitations on door open counts during the valid period.

  - Never: Prohibits door opening.

RF Card Code Format

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

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



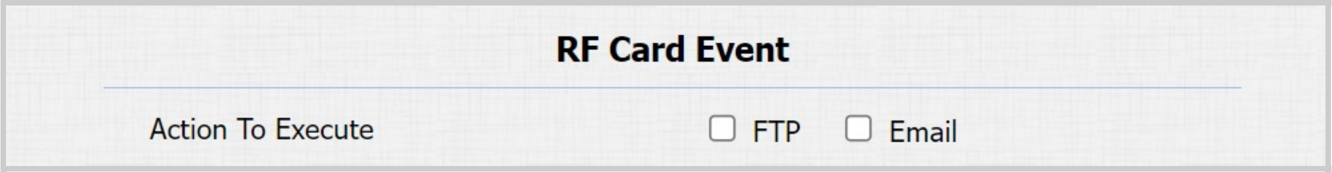
RFID

IC Card Display Mode: 8HN

- **IC Card Display Mode**: Set the card number format from the provided options. The default format in the device is 8HN.

Events Triggered by Using RF Cards

You can set up the events triggered by swiping the RF cards on the **Access Control** > **Card Setting** > **RF Card Event** interface.



RF Card Event

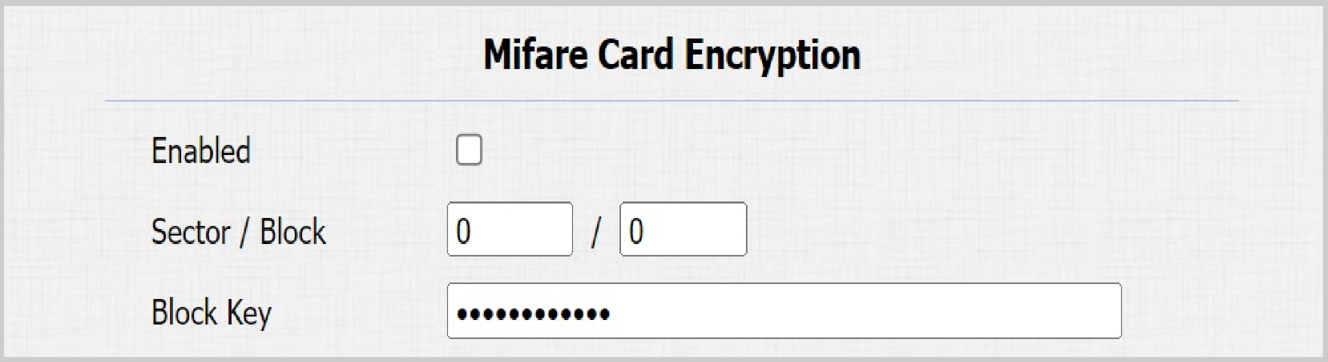
Action To Execute: □ FTP □ Email

- **Action to Execute**: Set the desired actions that occur when the door is opened by swiping the RF card.
    - **Email**: Send a message to the preconfigured Email address.
    - **FTP**: Send a message to the preconfigured FTP address.

Mifare Card Encryption

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

To encrypt the card, navigate to the **Access Control** > **Card Setting** > **Mifare Card Encryption** interface.



Mifare Card Encryption

Enabled □

Sector / Block 0 / 0

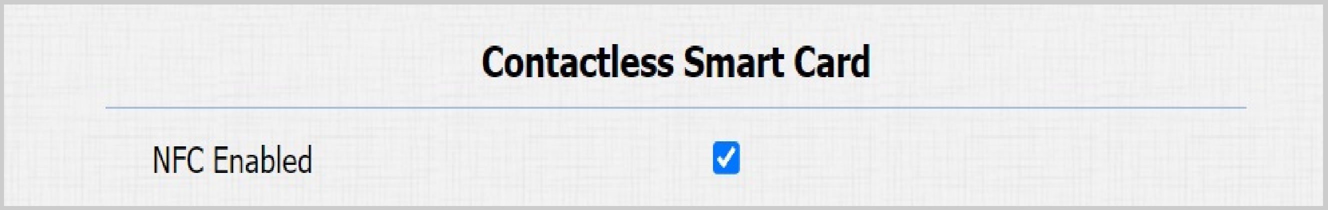
Block Key ••••••••••••

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

NFC Card

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

To use the specific card, go to **Access Control** > **Card Setting** > **Contactless Smart Card** interface



Contactless Smart Card

NFC Enabled ☑

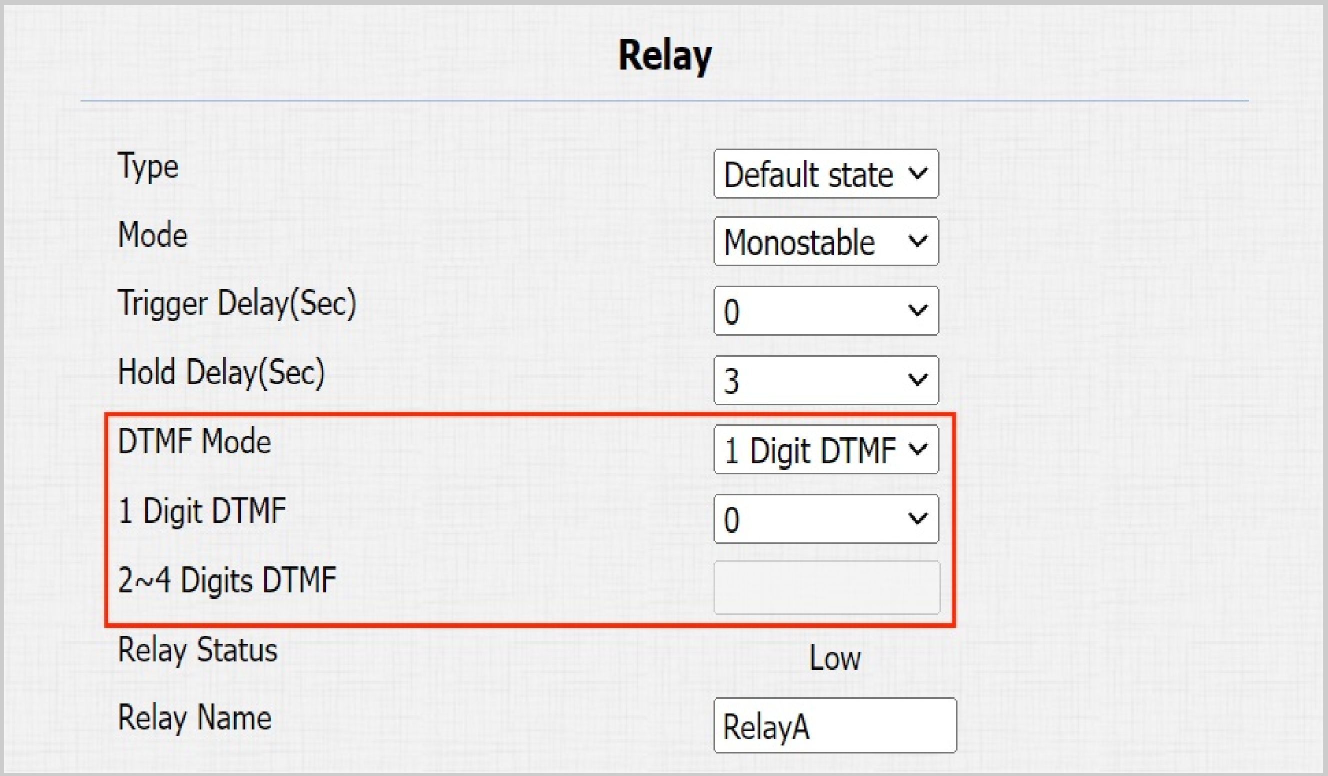
Note

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

Unlock by DTMF Code

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

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



Relay

Type: Default state

Mode: Monostable

Trigger Delay(Sec): 0

Hold Delay(Sec): 3

DTMF Mode: 1 Digit DTMF

1 Digit DTMF: 0

2~4 Digits DTMF:

Relay Status: Low

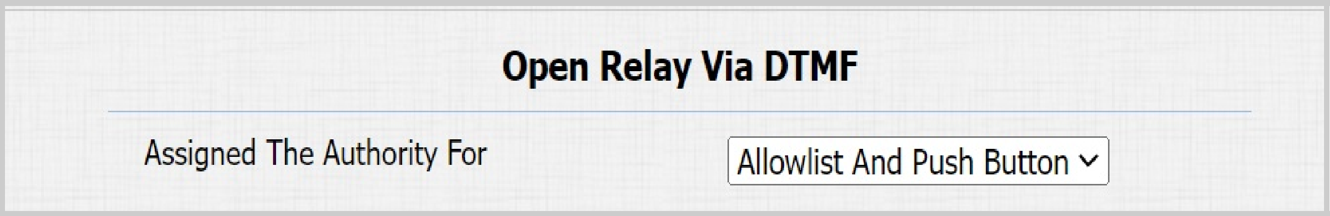
Relay Name: RelayA

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

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

DTMF White List

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



Open Relay Via DTMF

Assigned The Authority For: Allowlist And Push Button

- **Assigned The Authority For**: Specify the contacts authorized to open doors via DTMF:
  - Disabled: No numbers can unlock doors using DTMF.
  - Allowlist And Push Button: Doors can be opened by numbers added to the door phone's contact list and pressing the push button.
  - All Numbers: Any numbers can unlock using DTMF.

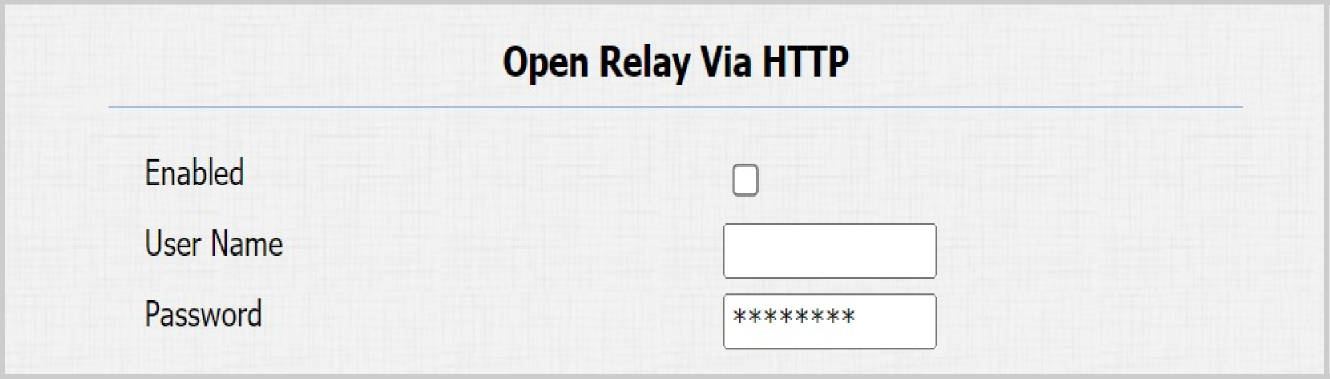
Note

When selecting this option, the calling indoor monitor(s) should be added into the door phone’s contact list.

Unlock by HTTP Command

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

Set it up on the web **Access Control > Relay > Open Relay Via HTTP** interface.



Open Relay Via HTTP

Enabled □

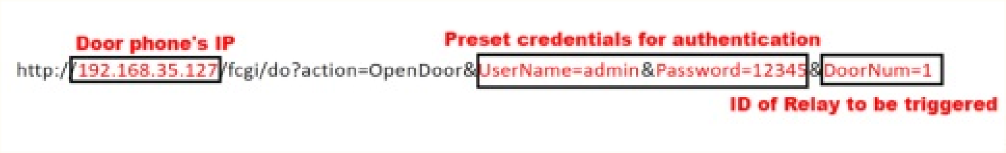
User Name:

Password: ********

- **Session Check**: Enable to enhance data transmission security.
- **User Name**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a password for authentication in HTTP command URLs.

Tip:

Here is an HTTP command URL example for relay triggering.



Door phone's IP

Preset credentials for authentication

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

ID of Relay to be triggered

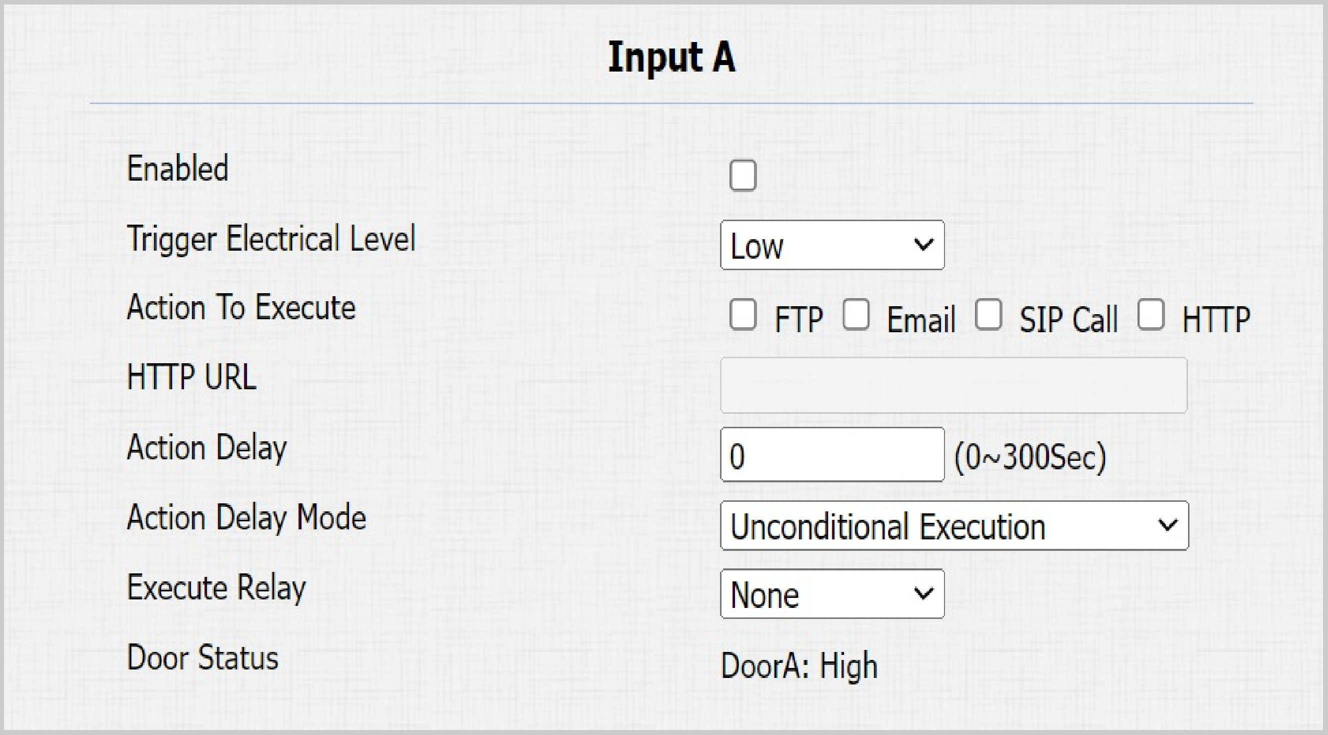
Note

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

Unlock by Exit Button

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

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



Input A

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

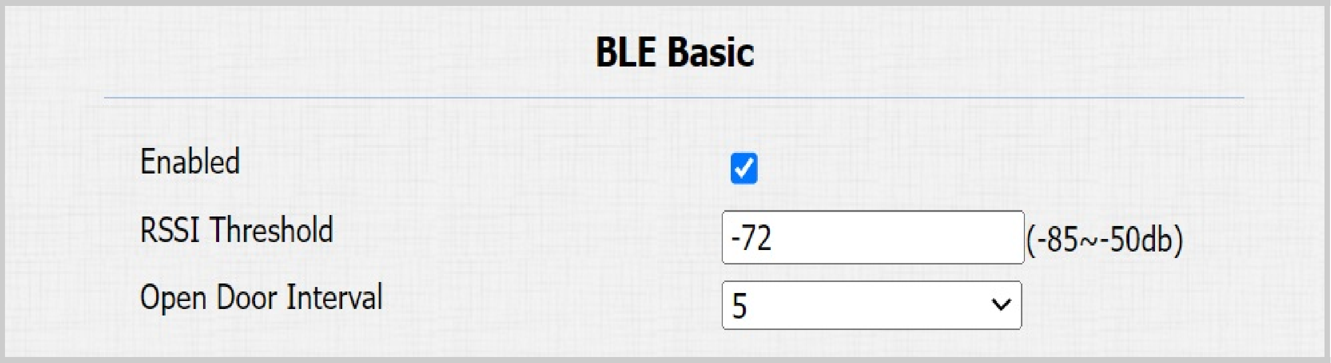
- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at a low or high electrical level.

- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - SIP Call: Call the preset number upon the trigger.
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode**:
  - Unconditional Execution: The action will be carried out when the input is triggered.
  - Execute If Input Still Triggered: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Door Status**: Display the status of the input signal.

Unlock by Bluetooth

The Bluetooth-enabled SmartPlus app enables users to enter the door hands-free. They can either open the door with the app in their pockets or wave their phones towards the door phone as they get closer to the door.

To configure Bluetooth, go to **Access Control > BLE** interface.



BLE Basic

Enabled ☑

RSSI Threshold -72 (-85~-50db)

Open Door Interval 5

- **RSSI Threshold**: Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.

- **Open Door Interval**: Set the interval(sec) between consecutive Bluetooth door access attempts.

Monitor and Image

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

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

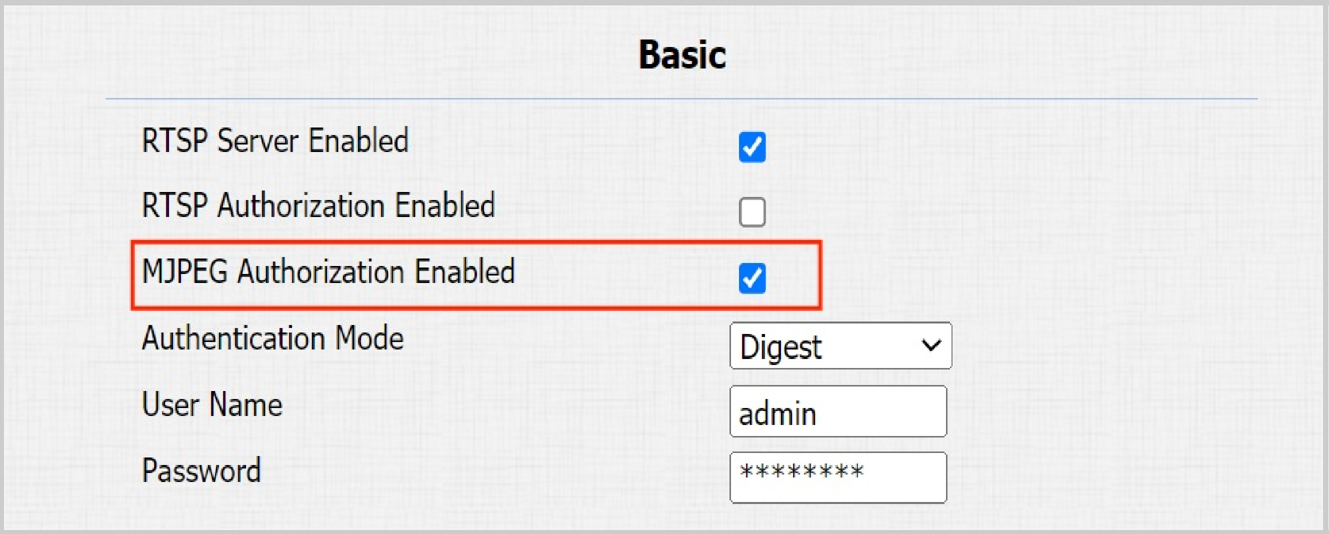
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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

MJPEG Image Capturing

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

To set it up, navigate to **Surveillance > RTSP > Basic** interface.



Basic

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

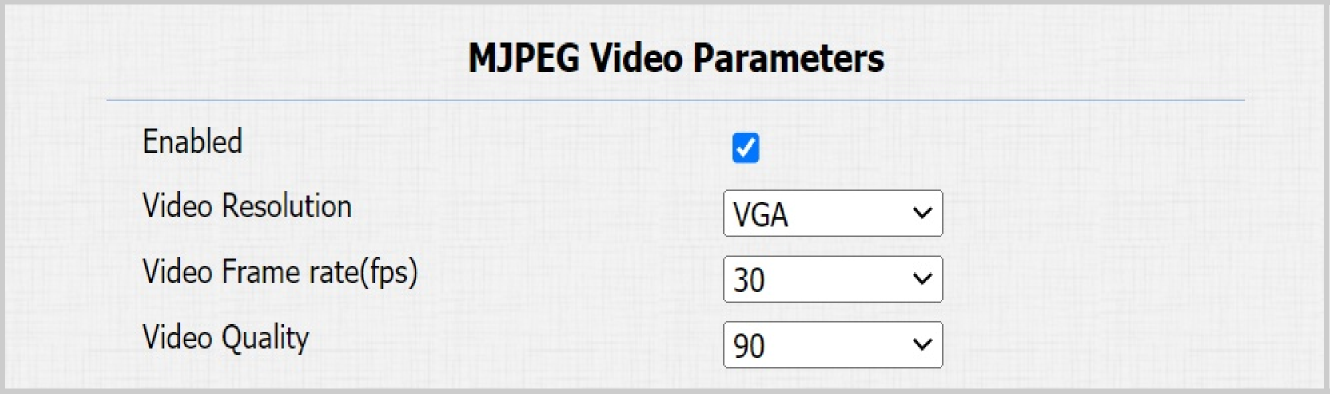
- **MJPEG Authorization Enabled**: Once enabled, accessing the door phone's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username, and RTSP Password.

Tip

- To view a dynamic stream, use the URL http://device_IP:8080/video.cgi.
- For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
    - http://device_IP:8080/picture.cgi
    - http://device_IP:8080/picture.jpg
    - http://device_IP:8080/jpeg.cgi

For example, if you want to capture the jpg format image of the door phone with the IP address 192.168.1.104, you can enter http://192.168.1.104:8080/picture.jpg on the web browser.

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



MJPEG Video Parameters

Enabled ☑

Video Resolution: VGA

Video Frame rate(fps): 30

Video Quality: 90

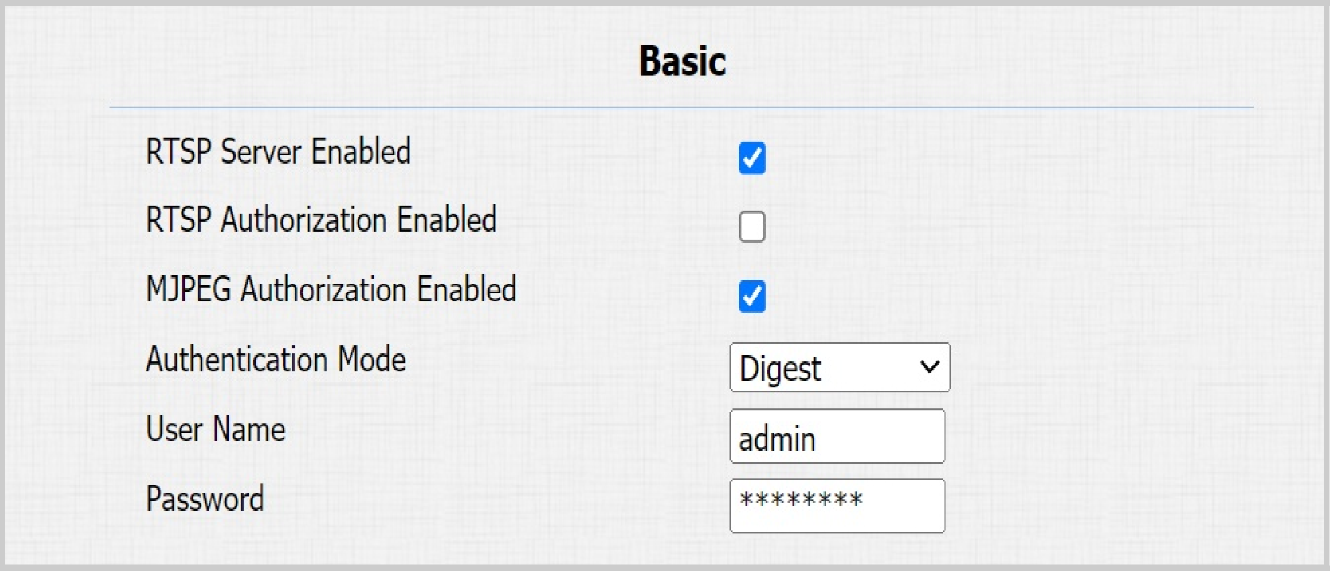
- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Frame rate(fps)**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Video Quality**: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

RTSP Stream Monitoring

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

RTSP Basic Setting

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



Basic

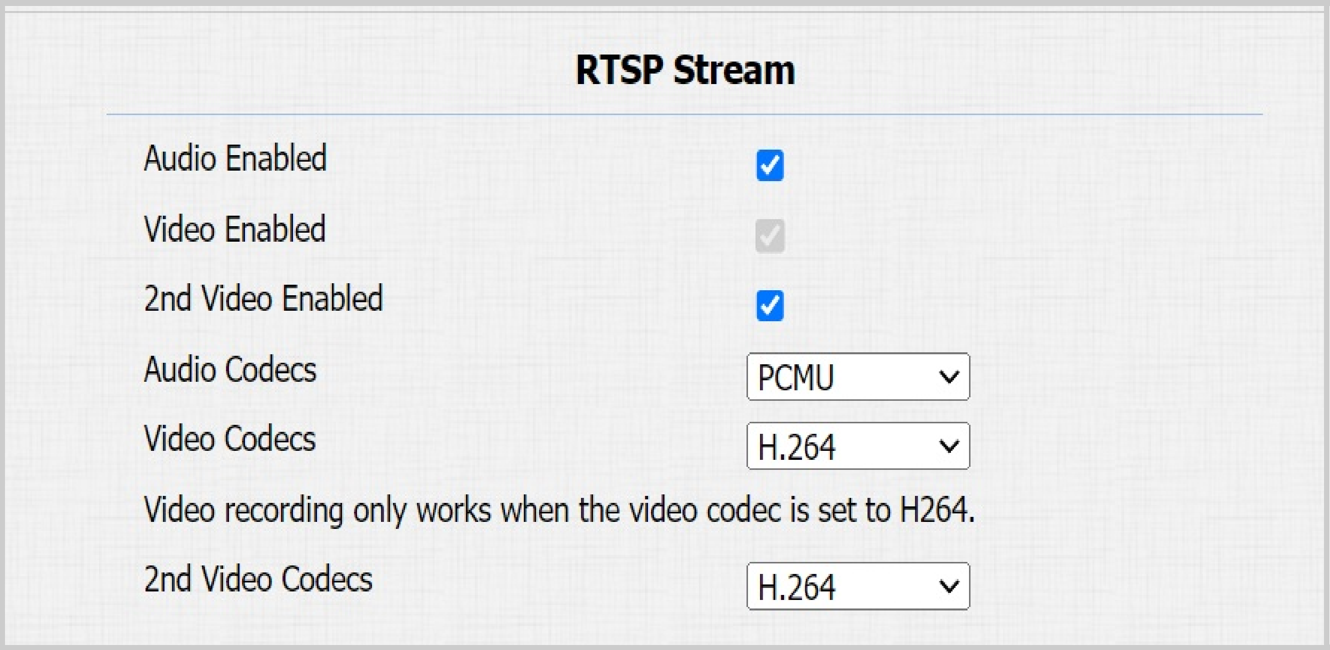
RTSP Server Enabled	☑
RTSP Authorization Enabled	□
MJPEG Authorization Enabled	☑
Authentication Mode	Digest
User Name	admin
Password	********

- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: Select between Basic and Digest. Basic is the default authentication type.
  - Basic: The username and password are joined in the form “username: password”, followed by the Base64 encoding before being sent to the server. The server then decrypts the string to retrieve the username and password for verification.
  - Digest: Use hashing instead of the easily reversible Base64 encoding. A token is used for verification.
- **User Name**: Set the username for authorization.
- **Password**: Set the password for authorization.

RTSP Stream Setting

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

Go to **Surveillance > RTSP > RTSP Stream** interface.



RTSP Stream

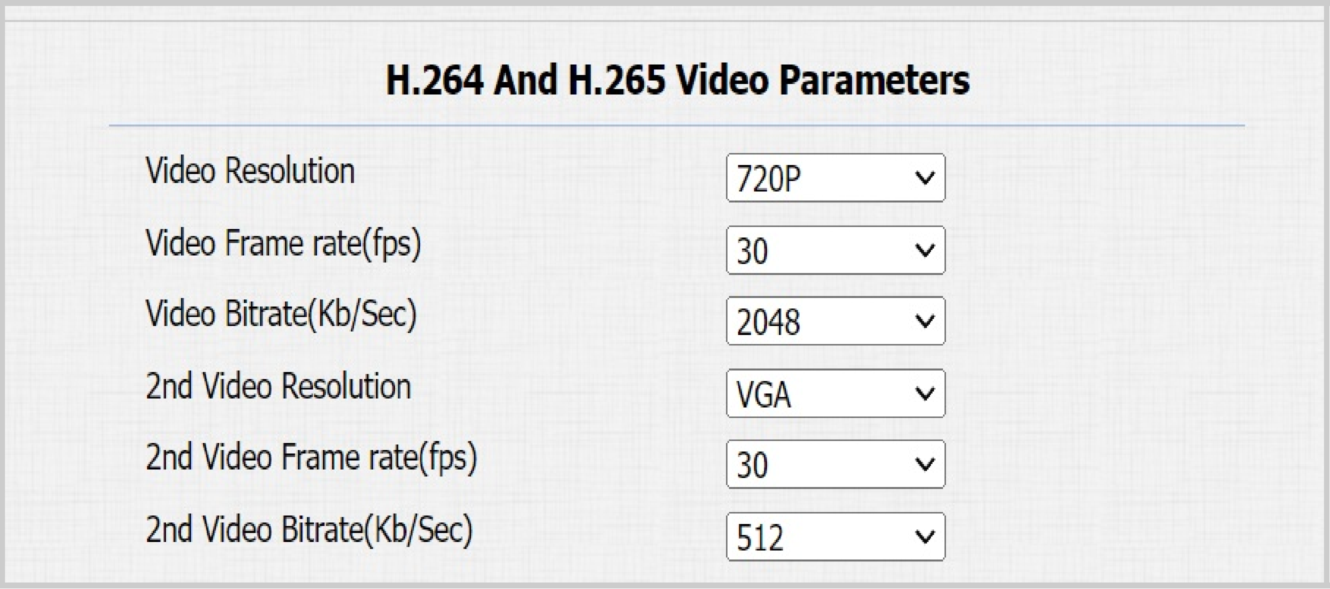
Audio Enabled	☑
Video Enabled	☑
2nd Video Enabled	☑
Audio Codecs	PCMU
Video Codecs	H.264

Video recording only works when the video codec is set to H264.

2nd Video Codecs	H.264

- **Audio Enabled:** Decide whether the RTSP stream has sound.
- **Video Enabled:** Decide whether the RTSP stream has video. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **2nd Video Enabled:** E12 supports two RTSP streams.
- **Audio Codecs:** Choose a suitable audio codec for RTSP audio.
- **Video Codecs:** Specify the video compression formats.
    - H.264: Offer highly efficient compression but at a cost of higher latency and computational load.
    - H.265: Offer superior compression efficiency and support for higher resolutions, but it comes with higher computational requirements and potential compatibility issues.
    - MJEPG: Offer improved quality but inefficient compression.

You can set up the video parameters for H.264 and H.265 on the **H.264 And H.265 Video Parameters** section.



H.264 And H.265 Video Parameters

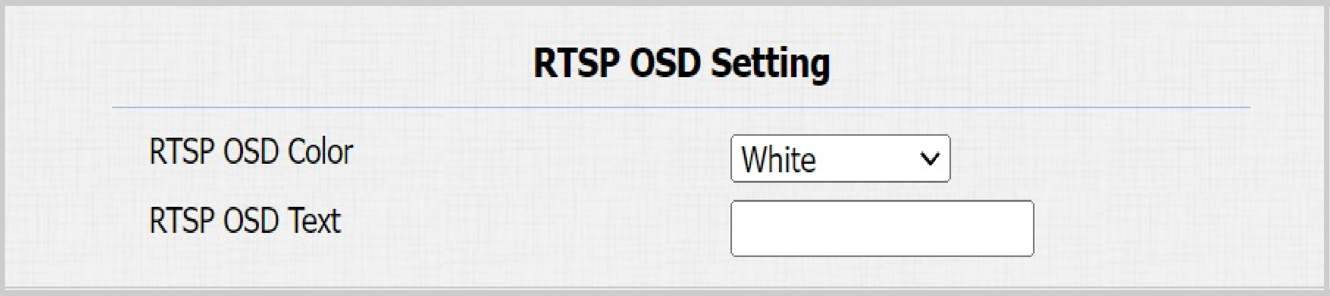
Video Resolution	720P
Video Frame rate(fps)	30
Video Bitrate(Kb/Sec)	2048
2nd Video Resolution	VGA
2nd Video Frame rate(fps)	30
2nd Video Bitrate(Kb/Sec)	512

- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Frame rate(fps)**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Video Bitrate(Kb/Sec)**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048 kbps.
- **2nd Video Resolution**: Specify the image resolution for the second video stream channel.
- **2nd Frame rate(fps)**: Set the frame rate for the second video stream channel.
- **2nd Video Bitrate(Kb/Sec)**: Set the bit rate for the second video stream channel. The default is 512 kbps.

RTSP OSD Setting

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

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



RTSP OSD Setting

RTSP OSD Color: White

RTSP OSD Text:

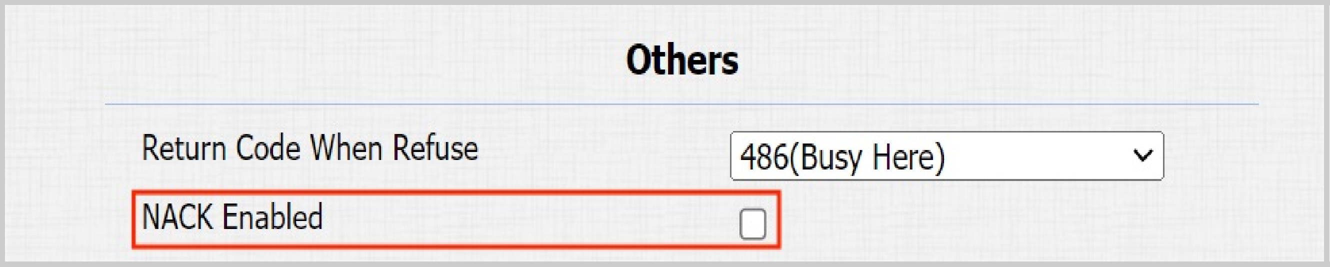
- **RTSP OSD Color**: There are five color options, White, Black, Red, Green, and Blue for RTSP watermark text.

- **RTSP OSD Text**: Customize the watermark text.

NACK

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

To enable NACK, navigate to the **Intercom > Call Feature > Others** interface.



Others

Return Code When Refuse: 486(Busy Here)

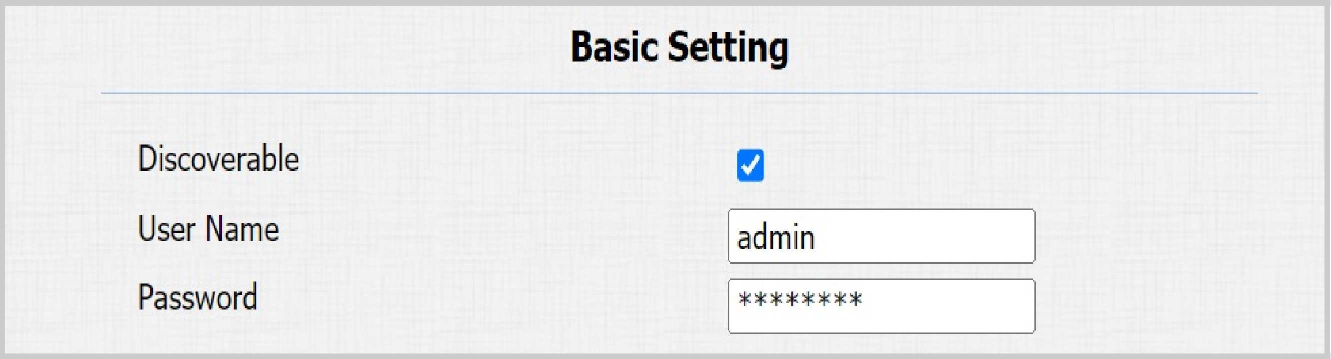
NACK Enabled ☐

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

ONVIF

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

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



Basic Setting

Discoverable ☑

User Name: admin

Password: ********

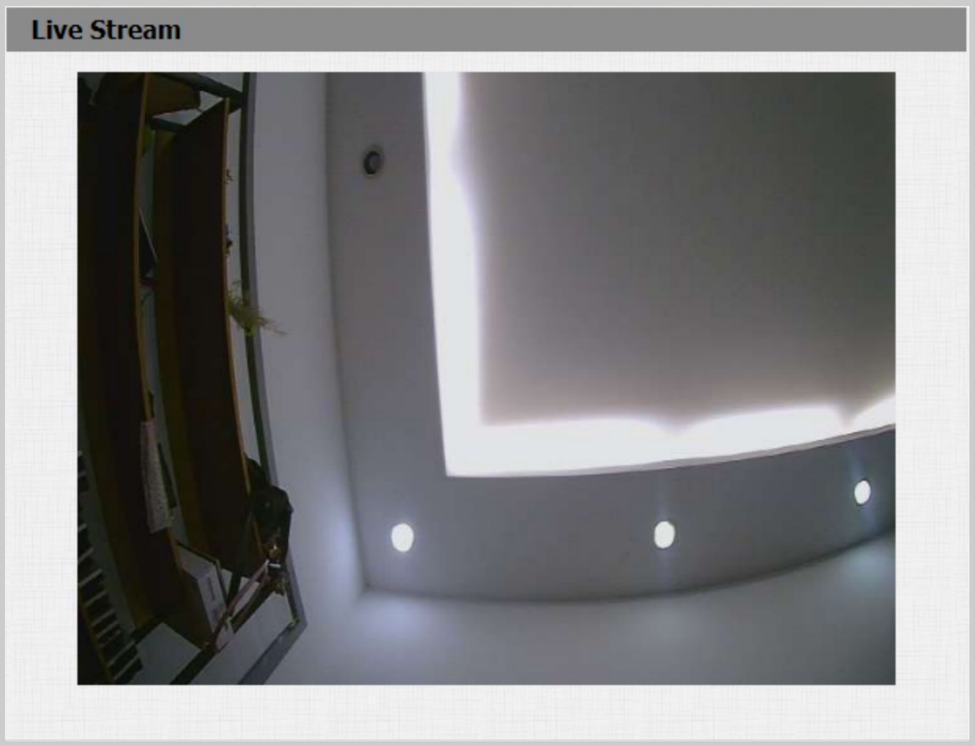
- **Discoverable**: When enabled, the video from the door phone camera can be searched by other devices.
- **User Name**: Set the username required for accessing the door phone's video stream on other devices. It is admin by default.
- **Password**: Set the password required for accessing the door phone's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

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

Live Stream

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

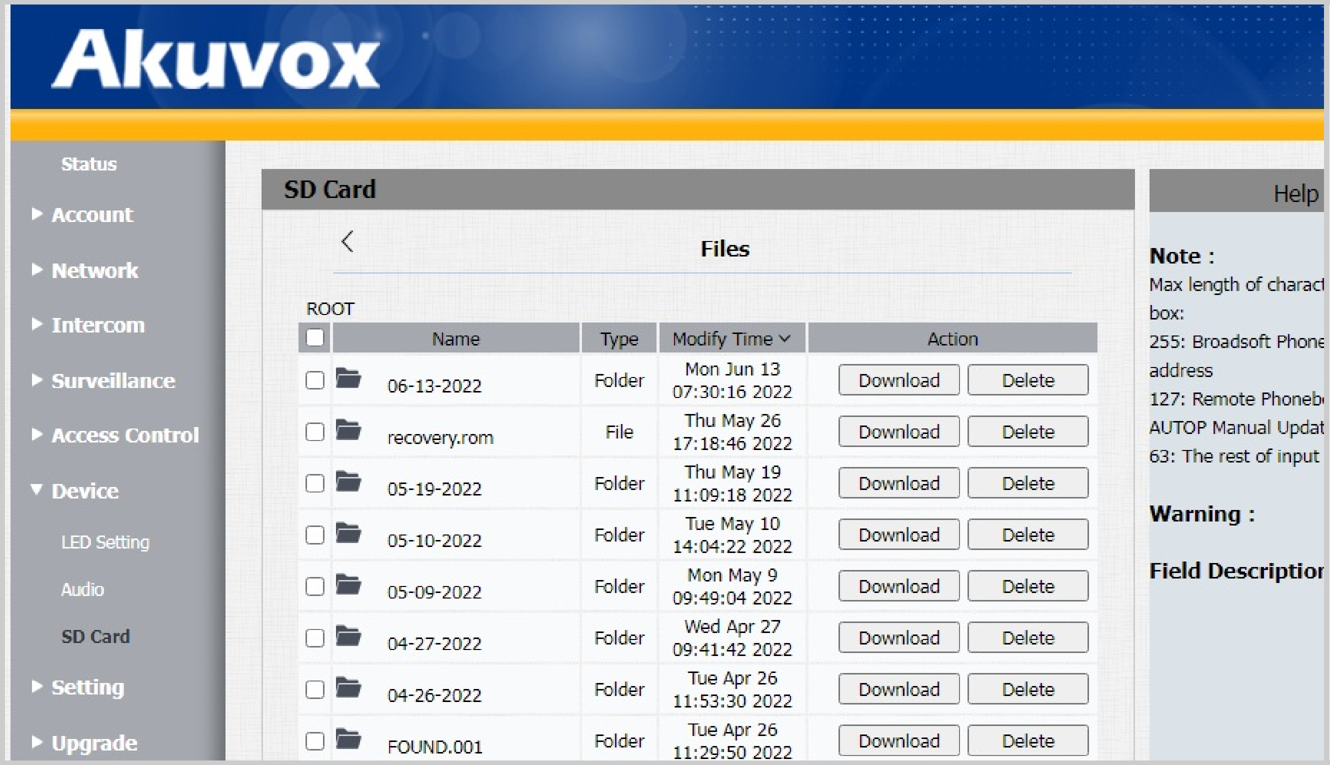
See live stream on the device **Surveillance > Live Stream** interface.



SD Card for Storing Videos

The device can be inserted into an SD card for storing motion and call videos.

To check the videos, go to **Device > SD Card** interface. When there is not enough space in the SD card to record the next video, the system automatically deletes the oldest video.



	Name	Type	Modify Time	Action	
☐	06-13-2022	Folder	Mon Jun 13 07:30:16 2022	Download	Delete
☐	recovery.rom	File	Thu May 26 17:18:46 2022	Download	Delete
☐	05-19-2022	Folder	Thu May 19 11:09:18 2022	Download	Delete
☐	05-10-2022	Folder	Tue May 10 14:04:22 2022	Download	Delete
☐	05-09-2022	Folder	Mon May 9 09:49:04 2022	Download	Delete
☐	04-27-2022	Folder	Wed Apr 27 09:41:42 2022	Download	Delete
☐	04-26-2022	Folder	Tue Apr 26 11:53:30 2022	Download	Delete
☐	FOUND.001	Folder	Tue Apr 26 11:29:50 2022	Download	Delete

Note :
Max length of charact
box:
255: Broadsoft Phone
address
127: Remote Phoneb
AUTOP Manual Updat
63: The rest of input

Warning :

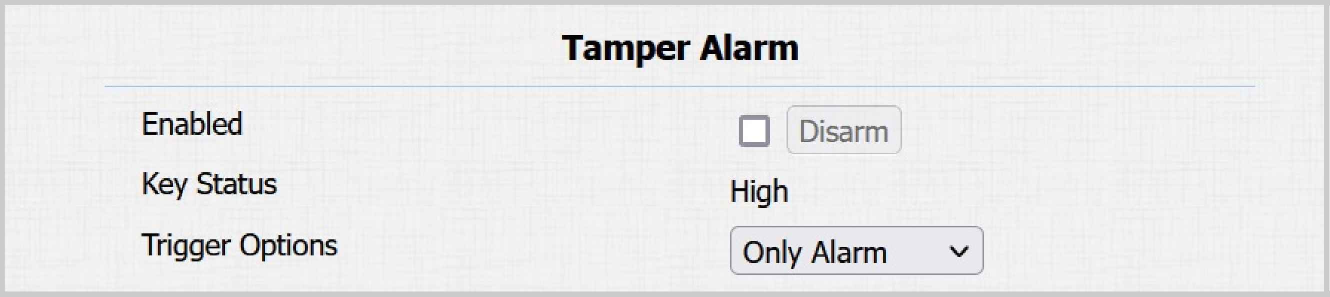
Field Descriptior

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.

Set it up on the **Security** > **Basic** > **Tamper Alarm** interface. Click Disarm to clear the alarm.



Tamper Alarm

Enabled	☐ Disarm
Key Status	High
Trigger Options	Only Alarm

- **Trigger Options:** Select what can be triggered when the gravity sensor is triggered.

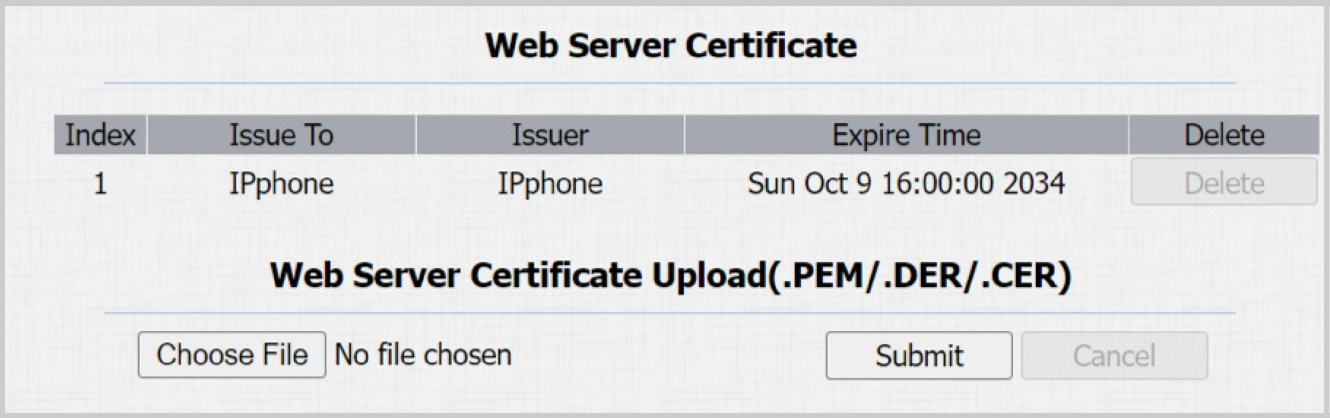
Client Certificate Setting

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

Web Server Certificate

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

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



Web Server Certificate

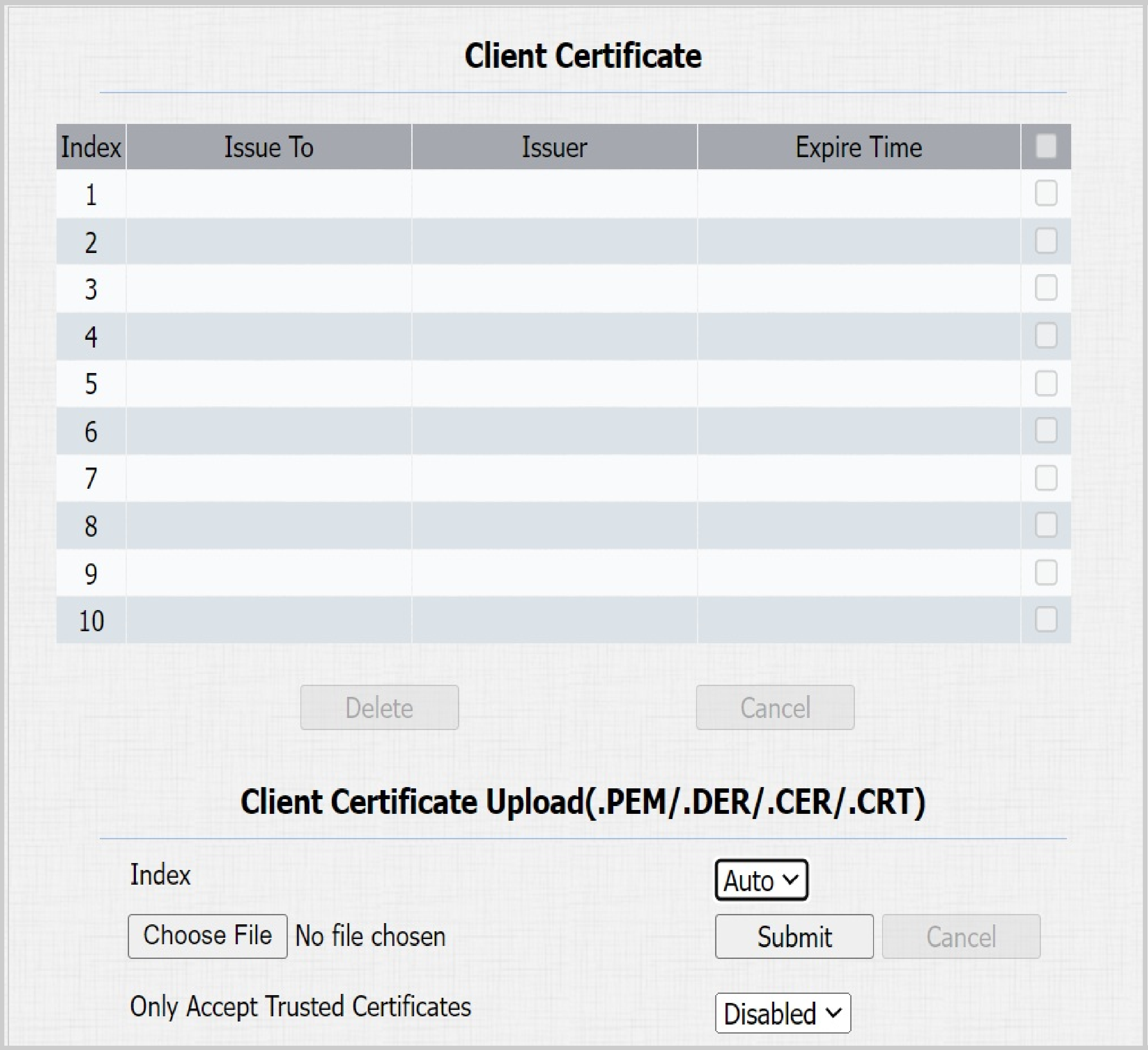
Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

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

Client Certificate

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

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



Client Certificate

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

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

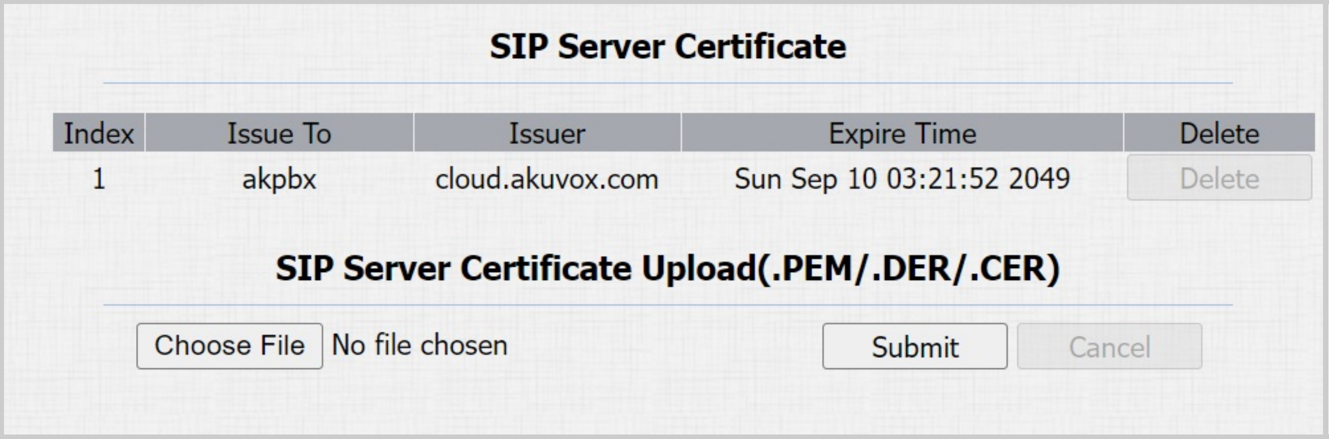
Index	Auto
Choose File No file chosen	Submit Cancel
Only Accept Trusted Certificates	Disabled

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

Upload TLS Certificate for SIP Account Registration

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

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



SIP Server Certificate

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

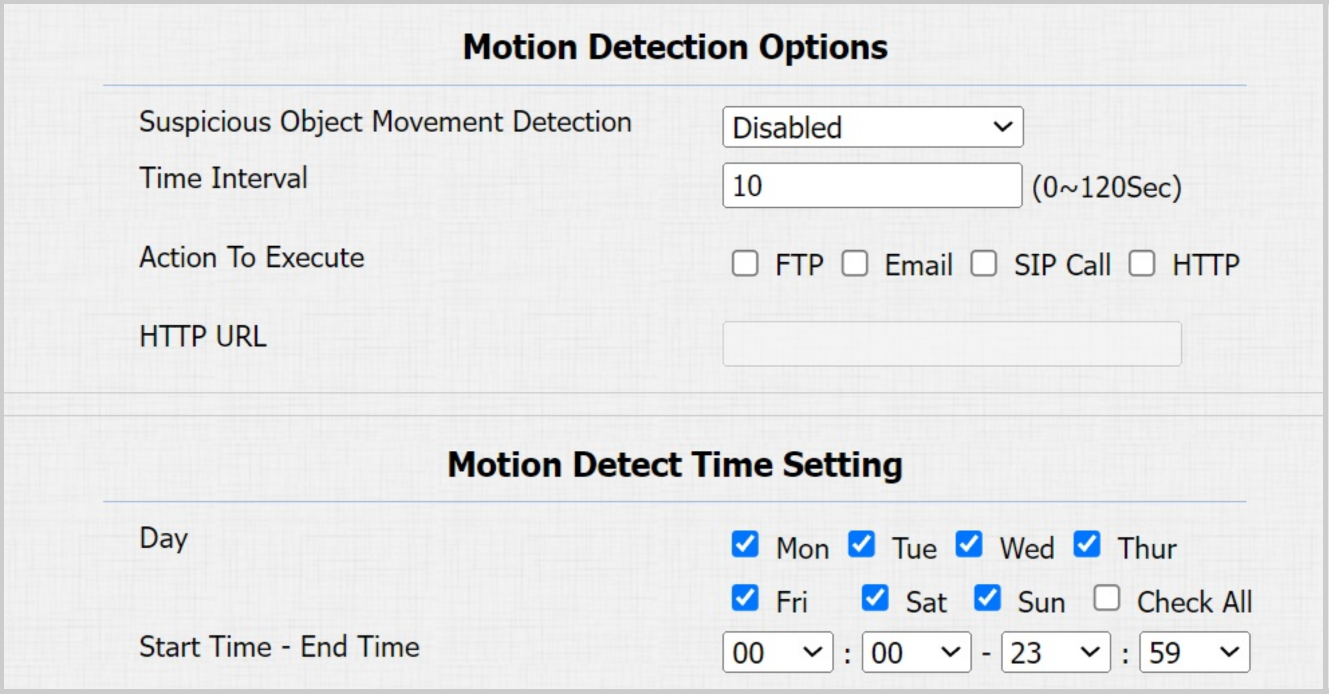
SIP Server Certificate Upload(.PEM/.DER/.CER)

Choose File No file chosen

Motion Detection

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

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



Motion Detection Options

Suspicious Object Movement Detection: Disabled

Time Interval: 10 (0~120Sec)

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

HTTP URL:

Motion Detect Time Setting

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

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

- **Suspicious Object Movement Detection:** Select Video Detection to enable video-based motion detection during the monitoring of the suspicious moving object.

- **Time Interval:** If you set the default time interval as 10 sec, the motion detection period will be 10 seconds. Assuming that we set the time interval as 10, and the first movement captured can be seen as the start point of the motion detection, and if the movement continues through 7 seconds of the 10 seconds interval, the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) anywhere between 7-10 seconds once the movement is detected. A 10-second interval is a complete cycle of motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the **Time interval minus three**.
- **Action To Execute**: Set the desired actions that occur when suspicious movement is detected.
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - SIP Call: Call the preset number upon trigger.
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

Security Notification

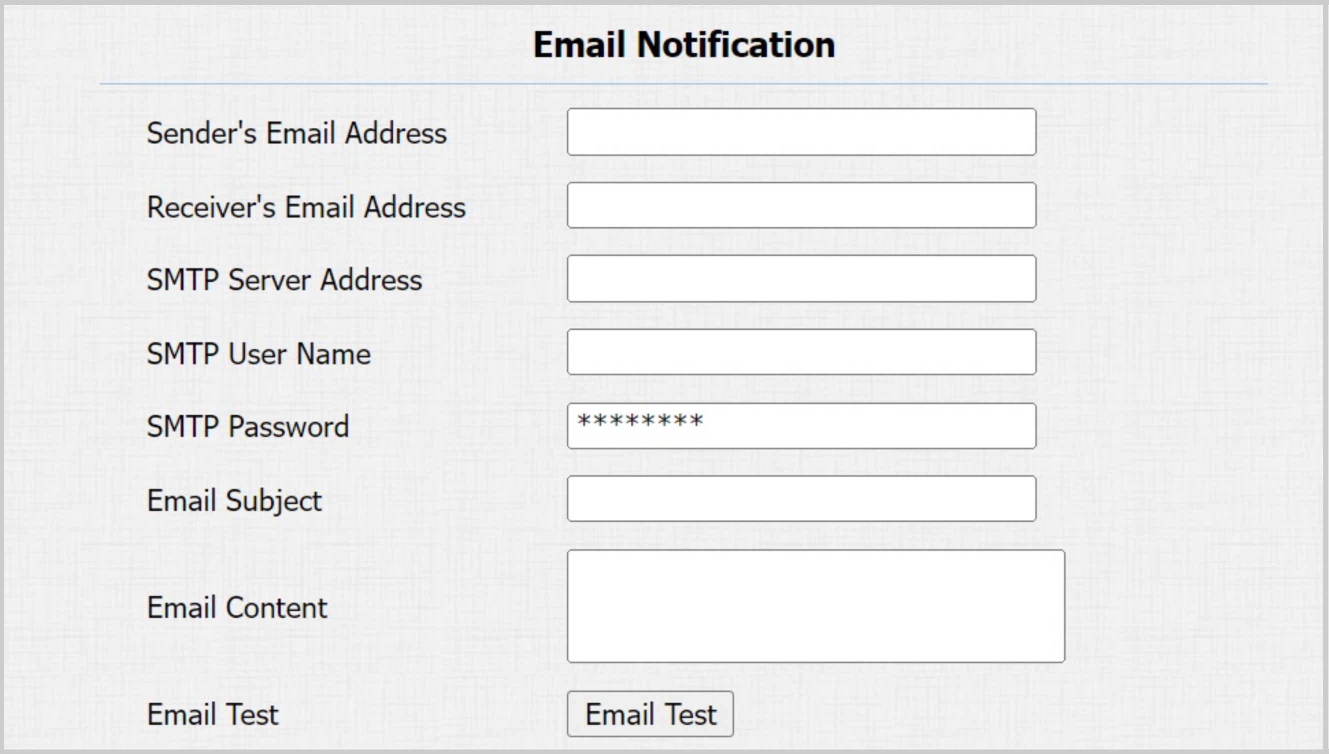
A security notification informs users or security personnel of any breach or threat that the door phone detects. For example, if the door phone detects something unusual, the system sends a notification to users or security through email, phone call, or other methods.

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

Email Notification

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

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



Email Notification

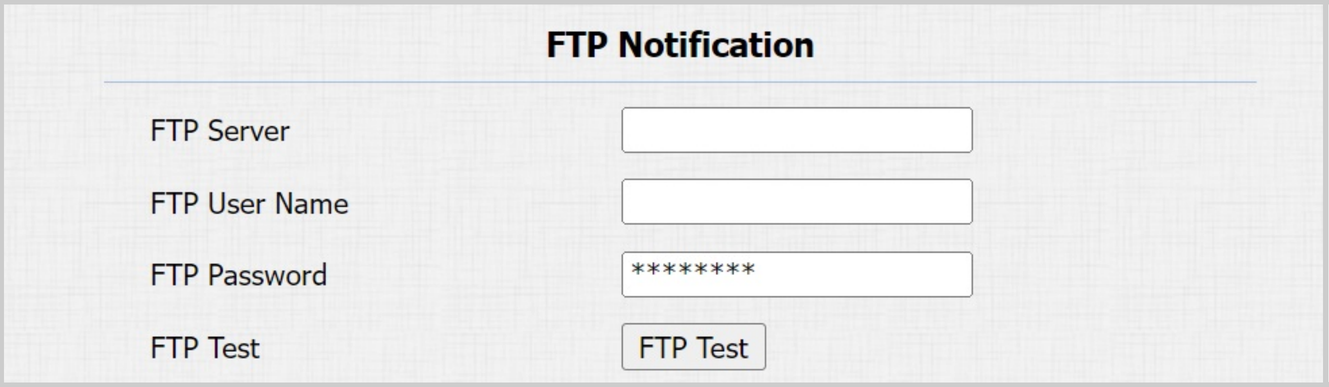
Sender's Email Address	
Receiver's Email Address	
SMTP Server Address	
SMTP User Name	
SMTP Password	********
Email Subject	
Email Content	
Email Test	Email Test

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

FTP Notification

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

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



FTP Notification

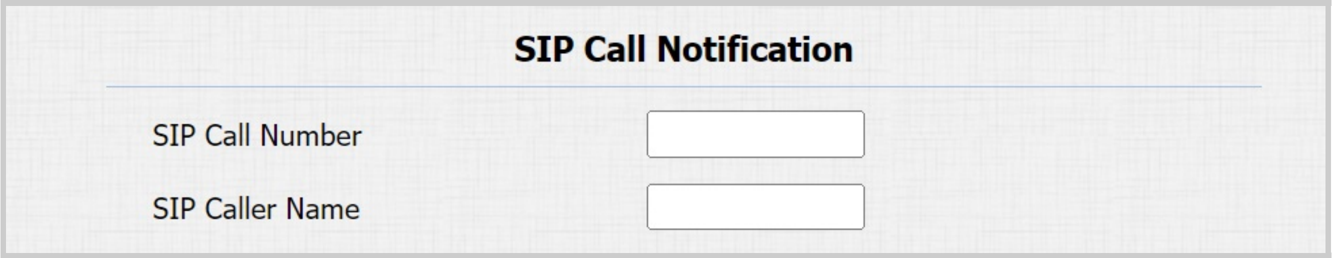
FTP Server	
FTP User Name	
FTP Password	********
FTP Test	FTP Test

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

SIP Call Notification

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

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



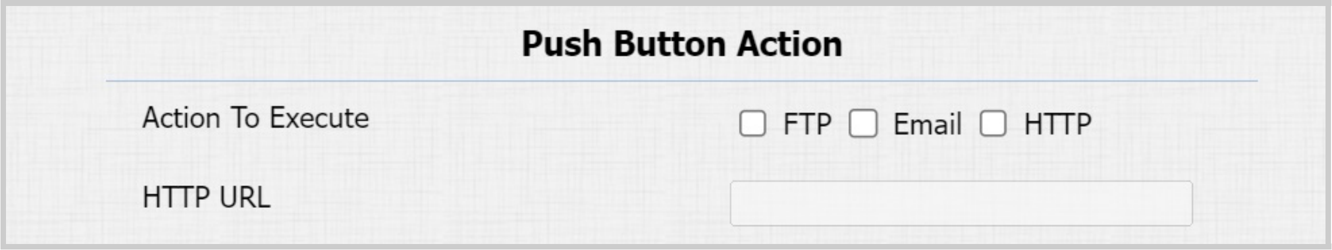
SIP Call Notification

SIP Call Number	
SIP Caller Name	

HTTP Notification

You can also set up an HTTP message sent to the HTTP server.

Set up the HTTP URL when configuring desired actions. The URL format is http://HTTP server's IP/Message content.



Push Button Action

Action To Execute	□ FTP □ Email □ HTTP
HTTP URL	

Action URL

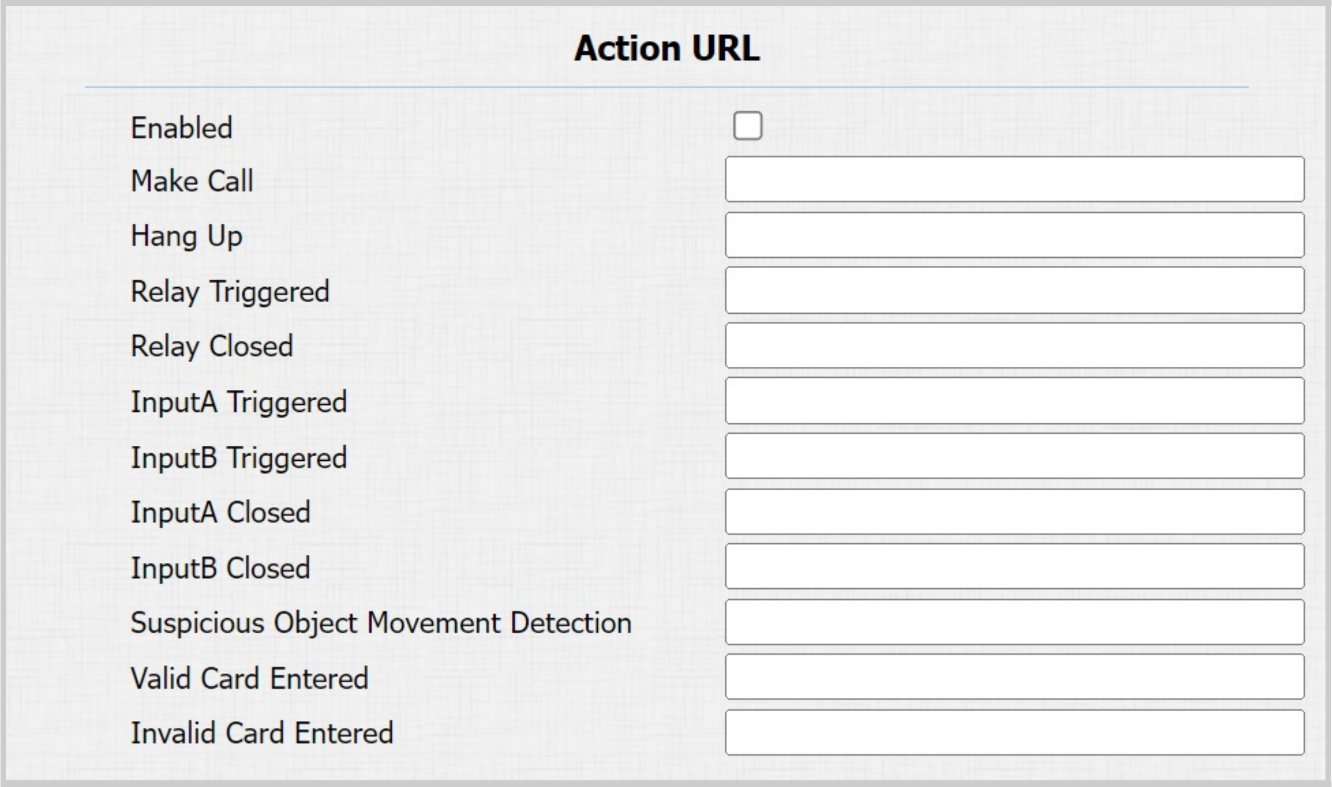
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, or RF card access changes.

Akuvox Action URL:

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

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

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



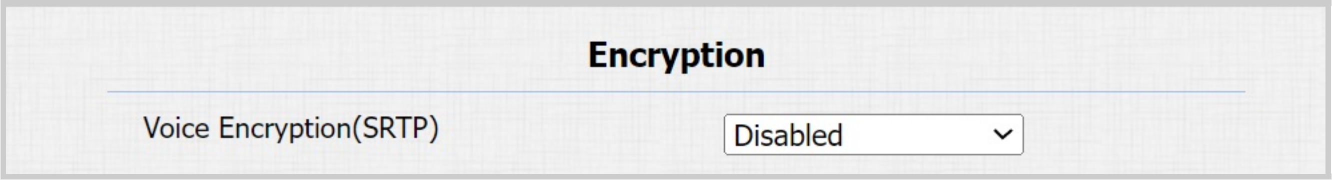
Action URL

Enabled	□
Make Call	
Hang Up	
Relay Triggered	
Relay Closed	
InputA Triggered	
InputB Triggered	
InputA Closed	
InputB Closed	
Suspicious Object Movement Detection	
Valid Card Entered	
Invalid Card Entered	

Voice Encryption

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

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



Encryption

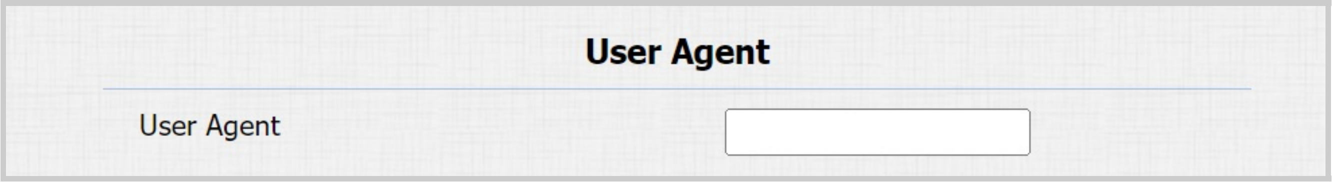
Voice Encryption(SRTP) Disabled

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

User Agent

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

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



User Agent

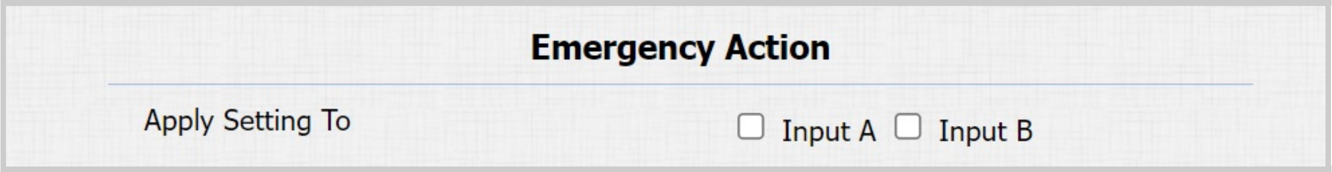
User Agent	

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

Emergency Action

This feature works with Akuvox SmartPlus Cloud. It keeps the door open when an emergency happens.

To set it up, go to **Security** > **Basic** > **Emergency Action** interface. Select the Input(s) to be triggered.



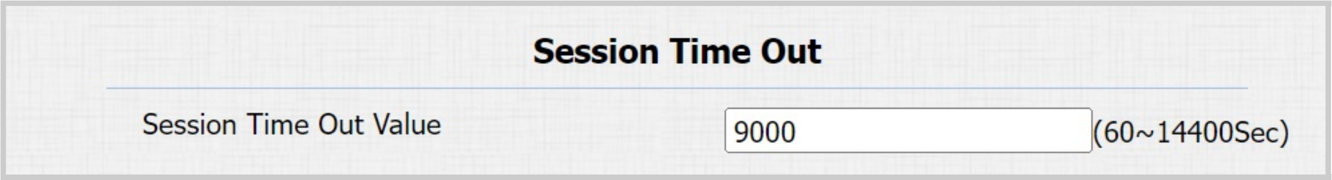
Emergency Action

Apply Setting To	☐ Input A ☐ Input B

Web Interface Automatic Log-out

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

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



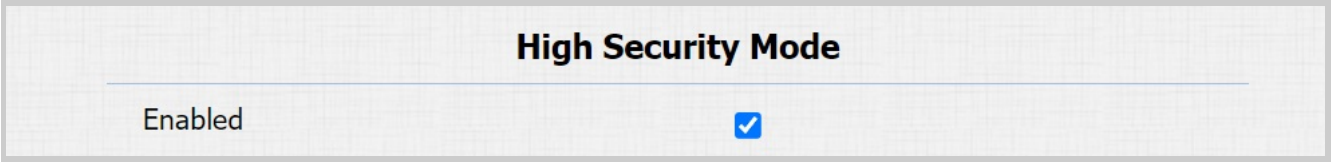
Session Time Out

Session Time Out Value	9000 (60~14400Sec)

High Security Mode

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

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



High Security Mode

Enabled	☑

Important Notes

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

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

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

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

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

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

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

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

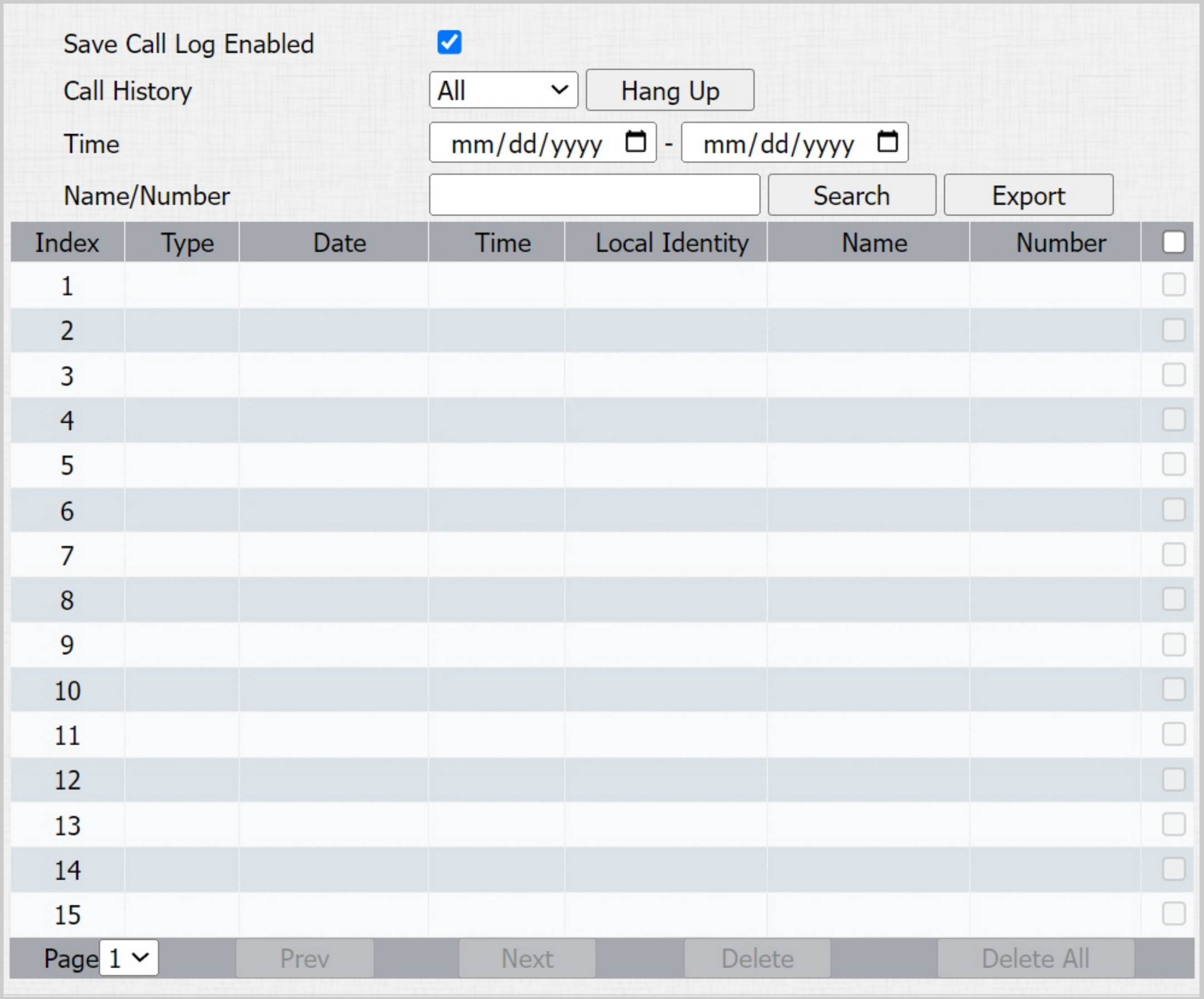
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

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

Go to the **Intercom** > **Call Log** interface.



Save Call Log Enabled ☑

Call History: All — Hang Up

Time: mm/dd/yyyy - mm/dd/yyyy

Name/Number: — Search — Export

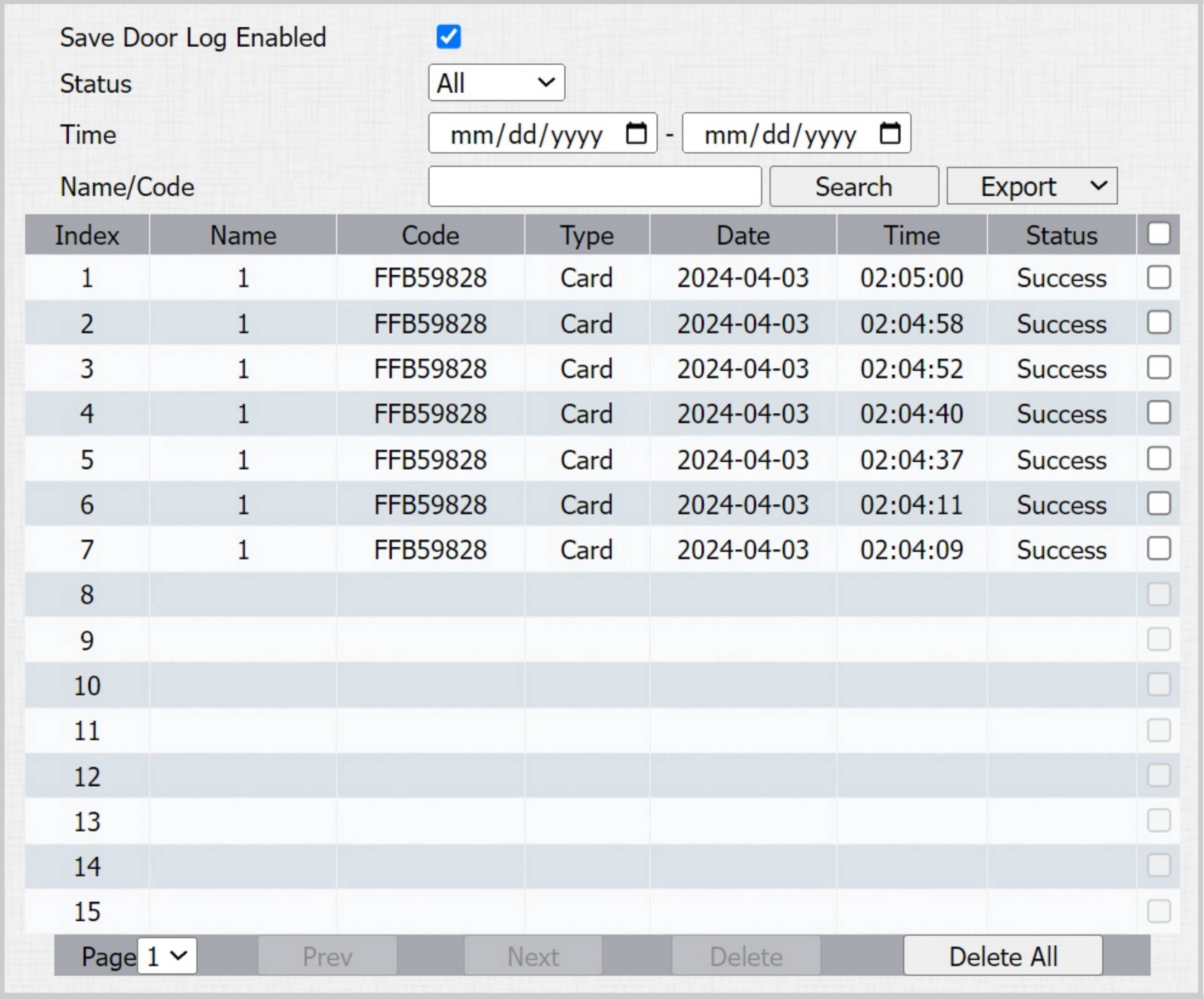
Index	Type	Date	Time	Local Identity	Name	Number	□
1							□
2							□
3							□
4							□
5							□
6							□
7							□
8							□
9							□
10							□
11							□
12							□
13							□
14							□
15							□

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

Door Logs

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

Go to the **Access Control** > **Door Log** interface.



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

Index	Name	Code	Type	Date	Time	Status	□
1	1	FFB59828	Card	2024-04-03	02:05:00	Success	□
2	1	FFB59828	Card	2024-04-03	02:04:58	Success	□
3	1	FFB59828	Card	2024-04-03	02:04:52	Success	□
4	1	FFB59828	Card	2024-04-03	02:04:40	Success	□
5	1	FFB59828	Card	2024-04-03	02:04:37	Success	□
6	1	FFB59828	Card	2024-04-03	02:04:11	Success	□
7	1	FFB59828	Card	2024-04-03	02:04:09	Success	□
8							□
9							□
10							□
11							□
12							□
13							□
14							□
15							□

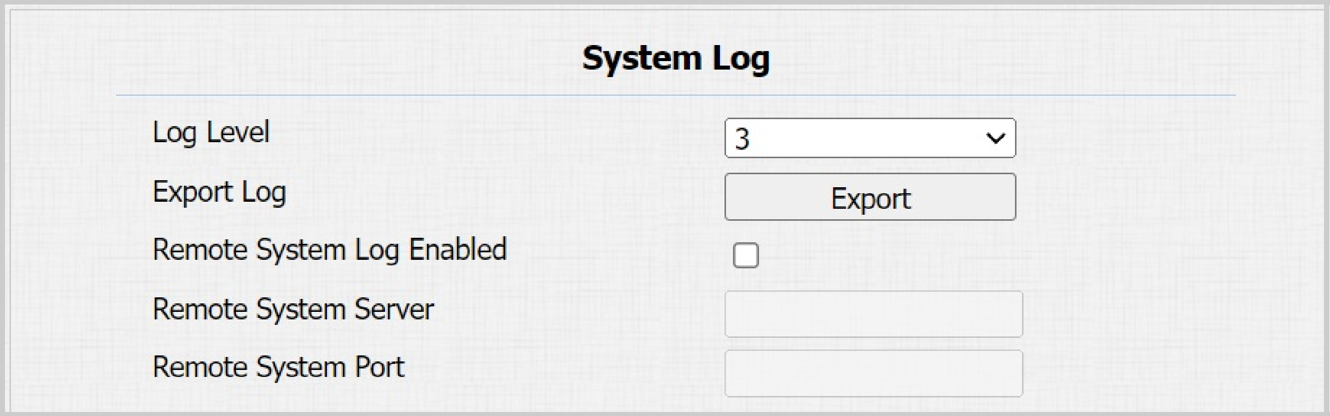
- **Status:** Display All, Successful, and Failed door-opening records.
- **Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card code will be displayed.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

Debug

System Log

System logs can be used for debugging purposes.

To set it up, navigate to the web **Upgrade > Diagnose > System Log** interface.



System Log

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

- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.

- **Export Log:** Click the Export tab to export a temporary debug log file to a local PC.

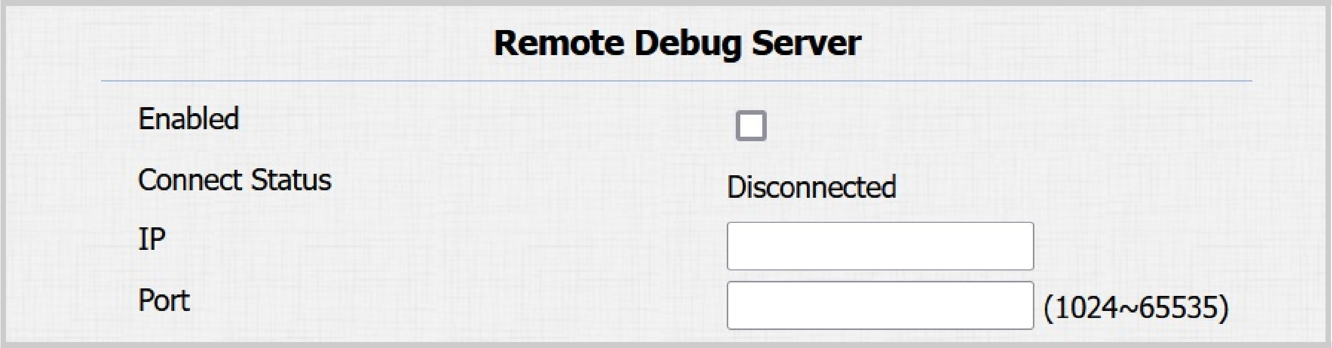
- **Remote System Server:** Set the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.

- **Remote System Port**: Set the remote system server’s port.

Remote Debug Server

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

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



Remote Debug Server

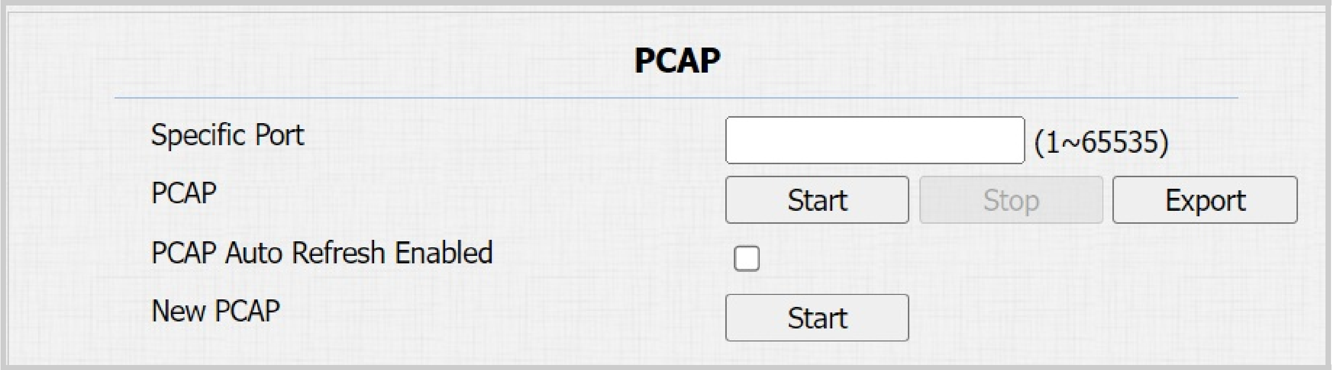
Enabled	□
Connect Status	Disconnected
IP	
Port	(1024~65535)

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

PCAP

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

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



PCAP

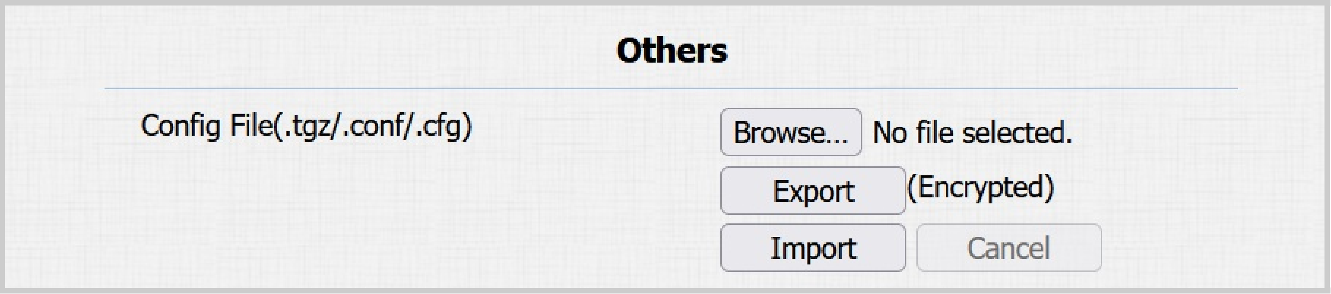
Specific Port	(1~65535)
PCAP	Start Stop Export
PCAP Auto Refresh Enabled	□
New PCAP	Start

- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum in capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.
- **New PCAP:** Click Start to capture a bigger data package.

Backup

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

Export the file on the **Upgrade > Diagnose > Others** interface



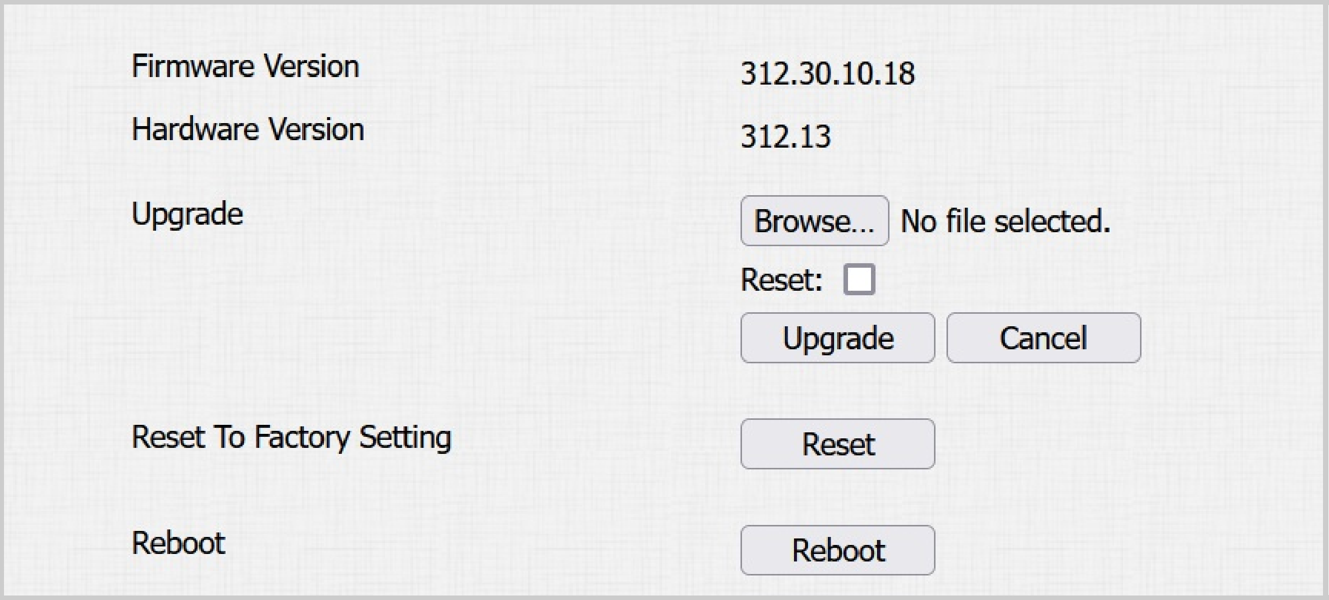
Others

Config File(.tgz/.conf/.cfg) Browse... No file selected.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Firmware Version 312.30.10.18

Hardware Version 312.13

Upgrade No file selected.

Reset: □

Reset To Factory Setting

Reboot

Note

The upgrade files should be in .rom format.

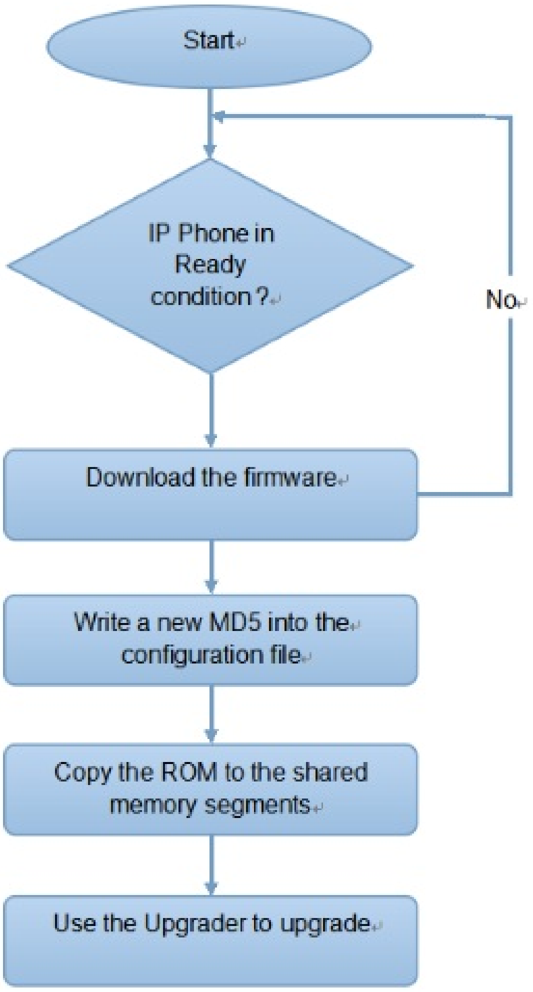
Auto-provisioning via Configuration File

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:


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

Configuration Files for Auto-provisioning

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

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

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

Note

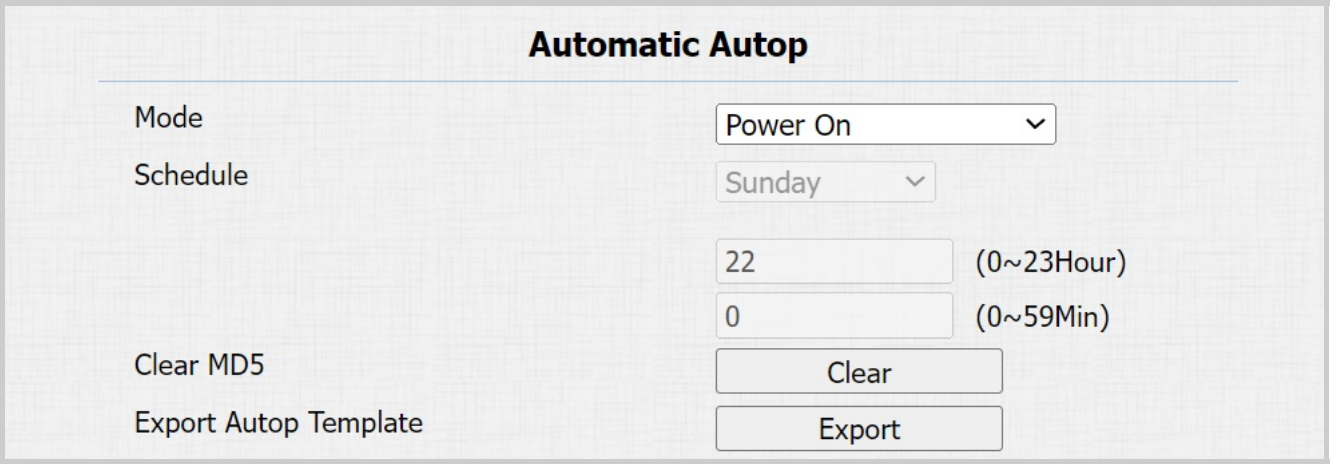
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will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

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

AutoP Schedule

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

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



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

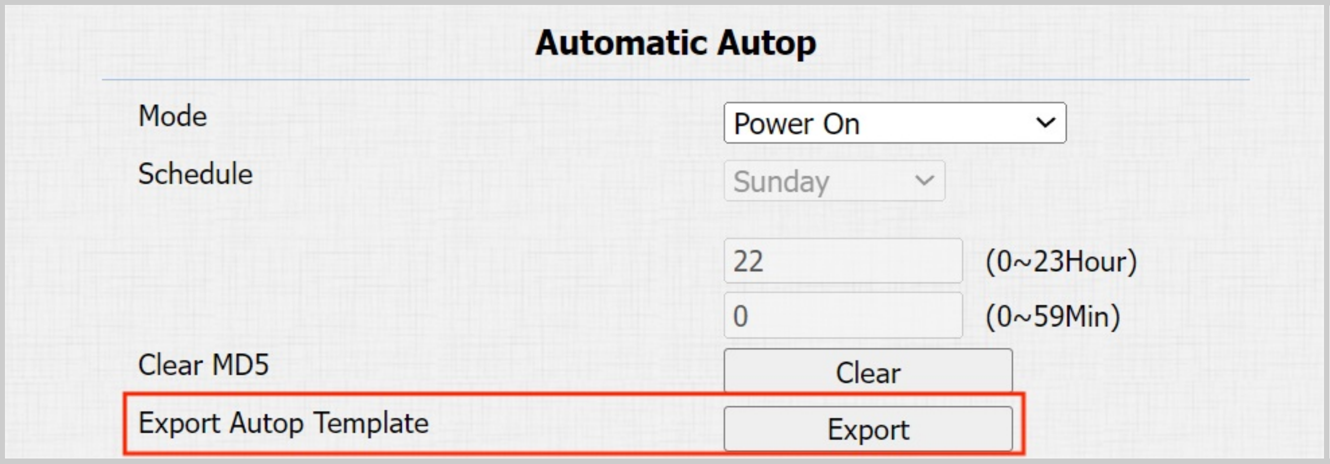
Export Autop Template: Export

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

Static Provisioning

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

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



Automatic Autop

Mode: Power On

Schedule: Sunday

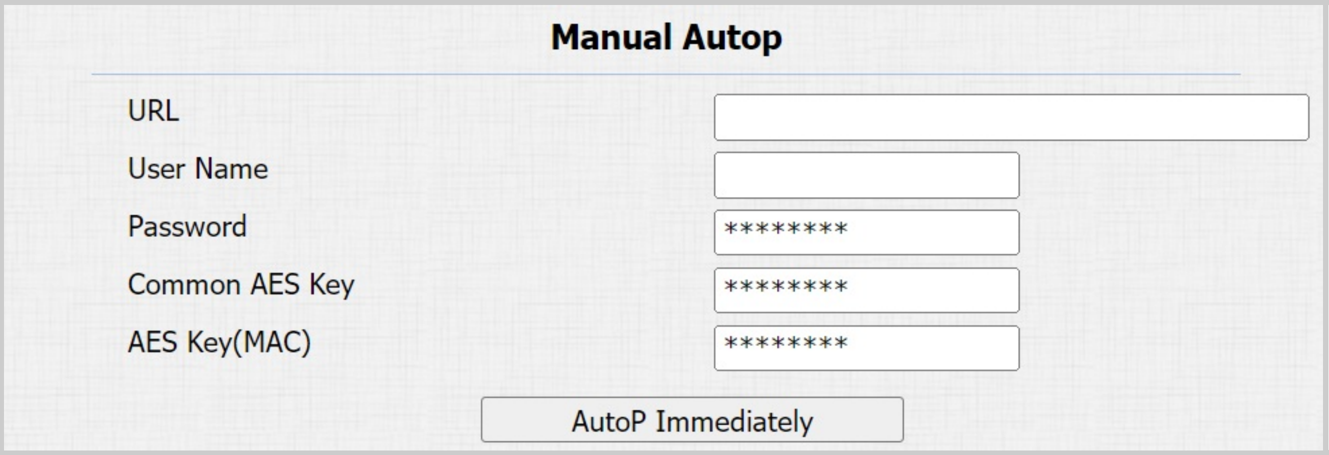
22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

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



Manual Autop

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

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

Note

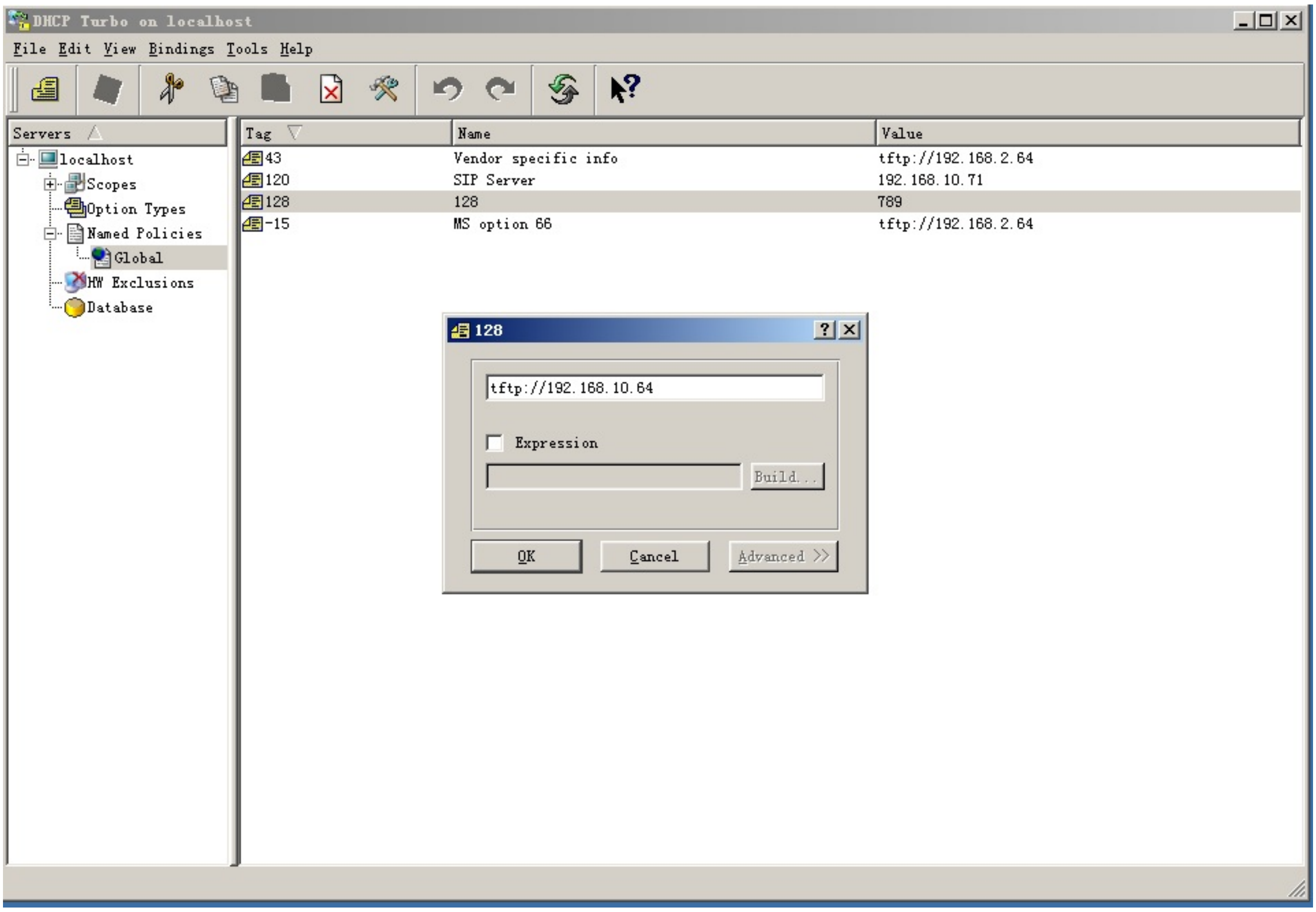
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning Configuration

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



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

tftp://192.168.10.64

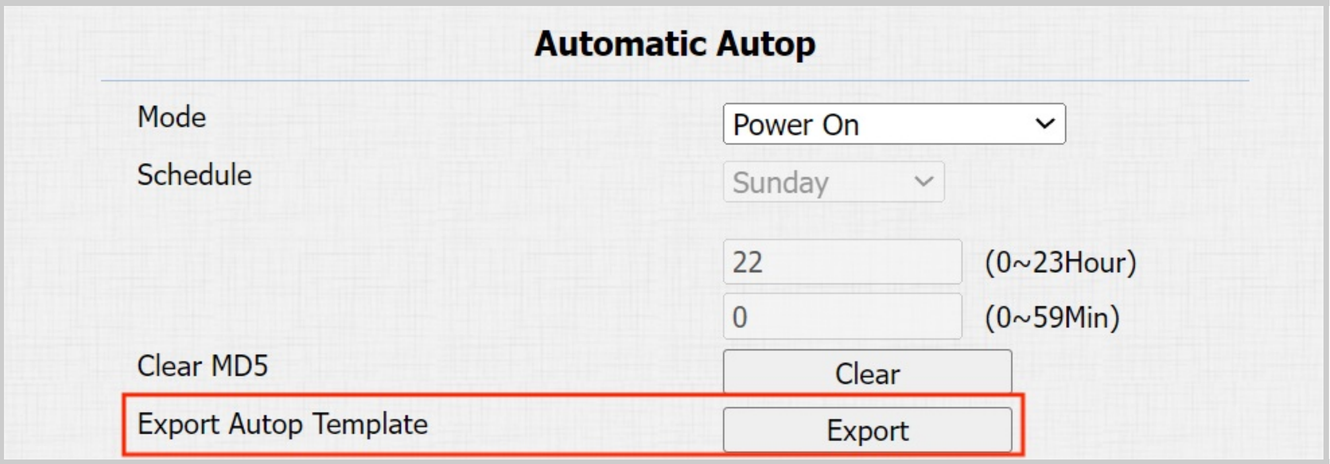
☐ Expression

Note

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

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

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



Automatic Autop

Mode: Power On

Schedule: Sunday

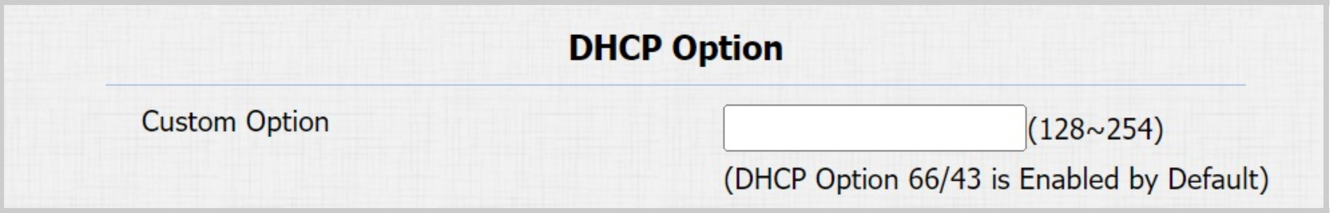
22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

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



DHCP Option

Custom Option: (128~254)

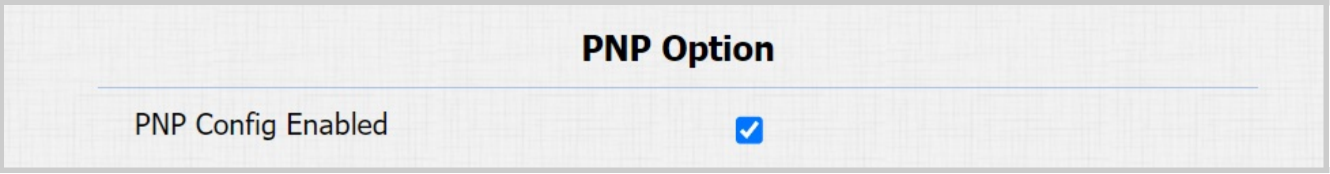
(DHCP Option 66/43 is Enabled by Default)

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

PNP Configuration

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

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



PNP Option

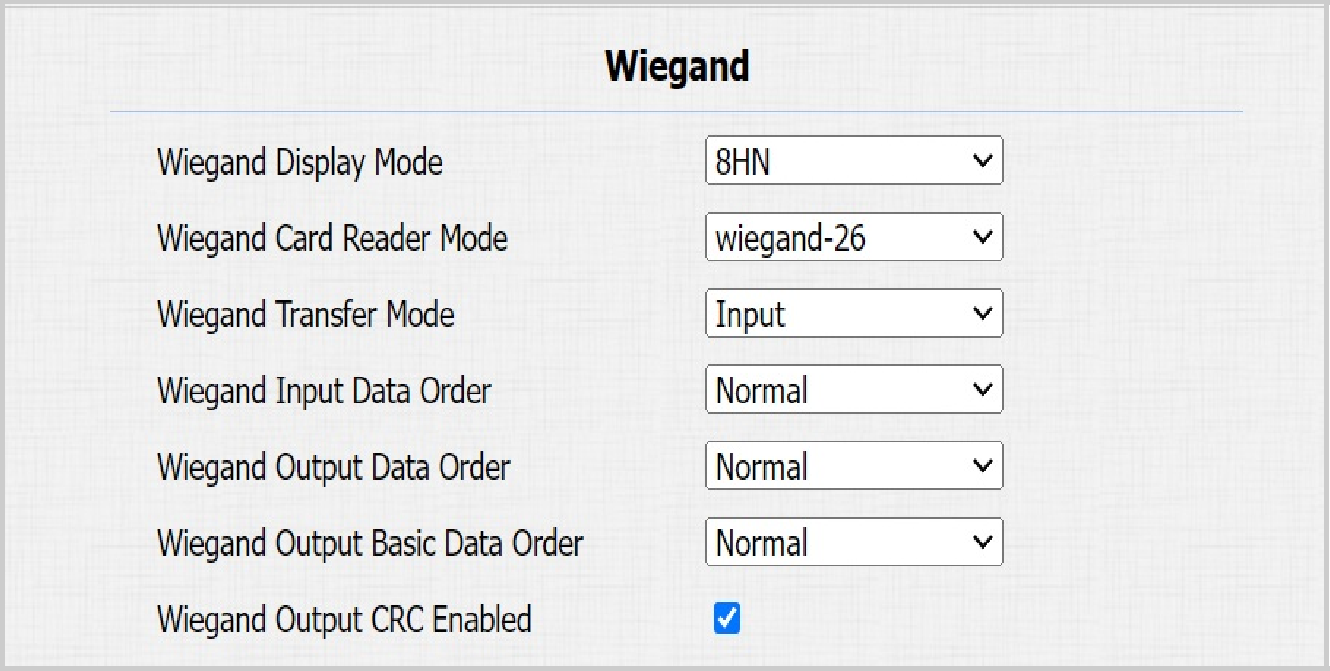
PNP Config Enabled ☑

Integration with Third Party Device

Integration via Wiegand

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

Set it up on the **Access Control > Card Setting > Wiegand** interface.



Wiegand

Wiegand Display Mode	8HN
Wiegand Card Reader Mode	wiegand-26
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output CRC Enabled	☑

- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the access control terminal and the third-party device. It is automatically configured.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender. If users can only open the door by swiping an RF card, select the Wiegand transfer mode as Output.
  - **Convert To Card No. Output**: The device serves as a sender. If users are assigned multiple door-opening methods, select the Wiegand transfer mode as Convert To Card No. Output.

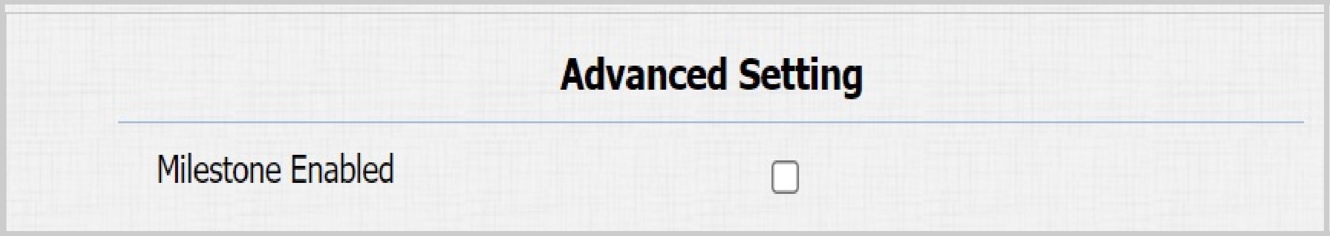
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- **Wiegand Output Data Order:** Determine the sequence of the card number.
  - **Normal**: The card number is displayed as received.
  - **Reversed**: The order of the card number is reversed.
- **Wiegand Output Basic Data Order**: Set the sequence of the Wiegand output data.
  - **Normal**: The data is displayed as received.
  - **Reversed**: The order of the data bits is reversed.
- **Wiegand Output CRC Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.

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

Integration with Milestone

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

Enable it on the **Surveillance** > **ONVIF** > **Advanced Setting** interface.



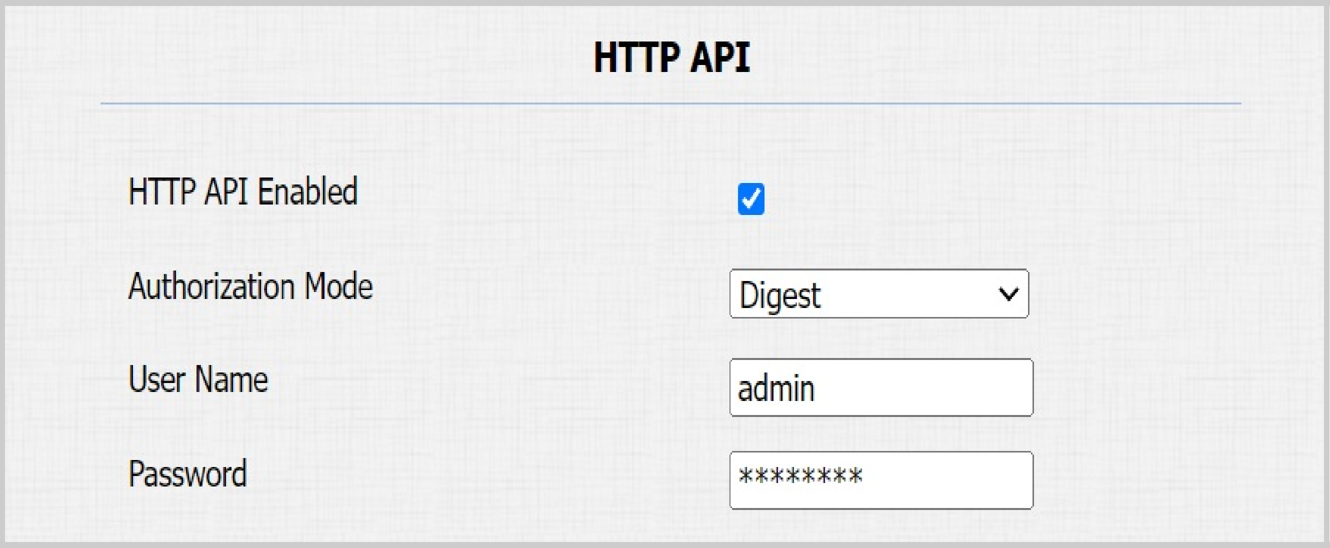
Advanced Setting

Milestone Enabled □

Integration via HTTP API

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

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



HTTP API

HTTP API Enabled ☑

Authorization Mode: Digest

User Name: admin

Password: ********

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

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

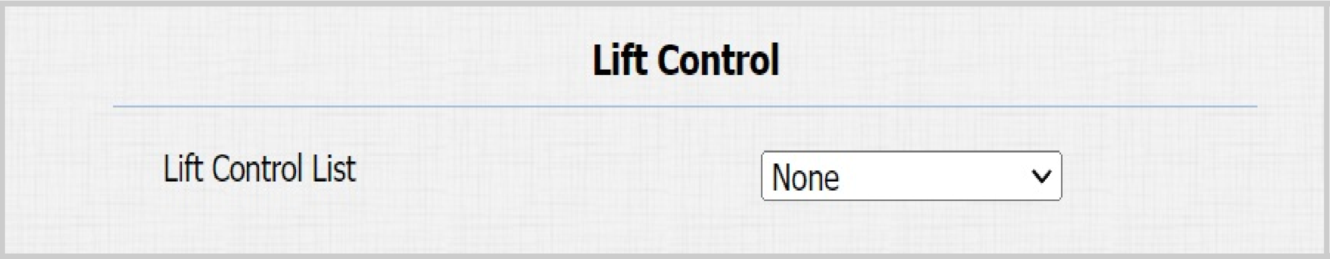
- **Username**: Enter the user name for authentication. The default is admin.

- **Password**: Enter the password for authentication. The default is admin.

Lift Control

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

Set it up on the **Access Control > Lift Control** interface.



Lift Control

Lift Control List: None

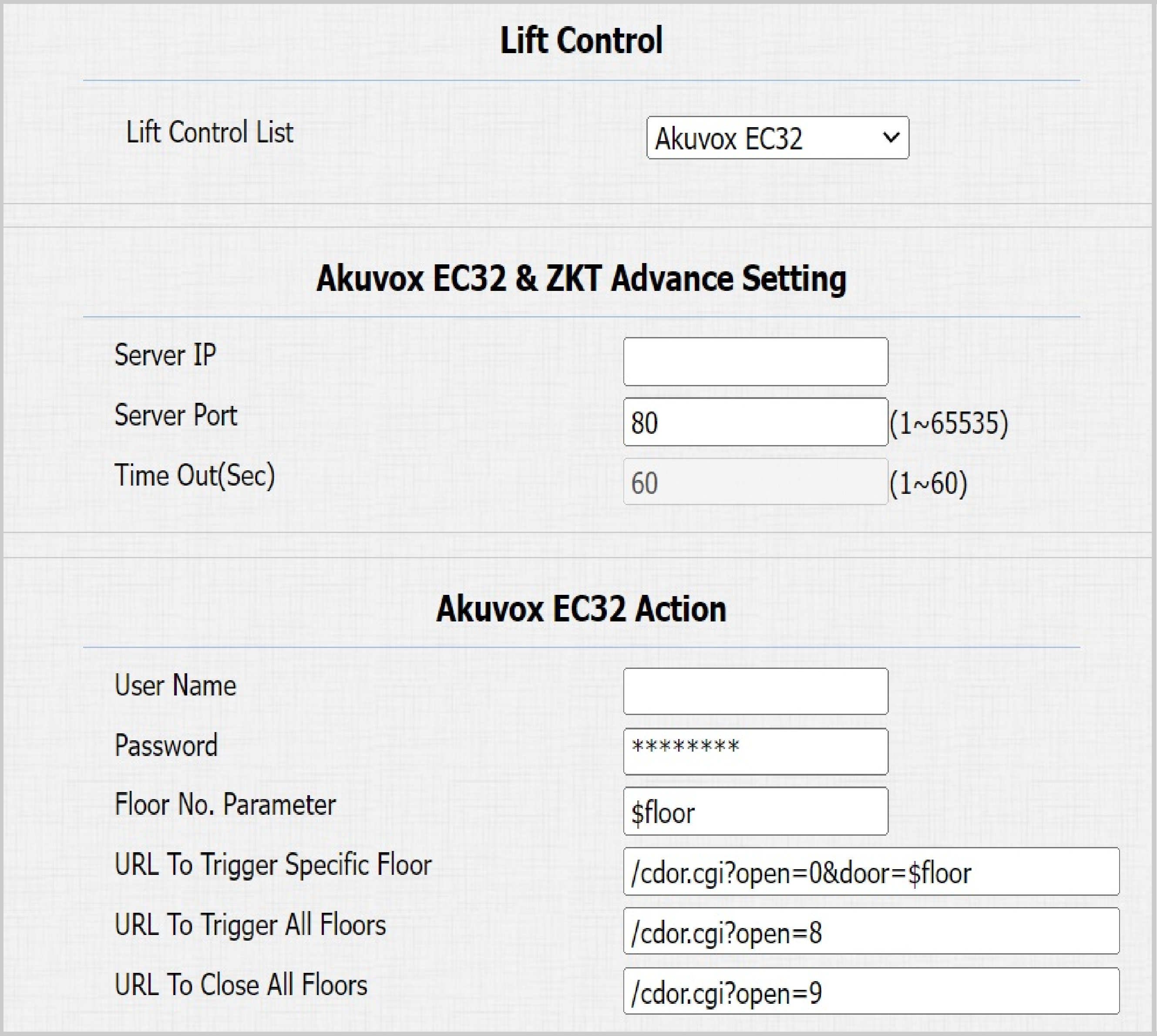
- **Life Control List:** Select the lift controller brand.
  - None: The RS485 integration will be disabled.

  - Akuvox EC32: Connect the device with the Akuvox EC33 lift controller.
  - ZKT: Integrate with ZKTeco 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.
> You may click here to view Lift Control configuration example.

Akuvox Lift Controller

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



Lift Control

Lift Control List: Akuvox EC32

Akuvox EC32 & ZKT Advance Setting

Server IP		
Server Port	80	(1~65535)
Time Out(Sec)	60	(1~60)

Akuvox EC32 Action

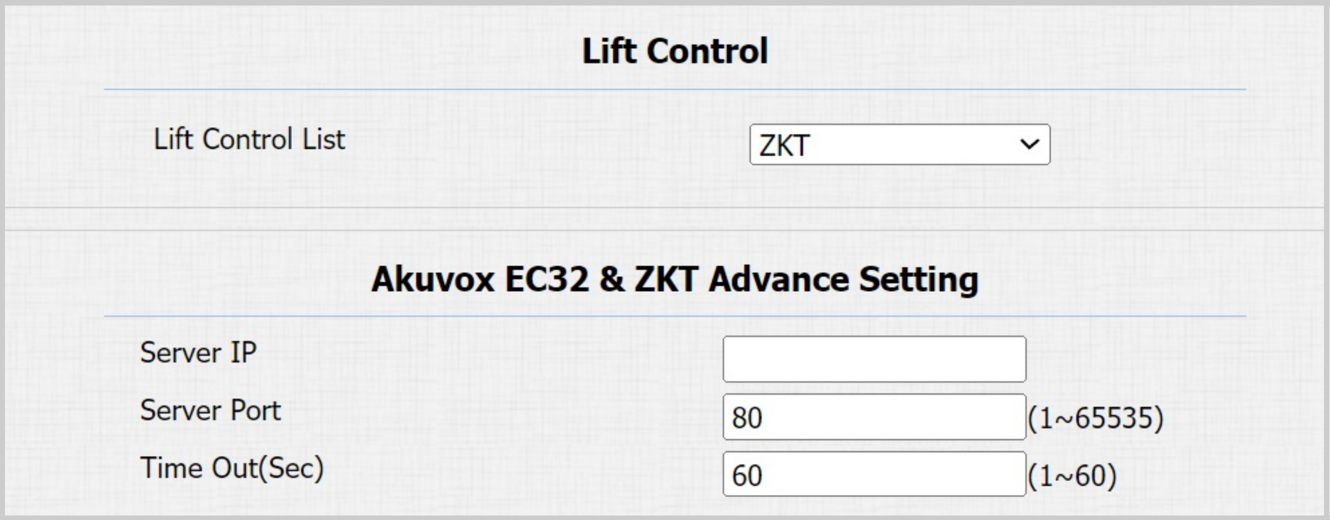
User Name	
Password	********
Floor No. Parameter	$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=$floor
URL To Trigger All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9

- **Server IP:** Enter the IP address of the Akuvox lift controller.

- **Server Port:** Enter the port of the Akuvox lift controller.
- **Time Out(Sec):** Decide the time limit within which users should press the lift button of their desired floors.
- **User Name:** Enter the user name set in the lift controller.
- **Password:** Enter the password set in the lift controller.
- **Floor NO. Parameter:** The floor number parameter is provided by Akuvox. The default is **$floor**. You can define your parameter string.
- **URL To Trigger Specific Floor:** The Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$ floor, but the string $floor at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors:** The Akuvox URL for triggering all floors.
- **URL To Close All Floors:** The Akuvox URL for closing all floors.

ZKT Lift Controller

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



Lift Control

Lift Control List: ZKT

Akuvox EC32 & ZKT Advance Setting

Server IP:

Server Port: 80 (1~65535)

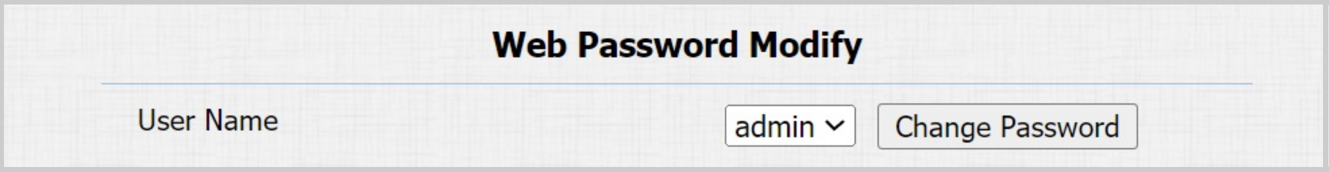
Time Out(Sec): 60 (1~60)

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

Password Modification

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

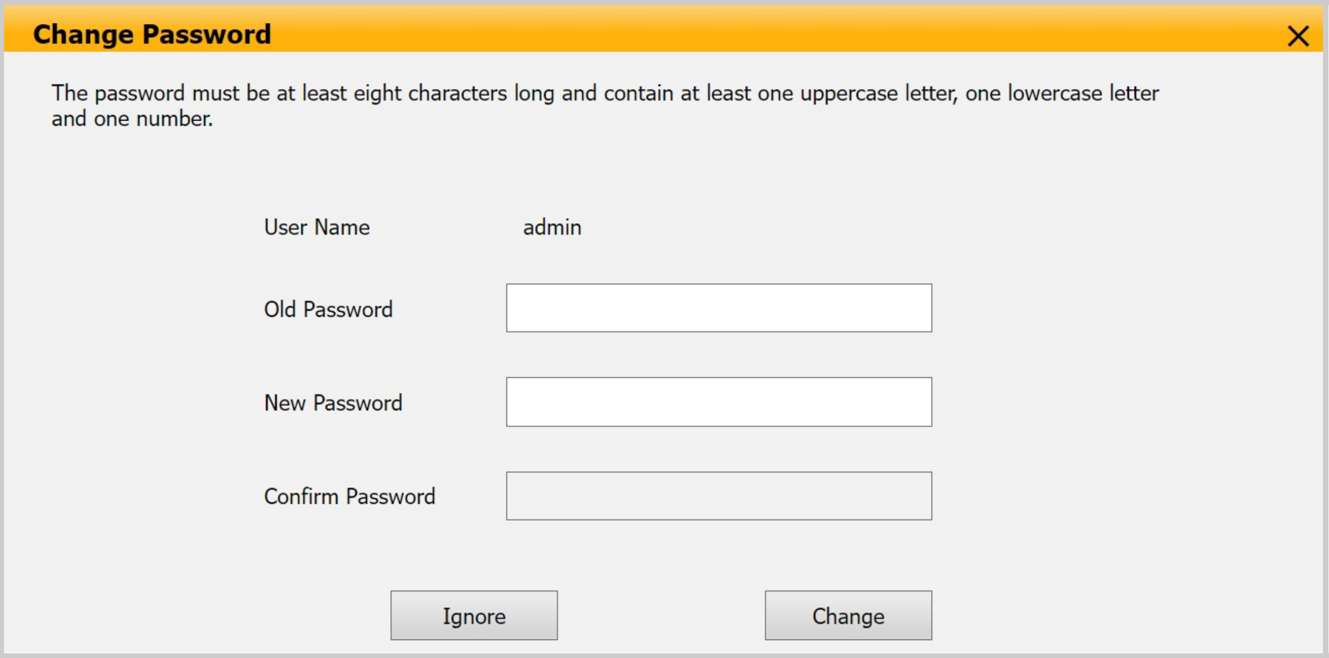
To set it up, go to **Security** > **Basic** > **Web Password Modify** interface.



Web Password Modify

User Name: admin

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



Change Password

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

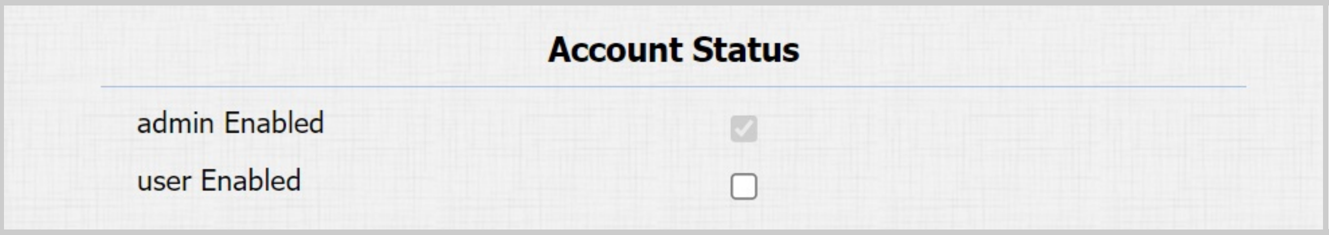
User Name: admin

Old Password

New Password

Confirm Password

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



Account Status

admin Enabled ☑

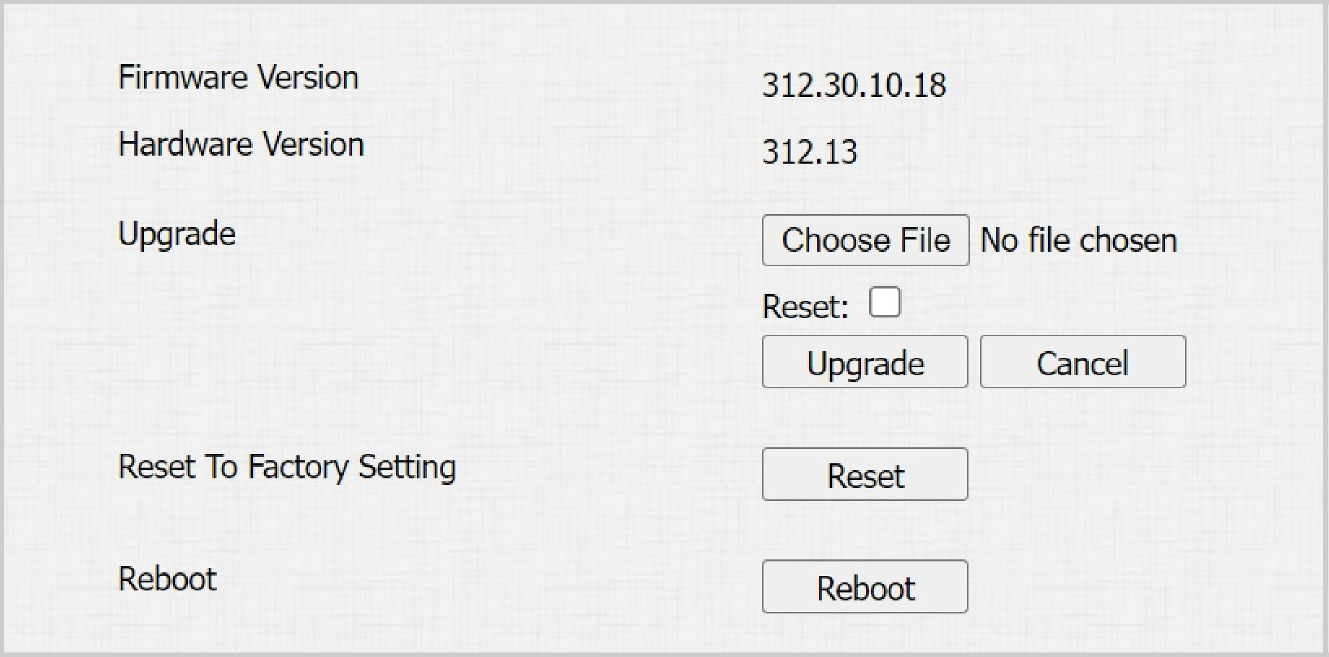
user Enabled □

System Reboot&Reset

Reboot

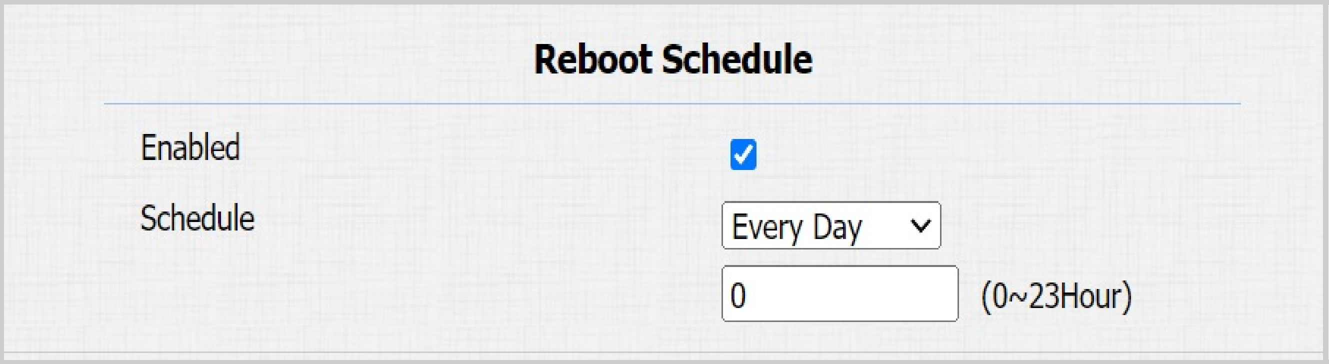
If you want to restart the device system, you can operate it on the device web. Moreover, you can set up a schedule for the device to be restarted.

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



Firmware Version	312.30.10.18
Hardware Version	312.13
Upgrade	Choose File No file chosen Reset: □ Upgrade Cancel
Reset To Factory Setting	Reset
Reboot	Reboot

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

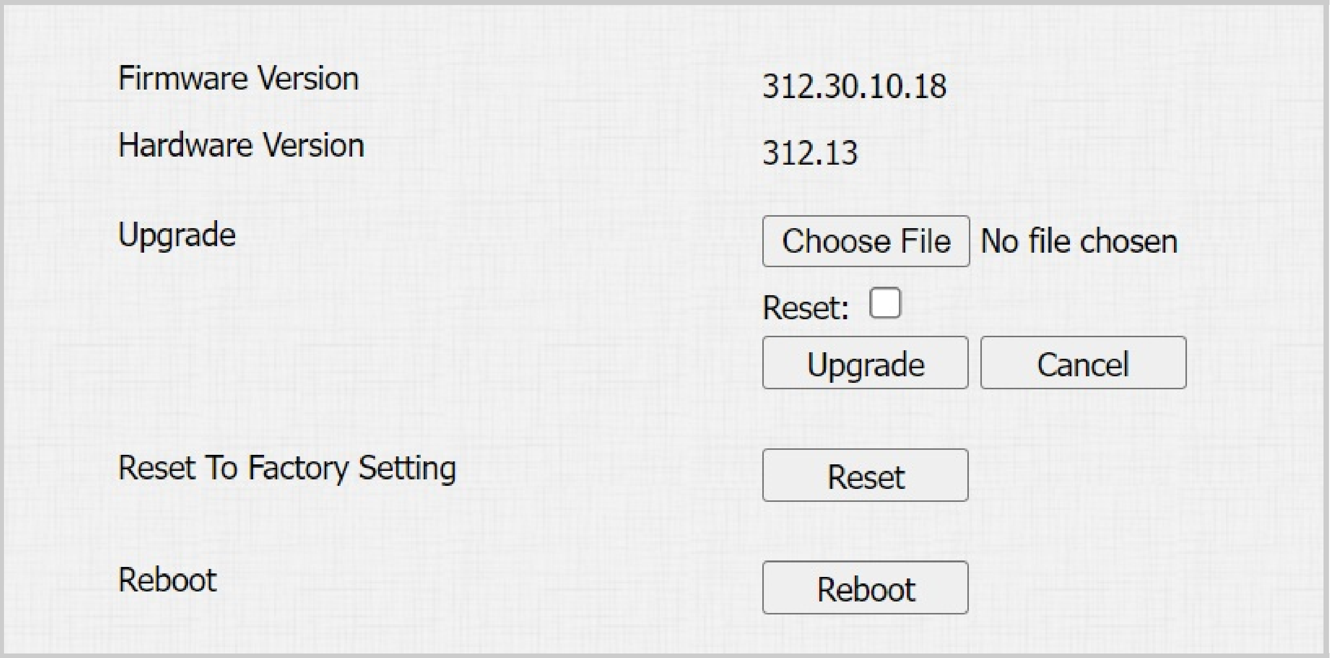


Reboot Schedule

Enabled	☑
Schedule	Every Day 0 (0~23Hour)

Reset

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



Firmware Version	312.30.10.18
Hardware Version	312.13
Upgrade	Choose File No file chosen Reset: □ Upgrade Cancel
Reset To Factory Setting	Reset
Reboot	Reboot