# Table of contents

**Akuvox E12 Series Door Phone Administrator Guide**


About This Manual ..... 5
Product Overview ..... 7
Changelog ..... 8
Model Specification and Differences ..... 9
  Supported Card Types ..... 10
Access the Device ..... 11
  Obtain Device IP Address ..... 11
  Access the Device Settings ..... 11
Introduction to Configuration Menu ..... 13
  Introduction to Quick Start Module ..... 14
Language and Time ..... 16
  Language ..... 16
  Time ..... 16
Volume and Tone ..... 18
  Volumes ..... 18
  Open Door Tones ..... 18
  Upload Tone Files ..... 19
  Ringback Tone Setting ..... 20
  Open Door Tone Mode ..... 20
LED Setting ..... 22
  LED Light Setting ..... 22
  LED Light Status ..... 22
  Card Reader Area LED Control ..... 23
Network Setting ..... 24
  Network Status ..... 24
  Device Network Configuration ..... 24
  Device Deployment in Network ..... 25
  NAT Setting ..... 27
  Device Web HTTP Setting ..... 28
  Wi-Fi Connection ..... 28
Intercom Call Configuration ..... 31
  IP Call Configuration ..... 31
  SIP Call Configuration ..... 31
    SIP Account Registration ..... 31
    SIP Server Configuration ..... 33

Outbound Proxy Server ..... 33
Data Transmission Type ..... 34
SIP Hacking Protection ..... 34
Video Transport Type ..... 35
Call Settings ..... 36
Call Auto-answer ..... 36
Sequence Call ..... 36
Group Call ..... 37
Do Not Disturb ..... 38
Push To Hang Up ..... 39
Multicast ..... 39
Maximum Call Duration ..... 40
Maximum Dial Duration ..... 41
Hang Up After Open Door ..... 42
Chime Bell Setting ..... 42
Audio & Video Codec Configuration ..... 44
Audio Codec ..... 44
Video Codec ..... 45
Video Codec for IP Calls ..... 45
Contacts Configuration ..... 47
Relay Setting ..... 49
Local Relay ..... 49
Security Relay ..... 50
Web Relay ..... 51
Access Control Schedule Management ..... 54
Configure Door Access Schedule ..... 54
Create Door Access Schedule ..... 54
Import and Export Door Access Schedule ..... 55
Relay Schedule ..... 55
Holiday Schedule ..... 56
Holiday Schedule Import/Export ..... 58
Door-opening Configuration ..... 60
Unlock by RF Cards ..... 60
Access Settings ..... 61
RF Card Code Format ..... 63
Events Triggered by Using RF Cards ..... 63
Mifare Card Encryption ..... 63
NFC Card ..... 64
Unlock by DTMF Code ..... 65
DTMF White List ..... 66

Configure DTMF Data Transmission ..... 67
Unlock by HTTP Command ..... 69
Unlock by Exit Button ..... 70
Unlock by Bluetooth ..... 71
Monitor and Image ..... 73
MJPEG Image Capturing ..... 73
RTSP Stream Monitoring ..... 74
RTSP Basic Setting ..... 75
RTSP Stream Setting ..... 75
RTSP OSD Setting ..... 77
NACK ..... 77
ONVIF ..... 78
Live Stream ..... 79
SD Card for Storing Videos ..... 79
Camera Mode ..... 80
Security ..... 82
Tamper Alarm ..... 82
Client Certificate Setting ..... 82
Web Server Certificate ..... 82
Client Certificate ..... 83
Upload TLS Certificate for SIP Account Registration ..... 84
Motion Detection ..... 85
Security Notification ..... 86
Email Notification ..... 87
FTP Notification ..... 87
SIP Call Notification ..... 88
HTTP Notification ..... 88
Action URL ..... 89
Voice Encryption ..... 91
User Agent ..... 92
Emergency Action ..... 92
Web Interface Automatic Log-out ..... 92
High Security Mode ..... 93
Real-time Monitoring ..... 94
Logs ..... 95
Call Logs ..... 95
Door Logs ..... 96
Event Logs ..... 97
Integration with Third Party Device ..... 98
Integration via Wiegand ..... 98

Facility Code Setting ..... 99
Integration via HTTP API ..... 100
Lift Control ..... 102
Akuvox Lift Controller ..... 102
ZKT Lift Controller ..... 103
Firmware Upgrade ..... 105
Auto-provisioning via Configuration File ..... 106
Provisioning Principle ..... 106
Configuration Files for Auto-provisioning ..... 107
AutoP Schedule ..... 108
Static Provisioning ..... 109
DHCP Provisioning ..... 110
PNP Configuration ..... 112
Debug ..... 114
System Log ..... 114
Remote Debug Server ..... 114
PCAP ..... 115
Web Call ..... 116
Ping ..... 116
Backup ..... 117
Password Modification ..... 118
Modify Web Password ..... 118
Modify Security Questions ..... 119
System Reboot&Reset ..... 121
Reboot ..... 121
Reset ..... 121

# 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 administrators who need to properly configure the door phone. This manual applies to firmware version 312.30.11.30, 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.

# Changelog

What's new in version 312.30.11.30:

- Support the 2-Wire LP Intercom Solution.

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

# 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<br>12V DC Connector(If not using PoE) | 802.3af Power-over-Ethernet<br>12V DC Connector(If not using PoE) |

# Supported Card Types

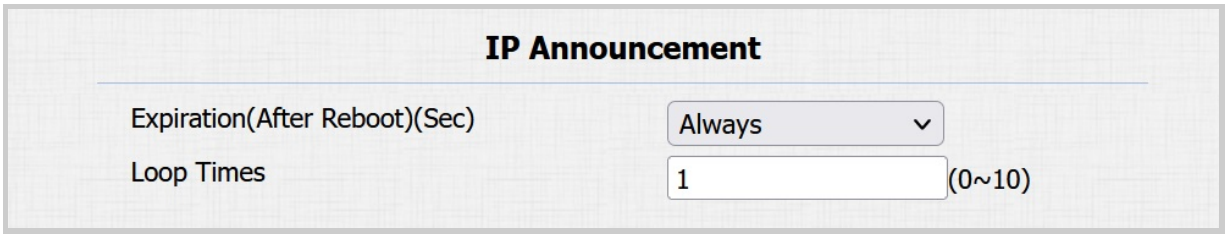
The device's firmware should be 312.30.10.208 or higher:

- IC Card:
    - Mifare Ultralight C/EV1
    - Mifare Classic Compatible Card
    - Mifare Plus-S 2K
    - NFC Type2 216
    - NFC Type2 215
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
    - Mifare Classic 1K
    - Mifare S50-1K Card
    - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

# Access the Device

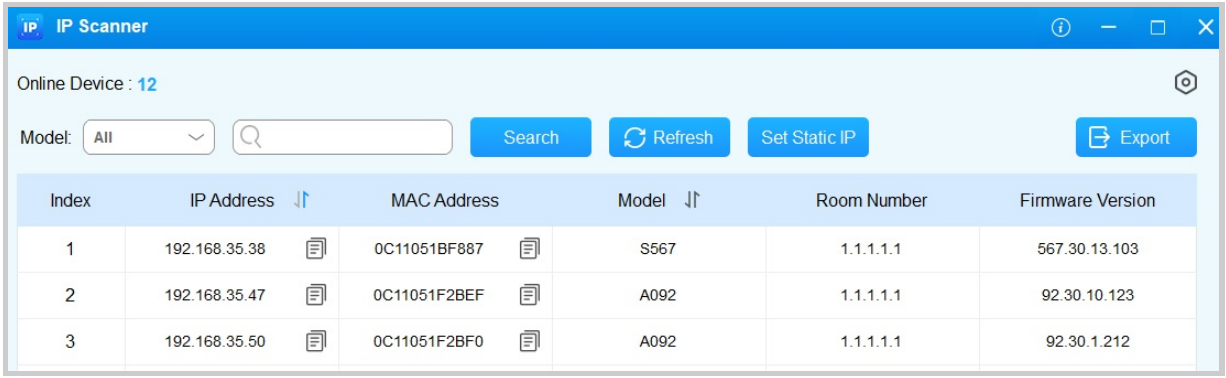
## Obtain Device IP Address

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




- **Expiration(After Reboot)(Sec):** Set the time within which users should hold the call button to make the device pronounce the IP address after the device reboots.
  If you select **Always**, users can hold the call button at any time for IP announcement after the reboot.
- **Loop Times:** Set the IP announcement loop times.

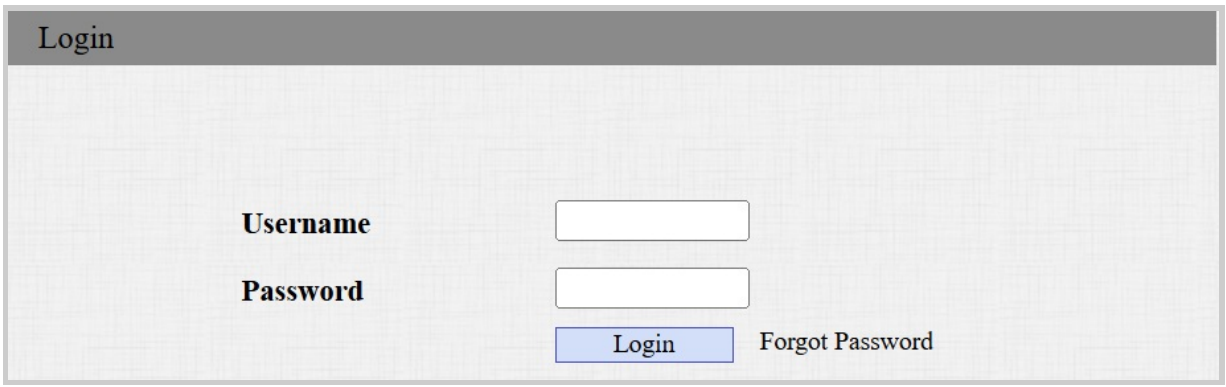
Or, search the device IP with the IP scanner on the same LAN network. Click **Refresh** to update the list.




## Access the Device Settings

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

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




**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.
- Your computer should be on the same network as the device.

# Introduction to Configuration Menu

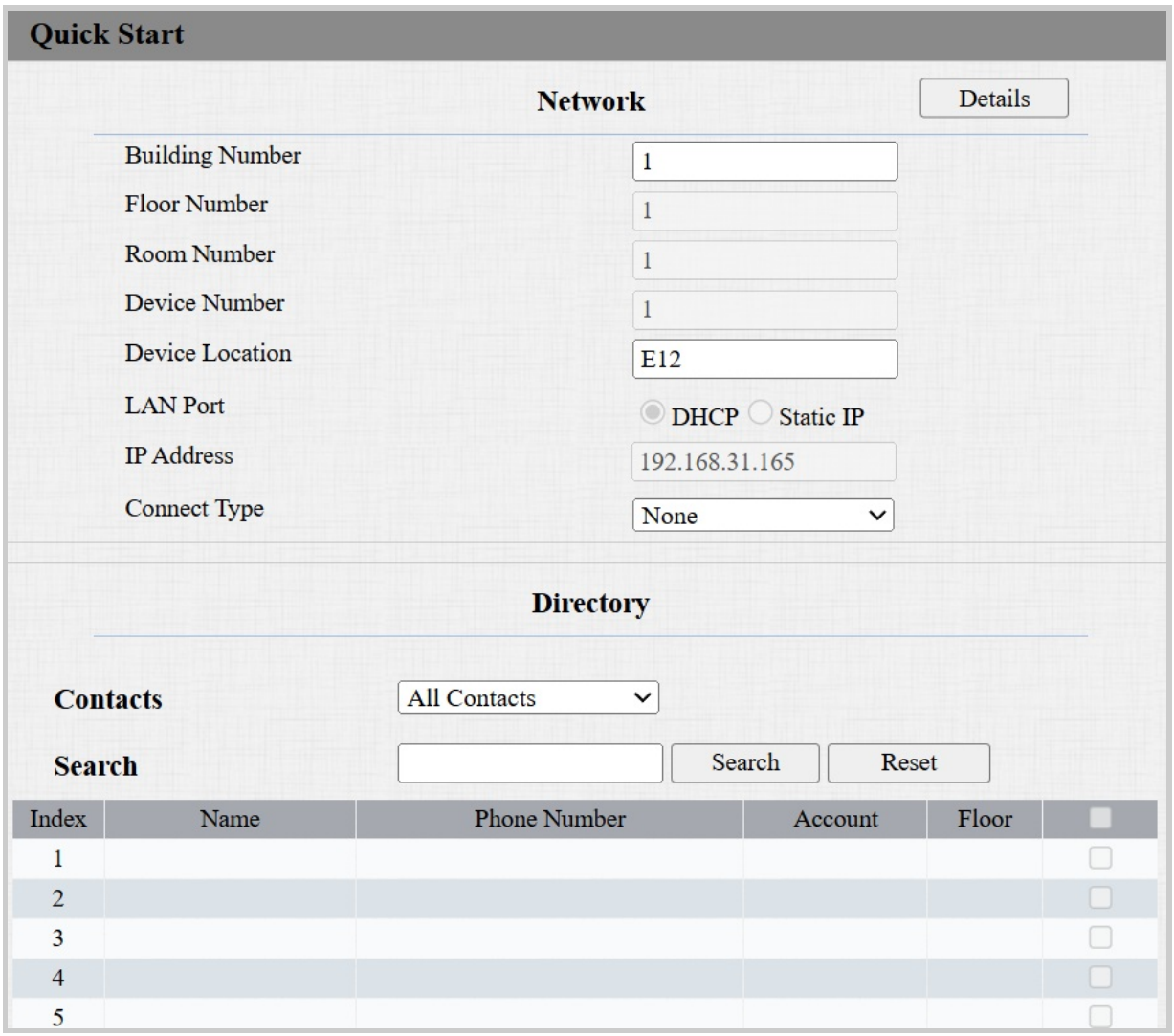
- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, etc.
- **Network:** This section mainly 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.
- **Directory**: This section is for user management.
- **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.
- **System:** This section covers device security settings, password modification, device reboot and reset, etc.




# Introduction to Quick Start Module

The Quick Start module allows you to configure the device's core features on a single interface, instead of switching between different interfaces.

You can redirect to the feature detail interface by clicking **Details** in the upper right corner.




- **Network**: Display the location information of the device.
  - **Device Location**: Enter the device's location to distinguish it from others. By default, it is [*the device name_the last 4 characters of its MAC address*].
  - **Connect Type**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None.
- **Directory**: Display all local contacts.
- **Open Relay Via HTTP**:
  - **Username**: Set a username for authentication in HTTP command URLs.
  - **Password**: Set a password for authentication in HTTP command URLs.

# Language and Time

## Language

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, Simplified Chinese, Traditional Chinese, Russian, Portuguese, Spanish, Italian, Dutch, French, German, Turkish, and Korean.

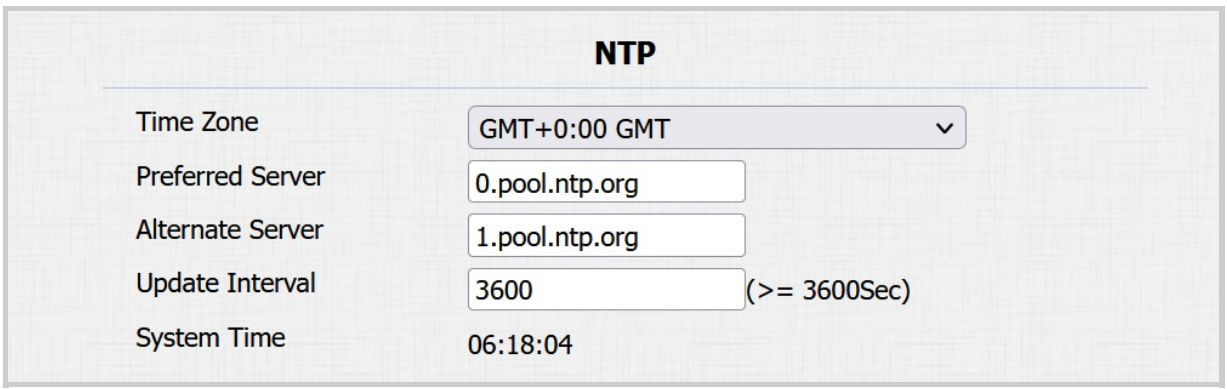



- **Mode:** English is the default web language.

## Time

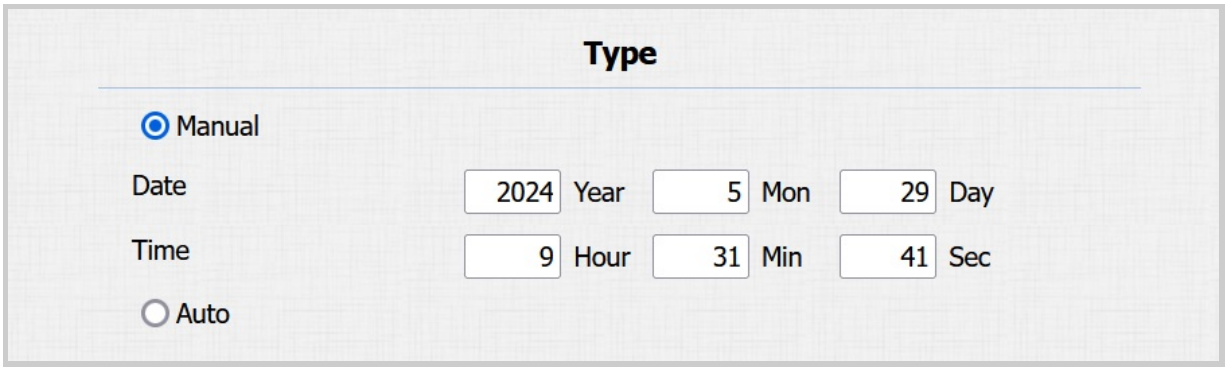
The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on your device.

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



- **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 NTP server address when the primary one fails.
- **Update Interval**: Set the time update interval. For example, if you set it as 3600 seconds, the device will send a request to the NTP 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.

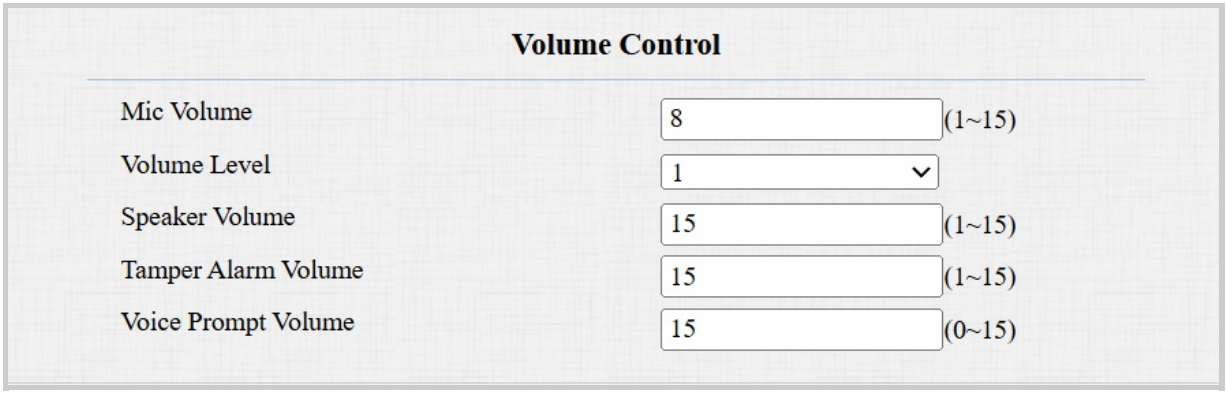


# Volume and Tone

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

## Volumes

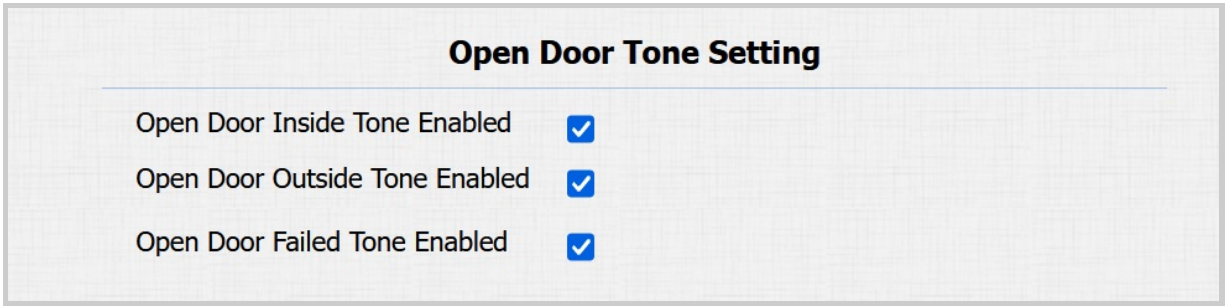
To set up volumes, go to the web **Device > Audio** interface.




- **Volume Level**: Set the overall volume. The Level 1 volume range is roughly 80-95, and Level 2 is 95-109.
- **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.

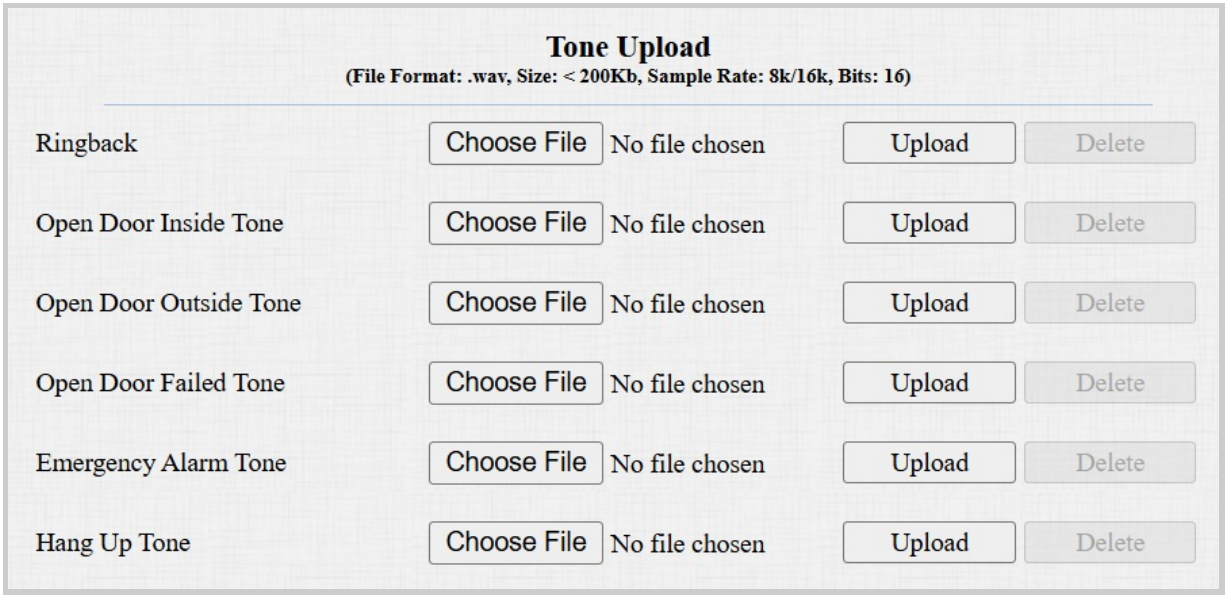


- **Open Door Inside Tone Enabled:** The tone sounds when users open the door by pressing the Exit Button.
- **Open Door Outside Tone Enabled:** The tone sounds when users open doors via various device-supported access methods.
- **Open Door Failed Tone Enabled**: The tone sounds when opening the door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

## Upload Tone Files

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

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




- **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.
- **Hang-Up Tone**: The tone sounds when a call is hung up.

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

## Ringback Tone Setting

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

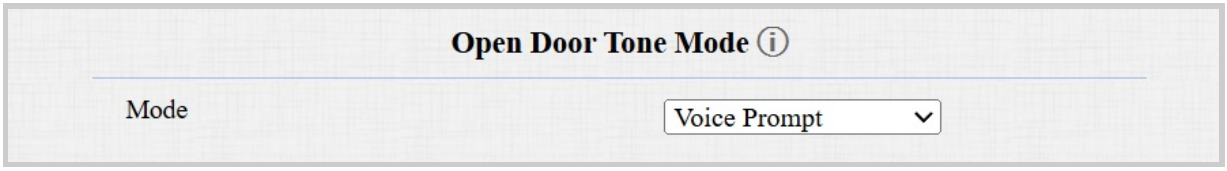
Set it up on the **Device > Audio > Ringback Tone Setting** interface.




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

## Open Door Tone Mode

You can decide the door-opening tone mode on the **Device > Audio** interface.



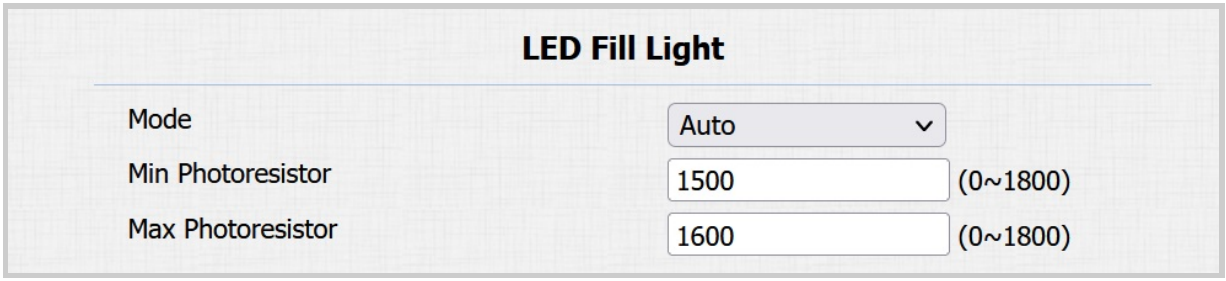

- **Voice Prompt**: Play the default prompt “Welcome, please come in” when the door is opened.
- **Sound Effect**: Play the Beep sound when the door is opened.

# 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 > Light > LED Fill Light** interface.

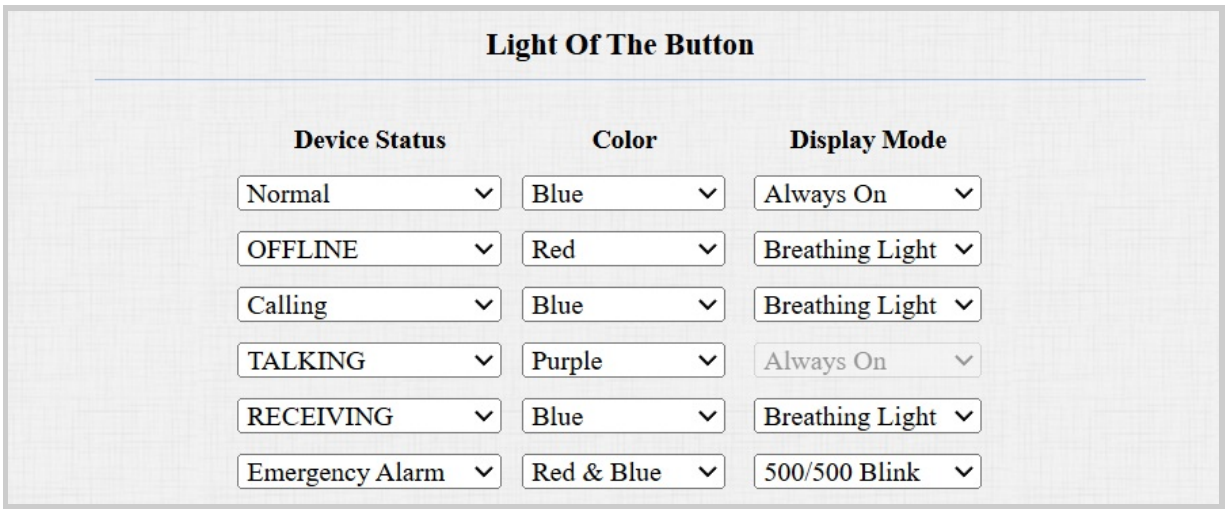



- **Mode:**
  - **Auto**: Turn on the LED light automatically based on the minimum and maximum photoresistor value.
  - **Always OFF:** Turn off the LED light.
  - **Specific Time:** Turn on the LED according to the schedule.
- **Min/Max Photoresistor:** Set the minimum and maximum photoresistor value to automatically control the ON-OFF of the LED light. If the photoresistor value is less than the minimum threshold, turn off the LED. If the photoresistor value is greater than the maximum threshold, turn on the LED.

## LED 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 > Light > Light of The Button** interface.

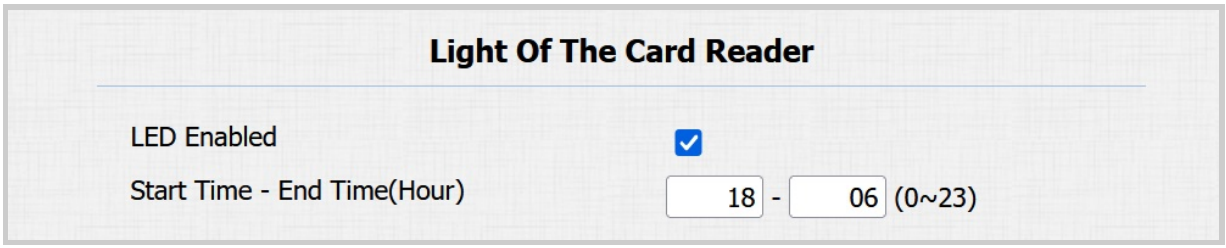



- **Device Status:** There are six statuses: Normal, Offline, Calling, Talking, Receiving, and Emergency Alarm. The status cannot be changed.
- **Color:** Select from Blue, Red, and Purple. You can select Red & Blue(flashing red and blue alternately) for Emergency Alarm status.
- **Display Mode:** Set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

## Card Reader Area LED Control

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

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

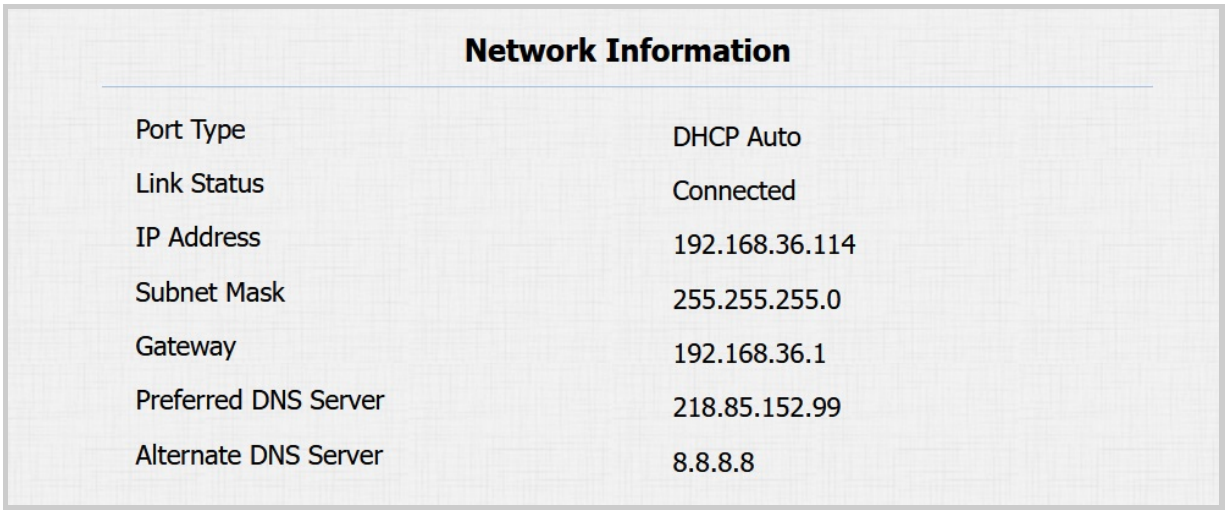



- **Start Time - End Time(Hour):** Set the LED light valid time. If the time is set from 8-0(Start time - End time), the LED light will stay on from 8:00 a.m. to 12:00 p.m. for one day(24 hours).

# Network Setting

## Network Status

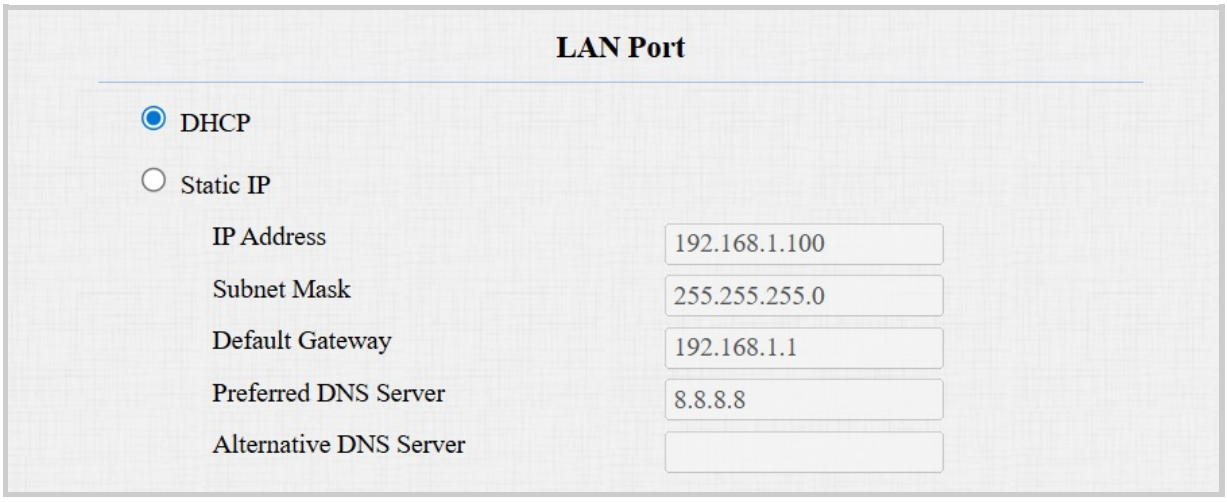
Check the network status on the web **Status > Info > Network Information** interface.




## Device Network Configuration

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

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

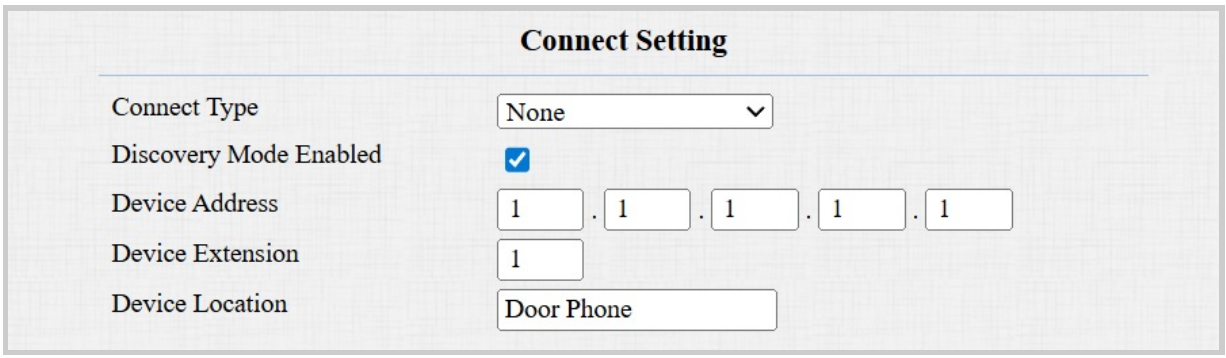


- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: When static IP mode is selected, the IP address, subnet mask, 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. To access the device's web settings, your computer should be on the same local network as the device.
- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.
- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **Preferred/Alternative DNS Server**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The door phone connects to the alternate DNS server when the primary one is unavailable.

## Device Deployment in Network

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

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




- **Connect Type**: It is automatically set up according to the device connection with a specific server in the network, such as SDMC, Cloud, or None.
  - **None**: None is the default factory setting, indicating the device is not in any server type. Devices connect directly to each other or within a local area network (LAN) without relying on external servers.
  - **Cloud**: The device is connected to the SmartPlus Cloud, a cloud-based system simplifying property access management. The Cloud mode allows devices to interact intelligently with one another and the mobile SmartPlus App, backing up data daily and on different hosts. It suits projects requiring smart, flexible, and secure deployment and management.
  - **SDMC**: The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.

- **Discovery Mode Enabled**: Enabled by default. Available for None server mode. 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**: Available for None server mode. It can be used to call the device. Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for None server mode. The device extension number ranges from 0 to 10.

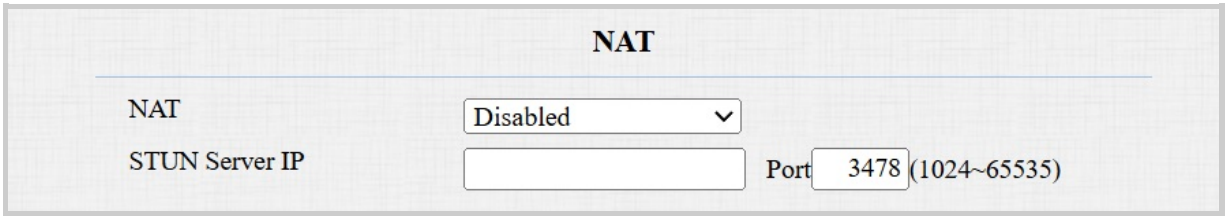
- **Device Location**: The location where the device is installed and used.

## 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.

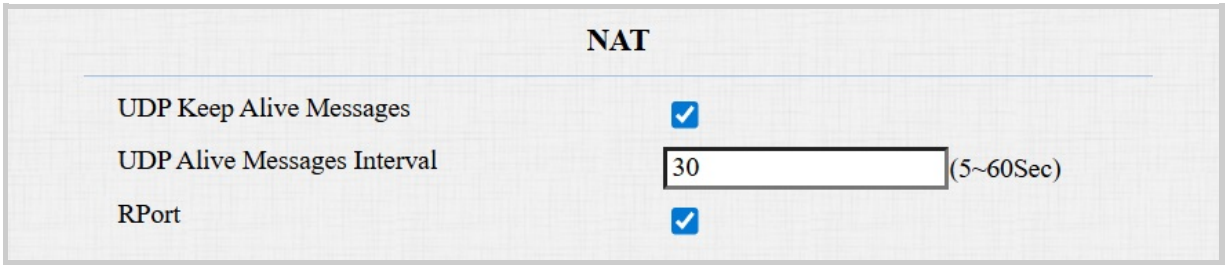
To register SIP accounts on third-party servers in a Wide Area Network(WAN), you need to enable the RPort feature on the intercom devices to establish a stable connection.

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




- **STUN Server IP**: 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.

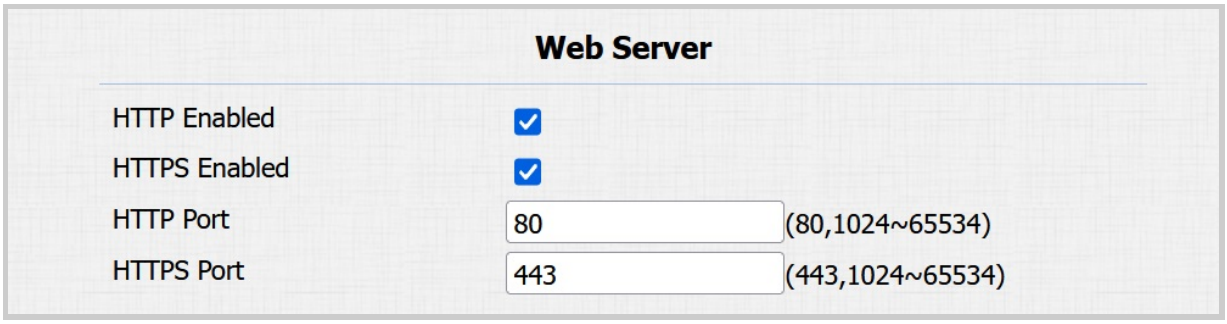



- **UDP Keep Alive Messages:** If enabled, the device will send the message to the SIP server, which will recognize whether the device is online.
- **UDP Alive Messages Interval:** Set the message-sending interval from 5-60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when the SIP server is in a WAN.

# Device Web HTTP Setting

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

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

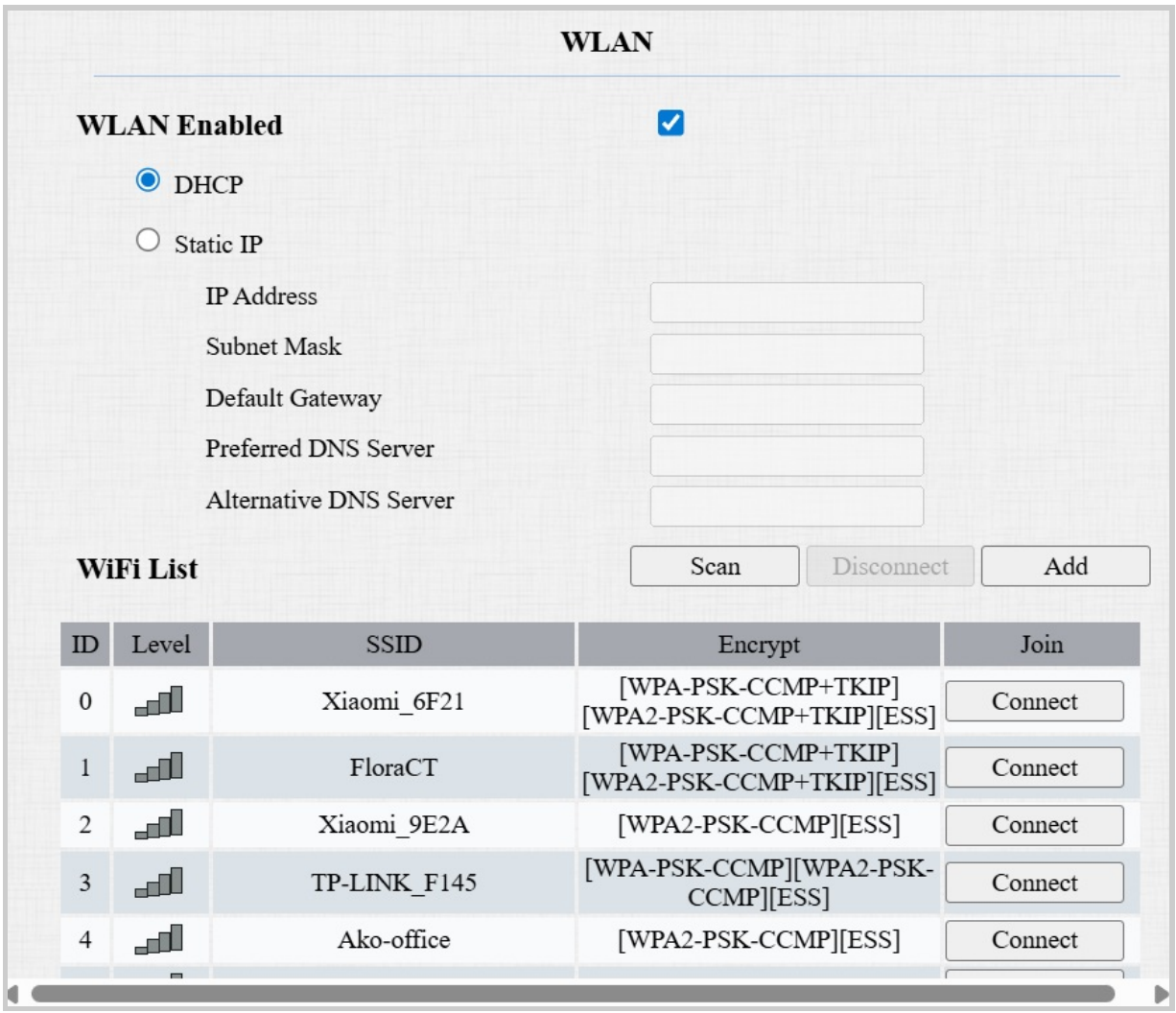



- **HTTP/HTTPS Enabled**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

# Wi-Fi Connection

E12W supports connecting to the network via Wi-Fi. Set it up on the **Network > Basic** interface.

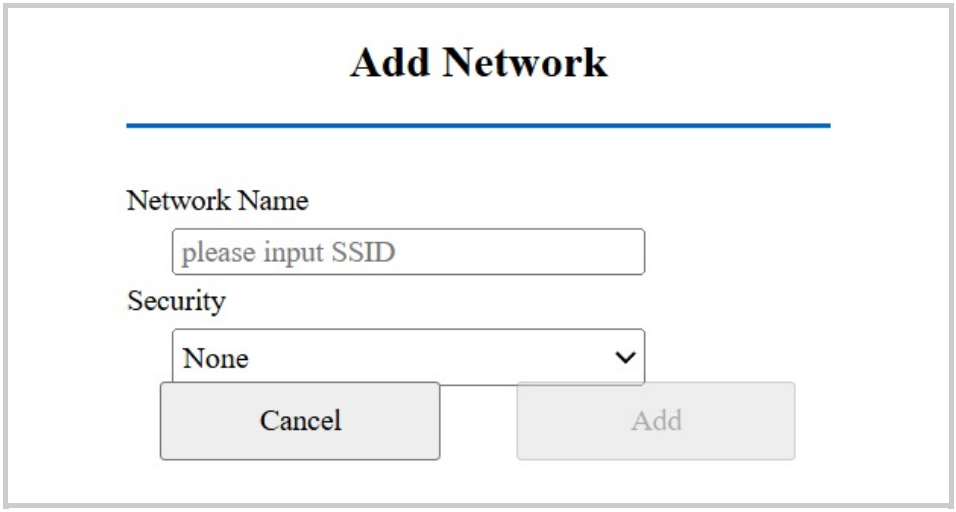
Connect to the desired Wi-Fi by clicking **Connect** and entering the password.




- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server with an 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/Alternative 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.

- **Add**: Click to add Wi-Fi manually.
  - **Network Name**: Enter the name of the Wi-Fi network.
  - **Security**: Select the network encryption type and enter the password to connect. The default is None.

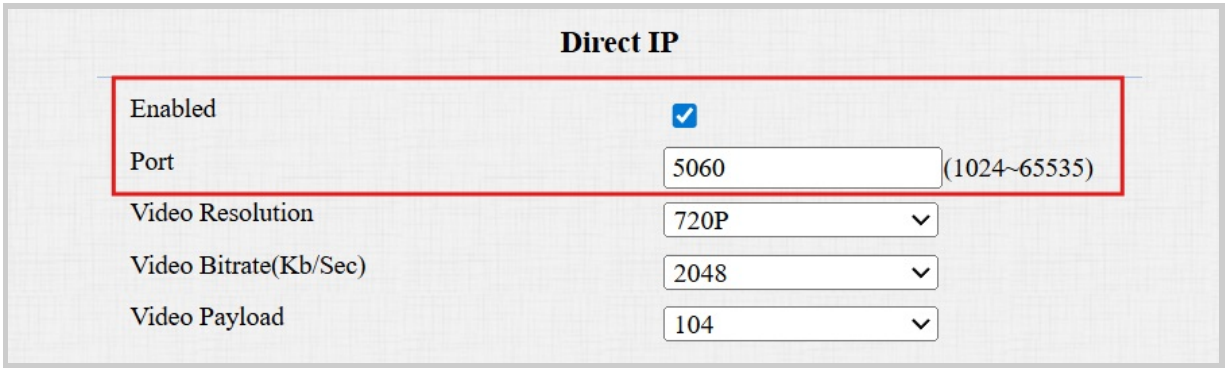


# Intercom Call Configuration

## 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 > Call Feature > Direct IP** interface.




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

## SIP Call Configuration

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

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

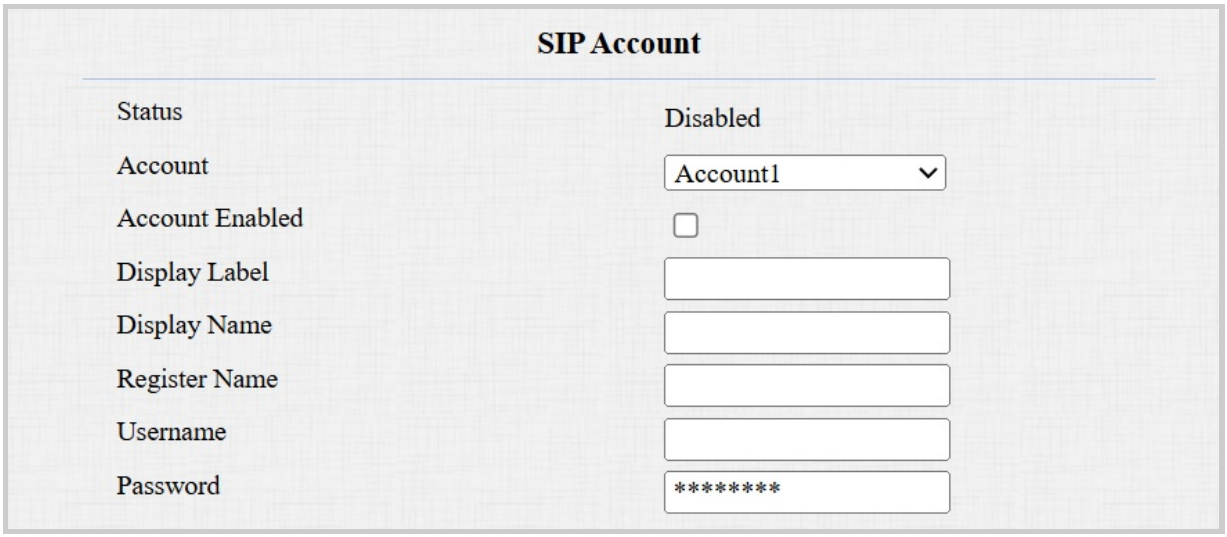
### SIP Account Registration

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

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

Click here to view the SIP account registration example.

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




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

- **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.

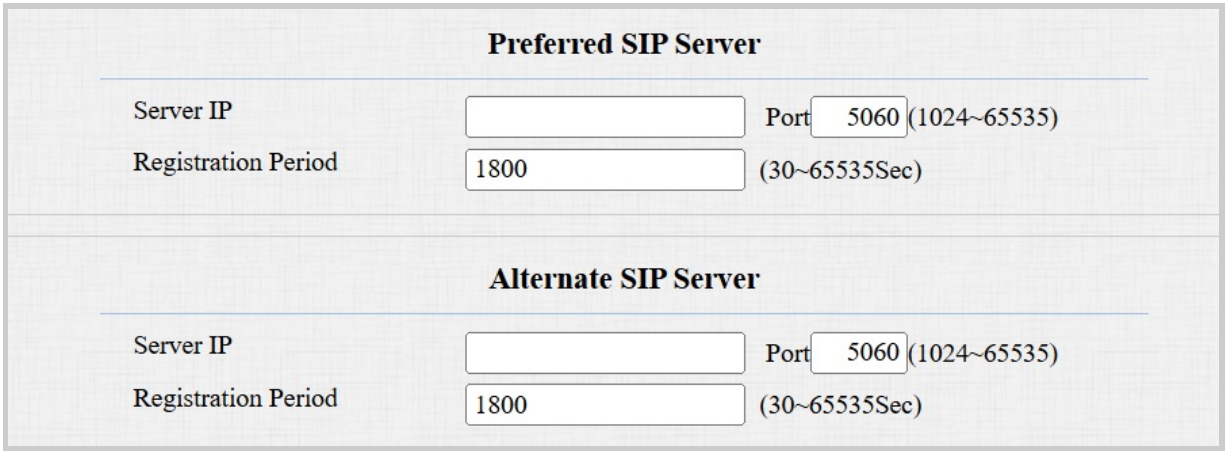
**Tip**

When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

## SIP Server Configuration

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

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

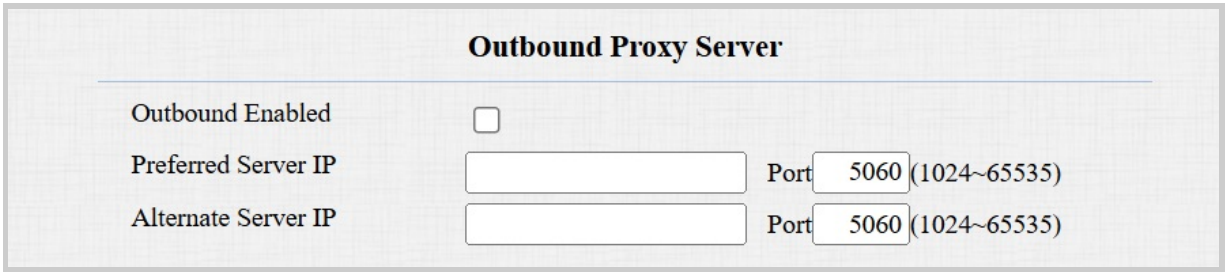



- **Server IP**: Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified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

# Outbound Proxy Server

An outbound proxy server 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.



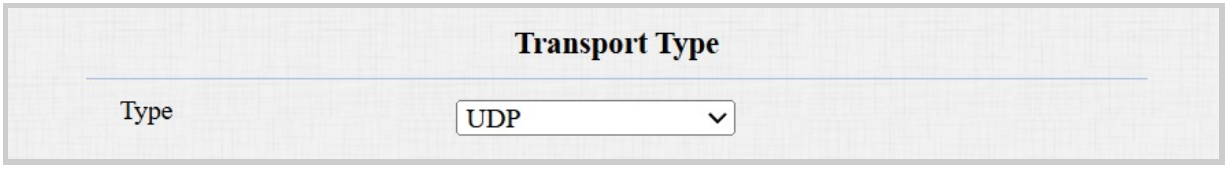

- **Preferred Server IP:** Enter the SIP proxy server's IP address.

- **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.

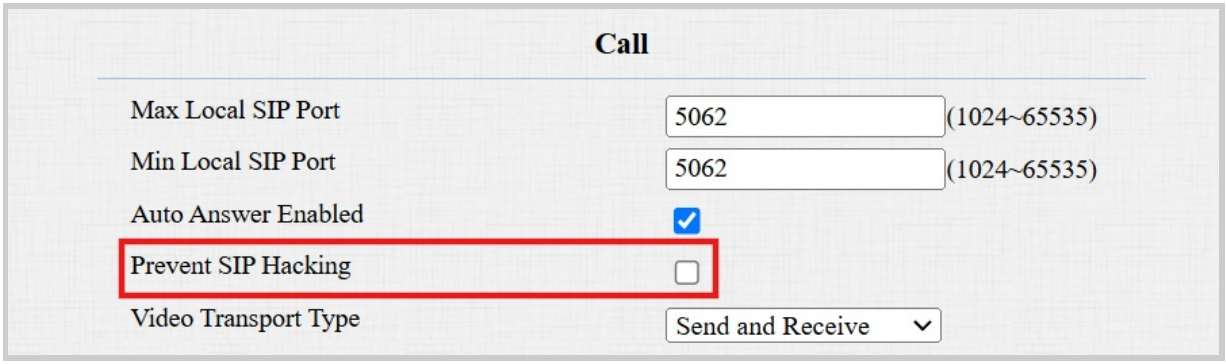



- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced 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

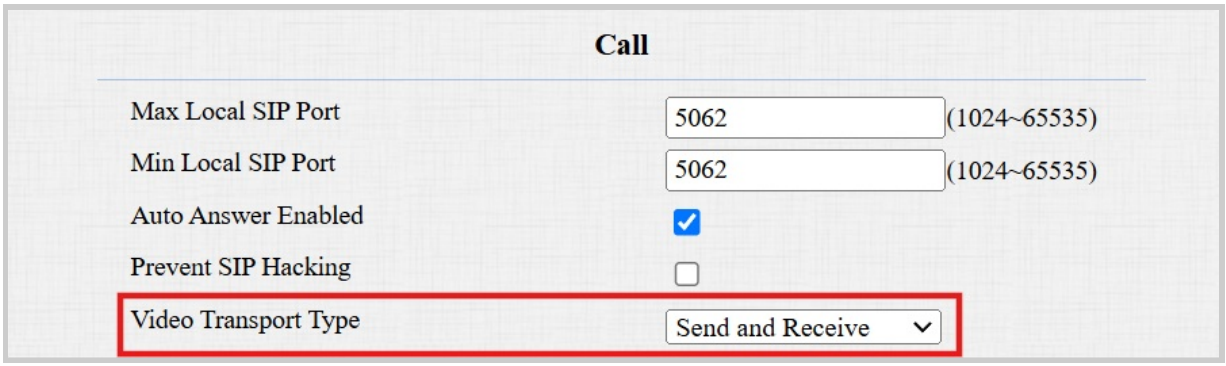
Internet phone eavesdropping is a network attack that allows unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls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

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




# Video Transport Type

You can set the video transport type for SIP calls on the **Account > Advanced > Call** interface.



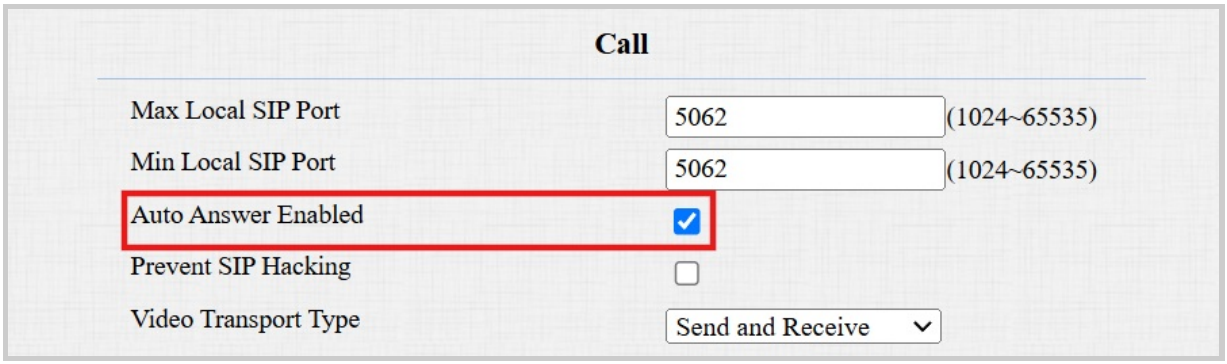

- **Video Transport Type**: It is Send and Receive by default.
  - **Inactive**: Disable the function.
  - **Send Only**: The device sends the video stream to the other party.
  - **Receive Only**: The device only receives the video stream from the other party.
  - **Send and Receive**: The device can send and receive video streams to and from the other party.

# Call Settings

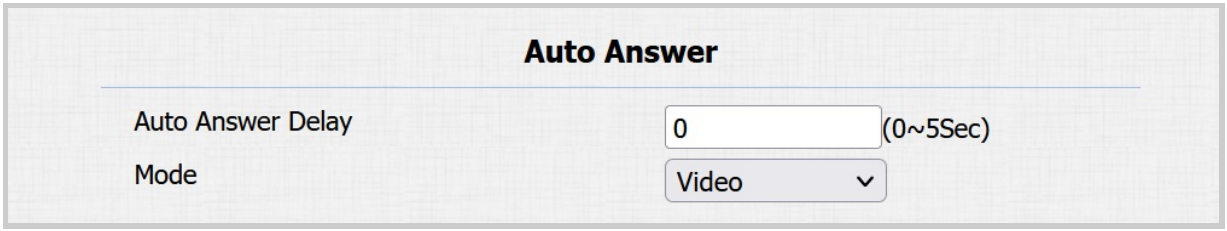
## Call Auto-answer

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

To enable the Auto Answer feature, go to **Account > Advanced > Call** interface.




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

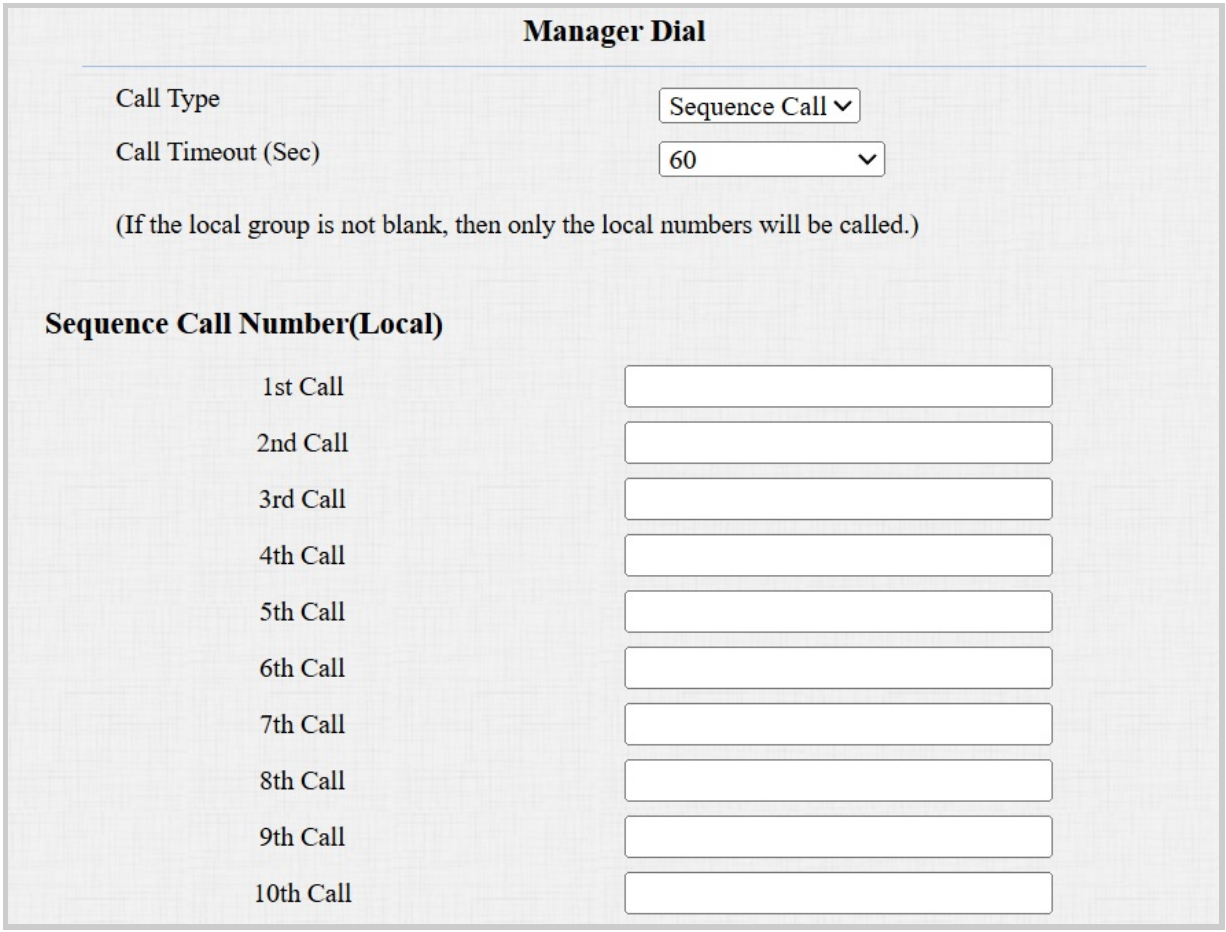



- **Auto Answer Delay:** Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode:** Determine whether to auto-answer the call as a video or audio call.

## Sequence Call

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

You can also configure the local sequence call number. Go to **Intercom > Basic > Manager Dial** interface.



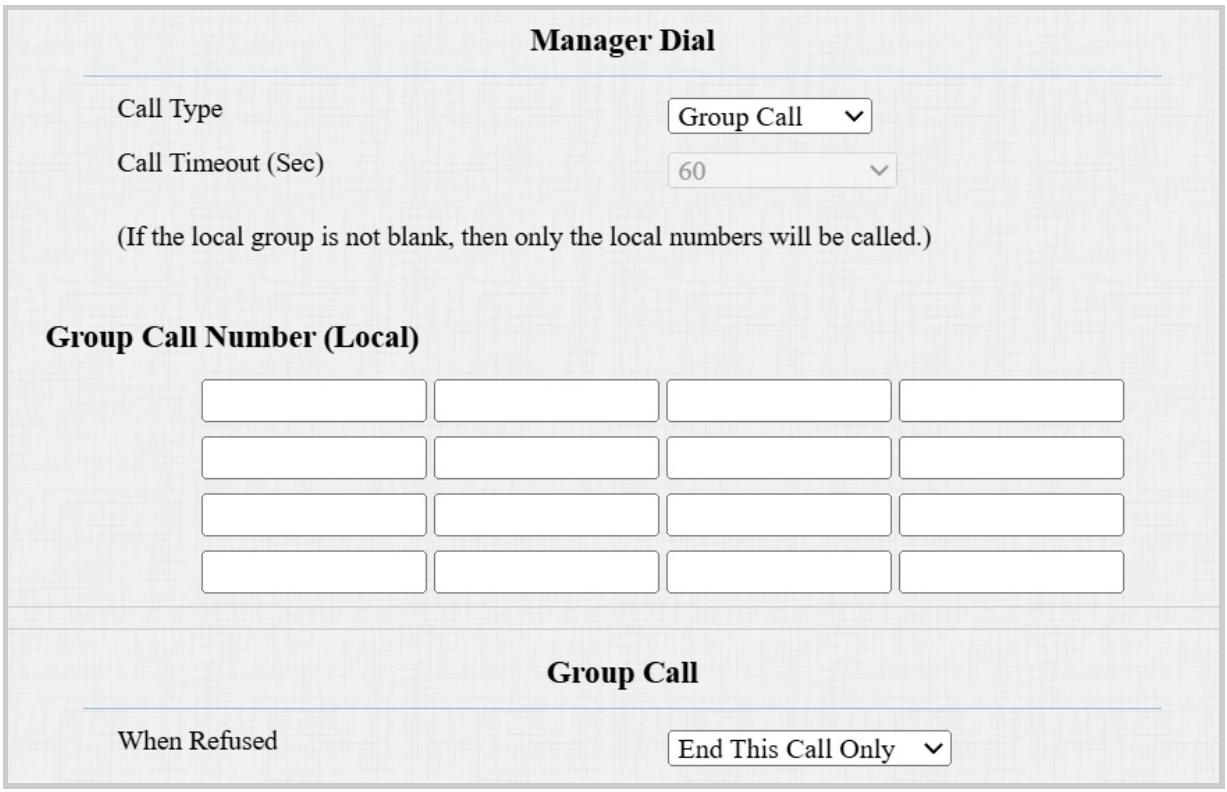

- **Call Type**: Select Sequence Call.
- **Call Timeout(Sec)**: Determine the duration before calling the next number when the previous call is not answered.
- **Sequence Call Number(Local)**: Enter the target IP/SIP numbers.

> **Note**
>
> When the device is connected to SmartPlus Cloud, the local Sequence Call option will be unavailable.

# Group Call

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

To set up local group call numbers, go to **Intercom > Basic > Manager Dial** interface.

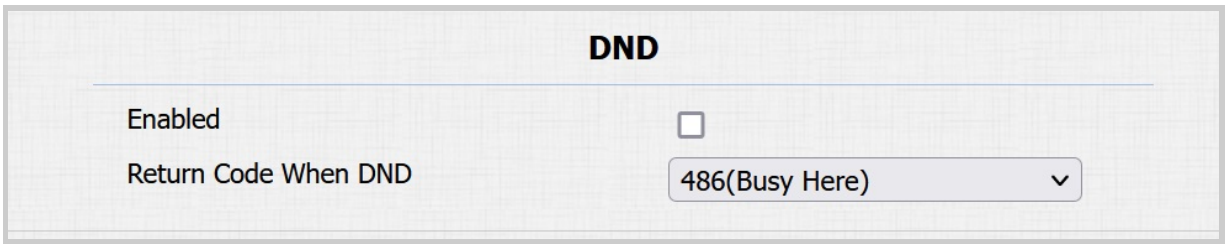



- **Call Type**: Select Group Call.
- **Group Call Number(Local)**: Enter the target IP/SIP numbers.
- **When Refused:**
  - **End This Call Only**: The device will continue to call the next number.
  - **End All Calls**: The device will stop calling.

# Do Not Disturb

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

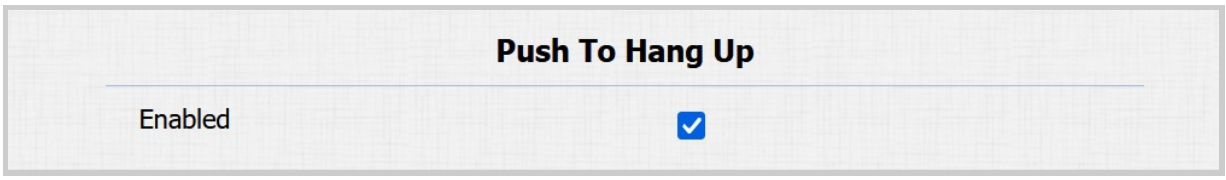
Set it up on the **Intercom > Call Feature** interface.




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

## Push To Hang Up

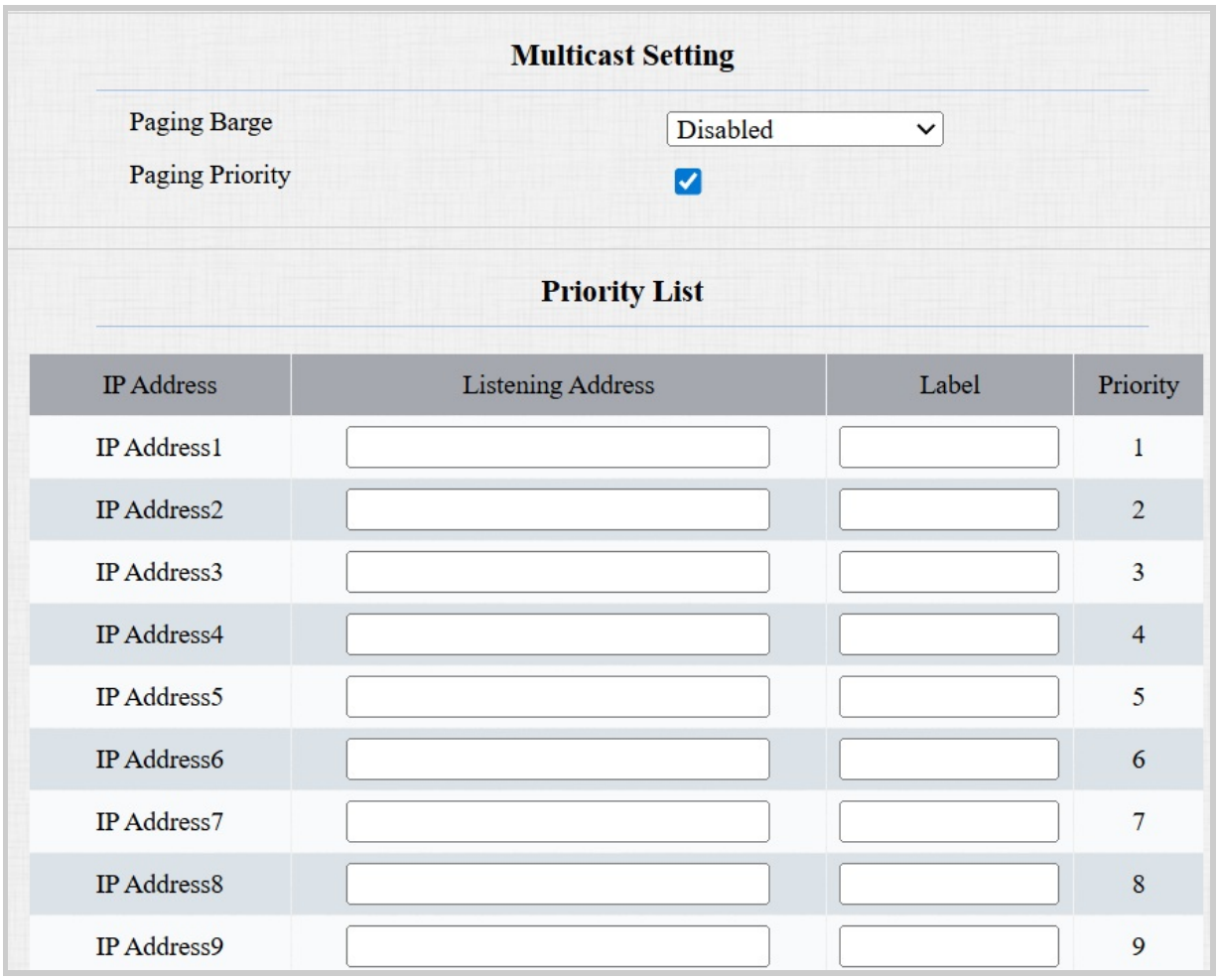
Users can hang up the call on the door phone by pressing the push button. To enable the feature, navigate to **Intercom > Basic** > **Push To Hang Up** interface.




## Multicast

Multicast is a one-to-many communication within a range. The door phone can act as a listener and receive audio from the broadcasting source.

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




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

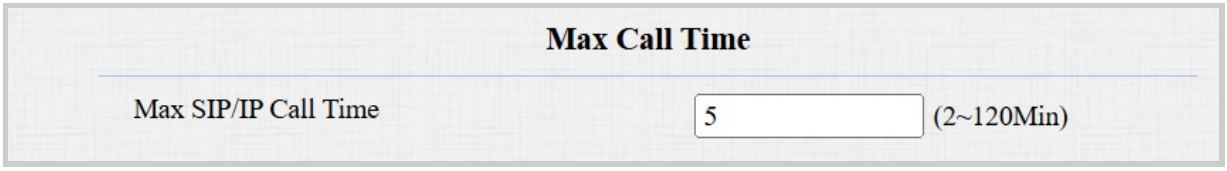
> **Note**
>
> Please contact Akuvox tech team for valid multicast address.

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

# Maximum Call Duration

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

To set up call time duration, navigate to the web **Intercom > Call Feature > Max Call Time** interface.




- **Max SIP/IP Call Time:** Specify the maximum duration of all calls. The door phone will end the call automatically when the time limit is reached.

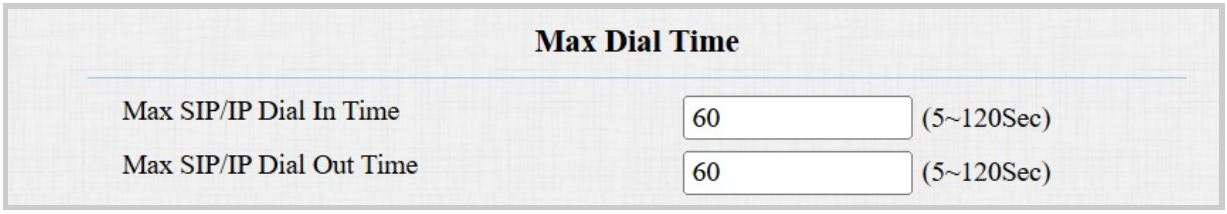
**Note**

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

## Maximum Dial Duration

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

To set it up, navigate to **Intercom > Call Feature > Max Dial Time** interface.




- **Dial SIP/IP Dial In Time:** Specify the maximum duration of an incoming call. The door phone will automatically end the incoming call if it is not answered within the preset time.

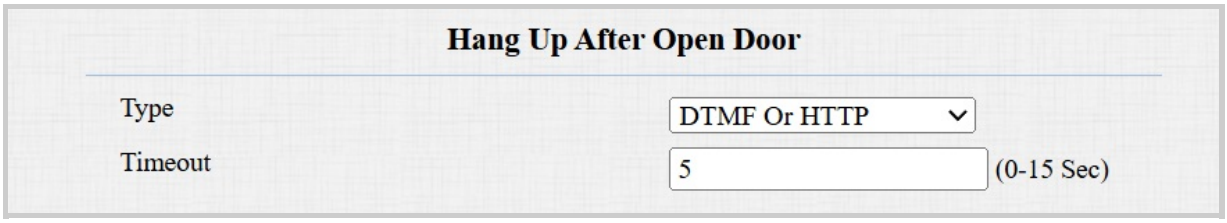
- **Dial SIP/IP Dial Out Time:** Specify the maximum duration of an outgoing call. The door phone will automatically end the call it dialed out if there is no answer from the recipient within the preset time.

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

## Hang Up After Open Door

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

Set it up on the **Intercom > Call Feature** interface.




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

## Chime Bell Setting

The device can be connected to a chime bell via its relay ports. The chimebell sounds by pressing the push button and triggering the relay during a call.

To set it up, go to **Access Control > Relay > Output To Chime Bell** interface.




- **Execute Relay**: Select None to disable the function; select Relay to turn it on.

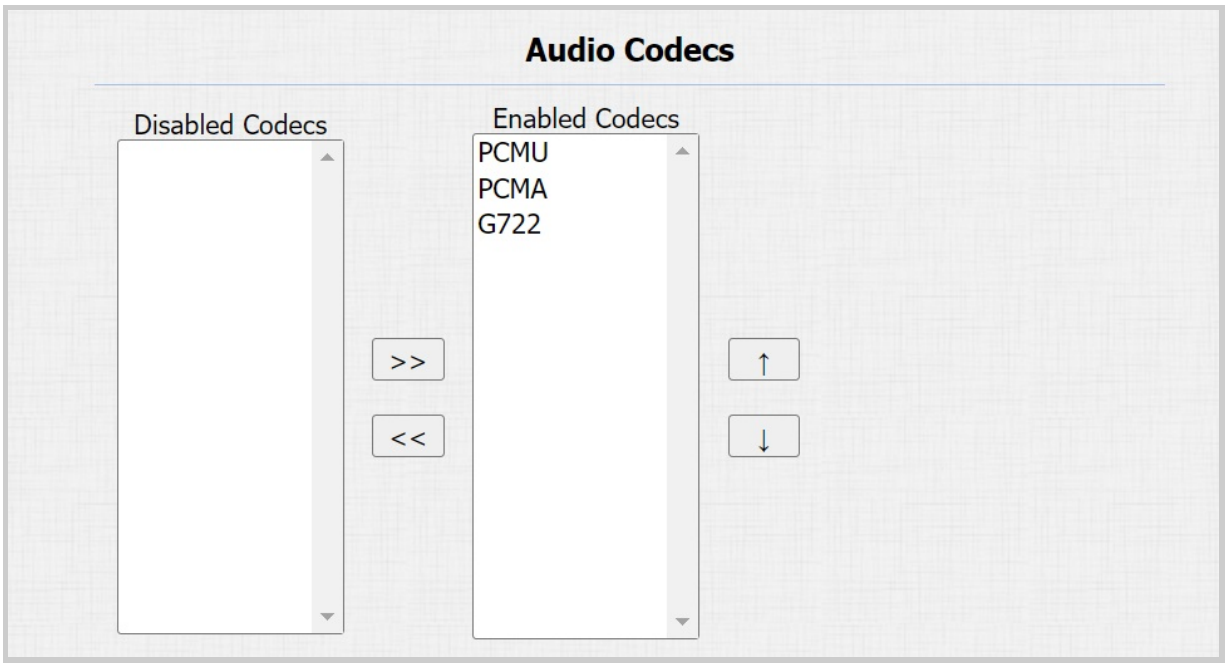
# Audio & Video Codec Configuration

## 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. PCMU and PCMA are well-suited for traditional telephony and bandwidth-constrained environments, while G722 delivers better audio quality for more modern communication needs.

You can select the specific codec according to the actual network environment.

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



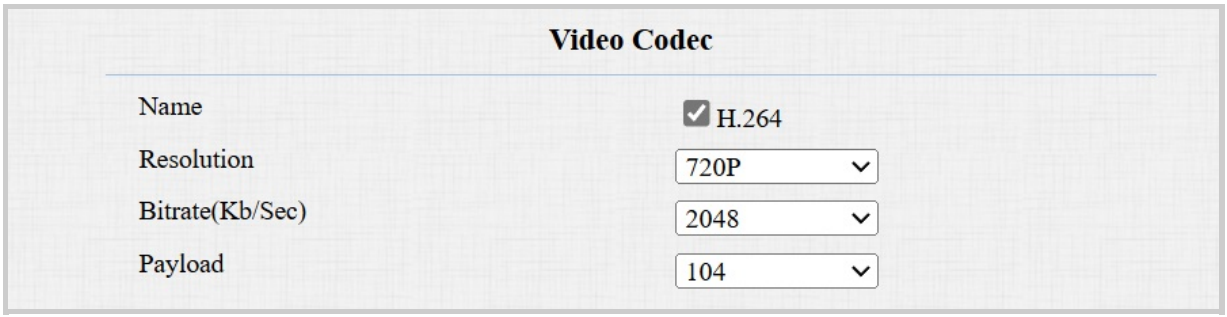

Please refer to the bandwidth consumption and sample rate for the three codec types below:

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

## Video Codec

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

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

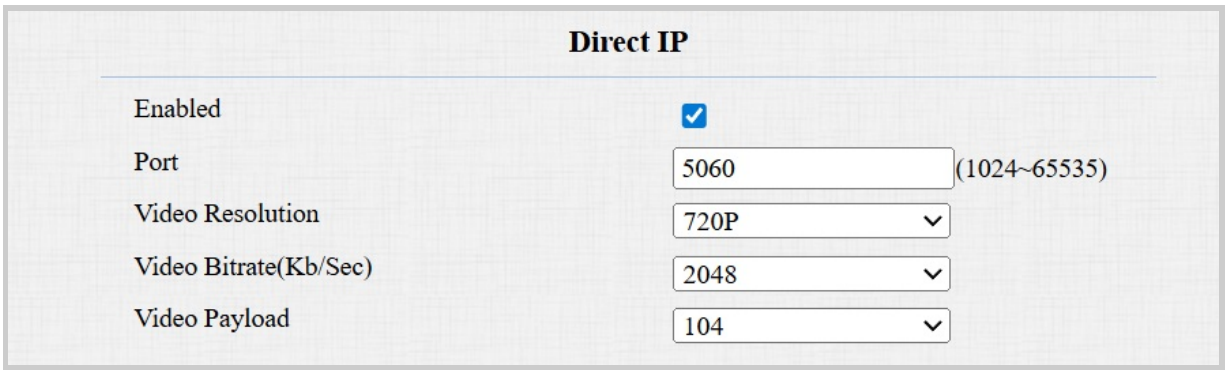



- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default code resolution is 720P(1280×720 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, 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 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 > Call Feature > Direct IP** interface.



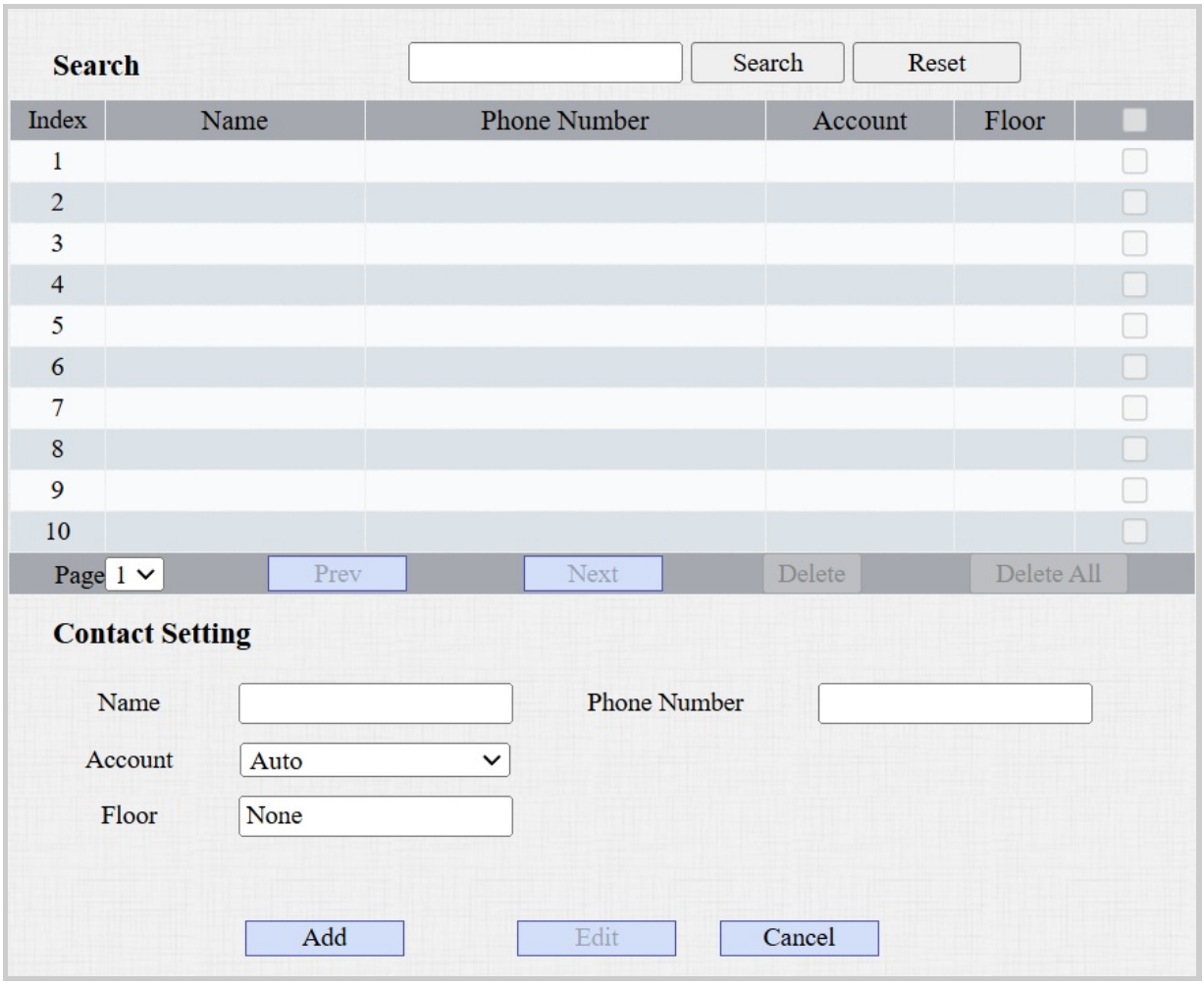

- **Video Resolution**: Select the resolution from the provided options. The default is 720P(1280×720 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The default bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

# Contacts Configuration

The local contact information is used to initiate SIP or IP calls to users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls. The door phone can store up to 1,000 contacts.

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

Set it up on the **Directory > Directory Setting** interface.




- **Name:** Name the contact.
- **Phone Number:** The phone number of the contact. It supports IP addresses and SIP numbers.
- **Account:** Select the account to receive the call from the contact.

- **Floor:** Specify the accessible floor(s) to the contact via the elevator.

# Relay Setting

## Local Relay

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

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




- **Relay 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.

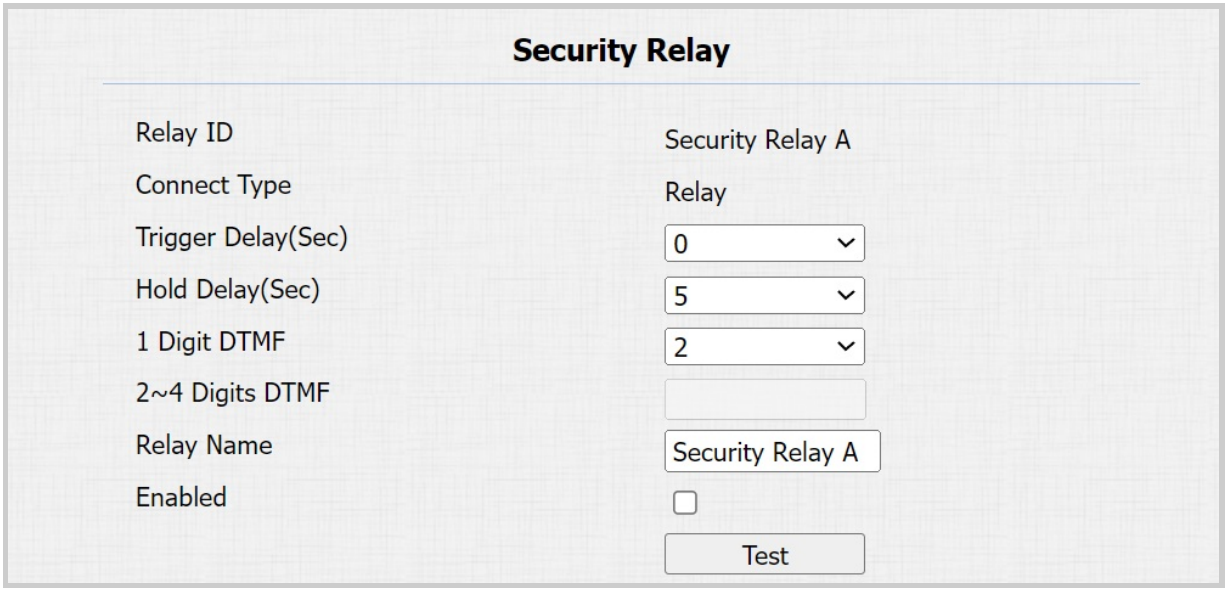
## Security Relay

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




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

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




- **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.

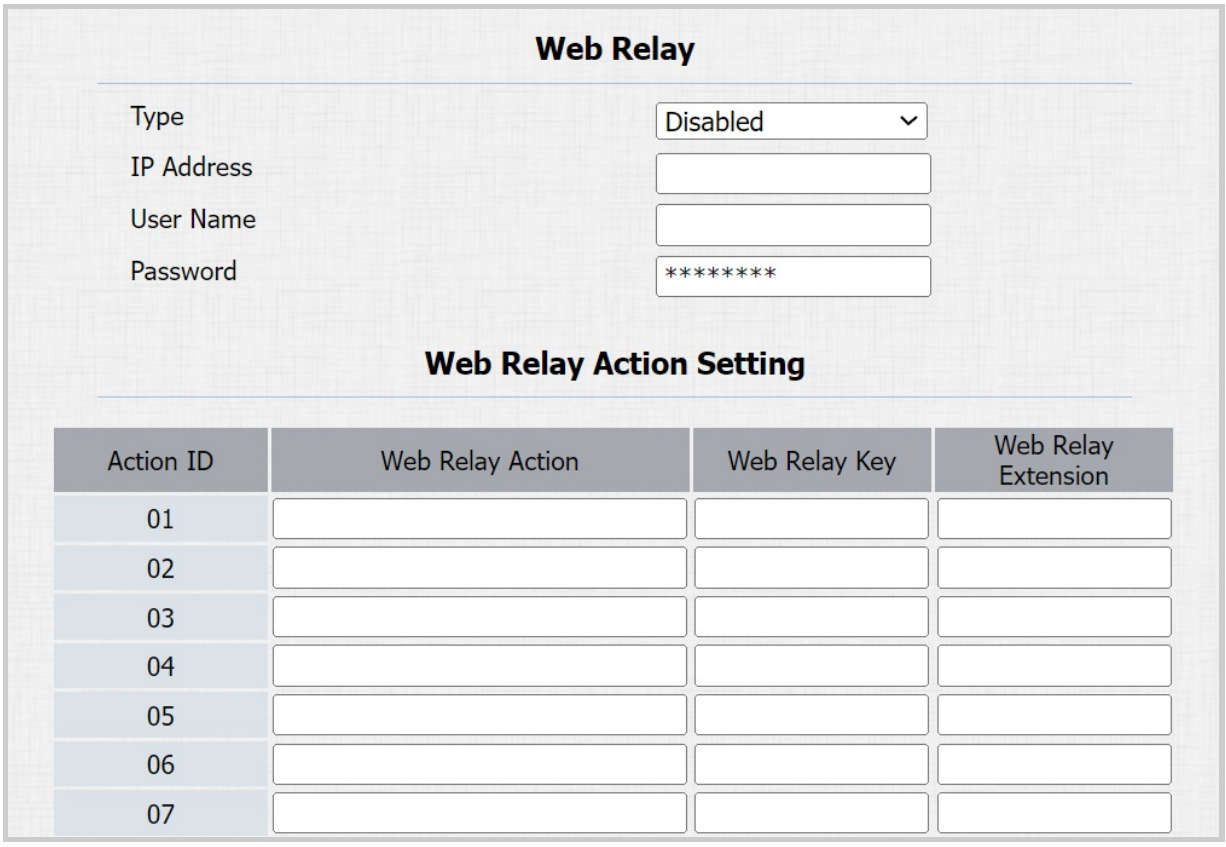
# Web Relay

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




Click here to view how to set up web relay.

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




- **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.

# Access Control Schedule Management

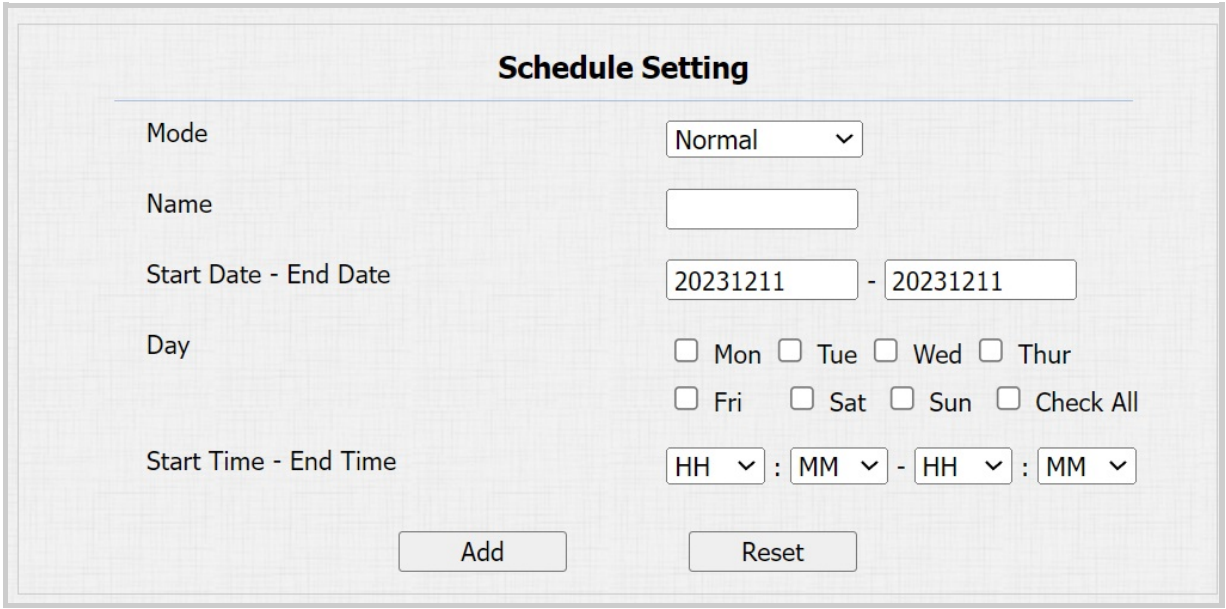
## Configure Door Access Schedule

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. You can add 100 local schedules.

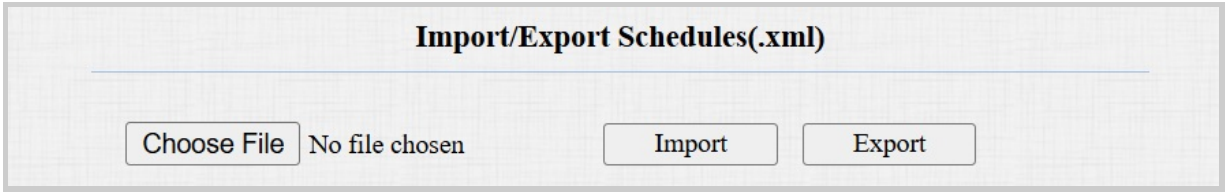



- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Name**: Name the schedule.

## 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.

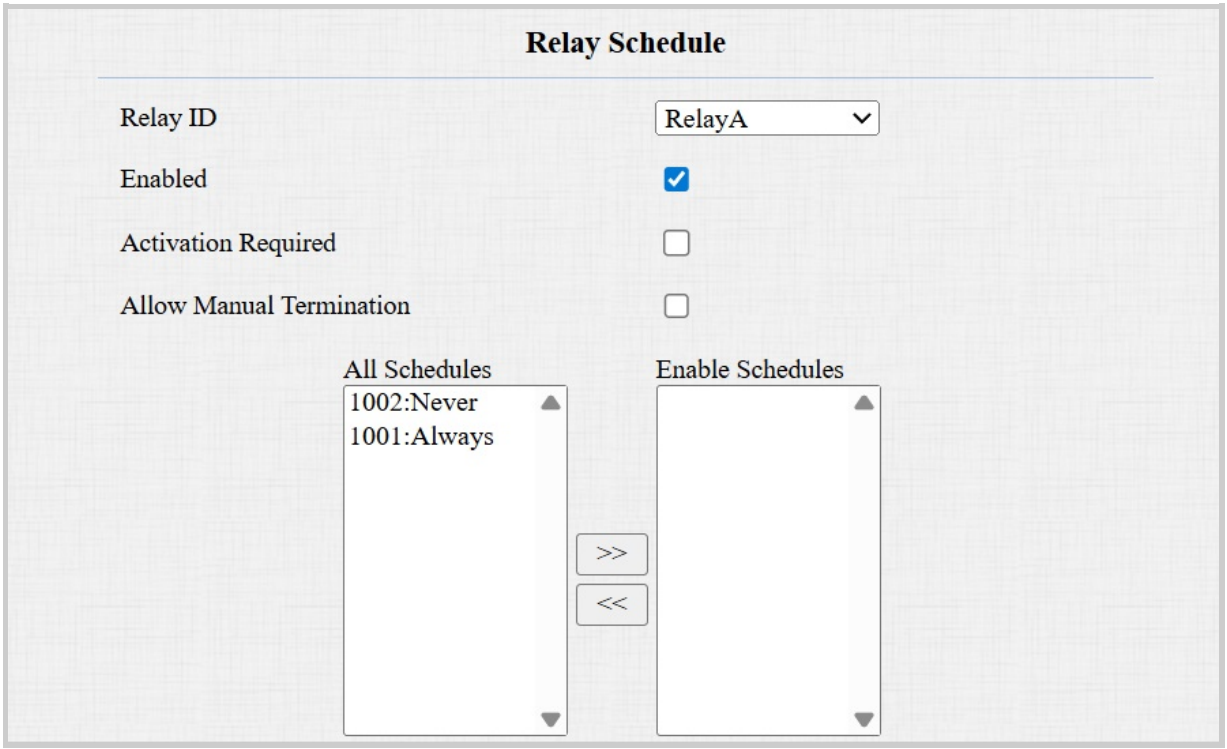
To set it up, go to the **Setting > Schedule** interface. The export file is in **TGZ** format. The import file should be in **XML** format.




# 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 Schedule** interface.



- **Relay ID**: When **Security Relay** is enabled, the relay security applies to the security relay A.
- **Activation Required**: Disabled by default. It means that only after the relay is triggered successfully for the first time can it be kept open within the schedule.
- **Allow Manual Termination**: Disabled by default. When enabled, users can close doors with the device-supported access methods within the schedule.
- **Schedule Enabled**: Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

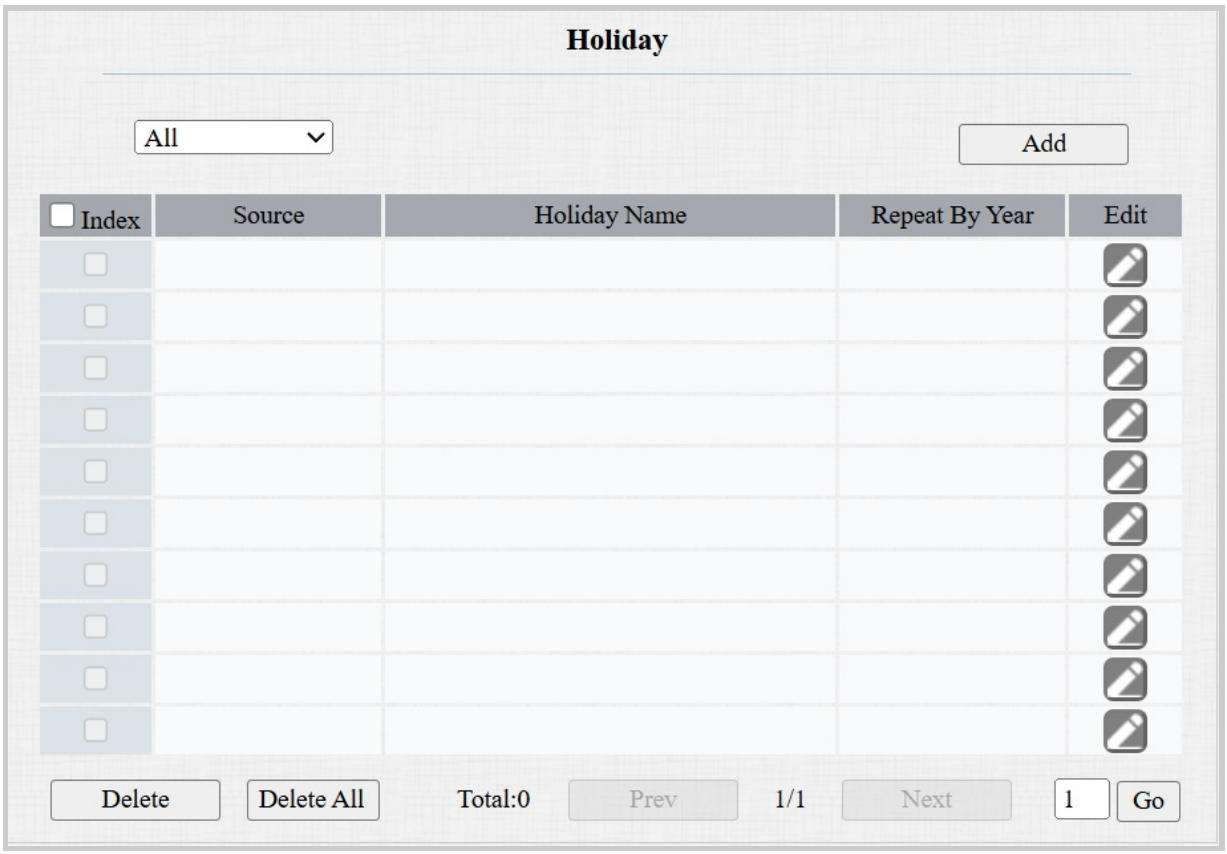
> **Note**
>
> Click **here** to view the details of the Activation Required feature

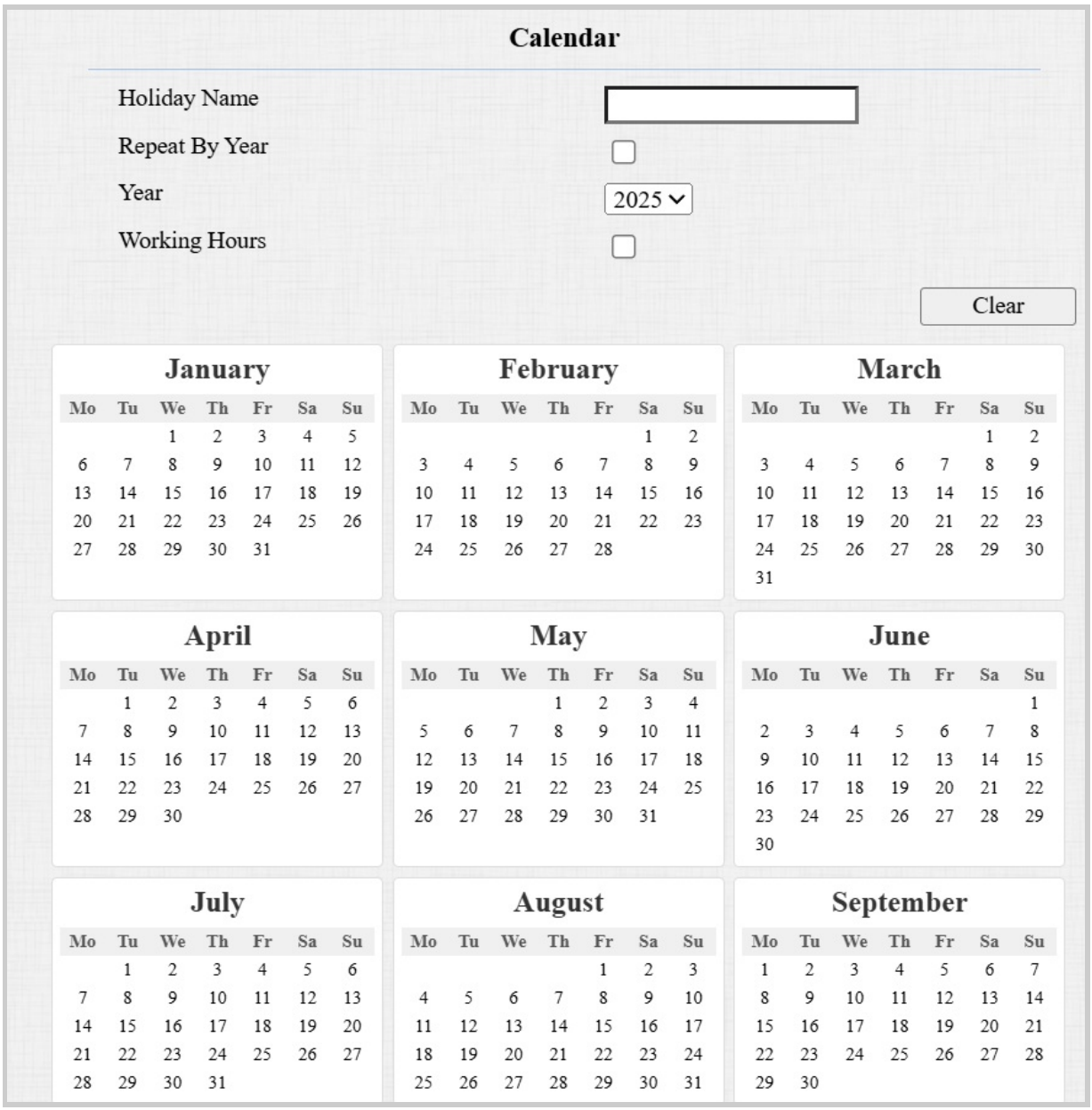
For instructions on creating schedules, kindly consult the Create Door Access Schedule section.

## Holiday Schedule

You can define the holidays when users cannot open doors to enhance access control security. You can also set the Working Hours to allow authorized users to open doors.

Set it up on the **Setting > Holiday** interface. Click **+Add.**


Holiday
All
Add
Index
Source
Holiday Name
Repeat By Year
Edit
Delete
Delete All
Total:0
Prev
1/1
Next
1
Go

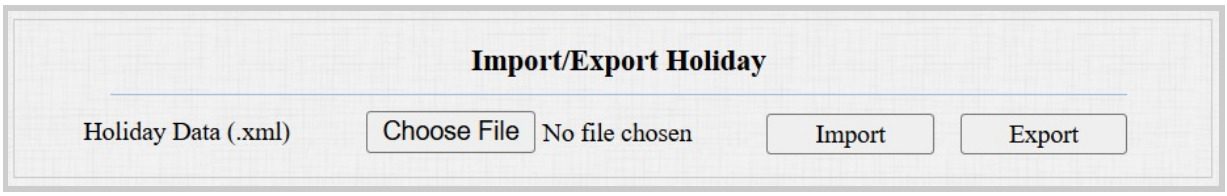



- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

## Holiday Schedule Import/Export

You can import or export holiday schedules for quick setup on the **Setting > Holiday > Import/Export Holiday** interface.

The import/export file format is .xml.


Import/Export Holiday
Holiday Data (.xml)
Choose File
No file chosen
Import
Export

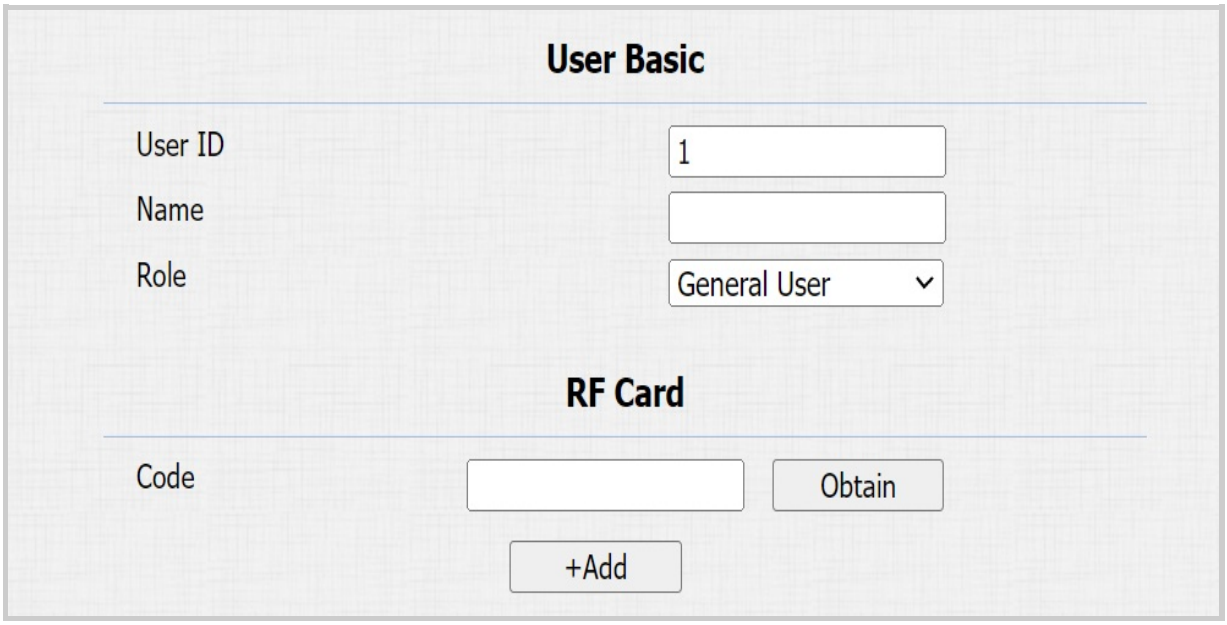
# Door-opening Configuration

## Unlock by RF Cards

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

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

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

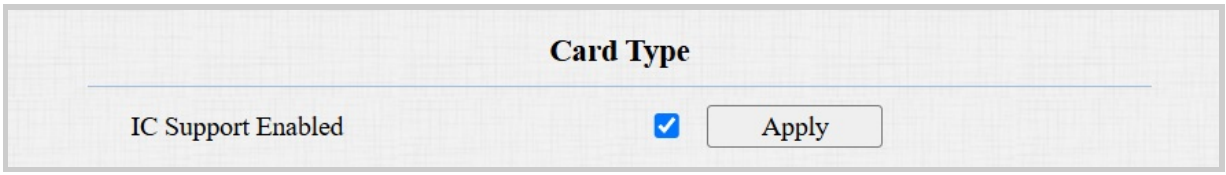



- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.
- **Role**: Define the user as a General User or an Administrator. The Admin card can be used to add a user card. Please refer to Configure Admin Cards and User Cards for detailed configuration.
-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

**Note:**

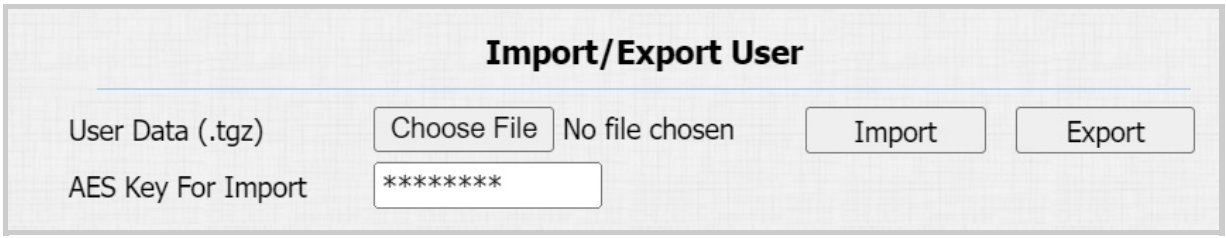
- Each user can have a maximum of 5 cards added.
- The device allows to add 5,000 users.
- RF cards operating at 13.56 MHz frequencies are compatible with the door phone for access.

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



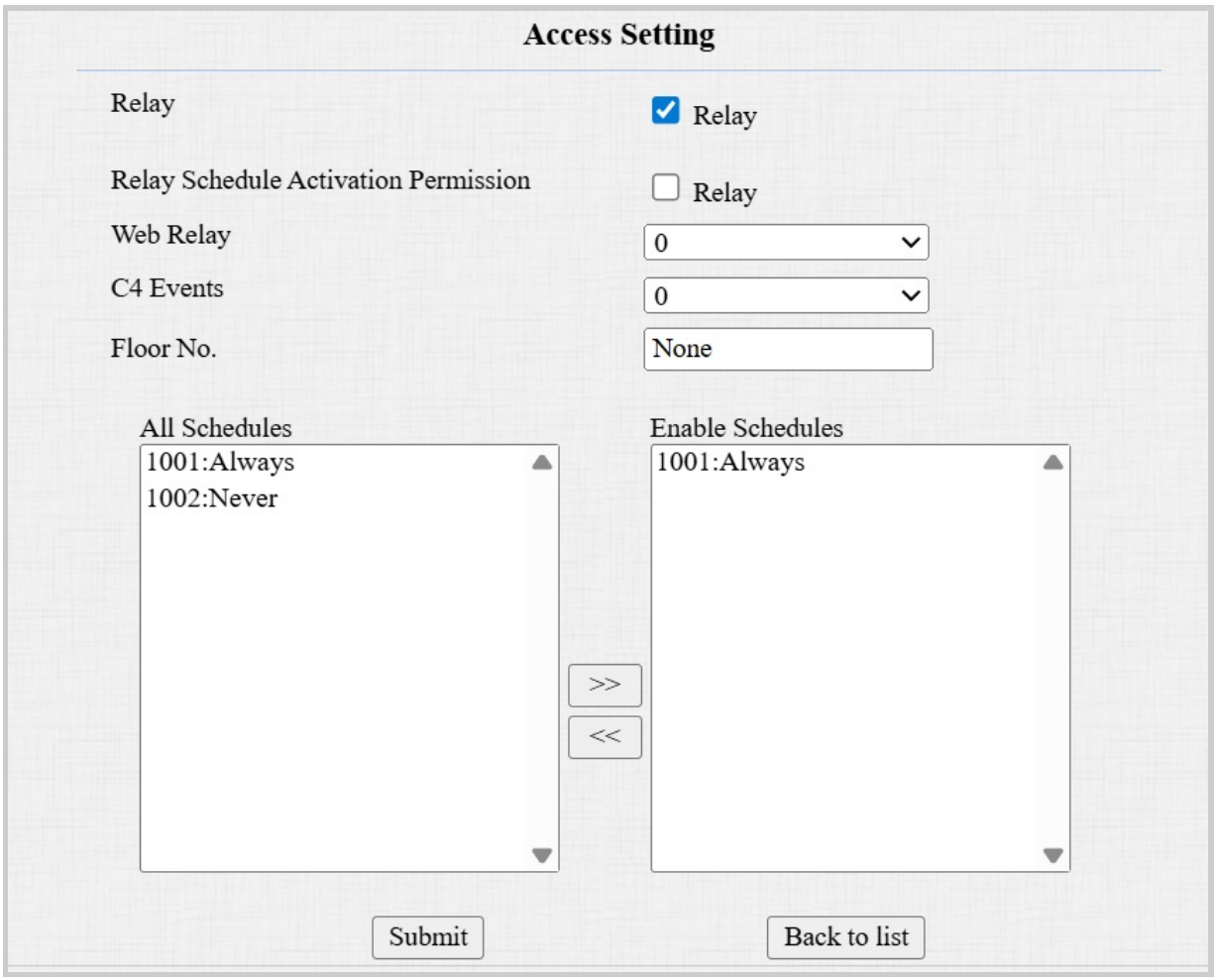

After adding users, you can export the user data and import it to another intercom device for quick management.

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




## Access Settings

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



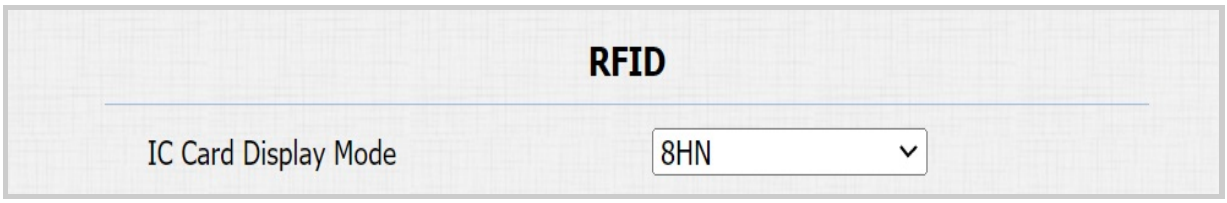

- **Relay**: The relay to be unlocked using the door-opening methods should be assigned to the user.
- **Relay Schedule Activation Permission**: This decides whether the user can keep the relay open during the scheduled time after activating it.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **C4 Events**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **Floor No.**: Specify the accessible floor(s) to the user via the elevator.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:

- Always: Allows door opening without limitations on door open counts during the valid period.
- Never: Prohibits door opening.

### 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.

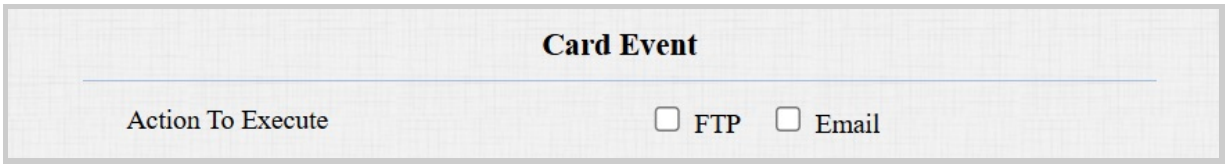
To set it up, go to **Access Control > Card Setting > RFID** interface.




- **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 > Card Event** interface.



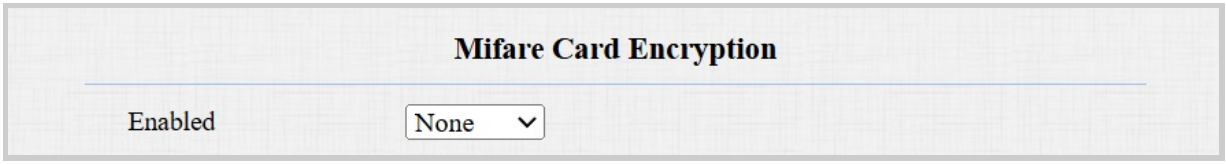

- **Action to Execute**: Set the desired actions that occur when the door is opened by swiping the RF card.
  - **Email**: Send a message to the preconfigured Email address.
  - **FTP**: Send a message to the preconfigured FTP address.

## Mifare Card Encryption

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

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

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




- **Classic**:
  - **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.
- **DESFire**:
  - **App ID**: A 6-digit hexadecimal number
  - **File ID**: The ID of the encrypted file of the app, which can be a number from 0 to 31.
  - **Crypto**: The encryption method, either AES or DES.
  - **Read Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.
  - **Byte Order**: The byte reading order. The default is MSB. The device starts reading bytes after performing **Data Offset** and **Data Length**.
    - **MSB**: Most Significant Bit means the reading order is normal(from left to right).
    - **LSB**: Least Significant Bit means the reading order is reversed(from right to left).
  - **Data Offset**: Define from which byte position to start reading data, with a range of 0 to 43. The default is 0.
  - **Data Length**: Define the length of valid byte data, with a range of 1 to 8. The default is 4.

# 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



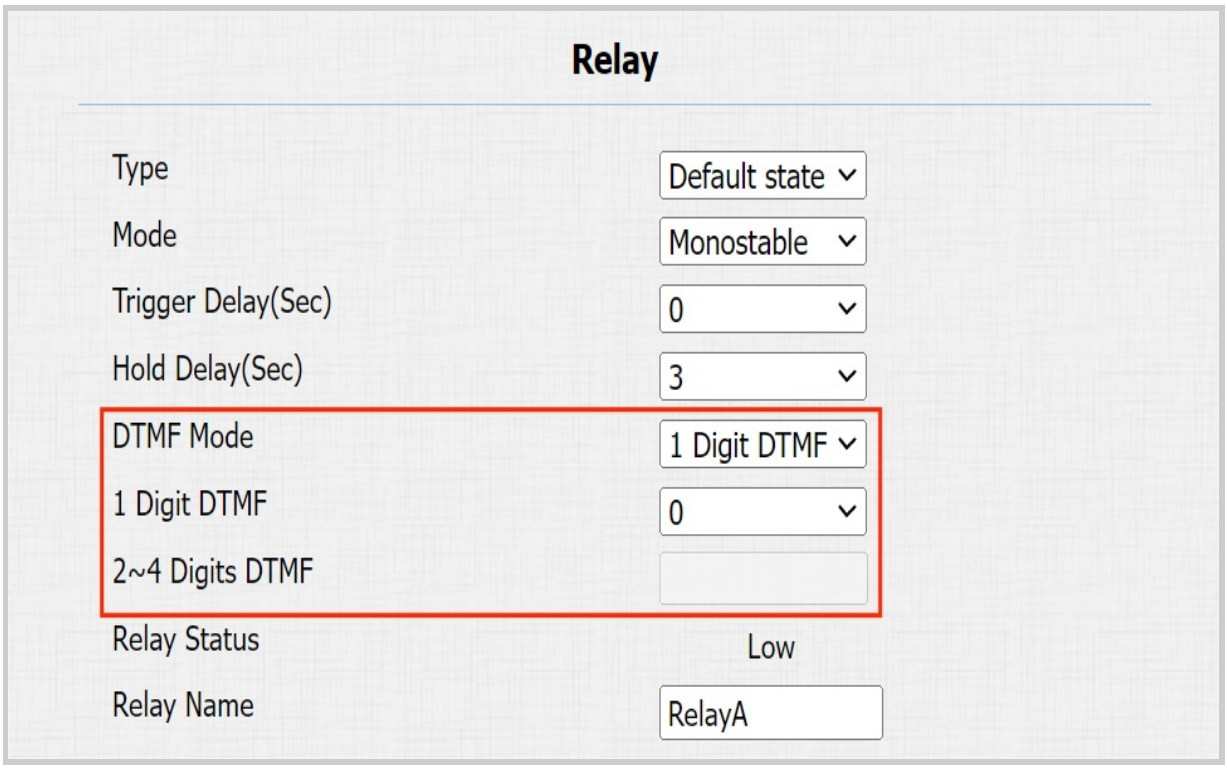

**Note**

- 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.



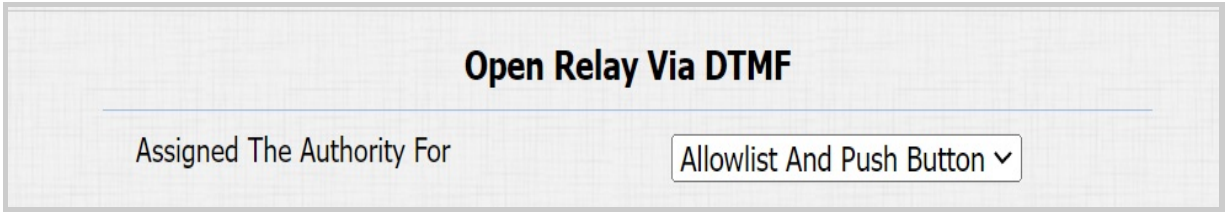

- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

**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.



- **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.

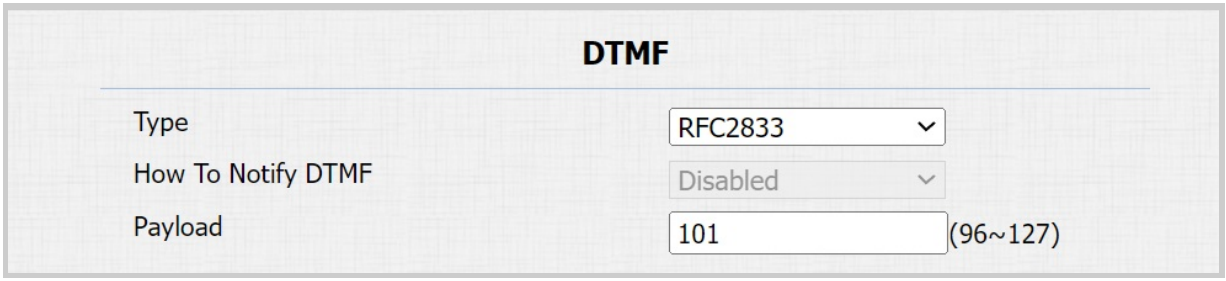
## Configure DTMF Data Transmission

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 device and other intercom devices.

**DTMF Type Differences**:

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

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



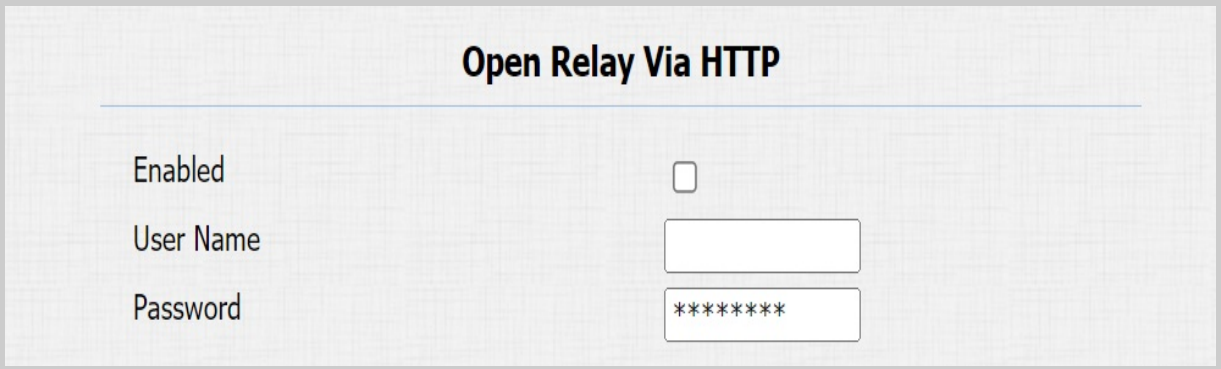

- **Type:** Select from the available options based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, or **Telephone-Event** according to the specific type adopted 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.

## 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.




- **User Name**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a password for authentication in HTTP command URLs.

**Tip:**

Here is an HTTP command URL example for relay triggering.




**Note**

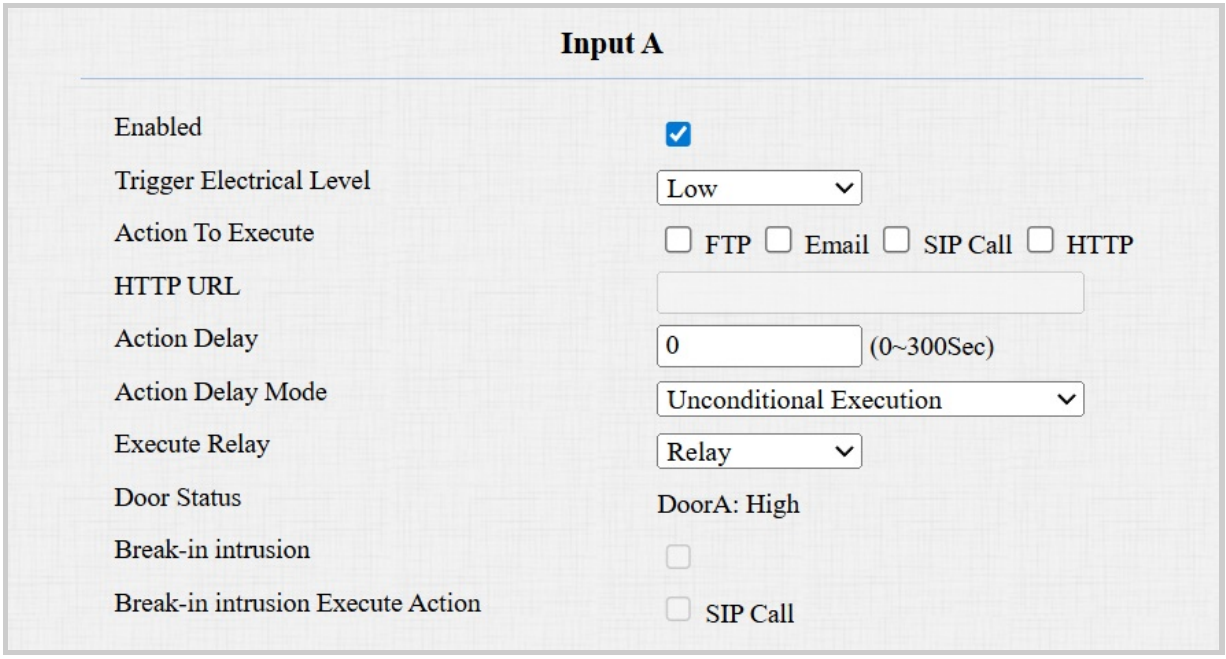
The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide **Opening the Door via HTTP Command** for more information.

# Unlock by Exit Button

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

Click here to watch the instruction video.

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




- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at a low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
    - **FTP**: Send a screenshot to the preconfigured FTP server.
    - **Email**: Send a screenshot to the preconfigured Email address.
    - **SIP Call**: Call the preset number upon the trigger.
    - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

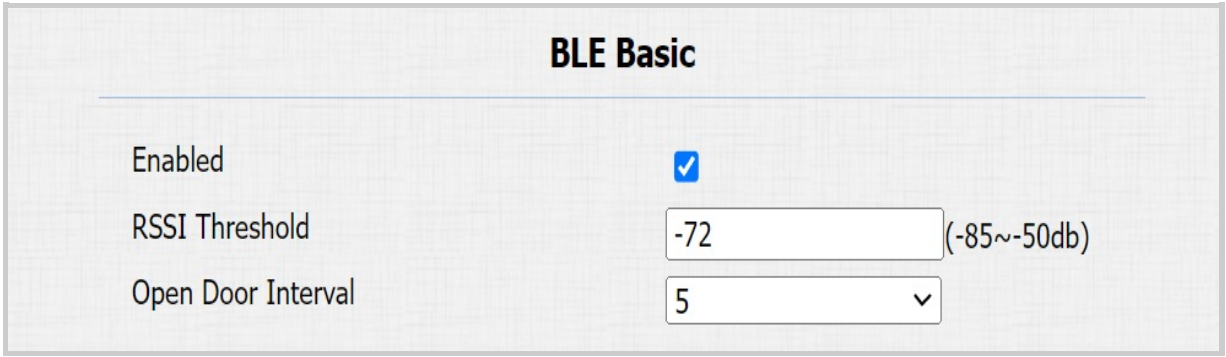
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode**:
    - **Unconditional Execution**: The action will be carried out when the input is triggered.
    - **Execute If Input Still Triggered**: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered along with the input triggering.
- **Door Status**: Display the status of the input signal.
- **Break-in Intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. It is incompatible with the **Execute Relay** feature. Click here to learn more about this feature.
- **Break-in Intrusion Execute Action**: If the SIP Call is checked, when the break-in intrusion occurs, a call will be made to the preconfigured number.

## Unlock by Bluetooth

The Bluetooth-enabled SmartPlus App enables users to enter the door without tapping on the device. They can open the door with the app in their pockets or wave their phones toward the door phone as they get closer to the door.

This feature requires the device to be connected to the SmartPlus Cloud.

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



- **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.

**Note**

Click **here** to view the detailed configuration of Bluetooth-based door opening.

# 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.

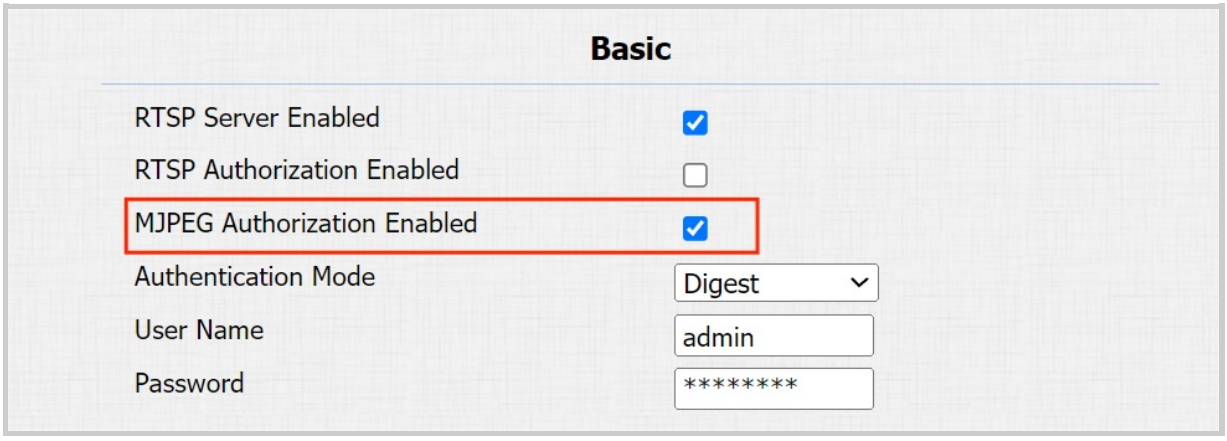
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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.



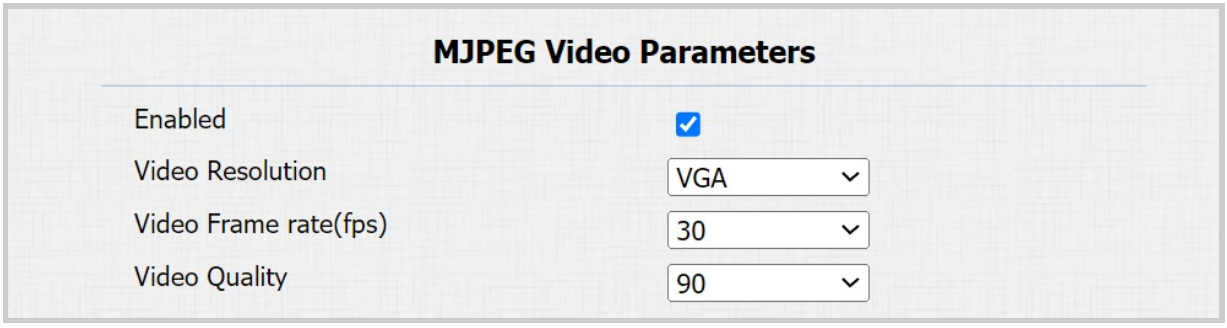
- **MJPEG  Authorization Enabled**: Once enabled, accessing the door phone's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username, and RTSP Password.

**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.




- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels). The default is VGA.
- **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.

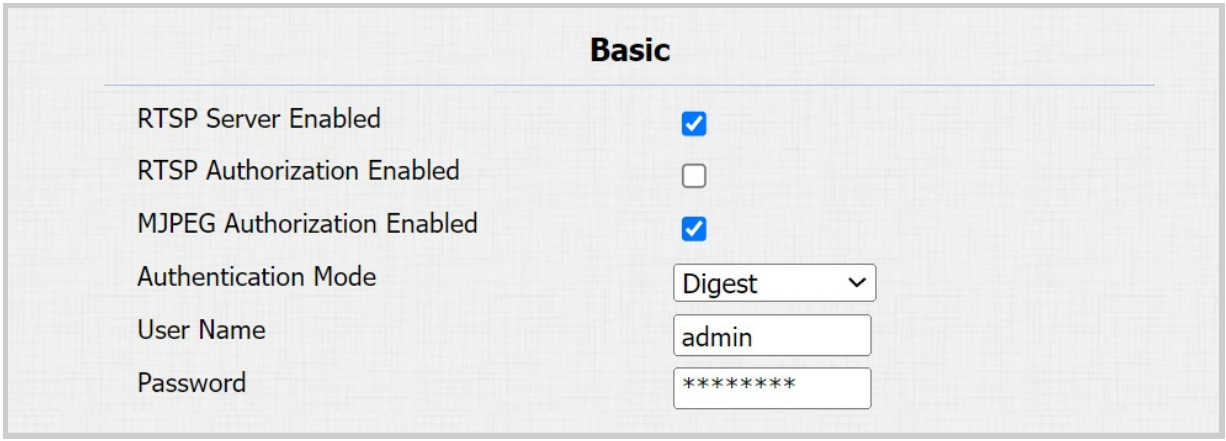
# RTSP Stream Monitoring

The RTSP feature allows Akuvox indoor monitors, or third-party devices, to obtain the live stream from the door phone.

You can set up the RTSP authentication credentials and video parameters.

## 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.

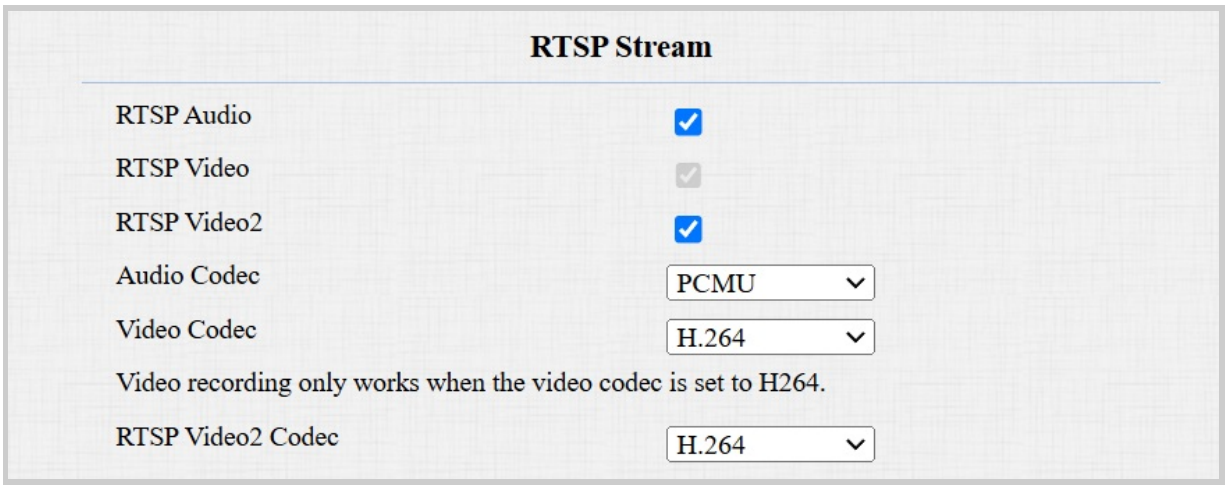



- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: It is Digest by default which uses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

## RTSP Stream Setting

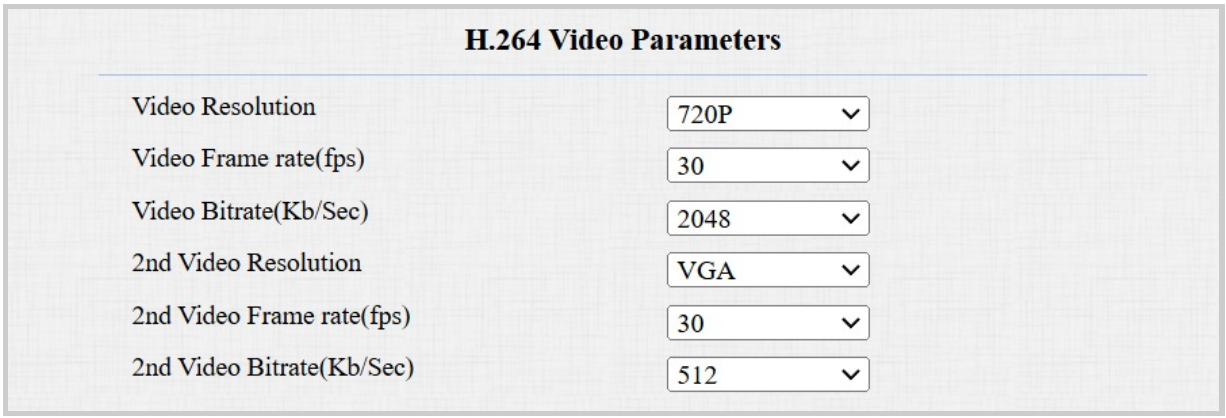
The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

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




- **RTSP Audio:** Decide whether the RTSP stream has sound.
- **RTSP Video:** Decide whether the RTSP stream has video. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **RTSP Video2:** E12 supports two RTSP streams.
- **Audio Codec:** Choose a suitable audio codec for RTSP audio.
- **Video Codec:** Specify the video compression formats.
    - H.264: Offer highly efficient compression but at the cost of higher latency and computational load.
    - MJEPG: Offer improved quality but inefficient compression.
- **RTSP Video2 Codec**: Specify the video compression format for the second RTSP channel.

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



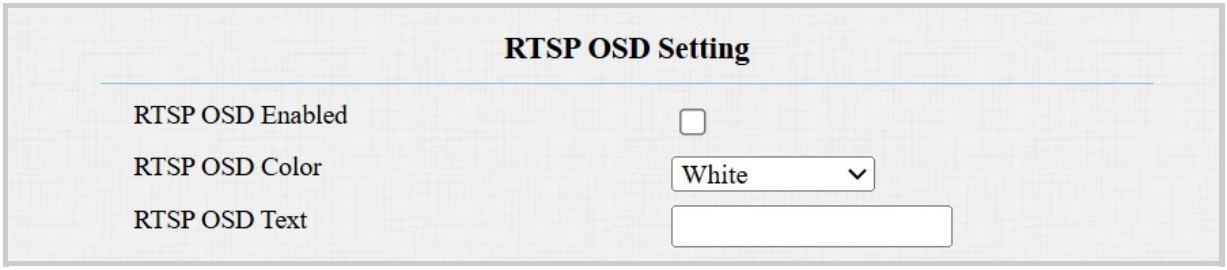

- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.

- **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. It is disabled by default.

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

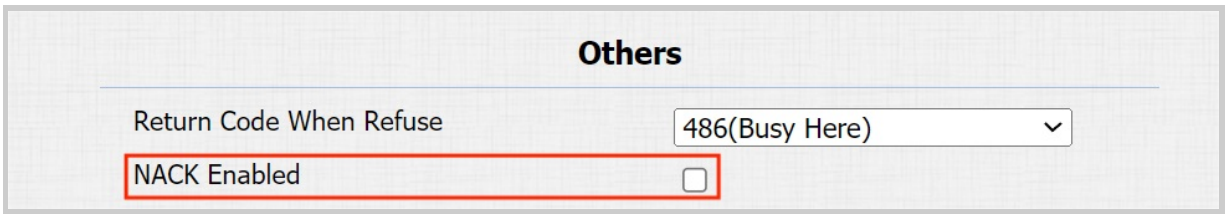



- **RTSP OSD Color**: There are five color options, White, Black, Red, Green, and Blue for RTSP watermark text.
- **RTSP OSD Text**: Customize the watermark text.

## NACK

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

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



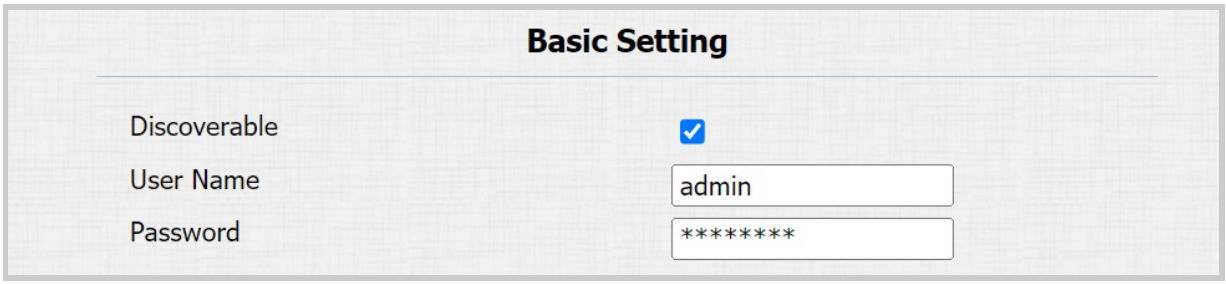

- **NACK Enabled:** It can be used to prevent losing data packets in the weak network environment when discontinued and mosaic video images occur.

## ONVIF

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

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

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




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

**Tip**

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

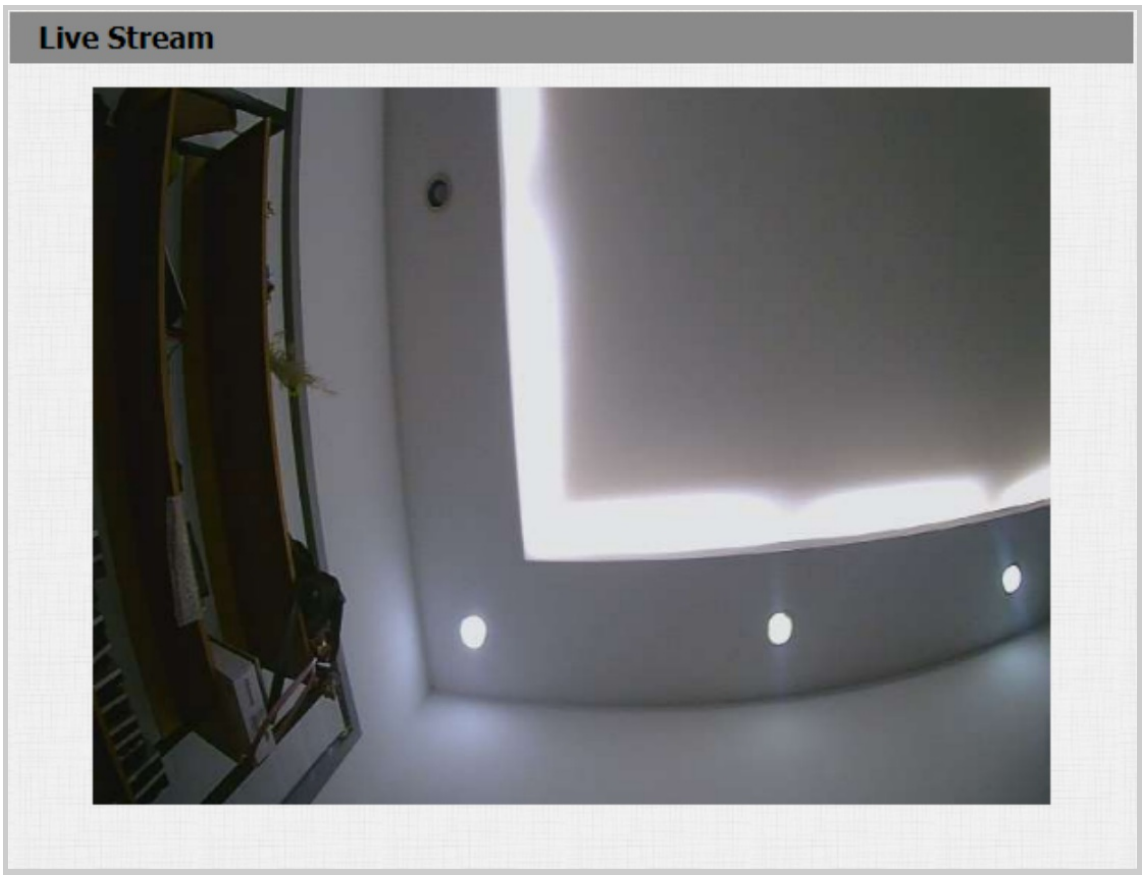
Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.




## 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.

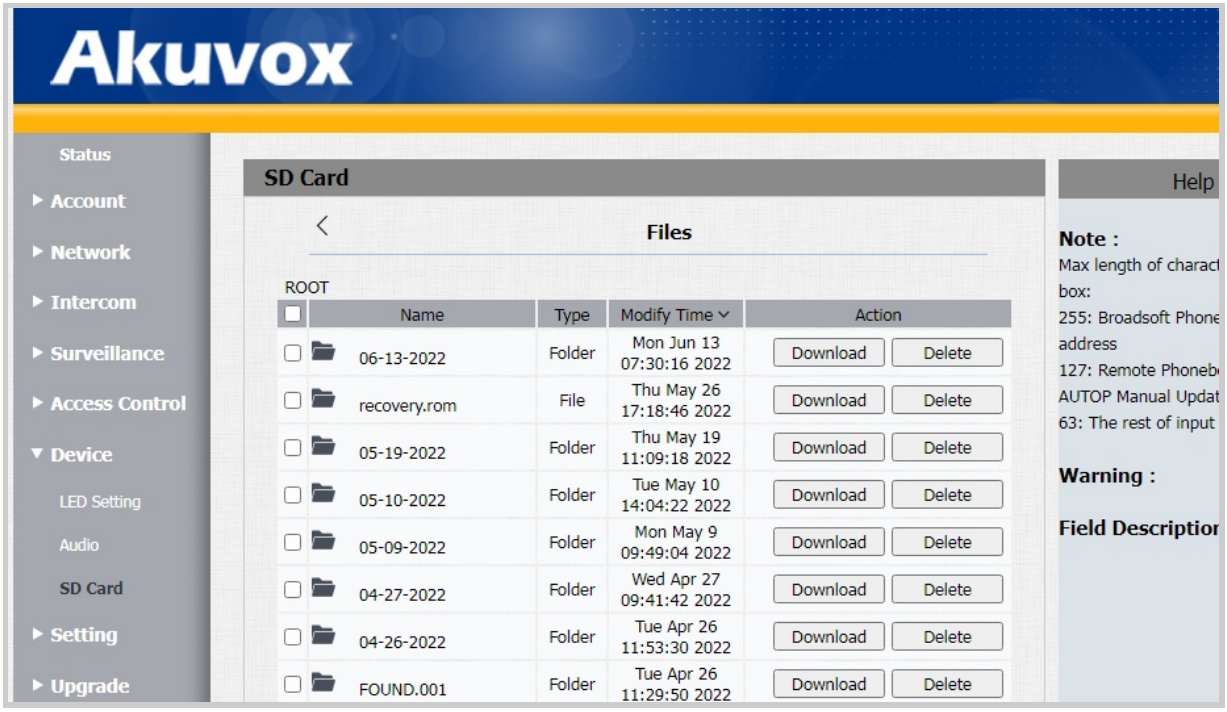
See live stream on the device **Surveillance > Live Stream** interface. You are required to enter the username and password set in the RTSP basic section before viewing the stream.




## SD Card for Storing Videos

The device can be inserted into an SD card to store motion and call videos.

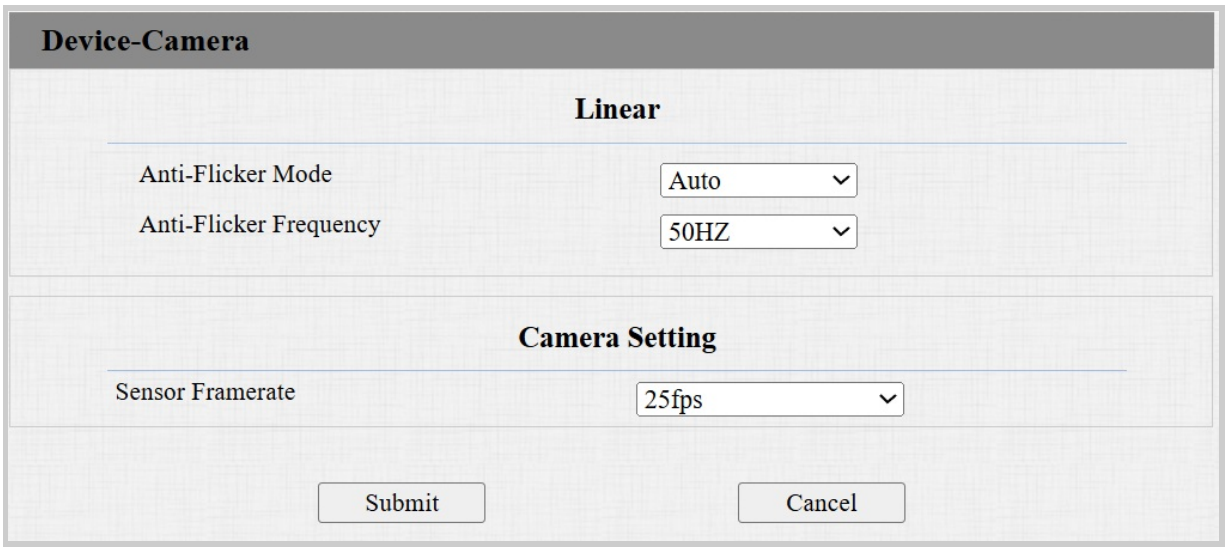
To check the videos, go to **Device > SD Card** interface. When there is not enough space in the SD card to record the next video, the system automatically deletes the oldest video.




# Camera Mode

Linear refers to a straightforward representation of brightness in images. Linear images are commonly used in controlled lighting environments, such as indoor scenes, where consistent brightness is present.

To set it up, go to the **Device > Camera** interface.




- **Anti-Flicker Mode**: The anti-flicker feature reduces or eliminates flickering in images or videos caused by varying light sources.
    - **Auto**: The device will switch automatically between 50Hz and 60Hz anti-flicker frequency.
    - **Manual**: Select the anti-flicker frequency manually.
    - **Off**: Disable the anti-flicker function.
- **Anti-Flicker Frequency**: Select the anti-flicker frequency between 50Hz and 60Hz.
- **Sensor Framerate**: Adjust the camera frame rate.
    - **30fps**: Better for applications needing higher smoothness.
    - **25fps**: Suitable for standard video recording and playback, especially under a 50Hz power frequency to minimize flicker.

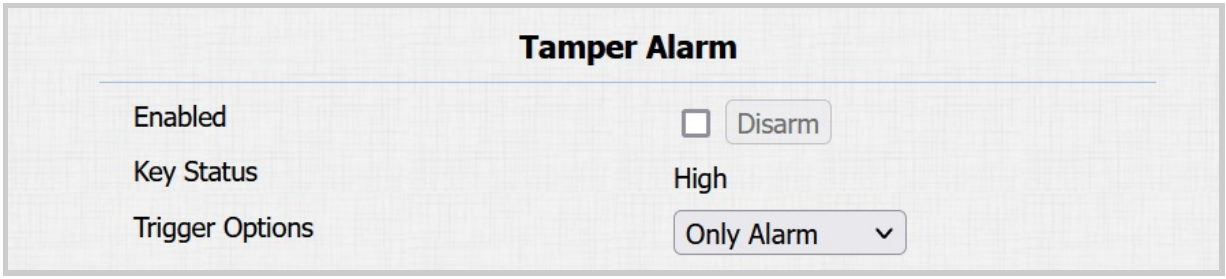
# Security

## Tamper Alarm

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

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

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




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

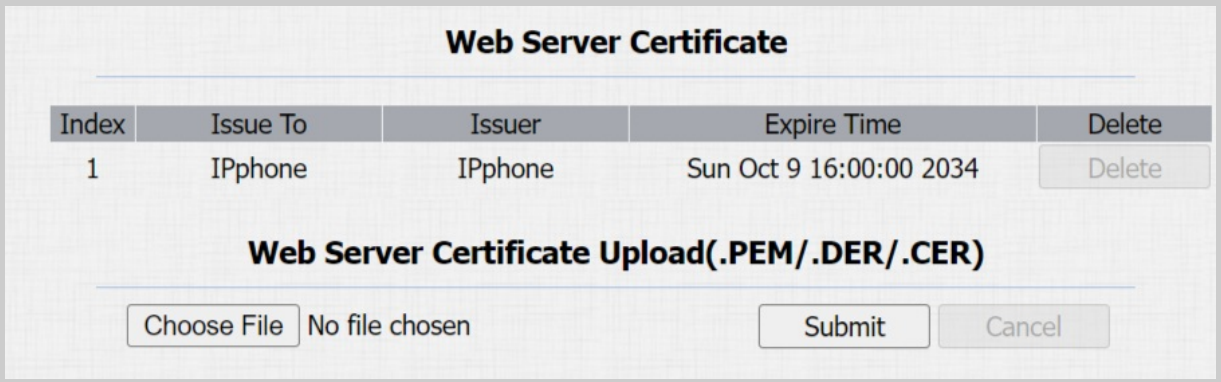
## Client Certificate Setting

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.

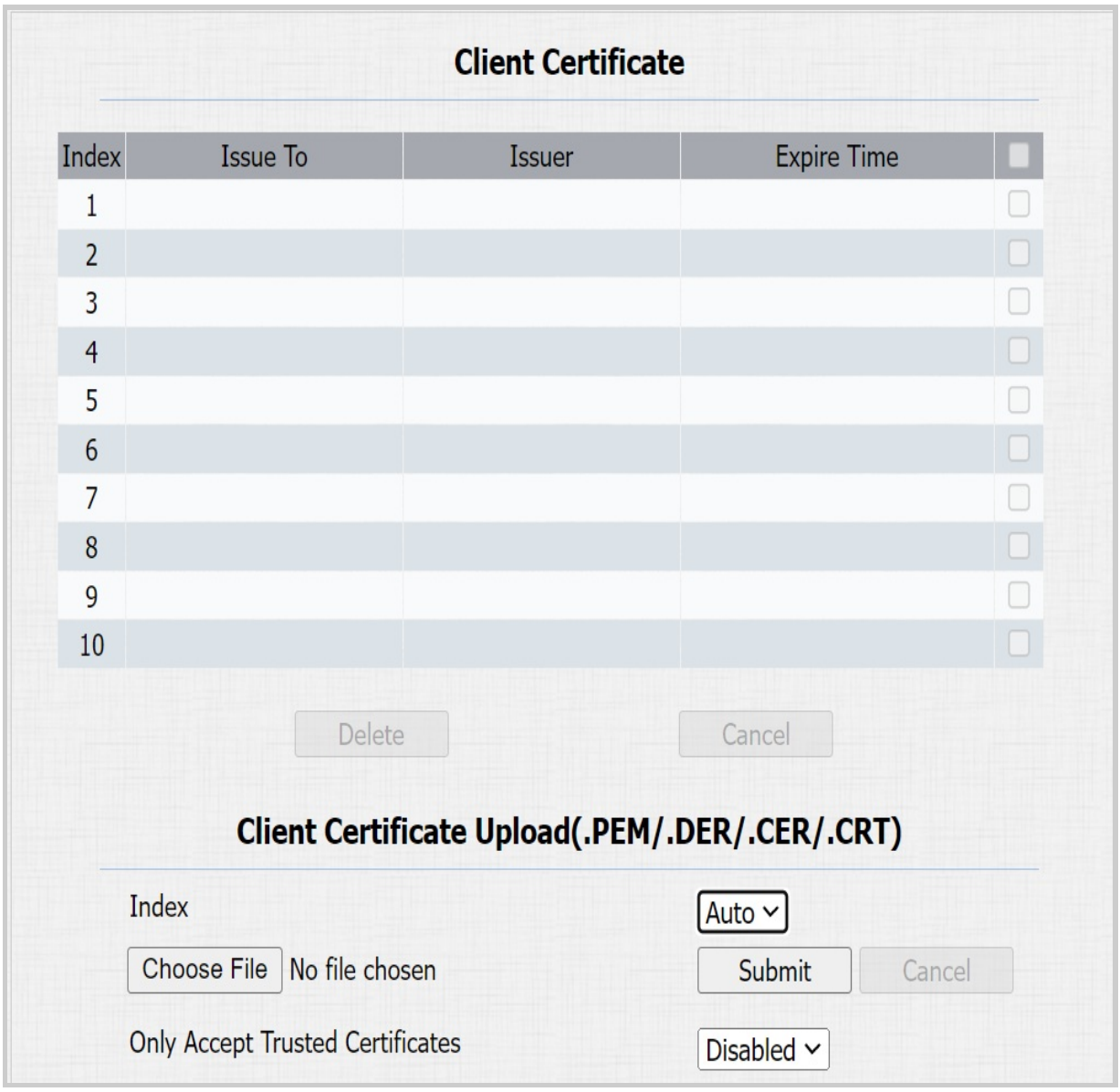
Upload the Web Server Certificate on the **System > Certificate > Client Certificate** interface.




## Client Certificate

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

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

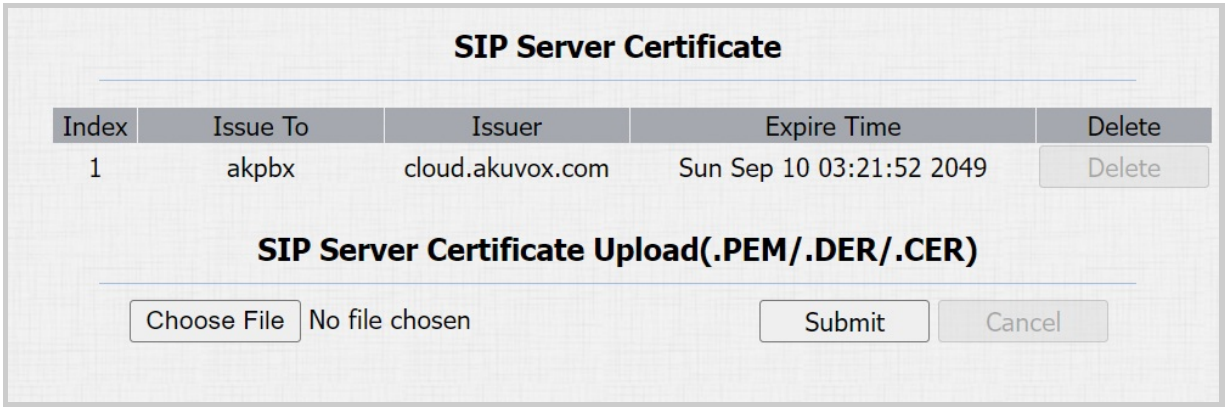



- **Index:**
  - Auto: The uploaded certificate will be displayed in numeric order.
  - 1 to 10: The uploaded certificate will be displayed according to the value selected.
- **Choose File:** Click Choose File to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, as long as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

## Upload TLS Certificate for SIP Account Registration

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

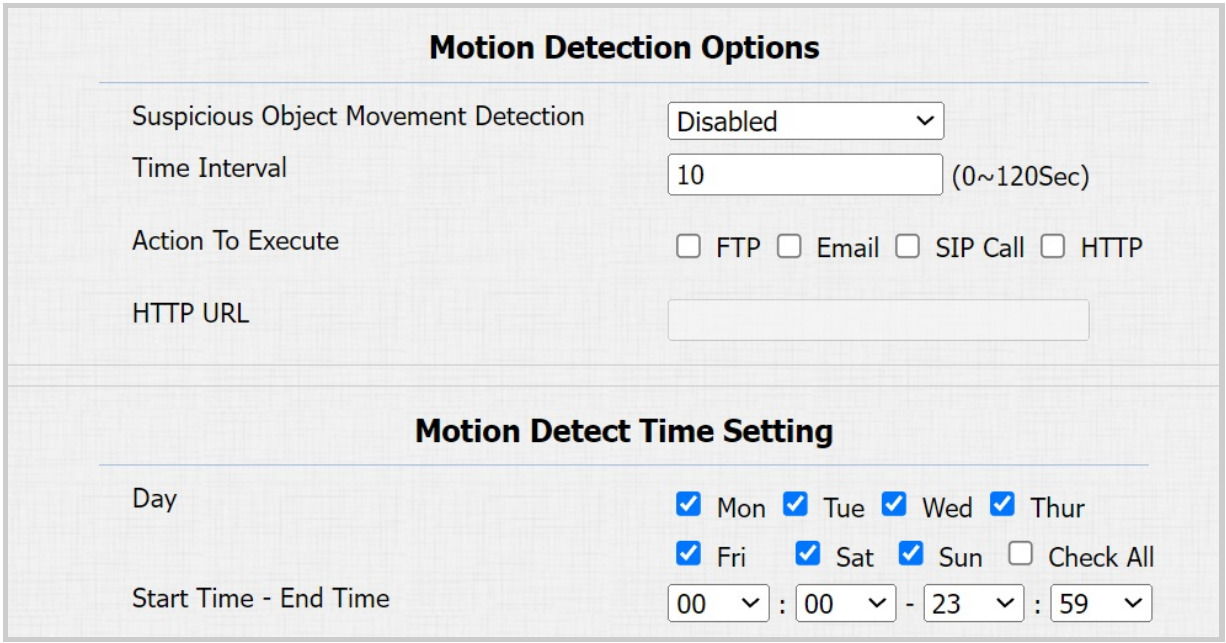
To set it up, go to **System > Certificate** interface.




# Motion Detection

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

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



- **Suspicious Object Movement Detection:** Select Video Detection to enable video-based motion detection during the monitoring of the suspicious moving object.
- **Detection Area**: You can click and hold the mouse button to select a detection area, or enter the width and height percentage. The full size of the detection area is calculated by percentage (100%) from left to right. Pick the horizontal detection range anywhere from 0% to 100%, and pick the vertical detection range anywhere from 0% to 100%.
- **Sensitivity Threshold**: The detection sensitivity. The greater the value is, the more accurate the detection is. The default value is 3.
- **Time Interval:** Determine how to delay and trigger motion detection.
    - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.
    - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
    - The default interval is 10 seconds.
- **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 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 URL 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 device detects. For example, if the device detects something unusual, the system sends a notification to users or security through email, phone calls, or other methods.

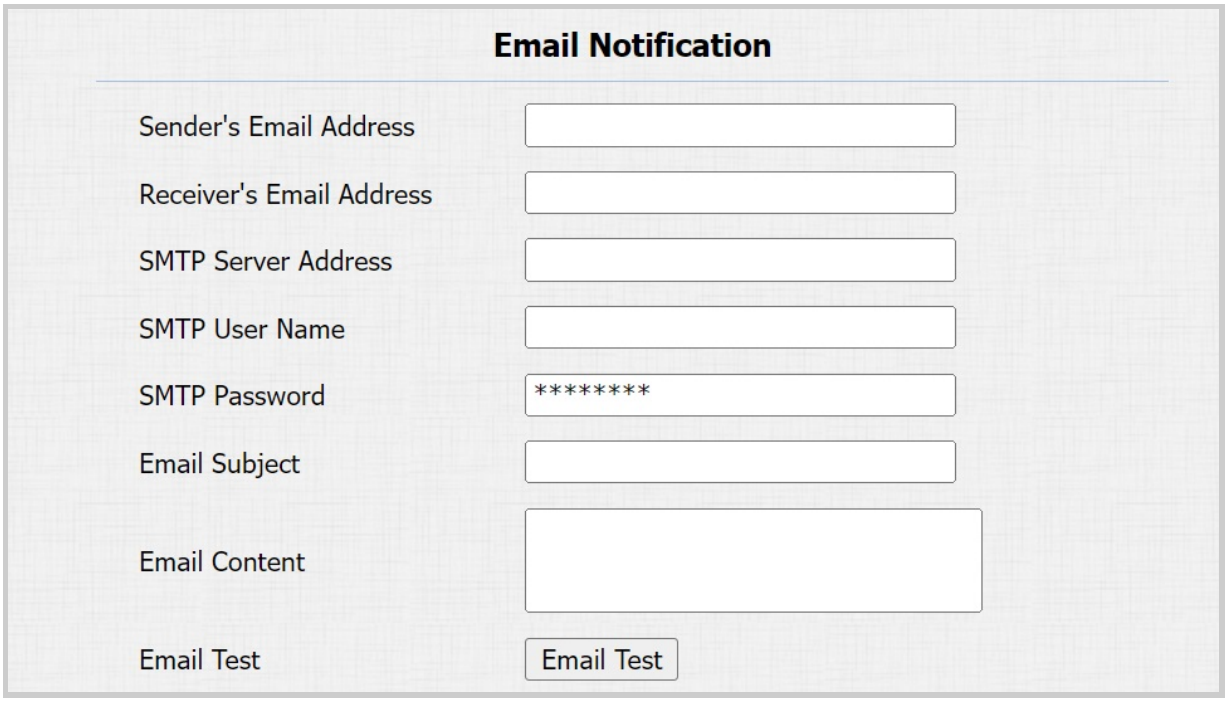
To set up security notifications, go to **Setting > Action** interface.

## Email Notification

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

Click here to view how to set this feature up.

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



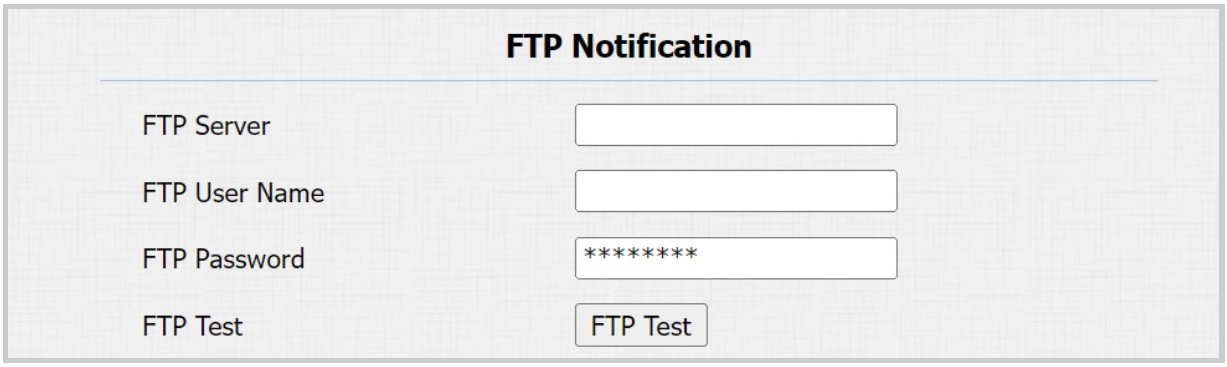

- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.
- **Email Test**: Used to test whether the email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

## FTP Notification

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

Click here to view the configuration steps.

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

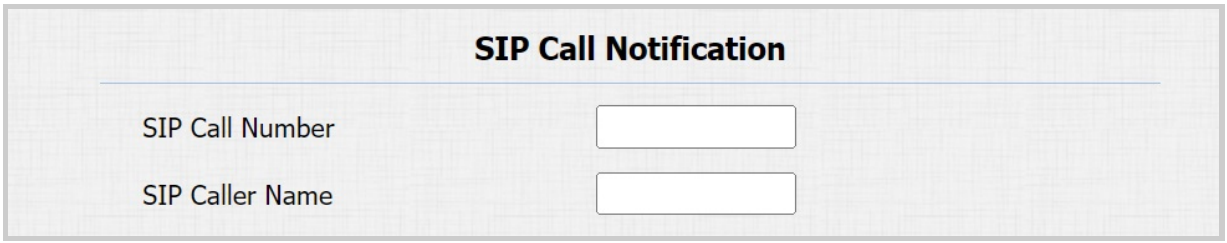



- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.
- **FTP Test:** Used for testing whether the FTP notification can be sent and received by the FTP server.

## 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.




## 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.




## Action URL

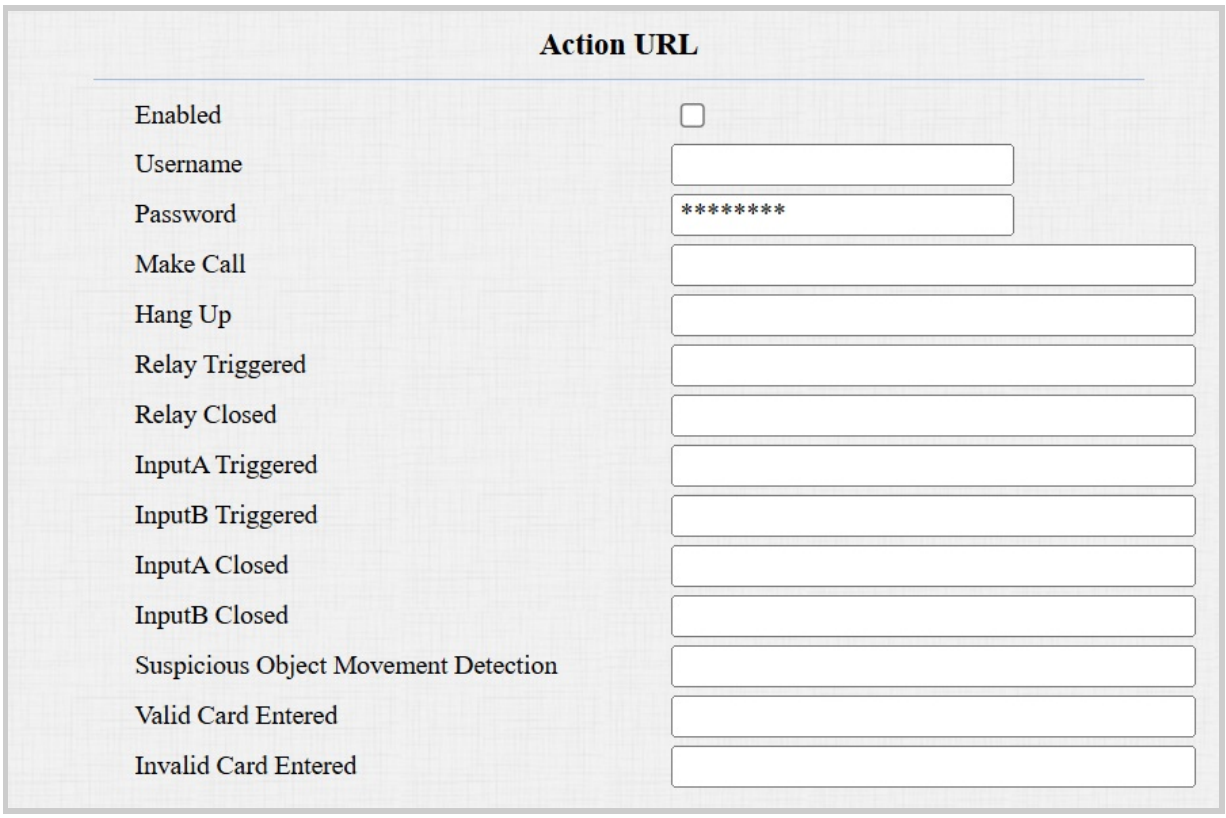
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, or RF card access changes.

**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.




- **Valid/Invalid Card Entered**: When using Bluetooth to open the door and trigger the action URL, the Bluetooth code will replace $card_sn in the URL sent to the HTTP server.

# 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.

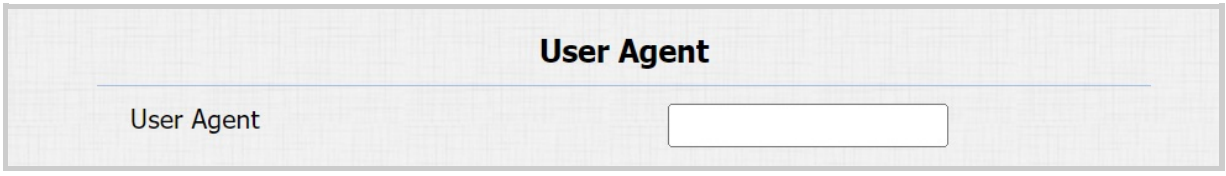



- **Voice Encryption(SRTP):** Choose Disabled, Optional, or Compulsory for SRTP. If **Optional** or **Compulsory** is selected, the voice during the call is encrypted, and you can grab the RTP packet to view it.

# 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:** Akuvox is by default.

# Emergency Action

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

Click here to view the detailed configuration of this feature.

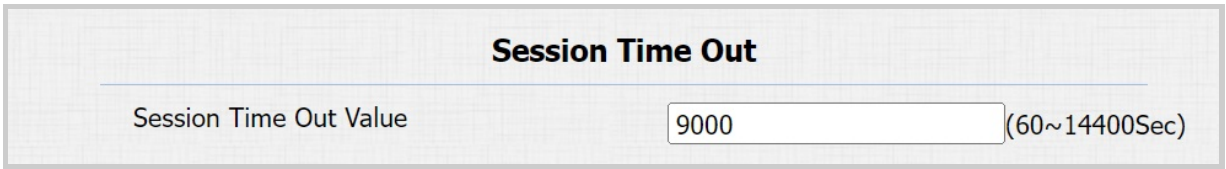
To set it up, go to **System > Security > Emergency Action** interface. Select the Input(s) to be triggered.




# 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 **System > Security > Session Time Out** interface.



# High Security Mode

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

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




**Important Notes**

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

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

- PC Manager: 1.2.0.0
- IP Scanner: 2.2.0.0
- Upgrade Tool: 4.1.0.0
- SDMC: 6.0.0.34

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

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

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

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

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

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

## Real-time Monitoring

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

Click here to see the detailed configuration.

To set it up, go to the **System > Security > Real-time Monitoring** interface.



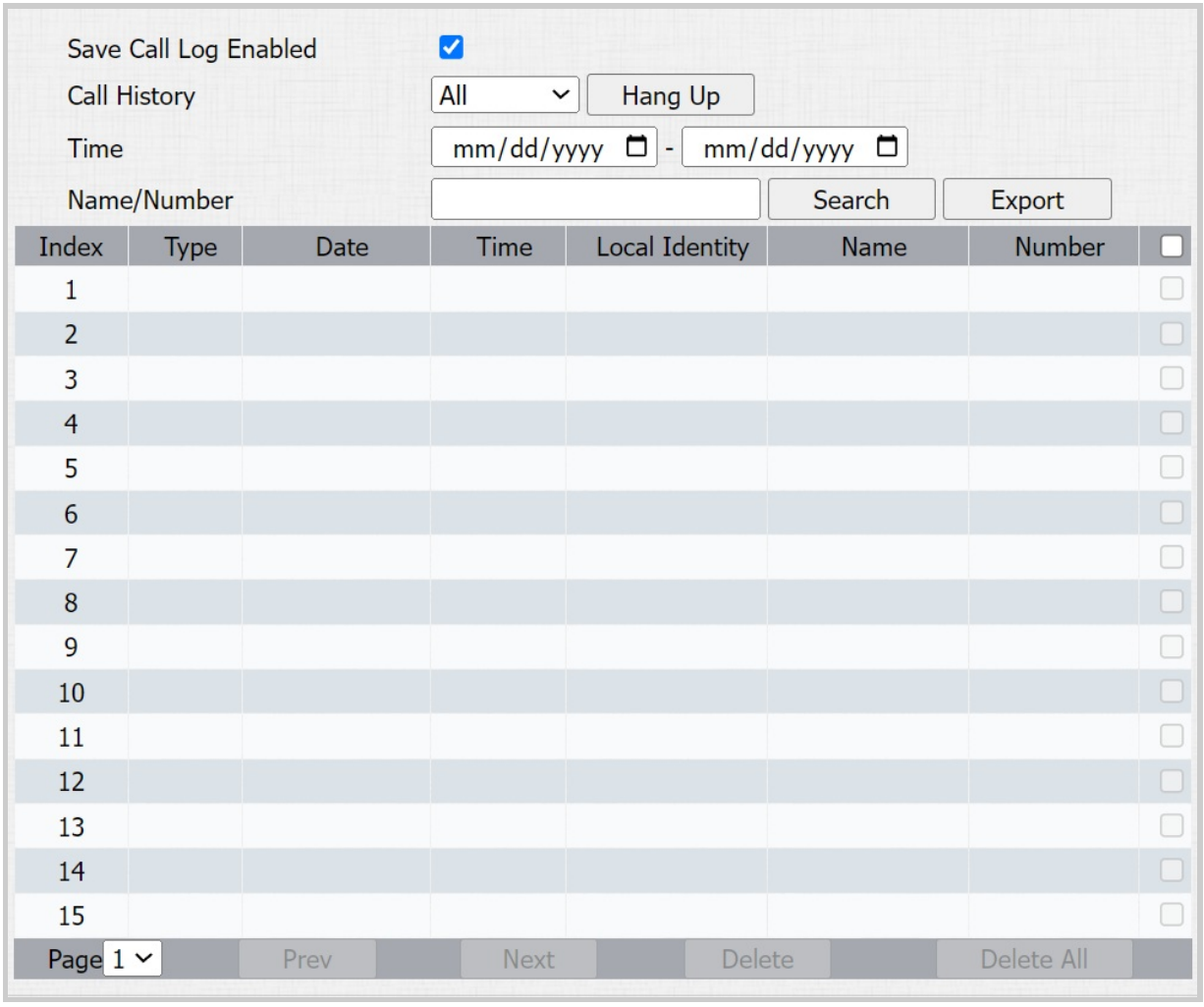

- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering the input.
  - **Relay**: The door is opened by triggering the relay.

# Logs

## Call Logs

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

Go to the **Status > Call Log** interface. The device supports 100 call logs.

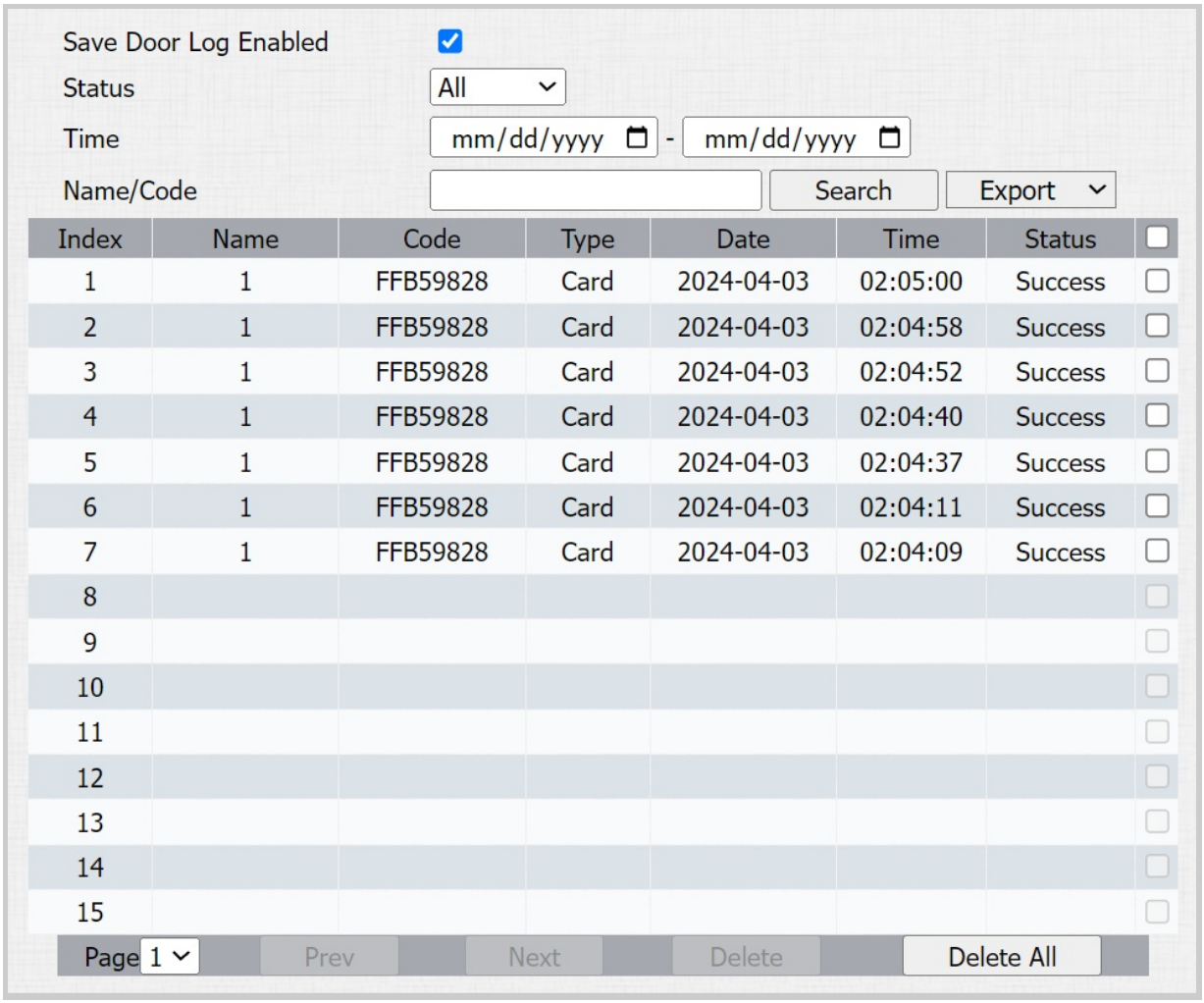



- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.

# Door Logs

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

Go to the **Status > Access Log** interface. The device supports 200 door logs.

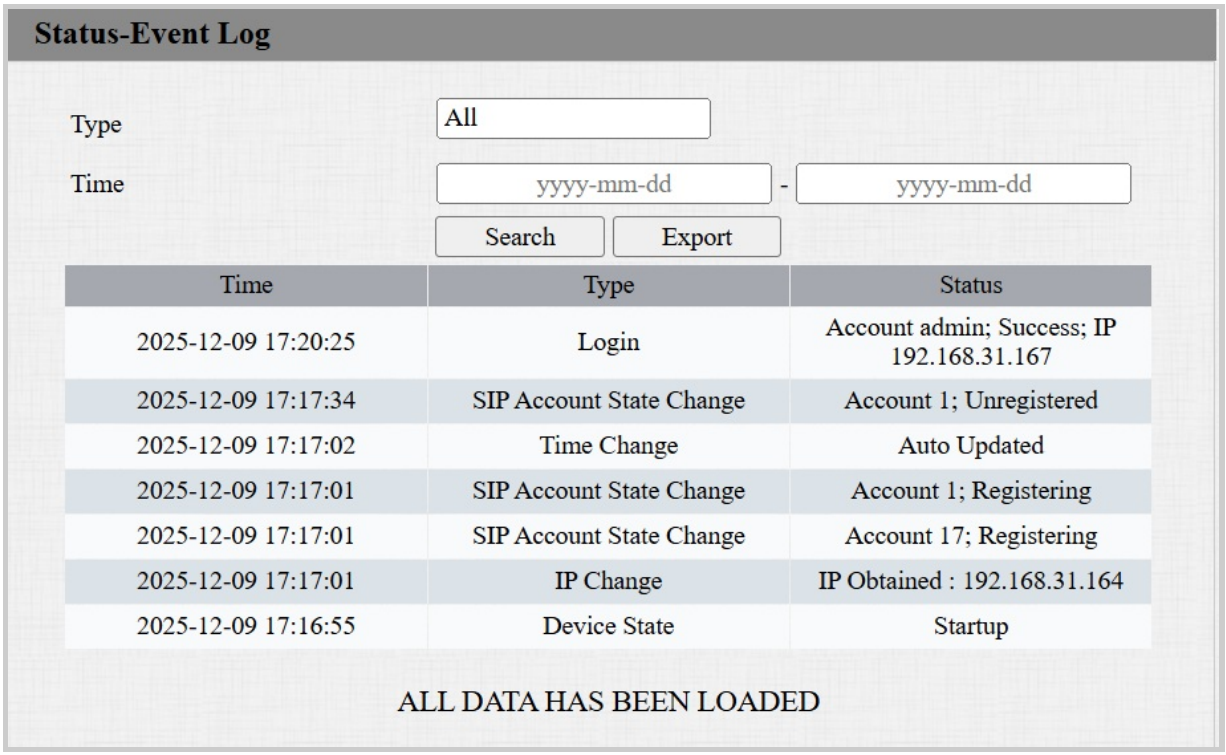



- **Status:** Display All, Successful, and Failed door-opening records.
- **Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card code will be displayed.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

# Event Logs

The event logs record the key events such as the status change of input, relay, tamper alarm, etc. This helps track the status and changes of the device.

Check event logs on the **Status > Event Logs** interface. The device supports up to 100,000 logs, which can be exported in CSV format.

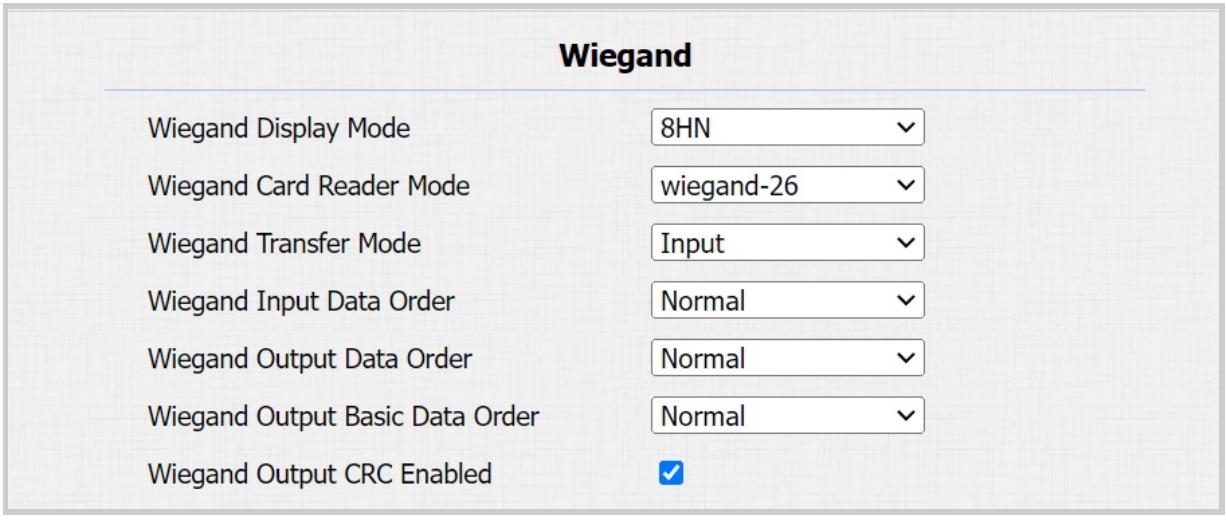


# Integration with Third Party Device

## Integration via Wiegand

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

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




- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender and can directly output the data, such as a card code.
  - **Convert To Card No. Output**: The device serves as a sender and cannot directly output the data.
- **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 data after the Wiegand conversion.
  For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If Reversed is selected, the card data is 0x55 0x44 0x33.

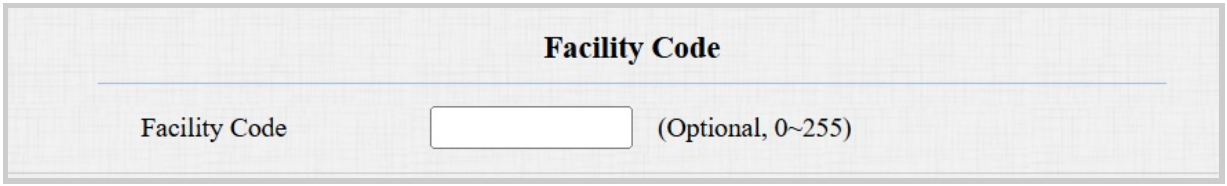
- **Wiegand Output Basic Data Order**: Set the sequence of the card data before going through Wiegand conversion and outputting the card code.
  For example, if the card data is 0x11 0x22 0x33 0x44 and the Reversed option is selected, the data will be 0x44 0x33 0x22 0x11.
- **Wiegand Output CRC Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.

> **Note**
>
> Click **here** to view more information on Wiegand settings including:
>
> - Akuvox devices work as Wiegand input/output;
> - Wiegand Card Reader Connection.

## Facility Code Setting

A facility code is a unique number in access control cards. It identifies the device that issued the card.

When the **Wiegand Transfer Mode** is **Output**, you can set up the facility code on the **Device > Wiegand** interface.




- **Facility Code**: The value ranges from 0 to 255. If filled in, the first two digits of the card number will be replaced by the code. If the code is less than 2 digits, a zero will be automatically added to the card number.

**Tip**

Since the Facility Code replaces the first two digits of the original card number, to keep the original card number intact, you can manually configure the Wiegand Card Reader Mode.
For example, if the card number is 3 bytes (Wiegand-26), you can select Wiegand-34 (4 bytes) to ensure the Facility Code replaces the first two digits with 0 instead of the original number.

## 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 **Setting > HTTP API** interface.




- **HTTP API Enabled**: Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode**: It is Digest by default. You are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode the username and password.
- **User Name**: Enter the user name for authentication. The default is admin.

- **Password**: Enter the password for authentication. The default is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

**Please refer to the following description for the authentication mode:**

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

# Lift Control

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

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

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

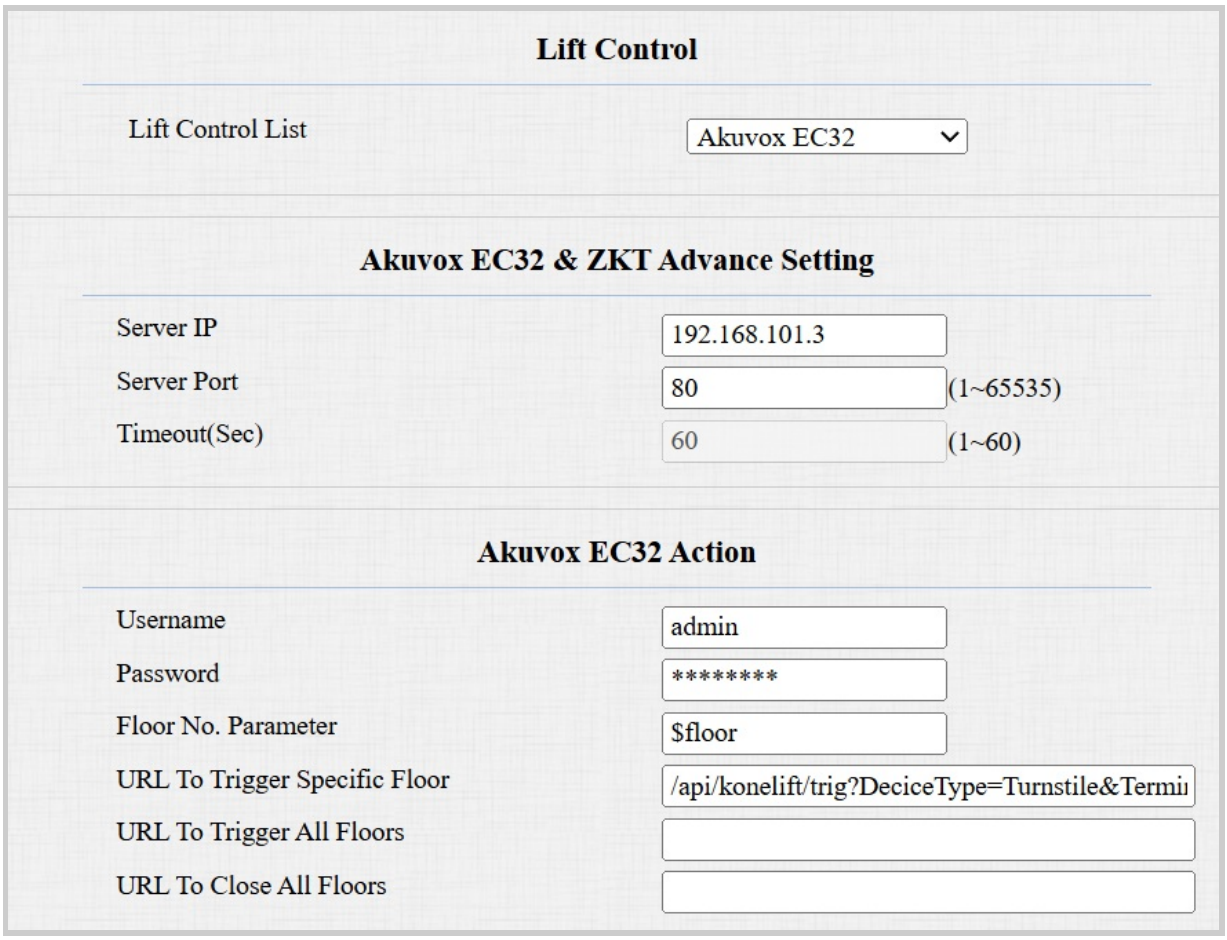



- **Lift Control List:** Select the lift controller brand.
  - **None**: The RS485 integration will be disabled.
  - **Akuvox EC32**: Connect the device with the Akuvox EC33 lift controller.
  - **ZKT**: Integrate with ZKTeco lift controller.

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

## Akuvox Lift Controller

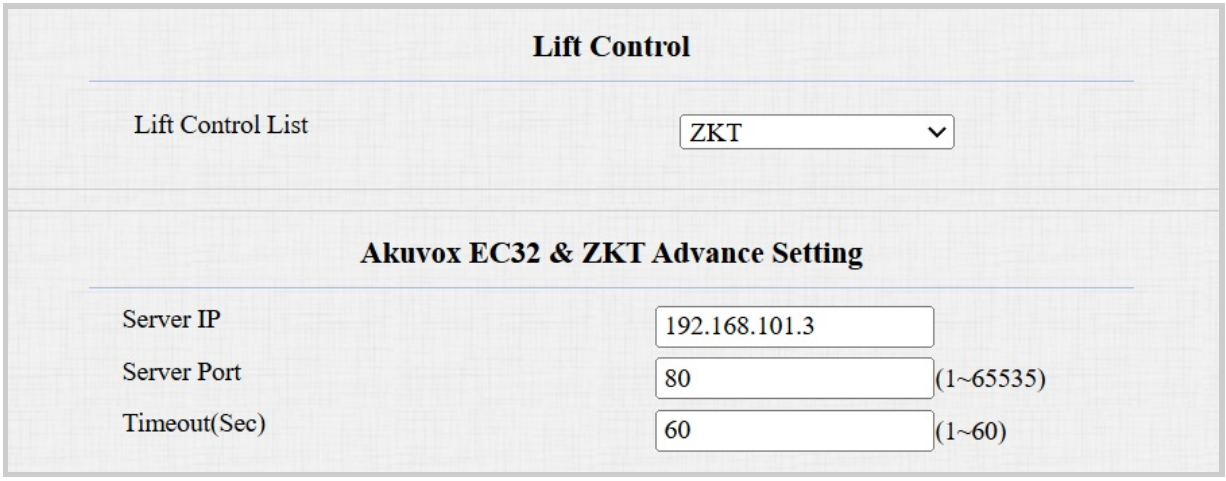
After selecting Akuvox EC32 in the Lift Control List, you need to set up relevant parameters.




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

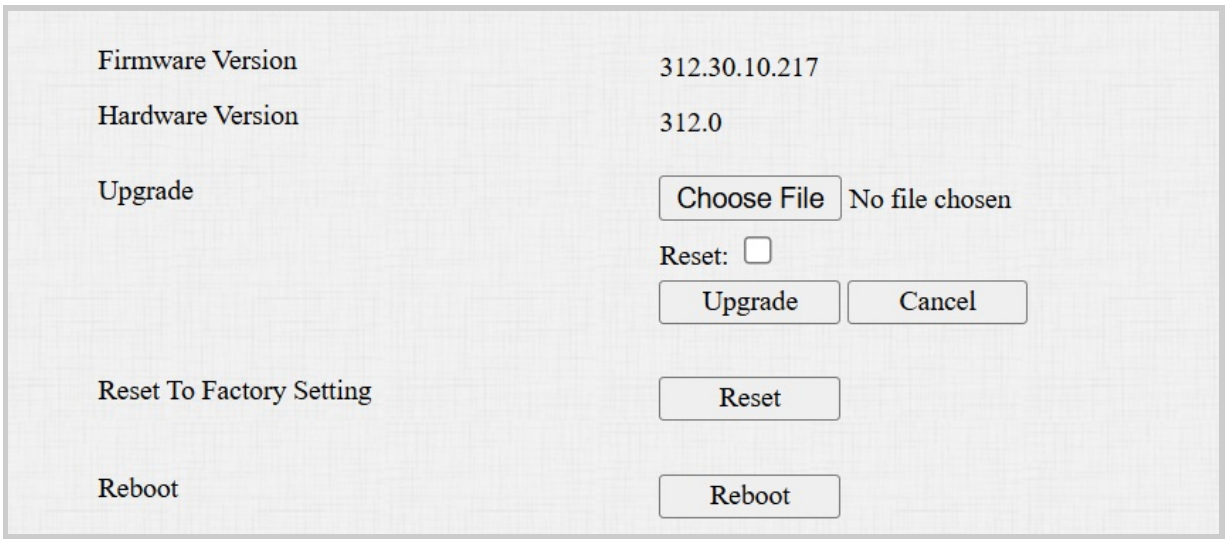



- **Server IP:** Enter the IP address of the controller server.
- **Port:** Enter the port of the controller server.
- **Timeout(Sec):** Decide the time limit within which users should press the lift button of their desired floors.

# Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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




**Note**

- The upgrade files should be in .rom format.
- Click **here** to download the latest firmware and check new features.

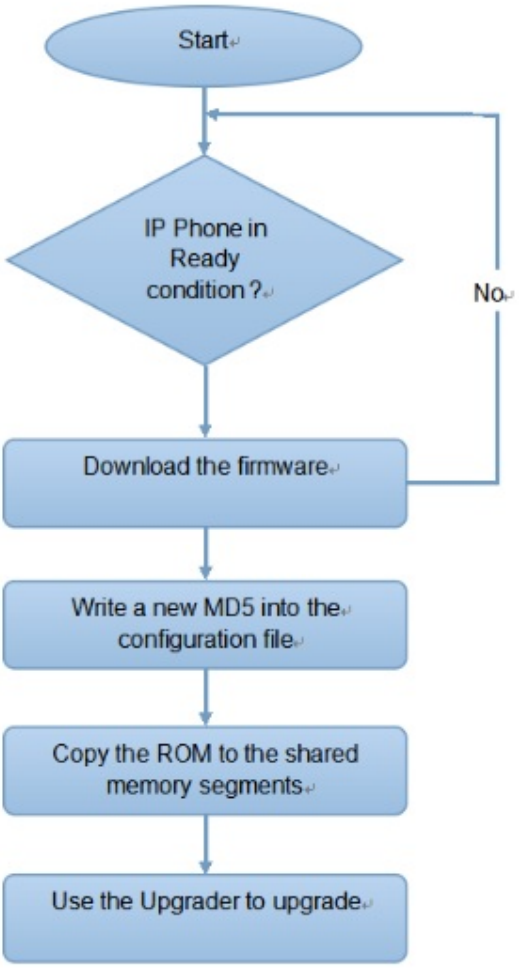
# Auto-provisioning via Configuration File

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

## Provisioning Principle

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

**Please see the flow chart below:**




## Configuration Files for Auto-provisioning

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

**Differences**:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

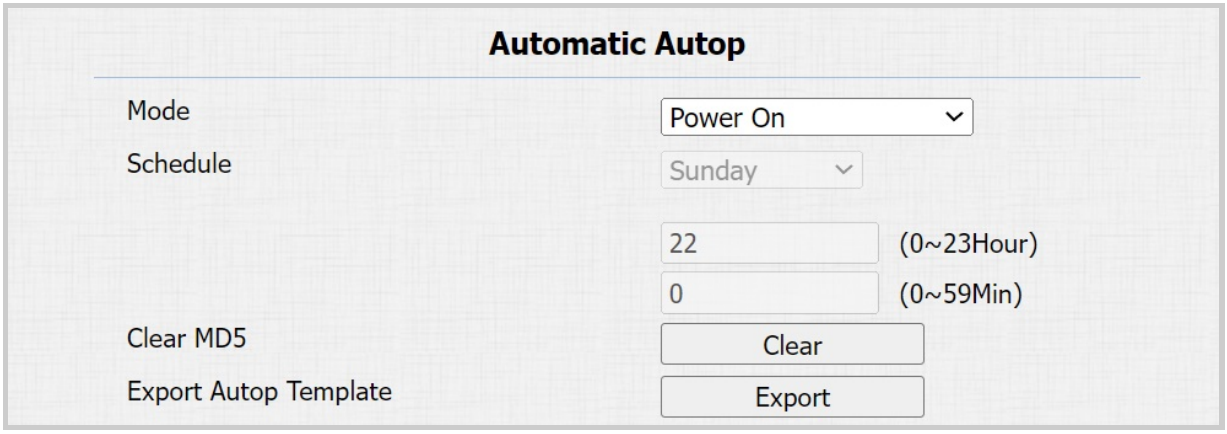
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

## AutoP Schedule

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

To set it up, go to **System > Auto Provisioning > Automatic AutoP** interface.



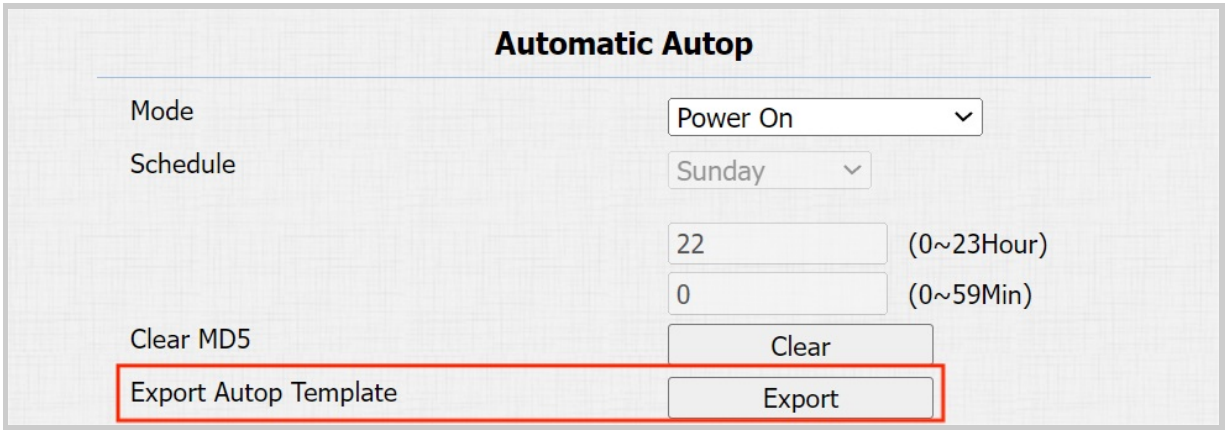

- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.

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

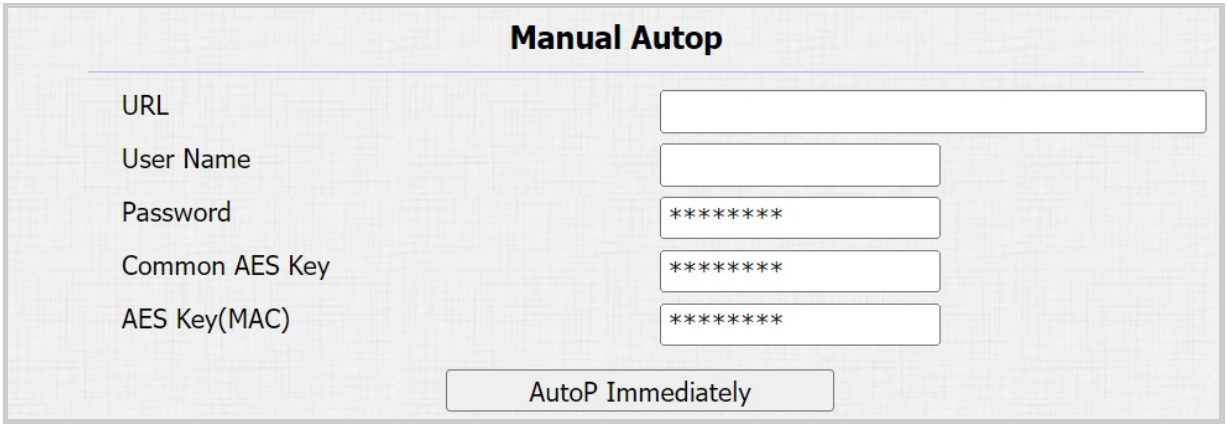
## Static Provisioning

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

To set it up, download the template on **System > Auto Provisioning > Automatic AutoP** interface first.




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



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

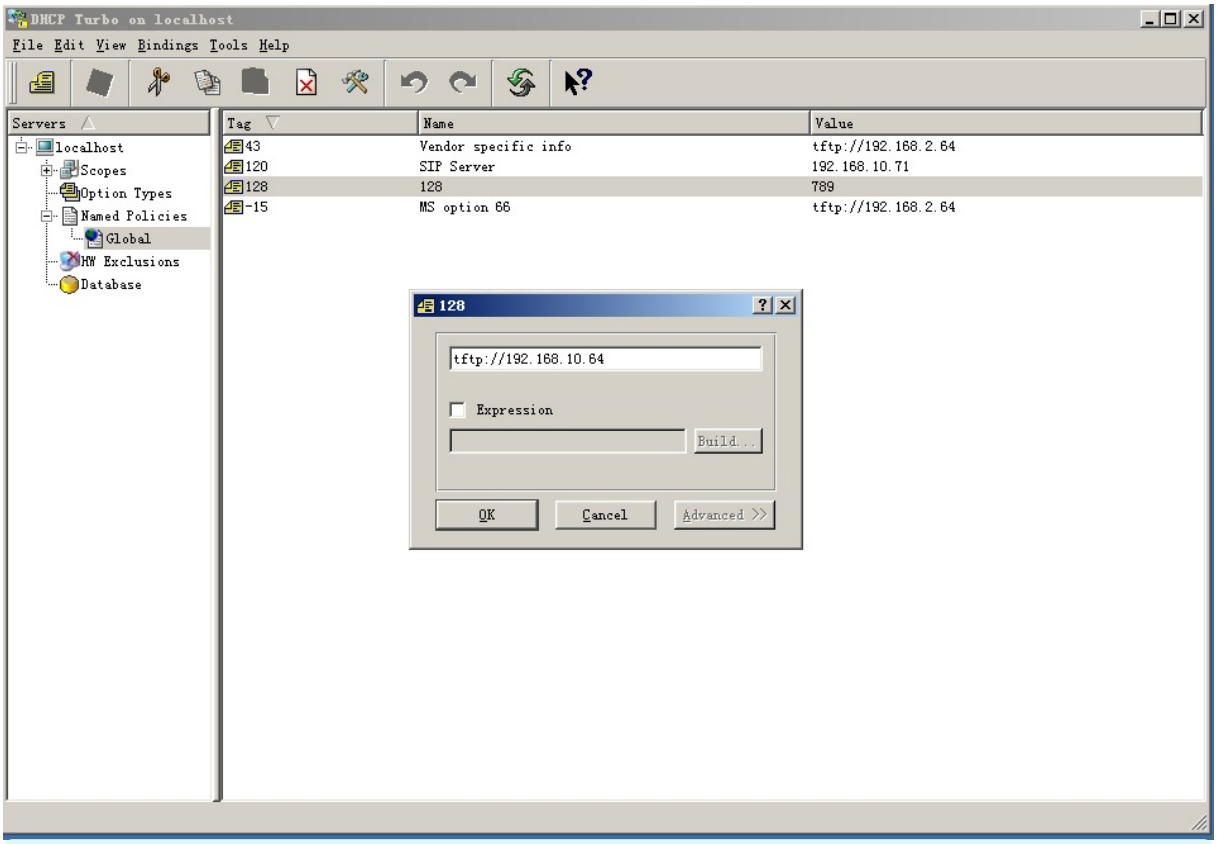
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

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 **CustomOption**as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.

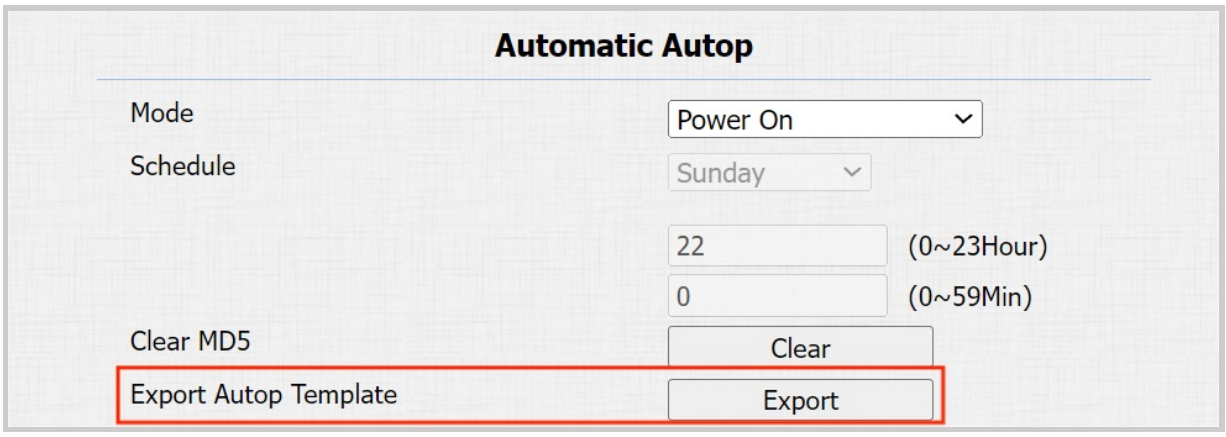



Note

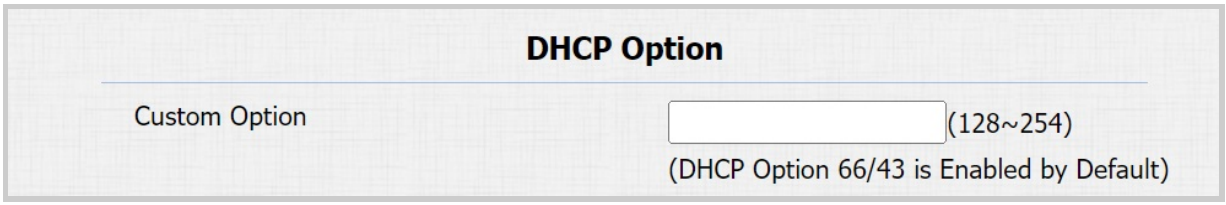
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

Go to **System > Auto Provisioning > Automatic AutoP** interface.




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



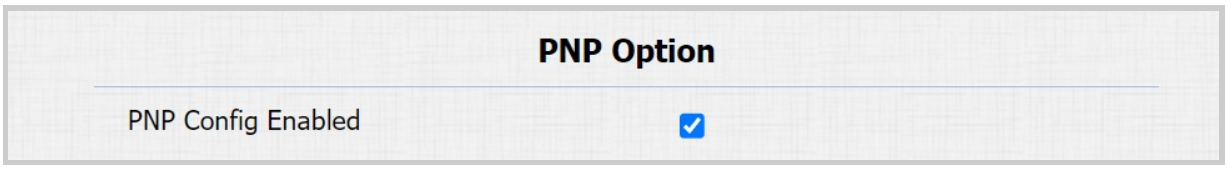

- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done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

# PNP Configuration

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

Click here to watch the configuration video.

Set it up on the web **System > Auto Provisioning > PNP Option** interface.

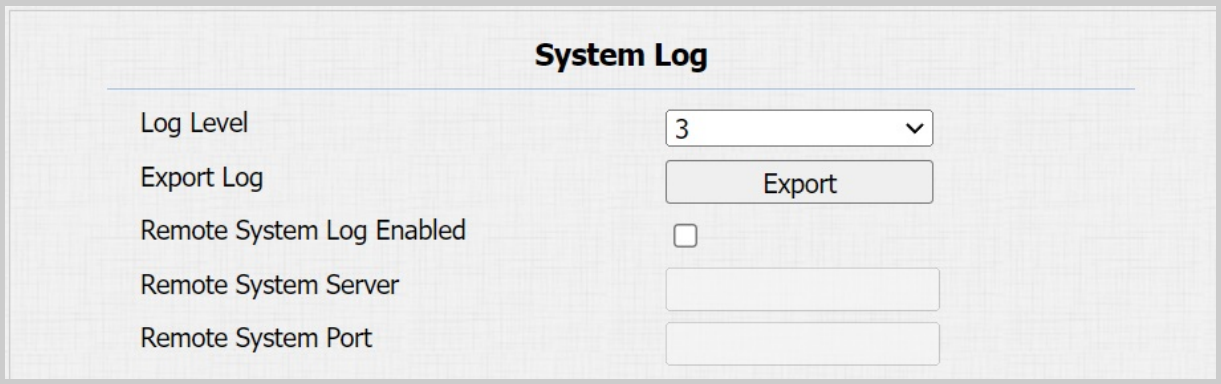

PNP Option
PNP Config Enabled

# Debug

## System Log

System logs can be used for debugging purposes.

To set it up, navigate to the web **System > Maintenance** interface.

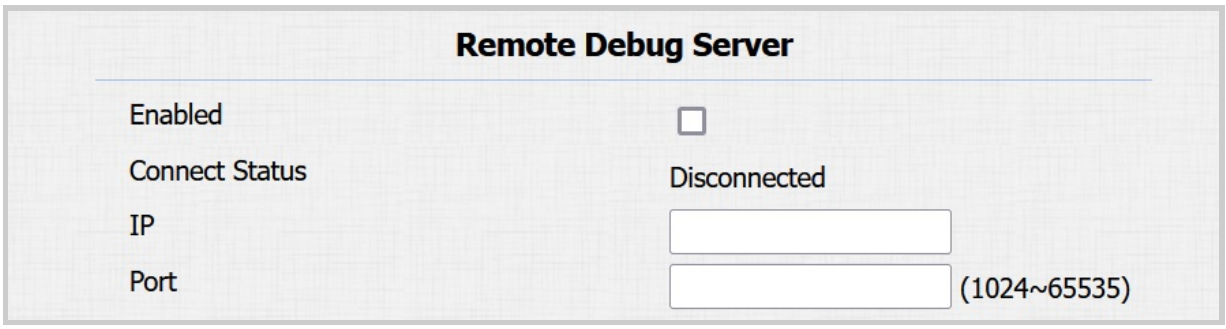



- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export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

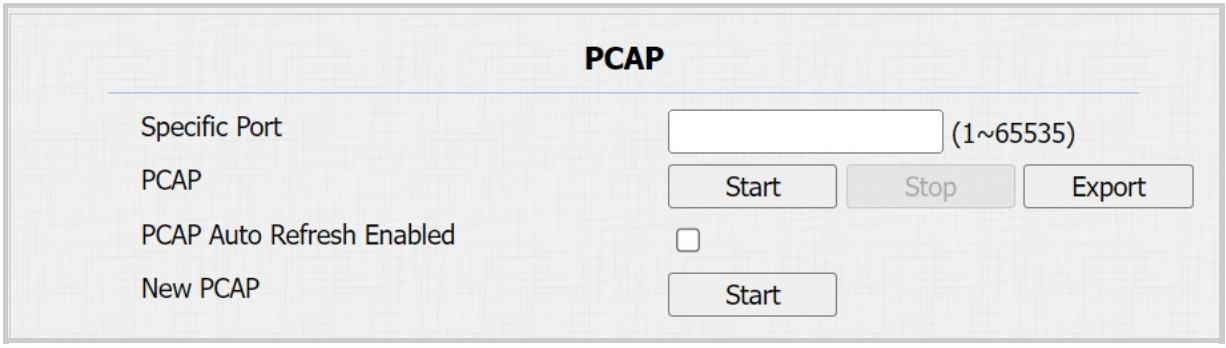



- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.
- **Port**: Enter the port of the server.

## PCAP

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

Set up the PCAP on the web **System > Maintenance** interface.

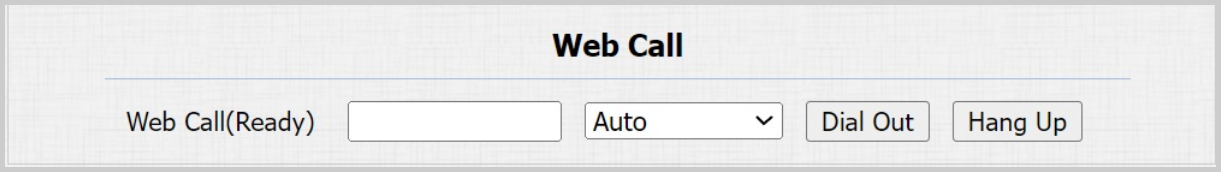



- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the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

# Web Call

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

Make a web call on **System > Maintenance > Web Call** interface.

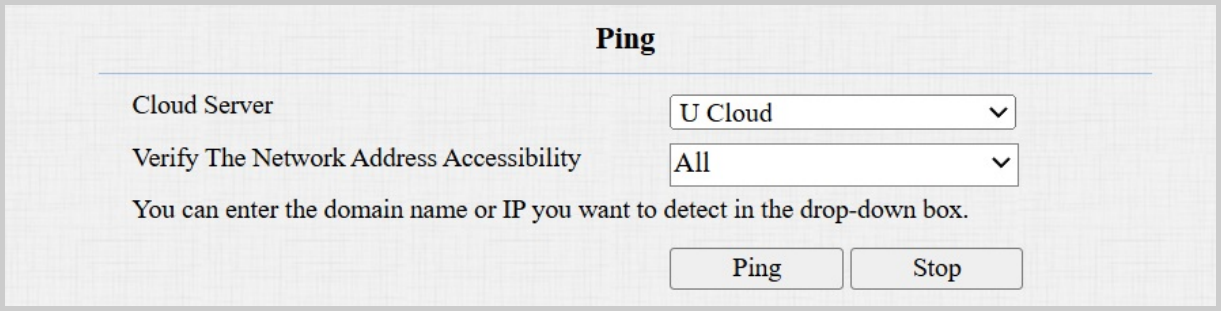



- **Web Call(Ready):** Enter the target IP/SIP number and select the account to dial out.

# Ping

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

To set it up, go to the **System > Maintenance > Ping** interface. Click **Ping** to start the detection, and the results will display on the web.

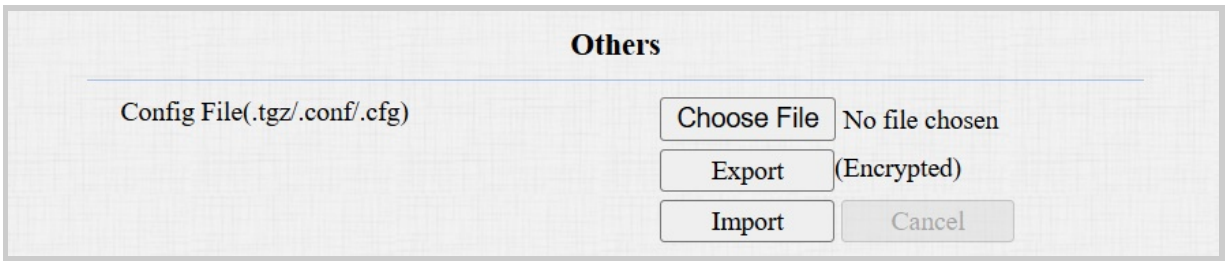



- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

# Backup

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

Export the file on the **System > Maintenance** interface



# Password Modification

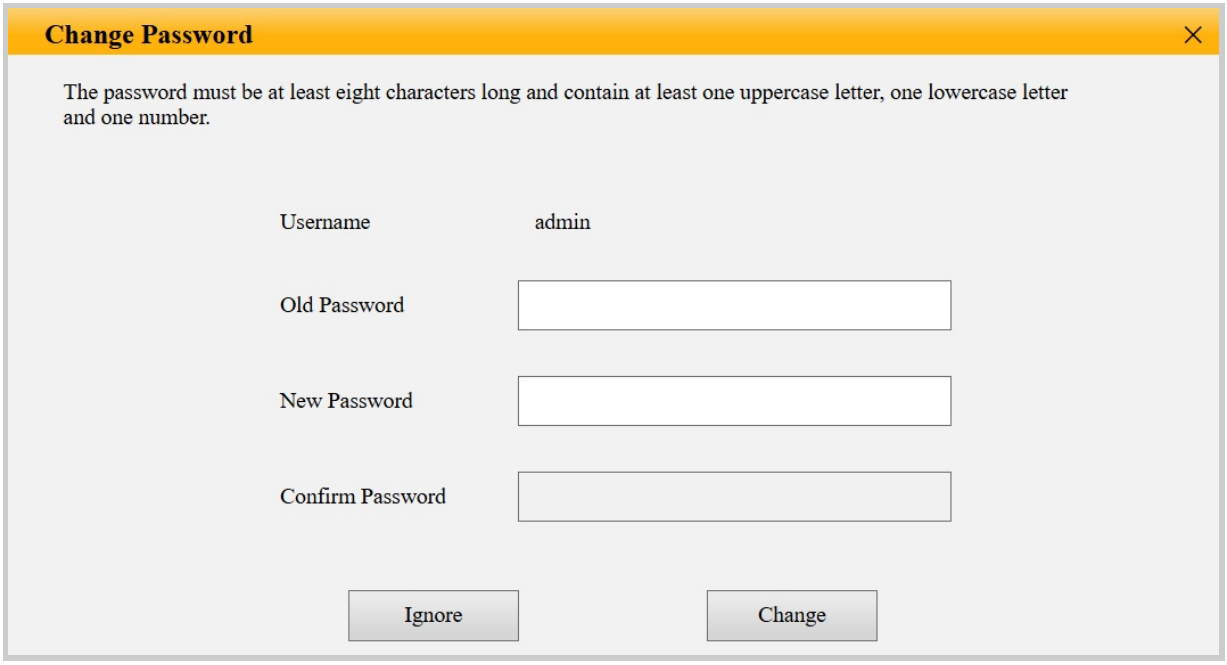
## Modify Web Password

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

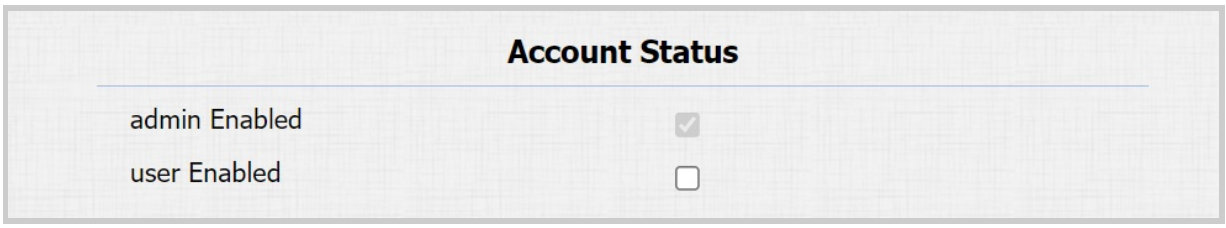
To set it up, go to **System > Security > Web Password Modify** interface.




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




To enable or disable the user account, scroll to the **Account Status** section. The default password for the user account is **user**.




# Modify Security Questions

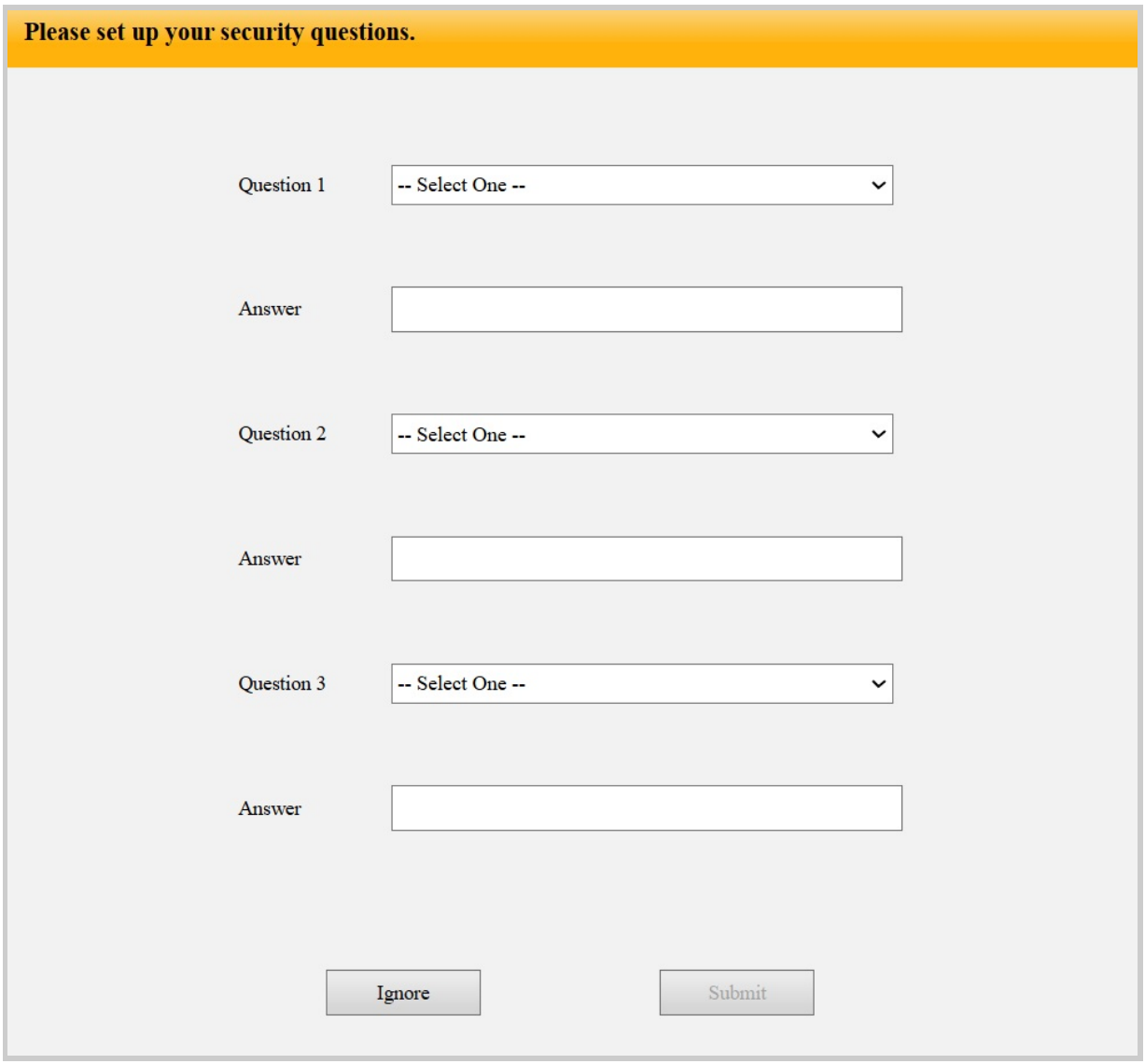
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

Set it up on the **System > Security** interface.




You need to enter the right password for verification and then set up the security questions.

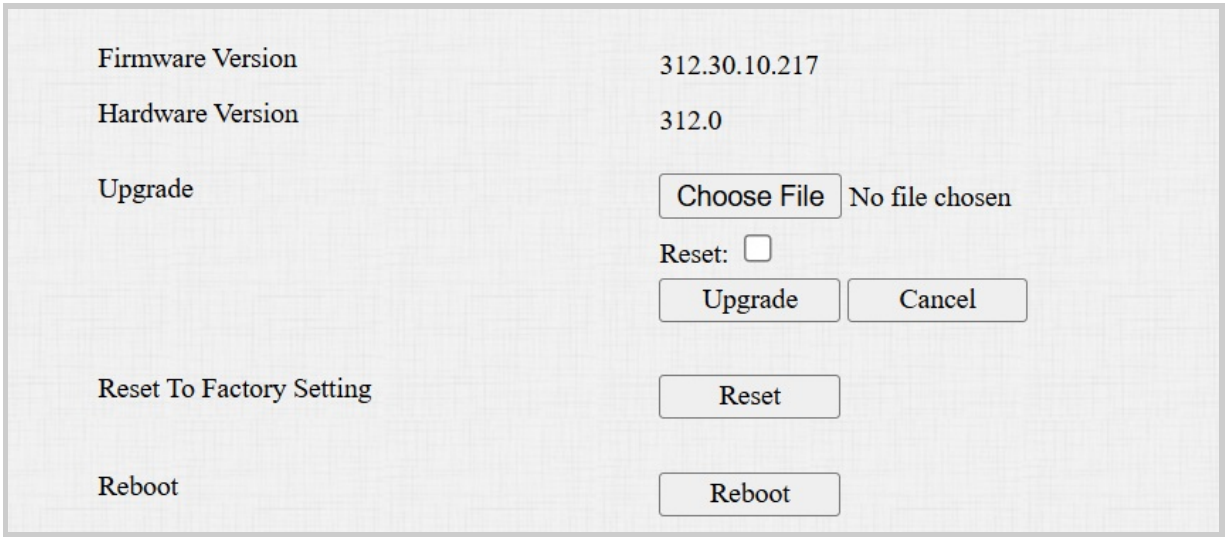

Please set up your security questions.
Question 1
-- Select One --
Answer
Question 2
-- Select One --
Answer
Question 3
-- Select One --
Answer
Ignore
Submit

# System Reboot&Reset

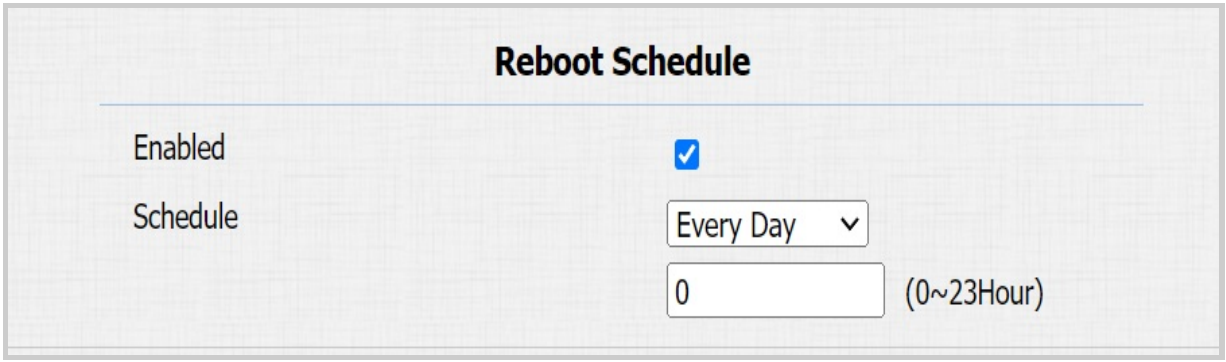
## Reboot

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 **System > Upgrade** interface.

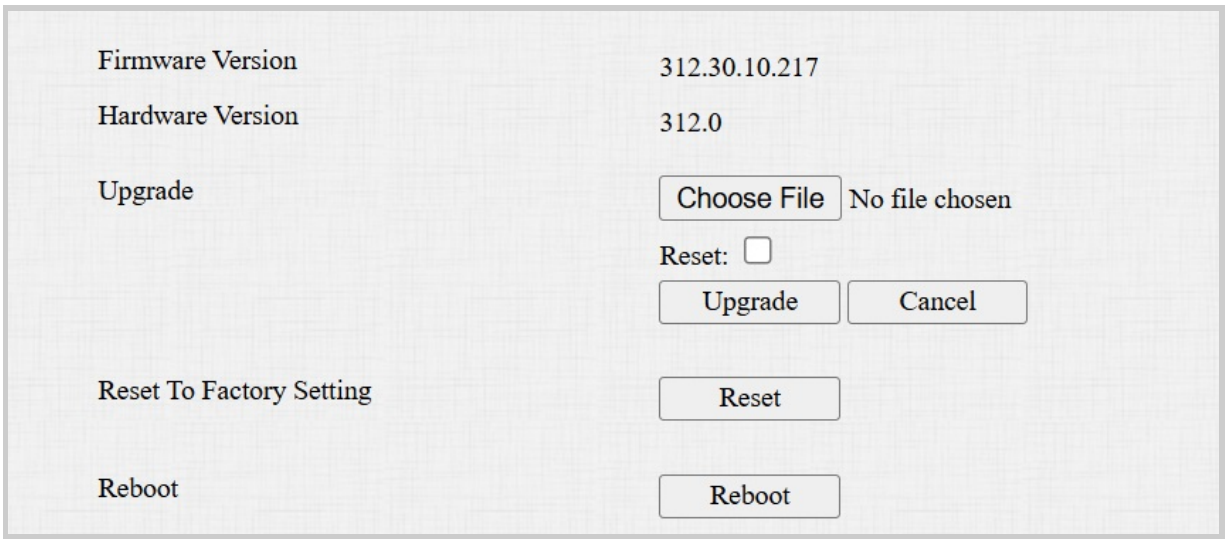



To set up the schedule, go to the **System > Auto Provisioning** interface.




## Reset

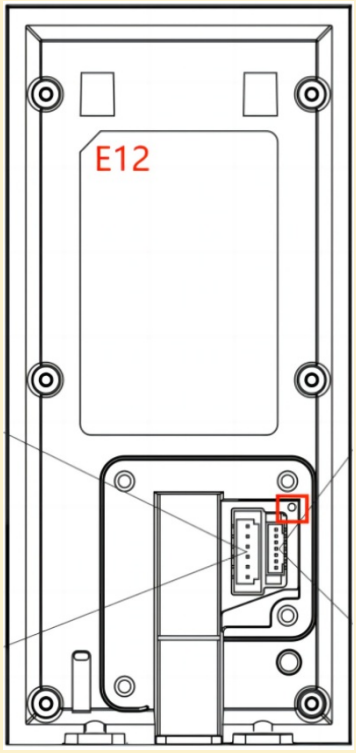
Reset the device on the web **System > Upgrade** interface.




**Tip**

The device can be reset by a physical button.

1. Remove the back cover of the device and power it on.
2. Insert a PIN into the hole and hold it the reset button for about 10 seconds.
   The LED light, fill light, and card reader's light will all light up, and the device goes into factory reset and reboot. After rebooting, the LED light remains blue.




Powered by Document360