Table of contents

Akuvox R28 Series Door Phone Administrator Guide

About This Manual 6
Product Overview 8
Changelog 9
Model Specification 10
  Supported Card Types 10
Access the Device 12
  Obtain Device IP Address 12
  Access the Device Settings 12
  Access Device's Web Settings 12
Introduction to Configuration Menu 14
  Introduction to Quick Start Module 15
Language and Time 18
  Language 18
    Custom Language 18
  Time 19
Volume and Tone 21
  Volume Control 21
  Door-opening Tones 21
    Open Door Outside Tone Setting 22
    Open Door Inside Tone Setting 22
  Ringback Tone Setting 23
  Upload Tones 24
  Open Door Tone Mode 25
Screen Display and LED Settings 26
  Infrared LED Setting 26
  LED Wakeup Mode 26
  Card Reader LED Control 27
  Keypad LED Control 27
  LED Settings on Screen 28
  Backlight Setting 28
  Screensaver Setting 29
    Upload Screensavers 30
  Homepage Display 30
  LCD Display 31
  Key Code Exchange 32

Network Setting 33
Network Status 33
Device Network Configuration 33
Device Deployment in Network 34
Device Local RTP Configuration 36
NAT Setting 36
SNMP Setting 37
VLAN Setting 37
TR069 Setting 38
Device Web HTTP Setting 39
Intercom Call Configuration 41
IP Call Configuration 41
Make IP Calls 41
IP Call Setup 41
SIP Call Configuration 41
SIP Account Registration 42
SIP Server Configuration 43
Outbound Proxy Server 43
Data Transmission Type 44
SIP Hacking Prevention 44
Call Settings 46
Do Not Disturb 46
Call Auto-answer 46
Group Call 47
Sequence Call 48
Multicast 49
Maximum Dial Duration 50
Maximum Call Duration 52
Hang up After Open Door 52
Dial Plan 53
Actions Triggered by Calling 54
Audio and Video Codec Configuration 56
Audio Codec 56
Video Codec 57
Video Codec for Direct IP Calls 57
Contacts Management 59
Manage Contact Group 59
Manage Contacts 60
Add Contacts 60
Export/Import Contacts 60

Contact List Display 61
Relay Setting 63
Local Relay 63
Security Relay 64
Web Relay 66
Access Control Schedule Management 69
Create a Door Access Schedule 69
Import and Export Door Access Schedule 70
Relay Schedule 71
Holiday Schedule 73
Holiday Schedule Import/Export 74
Door-opening Configuration 76
Unlock by Public PIN Code 76
User-specific Access Methods 76
Unlock by Private PIN Code 77
Unlock by RF Card 78
Unlock by License Plate 80
Access Setting 80
Import/Export User Data 82
Send Card Numbers to Third-Party Servers 82
Mifare Card Encryption 83
Unlock by NFC 84
Unlock by HTTP Command 84
Unlock by DTMF Code 85
DTMF White List 86
DTMF Data Transmission 87
Unlock by Exit Button 89
Monitor and Image 91
MJPEG Video Stream 91
MJPEG Authorization 92
RTSP Stream Monitoring 93
RTSP Basic Setting 94
H.264 Video Parameters Setup 95
RTSP OSD Setting 95
NACK 96
ONVIF 96
Live Stream 97
Camera Mode 98
Data Transmission Type for Third-party Camera 99
Security 101

Tamper Alarm 101
Client Certificate Setting 101
Web Server Certificate 101
Client Certificate 102
Upload TLS Certificate for SIP Account Registration 103
Motion Detection 104
Motion Detection Schedule 105
Security Notification 105
Email Notification 106
FTP Notification 106
SIP Call Notification 107
Action URL 107
Whitelist Of Make Call Action 109
Voice Encryption 110
User Agent 110
Web Interface Automatic Log-out 111
High Security Mode 111
Real-time Monitoring 112
Emergency Action 113
Logs 114
Call Logs 114
Door Logs 114
Event Logs 115
Integration with Third-party Devices 117
Integration via Wiegand 117
Integration via HTTP API 120
Power Output Control 121
Lift Control 122
Akuvox Lift Controller 122
KeyKing Lift Controller 123
ZKT Lift Controller 124
Firmware Upgrade 125
Auto-provisioning 126
Provisioning Principle 126
Configuration Files for Auto-provisioning 127
AutoP Schedule 128
Static Provisioning 129
PNP Configuration 130
DHCP Provisioning 131
Debug 133

System Log 133
Remote Debug Server 133
PCAP for Debugging 134
Web Call 135
Ping 135
Backup 136
Password Modification 137
Modify Web Interface Password 137
Modify System Password 138
Modify Service Password 138
Modify Security Questions 139
System Reboot&Reset 141
Reboot 141
Reset 141

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

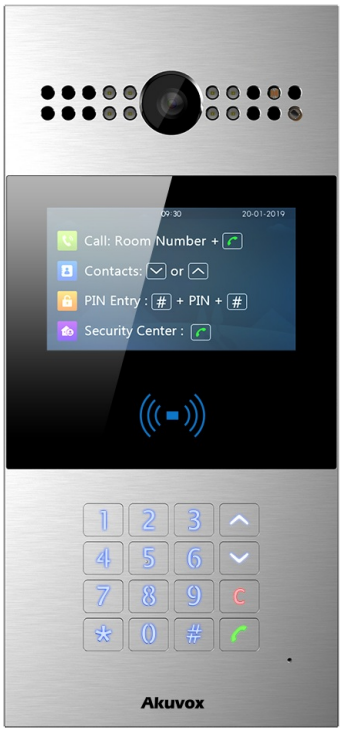


AKUVOX R28 SERIES DOOR PHONE

Administrator Guide

Thank you for choosing the Akuvox R28 series door phones. This manual is intended for administrators who need to properly configure the door phone. This manual is based on the 228.30.11.17 version and provides all the necessary configurations for the functions and features of the Akuvox door phone. Please visit the Akuvox website or consult technical support for any new information or the latest firmware.

Product Overview



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

Changelog

What's new in version 228.30.11.17:

The following new features require the device's connection to the SmartPlus Cloud.

- Support the Elevator Control feature.
- Support the Parking Restrictions feature.
- Support reporting access failure reasons to the cloud.
- Support the optimized event report.
- Support displaying snapshots from third-party cameras in the Door Log when linked to the device.

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

Model Specification

Model	R28A
Camera	2 Megapixels, automatic lighting
Light Sensor	✔
Motion Sensor	✔
Wiegand Port	✔
Relay In	x3
Relay Out	x3
RS485	✔
Card Reader	13.56MHz & 125kHz, NFC
Microphone	x1
Speaker	x1
Power Out	12V/400mA(Max.)
Tamper Alarm	✔
Power Supply	802.3af Power-over-Ethernet or 12V power adapter

Supported Card Types

The device's firmware should be 228.30.10.127 or higher:

- ID Card:
  - EM4100
  - EM4200
- IC Card:

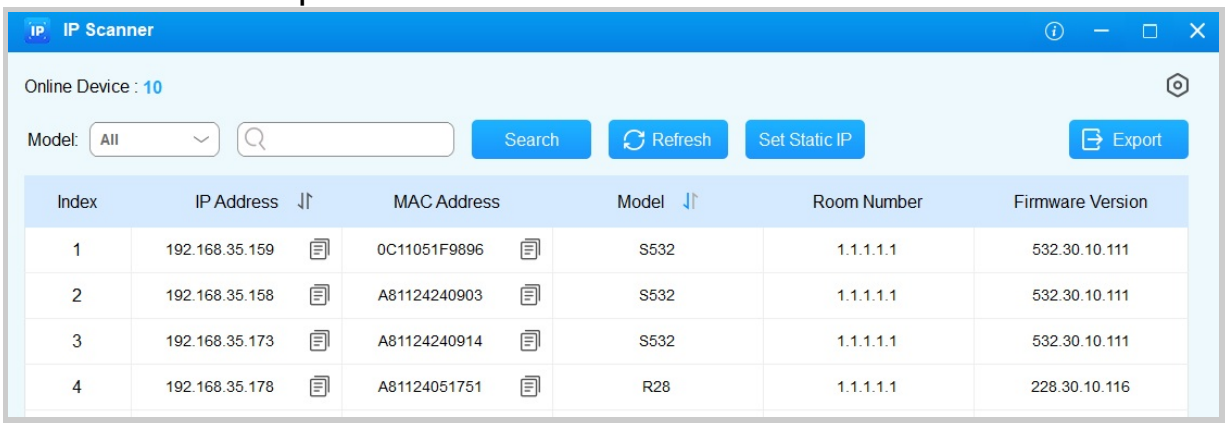
    - Mifare Ultralight C/EV1
    - Mifare Classic Compatible Card
    - Mifare Plus-S 2K
    - Mifare Desfire EV1 2K D21
    - Mifare Desfire EV2 D42
    - Mifare Desfire EV2 D22
    - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
    - NFC Type2 216
    - NFC Type2 215
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- 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

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

Obtain Device IP Address

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



Access the Device Settings

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

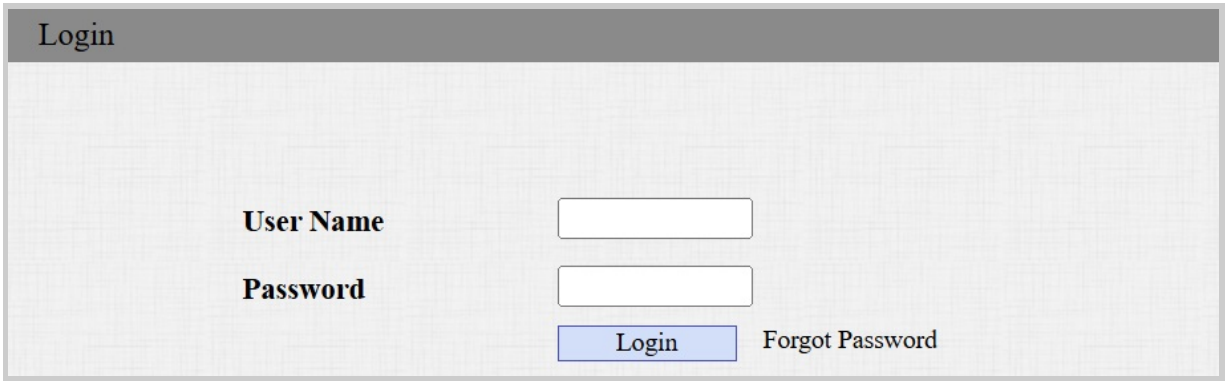
- system information;
- admin password and admin card management;
- system network settings;
- system reset.

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

Access Device’s Web Settings

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

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

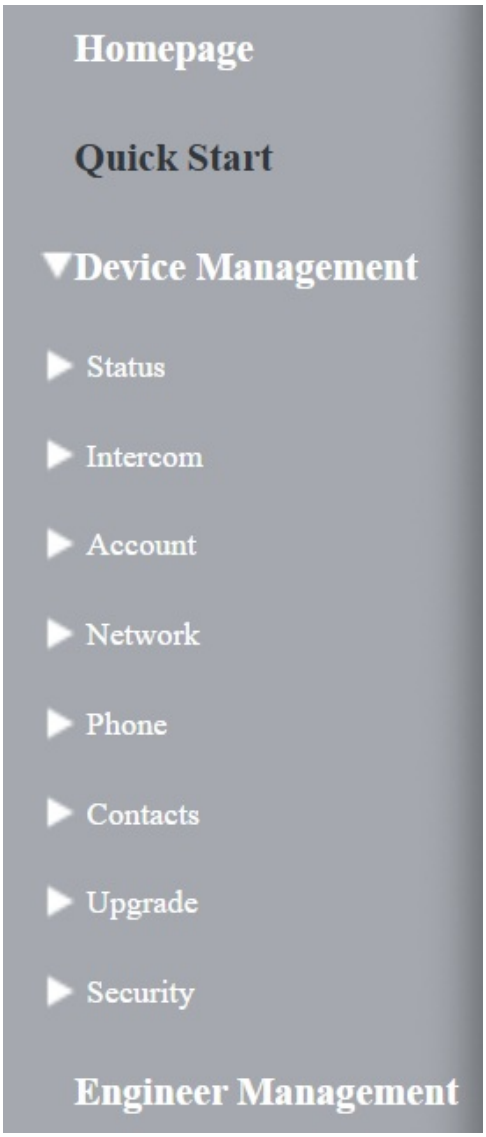


Note

- Download the IP Scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- Your computer should be on the same network as the device.

Introduction to Configuration Menu

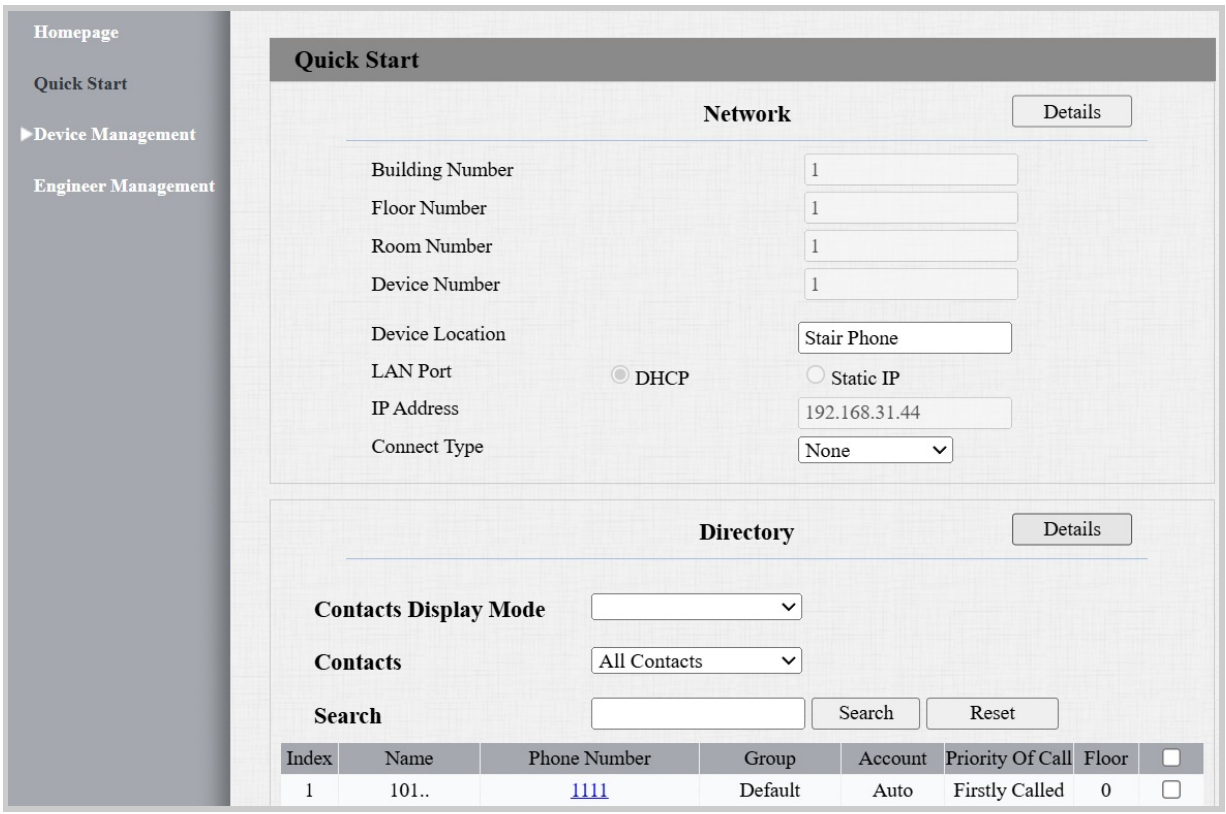
- **Quick Start**: This section provides quick access to the device's key settings, such as network, user, relay, etc.
- **Device Management**:
    - **Status**: This section gives you basic information, such as product information, network information, account information, etc.
    - **Intercom**: This section includes basic call settings, user management, access methods, video streams setup, 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.
    - **Phone**: This section includes time and language selection, volumes and tones configuration, logs, etc.
    - **Contacts**: This section is for contacts management.
    - **Upgrade**: This section is for upgrading the device firmware.
    - **Security**: This section includes web password modification, device debugging, maintenance, etc.
- **Engineer Management**: This section provides quick access to upgrading, maintaining, and debugging the device.



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*] in the Self-organizing Network Solution.
  - **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 local contacts. Click **Add** to add a new contact after filling in its information.
  - **Contact Display Mode**:
    - **All Contacts**: Display all the contacts.
    - **Groups Only**: Display contact groups. Press the desired group on the device screen to make a group call.
    - **Contact Display by Group**: Display contacts by groups. Press the group, and users can see the contacts in it.
- **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 select the device's LCD and web language on the **Phone > Time/Lang** interface.

The device web supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Russian, Portuguese, Spanish, Italian, Dutch, French, German, Vietnamese, Polish, Turkish, Japanese, Czech, Norwegian, Montenegrin, Ukrainian, Danish, and Bosnian.

The device LCD supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Russian, Portuguese, Spanish, Italian, Dutch, French, German, Hebrew, Polish, Turkish, Japanese, Czech, Norwegian, Montenegrin, Ukrainian, Danish, Bosnian, Vietnamese, and Arabic.



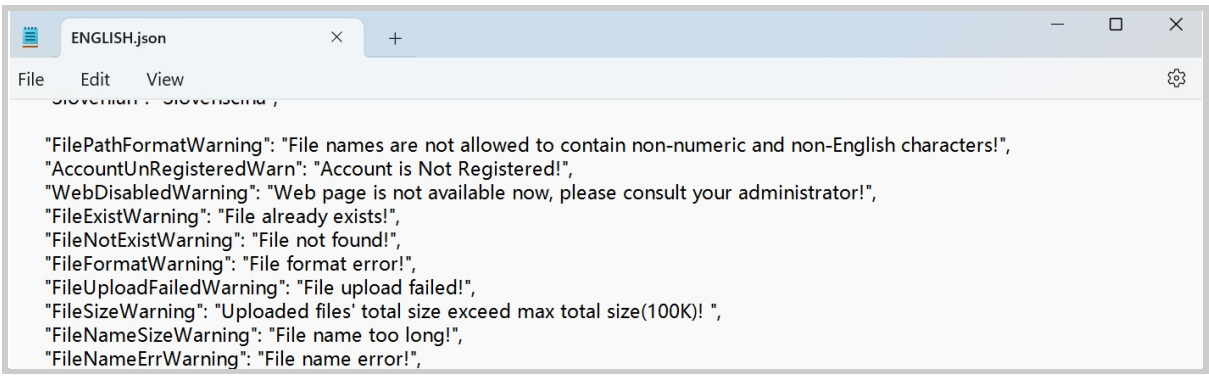
Custom Language

You can customize the configuration names and prompt texts on the device and its web portal such as the file name error warning.

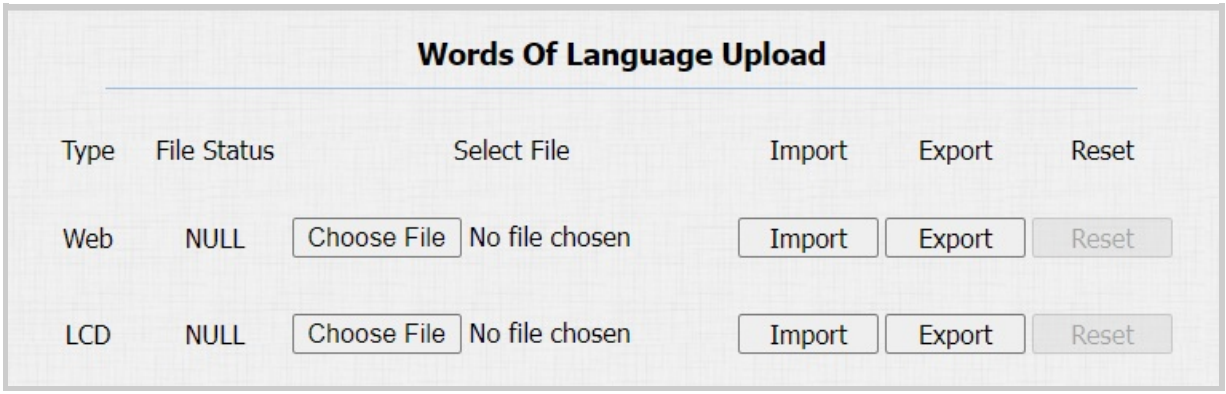
Export the .json file for editing. You may edit it with the notepad on your computer.

Import the .json file and its size should be smaller than 1 MB.

File Example:



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



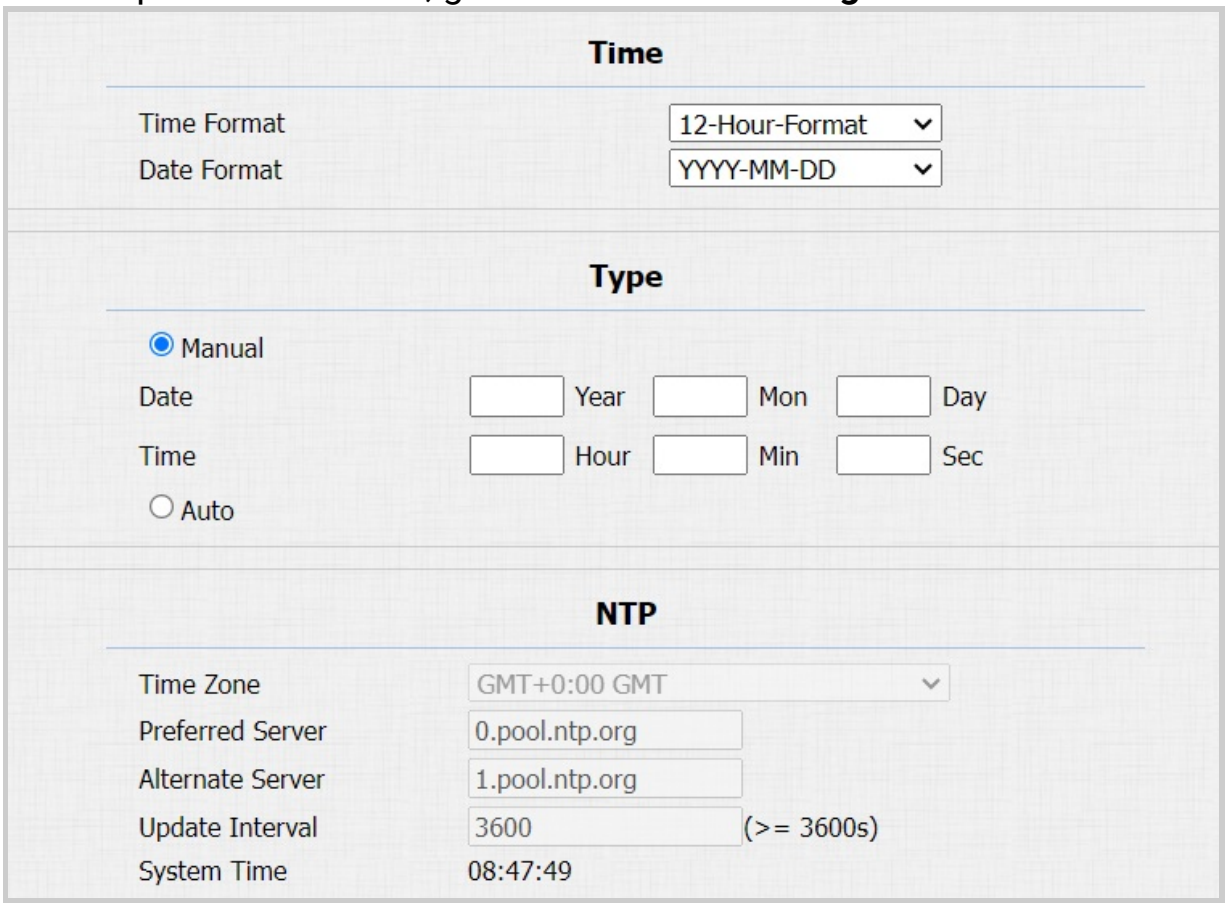
Note

- The uploaded file for customizing web language should be in .json format.
- The uploaded file for customizing LCD language should be in .xml format.

Time

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

To set up the device time, go to **Phone > Time/Lang> Time**.



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

Tip

You can also change the time directly on the device.

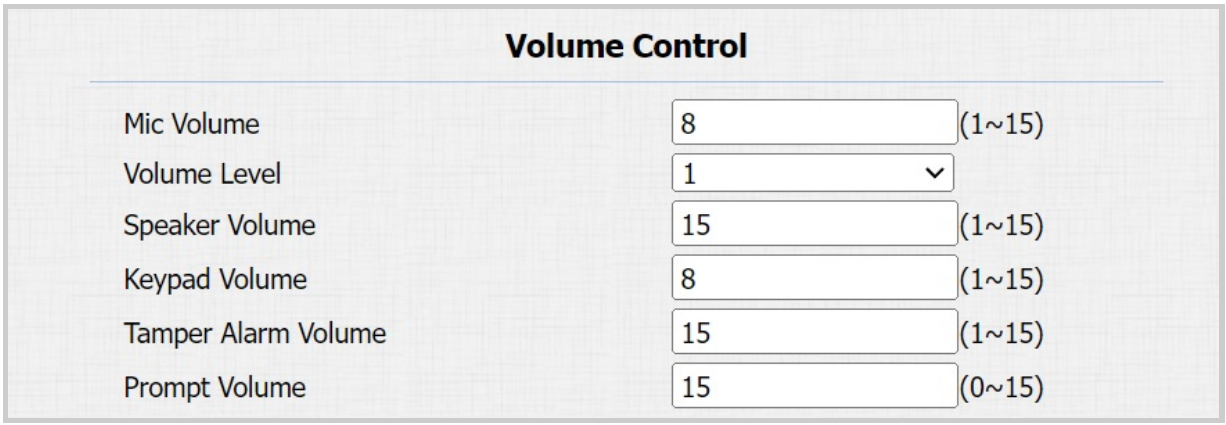
1. Press *2396# to enter **Admin Settings**.
2. Select **System Settings**.
3. Select **Time Setting**.
4. Select **Auto** to automatically set up the time; select **Manual** to input the date and time.

Volume and Tone

Volume and tone configurations include microphone volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone configuration. Moreover, you can upload the tone to enrich the user experience.

Volume Control

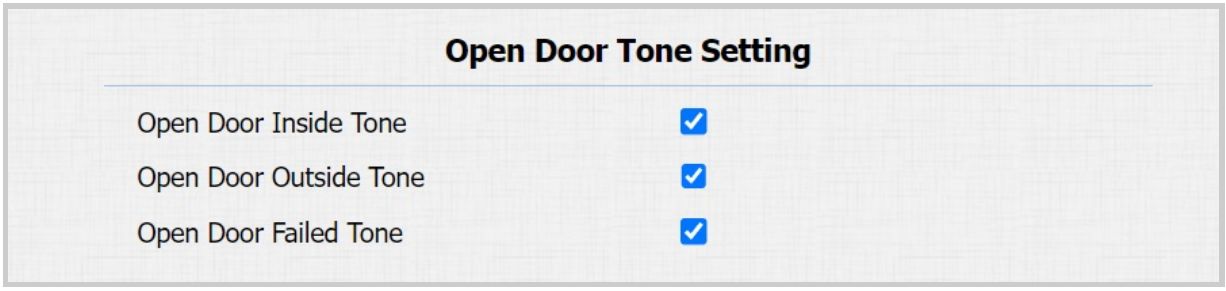
You can set up various volumes on the **Phone > Audio > Volume Control** interface. The default value of all volumes is 8.



- **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.
- **Prompt Volume**: Various prompts, including door-opening success and failure prompts.

Door-opening Tones

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

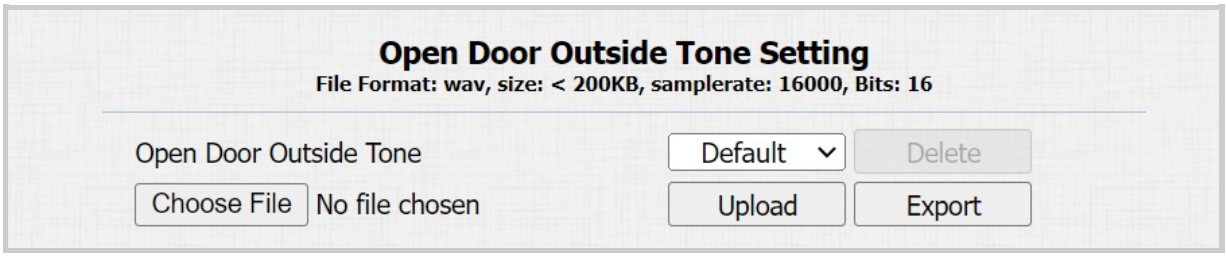


- **Open Door Inside Tone**: The input-triggered tone. The door-opening tone can be heard when users open doors by pressing an exit button.
- **Open Door Outside Tone**: The relay-triggered tone. The door-opening tone can be heard when users open doors by the device-supported access methods, except for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

Open Door Outside Tone Setting

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

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



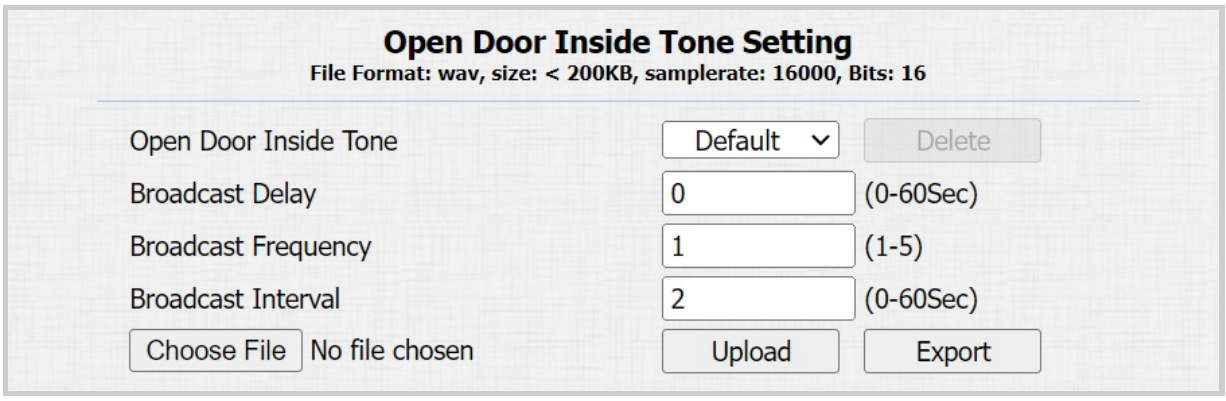
> **Note**
>
> File Format: WAV; Size: <200KB; Sample Rate: 16K; Bit Depth: 16 Bits.

Open Door Inside Tone Setting

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

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

- Click **Export** to download the existing tone.



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

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

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

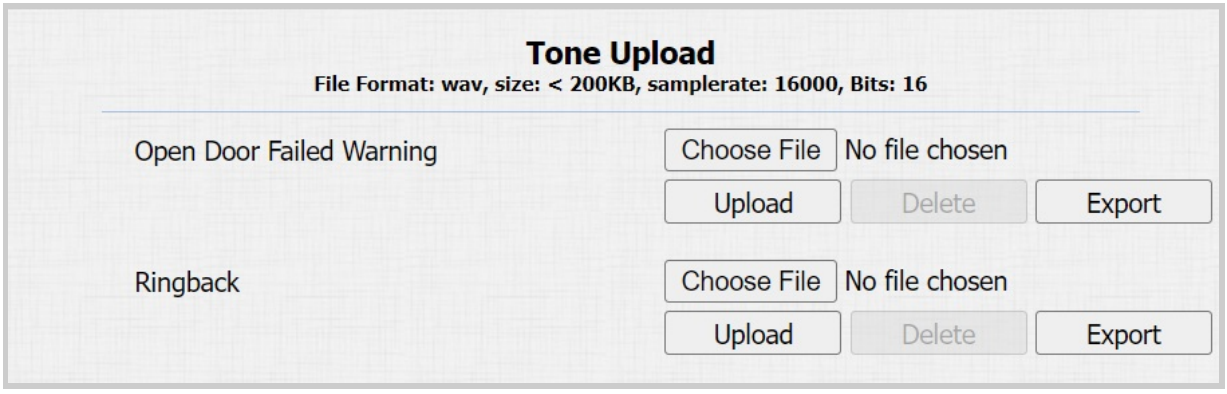
    - If the SIP server returns 183, the indoor monitor will receive the video preview without voice.
- **Local**: The local ringtone will be played. Whether the SIP server returns 183 or not, the callee will not have any intercom preview.
- **Remote:**
    - If the SIP server returns non-183, the local 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.

Upload Tones

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

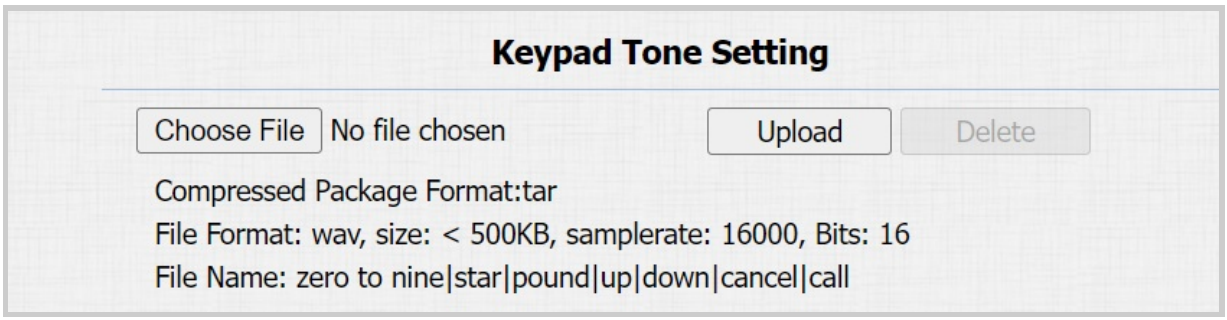
Upload tones on the **Phone > Audio > Tone Upload** interface.

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



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

Upload the keypad tone in the **Keypad Tone Setting** section. You can upload a keypad tone for each key. When pressing any key, the corresponding tone can be heard so that you can distinguish the key from others.



Note

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

Open Door Tone Mode

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



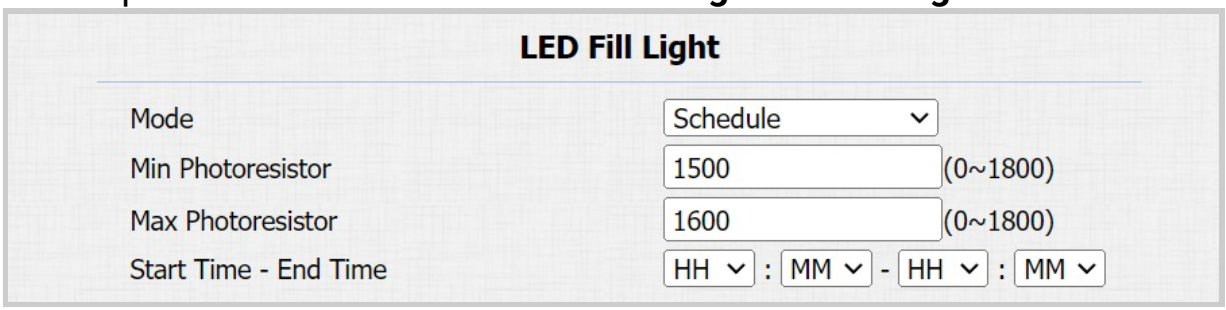
- **Voice Prompt**: Play the default prompt “Welcome, please come in” when the door is opened.
- **Sound Effect**: Play the Beep sound when the door is opened.

Screen Display and LED Settings

Infrared LED Setting

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

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

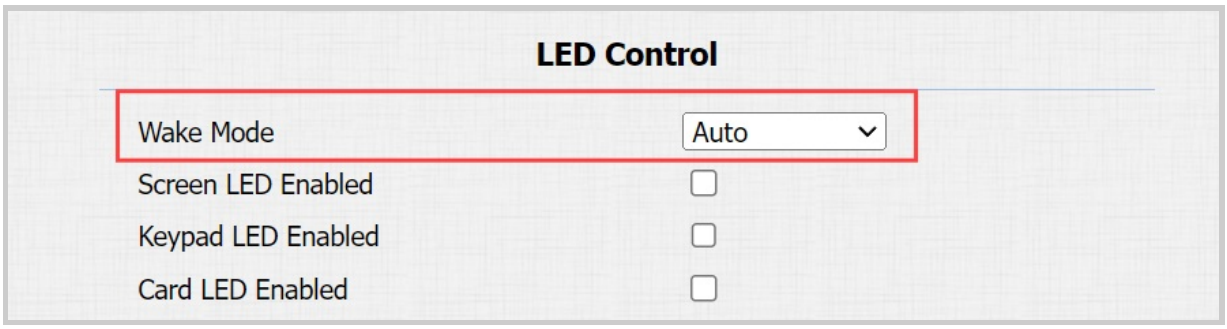


- **Mode**:
  - **Auto**: Turn on the LED light automatically based on the minimum and maximum photoresistor value.
  - **Always On**: Enable the LED light.
  - **Always Off**: Disable the LED light.
  - **Schedule**: Turn on the LED light based on the schedule. Specify the Start Time and End Time when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

LED Wakeup Mode

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

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

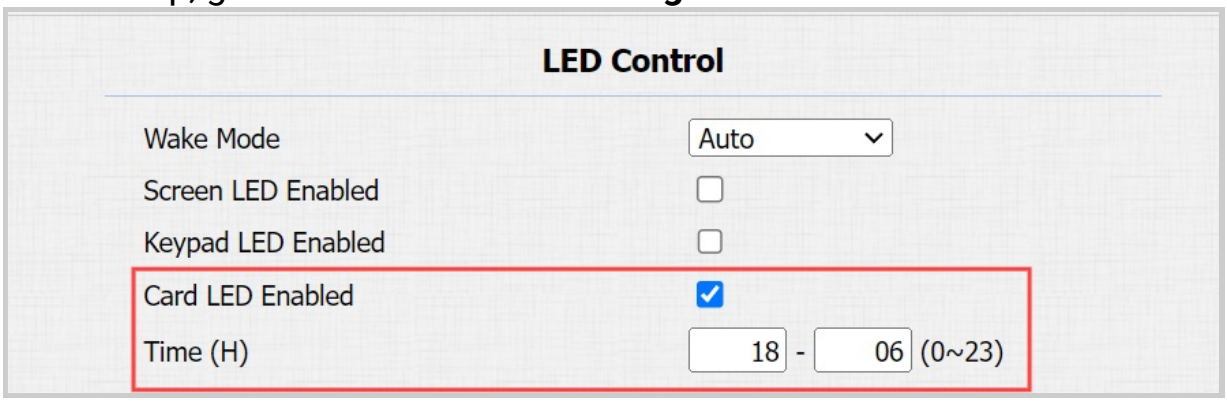


- **Wake Mode**:
  - **Auto**: When the infrared detection is triggered, the card reader light will be on.
  - **Manual**: The LED is not controlled by infrared detection.

Card Reader LED Control

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

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

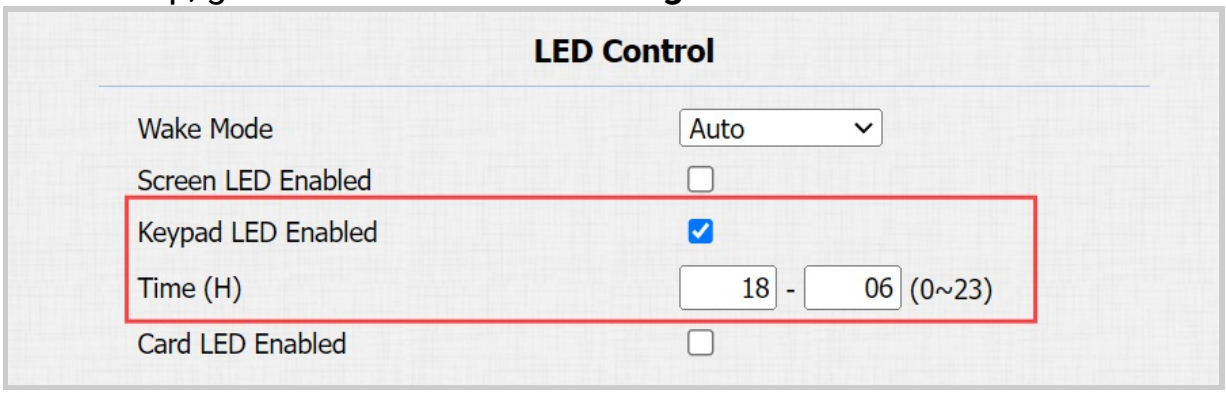


- **Card LED Enabled**: When enabled, specify the period when the light is on.

Keypad LED Control

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

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

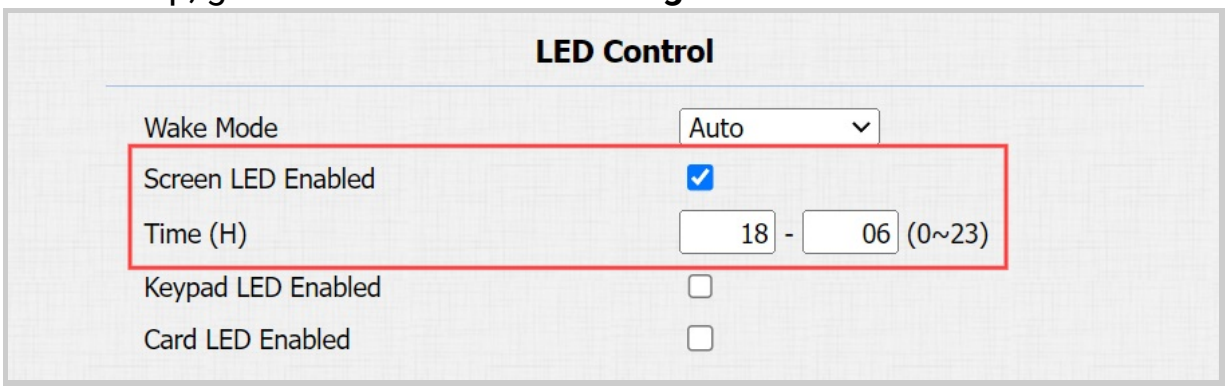


- **Keypad LED Enabled**: When enabled, specify the period when the light is on.

LED Settings on Screen

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

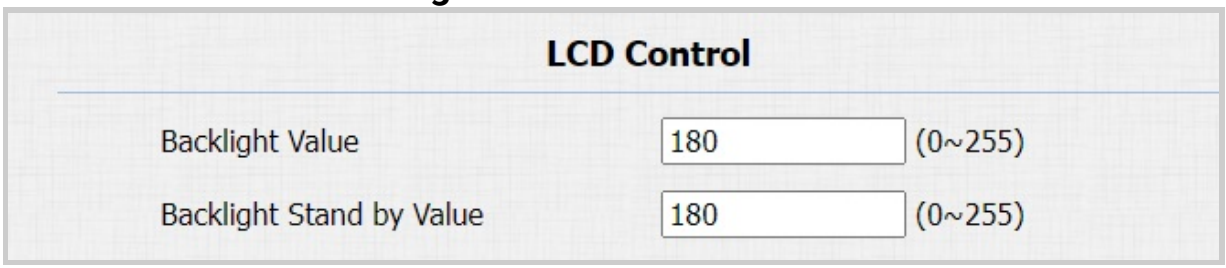
To set it up, go to **Intercom > LED Setting > LED Control**.



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

Backlight Setting

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

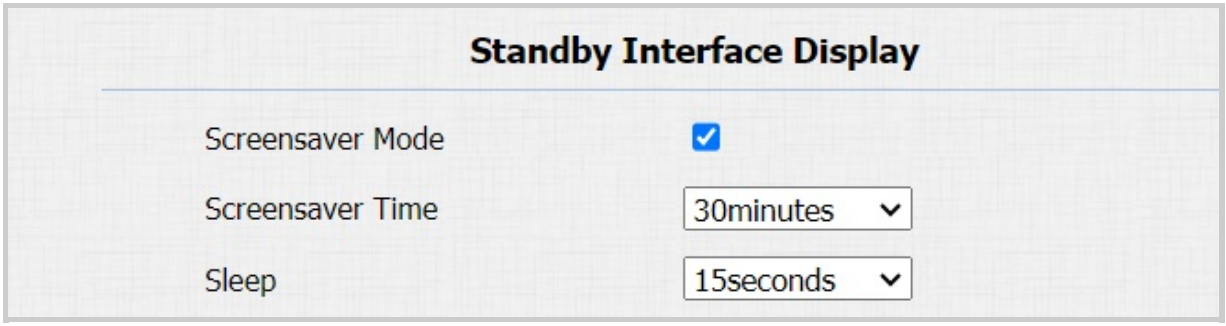


- **Backlight Value**: Set the backlight value when the device is working from 0-255.
- **Backlight Standby Value**: Adjust the backlight for the screen in standby mode from 0-255.

Screensaver Setting

You can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction.

To set it up, go to **Intercom > LED Setting > Standby Interface Display** interface.



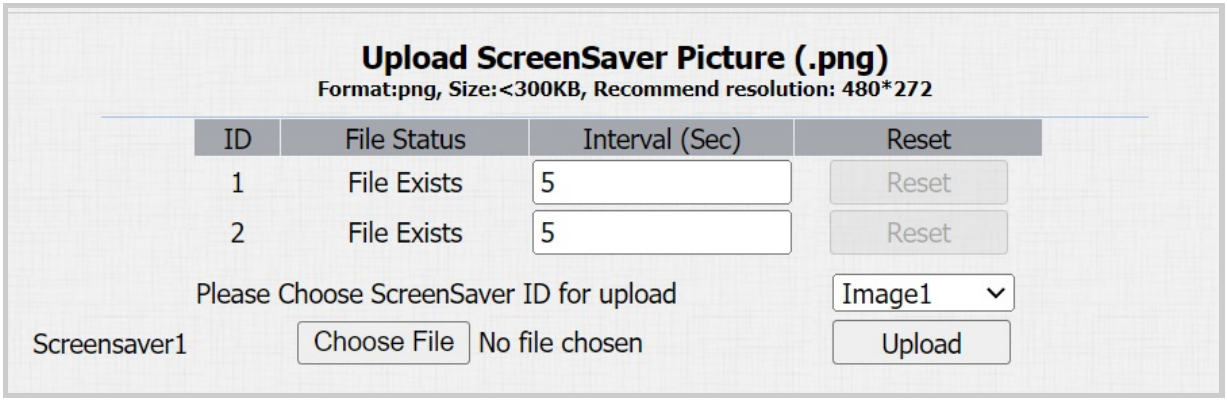
- **Screensaver Mode:** Enable or disable the use of the screensaver. If disabled, the device screen will directly turn dark when it is in standby mode.
- **Screensaver Time**: Set the screen saver duration time(5 seconds to 2 hours).
- **Sleep**: The time to start the screen saver mode(5 seconds to 30 minutes). For example, if it is set to 15 seconds, the device will go into screen saver mode when the device detects no operation or no approaching object for 15 consecutive seconds. When screen saver mode is disabled, the device screen will be turned off directly in 15 seconds.

Upload Screensavers

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

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

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



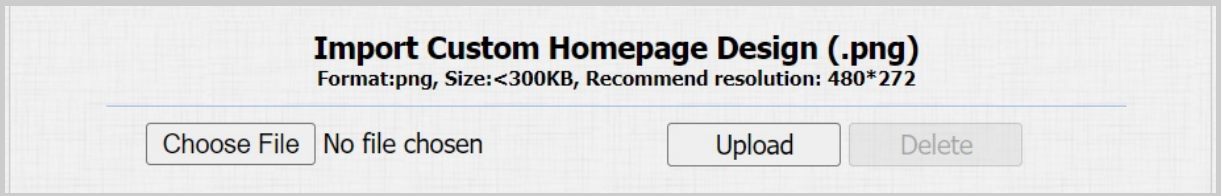
Note

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

Homepage Display

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

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

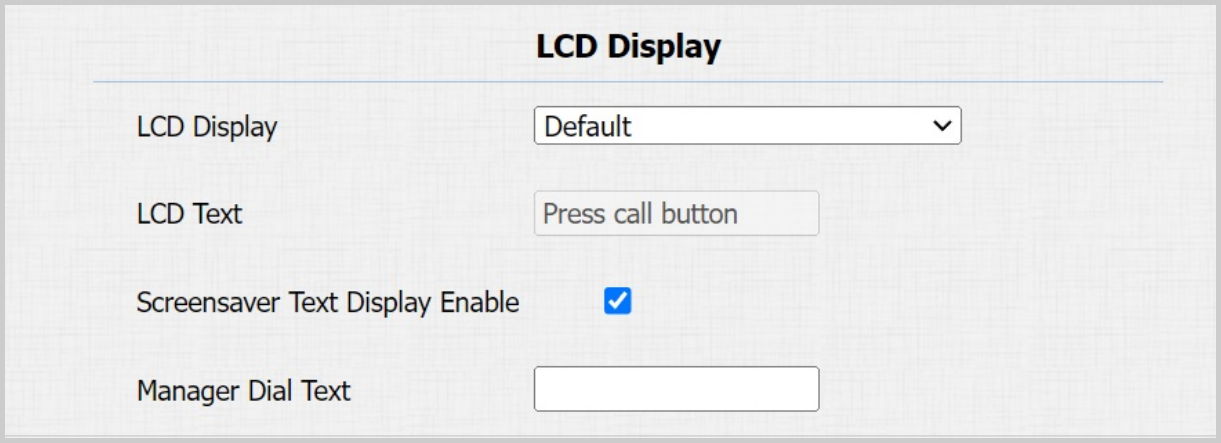


Note

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

LCD Display

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



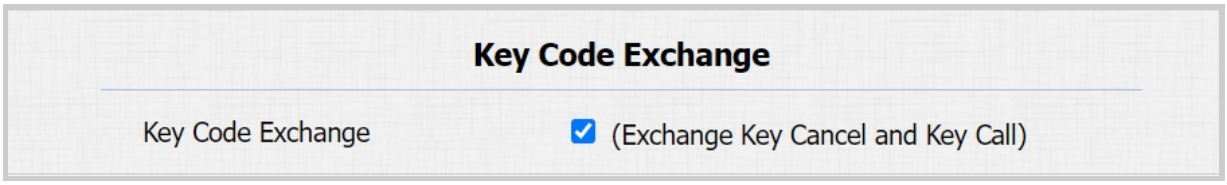
- **LCD Display**:
  - **Default**: Display Call, Contacts, PIN Entry, and Security Center instructions on the home screen.
  - **Hidden Contacts**: Display Call, PIN Entry, and Security Center instructions, but hide the Contacts.
  - **Text Only**: Only display the content you enter in the LCD Text box.
    - **LCD Text**: Customize the text to be displayed on the home screen.
  - **Contacts Only**: Only display contacts.
  - **Hide Contacts & Room Number**: Display PIN Entry and Security Center instructions.

- **Manager Dial Text**: Name the Manager Dial key(Press the Call key to call). Its default name is Security Center.

Key Code Exchange

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

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

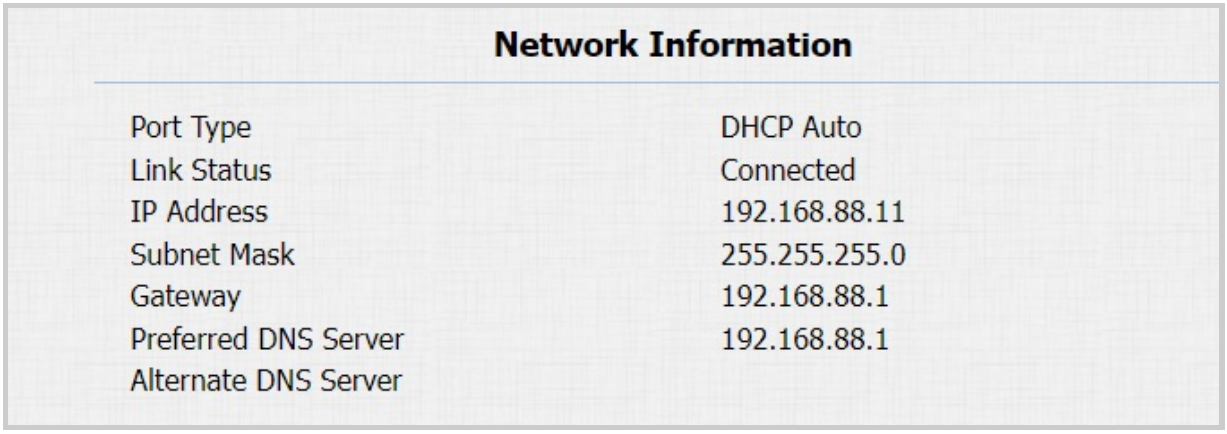


- **Key Code Exchange**: When enabled, the Cancel function will be linked to the Cancel key right on top of the Call key on the keypad. When disabled, the function of the Cancel and the Call key will be reversed.

Network Setting

Network Status

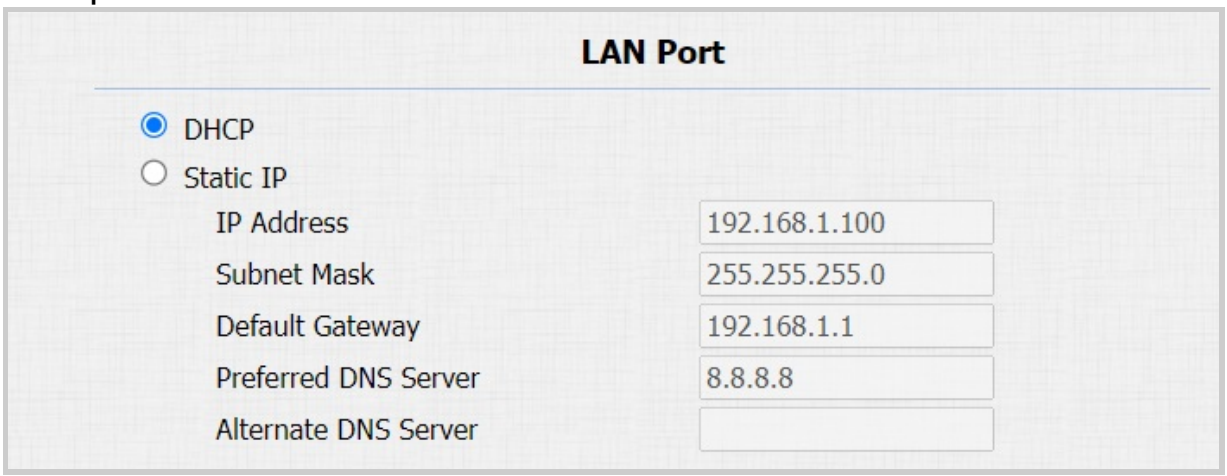
Check the network status on the web **Status > Network Information** interface.



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.

Set up the network on the **Network > Basic** interface.



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

- **Static IP**: The IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **IP Address**: 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 & Alternate 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.

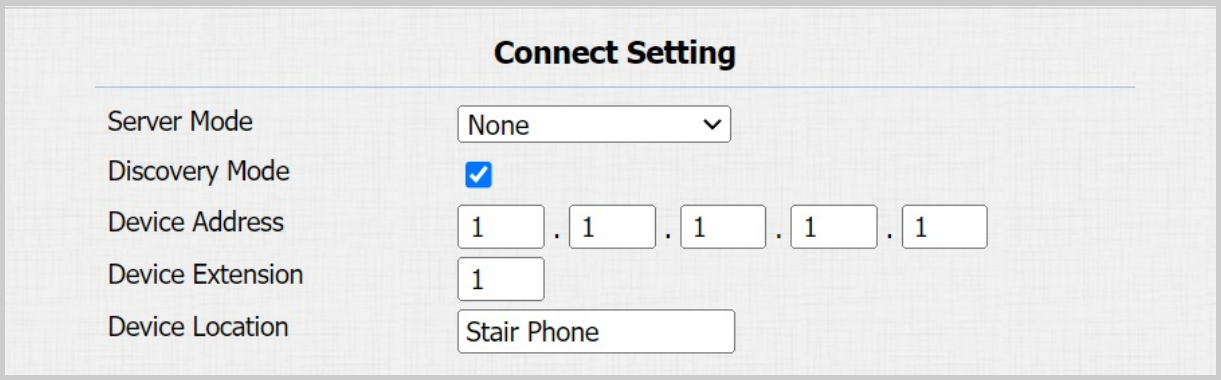
Tip

1. You can also set the network on the device by pressing "*2396#".
2. Press "3" to enter the System Setting.
3. Select Network Settings to set up the device's network.

Device Deployment in Network

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

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



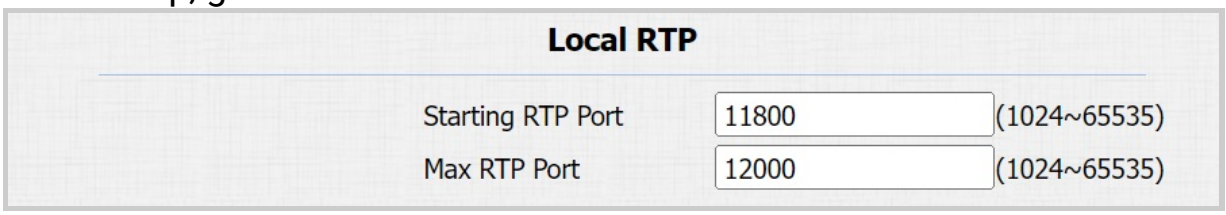
- **Server Mode**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None. You can select the mode manually.
  - **None**: None is the default factory setting, indicating the device is not in any server type. Devices connect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

Device Local RTP Configuration

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

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

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



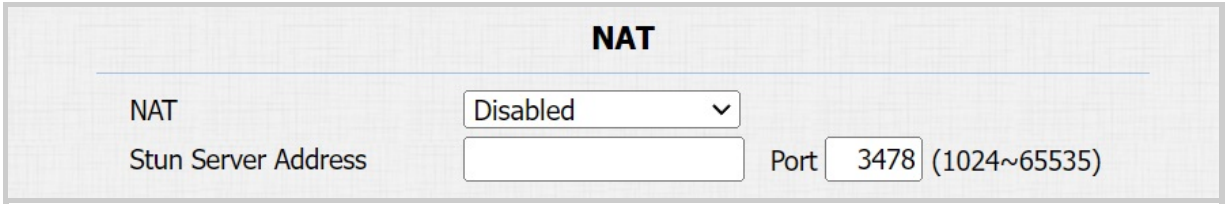
- **Starting RTP Port**: The port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: The port value to establish the endpoint for the exclusive data transmission range.

NAT Setting

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

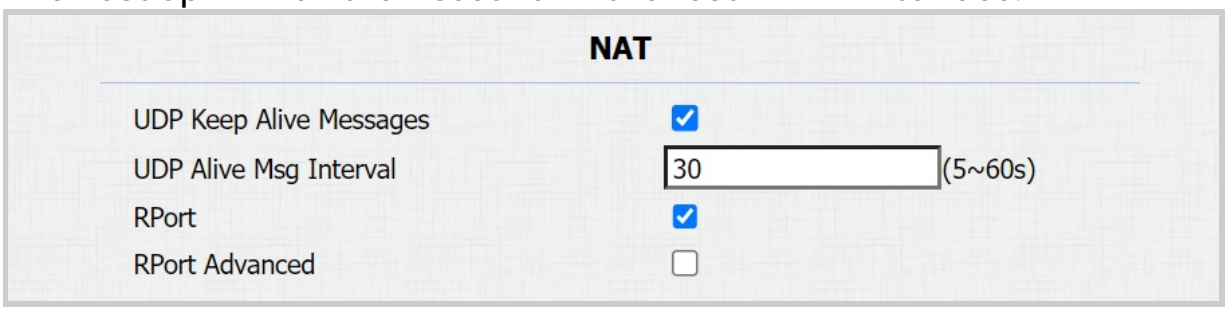
To register SIP accounts on third-party servers in a Wide Area Network(WAN), you need to enable the RPort feature on the intercom devices to establish a stable connection.

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



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

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

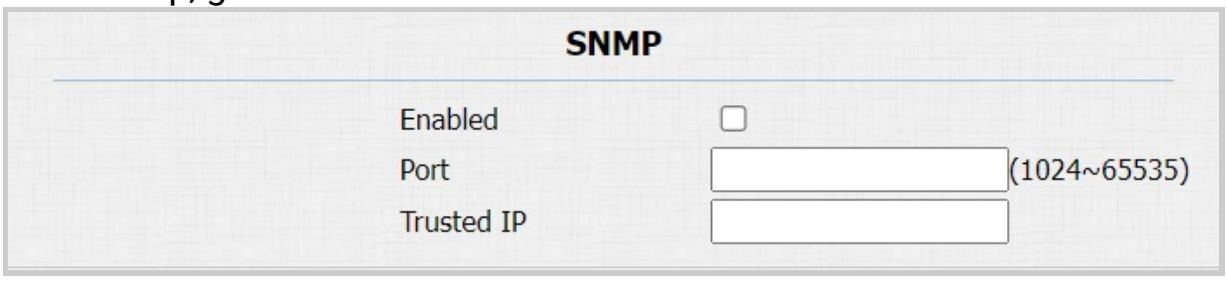


- **UDP Keep Alive Messages**: If enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Msg Interval**: The message-sending time interval ranges from 5 to 60 seconds. The default is 30 seconds.
- **RPort**: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

SNMP Setting

Simple Network Management Protocol**(SNMP)** is a protocol for managing IP network devices. It allows network administrators to monitor devices and receive alerts for attention-worthy conditions. SNMP provides variables describing system configuration, organized in hierarchies and described by Management Information Bases (MIBs).

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



- **Port**: Enter the SNMP server's port.
- **Trusted IP**: The allowed SNMP server address. It can be an IP address or any valid URL domain name.

VLAN Setting

A Virtual Local Area Network (VLAN) is a logical group of nodes from the same IP domain, regardless of their physical network segment. It separates the layer 2 broadcast domain via switches or routers, sending tagged packets only to ports with matching VLAN IDs. Utilizing VLANs enhances security by limiting ARP attacks to specific hosts and improves network performance by minimizing unnecessary broadcast frames, thereby conserving bandwidth for increased efficiency.

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

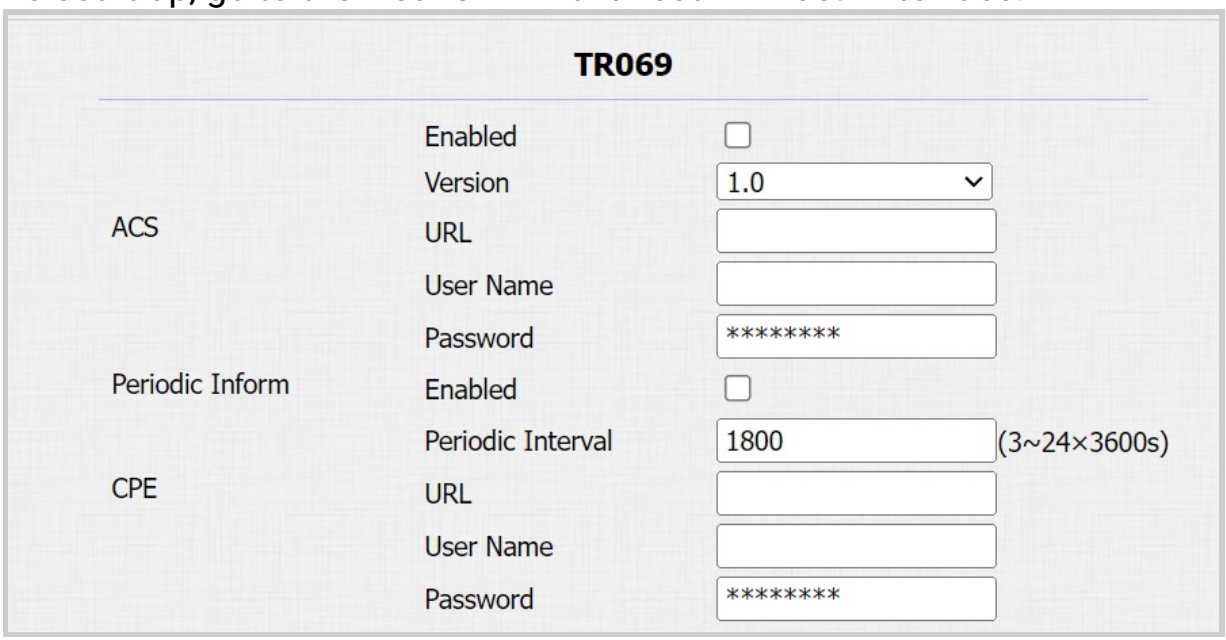


- **VID**: The VLAN ID for the designated port.
- **Priority**: The VLAN priority for the designated port.

TR069 Setting

TR-069 (Technical Report 069) provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. For door phones, the administrators can manage all the devices on a common TR-069 Platform. IP phones can be easily and securely configured on the TR-069 platform to make mass deployment more efficient.

To set it up, go to the **Network > Advanced > TR069** interface.

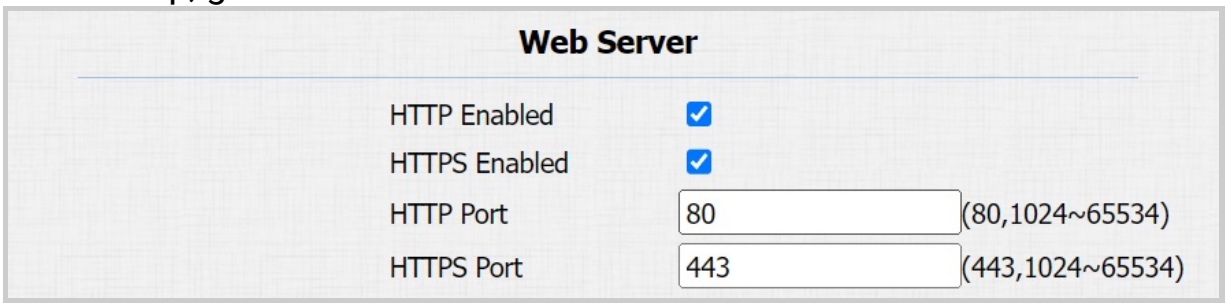


- **Version**: Select the supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE**: ACS is short for auto-configuration servers on the server side, and CPE is short for customer-premise equipment, as client-side devices.
- **URL**: The URL for ACS or CPE.
- **Periodic Interval**: The interval for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

Device Web HTTP Setting

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

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



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

Intercom Call Configuration

IP Call Configuration

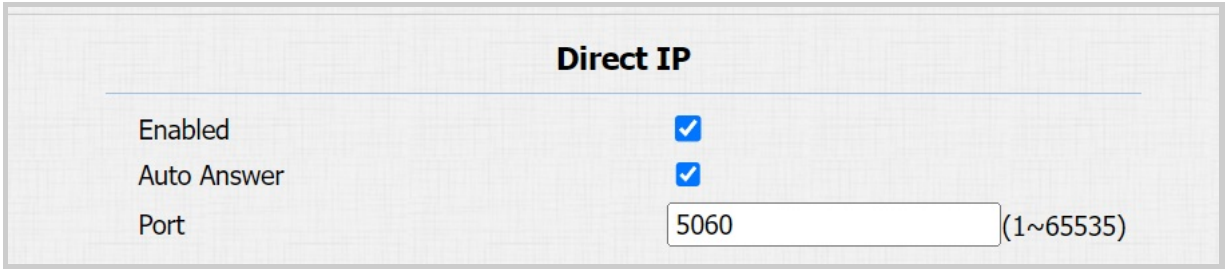
Make IP Calls

Make IP calls by entering the IP number, such as “192✳168✳35✳123”, and pressing the Call button.

IP Call Setup

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

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



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

SIP Call Configuration

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

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

SIP Account Registration

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

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

Click here to view the SIP account registration example.

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



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

Tip

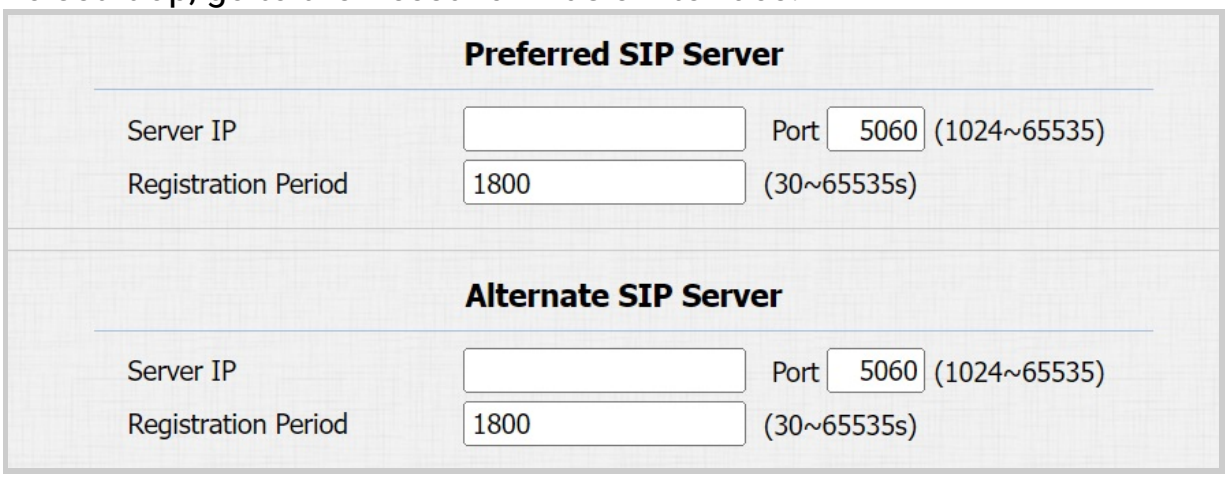
When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

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

SIP Server Configuration

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

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

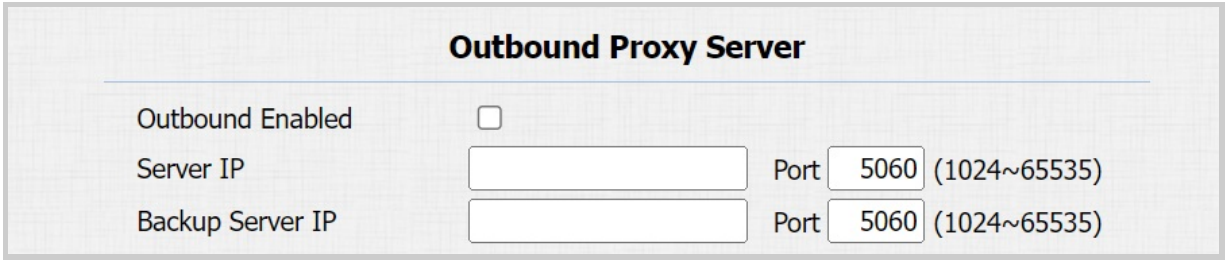


- **Server IP:** Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified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

Outbound Proxy Server

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

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



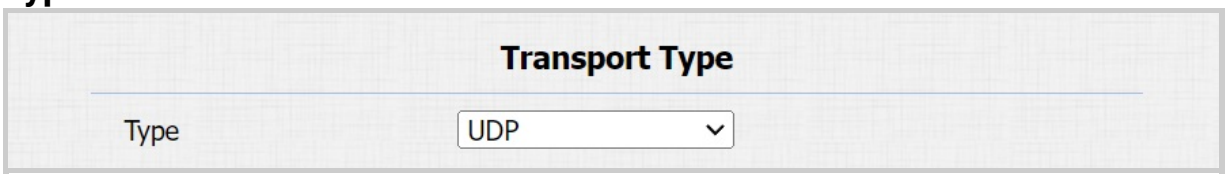
- **Server IP:** Enter the SIP proxy server's IP address.

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

Data Transmission Type

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

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

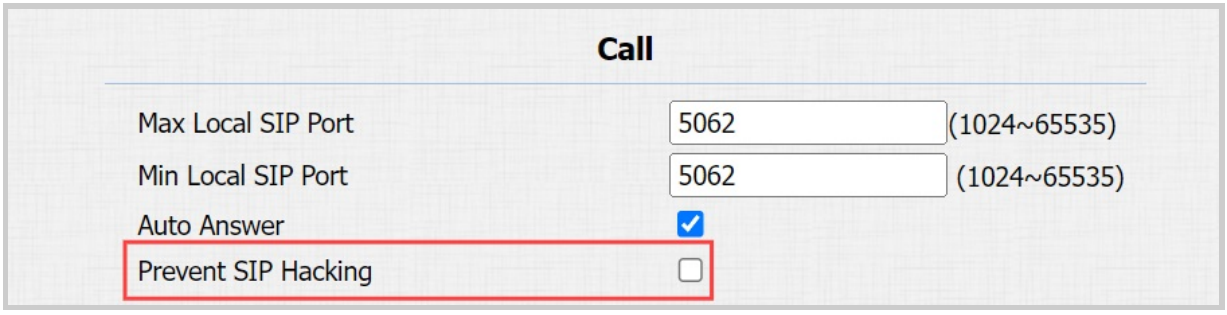


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

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

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



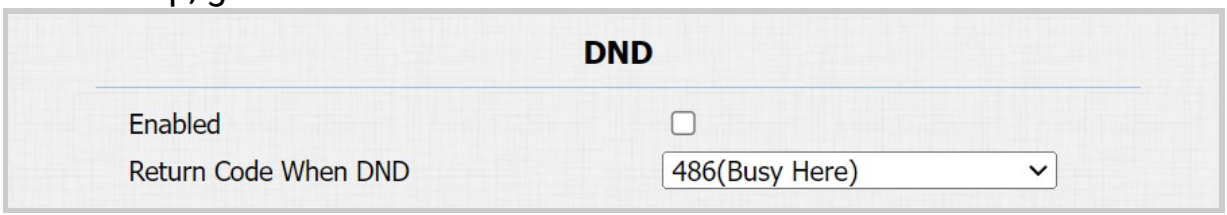
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Settings

Do Not Disturb

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

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

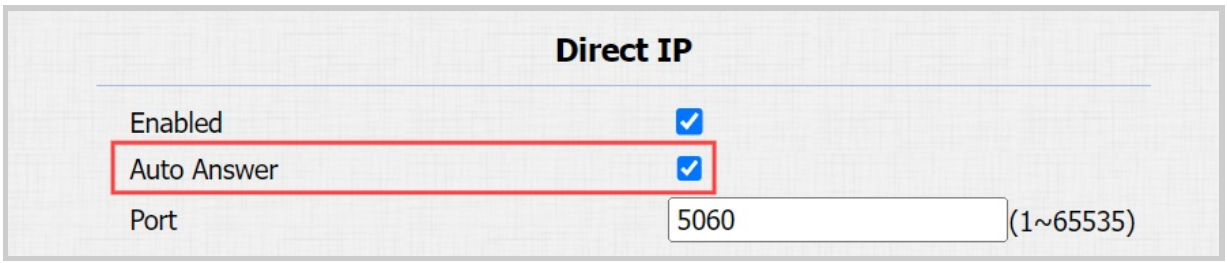


- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

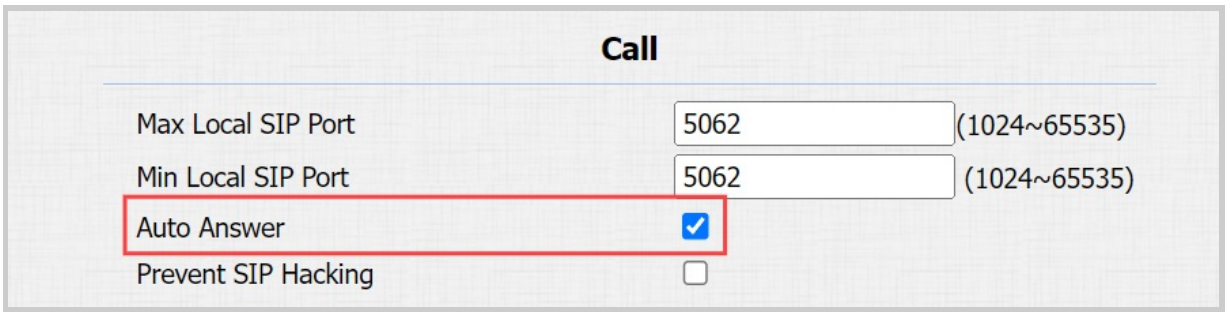
Call Auto-answer

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

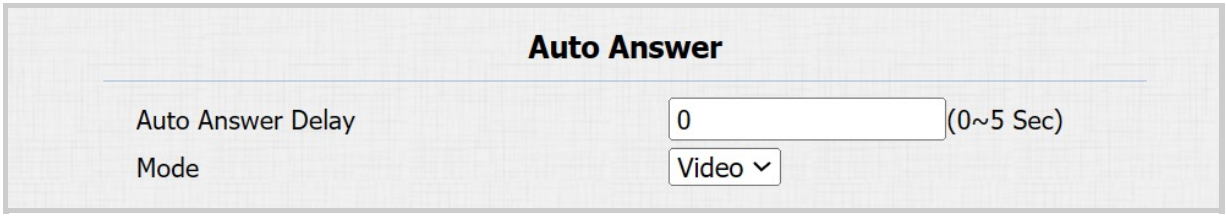
Enable auto-answer for direct IP calls on the **Phone > Call Feature > Direct IP** interface.



Enable auto-answer for SIP calls on the **Account > Advanced > Call** interface.



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

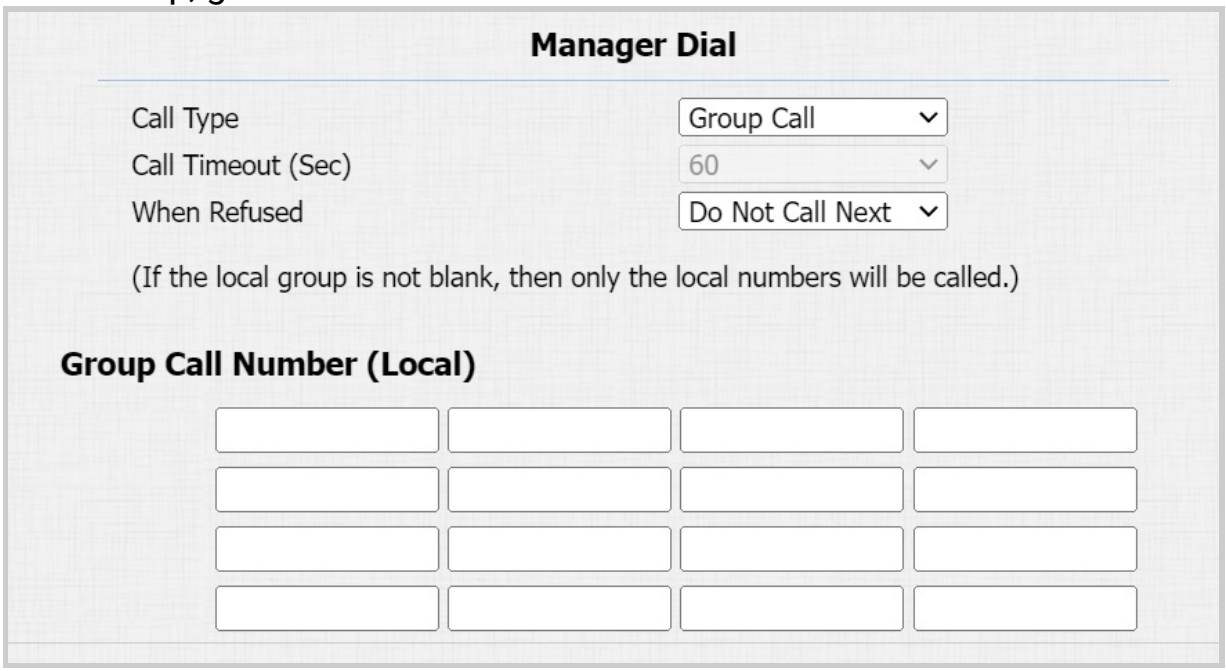


- **Auto Answer Delay**: Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode**: Determine whether to auto-answer the call as a video or audio call.

Group Call

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

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

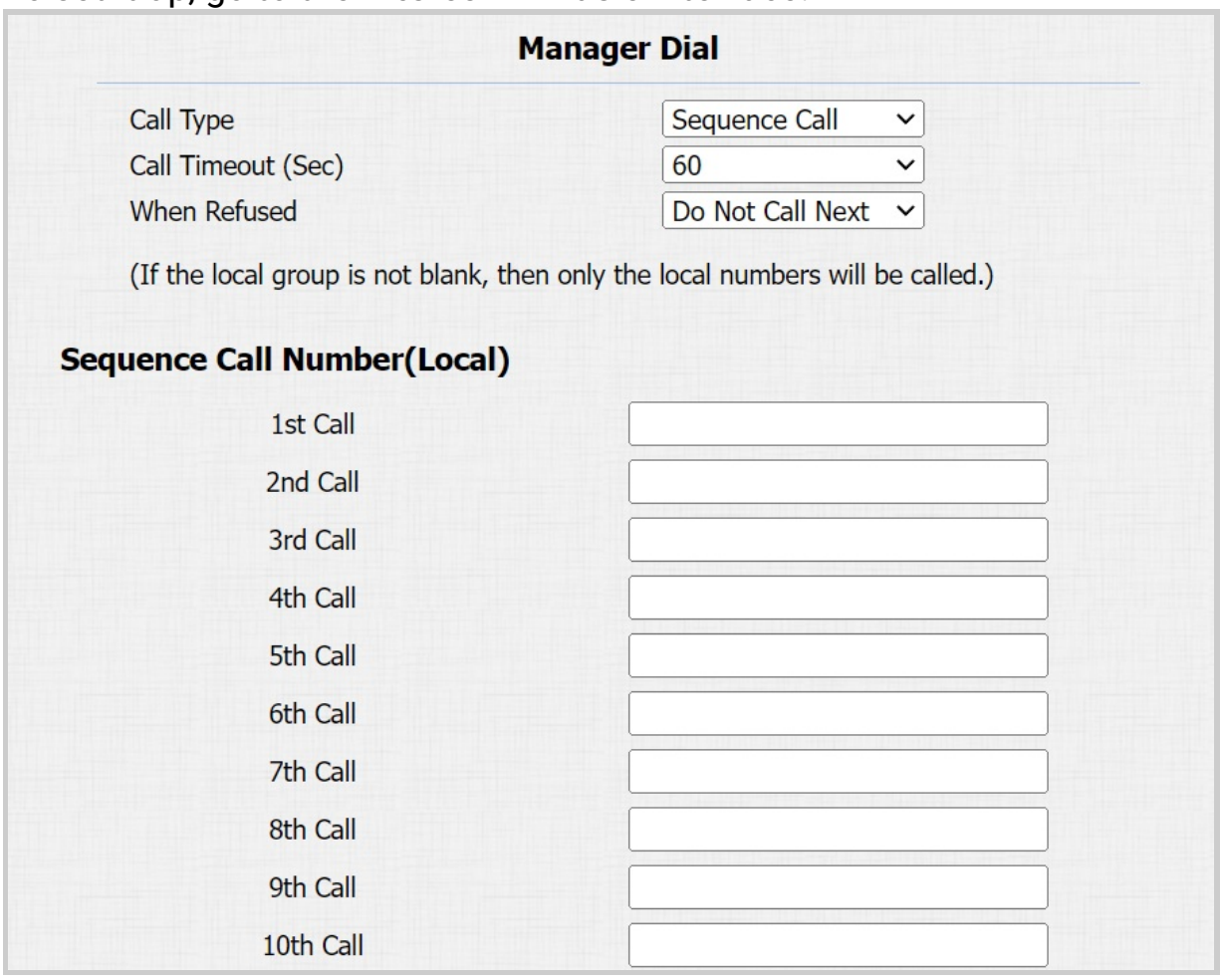


- **Call Type**: Select Group Call.
- **When Refused**:
  - **Do Not Call Next**: The device will stop calling.
  - **Call Next**: The device will continue to call other numbers.
- **Group Call Number(Local)**: Enter the target numbers.

Sequence Call

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. 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.

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

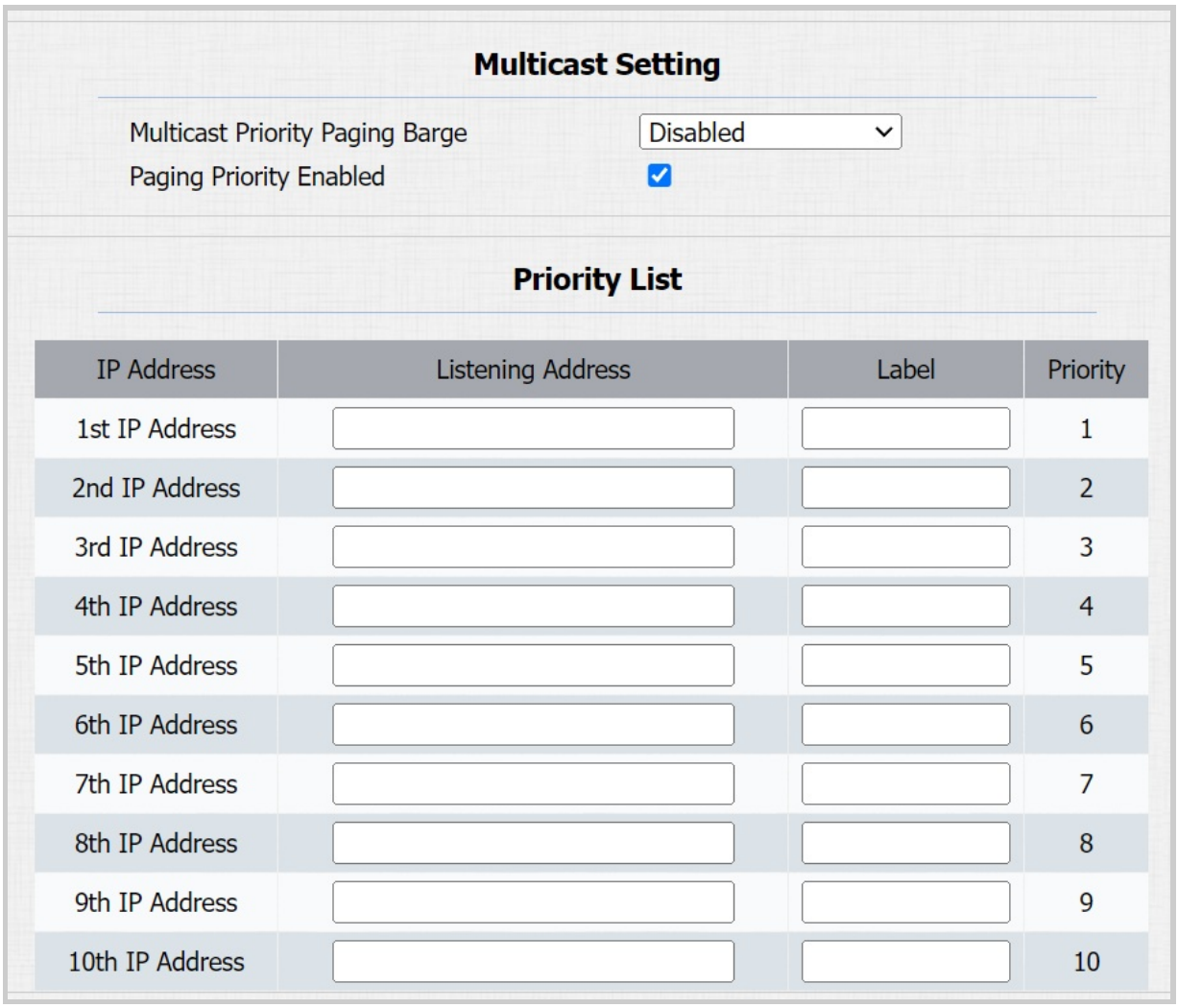


- **Call Type**: Select Sequence Call.
- **Call Timeout(Sec)**: Determine the duration before calling the next number when the previous call is not answered.
- **When Refused**:
    - **Do Not Call Next**: The device will stop calling.
    - **Call Next**: The device will continue to call other numbers.
- **Sequence Call Number(Local)**: Enter the target numbers.

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 the **Phone > Multicast** interface.



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

Note

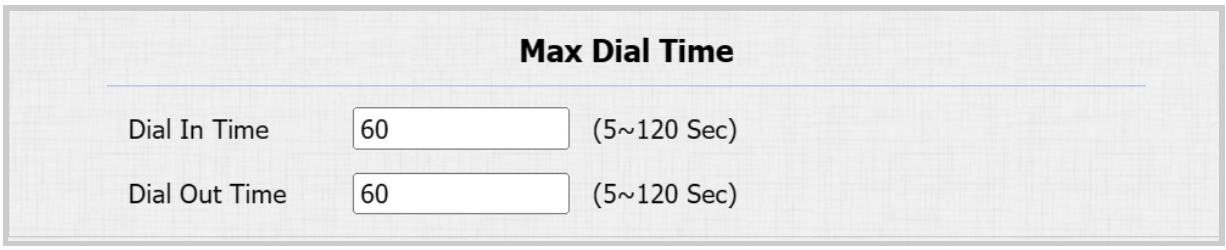
Please contact Akuvox tech team for a valid multicast address.

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

Maximum Dial Duration

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

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



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

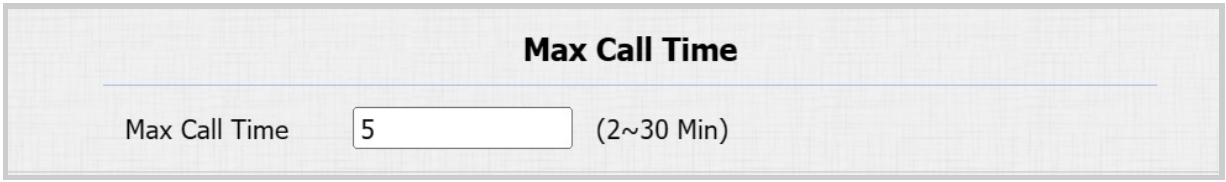
Note

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

Maximum Call Duration

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

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



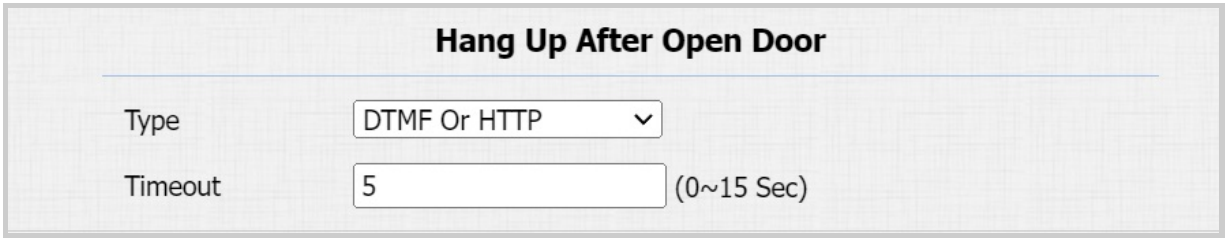
Note

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

Hang up After Open Door

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

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



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

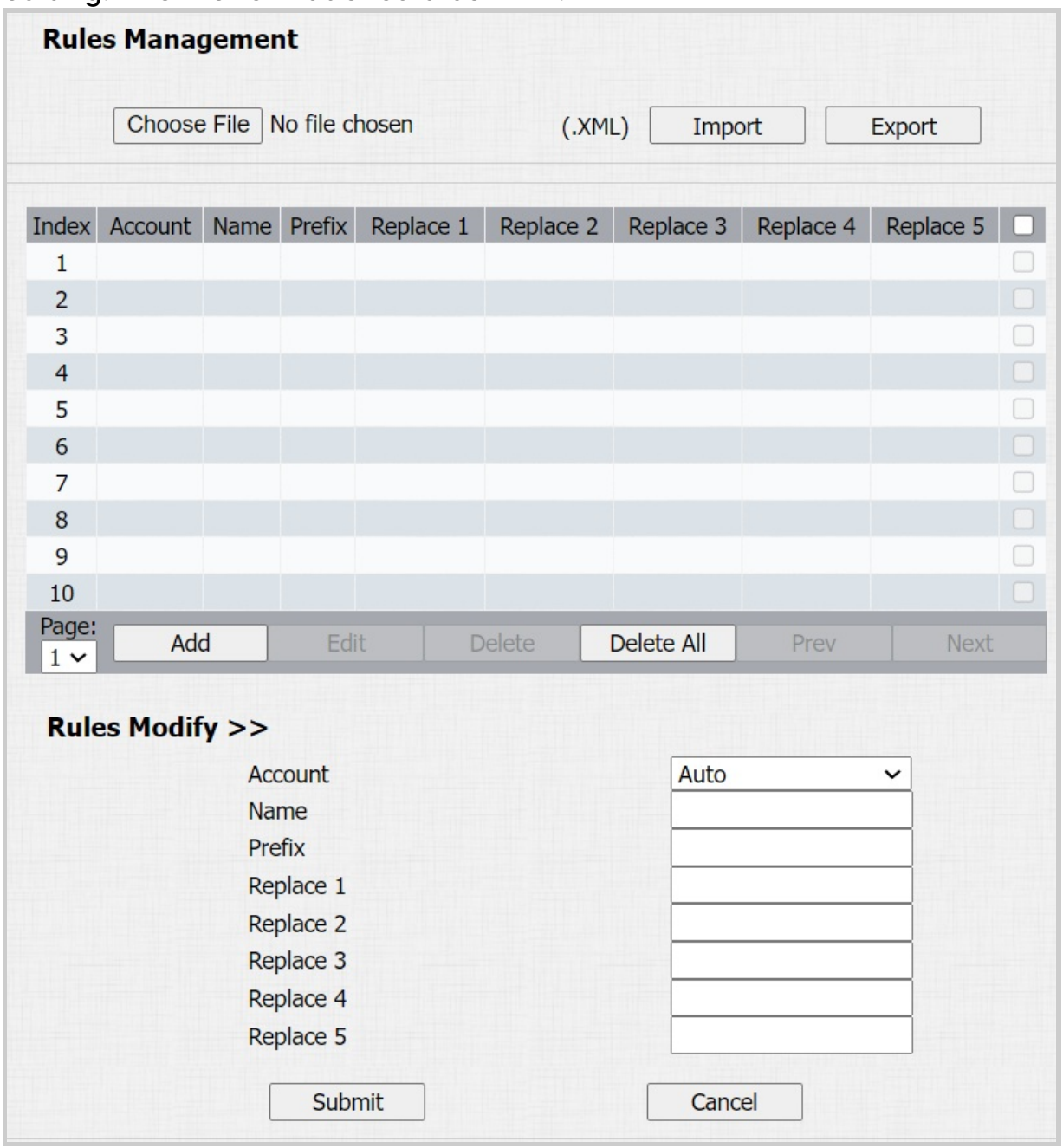
Dial Plan

The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

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

Click **Add** to set up a dial plan rule. You can add up to 1,000 rules.

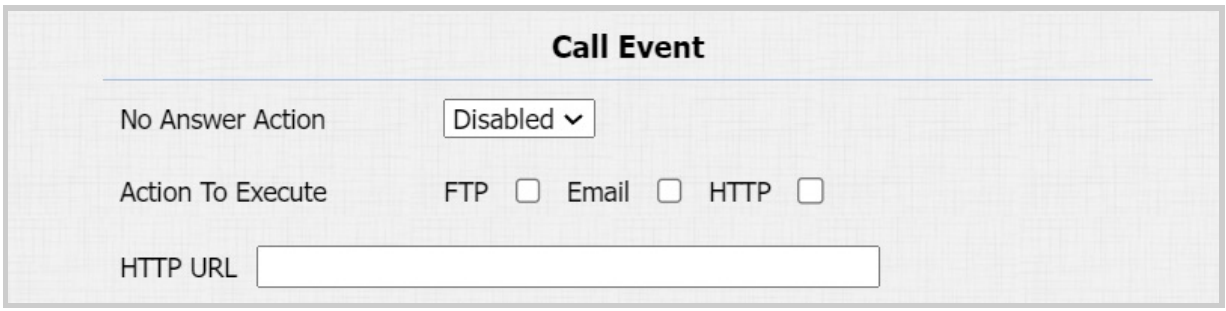
You can click **Export** to export the dial plan template. Click **Import** after editing. The file format should be XML.



- **Account**: Select the account to make the dial plan call.
- **Name**: Name this rule.
- **Prefix**: The short number replaces the IP/SIP number.
- **Replace 1-5**: The IP/SIP number to be replaced.

Actions Triggered by Calling

You can set up actions triggered when a call made by the device is not answered on the **Intercom > Basic > Call Event** interface.



- **No Answer Action**: Enable or disable the function of triggering actions when a call is not answered.
- **Action To Execute**:
  - **FTP**: Send a screenshot to the preconfigured FTP server.
  - **Email**: Send a screenshot to the preconfigured Email address.
  - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

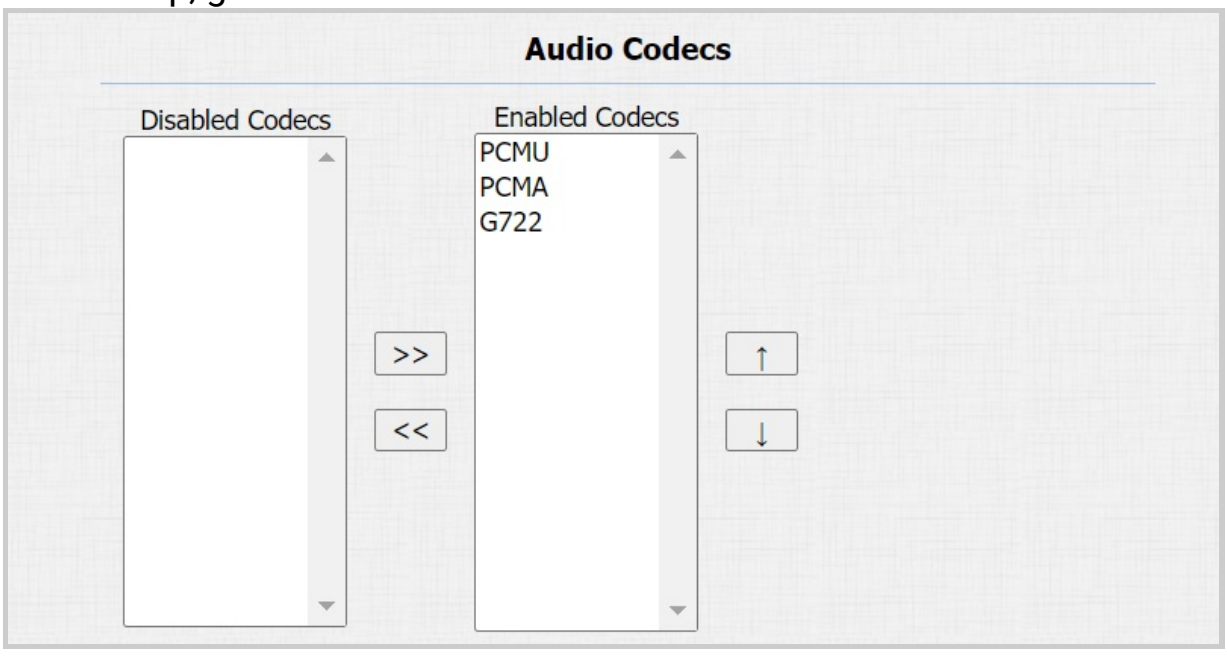
Audio and Video Codec Configuration

Audio Codec

The door phone supports three types of codecs (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each type varies in terms of sound quality. 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.

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



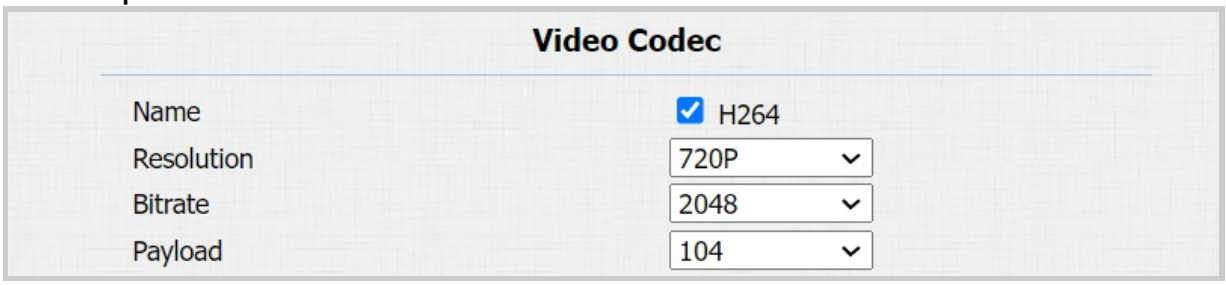
Please refer to the bandwidth consumption and sample rate for the codec types below:

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

Video Codec

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

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

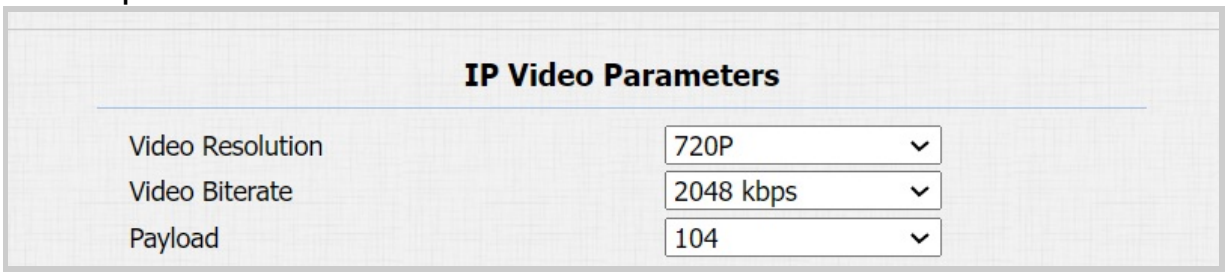


- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default resolution is 720P(720 × 480 pixels).
- **Bitrate**: The video stream bitrate ranges from 64 to 2048 kbps. The greater the bitrate, the more data is transmitted every second, and the clearer the video will be. The default code bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for Direct IP Calls

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

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



- **Video Resolution**: Select the resolution from the provided options. The default resolution is 720P(720 × 480 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 64 to 2048 kbps. The default bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Contacts Management

The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

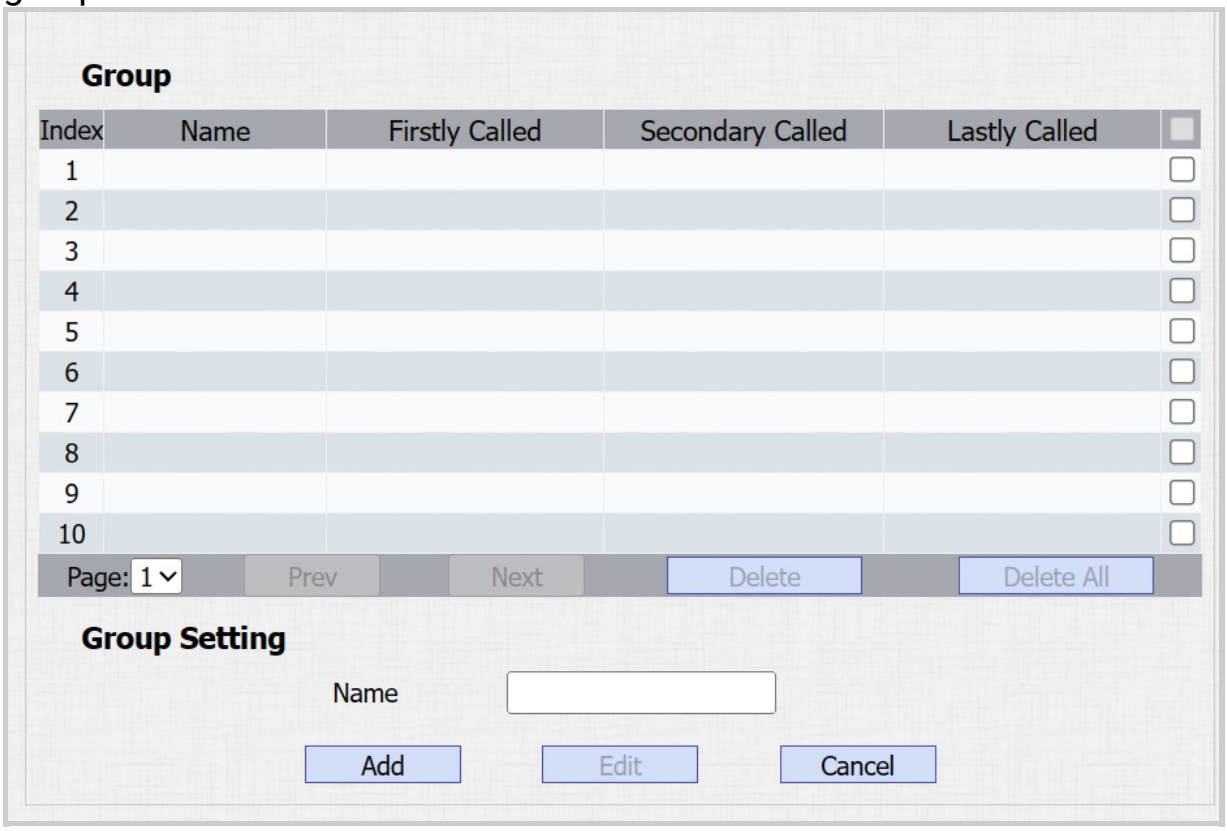
When the device is deployed on the SmartPlus Cloud, cloud contacts will display on the device web but not editable.

Manage Contact Group

You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

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

Enter the group name and click **Add** to add a group. You can add 1,000 groups.

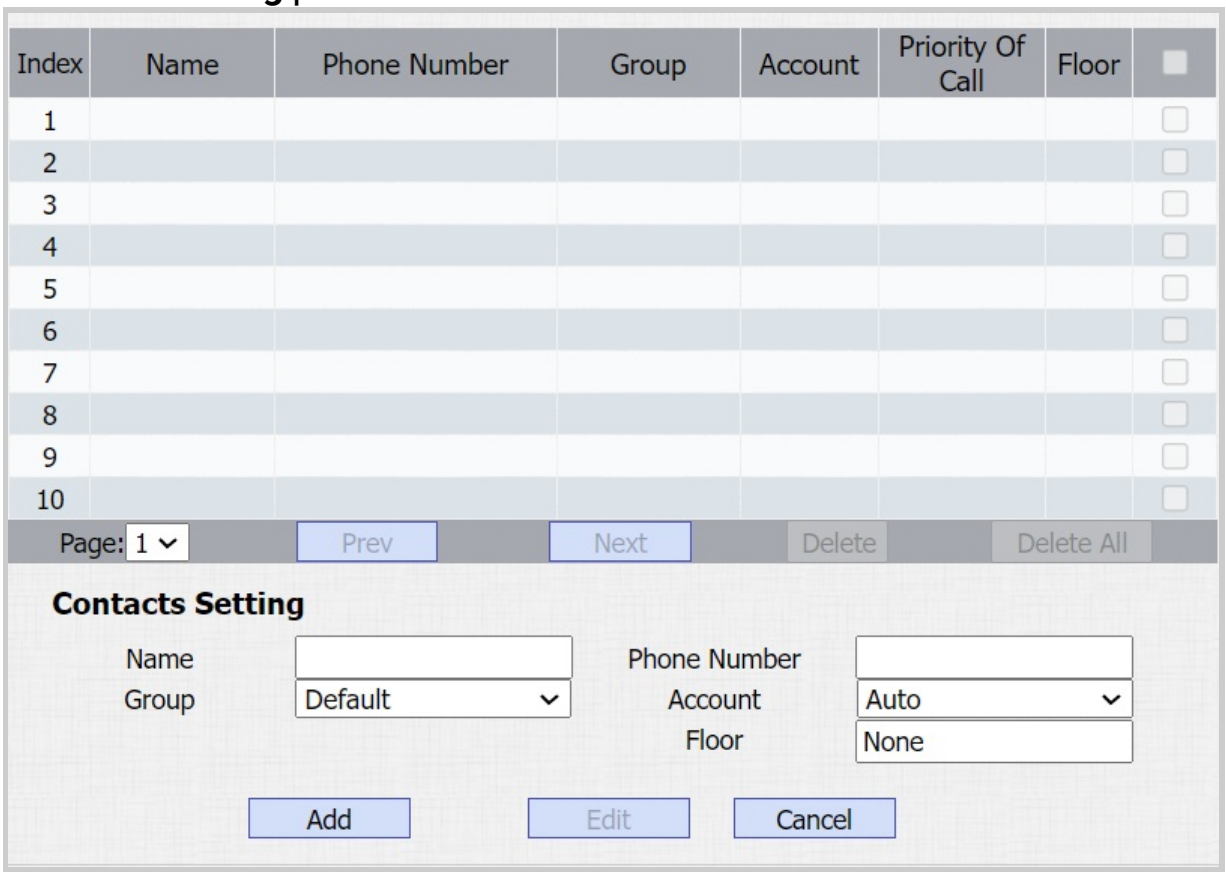


Manage Contacts

You can search, create, display, edit, and delete the contacts. You can add 1,000 contacts.

Add Contacts

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



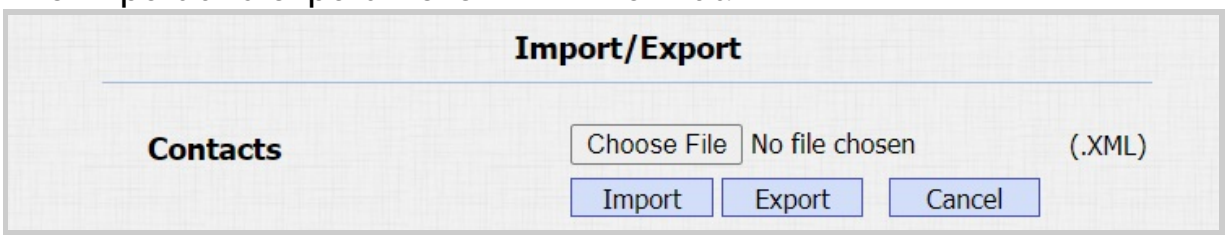
- **Name**: Enter the contact's name.
- **Phone Number**: Enter the contact's IP or SIP number.
- **Group**: Assign the contact to the default or a self-created group.
- **Account**: The account is used when making calls to the contact.
- **Floor**: Specify the accessible floor(s) to the contact via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

Export/Import Contacts

You can easily import and export contacts for quick management.

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

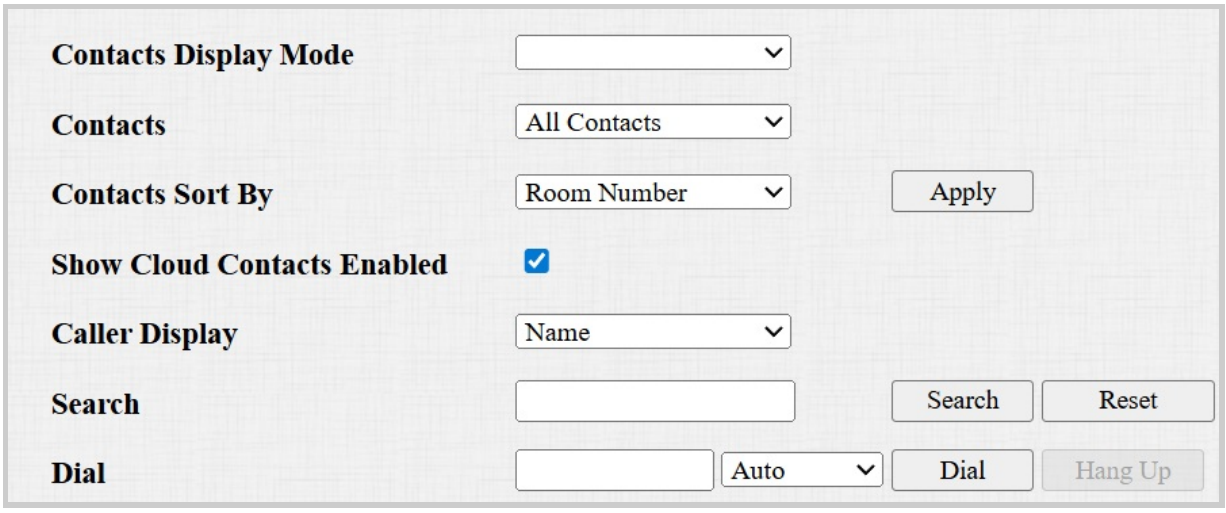
The import and export file is in XML format.



Contact List Display

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

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



- **Contacts Display Mode**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only:** Display contact groups. Press the desired group on the device screen to make a group call.
  - **Contact Display by Group:** Display contacts by groups. Press the group, and users can see the contacts in it.
- **Contacts**: Select to display all contacts or contacts in a specific group.
- **Contacts Sort By**:
  - **ASCII Code**: List the contacts by their names in the sequence of the ASCII code.
  - **Room Number**: List the contacts according to their room number. This feature works with SmartPlus Cloud.
  - **Room Name**: List the contacts based on room names.

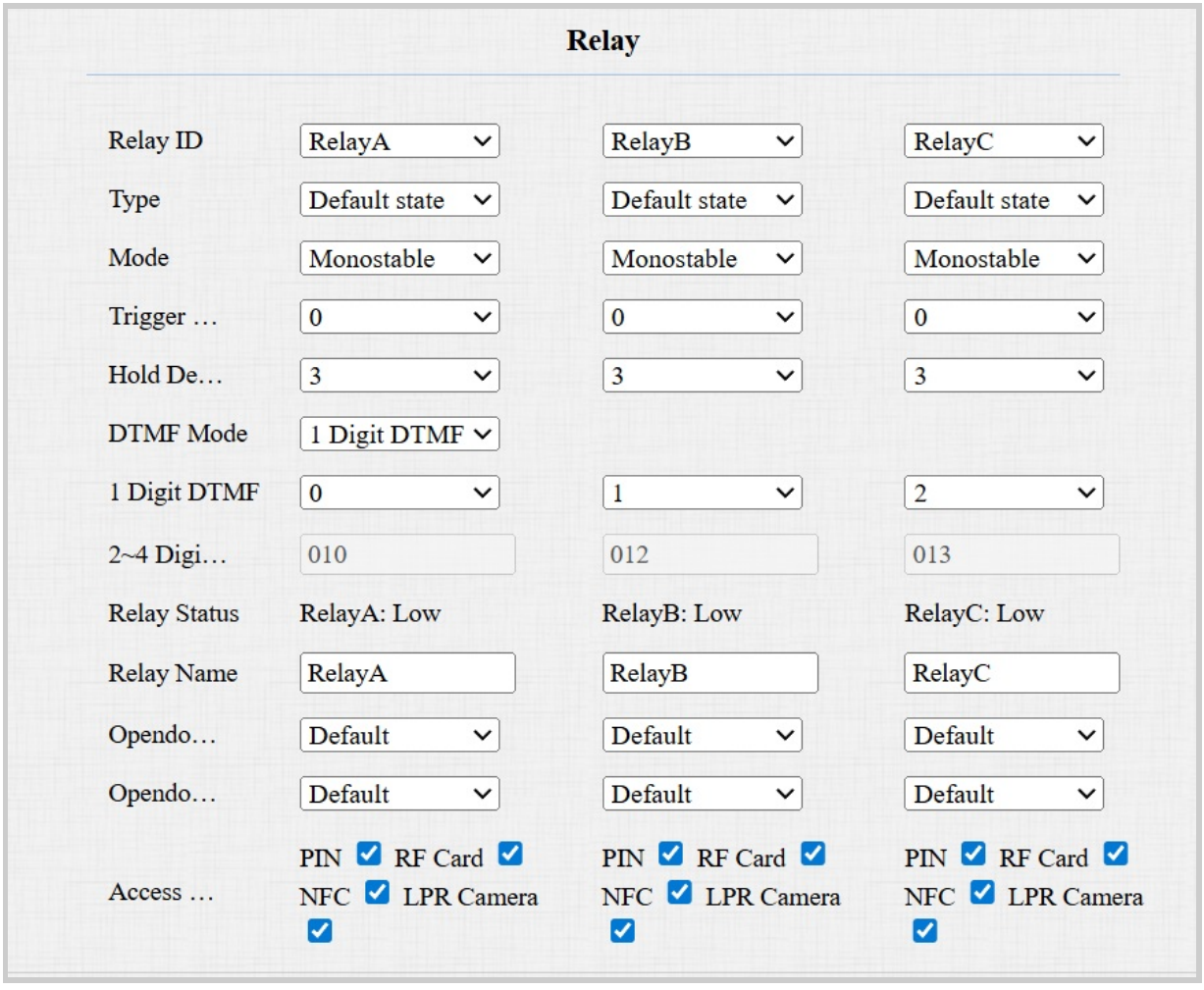
    - **Import**: List the contacts based on their order in the import file.
- **Show Cloud Contacts Enabled**: When enabled, the contacts synchronized from the SmartPlus Cloud can be displayed.
- **Cloud Call Permission Control**: This option will display when the device is connected to the SmartPlus Cloud. It decides whether to link the SmartPlus user's permissions to open doors and make calls.
    - For example, when users are not authorized to open doors during a specific time and the Cloud Call Permission Control feature is enabled, their SmartPlus App and/or indoor monitors will not receive calls from the door phone.
    - If this feature is disabled, even if users cannot open doors, they can receive calls.
- **Caller Display**: Choose what to be displayed on the device screen when receiving calls from contacts.
    - **Name**: Display the contact name.
    - **Group**: Display the group the contact belongs to.
- **Search**: Enter the contact name to search for a specific contact. Click Reset to clear the box.
- **Dial**: You can directly call a contact by checking it and selecting the account on the web interface. Click Dial to make the call.

Relay Setting

Local Relay

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

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



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

    - **Invert State**: A “Low” status in the Relay Status field indicates an open door, while “High” indicates a closed one.
- **Mode**: Specify the conditions for automatically resetting the relay status.
    - **Monostable**: The relay status resets automatically within the relay delay time after activation.
    - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Open Door Outside Tone**: Select the tone to be heard when the relay is triggered by the device-supported access methods, except for pressing the exit button.
- **Open Door Inside Tone**: Select the tone to be heard when the door is opened by triggering the input(pressing the exit button).
- **Access Method**: Check the access method(s) to open doors.

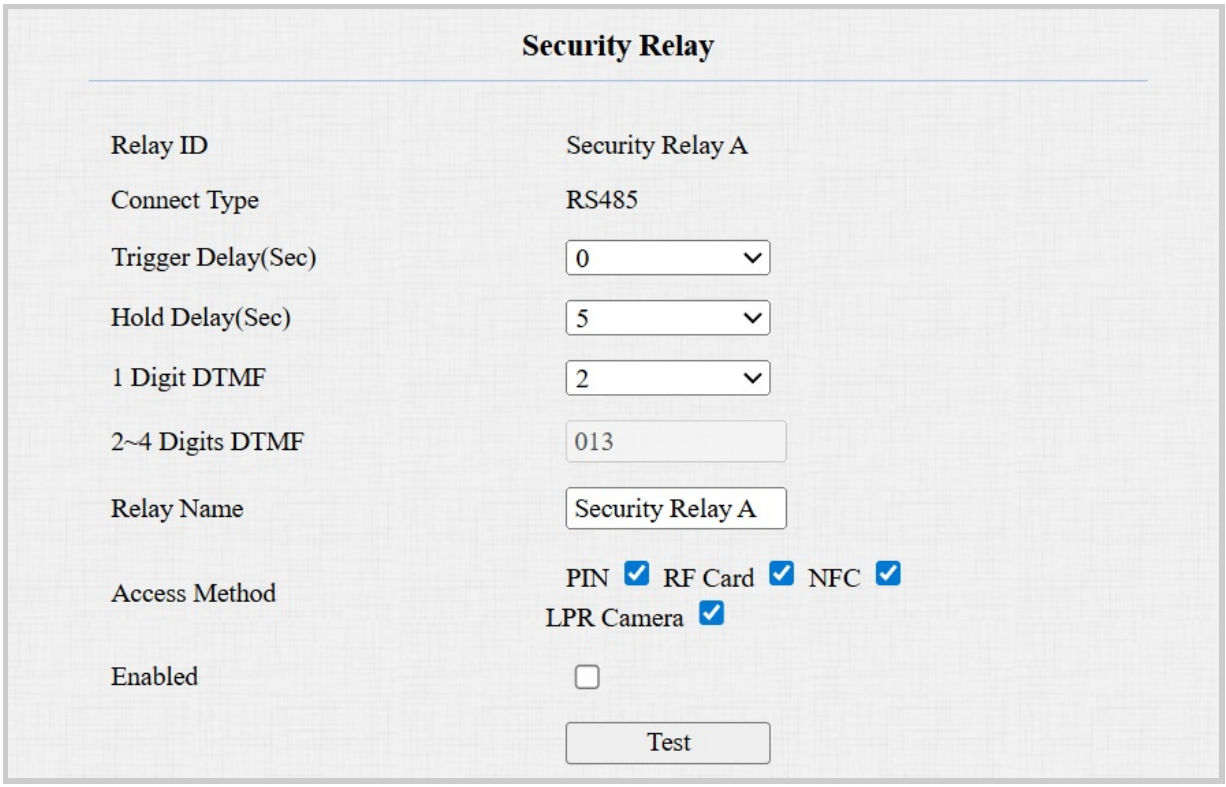
Security Relay

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.

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



- **Connect Type**: The connection type is RS485 by default.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

- **Relay Name**: Name the security relay. The name can be displayed in door-opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method**: Check the access method(s) to open doors.
- **Enabled**: Enable or disable the use of the security relay.
- **Test**: Click to send the signal to the SR01. When the door phone and SR01 are pairing, click Test to finish the matching.

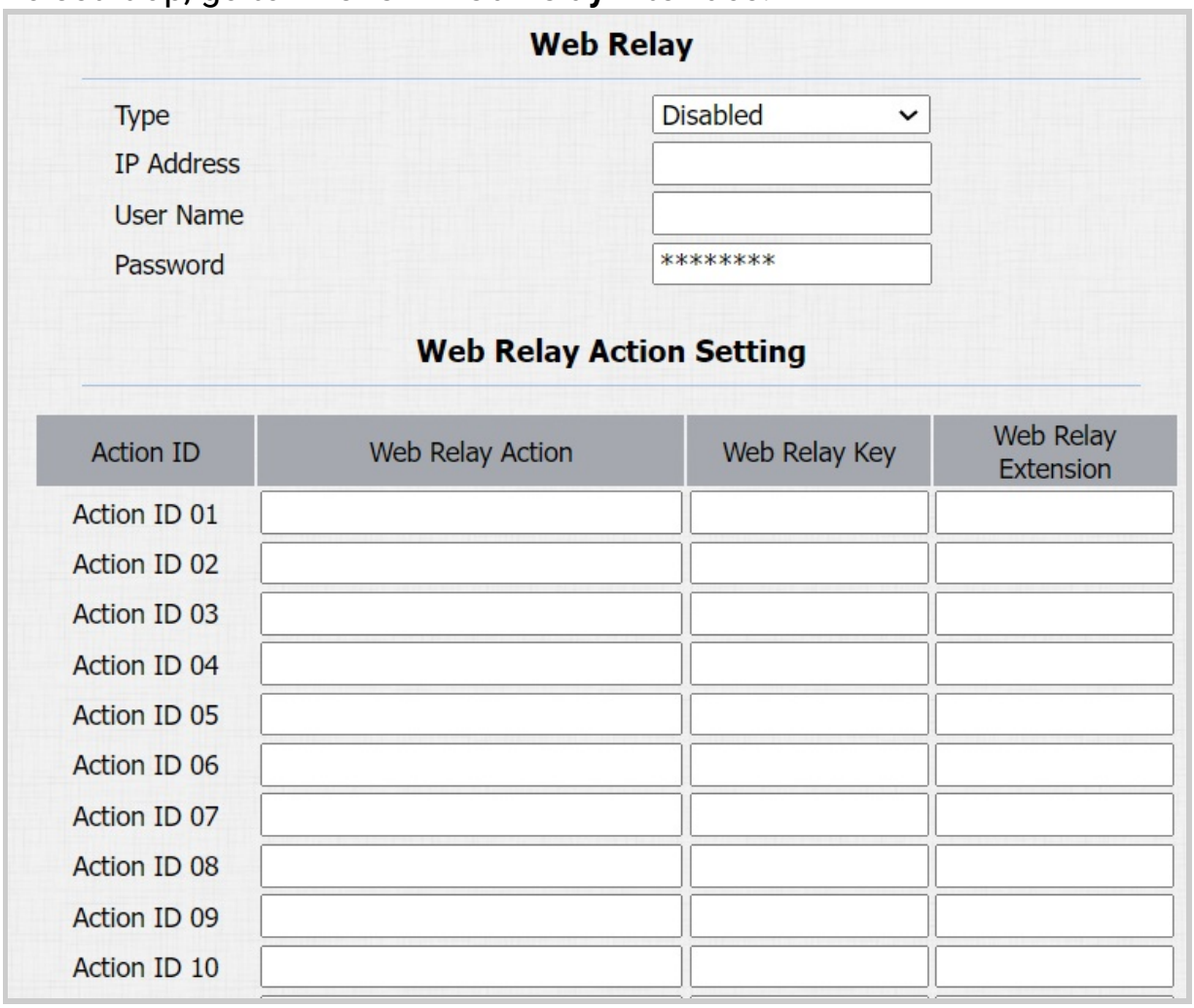
Web Relay

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



Click here to view how to set up web relay.

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



- **Type**: Determine the type of relay activated when employing door access methods for entry.
    - **Disabled**: Only activate the local relay.
    - **Web Relay**: Only activate the web relay.
    - **Both**: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **User Name**: The user name provided by the web relay manufacturer.
- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.

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

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

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

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

- Leaving it blank enables all door-opening methods.

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

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

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

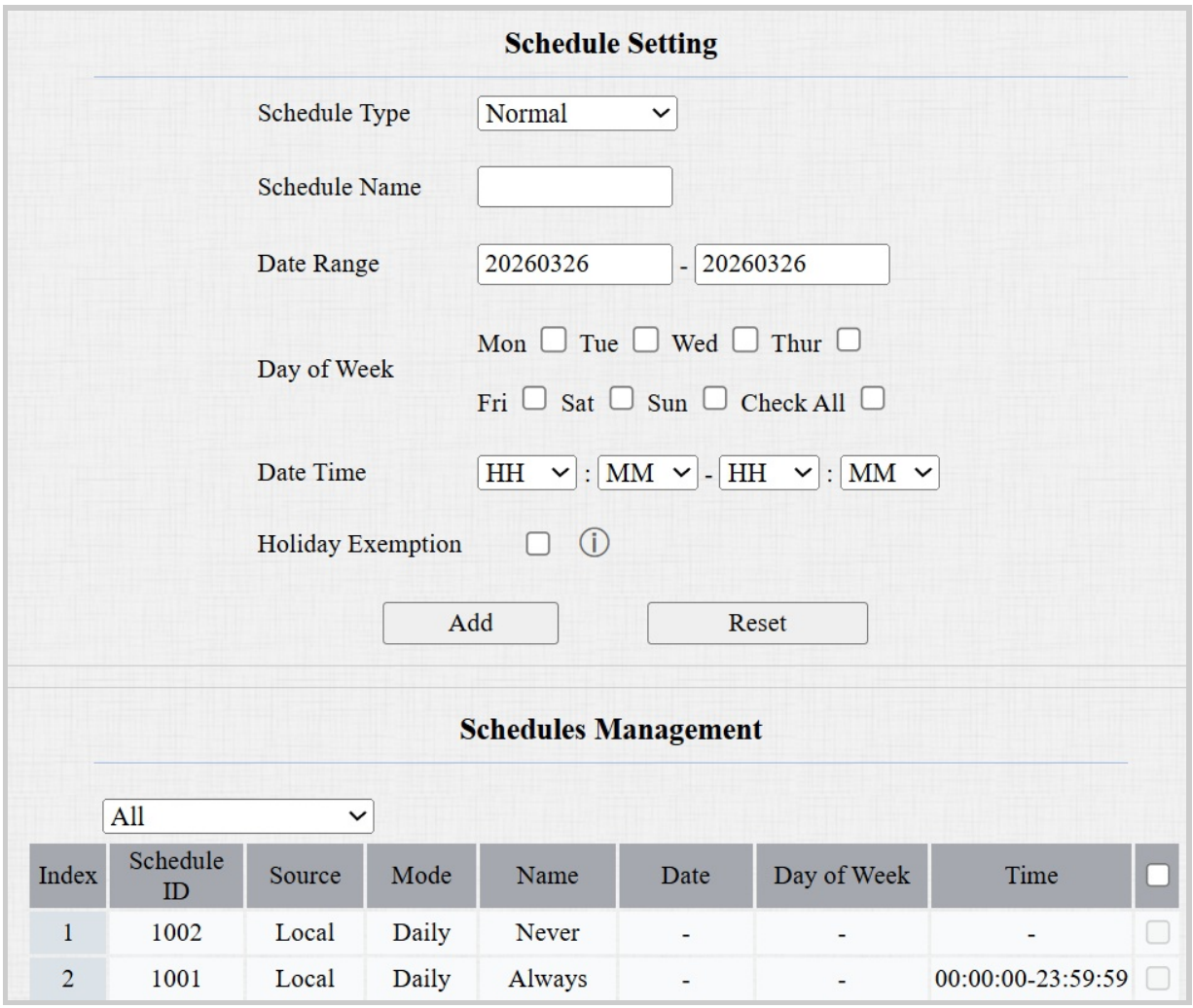
Access Control Schedule Management

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

Create a Door Access Schedule

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

Set it up on the web **Intercom > Schedule** interface. You can add 100 local schedules.

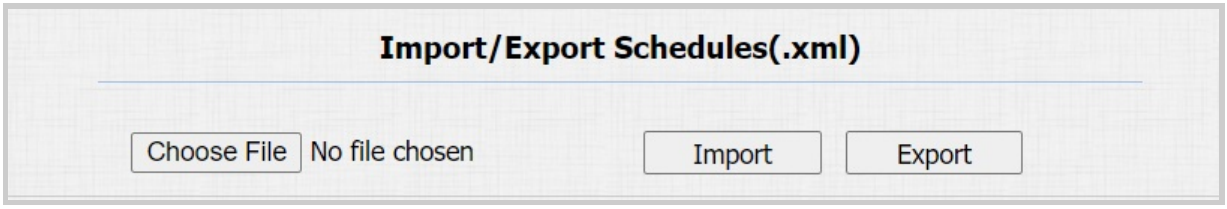


- **Schedule Type**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long-term schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Schedule Name**: Name the schedule.
- **Holiday Exemption**: The holiday schedule has higher priority over the access schedule, which limits users from opening doors. If users want to open doors during holidays within the access schedule, you need to check this option.

Import and Export Door Access Schedule

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

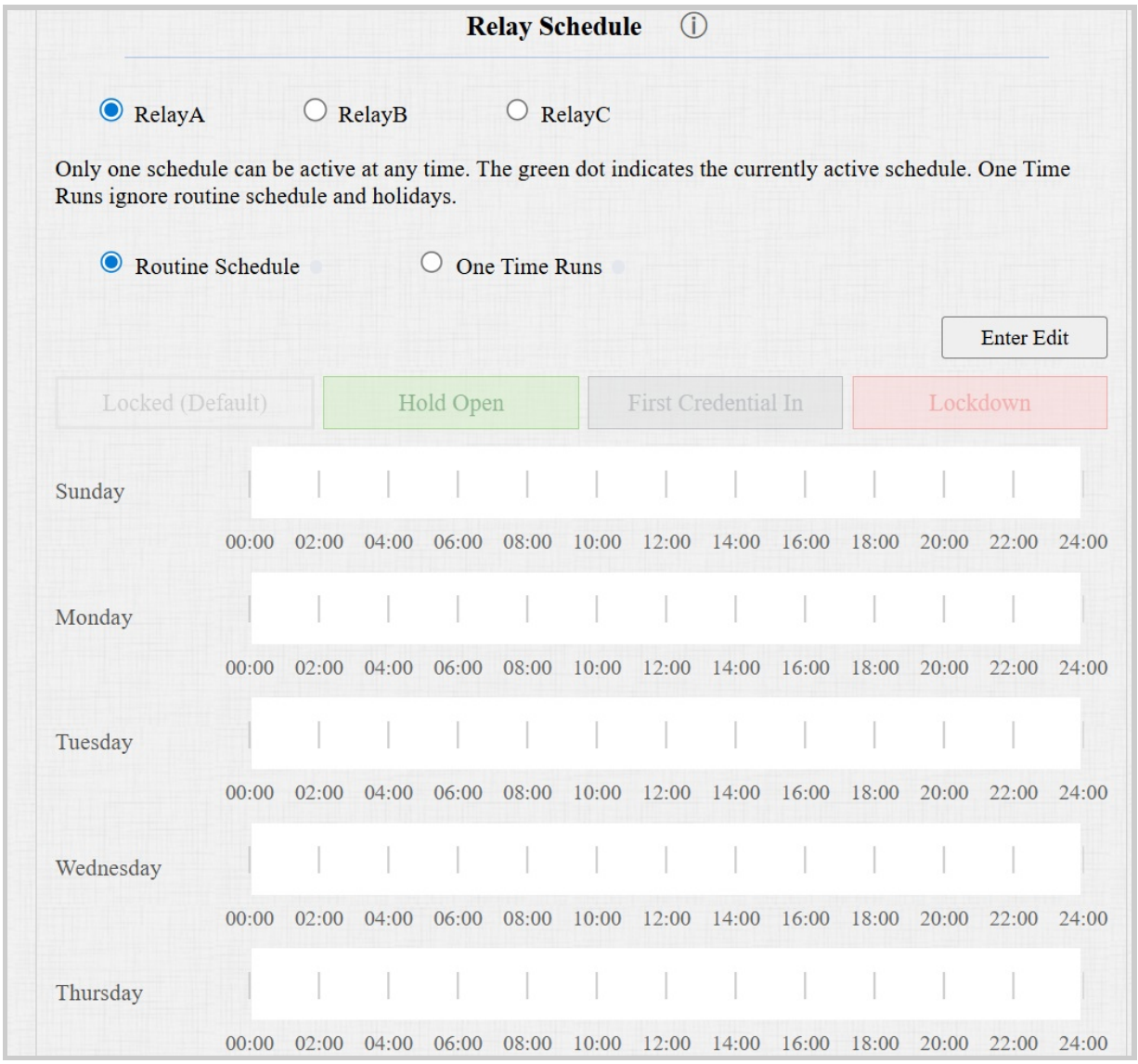
To set it up, go to the **Intercom > Schedule** interface. The import file should be in **XML** format.



Relay Schedule

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

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



- **Relay ID**: Specify the relay that applies the schedule.
- **Repeat Type**:
  - **Routine Schedule**: The schedule repeats every week. Click **Edit** on the right to configure.
  - **One-Time Runs**: Set the daily or weekly schedule that repeats during a defined period.
- **Schedule Mode:**
  - **Hold Open**: The door remains open during the scheduled time.
  - **First Credential In:** The door remains open during the scheduled time after users use their credentials for the first time.
  - **Lockdown**: The door remains closed during the scheduled time.

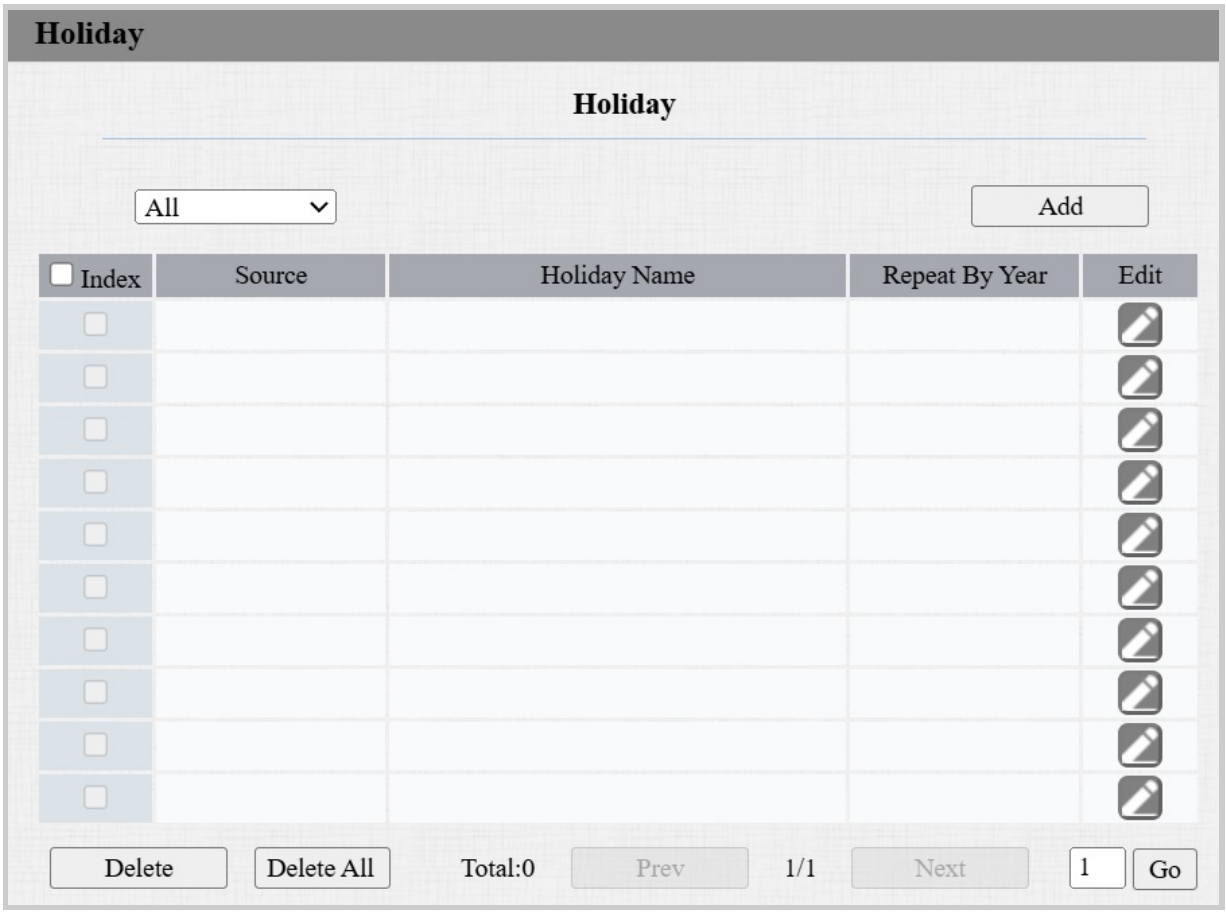
Note

Click **here** to view the detailed configuration of each schedule mode.

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.

To set it up, go to the **Intercom > Holiday** interface. Click **Add**.



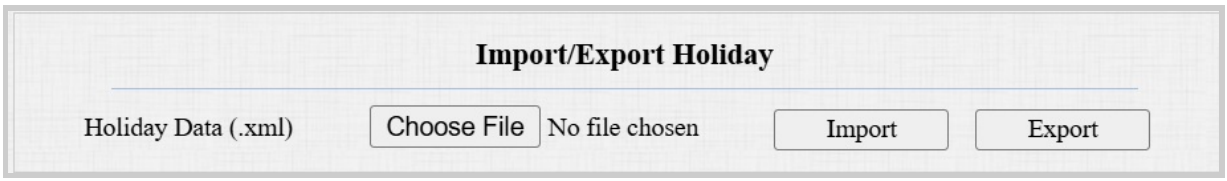


- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

Holiday Schedule Import/Export

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

The import/export file format is XML.

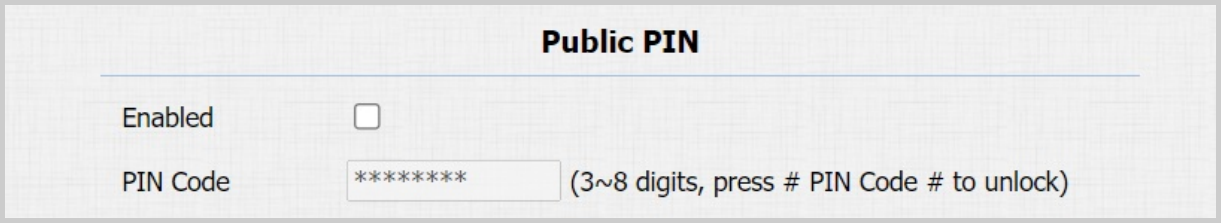

Import/Export Holiday
Holiday Data (.xml)
Choose File
No file chosen
Import
Export

Door-opening Configuration

Unlock by Public PIN Code

There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex. You can create and modify both the public and private PIN codes.

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



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

Tip

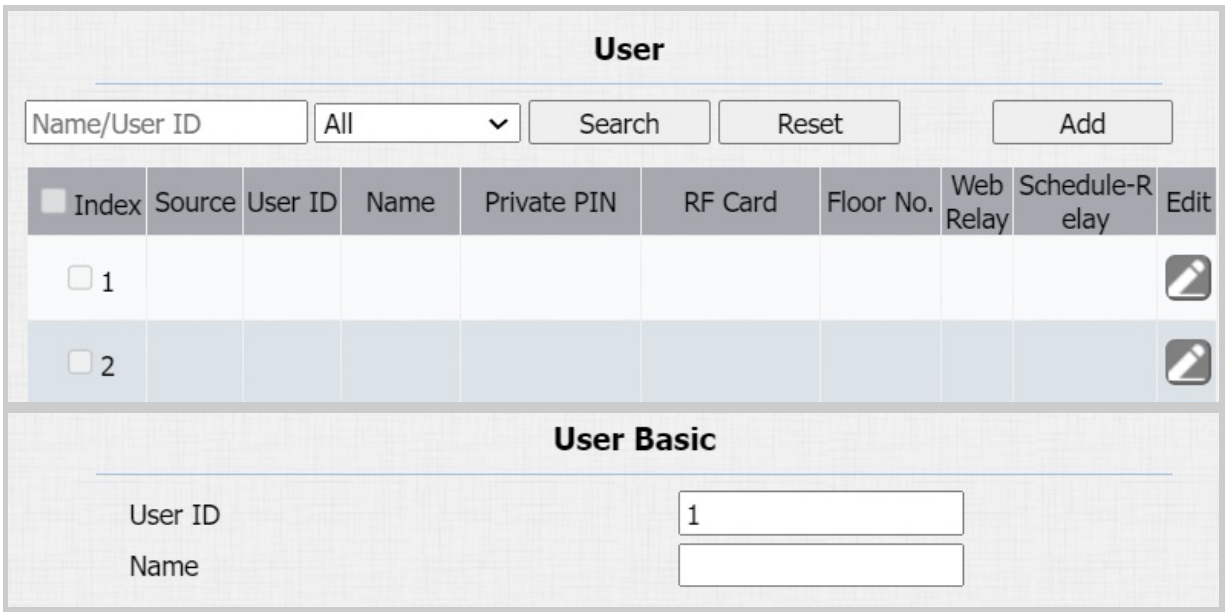
You can also modify the Public PIN on the device by pressing "*3888#" on the keypad to enter the Access Method Settings screen.

User-specific Access Methods

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

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

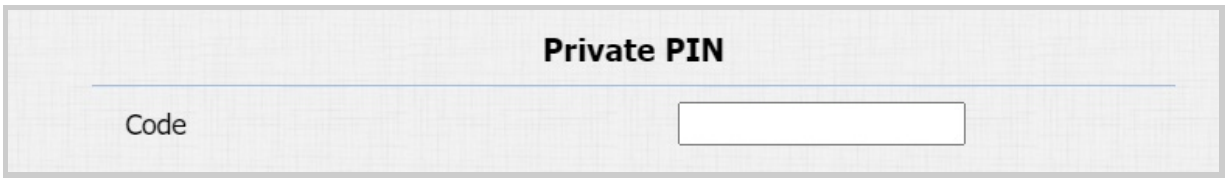
To add a user, go to **Intercom > User** interface and click **+Add**.



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

Unlock by Private PIN Code

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



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

Tip

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

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



Unlock by RF Card

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



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

Note

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

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



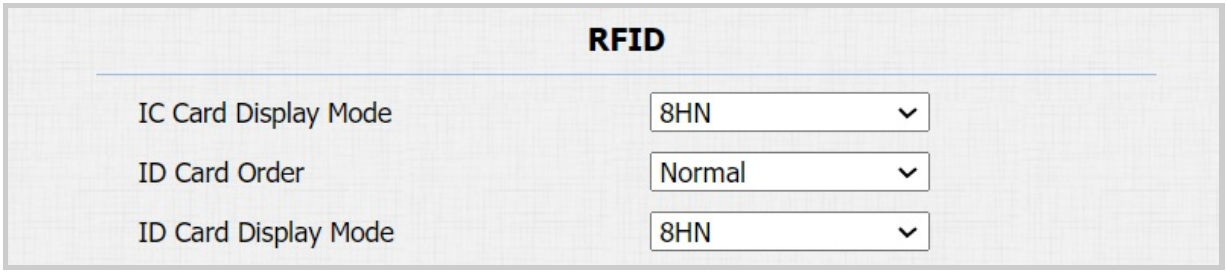
Tip

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

RF Card Code Format

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

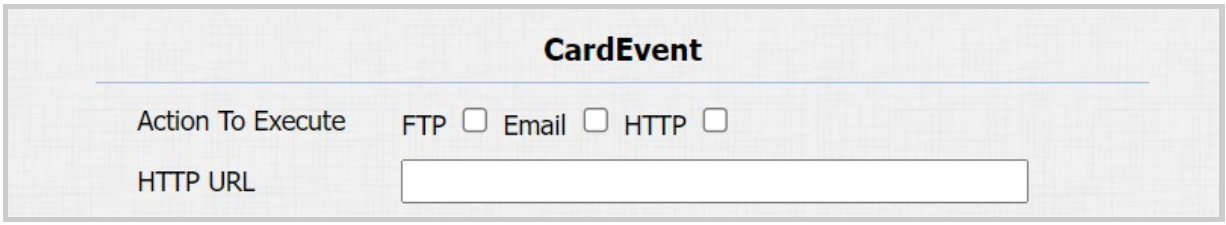
To set it up, go to **Intercom > Card Setting > RFID** interface.



- **IC/ID Card Display Mode**: Set the card number format from the provided options: 8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26), and 8HR10D.
- **ID Card Order**: Set the ID card reading mode between Normal and Reversed.

Actions Triggered by Swiping Cards

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



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

Unlock by License Plate

Akuvox offers two main ways to identify vehicles and open gates.

- Use a third-party LPR(License Plate Recognition) camera to recognize the license plate of the vehicle.
- Use the Akuvox long-range card reader ACR-CPR12 to recognize the UHF card attached to the vehicle's windshield.

To assign the license plate to a user, find the **License Plate** part on the **Directory > User > +Add** interface.

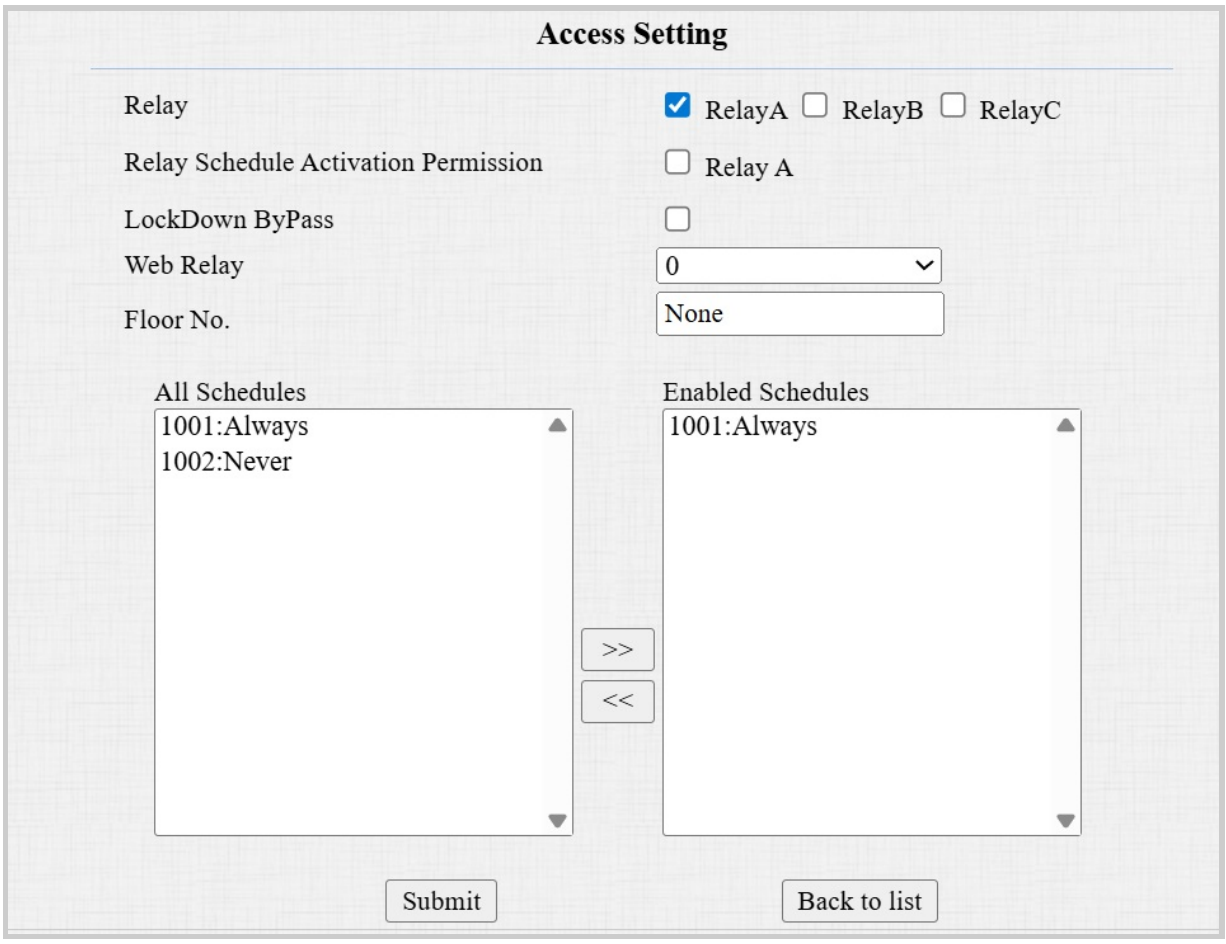


- **Add**: A user can have up to 5 license plates.
- **Duration**: Enable/disable Long-term Vehicle. It is enabled by default. If disabled, specify when the vehicle can enter or exit the parking lot.

Access Setting

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

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



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

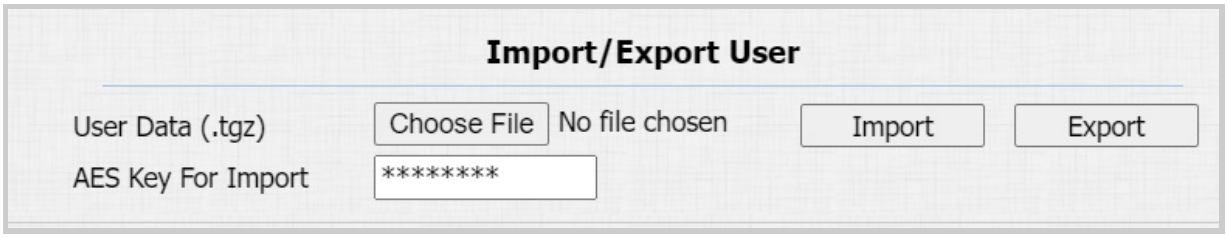
Import/Export User Data

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

Click here to view how to import and export user data between Akuvox door phones.

To set it up, go to the **Intercom > User > Import/Export User** interface. You can add 5,000 users.

The import/export file should be in TGZ format.

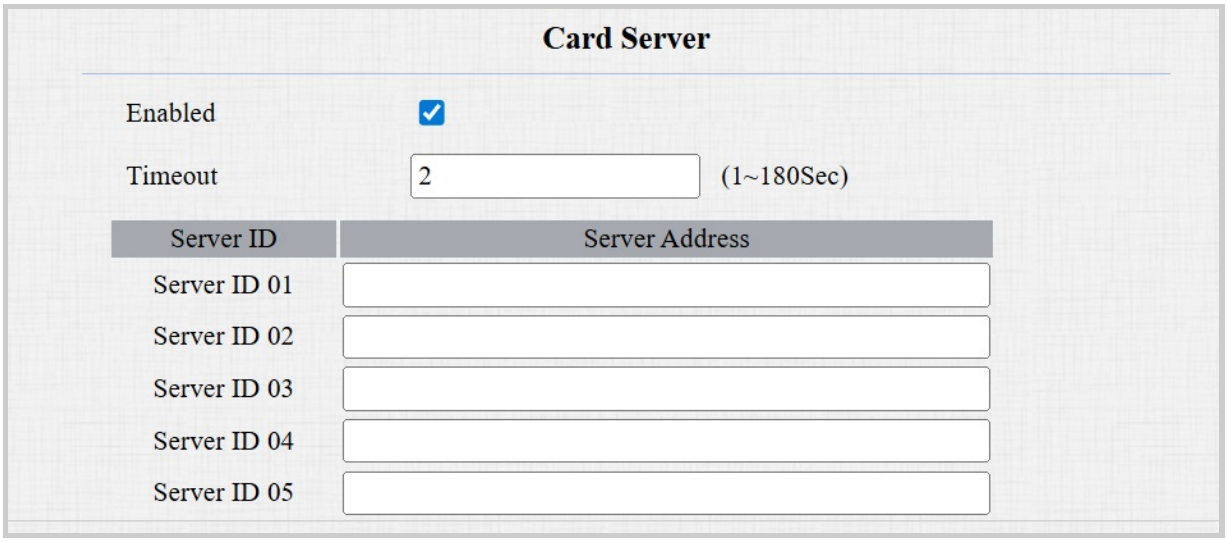


- **AES Key For Import**: When the imported file is encrypted, enter its password here.

Send Card Numbers to Third-Party Servers

The device supports sending card numbers to third-party servers when users swipe cards.

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



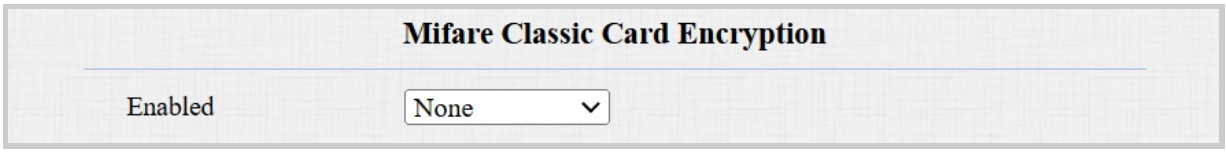
- **Enabled**: Once enabled, when users swipe cards, the device will play a Di sound.
- **Timeout**: Define the timeout of sending the card number(1~180 seconds).
    - For example, if it is set to 5 seconds, when the first server does not respond in 5 seconds, the device will try the next server.
    - This process continues through up to five servers until one of them responds.
    - If all five servers fail to respond, the device will repeat the cycle, with a maximum of three attempts in total.
- **Server Address**: Support up to 5 addresses in HTTP/HTTPS format with a maximum of 256 characters and no restrictions on special characters.

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 set it up, go to **Intercom > Card Setting > Mifare Classic 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.
- **Plus**: There are three block choices. The device can read the encrypted data in SL1 and SL3.
    - **Block**: The block number where the encrypted data is located.
    - **SL3**: The key number within 32 bits.

- **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 16.
  - **Crypto**: The encryption method. It is AES by default.
  - **Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.

Unlock by NFC

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

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



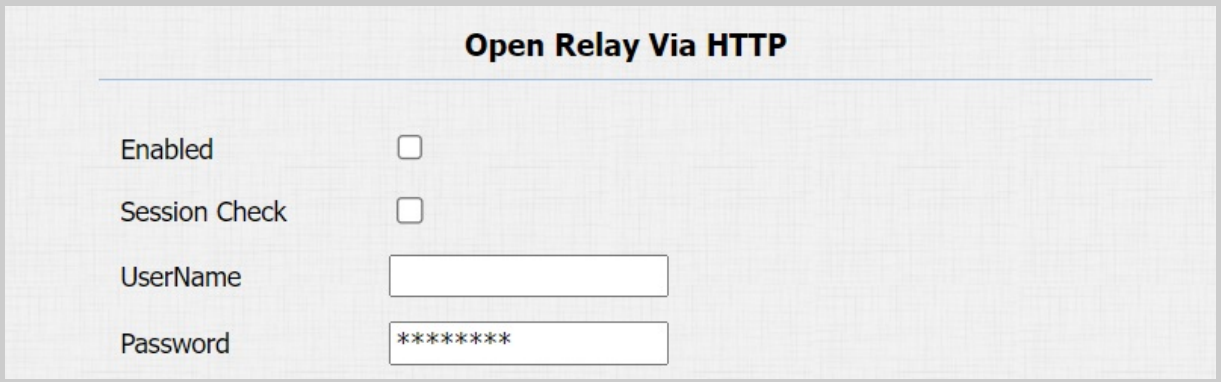
Note

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

Unlock by HTTP Command

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

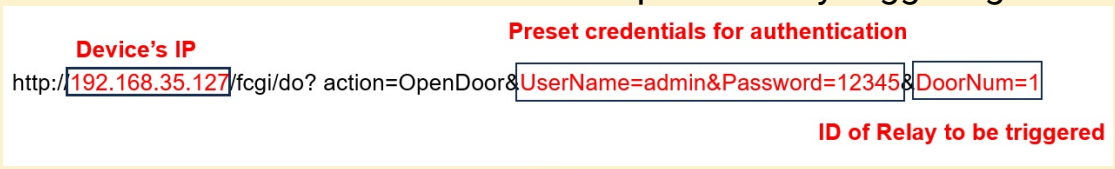
To set it up, go to **Intercom > Relay > Open Relay Via HTTP** interface.



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

Tip

Here is an HTTP command URL example for relay triggering.



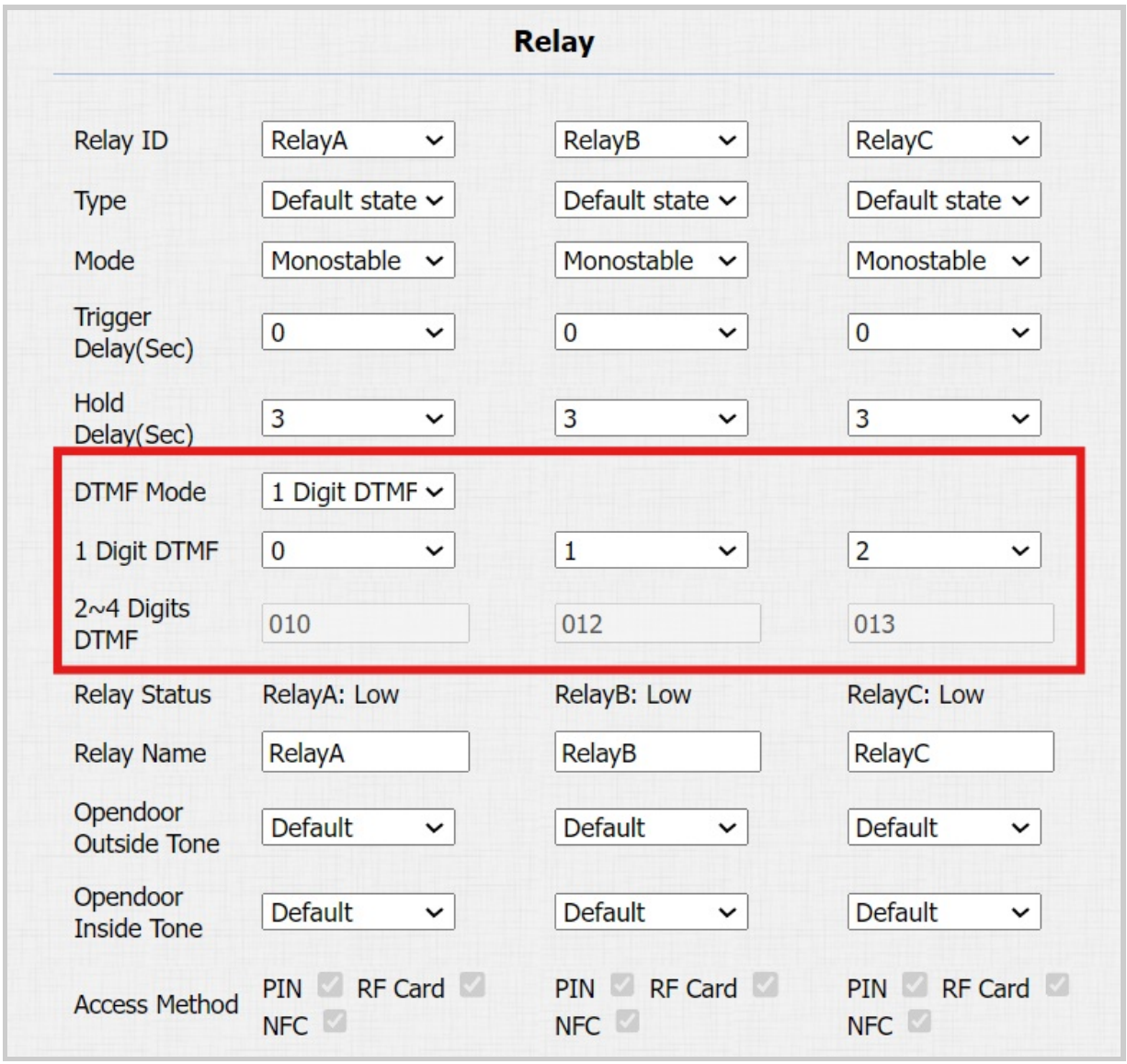
Note

Click **here** to view how to set up door opening by HTTP commands.

Unlock by DTMF Code

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

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



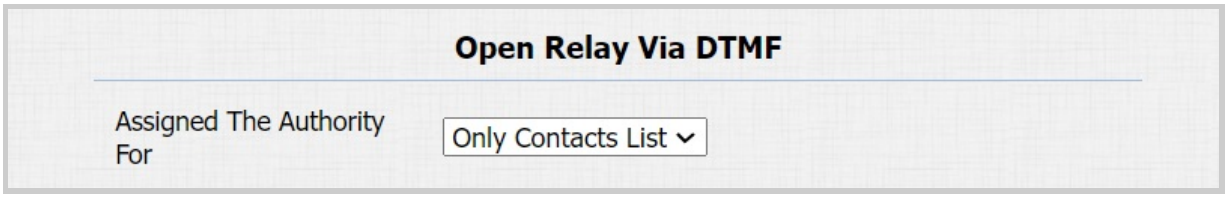
- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

Note

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

DTMF White List

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



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

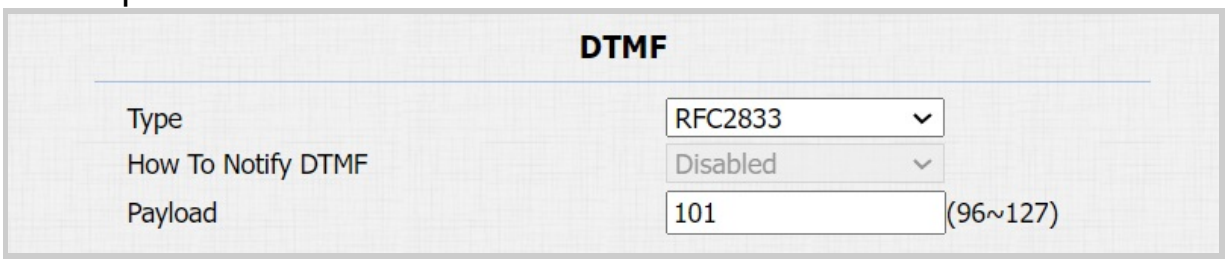
DTMF Data Transmission

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

DTMF Type Differences:

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

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



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

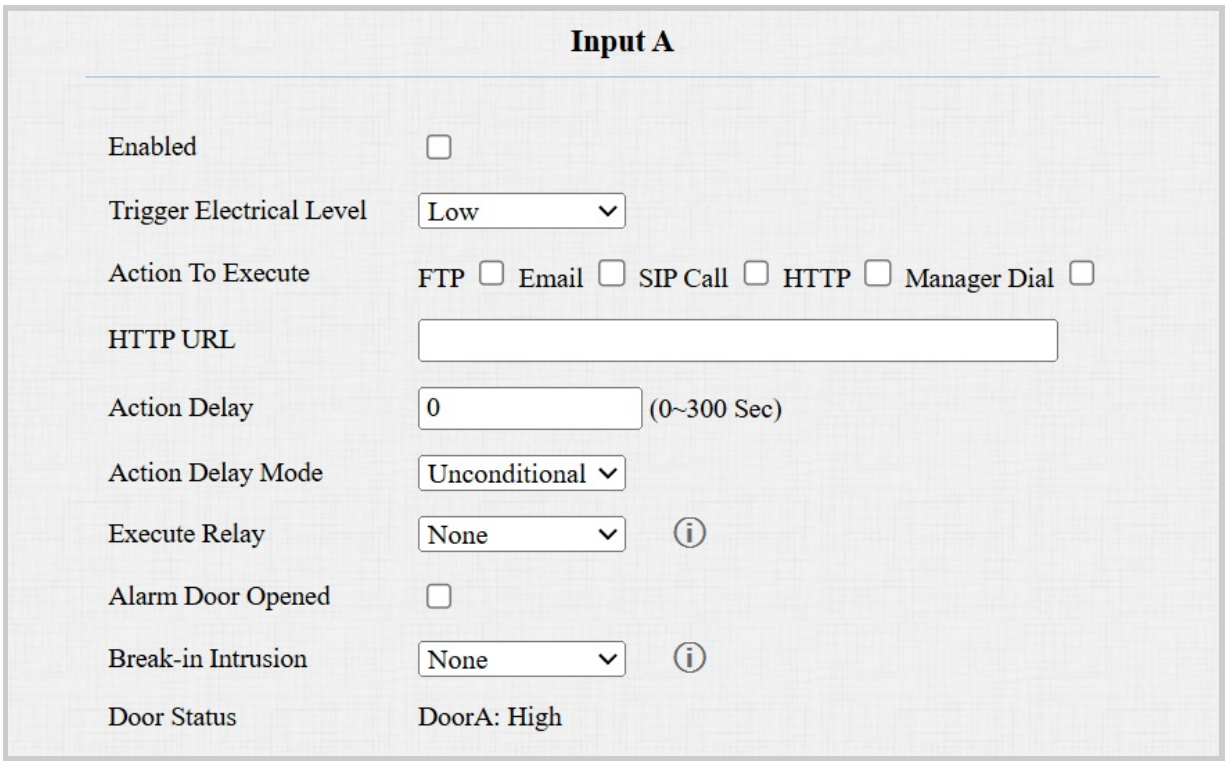
- **Payload**: Set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

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 **Intercom > Input** interface.



- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at a low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
    - **FTP**: Send a screenshot to the preconfigured FTP server.
    - **Email**: Send a screenshot to the preconfigured Email address.
    - **SIP Call**: Call the preset number upon the trigger.

    - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
    - **Manager Dial**: When the input is triggered, a call will be made to the number(s) set on the **Intercom > Basic > Manager Dial** interface.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode**:
    - **Unconditional Execution**: The action will be carried out when the input is triggered.
    - **Execute If Input Still Triggered**: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Alarm Door Opened**: If enabled, when the door-opening time exceeds a limit, an alarm will be triggered.
    - **Door Opened Timeout**: The door-opening time limit.
- **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. Click here to learn more information about this feature.
- **Door Status**: Display the status of the input signal.

Monitor and Image

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

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

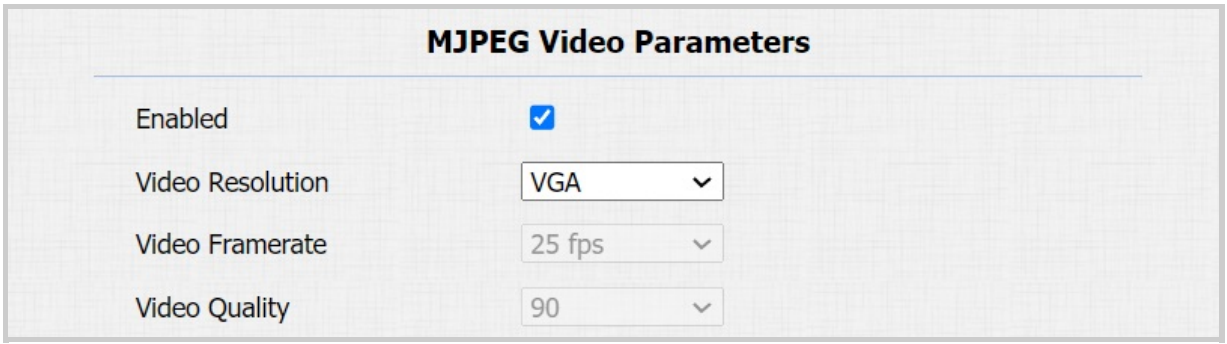
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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

MJPEG Video Stream

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

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

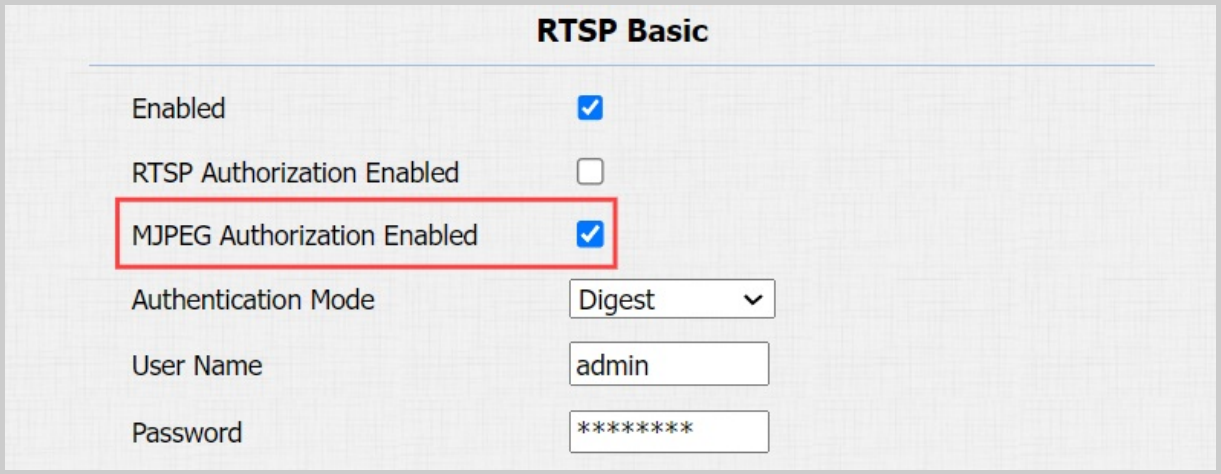


- **Video Resolution**: Specify the video resolution from the lowest CIF(352×288 pixels) to the highest 1080P(1920×1080 pixels).
- **Video Framerate**: It is 25 fps by default.
- **Video Quality**: It is 90 by default.

MJPEG Authorization

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

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



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

Tip

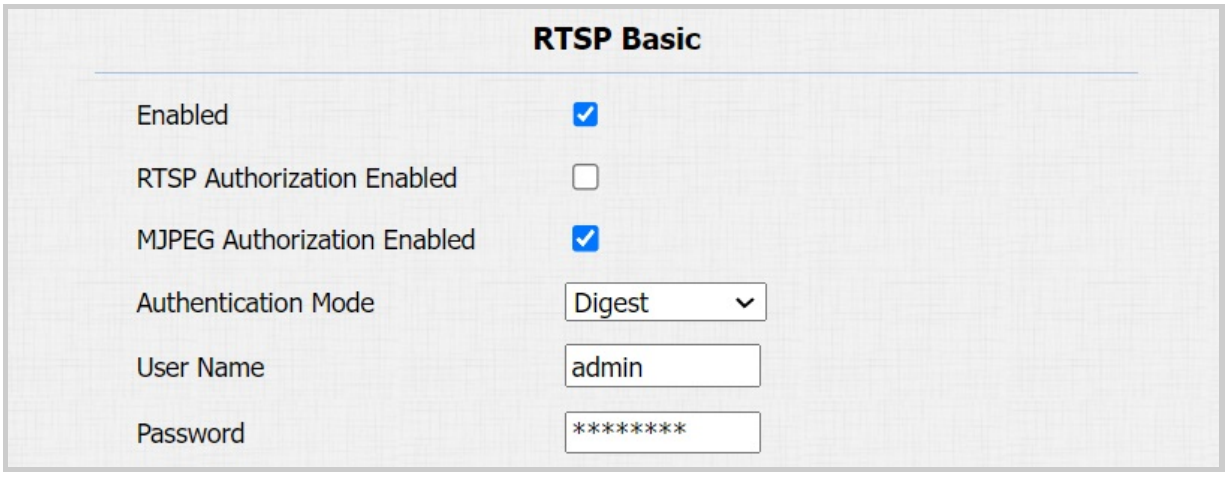
- To view a dynamic stream, use the URL http://device_IP:8080/video.cgi.
- For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi
- For example, if you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

RTSP Stream Monitoring

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.

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



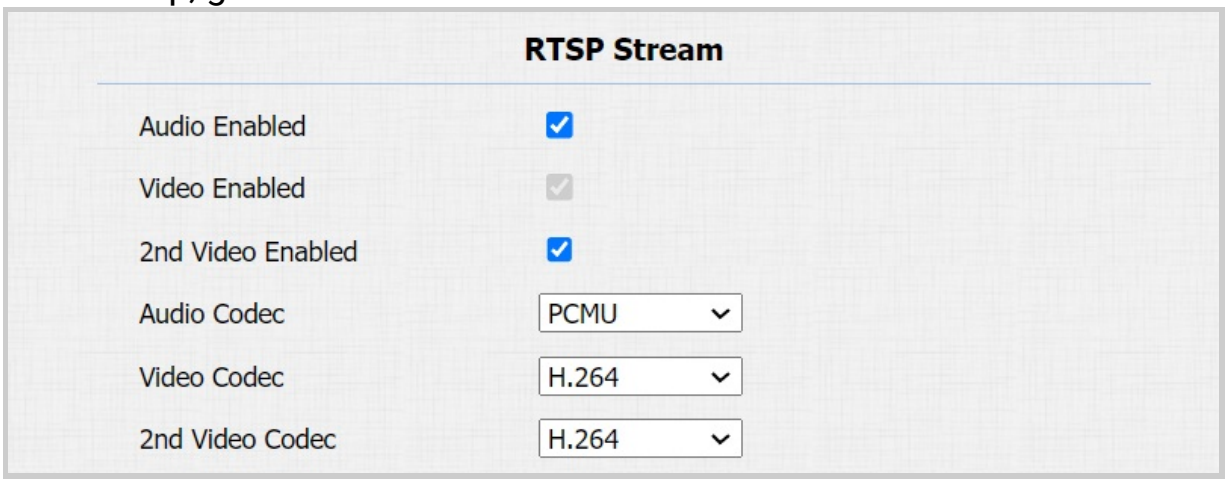
- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.

- **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 Basic Setting

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

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



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

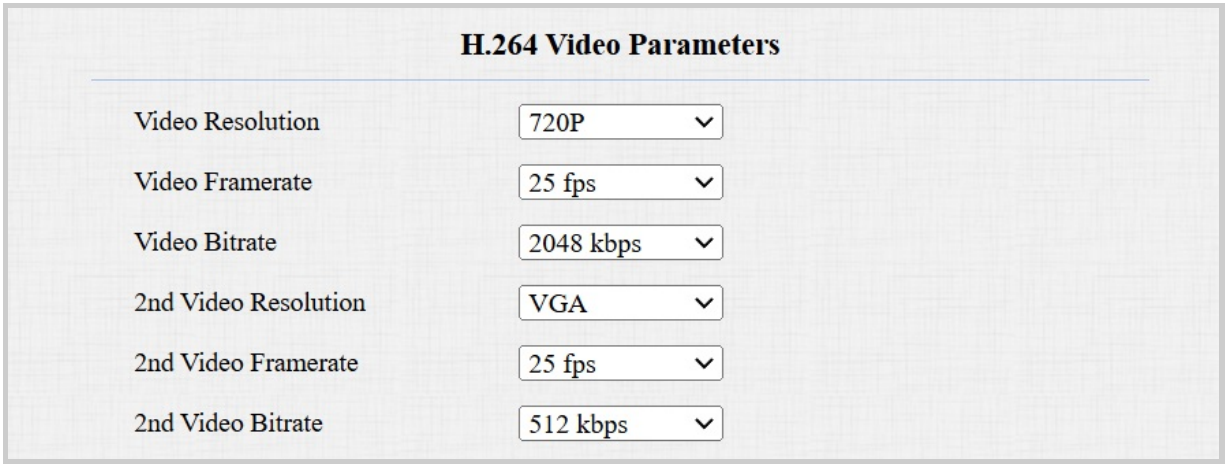
Tip

To view the audio and video stream using RTSP:

- First channel: rtsp://Device's IP/live/ch00_0
- Second channel: rtsp://Device's IP/live/ch00_1

H.264 Video Parameters Setup

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

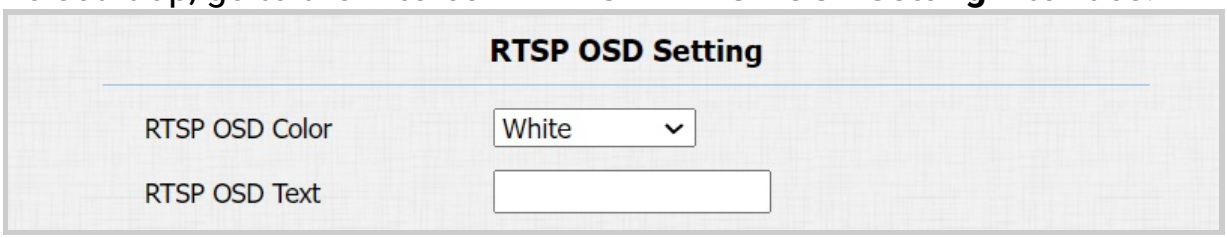


- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920×1080 pixels).
- **Video Framerate**: Frames per second refers to how many frames are displayed in one second of video.
- **Video Bitrate**: The amount of video data transferred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

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture. To protect the owner of the video or image.

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



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

NACK

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

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

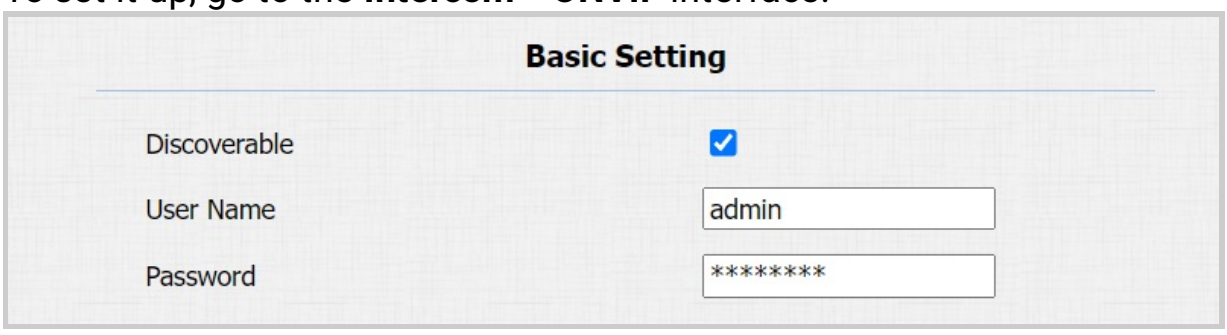


ONVIF

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

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

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

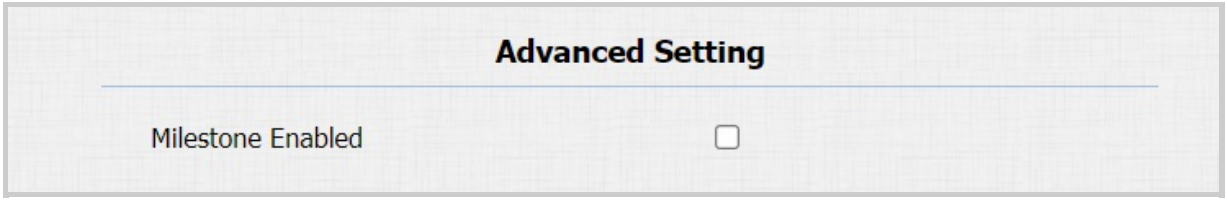


- **Discoverable**: When enabled, the video from the door phone camera is searchable by other devices.
- **User Name**: Set the username required for accessing the door phone's video stream on other devices. It is admin by default.
- **Password**: Set the password required for accessing the door phone's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

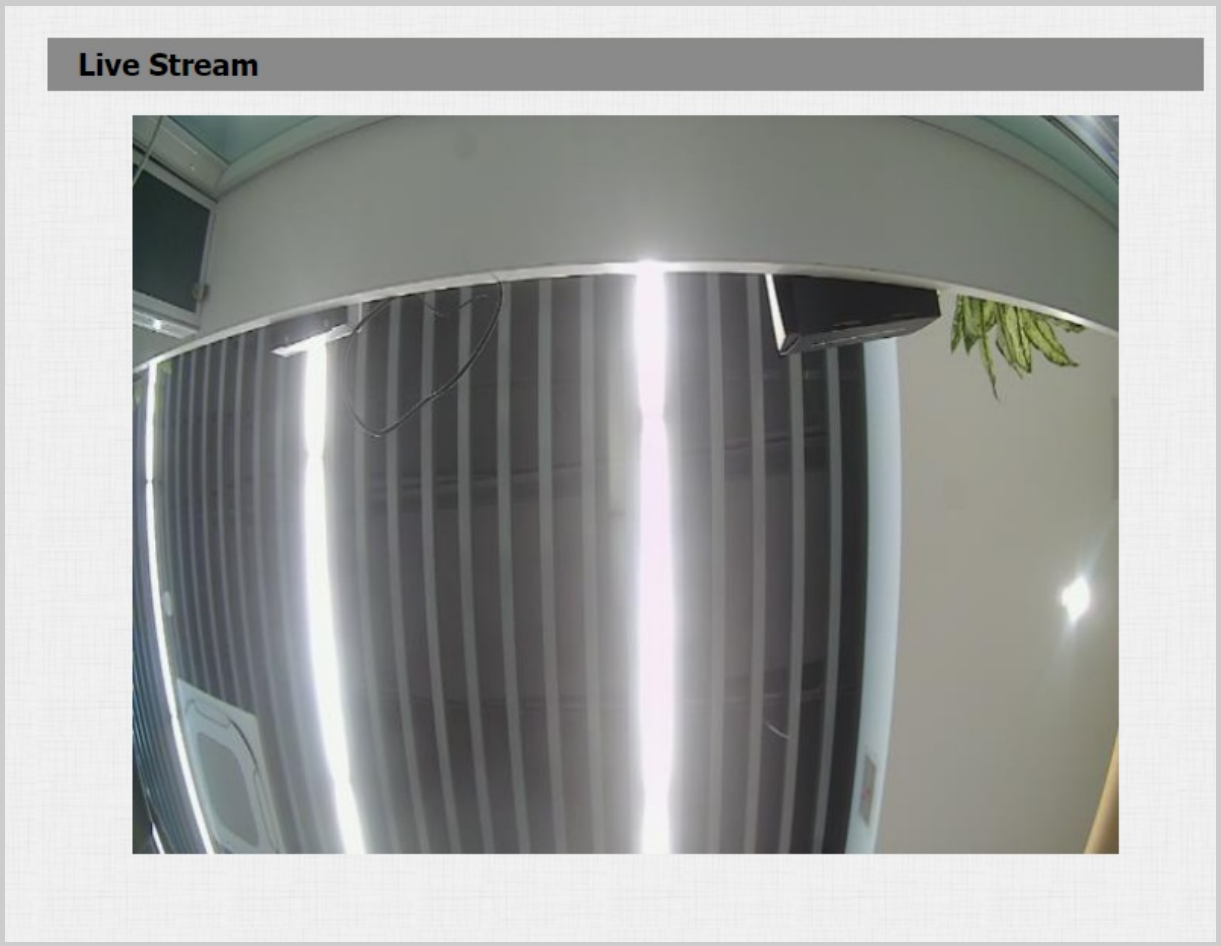
Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.



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.

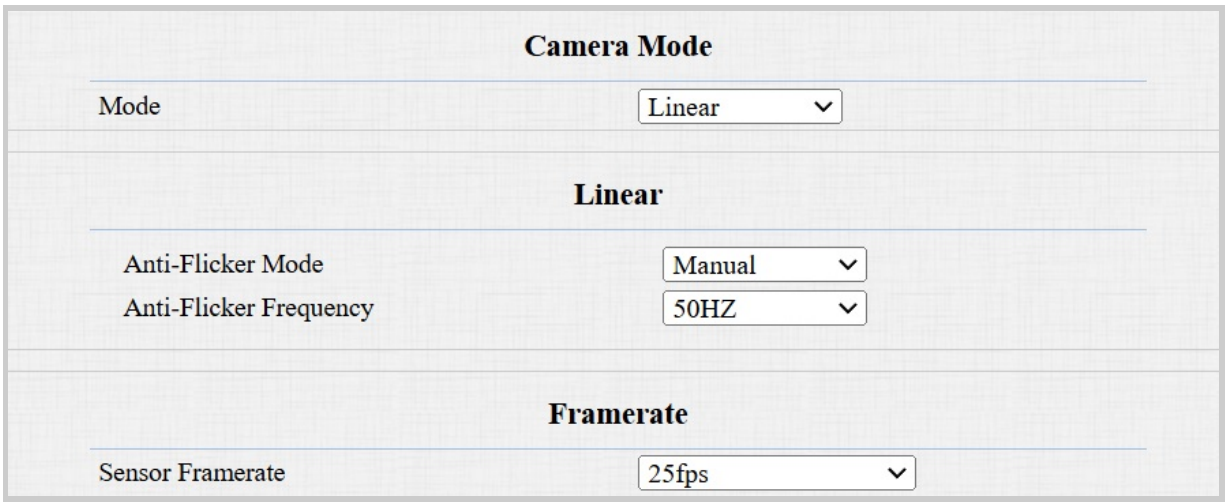
View the video stream on the **Intercom > Live Stream** interface. If you have enabled RTSP authorization, you need to enter the user name and password set in the RTSP Basic section for viewing the stream.



Camera Mode

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

You can set the camera mode between HDR and Linear on the **Phone > Camera** interface.

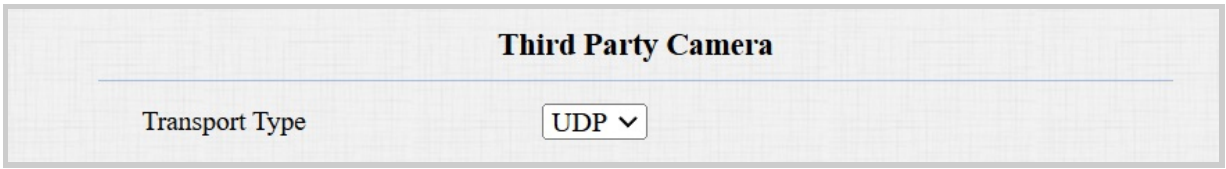


- **Anti-Flicker Mode**: The anti-flicker feature reduces or eliminates flickering in images or videos caused by varying light sources.
  - **Auto**: The device will switch automatically between 50 Hz and 60 Hz anti-flicker frequency.
  - **Manual**: Select the anti-flicker frequency manually between 50 Hz and 60 Hz.
  - **Off**: Disable the anti-flicker function.
- **Anti-Flicker Frequency**: Select the anti-flicker frequency between 50 Hz and 60 Hz.
- **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.

Data Transmission Type for Third-party Camera

You can select the data transmission type between the device and a third-party camera when it is connected to the SmartPlus Cloud.

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



- **UDP**: An unreliable but very efficient transport layer protocol.

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

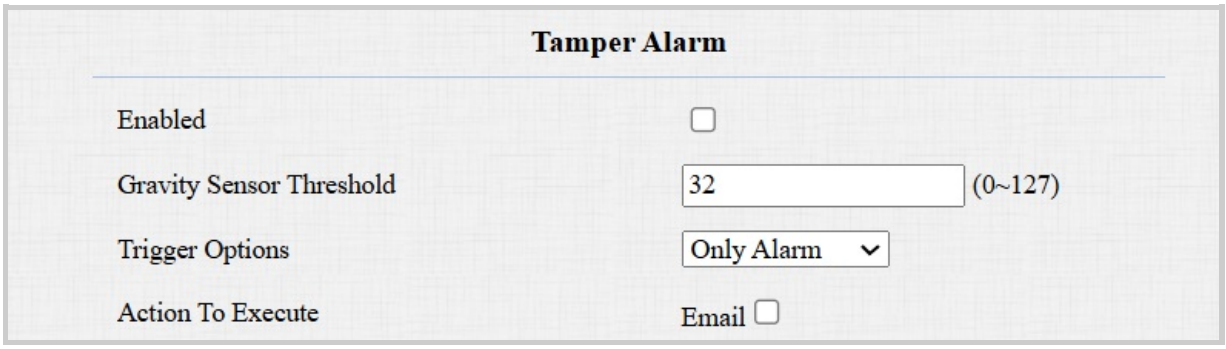
Security

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.

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



- **Gravity Sensor Threshold**: The threshold for the gravity sensor sensitivity. The lower the value is, the easier the tamper alarm will be triggered. It is 32 by default.
- **Trigger Options**: Select what can be triggered when the gravity sensor is triggered.
- **Action To Execute**: When the tamper alarm is triggered, the device can send a screenshot to the pre-configured email address.

Client Certificate Setting

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

Web Server Certificate

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

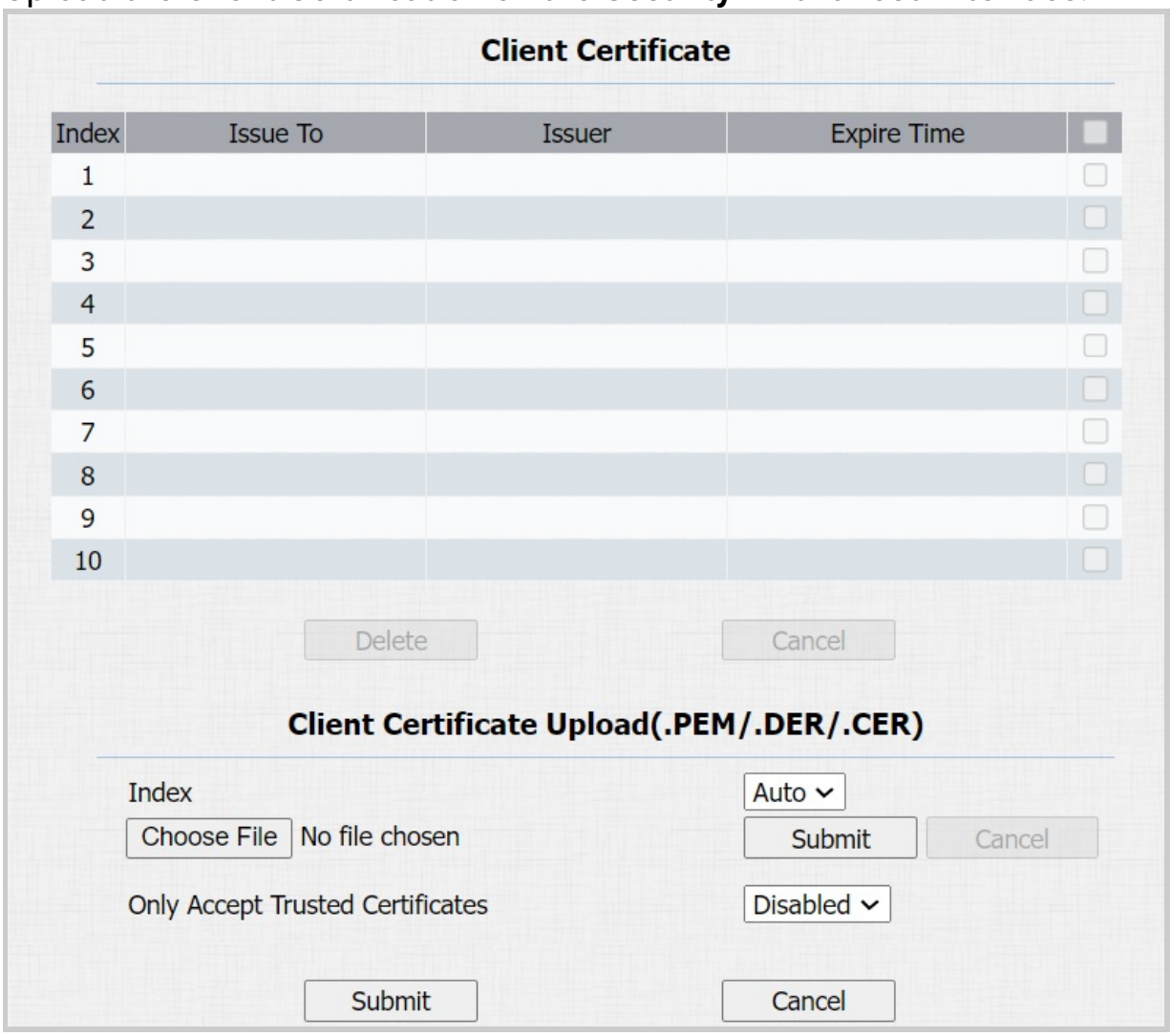
Upload the Web Server Certificate on the **Security > Advanced** interface.



Client Certificate

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

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

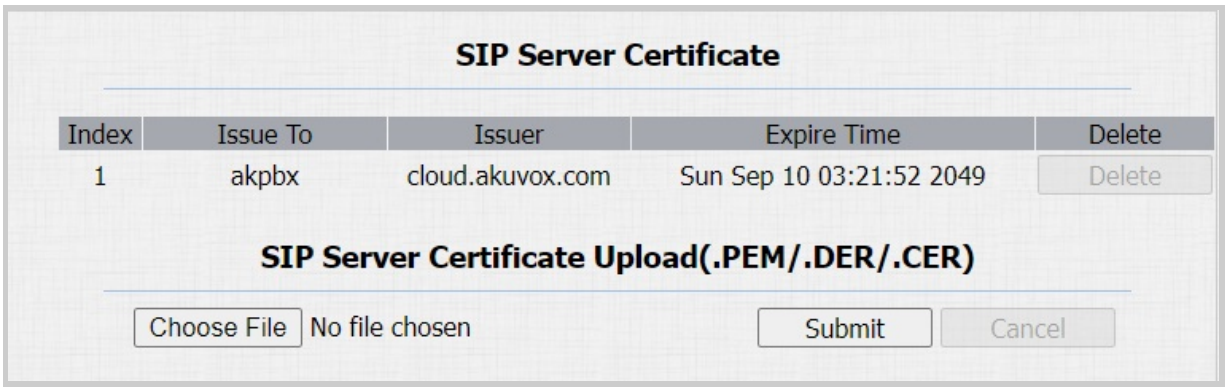


- **Index:**
  - **Auto**: The uploaded certificate will be displayed in numeric order.
  - **1 to 10**: The uploaded certificate will be displayed according to the value selected.
- **Upload:** Click Choose File to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, as long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

Upload TLS Certificate for SIP Account Registration

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

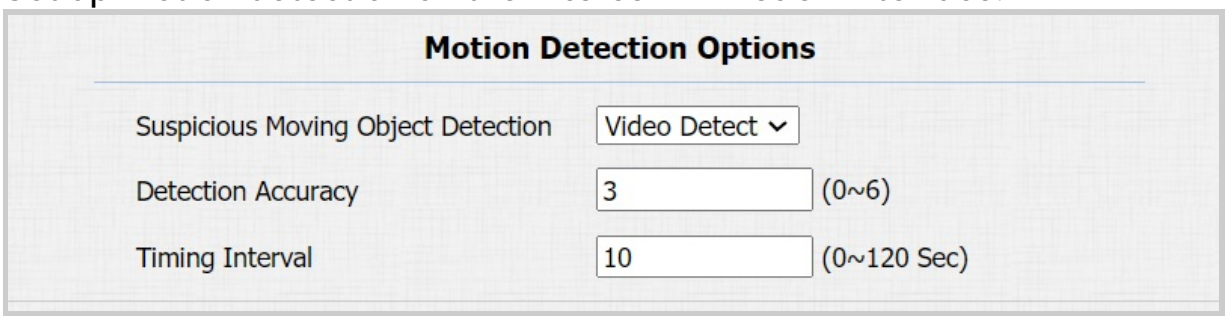
To upload the TLS certificate, go to **Security > Advanced > SIP Server Certificate** interface.



Motion Detection

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

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

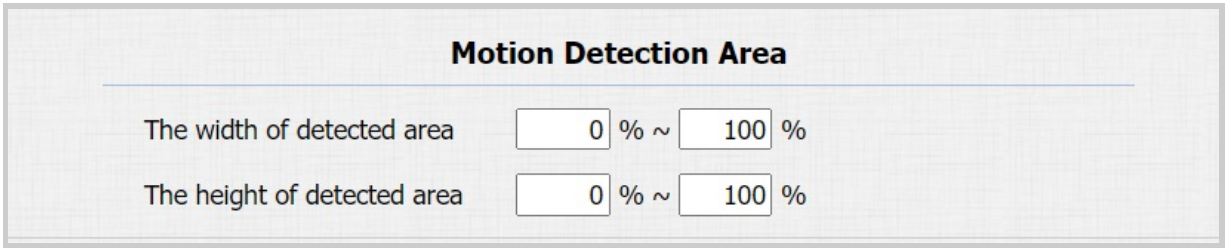


- **Suspicious Moving Object Detection**:
  - Disabled: Turn off the motion detection function.
  - IR Detection: When the infrared sensor detects moving objects, preset actions will be triggered.
  - Video Detection: When the video camera detects moving objects, preset actions will be triggered.
- **Detection Accuracy**: The detection sensitivity. Specify this option when selecting **Video Detection**. The greater the value is, the more accurate the detection is. The default value is 3.

- **Timing Interval**: 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.

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

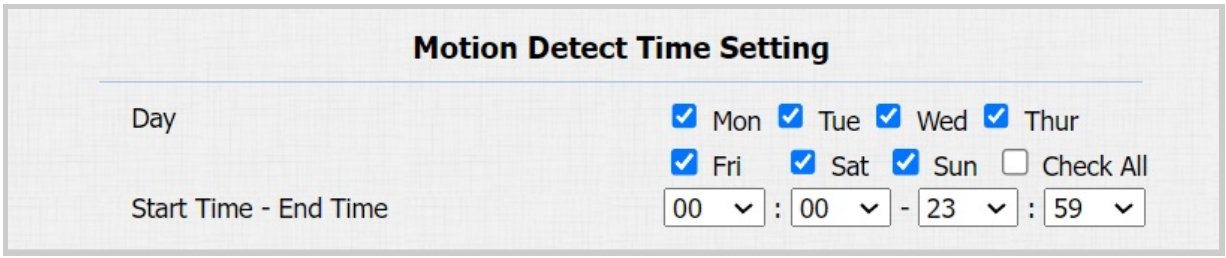
The full size of the detection area is calculated by percentage (100%) from left to right. Pick the horizontal detection range anywhere from 0% to 100%, and pick the vertical detection range anywhere from 0% to 100%.



Motion Detection Schedule

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

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



Security Notification

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

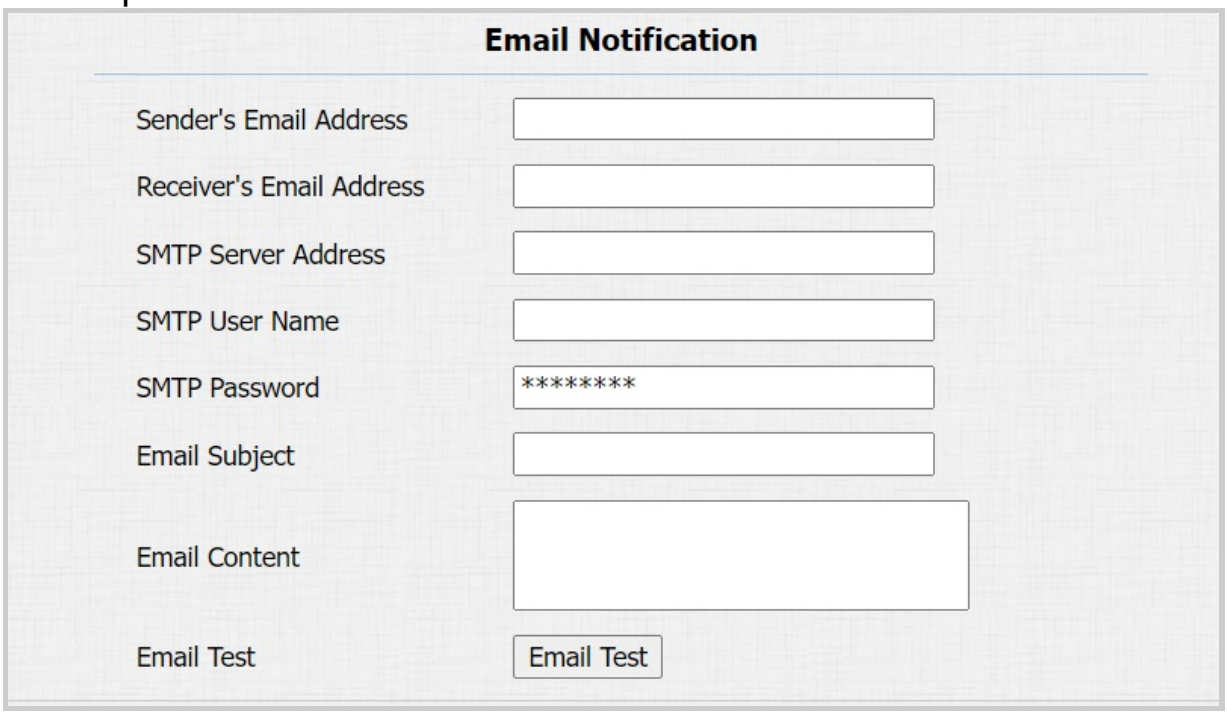
To set up security notifications, go to **Intercom > Action** interface.

Email Notification

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

Click here to view how to set this feature up.

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



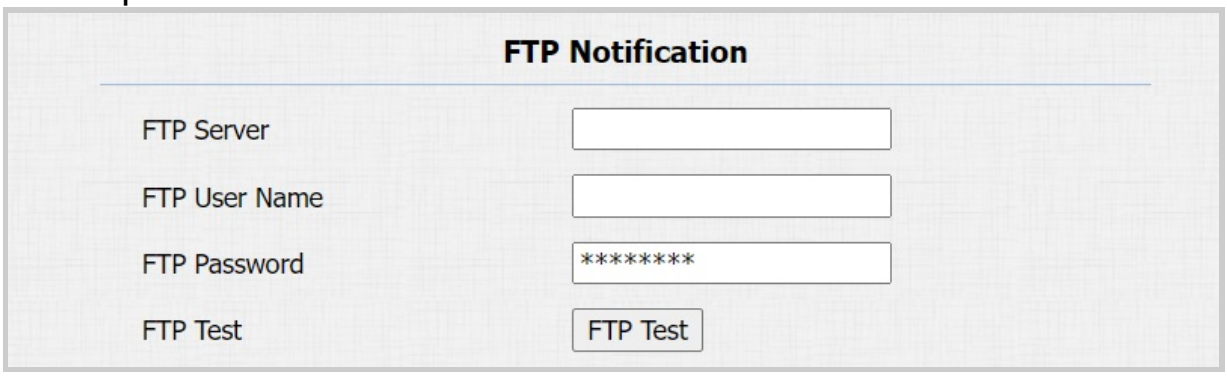
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

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.

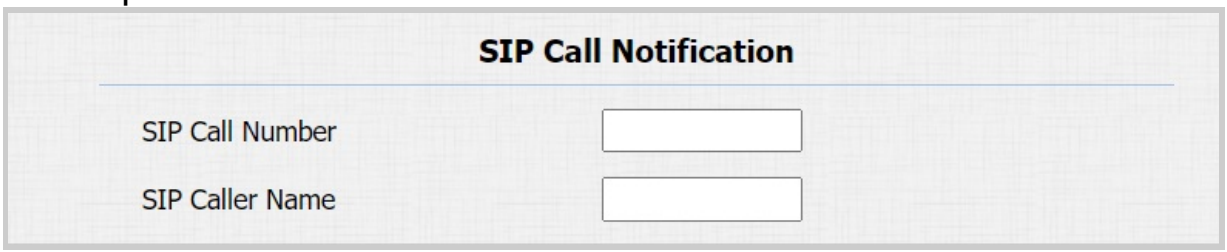


- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

SIP Call Notification

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

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



Action URL

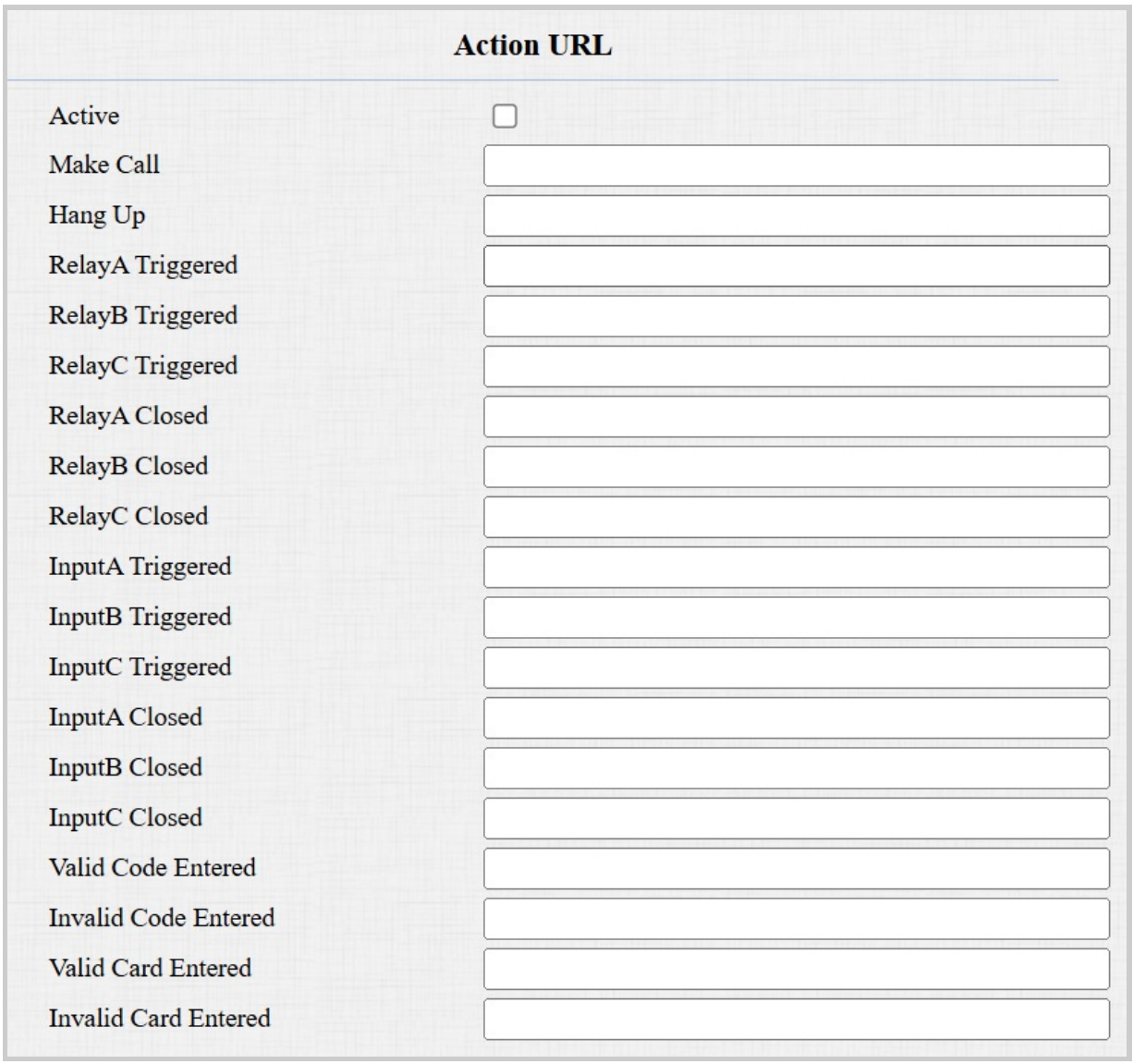
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

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

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

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



Whitelist Of Make Call Action

You can specify SIP or IP numbers to trigger the action URL in the **Make Call** field. This feature can be used in scenarios where only calls to the doctor's office number can trigger this URL to open the door.

Set it up on the **Phone > Action URL** interface.



- **Enabled**: It is disabled by default.
- **IP/SIP address**: You can add up to 10 numbers.

Voice Encryption

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

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

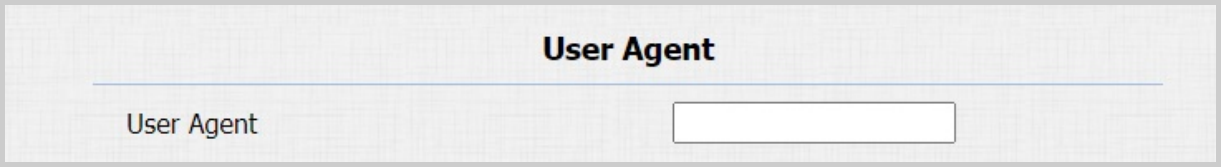


- **Voice Encryption(SRTP):** Choose Disabled, Optional, or Compulsory for SRTP. If **Optional** or **Compulsory** is selected, the voice during the call is encrypted, and you can grab the RTP packet to view it.

User Agent

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

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

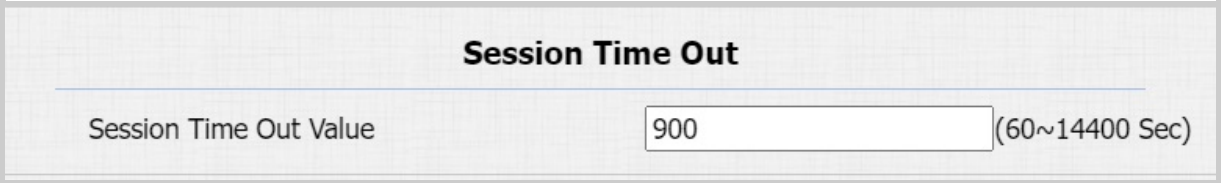


- **User Agent:** Akuvox is by default.

Web Interface Automatic Log-out

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

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



High Security Mode

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

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



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.

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



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

Emergency Action

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

Click here to view the detailed configuration of this feature.

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

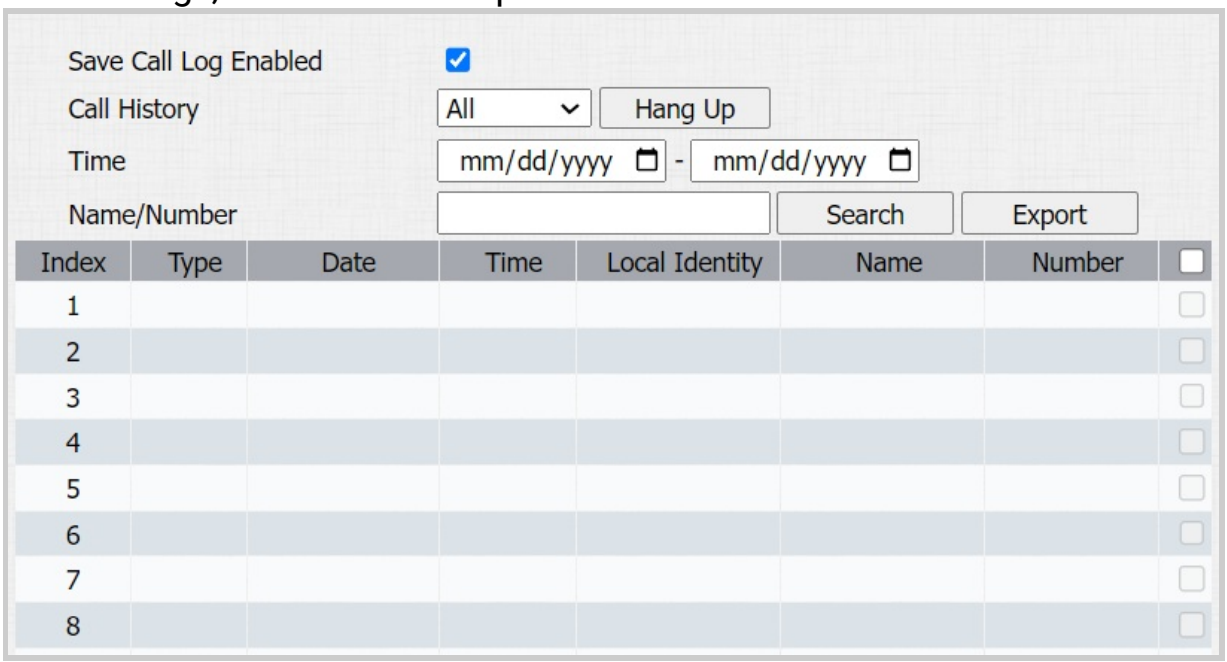


Logs

Call Logs

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

Check call logs on the **Phone > Call Log** interface. The device supports 200 call logs, which can be exported in CSV format.

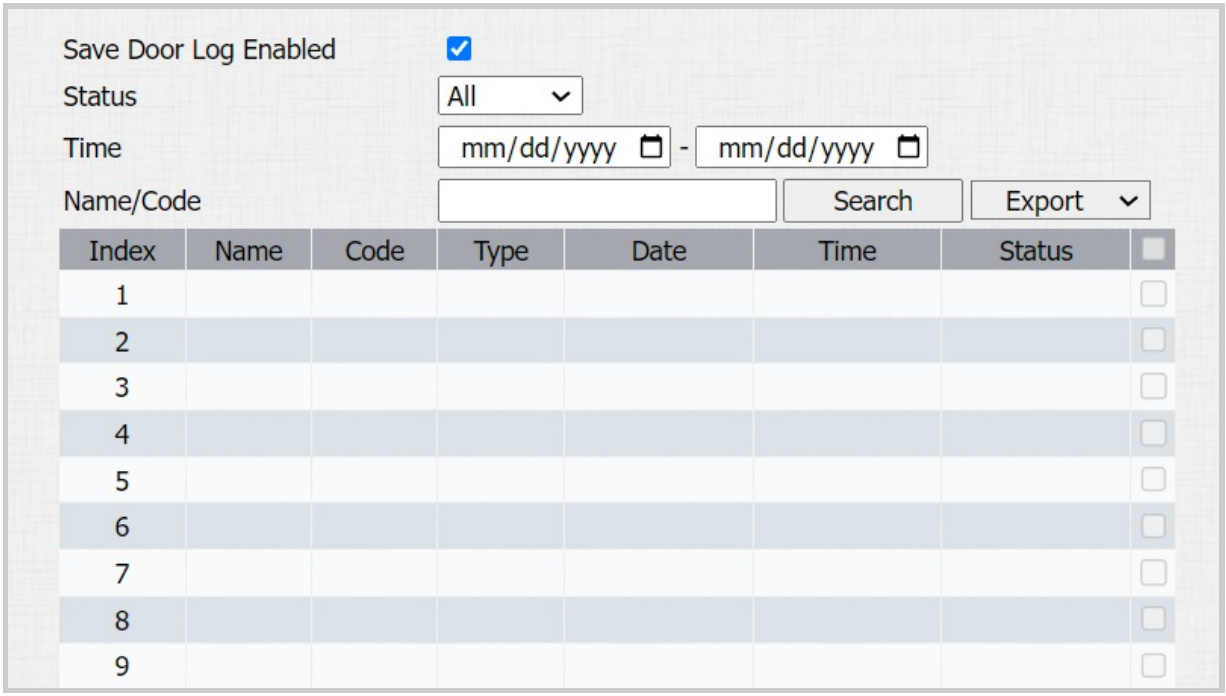


- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.

Door Logs

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

Check door logs on the **Phone > Door Log** interface. The device supports 200 door logs, which can be exported in XML or CSV files.

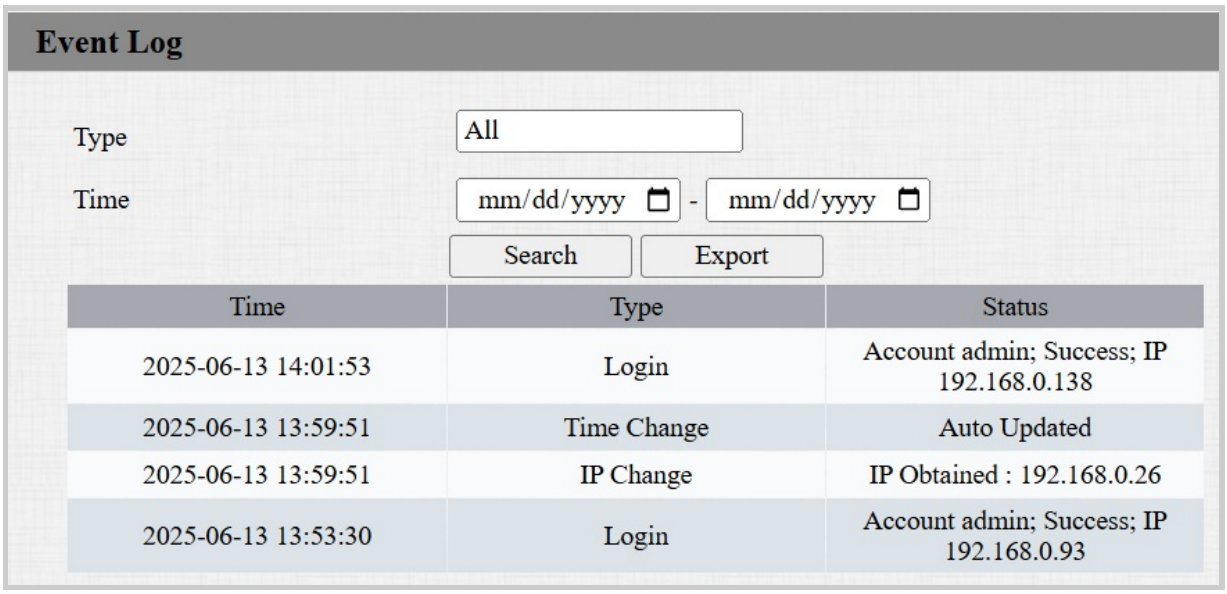


- **Status:** Display, All, Successful, or Failed door-opening records.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card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

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.

You can check the event logs on the **Phone > Event Log** interface. The device supports up to 100,000 logs, which can be exported in CSV format.

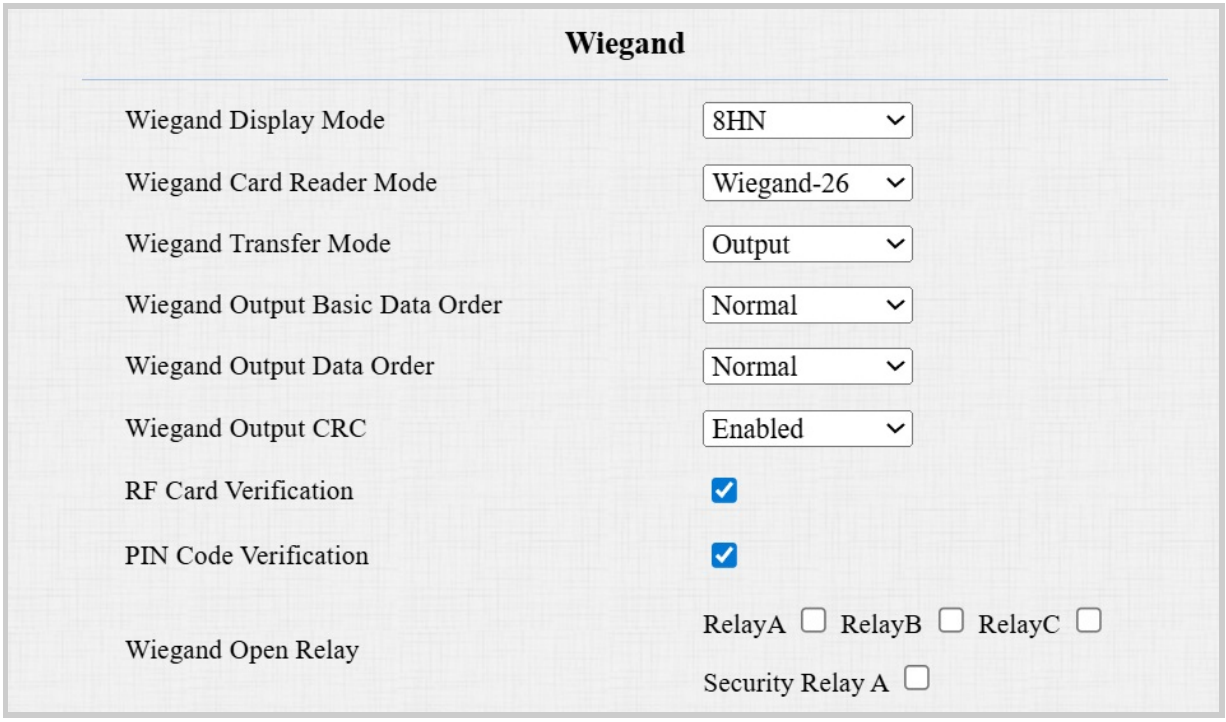

Event Log
Type
All
Time
mm/dd/yyyy
-
mm/dd/yyyy
Search
Export
Time
Type
Status
2025-06-13 14:01:53
Login
Account admin; Success; IP 192.168.0.138
2025-06-13 13:59:51
Time Change
Auto Updated
2025-06-13 13:59:51
IP Change
IP Obtained : 192.168.0.26
2025-06-13 13:53:30
Login
Account admin; Success; IP 192.168.0.93

Integration with Third-party Devices

Integration via Wiegand

The Wiegand feature enables the Akuvox device to act as a controller or a card reader.

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



- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device. It is automatically configured.
- **Wiegand Transfer Mode**:
    - **Input**: The device serves as a receiver.
    - **Output**: The device serves as a sender. If users can only open the door by swiping an RF card, select the Wiegand transfer mode as Output.

    - **Convert To Card No. Output**: The device serves as a sender. If users are assigned multiple door-opening methods, select the Wiegand transfer mode as Convert To Card No. Output.
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- **Wiegand Output Basic Data Order**: Set the sequence of the 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 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 CRC**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **RF Card/PIN Code Verification**: Available when **Output** or **Convert to Card No. Output** is selected.
    - When enabled, the device will verify whether the card code/PIN code is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the door phone screen.
    - When disabled, the door phone will not perform local verification.
- **Wiegand Open Relay**: Check the relay to be triggered through Wiegand.

Note

Click **here** to view more information on Wiegand settings including:

- Akuvox devices work as Wiegand input/output;
- Wiegand Card Reader Connection.

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

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



- **PIN**:
  - **8 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 8 bits, "11100001".
  - **4 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 4 bits, "0001".
  - **All at once**: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode.
- **PIN Output Basic Data Order**:
  - **Same as Global Settings**: Same as the Wiegand Output Basic Data Order.
  - **Normal**: Output the PIN data as it is before Wiegand conversion.
  - **Reversed**: Reverse the PIN data before Wiegand conversion.
- **PIN Output Data Order**:
  - **Same as Global Settings**: Same as the Wiegand Output Data Order.
  - **Normal**: Output the PIN data directly after the Wiegand conversion.
  - **Reversed**: Reverse the PIN data after the Wiegand conversion.

Note

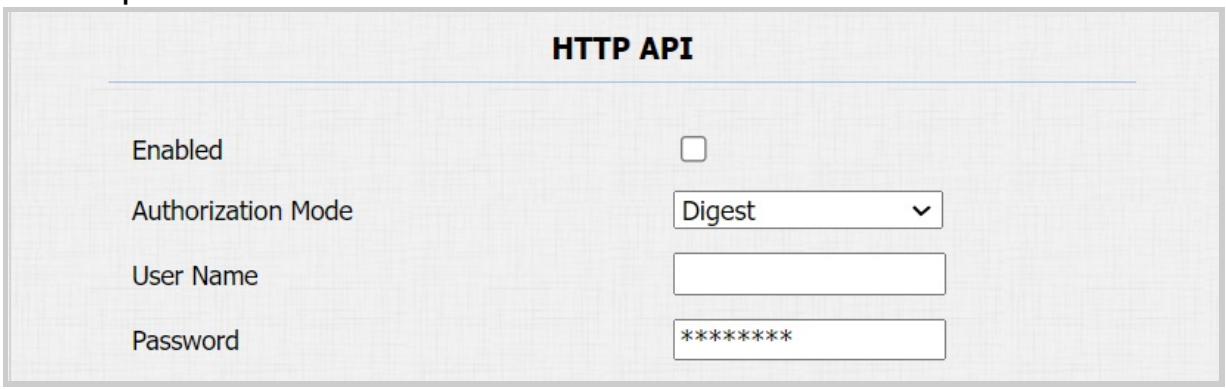
- The PIN output(basic) data order setting has the highest priority in the Wiegand output settings.
- For example, if the PIN is 1234 and you set the PIN output order to be Normal, the basic output data to be Reversed, and the Wiegand card reader mode to be Wiegand 34.
- The PIN data will be reversed before going through Wiegand 34 and output.

Original Data	Wiegand 34
000004D2	D2040000

Integration via HTTP API

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

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



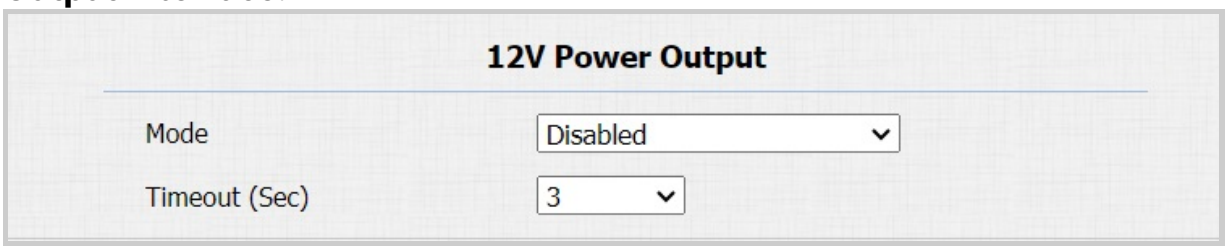
- **Enabled**: Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode**: It is Digest by default.
  - **Basic**: If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode of username and password.

    - **Digest**: The password encryption method only supports MD5(Message-Digest Algorithm). In the Authorization field of the HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
- **User Name**: Enter the user name for authentication. The default is admin.
- **Password**: Enter the password for authentication. The default is admin.

Power Output Control

The device can serve as a power supply for the external relays. Click here to view power output requirements.

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



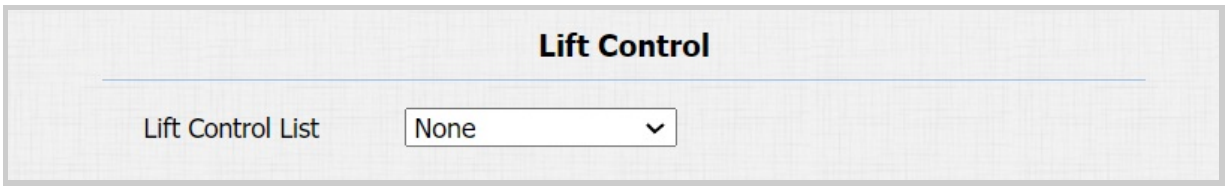
- **Power Output Type**:
    - **Always**: Provide continuous power to the third-party device.
    - **Triggered by Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.

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.

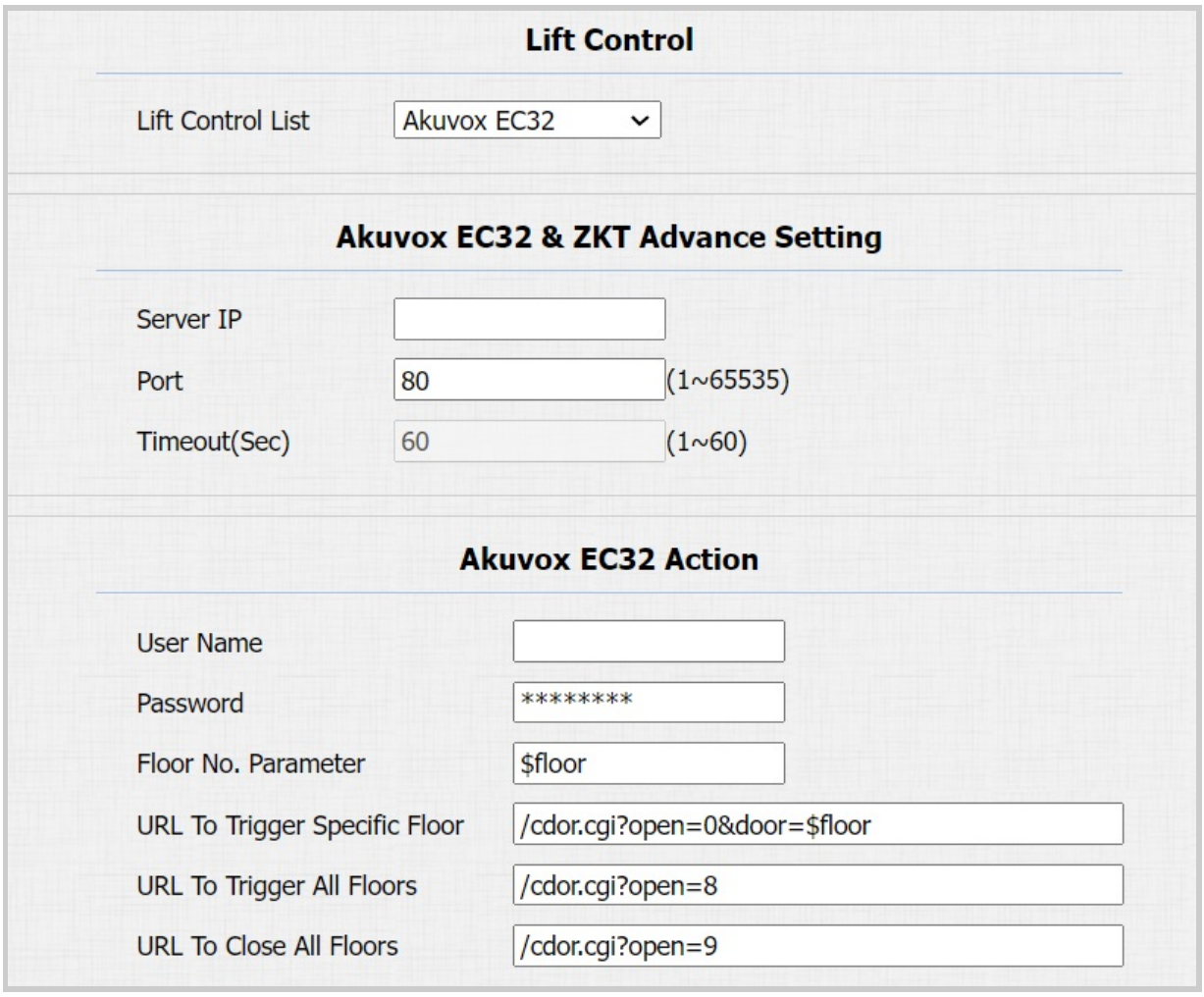
Set it up on the **Intercom > Lift Control** interface.



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

Akuvox Lift Controller

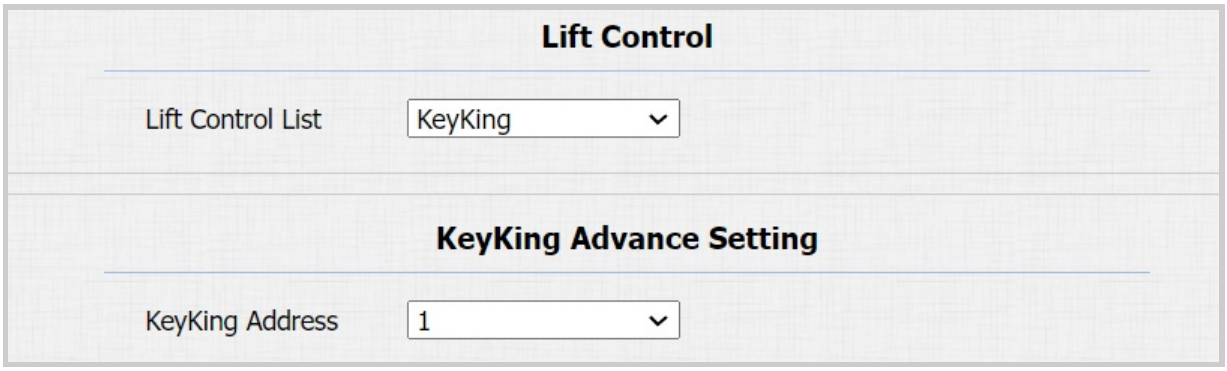
After selecting Akuvox EC32 in the Lift Control List, you need to set up relevant parameters.



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

KeyKing Lift Controller

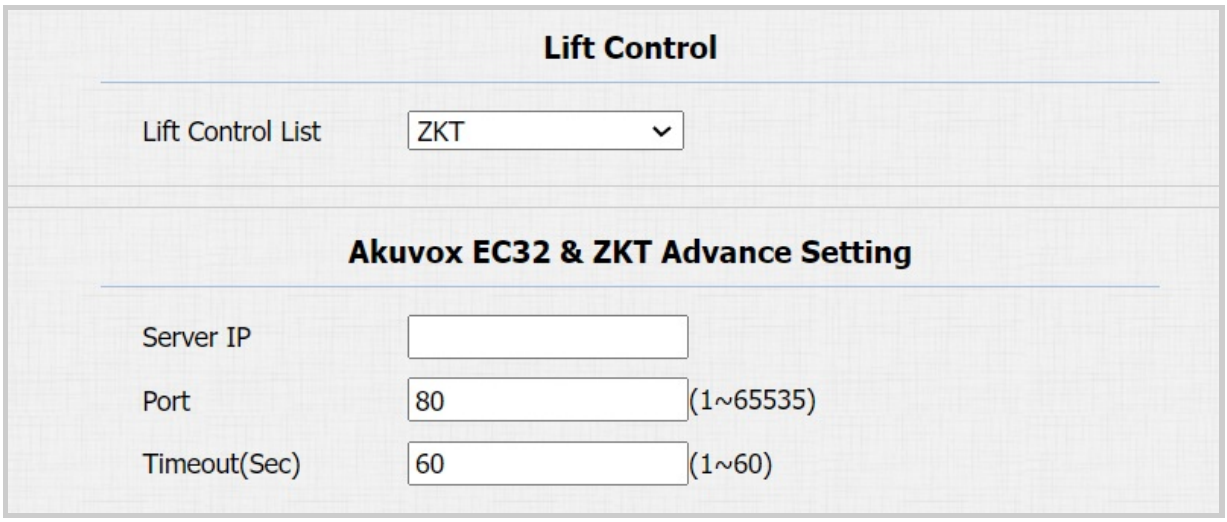
After selecting KeyKing, you need to set the KeyKing address.



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

ZKT Lift Controller

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



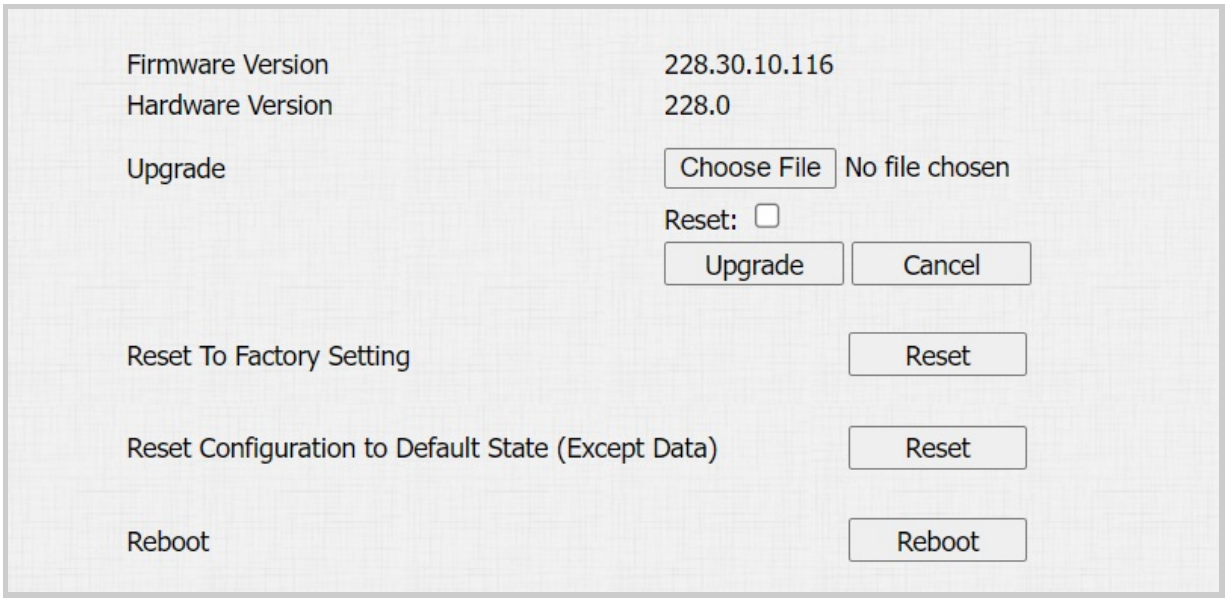
- **Server IP:** Enter the IP address of the controller server.
- **Port:** Enter the port of the controller server.
- **Timeout(Sec):** Decide the time limit within which users should press the lift button of their desired floors.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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

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



Note

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

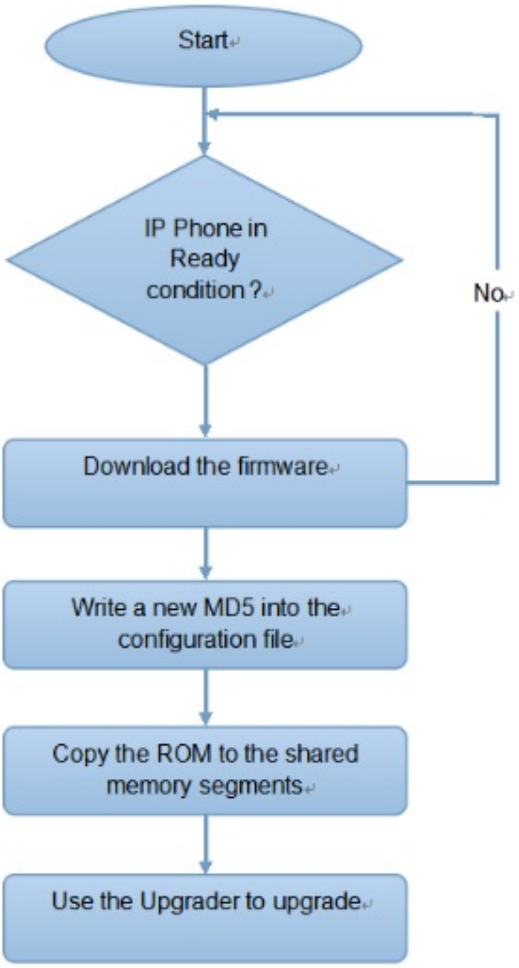
Auto-provisioning

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

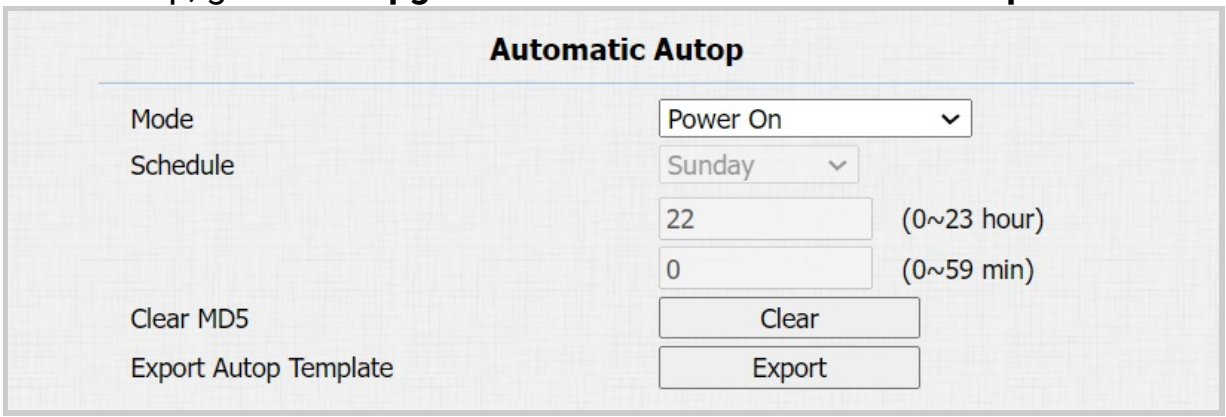
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

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

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



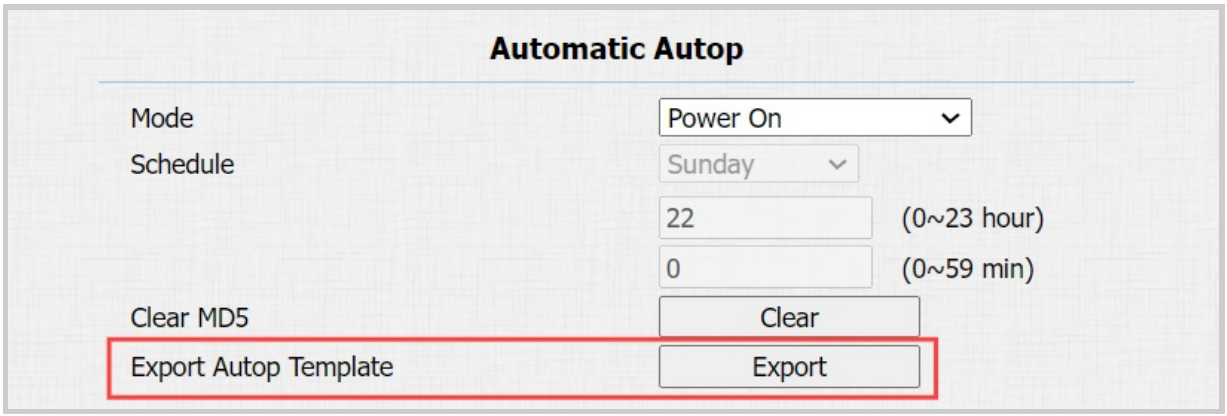
- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.

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

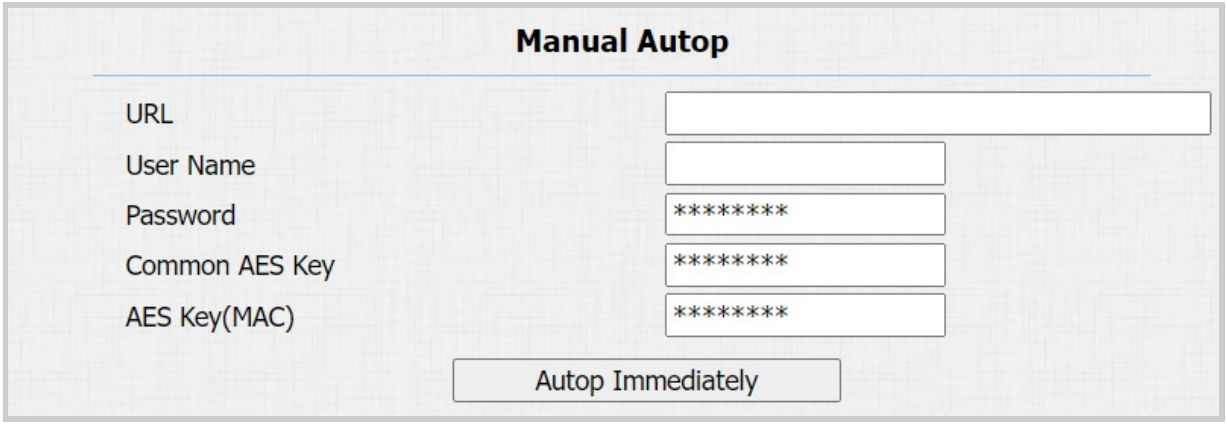
Static Provisioning

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

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



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



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

- **Username**: Enter the username if the server requires a username to be accessed.
- **Password**: Enter the password if the server requires a password to be accessed.
- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop configuration file.

Note

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

Tip

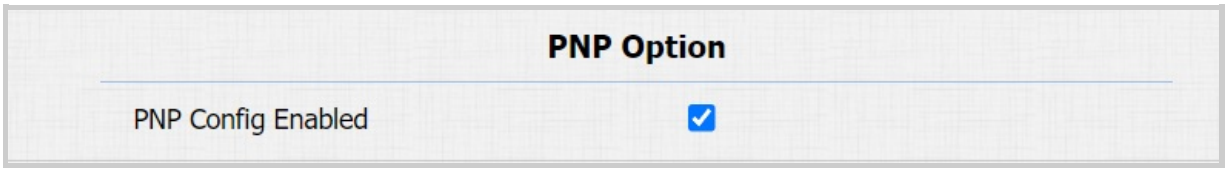
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

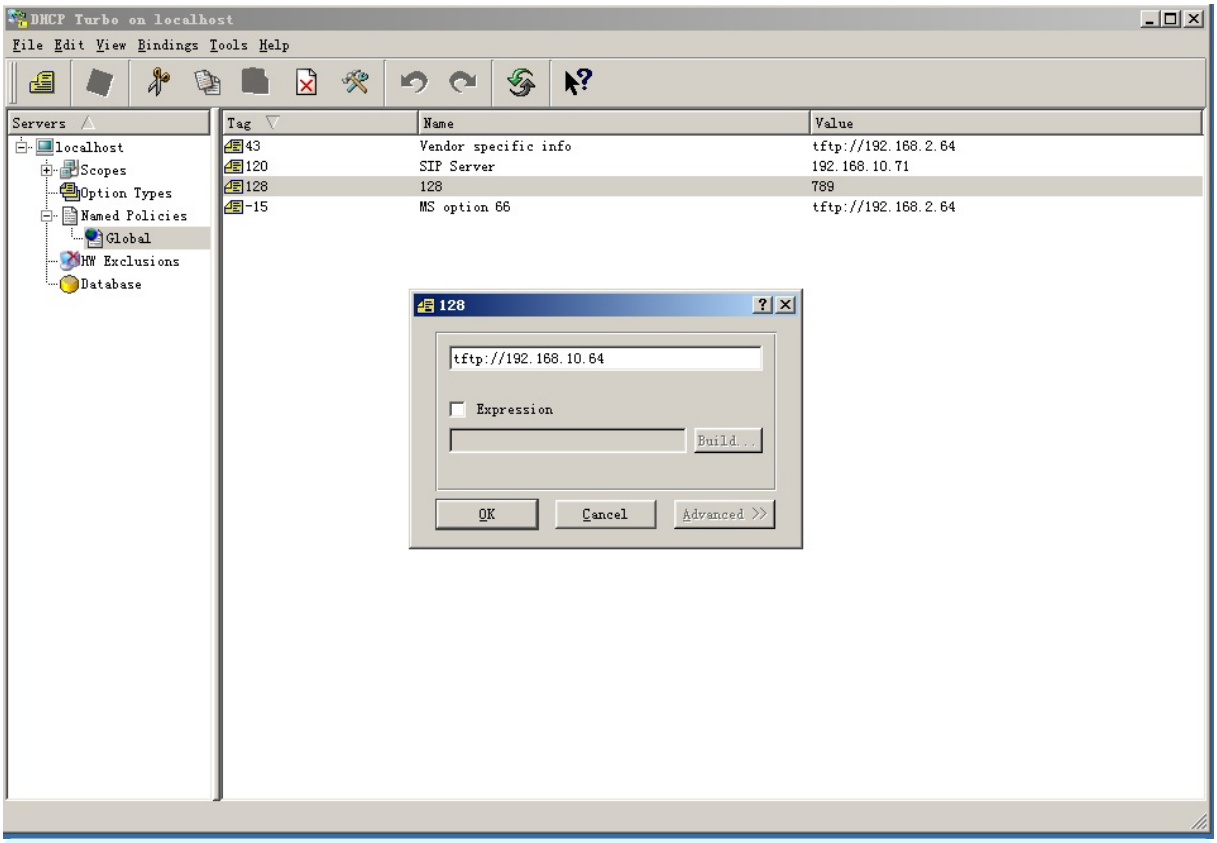
Click here to watch the configuration video.

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



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.

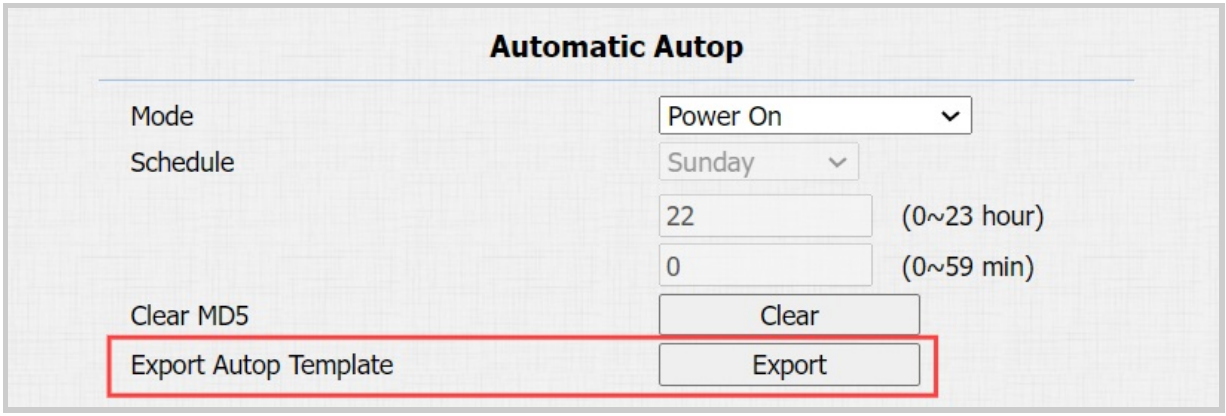


Note

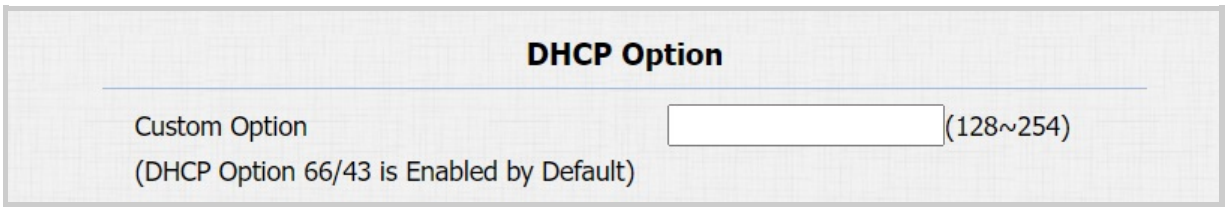
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

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



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



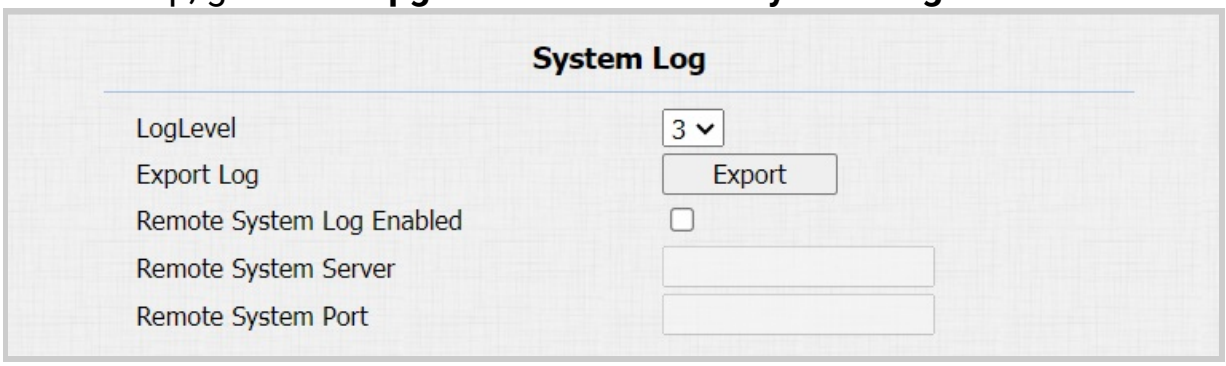
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done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

Debug

System Log

System logs can be used for debugging purposes.

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

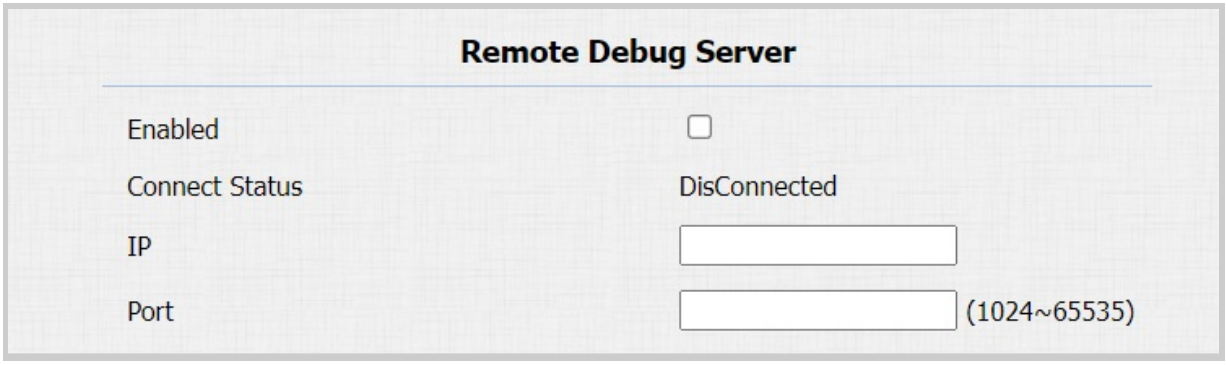


- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export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

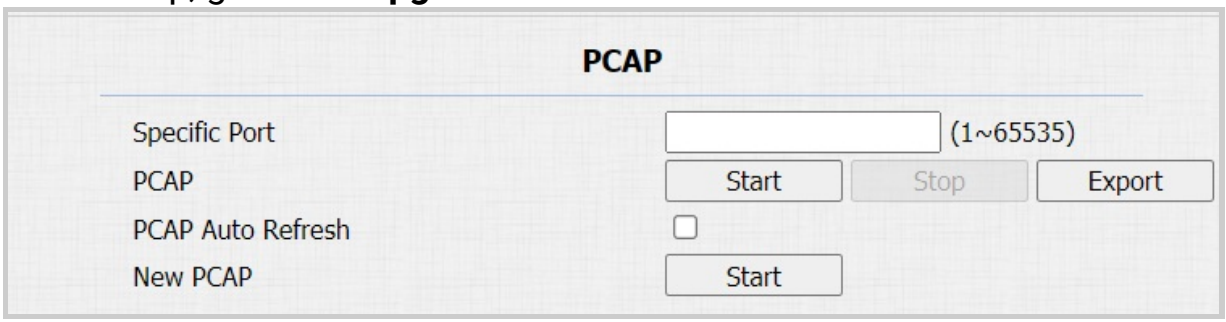


- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.
- **Port**: Enter the port of the server.

PCAP for Debugging

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

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



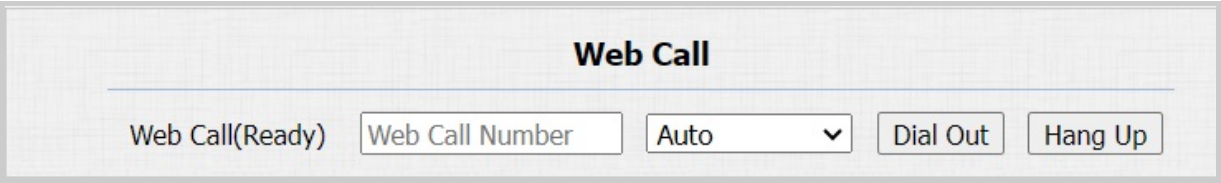
- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the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



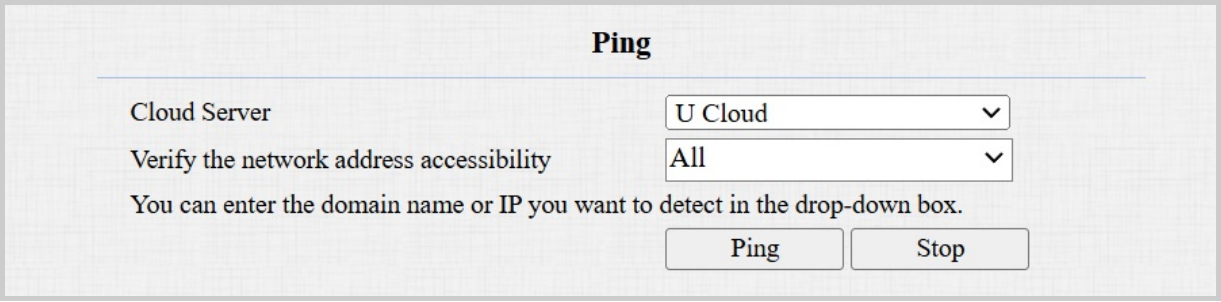
- **Web Call (Ready):** Enter the target IP/SIP number and select the account to dial out.

Ping

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

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

You can click **Export** to download the report.

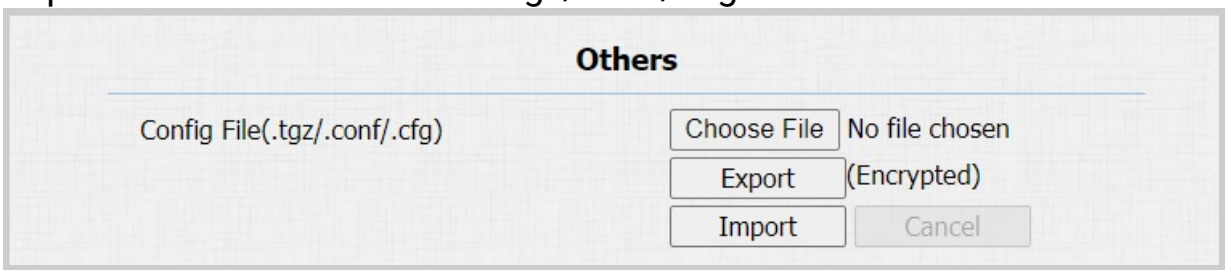


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Backup

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

Export the file on the **Upgrade > Advanced > Others** interface. The imported file should be in the .tgz/.conf/.cfg format.



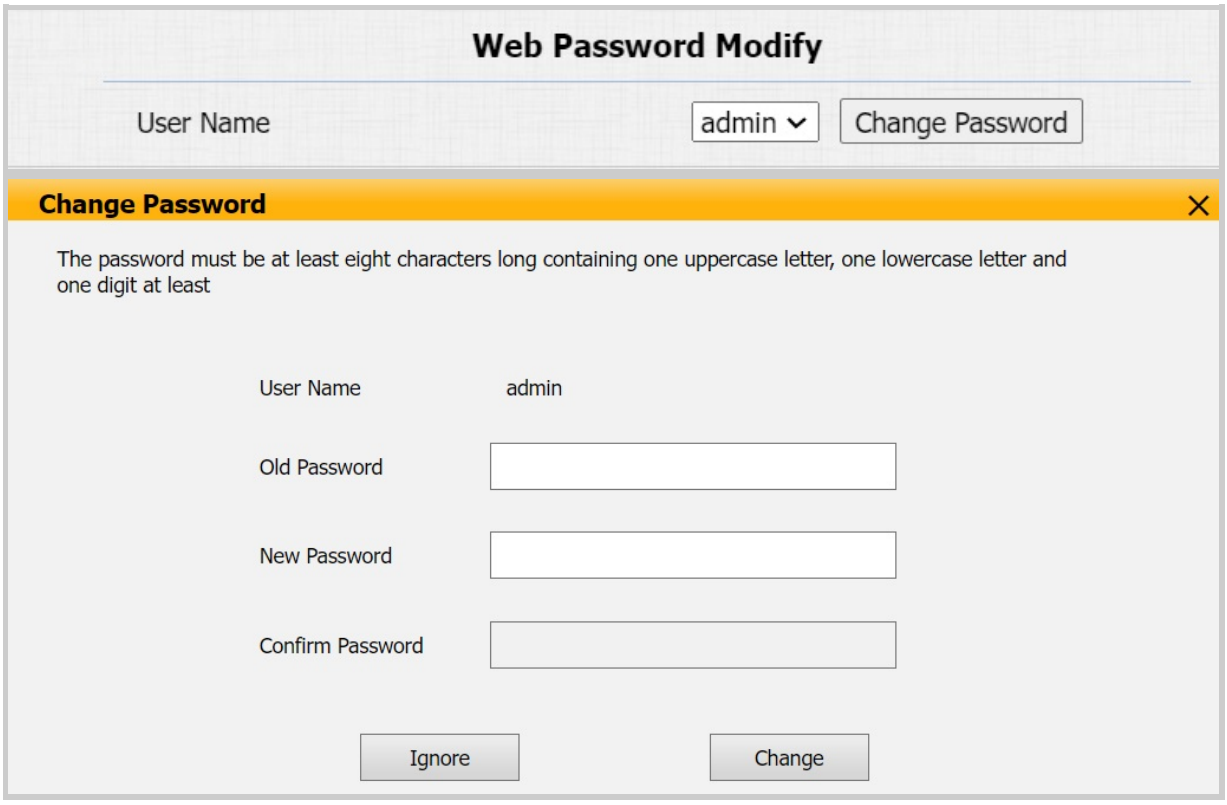
Password Modification

Modify Web Interface Password

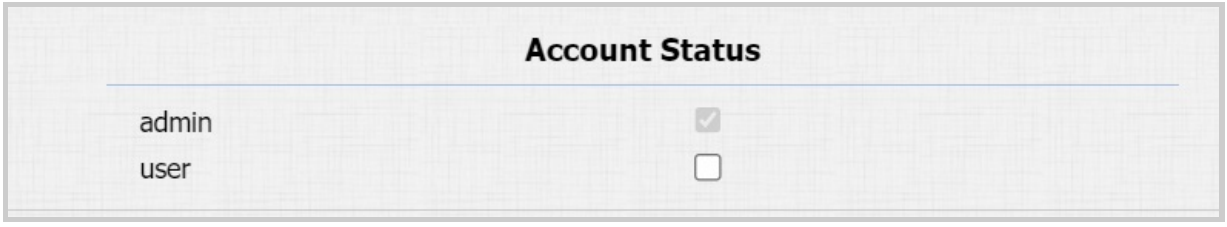
You can modify the device web interface login password for both administrator and user accounts.

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

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



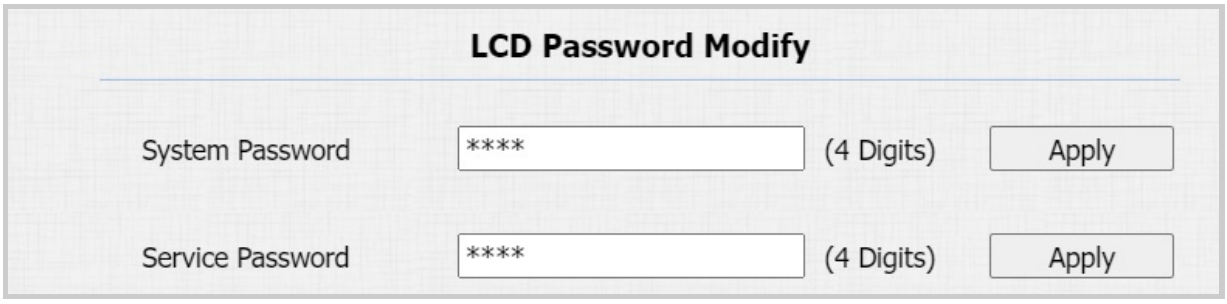
Scroll to the **Account Status** section to enable or disable the use of the user account.



Modify System Password

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

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



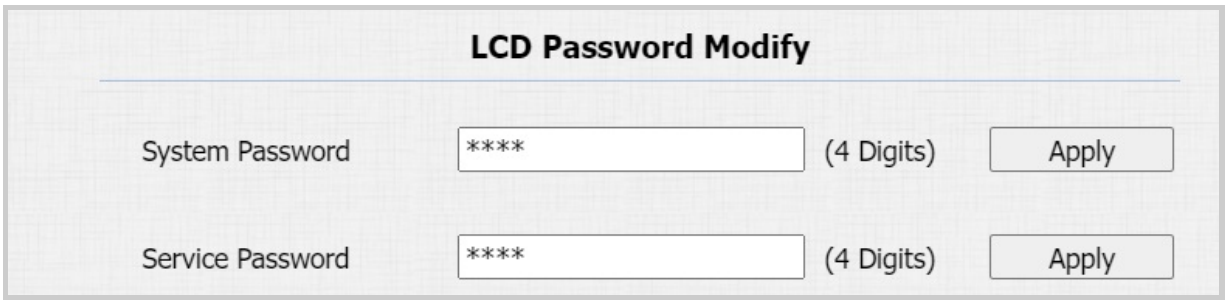
Tip

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

Modify Service Password

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

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



Tip

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

Modify Security Questions

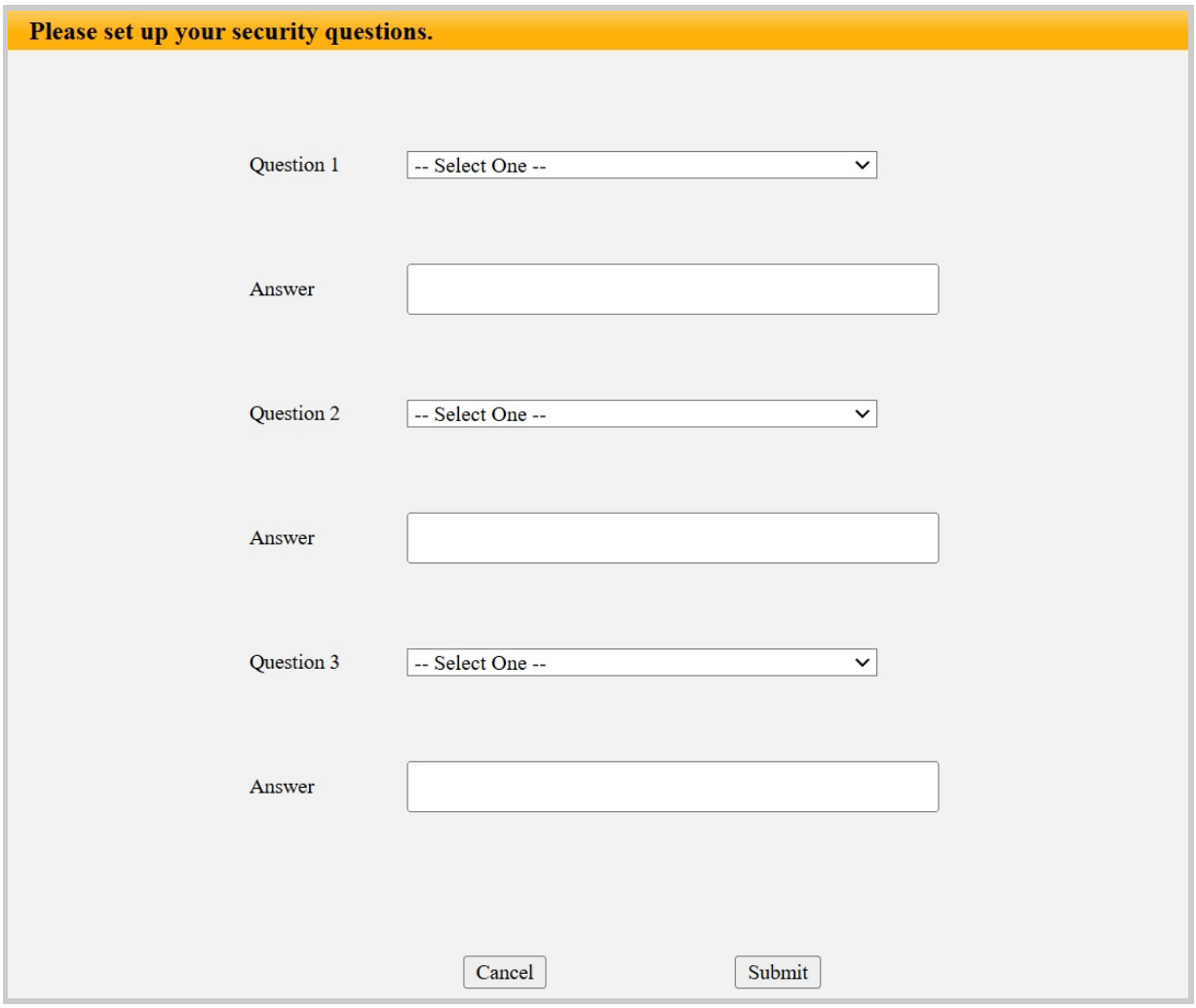
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

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



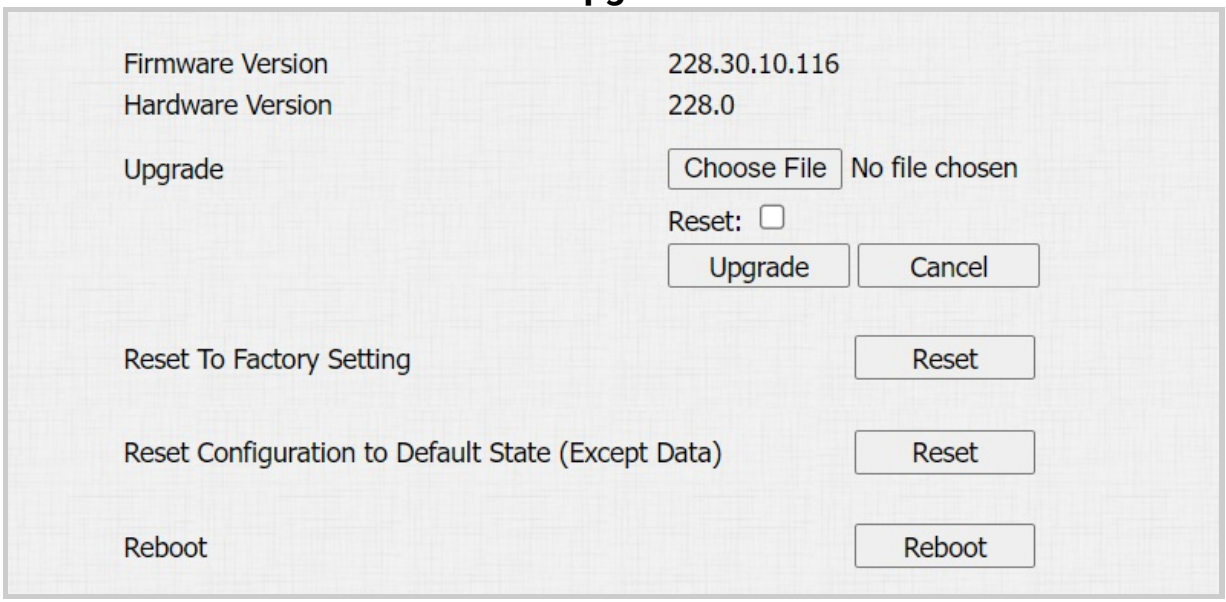
You are required to fill in the right password before modifying the security questions.


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

System Reboot&Reset

Reboot

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

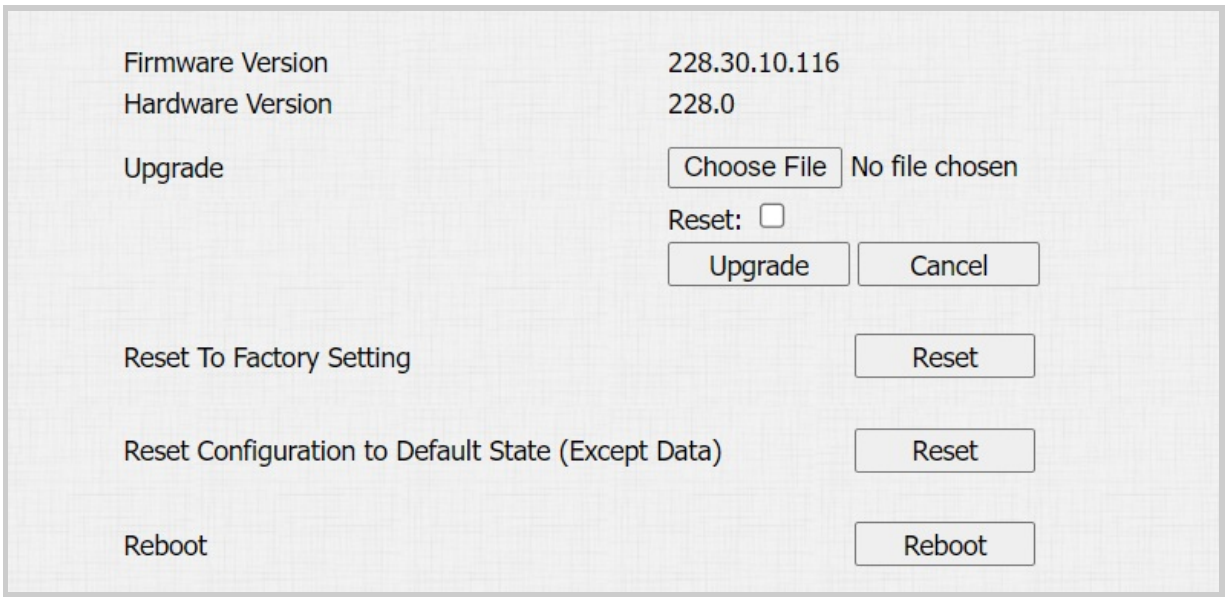


Reset

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

The device provides two reset options:

- **Reset to Factory Setting**: Reset all data to the factory default.
- **Reset Configuration to Default State(Except Data)**: Retain the user data such as the RF cards, face data, schedules, and call logs.



Tip

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

Powered by Document360