Akuvox

Table of contents

Akuvox S532 Door Phone Administrator Guide

About This Manual 10

Product Overview 13

Changelog 14

Model Specification 15

Supported Card Types 16

Access the Device 17

Obtain Device IP Address 17

Access the Device Settings 17

Access Device's Web Settings 18

Introduction to Configuration Menu 20

Introduction to Quick Start Module 22

Language and Time 24

Language 24

Custom Language 24

Time 25

Volume and Tone 27

Volume Configuration 27
Upload Tone Files 28
LED and LCD 29
Infrared LED Setting 29
Card Reader LED Control 30
Keypad LED Control 30
Home Screen Display 31
Screensaver Settings 33
Upload Screensaver 34
Screen Backlight Brightness 35
LCD Heat Control 37
Text Prompt for Door-opening and Calling 38
Network Setting 39
Network Status 39
Device Network Configuration 39
Device Deployment in Network 41
Device Local RTP Configuration 43
SNMP Setting 43
VLAN Setting 44
QoS Setting 45

TR069 Setting 46
Device Web HTTP Setting 47
NAT Setting 48
Intercom Call Configuration 50
IP Call Configuration 50
Make IP Calls 50
IP Call Setup 50
SIP Call Configuration 51
SIP Account Registration 51
SIP Server Configuration 53
Outbound Proxy Server 54
Data Transmission Type 55
Analog Setting 56
Call Setting 57
DND Configuration 57
Maximum Call Duration 57
Maximum Dial Duration 58
Auto-answer Configuration 59
Hang Up After Opening the Door 60
Prevent SIP Hacking 60

Speed Dial 61
Group Call 61
Sequence Call 63
Dial Plan 65
Multicast 67
Audio & Video Codec Configuration 69
Audio Codec Configuration 69
Video Codec Configuration 70
Video Codec for IP Direct Calls 71
Contacts Configuration 73
Manage Contact Groups 73
Set up Contact Details 73
Contact List Display 76
Cloud Contact List 77
Relay Setting 79
Local Relay 79
Security Relay 81
Web Relay 83
Door Access Schedule Management 86
Create a Door Access Schedule 86

Import and Export Door Access Schedule 87
Holiday Schedule 88
Relay Schedule 89
Door Opening Configuration 91
Unlock by Public PIN 91
User-specific Access Methods 91
Unlock by Private PIN 92
Unlock by QR Code 94
Unlock by RF Card/Bkey 95
Unlock by Bluetooth 97
Access Setting 100
Import/Export User Data 102
Mifare Card Encryption 102
Unlock by NFC 103
Unlock by HTTP Command 104
Unlock by DTMF Code 105
DTMF Whitelist 106
DTMF Data Transmission 107
DTMF Data Transmission for IP Calls 109
Unlock by Exit Button 109

Monitor and Image 112
MJPEG Video Stream 112
MJPEG Authorization 113
RTSP Stream Monitoring 114
RTSP Stream Setting 115
H.264 Video Parameters Setup 116
RTSP OSD Setting 117
NACK 118
ONVIF 118
Live Stream 120
Camera Mode 121
Data Transmission Type for Third-party Camera 122
Security 123
Tamper Alarm 123
Disarm Setting 123
Virtual PIN 124
Client Certificate Setting 124
Web Server Certificate 125
SIP TLS Certificate 125
Motion Detection 127

Motion Detection Schedule 130
Security Notification 130
Email Notification 130
FTP Notification 131
SIP Call Notification 132
Action URL 132
Voice Encryption 136
User Agent 136
Web Interface Automatic Log-out 137
High Security Mode 137
Low Power Mode 139
Emergency Action 139
Real-time Monitoring 139
Logs 141
Call Logs 141
Door Logs 142
Event Logs 143
Integration with Third-Party Device 144
Integration via Wiegand 144
Integration via HTTP API 146

Power Output Control 148
Integration via RS485 149
Lift Control 150
Firmware Upgrade 152
Auto-provisioning via Configuration File 153
Provisioning Principle 153
Configuration Files for Auto-provisioning 154
AutoP Schedule 155
Static Provisioning Configuration 156
DHCP Provisioning Configuration 158
PNP Configuration 161
Debug 162
System Log 162
Remote Debug Server 162
PCAP for Debugging 163
Ping 164
Web Call 164
Backup 166
Backup via SD Card 166
Password Modification 167

Accounts Management 167
Modify Web Interface Password 167
Modify Security Questions 168
Modify Admin Code 169
Modify Service Code 169
System Reboot & Reset 171
Reboot 171
Reset 171

About This Manual

Akuvox

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX S532 DOOR PHONE

Administrator Guide

Akuvox

Thank you for choosing Akuvox S532 series door phones. This manual is intended for administrators who need to properly configure the door phone. This manual applies to version 532.30.10.315, and it provides all the 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



- 2.8" LCD
- Aluminum Body
- **Linux OS**
- Numeric keypad
- Multiple access control (RFID, NFC, Bluetooth)
- **IP to Analog audio/video output (optional)**
- **IK08** & **IP66**

Changelog

What's new in version 532.30.10.315:

- Support the EC33 elevator control feature.

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

Model Specification

S532	
Camera	x 1
IR LEDs	✓
Card Reader	✓
Touch Screen	X
Ethernet	x 1, PoE+(802.3at)
Wiegand	x 1
RS485	x 1
Relay	x 2
Input	x 4
Analog Audio	Optional
Analog Video	Optional
TF Card Slot	x 1
Line Out	x 1
Power In	x 1, 12V/2A
MIC	x 1
Speaker	x 1

S532	
BLE	✓

Supported Card Types

The device firmware should be S532.30.10.111 or higher:

- Unencrypted ID Card:
  - EM4100
  - EM4200
- Unencrypted 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
- Felica Card
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Classic ev1 7-byte
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
  - Mifare Classic 1K
  - Mifare S50-1K Card
  - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

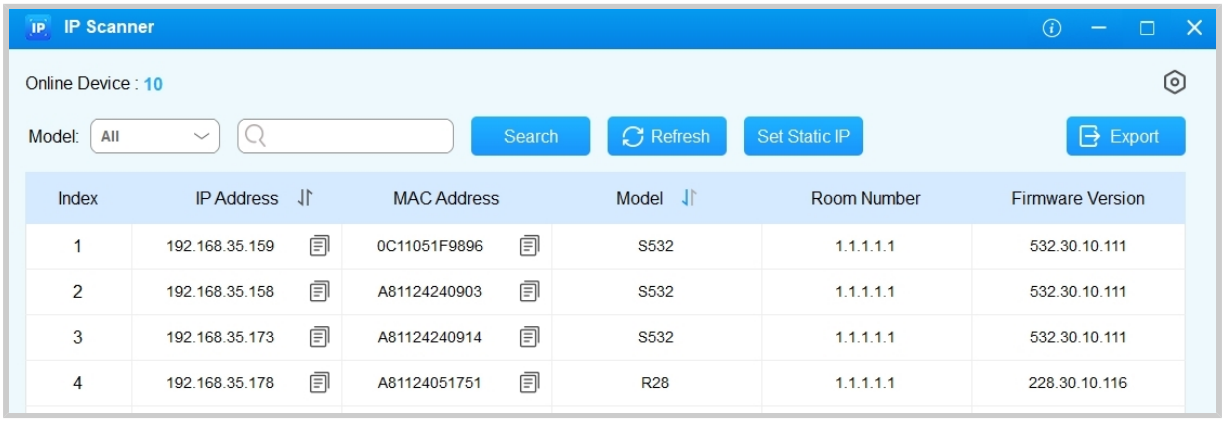
Access the Device

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 in the same local network(LAN). Click **Refresh** to update the list.

Your computer should be on the same LAN as the device.



Access the Device Settings

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

- system information;
- admin card, admin code, and service code 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 user name and password are both **admin** and please be case-sensitive to the user names and passwords entered.

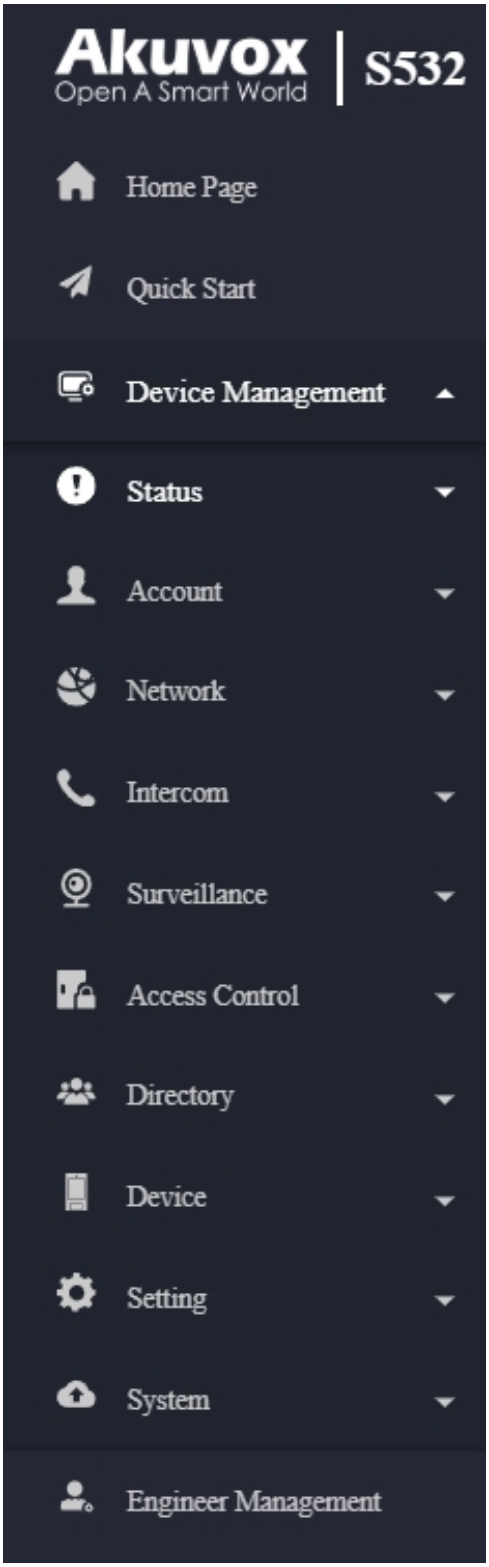


Note

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

Introduction to Configuration Menu

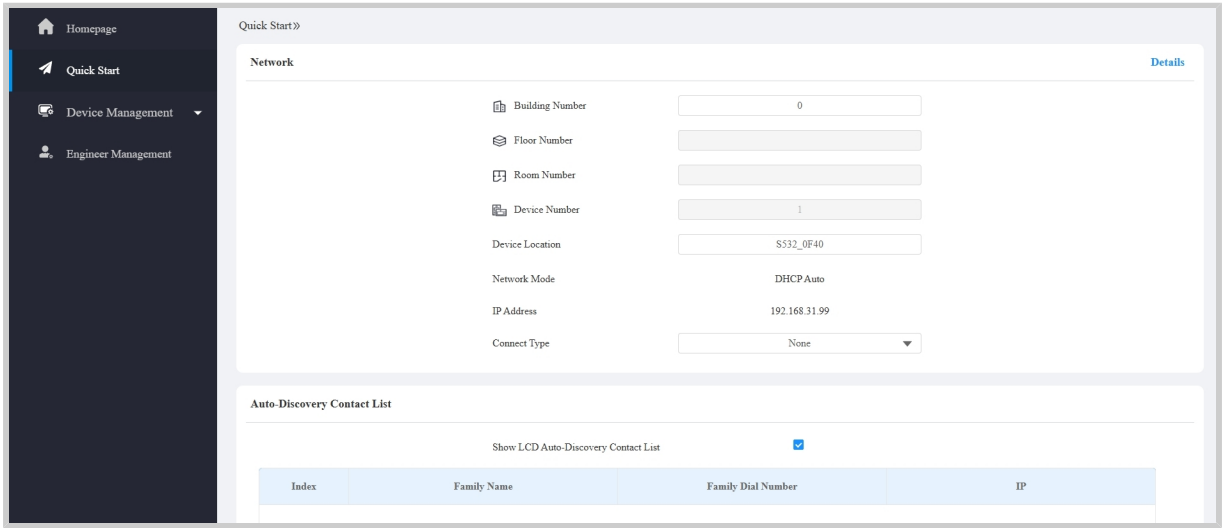
- **Quick Start**: This section provides quick access to the device's key settings, such as network, user, relay, etc.
  - **Status**: This section gives you basic information, such as product information, network information, account information, etc.
  - **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, etc.
  - **Network:** This section mainly deals with DHCP & static IP settings, RTP port settings, device deployment, etc.
  - **Intercom**: This section includes LCD settings, call features, multicast, etc.
  - **Surveillance**: the section covers motion detection, RTSP settings, ONVIF settings, etc.
  - **Access Control**: This section covers relay settings, card settings, PIN settings, etc.
  - **Directory**: This section is for user management.
  - **Device**: This section covers LCD, light, Wiegand, audio, and lift control settings.
  - **Setting**: This section covers time and language, action, schedule, and HTTP API settings.
  - **System**: This section is for upgrading, maintenance, auto-provisioning, 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*].
  - **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.
- **Auto-Discovery Contact List**: Display the contacts, such as indoor monitors, in the Self-organizing Network Solution.
  - **Show LCD Auto-Discovery Contact List**: Set whether to display these contacts on the device screen.
- **Directory**: **Contact Display Mode** sets how contacts will be displayed.
  - **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.

  - **Do Not Display Contacts**: Neither contacts nor groups will display.
- Open Relay Via HTTP:
  - **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.

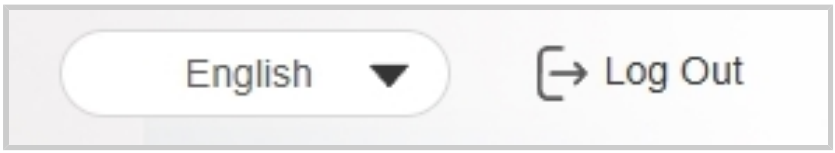
Language and Time

Language

You can select the device's LCD language on the **Setting > Time/Lang** interface. Currently, it supports English, Simplified Chinese, Traditional Chinese, Russian, Spanish, Italian, Dutch, French, German, Polish, Turkish, Estonian, Latvian, Lithuanian, and Bosnian.



You can switch the web language in the upper-right corner. Currently, it supports English, Simplified Chinese, Traditional Chinese, Russian, Spanish, Italian, Dutch, French, German, Polish, Turkish, Estonian, Latvian, and Lithuanian.



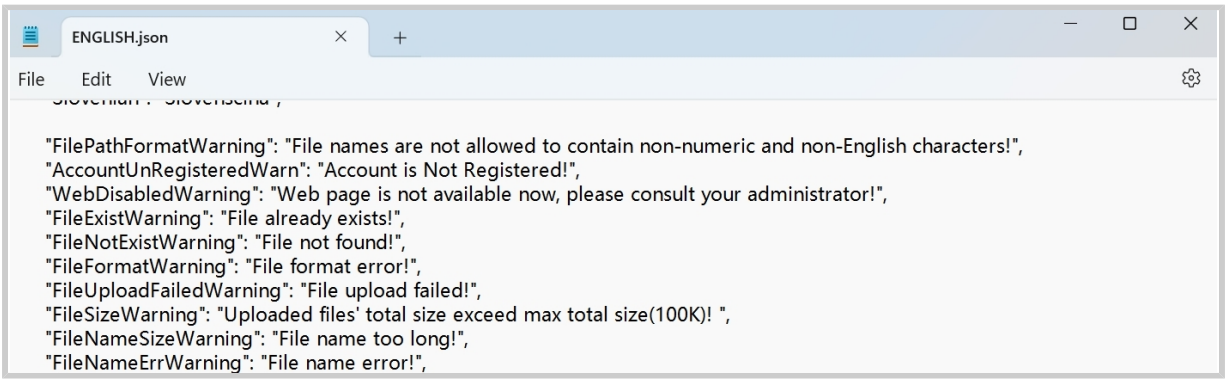
Custom Language

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

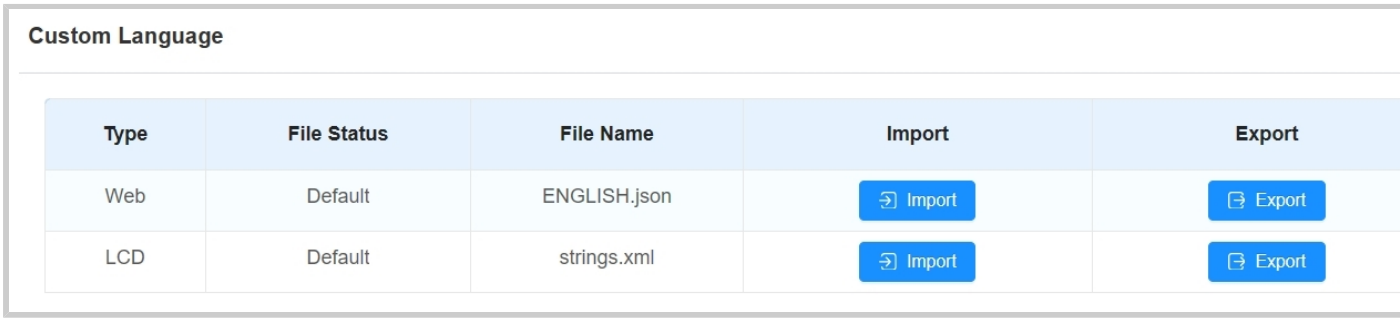
Export the .json file for editing. You may edit it with the notepad on your computer.

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

File Example:



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



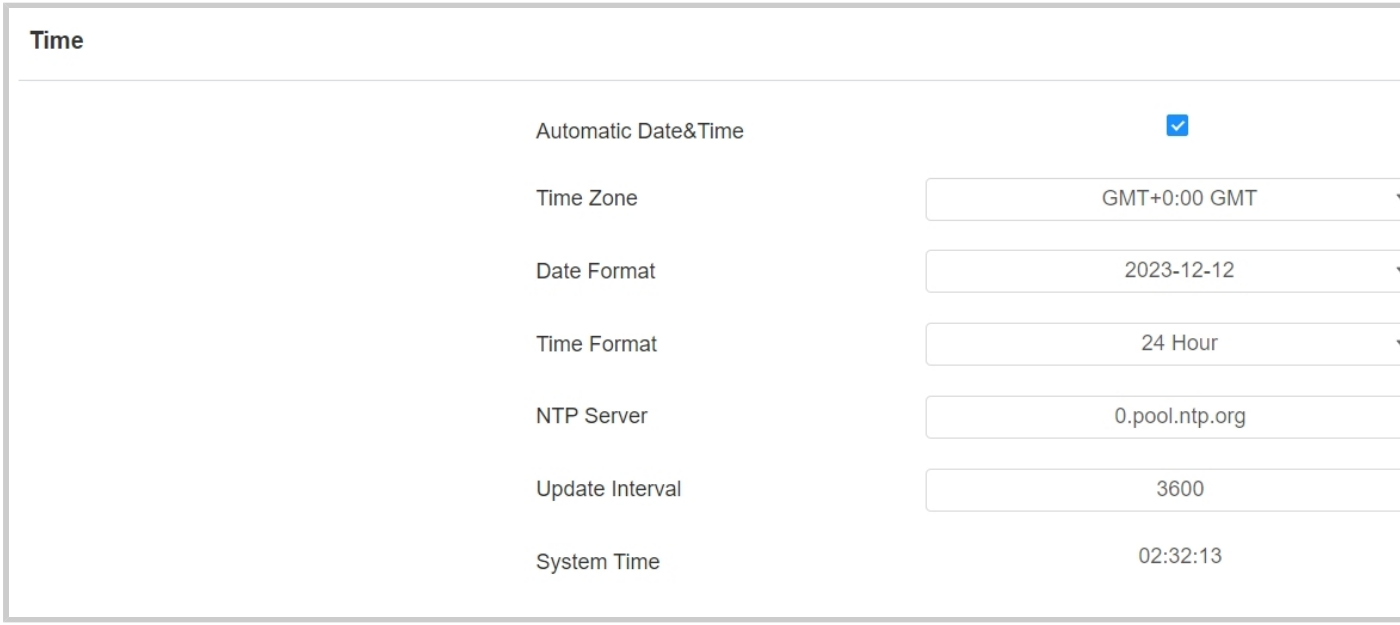
Note

- 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 configure time, navigate to the web **Setting > Time/Lang** interface.



- **Automatic Date & Time**: When enabled, the device's date and time are automatically set up and synchronized with the default time zone and the NTP server (Network Time Protocol).
- **NTP Server**: The NTP server address.
- **Update Interval**: The interval between two consecutive NTP requests.

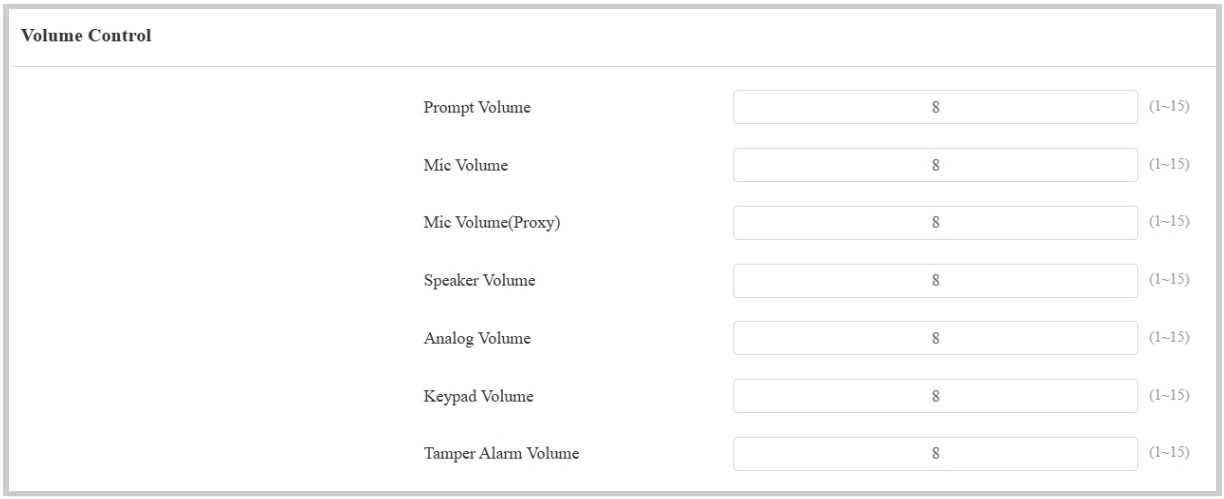
Volume and Tone

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 Configuration

You can configure the volume of the microphone, speaker, etc. Moreover, you can also set up the tamper alarm volume when unwanted removal of the device occurs.

Set up volumes on the web **Device > Audio** interface. The default value of all volumes is 8.

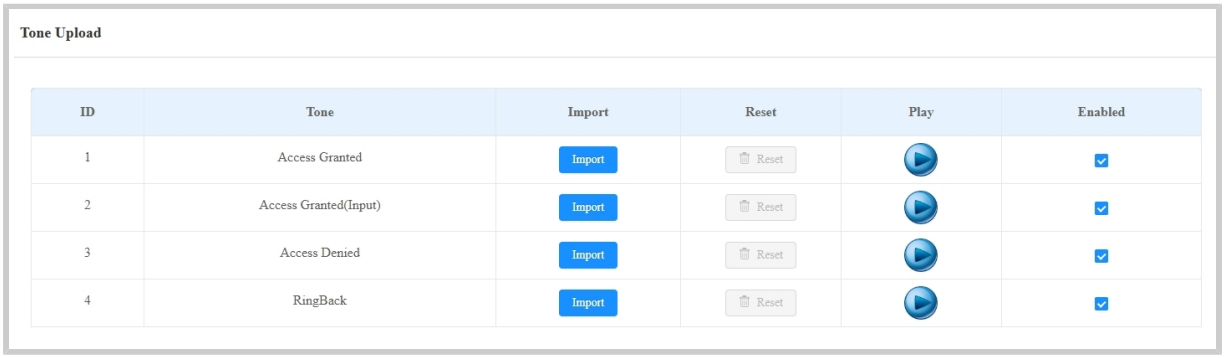


- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback.
- **Mic Volume(Proxy)**: The mic volume of the analog switch.
- **Analog Volume**: The volume of the analog switch during a call.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered.

Upload Tone Files

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

Upload tones on the web **Device > Audio** interface.



- **Access Granted(Input)**: The door is opened by pressing an exit button connected to the device's input.

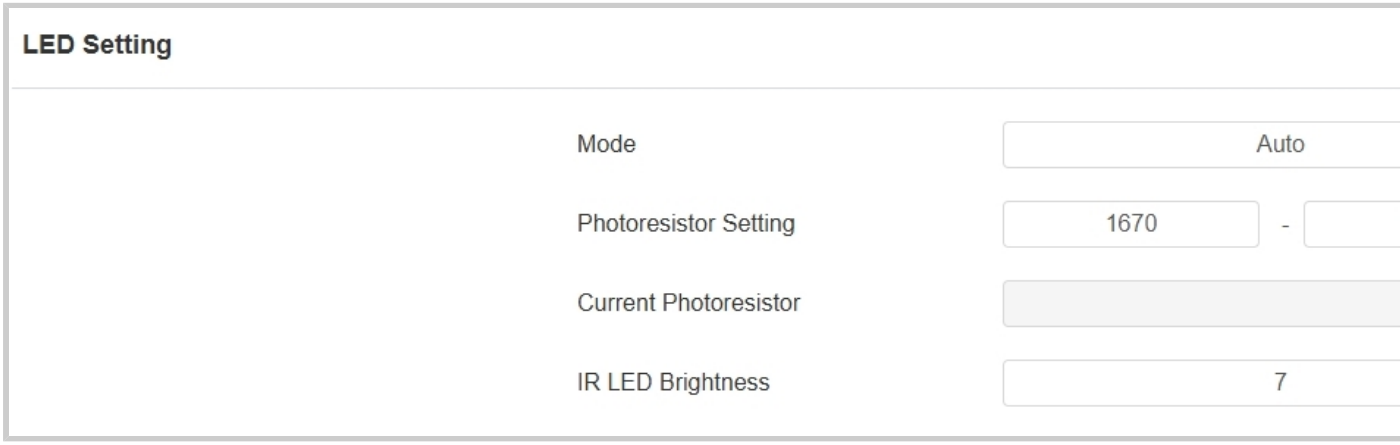
> **Note**
>
> File Format: wav; Size: < 200KB; Sample Rate: 16000; Bit Depth: 16 Bits.

LED and LCD

Infrared LED Setting

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

To set up the LED, navigate to the web **Device > Light > LED Setting** interface.



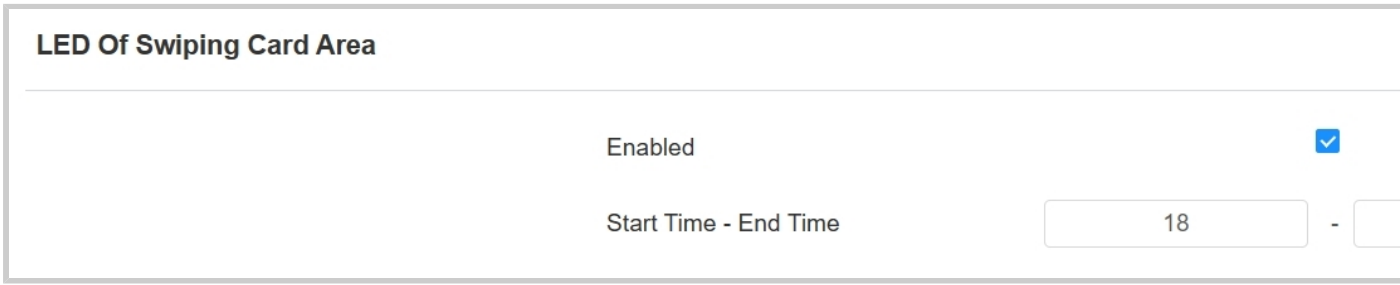
- **Mode**:
  - **Auto**: Turn on the infrared LED automatically based on the minimum and maximum photoresistor value.
  - **Always On**: Enable the infrared LED.
  - **Always Off**: Disable the infrared LED.
  - **Schedule**: Turn on the infrared LED based on the schedule. Specify the Start Time and End Time when this option is selected.
- **Photoresistor Setting**: Set the minimum and maximum photoresistor values to automatically control the ON-OFF of the infrared LED light. If the photoresistor value is less than the minimum threshold, turn it off. If the photoresistor value is greater than the maximum threshold, turn it on.

- **Current Photoresistor**: The current light intensity indicated by the photoresistor value. Click **Read** to display the value. The photoresistor values inversely relate to light intensity: higher values indicate lower light, and lower values indicate higher light.
- **IR LED Brightness**: Adjust the IR LED brightness from level 0 to 10. The higher the level is, the brighter it is.

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, navigate to the web **Device > Light > LED Of Swiping Card Area** interface.

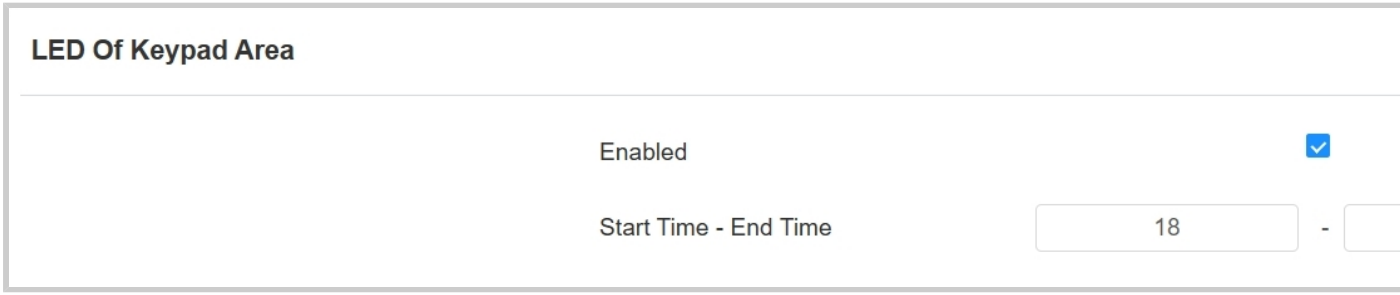


- **Start Time- End Time (H)**: Enter the time for the LED lighting to be valid, e.g., if the time is set from 8-0 (Start time- End time), it means LED light will stay on during the time from 8:00 am to 12:00 pm during one day (24 hours).

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, navigate to the web **Device > Light > LED Of Keypad Area** interface.

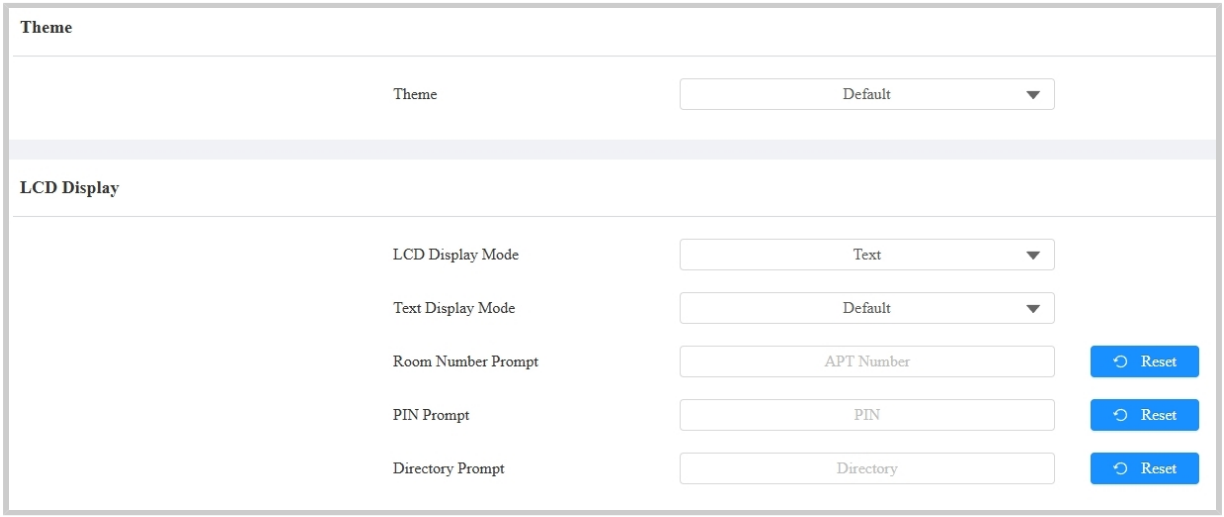


- **Start Time- End Time (H)**: Enter the time for the LED lighting to be valid, e.g., if the time is set from 8-0 (Start time- End time), it means LED light will stay on during the time from 8:00 am to 12:00 pm during one day (24 hours).

Home Screen Display

Three types of home screen display themes are available for different applications.

To set it up, go to the **Setting > Key/Display** interface.

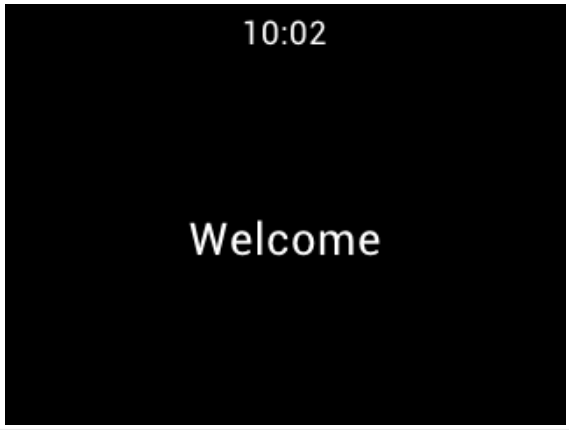
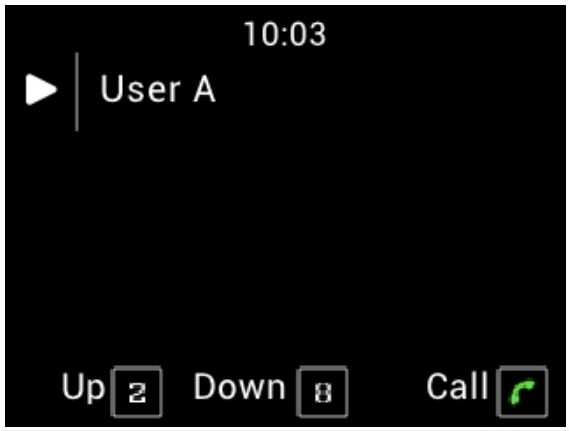
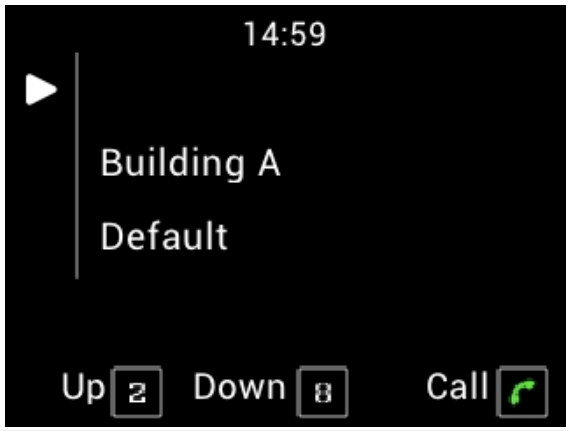


- **Theme**:
  - **Default**: Display the instructions for making calls by room numbers, opening doors by entering PINs, and entering the directory list screen.

- **Customized Text**: Display customized text on the home screen. When selected, enter the content in the Text box.
- **Directory**: Display the directory list.
- **Gate Mode**: This mode requires using the SmartPlus Cloud service and adding the device to the public area of community projects. It will display buildings and apartments in the Cloud. Users need to choose a specific building before calling a resident.

- **LCD Display**: Available for the Default theme.
  - **LCD Display Mode**: Choose to display text or an image. When selecting **Image**, you can upload a picture(Max size: 200KB, Format: .png/.jpg, Recommended Resolution: 320*240).
  - **Text Display Mode**:
    - **Hide Directory**: Hide the instructions for entering the directory list screen.
    - **Hide Directory & Room Number**: Only display the instructions for opening doors by entering PINs.
  - **Room Number Prompt**: The prompt for entering the apartment number to call.
  - **PIN Prompt**: The prompt for entering the PIN to open the door.
  - **Directory Prompt**: The prompt for entering the directory list screen.

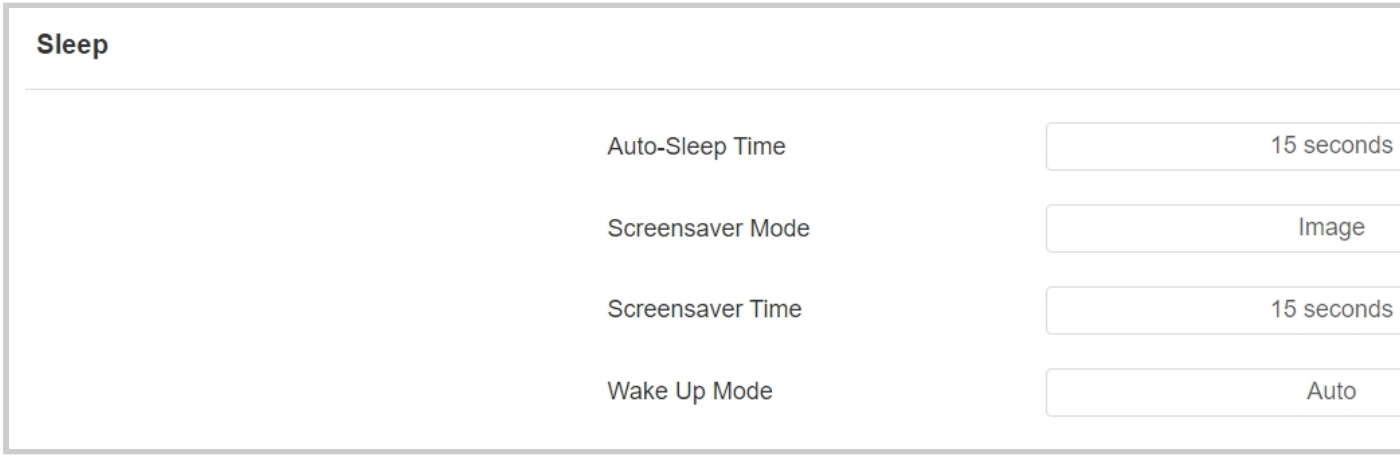


Default	Customized Text
	
Directory	**Gate Mode**
	

Screensaver Settings

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 the web **Device > LCD** interface.

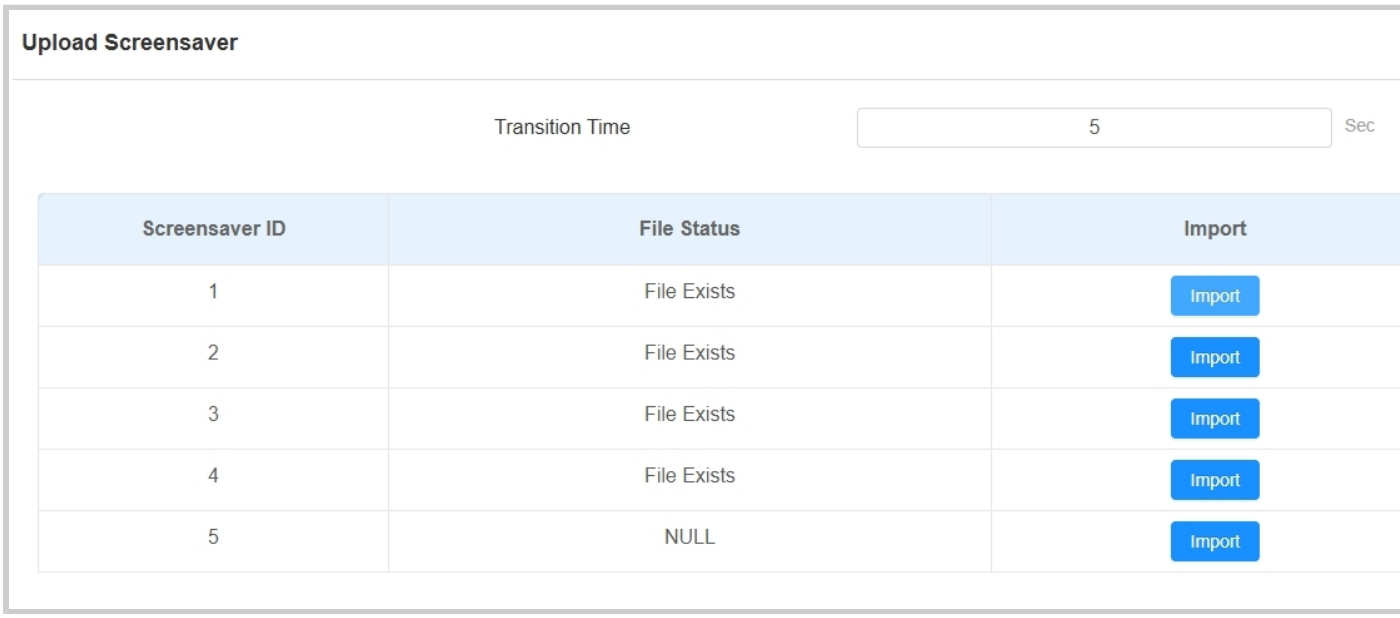


- **Auto-Sleep Time**: Within the Auto-Sleep Time, if the device detects no operation or no one approaching, it will start displaying the screensaver. It ranges from 5 seconds to 30 minutes. The default is 15 seconds.
- **Screensaver Mode**:
  - **Image:** Display the default picture or the picture uploaded.
  - **Disabled:** The device will not go into Screensaver Mode.
- **Screensaver Time**: The screensaver duration time. The screen will turn dark after a time.
- **Wake Up Mode**:
  - **Auto**: The screen can be awakened when someone approaches without it being touched.
  - **Manual**: Touch and wake up the screen.

Upload Screensaver

You can upload screen-saver pictures to the device for publicity purposes or a greater visual experience.

Navigate to the web **Device > LCD** interface.



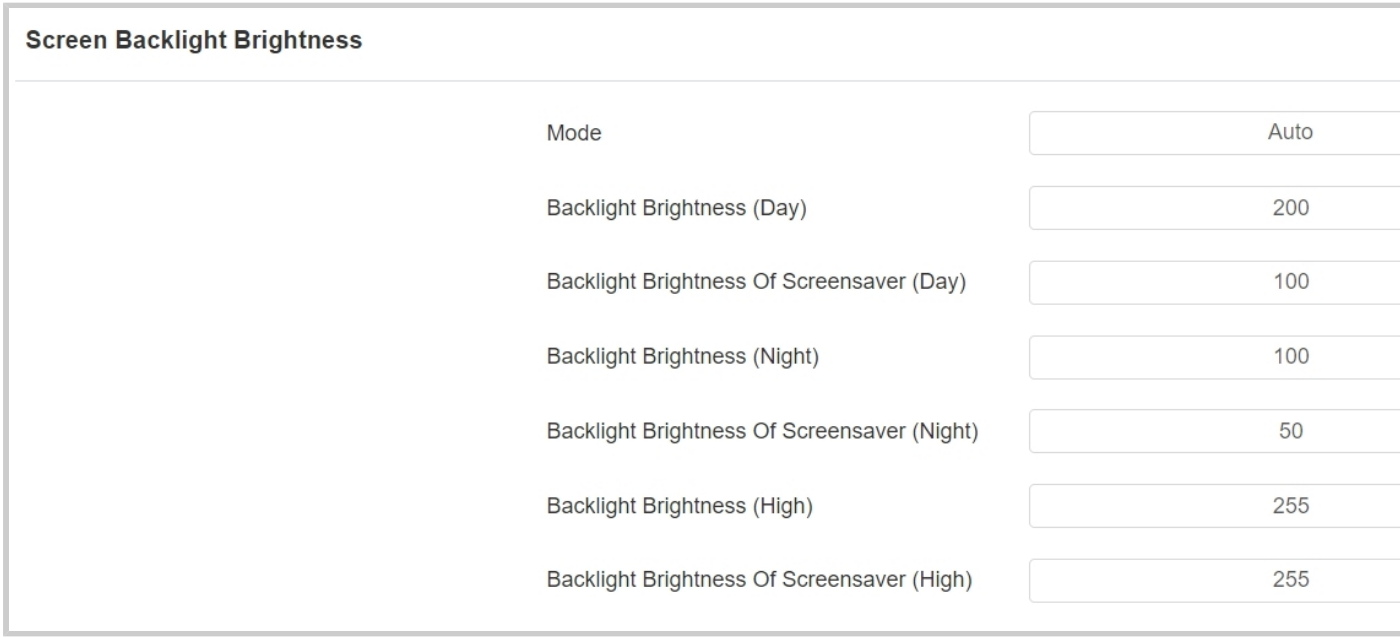
- **Transition Time**: The time interval switching between two pictures.

> **Note**
>
> - The file should be in .jpg format with a 1M max size.
> - The recommended resolution is 320×240.

Screen Backlight Brightness

You can adjust the backlight brightness for the screen and screensaver.

Navigate to the web **Device > LCD** interface.



- **Mode**: When **Auto** is selected, the screen backlight brightness will be adjusted automatically.

> **Note**
>
> The backlight brightness has three modes, Day, Night, and High. They are determined by the photoresistor.
>
> - If the current photoresistor is lower than the preset minimum photoresistor, the device is in **High** mode.
> - If the current value is between the minimum and maximum photoresistor, the device is in **Day** mode.
> - If the current value is higher than the maximum photoresistor, the device is in **Night** mode.

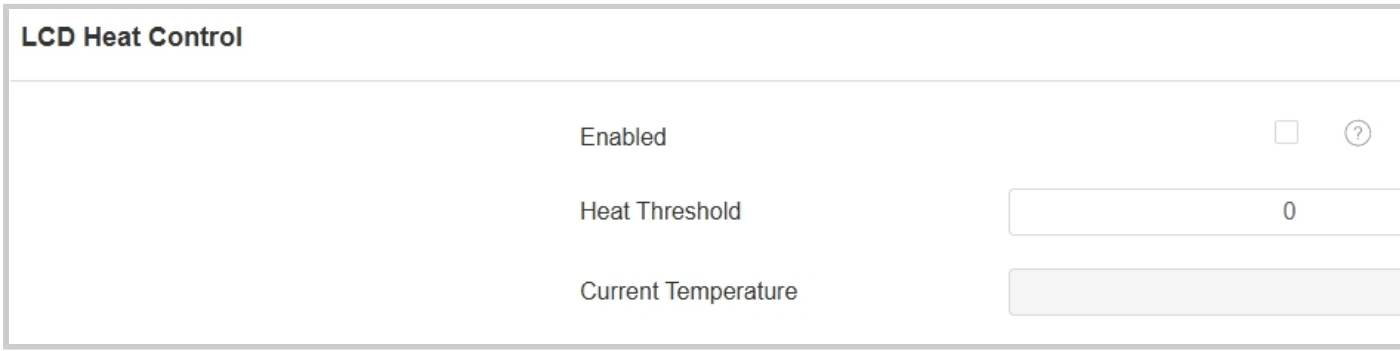
- **Backlight Brightness (Day)**: The brightness value ranges from 1-255. The default is 200. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screensaver (Day)**: The backlight for the screensaver in the daytime, with the value ranging from 1-255.

- **Backlight Brightness (Night)**: The backlight at night with a value ranging from 1-255.
- **Backlight Brightness Of Screensaver (Night)**: The backlight for the screensaver at night, with the value ranging from 1-255.
- **Backlight Brightness (High)**: The backlight with a value ranging from 1-255.
- **Backlight Brightness Of Screensaver (High)**: The backlight for the screensaver with a value ranging from 1-255.

LCD Heat Control

To ensure the normal operation of the door phone in low-temperature environments, you can heat up the device's LCD screen according to your heat control setting.

Navigate to **Intercom > Basic** interface.



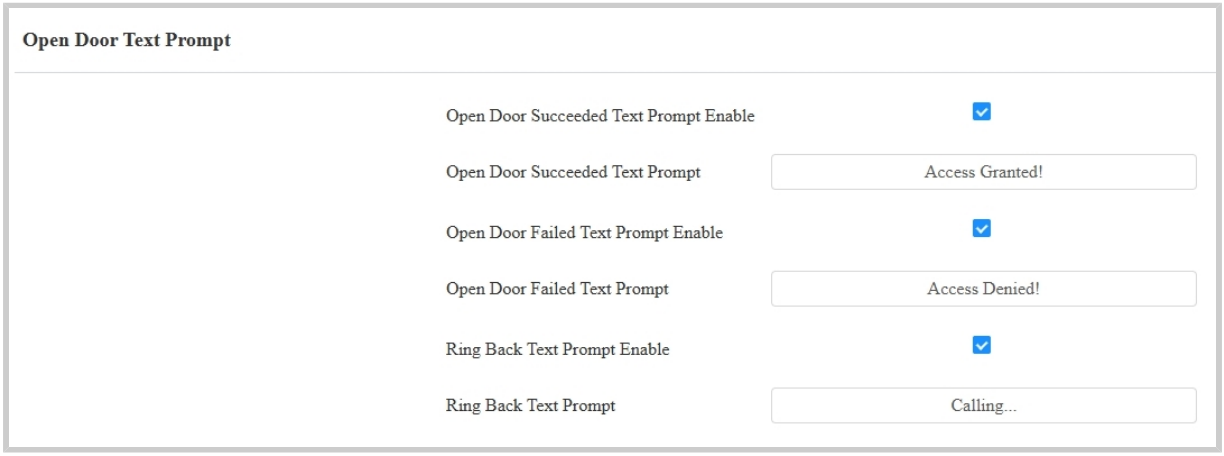
- **Enabled**: This function cannot be used in Low Power Mode. Use **POE+** or **a 12V DC power adapter** to ensure sufficient power supply.
- **Threshold**: When the device temperature reaches the threshold, the device will start heating up.
- **Current Temperature**: Click **Read** to acquire the device's current temperature.

Text Prompt for Door-opening and Calling

You can enable/disable the text prompts for both door-opening success and failure, and calling.

All these prompts are enabled by default.

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

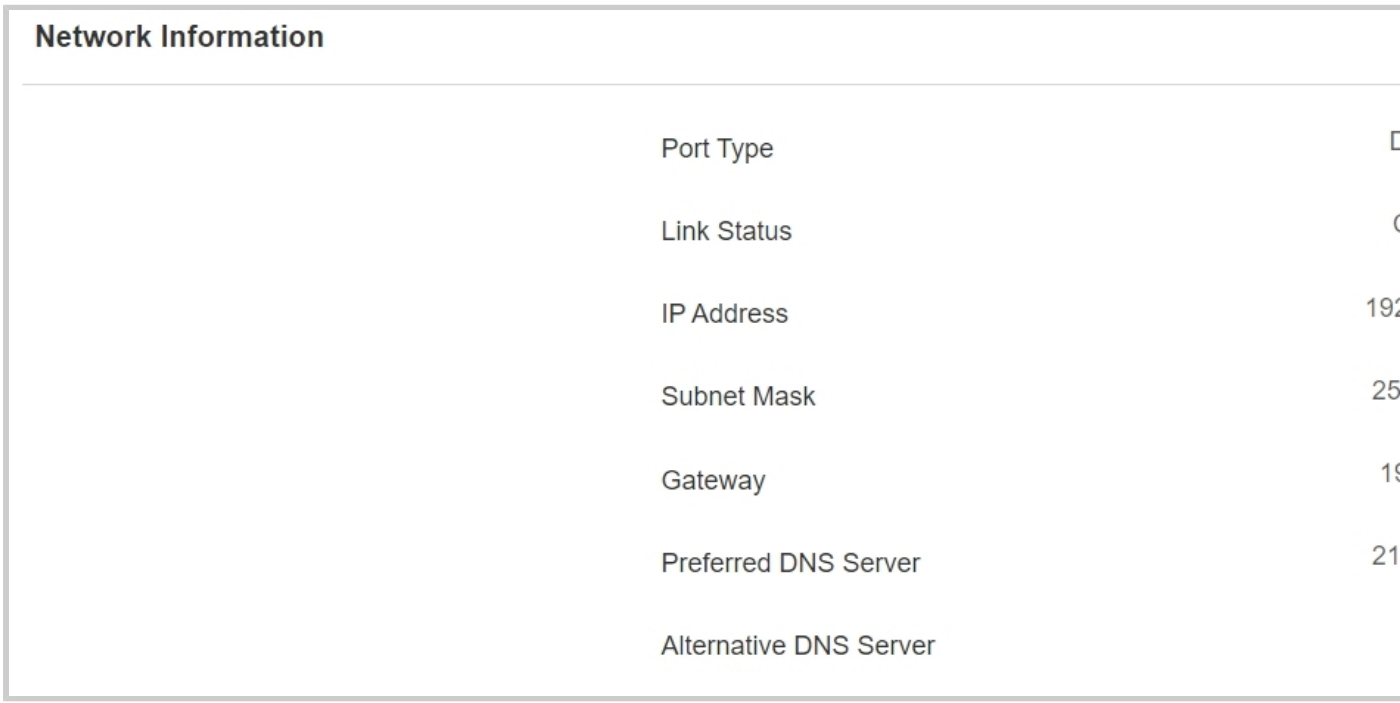


- **Open Door Succeeded Text Prompt**: Display a text prompt after the door is opened. The default prompt is “Access Granted”. You can customize the prompt with a maximum of 63 characters.
- **Open Door Failed Text Prompt**: Display a text prompt after opening the door fails. The default prompt is “Access Denied”. You can customize the prompt with a maximum of 63 characters.
- **Ring Back Text Prompt**: Display a text prompt when calling a number. The default prompt is “Calling”. You can customize the prompt with a maximum of 63 characters.

Network Setting

Network Status

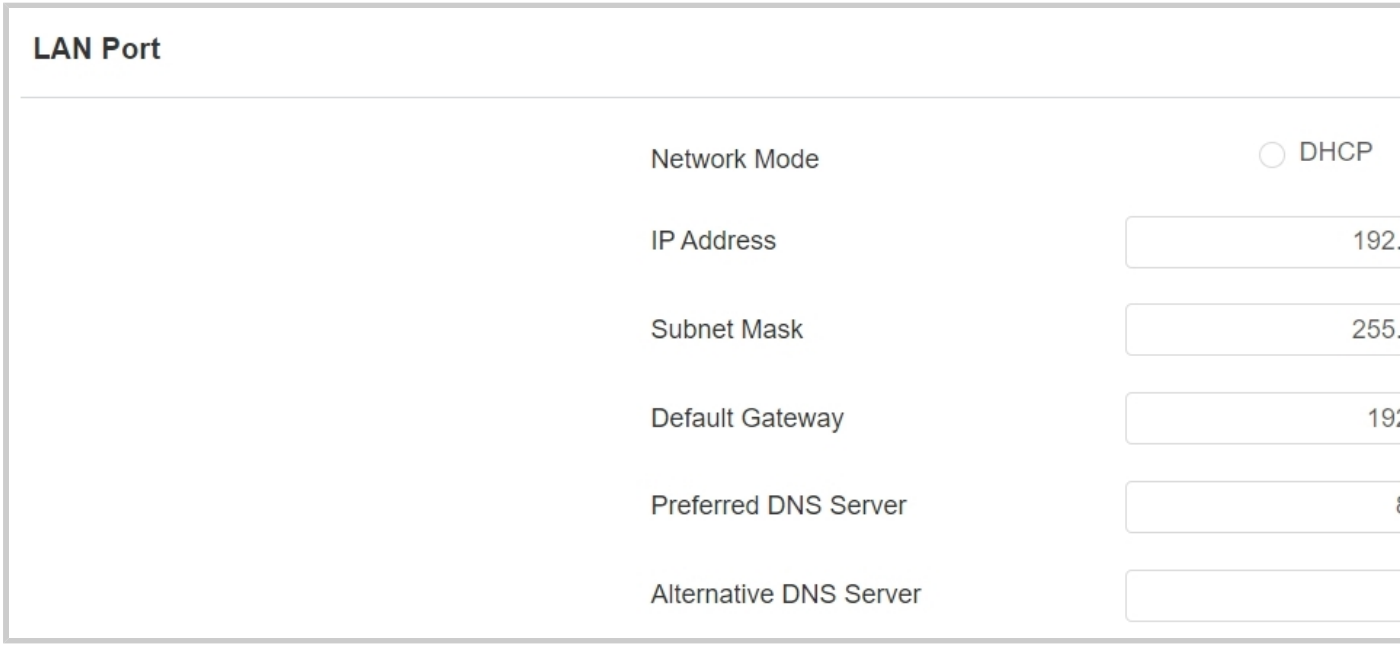
Check the network status on the web **Status > Info > Network Information** interface.



Device Network Configuration

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

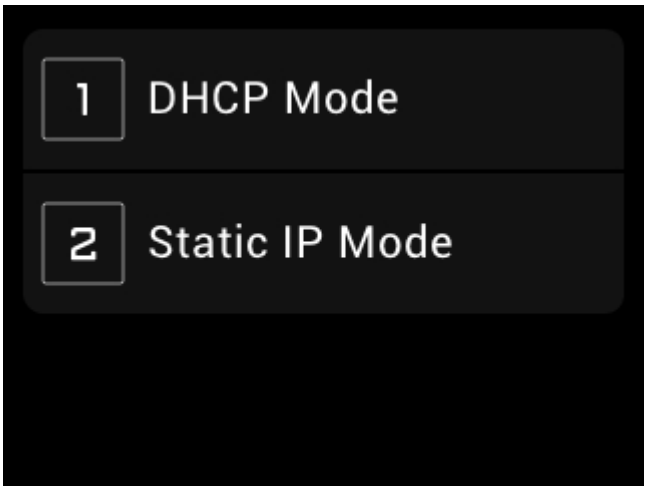
To set up the network, navigate to the web **Network > Basic** interface.



- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, the door phone will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: When static IP mode is selected, the IP address, subnet mask, default gateway, and DNS server address(es) 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/Alternative DNS**: 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.

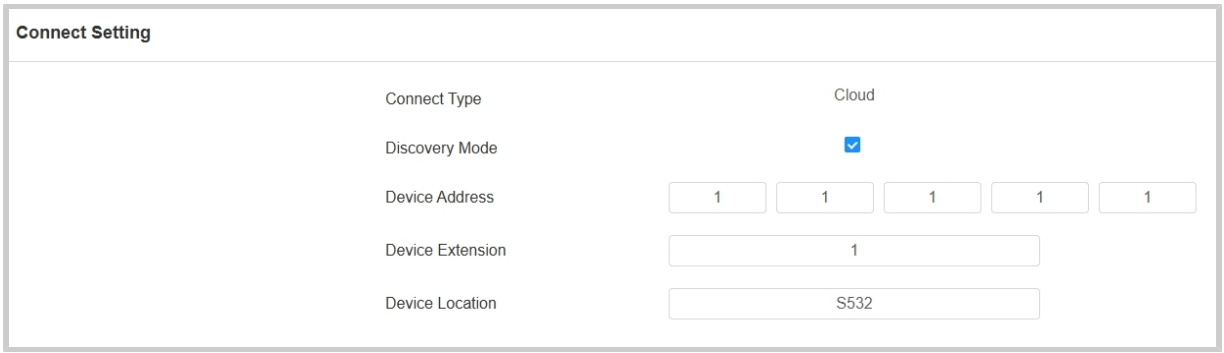
You can also configure the network on the device. Press *2396# on the device keypad and tap 3 and 1 to enter the network setting screen.



Device Deployment in Network

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

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



- **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.

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

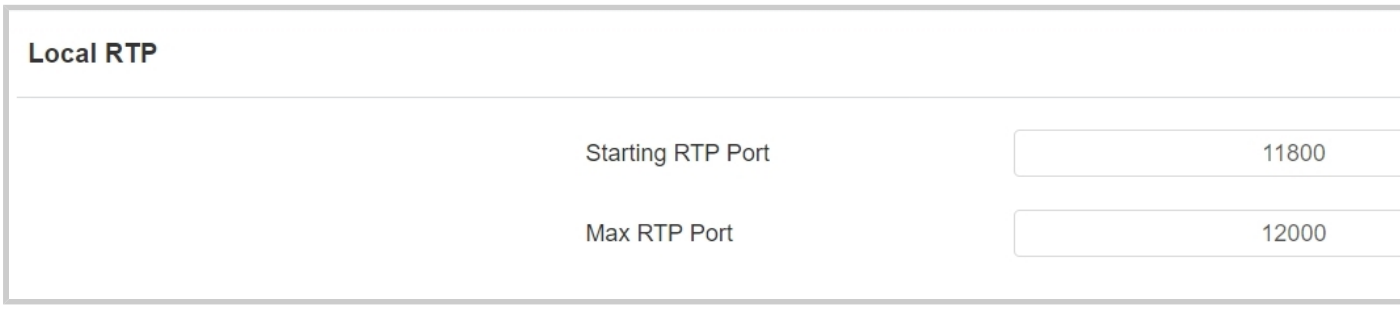
- **Discovery Mode**: Enabled by default. Available for **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address**: Available for None server mode. Uneditable in Cloud and SDMC mode. It can be used to call the device. Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for None server mode. Uneditable in Cloud and SDMC mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for None server mode.

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 configure RTP, navigate to the web **Network > Advanced** interface.

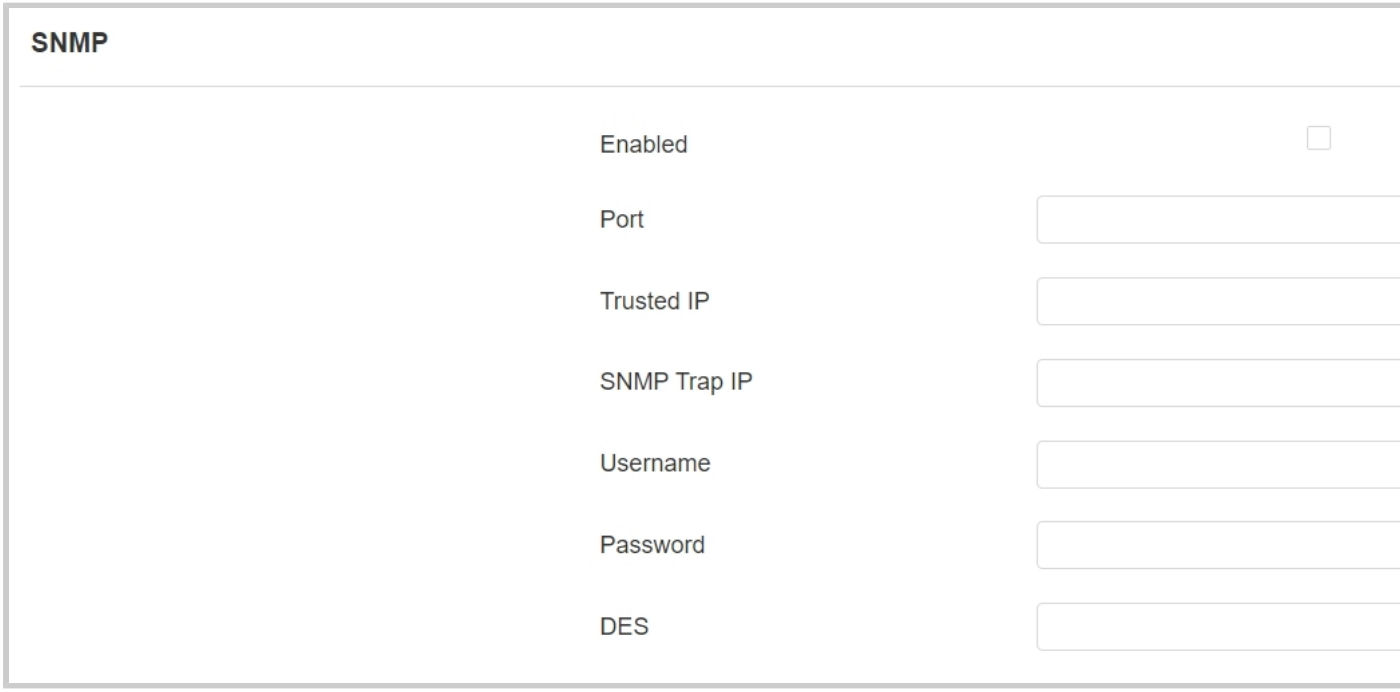


- **Starting RTP Port**: The port value for establishing the start point for the exclusive data transmission range.
- **Max RTP Port**: The port value for establishing the endpoint for the exclusive data transmission range.

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 configure SNMP, navigate to the web **Network > Advanced** interface.

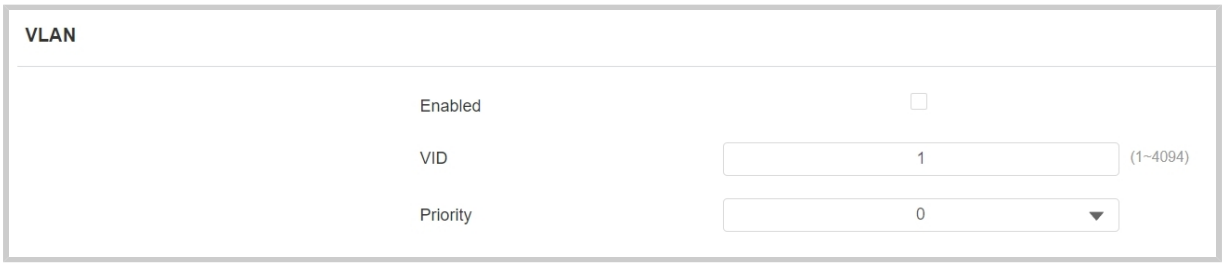


- **Port**: The SNMP server's port.
- **Trusted IP**: The allowed SNMP server address. It can be an IP address or any valid URL domain name.

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 configure VLAN, navigate to the web **Network > Advanced** interface.

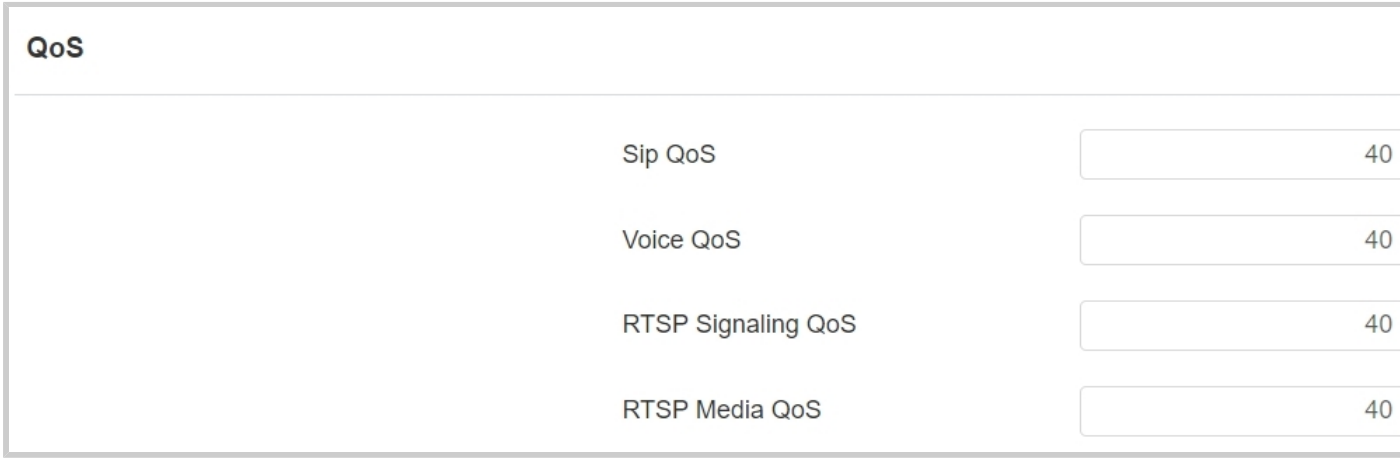


- **VID**: The VLAN ID for the designated port.
- **Priority**: The VLAN priority for the designated port.

QoS Setting

Quality of Service(**QoS**) is a network's ability to provide better service for specific network communications by utilizing various technologies. It serves as a security mechanism in networks, addressing issues like network latency and congestion. Ensuring QoS is crucial for networks with limited capacity, particularly for multimedia applications such as VoIP and IPTV. These applications often require a consistent transmission rate and are sensitive to delays.

To configure QoS, navigate to the web **Network > Advanced** interface.



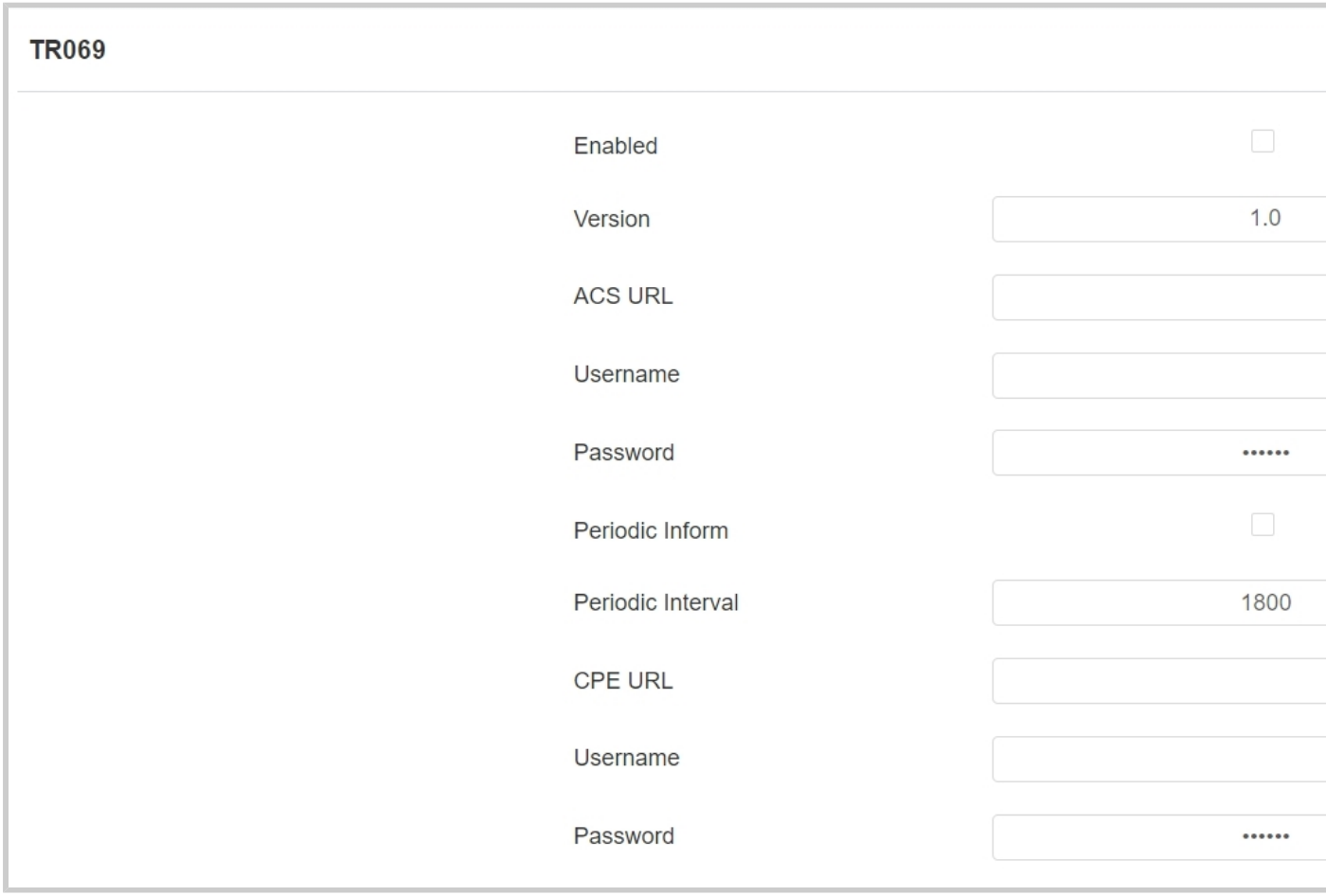
- **SIP QoS**: SIP QoS can be analyzed by registering an account and capturing SIP packets.

- **Voice QoS**: Voice QoS can be analyzed during a call by capturing and examining RTP packets.
- **RTSP Signaling QoS**: RTSP Signaling QoS can be analyzed using VLC and capture RTP packets.
- **RTSP Media QoS**: RTSP Media QoS can be analyzed by viewing the stream in VLC and capturing RTP packets.

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 configure it, navigate to the web **Network > Advanced** interface.



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

Device Web HTTP Setting

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

To configure it, navigate to the web **Network > Advanced** interface.



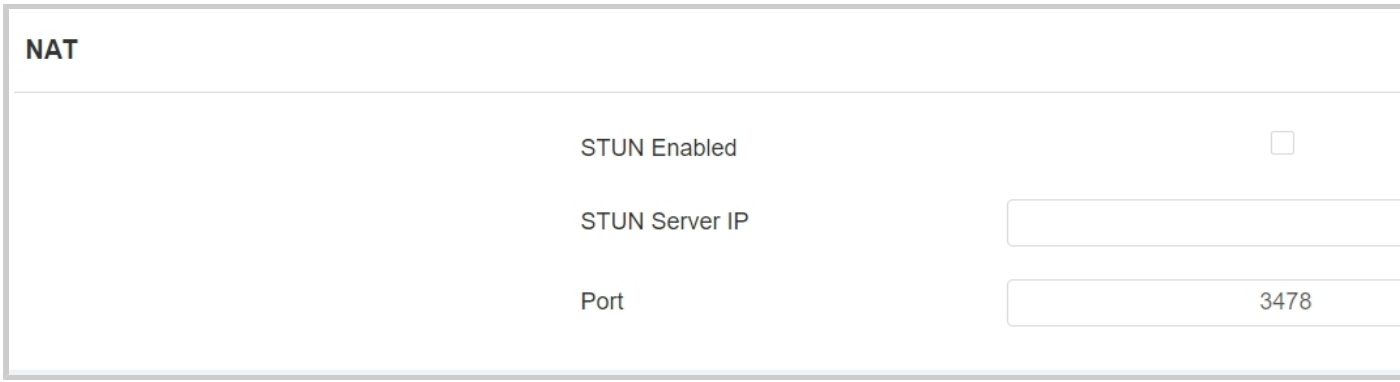
- **HTTP Port**: The port for the HTTP access method. 80 is the default port.

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.

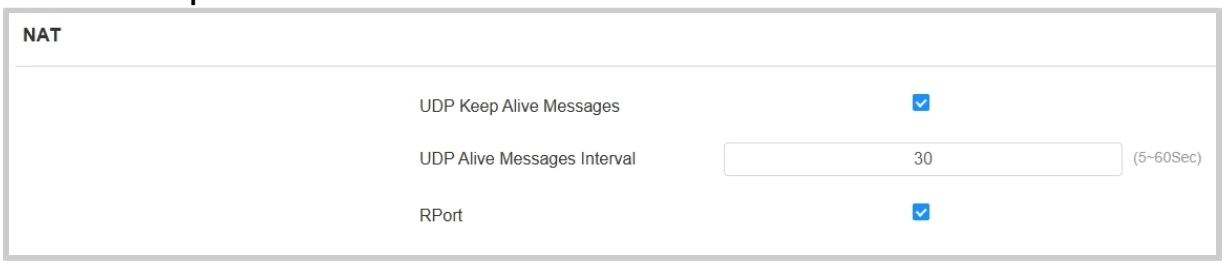
To register SIP accounts on third-party servers in a Wide Area Network(WAN), you need to enable the RPort feature on the intercom devices to establish a stable connection.

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



- **Stun Server IP**: 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 Messages Interval**: The message-sending time interval ranges from 5 to 60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when the SIP server is in WAN.

Intercom Call Configuration

IP Call Configuration

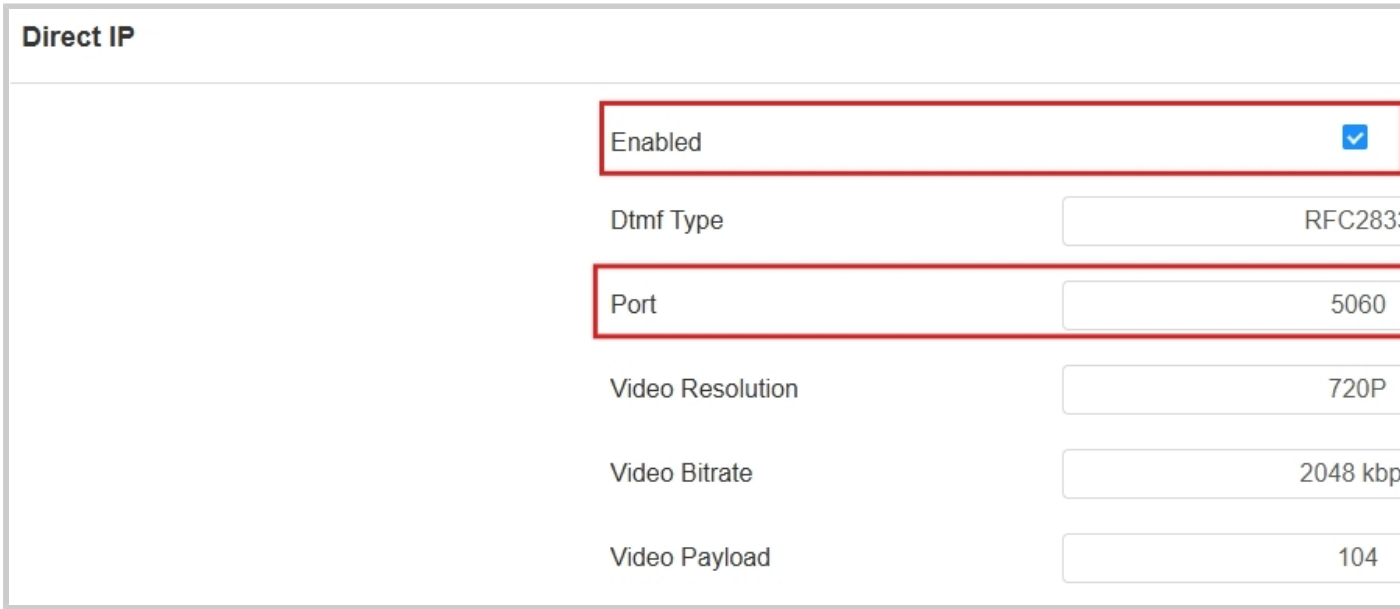
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

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

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



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

SIP Call Configuration

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

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

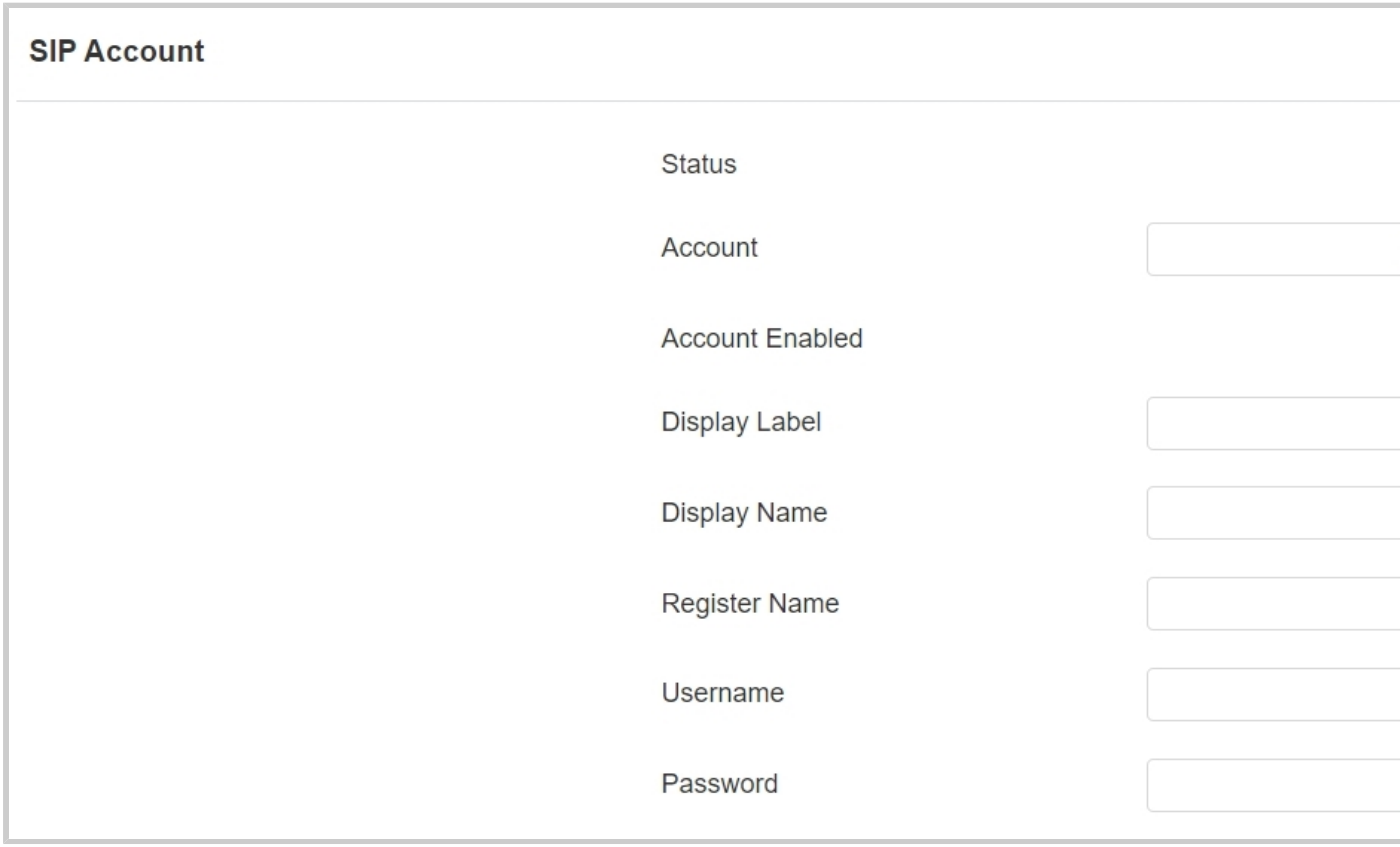
SIP Account Registration

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

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

Click here to view the SIP account registration example.

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



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

Tip

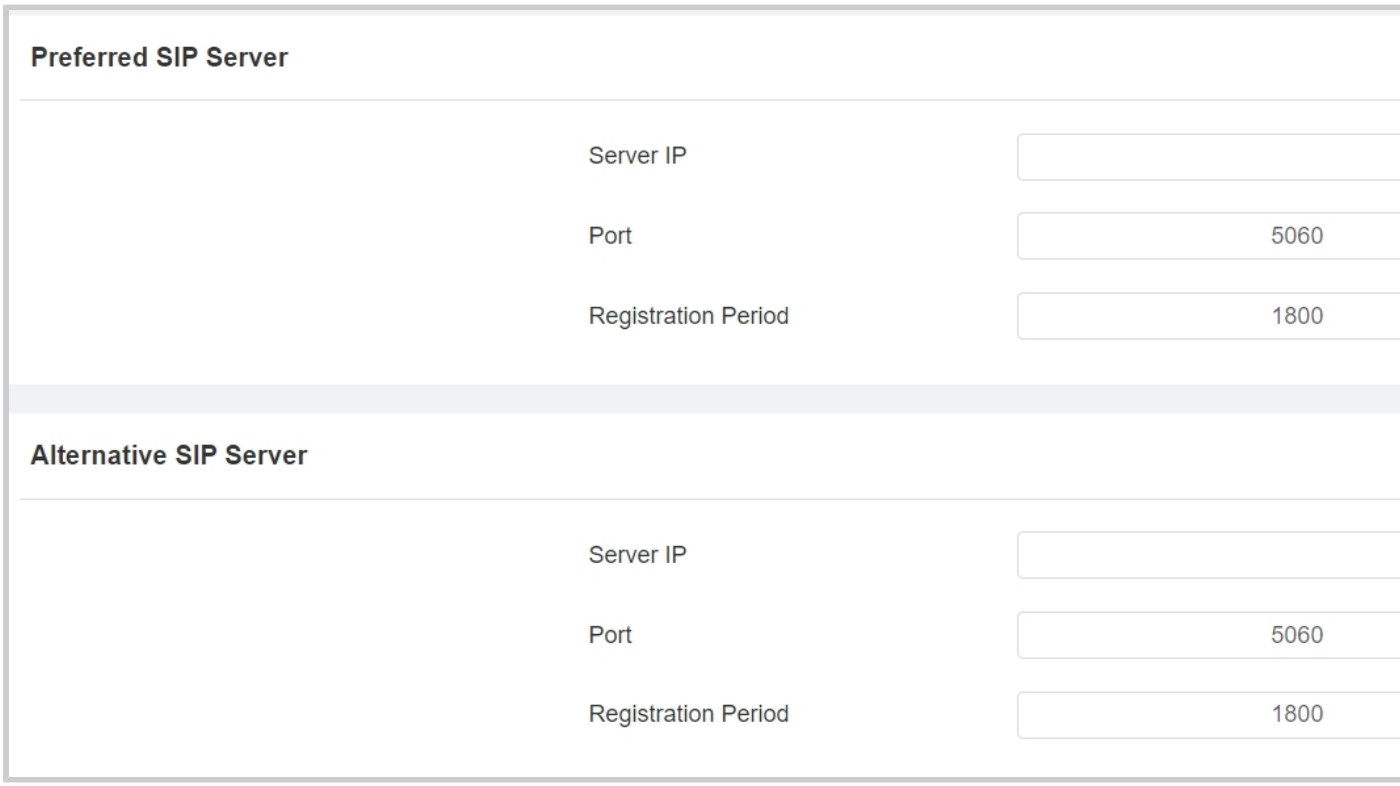
- For configuring contact call and dial plan, see here.
- When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

- **Account Enabled**: Check to activate the registered SIP account.
- **Display Label**: The device label to be shown on the device screen.
- **Display Name**: The device's name to be shown on the device being called to.
- **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 configure the SIP server, go to the web **Account > Basic** interface.

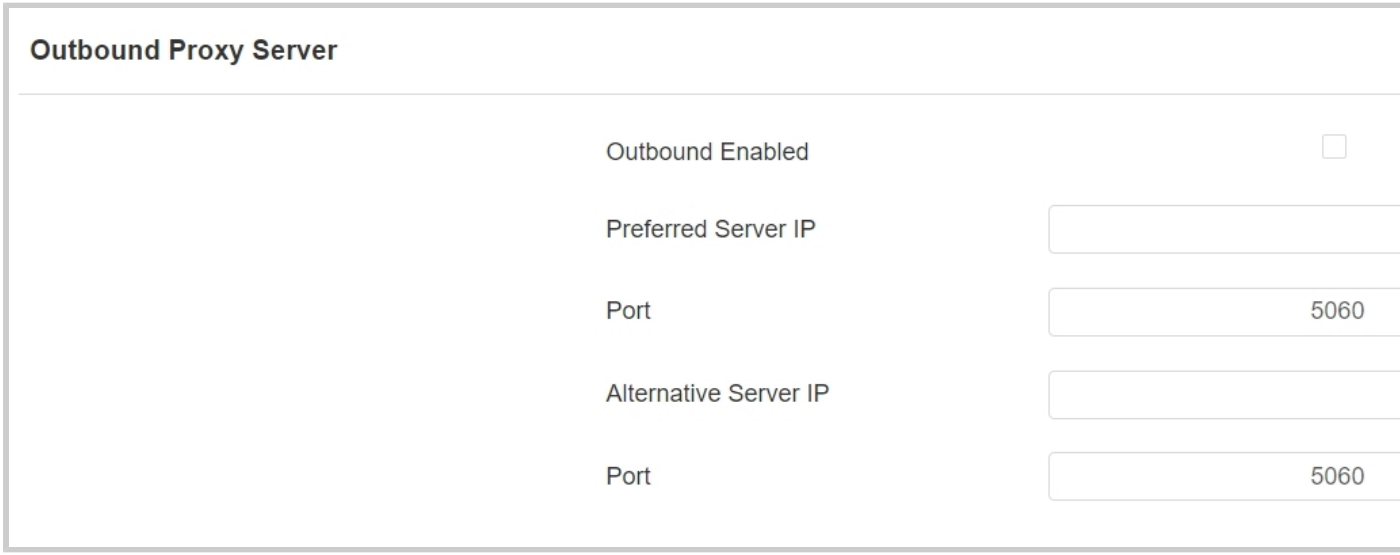


- **Server IP**: Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified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

Outbound Proxy Server

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

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



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

Data Transmission Type

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

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



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

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

Analog Setting

Users can use an analog switch to answer calls made to the door phone after it is connected to the door phone.

Set it up on the web **Intercom > Basic > Analog Setting** interface.



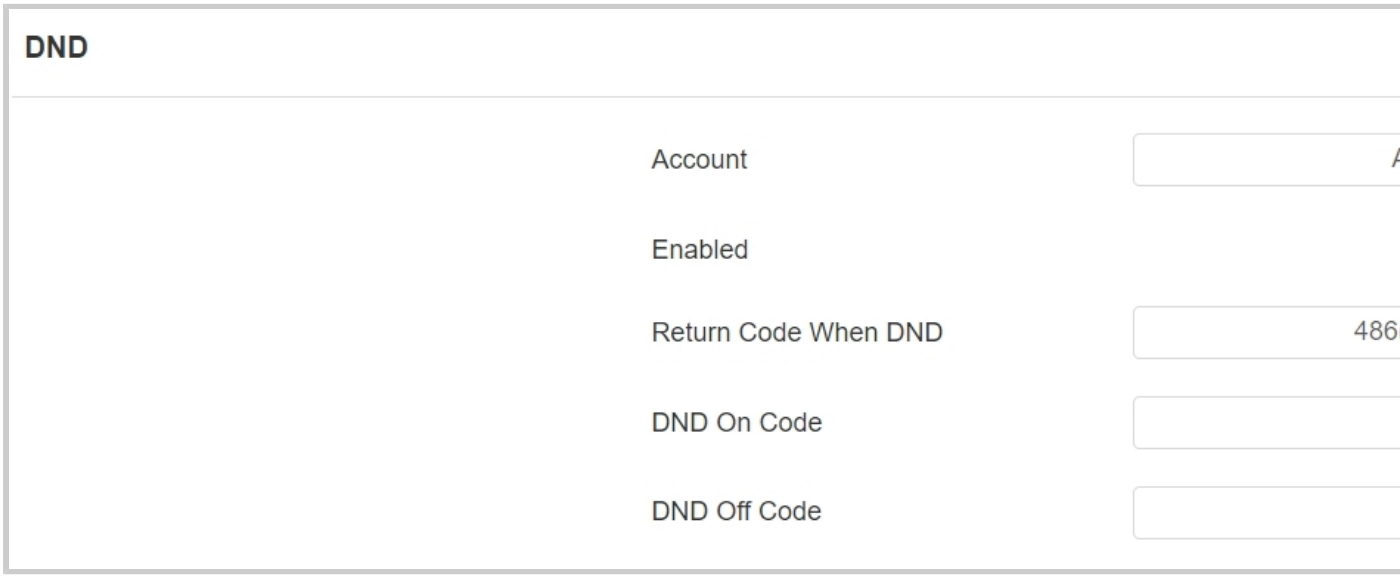
- **Adapter**: The brand of the analog switch that the door phone is connected to. You can select from **Akuvox, Vizit, Cyfral, Eltis, Metakom**, and **Lascomex**.

Call Setting

DND Configuration

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 configure DND, navigate to the web **Intercom > Call Feature** interface.

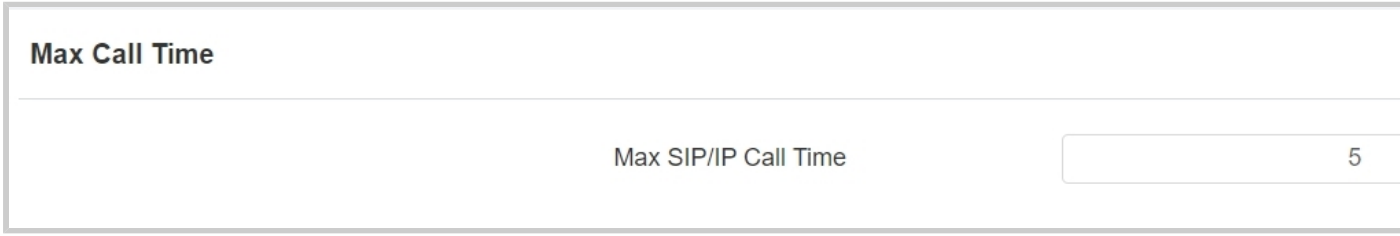


- **Account**: The account to apply the DND feature.
- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.
- **DND On Code**: The code used to turn on DND in the SIP server.
- **DND Off Code**: The code used to turn off DND in the 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 configure call time duration, navigate to the web **Intercom > Call Feature** interface.



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

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 configure maximum dial duration, navigate to the web **Intercom > Call Feature** interface.

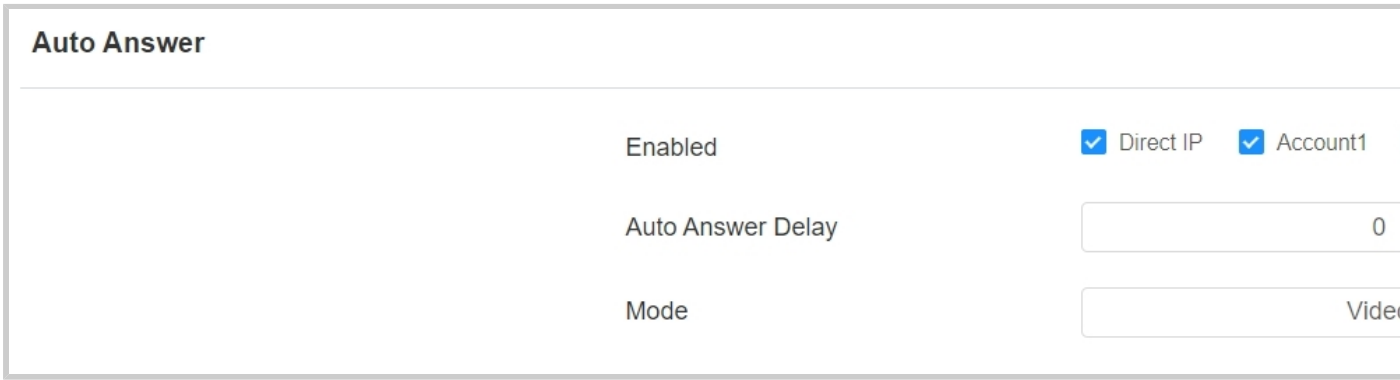


- **Max SIP/IP Dial In Time**: Specify the maximum duration of an incoming call. The door phone will automatically end the incoming call if it is not answered within the preset time.
- **Max SIP/IP Dial Out Time**: Specify the maximum duration of an outgoing call. The door phone will automatically end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

Auto-answer Configuration

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

To configure auto-answer, navigate to the web **Intercom > Call Feature** interface.

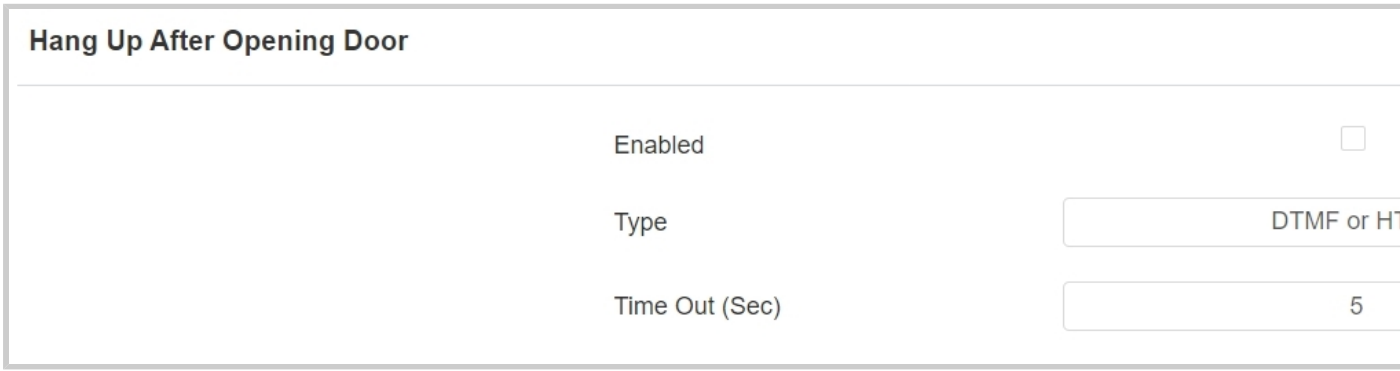


- **Enabled**: Apply auto-answer to IP calls and/or SIP calls.
- **Auto Answer Delay**: Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode**: Determine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

Hang Up After Opening the Door

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

To configure it, navigate to the web **Intercom > Call Feature** interface.



- **Type**: Specify the door unlock 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(Sec)**: 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.

Prevent SIP Hacking

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

To configure SIP hacking, navigate to the web **Account > Advanced** 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.

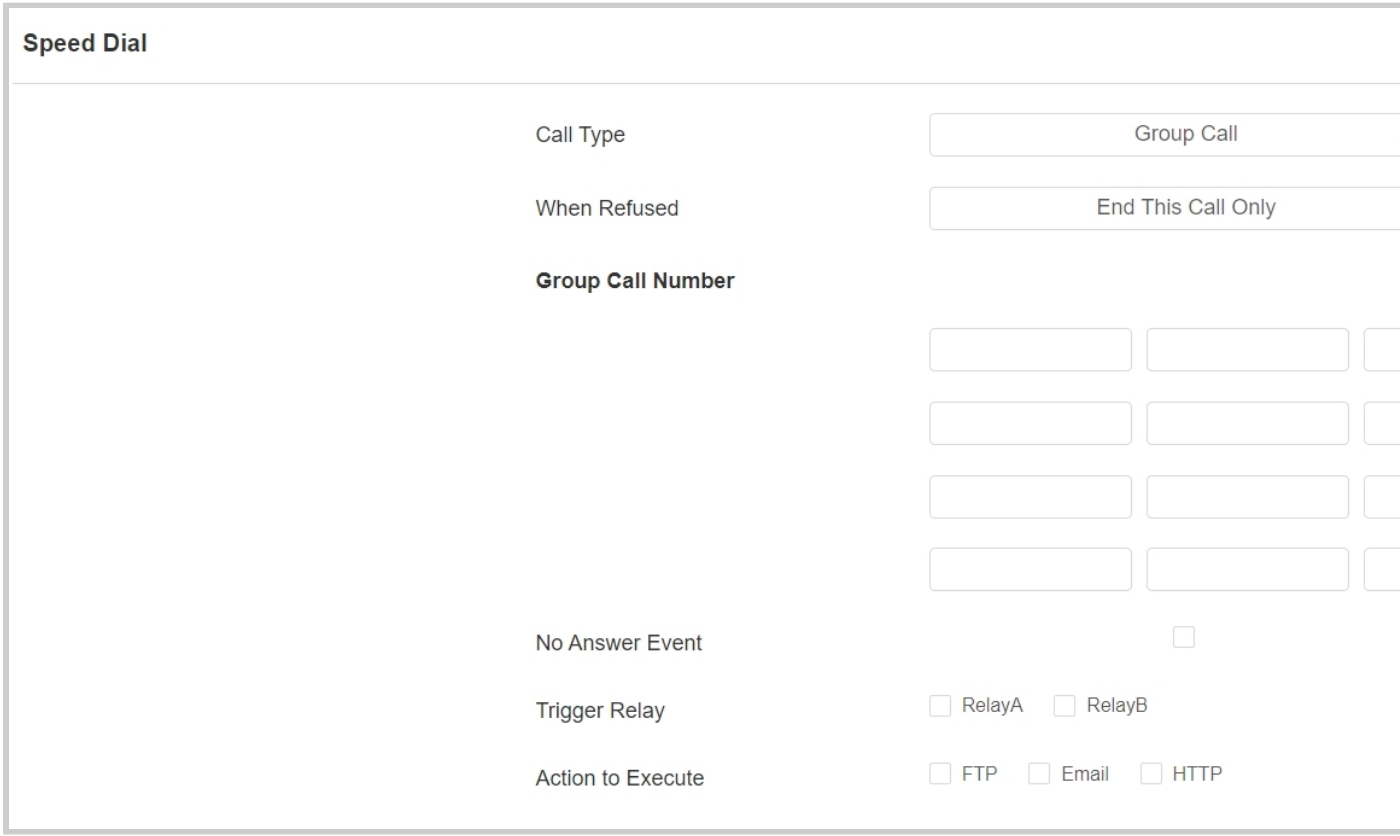
Speed Dial

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.

You can create up to 16 group call numbers.

To configure the group call, navigate to the web **Intercom > Basic** interface.



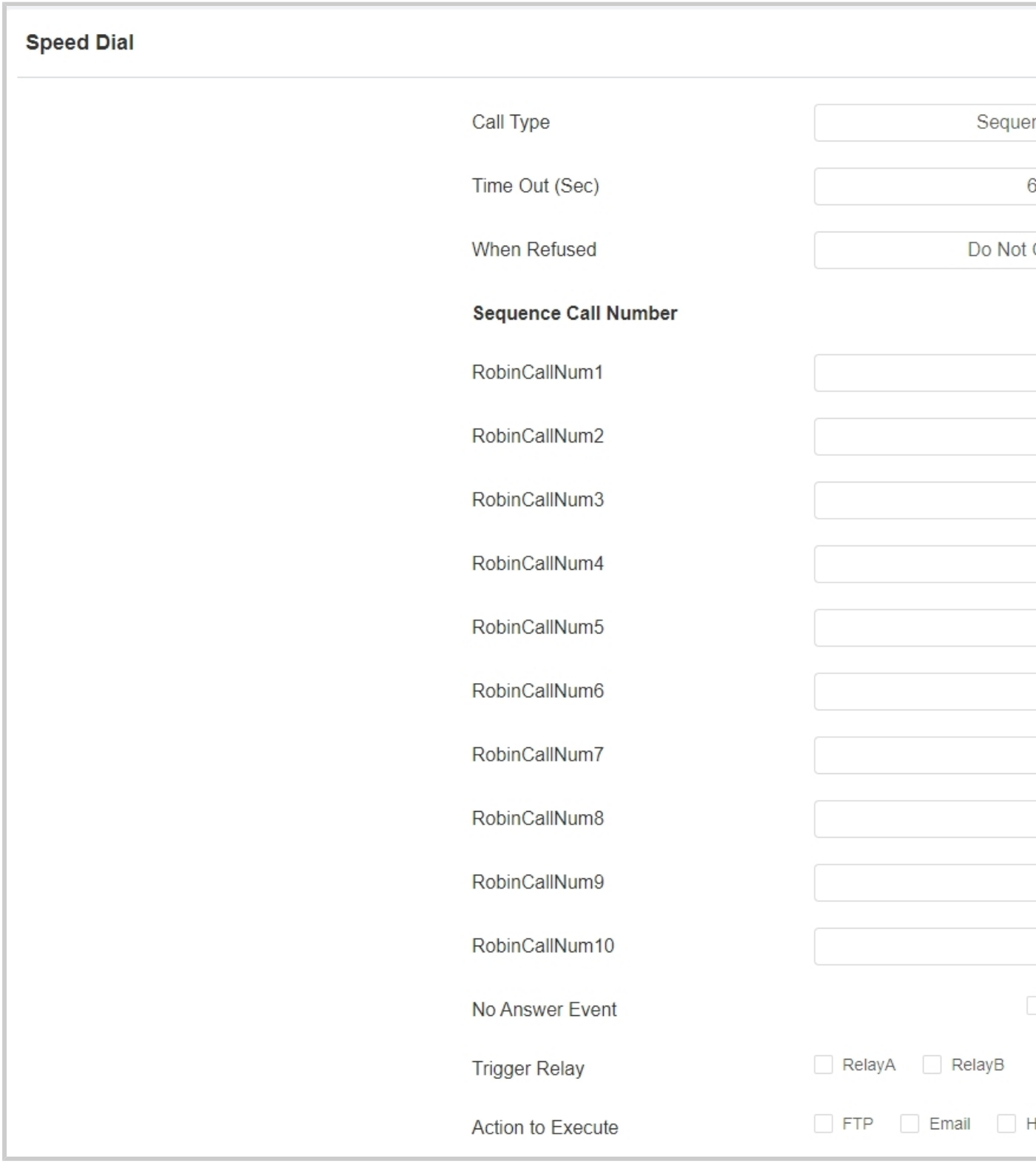
- **Call Type**: Group Call or Sequence Call.
- **When Refused**:
  - **End This Call Only**: The device will continue to call other numbers.
  - **End All Calls**: The device will stop calling.
- **Group Call Number**: If you fill in the local group call number, the local group number will be called instead of the SmartPlus group call number.
- **No Answer Event**: When the call is not answered, actions will be triggered.
- **Trigger Relay**: Relay to be triggered when the call is not answered.
- **Action to Execute**: Action(s) to be triggered when the call is not answered.
  - **FTP**: Send a screenshot to the designated FTP address.

- **Email**: Send a screenshot to the designated email address .
- **HTTP**: Send the HTTP message to the HTTP server.
  - **HTTP URL**: The format is http://HTTP server's IP/Message content.

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 configure the sequence call, navigate to the web **Intercom > Basic** interface.



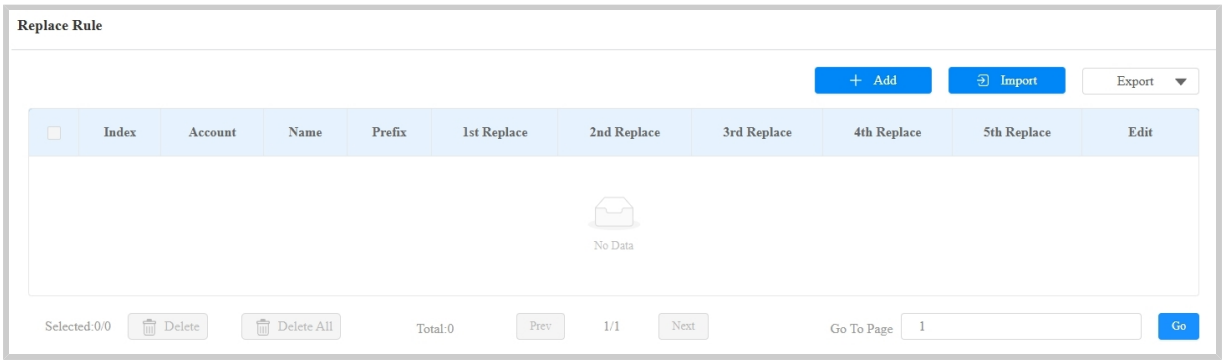
- **Call Type**: Group Call or Sequence Call.

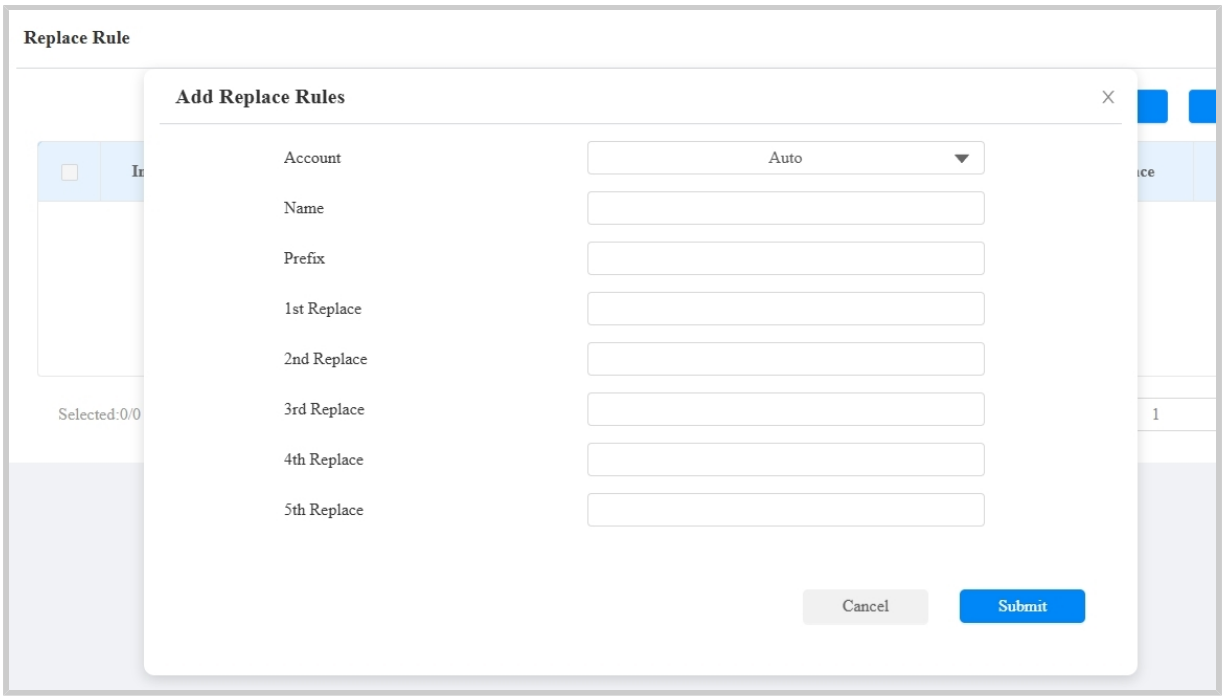
- **Time Out(Sec)**: Set the call timeout before calling the next called party when the first called party does not receive the call within the timeout.
- **When Refused**:
  - **Do Not Call Next**: The device will stop calling.
  - **Call Next**: The device will continue to call other numbers.
- **No Answer Event**: when the call is not answered, actions will be triggered.
- **Trigger Relay**: relay(s) to be triggered when the call is not answered.
- **Action to Execute**: Action(s) to be triggered when the call is not answered.
  - **FTP**: Send a screenshot to the designated FTP address.
  - **Email**: Send a screenshot to the designated email address .
  - **HTTP**: Send the HTTP message to the HTTP server.
    - **HTTP URL**: The format is http://HTTP server's IP/Message content.

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 configure the dial plan, navigate to the web **Intercom > Dial Plan** interface. Click **Add**. You can add up to 500 rules.



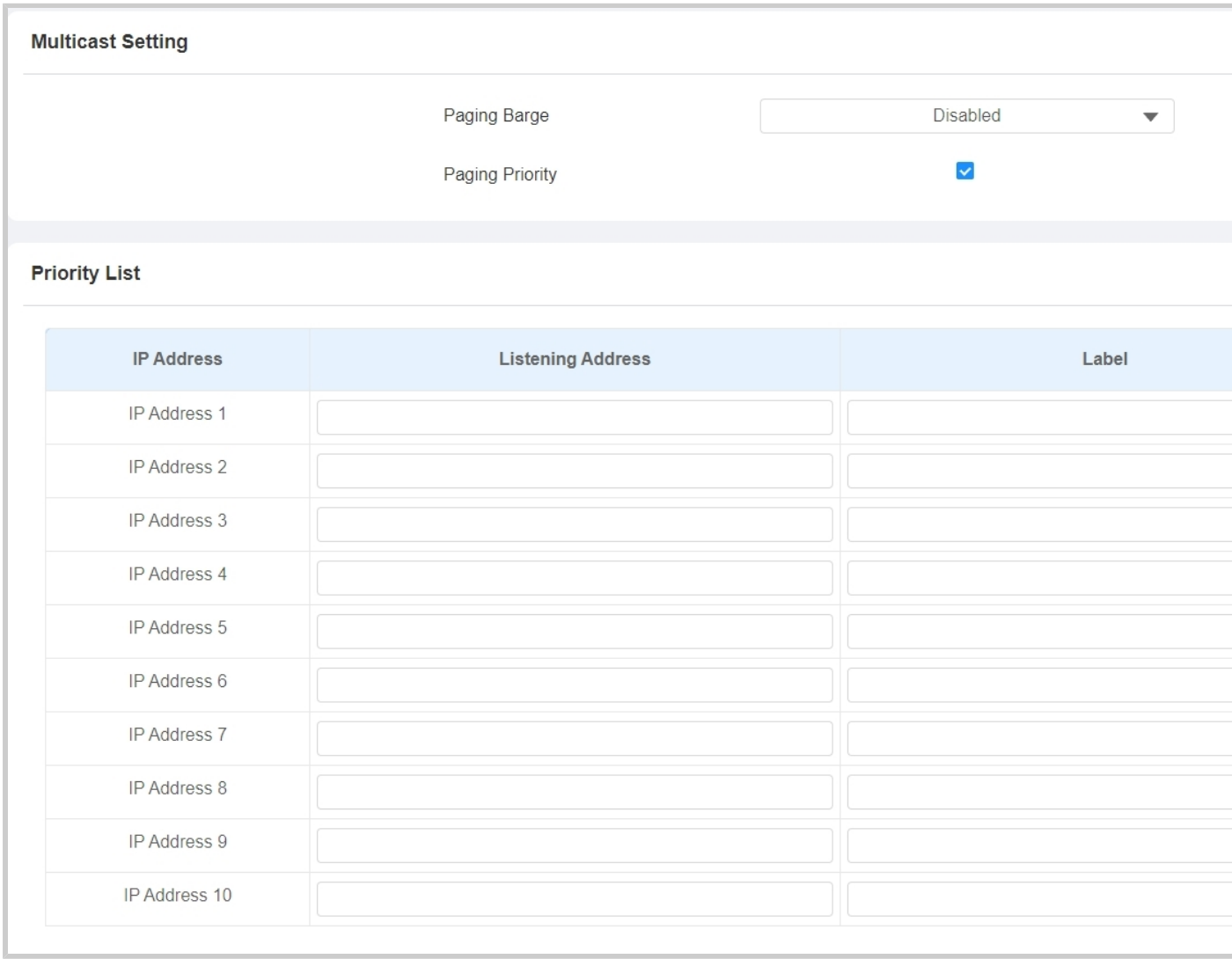


- **Account:** Select the dial-out account.
  - **Auto:** Dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.
  - **Account 1/2:** Dial-out using the chosen account.
- **Name**: Name this rule.
- **Prefix:** Specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** Specify up to 5 numbers, which can be SIP numbers or IP addresses, to be replaced by the prefix. All these numbers will be called simultaneously when the caller dials the prefix.

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 configure multicast, navigate to **Intercom > Multicast** interface.



- **Paging Barge**: Multicast or how many multicast calls have higher priority than SIP calls. If you disable Paging Priority, SIP calls will have higher priority.

- **Paging Priority**: Multicast calls are called in order of priority or not.
- **Listening Address**: The multicast IP address to be listened to. The multicast IP address needs to be the same as the listened part, and the multicast port cannot be the same for each IP address. Multicast IP addresses are from 224.0.0.0 to 239.255.255.255.

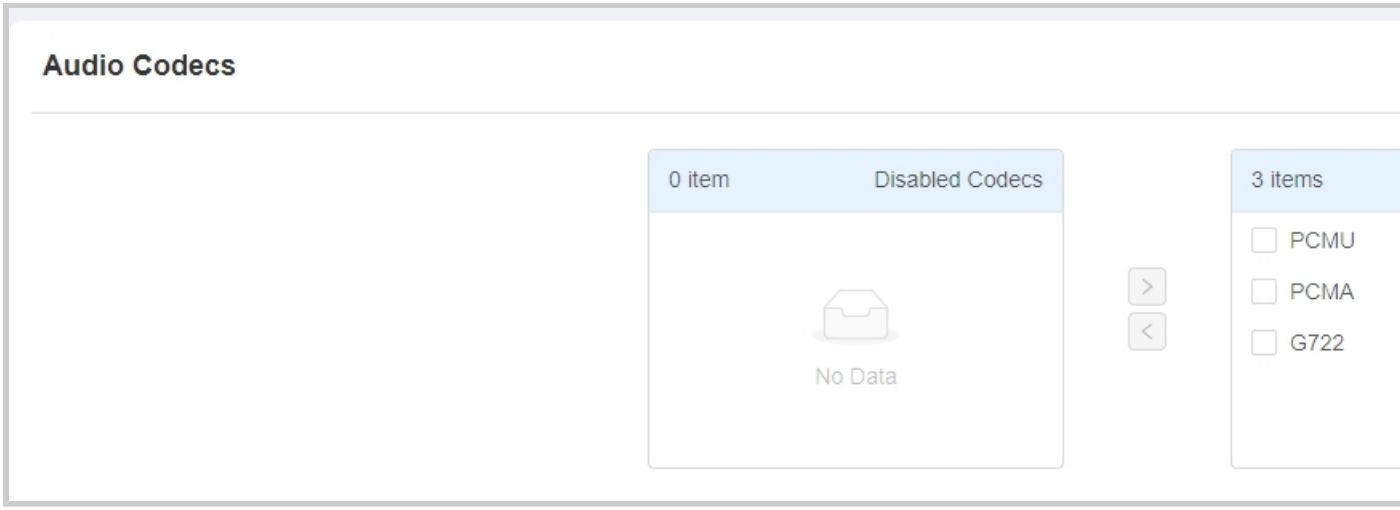
Audio & Video Codec Configuration

Audio Codec Configuration

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

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



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

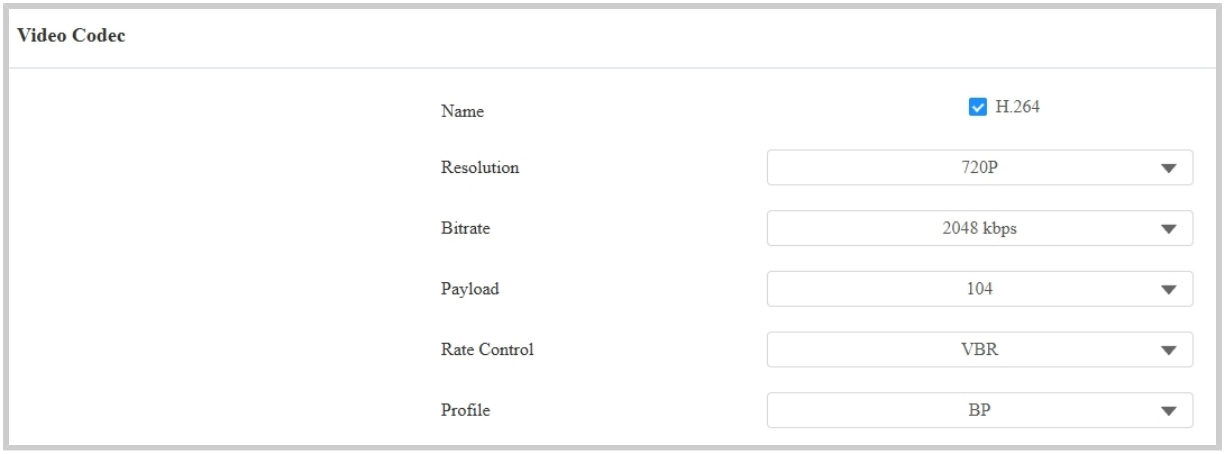
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ

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

Video Codec Configuration

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

To configure the video codec, navigate to the web **Account > Advanced** interface.



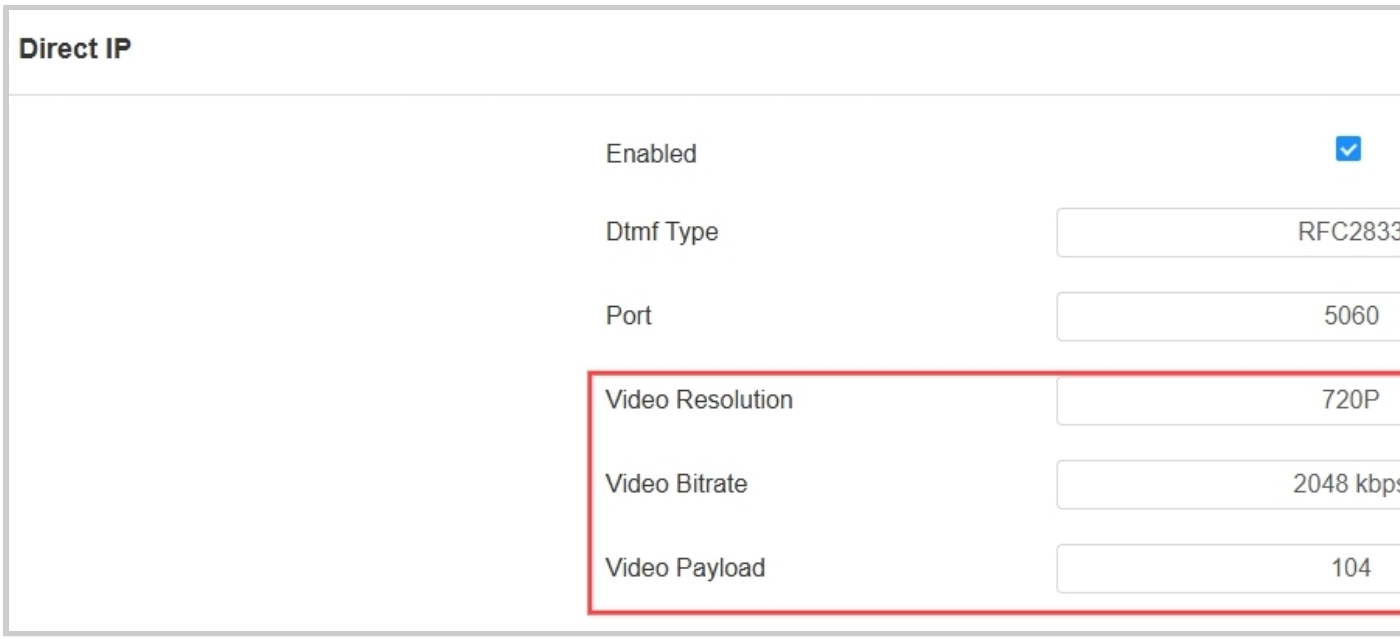
- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the code resolution for the video quality from available options. The default resolution is 720P(720 × 480 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the data transmitted every second the greater in amount, therefore, the clearer the video will be. The default code bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.
- **Rate Control**: Set the account's call bitrate. The default is VBR.

  - **VBR**: Variable Bit Rate, adjusts the bit rate dynamically based on content complexity.
  - **CBR**: Constant Bit Rate, maintains a fixed bit rate throughout the transmission.
- **Profile**: The attributes of locally encoded video, such as resolution, bitrate, and frame rate.
  - **BP**: Baseline Profile, designed for low complexity and real-time applications, such as video conferencing and mobile devices.
  - **MP**: Main Profile, provides higher compression efficiency and video quality than Baseline.
  - **HP**: High Profile, offers the highest video quality and compression efficiency, supporting advanced encoding features.

Video Codec for IP Direct Calls

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

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



- **Video Resolution**: Select the code resolution for the video quality from the available options. The default is 720P(720 × 480 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The default code bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Contacts Configuration

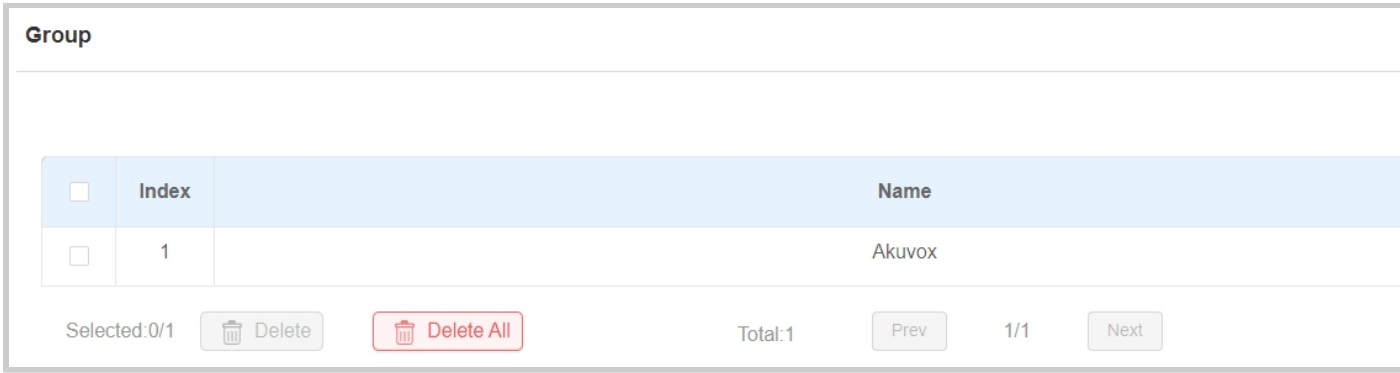
The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

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

Manage Contact Groups

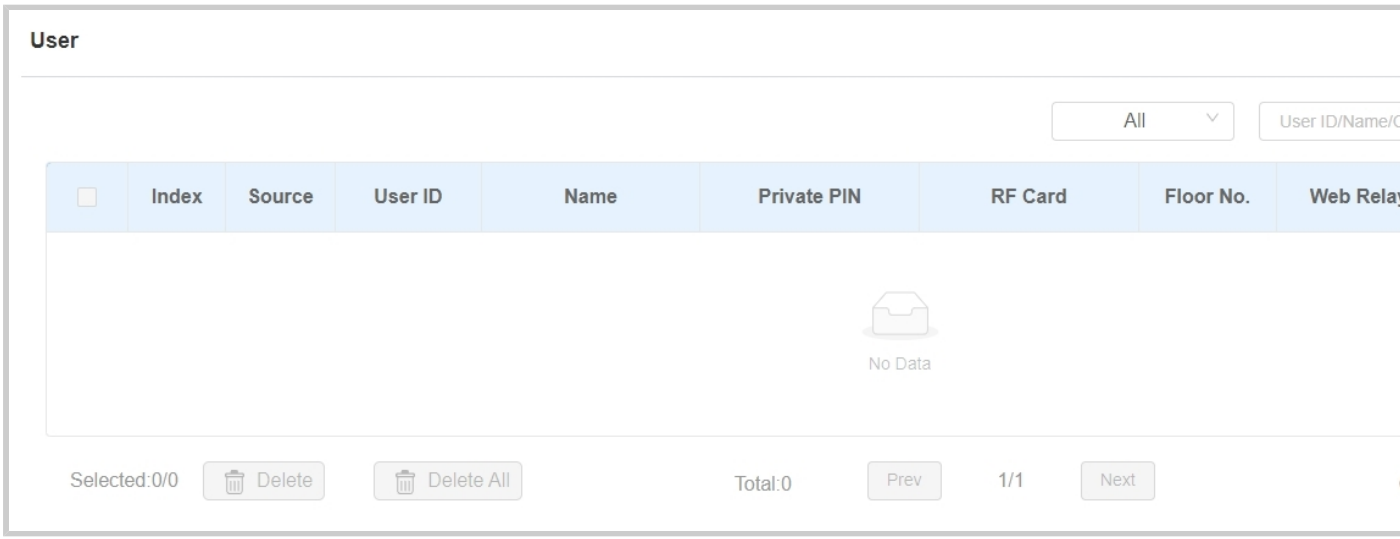
You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

Set it up on the web **Directory > User > Group** interface. Click **+Add** to add a group. The device supports adding up to 1,000 groups.

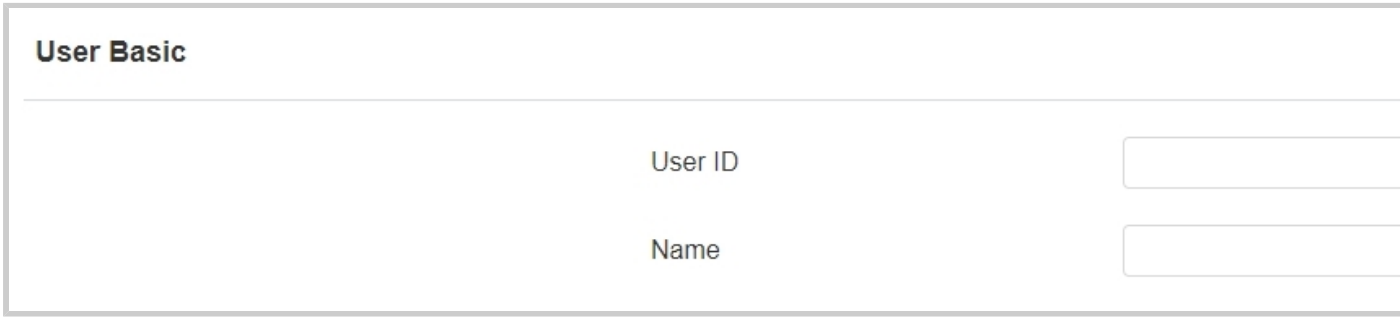


Set up Contact Details

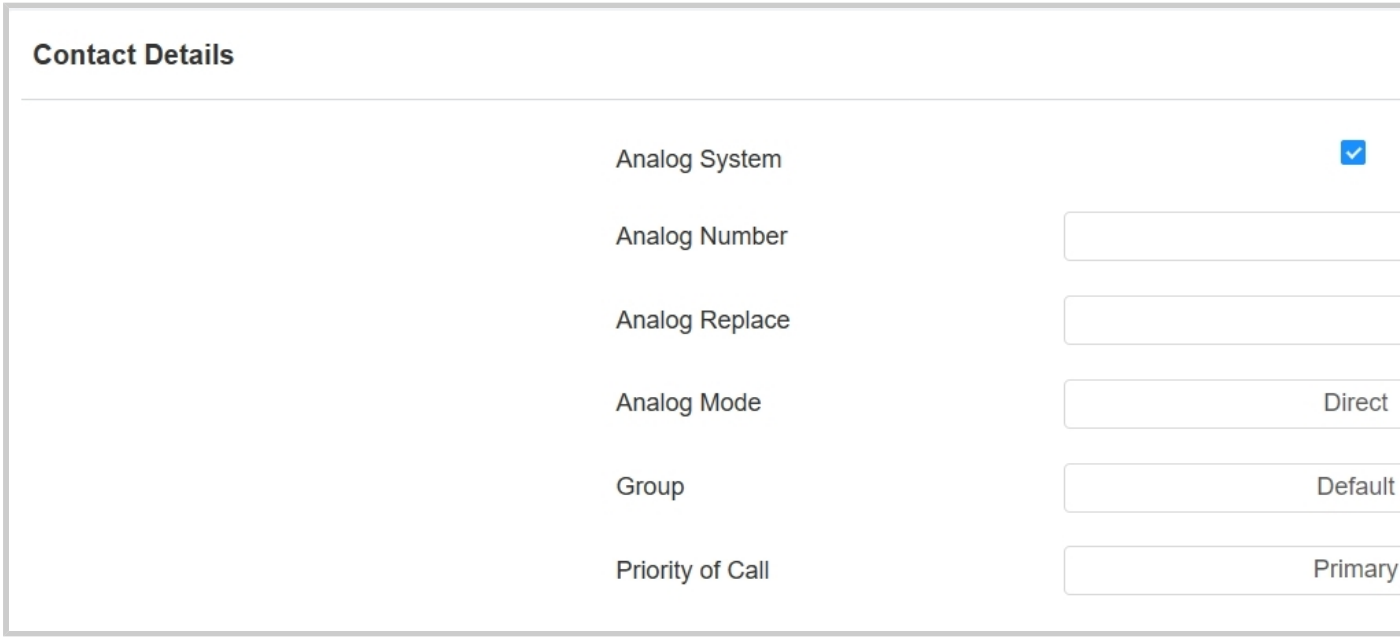
Add the contact information of users on the web **Directory > User** interface. The device supports up to 10,000 users. Click **+Add** to add a user.



Set the user ID and name.



Find the **Contact Details** part.



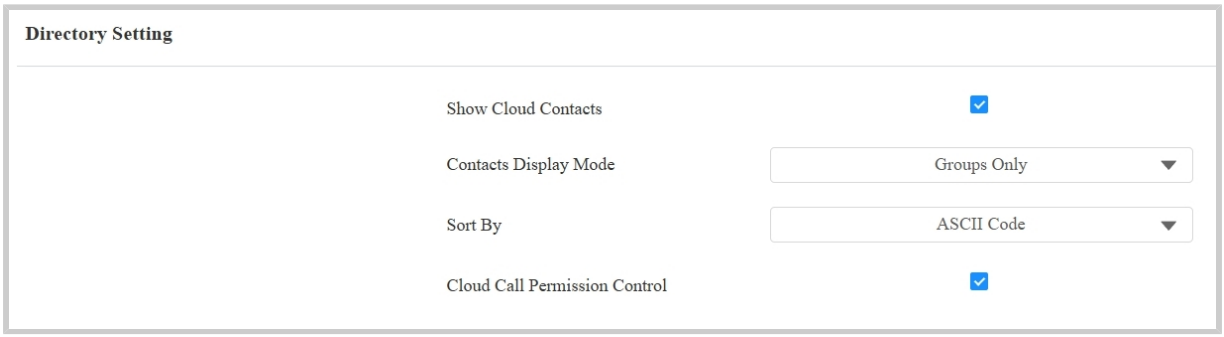
- **Analog System**: When enabled, configure the analog number, and users can call the analog handset.
- **Analog Number**: The number of the analog switch.
- **Analog Replace**: Optional configuration. The short number replaces the analog number. Users can call the analog handset by entering the short number on the door phone's keypad.
- **Analog Mode**: **Direct** means the analog switch is connected to the door phone through wires. **Proxy** means the analog switch is not connected to the door phone through wires and when this option is selected, the analog proxy address needs to be filled in.
- **Analog Proxy Address**: Available when **Proxy** mode is selected. The IP address of the door phone in **Direct** mode.
- **Group**: Put the contact in a desired contact group.
- **Priority of Call**: Set the priority of the call among three options: Primary, Secondary, and Tertiary. For example, if you set the priority of call for one of the contacts in a specific contact group as Primary, then the contact will be the first to be called among all the contacts when someone presses on the contact group to make a group call.
- **Dial Account**: The account to make the call.

> **Tip**
>
> To see detailed steps of configuring analog feature, please refer to:
>
> - Integration Between S532 and Analog Handsets.
> - Integration Between S532 and Akuvox Answering Units.
>
> Without filling in the contact number, the contact will not display on the Directory screen.

Contact List Display

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

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

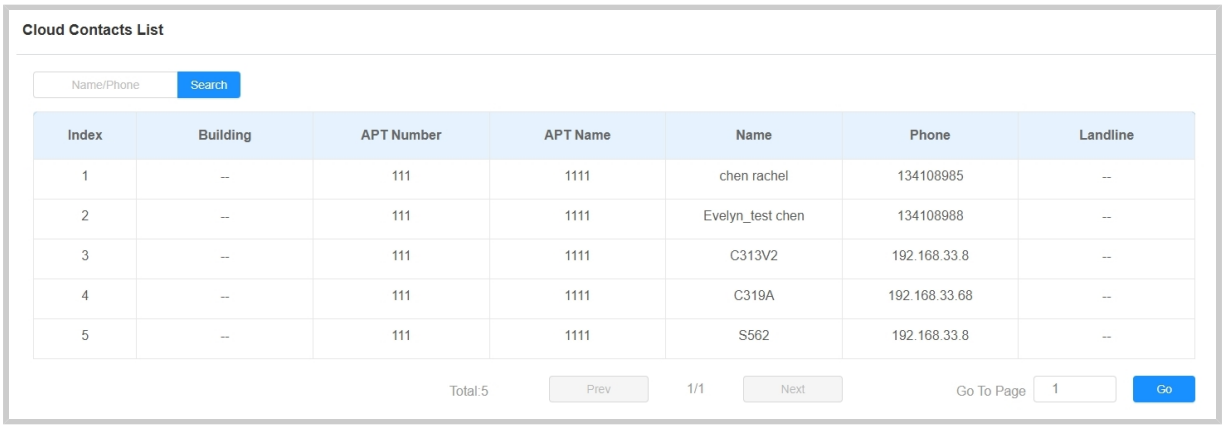


- **Show Cloud Contacts**: The contacts synchronized from the SmartPlus Cloud can be displayed.
- **Contacts Display Mode**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only:** Display contact groups. Press the desired group on the device screen to make a group call.
  - **Contact Display by Group:** Display contacts by groups. Press the group, and users can see the contacts in it.
  - **APT Only**: This option works when the device is deployed on the Akuvox Cloud and added to the Public Area.

    - Display all apartments in a single flat list. Visitors can select and call an apartment directly without entering a building directory.
    - Not supported in Self-Organizing Network Solution.
  - **Do Not Display Contacts**: Neither contacts nor groups will display.
- **Sort By**:
  - **ASCII Code** lists the tenants by their names in the sequence of the ASCII code.
  - **Room No.** lists the tenants according to their room numbers.
  - **Import** lists the tenants according to their order in the imported file.
- **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 the calls.

Cloud Contact List

When the device is connected to the SmartPlus Cloud, the cloud contacts will be displayed on the **Directory > Directory Settings > Cloud Contacts List**.

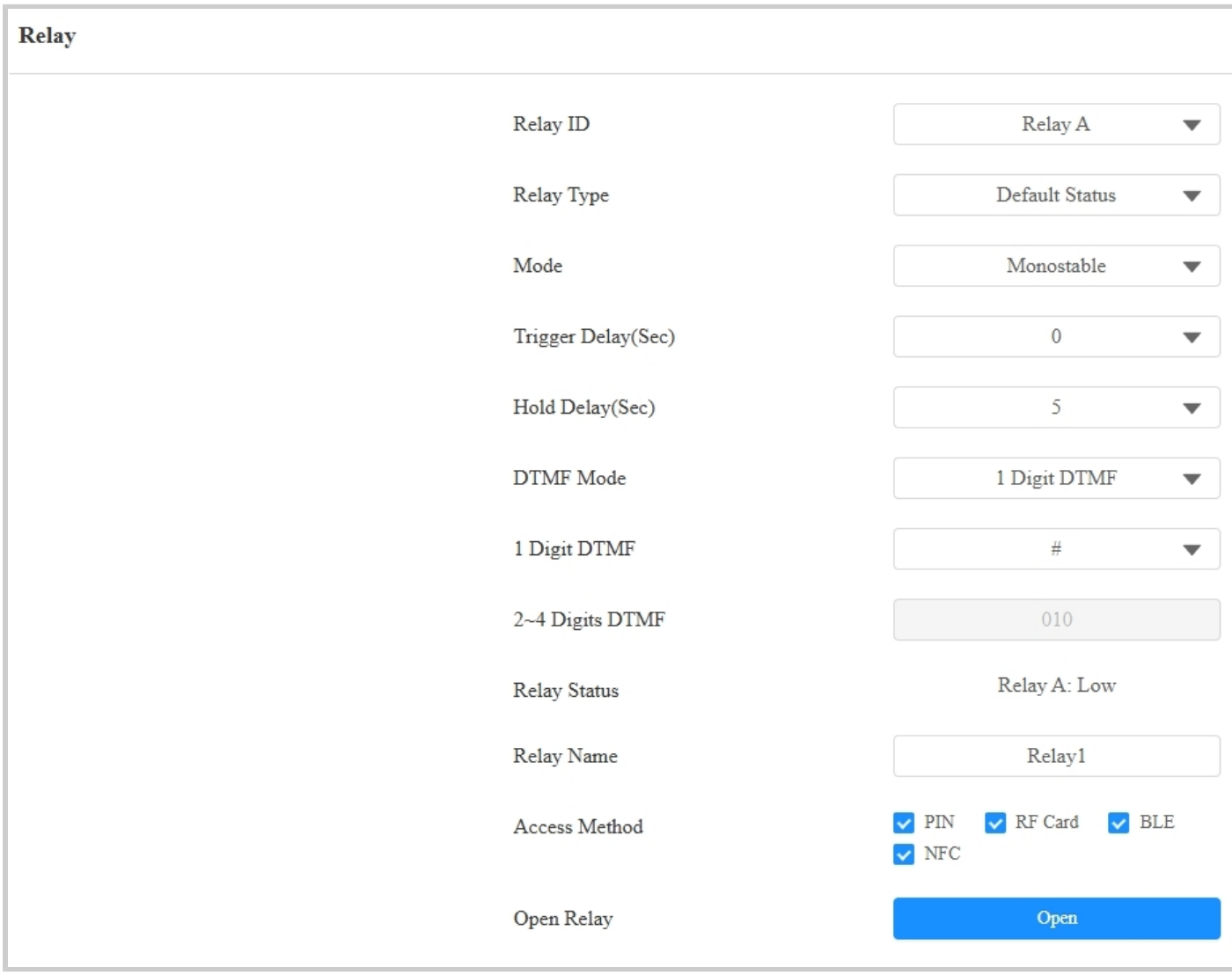

Cloud Contacts List
Name/Phone
Search
Index
Building
APT Number
APT Name
Name
Phone
Landline
1
--
111
1111
chen rachel
134108985
--
2
--
111
1111
Evelyn_test chen
134108988
--
3
--
111
1111
C313V2
192.168.33.8
--
4
--
111
1111
C319A
192.168.33.68
--
5
--
111
1111
S562
192.168.33.8
--
Total:5
Prev
1/1
Next
Go To Page
1
Go

Relay Setting

Local Relay

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

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



- **Relay ID**: The specific relay for door access.
- **Relay Type**: Determine the interpretation of the Relay Status regarding the state of the door:
  - **Default Status**: A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.
  - **Invert Status**: A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.
- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay (Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Access Method**: Check the method(s) to trigger the relay.
- **Open Relay**: You can click **Open** to trigger the relay manually.

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

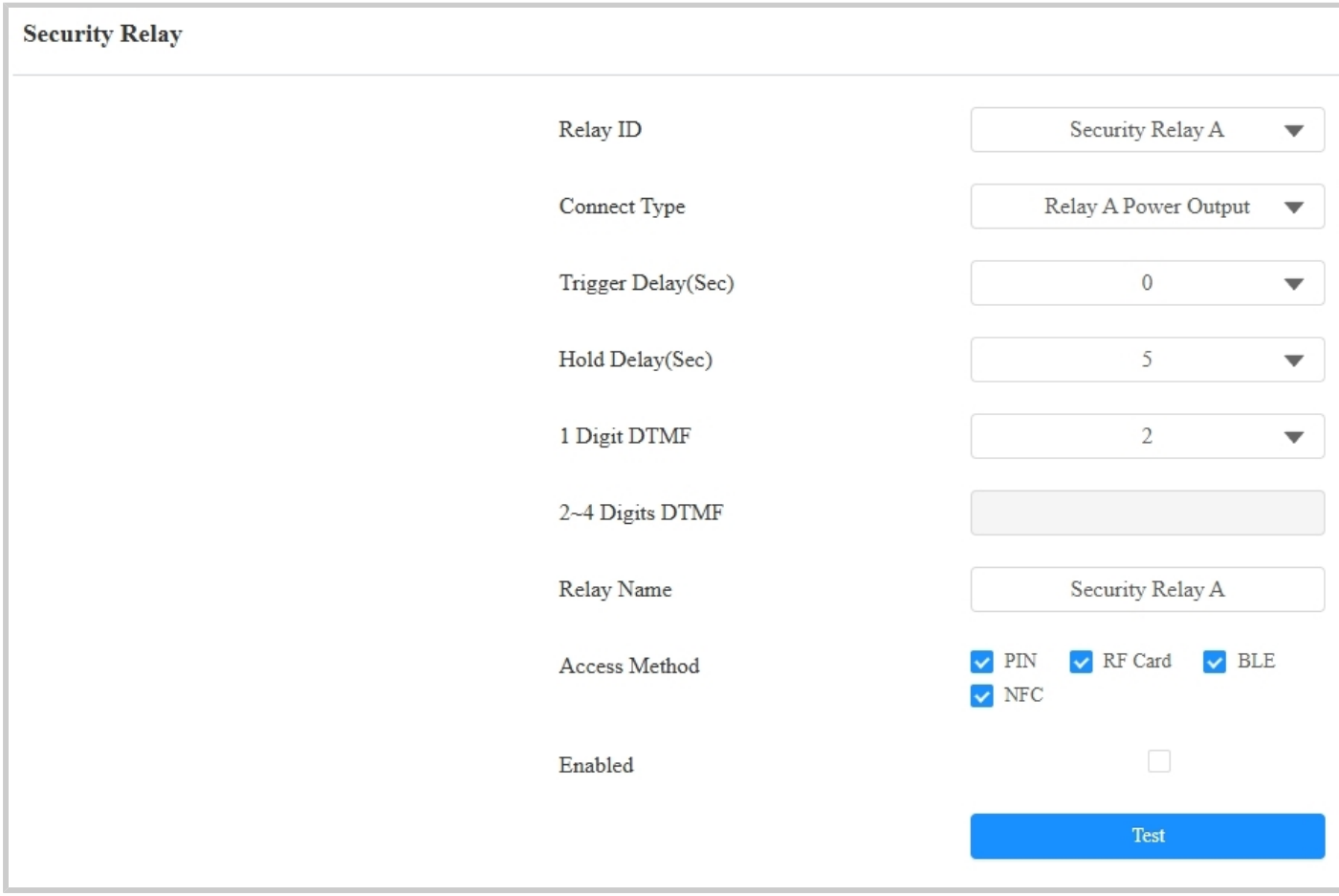
Security Relay

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



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

To configure the security relay, navigate to the web **Access Control > Relay** interface.



- **Connect Type**: Select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **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 method(s) to trigger the relay.

> **Note**
>
> When connecting the device to a SR01 via RS485, you need to select the RS485 mode as **Others** on the **Device > RS485** interface.

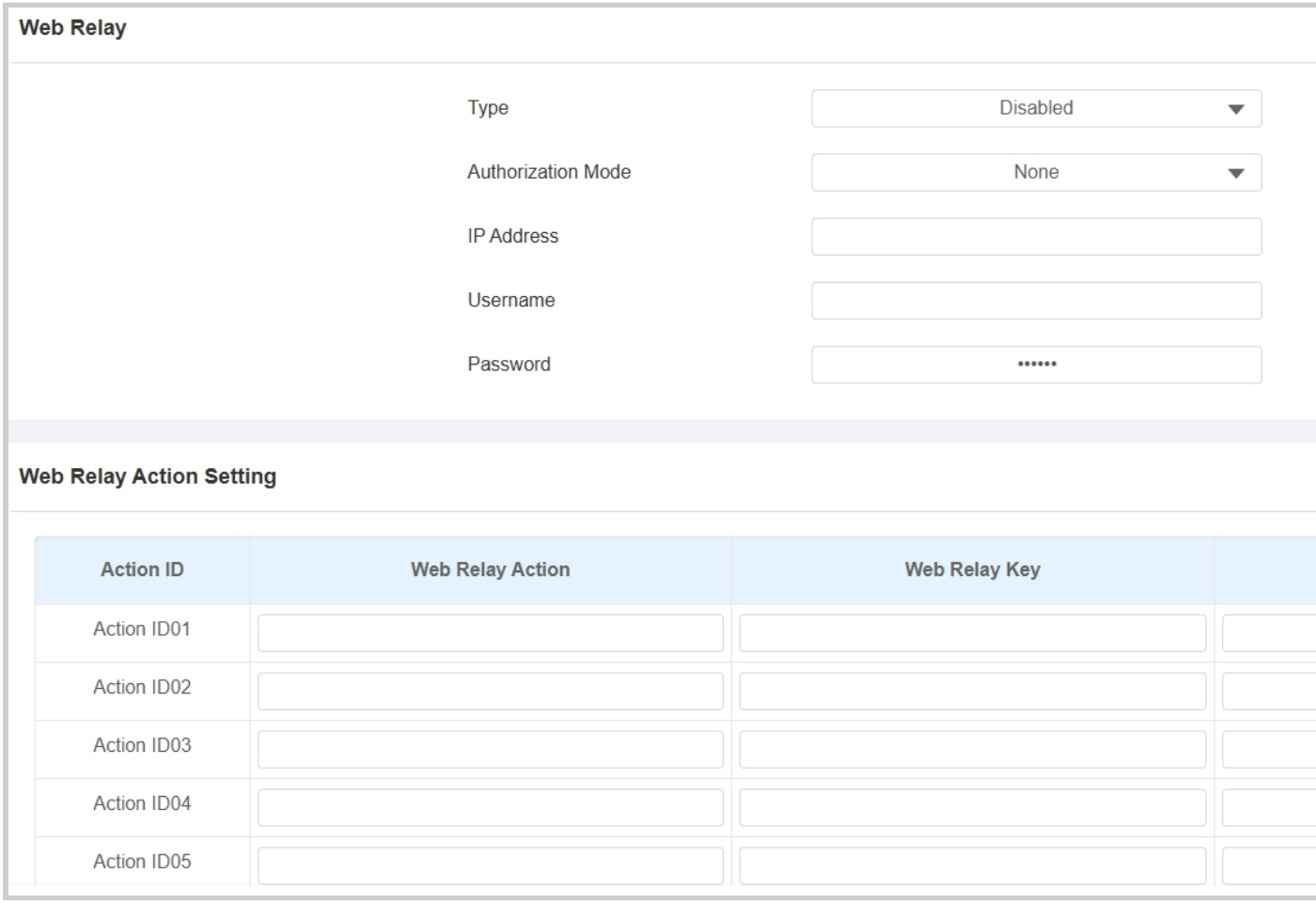
Web Relay

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 up a web relay, go to **Access Control > Web Relay** interface.



- **Type**:
  - **Disabled:** Only activate the local relay.
  - **Only WebRelay**: Only activate the web relay.
  - **Both Local Relay and Web Relay**: 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.
- **Authorization Mode**: Select the Authorization Mode between None and Digest. When Digest is selected, the username and password are used for authentication.
- **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**: The manufacturer-provided URLs for various actions, with up to 50 commands.

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

- **Web Relay Key**: Determine the methods to activate the web relay based on whether the DTMF code is filled.
  - Filling with the configured DTMF code restricts activation to card swiping and DTMF.
  - Leaving it blank enables all door-opening methods.
- **Web Relay Extension**: Specify the intercom device and the methods it can use to activate the web relay during calls.
  - When an intercom device's IP/SIP is specified, only that device can trigger the web relay (except for via card swiping or DTMF) during calls.
  - If left blank, all devices can trigger the relay during calls.

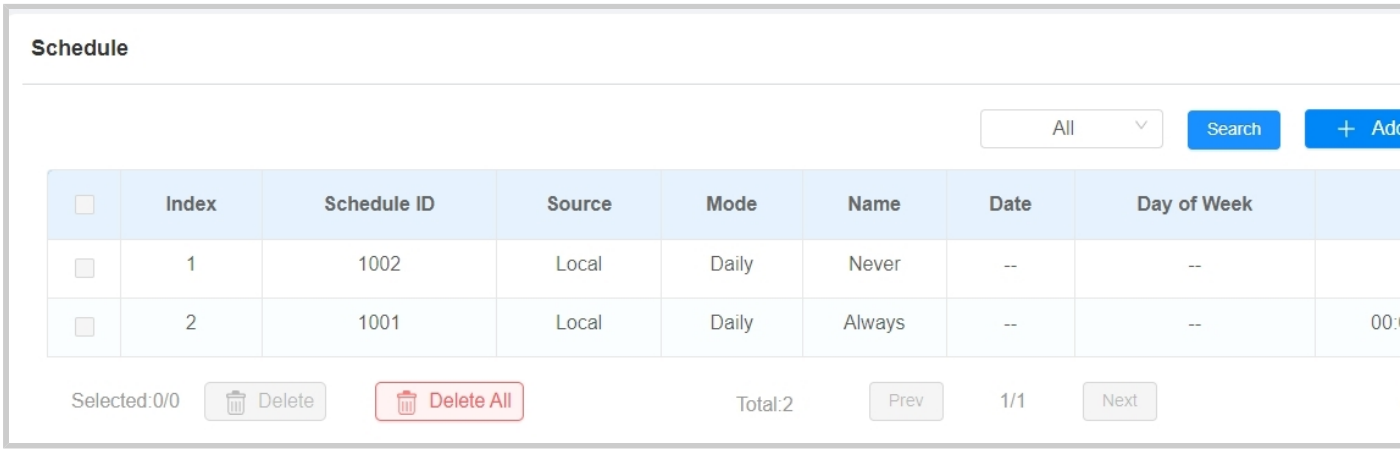
Door Access Schedule Management

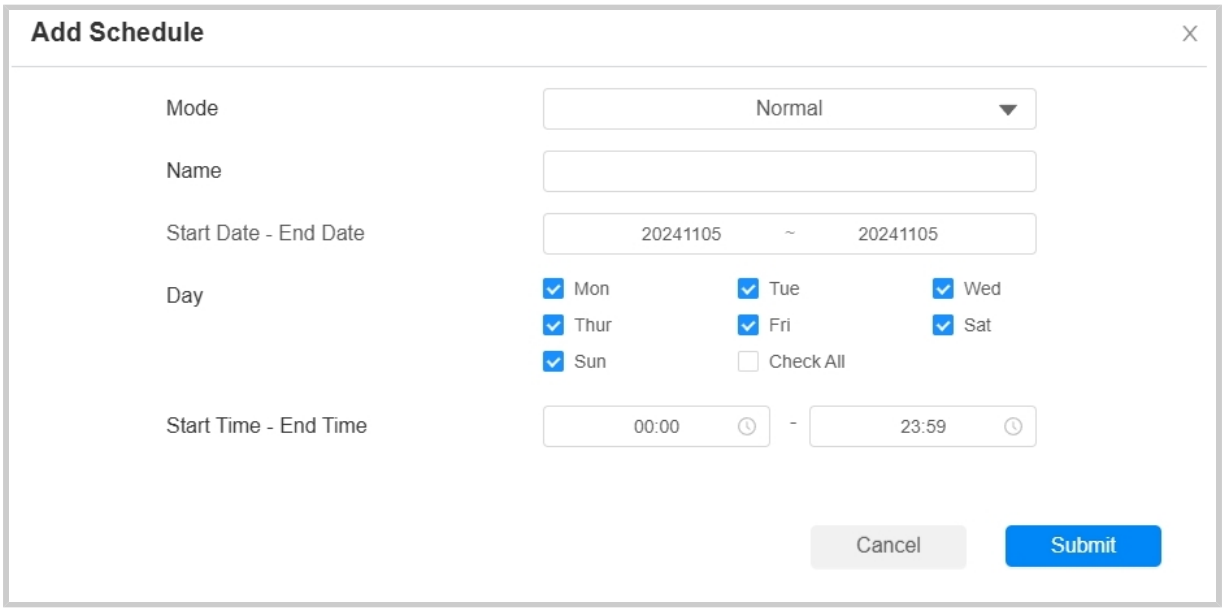
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create a Door Access Schedule

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

Set it up on the web **Setting > Schedule** interface. Click **+Add** to create a schedule. You can add up to 100 local schedules.



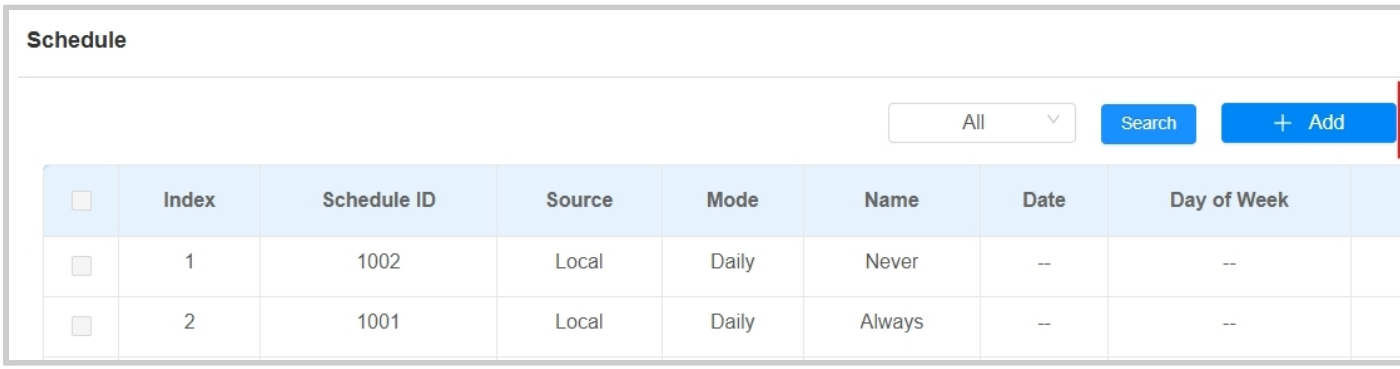


- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Name**: Name the schedule.

Import and Export Door Access Schedule

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

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



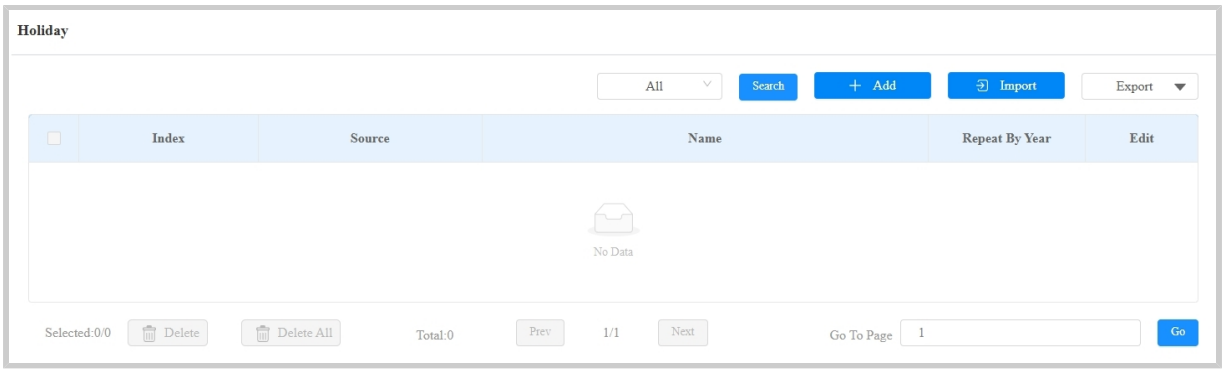
Note

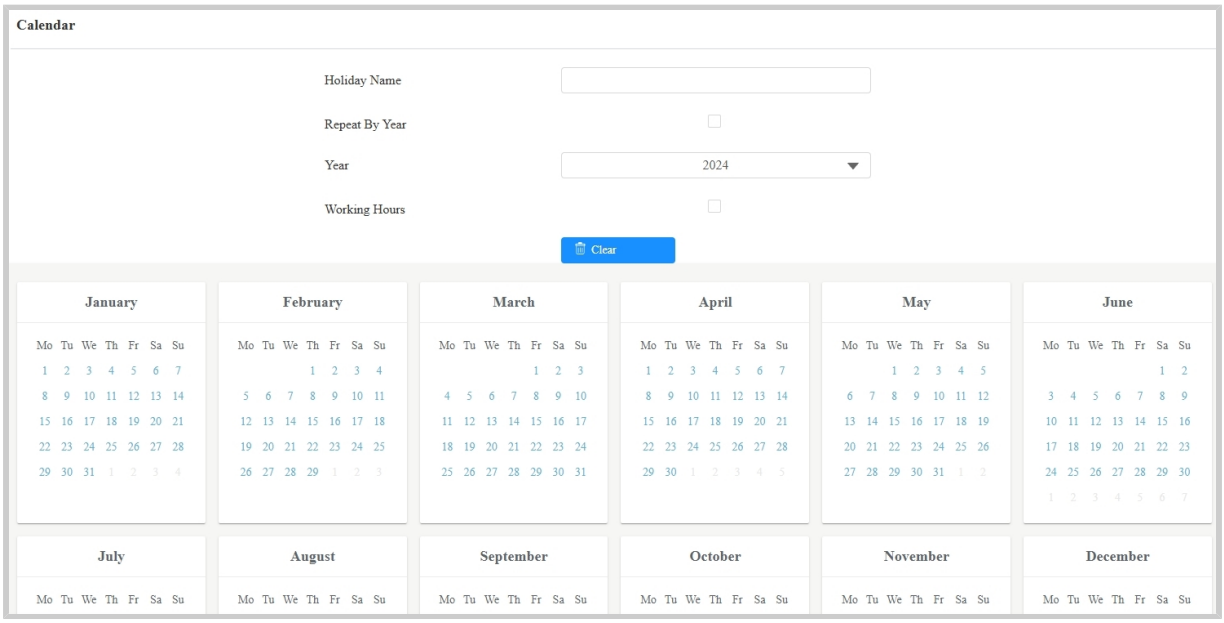
The imported/exported file is in .xml format.

Holiday Schedule

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

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



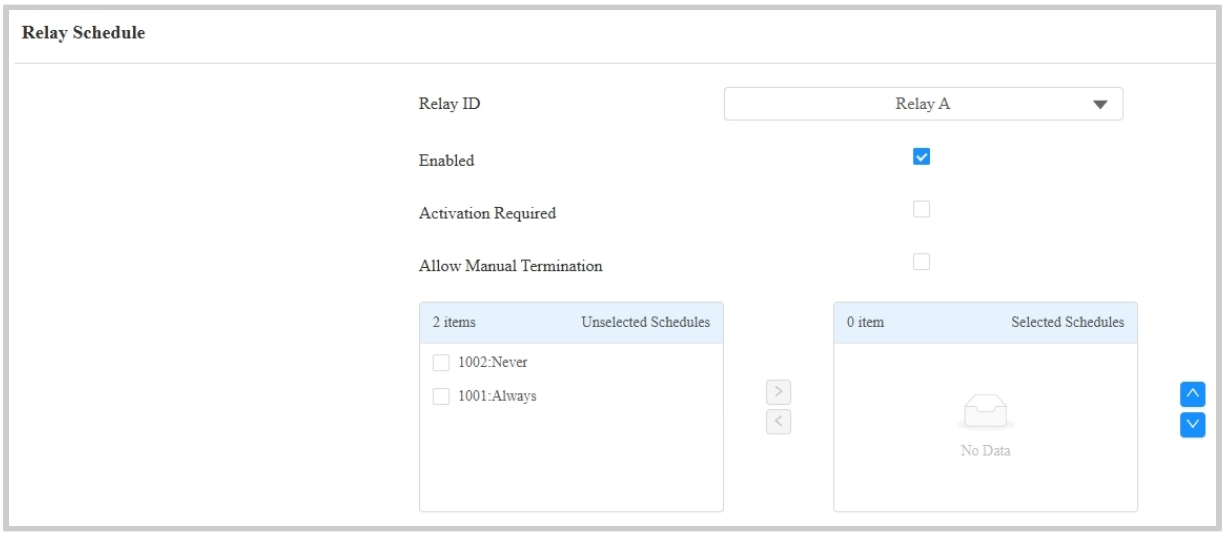


- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

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 it up, go to the **Access Control > Relay > Relay Schedule** interface.



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

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

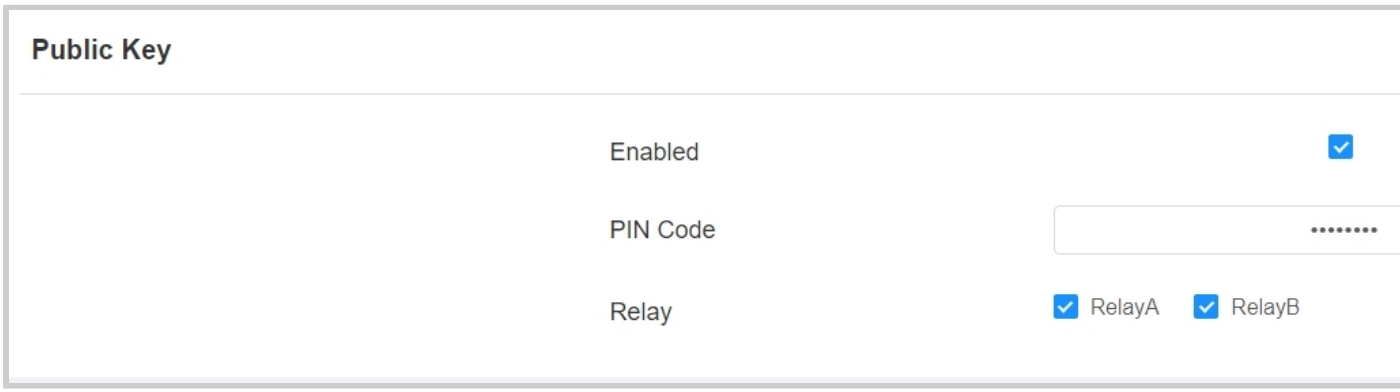
For instructions on creating schedules, kindly consult the Create Door Access Schedule section.

Door Opening Configuration

Unlock by Public PIN

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, go to the web **Access Control > PIN Setting** interface.



- **PIN Code**: Set a 5-8 digit PIN code accessible for universal use. The default is 33333333.
- **Relay**: The relay to be triggered.

> **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 **Directory > 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

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

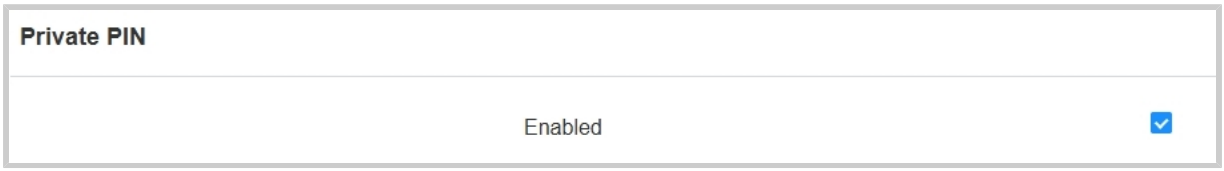


- **Code**: Set a 2-8 digit PIN code solely for the use of this user.

Tip

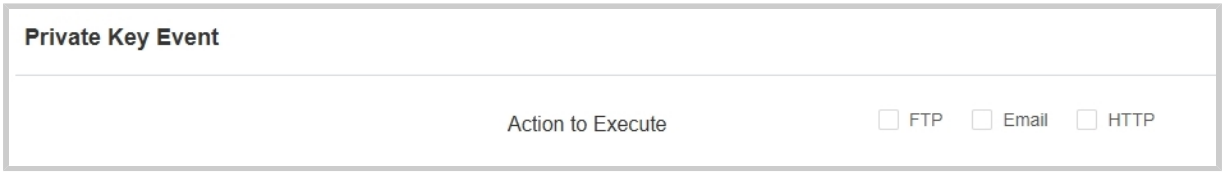
1. You can also modify the Private PIN on the device by pressing "*3888#" on the keypad to enter the Access Method Settings screen.
2. Then, enter the Admin Code "2396" to enter the Private PIN Adding and Deleting screen.

Enable/disable the Private PIN feature on the **Access Control > PIN Setting > Private PIN** interface.



Actions Triggered by Entering Private PINs

You can set actions triggered by entering private PINs on the **Access Control > PIN Setting > Private Key Event** interface.



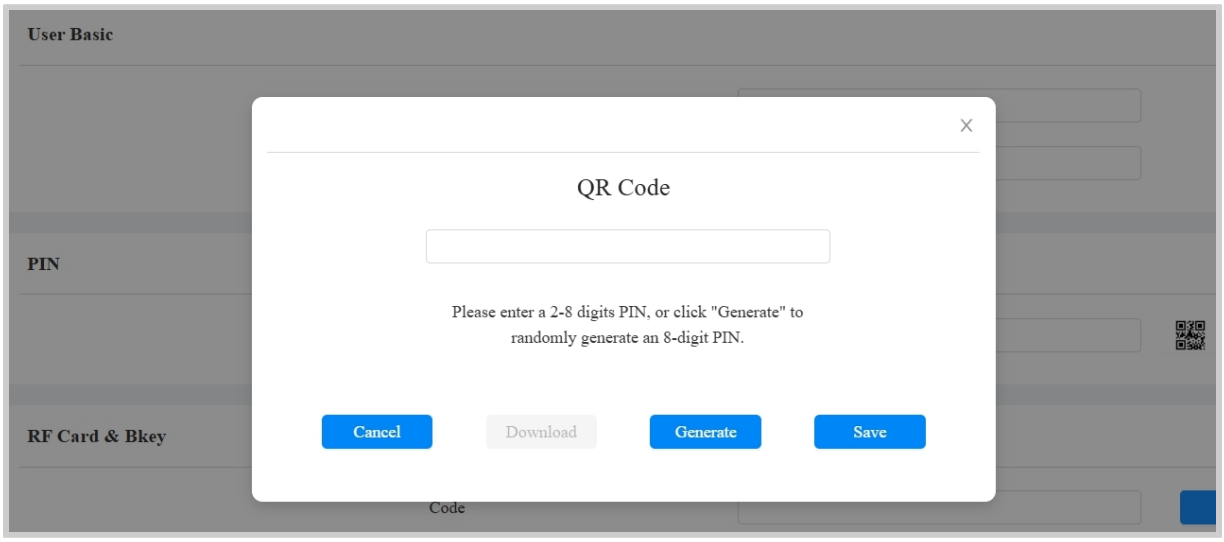
- **Action to Execute**:
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address .
  - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server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

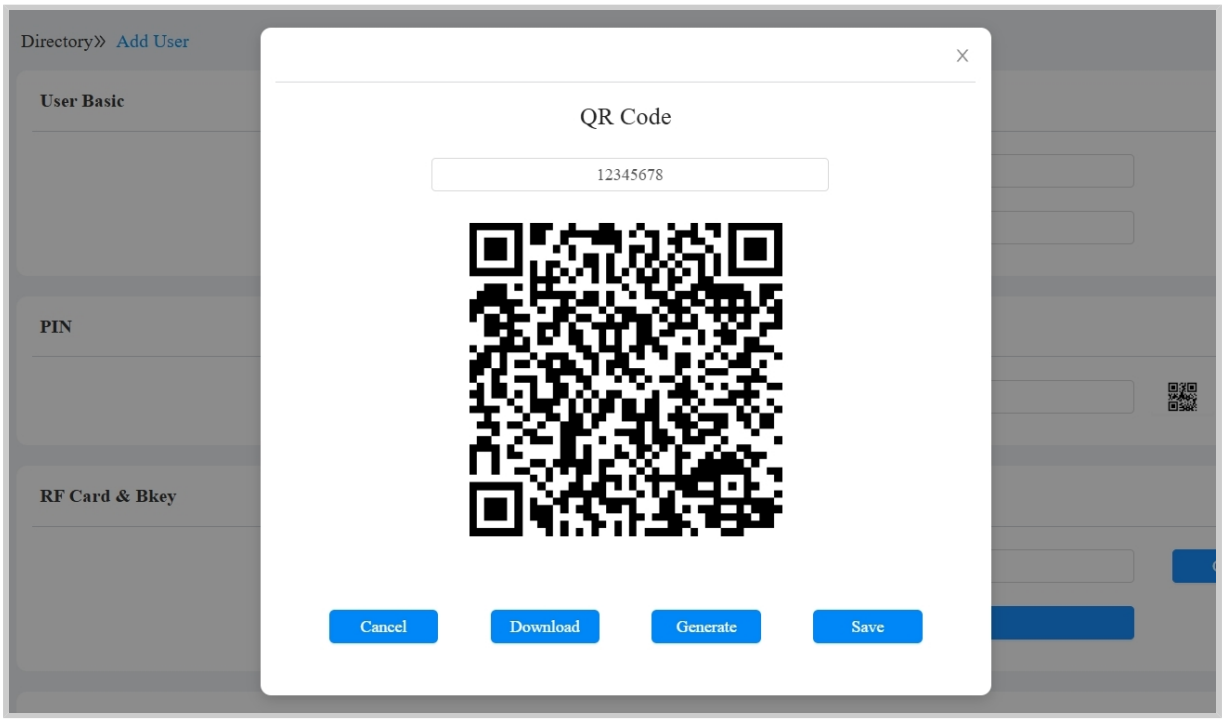
Unlock by QR Code

On the **Directory > User > +Add** interface, scroll to the **PIN** section. Click the QR code icon .



Click **Generate** to generate the QR code with an 8-digit PIN.





- **Cancel**: Click to return to the user editing interface. The QR code and the PIN code will not be saved.
- **Download**: Click to save the QR code to your PC.
- **Generate**: Click to generate another QR code and PIN code.
- **Save**: Click to return to the user editing interface and save the codes.

Unlock by RF Card/Bkey

On the **Directory > User > Add** interface, find the **RF Card & Bkey** part.

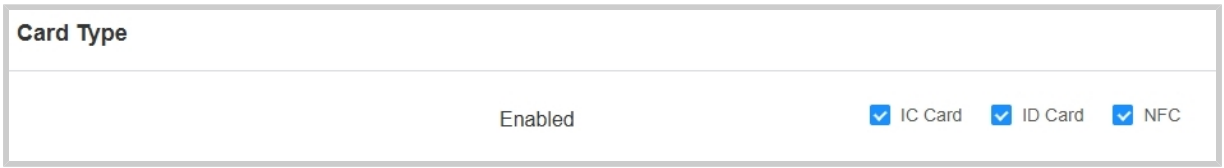


- **Code**: The card code or Bkey code that the device reads.

Note

- Click here to view the detailed steps of configuring Bkey.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device for access.
- Each user can have a maximum of 5 cards added.
- The device allows to add 10,000 users.
- You can also add admin cards on the device. Press *2396#, on the keypad. Then, tap 2 and 1 to enter the card setting screen where you can add or delete an RF card.

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



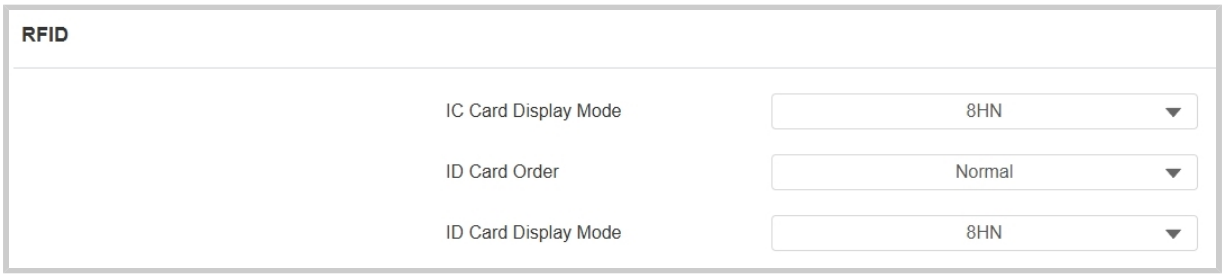
Tip

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.

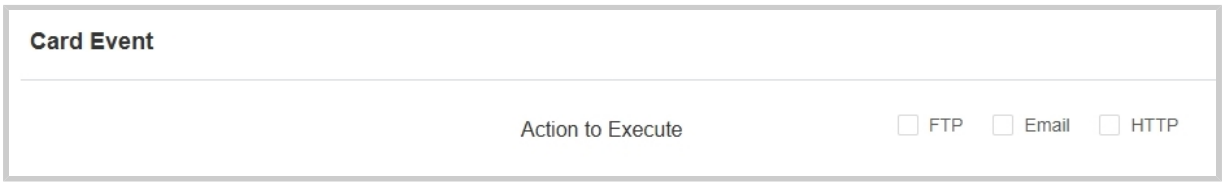
To set it up, go to **Access Control > Card Setting > RFID** interface.



- **IC/ID Card Display Mode**: Select the card number format from the provided options.
- **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 **Access Control > 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 Bluetooth

The device supports opening the door via Bluetooth-enabled My MobileKey or SmartPlus App. Users can either open the door with the apps in their pockets or wave their phones towards the device as they get closer to the door.

> **Note**
>
> Before using Bluetooth to open doors, you need to enable Bluetooth function on the **Access Control > BLE** interface.

Unlock via My MobileKey

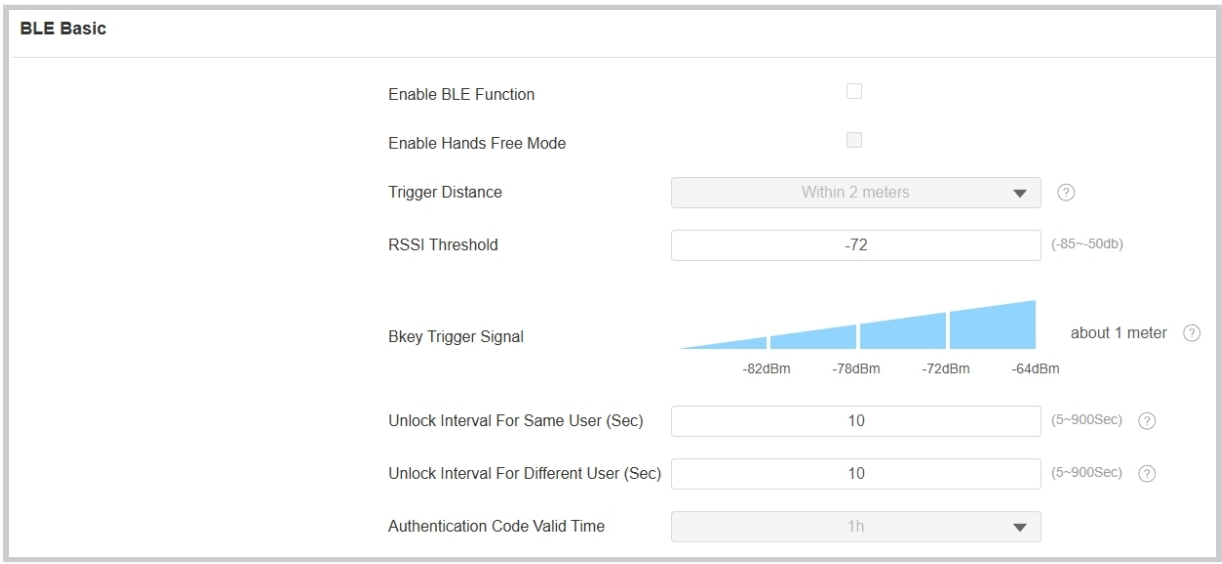
On the **Directory > User > +Add** interface, scroll to the BLE Setting section.



- **Authentication Code**: Click Generate to generate a 6-digit verification code.

Bluetooth Unlock Settings

Set up the Bluetooth-unlock feature on the **Access Control > BLE** interface.



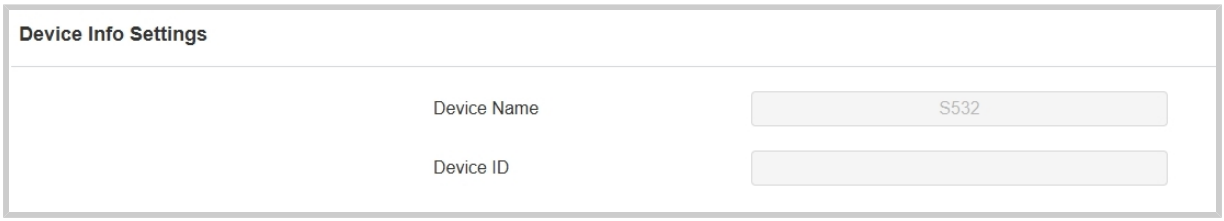
- **Enable Hands Free Mode**: If enabled, users can gain door access hands-free. If disabled, users have to wave their hands near the device to open doors.
- **Trigger Distance**: Set the triggering distance of the Bluetooth for the door access. You select Within 1 Meter, Within 2 Meters, and Within 3 Meters. The trigger distance is 3 meters maximum.
- **RSSI Threshold**: Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Bkey Trigger Signal**: There are four ranges that determine the Bkey trigger distance.
- **Unlock Interval For Same User(Sec)**: Set the time interval between consecutive Bluetooth door access attempts for the same user.
- **Unlock Interval For Different Users(Sec)**: Set the time interval between consecutive Bluetooth door access attempts for different users.
- **Authentication Code Valid Time**: The pairing valid time within which users need to finish the pairing with the My MobileKey App.

> **Note**
>
> To learn about detailed configuration steps of different Bluetooth-based access methods, you can click the following articles.
>
> - Open the Door via Bkey.
> - Unlock by Bluetooth via My MobileKey App.
> - Unlock by Bluetooth via SmartPlus App.

Device Info Settings

You can customize the device name and ID for convenient Bluetooth pairing.

To set it up, go to **Access Control > BLE > Device Info Settings** interface.

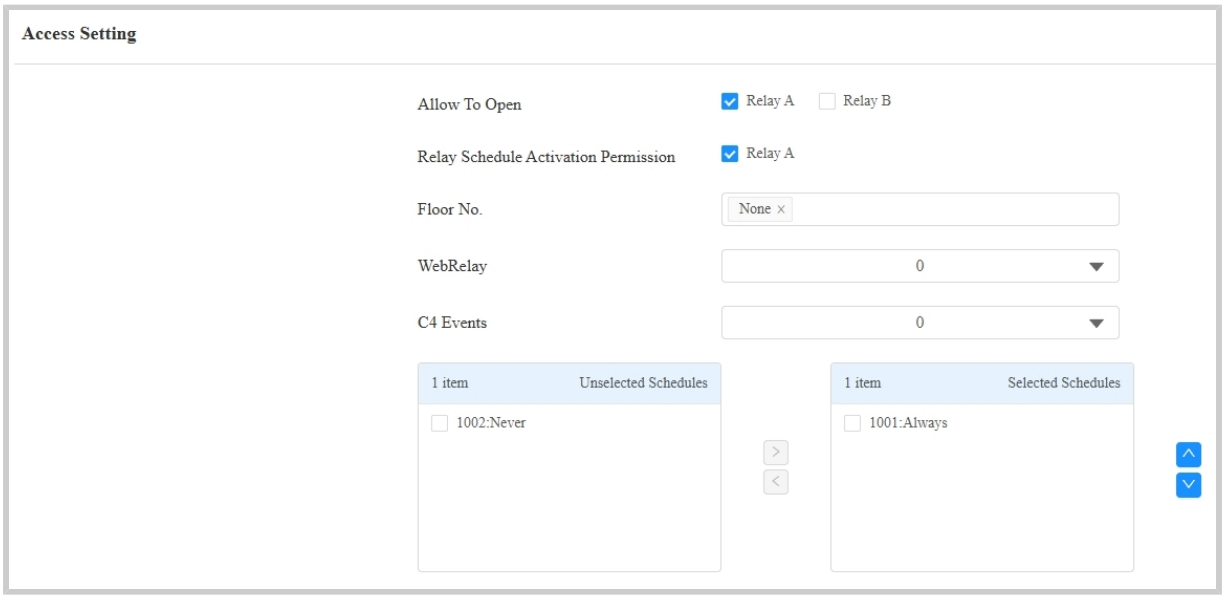


- **Device Name**: Limited to 1-63 numbers or characters.
- **Device ID**: Limited to 1-12 numbers or characters.

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



- **Allow To Open**: 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.
- **Floor NO.**: Specify the accessible floor(s) to the user via the elevator.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **C4 Events**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the right box to the left 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.

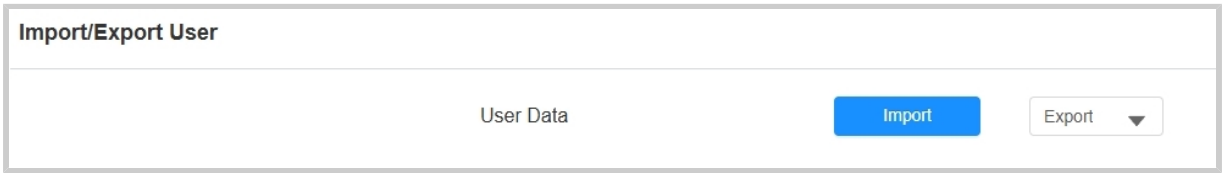
Import/Export User Data

The device supports access control user data to be shared among Akuvox devices through import and export, while you can also export the facial data and then import it to a third-party device.

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

To set it up, go to the **Directory > User > Import/Export User** interface.

The import file should be in XML or TGZ format. The export file is in XML or CSV format.

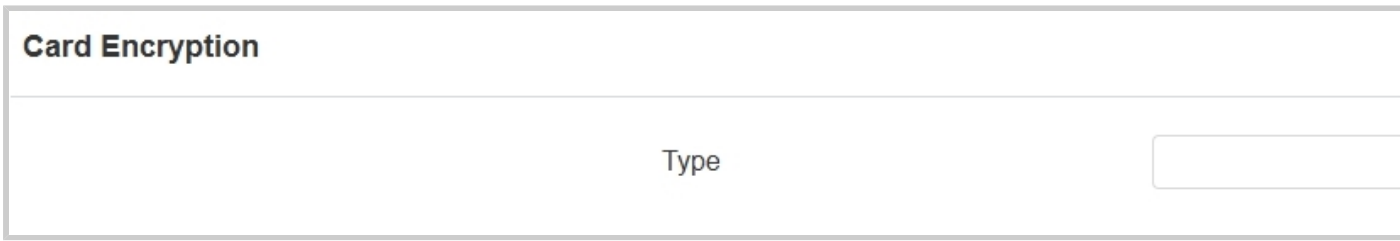


Mifare Card Encryption

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 configure the Mifare card, navigate to the web **Access Control > Card Setting** interface.

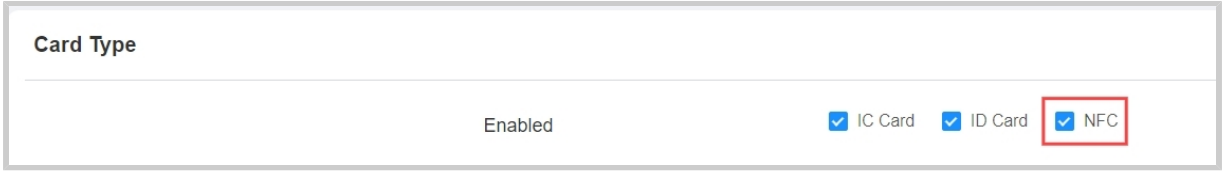


- **Type**: There are four options: **None, Classic, Plus,** and **DESfire**.
- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password 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, either AES or DES.
  - **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.

To configure NFC, navigate to the web **Access Control > Card Setting** interface. Enable the NFC function for door opening.

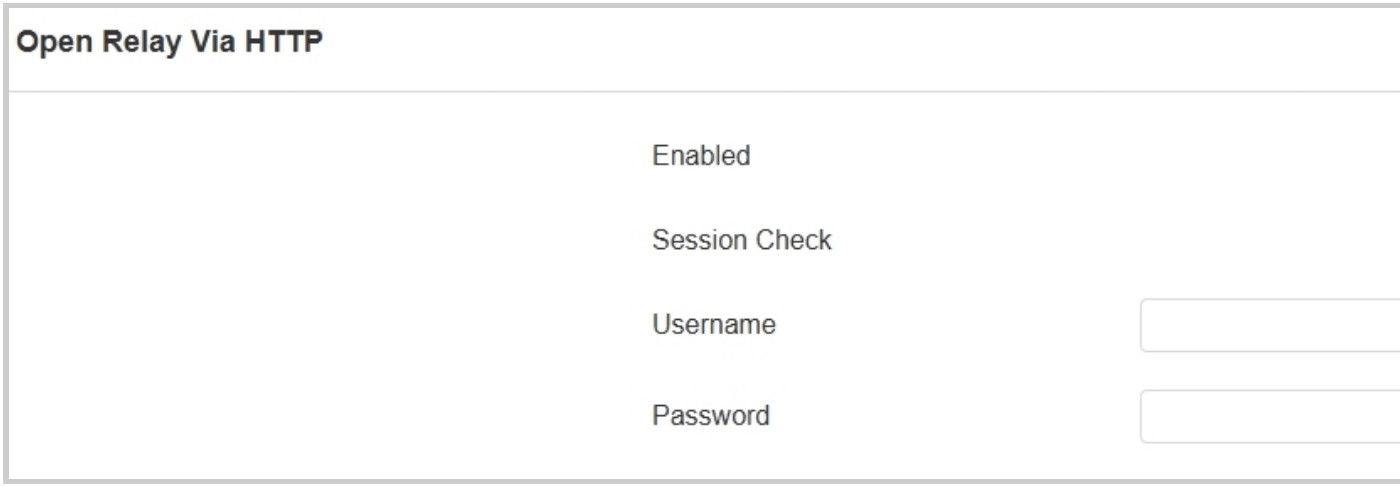


> **Note**
>
> Click here to view the detailed steps of setting up the NFC function.

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 configure it, navigate to the **Access Control > 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:



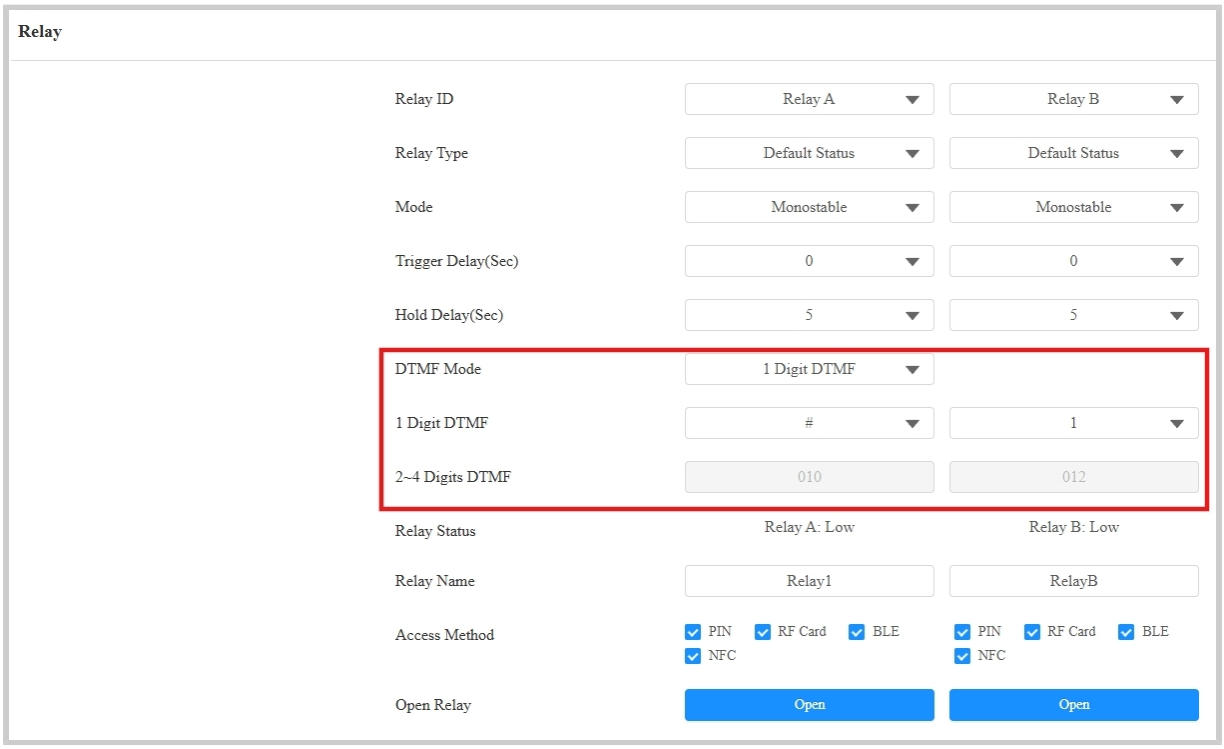
Note

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 **Access Control > Relay** interface.

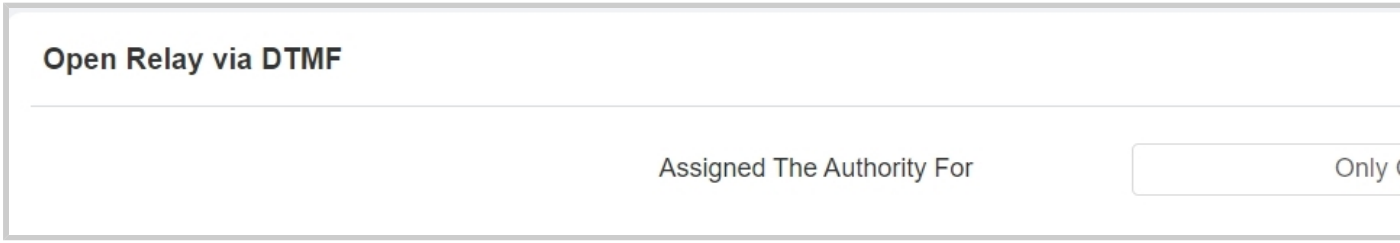


- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range (0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

> **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 Whitelist

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



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

DTMF Data Transmission

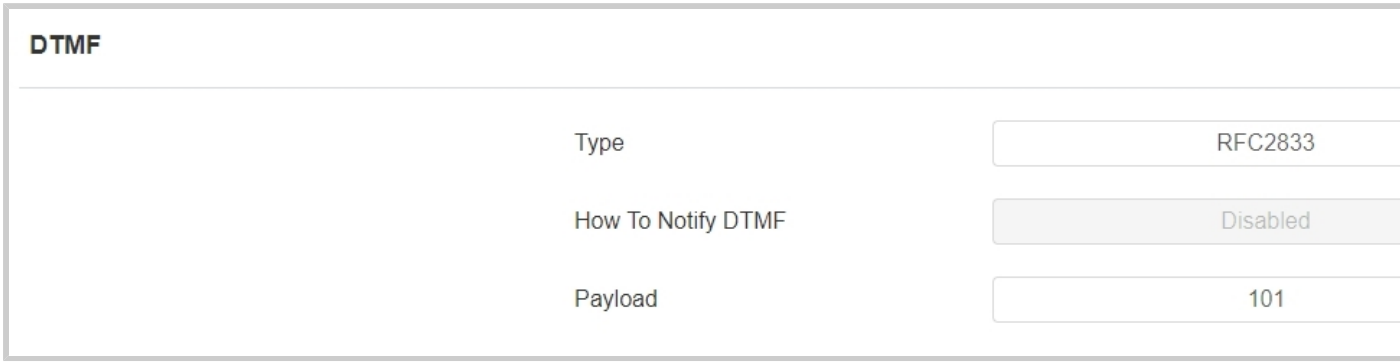
In order to achieve door access via DTMF code or some other applications, you are required to properly configure DTMF in order to establish a DTMF-based data transmission between the device and other intercom devices.

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.

To configure DTMF data transmission, navigate to the web **Account > Advanced > DTMF** interface.

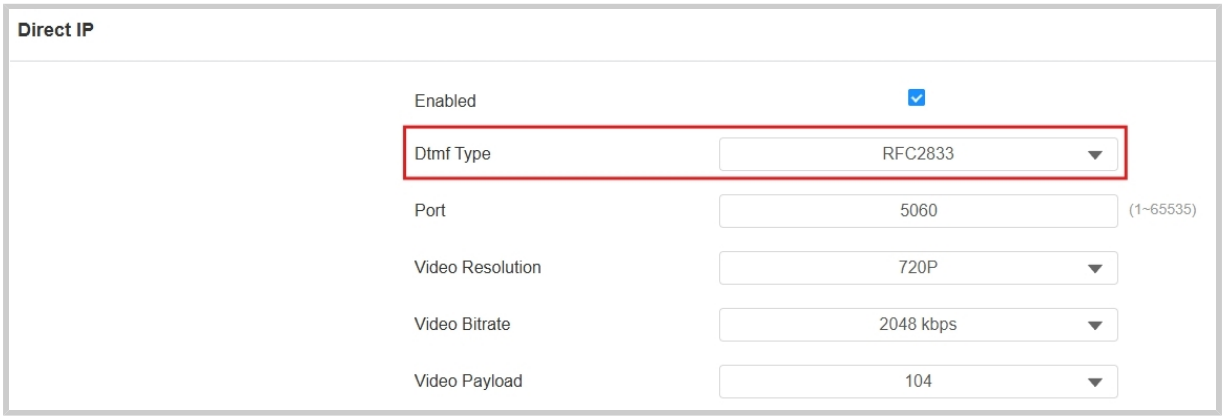


- **Type**: Select from the available options based on the specific DTMF transmission type of the third-party device for receiving signal data.
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, or **Telephone-Event** according to the specific type adopted by the third-party device. You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

DTMF Data Transmission for IP Calls

Select the DTMF data transmission type for IP calls on the **Intercom > Call Feature > Direct IP** interface.

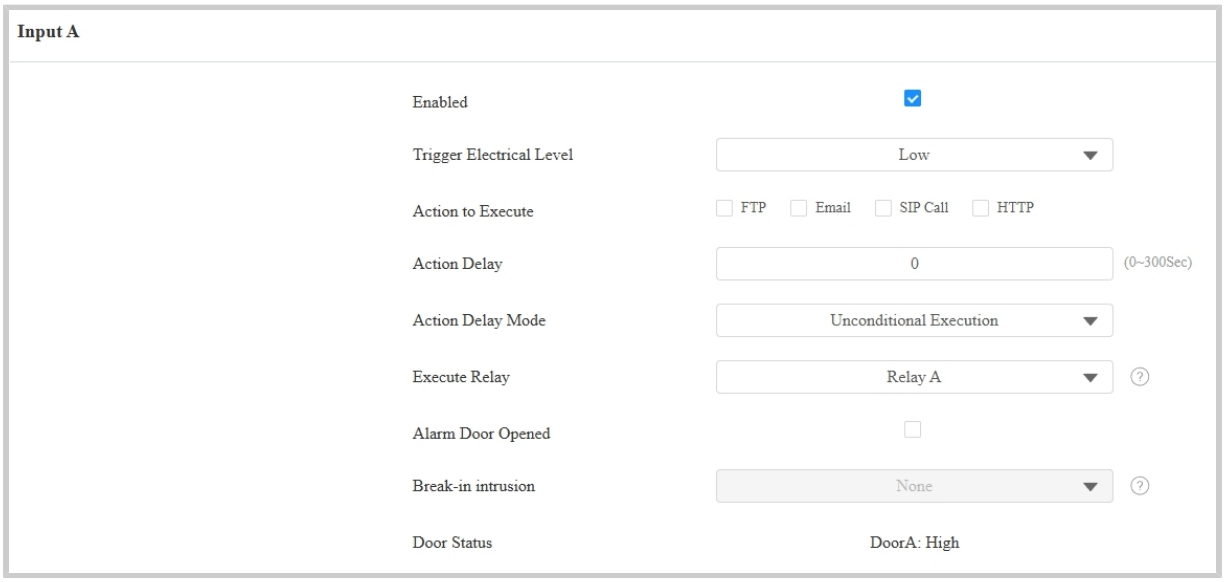


Unlock by Exit Button

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.

Set it up on the web **Access Control > Input** interface.



- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at 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 and enter the URL.
- **HTTP URL**: Enter the HTTP URL if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Delay**: Specify whether the relay can be triggered at any time or only within a scheduled period.
- **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.

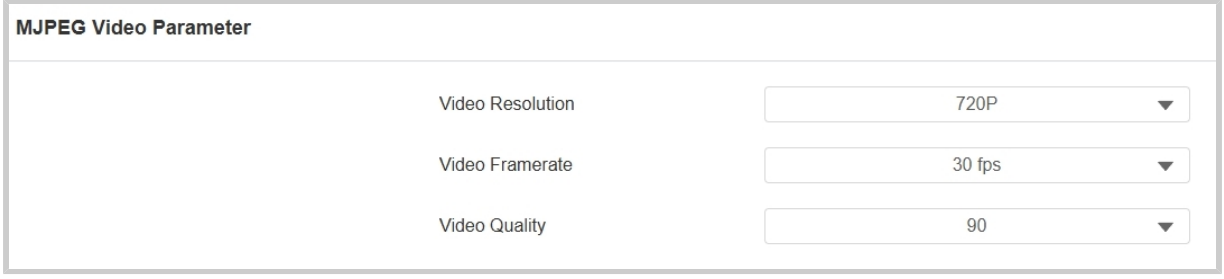
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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

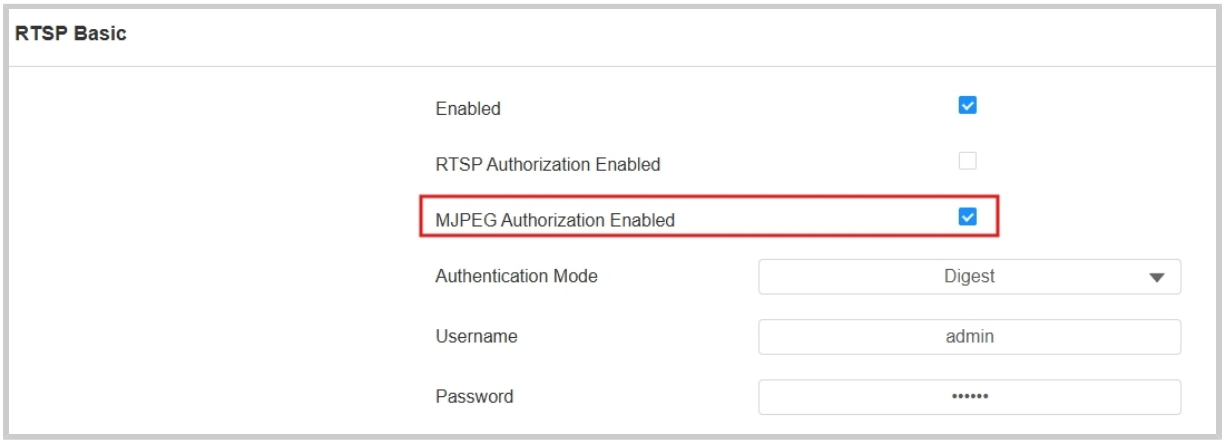


- **Video Resolution**: Specify the video resolution from the lowest QVGA(240×320 pixels) to the highest 1080P(1920×1080 pixels).
- **Video Framerate**: It is 30 fps by default.
- **Video Quality**: It is 90 by default.

MJPEG Authorization

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

To set it up, go to the **Surveillance > 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

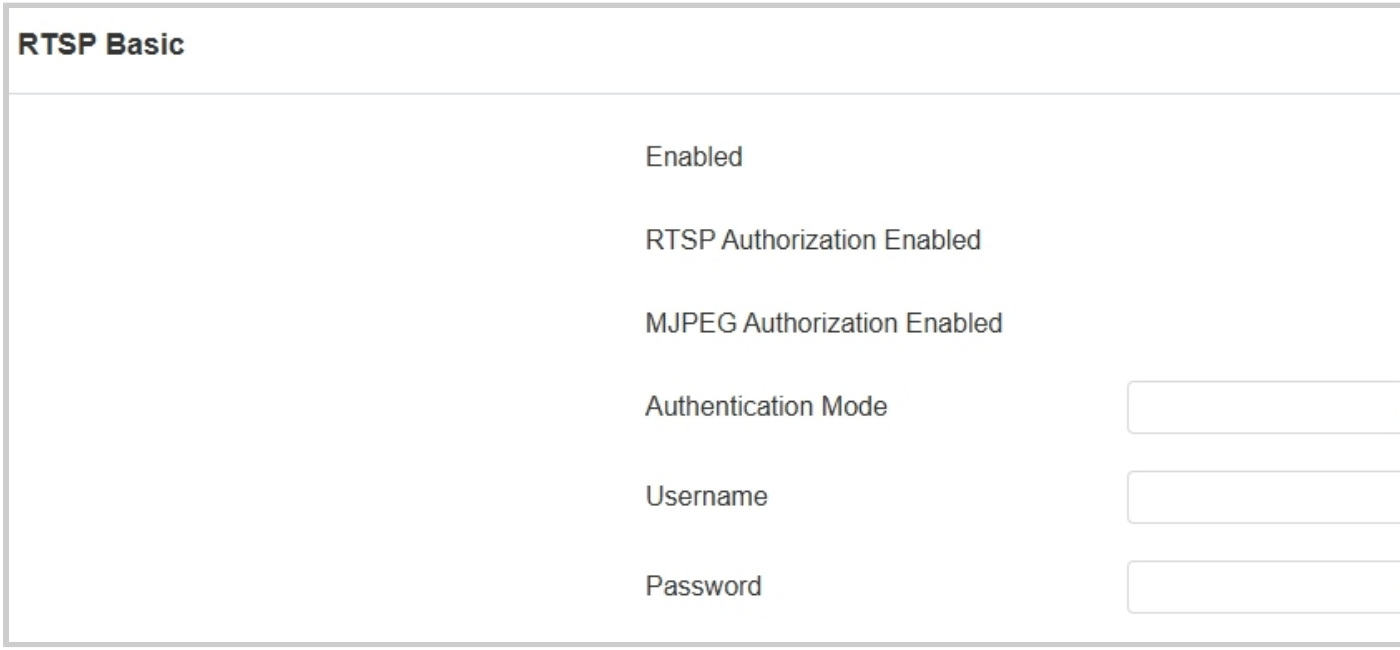
- To view a dynamic stream, use the URL http://device_IP:8080/video.cgi.
- For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi
- For example, if you 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 **Surveillance > RTSP > RTSP Basic** interface.

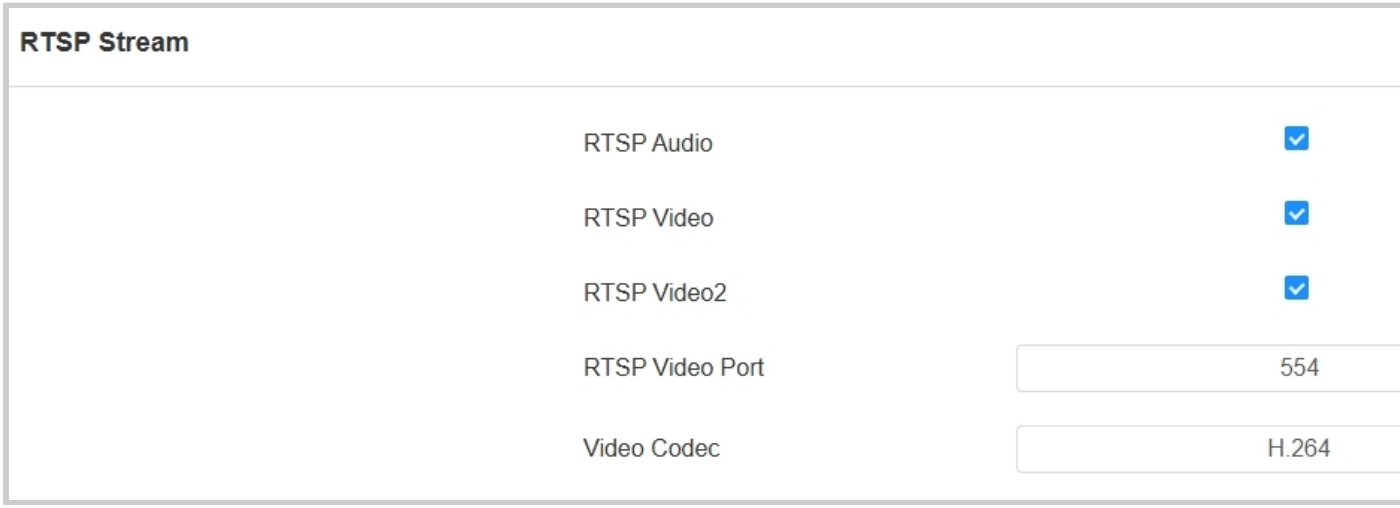


- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: Select between Basic and Digest.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

RTSP Stream Setting

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

To configure the RTSP stream, navigate to the web **Surveillance > RTSP > RTSP Stream** interface.

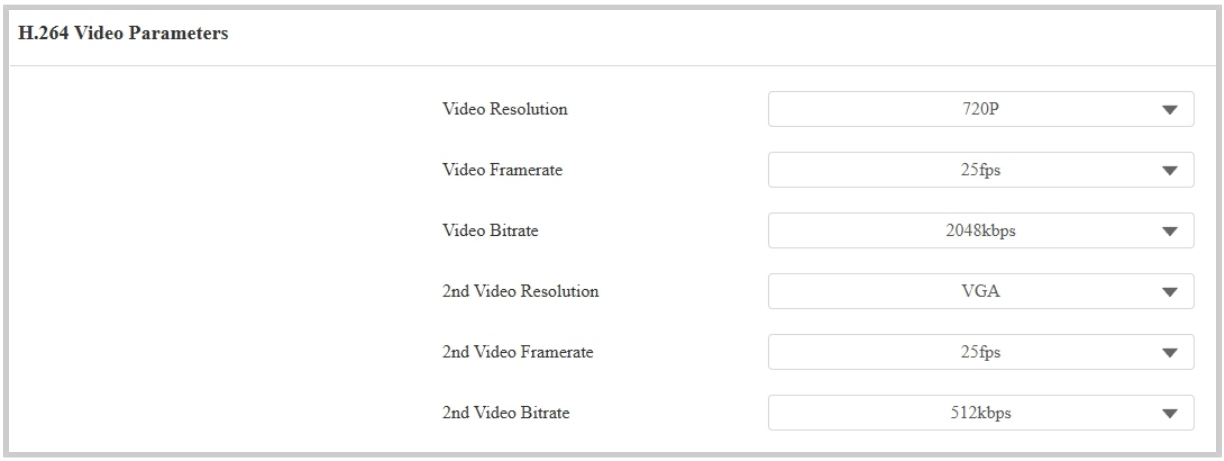


- **RTSP Audio**: Allow the door phone to send audio information to the monitor by RTSP.
- **RTSP Video**: The door phone can send the video information to the monitor. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **RTSP Video 2**: Akuvox door phones support 2 RTSP streams, you can enable the second one.
- **RTSP Video Port**: Specify the video port.
- **Video Codec**: Choose a suitable video codec for RTSP video.

> **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 **Surveillance > RTSP > H.264 Video Parameters** interface.

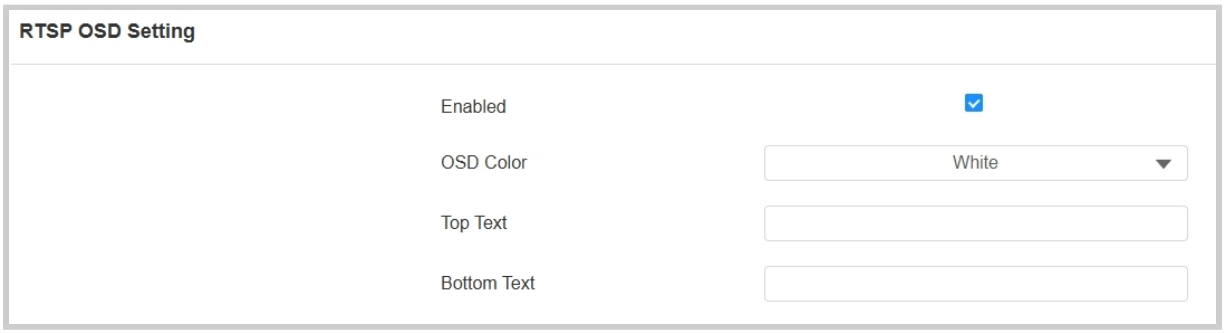


- **Video Resolution**: Specify the image resolution, varying from the lowest QVGA(240×320 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video. The default is 25fps.
- **Video Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048kbps.
- **2nd Video Resolution**: Specify the image resolution for the second video stream channel. The default is VGA.
- **2nd Video Framerate**: Set the frame rate for the second video stream channel. The default is 25fps.
- **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. It is disabled by default.

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



- **OSD Color**: Select the color from White, Black, Red, Green, and Blue.
- **Top/Bottom 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 **Intercom > Call Feature > Others** interface.

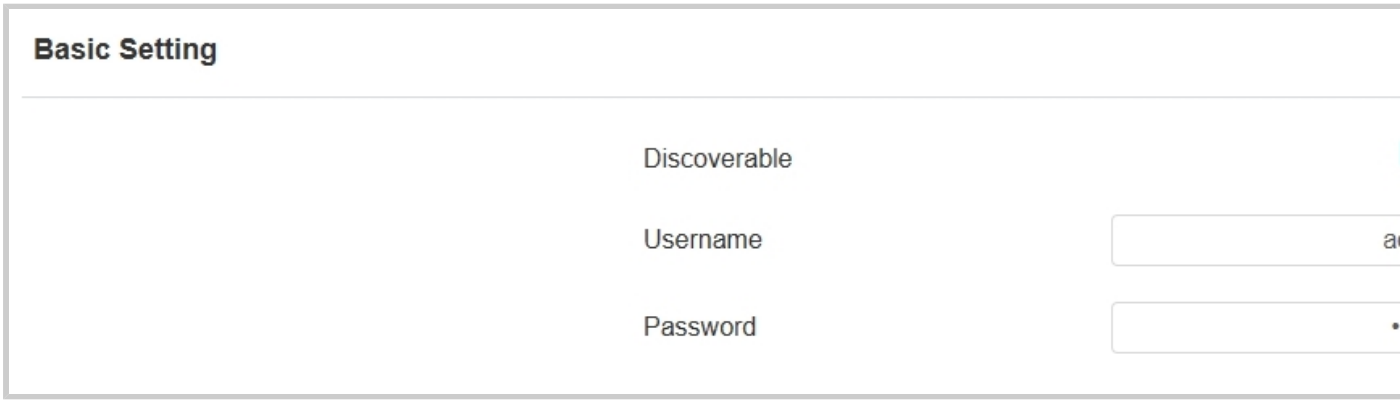


ONVIF

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 web **Surveillance > ONVIF** interface.



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

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

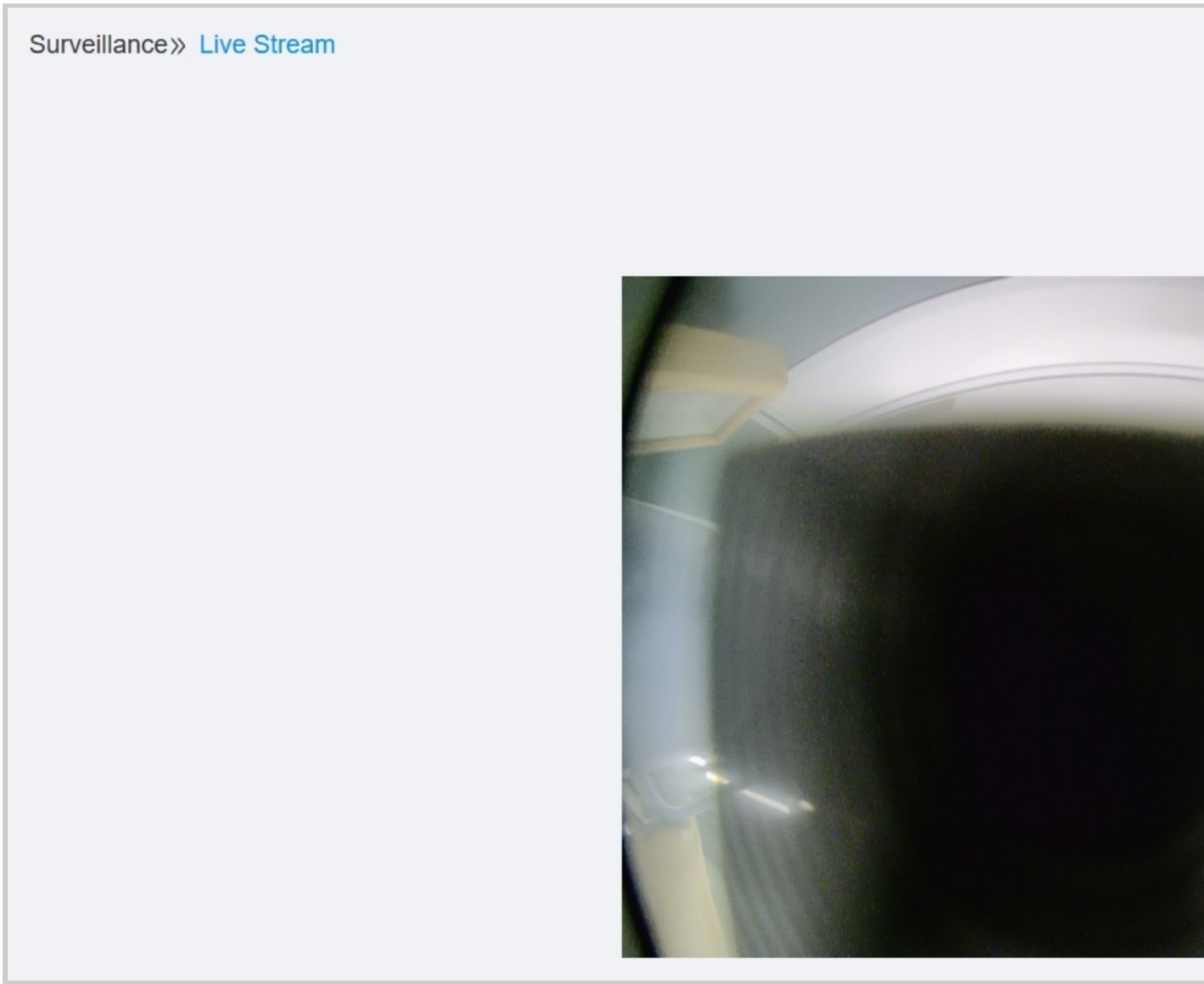
Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.



Live Stream

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

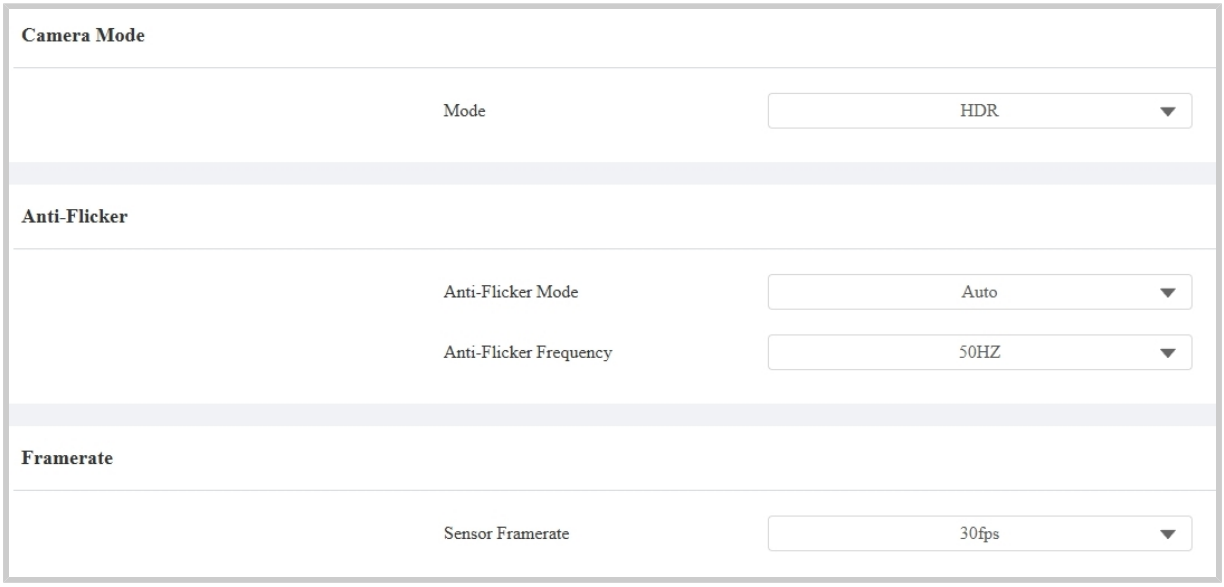
View the video stream on the **Surveillance > Live Stream** interface. If you have enabled RTSP authorization, you need to enter the user name and password set in the RTSP Basic section for viewing the stream.



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 **Device > Camera** interface. It is HDR by default.



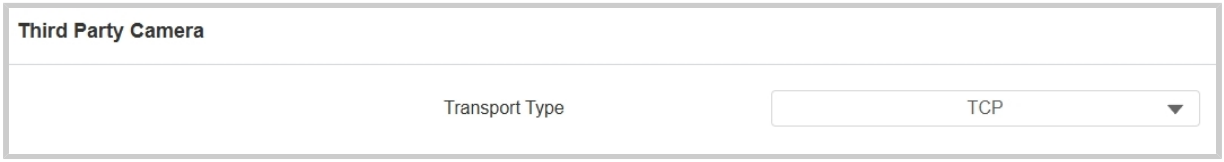
- **Anti-Flicker Mode**: The anti-flicker feature reduces or eliminates flickering in images or videos caused by varying light sources.
  - **Auto**: The device will switch automatically between 50HZ and 60HZ anti-flicker frequency.
  - **Manual**: Select the anti-flicker frequency manually.
  - **Off**: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

- **Sensor Framerate**: Adjust the camera frame rate.
  - **30fps**: Better for applications needing higher smoothness.
  - **25fps**: Suitable for standard video recording and playback, especially under a 50Hz power frequency to minimize flicker.

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 **Surveillance > 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.

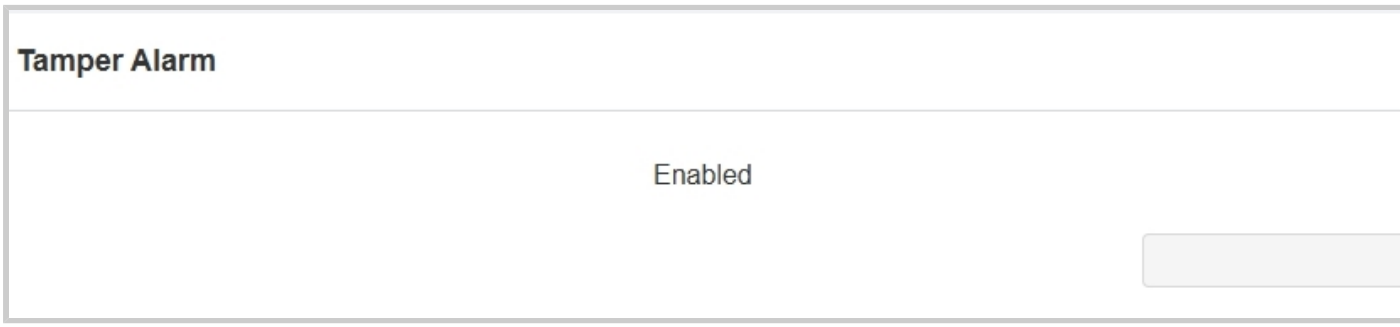
Security

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.

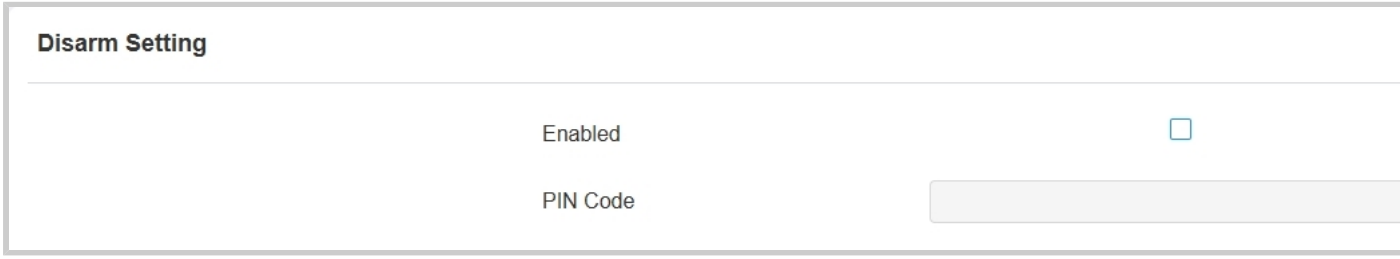
Click here to view which type is supported by the device and learn the function details.

To set it up, go to the web **System > Security > Tamper Alarm** interface. When the alarm is triggered, you can click **Disarm** to clear the alarm.



Disarm Setting

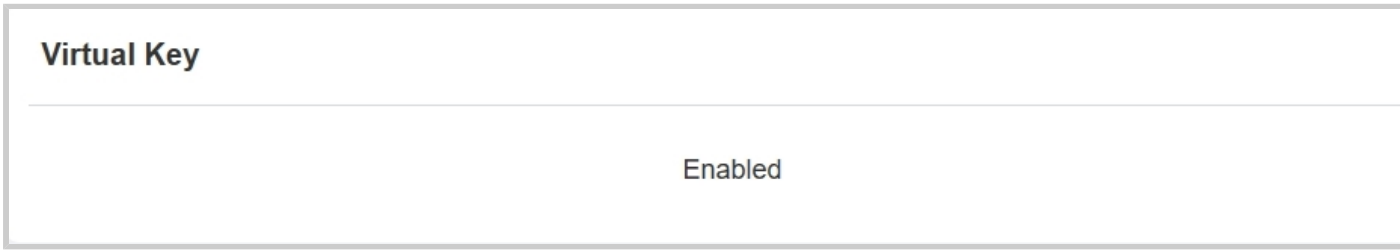
You can set the disarm code on the web **System > Security > Disarm Setting** interface. The default is 0000.



Virtual PIN

The virtual PIN allows you to protect your PIN code from being leaked to someone.

To set it up, go to the web **Access Control > PIN Setting > Virtual PIN** interface.



- **Enabled**: If enabled, you are allowed to put fake numbers on both sides of the PIN code for PIN code protection. For example, if your password is 1234567 you can put 99 and 88 on both sides (99123456788). The virtual password is matched to the users by the number of matched digits. For example, if user A has a greater number of digits that are matched with the virtual password entered than user B, then it will be regarded as user A's password. However, when the double authentication is applied, then the virtual password will be matched with the users who pass the first level of authentication, for example, Face + PIN.

> **Note**
>
> This feature is not used for Public PIN and Apartment+PIN.

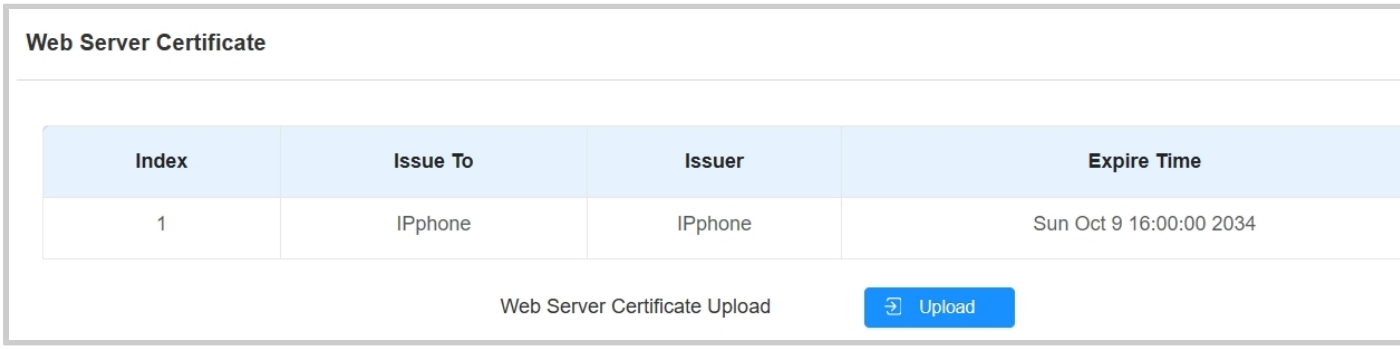
Client Certificate Setting

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.

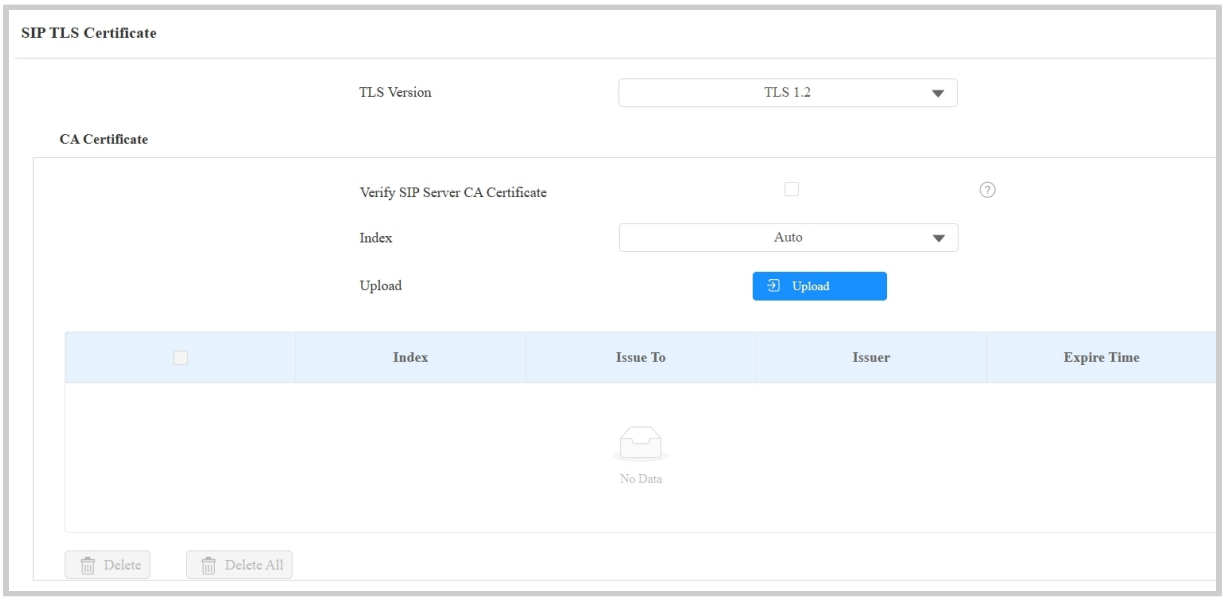
Upload the certificate on the web **System > Certificate** interface.



SIP TLS Certificate

Configure the TLS settings and certificates used for secure SIP communication. You can specify the TLS version, configure server certificate verification, and manage the certificates required for SIP TLS connections.

Upload the certificate on the web **System > Certificate** interface.



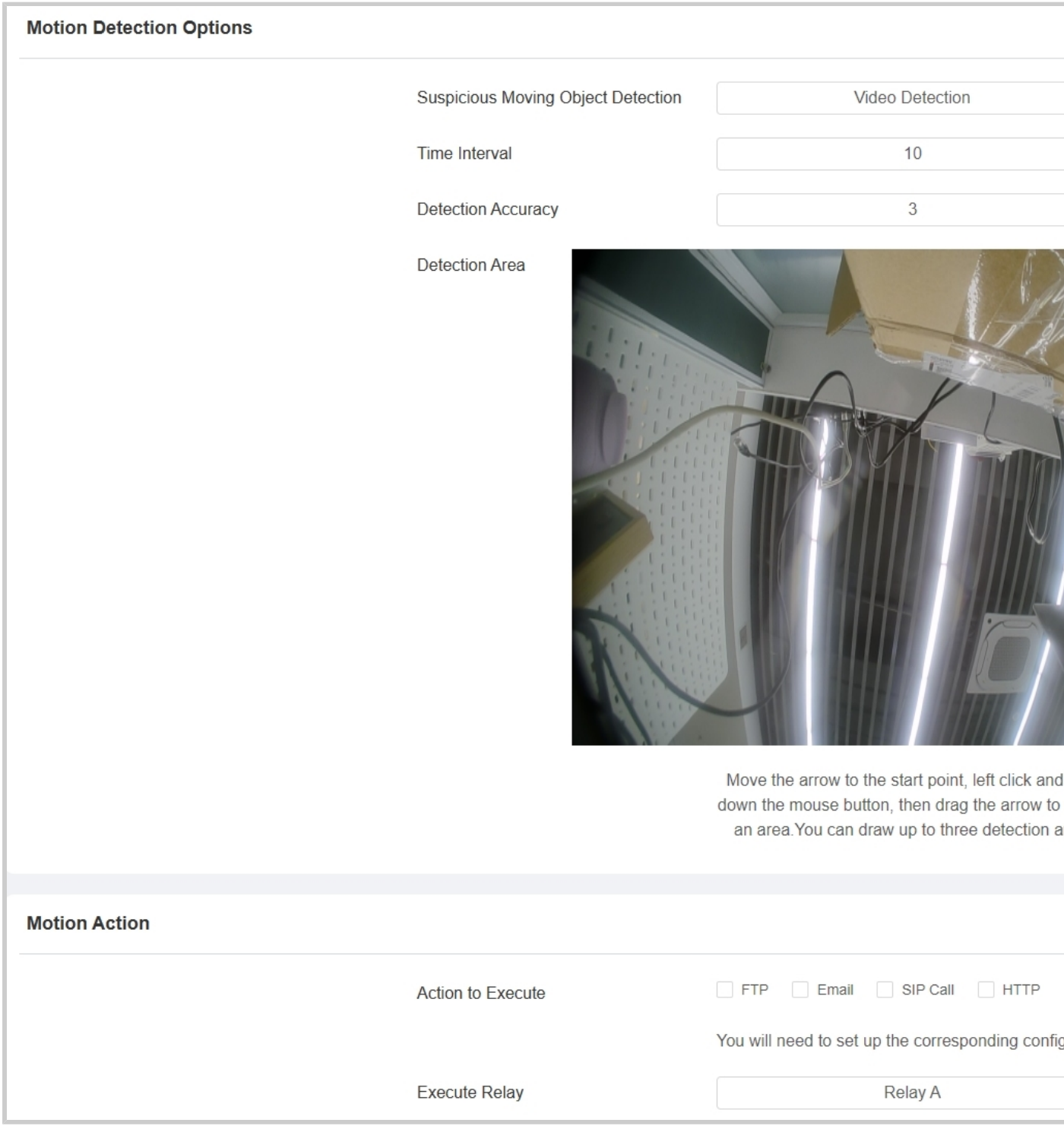


- **TLS Version**: TLS 1.2 provides stronger security with modern encryption algorithms and is recommended for secure communication. TLS 1.0 is an outdated protocol with known vulnerabilities and should be avoided unless required for legacy compatibility.
- **Verify SIP Server CA Certificate**: When enabled, the device verifies the SIP server certificate using the uploaded CA certificate before establishing a TLS connection. The connection will be rejected if the certificate is not trusted.
- **Index**: Select the desired value from the drop-down list of Index. If you select Auto, the uploaded certificate will be displayed in numeric order. If you select a value from 1 to 10, the uploaded certificate will be displayed according to the number.
- **CA Certificate Upload**: Supported formats: .pem, .der, .cer, .crt.
- **Client Certificate Upload**: Supported formats: .pem, .cer, .crt.

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.

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



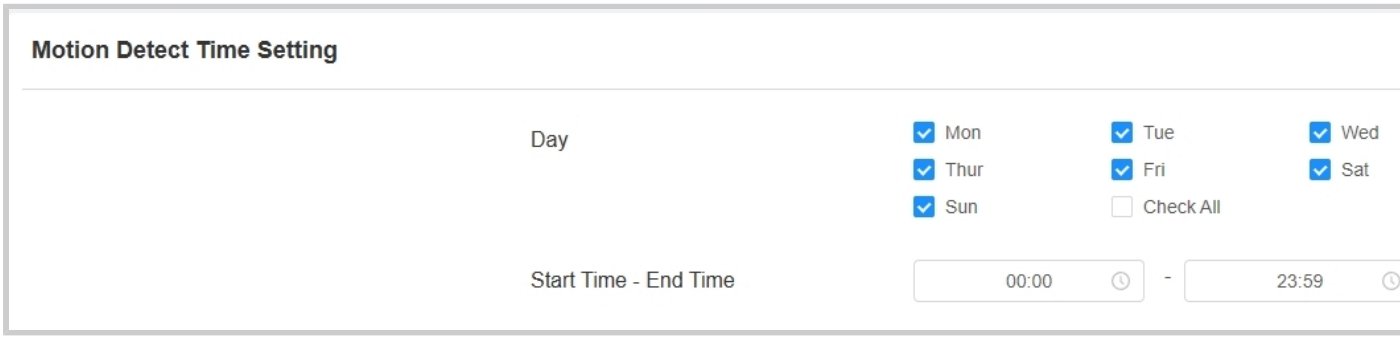
- **Suspicious Moving Object Detection**:
  - **Disabled**: Turn off the motion detection function.

  - **Video Detection**: When the video camera detects moving objects, preset actions will be triggered. Focus on analyzing visual information captured through cameras.
  - **Radar Detection** When the radar detects moving objects, preset actions will be triggered. It offers longer-range and better detection in poor visibility conditions.
  - Video + Radar: Detect motion with the combination of video camera and radar.
- **Detection Range**: After enabling radar detection, you can select the detection range among 1, 2, and 3 meters.
- **Time Interval**: Determine how to delay and trigger motion detection.
  - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.
  - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
  - The default interval is 10 seconds.
- **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.
- **Detection Area**: Click and hold down the mouse button to select up to three detection areas.
- **Action to Execute**: The notification type includes FTP, Email, SIP Call, and HTTP.
  - FTP: The notification will be sent to the designated FTP server.
  - Email: The email will be sent to the pre-configured email address.
  - SIP Call: A call will be made to the pre-configured number .
  - HTTP: The notification will be sent to the designated server.
    - HTTP URL: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Execute Relay**: The relay to be triggered.

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 **Surveillance > 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.

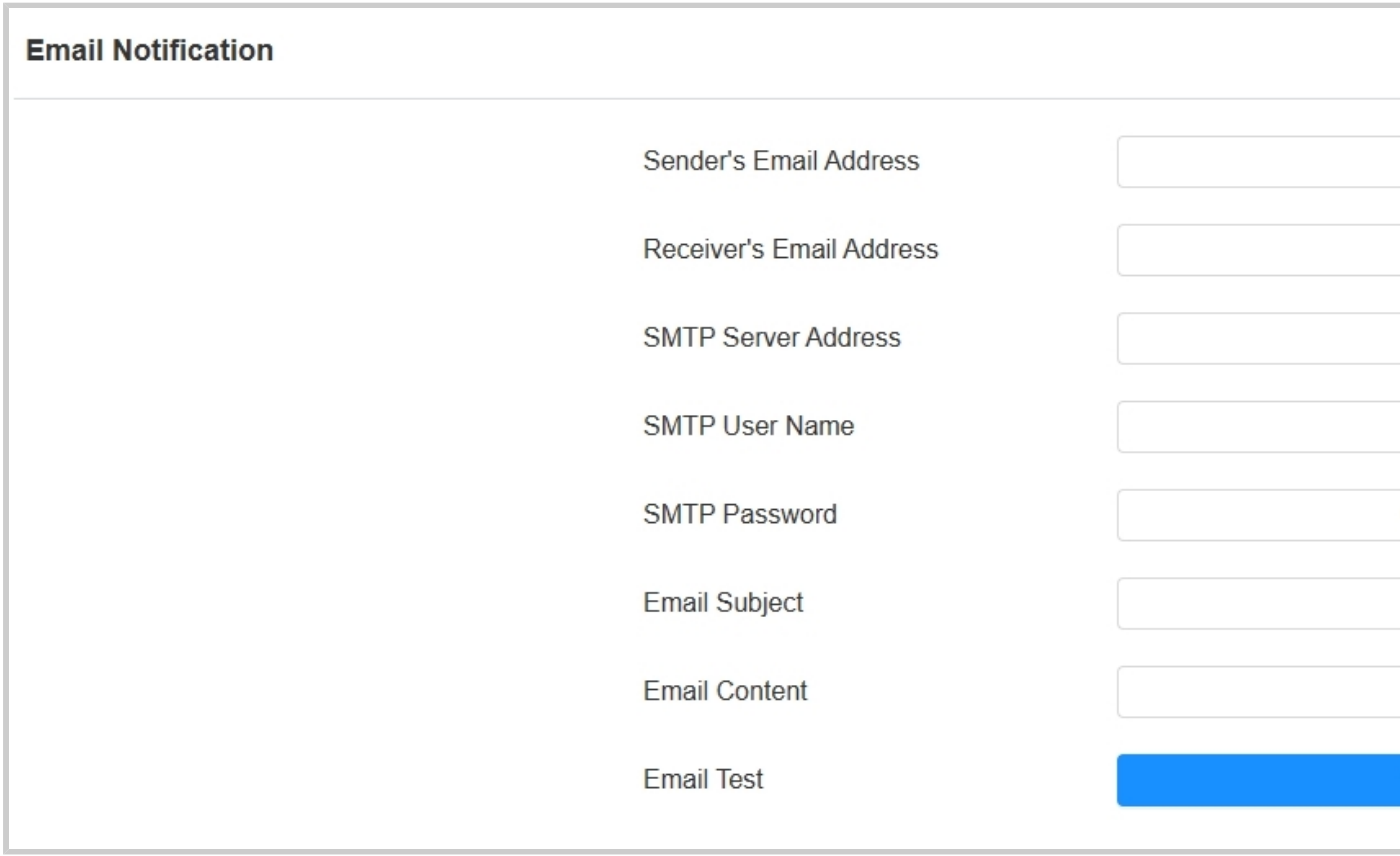
To set up security notifications, go to **Setting > Action** interface.

Email Notification

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

Click here to view how to set this feature up.

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



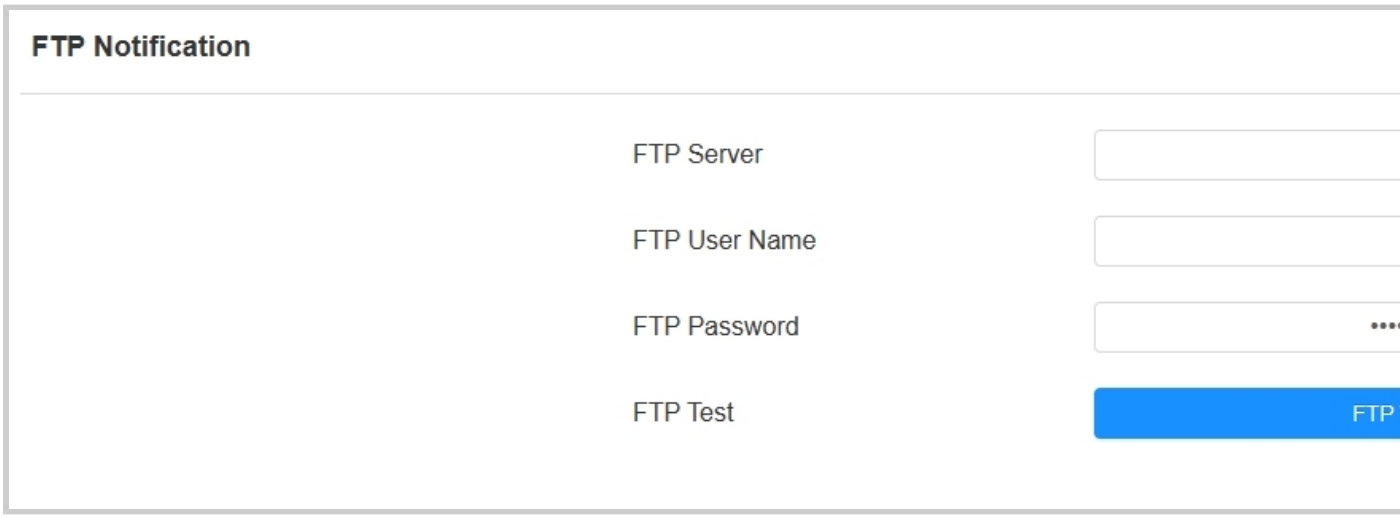
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

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.

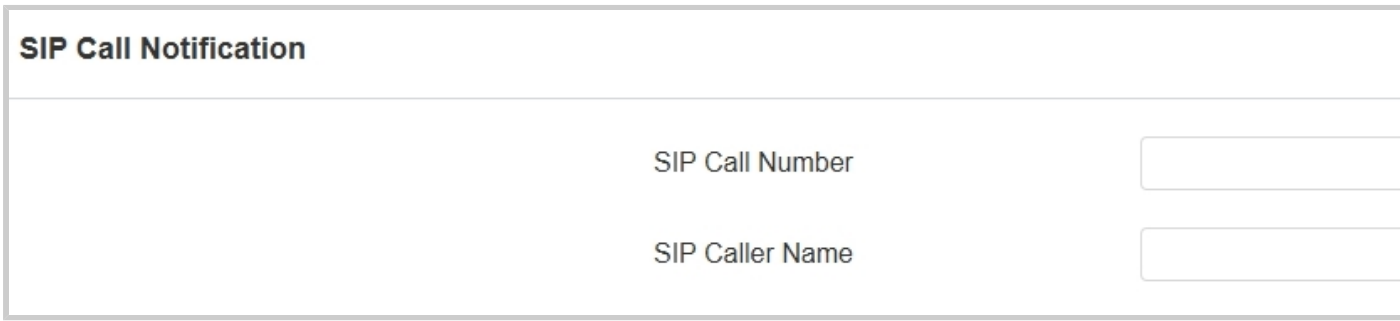


- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

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
1	Make Call	$remote
2	Hang Up	$remote
3	Relay Triggered	$relay1status
4	Relay Closed	$relay1status
5	Input Triggered	$input1status
6	Input Closed	$input1status
7	Valid Code Entered	$code
8	Invalid Code Entered	$code
9	Valid Card Entered	$card_sn
10	Invalid Card Entered	$card_sn

Example
Http://server ip/Callnumber=$remote
Http://server ip/Callnumber=$remote
Http://server ip/relaytrigger=$relay1status

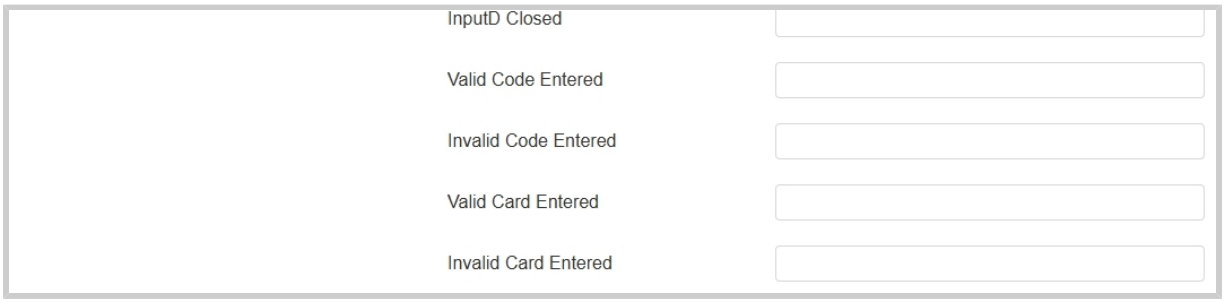
Http://server ip/relayclose=$relay1status
Http://server ip/inputtrigger=$input1status
Http://server ip/inputclose=$input1status
Http://server ip/validcode=$code
Http://server ip/invalidcode=$code
Http://server ip/validcard=$card_sn
Http://server ip/invalidcard=$card_sn

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

Set up the action URL on the **Setting > Action URL** interface.

Action URL

Enabled	
Authorization Mode	
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayA Closed	
RelayB Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	
InputD Triggered	
InputA Closed	
InputB Closed	
InputC Closed	

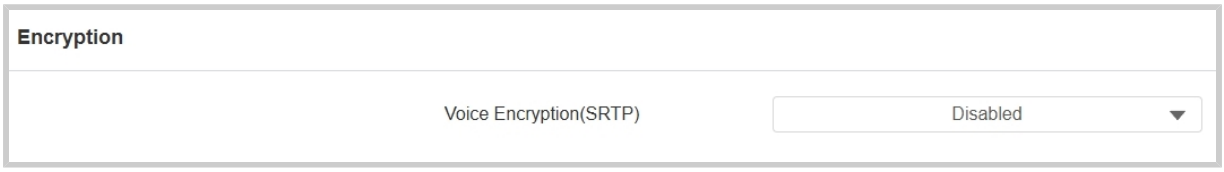


- **Authorization Mode**: Select the authorization mode. If Digest is selected, you can set up the username and password for authentication.

Voice Encryption

The encryption function provides three encryption methods to protect voice signals from eavesdropping during a call.

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



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

User Agent

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

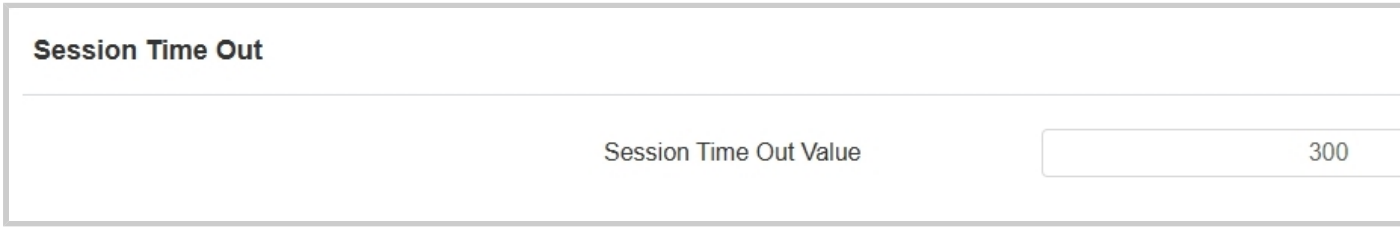
To set it up, go to the **Account > Advanced > User Agent** interface.



Web Interface Automatic Log-out

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

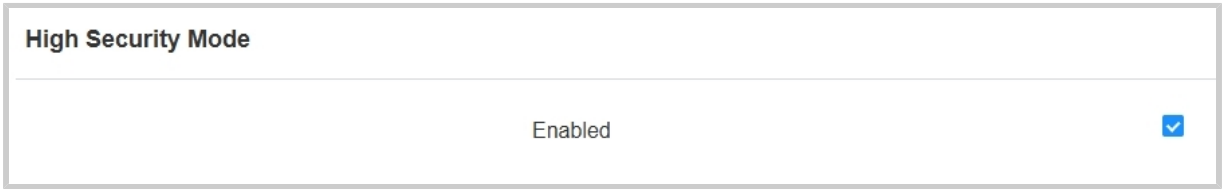
To set it up, go to the **System > Security > Session Time Out** interface.



High Security Mode

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

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



Important Notes

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

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

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

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

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

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

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

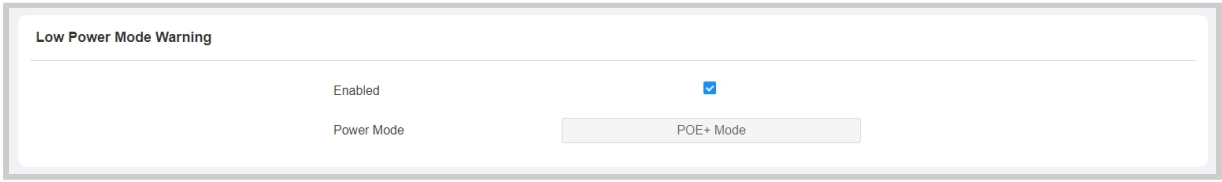
- http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

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

Low Power Mode

It displays the device's power mode. When the device is powered by POE, it displays POE+Mode. When it is powered by the 12-volt power supply, it displays Low Power Mode.

See the power mode on the **System > Security > Low Power Mode Warning** interface.

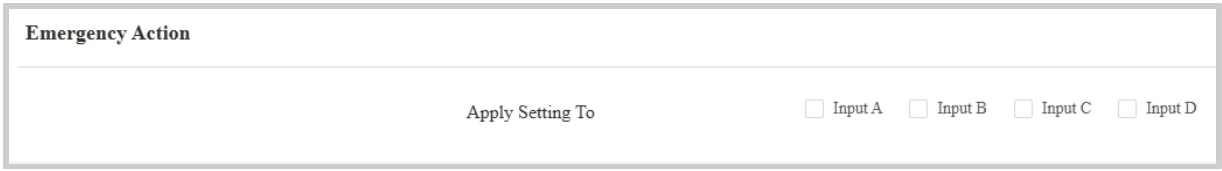


Emergency Action

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 **System > Security > Emergency Action** interface.



Real-time Monitoring

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

Click here to see the detailed configuration.

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



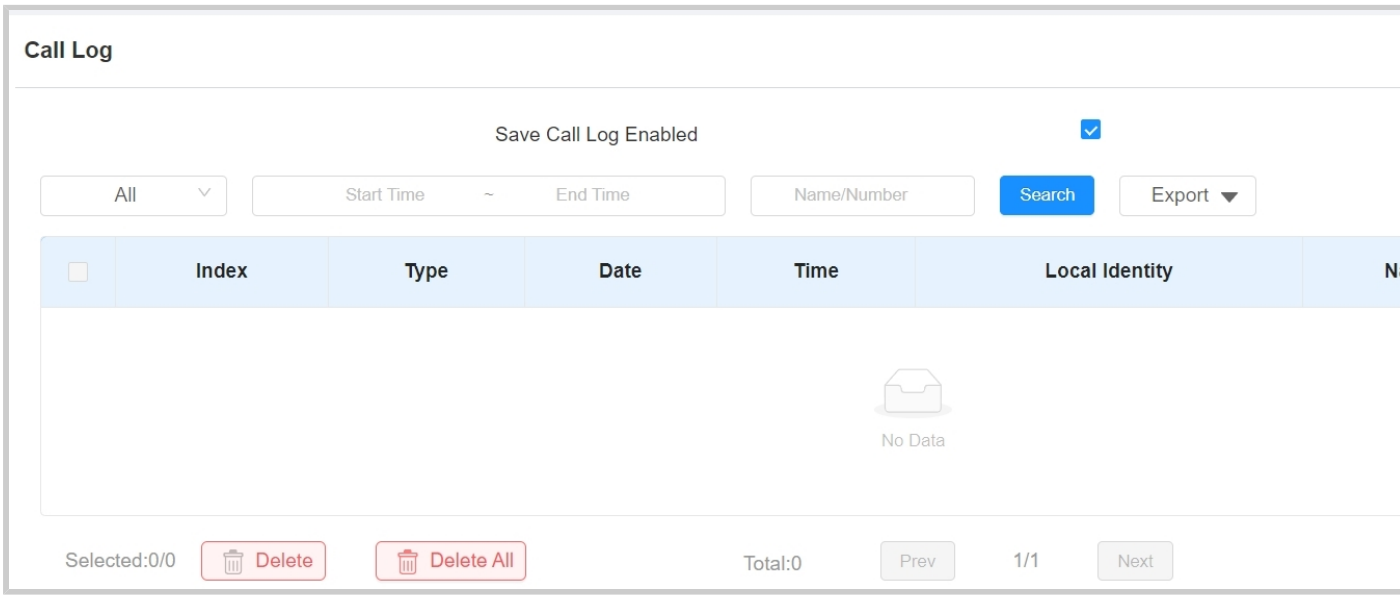
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering input.
  - **Relay**: The door is opened by triggering the relay.

Logs

Call Logs

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

Check call logs on the web **Status > Call Log** interface. The device can store 1,000 call logs.

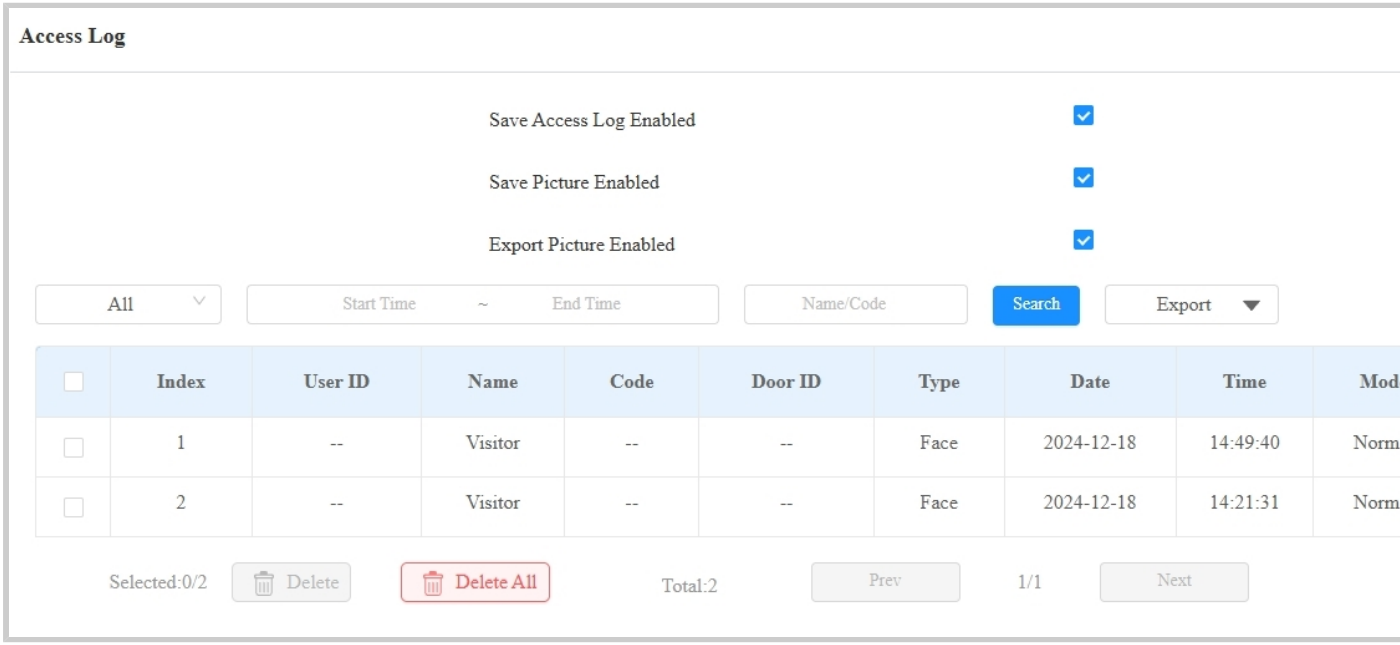


- **All**: Four types of call history are available: All, Dialed, Received, and Missed.
- **Start Time-End Time**: The specific time of the call logs you want to search, check, or export.
- **Name/Number**: Search the call log by the name or by the SIP or IP number.
- **Export**: Call logs can be exported in .csv format.

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 web **Status > Access Log** interface. The device can store 5,000 door logs.

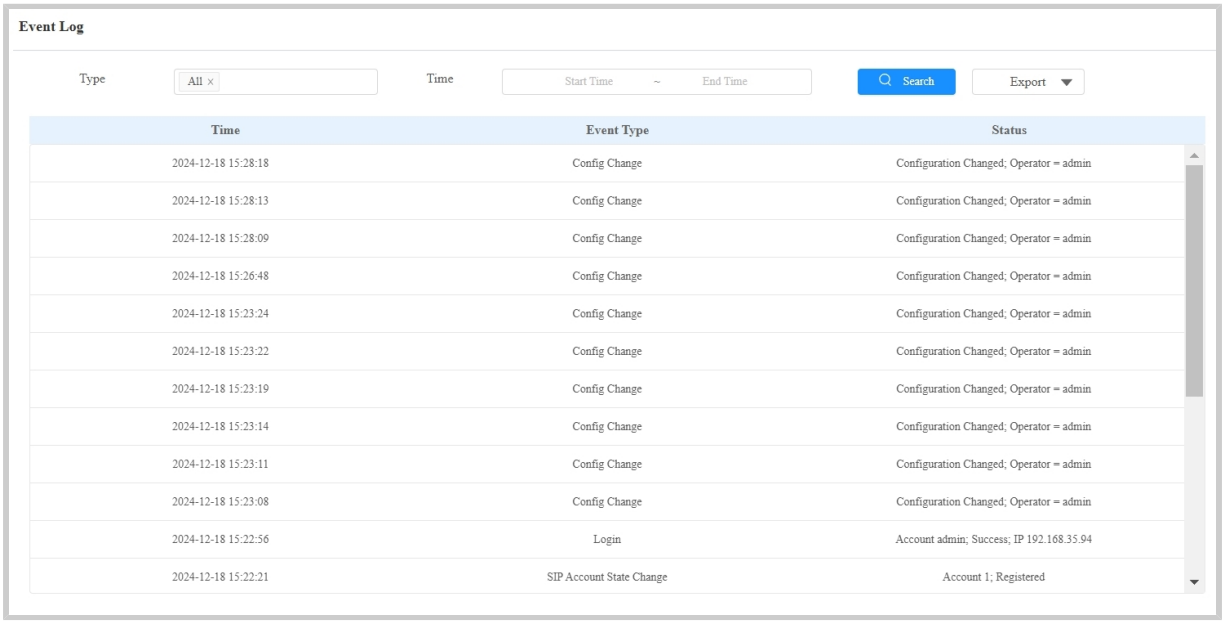


- **Save Picture Enabled**: When enabled, the device will capture pictures of the door opening and you can click **Picture** in the Action column to view the screenshot.
- **Export Picture Enabled**: Set whether to export the captured images when exporting the door logs.
- **All**: Three types of access logs are available, All, Success, and Failed.
- **Start Time-End Time**: The specific time of the call logs you want to search, check, or export.
- **Name/Code**: Search the door log by the name or by the PIN code.
- **Export**: Door logs can be exported in .csv or .xml format.
- **Picture**: Click to view the captured image.

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 **Status > Event Log** interface. The device supports up to 100,000 logs, which can be exported in CSV format.



Integration with Third-Party Device

Integration via Wiegand

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

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



- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device. It is automatically configured.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender and can directly output the data, such as the card code.
  - **Convert To Card No. Output**: The device serves as a sender and cannot directly output the data, such as the face data.
- **Wiegand Input Clear Time**: When the interval of entering passwords exceeds the time. All entered passwords will be cleared.
- **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 the 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 Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **RF Card Verification**: When enabled, the device will verify whether the card is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the door phone screen, but the door can still be opened. 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 see detailed configuration steps.

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

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

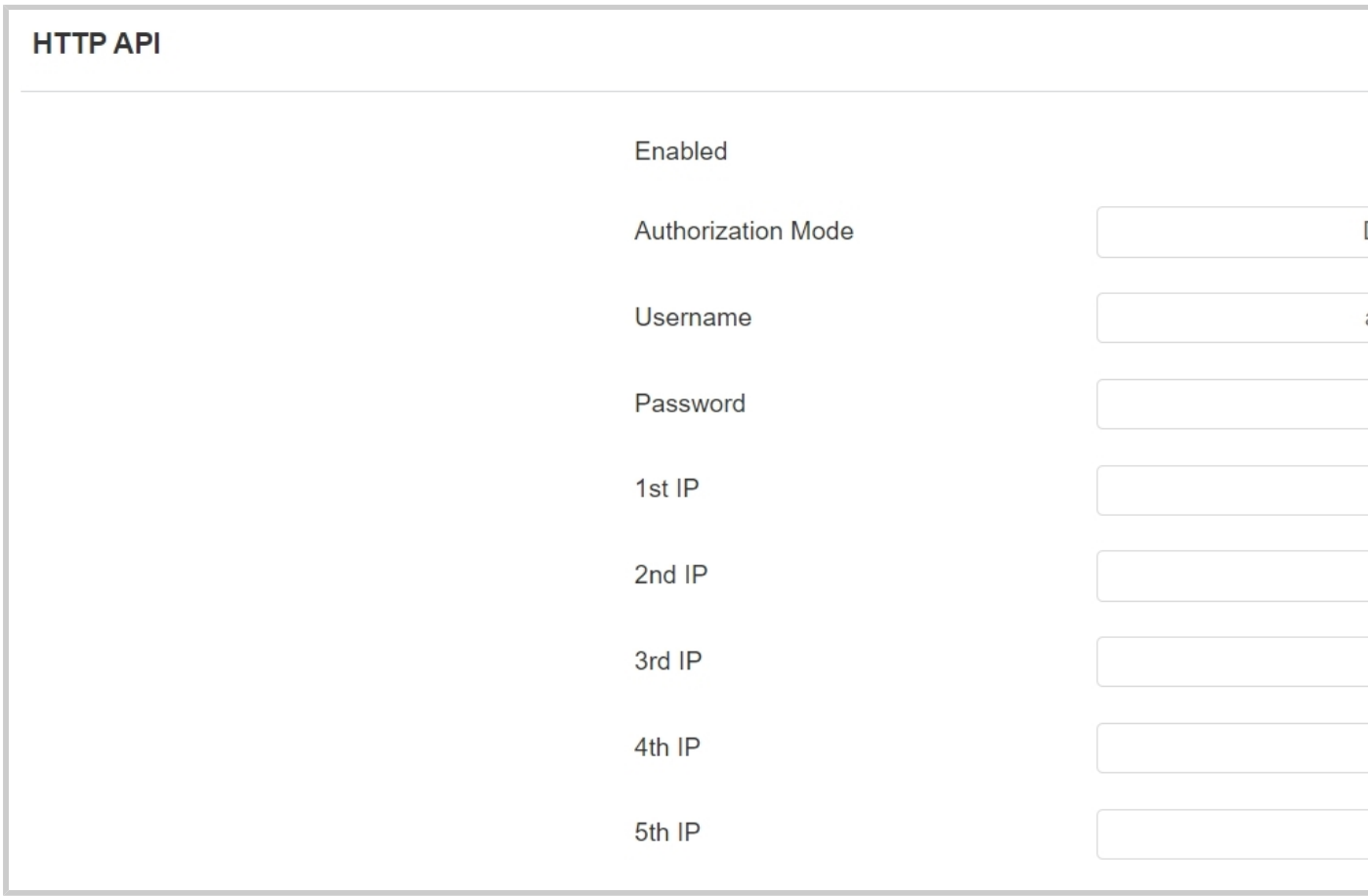


- **8 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 8 bits, "11100001".
- **4 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 4 bits, "0001".

Integration via HTTP API

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

To set it up, go to the web **Setting > 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**: Select among the following options: None, Normal, Allowlist, Basic, Digest, and Token for authorization type, which will be explained in detail in the following chart.
- **Username**: Enter the user name when **Basic** or **Digest** authorization mode is selected. The default username is admin.
- **Password**: Enter the password when **Basic** or **Digest** authorization mode is selected. The default password is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

Please refer to the following description for the authentication mode:

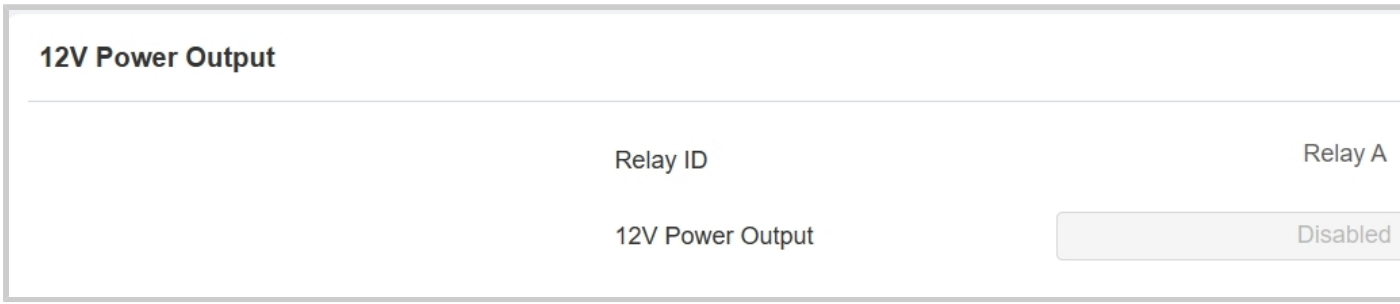
NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication. The allowlist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode of username and password.

NO.	Authorization Mode	Description
5	Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

Power Output Control

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

To set it up, go to the web **Access Control > Relay > 12V Relay Output** interface.



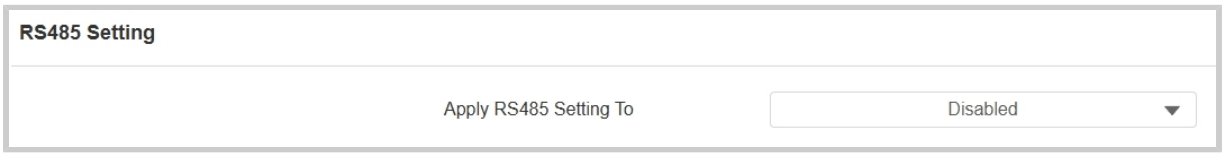
- **12V Power Output**:
  - **Always**: Provide continuous power to the third-party device.
  - **Triggered by Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.
  - **Security Relay A**: The device can work with the security relay, SR01.

Integration via RS485

You can connect the device to an external device such as SR01 or an OSDP-based card reader via RS485. To make the connection effective, you need to select the right RS485 mode.

Click here to view the detailed configuration of the OSDP feature.

To make the connection effective, you need to set up the RS485 on the **Device > RS485** interface.



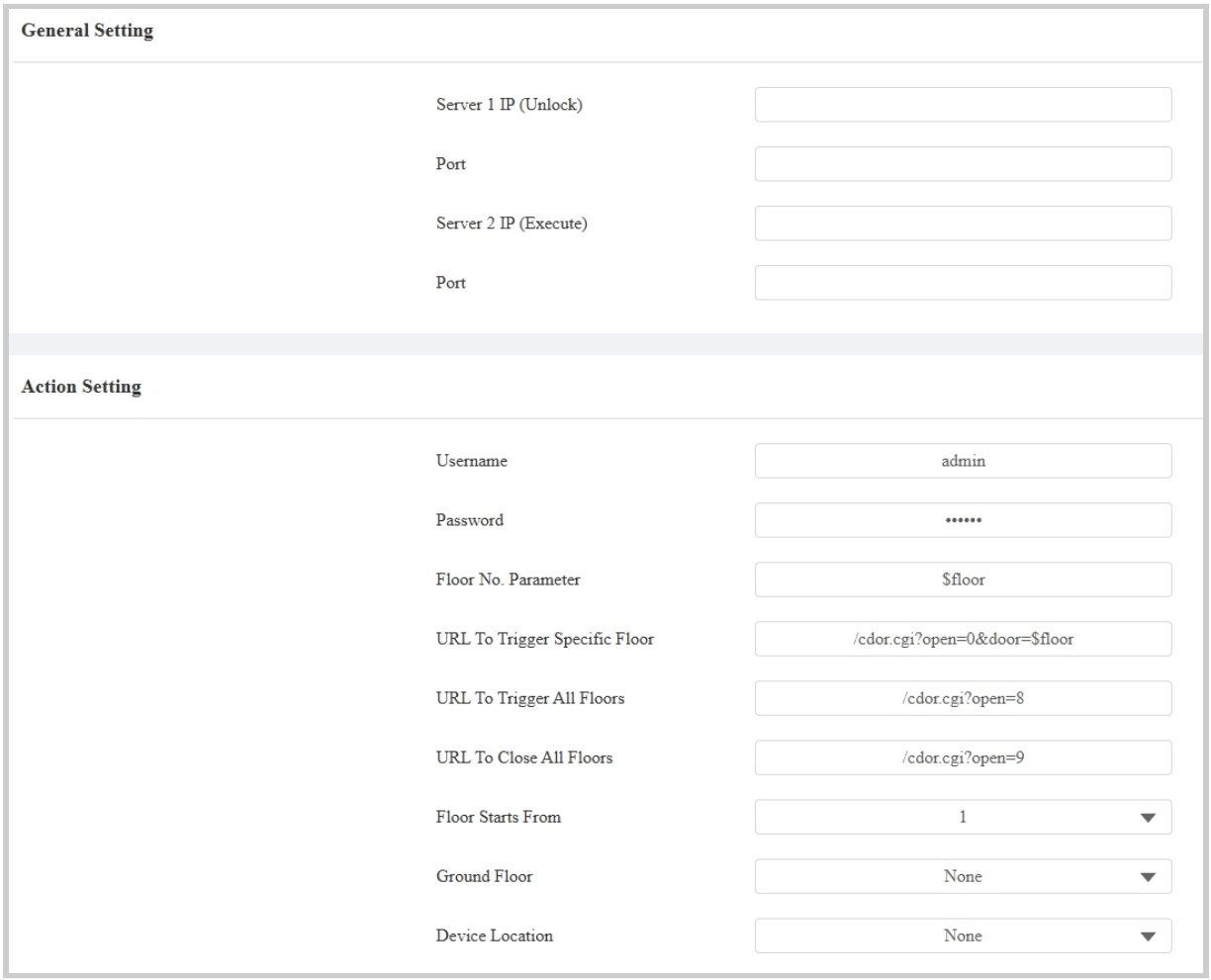
- **Disabled**: The RS485 function is disabled.
- **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **SCBK Value**: Secure Communication Key Value.
    - When it is filled, OSDP will use this value for encryption, employing a customized protocol for communication.
    - When it is left empty, OSDP will use the default encrypted protocol for communication.
- **Others**: Select this option when the device works with the SR01.

Lift Control

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

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

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



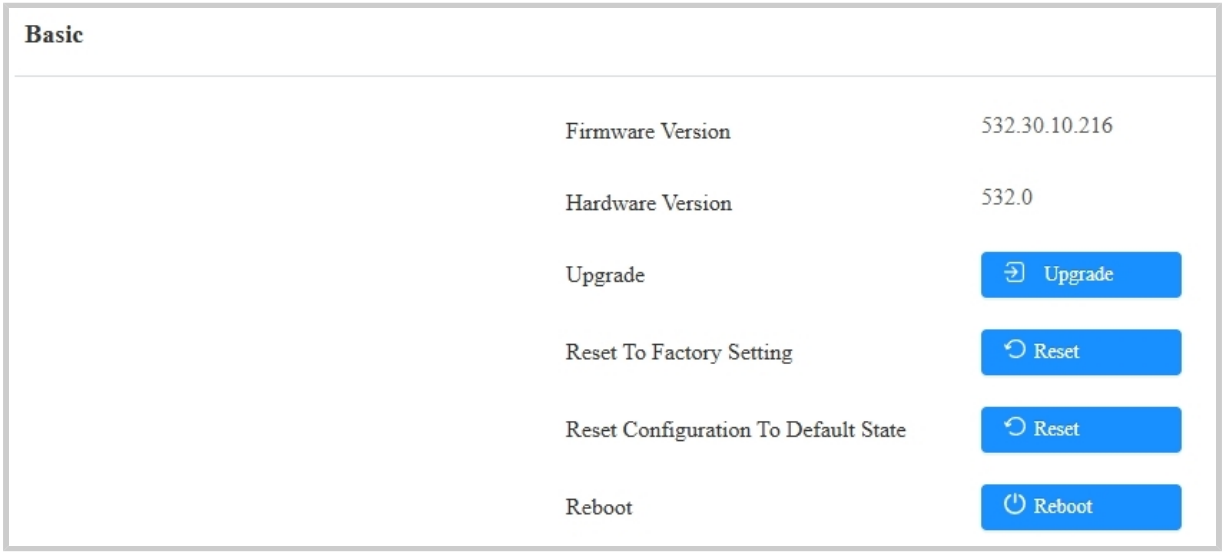
- **Lift Control List**: Select None to disable the function, and select Akuvox to integrate the door phone with the Akuvox controller.

- **Server 1 IP(Unlock)**: The IP address of the lift controller that unlocks the elevator button(s). It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute)**: The IP address of the lift controller that sends the lift control commands.
- **Port**: The server port of the lift controller server.
- **Username**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **Ground Floor**: If there are ground floors between the -1 and 1 floors, configure this option.
- **Device Location**: Select the floor where the device is installed.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Upgrade the firmware on the web **System > Upgrade** interface.



Note

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

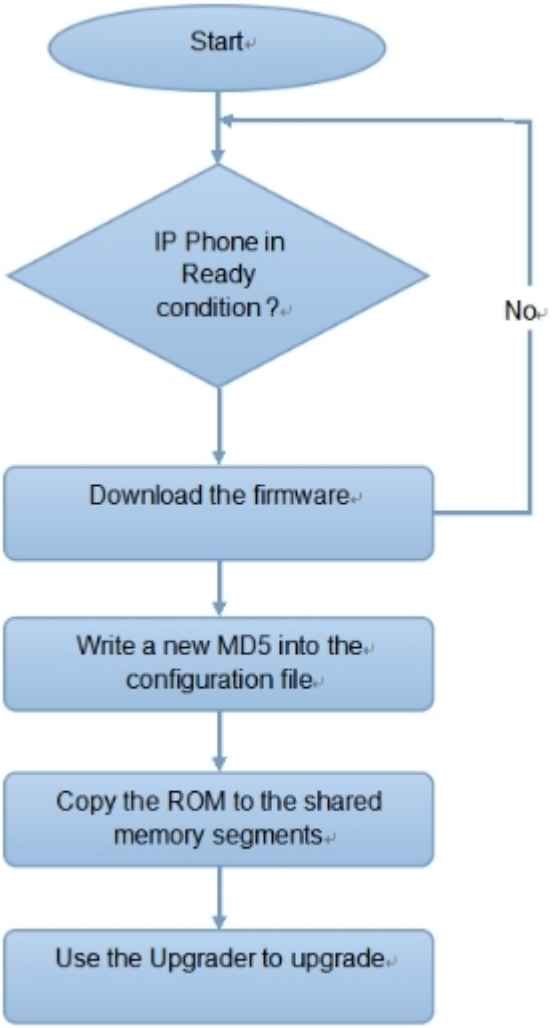
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

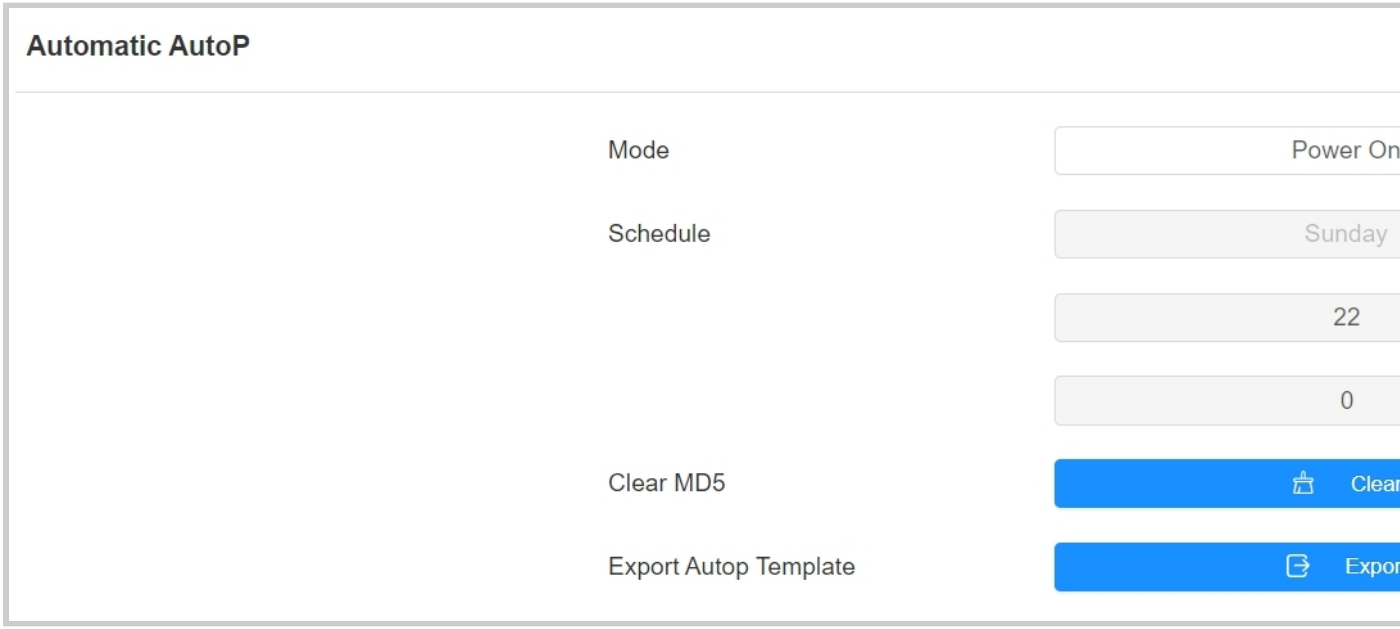
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

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

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

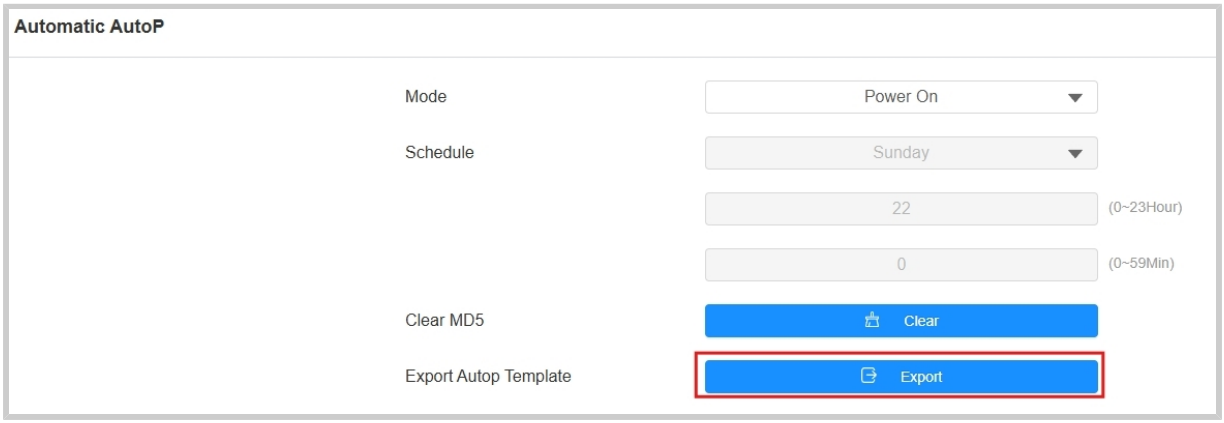


- **Mode**:
  - **Power On**: Allow the device to perform Autop every time it boots up.
  - **Repeatedly**: Allow the device to perform Autop according to the schedule.
  - **Power On + Repeatedly**: Combine **Power On** and **Repeatedly** modes, allowing the device to perform Autop every time it boots up or according to the schedule.
  - **Hourly Repeat**: Allow the device to perform Autop every hour.
- **Schedule**: When **Power On + Repeatedly** mode is selected, you can select the specific day and time for the Autop.
- **Clear MD5**: Used to compare the existing autop file with the autop file in the server, if the files are the same, then the provisioning will be stopped, thus avoiding unnecessary auto-provisioning.

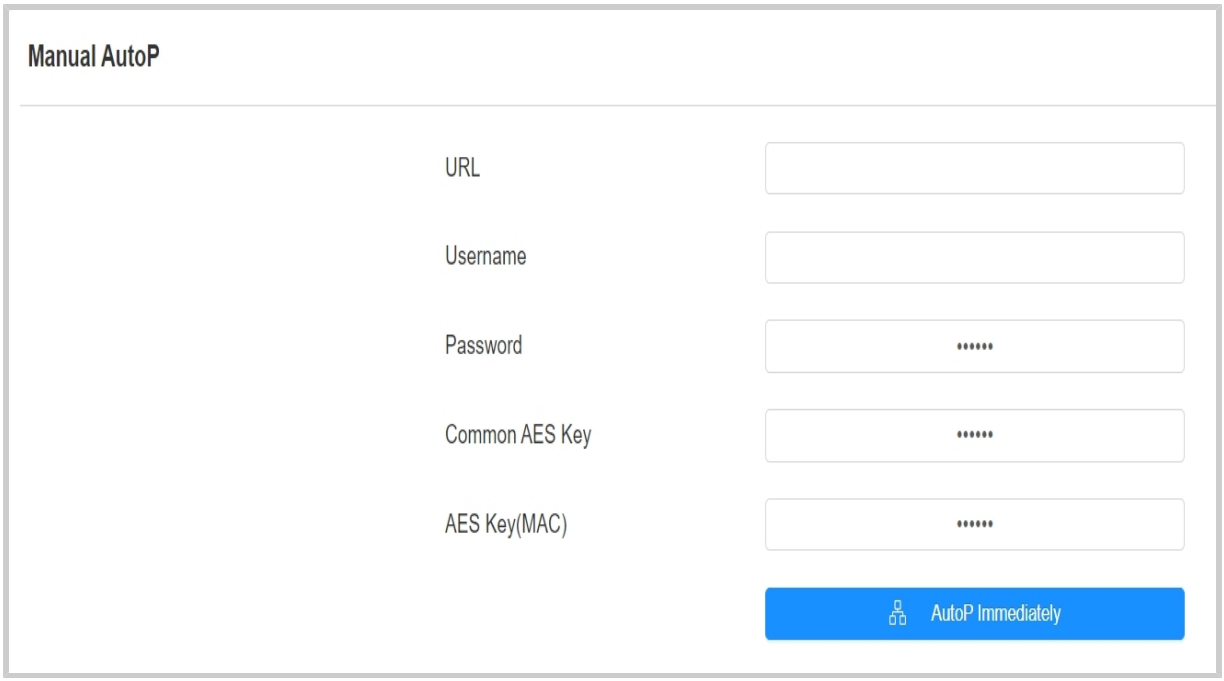
Static Provisioning Configuration

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

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



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



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

Note

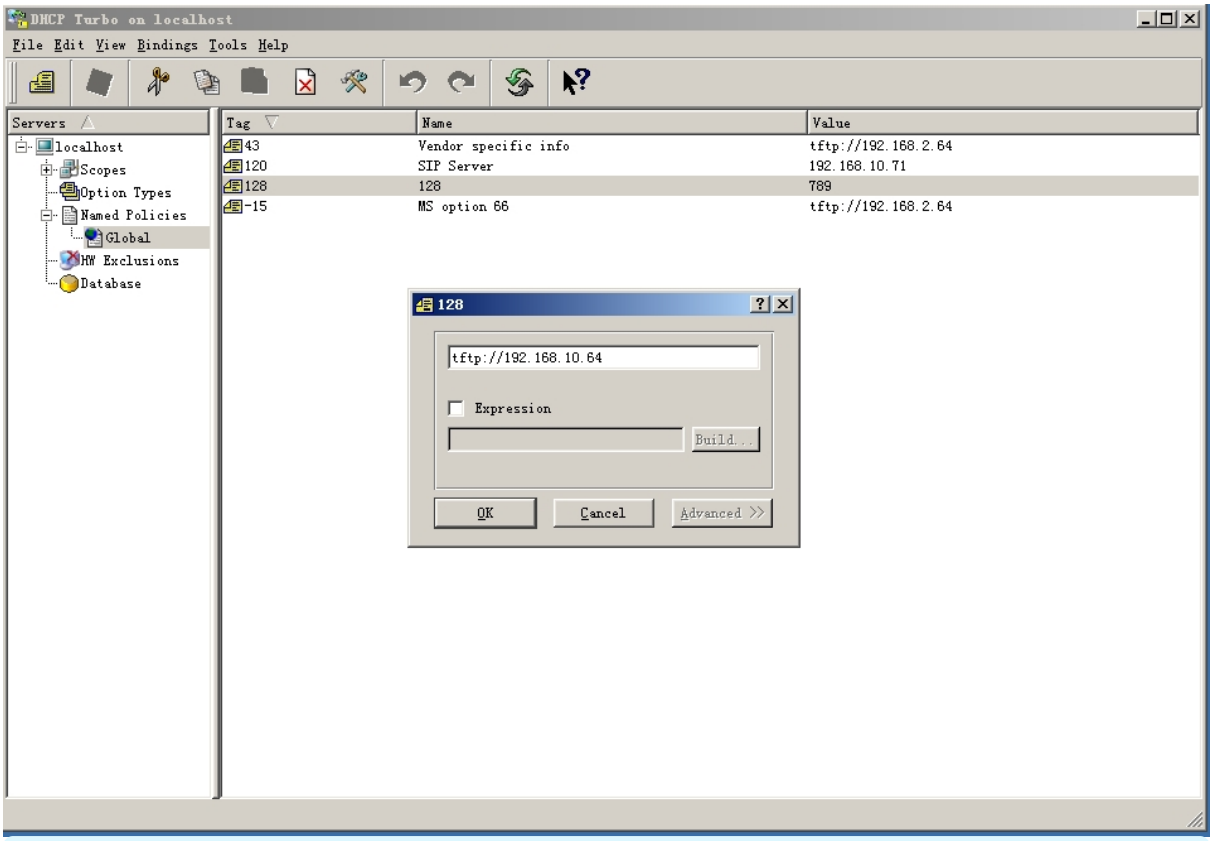
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning Configuration

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

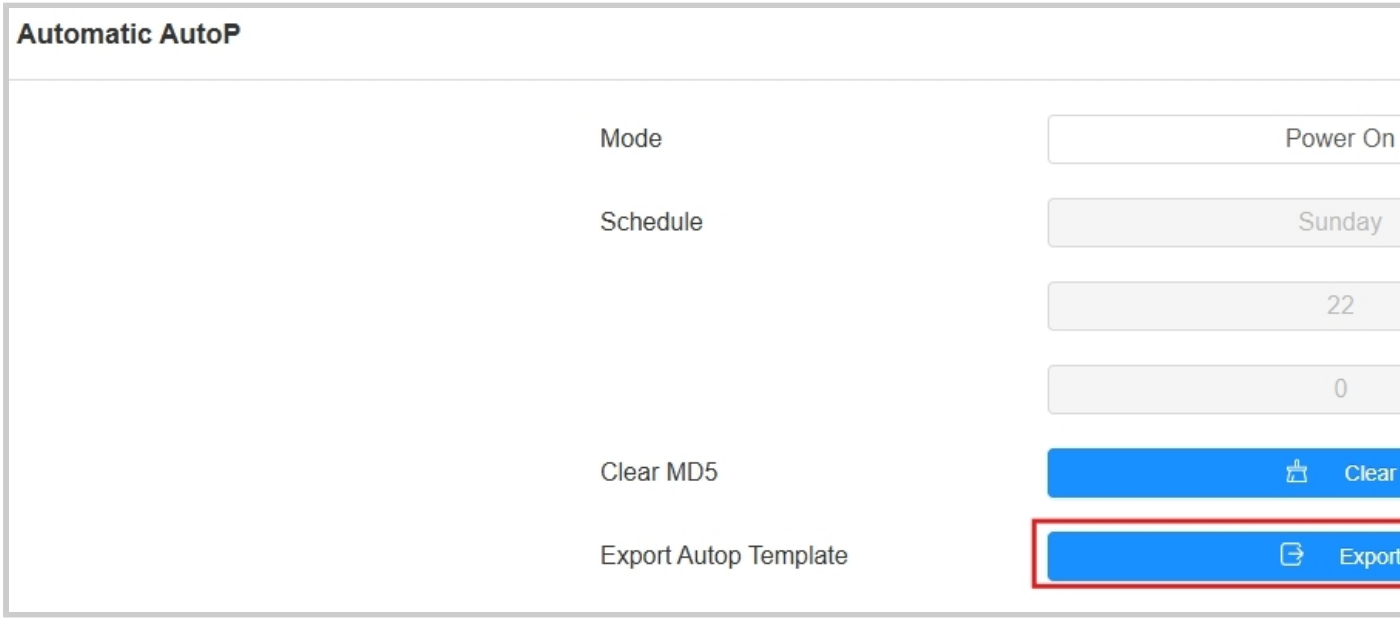


Note

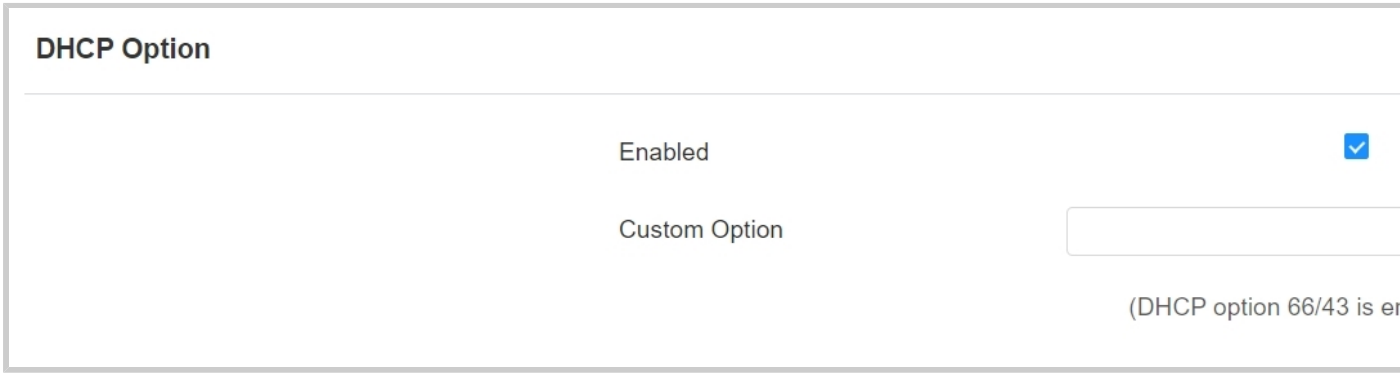
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

Download the template on **System > Auto Provisioning > Automatic AutoP** interface.



Then, set up the DHCP.



- **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 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 updated server URL in it.

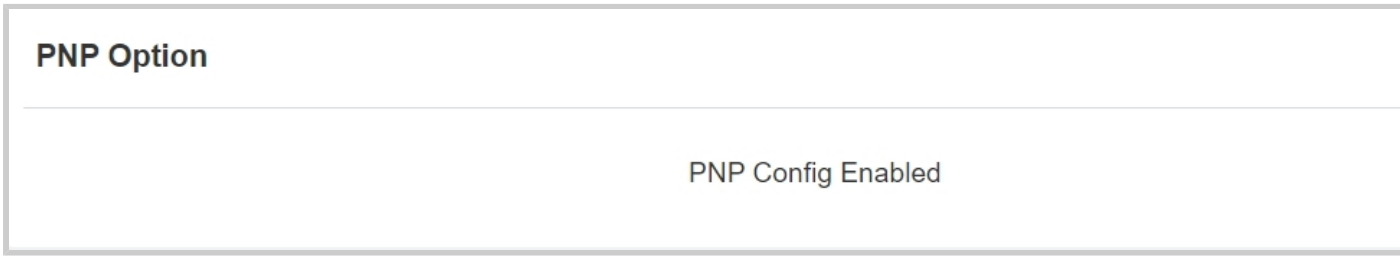
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

PNP Configuration

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

Click here to watch the configuration video.

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

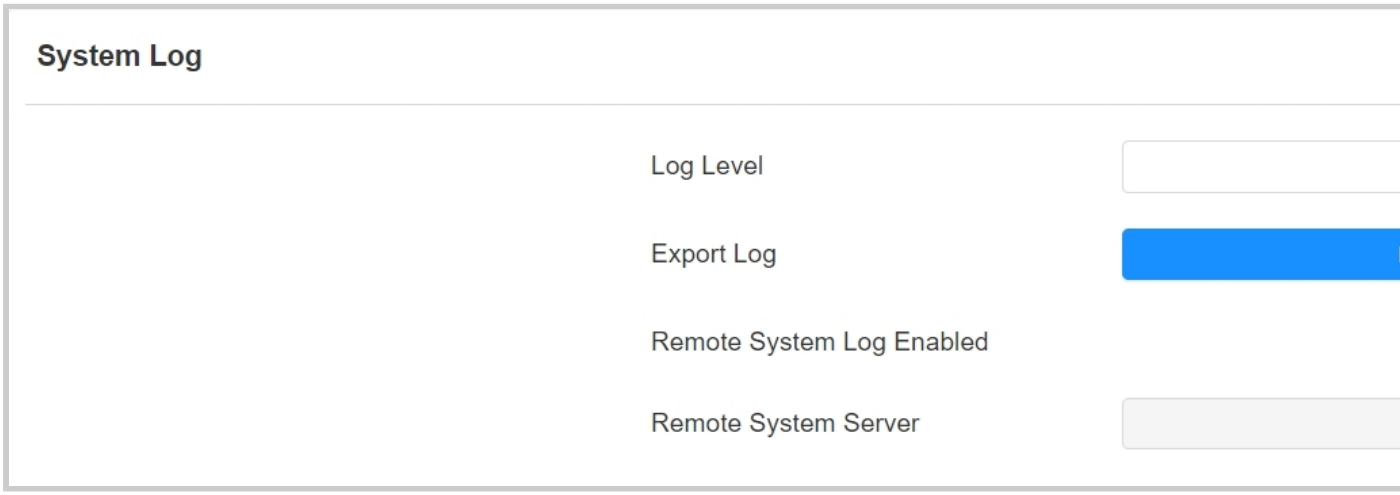


Debug

System Log

System logs can be used for debugging purposes.

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

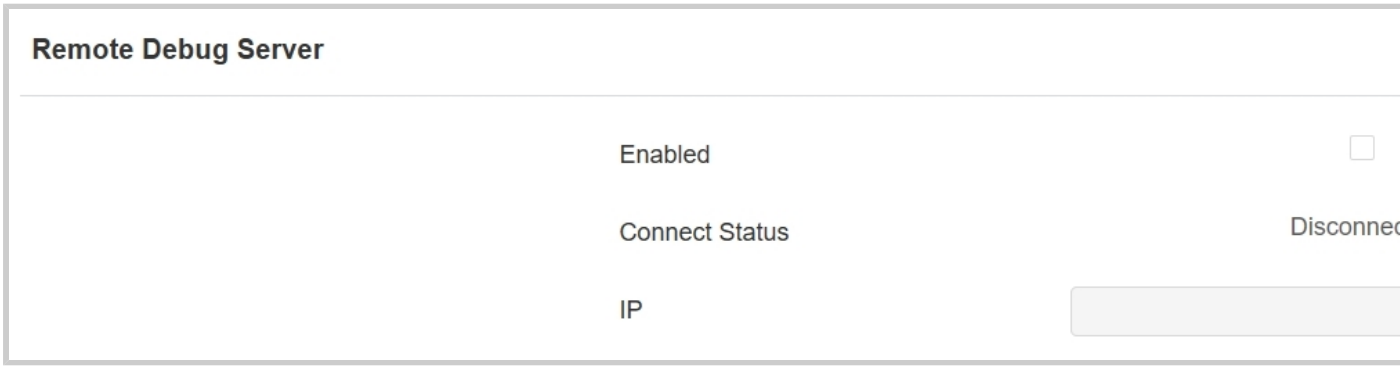


- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export a temporary debug log file to a local PC.
- **Remote System Server:** Set the remote server address to receive the device log. Akuvox technical support will provide the remote server address.
- **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 web **System > Maintenance** interface.

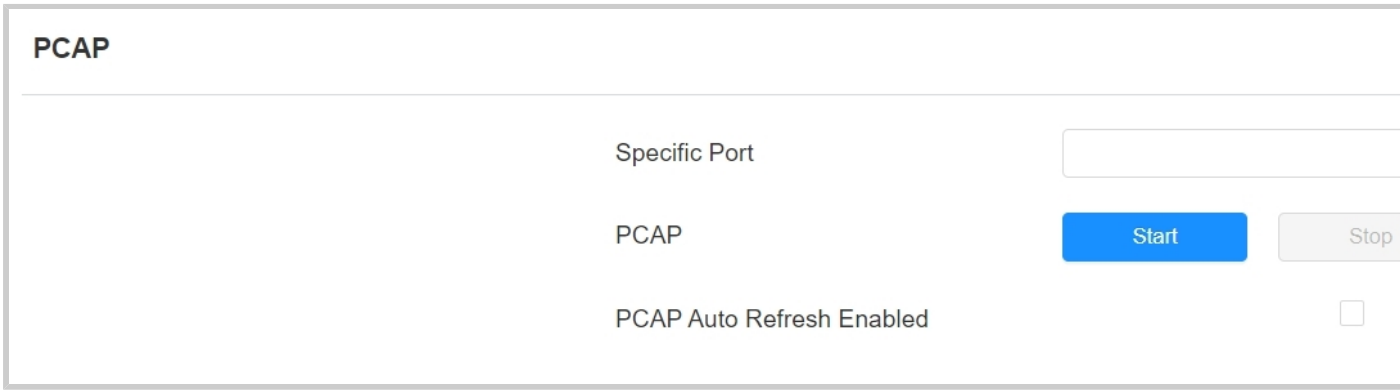


- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.

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 web **System > Maintenance** interface.



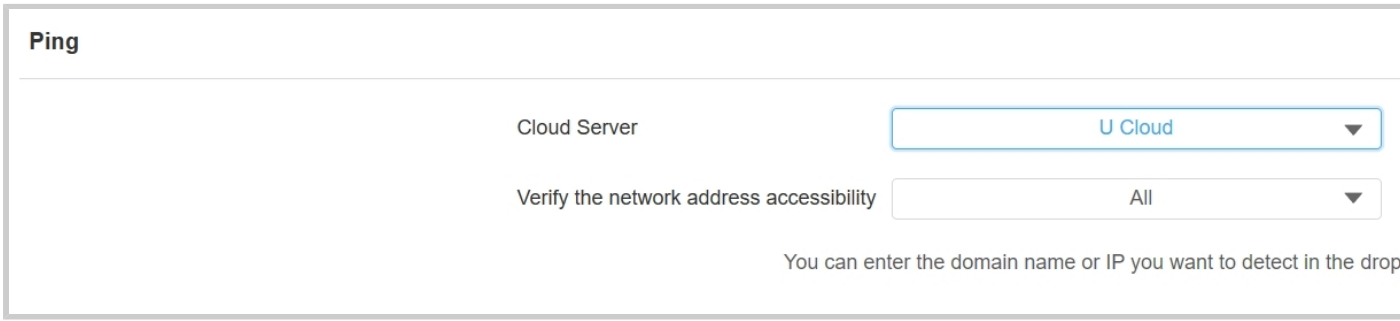
- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.

- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the data packets to your Local PC.
- **PCAP Auto Refresh Enabled:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum in capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.

Ping

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

To set it up, go to the **System > Maintenance > Ping** interface.

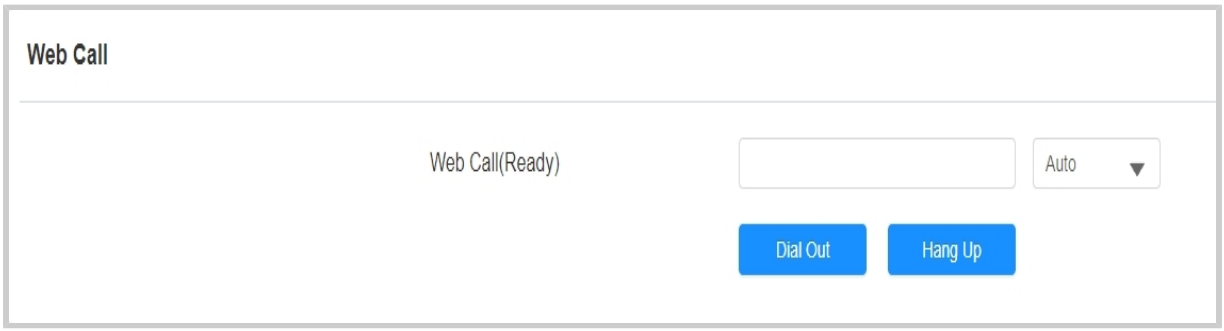


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Web Call

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

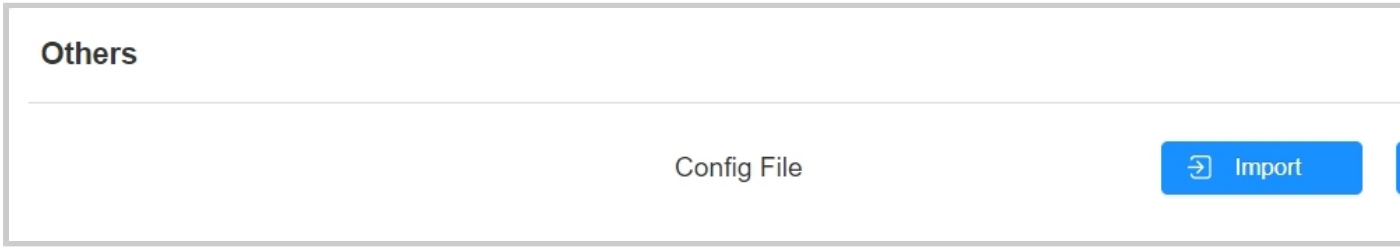
To set it up, go to the web **System > Maintenance > Web Call** interface. Select the registered SIP account, enter the IP/SIP number, and click Dial Out to make the call.


Web Call
Web Call(Ready)
Auto
Dial Out
Hang Up

Backup

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

Export the file on the **System > Maintenance** interface. The import file should be in .tgz/.conf/.cfg format.

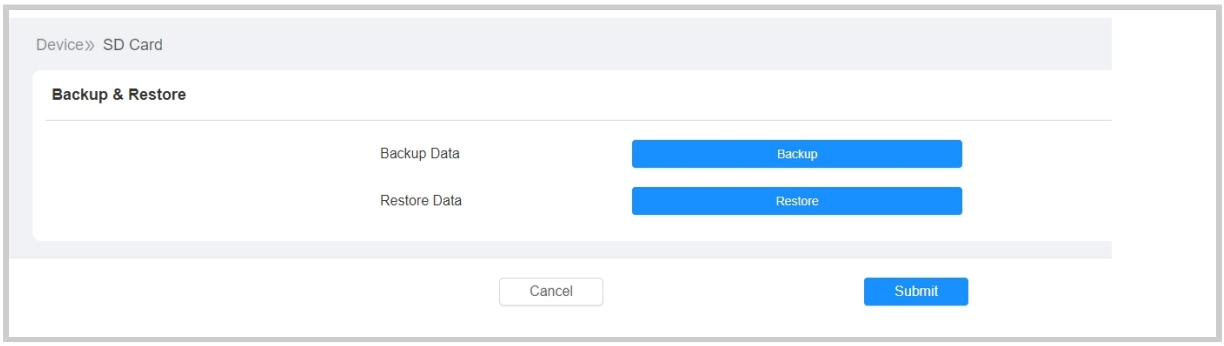


- **Config File**: Click **Export** to export configuration items as an encrypted file; click **Import** to import a configuration file to the device. The Config File includes configuration settings, user data, and contact data.

Backup via SD Card

The device supports inserting an SD card for importing and exporting configuration files.

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

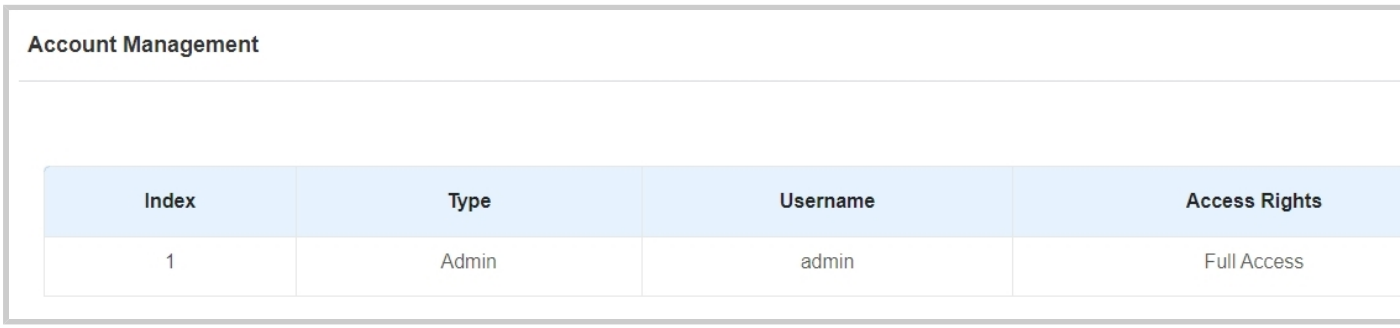


Password Modification

Accounts Management

You can add administrator and user accounts and configure their passwords for logging into the device web interface.

Navigate to the web **System > Security > Account Management** interface. Click **+Add** to create an account.

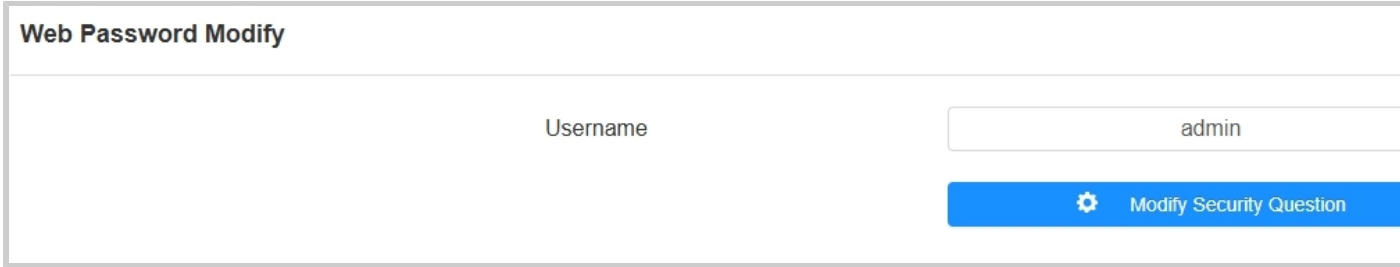


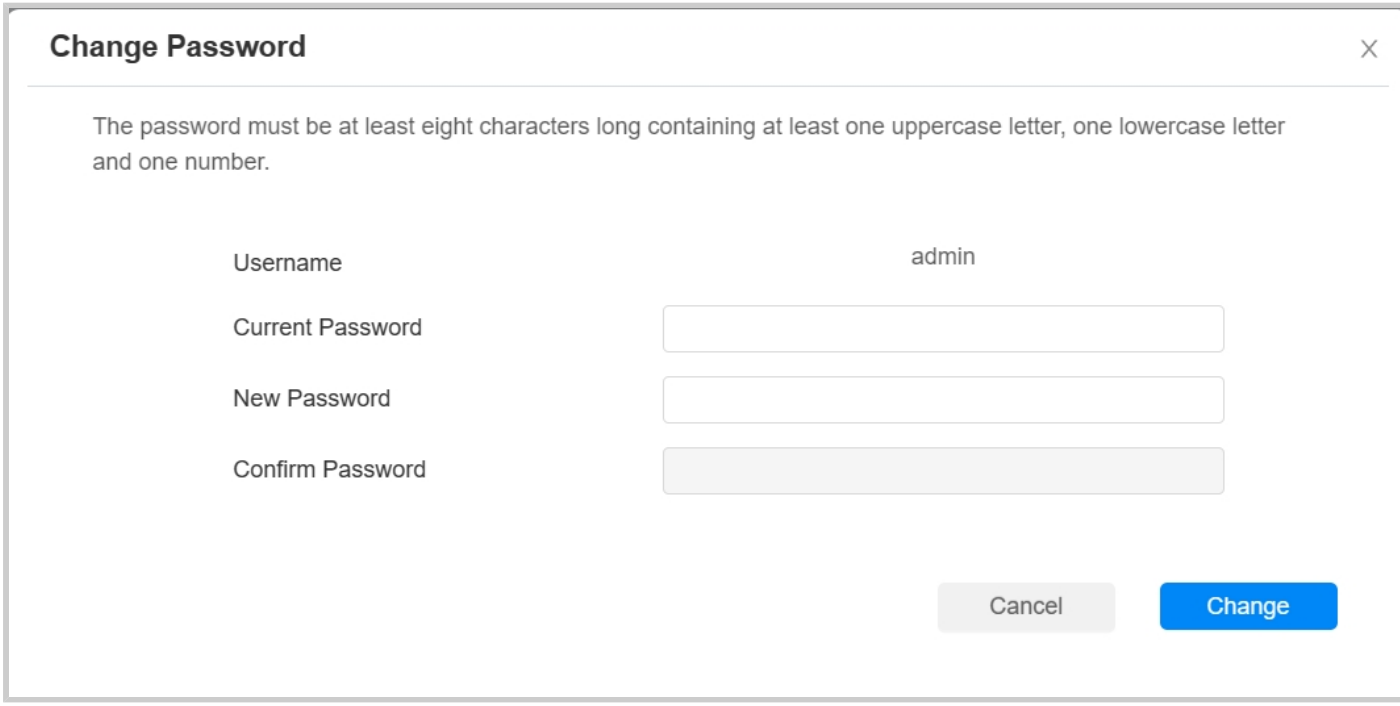
Modify Web Interface Password

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

Go to the **System > Security > Web Password Modify** interface. Select admin for the administrator account and select user for the user account.

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



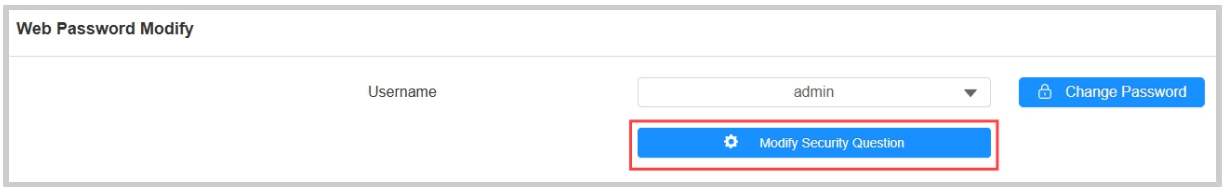


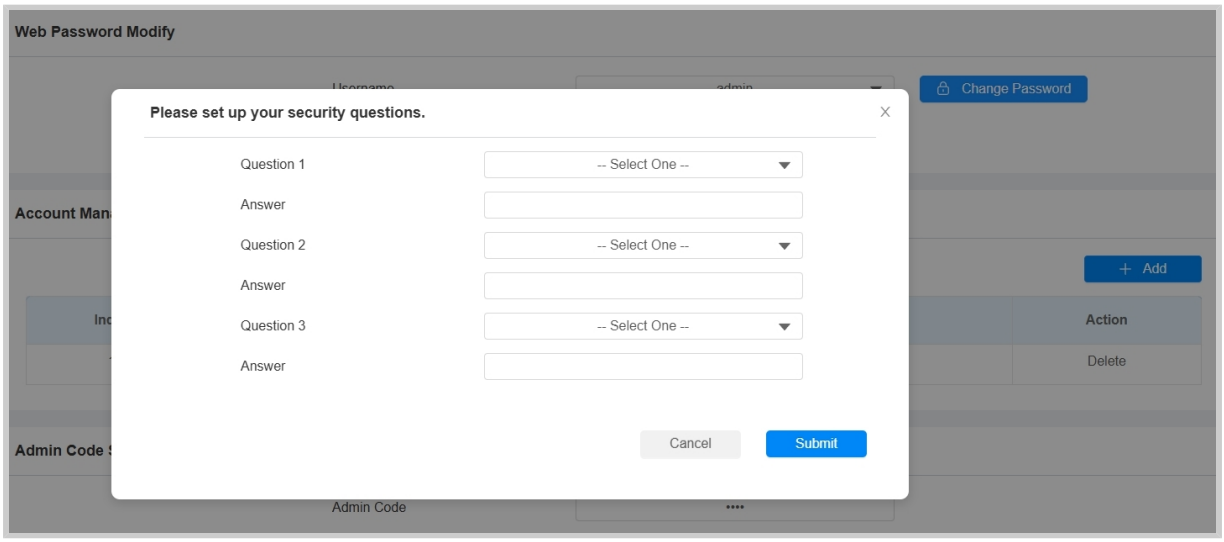
Modify Security Questions

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 **System > Security > Web Password Modify** interface.

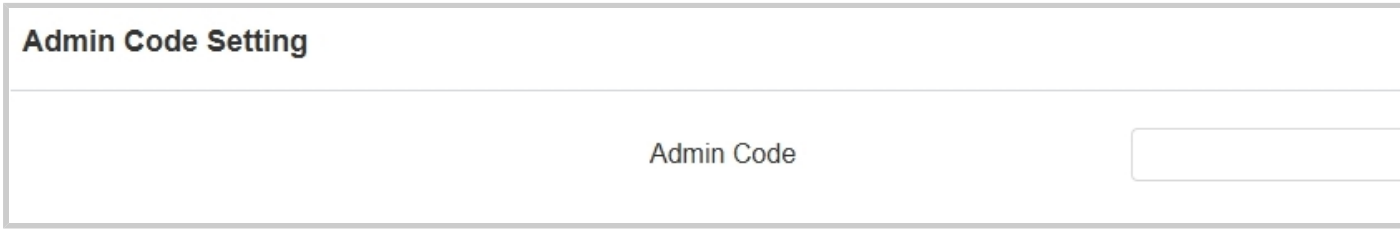




Modify Admin Code

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

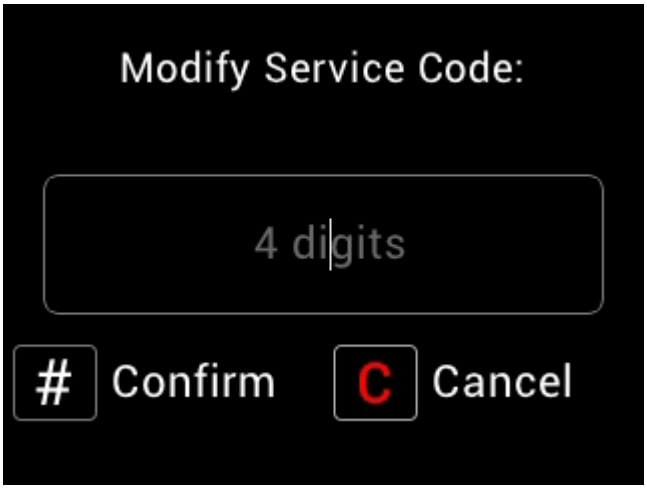
The default is 2396. You can change the password on the **System > Security > Admin Code Setting** interface.



Modify Service Code

The service code is used to access the settings that include public PIN, private PIN, and user card code modification. You can modify the code on the device.

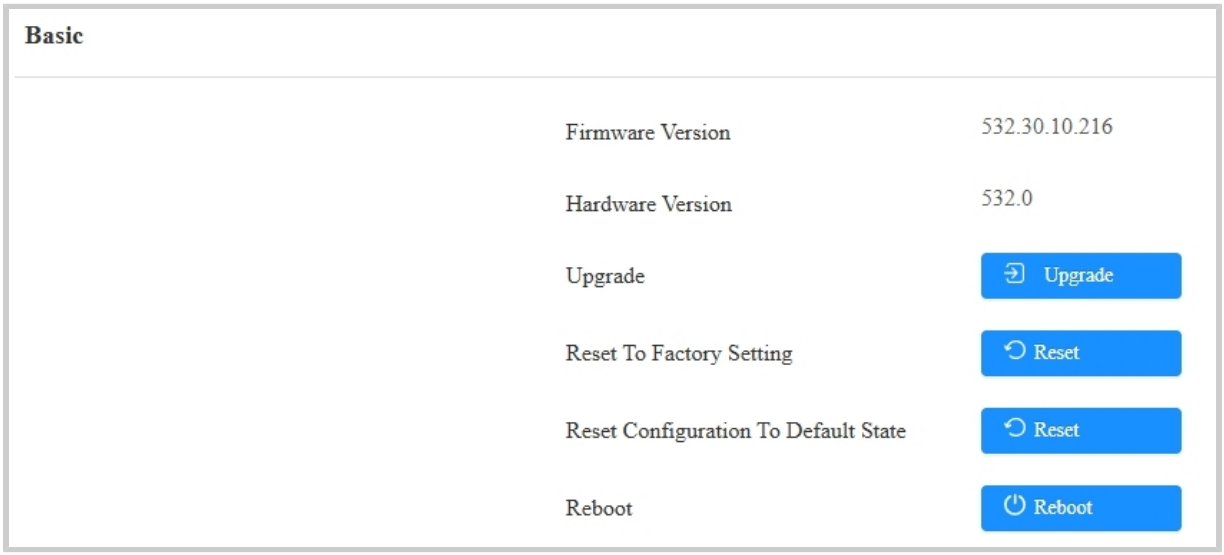
Press *2396# on the device keypad and press 2 and then 3 to enter the **Service Code Setting** screen.


Modify Service Code:
4 digits
Confirm
C Cancel

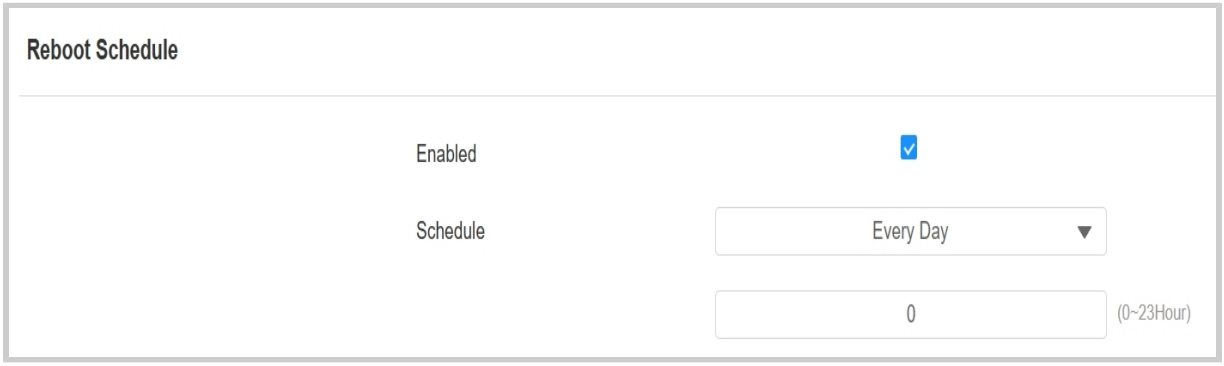
System Reboot & Reset

Reboot

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



You can set up the reboot schedule on the web **System > Auto Provisioning > Reboot Schedule** interface.



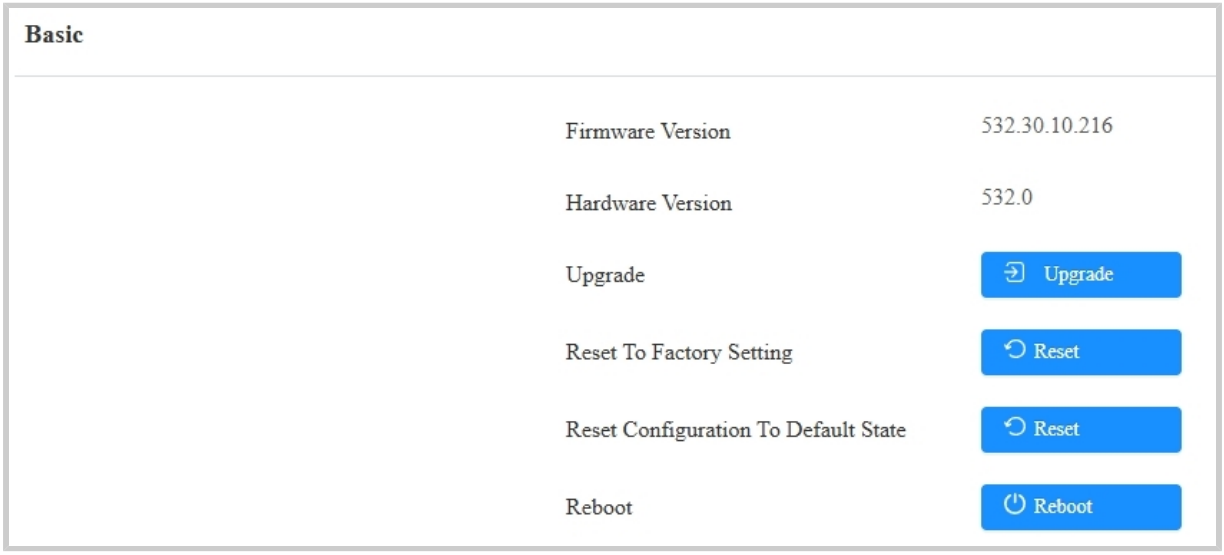
Reset

The device provides two reset options:

- **Reset to Factory Setting**: Reset all data to the factory default.

- **Reset Configuration to Default State**: Retain the user data such as the RF cards, face data, schedules, and call logs.

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



Tip

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

