Akuvox

Table of contents

Akuvox S535 Door Phone Administrator Guide

Akuvox

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX S535 DOOR PHONE

Administrator Guide

Akuvox

Thank you for choosing the Akuvox S535 series door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to version 535.30.11.27, and it provides all the configurations for the functions and features of the S535 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

The S535 touchscreen intercom is a cutting-edge device with a compact design featuring a robust metal exterior that provides excellent weather resistance and aesthetic appeal. The luxurious combination of gunmetal stainless steel and black glass enhances its high-end quality. User-friendly with clearly defined functional zones and an intuitive touchscreen, the S535 integrates seamlessly with Akuvox indoor units, SmartPlus cloud platform, and smart home systems, enabling features like audio/video intercom, access control, and remote management. Additionally, it addresses key customer pain points by offering stable LTE connectivity, improved intercom quality, quick deployment, and fingerprint recognition, ensuring convenience and accessibility for all users.

Changelog

What's new in version 535.30.11.27:

- Added a new web and LCD language: Turkish.
- Support Pose Detection Option for facial recognition.

Click here to view the device's previous changelog.

Model Specification

Model	S535
Operation System	Linux
Touch Screen	✓
Power Supply	PoE or a DC power adapter 12V/4A(max.)
Power Output	Provide power(12V/1A) when PoE+ or a power adapter powers the device.
Relay Port	1
Alarm Port	2
Wiegand Port	1
RS485 Port	1
USB Port	1
Fingerprint Module	Optional
Induction Loop Module	Optional
LTE Module	Optional
Camera	1
Fill Light	✓

Model	S535
Reset Button	✓
Bluetooth	✓
Wi-Fi	X
Card Reader	NFC, 13.56MHZ & 125KHZ
Microphone	1
Speaker	1

Supported Card Types

The device firmware should be S535.30.10.233 or higher:

- Unencrypted ID Card:
  - EM4100
  - EM4200
- Unencrypted IC Card:
  - Mifare Ultralight C/EV1
  - Mifare Classic Compatible Card
  - 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 SL1 Encrypted Card
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
  - Mifare Classic 1K
  - Mifare S50-1K Card
  - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

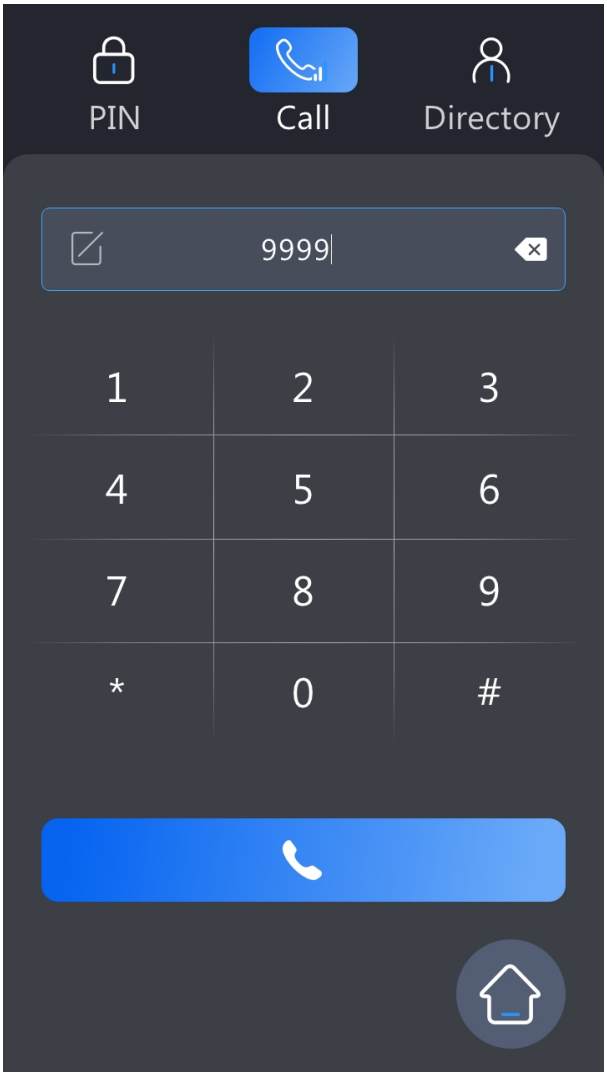
Access the Device

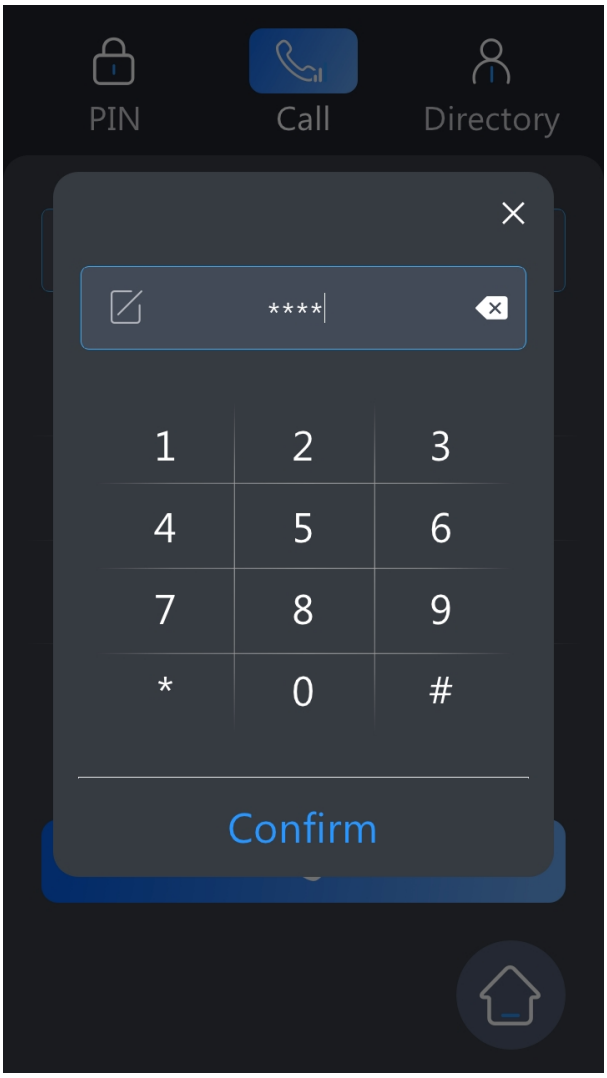
Door phones' system settings can be either accessed on the device or on its interface.

Access the Device Settings on the Device

Before configuring the door phone, please make sure the device is installed correctly and connected to a normal network.

You can set up some basic settings on the device screen by pressing **9999** + **Dial key** + **3888** (password) on the **Dial** screen.


PIN
Call
Directory
9999
1
2
3
4
5
6
7
8
9
*
0
#



Access the Device 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.

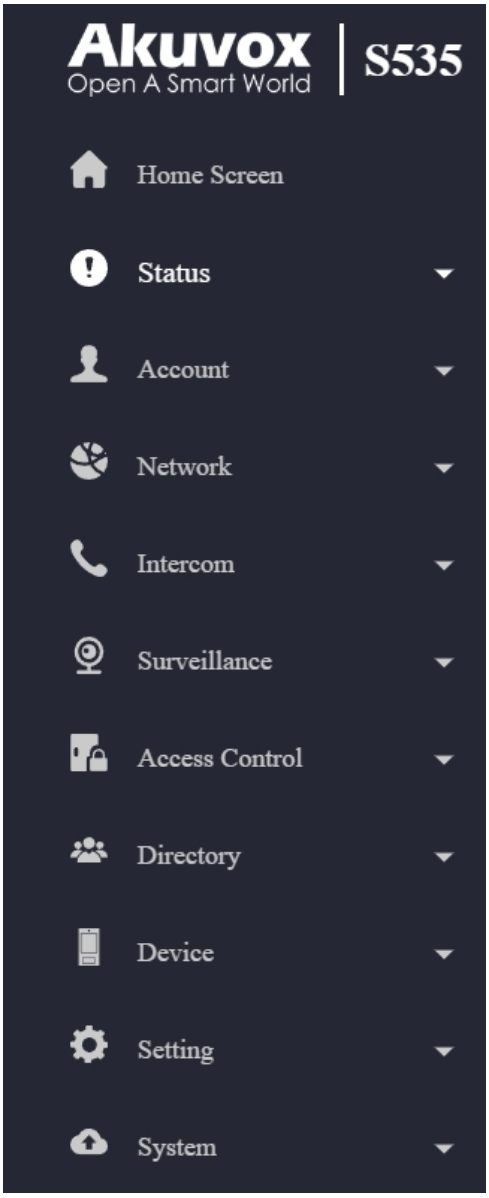
Check the device IP on the **Setting > System Info > Network** screen. Or, use the IP scanner to scan device IPs on the same local network. Enter the IP in a browser to see the login page.

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.
- The initial user name and password are **admin** and please be case-sensitive.
- Your computer should be on the same network as the device.

Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, call log, and door log.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, etc.
- **Network**: This section mainly deals with DHCP and Static IP settings, RTP port settings, device deployment, etc.
- **Intercom**: This section covers intercom settings, call features, dial plans, etc.
- **Surveillance**: This section covers motion detection, RTSP, MJPEG, ONVIF, live stream, etc.
- **Access Control**: This section covers input control, relay, card settings, face recognition settings, private PIN codes, etc.
- **Directory**: This section involves user management, RF card, PIN, face recognition management, etc.
- **Device**: This section includes light settings, LCD settings, audio settings, lift control, and Wiegand.
- **Setting**: This section includes time, language, action settings, schedule for access control, screen display, and HTTP API.
- **System**: This section covers firmware upgrade, device reset and reboot, configuration file auto-provisioning, fault diagnosis, security, PCAP, system log, web call, tamper alarm, and password modification.


Akuvox
Open A Smart World
S535
Home Screen
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System

Language and Time

Language

Set up the language during initial device setup or later through the device or web interface according to your preference.

On the Web

Select the LCD language on the **Setting > Time/Lang > LCD Language** interface.

The following languages are supported:

- English, Simplified Chinese, Traditional Chinese, Russian, Czech, Portuguese, Spanish, Italian, Dutch, French, German, Polish, Ukrainian, and Turkish.

Switch the device's web language in the upper right corner.

The following languages are supported:

- English, Simplified Chinese, Traditional Chinese, Russian, Czech, Portuguese, Spanish, Dutch, French, German, Polish, Italian, Ukrainian, and Turkish.

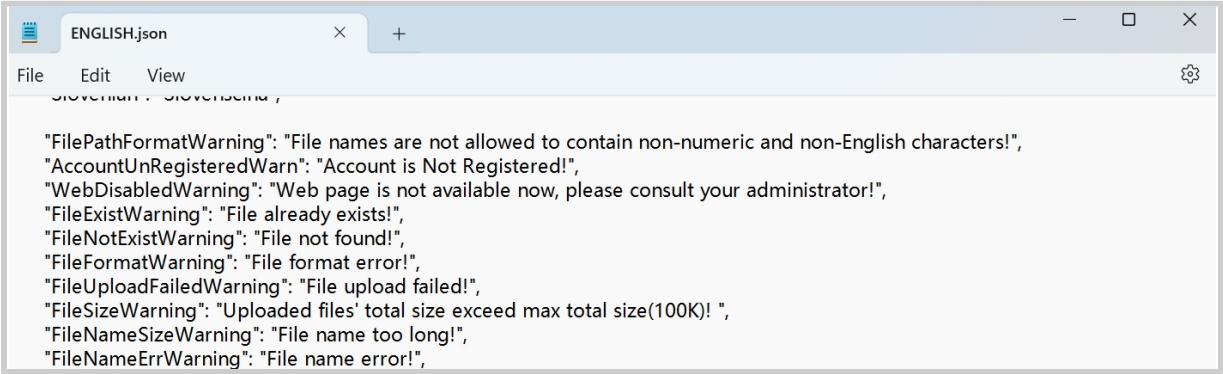
Custom Language

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

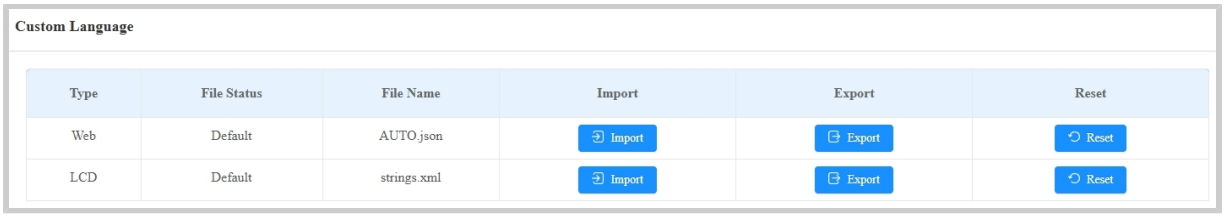
Export the .json file for editing. You may edit it with the notepad on your computer.

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.



On the Device

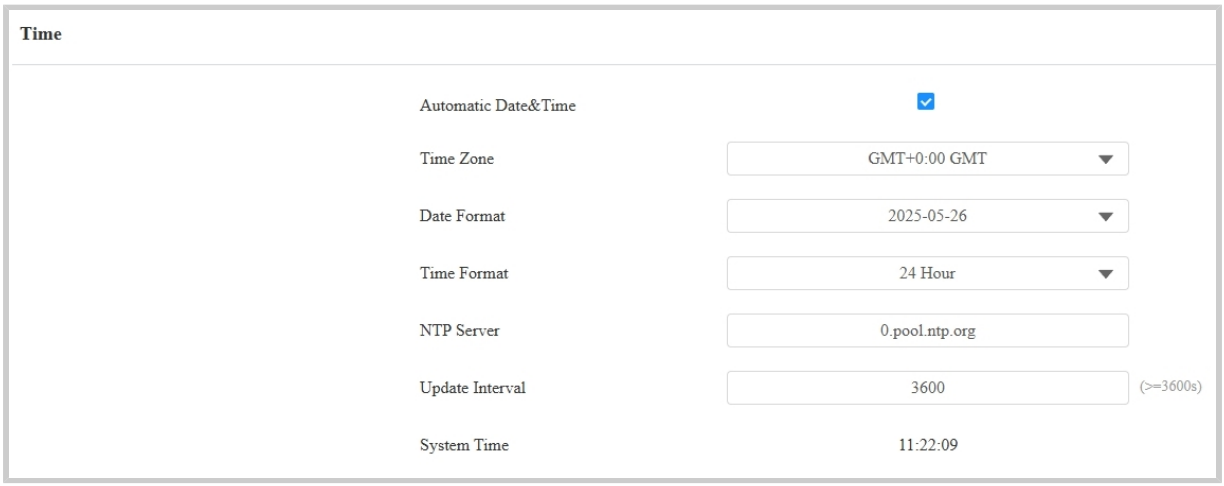
You can select the LCD language on the **Setting > Basic Setting > Language** screen.

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.

On the Web

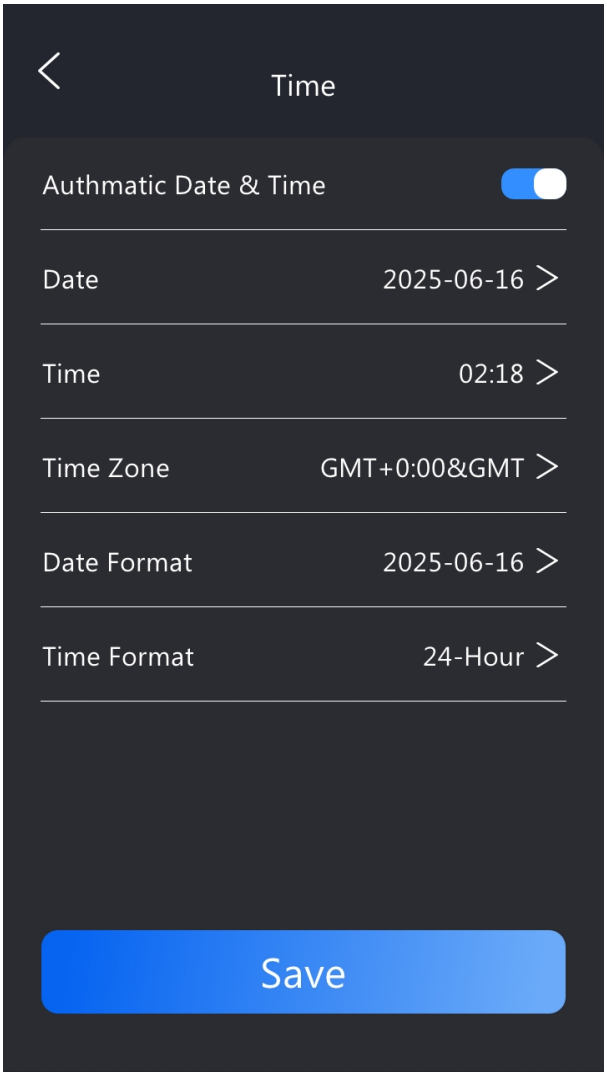
Set up time on the **Setting > Time/Lang > Time** interface.



- **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.

On the Device

Set up time on the **Setting > Basic Setting > Time** screen.


Time
Authmatic Date & Time
Date
2025-06-16
Time
02:18
Time Zone
GMT+0:00&GMT
Date Format
2025-06-16
Time Format
24-Hour
Save

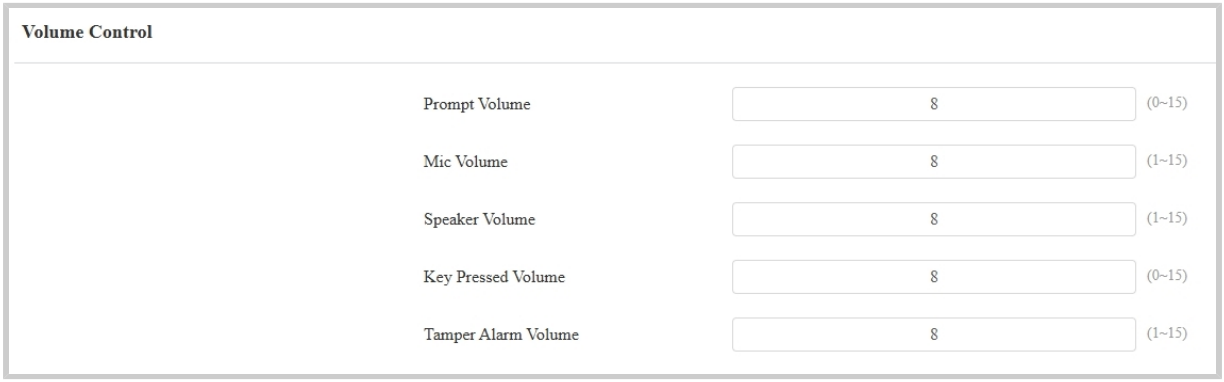
Volume and Tone

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.

On the Web

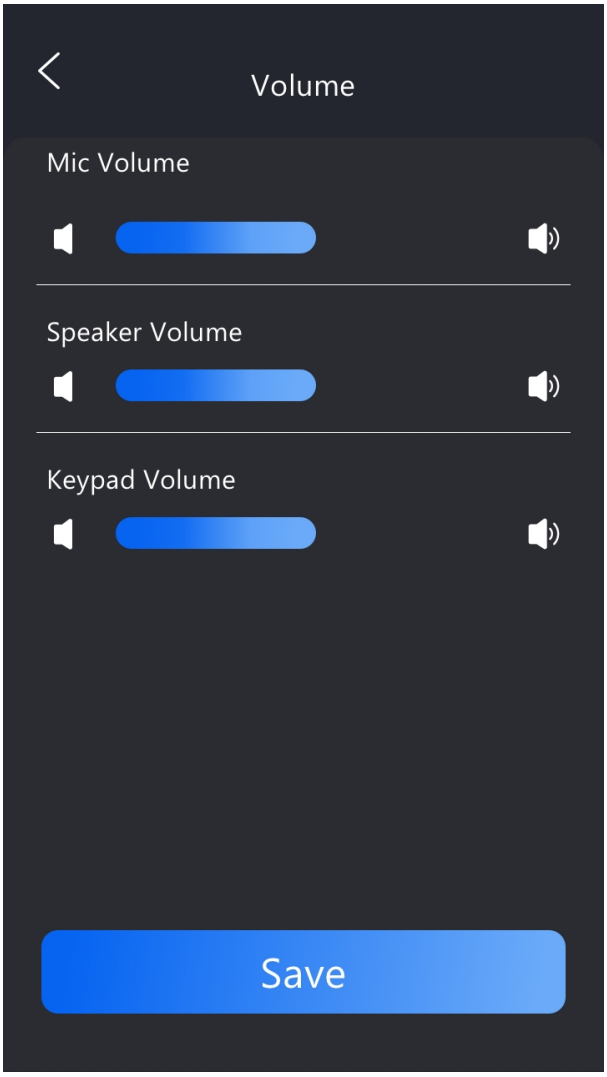
Set up volumes on the web **Device > Audio** interface.



- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 8.
- **Mic Volume**: The default is 8.
- **Speaker Volume**: The default is 8.
- **Key Pressed Volume**: The icon tapping sound. The default is 8.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 8.

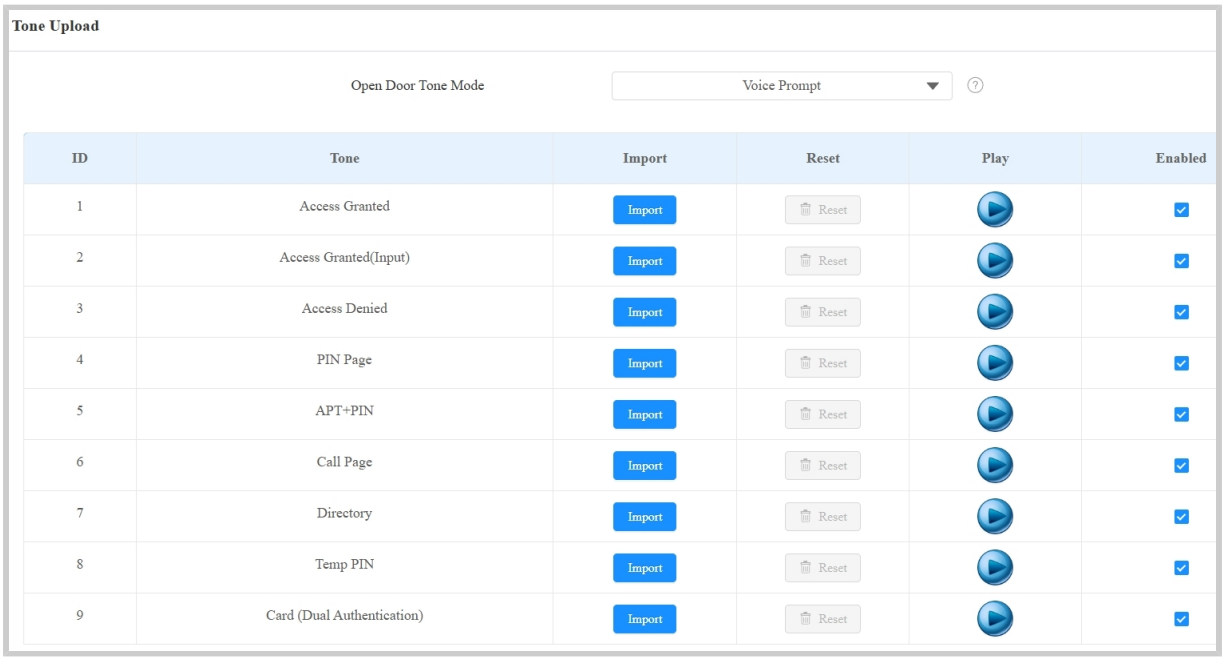
On the Device

You can set up volumes on the **Setting > Basic Setting > Volume** screen.



Upload Tones

You can upload the tone for different scenarios on the **Device > Audio > Tone Upload** interface.



- **Access Granted(Input)**: The tone is played when the door is opened by pressing an exit button connected to the device's input.
- **PIN Page**: The tone is played when entering the PIN screen.
- **APT+PIN**: The tone is played when entering the Apartment number and PIN code for door access.
- **Call Page**: The tone is played when entering the Call screen.
- **Directory**: The tone is played when entering the Directory screen.
- **Temp PIN**: The tone is played when entering the temporary PIN for door access.
- **Card(Dual Authentication)**: The tone is played, prompting the user to swipe the card for door access in two-factor authentication mode.

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

Ringback Tone

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

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

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

Open Door Tone Mode

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

- **Voice Prompt**: Play the default prompt "Welcome, please come in" when the door is opened.

- **Sound Effect**: Play the Beep sound when the door is opened.

LED and LCD

Infrared LED Setting

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

Set it up on the web **Device > Light > LED** 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 default is 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 the LED light will stay on during the time from 8:00 am to 12:00 pm during one day (24 hours).

LED White Light

White light LED is mainly used to reinforce the lighting for the QR code access and for the greater visibility of the visitors when seeing their images from indoors in a dark environment.

Set it up on the web **Device > Light > White Light** interface.

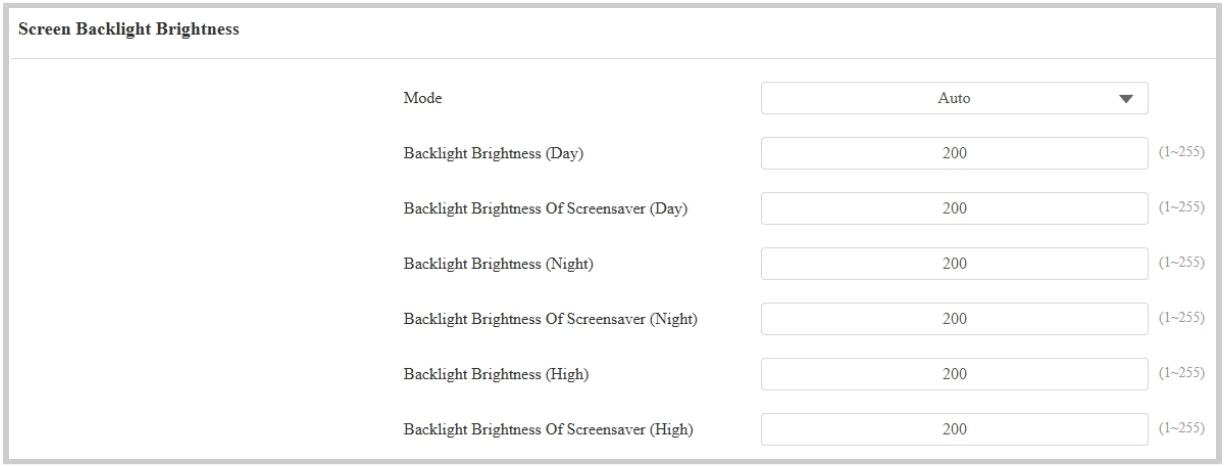
- **Mode**: Select **Auto** or **OFF**. If you select **Auto**, the white light will turn on for 5 minutes for facial recognition and QR code scanning.
- **White Light Value**: Set the white light value from 1 to 10. The default is 3. The higher the value, the brighter the light.

LCD Screen Brightness

You can set up the backlight brightness so that users can better see the screen in an environment with high or low light intensity.

On the Web

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



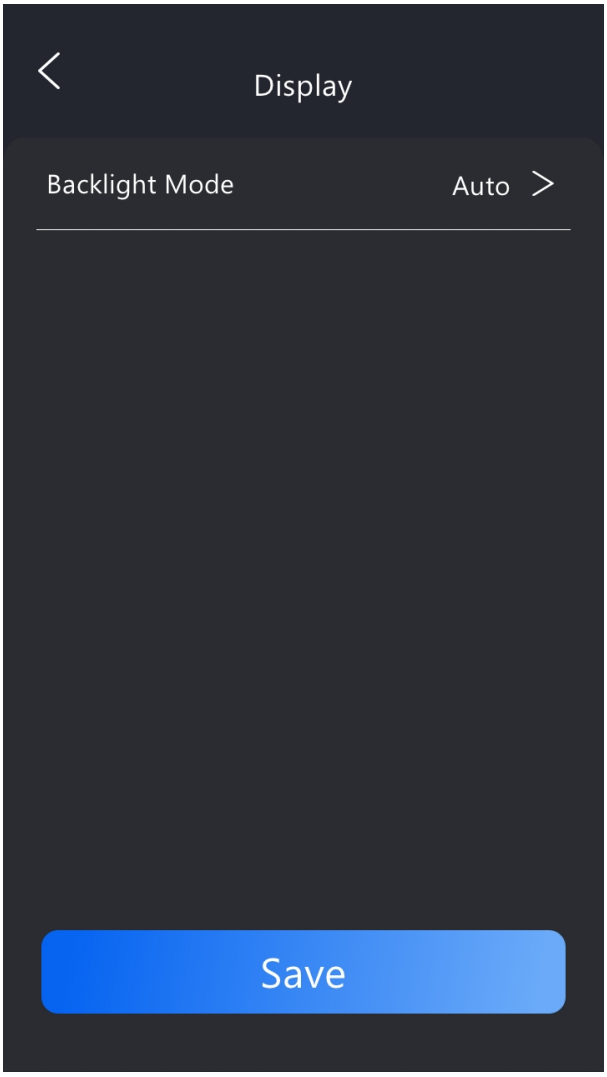
- **Mode**:
  - **Manual**: Set the backlight brightness value manually.
  - **Auto**: The screen backlight brightness will be adjusted automatically.

> **Note**
>
> The Day and Night backlight modes are determined by the photoresistor.
>
> - If the current value is between the minimum and maximum photoresistor values, the device is in Day mode.
> - If the current value is higher than the maximum photoresistor value, the device is in Night mode.

- **Backlight Brightness (Day)**: Select the brightness value from 1-255. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screensaver (Day)**: Adjust the backlight for the screensaver in the daytime with the value ranging from 1-255.
- **Backlight Brightness (Night)**: Select the brightness value from 1-255. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screensaver (Night)**: Adjust the backlight for the screensaver at night with the value ranging from 1-255.
- **Backlight Brightness (High)**: Select the brightness value from 1-255 in an environment with strong light. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screensaver (High)**: Adjust the backlight for the screensaver in an environment with strong light. The value ranges from 1-255.

On the Device

You can set the backlight mode on the device **Setting > Basic Setting > Display** screen.



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 **a 12V DC power adapter** to ensure sufficient power supply.
- **Heat 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.

Screen Display

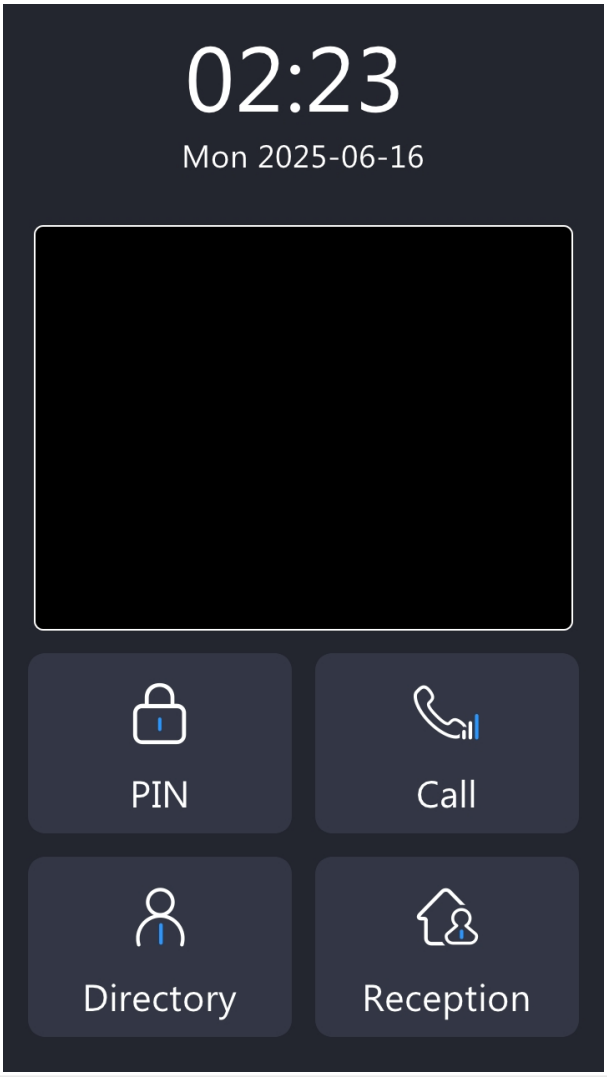
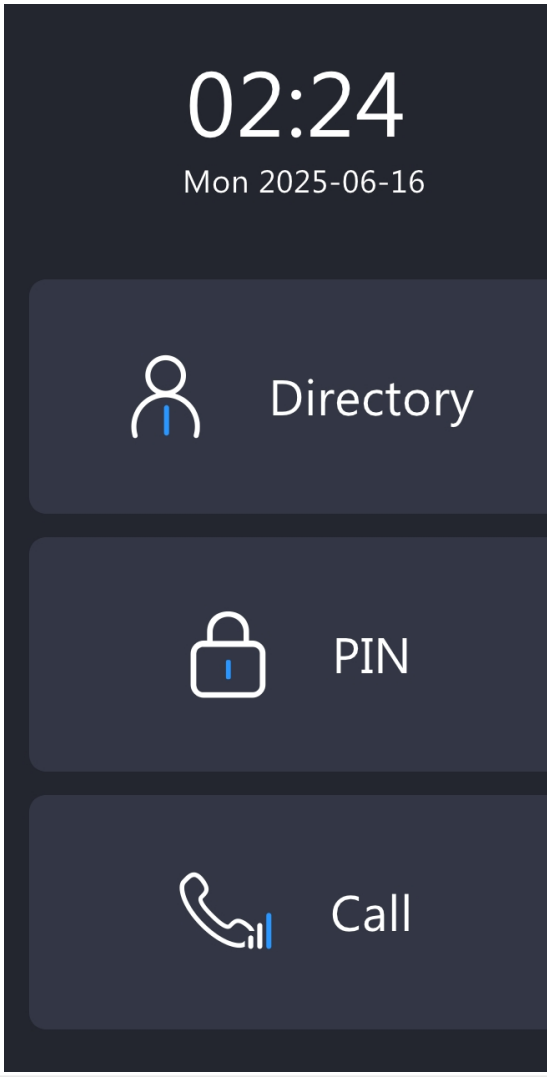
You can set up the device's screen display features such as screensaver to give users a better visual and operational experience.

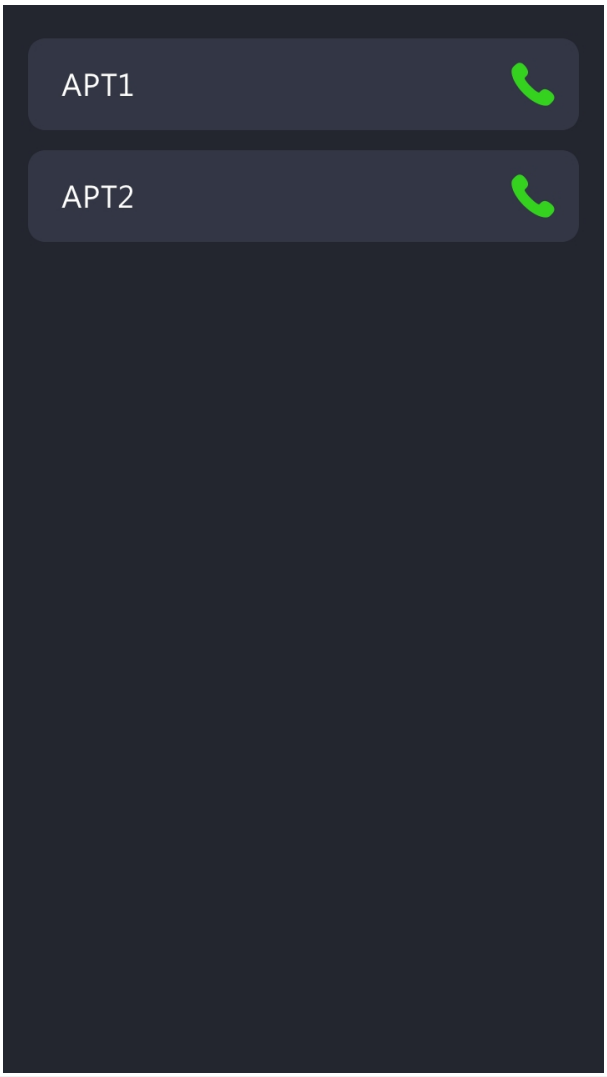
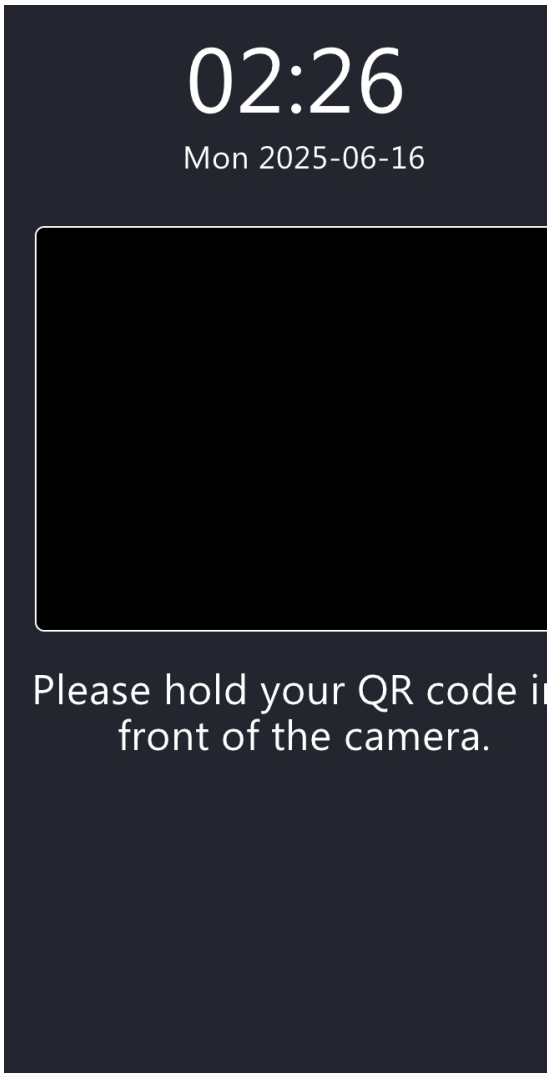
Home Screen Display

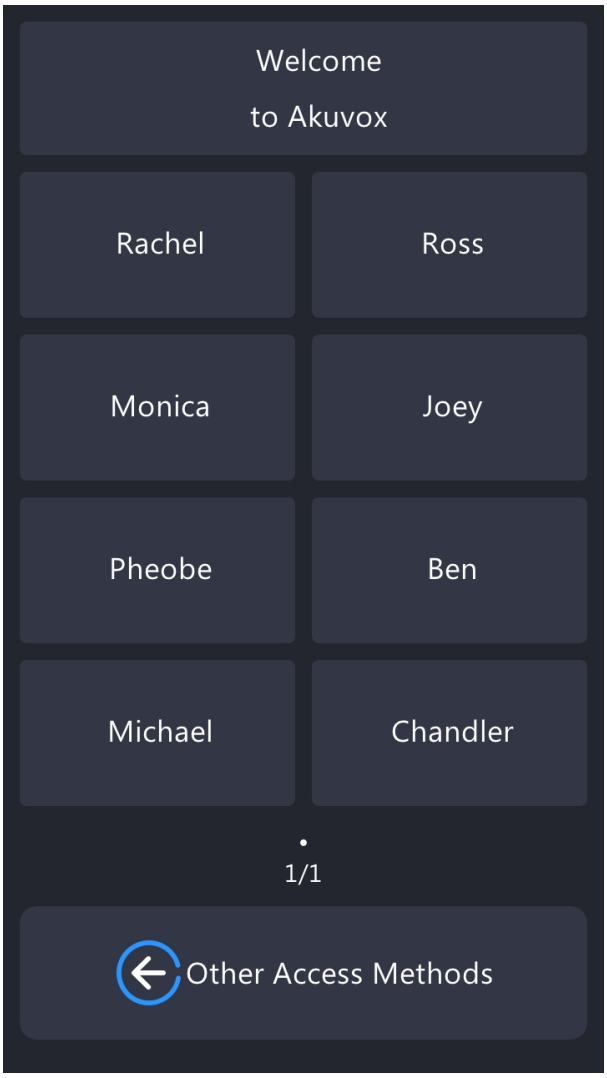
The device supports **Villa**, **Building**, **Speed Dial**, **QR code,** and **Two Column Speed Dial** themes. You can apply the desired theme to different scenarios.

Select the theme on the **Setting > Key/Display > Theme** interface.

- **Villa**: Display the Directory, PIN, and Call tabs vertically on the home screen.
- **Building**: Display PIN, Call, Directory, and Reception tabs and the facial recognition box on the home screen.
- **Speed Dial**: Display the contact for making a speed dial call.
- **QR Code**: Display the QR code scanning box.

Building Theme	Villa Theme
	
Speed Dial Theme	QR Code Theme

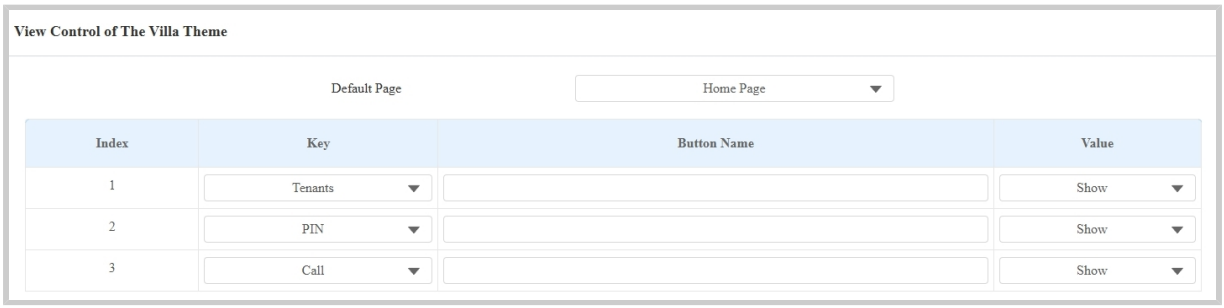
Building Theme	Villa Theme
	
Two Column Speed Dial	

Building Theme	Villa Theme
	

Villa Theme

You can select the functional tabs to be displayed and modify their names.

Set it up on the **View Control of The Villa Theme** section.



- **Default Page**: Select the homepage display type.
  - **Home Page**: The default display with three vertical round icons, Directory, PIN, and Call.
  - **Call**: Display the Dial screen as the homepage.
  - **Tenants**: Display the Contact screen as the homepage.
  - **PIN**: Display the PIN screen as the homepage.

> **Note**
>
> If you switch from Building mode to Villa mode and your previous home screen was set to Home Page, the three round icons for Tenants, PIN, and Call will be displayed. However, if your previous display type was Call, Tenants, or PIN, only the corresponding highlighted icons will appear at the top of the home screen instead of the three round icons for the Homepage.

- **Key**: Select the key to be displayed from Tenants, PIN, and Call.
- **Button Name**: Name the key. The name will not change the attribute of the key.
- **Value**: Display the key or not.

Speed Dial in Villa Theme

Speed dial is a feature that enables the creation of tabs or organized tab combinations to be displayed on the device's dial screen. By pressing these specific tabs, you can make swift calls without the need to enter any dial numbers.

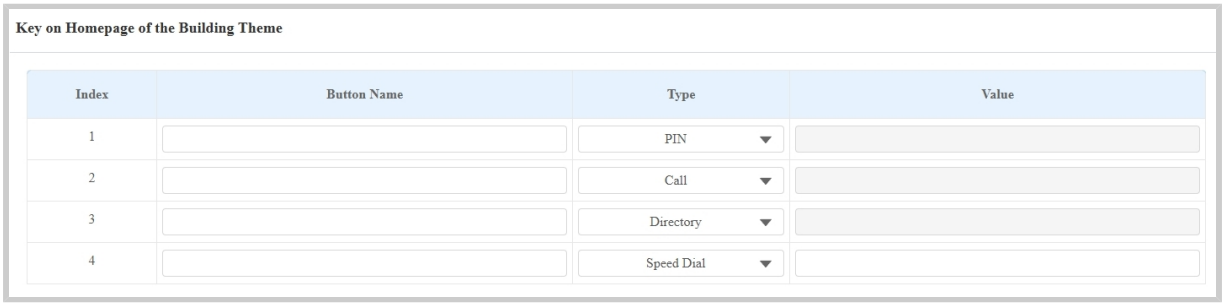
Set it up on the **Setting > Key/Display > Display Mode of Call Interface (Speed Dial)** interface.

Options	Descriptions
Standard	Display time and keypad.
Auto	Display all speed dial buttons set by the users.
1 Key	Display a single contract without the keypad.
1 Key + Keypad	Display a single dial button with the keypad.
2 Keys+ Keypad	Display up to 2 dial buttons with the keypad.
4 Keys+ Keypad	Display up to 4 dial buttons with the keypad.
8 Keys	Display up to 8 dial buttons without the keypad.
16 Keys	Display up to 16 dial buttons without the keypad.
64 Keys	Display up to 64 dial buttons without the keypad.

Building Theme

You can select the functional tabs to be displayed and modify their names.

Set it up on the **Key on Homepage of the Building Theme** section.

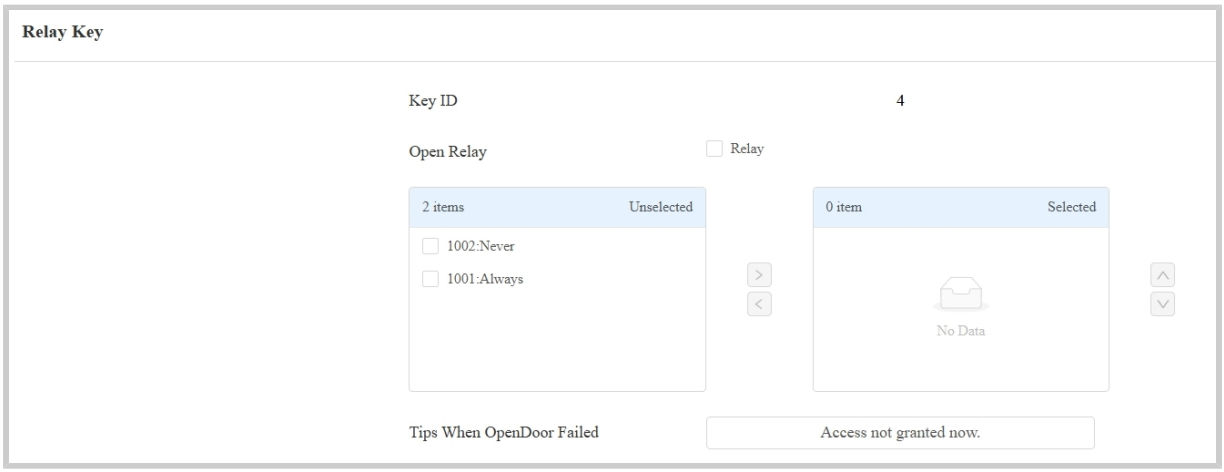


- **Button Name**: Name the key. The name will not change the attribute of the key.
- **Type**: Select the key type.
- **Value**: Set the value when **Speed Dial** is selected as the button type.
  - When the device is deployed on-premise, enter the local contact's IP/SIP number.
  - When the device is deployed on the SmartPlus Cloud, it follows the cloud contact display rules and displays cloud contacts and devices.

Relay Key Settings in Building Theme

This feature applies to the **Building** theme. When the **Relay** tab is selected to be displayed, you can set up which relay and when it can be unlocked.

Scroll to the **Relay Key** section on the **Setting > Key/Display** interface.



- **Key ID**: Specify which tab is set to be Relay.
- **Open Relay**: Check the relay to be triggered.
- **Schedule**: The relay can only be triggered within the schedule.
- **Tips When Open Door Failed**: The text prompt appears when the door opening fails.

Speed Dial in Building Theme

The Speed Dial feature allows users to make speedy calls by pressing the Speed Dial tab(Reception) without entering any numbers.

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

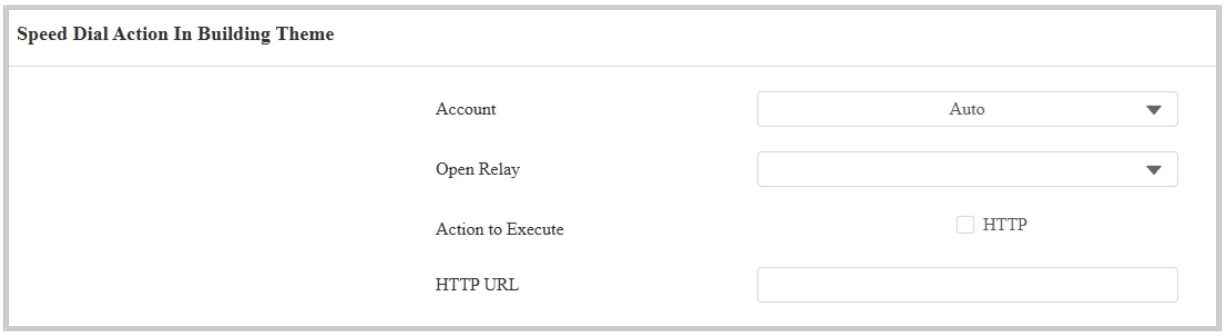
- **Speed Dial(Cloud)**: Display the speed dial number(s) updated from the SmartPlus Cloud that cannot be changed.
- **Group**:
  - **Disabled**:

    - When the device is connected to the Cloud, Disabled means the call will be made to other devices and the SmartPlus App, based on where it is installed.
    - When the device is deployed locally, the call will be made to the number you fill in the value field of the Speed Dial(Reception) key.
  - [Cloud Group Name]: The call will be made to all contacts in the group. The Cloud group name is the APT name.
- **Dial Out Forward**: When enabled, all outgoing calls from the device — regardless of call type (IP, SIP, Contact, Web Call, etc.) — will be redirected to the target number configured for the Reception key. If multiple numbers are configured, the first one will be used.
  - **Mode**: When Dial Out Forward is enabled, configure the schedule when the feature is working. You can also select **Auto Disable** and decide after how many hours the feature will be turned off.

Speed Dial Action In Building Theme

You can set up the reception tab in the Building or Multi-factor Authentication theme, with which users can make a call and open the door.

Set it up on the **Setting > Key/Display > Speed Dial Action In Building Theme** interface.

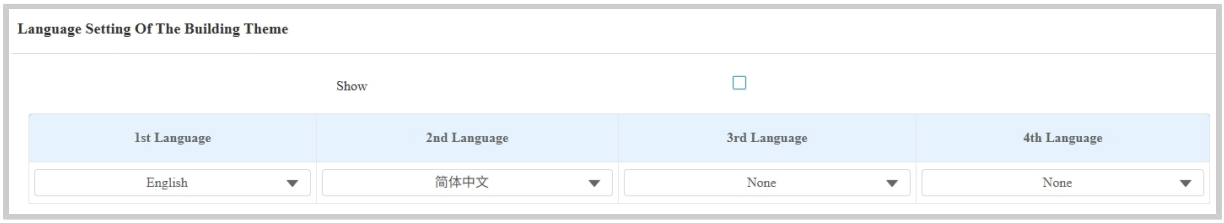


- **Account**: Select the account to make the call. It applies to the registered account. If both accounts are registered, Account1 is used when Default is selected.

- **Open Relay**: Select the relay to be triggered along with the call.
- **Action to Execute**: Set the action to be triggered with the call. 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 to perform certain actions. The format of sending the message is *http://HTTP server's IP/Message content*.

Language Setting Of The Building Theme

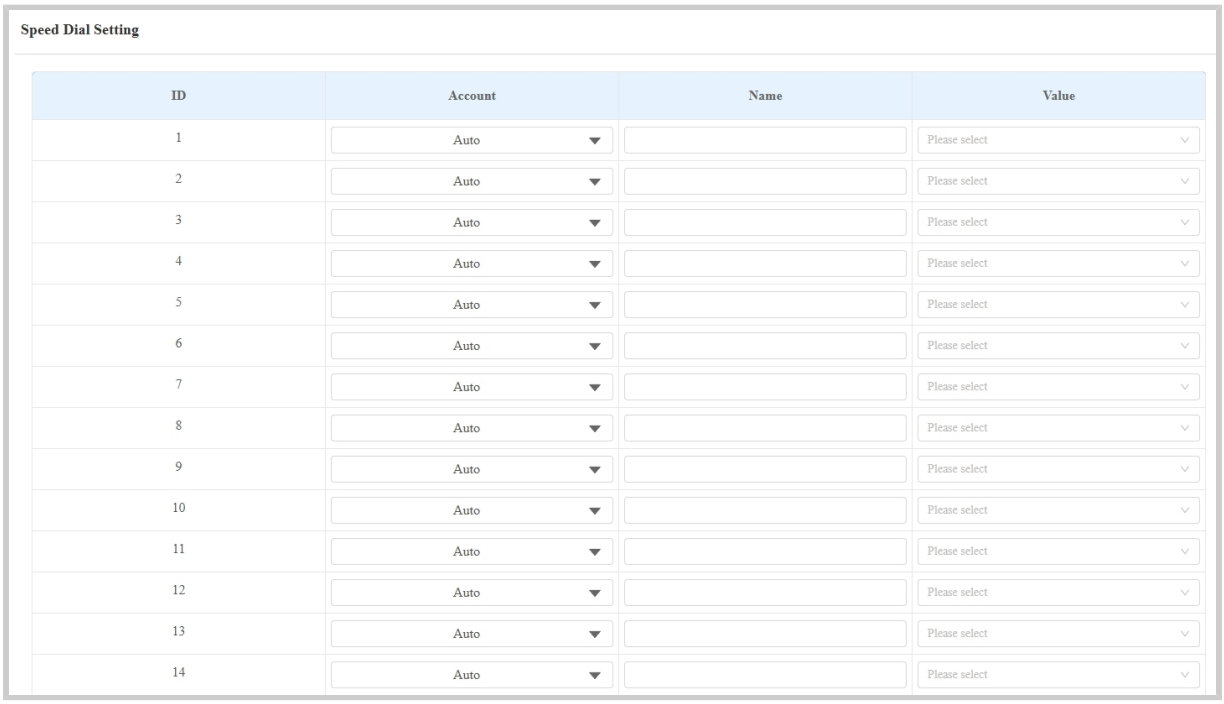
You can set up the language display in the Building or Multi-factor Authentication theme on the **Setting > Key/Display > Language Setting of The Building/Multi-factor Authentication Theme** interface.



- **Show**: When disabled, the language options will be hidden on the home screen.
- **Language 1-4**: You can select four languages to be displayed on the home screen.

Speed Dial Theme

You can set up 16 speed dial numbers at a maximum on the **Setting > Key/Display** interface.



- **Account**: Choose the account to make the speed dial call if it is a SIP call.
- **Name**: Name the contact.
- **Value**: Set the speed dial value.
  - When the device is deployed on-premise, enter the local contact's IP/SIP number.
  - When the device is deployed on the SmartPlus Cloud, it follows the cloud contact display rules and displays cloud contacts and devices.

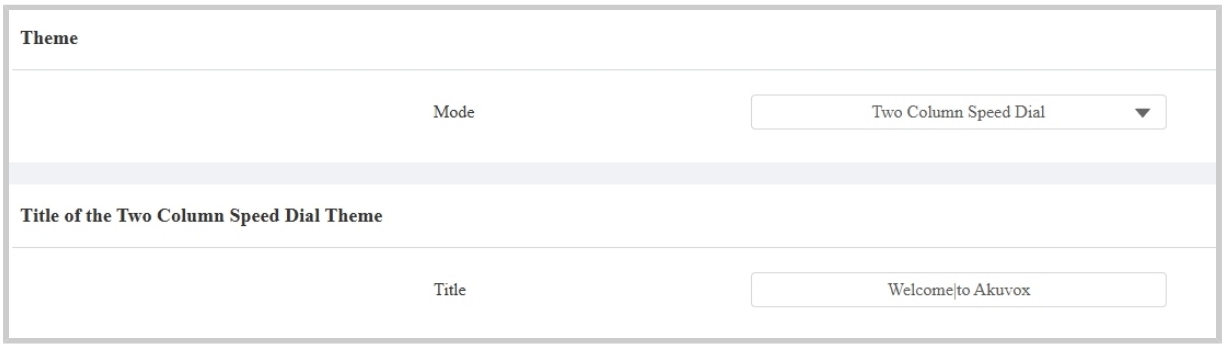
QR Code Theme

You can define the QR code scanning interval on the **Setting > Key/Display** interface.

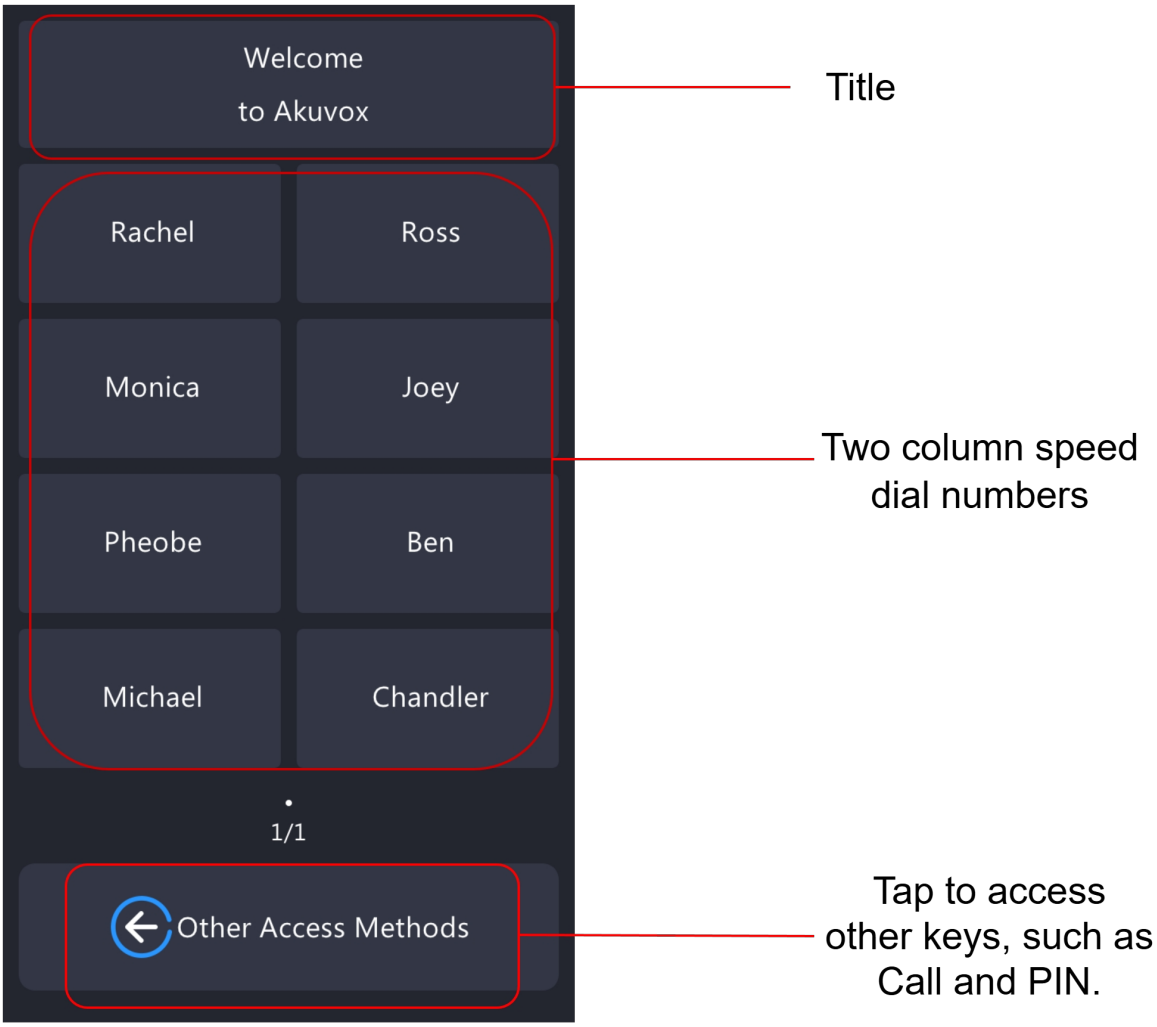
Two Column Speed Dial Theme

This theme allows you to display speed dial numbers in two columns, making it easy for visitors to call residents.

Set it up on the **Setting > Key/Display** interface.



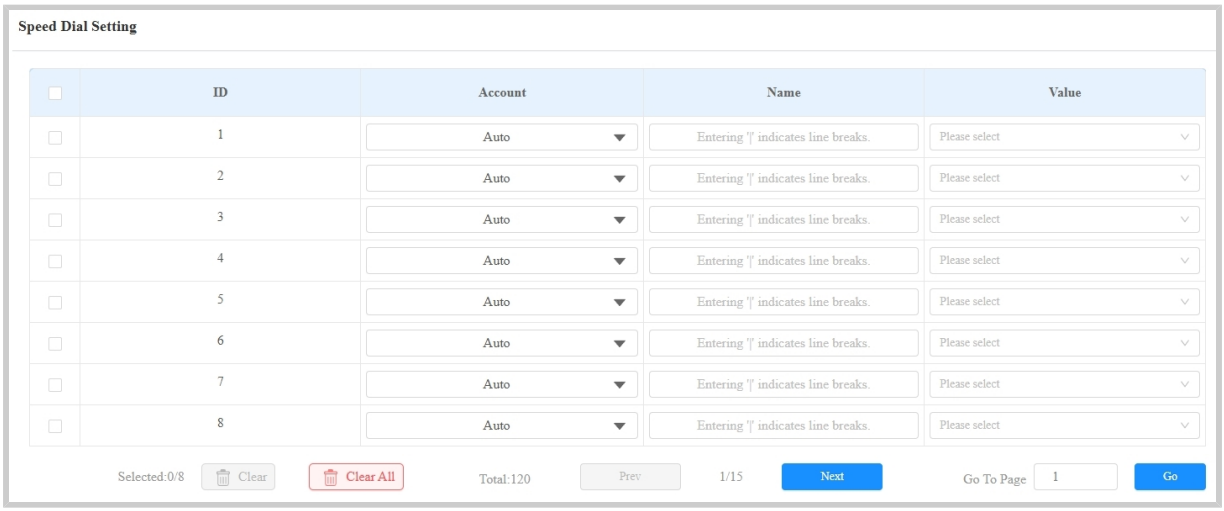
- **Title of the Two Column Speed Dial Theme**: Customize the title(63 characters at maximum) shown at the top of the screen, which can be the community name or building number. Entering '|' indicates line breaks.



Speed Dial Setting

You can add up to 120 speed dial numbers, with 8 numbers displayed per page.

Set up numbers on the **Setting > Key/Display** interface. Click **Prev/Next** to turn the page.

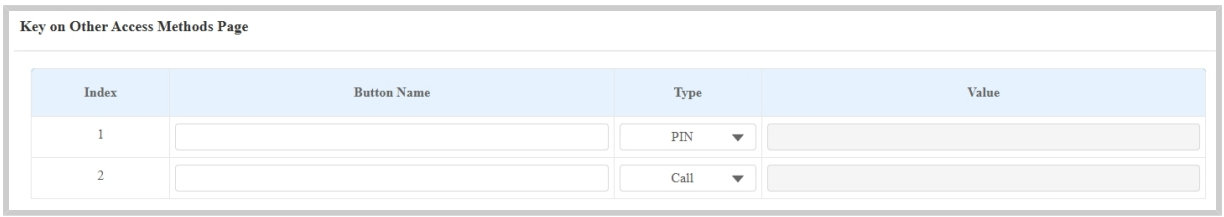


- **Account**: The account to make the call.
- **Name**: The contact name. Entering '|' indicates line breaks.
- **Value**: Set the speed dial value.
  - When the device is deployed on-premise, enter the local contact's IP/SIP number.
  - When the device is deployed on the SmartPlus Cloud, it follows the cloud contact display rules and displays cloud contacts and devices.

Key Display on the Other Access Methods Page

You can choose key(s) to display on the **Other Access Methods** page. This page simulates the Building theme page for other functions, such as PIN entry and door access.

Set it up on the **Setting > Key/Display** interface.



- **Button Name**: Name the key. The name will not change the attribute of the key.
- **Type**: Select the key type.

- **Value**: Set the value when **Speed Dial** is selected as the button type.
  - When the device is deployed on-premise, enter the local contact's IP/SIP number.
  - When the device is deployed on the SmartPlus Cloud, it follows the cloud contact display rules and displays cloud contacts and devices.

Return Timeout Setting

You can specify the inactivity duration after which the device will automatically return to the Two Column Speed Dial page from the Other Access Methods page.

Set it up on the **Setting > Key/Display** interface.

- **Enabled**: Disabled by default. Check to activate the feature.
- **Timeout**: Set the time(5~300 seconds).

Auto Scroll Setting

The Auto Scroll feature allows pages to switch automatically at a specified interval.

Set it up on the **Setting > Key/Display** interface.

- **Enabled**: Disabled by default.

- **Interval**: Sets the page switching interval, ranging from 1 to 60 seconds. The default value is 5 seconds.

Dial Key Order

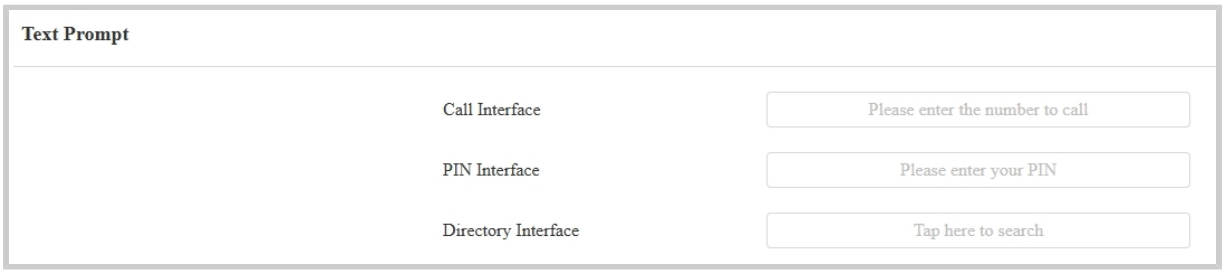
The device provides normal and scrambled keypad display options. Opting for the scrambled setting means that the arrangement of keys is randomized each time, enhancing security by preventing password spying.

Set it up on the **Setting > Key/Display > Keypad Display Mode Of PIN Interface**. The setting is available for Villa and Building themes.

Text Prompt Display

You can set up the text prompts on the Call, PIN, and Directory screens. The setting is available for the Building theme.

Set them up on the **Setting > Key/Display > Text Prompt** screen. The text prompt is 63 characters maximum in length.

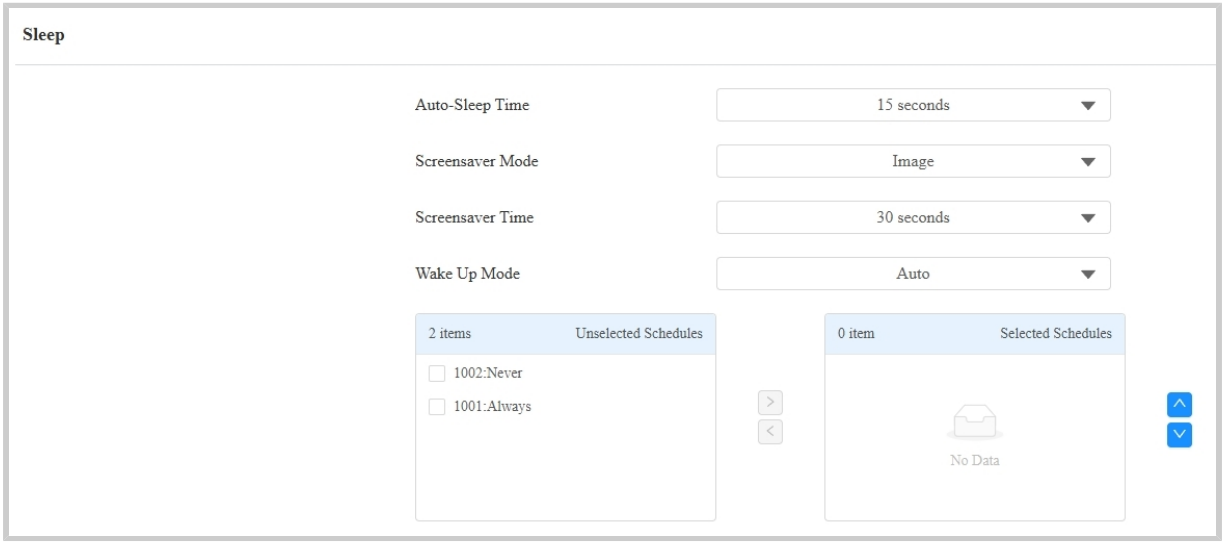


Screensaver Settings

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.

On the Web

Set up screensaver on the web **Device > LCD** interface.



- **Auto-Sleep Time**: The no-operation time for the device screen to turn dark or show the screensaver.
- **Screensaver Mode:**
  - **Disabled:** The screen will directly turn dark after the auto-sleep time.
  - **Image**: The picture uploaded will be shown as the screensaver.
- **Screensaver Time**: Set the screensaver duration from 5 seconds up to 30 minutes, or Forever. The screensaver starts when the device detects no operation or when no one is approaching.
- **Wake Up Mode**:
  - **Auto**: The screen can be awakened when someone approaches without it being touched. When selected, you can select a schedule to limit the setting's effective time.
  - **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.

- **Interval**: The time interval switching between two pictures.

> **Note**
>
> - The file should be in .jpg format with a 2M max size.
> - The recommended resolution is 800*1280.

Open Door Text Prompt

You can enable the open door text prompt for both door-opening success and failure. And you can also make the door phone display the user information when users use credentials such as RF cards for access.

Set it up on the web **Access Control > Relay > Open Door Text Prompt** interface.

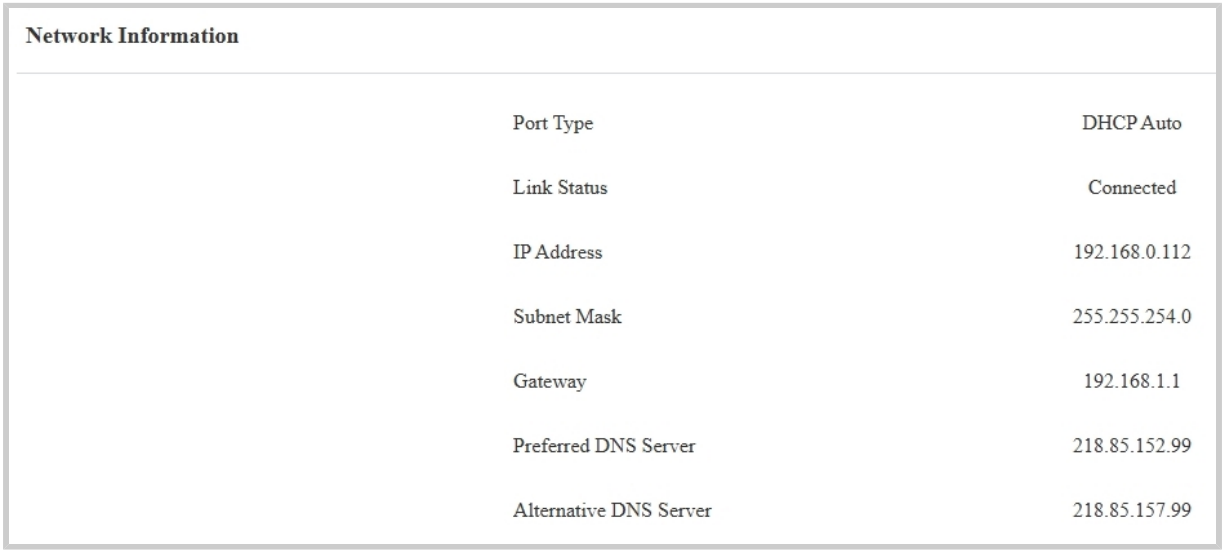
- **Open Door Outside Succeeded Text Prompt:** Display a text prompt after the door is opened by the device-supported access methods, except for the exit button.
- **Open Door Inside Succeeded Text Prompt:** Display a text prompt after the door is opened by pressing an exit button(the input is triggered).
- **Open Door Failed Text Prompt:** Display a text prompt after opening the door fails.
- **Display User Info**: Display the user information after facial recognition or card swiping. For example, if facial recognition succeeds, the text prompt “Access Granted” with the user ID and name will pop up on the device screen. If it fails, the text prompt “Access Denied” with “Stranger, Name: Unknown” will be displayed.

Network Settings

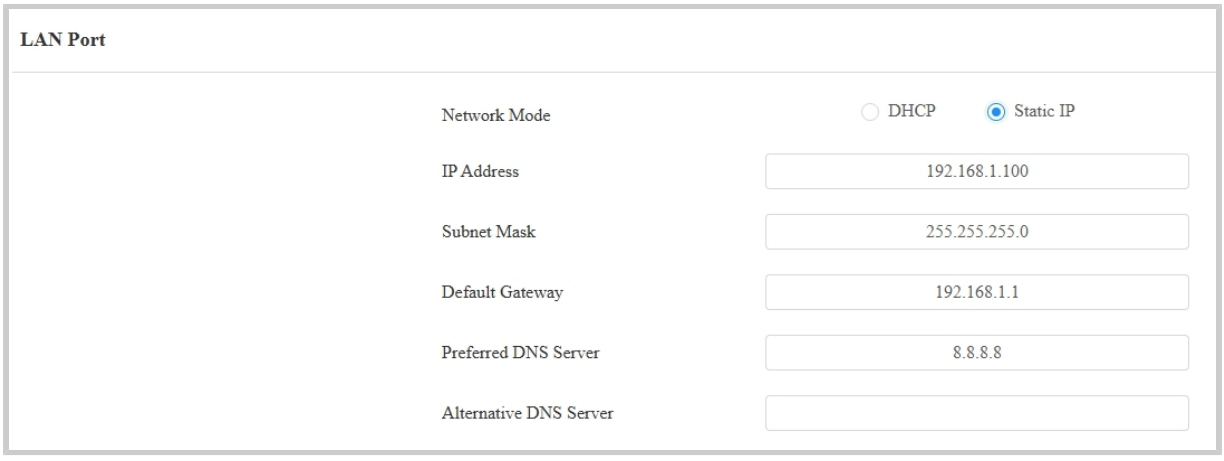
Device Network Configuration

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

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



Set the network connection on 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, you 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.

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. It can be used to call the device. Specify the device address by entering device location information from left to right: Community, Building, Unit, Floor, and Room in sequence.

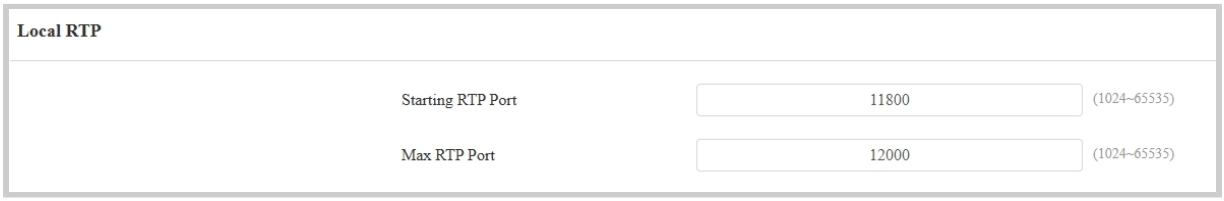
- **Device Extension**: Available for None server mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for None server mode.

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).

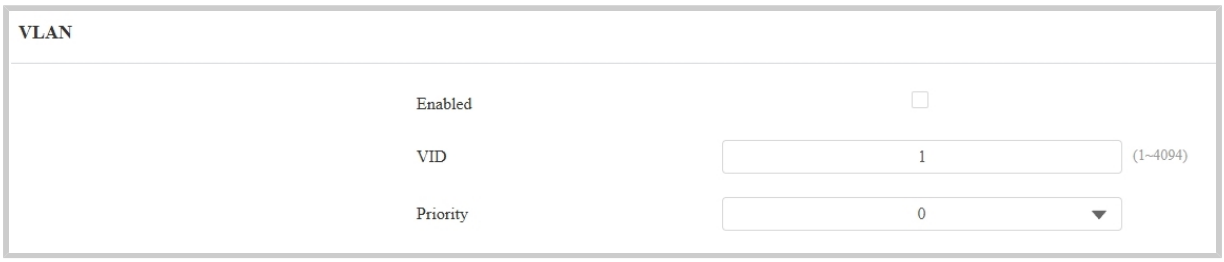
To configure SNMP, navigate to the web **Network > Advanced** interface.

- **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.

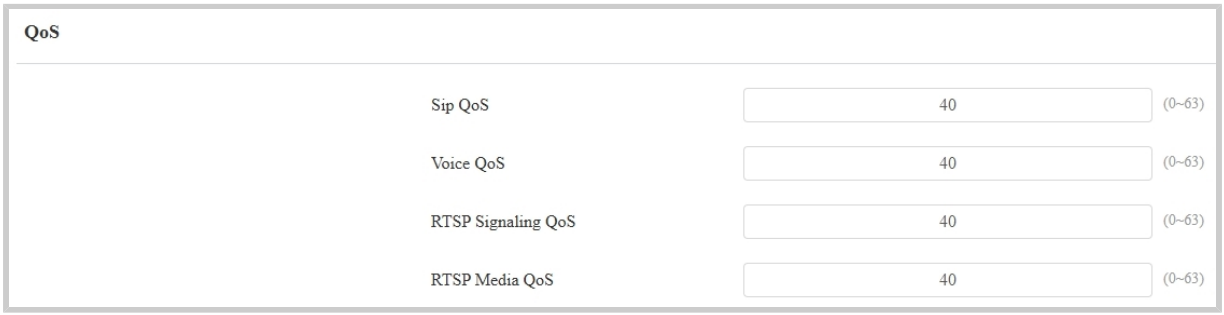


- **VID**: The VLAN ID for the designated port.
- **Priority**: The VLAN priority for the designated port.

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.

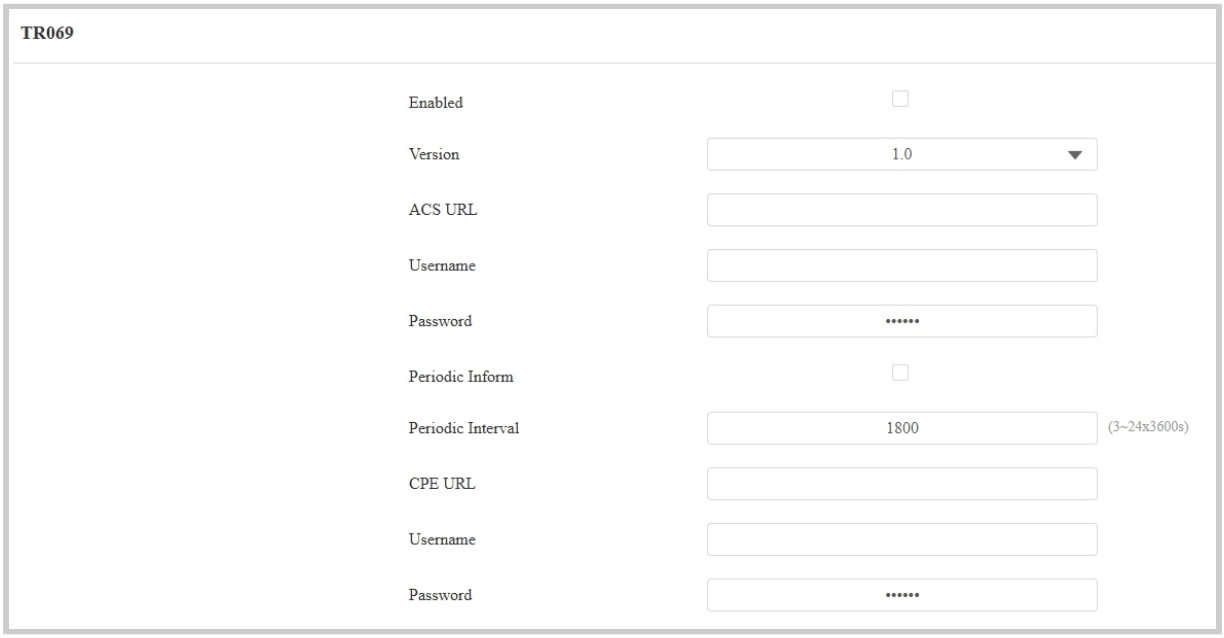


- **SIP QoS**: SIP QoS can be analyzed by registering an account and capturing SIP packets.
- **Voice QoS**: Voice QoS can be analyzed during a call by capturing and examining RTP packets.
- **RTSP Signaling QoS**: RTSP Signaling QoS can be analyzed using VLC and capturing RTP packets.
- **RTSP Media 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.

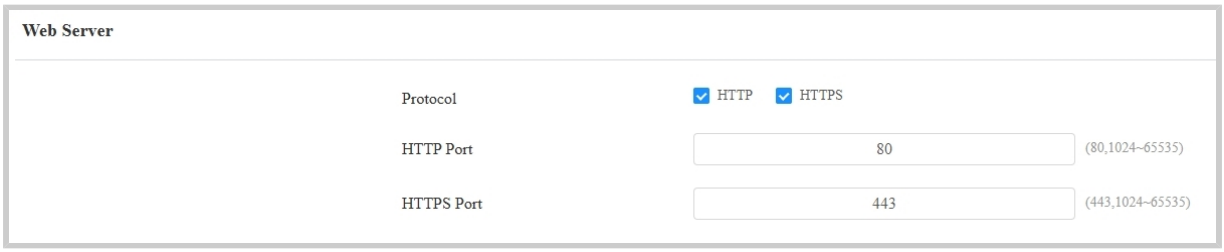


- **Version**: Select the supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE URL**: The URL address for ACS or CPE. ACS is short for auto-configuration servers on the server side, and CPE is short for customer-premise equipment, as the client-side device.
- **Periodic Interval**: The interval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



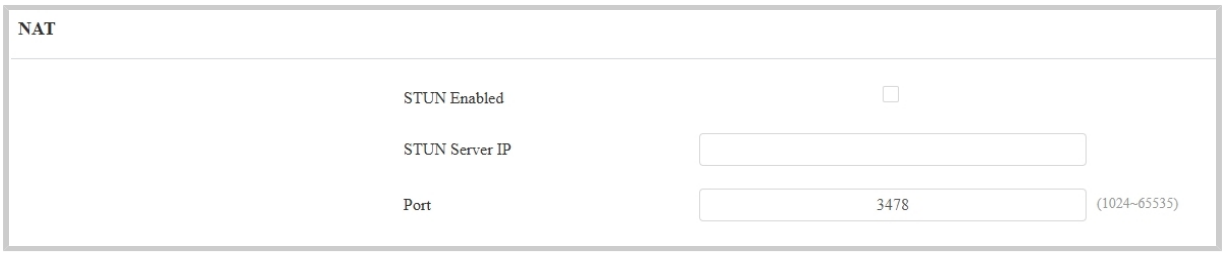
- **HTTP Port**: The port for the HTTP access method. 80 is the default port.
- **HTTPS Port**: The port for the HTTPS access method. 443 is the default port.

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 the WAN.

LTE Wireless Connection

The LTE module enables cellular network connectivity for the device in areas where wired networks are unavailable, particularly beneficial for installations in older buildings.

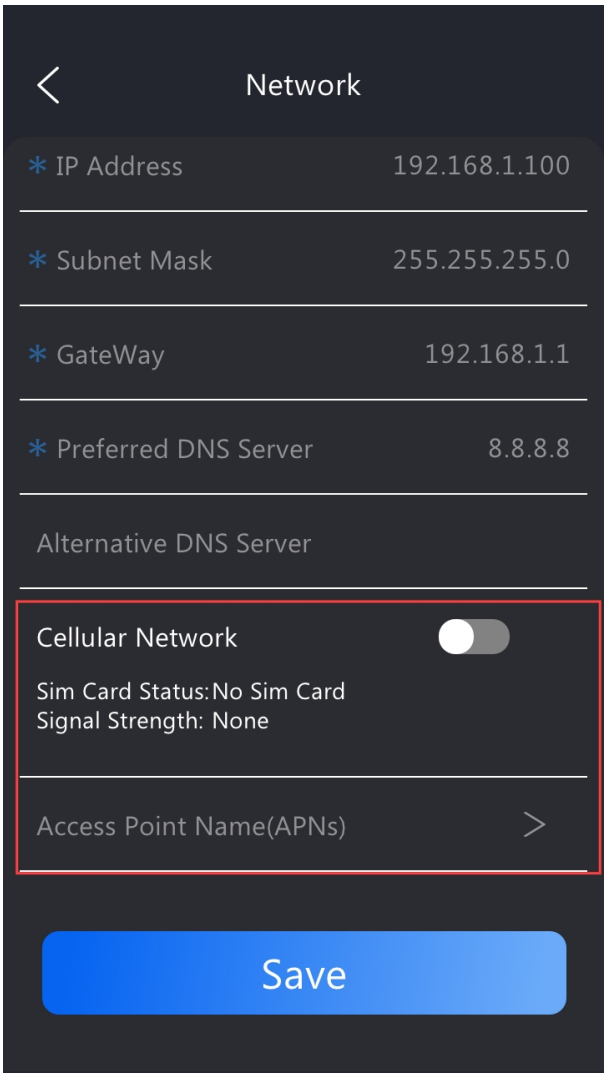
Only the S535 with the LTE module installed displays the settings.

Set this feature up on the **Network > Advanced** interface.

- **Signal Strength**: Indicate the network connection.
  - **None**: No SIM card inserted or the SIM card is not properly inserted, unable to detect signal.
  - **Weak**: The network signal is poor, typically when the signal strength is below -100 dBm.
  - **Fair**: The network signal is average, usually when the signal strength is between -90 and -100 dBm.

- **Good**: The network signal is good, generally when the signal strength is between -70 and -90 dBm.
- **Excellent**: The network signal is excellent, typically when the signal strength is between -50 and -70 dBm.

You can also set up the LTE connection on the **Setting > Network** screen.



- **Access Point Name(APNs)**: You can press this option to add new APNs. Fill in the information from your network provider.

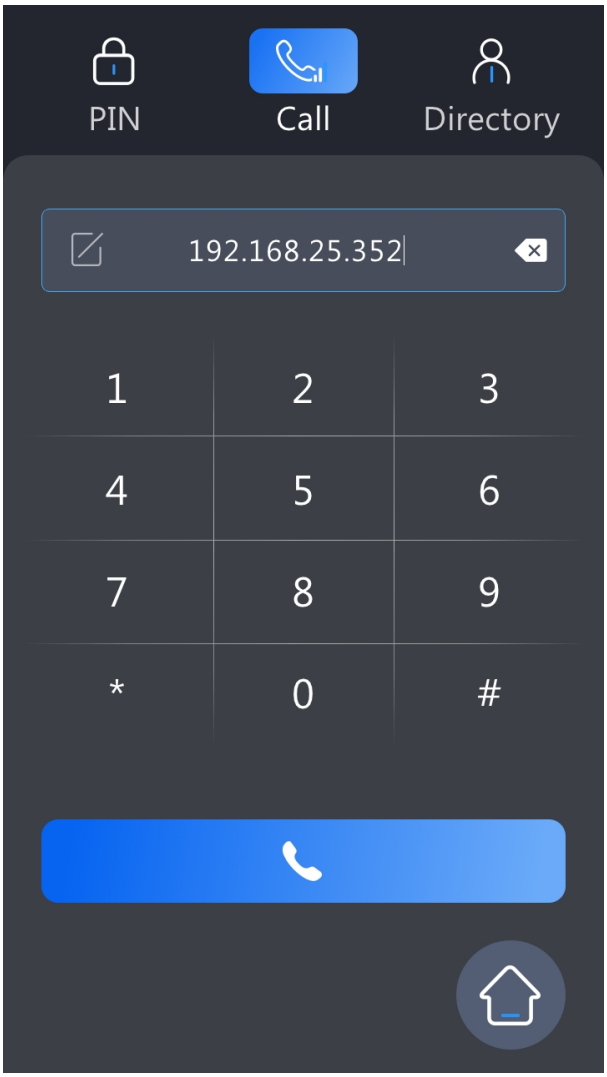
Intercom Call Configuration

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.

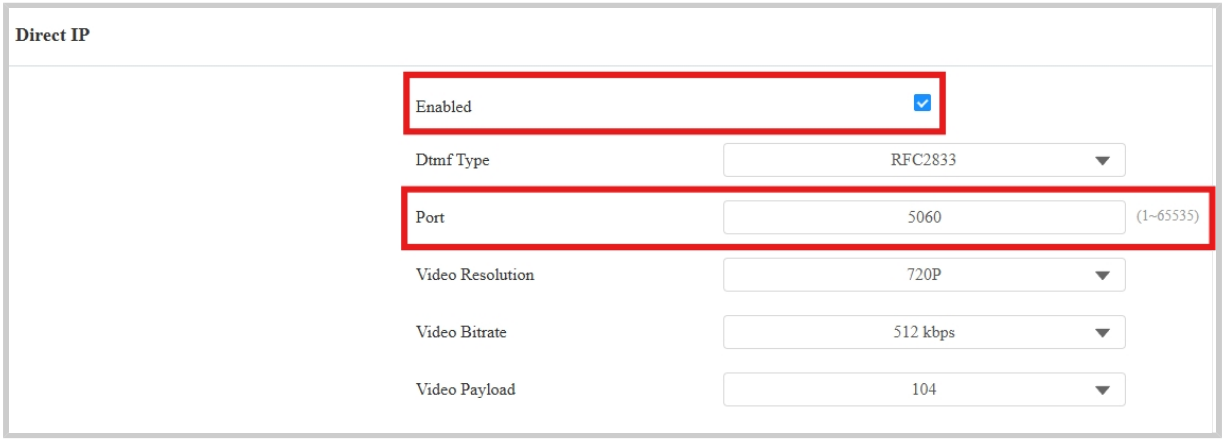
Make IP Calls

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.

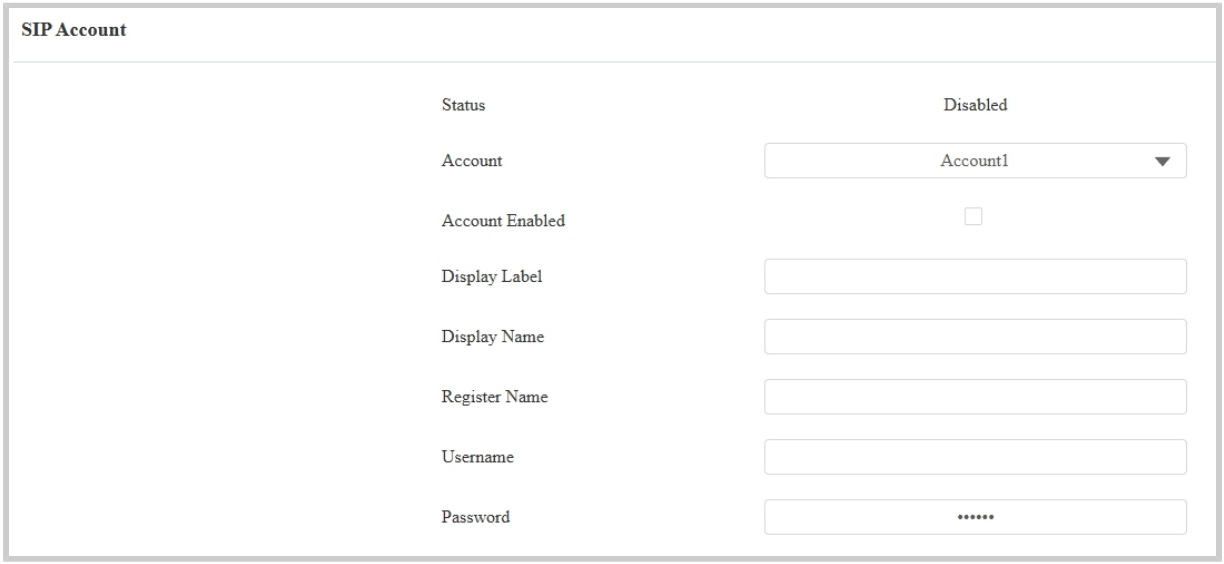
SIP Account Registration

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

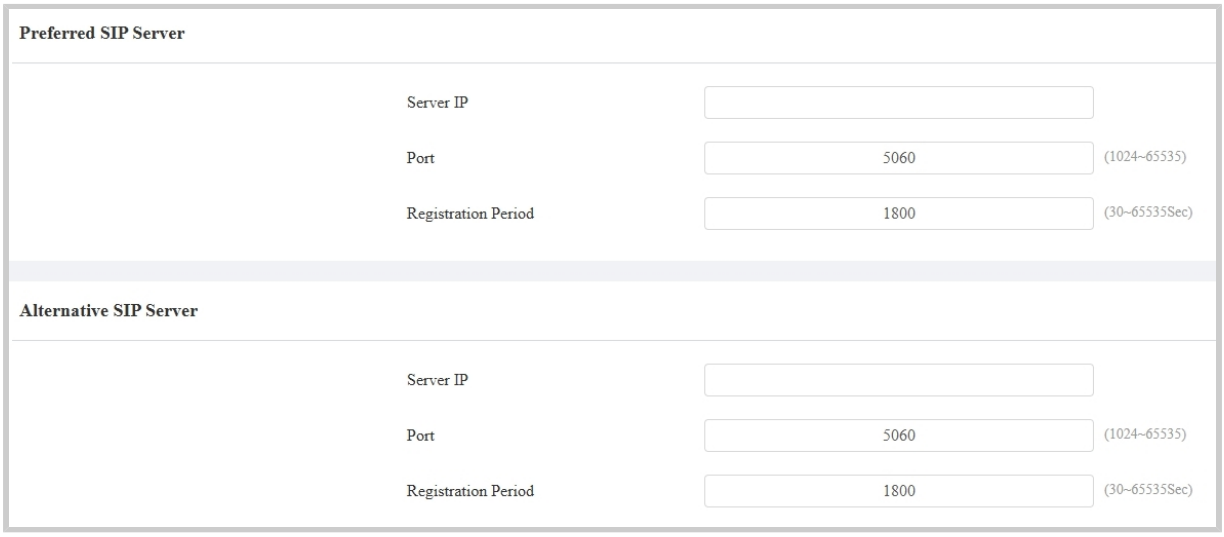
- For configuring contact call and dial plan, see here.
- When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

- **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.
- **Register Name:** Same as the username from the PBX server.
- **Username:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

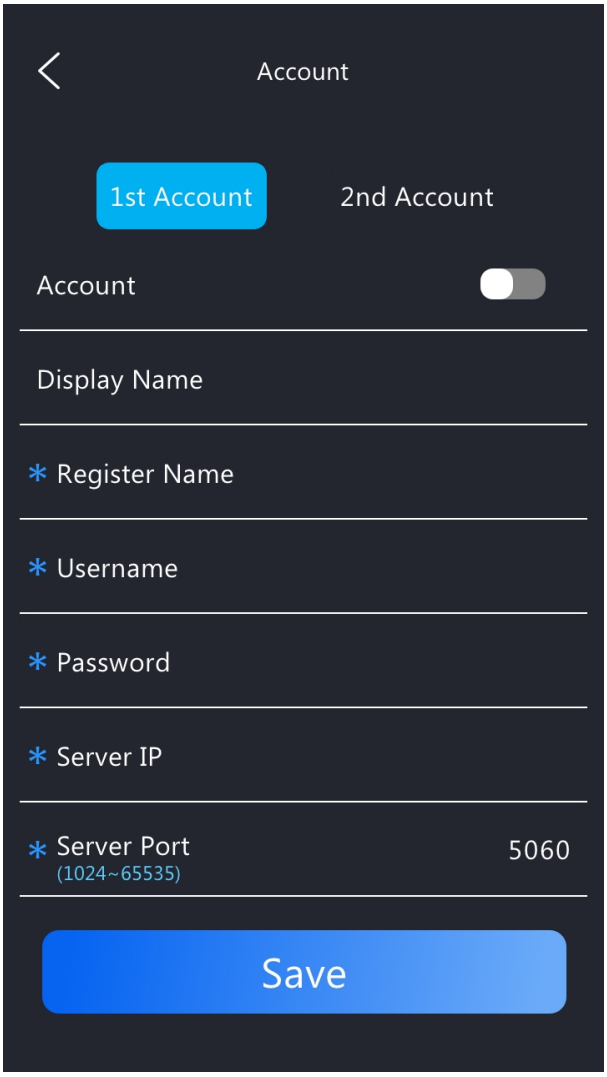
SIP Server Configuration

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.



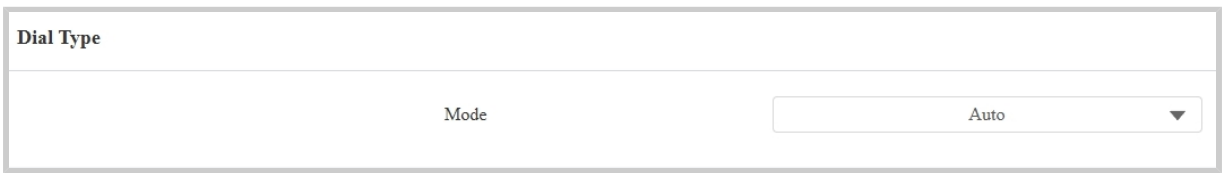
You can also register SIP accounts on the **Setting > Account** screen.



SIP Account Selection

The Dial Type feature decides the default account to make SIP calls. It applies to calls by pressing the contacts and entering the SIP numbers on the device's keypad.

You can select the default account on the **Intercom > Call Feature > Dial Type** interface.



- **Mode**:
  - **Auto**: The device will use the registered account to make SIP calls. If both are registered, Account 1 will be used by default.
  - **Account 1**: Calls can only be made to Account 1's contacts.
  - **Account 2**: Calls can only be made to Account 2's contacts.

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.

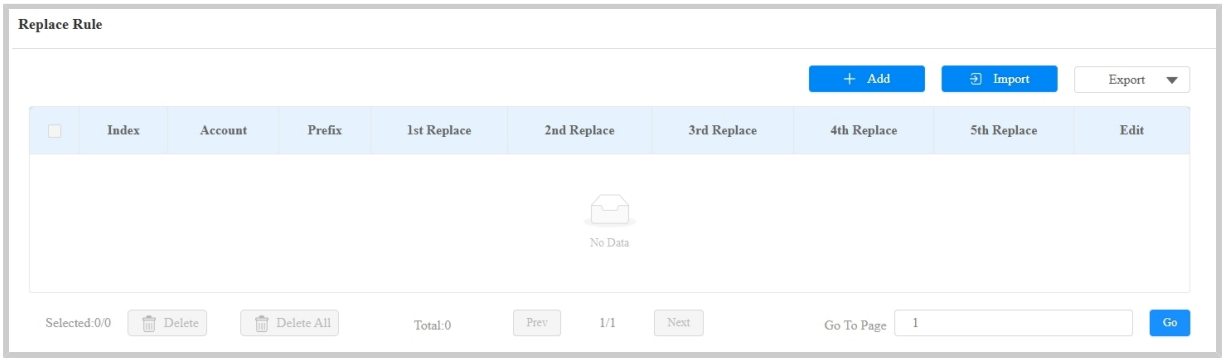
- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

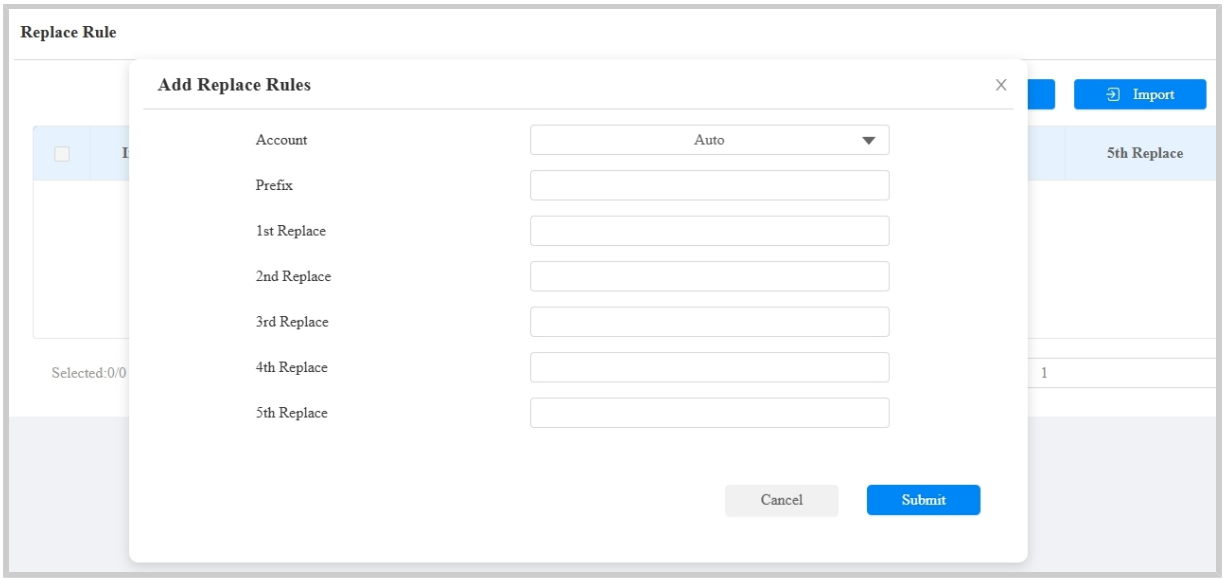
Call Settings

Quick Dial By Number Replacement

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.

Set it up on the **Intercom > Dial Plan** interface. Click **Add**.



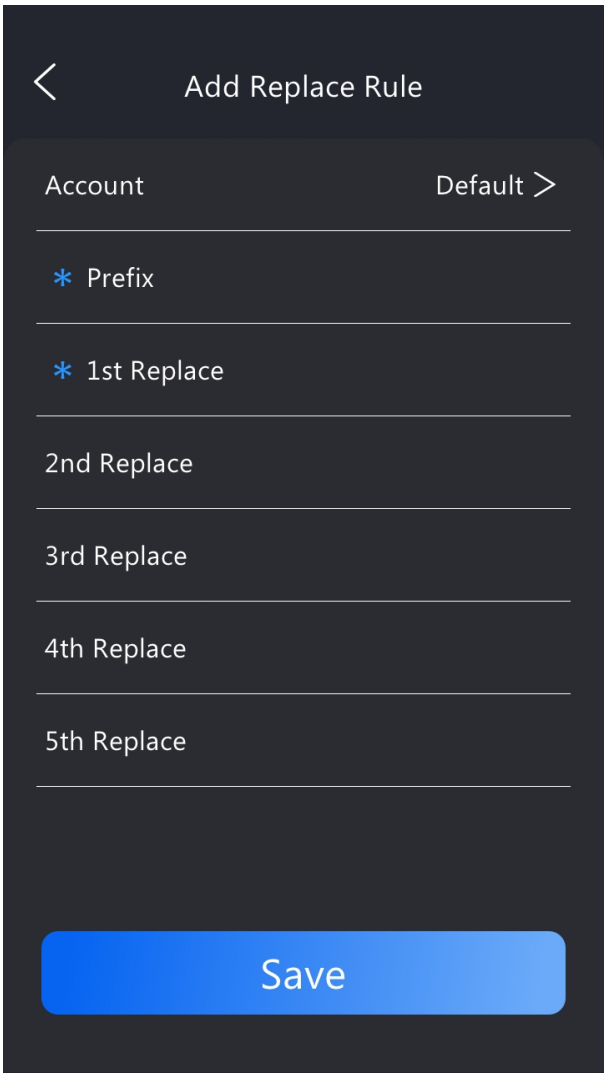


- **Account:** Select the dial-out account.
  - Auto: Dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.

- **Account 1/2:** Dial-out using the chosen account.

- **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.

You can also set up the dial plan on the **Setting > Replace Rule** screen.



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.

Set it up on the web **Intercom > Basic > Sequence Call** interface.

- **Time Out(Sec):** Specify the time limit for the call between two sequential call numbers. For example, if the time value is set to 10, the call that is not answered in 10 seconds will be ended automatically and transferred to the next call number in order.
- **When Refused:** Determine whether to call the next if a call was rejected by the previously called party.
  - Do Not Call Next: The sequence call will stop when the call is refused.
  - Call Next: The device will call the next number in order when the call is refused.

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 configure the action when a group call is refused on the web **Intercom > Basic > Group Call** interface.

- **When Refused**:
  - **End This Call Only**: The device will continue to call other numbers.
  - **End All Calls**: The call ends.

Maximum Call Duration

The device allows you to set up the call time duration for 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 device 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 device. If configured, the device will automatically terminate the call if no one answers the call within the preset time, whether it is incoming or outgoing.

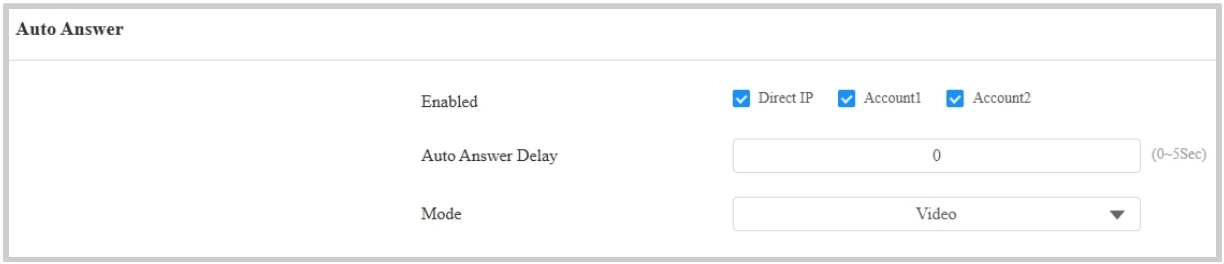
To configure maximum dial duration, navigate to the web **Intercom > Call Feature** interface.

- **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.

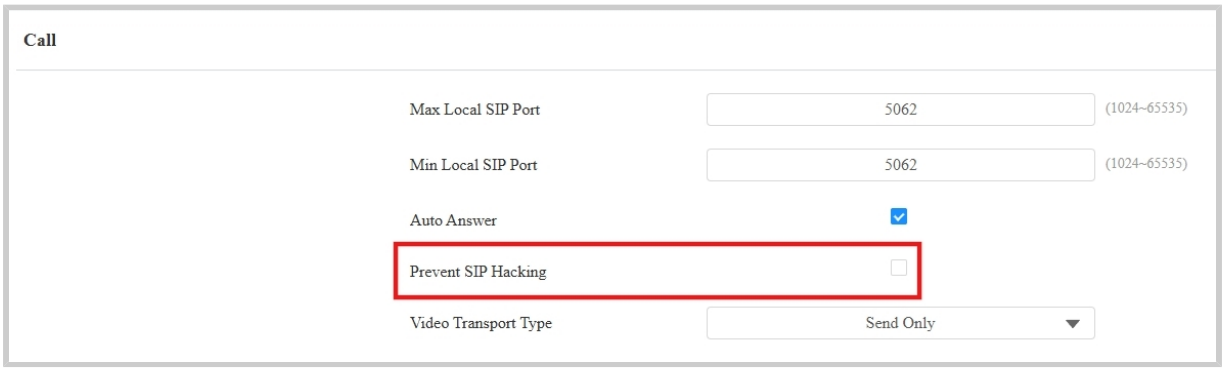
To configure it, navigate to the web **Intercom > Call Feature** interface.

- **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

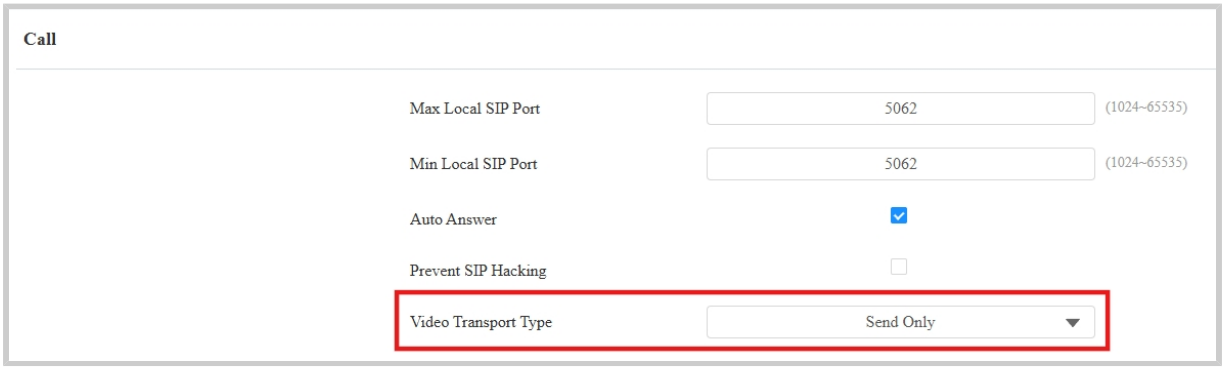
Internet phone eavesdropping is a network attack that allows unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls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

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



Video Transport Type

You can select the video transport type for SIP call preview on the **Account > Advanced > Call** interface. The setting does not apply to IP calls.



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

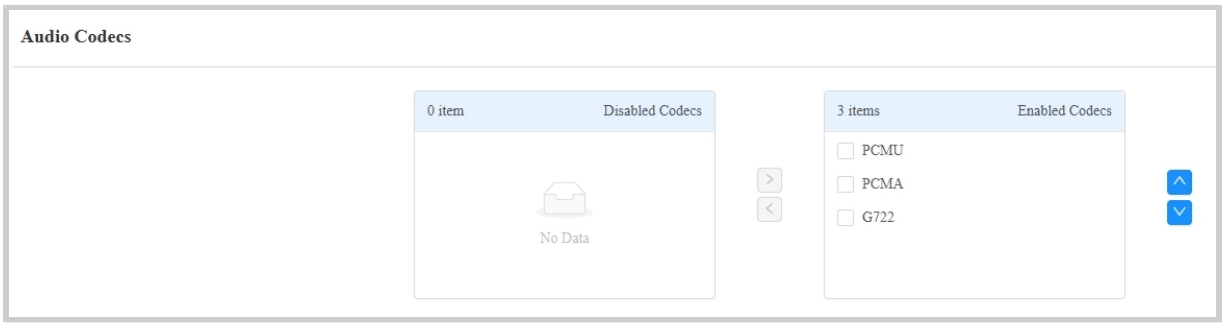
Audio & Video Codec Configuration

Audio Codec

The door phone supports three types of codecs (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each type of 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 **Account > Advanced > SIP Account** interface.

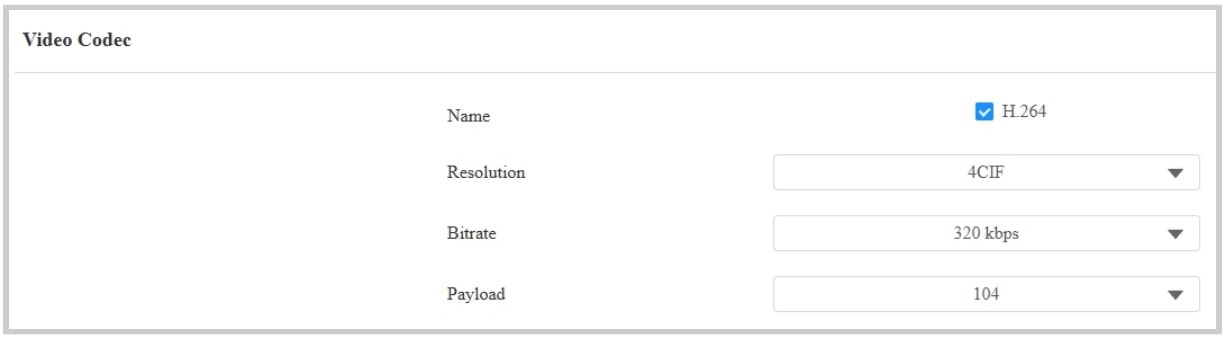


Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec

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

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

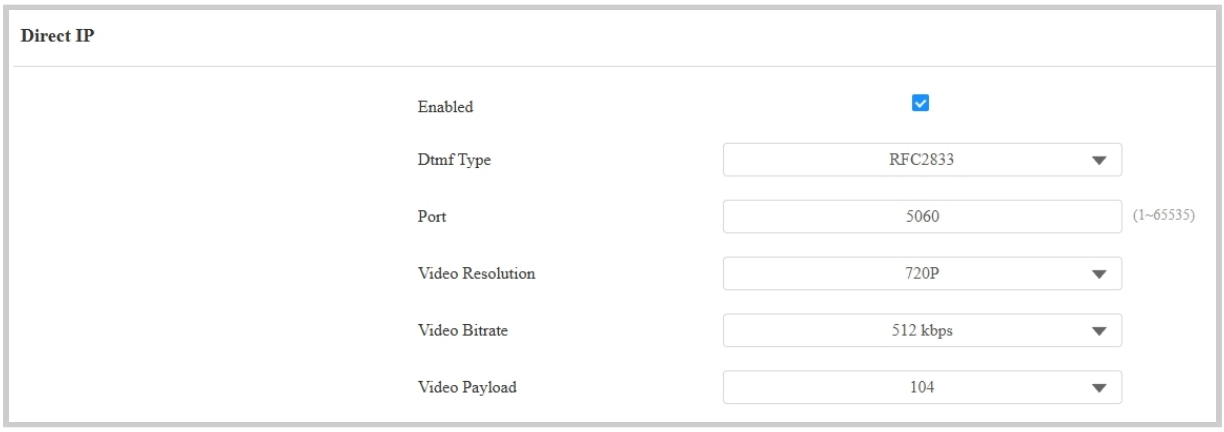


- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default resolution is 4CIF(704x576 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data is transmitted every second, and the clearer the video will be. The default code bitrate is 320.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for IP Calls

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

Set it up on the web **Intercom > Call Feature > IP Video Parameters** interface.



- **Video Resolution**: Select the resolution from the provided options. The default resolution is 720P(720 × 480 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The default bitrate is 512.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Contact Configuration

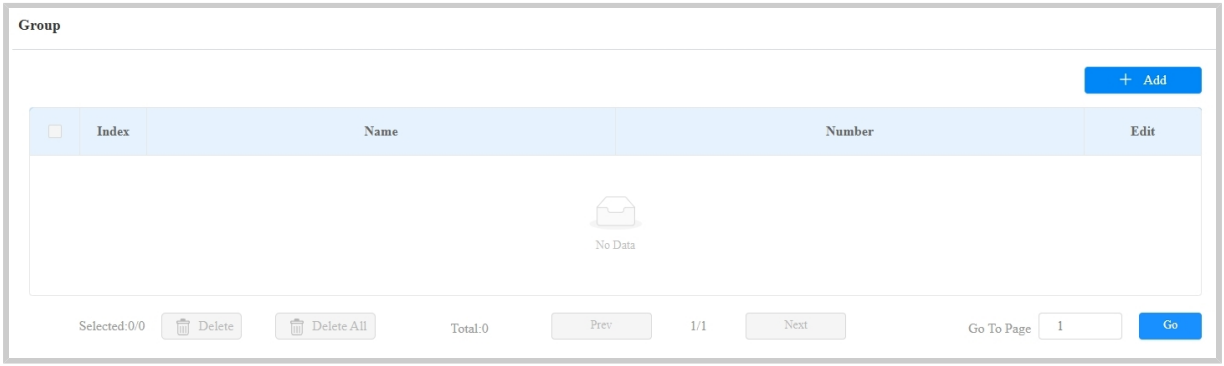
The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

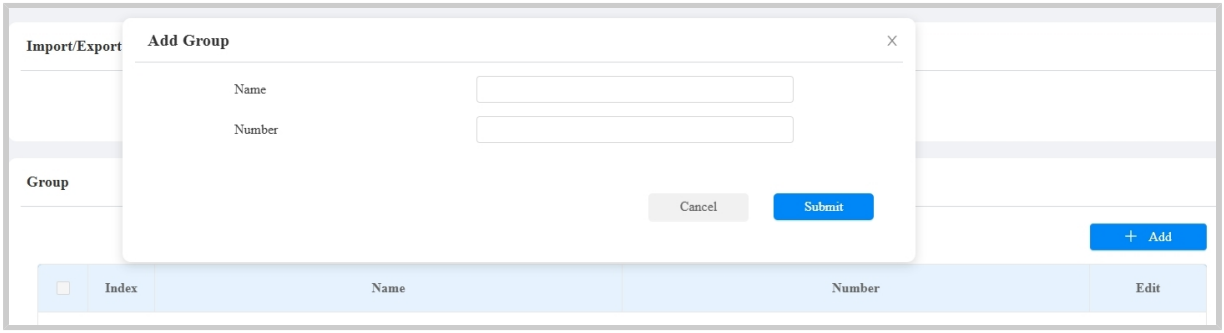
When the device is deployed on the SmartPlus Cloud, cloud contacts will display on the device web but not editable.

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.

To set it up, navigate to the web **Directory > User > Group** interface. Click **+Add** to create a group. You can also add groups on the **Setting > User > Group** screen. You can add 1,000 local groups.





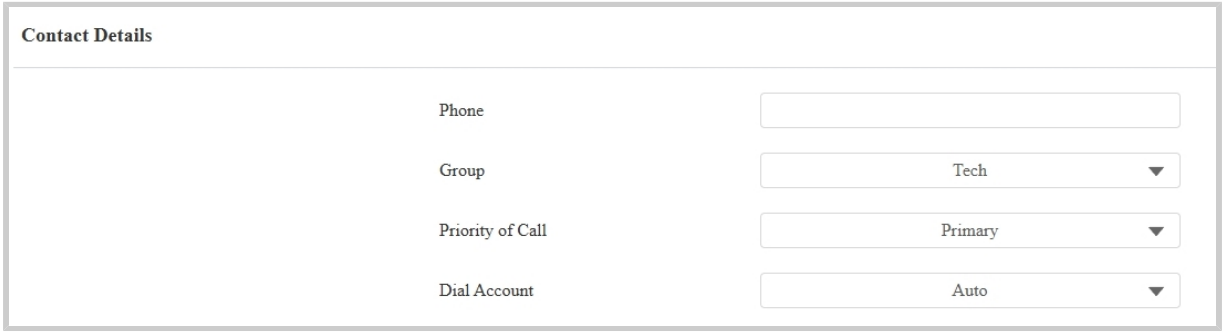
- **Name**: Name the group.

- **Number**: You can fill in the number of an intercom device to be called.

Set up Contact Details

You can add users' contact information when adding or editing a user on the **Directory > User** interface. The users added will be displayed on the device's Directory screen.

Click **+Add** to add a user or click to modify a user. Scroll to the **Contact Details** section.

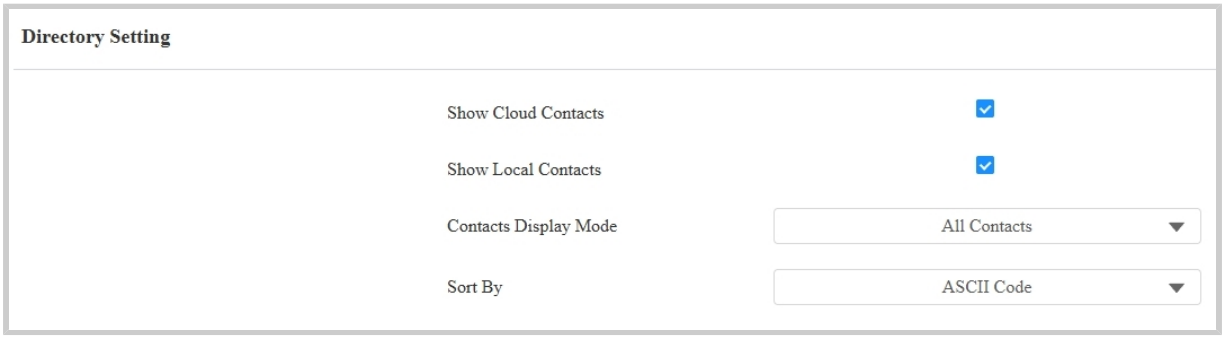


- **Phone**: The IP or SIP number.
- **Group**: Assign the contact to the Default, Hidden Contact, or a self-created group.
  - **Priority of Call**: When assigning the contact to a self-created group, set the priority of the call among three options: Primary, Secondary, and Tertiary. For example, if you set the priority of a 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 in the same contact group when someone presses on the contact group to make a group call.
- **Dial Account**: Select the account to make a call to the contact.

Contacts 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.



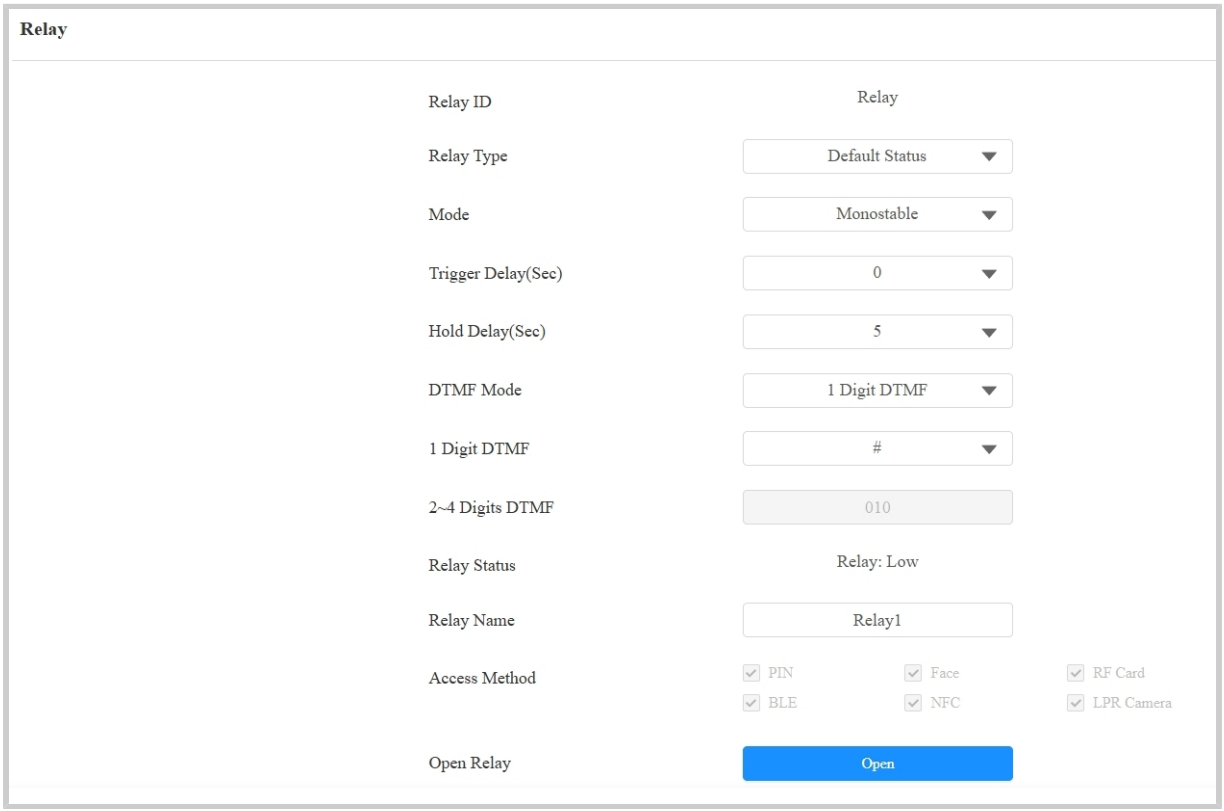
- **Show Cloud Contacts**: The contacts synchronized from the SmartPlus Cloud can be displayed.
- **Contacts Display Mode**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only:** Display contact groups. Press the desired group on the device screen to make a group call.
  - **Contact Display by Group:** Display contacts by groups. Press the group, and users can see the contacts in it.
  - **Do Not Display Contacts**: Neither contacts nor groups will display.
- **Sort By**:
  - **ASCII Code** lists contacts by their names in the sequence of the ASCII code.
  - **Room No.** lists contacts according to their room numbers.
  - **Import** lists contacts 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 calls.

Relay Settings

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 and DTMF for the door access on the web **Access Control > Relay** interface.



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

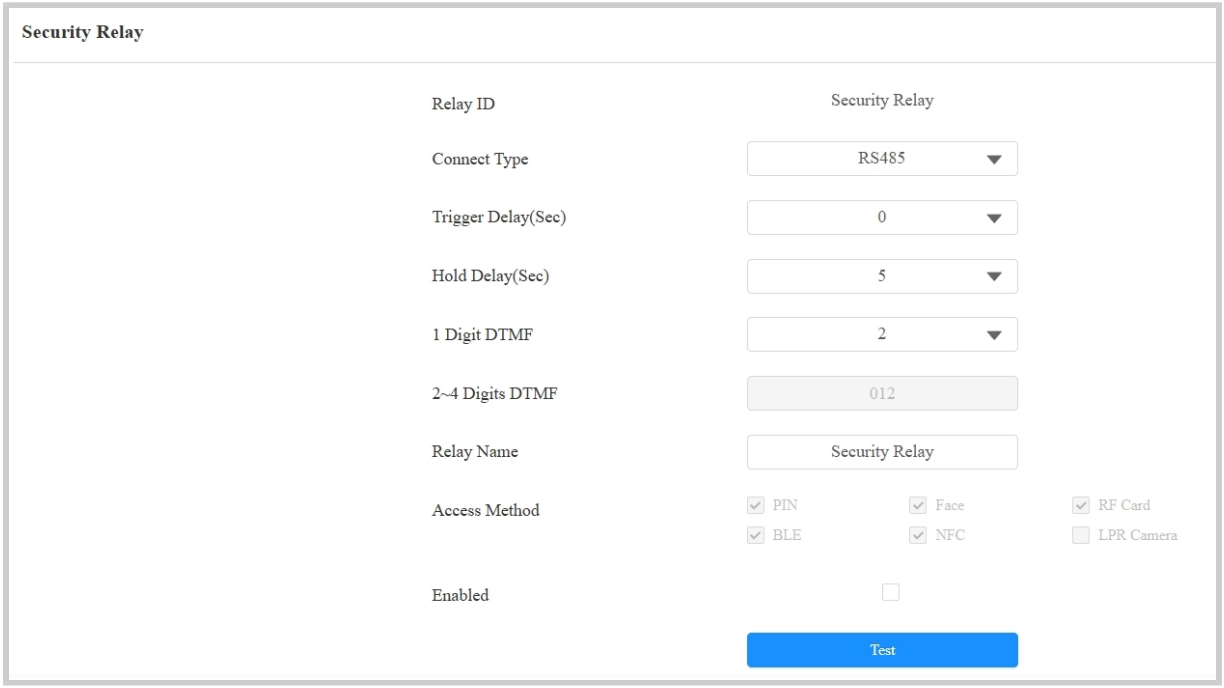
  - **Invert Status**: A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.
- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **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 open 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 open 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.

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**: It is RS485 by default.
- **Trigger Delay (Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open 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.

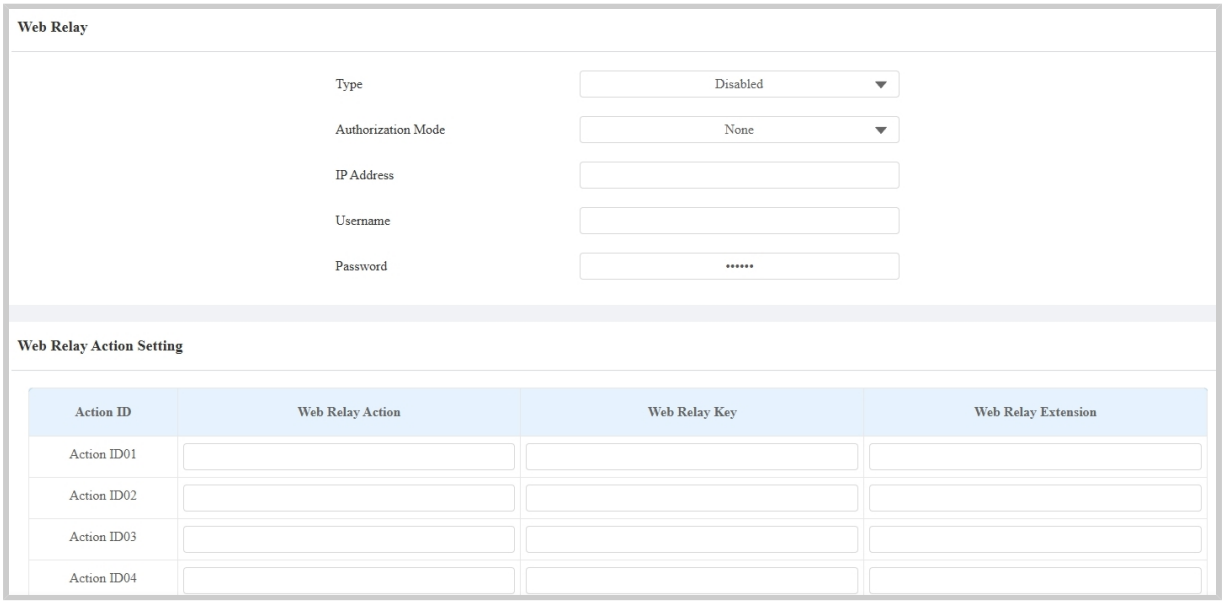
> **Note**
>
> When connecting the device to an SR01 via RS485, you need to select the RS485 mode as **Others** on the **Device > RS485** interface.

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.
- **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.

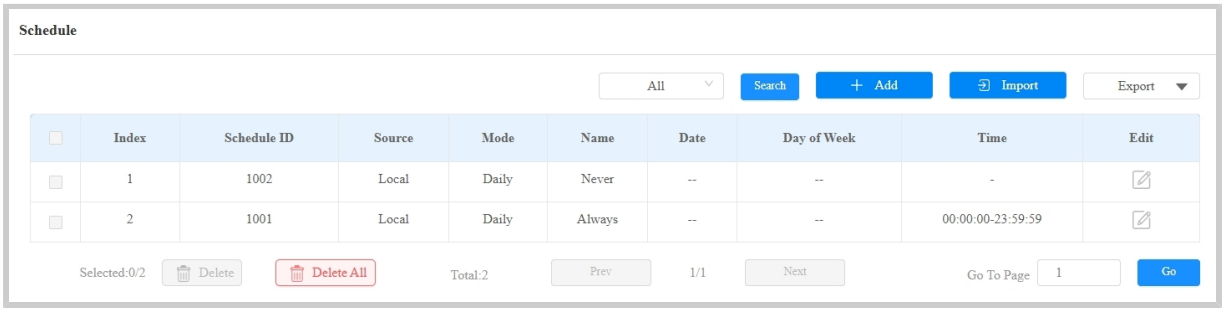
Access Control Schedule Management

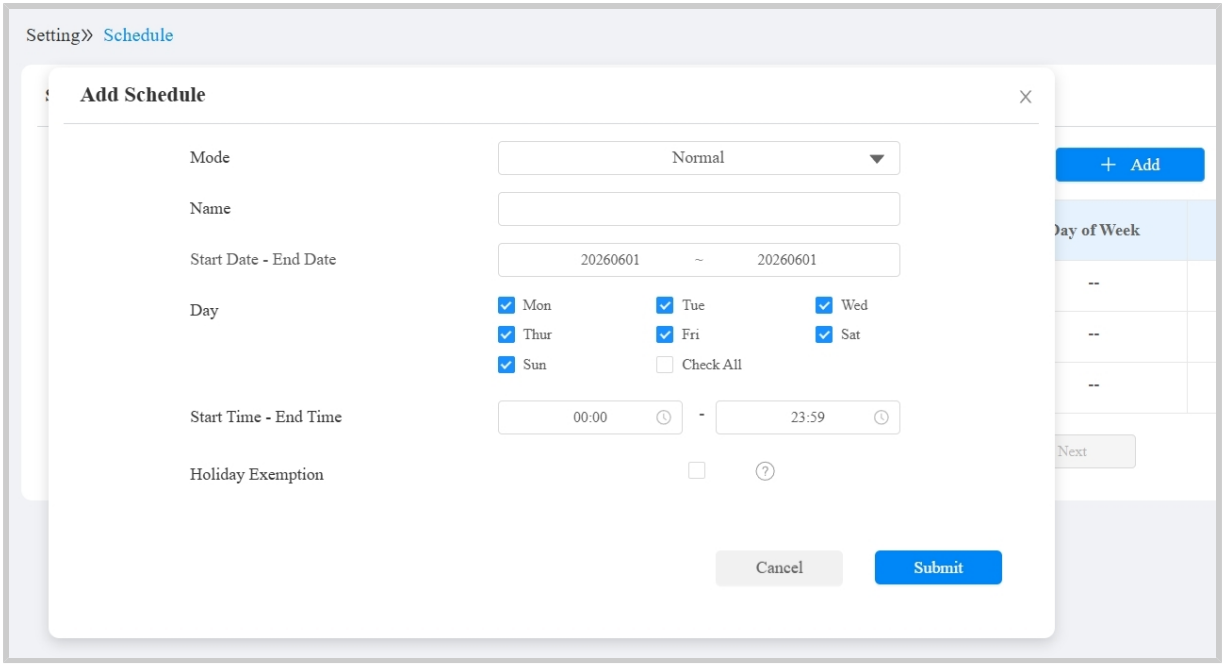
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create a Door Access Schedule

You can create 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.



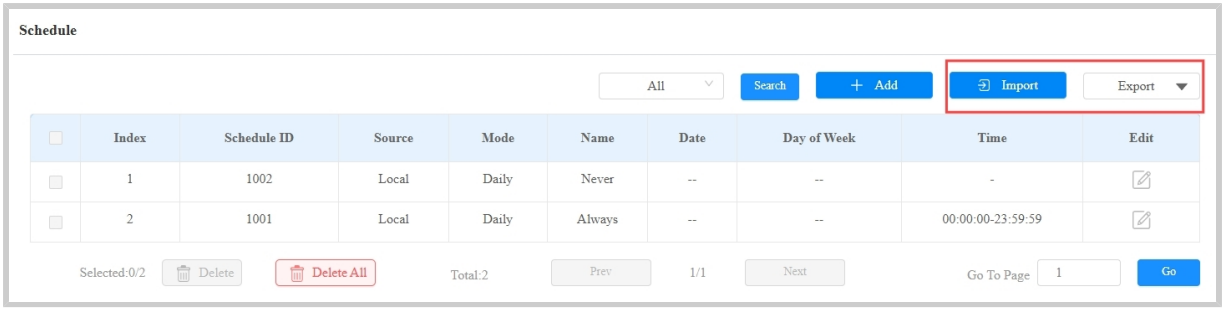


- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long-term schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Name**: Name the schedule.
- **Holiday Exemption**: The holiday schedule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

Import and Export Door Access Schedule

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.

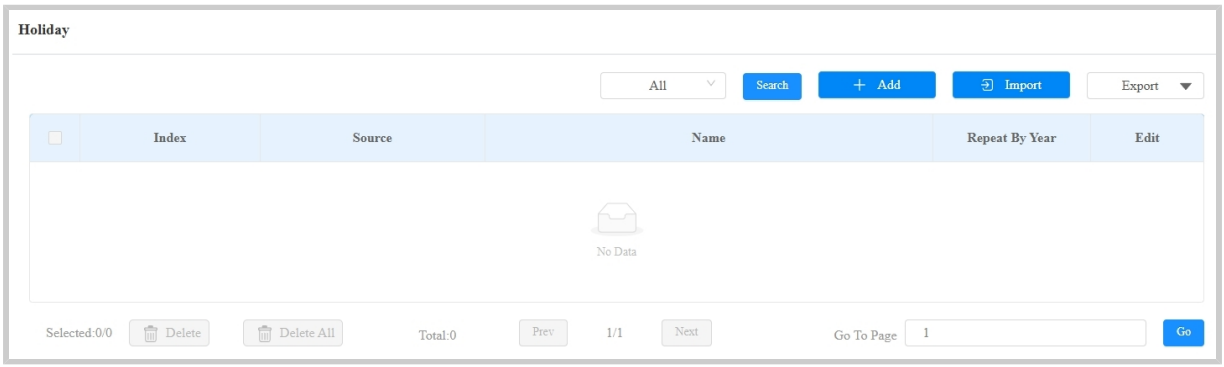


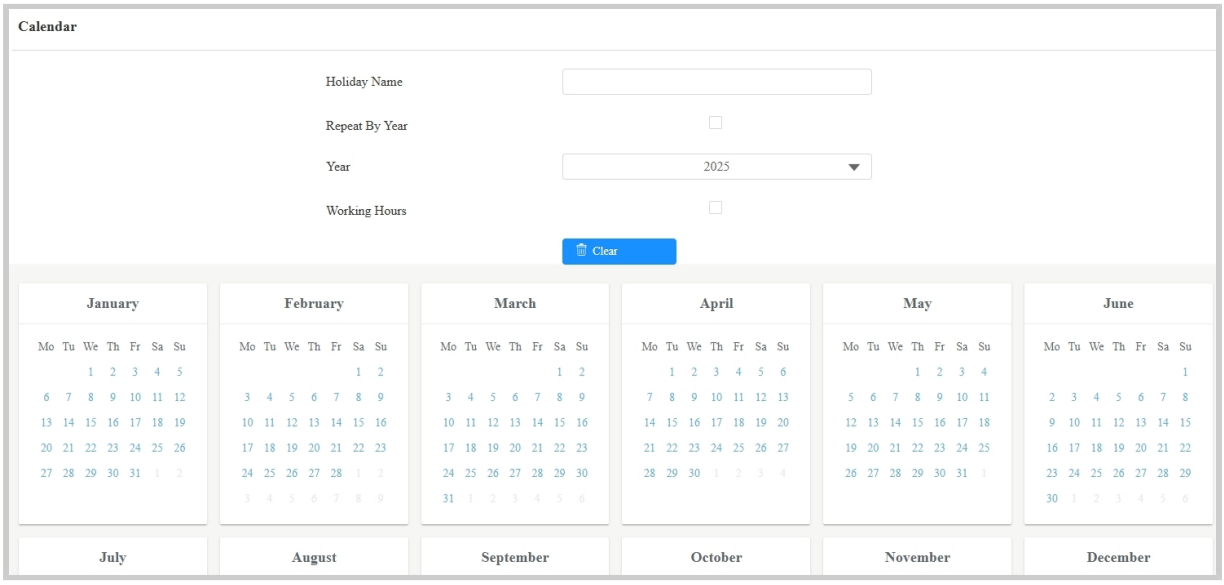
> **Note**
>
> The imported/exported file is in .xml format.

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.



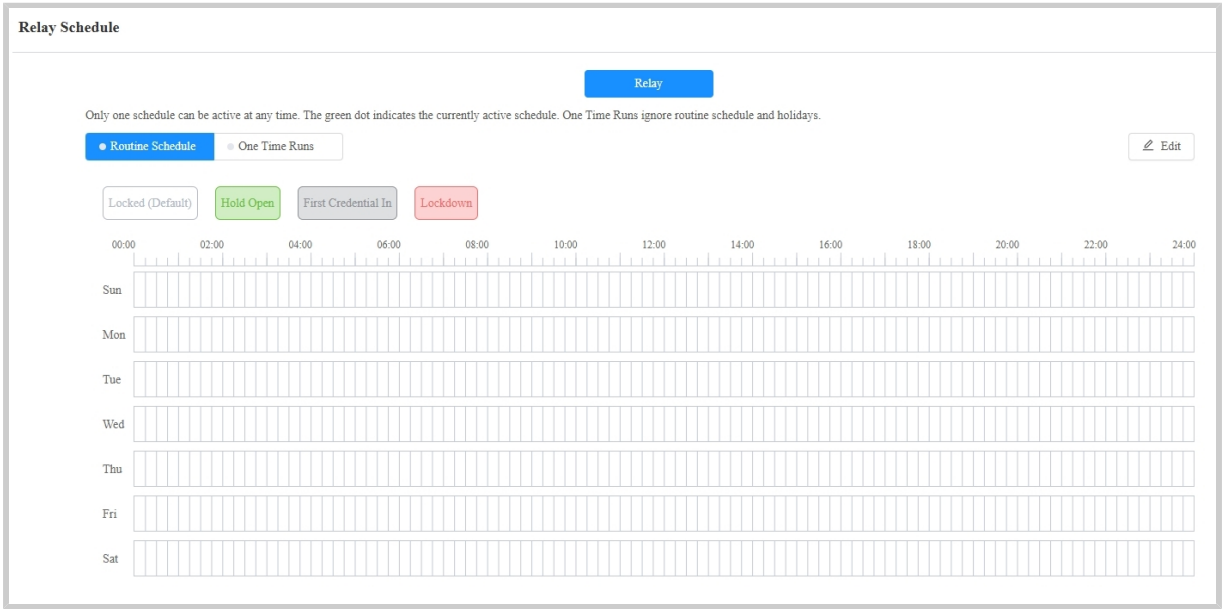


- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

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.



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

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

Door-opening Configuration

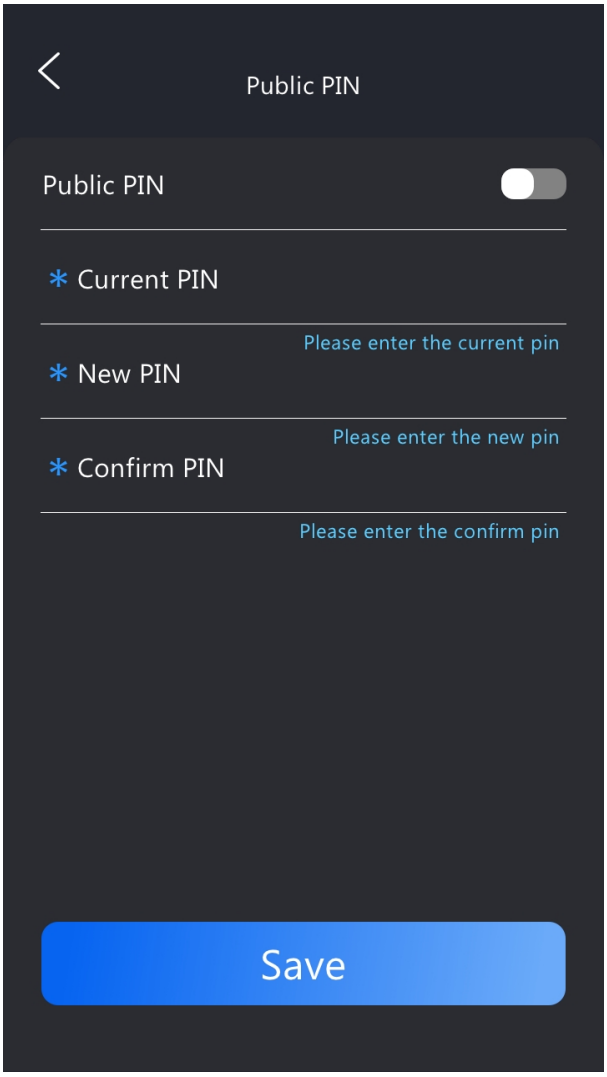
Unlock by Public PIN

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.

You can also set it up on the **Setting > Security > Public PIN** screen.



Virtual PIN

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

To enable the virtual PIN feature, navigate to the **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 user 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.

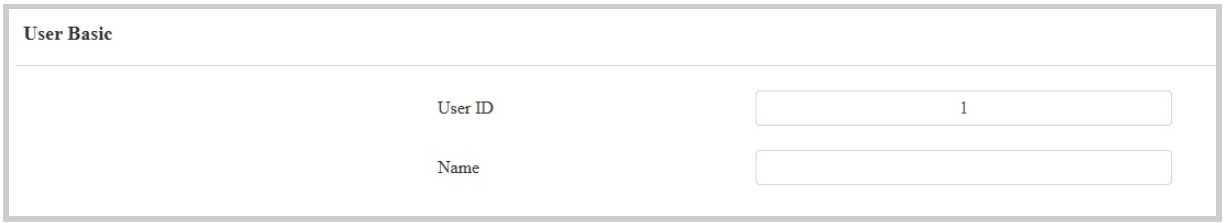
> **Note**
>
> This feature is not used for Public PIN and Apartment+PIN.

User-specific Access Methods

The private PIN code, RF card, Bkey, facial recognition settings, etc, 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. You can add up to 20,000 users.

To add a user, go to **Directory > User** interface and click **+Add**. You can also add a user on the device **Setting > User** screen.



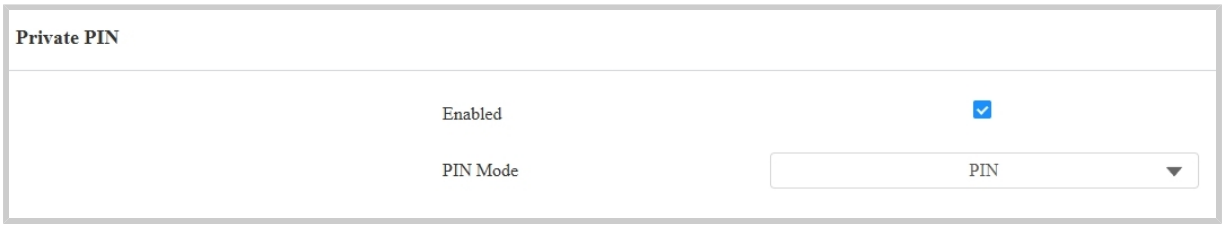
- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.

Unlock by Private PIN Code

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

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

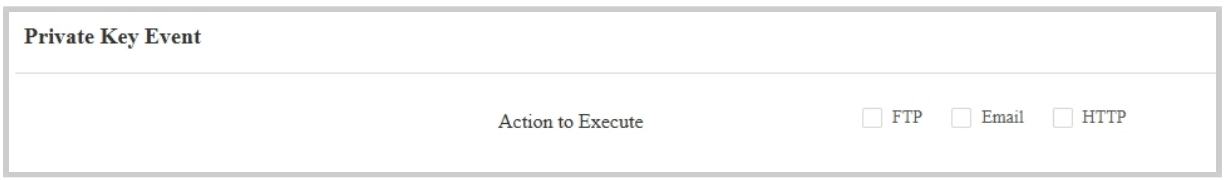
You can disable the use of private PINs and set the PIN mode on the **Access Control > PIN Setting > Private PIN** interface.



- **PIN Mode**:
- **PIN**: Solely enter the PIN code for door access.
- **APT+Key**: Enter the Apartment Number first before entering the PIN code for the door access. **Apartment Number** can only be applicable when the device is connected to the Akuvox SmartPlus.

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 message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

Unlock by Duress Code

The duress code is a special PIN designed for emergency situations. When a valid duress code is entered, the door is unlocked as usual, while the configured Action URL is sent to notify external systems or initiate predefined actions.

On the **Directory > User > +Add** interface, find the **Duress Code** section.

- **Code**: 4 to 6 digits.

> **Note**
>
> Click here to view the feature details.

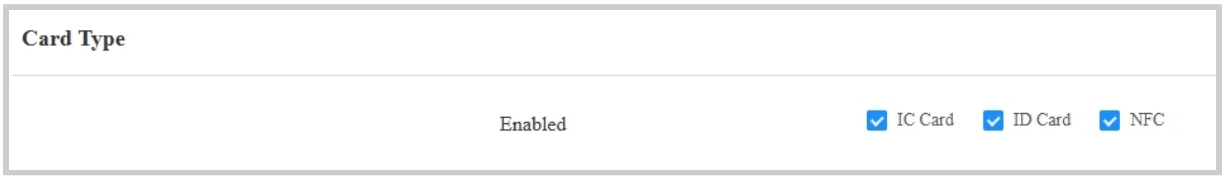
Unlock by RF Card/Bkey

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

- **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 adding 20,000 users.

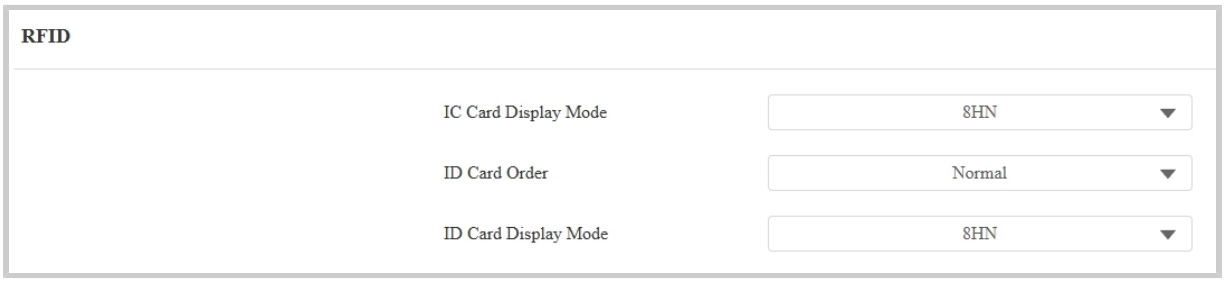
You can disable the use of cards on the **Access Control > Card Setting > Card Type** interface.



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. The default is 8HN.
- **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 License Plate

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

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

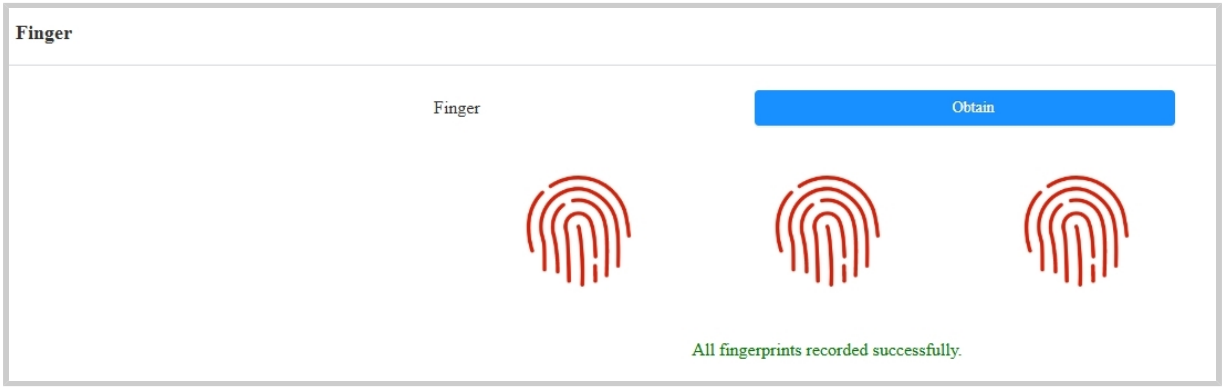
To assign the license plate to a user, find the **License Plate** part on the **Directory > User > +Add** interface.

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

Unlock by Fingerprint

The S535 with the fingerprint module installed supports opening doors via fingerprint keys.

On the **Directory > User > +Add** interface, find the **Finger** section. Click **Obtain** to start registering the fingerprint.



Place the user's finger that is used to open the door in the fingerprint reader area. The same fingerprint needs to be recorded three times.

Unlock by Facial Recognition

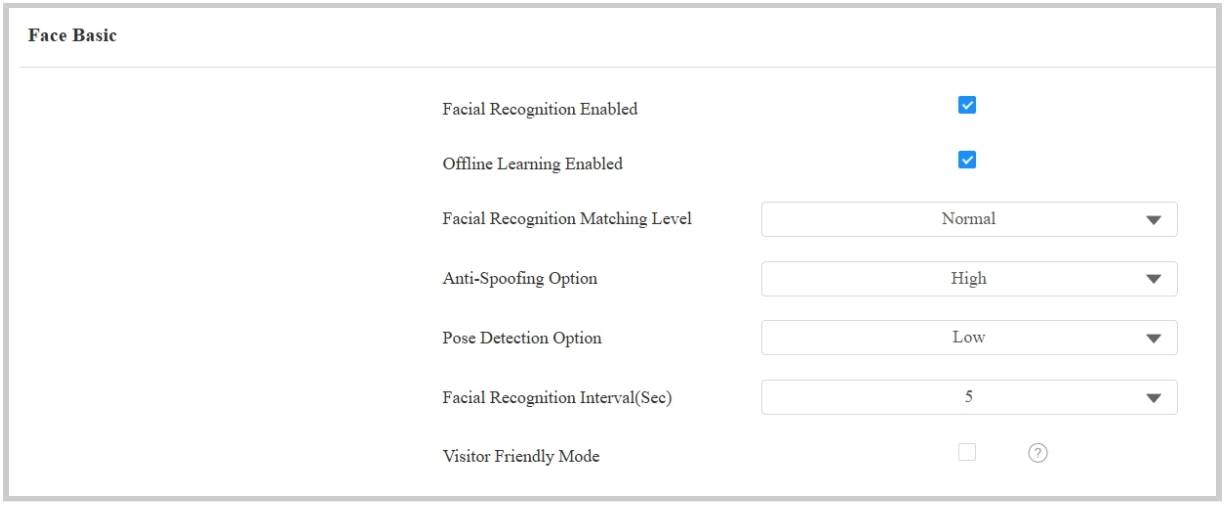
On the **Directory > User > +Add** interface, find the **Face** section.

- **Photo**: Max File Size: 2M; Format: .jpg/.png.

Facial Recognition Settings

The device allows you to adjust facial recognition accuracy, recognition intervals, and more to enhance user experience.

Set it up on the **Access Control > Face Settings** interface.



- **Facial Recognition Enabled**: Enable/disable the facial recognition function.
- **Offline Learning Enabled**: Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level**: Determine how strict the facial recognition system is in comparing a person's face with uploaded face data. Each level allows a different degree of difference or face covering (**excluding the mouth area**) to pass the recognition.
  - Low: Allow slight differences from the uploaded face data, with little face coverage.

  - Highest: Require the face to be identical to the uploaded one, with minimal or no covering.
  - The other two levels are in between.
- **Anti-Spoofing Option**: Set how strict the system is in preventing fake faces.
  - Close: Disable the facial anti-spoofing function. Facial verification can be passed using non-living substitutes for an authorized person's face, such as a photo.
  - Highest: The system cannot be fooled by any non-living substitutes for an authorized person's face.
  - The other three levels are in between.
- **Pose Detection Option**: Set the pose detection level from Close, Low, Normal, or High. The higher the level is, the more accurate the detection is. Users will be prompted to “please face the camera directly” when they do not face the camera.
- **Facial Recognition Interval**: Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.
- **Visitor-Friendly Mode**: Decide whether to display prompts when facial recognition fails. When enabled, no visual or auditory prompts will be given when the recognition fails.

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 the Bluetooth function on the **Access Control > BLE** interface.

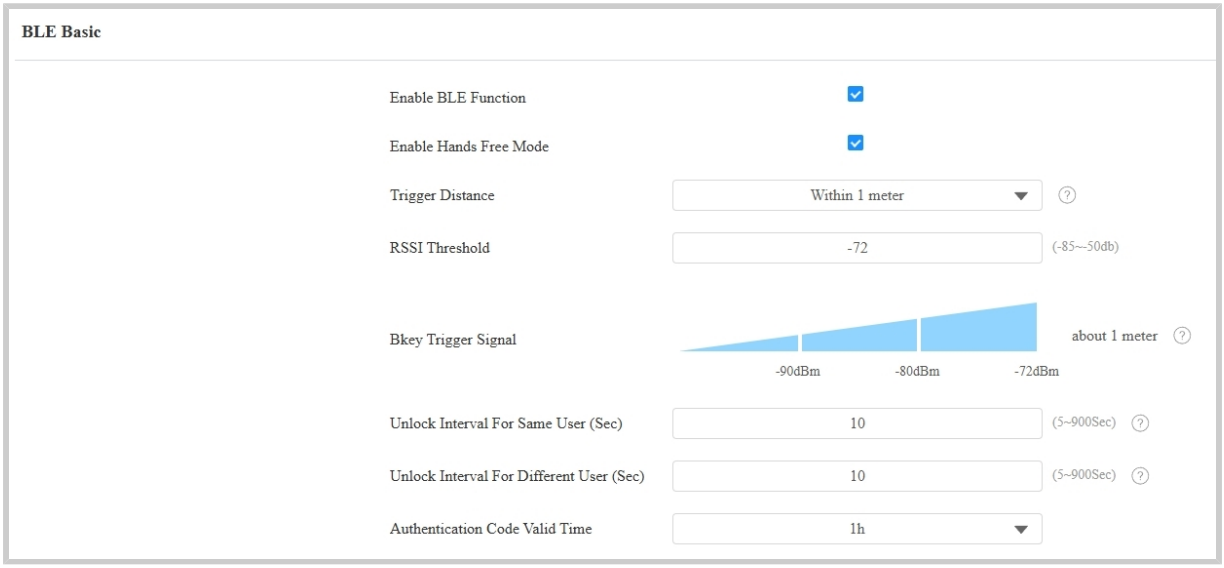
Unlock via My MobileKey

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 three ranges that determine the Bkey trigger distance, ranging from 1 meter to 5 meters.

- **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.
>
> - Unlock by Bluetooth via My MobileKey App.
> - Unlock by Bluetooth via SmartPlus App.
> - Open the Door via Bkey.

Device Info Settings

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

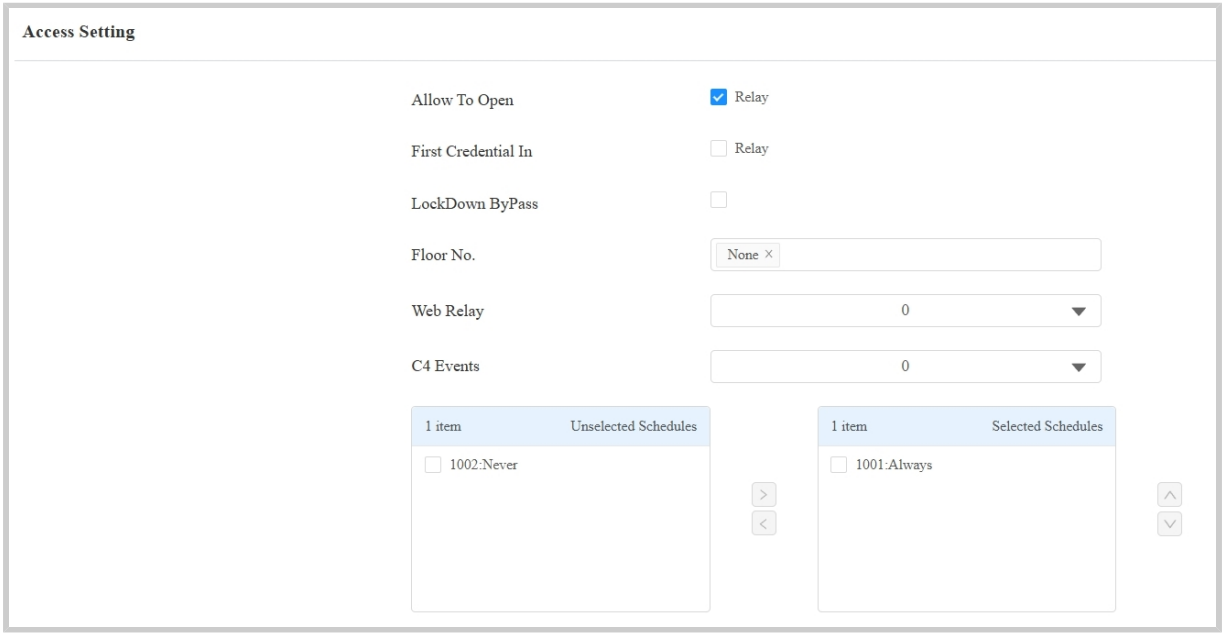
To set it up, go to **Access Control > BLE > Device Info Settings** interface.

- **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.

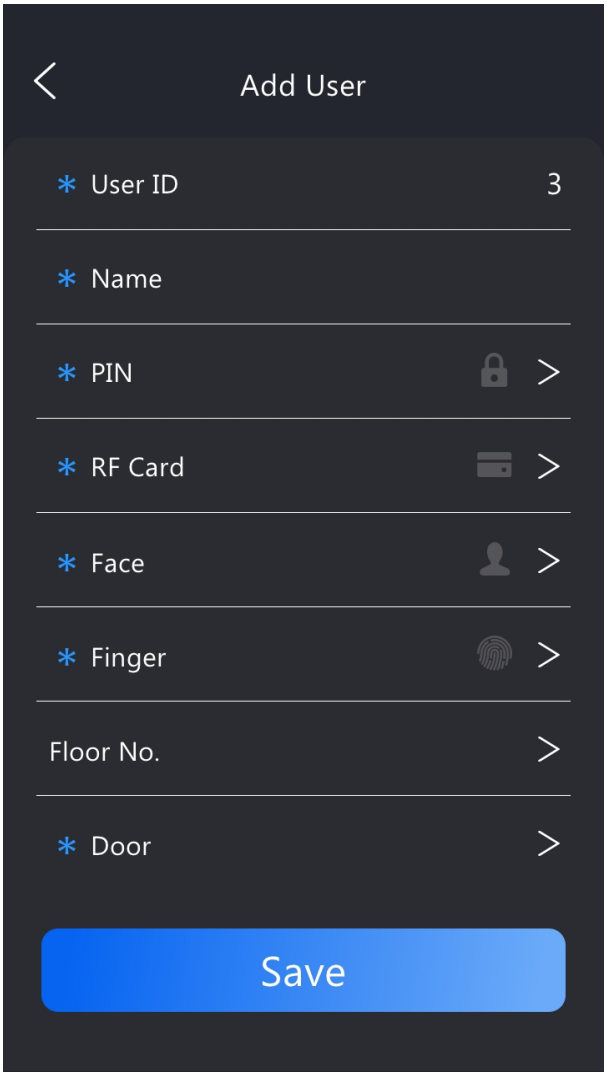
On the **Directory > User > +Add** interface, scroll to the **Access Setting** section.



- **Allow To Open**: Check the relay to be opened.
- **First Credential In:** This decides whether the user can keep the door open during the scheduled time after activating it.
- **Lockdown Bypass**: This decides whether the user can open the door when the door is locked during the scheduled time.
- **Floor No.**: Specify the floor(s) that are accessible to the user via the elevator.
- **Web Relay**: Specify the ID of the 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 left box to the right one. Besides custom schedules, there are 2 default options:
  - **Always**: Allows door opening without limitations on door open counts during the valid period.
  - **Never**: Prohibits door opening.

You can also set up users' access methods on the **Setting > User > User List** screen.



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.

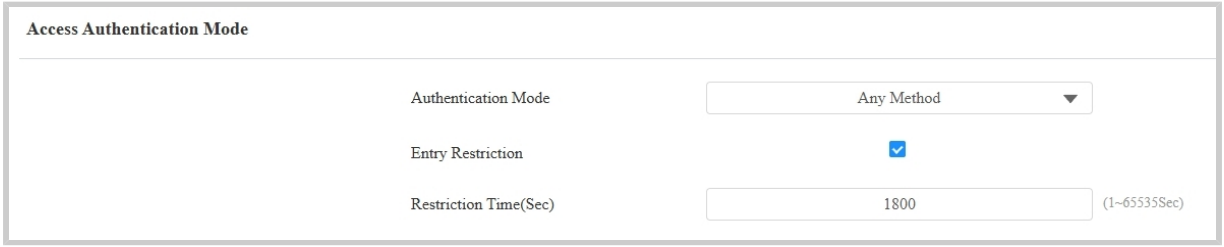
Navigate to the web **Directory > User > Import/Export User** interface. The device supports 20,000 users.

> **Note**
>
> The exported file is in TGZ format; the imported file should be in XML or CSV format.

Access Authentication

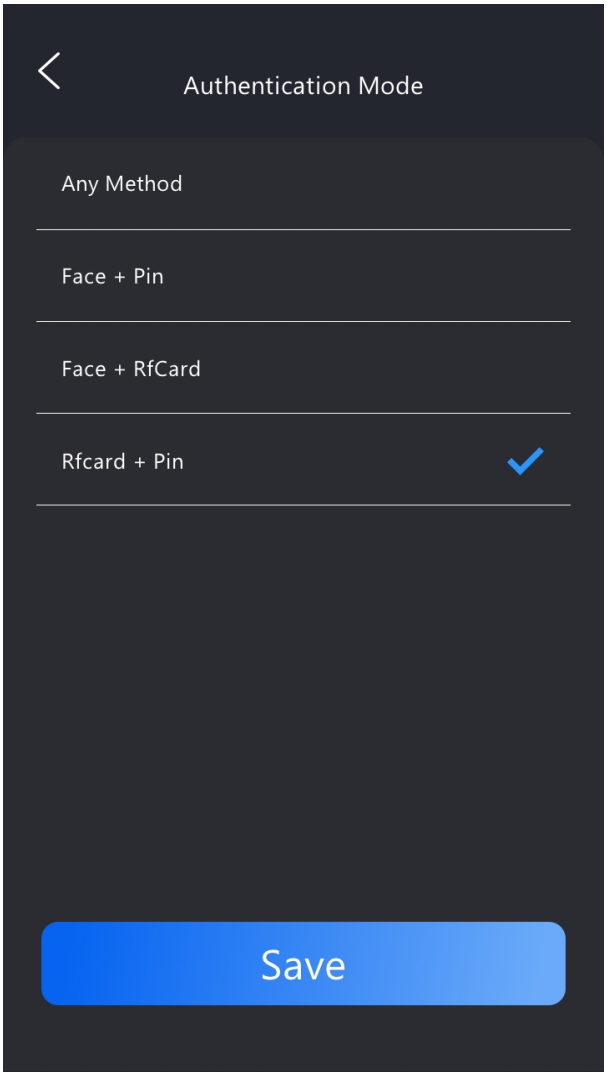
You can set up multiple access authentication modes, and set up authentication security as needed.

Set it up on the **Access Control > Relay > Access Authentication Mode** interface. This feature applies to the **Building** theme.



- **Authentication Mode**: Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.
  - **Any Method**: Allows all access methods.
  - **Face + PIN**: Scan the face first, then enter the PIN code.
  - **Face + RF Card**: Scan the face first, then swipe the RF card.
  - **RF Card + PIN**: Swipe the RF card first, then enter the PIN code.

You can also set up the access authentication on the **Setting > Security > Authentication Mode** screen.



Entry Restriction

You can limit users from opening the door repeatedly for a short time.

To set it up, go to the **Access Control > Relay > Access Authentication Mode** interface. It is disabled by default.

- **Restriction Time(Sec)**: Specify the time within which the same user cannot open the door twice. For example, if it is set to 1800 seconds, the user cannot open the door again until 30 minutes later.

CEPAS Card Reading

The device supports reading CEPAS cards. Under the **CEPAS** functionality module, there are two toggle options available: **CSN** (Card Serial Number) and **CAN** (Card Number).

Enable the card reading on the **Access Control > Card Setting > CEPAS** interface.

- **CSN**: The default option. This option allows the device to read the **UID** (Unique Identifier) of the CEPAS card, which is a unique value assigned to each card.

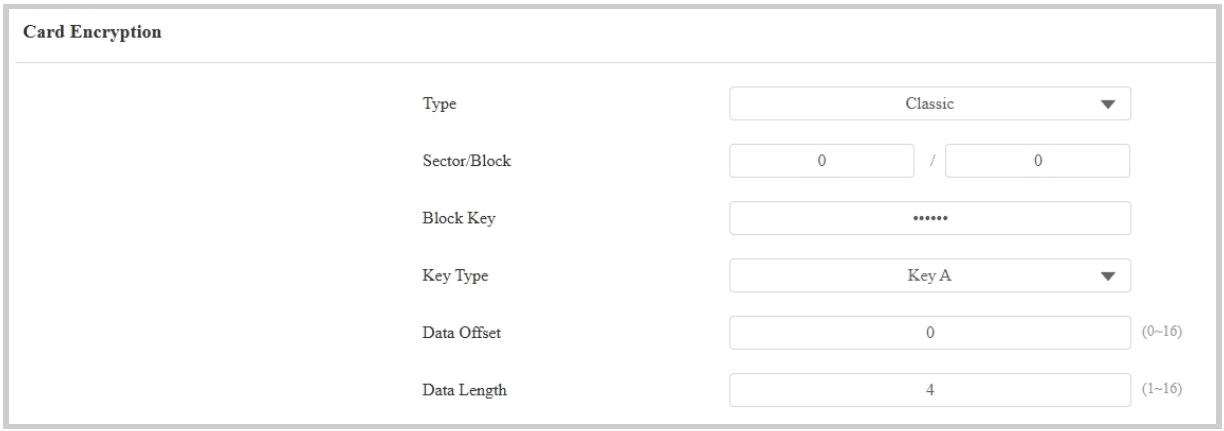
- **CAN**: This option allows the device to read the **card number** stored on the CEPAS card, which can be used for identification or access control.

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.

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



- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
  - **Key Type**: The authentication key type used to read the Mifare Classic card
  - **Data Offset**: The starting byte position from which card data is read. The default is 0.

    - **Data Length**: The number of valid data bytes to read from the card. The default is 4.
- **Plus**: You can set up three choices. This means you can use three types of Mifare Plus cards. When swiping a card, as long as one of the choices matches its SL key, the card code in the block you specified will be output.
    - **Block**: Specify the block(s) to be read.
    - **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.
    - **Read Key**: The file key.
    - **Key Index**: The index number for the key, which can be a number from 0 to 11.
    - **Byte Order**: The byte reading order. The default is MSB. The device starts reading bytes after performing **Data Offset** and **Data Length**.
        - **MSB**: Most Significant Bit means the reading order is normal(from left to right).
        - **LSB**: Least Significant Bit means the reading order is reversed(from right to left).
    - **Data Offset**: Define from which byte position to start reading data, with a range of 0 to 43. The default is 0.
    - **Data Length**: Define the length of valid byte data, with a range of 1 to 8. The default is 4.

Unlock by QR Code

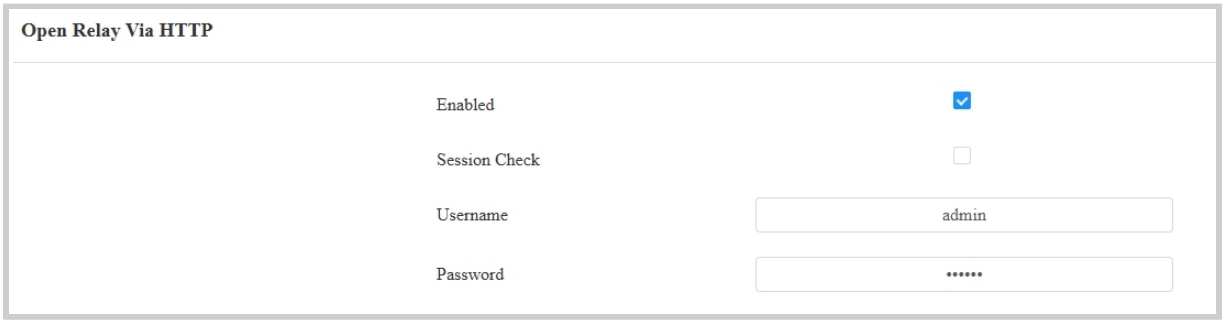
You can use a QR code to unlock the door with the door phone. This method requires the Akuvox SmartPlus cloud service. You have to activate this feature before using it.

Enable the QR code door-opening function on the **Access Control > Relay > Open Relay Via QR Code** interface.

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.

Set it up on the web **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.

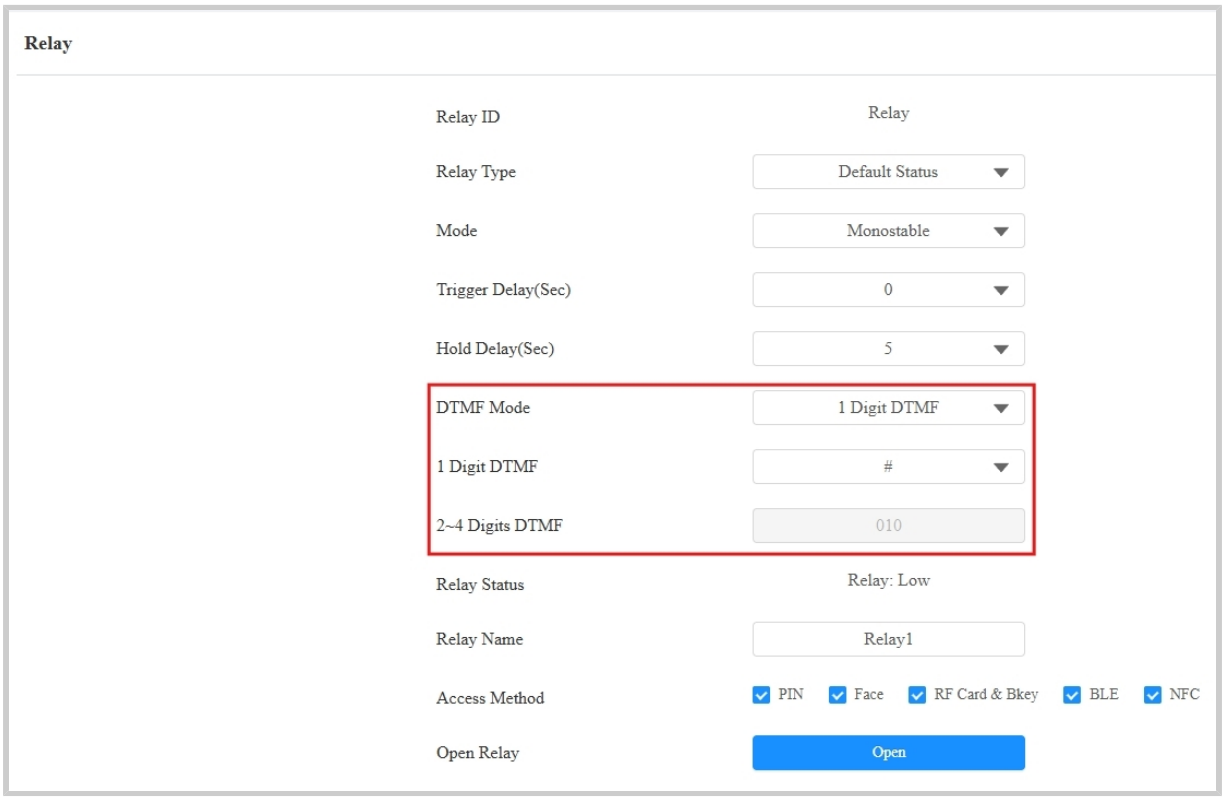
> **Tip**
>
> Here is an HTTP command URL example:
>
> Door phone's IP
> Preset credentials for authentication
> http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1
> ID of Relay to be triggered

> **Note**
>
> 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.

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



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

- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

DTMF Data Transmission

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

DTMF Type Differences:

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

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

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.

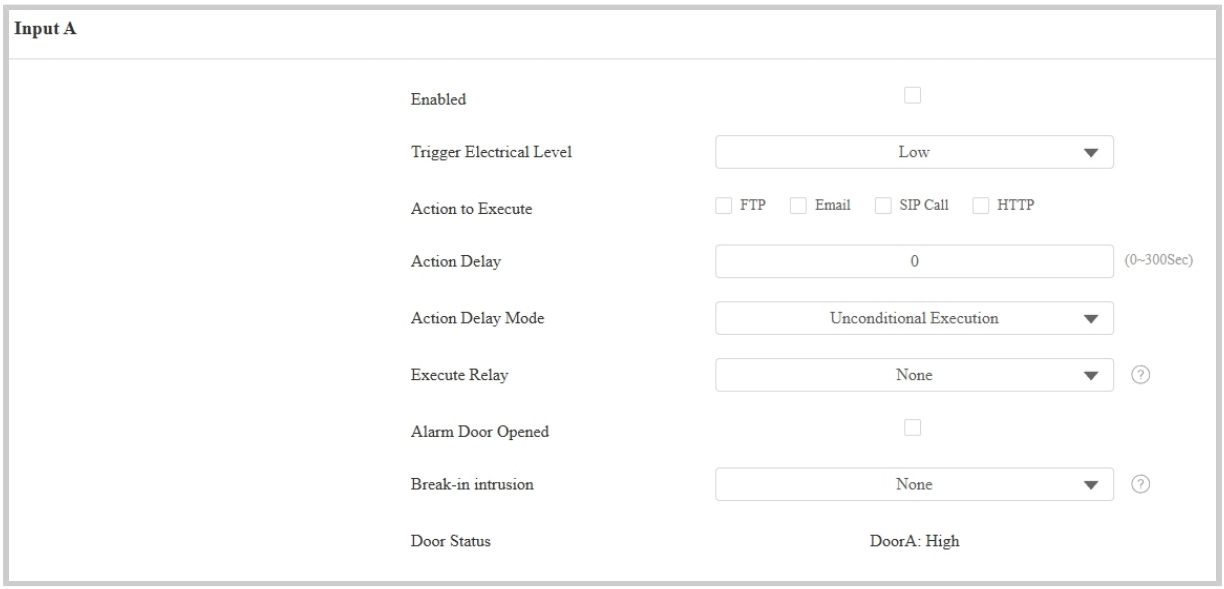
- **Assigned The Authority For**: Specify the contacts authorized to open doors via DTMF:
  - **None**: No numbers can unlock doors using DTMF.
  - **Only Contacts List**: Only numbers added to the door phone's contact list can unlock via DTMF.
  - **All Numbers**: Any numbers can unlock using DTMF.

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 > Input** interface.



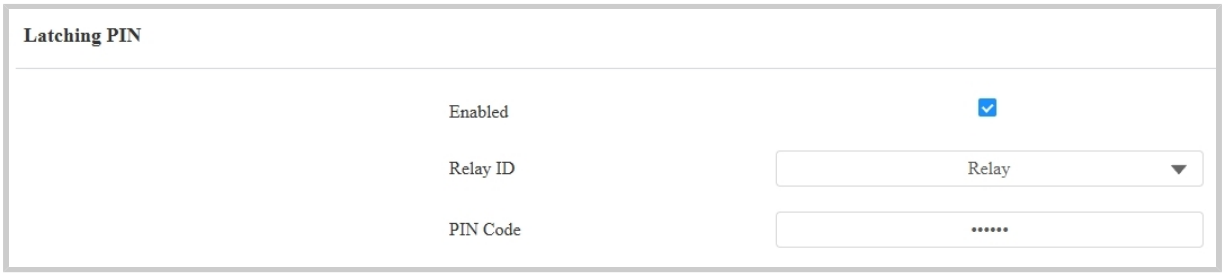
- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - **FTP**: Send a screenshot to the preconfigured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

  - **Execute If Input Still Triggered**: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **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. It is incompatible with the Execute Relay feature. Click here to learn more about this feature.
- **Door Status**: Display the status of the input signal.

Latching PIN

The door opens when the user enters the PIN and stays open until the PIN is entered again.

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



- **Enabled**: The function is disabled by default.
- **PIN Code**: The code should be within 4 to 8 digits. It cannot be the same as the public or private PIN. The PIN code must be set up. Otherwise, the function will not take effect.

Note

- The relay schedule takes priority over the latching PIN feature, keeping the door open during scheduled times. Users cannot close the door with the latching PIN.
- The latching PIN feature takes priority over user credentials. When the door is opened with the latching PIN, it cannot be closed using credentials like an RF card.

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.

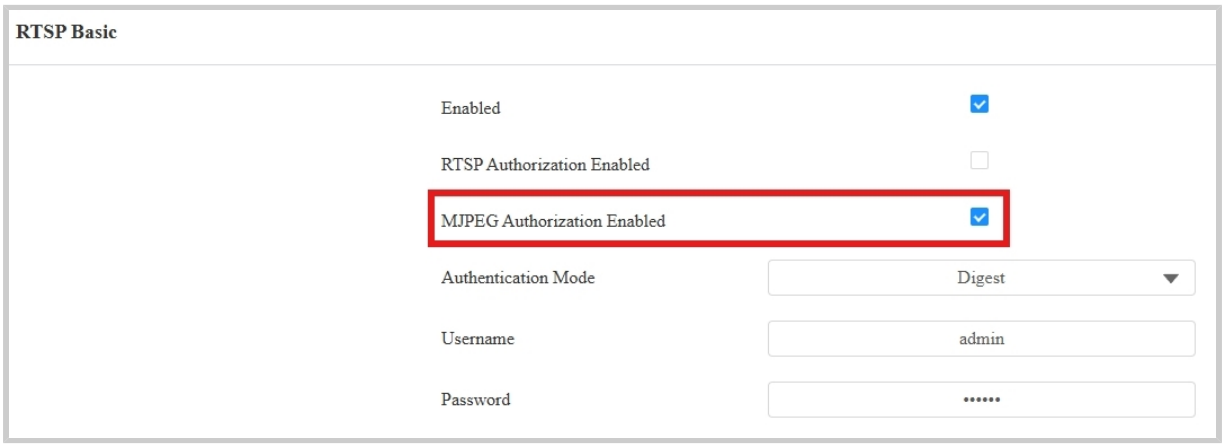
To set it up, go to the **Surveillance > RTSP > MJPEG Video Parameters** interface.

- **Video Resolution**: Specify the video resolution from the lowest QVGA(240×320 pixels) to the highest 1080P(1920×1080 pixels). The default is 720P.
- **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

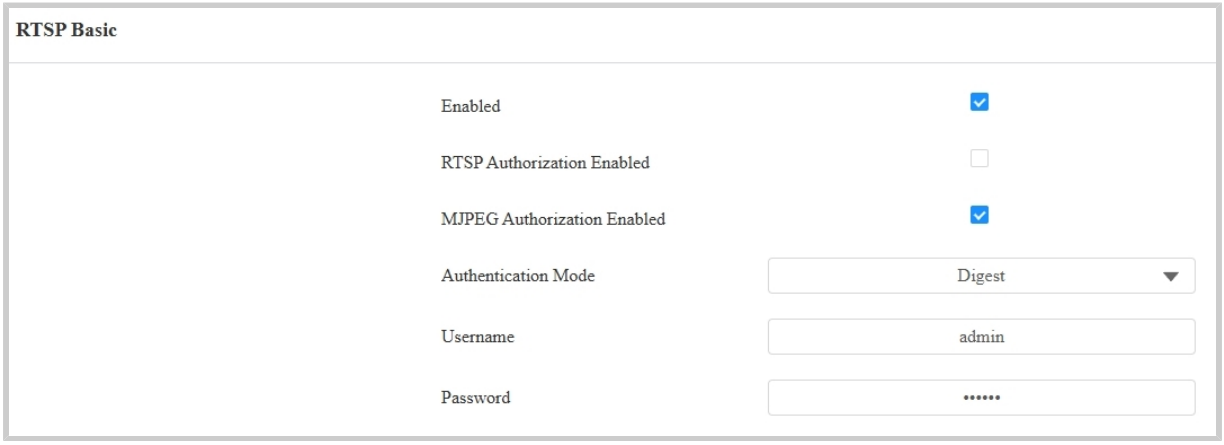
- To view a dynamic stream, use the URL http://device_IP:8080/video.cgi.
- For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi
- For example, if you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

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

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

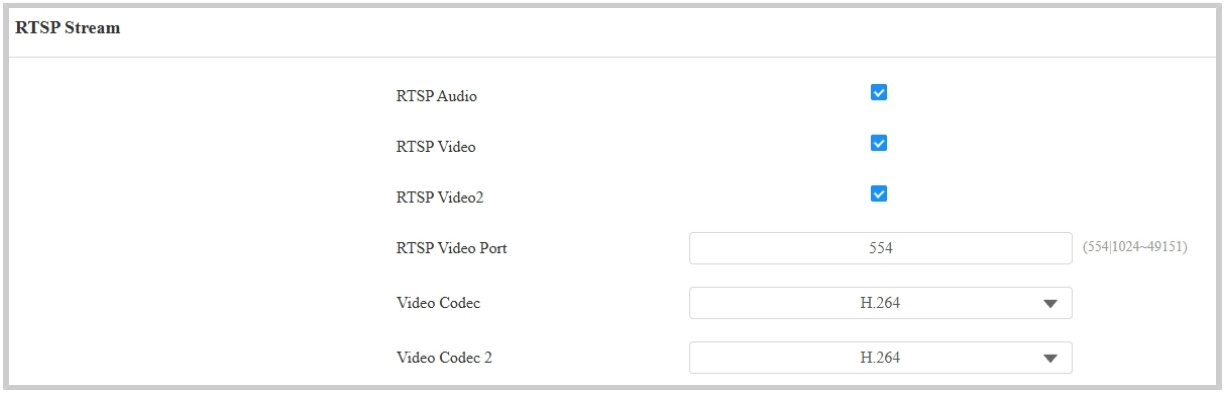


- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: It is Digest by default, which uses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



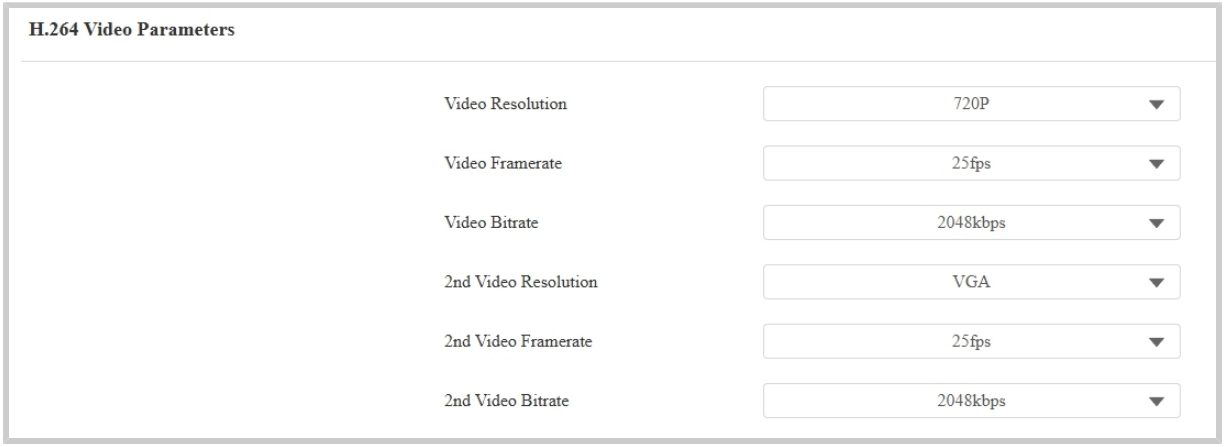
- **RTSP Audio**: Allow the door phone to send audio information to the monitor via RTSP.
- **RTSP Video**: The door phone can send the video information to the monitor. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **RTSP Video 2**: Akuvox door phones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

- **Video Codec/Video Codec 2**: Choose the video codec between H.264 and MJPEG.

> **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.



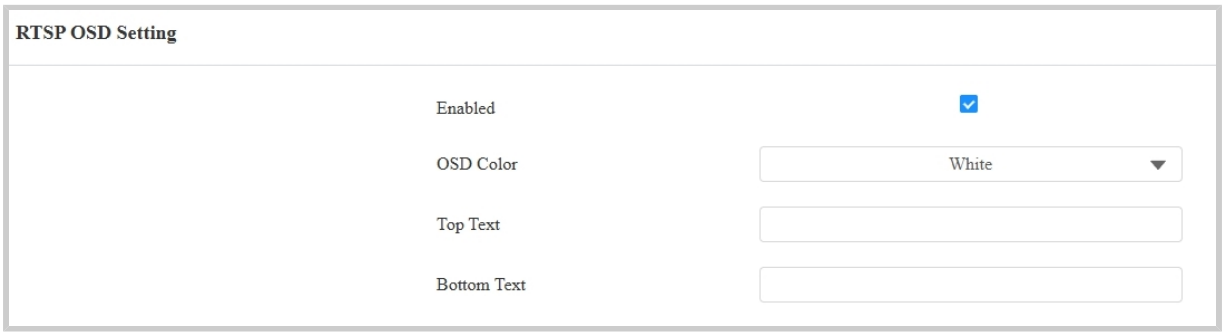
- **Video Resolution**: Specify the image resolution, varying from the lowest QVGA(240×320 pixels) to the highest 1080P(1920×1080 pixels). The default is 720P.
- **Video Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default is 25fps.
- **Video Bitrate**: 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.

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.



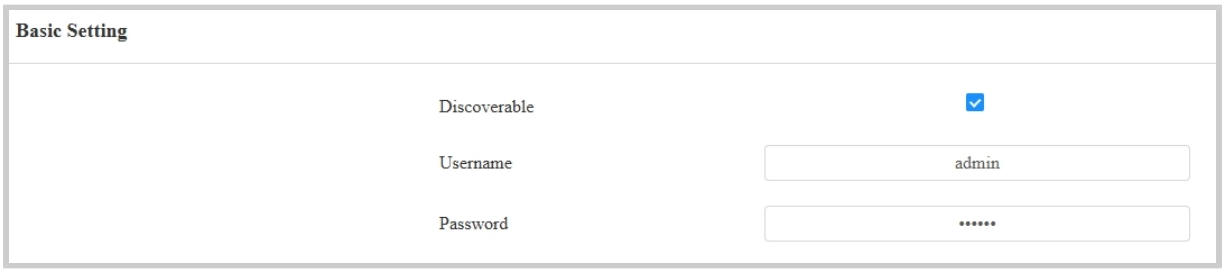
- **OSD Color**: Select the color from White, Black, Red, Green, or Blue.
- **Top/Bottom Text**: Customize the OSD content.

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 is searchable by other devices.
- **Username**: 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.

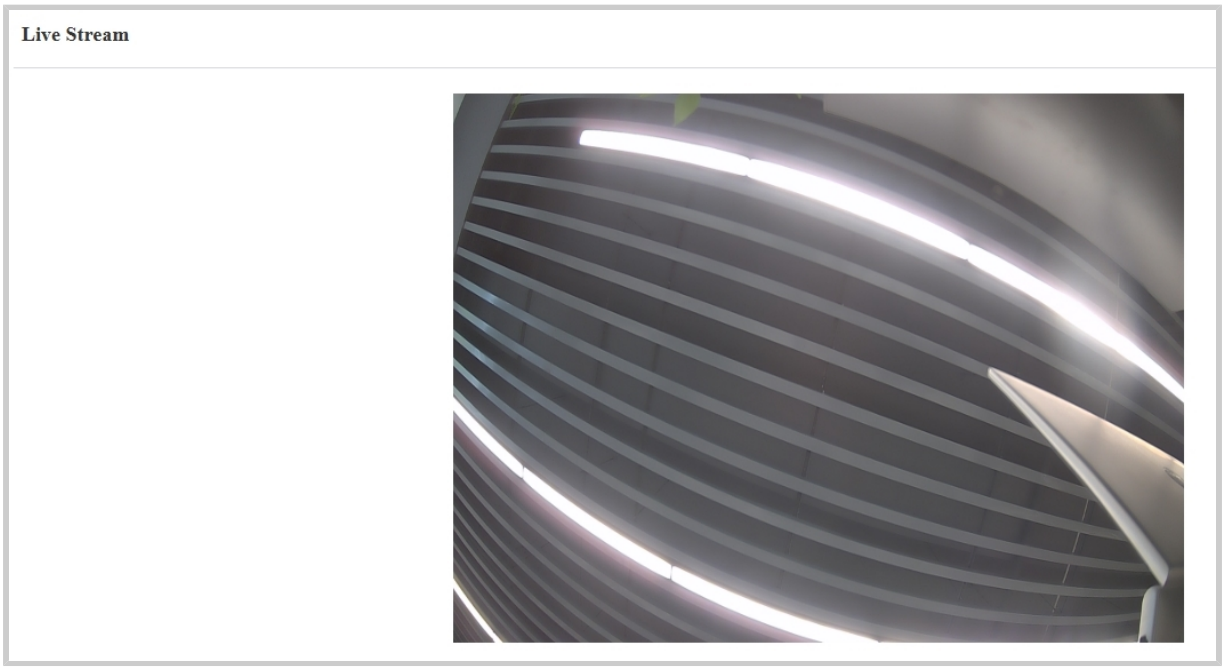
> **Tip**
>
> Once the settings are configured, to access the video stream on the third-party device, simply enter the ONVIF URL: http://Device's IP:80/onvif/device_service.

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.

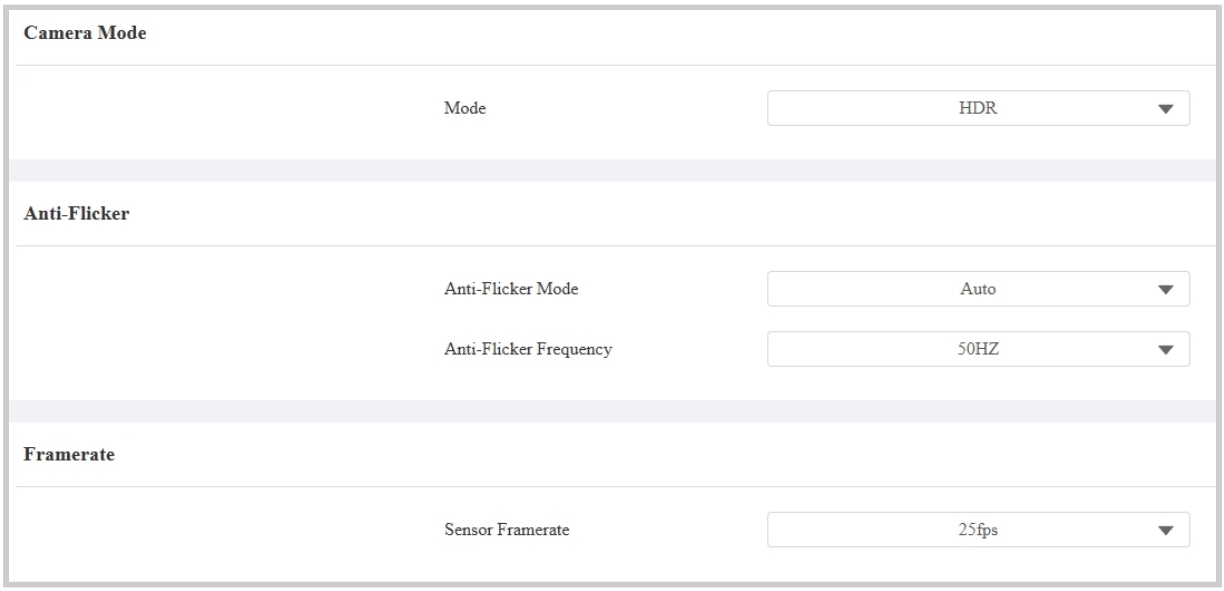
View the video stream on the **Surveillance > Live Stream** interface.



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.

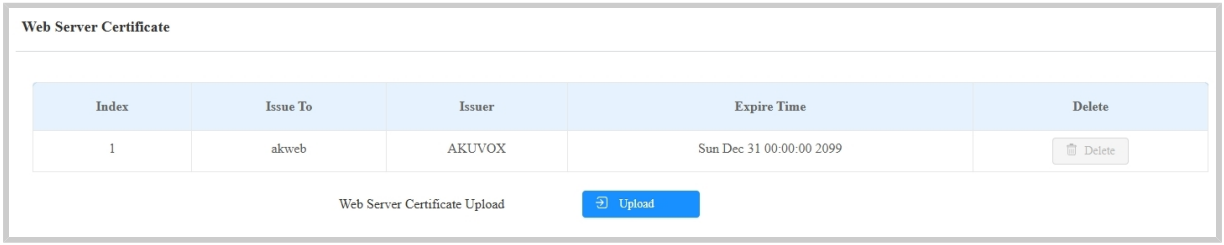
Client Certificate Setting

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.

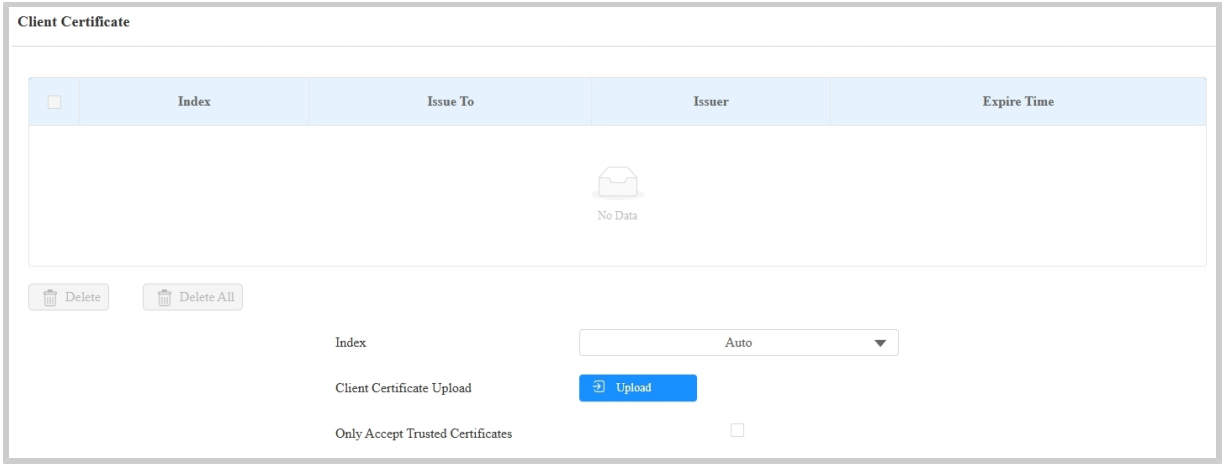
Upload the certificate on the web **System > Certificate** interface.



Client Certificate

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

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



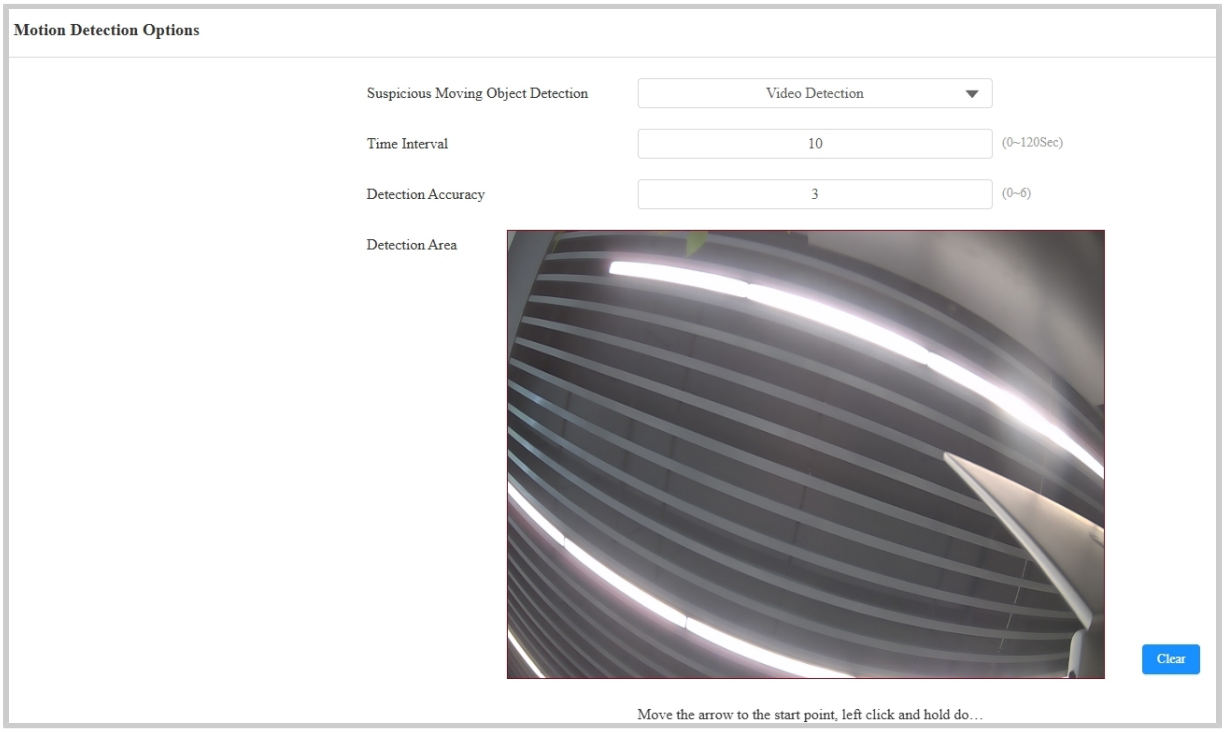
- **Index**: Select the desired value from the drop-down list of Index. If you select Auto, the uploaded certificate will be displayed in numeric order. If you select a value from 1 to 10, the uploaded certificate will be displayed according to the number.

- **Client Certificate Upload**: Locate and upload the desired certificate (*.pem only).
- **Only Accept Trusted Certificates**: When enabled, as long as the authentication is successful, the phone will verify the server certificate based on the client certificate list. When disabled, the phone will not verify the server certificate no matter whether the certificate is valid or not.

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.

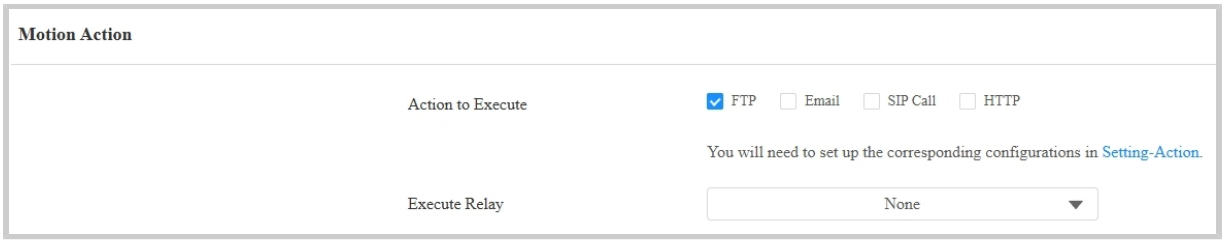
To set it up, go to the web **Surveillance > Motion** interface.



- **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 a longer range and better detection in poor visibility conditions.
  - **Video + Radar**: Detect motion with the combination of the 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.

Besides, you can set up the actions triggered by motion detection.



- **Action to Execute**: The notification type includes FTP, Email, SIP Call, HTTP, and TFTP.
  - **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.

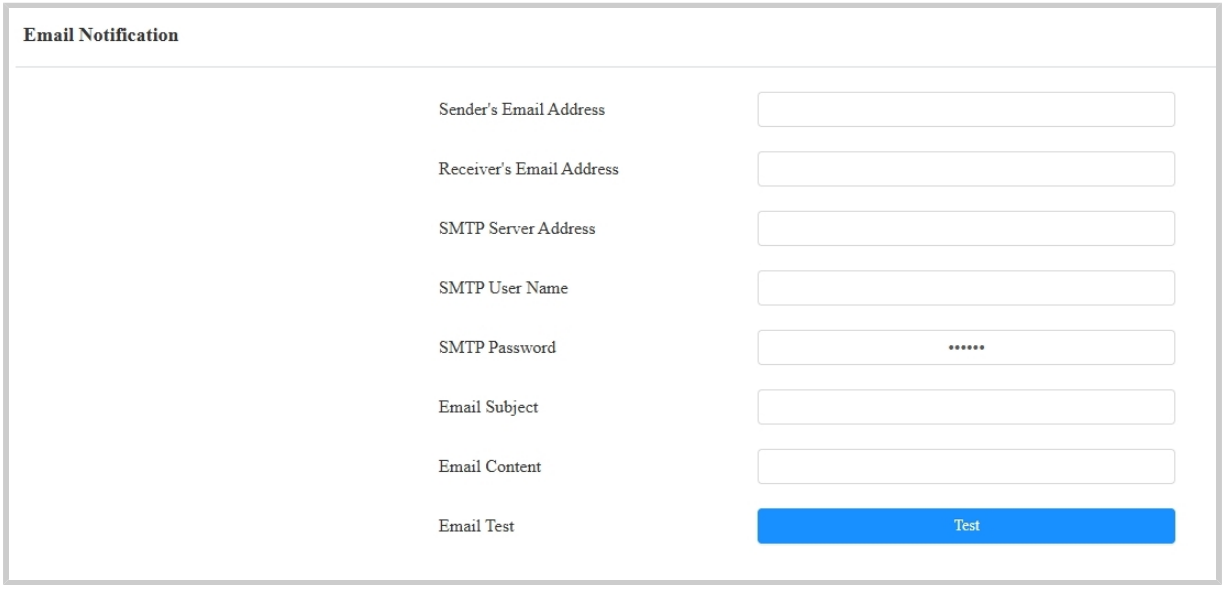
Set up notifications on the **Setting > Action** interface.

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.

Find the **Email Notification** section.



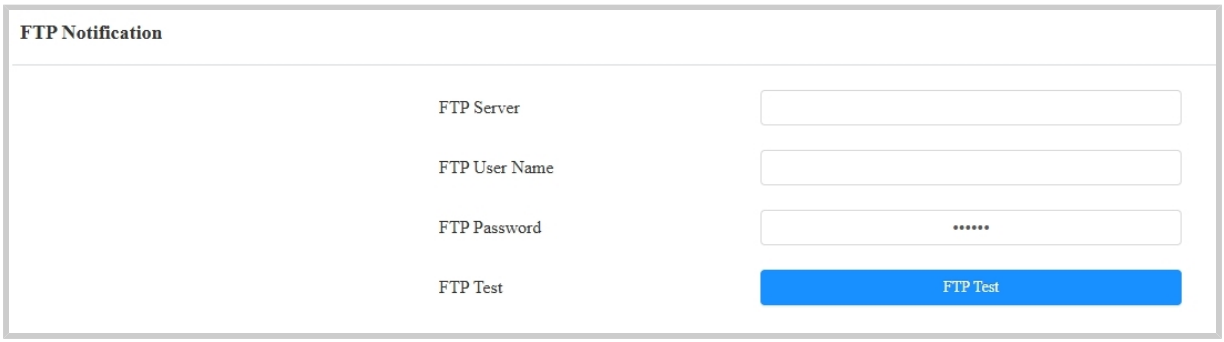
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

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.

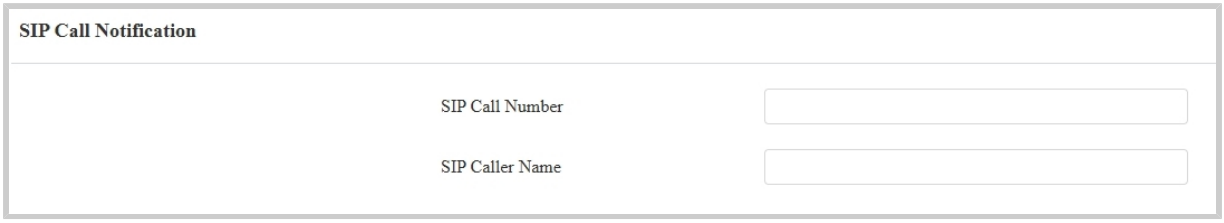
Set it up on the **FTP Notification** section.



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:

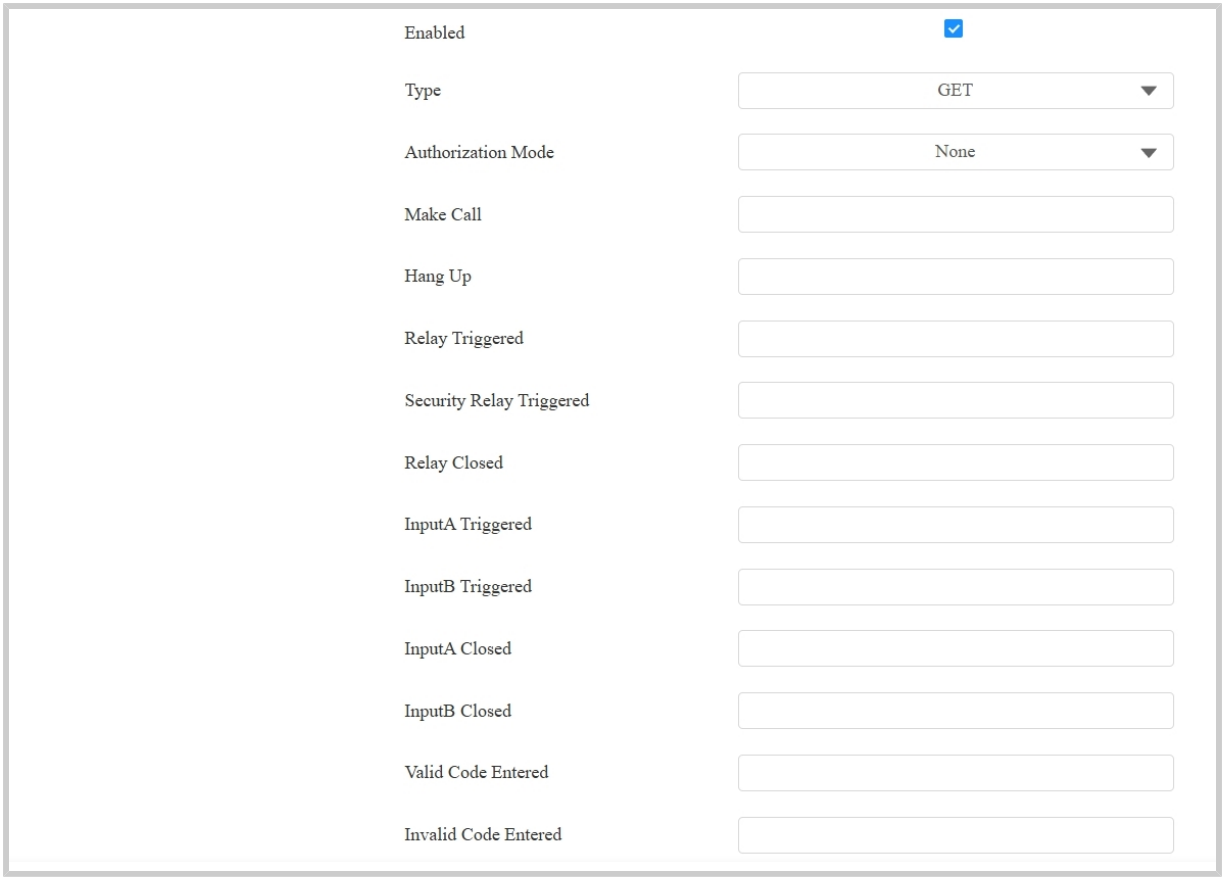
Event	Parameter format	Example
Make Call	$remote	Http://server ip/Callnumber= $remote

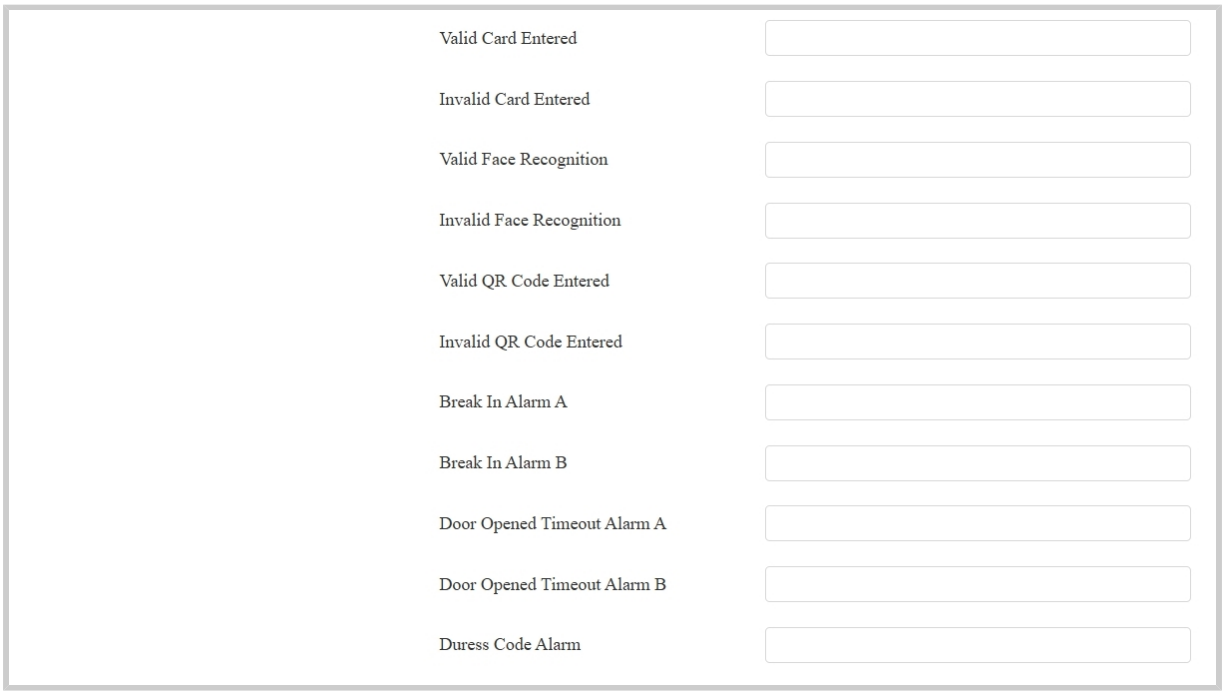
Hang Up	$remote	Http://server ip/Callnumber=$remote
Relay Triggered	$relay1status	Http://server ip/relaytrigger=$relay1status
Relay Closed	$relay1status	Http://server ip/relayclose=$relay1status
Security Relay Triggered	Null	Http://server ip/securityrelaytrigger
Input Triggered	$input1status	Http://server ip/inputtrigger=$input1status
Input Closed	$input1status	Http://server ip/inputclose=$input1status
Valid Code Entered	$code	Http://server ip/validcode=$code
Invalid Code Entered	$code	Http://server ip/invalidcode=$code
Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
Invalid Card Entered	$card_sn	Http://server ip/invalidcard=$card_sn
Facial Recognition	$open_type	Http://serverip/unlocktype=$open_type
QR Code	$open_type	Http://serverip/unlocktype=$open_type

Break-in Alarm	$input1status	Http://server ip/inputtrigger= $input1status **NOTE**: $input1/2status corresponds to Input A/B.
Alarm Door Opened Timeout	$input_id	http://server ip/inputID= $input_id

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

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





- **Authorization Mode**: Select the authorization mode. If Digest is selected, you need to set up the username and password.
- **Door Opened Timeout Alarm A/B**: The HTTP URL will be sent when the door sensor connected to input A/B detects that the door-opening time exceeds a limit.
  - $input_id in the URL refers to the input triggered. InputID=1 indicates InputA; InputID=2 indicates InputB.

> **Note**
>
> To enable the Door Opened Timeout Alarm feature and set the time limit, go to the **Access Control > Input** interface.

Voice Encryption

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

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

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

User Agent

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

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

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

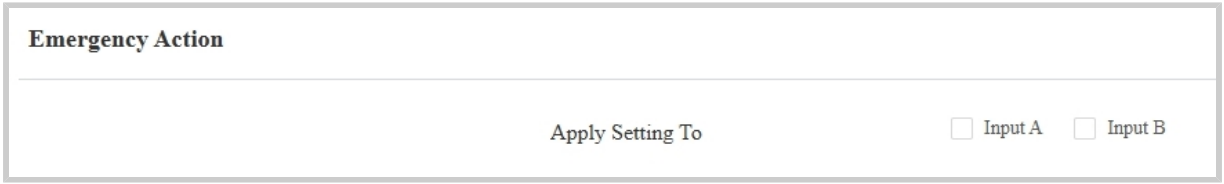
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

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.

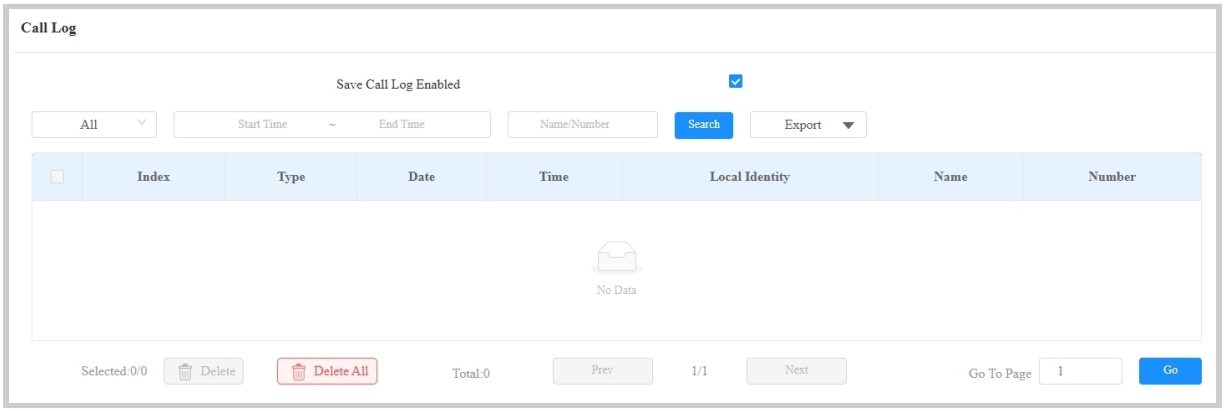
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering the input.
  - **Relay**: The door is opened by triggering the relay.

Logs

Call Logs

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

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

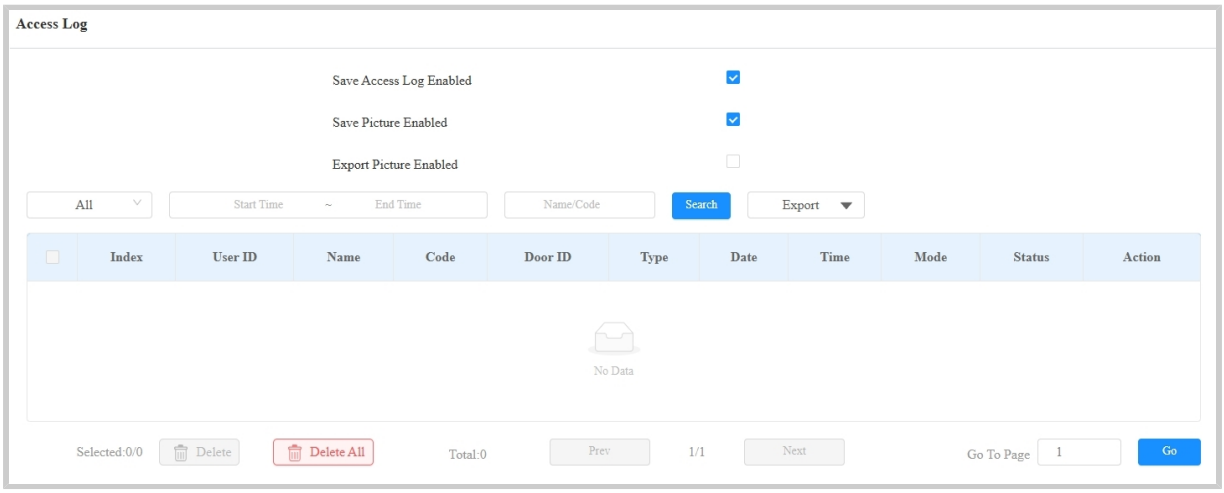


- **All**: Four types of call history are available: All, Dialed, Received, and Missed.
- **Start Time-End Time**: The specific time of the call logs you want to search, check, or export.
- **Name/Number**: Search the call log by the name or by the SIP or IP number.
- **Export**: Call logs can be exported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

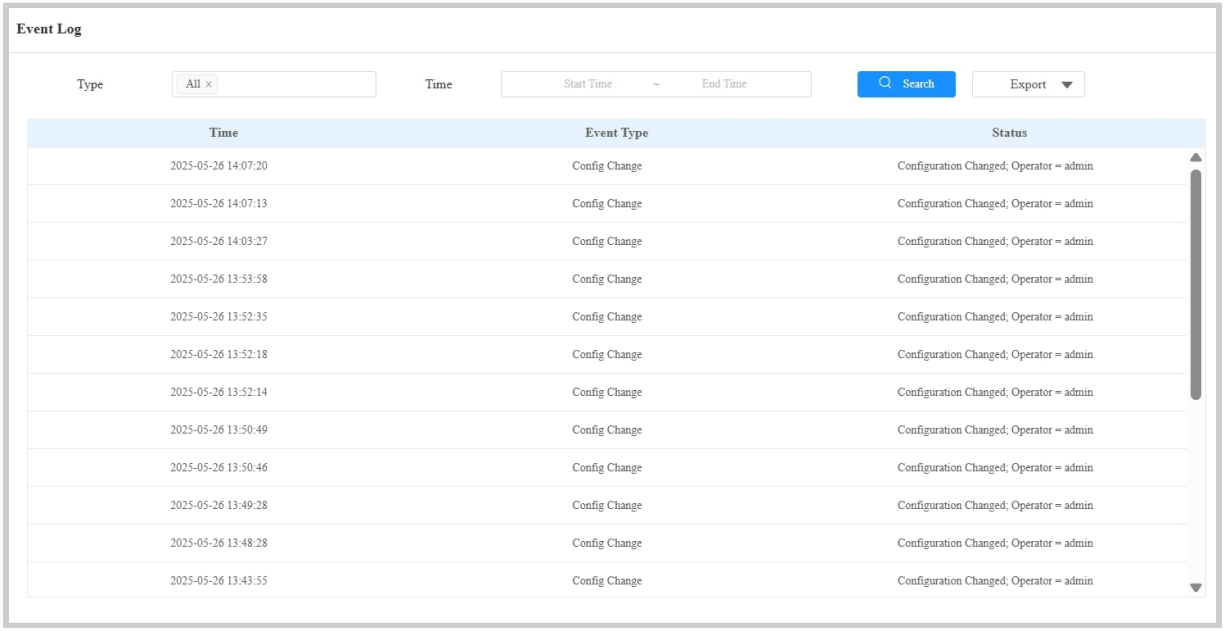


- **Save Picture Enabled**: When enabled, the device will capture pictures of the door opening, and you can click **Picture** in the Action column to view the screenshot.
- **Export Picture Enabled**: Set whether to export the captured images when exporting the door logs.
- **All**: Three types of access 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.

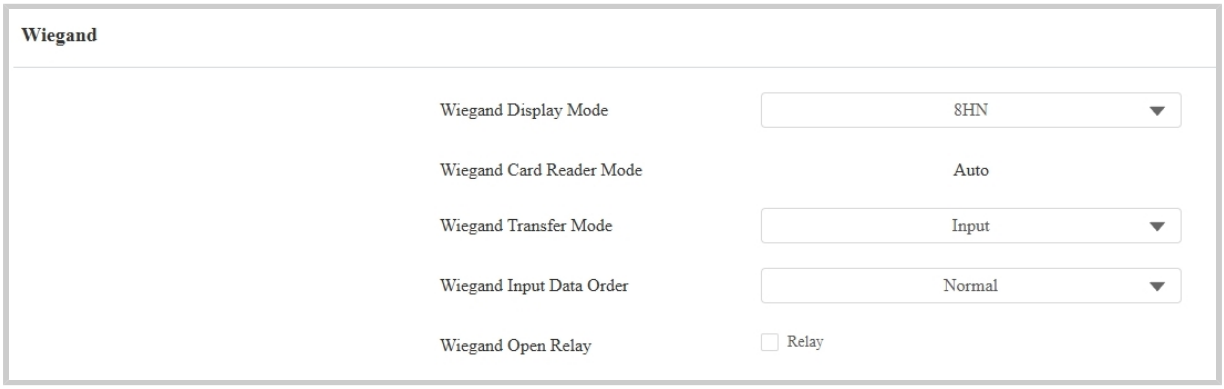


Integration with Third-Party Device

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 following options: 8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26), 8HR10D, and RAW.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device. It is automatically configured for **Input** Wiegand transfer mode.
- **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 and fingerprint data.
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.

- **Wiegand Output Basic Data Order**: Set the sequence of the card data before going through Wiegand conversion and outputting the card code.
  For example, if the card data is 0x11 0x22 0x33 0x44 and the **Reversed** option is selected, the data will be 0x44 0x33 0x22 0x11.
- **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
  For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If **Reversed** is selected, the card data is 0x55 0x44 0x33.
- **Wiegand Output CRC Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **RF Card Verification**: Available when **Output** or **Convert to Card No. Output** is selected. When enabled, the device will verify whether the card code is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the door phone screen. When disabled, the door phone will not perform local verification.
- **PIN/QR Code Verification**: Available when **Output** is selected as Wiegand Transfer Mode. When enabled, the device will verify whether the credential is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the door phone screen. When disabled, the door phone will not perform local verification.
- **Wiegand Open Relay**: Check the relay to be triggered through Wiegand.

Note

Click here to view more information on Wiegand settings including:

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

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

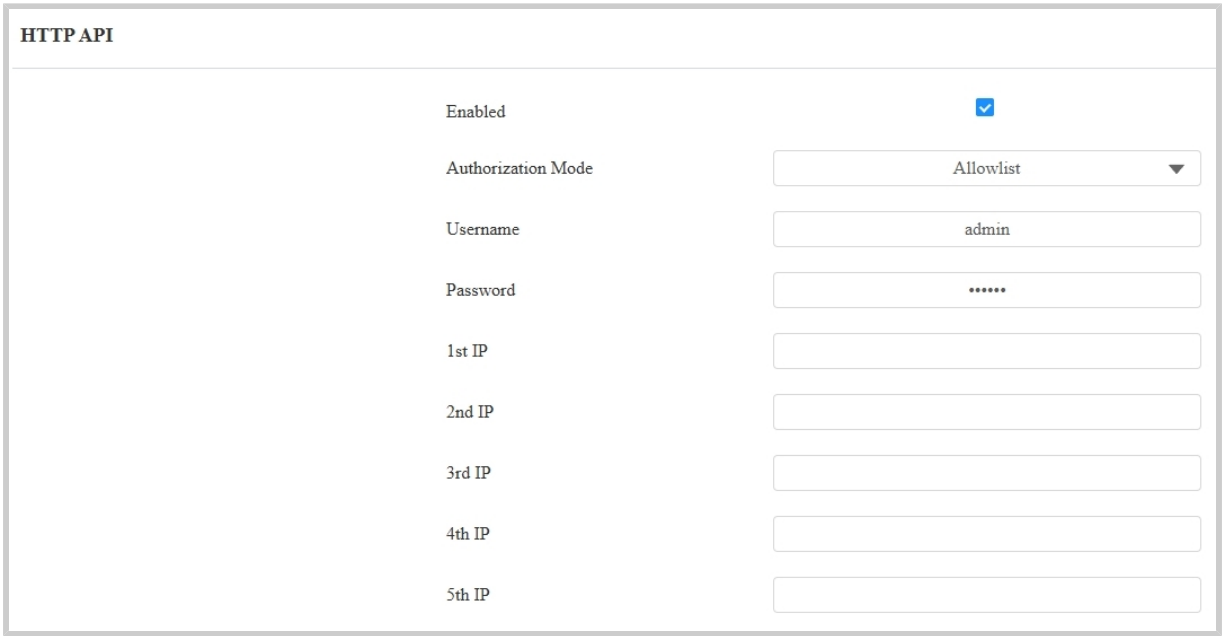
Set it up on the **Device > Wiegand > Convert To Wiegand Output** interface.

- **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 an 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 username 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 **Allowlist** authorization is selected for the integration.

Please refer to the following description for the authentication mode:

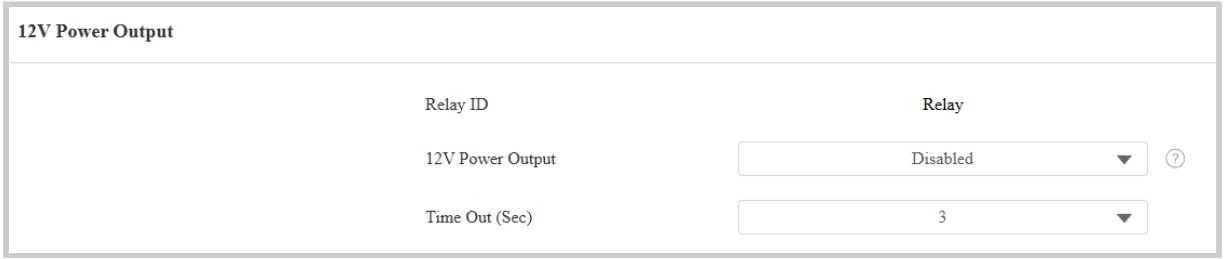
NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication. The allowlist is suitable for operation in the LAN.

NO.	Authorization Mode	Description
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 encoding method to encode of username and password.
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**:

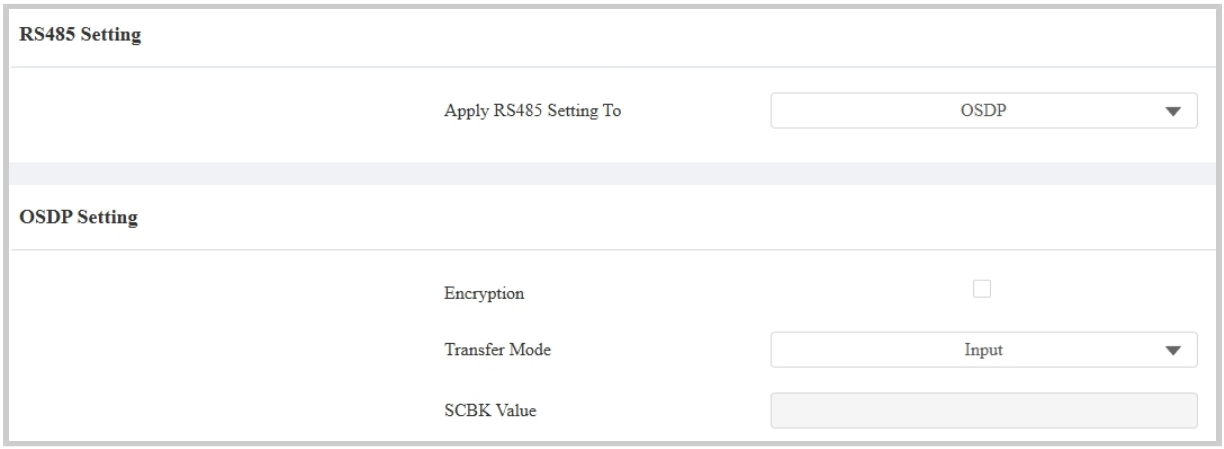
- **Always**: Provide continuous power to the third-party device.
- **Triggered by Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.

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.



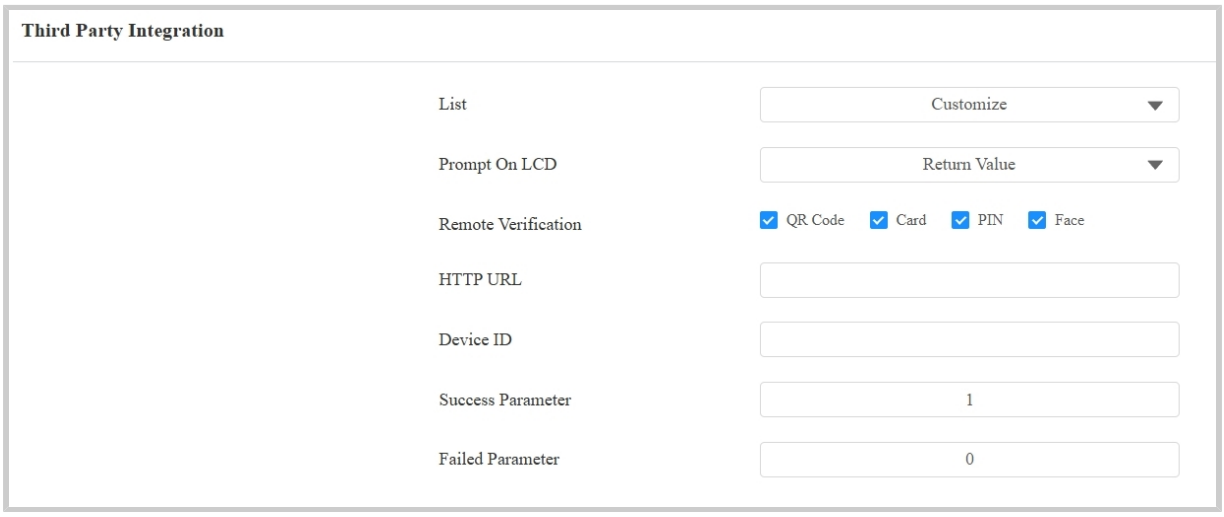
- **Disabled**: The RS485 function is disabled.
- **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **Transfer Mode**: Select the RS485 working mode, Output, or Input.
    - **Local Relay Verification**: When Output is selected, set whether to carry out the access credentials verification. When unchecked, door-opening failure prompts will not be given.
  - **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.

Integration with Third-party Access Control Server

The device can transmit access credential data to a third-party server without doing local verification. The generation and verification of the data are conducted on the third-party server.

To set it up, go to **Access Control > Relay > Third Party Integration** interface.



- **List**:
  - **None**: Disable the function.
  - **General**: Transmit the QR code-linked HTTP URL in Akuvox's method.

- **HTTP URL**: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before it is sent to the QR code server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode} &deviceId={DeviceID}.*
- **Device ID**: The device ID is provided by the third-party server. It will be added to the HTTP command automatically when using a QR code for door access.
- **Success Parameter**: Receiving this value indicates that opening the door succeeds.
- **Failed Parameter**: Receiving this value indicates that opening the door fails.

- **Customize**: Transmit access credential data in a customized method.
  - **Prompt on LCD**: Select **Default** to adopt the Akuvox door phone's door-opening prompt; Select **Return Value** to use the return value from the third-party server as the prompt.
  - **Remote Verification**: Check the access method(s) to be verified by the third-party server. When **Face** is selected, the device performs local face recognition first. If no matching face is detected, authentication fails. If a match is found, the associated **User ID** or **PIN** is submitted to the third-party server for further verification.
  - **HTTP URL**: Enter the HTTP command in a format provided by the third-party service provider. After QR code scanning, card swiping, PIN entry, or facial recognition, the HTTP command will carry the dynamic information automatically before it is sent to the server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan? codeKey={QRCode}/{Card}/{Pin}/{UserID} &deviceId={DeviceID}.* For example, if a user swipes the RF card, the URL will be *http://192.168.35.123:8090/api/visitor/scan? codeKey={QRCode}/45678999/{Pin}/{UserID}&deviceId=1*.

- **Device ID**: The device ID is provided by the third-party server. It will be added to the HTTP command automatically when using the access credential for door access.
- **Success Parameter**: Receiving this value indicates that opening the door succeeds.
- **Failed Parameter**: Receiving this value indicates that opening the door fails.

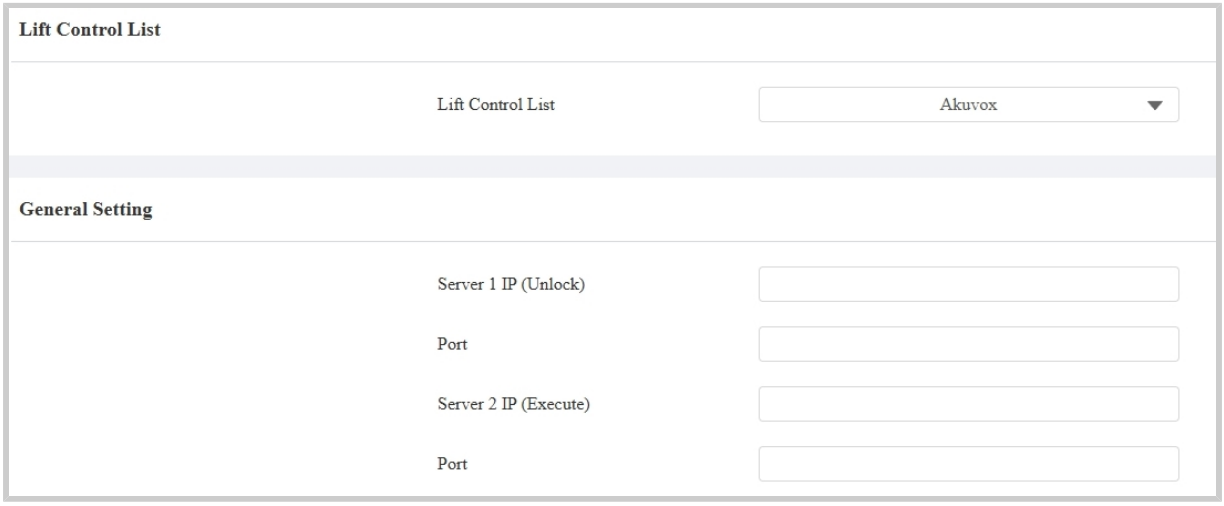
Lift Control

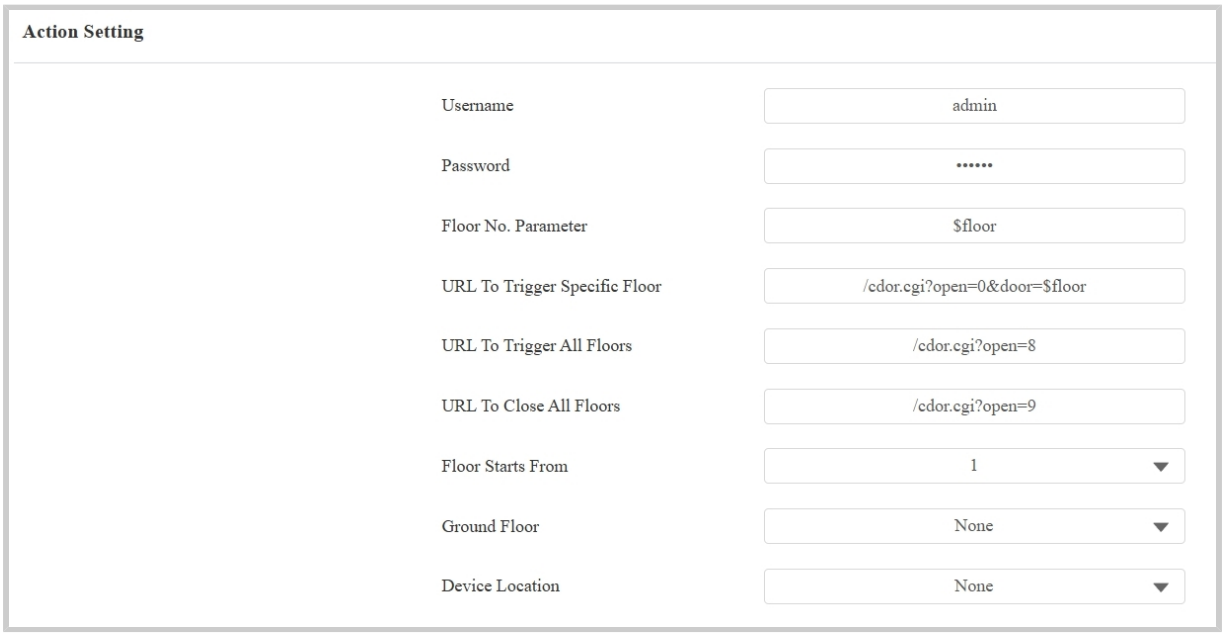
Akuvox Lift Control

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.

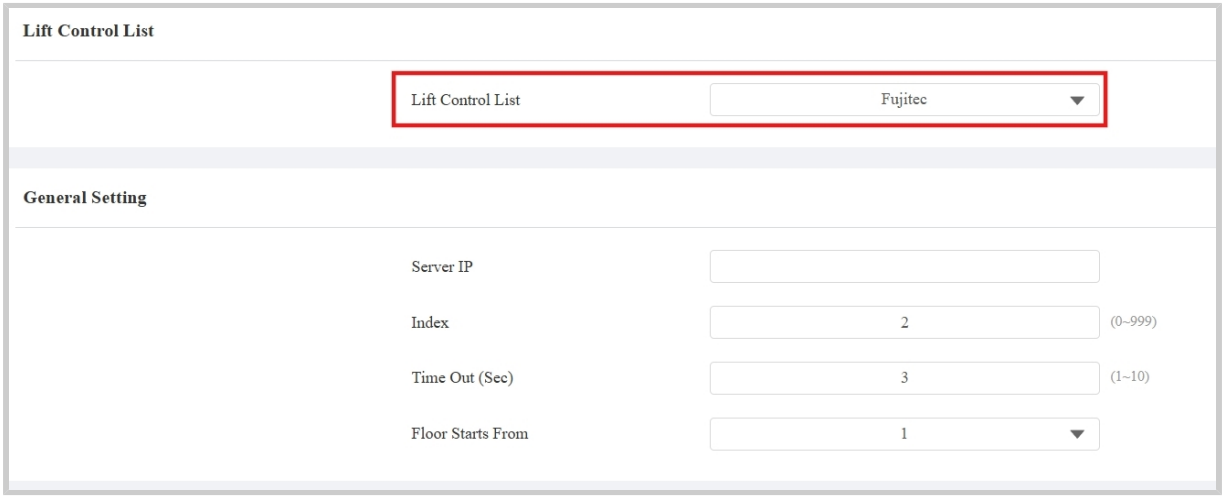
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in 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.

Fujitec Lift Control

The device supports the integration with the Fujitec lift control system. Users can use their credentials configured on the door phone to call the lift and access the destination floor.

Click here to view the detailed guide.

Set it up on the **Device > Lift Control** interface. Select **Fujitec** in the Lift Control List.



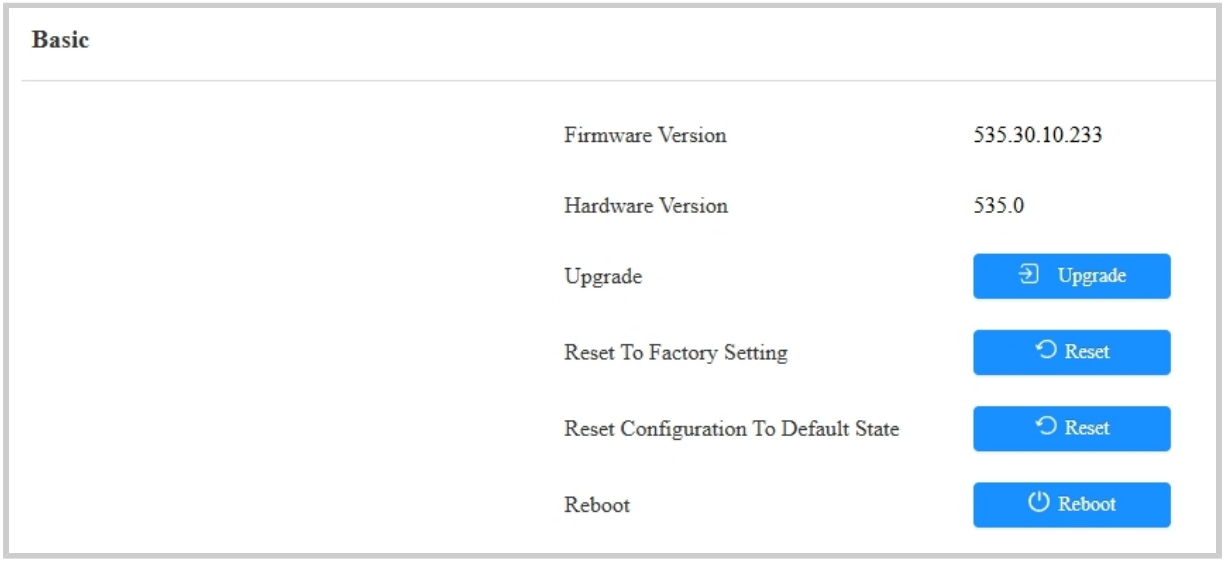
- **Server IP**: The IP address of the Fujitec lift system.
- **Index**: Provided by the Fujitec lift system.
- **Time Out(Sec)**: The timeout period for sending requests to the Fujitec lift system.

- **Floor Starts From**: The starting floor.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



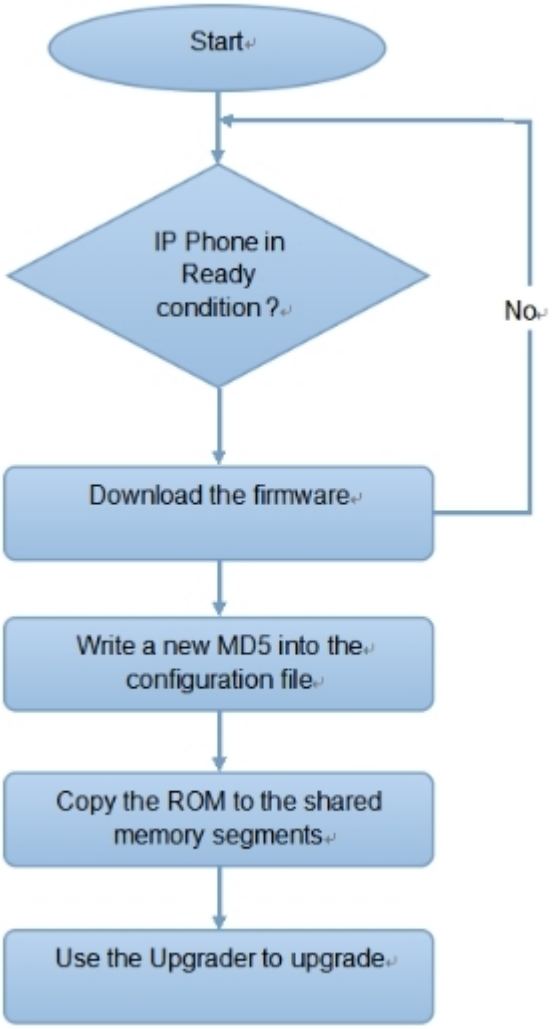
> **Note**
>
> Firmware files should be in .rom format for upgrade.

Auto-provisioning via Configuration File

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

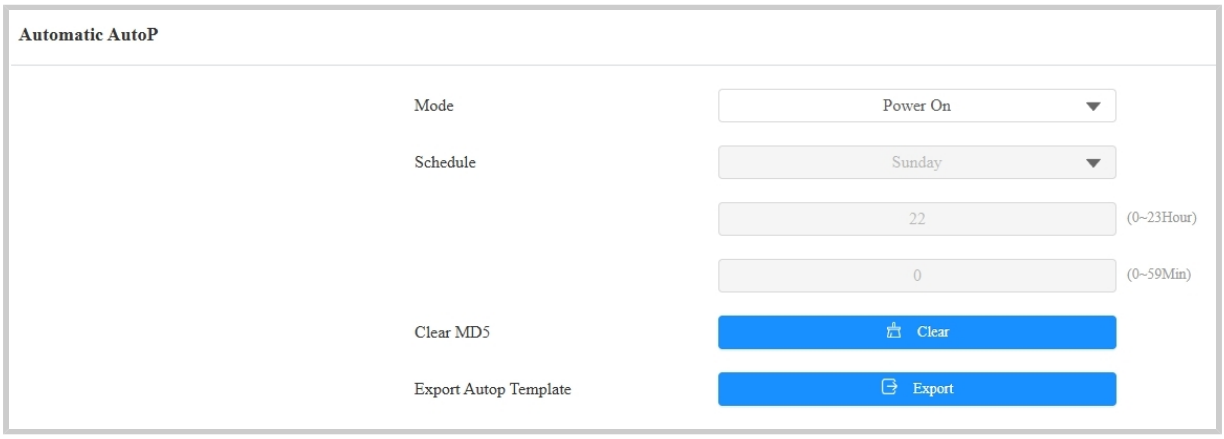
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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.

Set it up on the web **System > Auto Provisioning > Automatic Autop** interface.

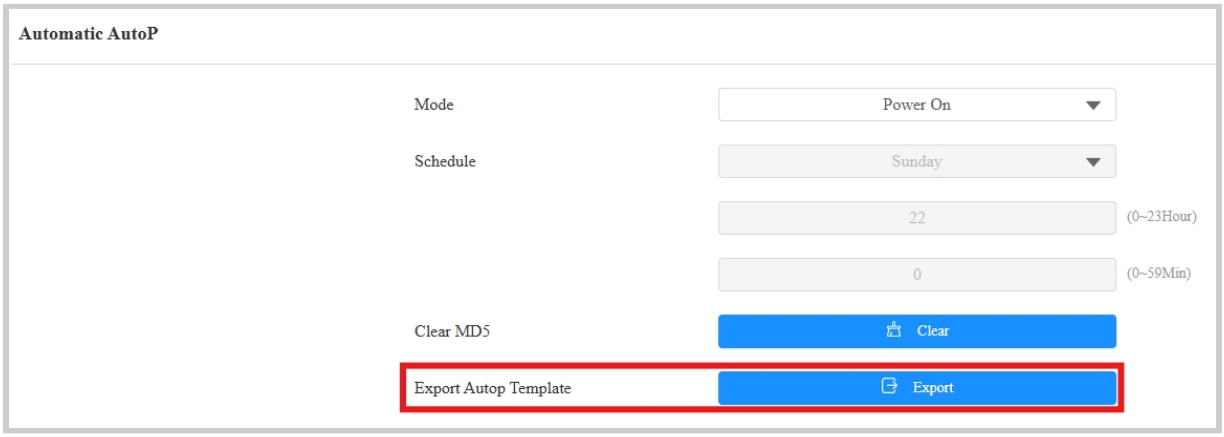


- **Mode**:
  - **Power On**: Allow the device to perform Autop every time it boots up.
  - **Repeatedly**: Allow the device to perform Autop according to the schedule.
  - **Power On + Repeatedly**: Combine Power On and Repeatedly modes, allowing the device to perform Autop every time it boots up or 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.

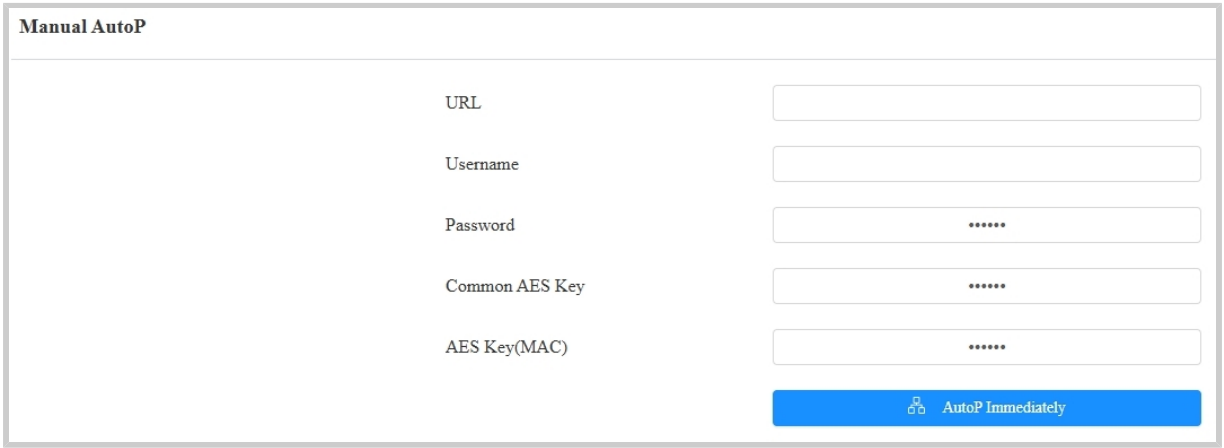
Static Provisioning

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.

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



Set the Autop server on **System > Auto Provisioning > Manual Autop** interface.



- **URL**: The TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Set up a username if the server requires a username to access.

- **Password**: Set up a password if the server requires a password to access.
- **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

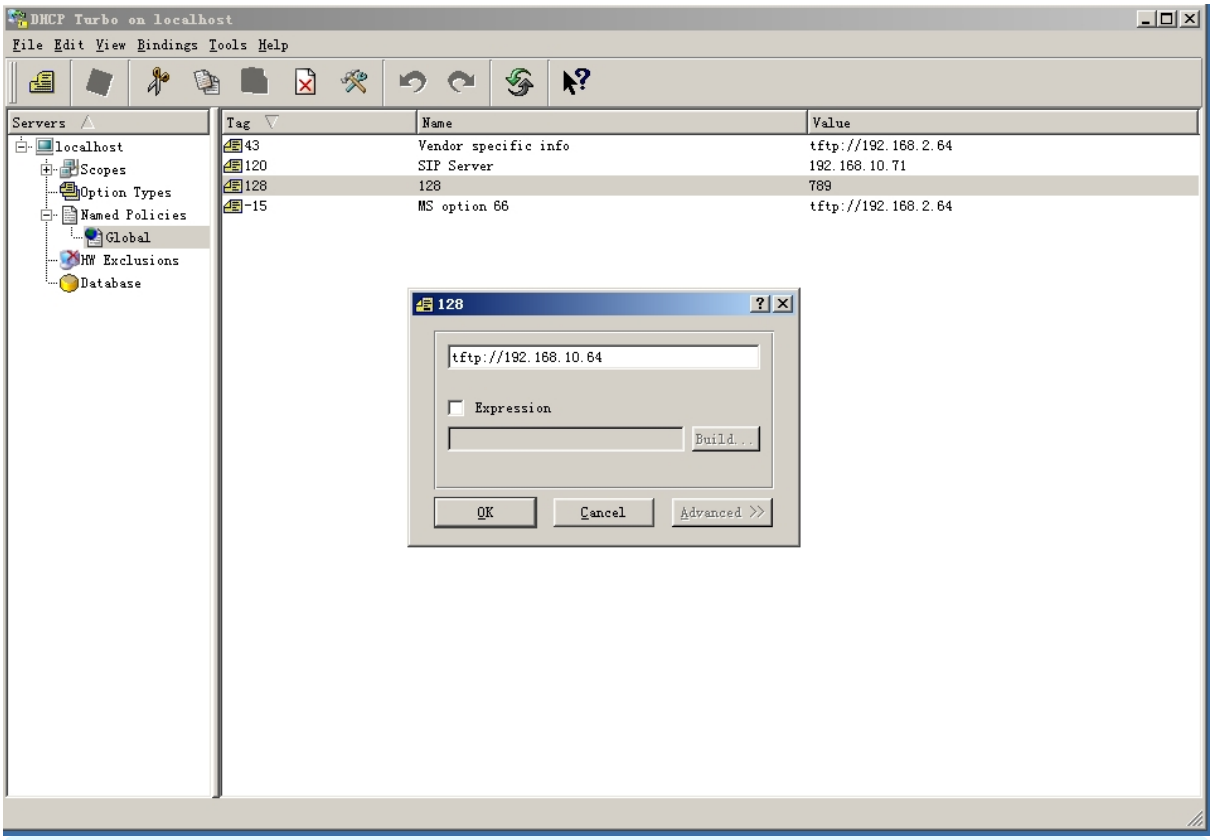
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

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.

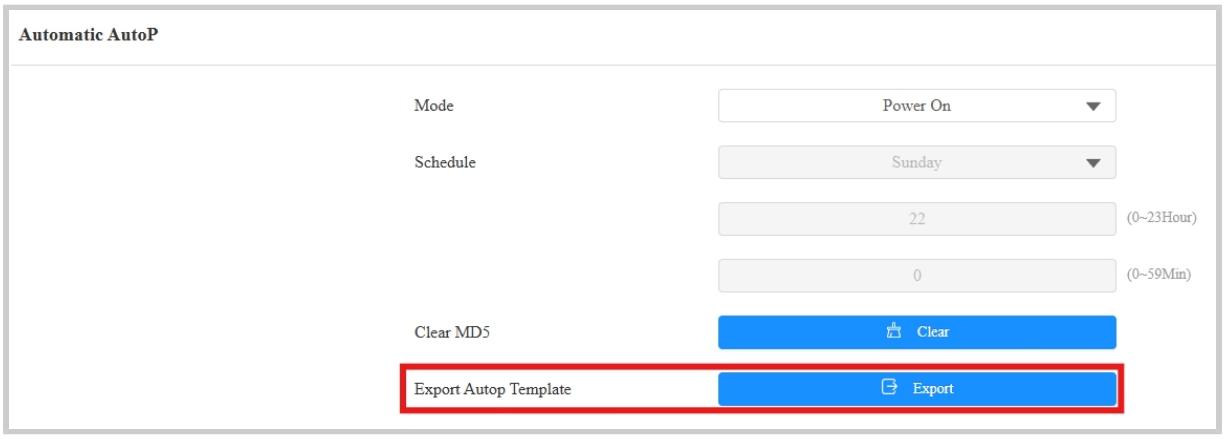


Note

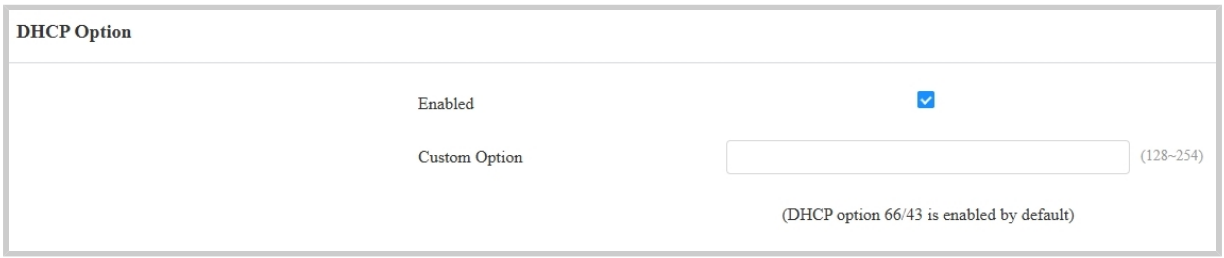
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

Download the Autop template on the **System > Auto Provisioning > Automatic Autop.**



Set it up on **System > Auto Provisioning > DHCP Option** interface.



- **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.

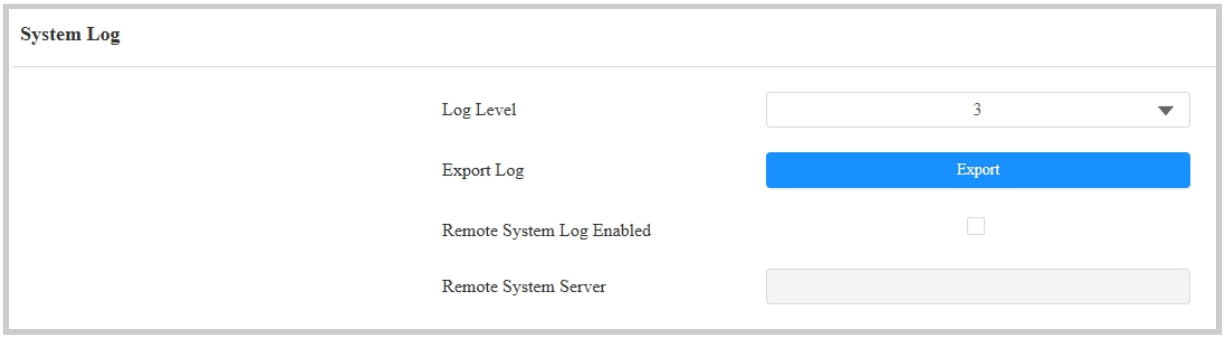
Enable/disable it on the web **System > Auto Provisioning > PNP Option** interface.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Set it up on the web **System > Maintenance > System Log** interface.

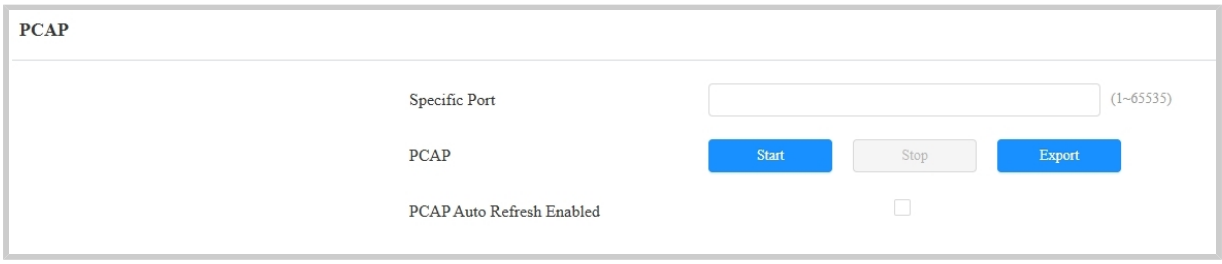


- **Log Level**: Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is **3**. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab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

PCAP for Debugging

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

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

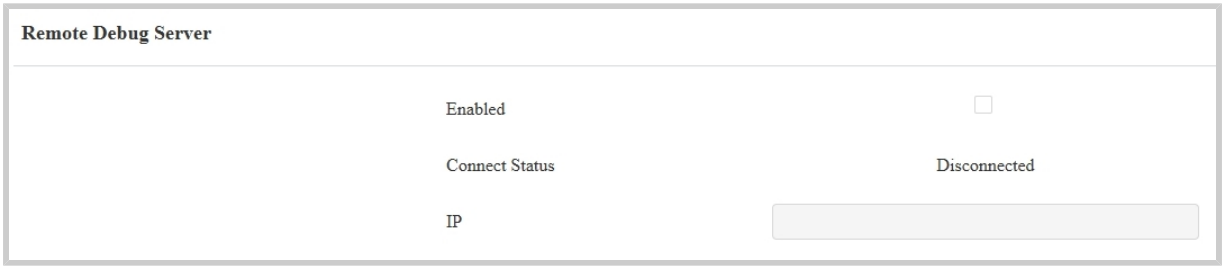


- **Specific Port**: Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the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

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.

Set it up on the **System > Maintenance > Remote Debug Server** interface.



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

Ping

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

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

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

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

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.

Backup

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

Set it up on the web **System > Maintenance > Others** interface. The import file should be in .tgz/.conf/.cfg format.

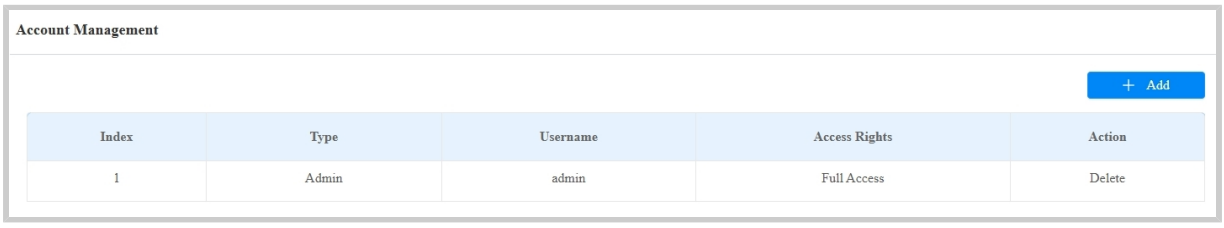
- **Config File**: Click **Export** to export configuration items as an encrypted file; click **Import** to import a configuration file to the device. The Config File includes configuration settings, user data, and contact data.

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.

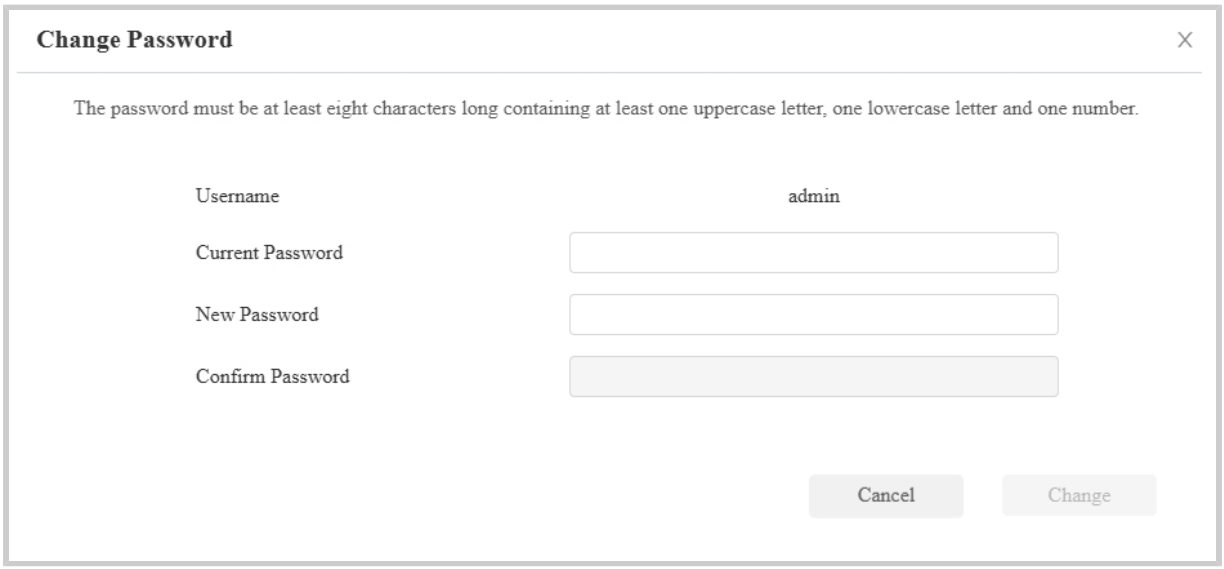


Modify Web Interface Password

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.

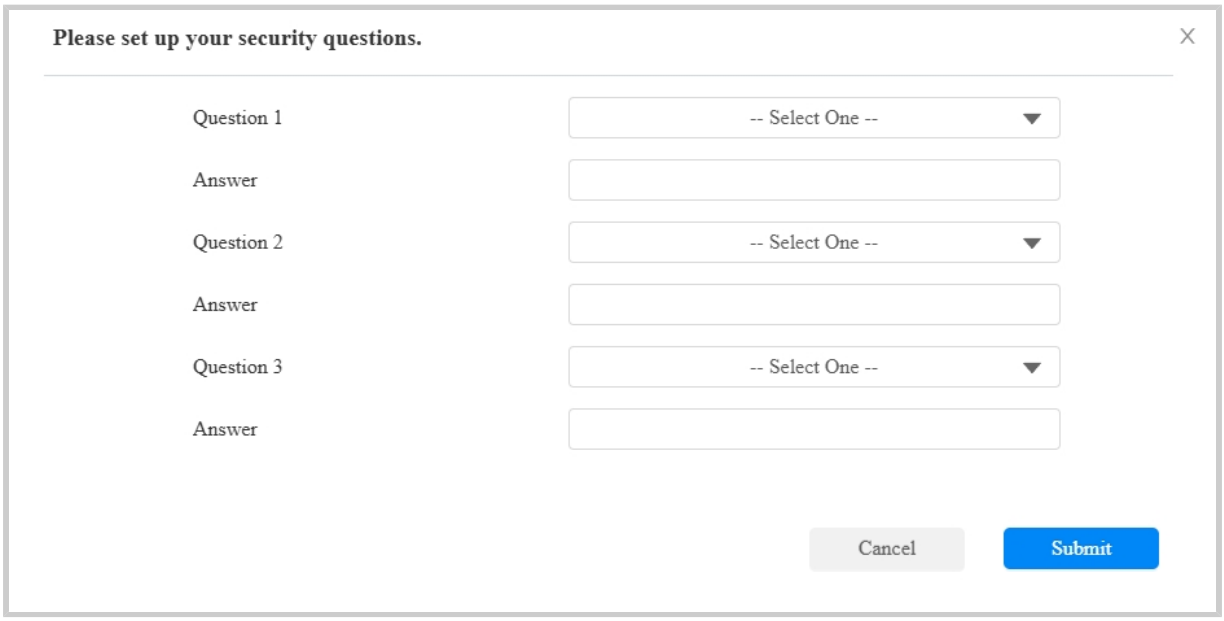


Modify Security Questions

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.



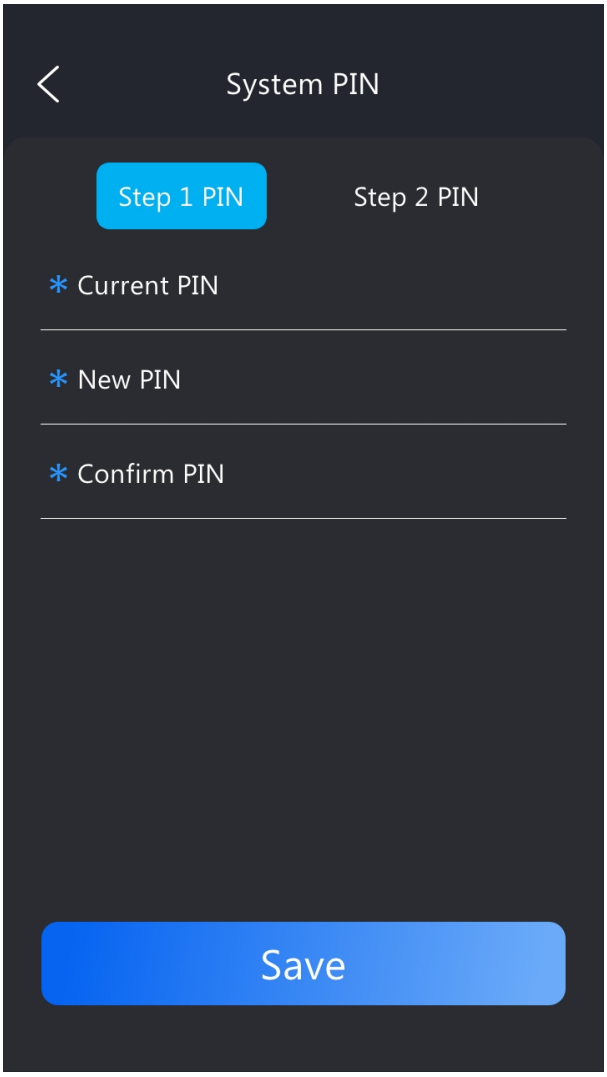
Modify System Password

You can enter the Step1 PIN and then the Step2 PIN on the device's Dial screen to access the system settings.

Change them on the **System > Security > System PIN** interface.

- **Step 1 PIN**: Set a 4-digit password. The default is 9999.
- **Step 2 PIN**: Set a 4-digit password. The default is 3888.

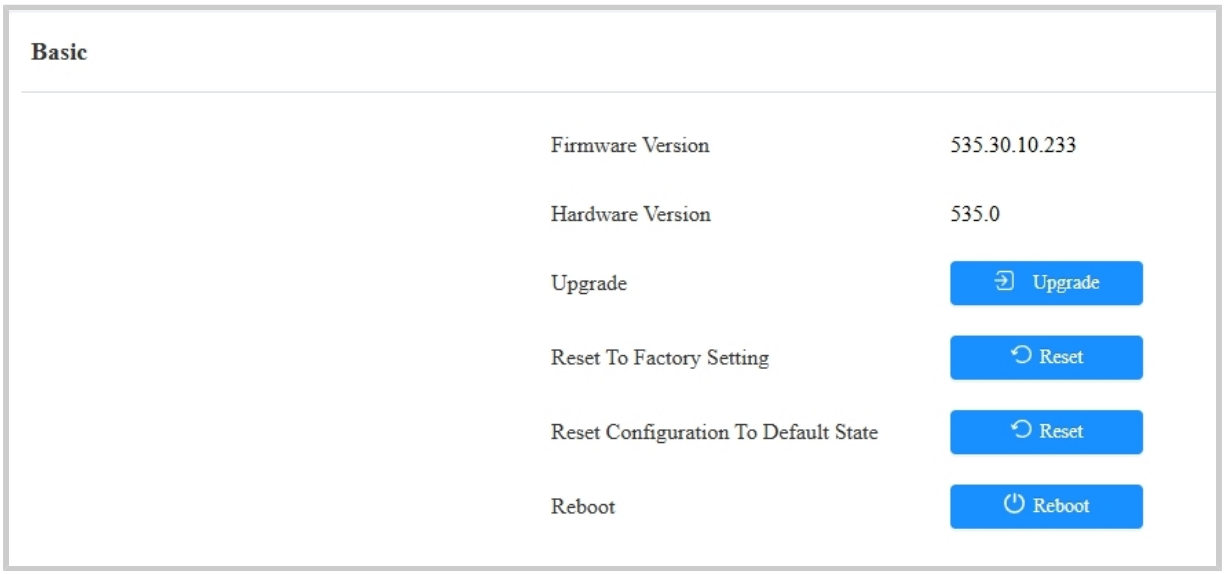
You can also set them up on the **Setting > Security > System PIN** screen.

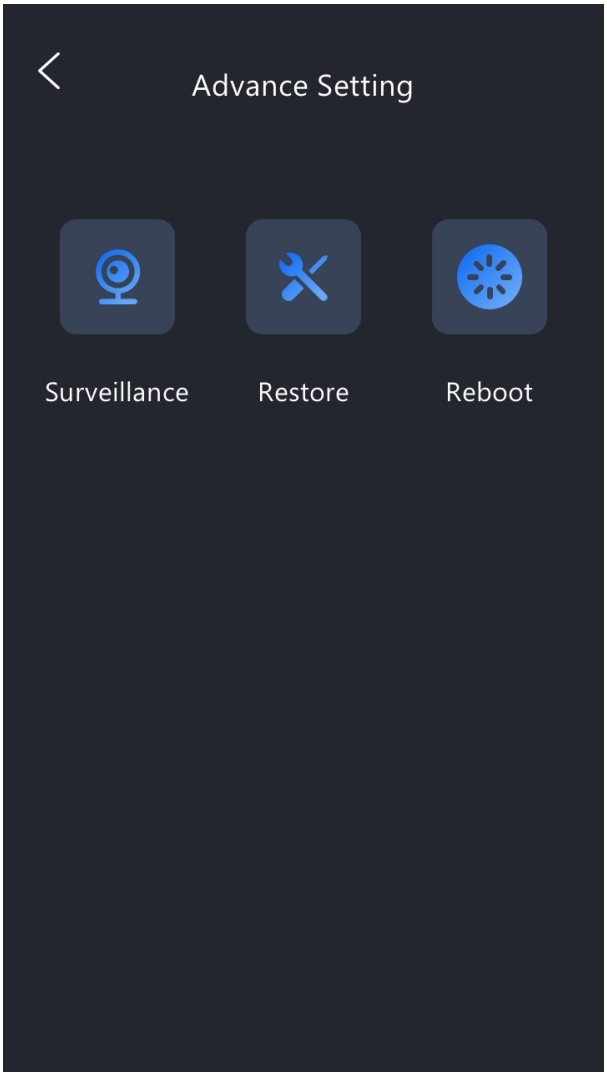

System PIN
Step 1 PIN
Step 2 PIN
* Current PIN
* New PIN
* Confirm PIN
Save

System Reboot&Reset

Reboot

Reboot the device on the web **System > Upgrade** interface, or on the **Setting > Advanced Setting** screen.





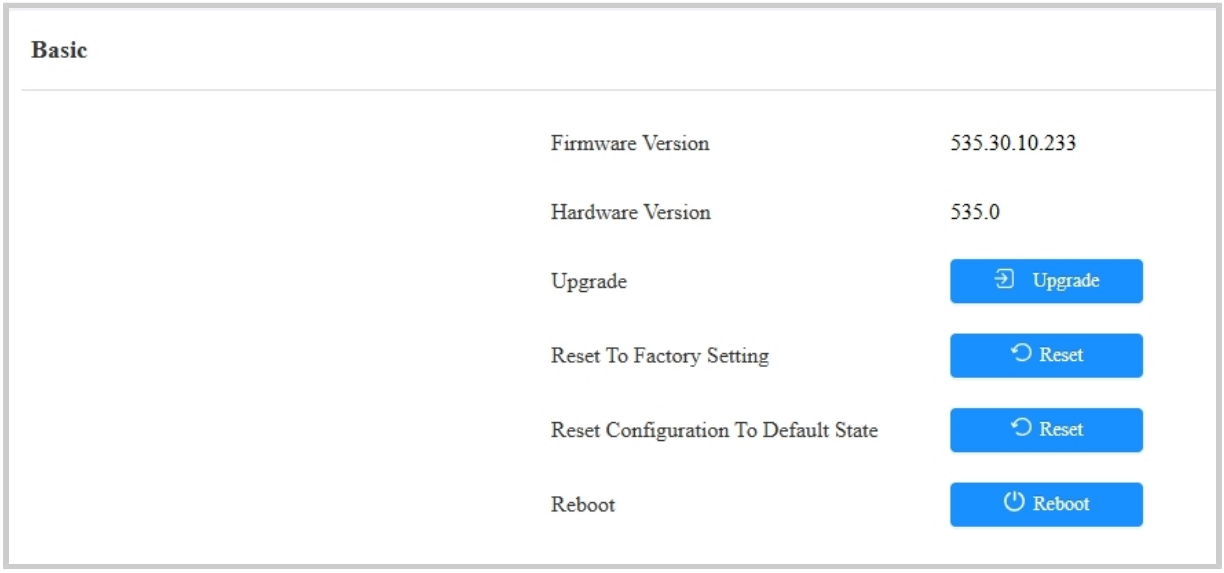
You can set up the reboot schedule on the web **System > Auto Provisioning > Reboot Schedule** interface.

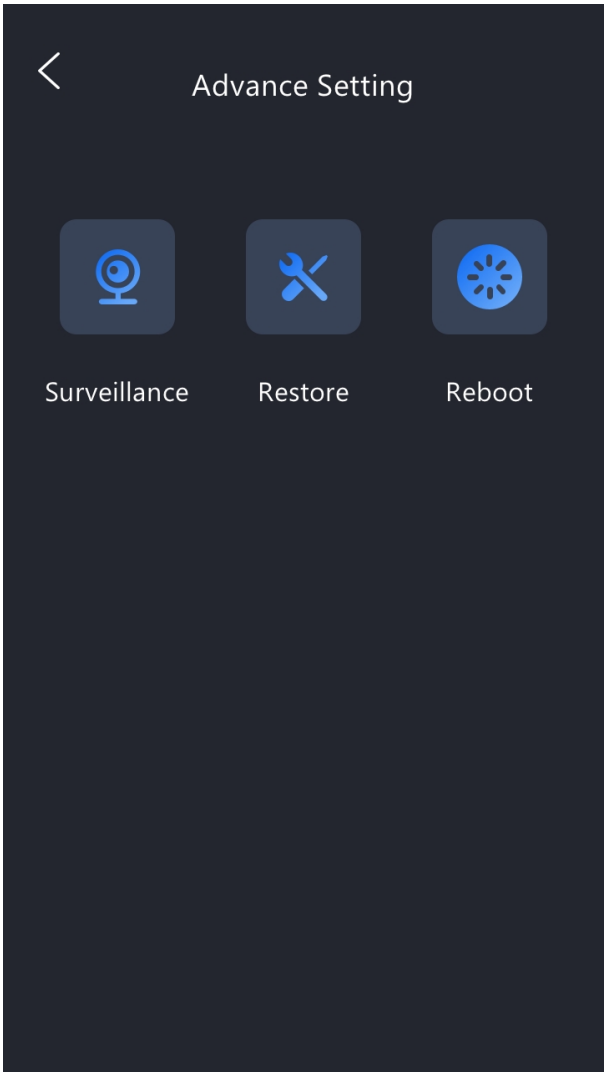
Reset

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, or on the **Setting > Advanced Setting** screen.




Advance Setting
Surveillance
Restore
Reboot

Tip

The device also supports resetting via a physical button on its back.

- Remove its back cover, press the button, and hold it for about 3 seconds.
- The backlight of the card reader area and fill light will light up, and the device will go into factory reset and reboot.