About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

X915 SERIES
DOOR PHONE
Administrator Guide

Thank you for choosing the Akuvox X915 series door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to version 2915.30.10.510, and it provides all the configurations for the functions and features of the X915 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

The Akuvox X915 series is an Android-based IP video door phone with a touch screen. It combines audio and video communication, access control, and video surveillance functionalities. With its advanced Android OS, Cloud, and AI-based communication technology, it offers customizable features to meet your operational preferences. The X915 series supports multiple ports such as RS485 and Wiegand, allowing easy integration with external systems like elevator controllers and fire alarm detectors. This comprehensive solution provides complete control over building entrances and surroundings, ensuring enhanced security through various access methods such as card access, NFC, Bluetooth, QR code, voice-controlled door access, and body temperature measurement, ideal for residential and office buildings as well as complexes.

Changelog

What’s new in version 2915.30.10.510:

- Support speed dial setting in the Villa theme.
- Support customizing door-opening text prompts.
- Support customizing the text prompt on the calling screen.
- Added a switch to turn on the integration with Control4.
- Added Setup Completed action URL.

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

Model Specification

Model	X915S
Touch Screen	✔
Relay In	3
Relay Out	3
Alarm In	X
RS485	✔
Card Reader	13.56MHZ&125KHZ
Wi-Fi	X
Bluetooth	✔
Temperature Detection	Optional
Facial Recognition	✔
LTE	X
USB	X
External SD Card	X

Supported Card Types

The device’s firmware should be 2915.30.10.416 or higher:

- ID Card:
  - EM4100
  - EM4200
  - HID-Prox
  - HID-iClass
    Only X915 V2.0 with an HID-LF or HID-HF module supports reading the HID iClass or HID Prox card. And the firmware version should be 2915.30.10.311 or higher.
- IC Card:
  - Mifare Ultralight C/EV1
  - Mifare Classic Compatible Card
  - Mifare Plus-S 2K
  - Mifare Desfire EV1 2K D21
  - Mifare Desfire EV2 D42
  - Mifare Desfire EV2 D22
  - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
  - NFC Type2 216
  - NFC Type2 215
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Classic ev1 7-byte
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
  - Mifare Classic 1K
  - Mifare S50-1K Card
  - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
  - HID iClass Clamshell Card

- HID-PROXCARD-II Card
  Only X915 V2.0 with an HID-LF or HID-HF module supports reading the HID iClass or HID Prox card. And the firmware version should be 2915.30.10.311 or higher.

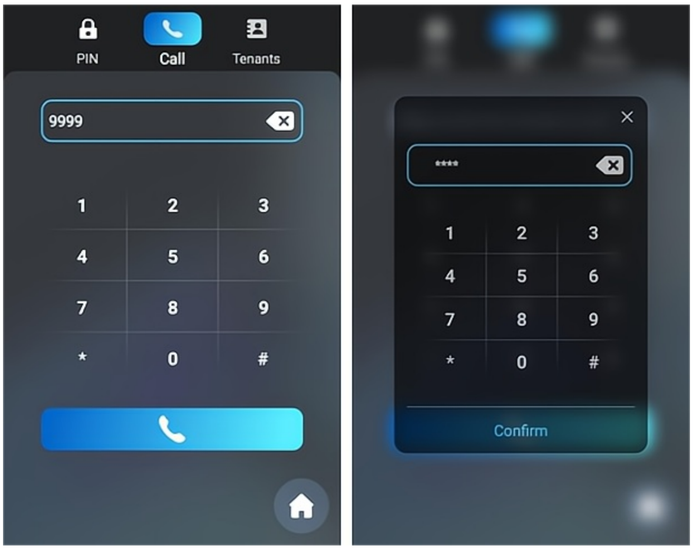
Access the Device

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

Access the Device Settings

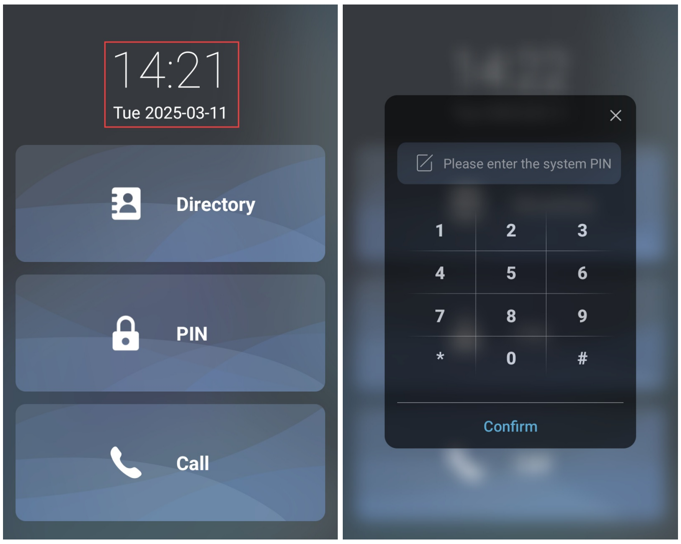
Before configuring the device, please ensure the device is installed correctly and connected to a normal network.

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

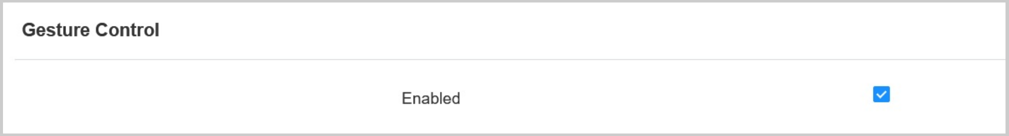


Gesture Control Setting

When the device is in the Building or Villa theme, tap on the time area ten times on the device’s home screen to access the settings screen. The default password is 3888.



To enable the feature, navigate to the web **System > Security > Gesture Control** interface.



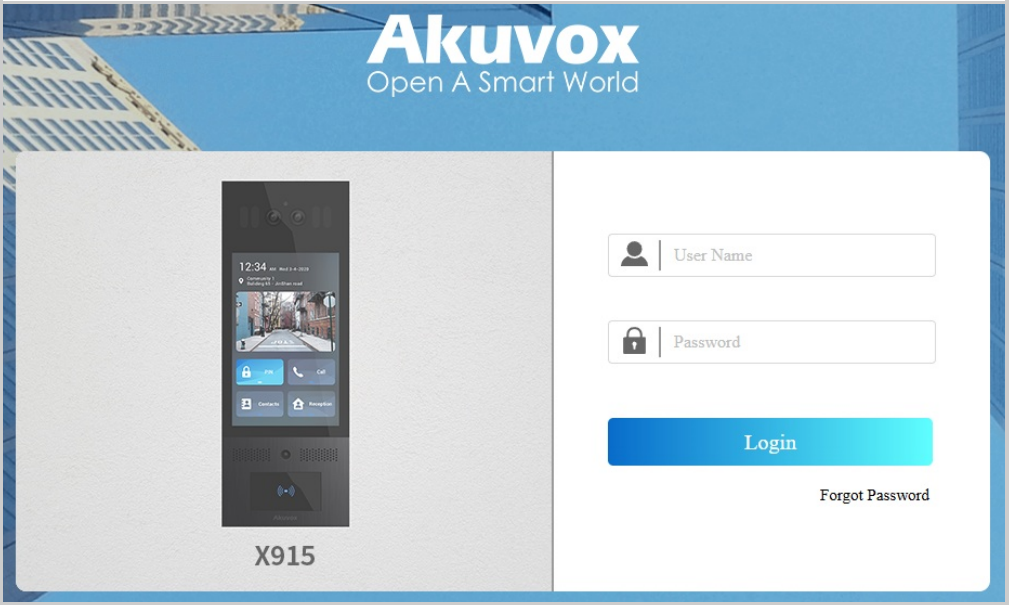
Gesture Control

Enabled ☑

> **Note**
>
> See theme configuration in [Screen Display Configuration] chapter.

Access Device Web Settings

You can use the Akuvox IP scanner tool to search the device's IP address in the same LAN. Then use the IP address to log into the web browser by user name and password **admin** and **admin**.

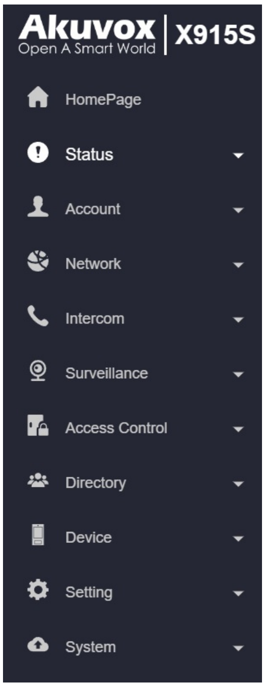


Note

- 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.

Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio and video codec, DTMF, session timer, etc.
- **Network:** This section mainly deals with DHCP & Static IP settings, RTP port settings, device deployment, etc.
- **Intercom:** This section covers intercom settings, call logs, etc.
- **Surveillance:** This section covers motion detection, RTSP, MJPEG, ONVIF, live stream, etc.
- **Access Control:** This section covers input control, relay, card settings, facial recognition, private PIN codes, Wiegand connection, etc.
- **Directory:** This section involves tenant management.
- **Device:** This section includes light settings, tab&button display, LCD settings, and voice settings.
- **Setting:** This section includes time & language, action settings, door settings, and schedule management for access control.
- **System:** This section includes firmware upgrade, automatic auto-provisioning, device maintenance, etc.



Language and Time

Language

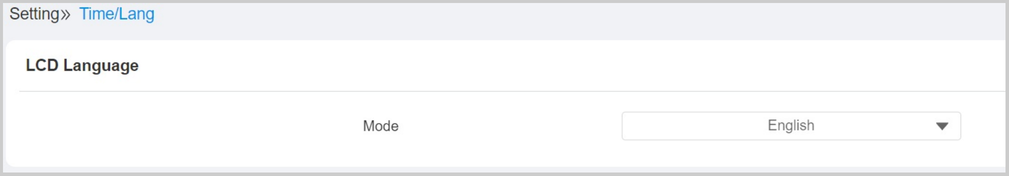
Set up the language during initial device setup or later through the device or web interface according to your preference.

On the Web

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

The device LCD supports the following languages:

- English, Simplified Chinese, Spanish, Danish, French, Czech, Traditional Chinese, Turkish, Japanese, Norwegian, Korean, Russian, Dutch, Polish, Swedish, German, Portuguese, Italian, Ukrainian, Hebrew, Svenska, and Slovenian.



Setting» Time/Lang

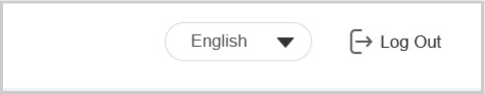
LCD Language

Mode: English

Switch the device web language in the upper right corner.

The device web supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Russian, Portuguese, Spanish, Hebrew, Dutch, French, German, Polish, Japanese, Korean, Italian, and Slovenian.



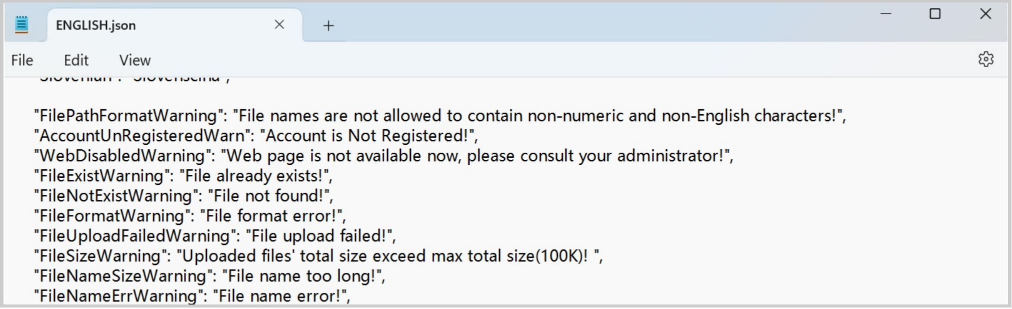
Custom Language

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.

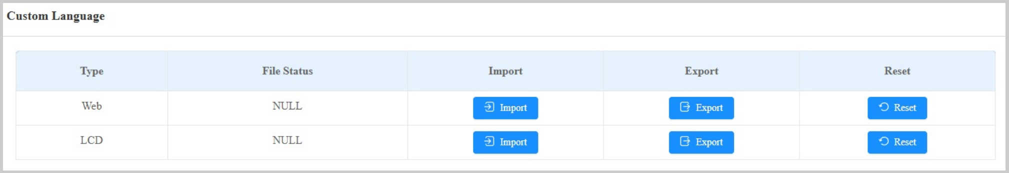
File Example:



```
"Slovenian": "Slovenscina",

"FilePathFormatWarning": "File names are not allowed to contain non-numeric and non-English characters!",
"AccountUnRegisteredWarn": "Account is Not Registered!",
"WebDisabledWarning": "Web page is not available now, please consult your administrator!",
"FileExistWarning": "File already exists!",
"FileNotExistWarning": "File not found!",
"FileFormatWarning": "File format error!",
"FileUploadFailedWarning": "File upload failed!",
"FileSizeWarning": "Uploaded files' total size exceed max total size(100K)! ",
"FileNameSizeWarning": "File name too long!",
"FileNameErrWarning": "File name error!",
```

Set it up on the **Setting > Time/Lang > Custom Language** interface. You can click **Reset** to clear the uploaded texts.

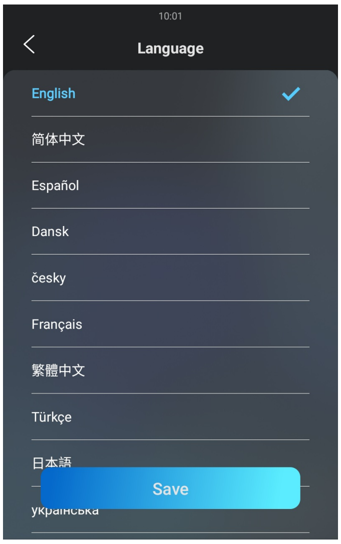


Custom Language

Type	File Status	Import	Export	Reset
Web	NULL	Import	Export	Reset
LCD	NULL	Import	Export	Reset

On the Device

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

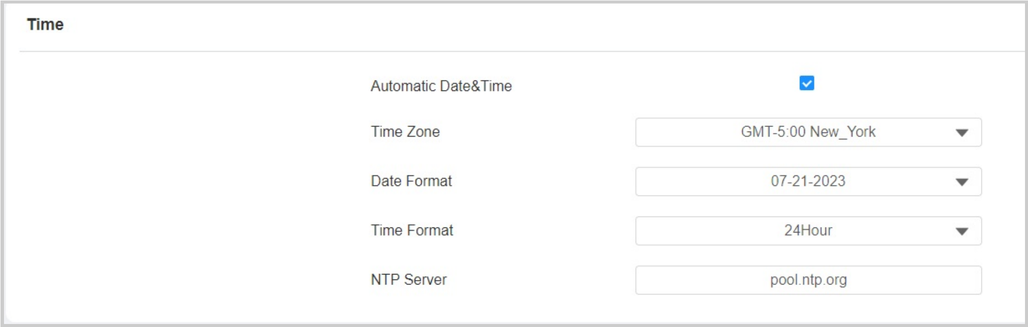


Time

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.



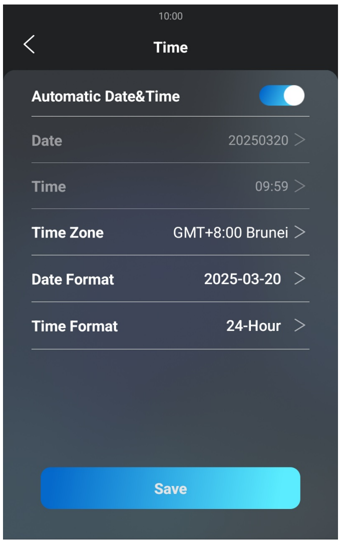
Time

Automatic Date&Time	☑
Time Zone	GMT-5:00 New_York
Date Format	07-21-2023
Time Format	24Hour
NTP Server	pool.ntp.org

- **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.



Automatic Date&Time	●
Date	20250320
Time	09:59
Time Zone	GMT+8:00 Brunei
Date Format	2025-03-20
Time Format	24-Hour

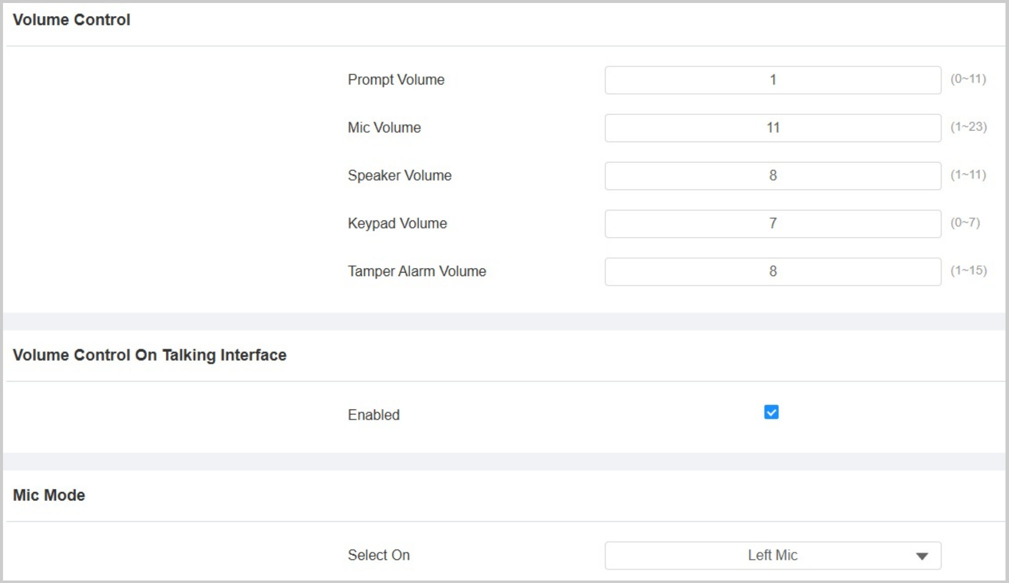
Volume and Tone

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.



Volume Control

Prompt Volume	1	(0~11)
Mic Volume	11	(1~23)
Speaker Volume	8	(1~11)
Keypad Volume	7	(0~7)
Tamper Alarm Volume	8	(1~15)

Volume Control On Talking Interface

Enabled ☑

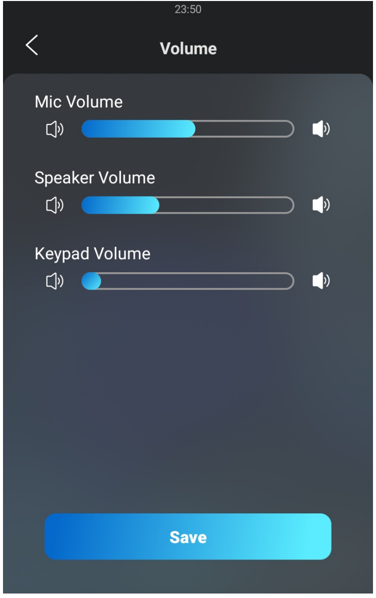
Mic Mode

Select On: Left Mic

- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 9.
- **Mic Volume**: The default is 11.
- **Speaker Volume**: The default is 8.
- **Keypad Volume**: The icon tapping sound. The default is 7.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 8.
- **Volume Control on Talking Interface**: When enabled, users can adjust the call volume during the call session.
- **Mic Mode**: Select which mic to be applied between the left and right microphones.

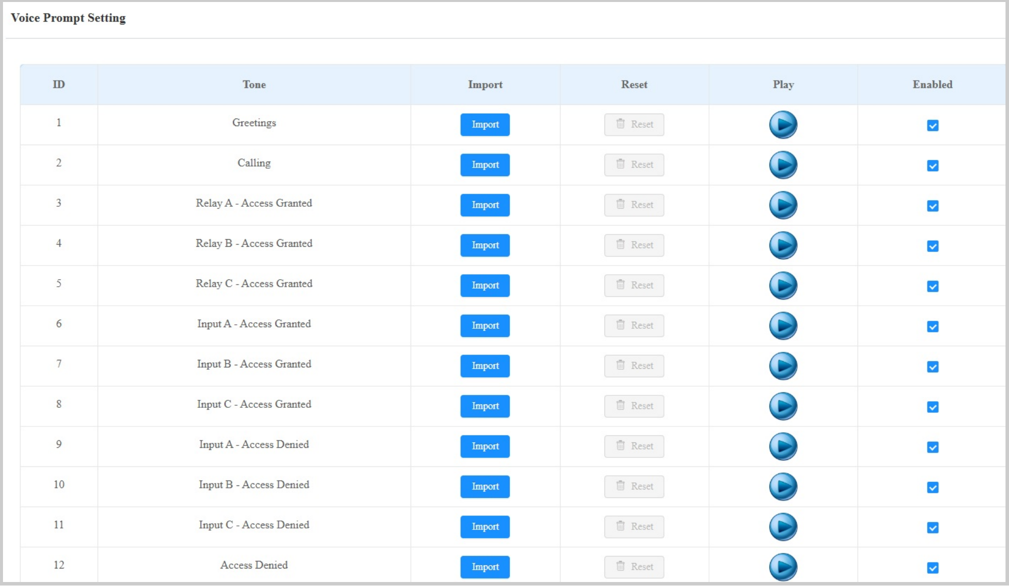
On the Device

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

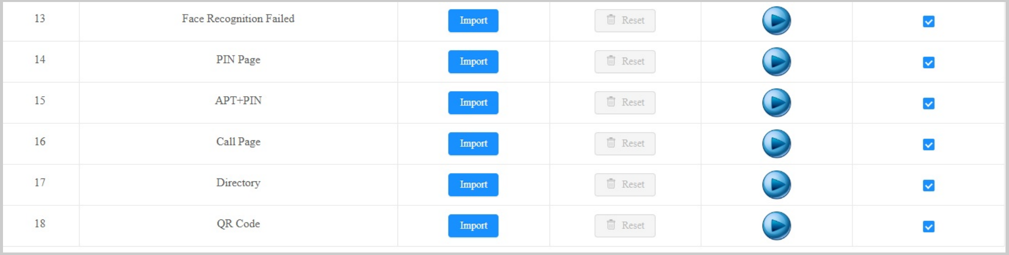


Upload Tones

You can upload the tone for different scenarios on the **Device > Audio > Voice Prompt Setting** interface.



Voice Prompt Setting



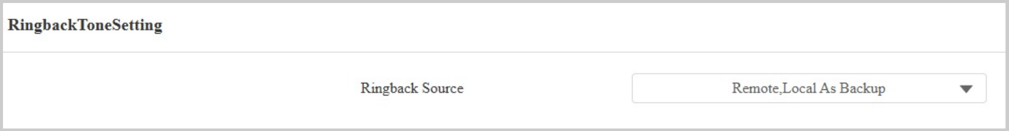
ID	Tone	Import	Reset	Play	Enabled
1	Greetings	Import	Reset	▶	☑
2	Calling	Import	Reset	▶	☑
3	Relay A - Access Granted	Import	Reset	▶	☑
4	Relay B - Access Granted	Import	Reset	▶	☑
5	Relay C - Access Granted	Import	Reset	▶	☑
6	Input A - Access Granted	Import	Reset	▶	☑
7	Input B - Access Granted	Import	Reset	▶	☑
8	Input C - Access Granted	Import	Reset	▶	☑
9	Input A - Access Denied	Import	Reset	▶	☑
10	Input B - Access Denied	Import	Reset	▶	☑
11	Input C - Access Denied	Import	Reset	▶	☑
12	Access Denied	Import	Reset	▶	☑
13	Face Recognition Failed	Import	Reset	▶	☑
14	PIN Page	Import	Reset	▶	☑
15	APT+PIN	Import	Reset	▶	☑
16	Call Page	Import	Reset	▶	☑
17	Directory	Import	Reset	▶	☑
18	QR Code	Import	Reset	▶	☑

> **Note**
>
> File Format: wav/mp3; 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 **Intercom > Call Feature** interface.



RingbackToneSetting

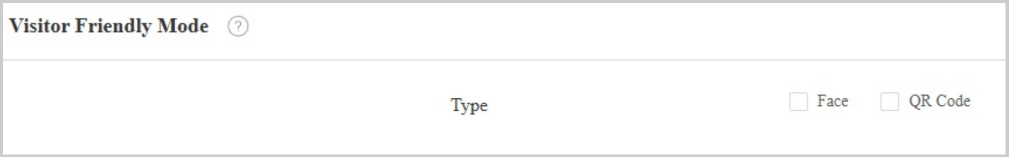
Ringback Source: Remote,Local As Backup

- **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.

Visitor-friendly Mode

This feature decides whether to give auditory or visual prompts when recognition fails.

Set it up on the **Device > Audio > Visitor-friendly Mode** interface.



Visitor Friendly Mode

Type □ Face □ QR Code

- **Face**: When enabled, no prompts are given when facial recognition fails.
- **QR Code**: When enabled, no prompts are given when scanning QR codes fails.

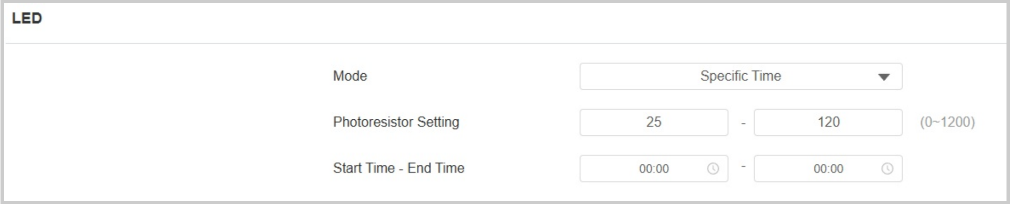
LED and LCD

Infrared LED Setting

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

On the Web

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



LED

Mode: Specific Time

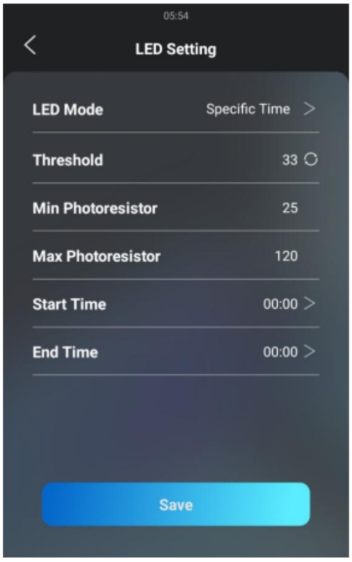
Photoresistor Setting: 25 - 120 (0~1200)

Start Time - End Time: 00:00 - 00:00

- **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. Beyond the schedule, the device adopts Auto mode.
- **Photoresistor Setting**: Set the minimum and maximum photoresistor value to automatically control the ON-OFF of the LED fill light(25 to 120 by default). The higher the value, the brighter the light is. If the photoresistor value is less than the minimum threshold, turn on the fill light. If it is greater than the maximum threshold, turn it off.

On the Device

Set up the LED on the **Setting > Basic Setting > Display > LED Setting** screen.



05:54

LED Setting

LED Mode: Specific Time

Threshold: 33

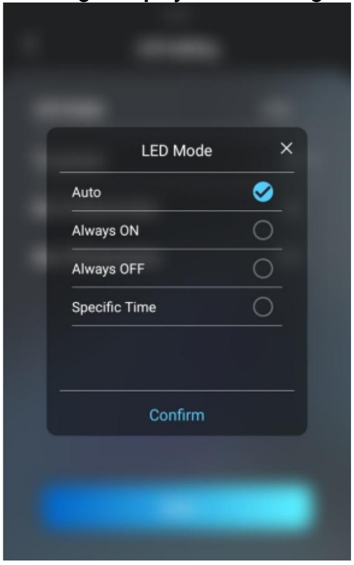
Min Photoresistor: 25

Max Photoresistor: 120

Start Time: 00:00

End Time: 00:00

Save



LED Mode

● Auto

○ Always ON

○ Always OFF

○ Specific Time

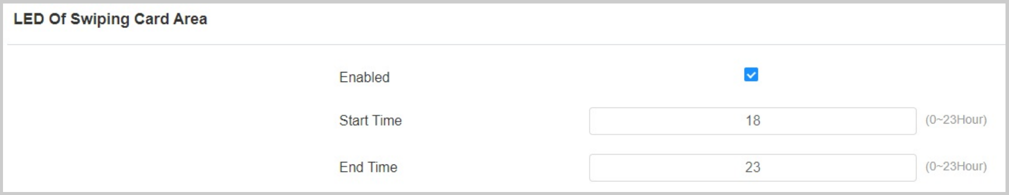
Confirm

- **LED 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.
  - **Specific Time**: Turn on the infrared LED based on the schedule. Specify the Start Time and End Time when this option is selected.
- **Threshold**: The current light intensity indicated by the photo-resistor value. The higher the value, the brighter the light is. The default photo-resistor value (**Threshold**) is 33. You can tap the circle icon several times to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is the basis of configuring the minimum and maximum photo-resistor values.
- **Min/Max Photoresistor**: Set the minimum and maximum photoresistor value to automatically control the ON-OFF of the LED fill light(25 to 120 by default). If the photoresistor value is less than the minimum threshold, turn on the fill light. If it is greater than the maximum threshold, turn it off.

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.

Set it up on the web **Device > Light > LED Of Swiping Card Area** interface.



LED Of Swiping Card Area

Enabled	☑	
Start Time	18	(0~23Hour)
End Time	23	(0~23Hour)

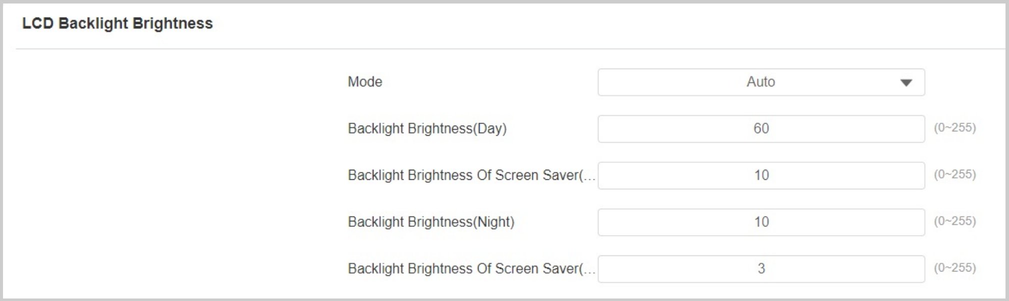
- **Start Time- End Time (H)**: Enter the time for the LED lighting to be valid, e.g., if the time is set from 8-0 (Start time-End time), it means the LED light will stay on during the time from 8:00 am to 12:00 pm during one day (24 hours).

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 > Light > LCD Backlight Brightness** interface.



LCD Backlight Brightness

Mode	Auto	
Backlight Brightness(Day)	60	(0~255)
Backlight Brightness Of Screen Saver(...	10	(0~255)
Backlight Brightness(Night)	10	(0~255)
Backlight Brightness Of Screen Saver(...	3	(0~255)

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

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

- **Backlight Brightness (Day)**: Select the brightness value from 0-255. The default value is 200. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screen Saver (Day)**: Adjust the backlight for the screensaver in the daytime with the value ranging from 0-255.
- **Backlight Brightness (Night)**: Select the brightness value from 0-255. The default value is 200. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screen Saver (Night)**: Adjust the backlight for the screensaver in the nighttime with the value ranging from 0-255.

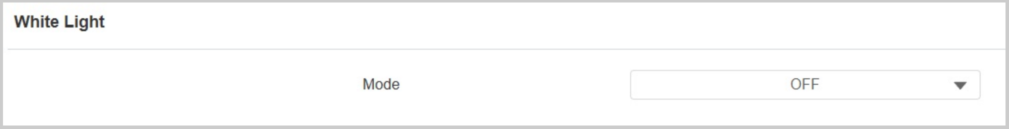
On the Device

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

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.



White Light

Mode: OFF

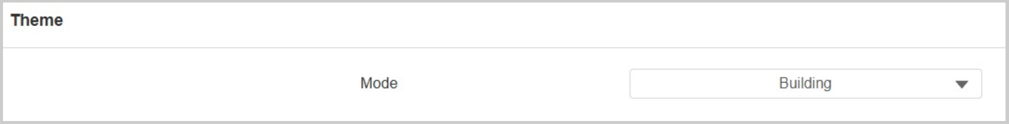
- **Mode**: Select **Auto** or **OFF**. If you select **Auto**, the white light will turn on for 5 minutes for facial recognition and QR code scan.

Screen Display

Home Screen Display

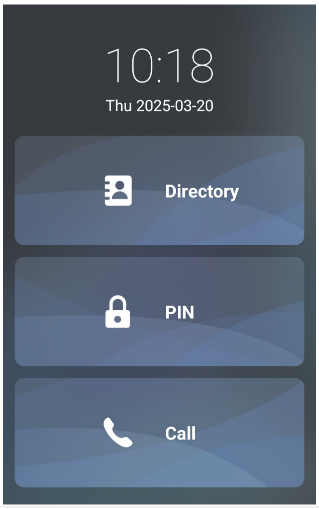
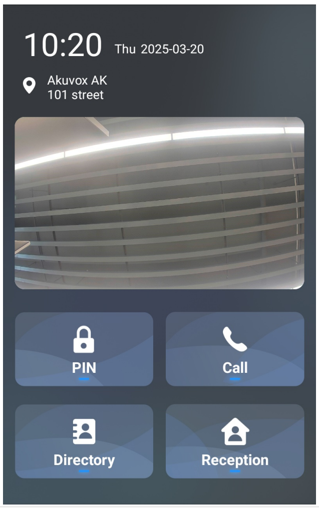
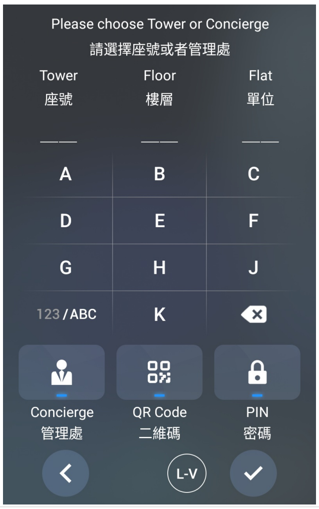
The device supports Villa, Building, and Alphanumeric themes. You can apply the desired theme for different scenarios.

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



Theme

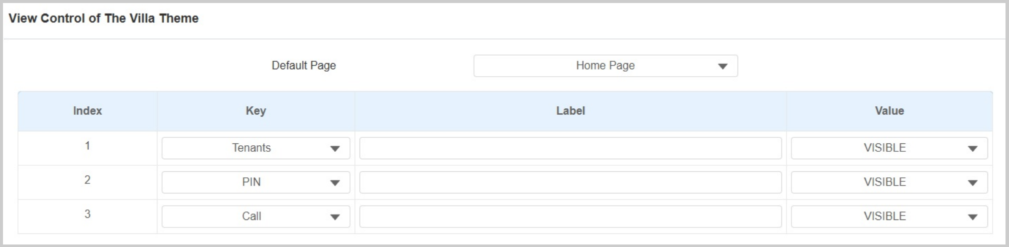
Mode: Building

Villa	Building	Alphanumeric
		

Villa Theme

You can configure the screen display for the layout of the Tenant icon, PIN icon, and Call icon on the home screen in Villa mode.

Set it up on the **Setting > Key/Display > View Control of The Villa Theme** interface.



View Control of The Villa Theme

Default Page: Home Page

Index	Key	Label	Value
1	Tenants		VISIBLE
2	PIN		VISIBLE
3	Call		VISIBLE

- **Default Page**: Select the homepage display type.
  - **Home Page**: The default display with three vertical round icons, Contact, 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.

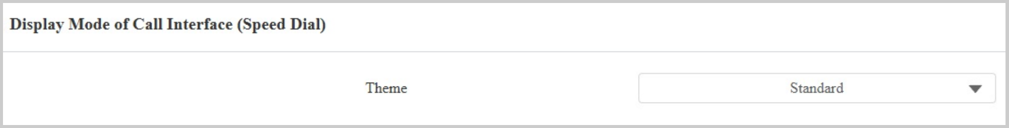
> **Note**
>
> If you switch from Building mode to Villa mode and your previous home screen was set to Home Page, the three round icons for Tenants, PIN, and Call will be displayed. However, if your previous display type was Call, Tenants, or PIN, only the corresponding highlighted icons will appear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



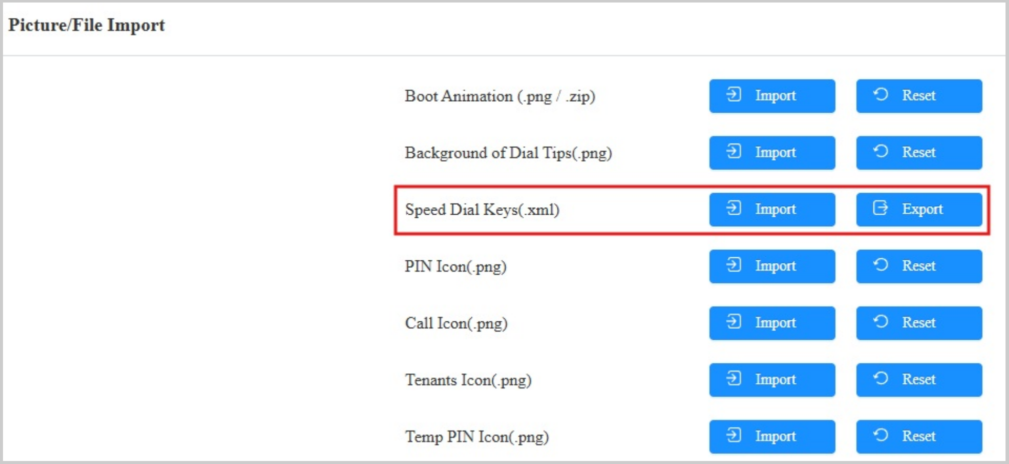
Display Mode of Call Interface (Speed Dial)

Theme: Standard

Options	Descriptions
Standard	Display time and keypad.
Auto	Display all speed dail 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.

You can import and export speed dial numbers for quick setup.

Scroll to the **Picture/File Import** section.

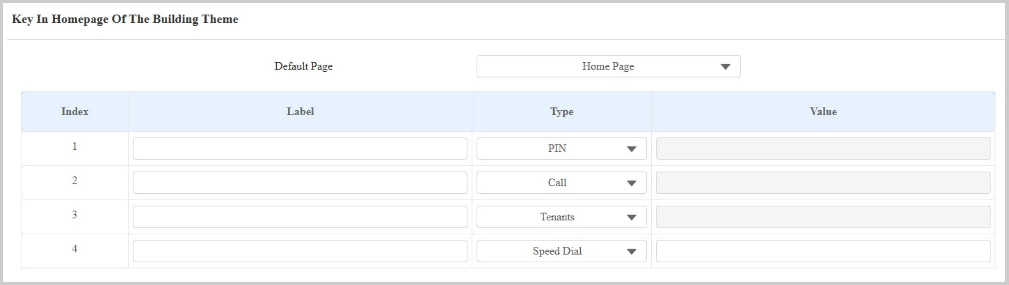


Picture/File Import

Boot Animation (.png / .zip)	Import	Reset
Background of Dial Tips(.png)	Import	Reset
Speed Dial Keys(.xml)	Import	Export
PIN Icon(.png)	Import	Reset
Call Icon(.png)	Import	Reset
Tenants Icon(.png)	Import	Reset
Temp PIN Icon(.png)	Import	Reset

Building Theme

You can set up the key display in the Building theme on the **Setting > Key/Display > Key In Homepage Of The Building Theme** interface.



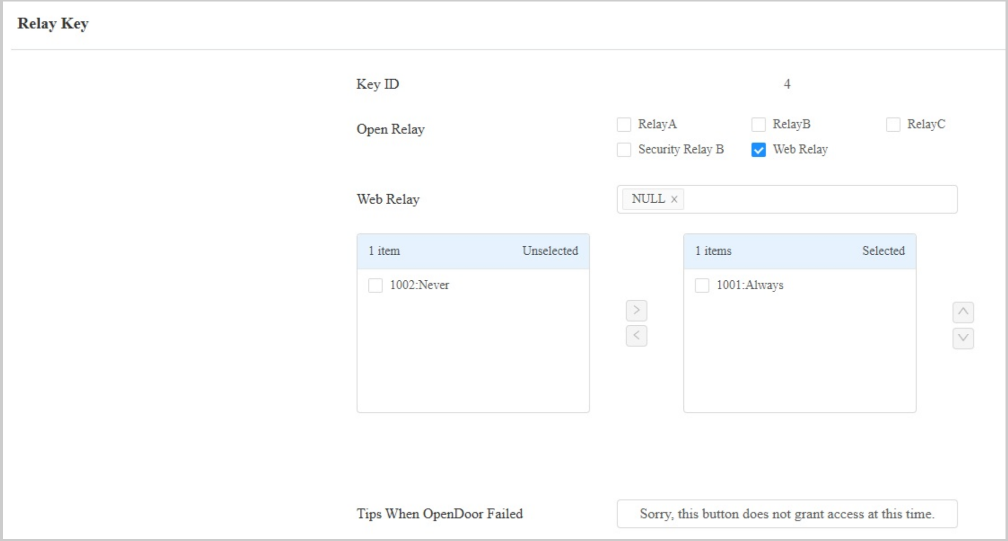
Key In Homepage Of The Building Theme

Default Page: Home Page

Index	Label	Type	Value
1		PIN	
2		Call	
3		Tenants	
4		Speed Dial	

- **Default Page**: Select the homepage display type.
  - **Home Page**: The default displays PIN, Call, Directory, and Reception tabs and the facial recognition box.

  - **PIN**: Display the PIN entry screen.
  - **Tenants**: Display the directory screen.
  - **Call**: Display the dial screen.
  - **Temp Key**: Display the temp key entry and the QR code scanning screen.
- **Label**: Name the key. The name will not change the attribute of the key.
- **Value**: It is available for those features that need to be set up with numbers, such as Speed Dial.
- **Type**: Select the key type.
  - When **Relay** is selected, you can specify which relay to open and apply a schedule within which the relay remains activated.



Relay Key

Key ID: 4

Open Relay: □ RelayA □ RelayB □ RelayC □ Security Relay B ☑ Web Relay

Web Relay: NULL ×

1 item	Unselected
□ 1002:Never	

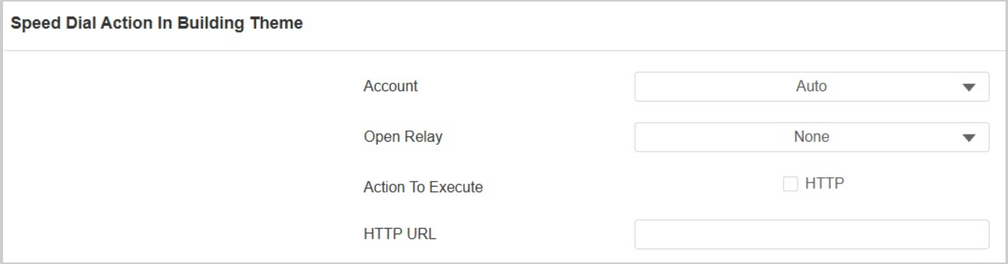
1 items	Selected
□ 1001:Always	

Tips When OpenDoor Failed: Sorry, this button does not grant access at this time.

Speed Dial Action in Building Theme

You can set up the reception tab in the Building 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.



Speed Dial Action In Building Theme

Account: Auto

Open Relay: None

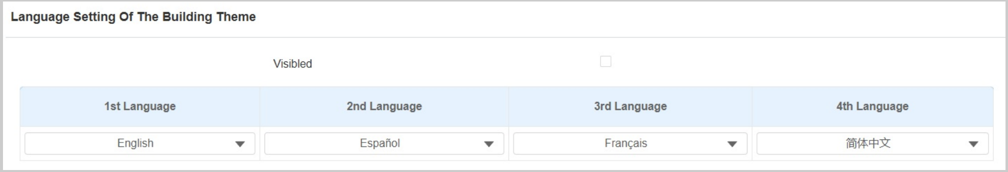
Action To Execute: □ HTTP

HTTP URL:

- **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 theme on the **Setting > Key/Display > Language Setting of The Building Theme** interface.



Language Setting Of The Building Theme

Visibled: □

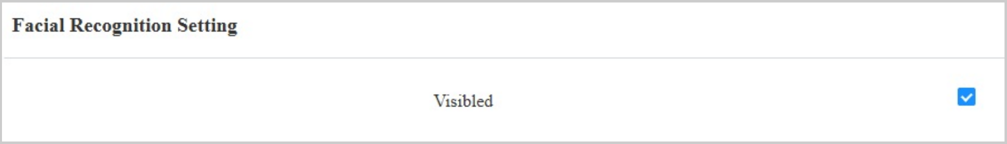
1st Language	2nd Language	3rd Language	4th Language
English	Español	Français	简体中文

- **Visible**: 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.

Facial Recognition Display

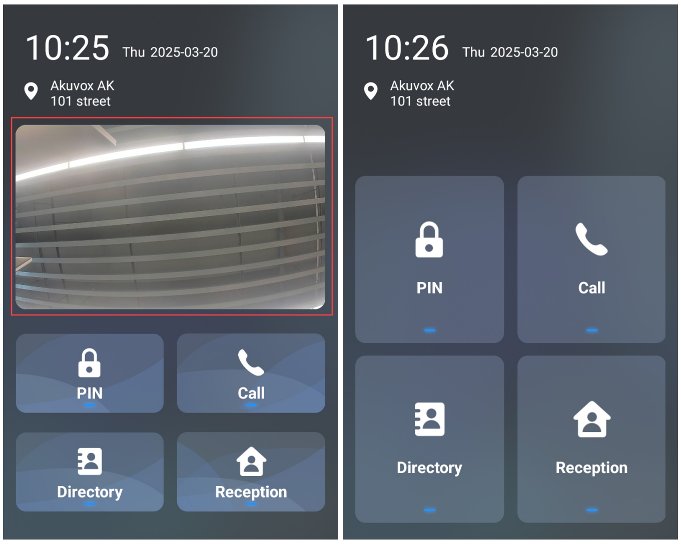
You can turn on or off the facial recognition scanning box in the Building theme.

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



Facial Recognition Setting

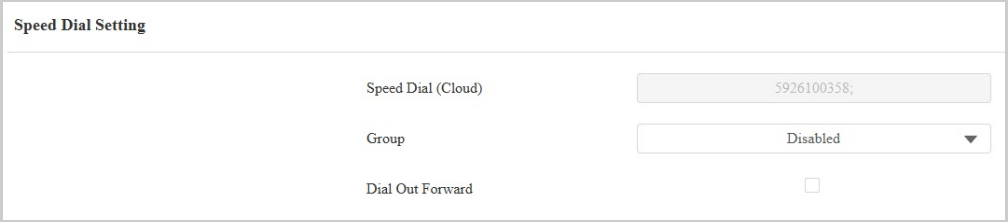
Visibled ☑



Speed Dial Setting in Building/Villa 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 Setting

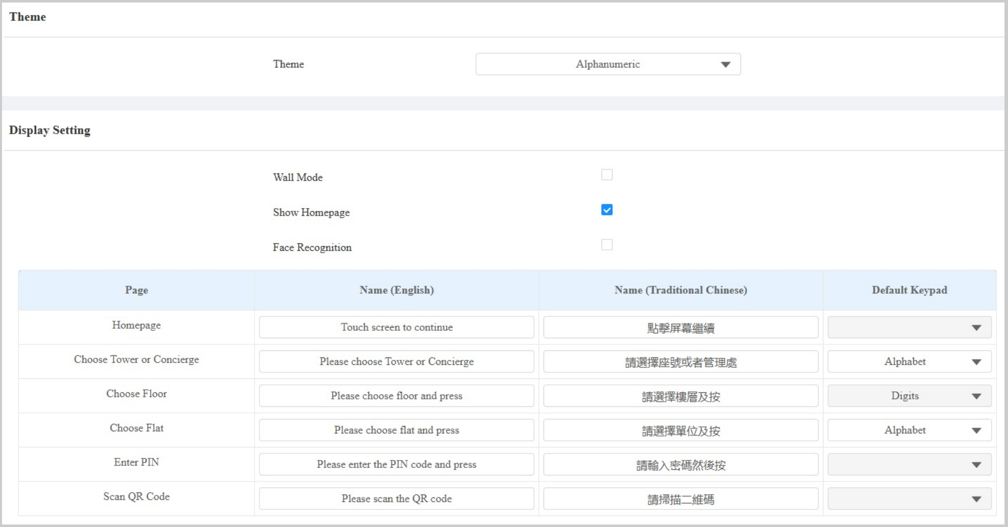
Speed Dial (Cloud)	5926100358;
Group	Disabled
Dial Out Forward	□

- **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 calls will be made to the same target number when pressing the Reception button.
    - **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.

Alphanumeric Theme

The Alphanumeric Theme is used in the apartment with room number that carries both English alphabetic and numbers.

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



Theme

Theme: Alphanumeric

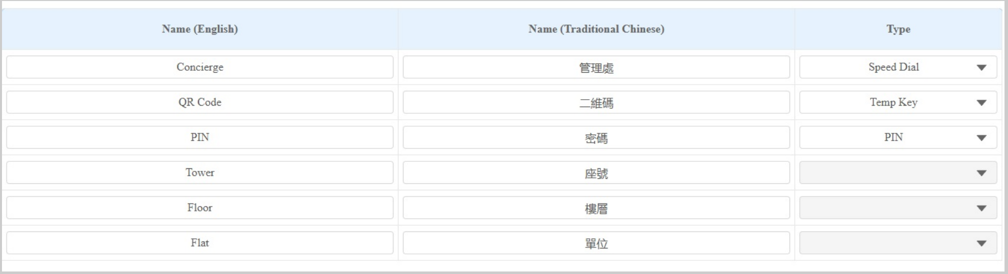
Display Setting

Wall Mode □

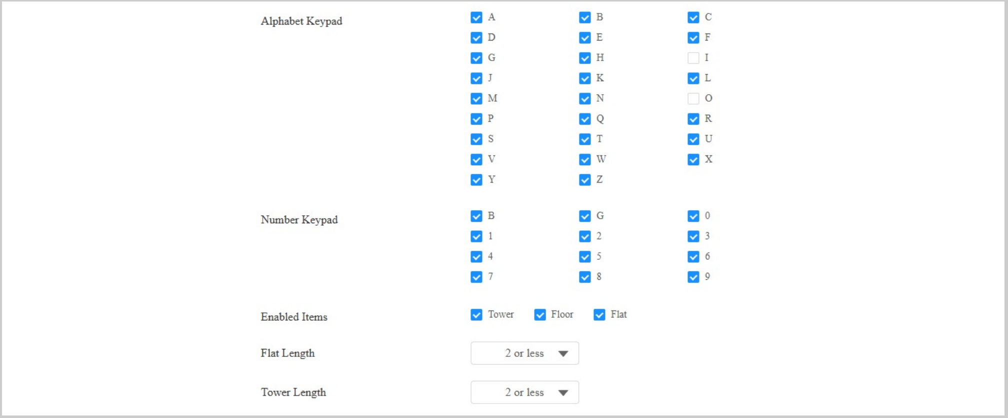
Show Homepage ☑

Face Recognition □

Page	Name (English)	Name (Traditional Chinese)	Default Keypad
Homepage	Touch screen to continue	點擊屏幕繼續	
Choose Tower or Concierge	Please choose Tower or Concierge	請選擇座號或者管理處	Alphabet
Choose Floor	Please choose floor and press	請選擇樓層及按	Digits
Choose Flat	Please choose flat and press	請選擇單位及按	Alphabet
Enter PIN	Please enter the PIN code and press	請輸入密碼然後按	
Scan QR Code	Please scan the QR code	請掃描二維碼	



Name (English)	Name (Traditional Chinese)	Type
Concierge	管理處	Speed Dial
QR Code	二維碼	Temp Key
PIN	密碼	PIN
Tower	座號	
Floor	樓層	
Flat	單位	



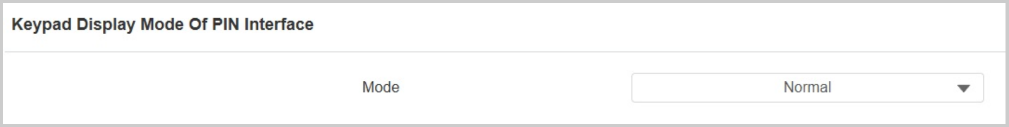
Alphabet Keypad	☑ A	☑ B	☑ C
	☑ D	☑ E	☑ F
	☑ G	☑ H	□ I
	☑ J	☑ K	☑ L
	☑ M	☑ N	□ O
	☑ P	☑ Q	☑ R
	☑ S	☑ T	☑ U
	☑ V	☑ W	☑ X
	☑ Y	☑ Z	
Number Keypad	☑ B	☑ G	☑ 0
	☑ 1	☑ 2	☑ 3
	☑ 4	☑ 5	☑ 6
	☑ 7	☑ 8	☑ 9
Enabled Items	☑ Tower ☑ Floor ☑ Flat		
Flat Length	2 or less		
Tower Length	2 or less		

- **Wall Mode**: Enable this to set the device as a peripheral. In this mode, visitors can only tap the Speed Dial tab (Concierge), Temp Key tab (QR code), and PIN tab on the home screen (with dial pad). They cannot make calls by entering tower, floor, or flat information.
- **Show Homepage**: Enable this to display a poster. This allows visitors to see a poster(screen) before accessing the home screen.
- **Face Recognition**: Enable or disable facial recognition.
- **Name**: Create prompts for the following screens: Home page, Choose Tower or Concierge, Choose Floor, Enter PIN, and Scan QR Code.
- **Default Keypad**: Choose between a numerical keypad or an alphabetical keypad for the Tower and Flat input.
- **Name**: Change the names for the Concierge, QR Code, and PIN icons if needed.
- **Type**: Select the function of the tab.
- **Alphabet Keypad**: Select the alphabetical letters you want displayed on the keypad.
- **Number Keypad**: Choose the numbers and alphabets to be displayed on the digital keypad.
- **Enabled Items**: Choose to show or hide the following tabs on the screen: Tower, Floor, and Flat.
- **Flat Length**: Select a maximum length for flats: 1 or less, 2 or less, 3 or less, and 4 or less.
- **Tower Length**: Select a maximum length for towers: 1 or less, 2 or less, 3 or less, and 4 or less.

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**.

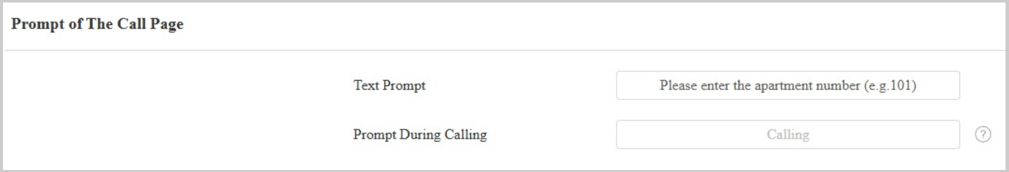


Keypad Display Mode Of PIN Interface

Mode: Normal

Dial Screen Prompt Display

You can set up the prompt displayed on the Dial and Calling screens on the **Setting > Key/Display > Prompt of The Call Page** interface.



Prompt of The Call Page

Text Prompt: Please enter the apartment number (e.g.101)

Prompt During Calling: Calling

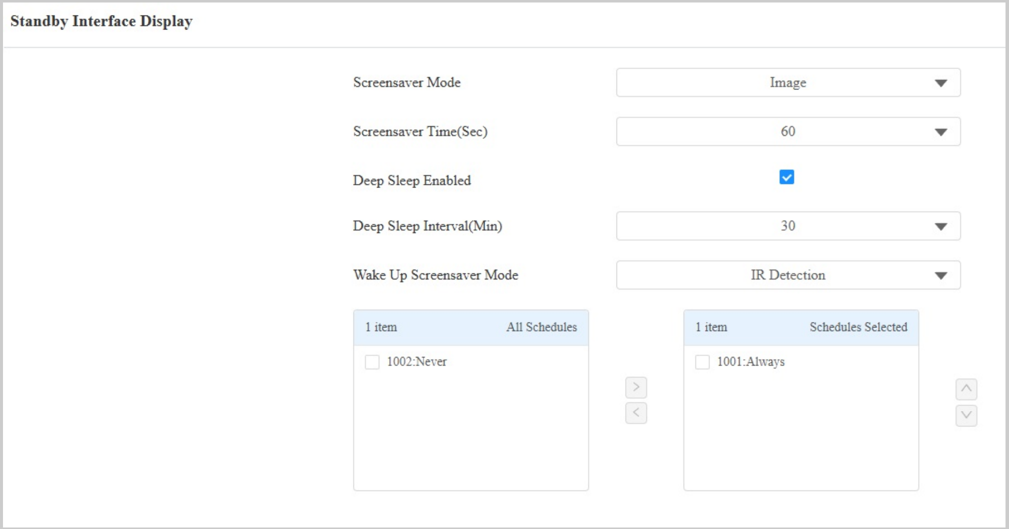
- **Text Prompt**: The default prompt is “Please enter the apartment number(e.g.101). You can customize it with a maximum of 128 characters.
- **Prompt During Calling**: The default prompt is “Calling”. You can customize it with a maximum of 63 characters.

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 > Standby Interface Display** interface.



Standby Interface Display

Screensaver Mode: Image

Screensaver Time(Sec): 60

Deep Sleep Enabled: ☑

Deep Sleep Interval(Min): 30

Wake Up Screensaver Mode: IR Detection

1 item — All Schedules: □ 1002:Never

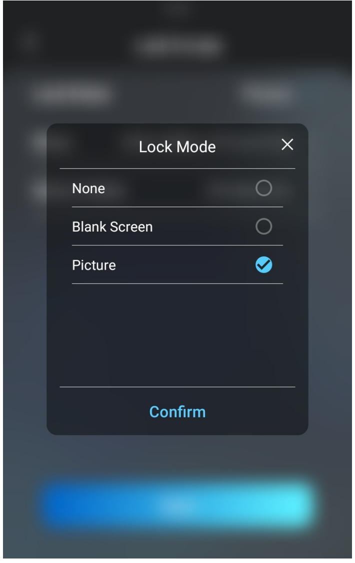
1 item — Schedules Selected: □ 1001:Always

- **Screensaver Mode:**
  - **None:** The screen will stay on without going into screen-saver mode.
  - **Blank**: The screen will go dark.
  - **Image**: The picture uploaded will be shown as the screen saver.
- **Screensaver Time (Sec)**: Set the screen saver start time from 5 seconds up to 180 seconds. The screen saver starts when the device detects no operation, or no one is approaching.
- **Deep Sleep Enabled**: The screen will turn off after the screensaver reaches the end of the duration as predefined.
- **Deep Sleep Interval (Min)**: Set the screensaver time duration before the screen turns off.
- **Wake Up Screensaver Mode**:
  - **IR Detection:** Wake up the screen by IR detection. It offers longer-range and better detection in poor visibility conditions.
  - **Video Detection:** Wake up the screen by video-based motion detection. Focus on analyzing visual information captured through cameras.
  - **Manual**: Touch and wake up the screen.
- **Schedule**: Select the schedule when the screensaver settings will be effective.

> **Note**
>
> Wake Up Screensaver Mode cannot be changed from **Auto** to **Manual** when the Screensaver Mode is set as **Blank** screen.

On the Device

You can also configure the screensaver on **Setting > Basic Settings> Lock Screen** screen.



Lock Mode

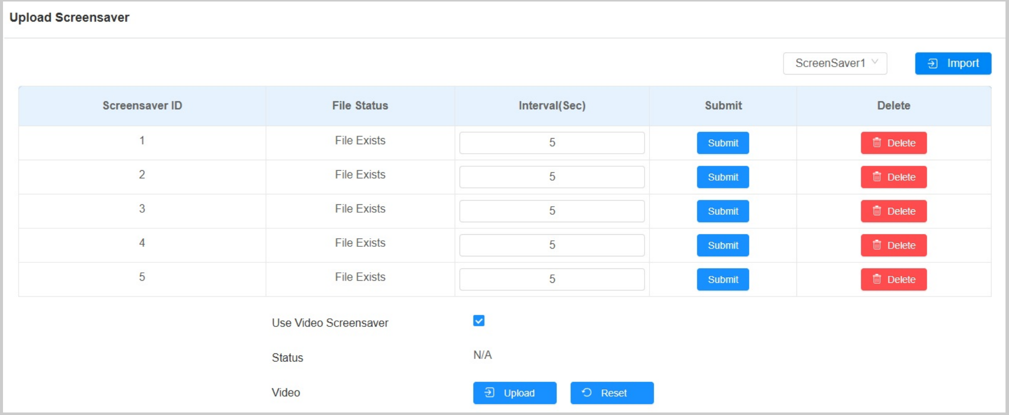
- None ○
- Blank Screen ○
- Picture ✓

Confirm

Upload Screensaver

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

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



Upload Screensaver

ScreenSaver1 | Import

Screensaver ID	File Status	Interval(Sec)	Submit	Delete
1	File Exists	5	Submit	Delete
2	File Exists	5	Submit	Delete
3	File Exists	5	Submit	Delete
4	File Exists	5	Submit	Delete
5	File Exists	5	Submit	Delete

Use Video Screensaver	☑
Status	N/A
Video	Upload Reset

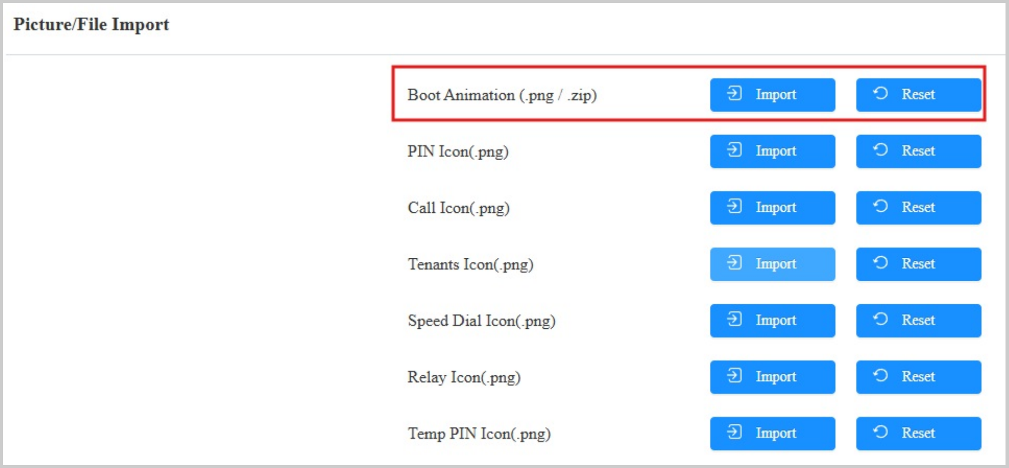
- **Use Video Screensaver**: Check to upload videos as screensaver.
  - The video screensaver takes effect only when the screensaver mode is **Image**.
  - The device only supports playing videos without sound.
  - If it is disabled, the photo screensaver will be used.
- **Status**: If the video is uploaded, it will display the file name.
- **Upload**: Max File Size: 100M, Format: .mp4/.avi/.3gp.

> **Note**
>
> - The pictures uploaded should be in JPG format with 2M pixels maximum.
> - The recommend resolution is 800×1280.
> - The previous picture with a specific ID order will be overwritten when picture with the same ID is uploaded.

Upload Device Booting Image

You can upload the booting image to be displayed during the device’s booting process.

Set it up on the web **Setting > Key/Display > Picture/File Import** interface.



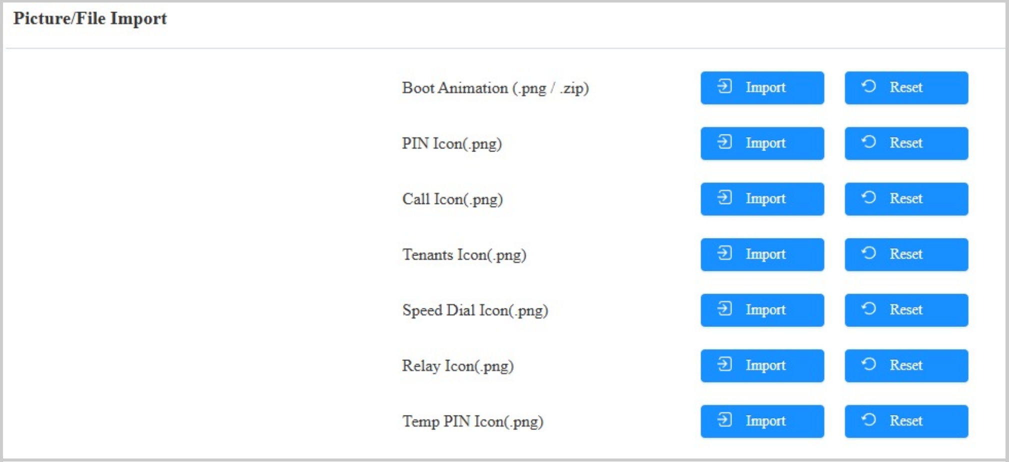
Note

- The pictures uploaded should be in **.**png or .zip format.
- Max .zip file size: 20MB; Max picture size: 1MB; Max resolution: 800*1280.

Upload Icon Pictures in the Building Theme

You can upload pictures of different icons.

Set it up on the web **Setting > Key/Display > Picture/File Import** interface.



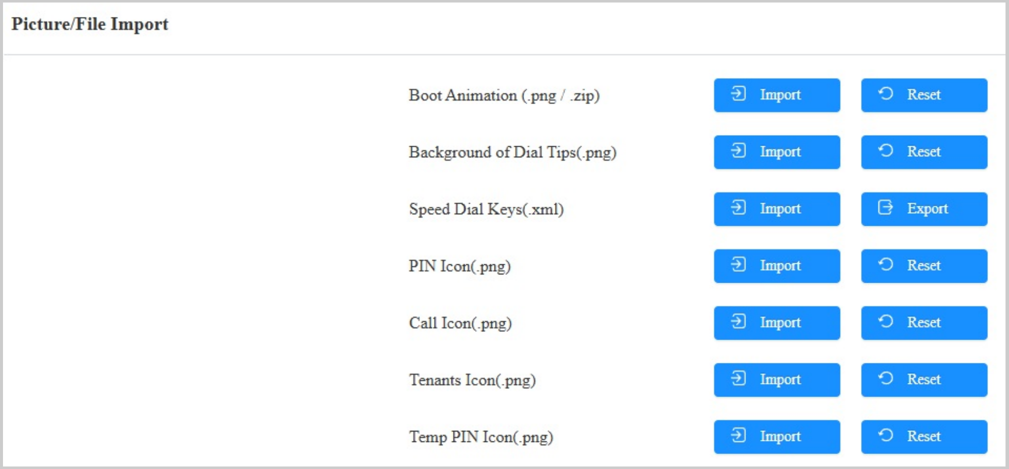
Note

- The pictures uploaded should be in .png format.
- Max picture size: 1MB; Max resolution: 120*120.

Upload Icon Pictures in the Villa Theme

You can upload pictures of different icons.

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



Picture/File Import

Boot Animation (.png / .zip)	Import	Reset
Background of Dial Tips(.png)	Import	Reset
Speed Dial Keys(.xml)	Import	Export
PIN Icon(.png)	Import	Reset
Call Icon(.png)	Import	Reset
Tenants Icon(.png)	Import	Reset
Temp PIN Icon(.png)	Import	Reset

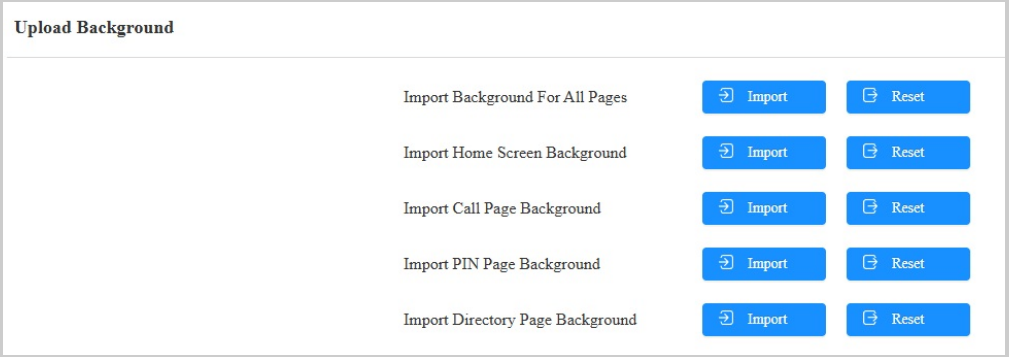
Note

Max picture Size: 1MB, Recommend Resolution: 120*120.

Upload Background Pictures

You can upload a background picture that works for all or specific screens. If you use the appearance function, the Upload Background setting will be hidden.

Set it up on the **Device > LCD > Upload Background** interface.



Upload Background

Import Background For All Pages	Import	Reset
Import Home Screen Background	Import	Reset
Import Call Page Background	Import	Reset
Import PIN Page Background	Import	Reset
Import Directory Page Background	Import	Reset

- **Import Background For All Pages**: This picture works for all screens and covers all themes. Pictures uploaded for other screens will be covered by the background picture.

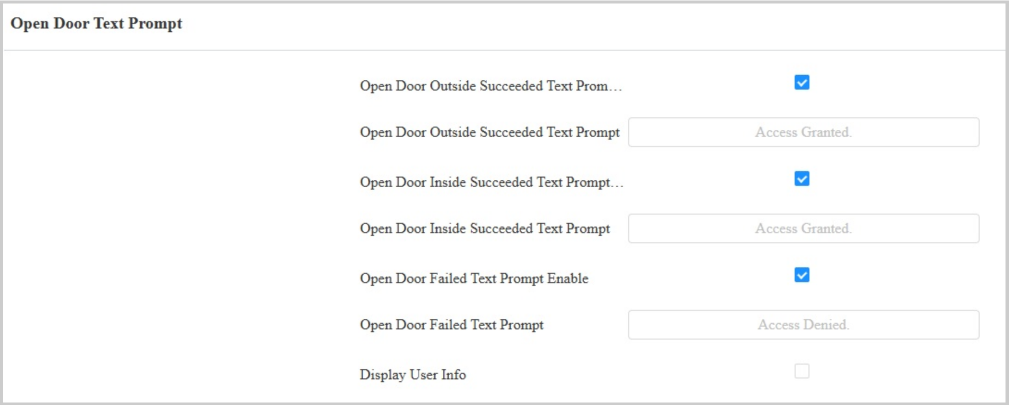
Note

Max Size: 1M, Format: .jpg/png, Max Resolution: 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.

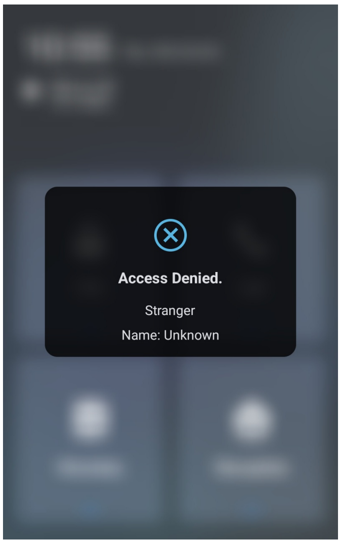
Set it up on the web **Access Control > Relay > Open Door Text Prompt** interface.



Open Door Text Prompt

Open Door Outside Succeeded Text Prom…	☑
Open Door Outside Succeeded Text Prompt	Access Granted.
Open Door Inside Succeeded Text Prompt…	☑
Open Door Inside Succeeded Text Prompt	Access Granted.
Open Door Failed Text Prompt Enable	☑
Open Door Failed Text Prompt	Access Denied.
Display User Info	☐

- **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. The default prompt is “Access Granted”. You can customize the prompt with a maximum of 63 characters.
- **Open Door Inside Succeeded Text Prompt:** Display a text prompt after the door is opened by pressing an exit button(the input is triggered). The default prompt is “Access Granted”. You can customize the prompt with a maximum of 63 characters.
- **Open Door Failed Text Prompt:** Display a text prompt after opening the door fails. The default prompt is “Access Denied”. You can customize the prompt with a maximum of 63 characters.
- **Display User Info**: Display the user information after facial recognition or RF 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” will be displayed with “Stranger, Name: Unknown”.



Access Denied.

Stranger

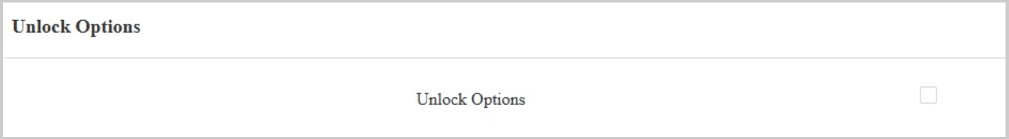
Name: Unknown

Unlock Options Display

Users can select the door to be opened when the device is connected to more than one door lock.

Click here to view the feature details.

To enable this feature, go to **Access Control > Relay > Unlock Options** interface. It is disabled by default.

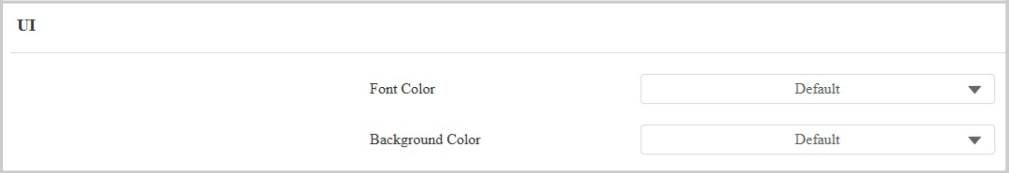


Unlock Options

Unlock Options	☐

Font and Background Color

You can change the device font and background color in the **Villa** theme on the **Device > LCD > UI** interface.



UI

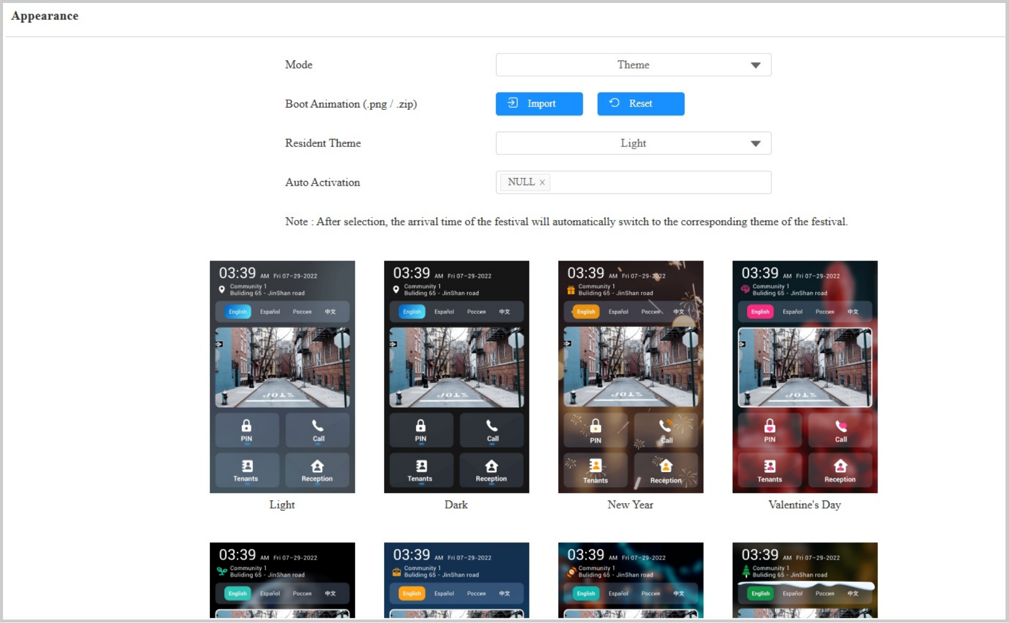
Font Color: Default

Background Color: Default

Appearance

In the **Building** theme, the device offers various appearance options, catering to different aesthetic needs and festival atmospheres.

Change the appearance on the **Setting > Key/Display > Appearance** interface.



Appearance

Mode: Theme

Boot Animation (.png / .zip)

Resident Theme: Light

Auto Activation: NULL ×

Note : After selection, the arrival time of the festival will automatically switch to the corresponding theme of the festival.

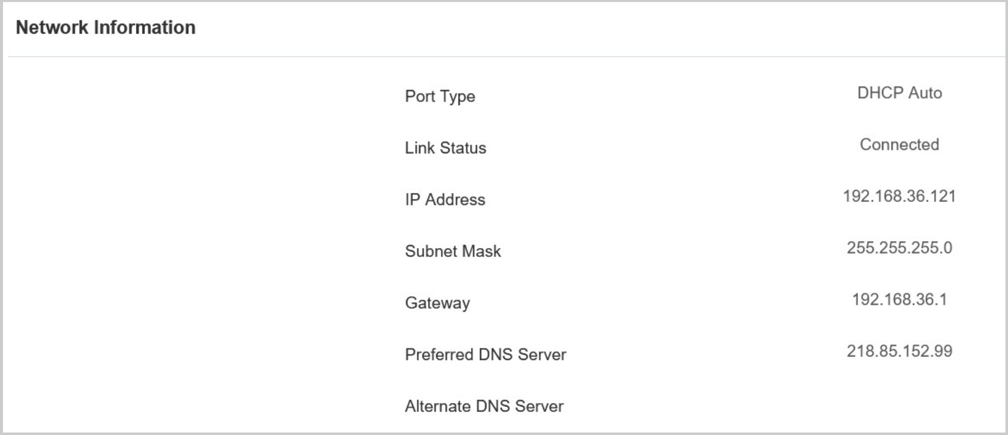
- **Mode**:
  - **Theme**: The default option. When selected, you can check the desired appearance option.
  - **Customization**: When selected, you can upload icon pictures for desired tabs, such as PIN, Call, and Tenants.
- **Resident Theme**: Select the desired appearance.
- **Auto Activation**: Null by default. Select the desired festival appearance(s). The device will automatically switch to the appearance during the festival.

Network Setting

Device Network Connection

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

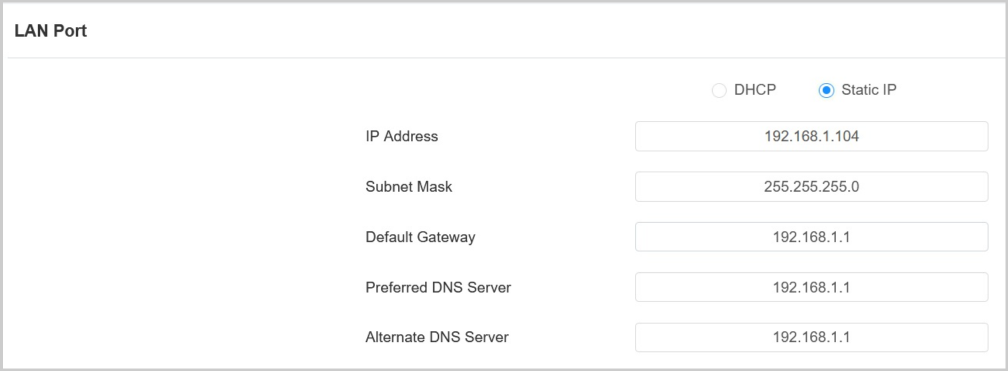
Check the network status on the web **Status > Info > Network Information** interface.



Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.121
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	

Set the network connection on the web **Network > Basic** interface.



LAN Port

○ DHCP ● Static IP

IP Address	192.168.1.104
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS Server	192.168.1.1
Alternate DNS Server	192.168.1.1

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

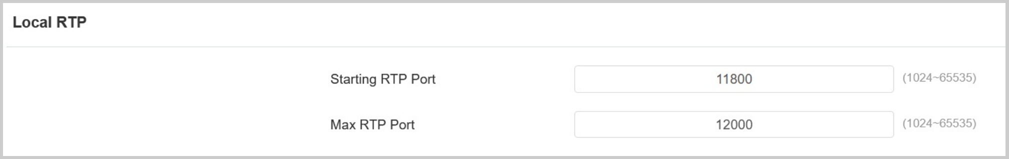
You can also set up the network on the **Setting > Network** screen.

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.

Set it up on the web **Network > Advanced > Local RTP** interface.



Local RTP

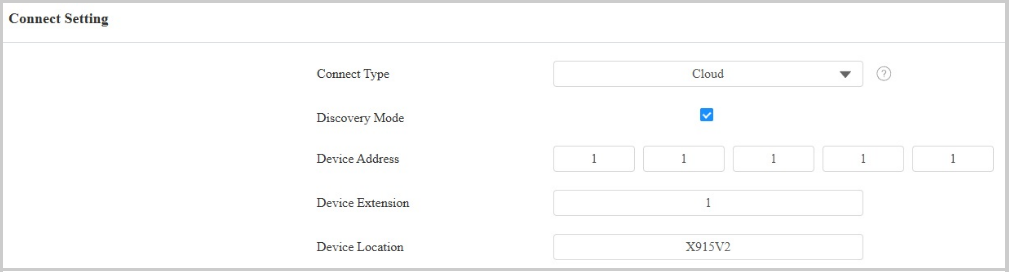
Starting RTP Port	11800	(1024~65535)
Max RTP Port	12000	(1024~65535)

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

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.

Set it up on the web **Network > Advanced > Connect Setting** interface.



Connect Setting

Connect Type	Cloud
Discovery Mode	☑
Device Address	1 1 1 1 1
Device Extension	1
Device Location	X915V2

- **Connect Mode**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None. You can also change it manually.

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

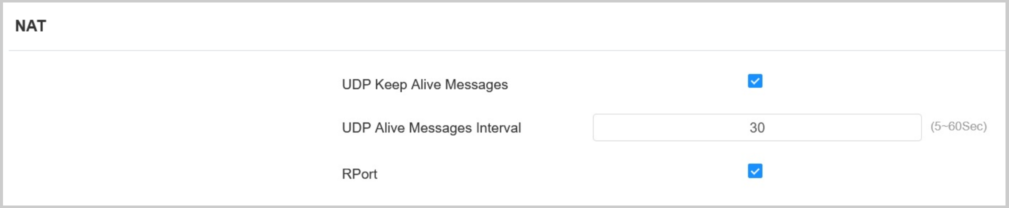
- **Discovery Mode**: Enabled by default. Available for **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address**: Available for **None** server mode. Uneditable in Cloud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

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.

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



NAT

UDP Keep Alive Messages ☑

UDP Alive Messages Interval 30 (5~60Sec)

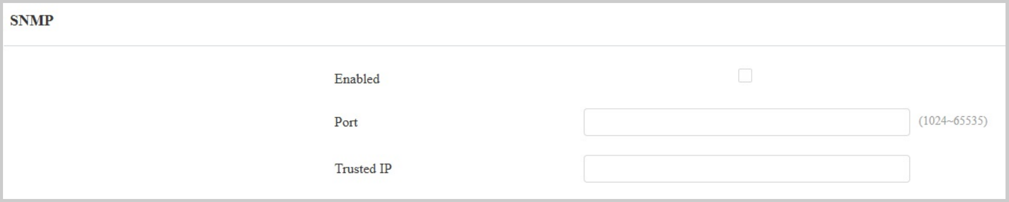
RPort ☑

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

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).

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



SNMP

Enabled □

Port (1024~65535)

Trusted IP

- **Port**: Set a specific port for the data transmission from 1024-65535.
- **Trusted IP**: Enter the third-party IP address.

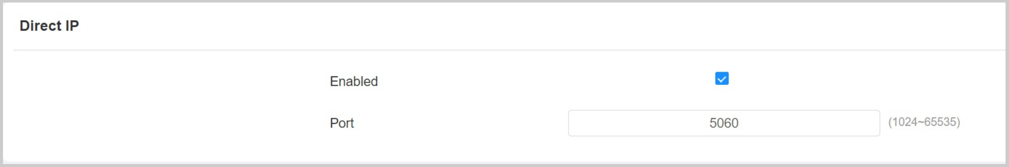
Intercom Call Configuration

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.

IP Call Setup

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



Direct IP

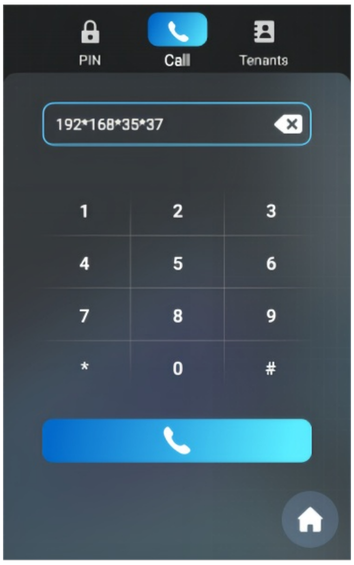
Enabled ☑

Port 5060 (1024~65535)

- **Port:** set the port for direct IP calls. The default is 5060, with a range from 1024-65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

Make IP Calls

To make SIP calls or IP calls on the device, tap the dial button and enter the IP number.



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.

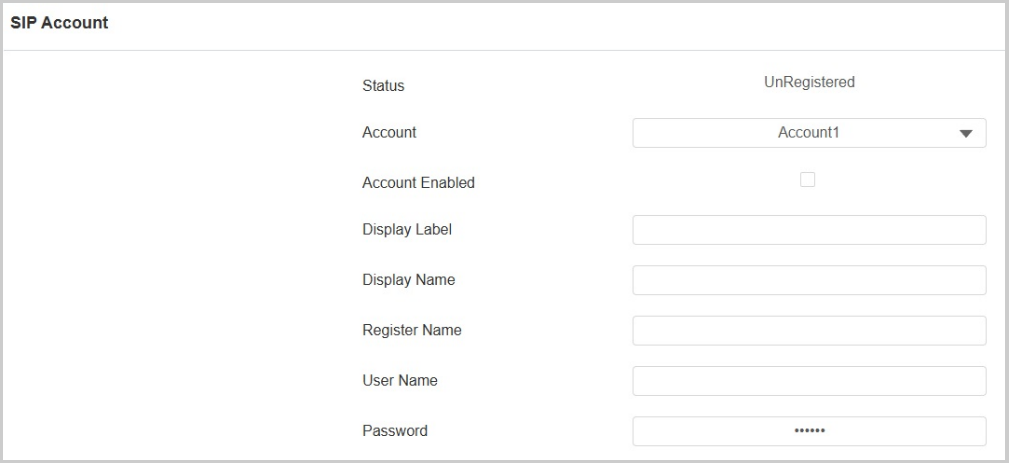
SIP Account Registration

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



SIP Account

Status	UnRegistered
Account	Account1
Account Enabled	□
Display Label	
Display Name	
Register Name	
User Name	
Password	••••••

- **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.

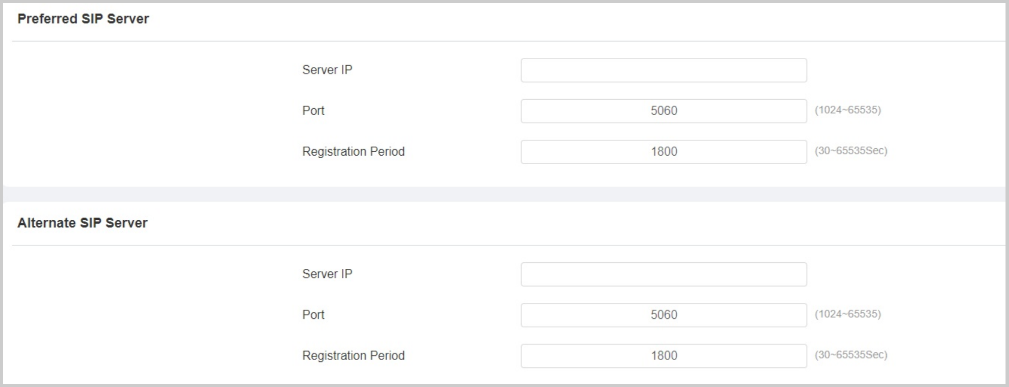
> **Tip**
>
> - For configuring contact call and dial plan, see here.
> - When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

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

SIP Server Configuration

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

Navigate to the web **Account > Basic > Preferred SIP Server** interface.



Preferred SIP Server

Server IP		
Port	5060	(1024~65535)
Registration Period	1800	(30~65535Sec)

Alternate SIP Server

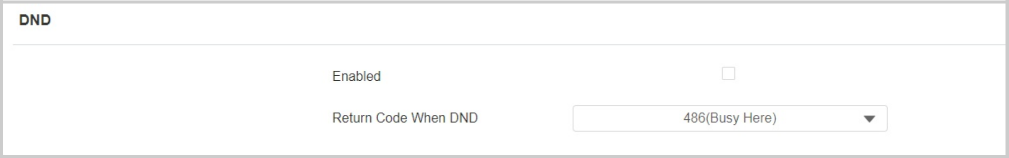
Server IP		
Port	5060	(1024~65535)
Registration Period	1800	(30~65535Sec)

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

SIP Call DND & Return Code Configuration

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

Navigate to the web **Intercom > Call Feature > DND** interface.



DND

Enabled □

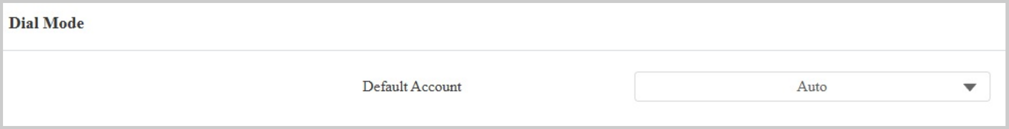
Return Code When DND: 486(Busy Here)

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

SIP Account Selection

The Dial Mode 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 Mode** interface.



Dial Mode

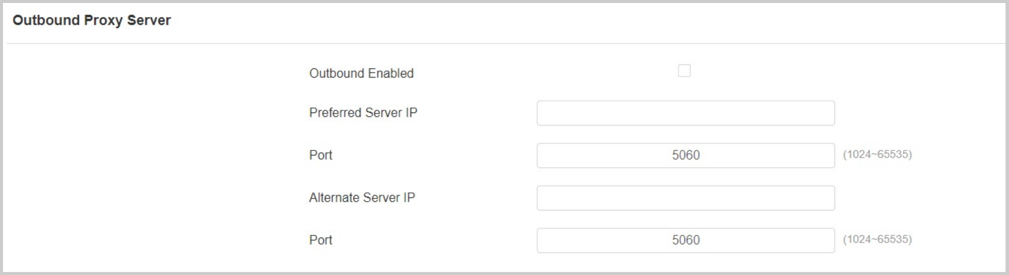
Default Account: Auto

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

Set it up on the web **Account > Basic > Outbound Proxy Server** interface.



Outbound Proxy Server

Outbound Enabled □

Preferred Server IP:

Port: 5060 (1024~65535)

Alternate Server IP:

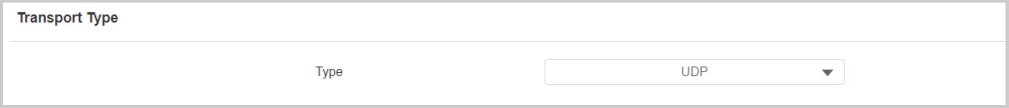
Port: 5060 (1024~65535)

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

Set it up on the web **Account > Basic > Transport Type** interface.



Transport Type

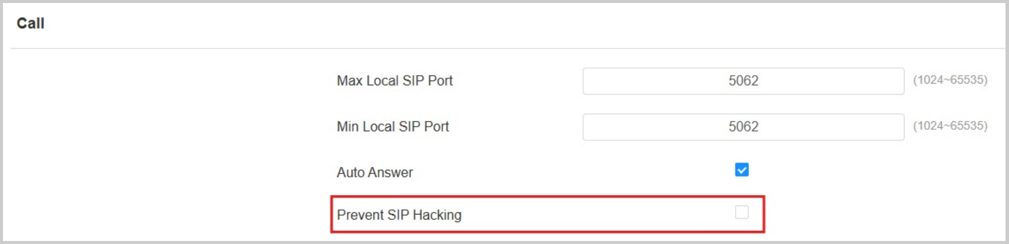
Type: UDP

- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.

SIP Hacking Protection

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

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



Call

Max Local SIP Port 5062 (1024~65535)

Min Local SIP Port 5062 (1024~65535)

Auto Answer ☑

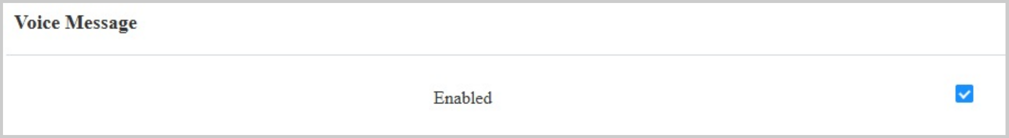
Prevent SIP Hacking □

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

Voice Message

When the device is connected to the SmartPlus Cloud, users can leave voice messages on the Directory screen or when the Cloud contacts do not respond to or hang up their calls from the device.

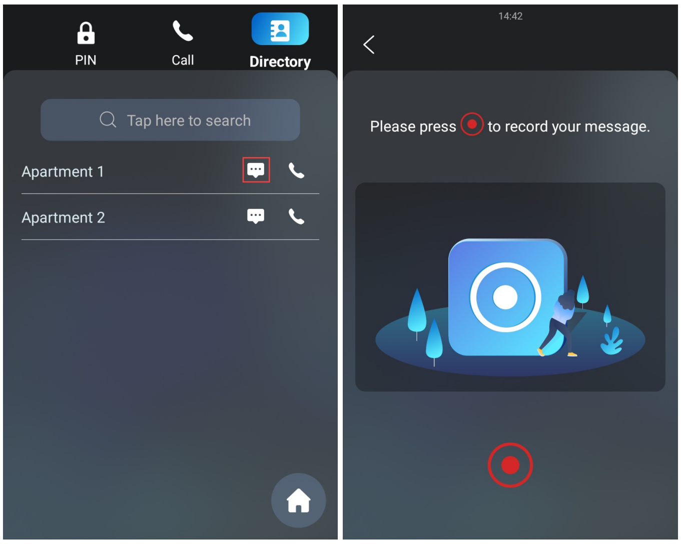
Enable/disable the voice message feature on the **Intercom > Basic > Voice Message** interface.



Voice Message

Enabled ☑

Tap the **Message** icon and follow the on-screen instructions to leave a message.



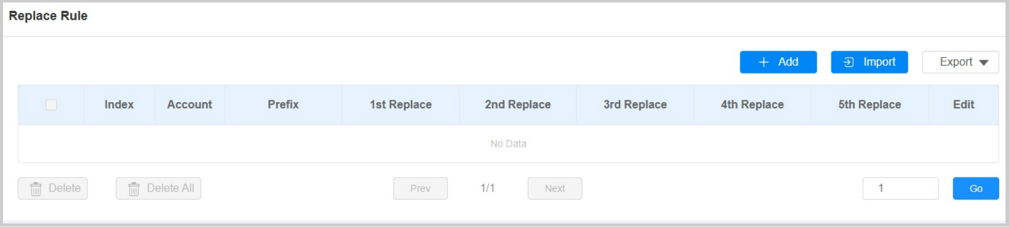
Please press ● to record your message.

Call Settings

Quick Dial By Number Replacement

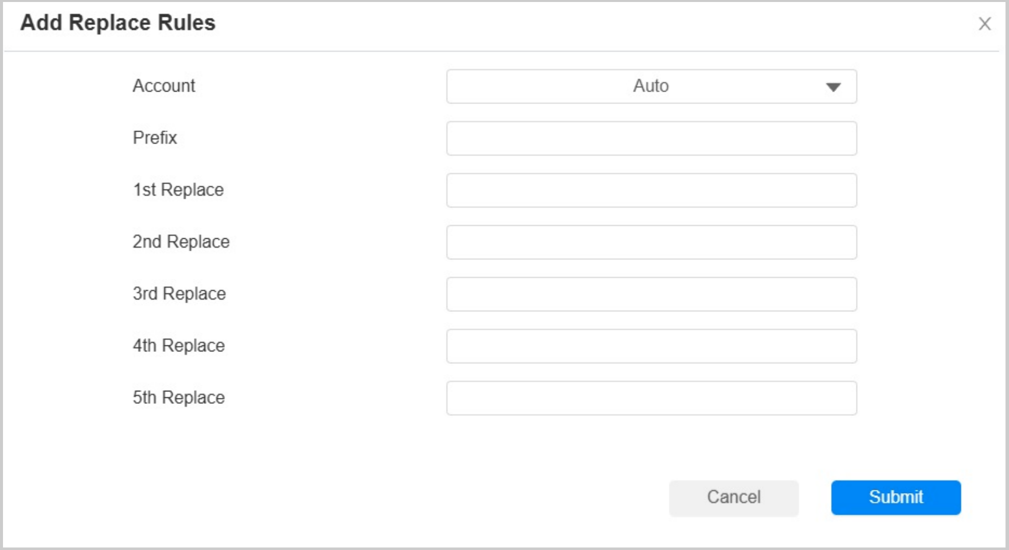
The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

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



Replace Rule

□	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
No Data									



Add Replace Rules

Account	Auto
Prefix	
1st Replace	
2nd Replace	
3rd Replace	
4th Replace	
5th Replace	

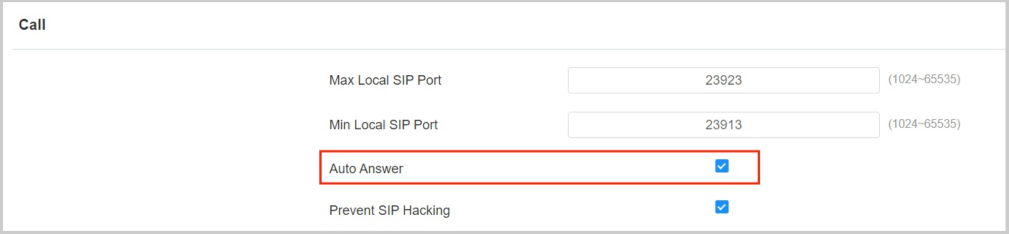
- **Account:** Select the dial-out account.
  - Auto: Dial out using the registered account. When there are 2 registered accounts, Account 1 is the default.
  - Account 1/2: Dial out using the chosen account.
- **Prefix:** Specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** 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 dial plan on the **Setting > Replace Rule** screen.

Call 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.

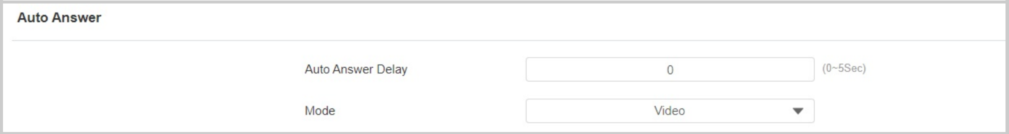
Enable the feature on the web **Account > Advanced > Call** interface.



Call

Max Local SIP Port	23923	(1024~65535)
Min Local SIP Port	23913	(1024~65535)
Auto Answer	☑	
Prevent SIP Hacking	☑	

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



Auto Answer

Auto Answer Delay: 0 (0~5Sec)

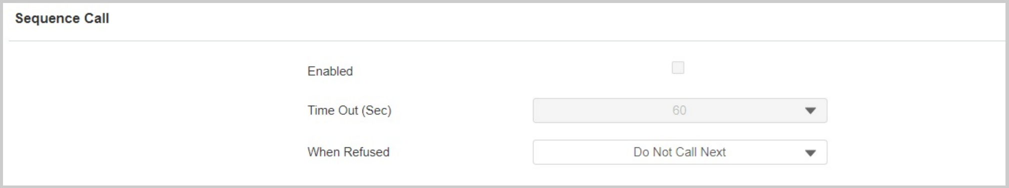
Mode: Video

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

Sequence Call

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

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



Sequence Call

Enabled: □

Time Out (Sec): 60

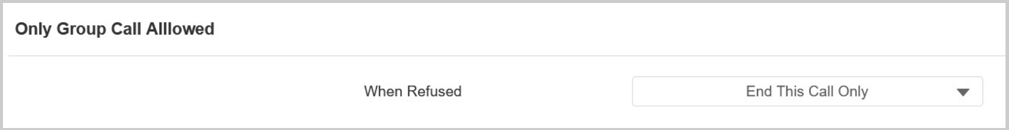
When Refused: Do Not Call Next

- **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 > Only Group Call Allowed** interface.



Only Group Call Alllowed

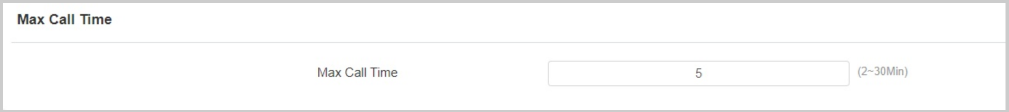
When Refused: End This Call Only

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

Maximum Call Duration

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

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



Max Call Time

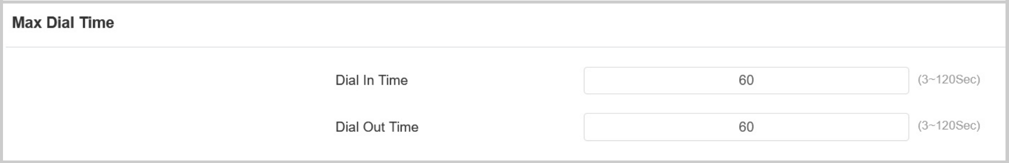
Max Call Time: 5 (2~30Min)

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

Maximum Dial Duration

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

Set it up on the web **Intercom > Call Feature > Max Dial Time** interface.



Max Dial Time

Dial In Time: 60 (3~120Sec)

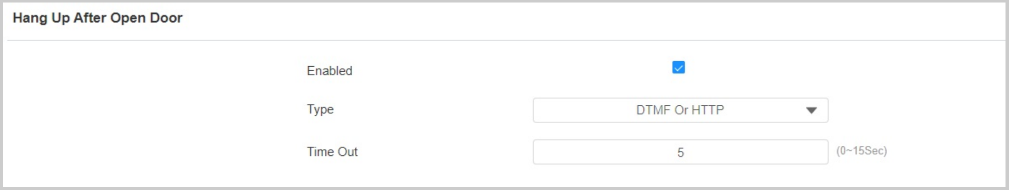
Dial Out Time: 60 (3~120Sec)

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

Hang Up After Open Door

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

Set it up on the web **Intercom > Call Feature > Hang Up After Open Door** interface.



Hang Up After Open Door

Enabled: ☑

Type: DTMF Or HTTP

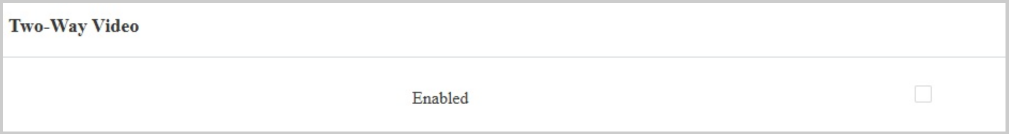
Time Out: 5 (0~15Sec)

- **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:** Specify the hang-up time limit. The door phone will automatically terminate the call when the specific time is reached after opening the door.

Two-way Video Call

The two-way video feature allows for visual connection with both callers and recipients via the door phone, providing a more interactive and secure conversation.

Set it up on the **Intercom > Basic > Two-way Video** interface.



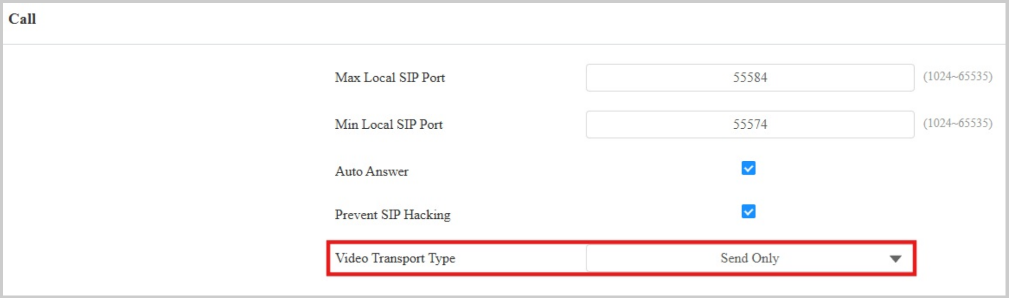
Two-Way Video

Enabled: □

- **Enabled**: Disabled by default. Activate this feature to allow callers to see the called party's video stream during a video call.
  - In the following situations, two-way video calls can be established:
    - The device initiates a video call and the other party with a camera answers it.
    - The other party with a camera initiates a video call and the device answers it.
  - In all other cases, only audio communication is displayed.

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.



Call

Max Local SIP Port: 55584 (1024~65535)

Min Local SIP Port: 55574 (1024~65535)

Auto Answer: ☑

Prevent SIP Hacking: ☑

Video Transport Type: Send Only

- **Video Transport Type**: It is Send and Receive by default.
  - **Inactive**: Disable the function.
  - **Send Only**: The device sends the video stream to the other party.

- **Receive Only**: The device only receives the video stream from the other party.
- **Send and Receive**: The device can send and receive video streams to and from the other party.

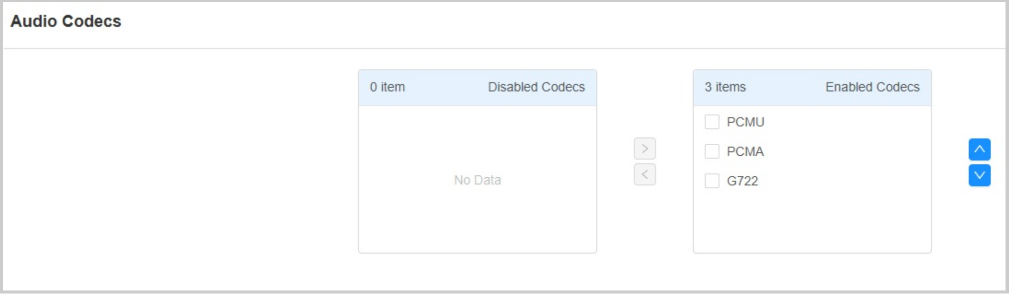
Audio & Video Codec Configuration

Audio Codec

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



Audio Codecs

0 item Disabled Codecs

No Data

3 items Enabled Codecs

☐ PCMU

☐ PCMA

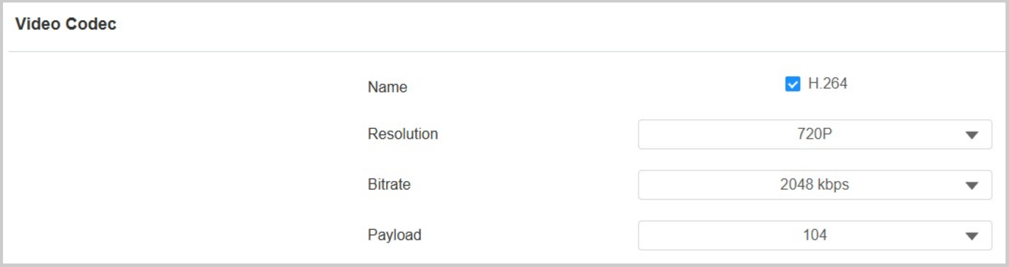
☐ G722

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.



Video Codec

Name: ☑ H.264

Resolution: 720P

Bitrate: 2048 kbps

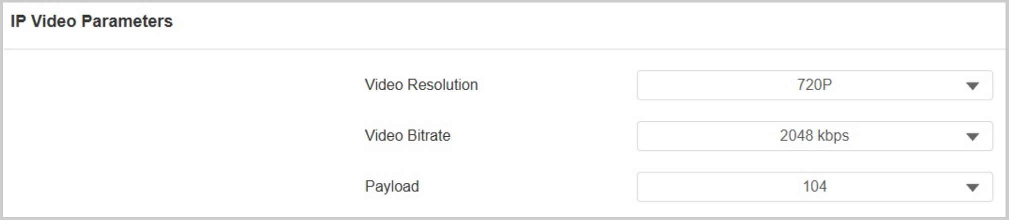
Payload: 104

- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default resolution is 720P(720 × 480 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data transmitted every second and the clearer the video will be. The default code bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for IP Direct Calls

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

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



IP Video Parameters

Video Resolution: 720P

Video Bitrate: 2048 kbps

Payload: 104

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

Contact Configuration

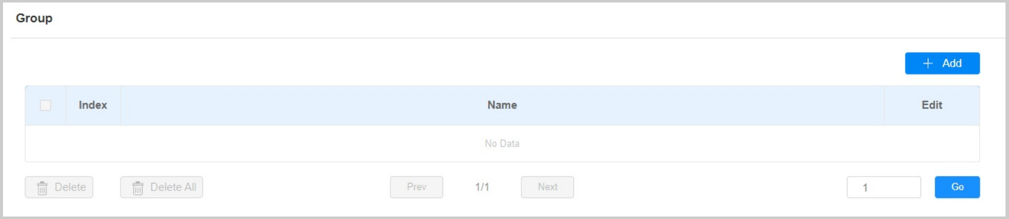
The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

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

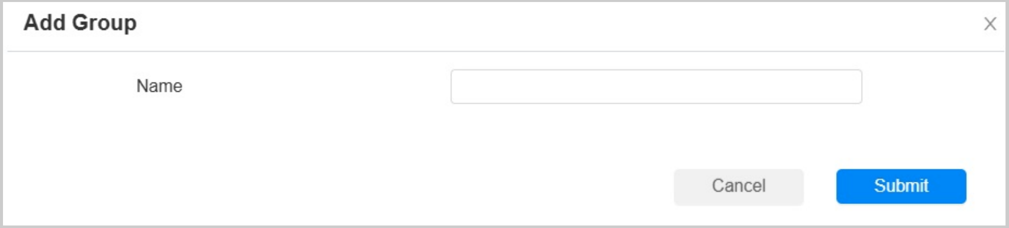
Manage Contact Groups

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 > Directory** screen. You can add 500 groups at a maximum.


Group

□	Index	Name	Edit
		No Data	

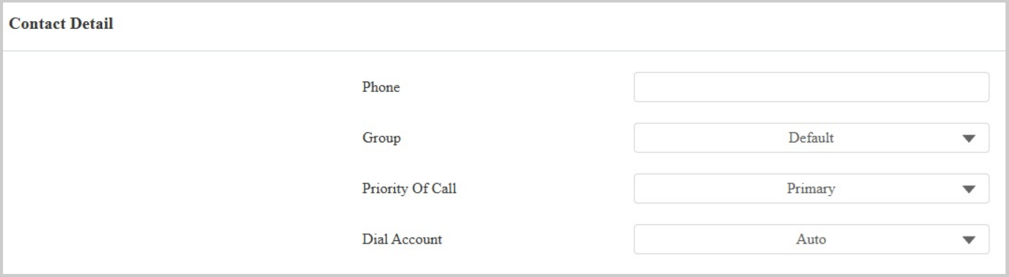

Add Group

Name

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.


Contact Detail

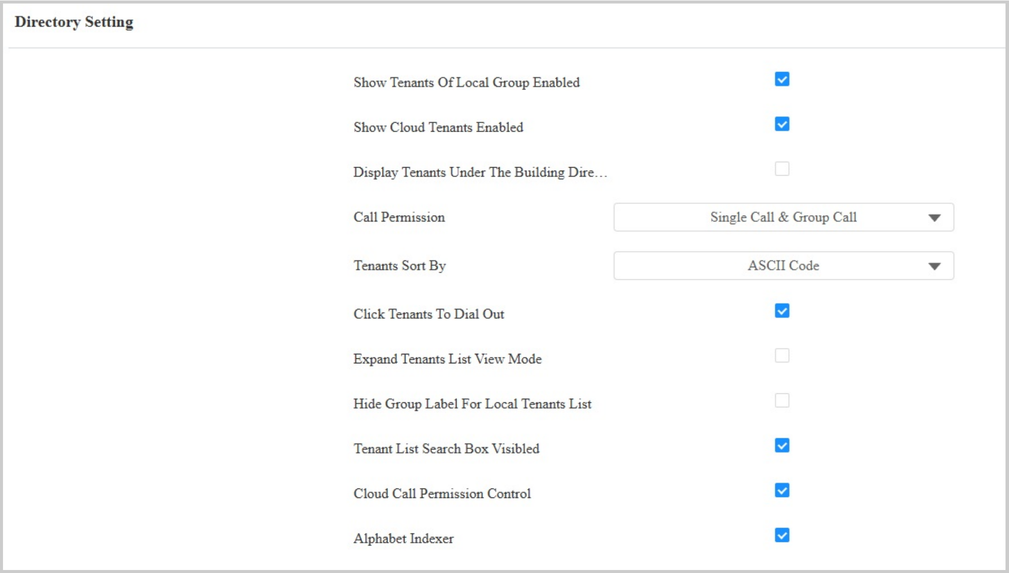
Phone	
Group	Default
Priority Of Call	Primary
Dial Account	Auto

- **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 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 web **Directory > Directory Setting** interface.



Directory Setting

Show Tenants Of Local Group Enabled ☑

Show Cloud Tenants Enabled ☑

Display Tenants Under The Building Dire… □

Call Permission: Single Call & Group Call

Tenants Sort By: ASCII Code

Click Tenants To Dial Out ☑

Expand Tenants List View Mode □

Hide Group Label For Local Tenants List □

Tenant List Search Box Visibled ☑

Cloud Call Permission Control ☑

Alphabet Indexer ☑

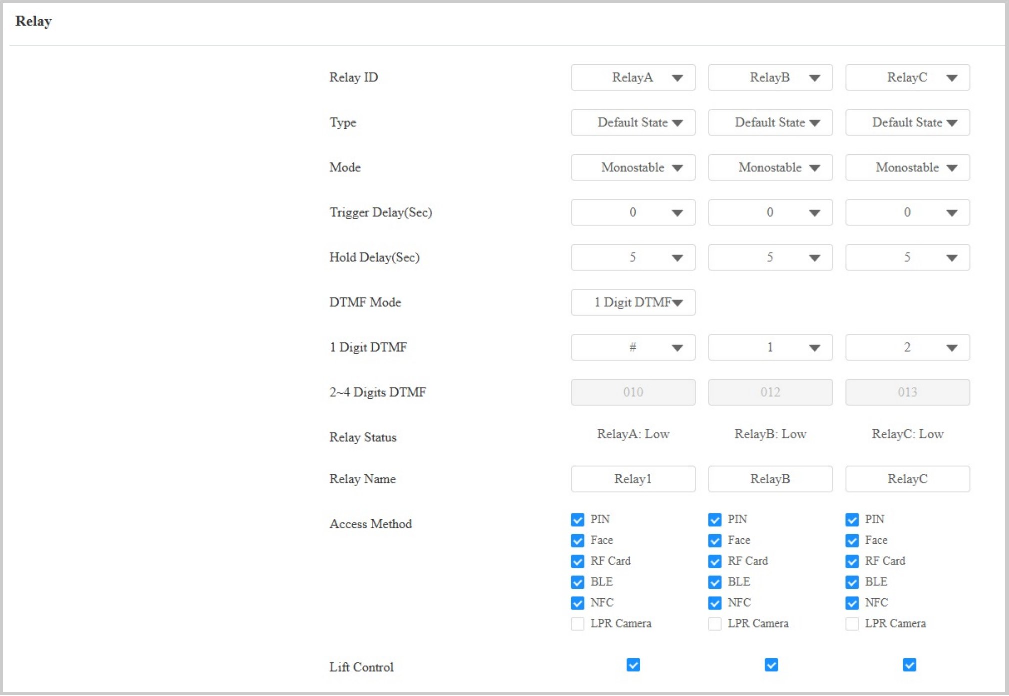
- **Show Tenants of Local Group Enabled**: Decide whether to display tenants in groups. If unchecked, only the group name will be displayed.
- **Show Cloud Tenants Enabled**: The contacts synchronized from the SmartPlus Cloud can be displayed.
- **Display Tenants Under The Building Directly**: Available when **Show Cloud Tenants Enabled** is checked. When enabled, users can tap the Building name to view the resident list on the **Directory** screen.
- **Call Permission**:
  - **Single Call & Group Call**: Users can call contacts one by one or simultaneously in a group.
  - **Only Single Call Allowed**: Users can only call contacts one by one.
  - **Only Group Call Allowed**: Users can only call contacts in a group simultaneously.
- **Tenants Sort By**:
  - **ASCII Code** lists the tenants by their names in the sequence of the ASCII code.
  - **Room No.** lists the tenants according to their room numbers.
    - **Group Member Sort By**: Decide the tenant display order in groups. You can choose **ASCII Code** or **Room No.**
  - **Import** lists the tenants according to their order in the imported file.
- **Click Tenants to Dial Out**: When enabled, users can press anywhere on the contact tab to dial out. When disabled, users need to press the Call icon to dial out.
- **Expand Tenants List View Mode**: Control the width of the contact tab. When enabled, the contact tab will be wider.
- **Hide Group Label for Local Tenants List**: Decide whether to display the local group name. When enabled, the tenants will be displayed directly instead of in the group.
- **Tenant List Search Box Visible**: Set whether to display the search box at the top of the screen.
- **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.
- **Alphabet Indexer**: When enabled, users can find the desired contact with the alphabet indexer on the Directory screen.

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.

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



Relay

Relay ID	RelayA	RelayB	RelayC
Type	Default State	Default State	Default State
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	5	5	5
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	#	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	Relay1	RelayB	RelayC
Access Method	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC ☐ LPR Camera	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC ☐ LPR Camera	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC ☐ LPR Camera
Lift Control	☑	☑	☑

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

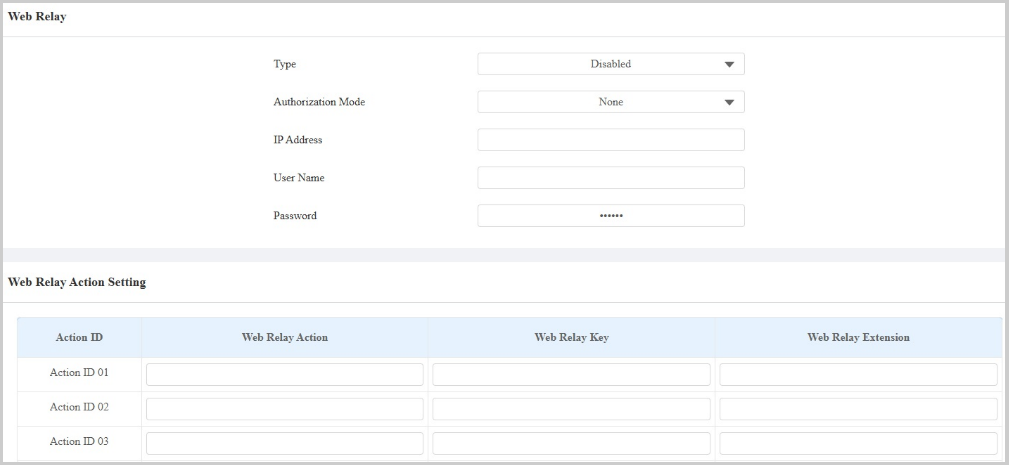
> **Note**
>
> External devices connected to the relay require separate power adapters.

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.



Web Relay

Type	Disabled
Authorization Mode	None
IP Address	
User Name	
Password	••••••

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01			
Action ID 02			
Action ID 03			

- **Type**: Determine the type of relay activated when employing door access methods for entry.
    - Disabled: Only activate the local relay.
    - Web Relay: Only activate the web relay.
    - Both: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **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**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

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

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

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

- Leaving it blank enables all door-opening methods.

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

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

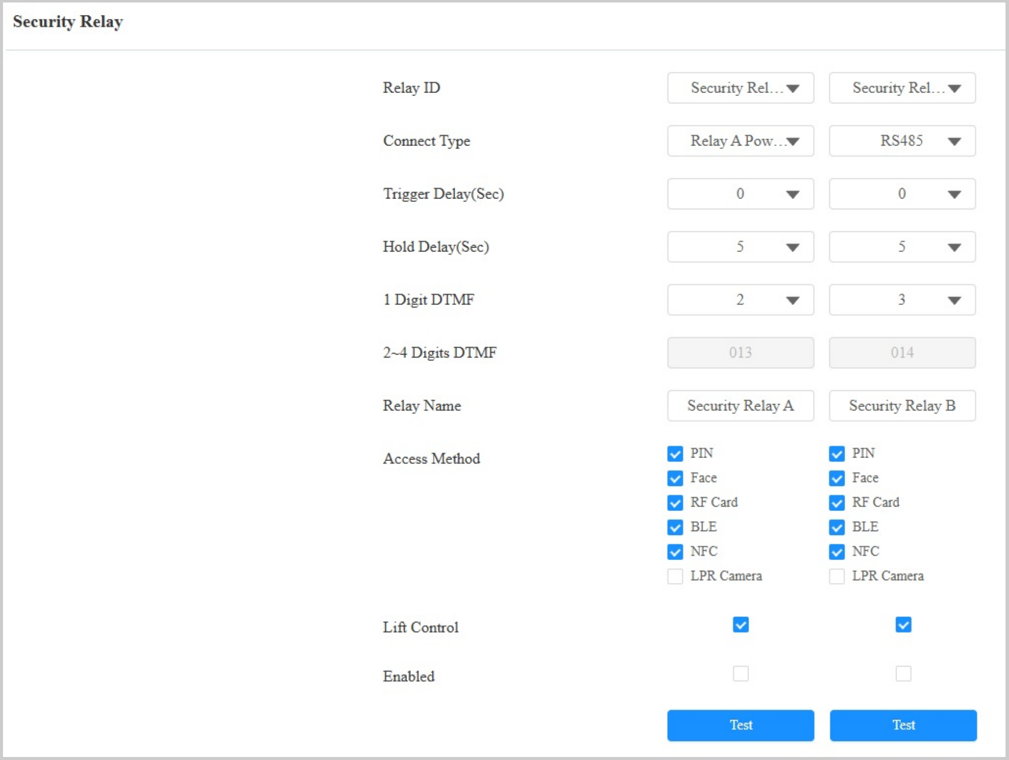
- If left blank, all devices can trigger the relay during calls.

Security Relay

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

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

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



Security Relay

Relay ID	Security Rel…	Security Rel…
Connect Type	Relay A Pow…	RS485
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
1 Digit DTMF	2	3
2~4 Digits DTMF	013	014
Relay Name	Security Relay A	Security Relay B
Access Method	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC ☐ LPR Camera	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC ☐ LPR Camera
Lift Control	☑	☑
Enabled	☐	☐
	Test	Test

- **Connect Type**: Select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Trigger Delay (Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name**: Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method**: Check the method(s) to trigger the security relay.
- **Lift Control**: Set whether to perform lift control when the specific relay is triggered.
- **Enabled**: When using the SR01 via RS485, you need to set the RS485 mode to **Security Relay** on the **Device > RS485** interface.

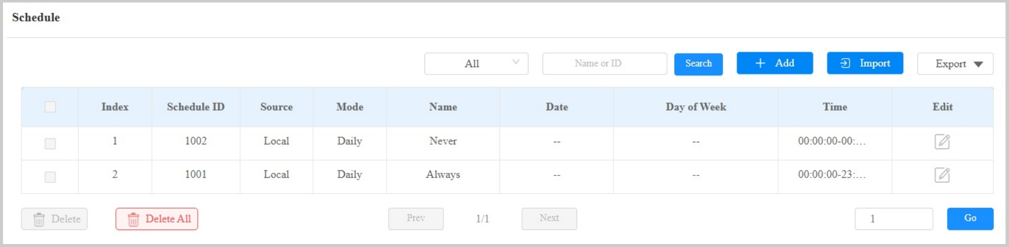
Door Access Schedule Management

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

Create a Door Access Schedule

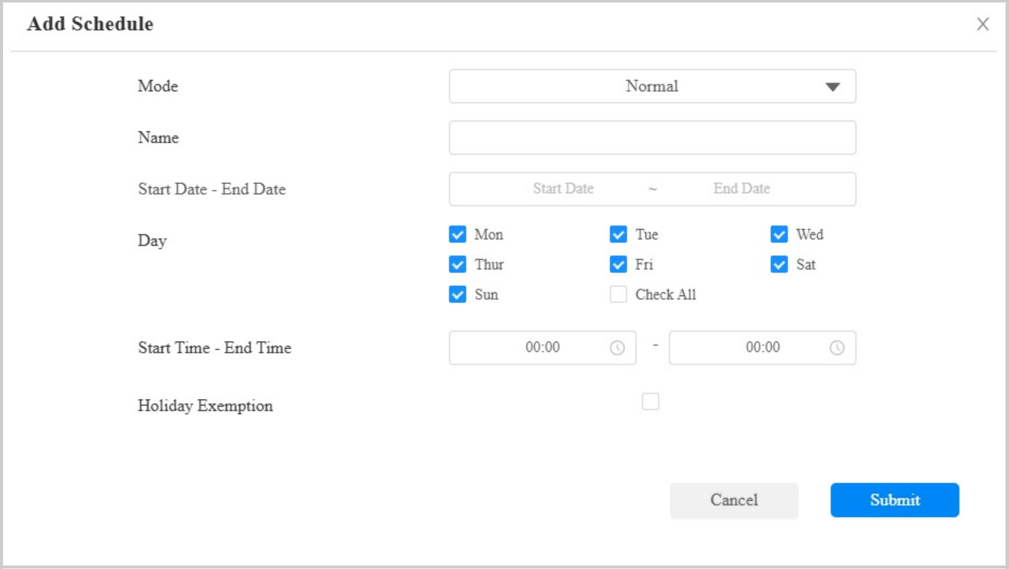
To configure the schedule, navigate to the web **Setting > Schedule** interface. Click +Add. You can add up to 100 local schedules.

You can also set up the schedule on the **Setting > Basic Setting > Schedule** screen.



Schedule

□	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
□	1	1002	Local	Daily	Never	--	--	00:00:00-00:...	
□	2	1001	Local	Daily	Always	--	--	00:00:00-23:...	



Add Schedule

Mode	Normal
Name	
Start Date - End Date	Start Date ~ End Date
Day	☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun □ Check All
Start Time - End Time	00:00 - 00:00
Holiday Exemption	□

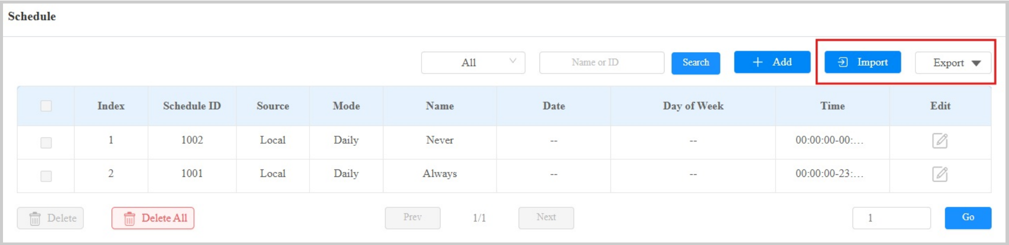
- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Name**: Name the schedule.
- **Holiday Exemption**: The holiday schedule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

> **Note**
>
> The access control schedule synchronized from the SmartPlus cannot be edited or deleted.

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.

Set it up on the **Setting > Schedule** interface. The import/export file is in .xml format.



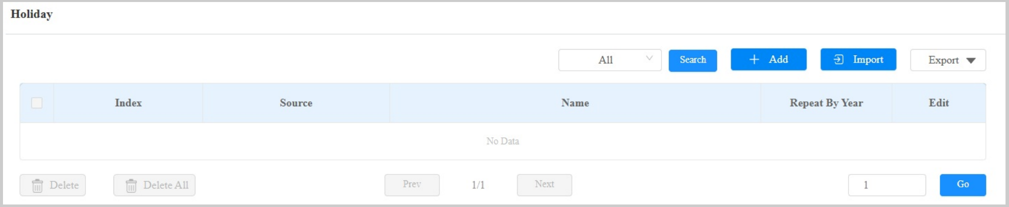
Schedule

□	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
□	1	1002	Local	Daily	Never	--	--	00:00:00-00:...	
□	2	1001	Local	Daily	Always	--	--	00:00:00-23:...	

Holiday Schedule

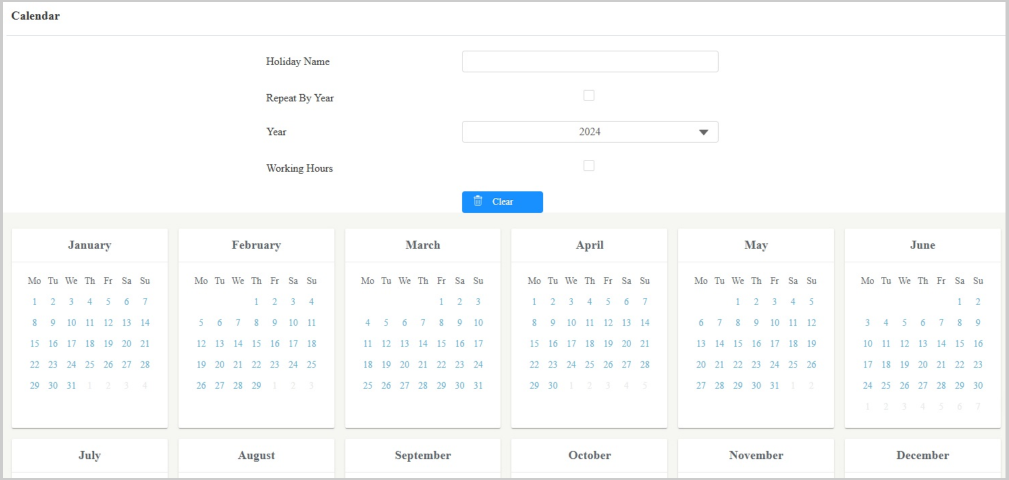
You can define the holidays when users cannot open doors to enhance access control security. You can also set the Working Hours to allow authorized users to open doors.

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



Holiday

□	Index	Source	Name	Repeat By Year	Edit
			No Data		



Calendar

Holiday Name

Repeat By Year □

Year: 2024

Working Hours □

January

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

February

Mo	Tu	We	Th	Fr	Sa	Su
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	1	2	3

March

Mo	Tu	We	Th	Fr	Sa	Su
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

April

Mo	Tu	We	Th	Fr	Sa	Su
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

May

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

June

Mo	Tu	We	Th	Fr	Sa	Su
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

July

August

September

October

November

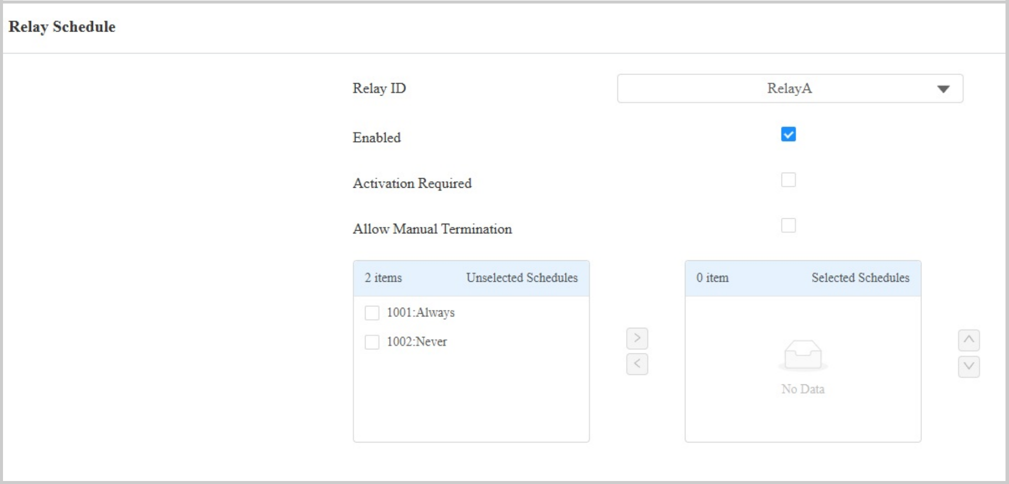
December

- **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.

Navigate to the web **Access Control > Relay > Relay Schedule** interface.



Relay Schedule

Relay ID: RelayA

Enabled ☑

Activation Required □

Allow Manual Termination □

2 items	Unselected Schedules
□ 1001:Always	
□ 1002:Never	

0 item	Selected Schedules
No Data	

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

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

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

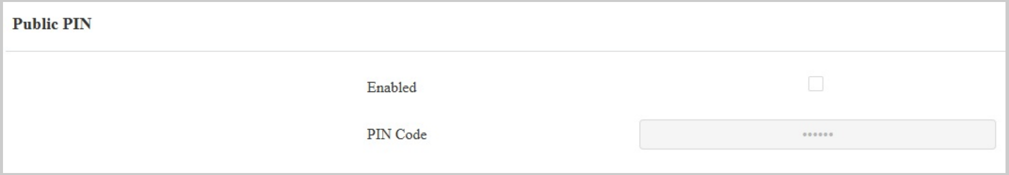
Door-opening Configuration

Unlock By Public PIN

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

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

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



Public PIN

Enabled	☐
PIN Code	******

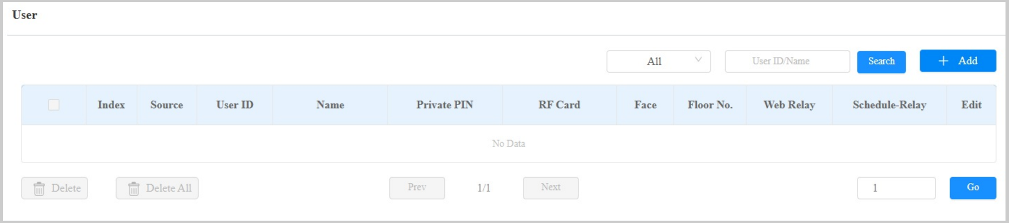
- **PIN Code**: Set the 4-8 digits code without 9 as the start.

User-specific Access Methods

The private PIN code, RF card, Bkey, and facial recognition setting should be assigned to a particular user for door opening.

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

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

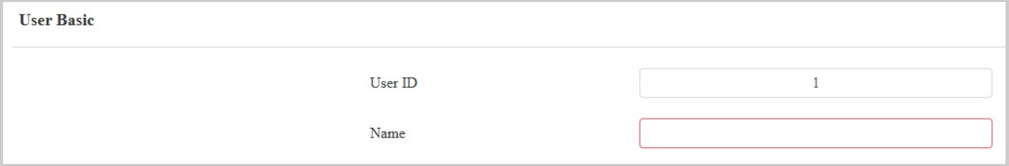


User

All | User ID/Name | Search | + Add

☐	Index	Source	User ID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											

Delete | Delete All | Prev | 1/1 | Next | 1 | Go



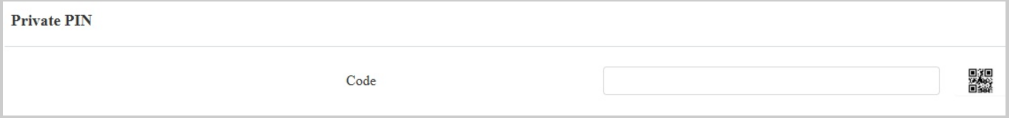
User Basic

User ID	1
Name	

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

Unlock by Private PIN

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

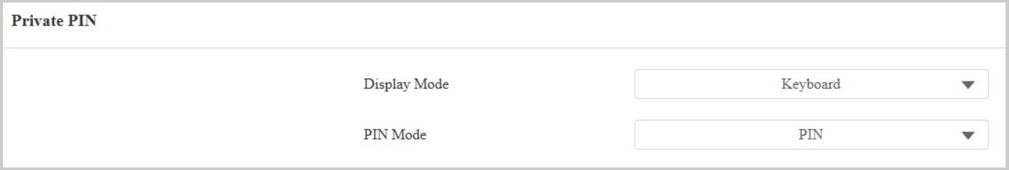


Private PIN

Code	

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

You can set the PIN mode on the **Access Control > PIN Setting > Private PIN** interface.



Private PIN

Display Mode	Keyboard
PIN Mode	PIN

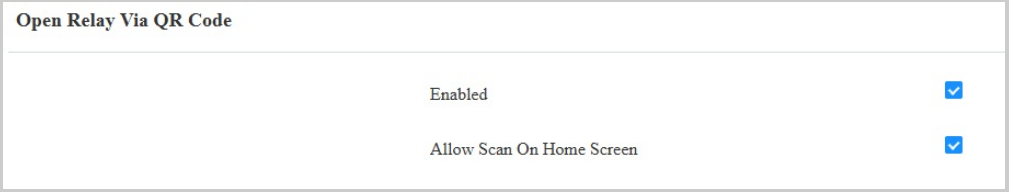
- **Display Mode**:
    - **Keyboard**: Display the keyboard on the PIN screen.
    - **QR Code**: Display the QR code scanning box on the PIN screen.
- **Authorization PIN**:
    - **PIN**: Solely enter the PIN code for door access.
    - **APT#+PIN**: Enter the Apartment Number first before entering the PIN code for the door access. **Apartment Number** can only be applicable when the device is connected to the Akuvox SmartPlus.

Unlock by QR Code

The device supports unlocking by QR codes generated on the web interface and on the SmartPlus Cloud when it is connected to the cloud.

> **Note**
>
> Click here to view how users and property managers create QR codes on SmartPlus.

The feature can be enabled on the **Access Control > Relay > Open Relay via QR Code** interface.

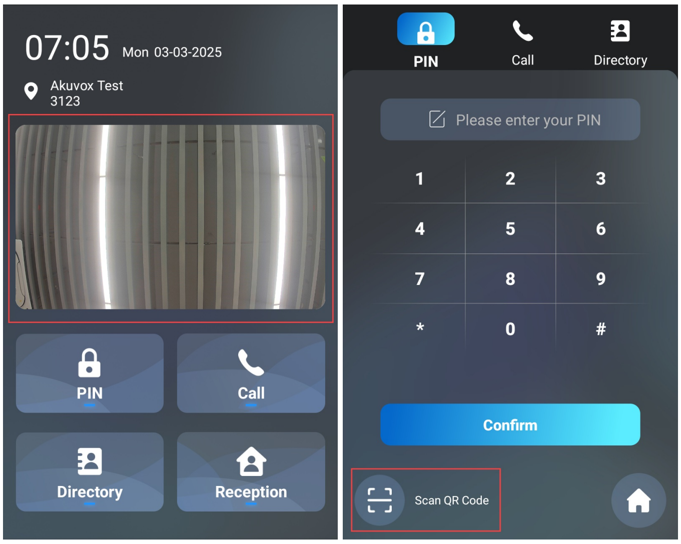


Open Relay Via QR Code

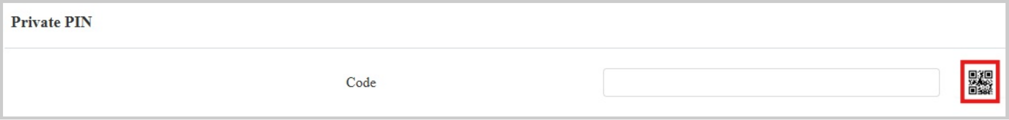
Enabled ☑

Allow Scan On Home Screen ☑

- **Allow Scan on Home Screen**: When enabled, users can open doors by placing QR code in the scanning box on the device's home screen. When disabled, users need to tap **PIN > Scan QR Code**.



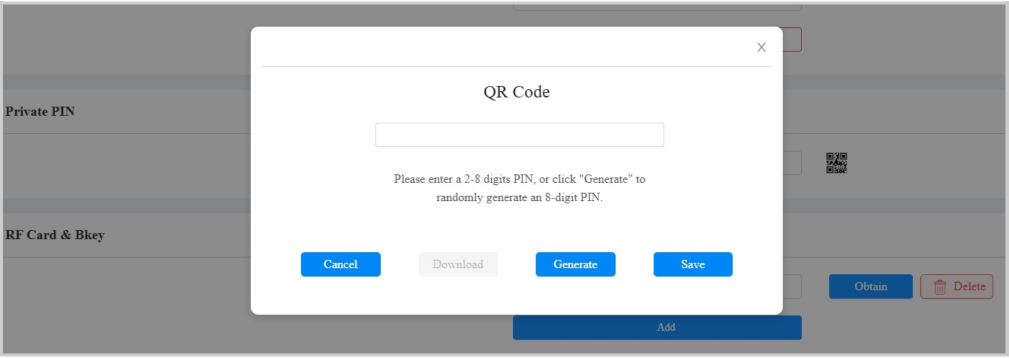
On the **Directory > User > +Add** interface, scroll to the **PIN** section. Click the QR code icon .



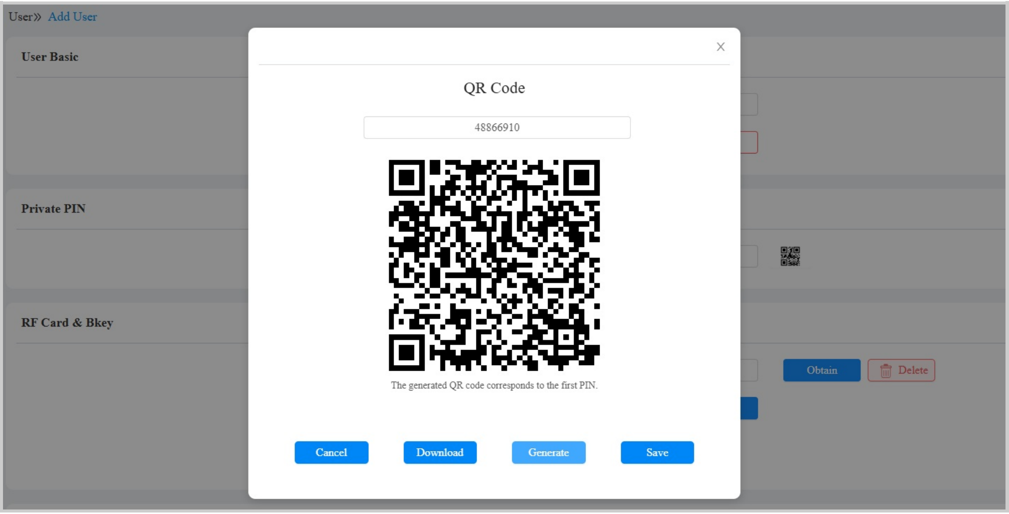
Private PIN

Code

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



Please enter a 2-8 digits PIN, or click "Generate" to randomly generate an 8-digit PIN.



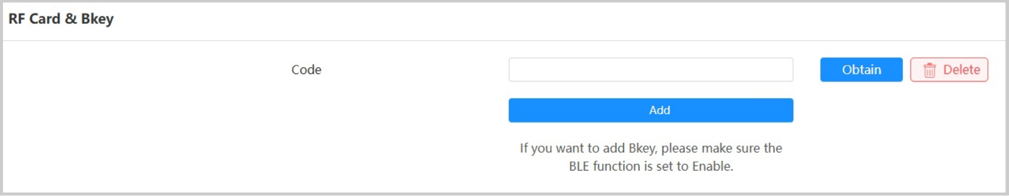
48866910

The generated QR code corresponds to the first PIN.

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

Unlock by RF Card/Bkey

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



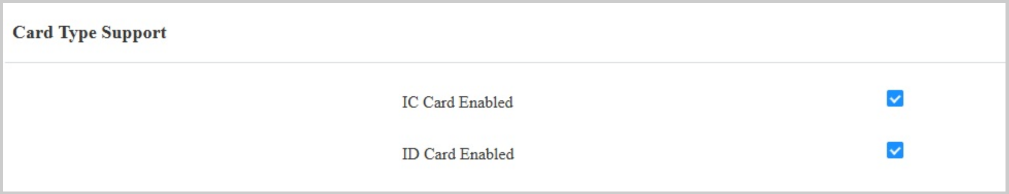
If you want to add Bkey, please make sure the BLE function is set to Enable.

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

Note

- Click here to view the detailed steps of configuring Bkey.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device for access.
- Each user can have a maximum of 5 cards added.
- The device allows to add 20,000 users.

You can enable/disable the use of IC/ID cards on the **Access Control > Card Setting** interface.



Card Type Support

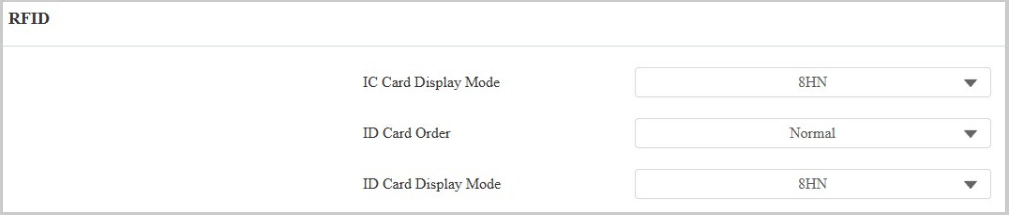
IC Card Enabled ☑

ID Card Enabled ☑

RF Card Code Format

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

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



RFID

IC Card Display Mode: 8HN

ID Card Order: Normal

ID Card Display Mode: 8HN

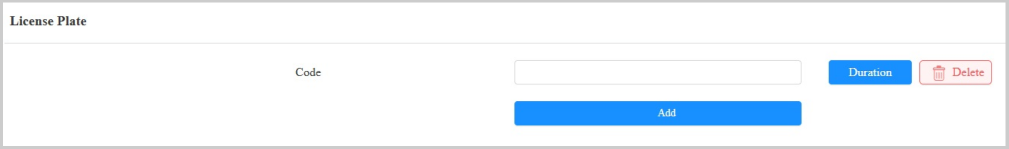
- **IC/ID Card Display Mode**: Select the card number format from the provided options.
- **ID Card Order**: Set the ID card reading mode between Normal and Reversed.

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.



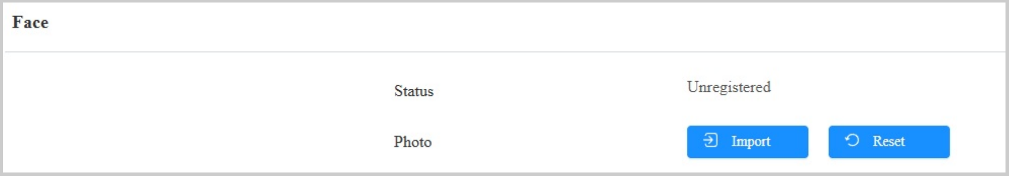
License Plate

Code:

- **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 Facial Recognition

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



Face

Status: Unregistered

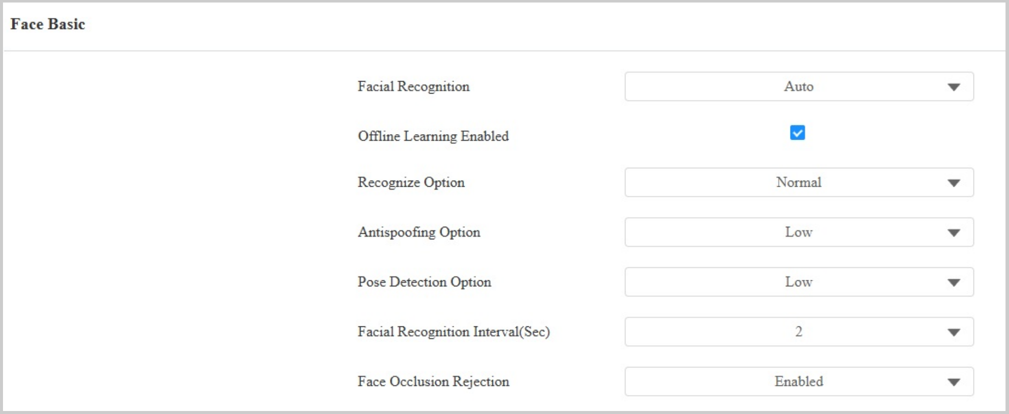
Photo

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

Facial Recognition Settings

The door phone 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.



Face Basic

Facial Recognition: Auto

Offline Learning Enabled: ☑

Recognize Option: Normal

Antispoofing Option: Low

Pose Detection Option: Low

Facial Recognition Interval(Sec): 2

Face Occlusion Rejection: Enabled

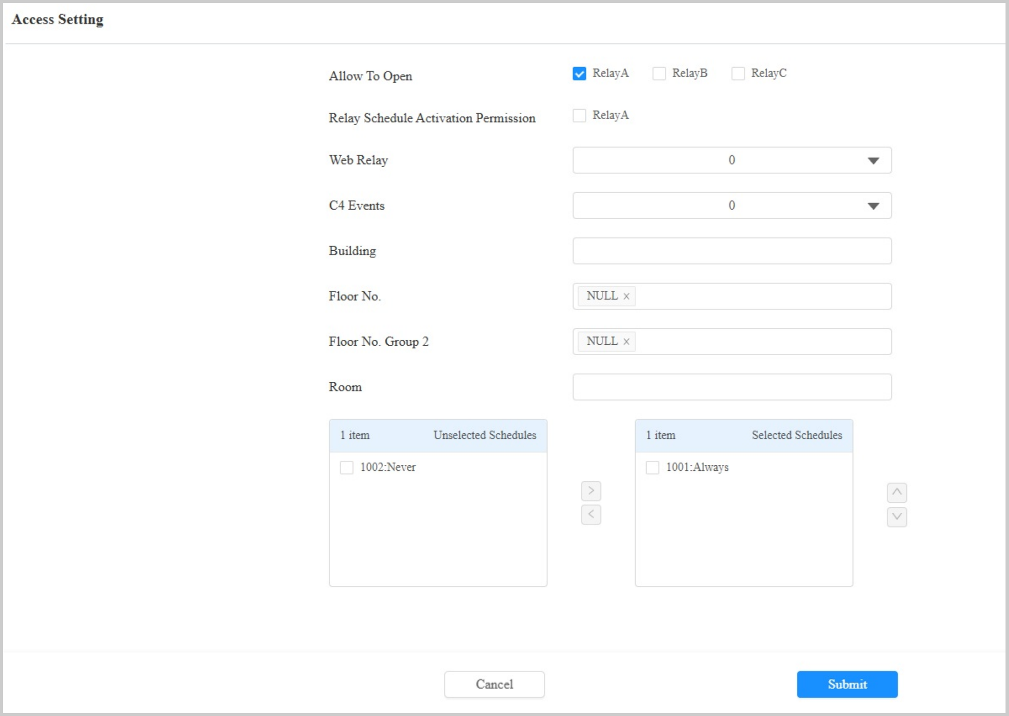
- **Facial Recognition**:
  - **Disabled**: Turn off the facial recognition function.

  - **Auto**: Display the facial recognition box on the home screen. The device starts recognition when it detects faces.
  - **Manual**: Display a prompt "Press to start face recognition." Users need to tap on the home screen to start recognition.
- **Offline Learning Enabled**: Facial recognition accuracy improves as the number of facial recognition increases.
- **Recognize Option**: 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.
- **Antispoofing 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, and 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(Sec)**: Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.
- **Face Occlusion Rejection**: When enabled, if the user is detected to be wearing a mask, he/she will not be able to pass the face recognition.

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.



Access Setting

Allow To Open	☑ RelayA □ RelayB □ RelayC
Relay Schedule Activation Permission	□ RelayA
Web Relay	0
C4 Events	0
Building	
Floor No.	NULL ×
Floor No. Group 2	NULL ×
Room	

1 item Unselected Schedules
□ 1002:Never

1 item Selected Schedules
□ 1001:Always

- **Allow To Open**: Specify the relay that can be unlocked by the user's credentials.
- **Relay Schedule Activation Permission**: This decides whether the user can keep the relay open during the scheduled time after activating it.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **Building**: Specify the building the user lives in.
- **Floor No.**: Specify the floor(s) that are accessible to the user via the elevator.
- **Room**: Enter the user's room number.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
  - Always: Allows door opening without limitations on door open counts during the valid period.

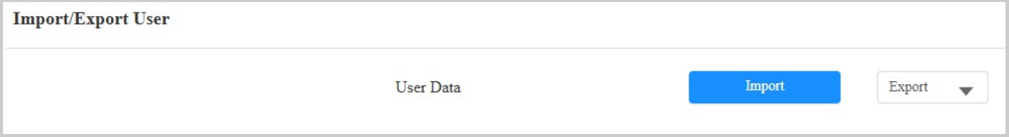
- Never: Prohibits door opening.

Import/Export User Data

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

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

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



Import/Export User

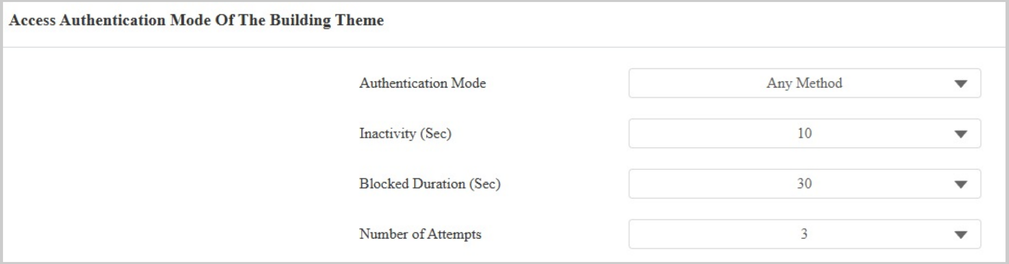
User Data

> **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 of The Building Theme** interface. This feature applies to the **Building** theme.

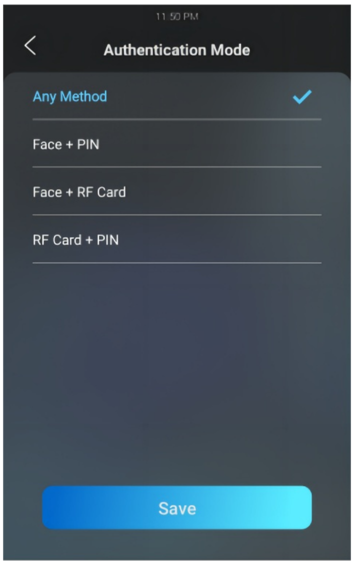


Access Authentication Mode Of The Building Theme

Authentication Mode	Any Method
Inactivity (Sec)	10
Blocked Duration (Sec)	30
Number of Attempts	3

- **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.
  - Card + PIN: Swipe the RF card first, then enter the PIN code.
- **Inactivity (Sec)**: Set the authentication timeout for the second authentication. For example, in **Face+PIN** authentication, if you set the authentication timeout as 10 seconds, then users have to enter the PIN code in ten seconds after they go through the face recognition, otherwise, the screen will return to the home screen.
- **Blocked Duration (Sec)**: Set the block time for the first authentication. For example, if you set the number of attempts as 3, and users fail to pass the second authentication three times, then users will be temporarily blocked from the first authentication according to the block time.
- **Number of Attempts**: The number of attempts users are allowed for the second authentication.

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

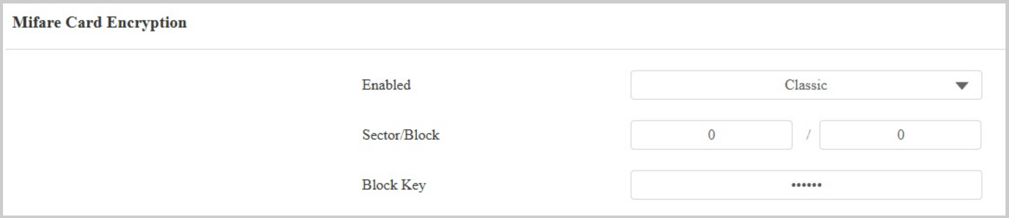


Mifare Card Encryption

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 > Mifare Card Encryption** interface.



Mifare Card Encryption

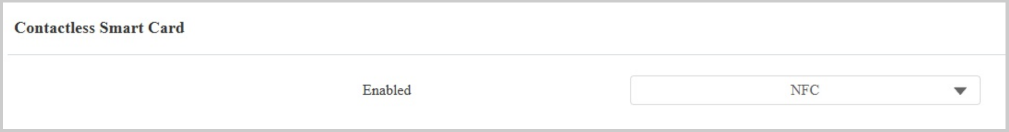
Enabled	Classic
Sector/Block	0 / 0
Block Key	••••••

- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
- **Plus**: 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 31.
  - **Crypto**: The encryption method, either AES or DES.
  - **Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.

Contactless Smart Card

You can select an NFC card or Felica card for contactless access. For example, if you enable both NFC and Felica cards, you can gain contactless entry with the two types of cards.

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



Contactless Smart Card

Enabled	NFC

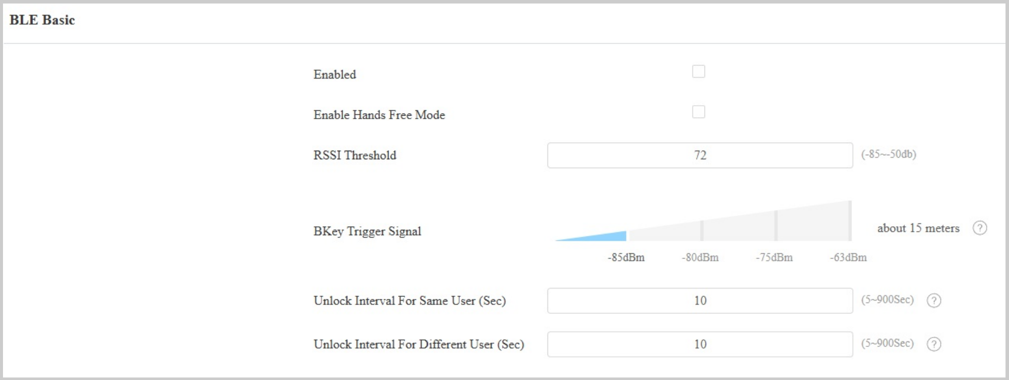
> **Note**
>
> The NFC feature is not available on iPhones.

Unlock by Bluetooth

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

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

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



BLE Basic

Enabled □

Enable Hands Free Mode □

RSSI Threshold 72 (-85~-50db)

BKey Trigger Signal about 15 meters

Unlock Interval For Same User (Sec) 10 (5~900Sec)

Unlock Interval For Different User (Sec) 10 (5~900Sec)

- **RSSI Threshold**: Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Bkey Trigger Signal**: There are four ranges that determine the Bkey trigger distance.
- **Unlock Interval For Same User(Sec)**: Set the time interval between consecutive Bluetooth door access attempts for the same user.
- **Unlock Interval For Different Users(Sec)**: Set the time interval between consecutive Bluetooth door access attempts for different users.

Note

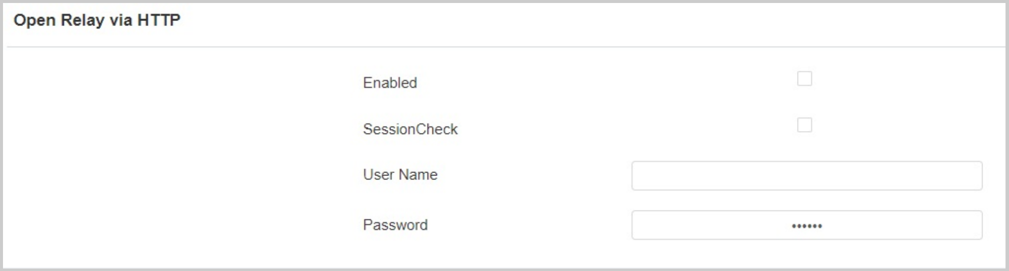
To learn about detailed configuration steps of different Bluetooth-based access methods, you can click the following articles.

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

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.



Open Relay via HTTP

Enabled □

SessionCheck □

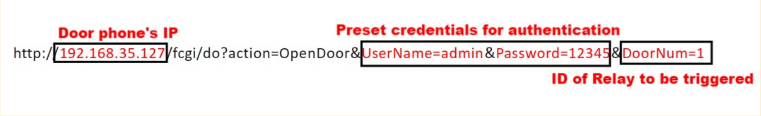
User Name

Password ••••••

- **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
ID of Relay to be triggered

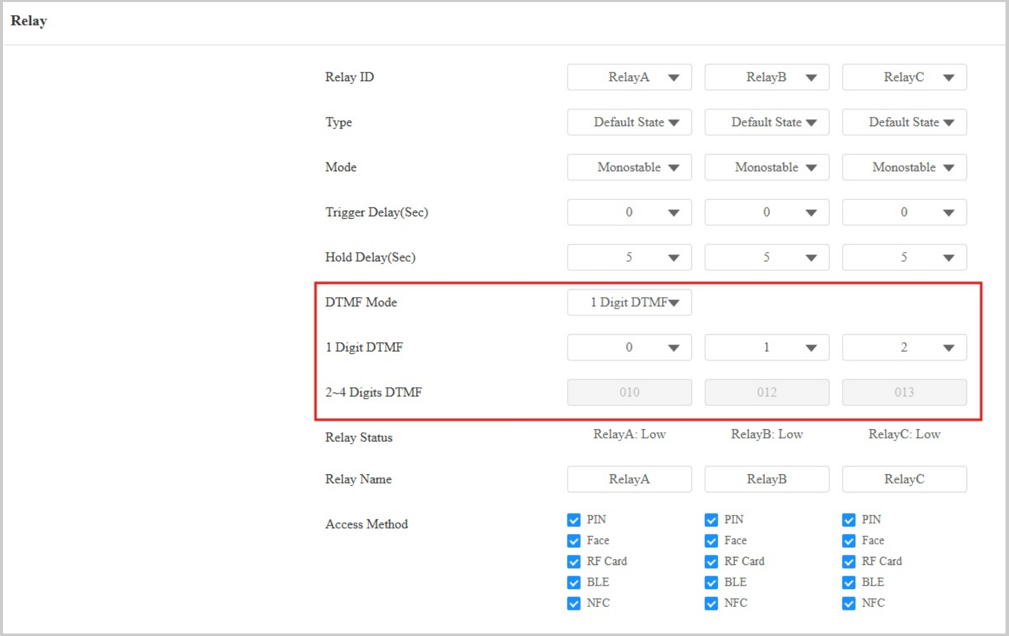
```
http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1
```

> **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.



Relay

Relay ID	RelayA	RelayB	RelayC
Type	Default State	Default State	Default State
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	5	5	5
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	0	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	RelayA	RelayB	RelayC
Access Method	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC	☑ PIN ☑ Face ☑ RF Card ☑ BLE ☑ NFC

- **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.

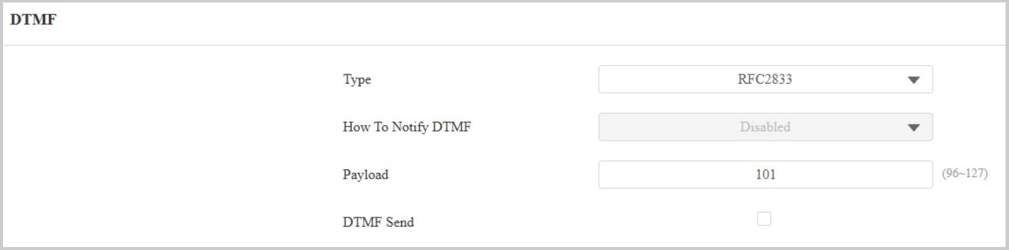
DTMF Data Transmission

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

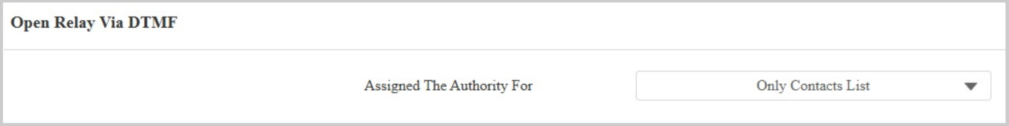
Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)
DTMF Send	□

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

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

DTMF Whitelist

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



Open Relay Via DTMF

Assigned The Authority For	Only Contacts List

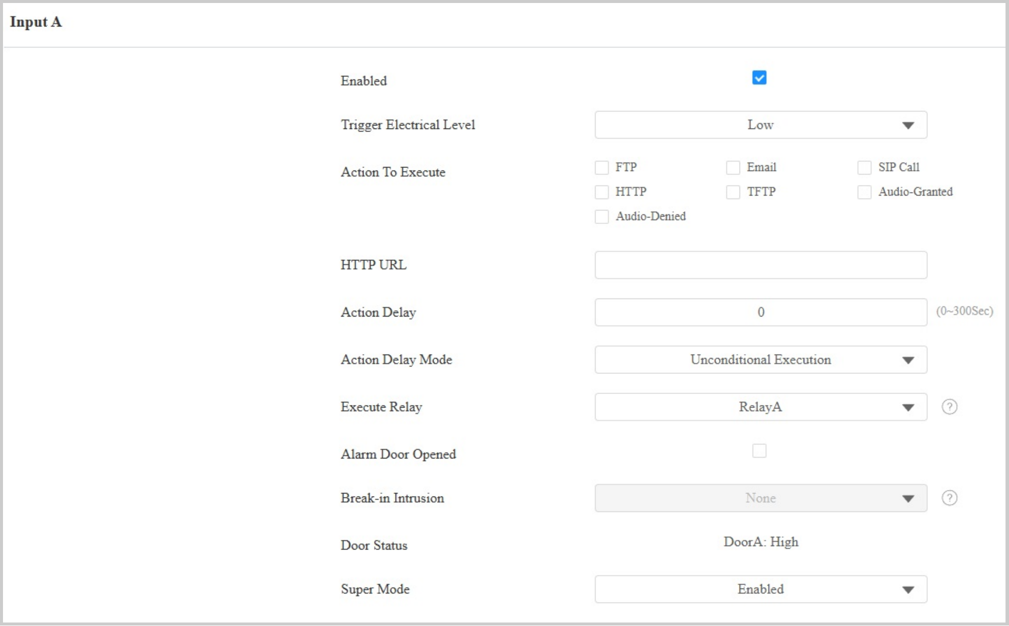
- **Assigned The Authority For**: Specify the contacts authorized to open doors via DTMF:
  - **None**: No numbers can unlock doors using DTMF.
  - **Only Contacts List**: Only numbers added to the door phone's contact list can unlock via DTMF.
  - **All Numbers**: Any numbers can unlock using DTMF.

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.



Input A

Enabled	☑
Trigger Electrical Level	Low
Action To Execute	☐ FTP ☐ Email ☐ SIP Call ☐ HTTP ☐ TFTP ☐ Audio-Granted ☐ Audio-Denied
HTTP URL	
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution
Execute Relay	RelayA
Alarm Door Opened	☐
Break-in Intrusion	None
Door Status	DoorA: High
Super Mode	Enabled

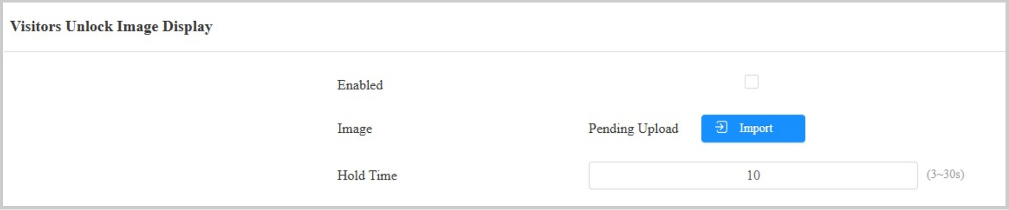
- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - FTP: Send a screenshot to the preconfigured 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.
    - TFTP: Send a screenshot to the preconfigured TFTP server.
    - Audio-Granted: The device will announce “Access Granted” when the door is opened.
    - Audio-Denied: The device will announce “Access Denied” when opening the door fails.
- **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.

Upload Guidance Picture for Visitors

You can upload a picture that will be shown to visitors when the door is opened with temporary keys, or unlocked by residents using SmartPlus Apps or indoor monitors during calls.

To set it up, go to the **Access Control > Relay > Visitors Unlock Image Display** interface.



Visitors Unlock Image Display

Enabled □

Image: Pending Upload

Hold Time: 10 (3~30s)

- **Image**: Max Size: 1M; Format: .jpg/png; Max resolution: 800*1280.
- **Hold Time**: The picture displaying duration. The default is 10 seconds.

Monitor and Image

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

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

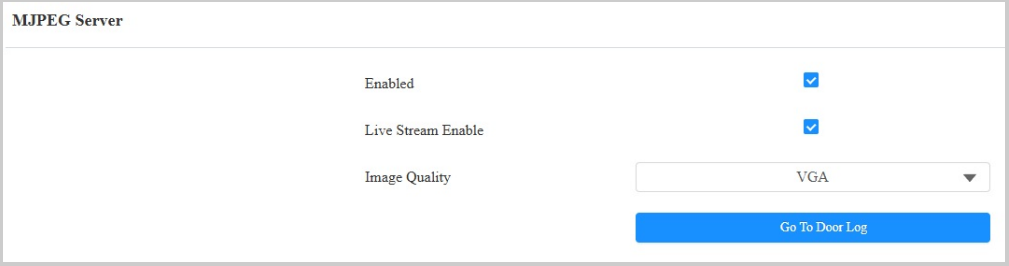
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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

MJPEG Image Capturing

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

Set it up on the web **Surveillance > MJPEG** interface.



MJPEG Server

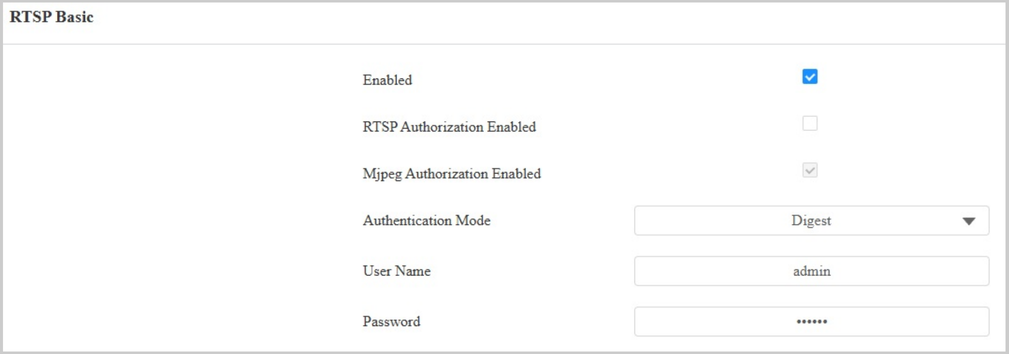
Enabled	☑
Live Stream Enable	☑
Image Quality	VGA
	Go To Door Log

- **Live Stream Enable**: Set whether to view the video stream via URLs(*http://ip:8080/video.cgi*; *http://ip:8080/picture.cgi*; *http://ip:8080/jpeg.cgi*). It is disabled by default.
- **Image Quality**: Specify the MJPEG image quality from the lowest QCIF(176×144 pixels) to the highest 1080P(1920×1080 pixels).
- **Go to Door Log**: Click to redirect to the access log interface. The selection of image quality affects the maximum number of logs stored and exported.

MJPEG Authorization

The MJPEG authorization is enabled by default to limit access to the MJPEG images and videos.

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



RTSP Basic

Enabled	☑
RTSP Authorization Enabled	□
Mjpeg Authorization Enabled	☑
Authentication Mode	Digest
User Name	admin
Password	••••••

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

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

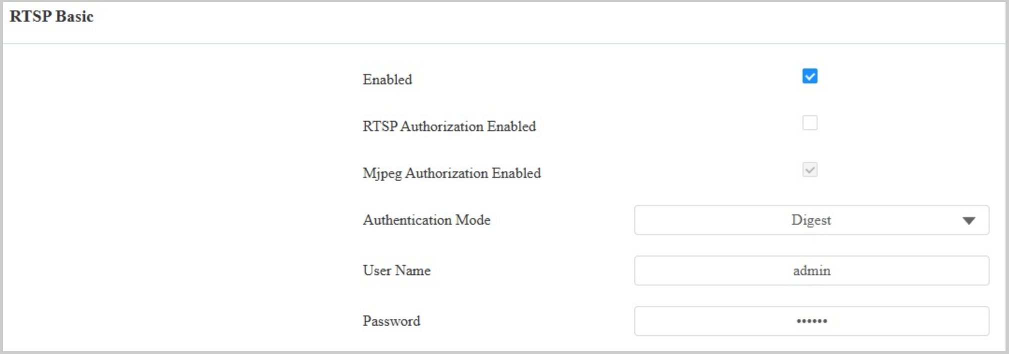
RTSP Stream Monitoring

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

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

RTSP Basic Setting

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



RTSP Basic

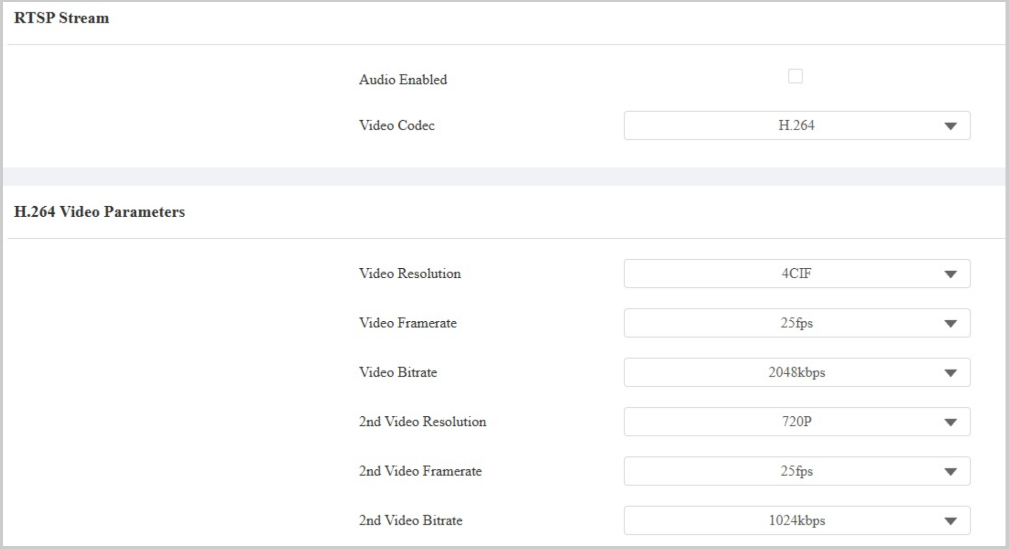
Enabled	☑
RTSP Authorization Enabled	□
Mjpeg Authorization Enabled	☑
Authentication Mode	Digest
User Name	admin
Password	••••••

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

RTSP Stream Setting

The RTSP stream can use H.264 as the video codec. You adjust the video resolution, bitrate, and other settings.

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



RTSP Stream

Audio Enabled	□
Video Codec	H.264

H.264 Video Parameters

Video Resolution	4CIF
Video Framerate	25fps
Video Bitrate	2048kbps
2nd Video Resolution	720P
2nd Video Framerate	25fps
2nd Video Bitrate	1024kbps

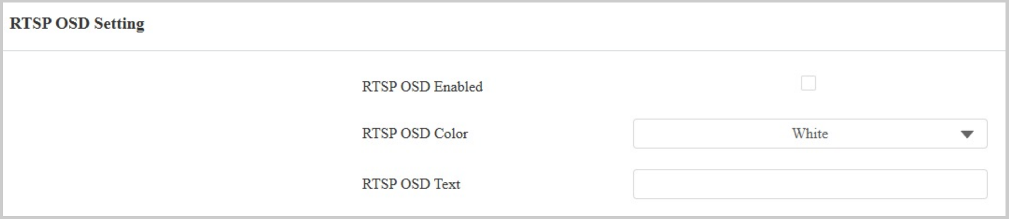
- **Audio Enabled**: Decide whether the RTSP stream has sound.
- **Video Resolution**: Specify the image resolution, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate 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 2048 kbps.
- **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.
- **2nd Video Bitrate**: Set the bit rate for the second video stream channel. The default is 512 kbps.

> **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

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.



RTSP OSD Setting

RTSP OSD Enabled	□
RTSP OSD Color	White ▼
RTSP OSD Text	

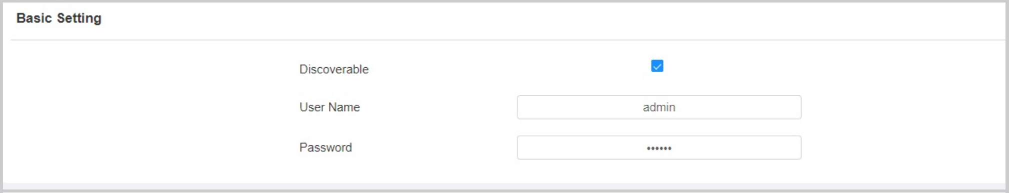
- **RTSP OSD Color**: Select the color from White, Black, Red, Green, and Blue.
- **RTSP OSD Text**: Customize the OSD content.

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.

Set it up on the web **Surveillance > ONVIF** interface.



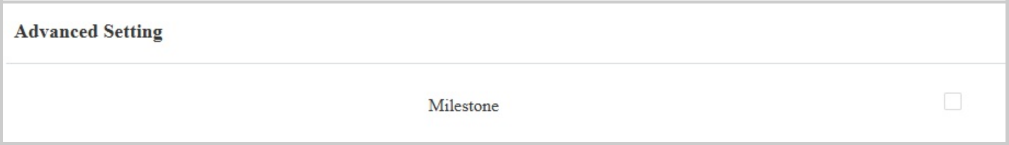
Basic Setting

Discoverable	☑
User Name	admin
Password	••••••

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

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

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



Advanced Setting

Milestone □

Live Stream

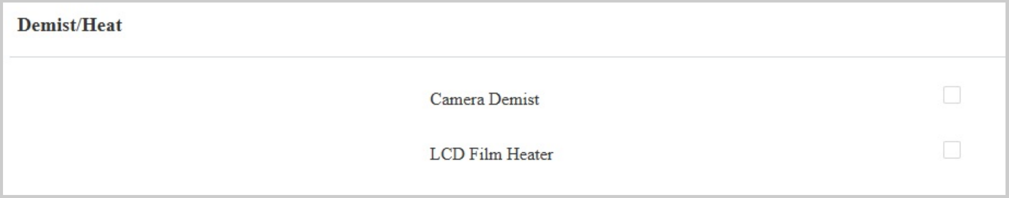
There are two ways to check the real-time video from the device. One is to go to the device web interface and view the video there. The other is to enter the correct URL on the web browser and access the video directly.

View the real-time video on the web **Surveillance > Live Stream** interface. Before viewing the live stream, you are required to enable the live stream feature and enter the username and password set on the MJPEG Authorization section.

Camera Demist and LCD Heating

The device’s camera and LCD may malfunction in an extremely cold environment. You can set up the camera demist and LCD heating feature to make sure the device works normally.

Go to the web **Device > Demist/Heat** interface.



Demist/Heat

Camera Demist □

LCD Film Heater □

- **Camera Demist**: The device will start heating the camera when the temperature is lower than 35℃. It will stop when the camera temperature reaches 55℃.
- **LCD Film Heater**: The device will start heating the LCD when the temperature is lower than 20℃. It will stop when the LCD temperature reaches 0℃.

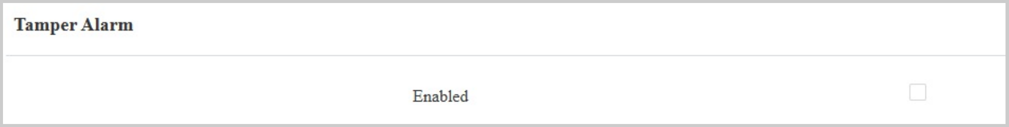
Security

Tamper Alarm

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

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

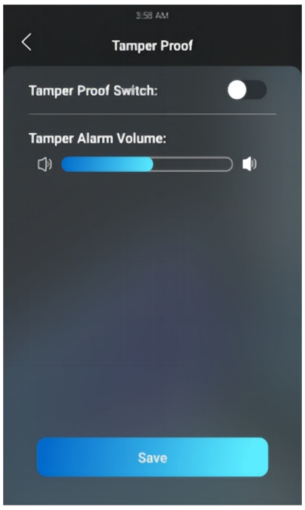
Set it up on the web **System > Security > Tamper Alarm** interface.



Tamper Alarm

Enabled □

You can also set up the tamper alarm on the **Setting > Security > Tamper Proof** screen.



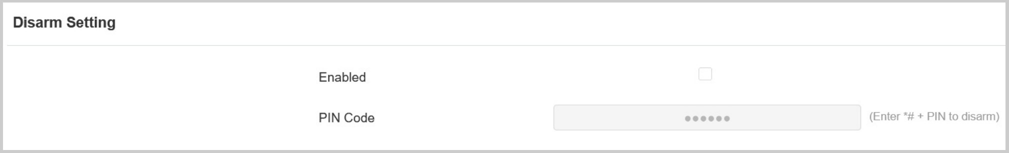
Tamper Proof Switch:

Tamper Alarm Volume:

Disarm Setting

When the tamper alarm is triggered, you can enter the disarm code to clear the alarm.

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



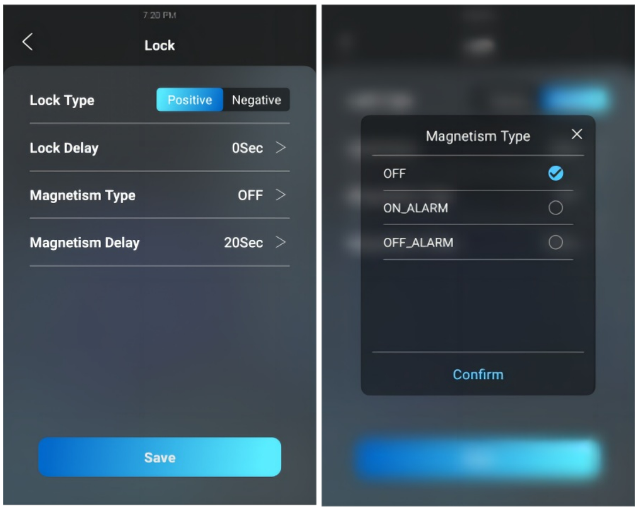
Disarm Setting

Enabled	□	
PIN Code	••••••	(Enter *# + PIN to disarm)

Lock Security

The door phone can work with other door locks and sensors to keep the lock secure. It will sound the alarm to alert users if the door sensor finds the door open or not fully closed.

On the device, go to **Setting > Security > Lock** for the setting.



Lock Type: Positive | Negative
Lock Delay: 0Sec
Magnetism Type: OFF
Magnetism Delay: 20Sec

Magnetism Type
- OFF ✓
- ON_ALARM ○
- OFF_ALARM ○

- **Lock Type**:
  - **Positive**: The lock unlocks when power is ON and locks when power is OFF. Suitable for scenarios where the door should remain locked during a power outage.
  - **Negative**: The lock unlocks when power is OFF and locks when power is ON. Commonly used in places like fire escapes or emergency exits, ensuring that the door opens automatically during a power outage, allowing people to evacuate safely.
- **Lock Delay**: Select door unlock delay time after users are granted door access. The delay time range is from 0-10 seconds.
- **Magnetism Type**:
  - **OFF**: Disable the door sensor and alarm.
  - **ON_ALARM**: The positive lock is used.
  - **OFF_ALARM**: The negative lock is used.
- **Magnetism Delay**: Select the alarm delay time after its being triggered. The delay range is from 10-120 seconds.

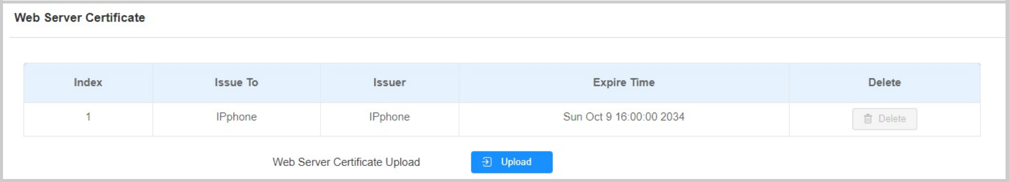
Client Certificate Setting

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 a web server certificate on the web **System > Certificate > Web Server Certificate** interface.



Web Server Certificate

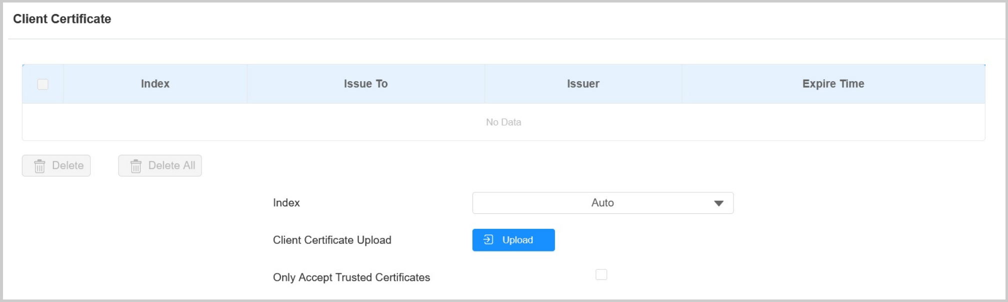
Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

Web Server Certificate Upload

Client Certificate

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

Upload and configure client certificates on the web **System > Certificate > Client Certificate** interface.



Client Certificate

□	Index	Issue To	Issuer	Expire Time
No Data				

Delete Delete All

Index: Auto

Client Certificate Upload: Upload

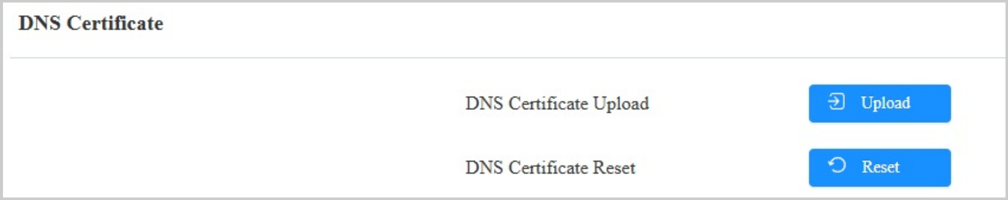
Only Accept Trusted Certificates: □

- **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 the value from 1 to 10, the uploaded certificate will be displayed according to the number.
- **Client Certificate Upload**: Locate and upload the desired certificate (Format: .pem,.der,.cer,.crt).
- **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.

Upload Certificate for SIP Account Registration

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

To upload the DNS certificate, go to **System > Certificate > DNS Certificate** interface.



DNS Certificate

DNS Certificate Upload: Upload

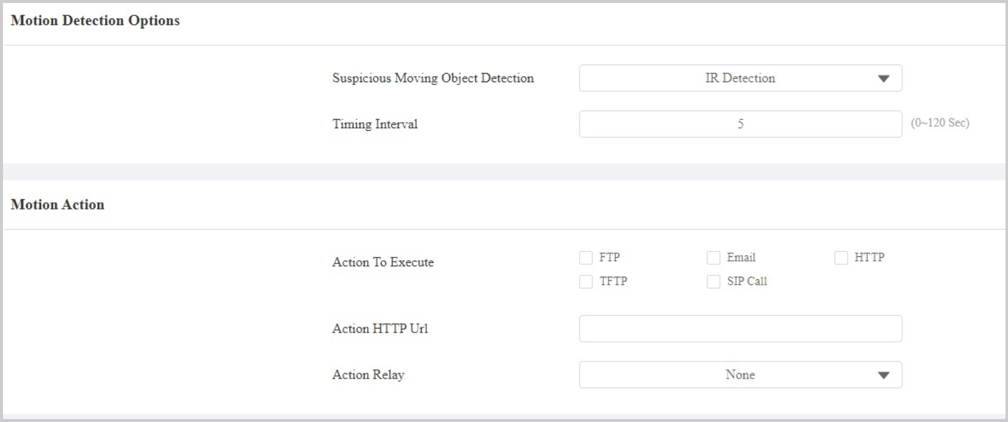
DNS Certificate Reset: Reset

- **DNS Certificate Upload**: Locate and upload the desired certificate (Format: .pem,.der,.cer,.crt).
- **DNS Certificate Reset**: Click Reset to remove the uploaded certificate.

Motion Detection

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

Set it up on the web **Surveillance > Motion > Motion Detection Options** interface.



Motion Detection Options

Suspicious Moving Object Detection: IR Detection

Timing Interval: 5 (0~120 Sec)

Motion Action

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

Action HTTP Url:

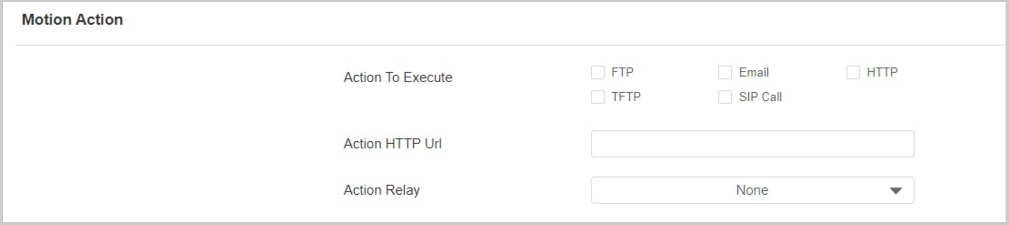
Action Relay: None

- **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.
  - **IR Detection**: When the infrared detects moving objects, preset actions will be triggered. It offers better detection in low-light or dark conditions.
  - **Pedestrian Detection**: When the device detects the upper body of the passersby, preset actions will be triggered.

- **Timing Interval**: Determine how to delay and trigger motion detection.
  - Timing Interval between 1–3 seconds: Once detection is triggered, preset actions will be performed.
  - 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 5 seconds.
- **Detection Accuracy**: Available for video and pedestrian detections. 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 the mouse button to select up to three detection areas.

Motion Detection Triggered Actions

You can set up the actions triggered by the motion detection on the **Surveillance > Motion > Motion Action** interface.



Motion Action

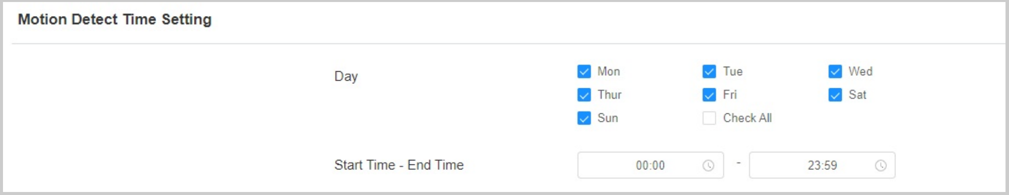
Action To Execute: □ FTP □ Email □ HTTP □ TFTP □ SIP Call

Action HTTP Url:

Action Relay: None

- **Action to Execute**: The notification type includes FTP, Email, SIP Call, and HTTP.
  - FTP: The notification will be sent to the designated FTP server.
  - Email: The email will be sent to the pre-configured email address.
  - SIP Call: A call will be made to the pre-configured number.
  - HTTP: The notification will be sent to the designated server.
  - TFTP: The notification will be sent to the designated TFTP 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.
- **Action Relay**: The relay to be triggered.

Scroll down to set the schedule for the motion detection to be effective.

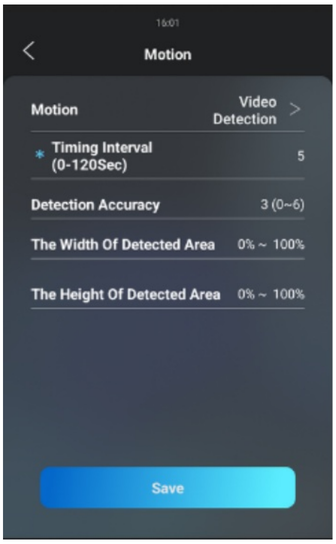


Motion Detect Time Setting

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

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

You can also set up motion detection on the **Setting > Advanced Setting > Surveillance > Motion** screen.



16:01

Motion

Motion: Video Detection

* Timing Interval (0-120Sec): 5

Detection Accuracy: 3 (0~6)

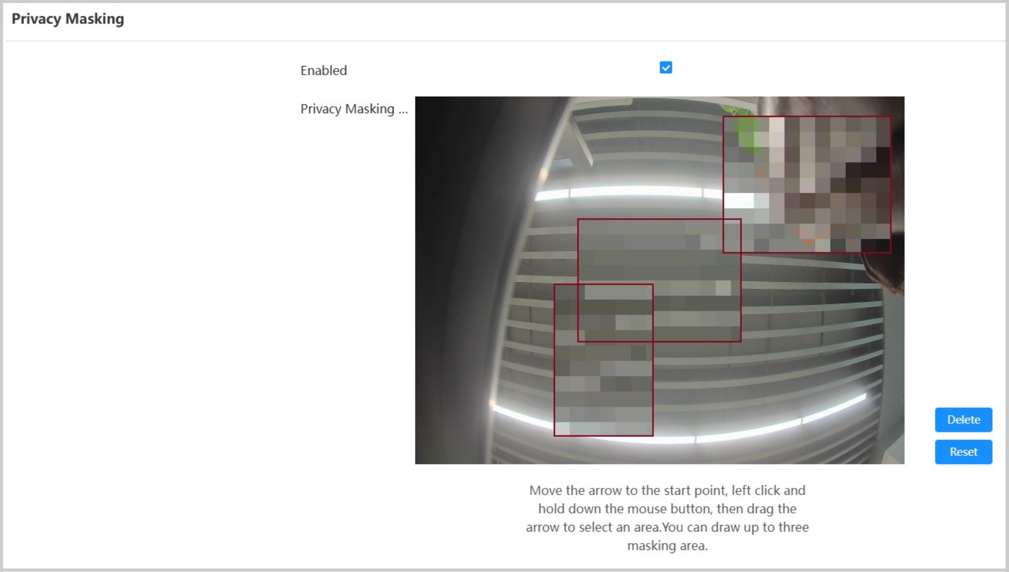
The Width Of Detected Area: 0% ~ 100%

The Height Of Detected Area: 0% ~ 100%

Privacy Masking

To protect the user's privacy, you can blur three areas of the video screen. This also applies to video calls, incoming call previews, surveillance screens, screenshots, etc.

To set it up, go to the **Surveillance > Privacy Masking** interface. You can click the target box and click **Delete** to remove it.



Move the arrow to the start point, left click and hold down the mouse button, then drag the arrow to select an area.You can draw up to three masking area.

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.

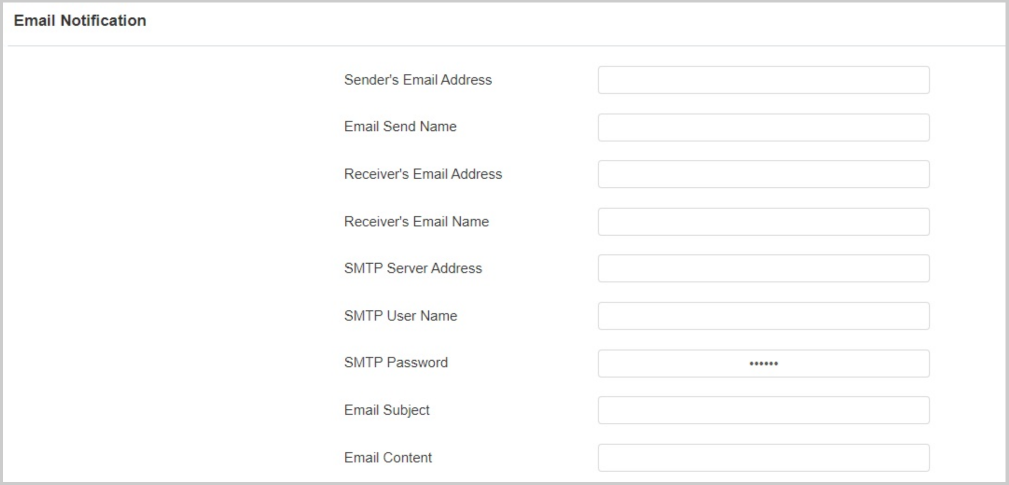
Set up notifications on the **Setting > Action** interface.

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.



Email Notification

Sender's Email Address	
Email Send Name	
Receiver's Email Address	
Receiver's Email Name	
SMTP Server Address	
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	

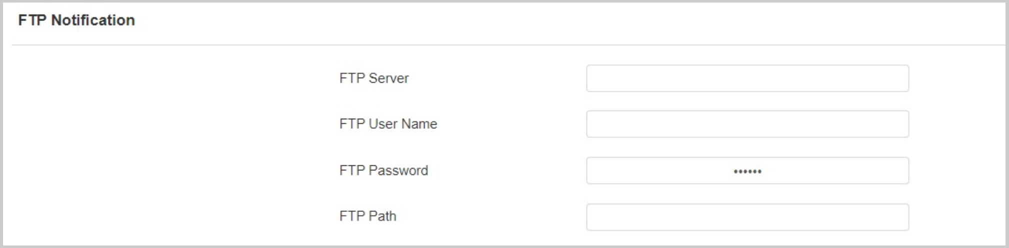
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

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.



FTP Notification

FTP Server

FTP User Name

FTP Password ••••••

FTP Path

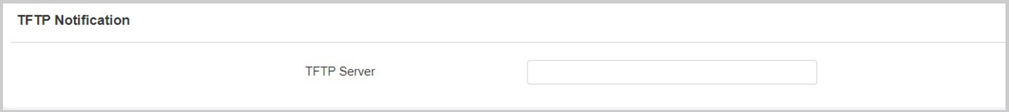
- **FTP Server**: Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

TFTP Notification

To receive security notifications via the TFTP server, you need to enter the TFTP server address.

Click here to view the configuration steps.

Navigate to the web **Setting > Action > TFTP Notification** interface.



TFTP Notification

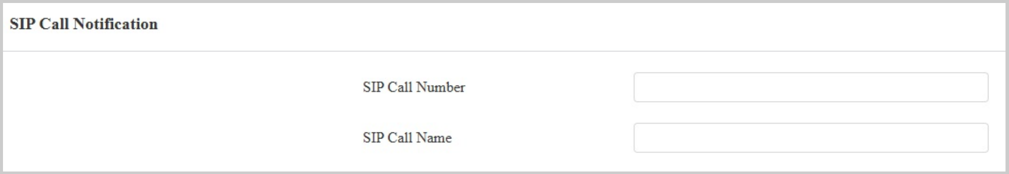
TFTP Server

- **TFTP Server**: Enter the address (URL) of the TFTP server for the TFTP notification.

SIP Call Notification

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

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



SIP Call Notification

SIP Call Number

SIP Call Name

Action URL

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

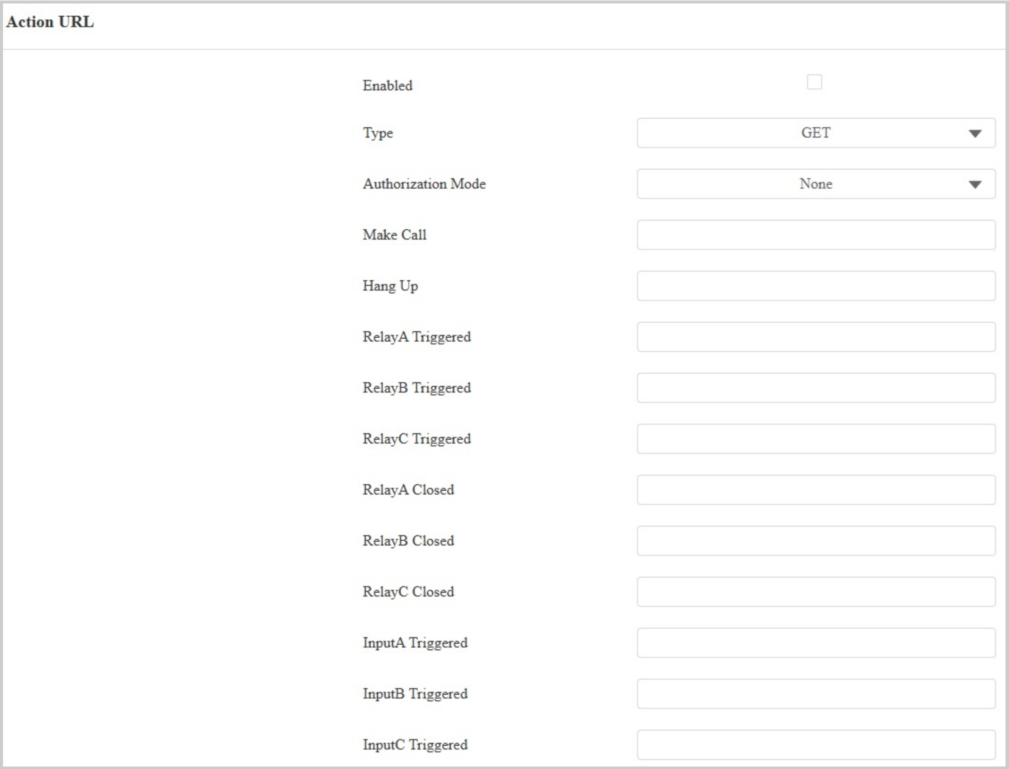
Akuvox Action URL:

No	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/Callnumber=$remote
2	Hang Up	$remote	Http://server ip/Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/relaytrigger=$relay1status
4	Relay Closed	$relay1status	Http://server ip/relayclose=$relay1status
5	Input Triggered	$input1status	Http://server ip/inputtrigger=$input1status
6	Input Closed	$input1status	Http://server ip/inputclose=$input1status
7	Valid Code Entered	$code	Http://server ip/validcode=$code
8	Invalid Code Entered	$code	Http://server ip/invalidcode=$code
9	Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
10	Invalid Card Entered	$card_sn	Http://server ip/invalidcard=$card_sn
11	Facial Recognition	$unlocktype	Http://serverip/unlocktype=$unlocktype:floor=$floor:webrelay=$webrelay:userid=$userid
12	QR Code	$unlocktype	Http://serverip/unlocktype=$unlocktype:floor=$floor:webrelay=$webrelay:userid=$userid
13	Break-in Alarm	$alarm status	Http://server ip/tampertrigger=$alarm status
14	Setup Completed	$model	Http://server ip/model/$model

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

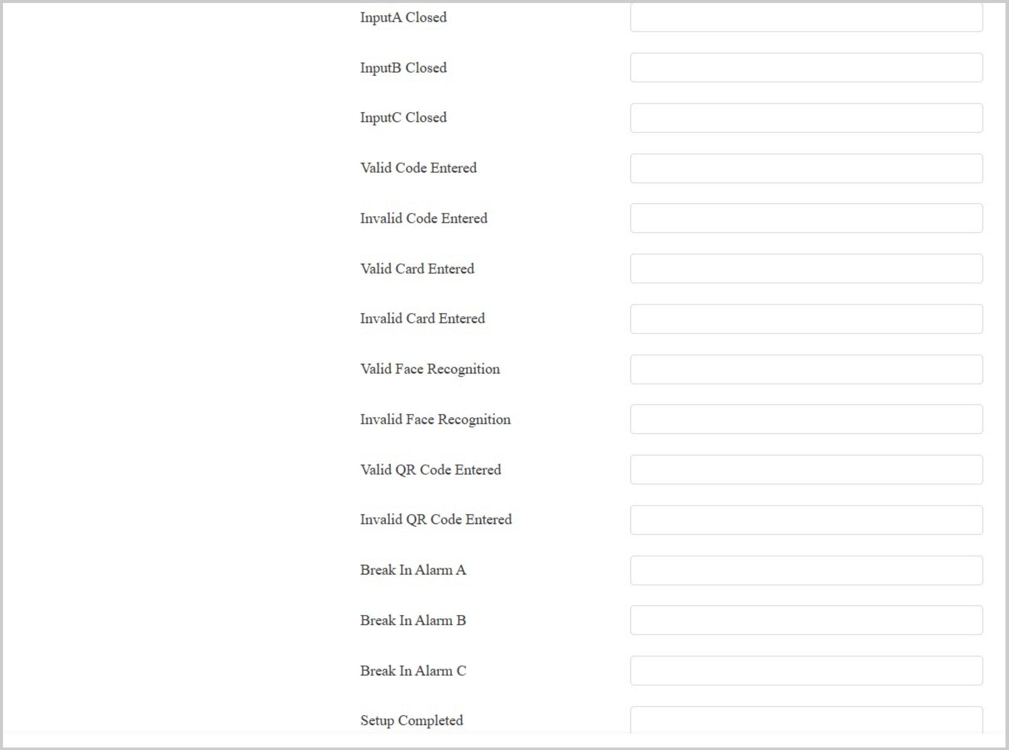
Set up action URLs on the web **Setting > Actions URL** interface.

> **Note**
>
> Action URLs and formats are provided by third-party manufacturers. Akuvox door phone only sends the URL to third-party devices.



Action URL

Enabled	□
Type	GET
Authorization Mode	None
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayC Triggered	
RelayA Closed	
RelayB Closed	
RelayC Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	



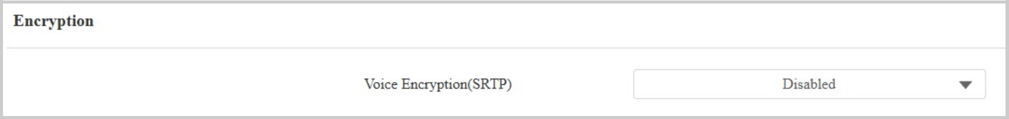
InputA Closed	
InputB Closed	
InputC Closed	
Valid Code Entered	
Invalid Code Entered	
Valid Card Entered	
Invalid Card Entered	
Valid Face Recognition	
Invalid Face Recognition	
Valid QR Code Entered	
Invalid QR Code Entered	
Break In Alarm A	
Break In Alarm B	
Break In Alarm C	
Setup Completed	

- **Type**: Select the request type between GET and POST.
- **Authorization Mode**: Select the authorization mode. If Digest is selected, you need to set up the username and password.
- **Setup Completed**: This URL is sent after the device boots up, and it is not controlled by the Action URL Enable switch. If you do not want to use this action URL, leave the field blank.

Voice Encryption

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

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



Encryption

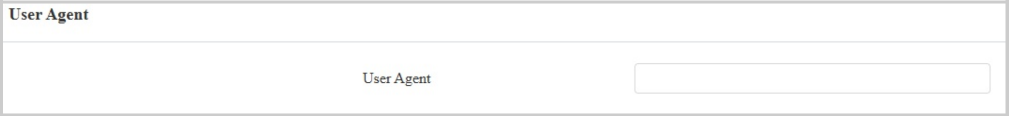
Voice Encryption(SRTP) Disabled

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

User Agent

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

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



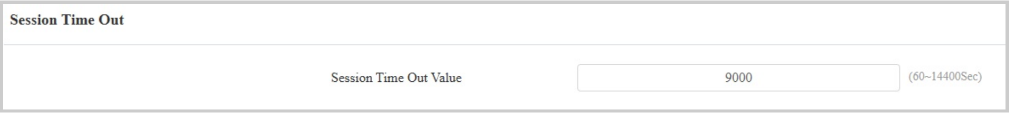
User Agent

User Agent

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.

Set it up on the web **System > Security > Session Time Out** interface.



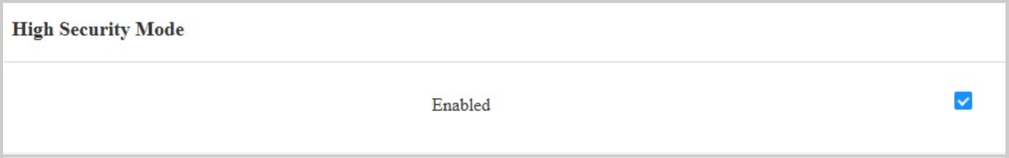
Session Time Out

Session Time Out Value 9000 (60~14400Sec)

High Security Mode

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

Enable/disable the high security mode on the web **System > Security > High Security Mode** interface.



High Security Mode

Enabled ☑

Important Notes

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

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

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

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

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

- 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

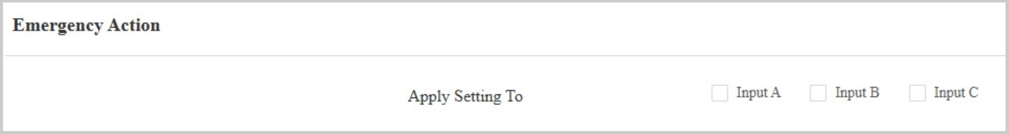
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

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.



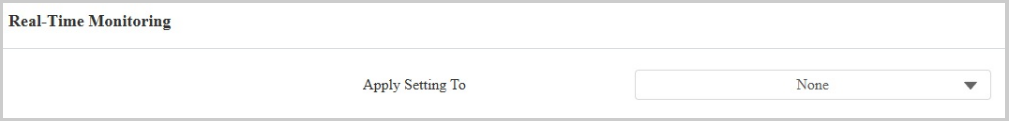
Emergency Action

Apply Setting To □ Input A □ Input B □ Input C

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.



Real-Time Monitoring

Apply Setting To: None

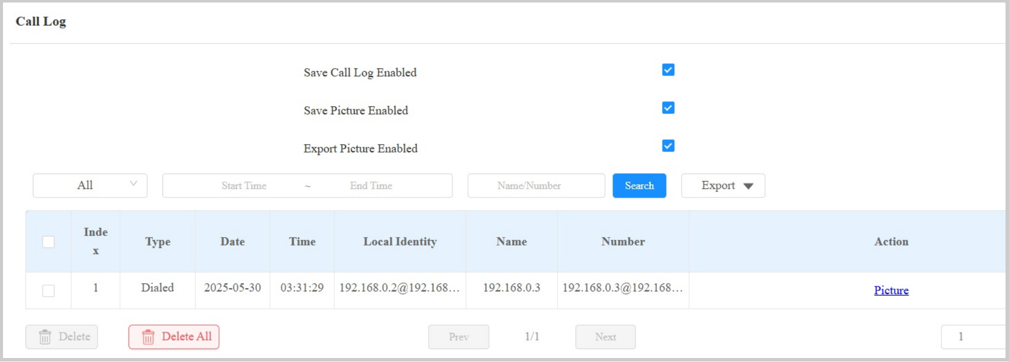
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: the door is opened by triggering input.
  - **Relay**: the door is opened by triggering the relay.

Logs

Call Logs

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

Check the call log on the web **Status > Call Log** interface. The device supports up to 600 call logs, which can be exported in CSV format.



Call Log

Save Call Log Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled ☑

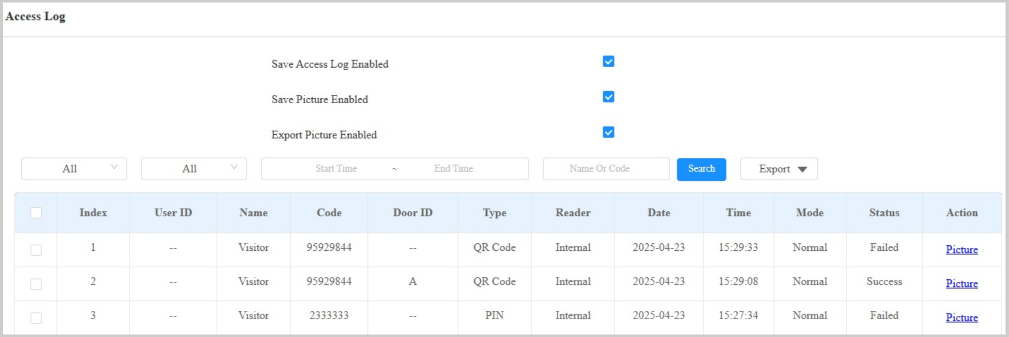
□	Index	Type	Date	Time	Local Identity	Name	Number	Action
□	1	Dialed	2025-05-30	03:31:29	192.168.0.2@192.168…	192.168.0.3	192.168.0.3@192.168…	Picture

- **Call History**: Four types of call history are available: All, Dialed, Received, and Missed.
- **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.
- **Save Picture Enabled**: When enabled, the device will capture pictures of calls, and you can click **Picture** in the Action column to view the screenshot.
- **Export Picture Enabled**: When enabled, you can export call logs with images.

Door Logs

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

Check the door log on the web **Status > Access Log** interface. Door logs can be exported in XML or CSV format.



Access Log

Save Access Log Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled ☑

□	Index	User ID	Name	Code	Door ID	Type	Reader	Date	Time	Mode	Status	Action
□	1	--	Visitor	95929844	--	QR Code	Internal	2025-04-23	15:29:33	Normal	Failed	Picture
□	2	--	Visitor	95929844	A	QR Code	Internal	2025-04-23	15:29:08	Normal	Success	Picture
□	3	--	Visitor	2333333	--	PIN	Internal	2025-04-23	15:27:34	Normal	Failed	Picture

- **All**: Three types of access logs are available: All, Success, and Failed.
- **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 Picture Enabled**: When enabled, you can export door logs with images.
- **Action**: Click **Picture** to view the captured image.

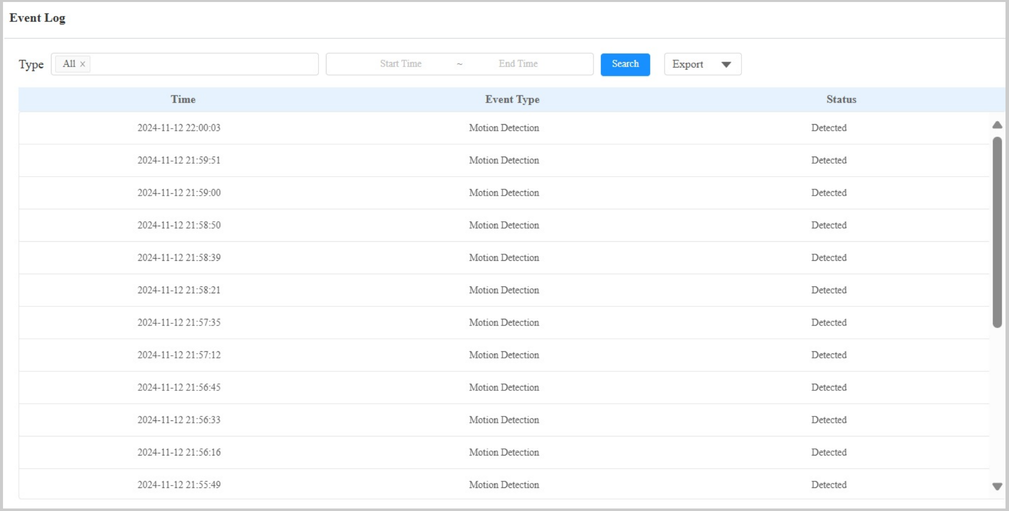
The supported number of door logs stored and exported varies by image resolution.

Resolution	Maximum Number of Stored Door Logs	Maximum Number of Exported Door Logs with 1.6G Export Capacity.
Null, Save Picture is disabled.	14,000	137,000
QCIF	14,000	137,000
QVGA	14,000	50,300
CIF	14,000	37,700
VGA	14,000	14,800
4CIF	10,000	10,800
720P	5,000	5,400
1080P	2,500	2,700

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.



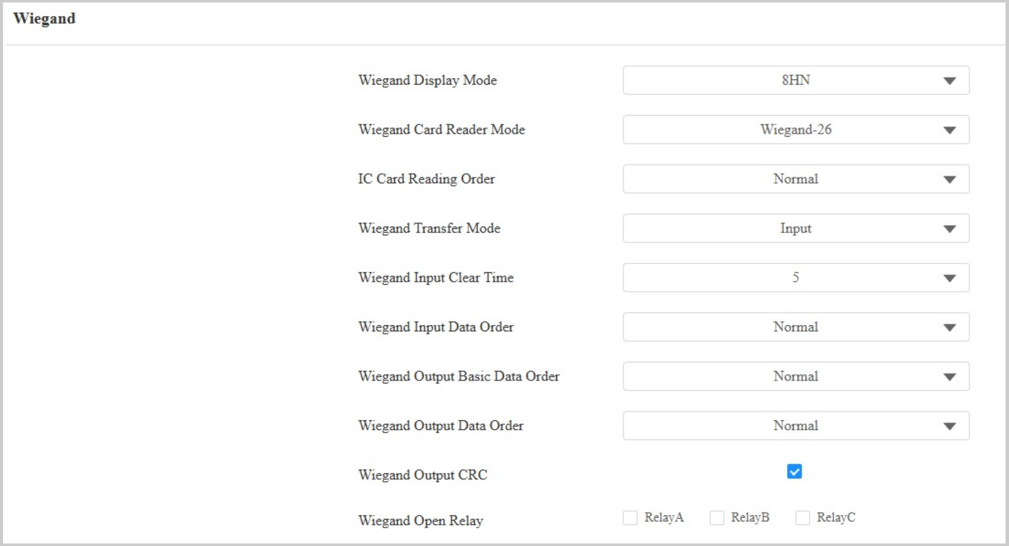
Time	Event Type	Status
2024-11-12 22:00:03	Motion Detection	Detected
2024-11-12 21:59:51	Motion Detection	Detected
2024-11-12 21:59:00	Motion Detection	Detected
2024-11-12 21:58:50	Motion Detection	Detected
2024-11-12 21:58:39	Motion Detection	Detected
2024-11-12 21:58:21	Motion Detection	Detected
2024-11-12 21:57:35	Motion Detection	Detected
2024-11-12 21:57:12	Motion Detection	Detected
2024-11-12 21:56:45	Motion Detection	Detected
2024-11-12 21:56:33	Motion Detection	Detected
2024-11-12 21:56:16	Motion Detection	Detected
2024-11-12 21:55:49	Motion Detection	Detected

Integration with Third-party Devices

Integration via Wiegand

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

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



Wiegand

Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Wiegand-26
IC Card Reading Order	Normal
Wiegand Transfer Mode	Input
Wiegand Input Clear Time	5
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output CRC	☑
Wiegand Open Relay	□ RelayA □ RelayB □ RelayC

- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
  - **Ignore Facility Code**: This option is available when 6H3D5D(WG26) is selected. When enabled, the first three bits of the cards will be ignored for successful card reading.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device. It is automatically configured.
- **IC Card Reading Order**: This option only works when Wiegand-26 is selected.
  - **Normal**: The device will read the last three bytes of the IC card. For example, if the IC card number is 840C9F50, 0C9F50 will be read.
  - **Reversed**: The device will read the first three bytes of the IC card. For example, if the IC card number is 840C9F50, 840C9F will be read.
- **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 card code.
  - **Convert To Card No. Output**: The device serves as a sender and cannot directly output the data such as the face data.
- **Wiegand Input Clear Time**: When the interval of entering passwords exceeds the time. All entered passwords will be cleared.
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- **Wiegand Output Basic Data Order**: Set the sequence of the card data before going through 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.
- **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 Output CRC**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **Wiegand Open Relay**: Check the relay to be triggered through Wiegand.
- **Convert To Wiegand Output**: Available when **Output** is selected as Wiegand Transfer Mode. This option determines the output PIN format.

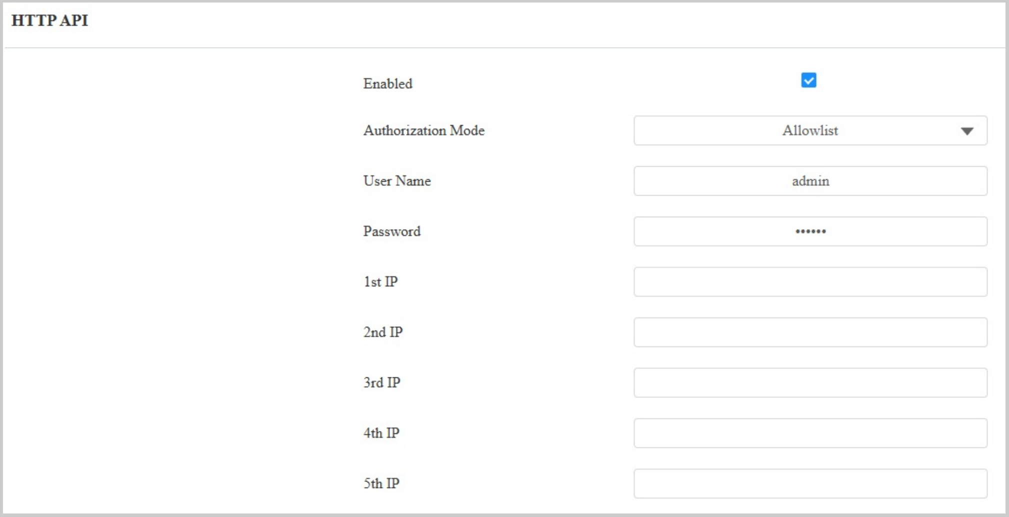
- Disabled: Turn off the feature.
- 8 bits per digit: When users press "1" on the keypad, the binary data will be transmitted in 8 bits "11100001".
- 4 bits per digit: When users press "1" on the keypad, the binary data will be transmitted in 4 bits "0001".
- All at once: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode. For example, “123456” will be converted to “01e240” in Wiegand 26.

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

Integration via HTTP API

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

Set it up on the web **Setting > HTTP API** interface for the integration.



HTTP API

Enabled	☑
Authorization Mode	Allowlist ▼
User Name	admin
Password	••••••
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

- **Enabled**: Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode**: Select among the following options: None, Normal, Allowlist, Basic, Digest, and Token for authorization type, which will be explained in detail in the following chart.
- **User Name**: Enter the user name when **Basic** or **Digest** authorization mode is selected. The default username is admin.
- **Password**: Enter the password when **Basic** or **Digest** authorization mode is selected. The default password is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

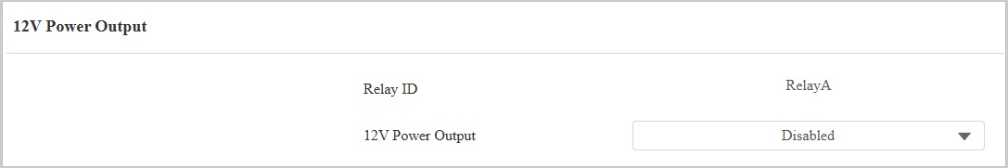
Please refer to the following description for the authentication mode:

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

Set it up on the web **Access Control > Relay >12V Power Output** interface.



12V Power Output

Relay ID: RelayA

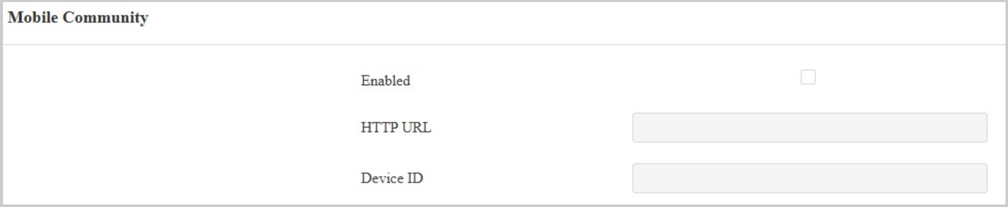
12V Power Output: Disabled

- **12V Power Output**:
  - **Disabled**: Disable the power output function;
  - **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.
    - **Time Out (Sec)**: Select the power supply time duration after the relay is triggered from 3, 5, and 10. It is 3 seconds by default. The power output is 12V, and the maximum output amperage is 0.8A.
  - **Security Relay A**: The device can work with the security relay.

Mobile Community

You can connect the door phone to the third-party QR code server for QR code verification. When you access the door using a QR code, the QR code will be sent to the QR code server for verification before granting you an access permission. This feature is applied to the devices not deployed in the SmartPlus platform for the QR code door access.

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



Mobile Community

Enabled: □

HTTP URL:

Device ID:

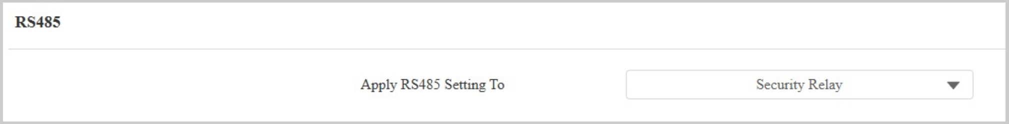
- **HTTP URL**: Enter the HTTP URL that sends requests to the third-party system server. It supports two parameters: {QRCode} and {DeviceID}.
  - Replace {QRCode} with the content of the QR code.
  - Replace {DeviceID} with the device number you fill in below.
- **Device ID**: Provided by the third-party server and used in the HTTP command.

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.

Set it up on the **Device > RS485** interface.



RS485

Apply RS485 Setting To: Security Relay

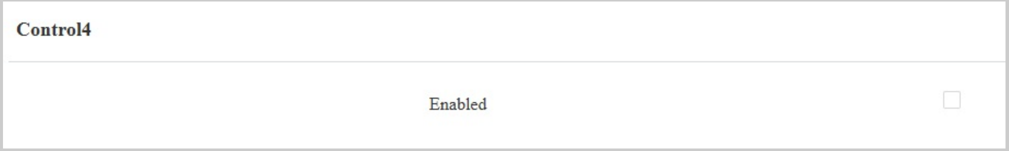
- **Disable**: The RS485 function is disabled.
- **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **Transfer Mode**: Select the RS485 working mode, Output, or Input.
    - **Local Relay 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.
- **Security Relay**: Select this option when the device works with the SR01.

Integration with Control4

The device supports integration with Control4, which enables users to call, monitor, and open doors on the Control4 panel.

Click here to learn the detailed configuration and other models supporting the integration.

To enable the integration, turn on a switch on the **Device > Control4** interface.



Control4

Enabled □

- **Control4**: When enabled, High Security Mode, RTSP Authentication, and Discovery Mode will all be disabled.

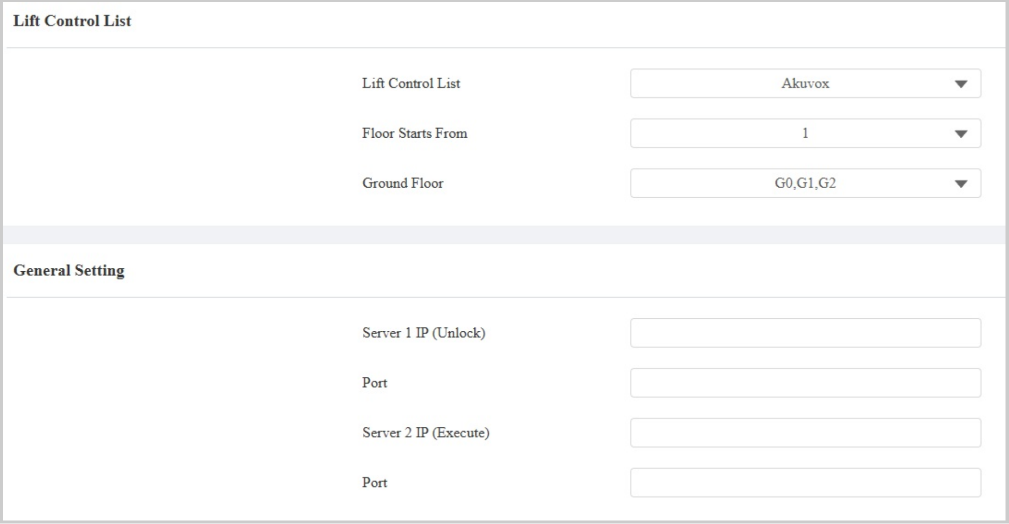
Lift Control

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 up the lift control, navigate to the web **Device > Lift Control** interface. Select **Akuvox** in the Lift Control List.

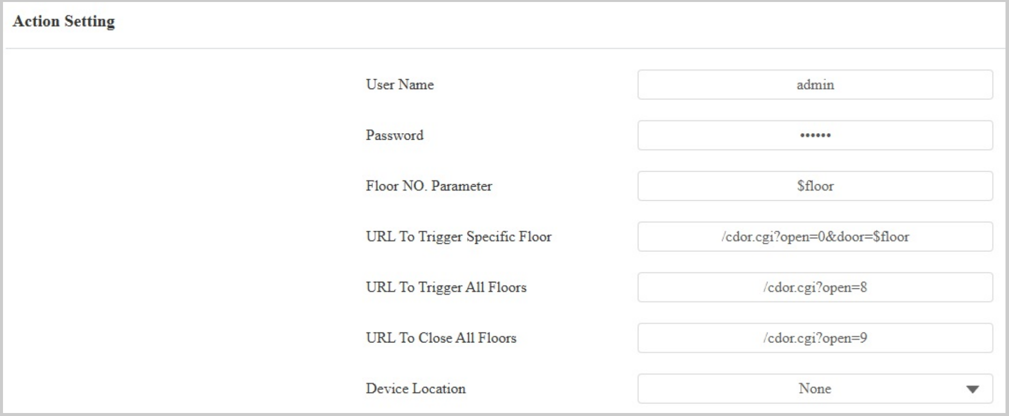


Lift Control List

Lift Control List	Akuvox ▼
Floor Starts From	1 ▼
Ground Floor	G0,G1,G2 ▼

General Setting

Server 1 IP (Unlock)	
Port	
Server 2 IP (Execute)	
Port	



Action Setting

User Name	admin
Password	••••••
Floor NO. Parameter	$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=$floor
URL To Trigger All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9
Device Location	None ▼

- **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.
- **Server 1 IP(Unlock)**: The IP address of the lift controller that unlocks the elevator button(s).
- **Port**: The server port of the lift controller server.
- **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.
- **User Name**: 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.
- **Device Location**: Select the floor where the device is installed.

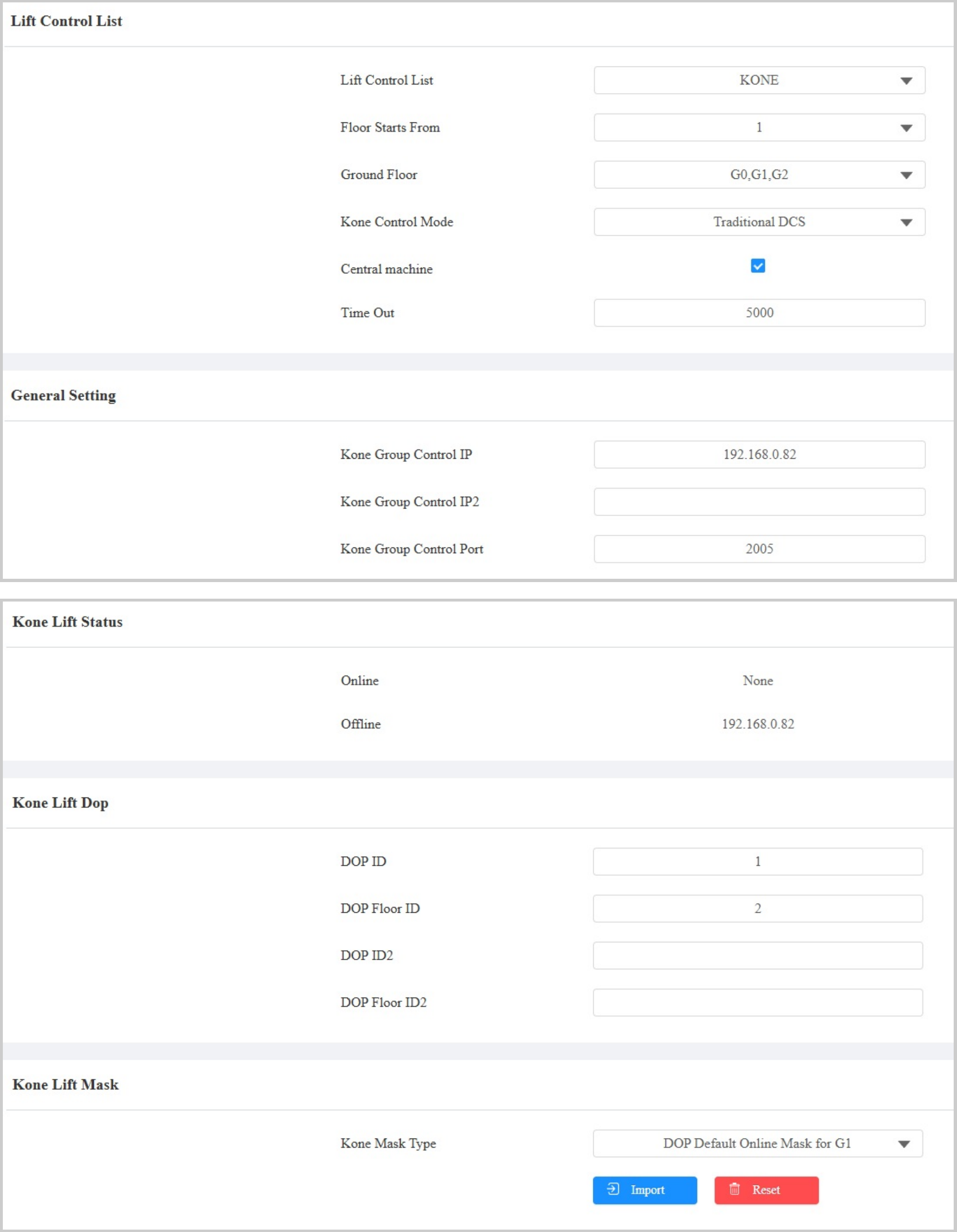
KONE Lift Control

The device supports the integration with the KONE lift control panel. Users can use their credentials configured on the door phone to unlock the lift button and access the desired floor.

Click the following articles to view the detailed configuration steps and different integration scenarios.

- KONE Turnstile Integration
- KONE Destination Control System(DCS) Integration

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



Lift Control List

Lift Control List	KONE
Floor Starts From	1
Ground Floor	G0,G1,G2
Kone Control Mode	Traditional DCS
Central machine	☑
Time Out	5000

General Setting

Kone Group Control IP	192.168.0.82
Kone Group Control IP2	
Kone Group Control Port	2005

Kone Lift Status

Online	None
Offline	192.168.0.82

Kone Lift Dop

DOP ID	1
DOP Floor ID	2
DOP ID2	
DOP Floor ID2	

Kone Lift Mask

Kone Mask Type	DOP Default Online Mask for G1

- **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.
- **KONE Control Mode**: Select the option based on the lift control scenario.
  - **Traditional DCS**: The destination operating panels are on all floors, and there are no buttons on the car operating panel.
  - **Conventional**: Passengers select their destination floors on the control panel inside the lift car.
  - **Hybrid DCS**: The destination operating panels are located only on the main floors, while other floors have conventional landing signalization. Cars have a conventional operating panel.
  - **Turnstile Integration**: Passengers use their credentials at the entrance and call the lift.
- **Central Machine**:
  When the door phone is used as the central machine, configure the following options.

  - **KONE Group Control IP/IP2**: The KONE control panel’s IP address. You can enter three IPs for each group, separated by “;”.
  - **Kone Group Control Port**: The KONE control panel’s port number.

  When the door phone is NOT used as the central machine, configure the following options.

  - **KONE Central IP**: The IP address of another door phone that is used as the central machine.
  - **KONE Central Port**: The port number of another door phone that is used as the central machine.
  - **Username**: The username of the HTTP API authentication set in the central machine.
  - **Password**: The password of the HTTP API authentication set in the central machine.
- **Time Out**: Available for Traditional DCS, Conventional, and Hybrid DCS. It is 5000ms by default; define the time for users to press the lift button.

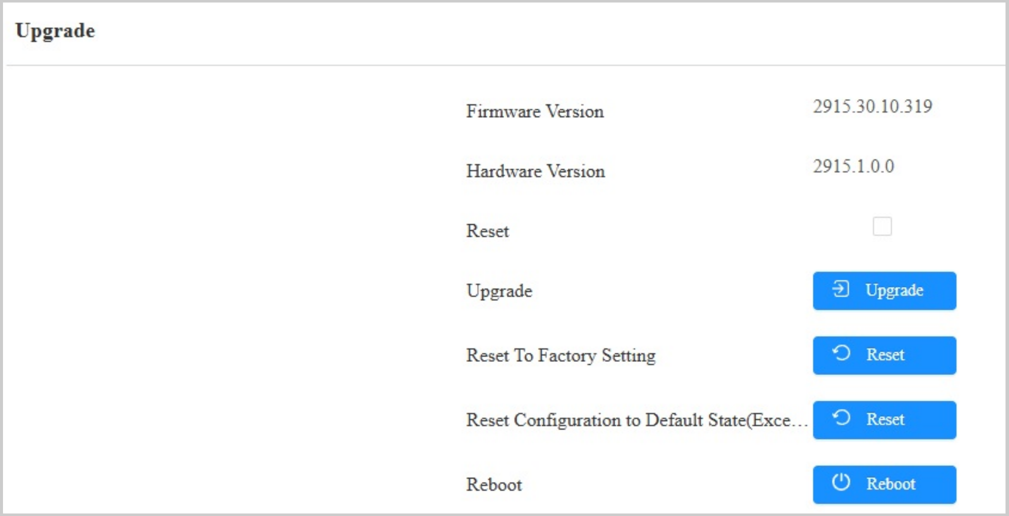
After choosing the KONE Control Mode, you need to fill in specific options. Please confirm them with the KONE service provider.

Kone Lift Dop	Kone Lift Cop	Lift Turnstile
DOP ID	COP Elevator ID	Device Terminal ID
DOP Floor ID	COP Group ID	Device Floor ID
DOP ID2	COP Elevator ID2	Device Door
DOP Floor ID2	COP Group ID2	Device Terminal ID2
		Device Floor ID2
		Device Floor ID2

- **KONE Mask Type**: Available when the **Central Machine** is checked. Upload the default or specific mask file. To obtain the configuration file, please contact the Akuvox tech team.

Firmware Upgrade

Upgrade the firmware on the **System > Upgrade > Basic** interface. If you want to reset the device after the upgrade, check the Reset box.



Upgrade

Firmware Version	2915.30.10.319
Hardware Version	2915.1.0.0
Reset	□
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reset Configuration to Default State(Exce…	Reset
Reboot	Reboot

Note

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

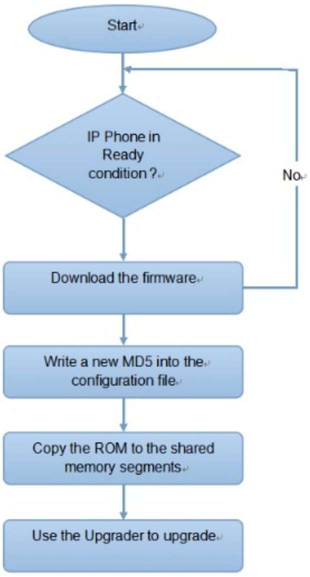
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:


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

Configuration Files for Auto-provisioning

Configuration files 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

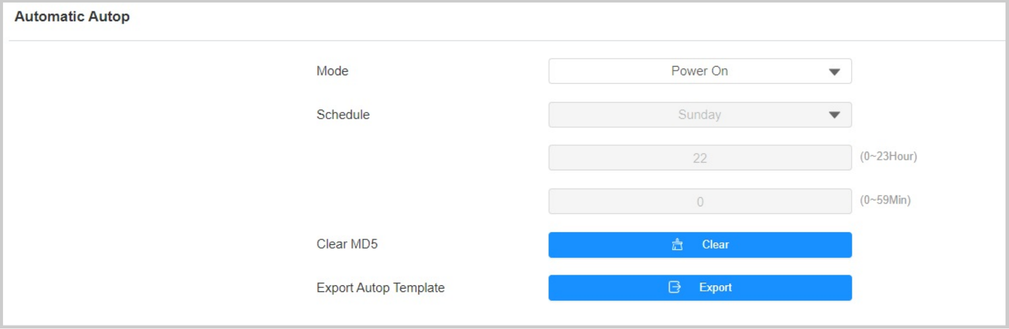
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5

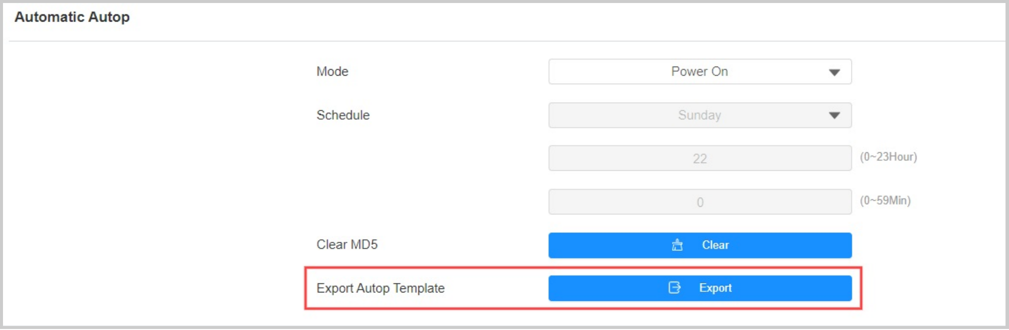
Export Autop Template

- **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.



Automatic Autop

Mode: Power On

Schedule: Sunday

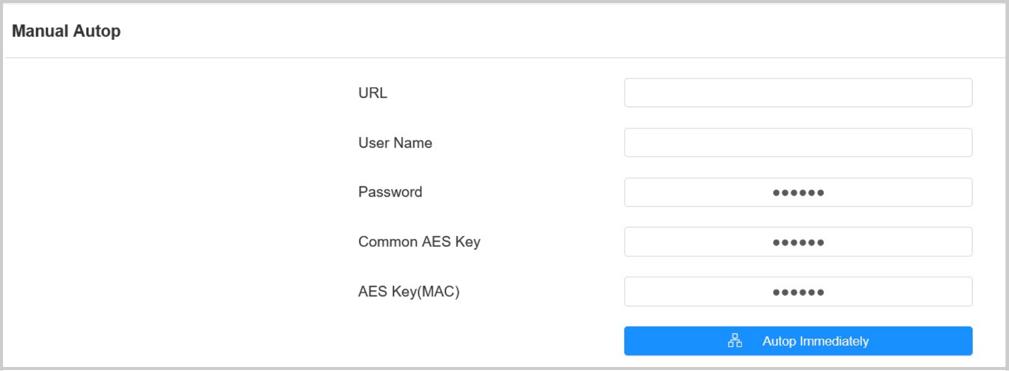
22 (0~23Hour)

0 (0~59Min)

Clear MD5

Export Autop Template

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



Manual Autop

URL:

User Name:

Password: ••••••

Common AES Key: ••••••

AES Key(MAC): ••••••

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

Note

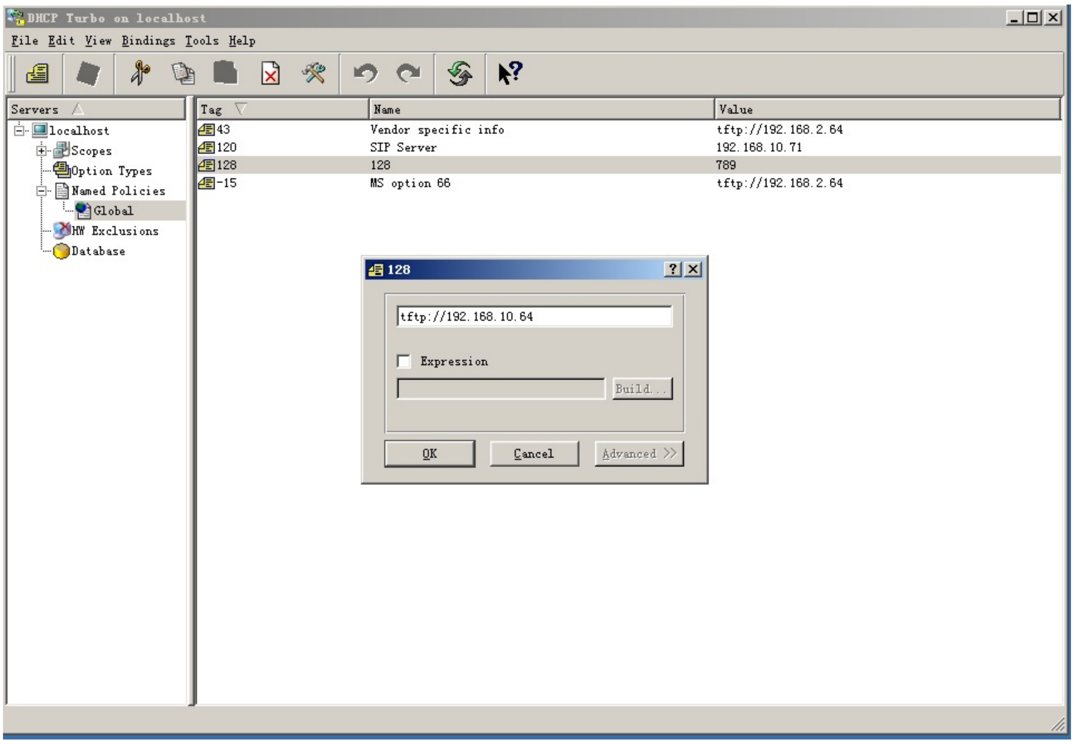
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning

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



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

128

tftp://192.168.10.64

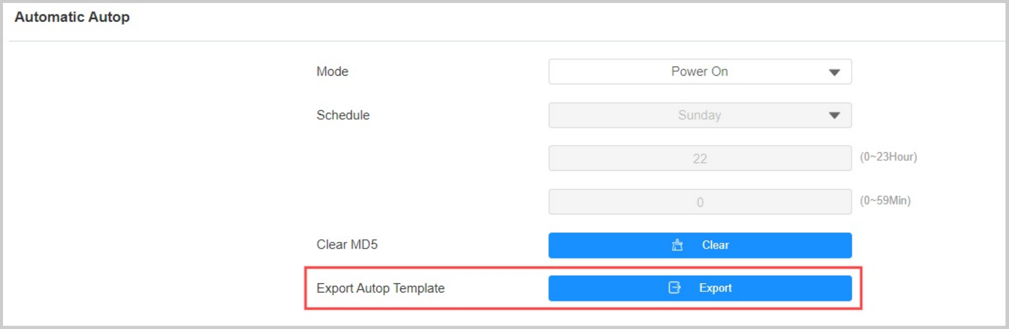
□ Expression

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.

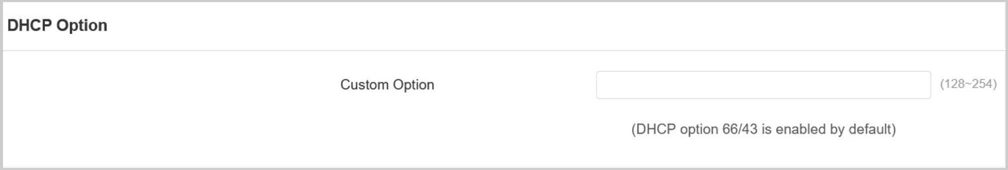
Download the Autop template on the **System > Auto Provisioning > Automatic Autop.**



Automatic Autop

Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

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



DHCP Option

Custom Option (128~254)

(DHCP option 66/43 is enabled by default)

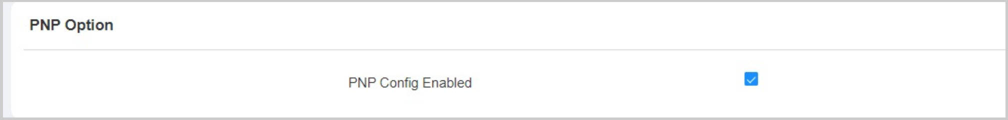
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL. 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.



PNP Option

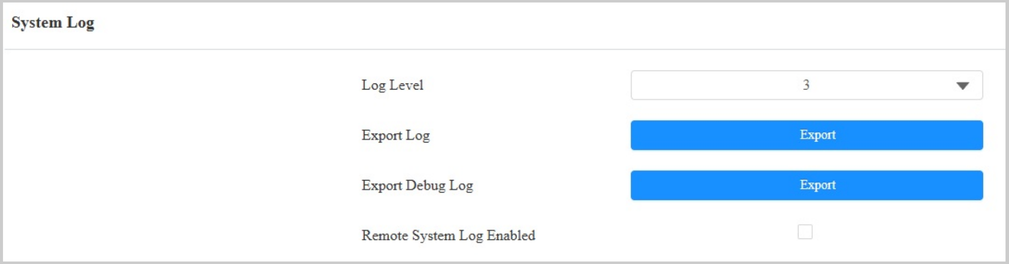
PNP Config Enabled ☑

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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



System Log

Log Level: 3

Export Log: Export

Export Debug Log: Export

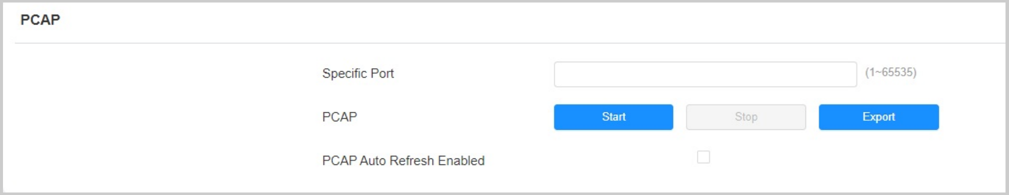
Remote System Log Enabled: □

- **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.
- **Export Debug Log**: Click the **Export** tab to export the 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.



PCAP

Specific Port: (1~65535)

PCAP: Start Stop Export

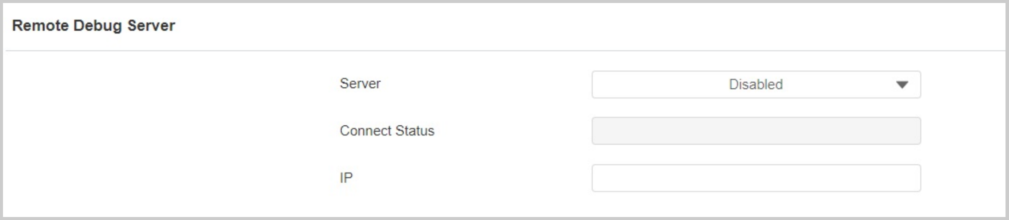
PCAP Auto Refresh Enabled: □

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

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.



Remote Debug Server

Server: Disabled

Connect Status:

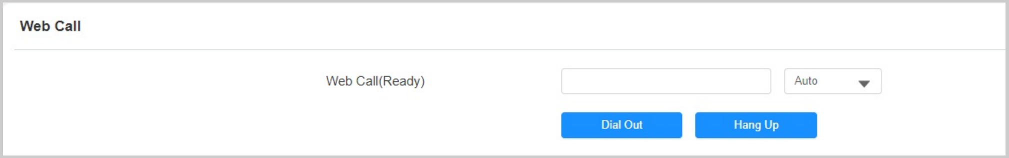
IP:

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

Web Call

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

Make a web call on the **System > Maintenance > Web Call** interface. Select the registered SIP account to make the web call.



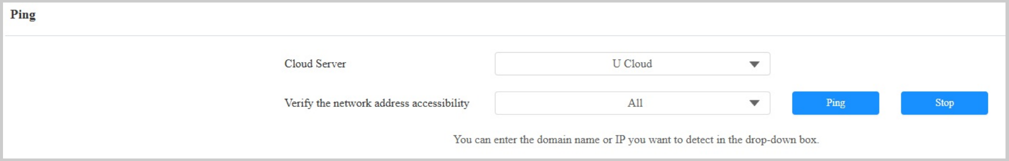
Web Call

Web Call(Ready)

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.



Ping

Cloud Server: U Cloud

Verify the network address accessibility: All

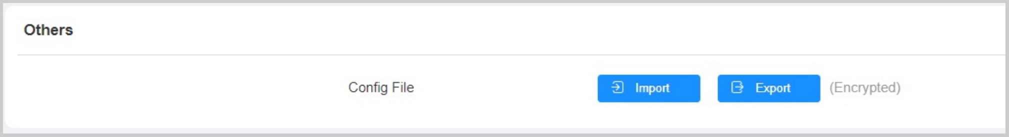
You can enter the domain name or IP you want to detect in the drop-down box.

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

Backup

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

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

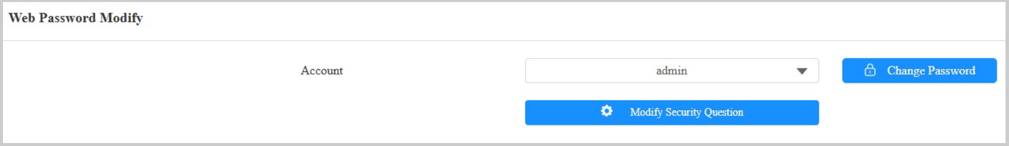


Password Modification

Modify Device Web Interface Password

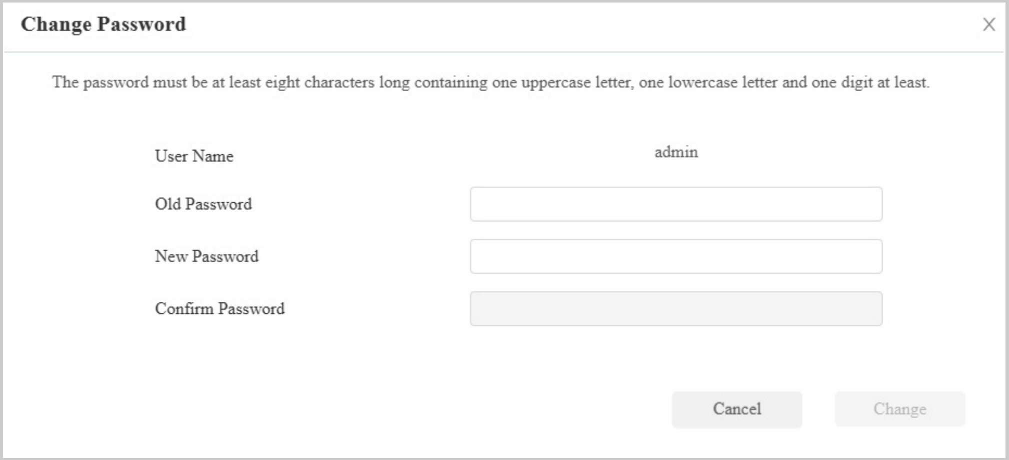
Change the web password on the web **System > Security > Web Password Modify** interface.

Select **Admin** for the administrator account and **User** for the user account. Click the **Change Password** tab to change the password.



Web Password Modify

Account: admin



Change Password

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

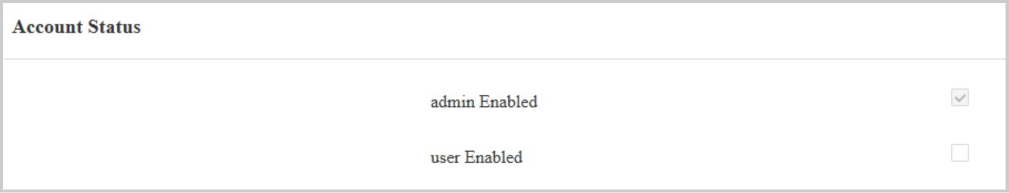
User Name: admin

Old Password:

New Password:

Confirm Password:

You can enable/disable the user account on the Account Status section. The default password for the user account is **user**.



Account Status

admin Enabled ☑

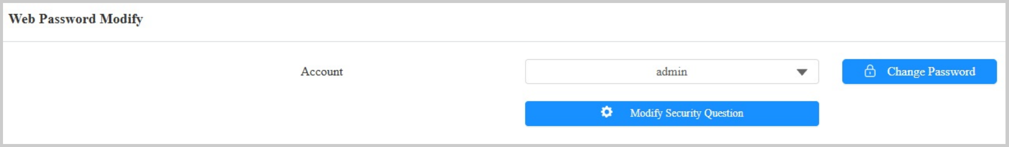
user Enabled □

Modify Security Questions

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

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

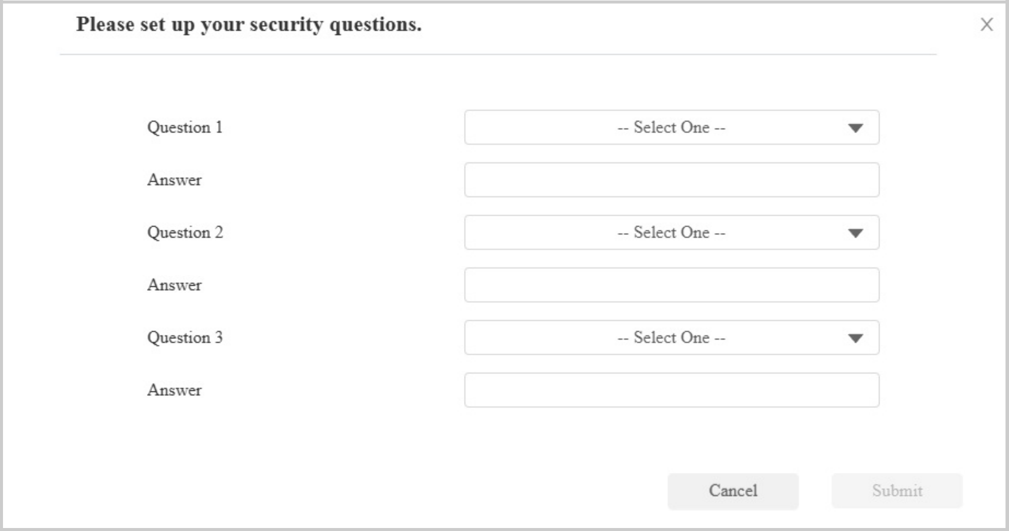
Set it up on the **System > Security** interface. Click **Modify Security Question**.



Web Password Modify

Account: admin

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



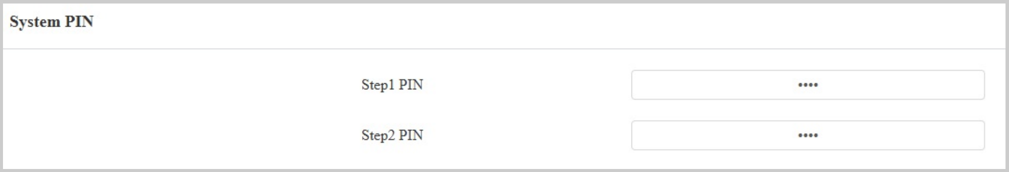
Please set up your security questions.

Question 1	-- Select One --
Answer	
Question 2	-- Select One --
Answer	
Question 3	-- Select One --
Answer	

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.

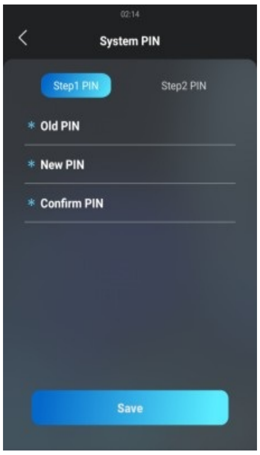


System PIN

Step1 PIN	••••
Step2 PIN	••••

- **Step1 PIN**: Set a 4-digit password. The default is 9999.
- **Step2 PIN**: Set a 4-digit password. The default is 3888.

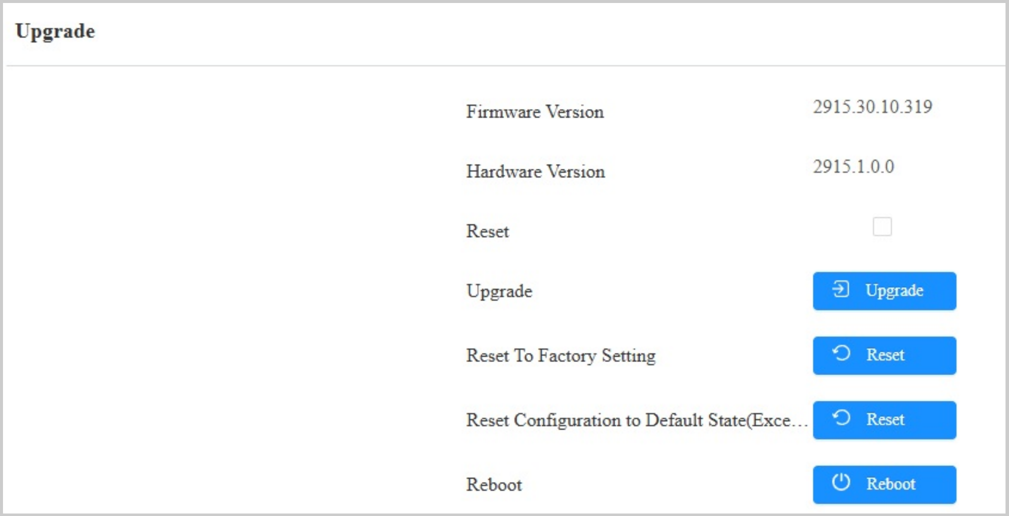
You can also set them up on the **Setting > Security > System PIN** screen.



System Reboot&Reset

Reboot

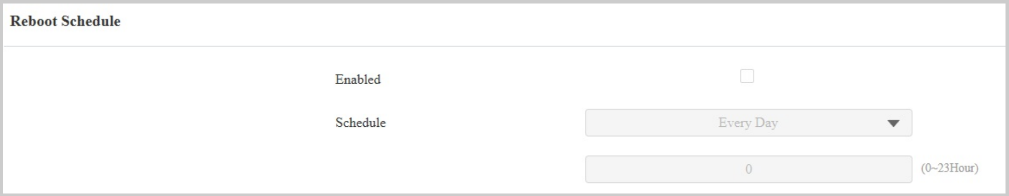
Reboot the device on the **System > Upgrade** interface.



Upgrade

Firmware Version	2915.30.10.319
Hardware Version	2915.1.0.0
Reset	□
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reset Configuration to Default State(Exce…	Reset
Reboot	Reboot

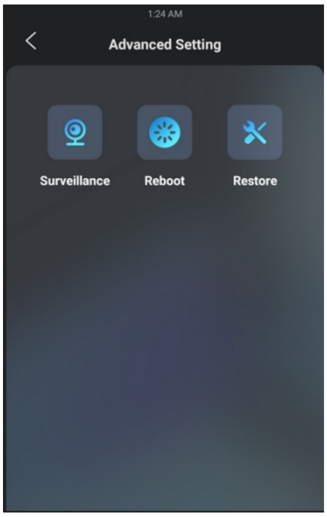
You can set up the reboot schedule on the **System > Auto Provisioning > Reboot Schedule** interface.



Reboot Schedule

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

You can also reboot the device on the **Setting > Advanced Setting > Reboot** screen.

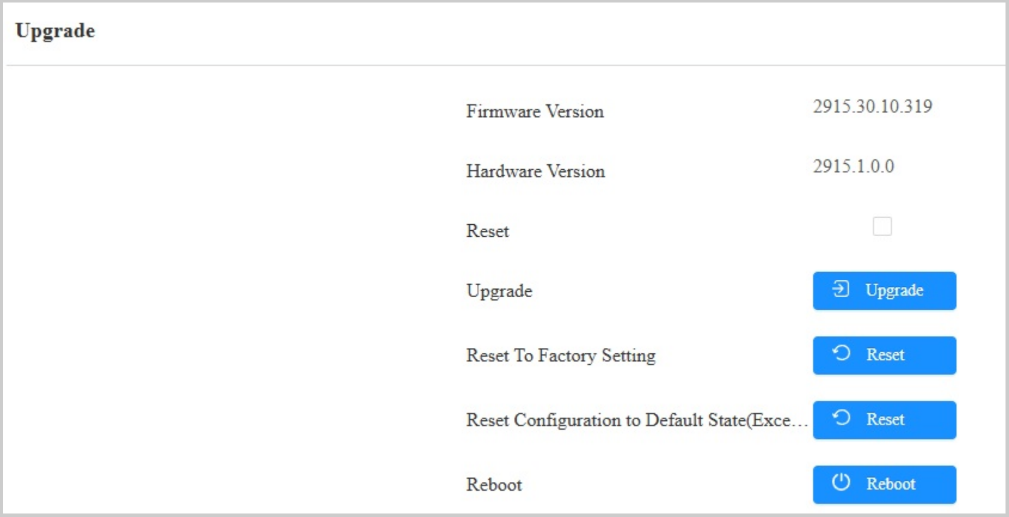


Reset

The device provides two reset options:

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

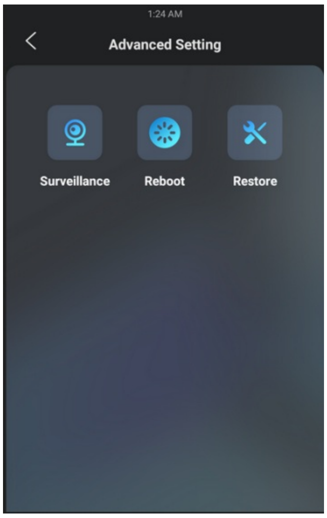
Reset the device on the **System > Upgrade** interface.



Upgrade

Firmware Version	2915.30.10.319
Hardware Version	2915.1.0.0
Reset	□
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reset Configuration to Default State(Exce…	Reset
Reboot	Reboot

You can also reset the device on the **Setting > Advanced Setting > Restore** screen.



Tip

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

- Remove its back cover, insert a PIN into the hole and hold it for about 3 seconds.
- The backlight of the card reader area and fill light will light up, and the device goes into factory reset and reboot.