Akuvox

Table of contents

Akuvox S538 Door Phone Administrator Guide

About This Manual 11

Product Overview 13

Changelog 15

Model Specification 16

Access the Device 17

- Access the Device Settings 17
- Access the Device Web Settings 19

Search for Your Desired Settings 21

Introduction to Configuration Menu 22

Language and Time 24

- Language 24
  - On the Web 24
  - On the Device 25
- Time 26
  - On the Web 26
  - On the Device 27

Volume and Tone 29
Volume Configuration 29
On the Web 29
On the Device 30
Upload Tones 30
Visitor-friendly Mode 32
Open Door Tone Mode 32
LED and LCD 33
Infrared LED Setting 33
On the Web 33
On the Device 33
Card Reader LED Control 35
LCD Screen Brightness 35
On the Web 35
On the Device 37
LED White Light 39
Screen Display 41
Home Screen Display 41
Villa Theme 43
Building Theme 45

Office Theme 46
Multi-factor Authentication Theme 48
Speed Dial Setting in Building/Office/Multi-factor Authentication Theme 49
Speed Dial Action In Building/Office/Multi-factor Authentication Theme 50
Language Setting Of The Building/Multi-factor Authentication Theme 51
Alphanumeric Theme 51
Dial Key Order 53
Text Prompt Display 54
Screensaver Settings 54
On the Web 54
On the Device 55
Upload Screensaver 56
Upload Device Booting Image 57
Upload Device Directory List Background Image 58
Upload Background of Dial Tips 59
Open Door Text Prompt 59
Appearance 60
Network Setting 62
Device Network Configuration 62
Device Local RTP Configuration 64

Device Deployment in Network 65
NAT Setting 66
Web HTTP Setting 67
Intercom Call Configuration 68
IP Call Configuration 68
IP Call Setup 68
Make IP Calls 68
SIP Call Configuration 69
SIP Account Registration 70
SIP Server Configuration 71
SIP Call DND & Return Code Configuration 72
Outbound Proxy Server 73
Data Transmission Type 74
SIP Hacking Protection 74
Voice Message 75
Call Settings 76
Quick Dial By Number Replacement 76
Call Auto-answer Configuration 77
Sequence Call 78
Group Call 79

Maximum Call Duration 80
Maximum Dial Duration 80
Hang Up After Open Door 81
Two-way Video Call 81
Audio and Video Codec Configuration 83
Audio Codec 83
Video Codec 84
Video Codec for IP Direct Calls 84
Contacts Configuration 86
Manage Contact Groups 86
Set up Contact Details 86
Contact List Display 87
Relay Setting 90
Local Relay 90
Web Relay 91
Security Relay 94
Upgrade SR01 96
Access Control Schedule Management 98
Create a Door Access Schedule 98
Import and Export Door Access Schedule 99

Relay Schedule 100
Holiday Schedule 101
Door-opening Configuration 103
Unlock By Public PIN 103
Virtual PIN 104
User-specific Access Methods 105
Unlock by Private PIN Code 106
Unlock by RF Card/Bkey 106
Unlock by License Plate 108
Unlock by Facial Recognition 108
Access Setting 110
Import/Export User Data 112
Access Authentication 112
Unlock by Bluetooth 114
Unlock by HTTP Command 116
Unlock by DTMF Code 117
DTMF Data Transmission 117
DTMF Whitelist 119
Unlock by QR Code 120
Unlock by Exit Button 120

Mifare Card Encryption 122
Contactless Smart Card 123
CEPAS Card Reading 124
Monitor and Image 125
MJPEG Image Capturing 125
MJPEG Authorization 126
RTSP Stream Monitoring 127
RTSP Basic Setting 128
RTSP Stream Setting 128
RTSP OSD Setting 130
ONVIF 130
Live Stream 131
Data Transmission Type for Third-party Camera 132
Security 133
Tamper Alarm 133
Disarm Setting 134
Lock Security 135
Motion Detection 138
Motion Detection Triggered Actions 140
Security Notification 141

Email Notification 141
FTP Notification 142
TFTP Notification 142
SIP Call Notification 143
Action URL 143
Voice Encryption 146
User Agent 147
Web Interface Automatic Log-out 147
Client Certificate Setting 147
Web Server Certificate 148
Client Certificate 148
High Security Mode 149
Emergency Action 150
Real-time Monitoring 151
Gesture Control Setting 151
Logs 154
Call Logs 154
Door Logs 154
Event Logs 156
Integration with Third-party Devices 157

Integration via Wiegand 157
Facility Code Setting 159
Wiegand Virtual Door Mode 160
Integration via HTTP API 161
Integration via RS485 163
Power Output Control 164
Mobile Community 165
Integration with Control4 166
Lift Control 167
Akuvox Lift Controller 167
KONE Lift Controller 169
Mitsubishi Lift Controller 172
Firmware Upgrade 176
Auto-provisioning via Configuration File 177
Provisioning Principle 177
Configuration Files for Auto-provisioning 178
AutoP Schedule 179
Static Provisioning 180
DHCP Provisioning 182
PNP Configuration 184

Debug 186
System Log for Debugging 186
PCAP for Debugging 186
Remote Debug Server 187
Web Call 188
Ping 188
Network Probe 188
Backup 190
Password Modification 191
Modify Device Web Interface Password 191
Modify Security Questions 192
Modify System Password 193
System Reboot&Reset 194
Reboot 194
Reset 195

Akuvox

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX S538 DOOR PHONE

Administrator Guide

Akuvox

Thank you for choosing the Akuvox S538 door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to version 538.30.10.720, and it provides all the configurations for the functions and features of the S538 door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



Akuvox S538 door phone is an Android-based SIP video door phone equipped with touch screens. They combine audio and video communication, access control, and video surveillance in a single device.

Powered by a finely optimized Android OS and cloud services, the S538 series supports flexible customization to better match user habits and project requirements.

The device offers rich hardware interfaces, including RS485 and Wiegand ports, enabling seamless integration with external systems such as elevator controllers and fire alarm systems. This helps build a comprehensive and centralized entrance control solution.

The device supports multiple access methods, including card, NFC, Bluetooth, QR code, and facial recognition, and can be integrated with body temperature measurement for enhanced safety scenarios.

The door phone is ideal for residential buildings, office buildings, and mixed-use complexes.

Changelog

What's new in version 538.30.10.720:

- Support for the Apple Wallet Unlock method.
- Support for integration with Akuvox IP cameras(VC50T/VC50B).
- Support for the Event Trigger Rule feature.
- Support for the Emergency Scenario feature.

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

Akuvox

Model Specification

Model	S538
Operation System	Android 12
Touch Screen	✓
Power Supply	PoE or DC24V / 2A power adapter
Power Output	Provide 12V / 0.5A output when powered by PoE+ or an external power supply.
Relay Port	3
Input Port	3
RS485	✓
Wiegand	✓
Light Sensor	✓
Motion Sensor	✓
Card Reader	13.56MHZ & 125KHZ
Wi-Fi	X
Bluetooth	✓
Face Recognition	✓
Reset Button	✓

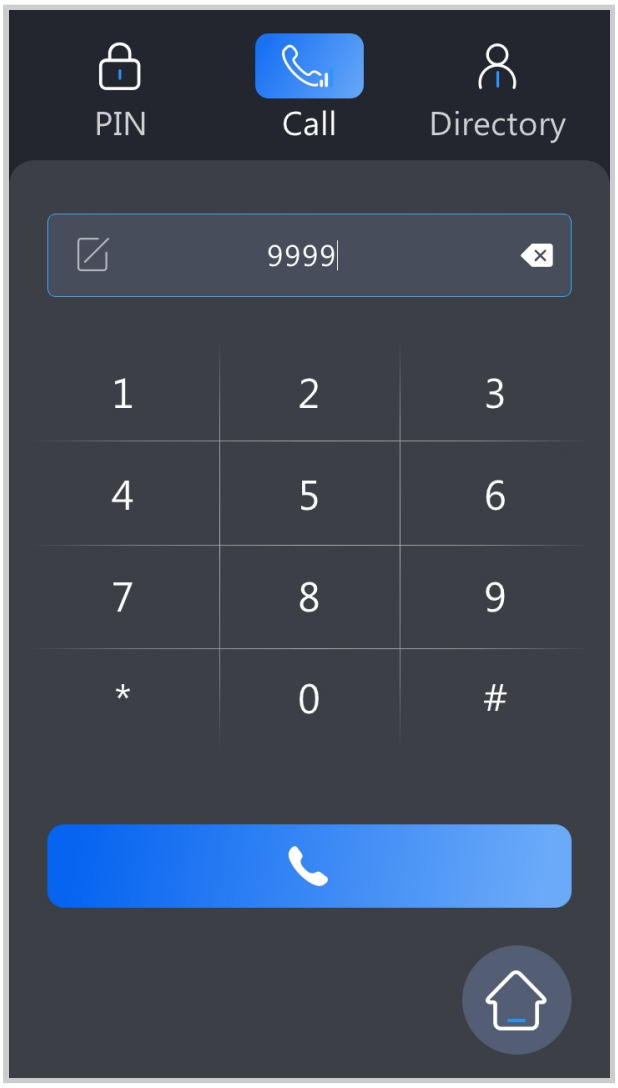
Access the Device

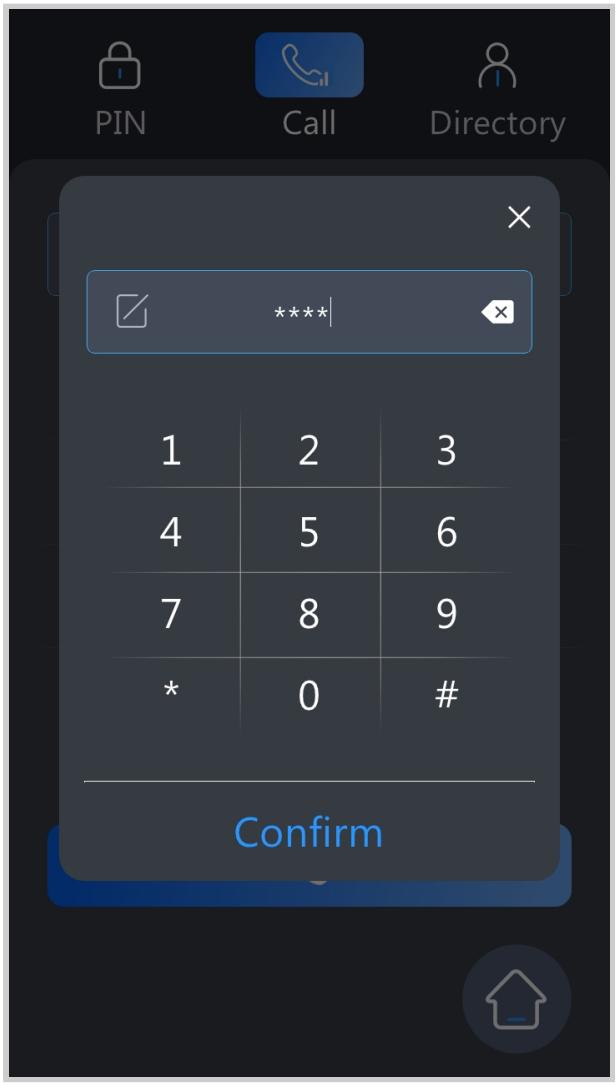
Door phones' system settings can be either accessed on the device or on its interface.

Access the Device Settings

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

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


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



Access the Device Web Settings

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

Check the device IP on the **Setting > System Info > Network** screen. Or, use the Akuvox IP Scanner tool to scan device IPs on the same local network.

Enter the IP in a browser to see the login page.



Note

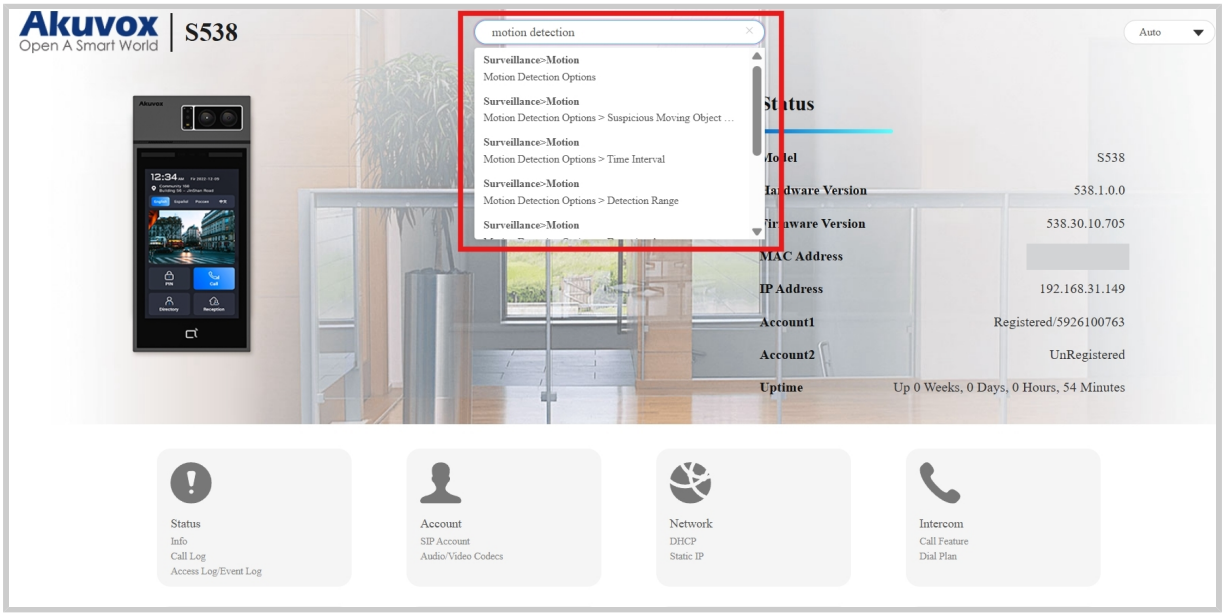
- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See the detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- The initial username and password are **admin,** and please be case-sensitive.
- Your computer should be on the same network as the device.

Search for Your Desired Settings

The device supports searching for features on its web portal.

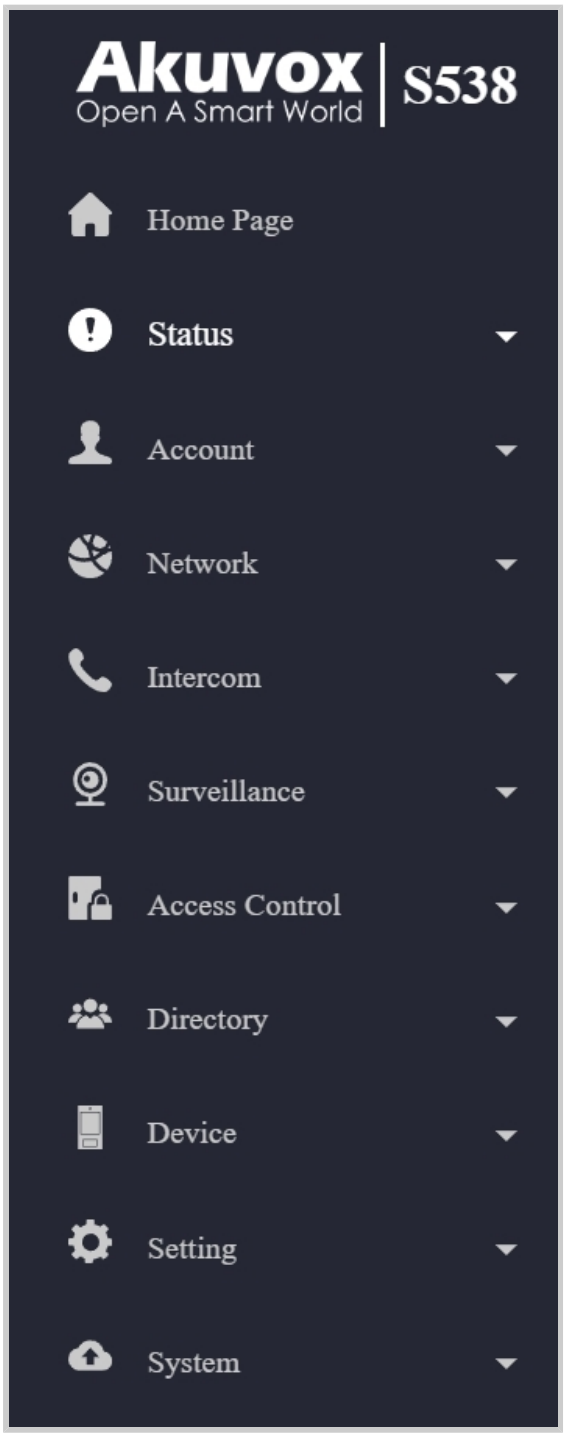
For example, if you want to search for motion detection, enter the value in the upper search box.

Then, select the desired option to redirect to the configuration interface.



Introduction to Configuration Menu

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


Akuvox
Open A Smart World
S538
Home Page
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System

Language and Time

Language

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

On the Web

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

The following languages are supported:

- English, Simplified Chinese, Spanish, Danish, Czech, French, Traditional Chinese, Turkish, Japanese, Ukrainian, Korean, Norwegian, Russian, Dutch, German, Polish, Arabic, and Italian.



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

The following languages are supported:

- English, Simplified Chinese, Traditional Chinese, Russian, Czech, Spanish, Turkish, Dutch, French, German, Korean, Danish, Polish, Italian, Japanese, Arabic, Norwegian, and Ukrainian.



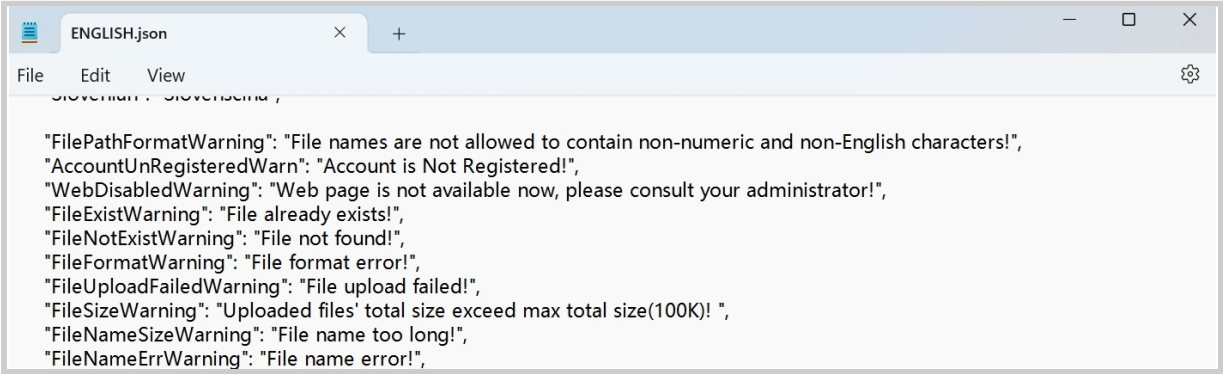
Custom Language

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

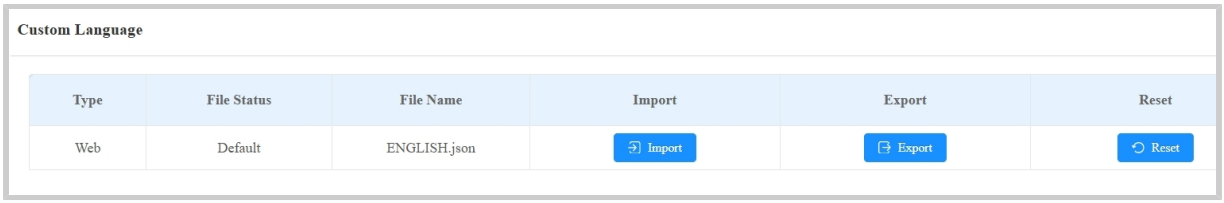
Export the .json file for editing. You may edit it with the notepad on your computer.

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

File Example:

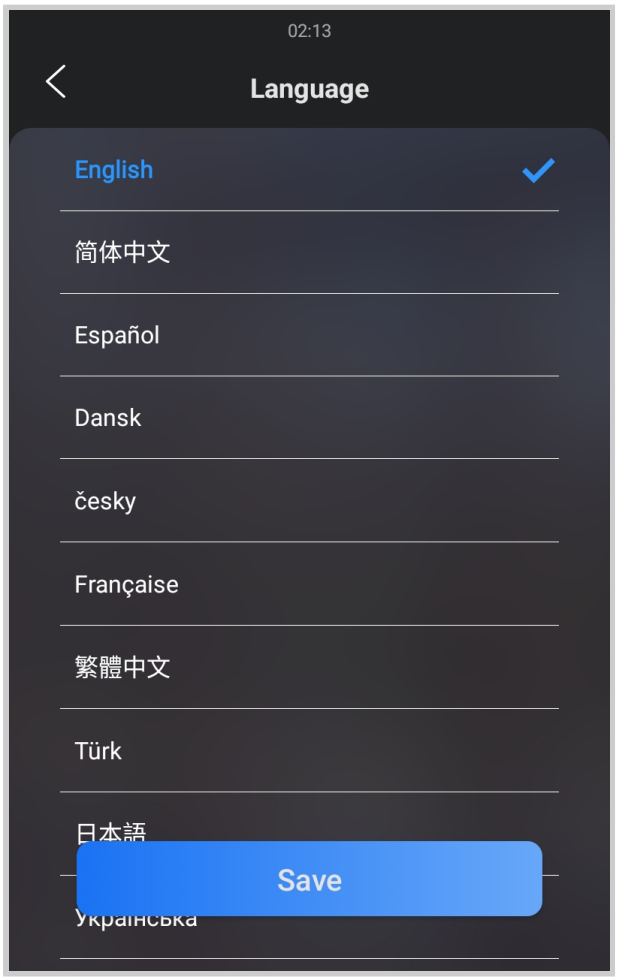


Set it up on the **Setting > Time/Lang > Custom Language** interface.



On the Device

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

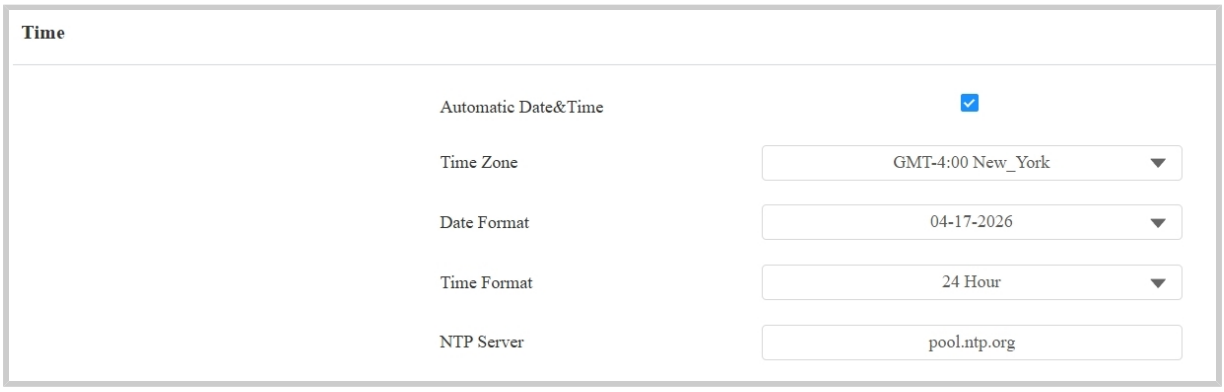


Time

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

On the Web

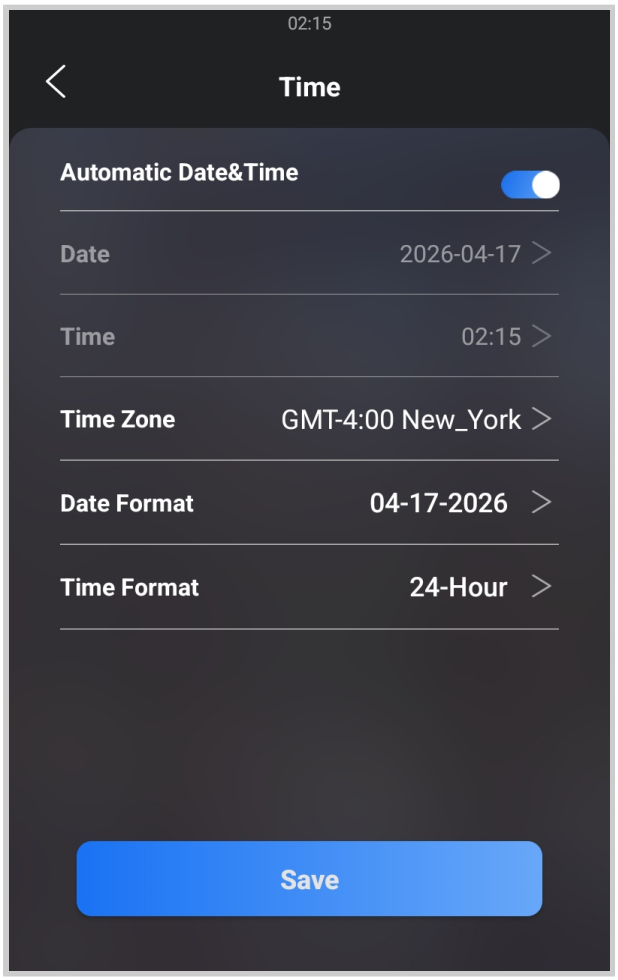
Set up time on the **Setting > Time/Lang > Time** interface.



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

On the Device

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


02:15
Time
Automatic Date&Time
Date
2026-04-17
Time
02:15
Time Zone
GMT-4:00 New_York
Date Format
04-17-2026
Time Format
24-Hour
Save

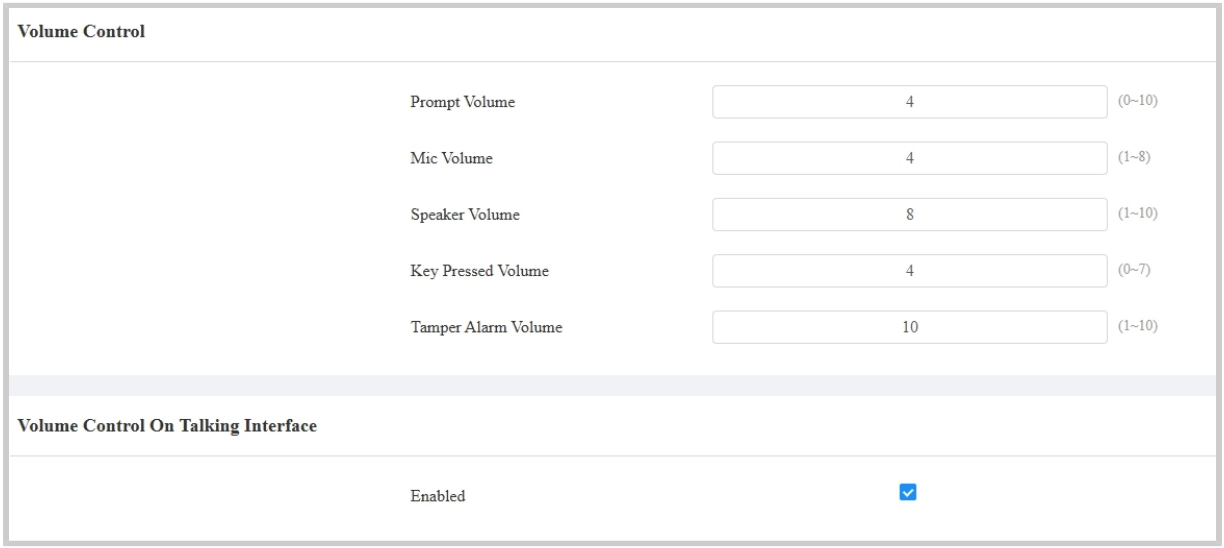
Volume and Tone

Volume Configuration

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

On the Web

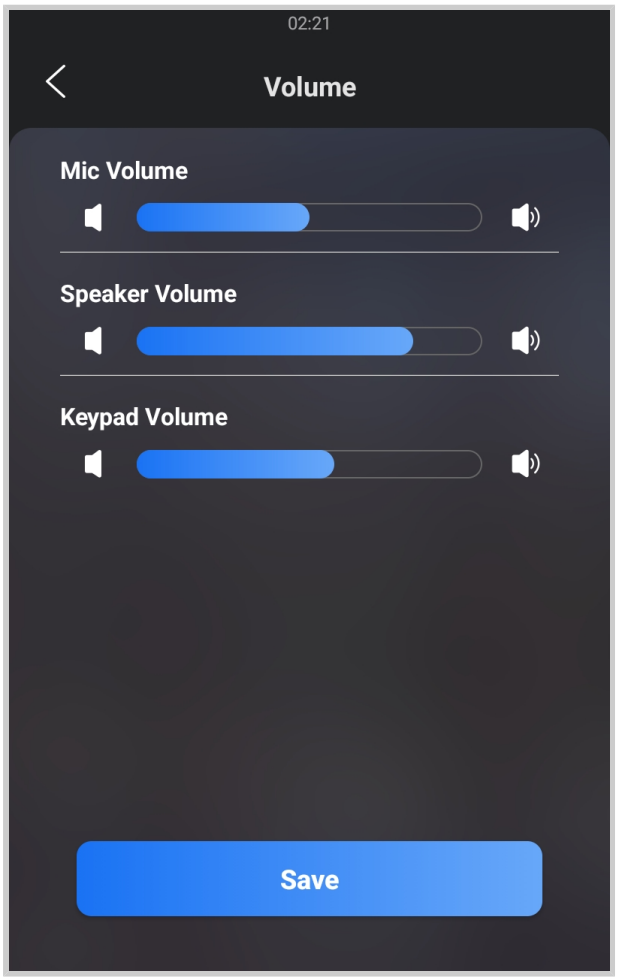
Set up volumes on the web **Device > Audio** interface.



- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 4.
- **Mic Volume**: The default is 4.
- **Speaker Volume**: The default is 8.
- **Key Pressed Volume**: The icon tapping sound. The default is 4.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 10.
- **Volume Control on Talking Interface**: When enabled, users can adjust the call volume during the call session.

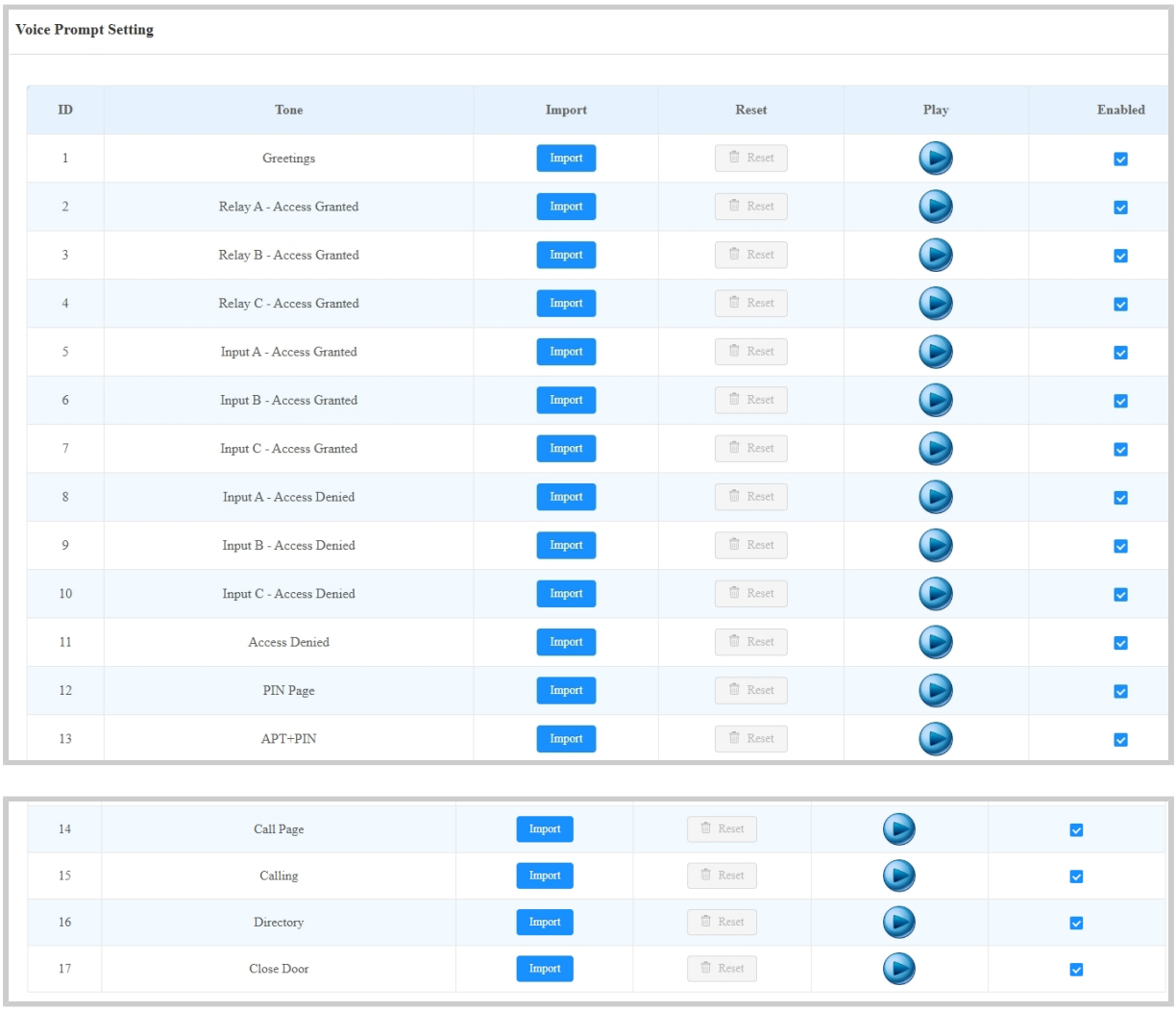
On the Device

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	Relay A - Access Granted	Import	Reset		
3	Relay B - Access Granted	Import	Reset		
4	Relay C - Access Granted	Import	Reset		
5	Input A - Access Granted	Import	Reset		
6	Input B - Access Granted	Import	Reset		
7	Input C - Access Granted	Import	Reset		
8	Input A - Access Denied	Import	Reset		
9	Input B - Access Denied	Import	Reset		
10	Input C - Access Denied	Import	Reset		
11	Access Denied	Import	Reset		
12	PIN Page	Import	Reset		
13	APT+PIN	Import	Reset		
14	Call Page	Import	Reset		
15	Calling	Import	Reset		
16	Directory	Import	Reset		
17	Close Door	Import	Reset		

- **Greetings**: The tone is played when the device is booted.
- **Access Granted**: The door-opening success tone.
- **Access Denied**: The door-opening failure tone.
- **PIN Page**: The tone is played when entering the PIN screen.
- **APT+PIN**: The tone is played when entering the Apartment number and PIN code for door access.
- **Call Page**: The tone is played when entering the Call screen.
- **Calling**: The tone is played when calling.
- **Directory**: The tone is played when entering the Directory screen.
- **Close Door**: The door-closing tone.

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

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.



- **Type**: When enabled, no prompts will be given when facial recognition/QR code scanning fails for door opening.

Open Door Tone Mode

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



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

LED and LCD

Infrared LED Setting

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

On the Web

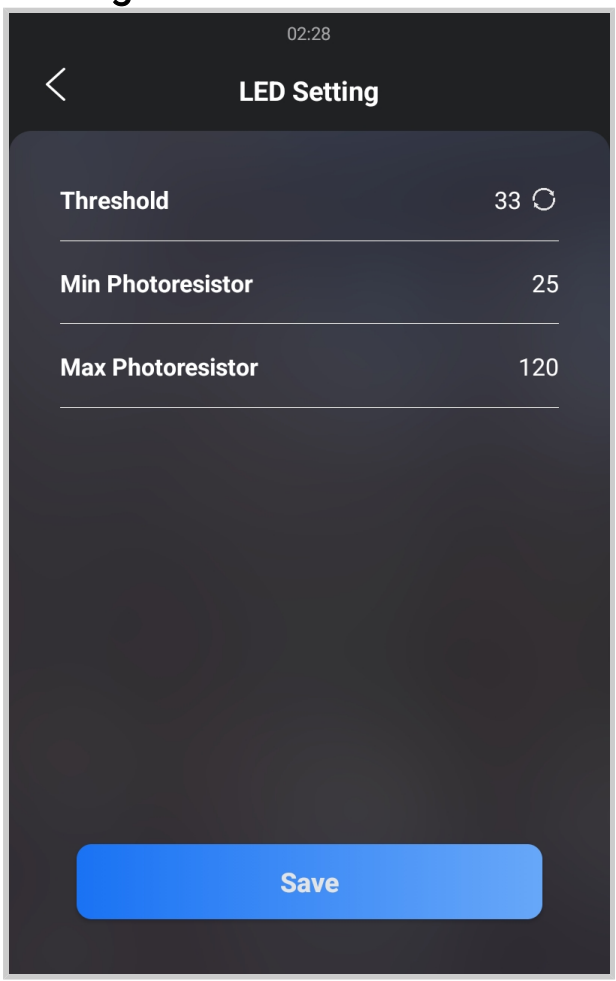
Set it up on the web **Device > Light > LED** interface.



- **Photoresistor Setting**: Set the minimum and maximum photoresistor values to automatically control the ON-OFF of the LED fill light. If the photoresistor value is less than the minimum threshold, turn off the fill light. If the photoresistor value is greater than the maximum threshold, turn on the fill light.

On the Device

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



- **Threshold**: The current light intensity indicated by the photo-resistor value. The higher the photo-resistor value is, the lower the light intensity. 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, and the value is the basis for configuring the minimum and maximum photo-resistor values.
- **Min/Max Photoresistor**: Set the minimum and maximum photoresistor values to automatically control the ON-OFF of the LED fill light. The default values are 25 and 120. If the photoresistor value is less than the minimum threshold, turn off the fill light. If the photoresistor value is greater than the maximum threshold, turn on the fill light.

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.



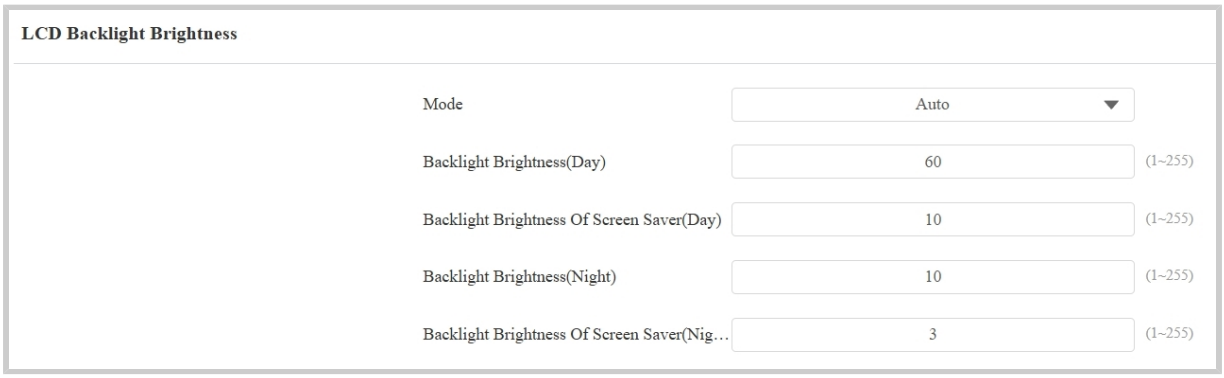
- **Start Time- End Time (H)**: Enter the time for the LED lighting to be valid, e.g., if the time is set from 8-0 (Start time- End time), it means the LED light will stay on during the time from 8:00 am to 12:00 pm for one day (24 hours).

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.



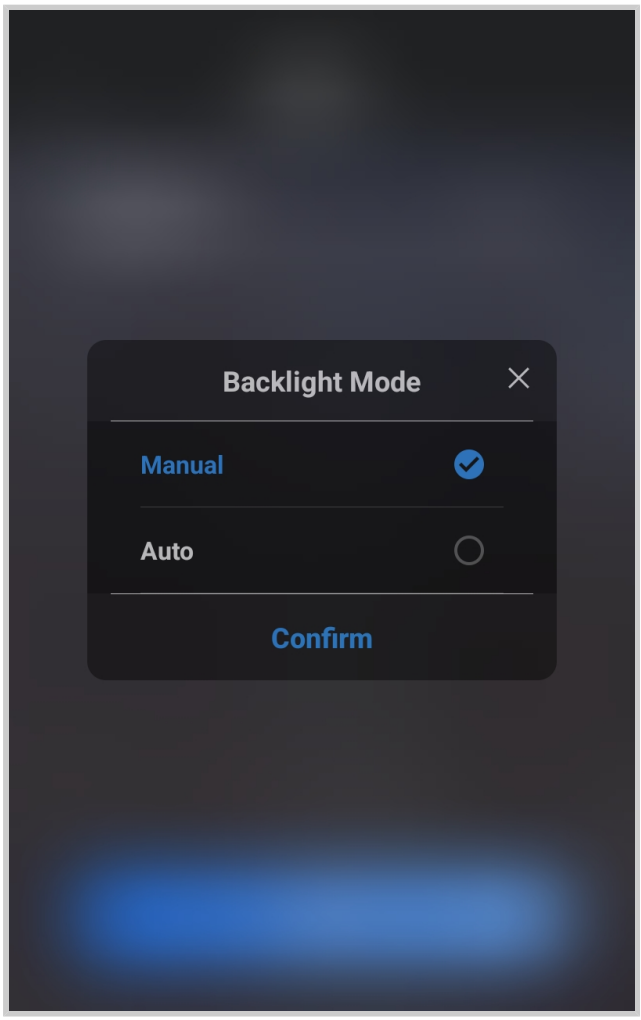
- **Mode**:
  - **Manual**: Set the backlight brightness value manually.
  - **Auto**: The screen backlight brightness will be adjusted automatically.

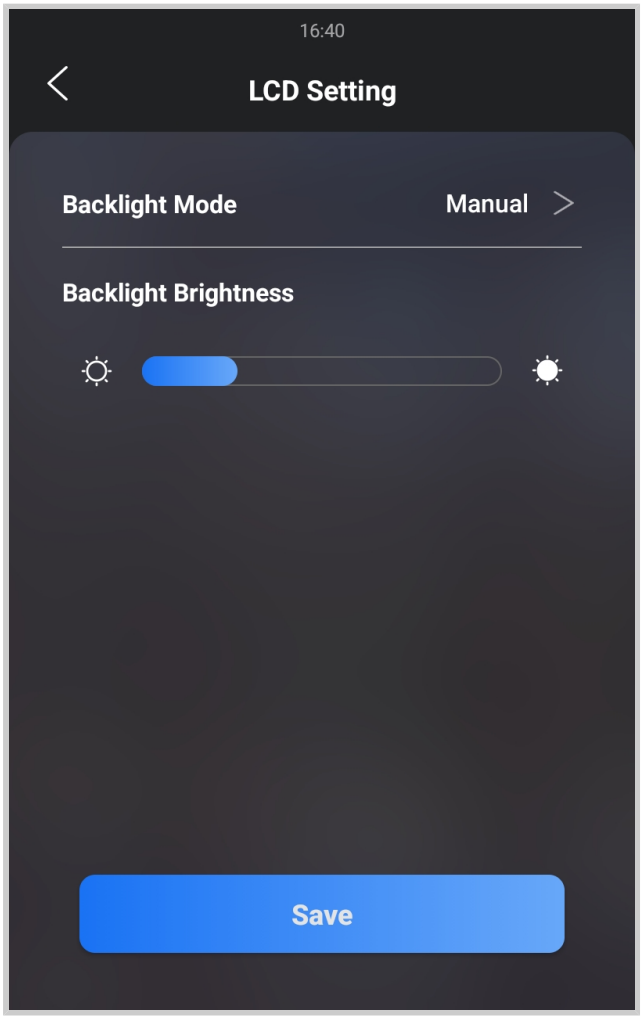
> **Note**
>
> The backlight brightness has two automatic modes, Day and Night. They are determined by the photoresistor.
>
> - If the current value is between the minimum and maximum photoresistor, the device is in Day mode.
> - If the current value is higher than the maximum photoresistor value, the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

- **Backlight Brightness (Day)**: Select the brightness value from 1-255. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screen Saver (Day)**: Adjust the backlight for the screensaver in the daytime with the value ranging from 1-255.
- **Backlight Brightness (Night)**: Select the brightness value from 1-255. The larger the value, the brighter the screen.
- **Backlight Brightness Of Screen Saver (Night)**: Adjust the backlight for the screensaver at night with the value ranging from 1-255.

On the Device

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


Backlight Mode
Manual
Auto
Confirm



LED White Light

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

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



- **Mode**: Select **Auto** or **OFF**. If you select **Auto**, the white light will turn on for 5 minutes for facial recognition and QR code scanning.
- **Limit Backlight Value**: Set the white light value from 1-255. The default is 50.
- **White Light PWM Value**: Set the white light PWM value from 0 to 100. PWM value affects the white light brightness that is set with the same white light value. For example, if the white light value remains the same, and you bring up the PWM value, you will get a brighter white light. In short, the higher the PMW value is, the brighter the light is.

Screen Display

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

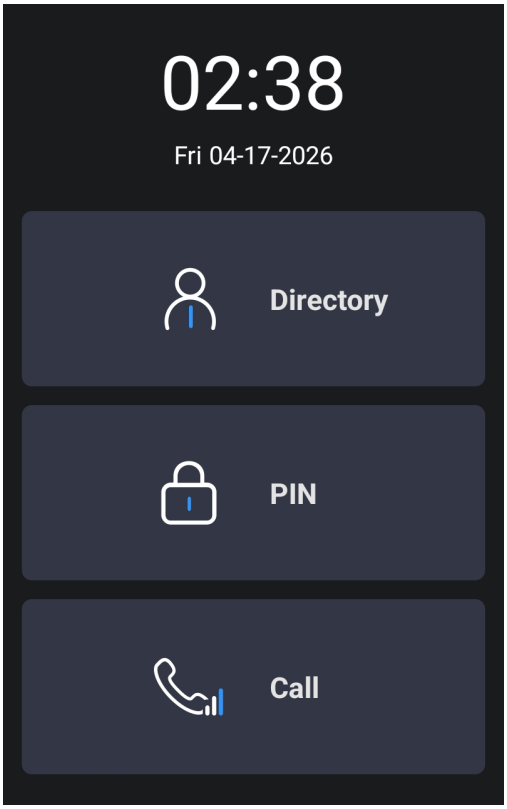
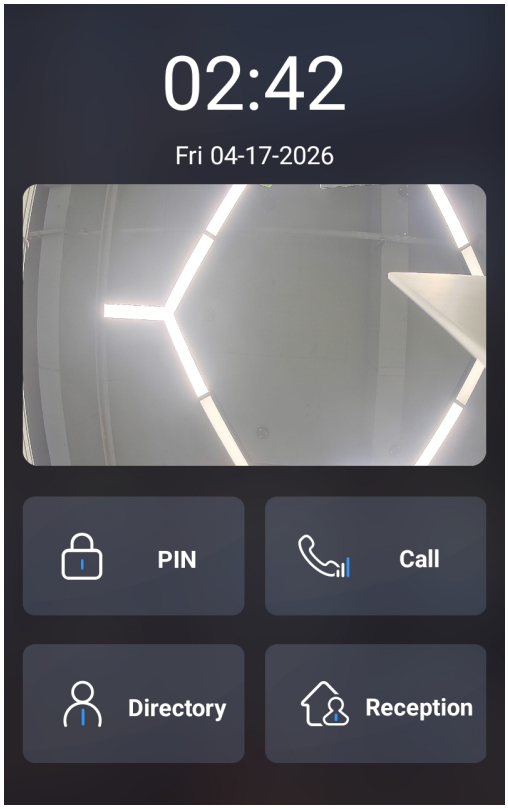
Home Screen Display

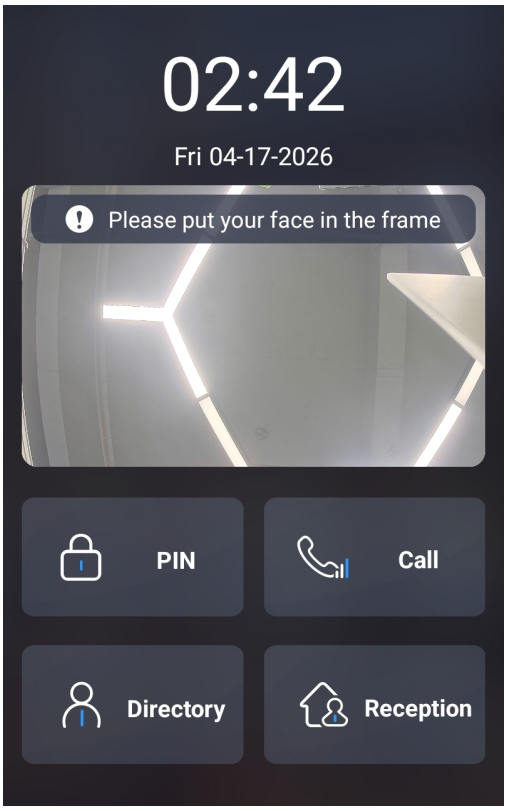
The device supports Villa, Building, Multi-factor Authentication, Office, and Alphanumeric themes. You can apply the desired theme to different scenarios.

> **Note**
>
> The Office theme is effective when the device is connected to the Smart Access Cloud.

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



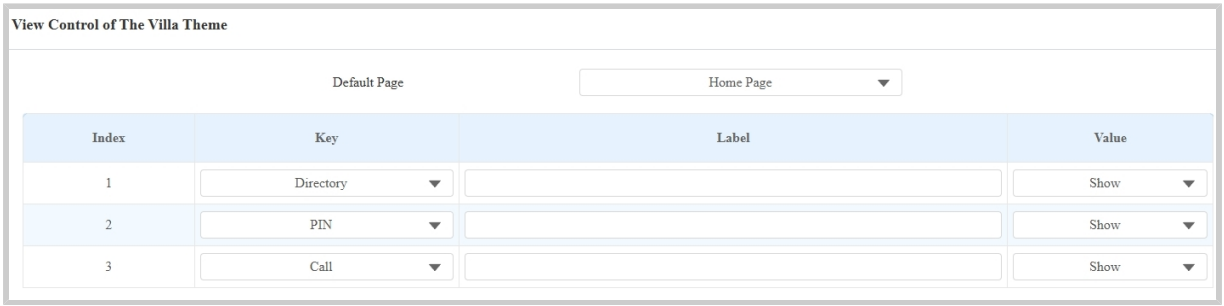
Villa	Building	Office
		
Multi-factor Authentication	Alphanumeric	

Villa	Building	Office
		

Villa Theme

You can configure the screen display for the layout of the Directory 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	Directory		Show
2	PIN		Show
3	Call		Show

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

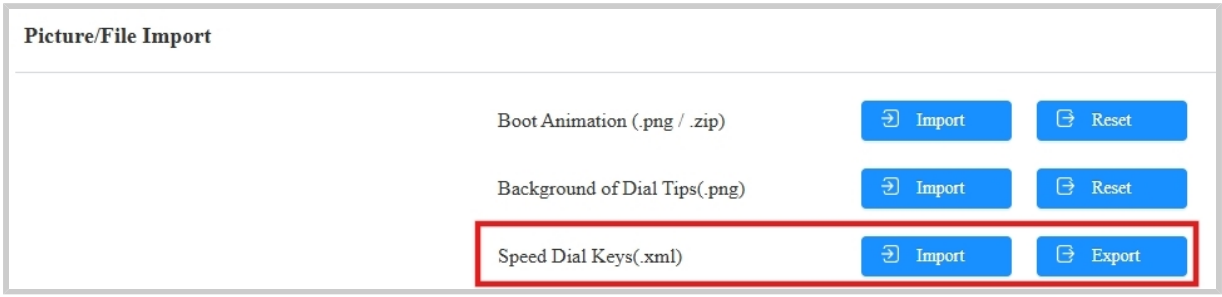


Options	Descriptions
Standard	Display time and keypad.
Auto	Display all speed dial buttons set by the users.
1 Key	Display a single contract without the keypad.
1 Key + Keypad	Display a single dial button with the keypad.

Options	Descriptions
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.

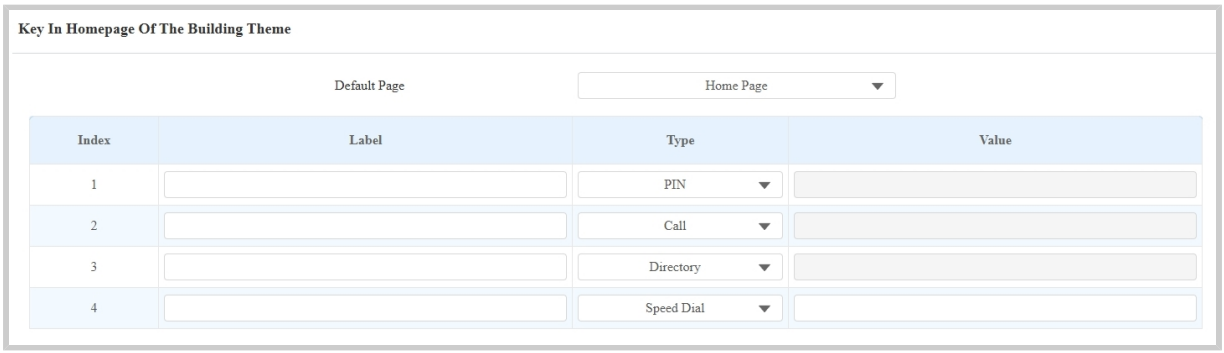
You can import and export speed dial numbers for quick setup.

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



Building Theme

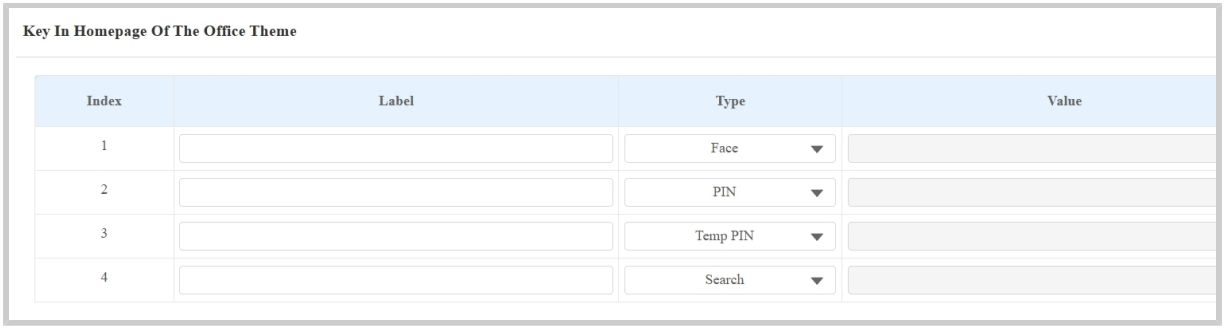
You can set up the key display in the Building theme on the **Setting > Key/Display > Key In Homepage Of The Building Theme** interface.



- **Default Page**: Select the homepage display type.
  - **Home Page**: The default displays PIN, Call, Directory, and Reception tabs and the facial recognition box.
  - **Call**: Display the Dial screen as the homepage.
  - **Directory**: Display the Contact screen as the homepage.
  - **PIN**: Display the PIN screen as the homepage.
- **Label**: Name the key. The name will not change the attribute of the key.
- **Type**: Select the key type.
- **Value**: It is available for those features that need to be set up with numbers, such as Speed Dial.

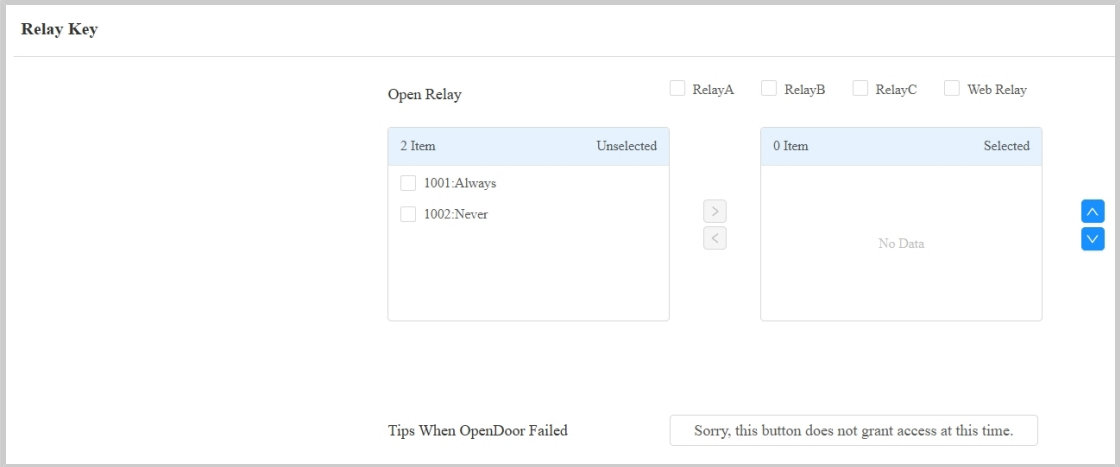
Office Theme

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



- **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.
  - The **Search** key allows for searching for groups and directories.
  - The **Face** key allows for displaying the facial recognition box.
  - When **Relay** is selected, you can specify which relay to open and apply a schedule within which the relay remains activated.



Time and Location Display in the Office Theme

You can set whether to display time and device location on the home screen.

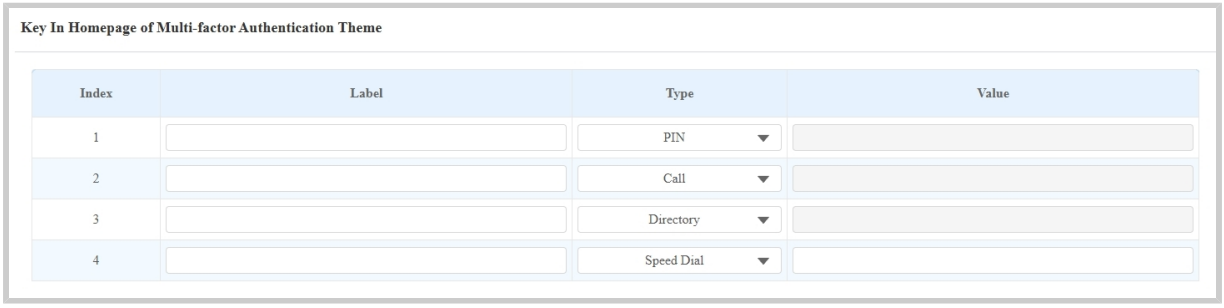
Set it up on the **Setting > Key/Display > Display of Home Page** interface.



- **Time Visible**: If disabled, time will not be displayed on the home screen.
- **Location Visible**: If disabled, the location will not be displayed on the home screen.

Multi-factor Authentication Theme

You can set up the key display in the Multi-factor Authentication theme on the **Setting > Key/Display > Key In Homepage of Multi-factor Authentication Theme** interface.

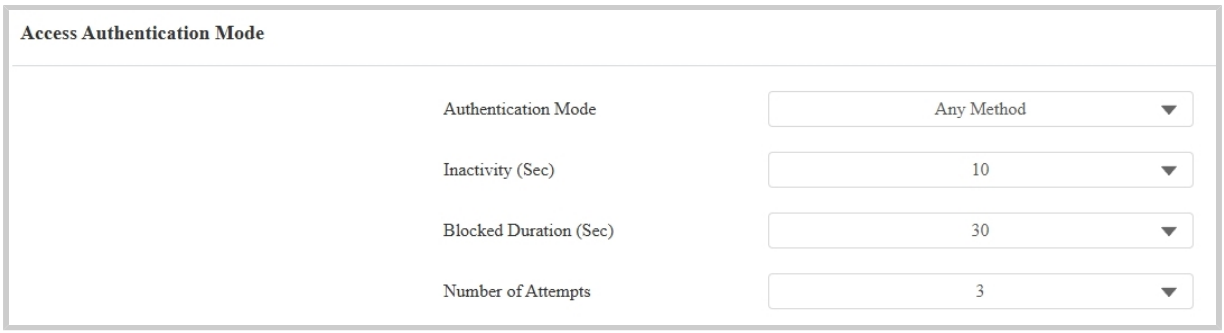


- **Label**: Name the key. The name will not change the attribute of the key.
- **Type**: Select the key type.
- **Value**: It is available for those features that need to be set up with numbers, such as Speed Dial.

Access Authentication Mode

The door phone allows dual authentication for door access, using a combination of any two methods: PIN, RF card, or facial recognition. When the mode is set up, users must open the door in the order of the chosen methods.

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



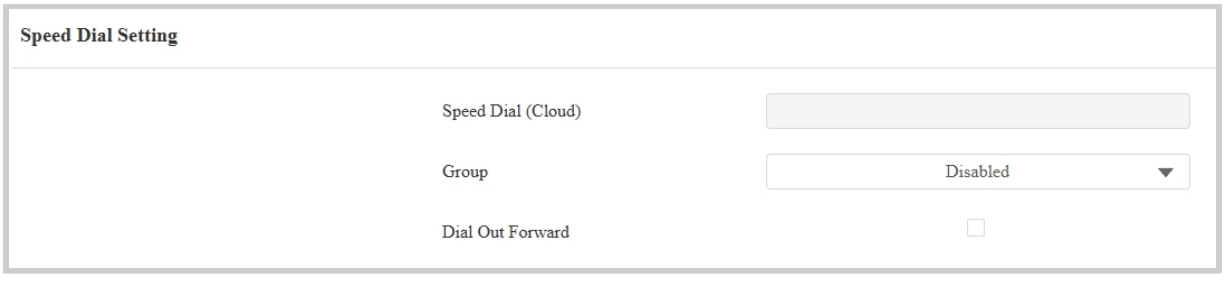
- **Authentication Mode**: Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.

  - **Any Method**: Allows all access methods.
  - **Face + PIN**: Scan the face first, then enter the PIN code.
  - **Face + 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 within 10 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.

Speed Dial Setting in Building/Office/Multi-factor Authentication Theme

The Speed Dial feature allows users to make speedy calls by pressing a specific tab without entering any numbers.

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



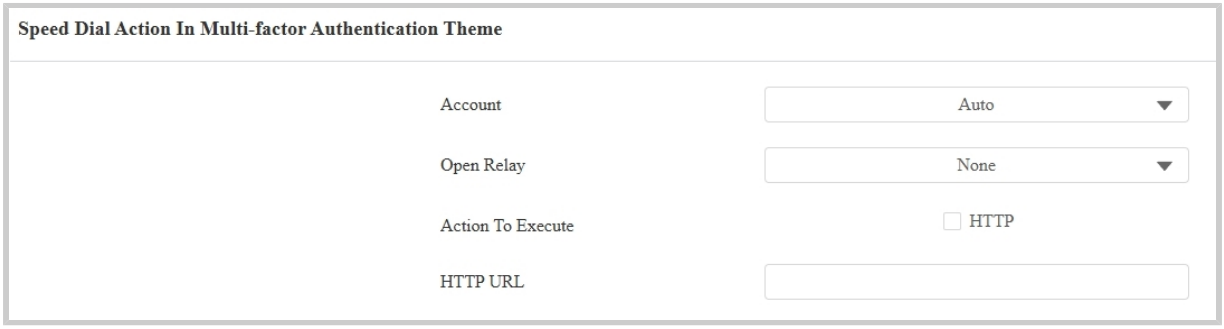
- **Group**:
  - **Disabled**:

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

Speed Dial Action In Building/Office/Multi-factor Authentication Theme

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

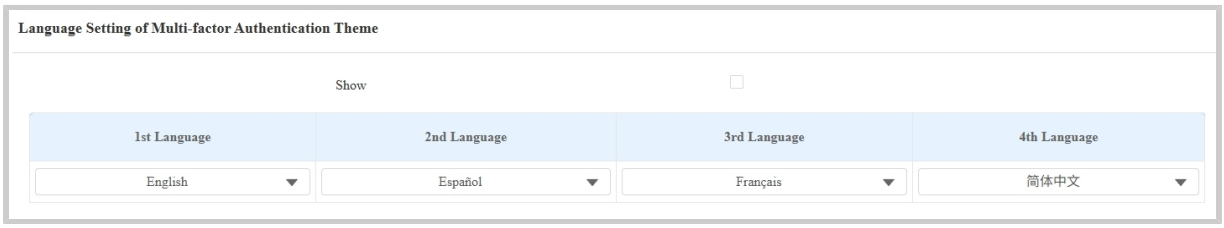
Set it up on the **Setting > Key/Display > Speed Dial Action In Multi-factor Authentication Theme** interface.



- **Account**: Select the account to make the call. It applies to the registered account. If both accounts are registered, Account1 is used when **Auto** 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/Multi-factor Authentication Theme

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

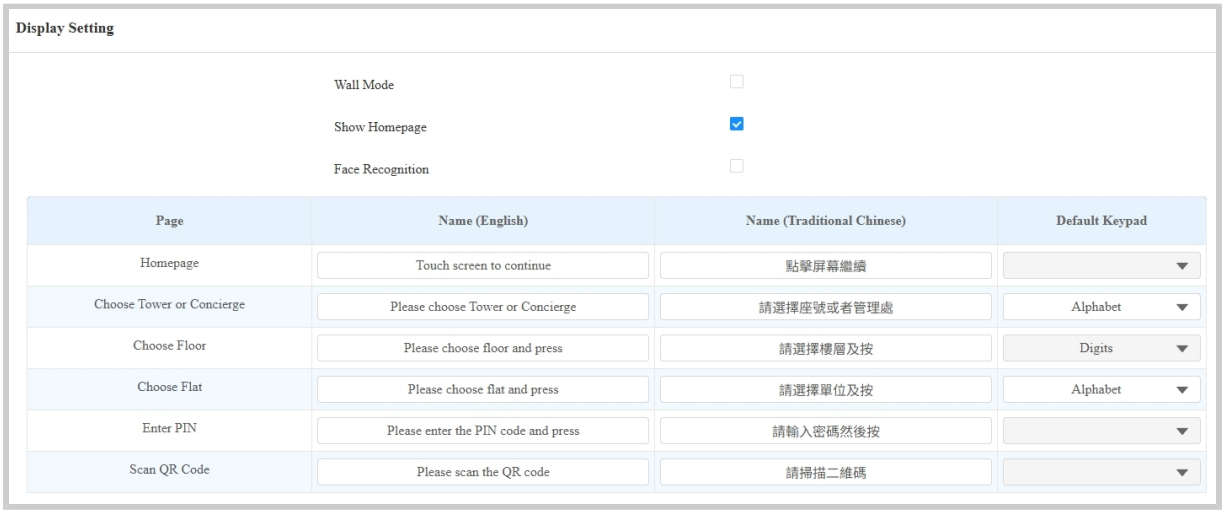


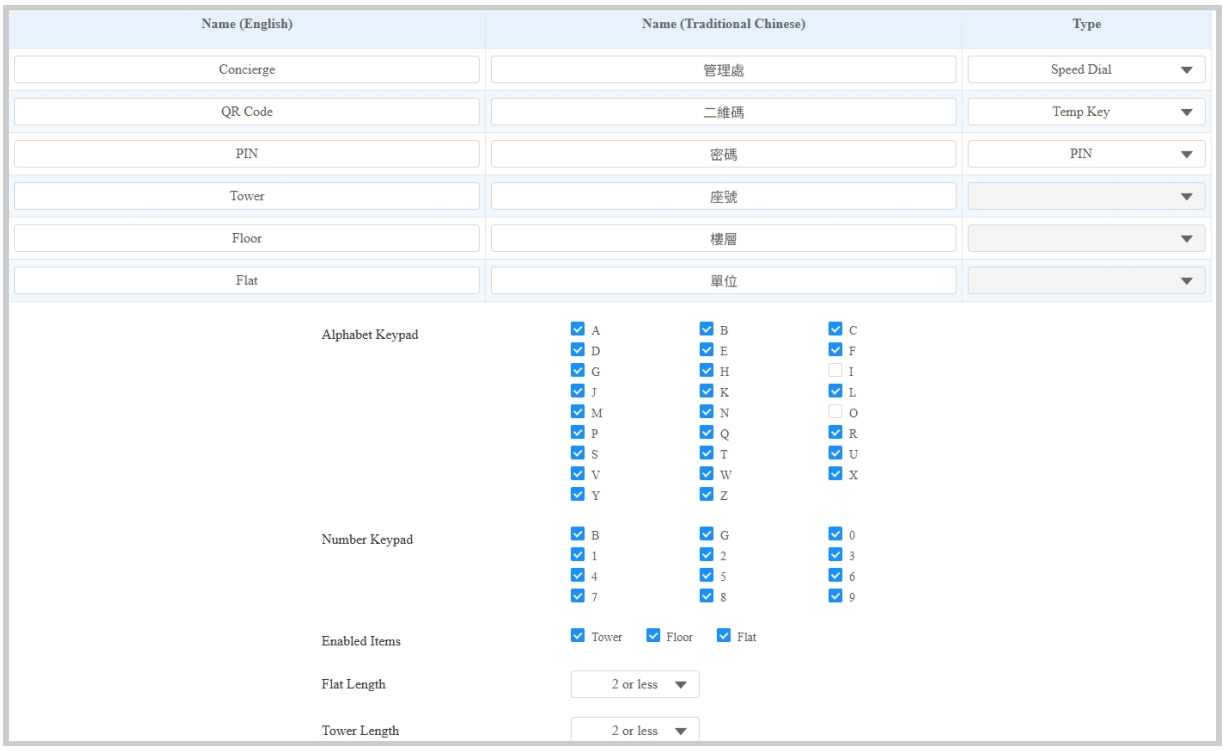
- **Show**: When disabled, the language options will be hidden on the home screen.
- **Language 1-4**: You can select four languages to be displayed on the home screen.

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.





- **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.
- **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.
- **Enable 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, 2 or less, 3 or less, and 4 or less.
- **Tower Length**: Select a maximum length for towers: 1, 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**.



Text Prompt Display

You can set up the text prompts on the Call, PIN, and Directory screens.

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

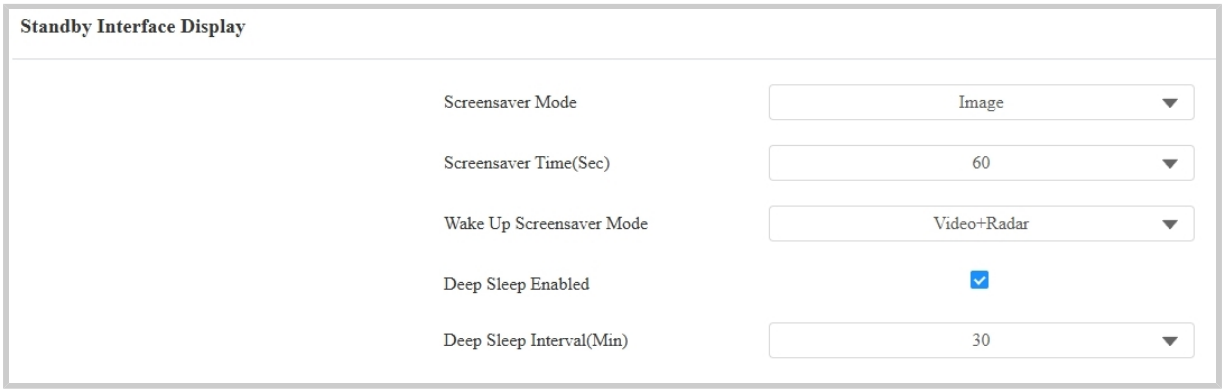


Screensaver Settings

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

On the Web

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



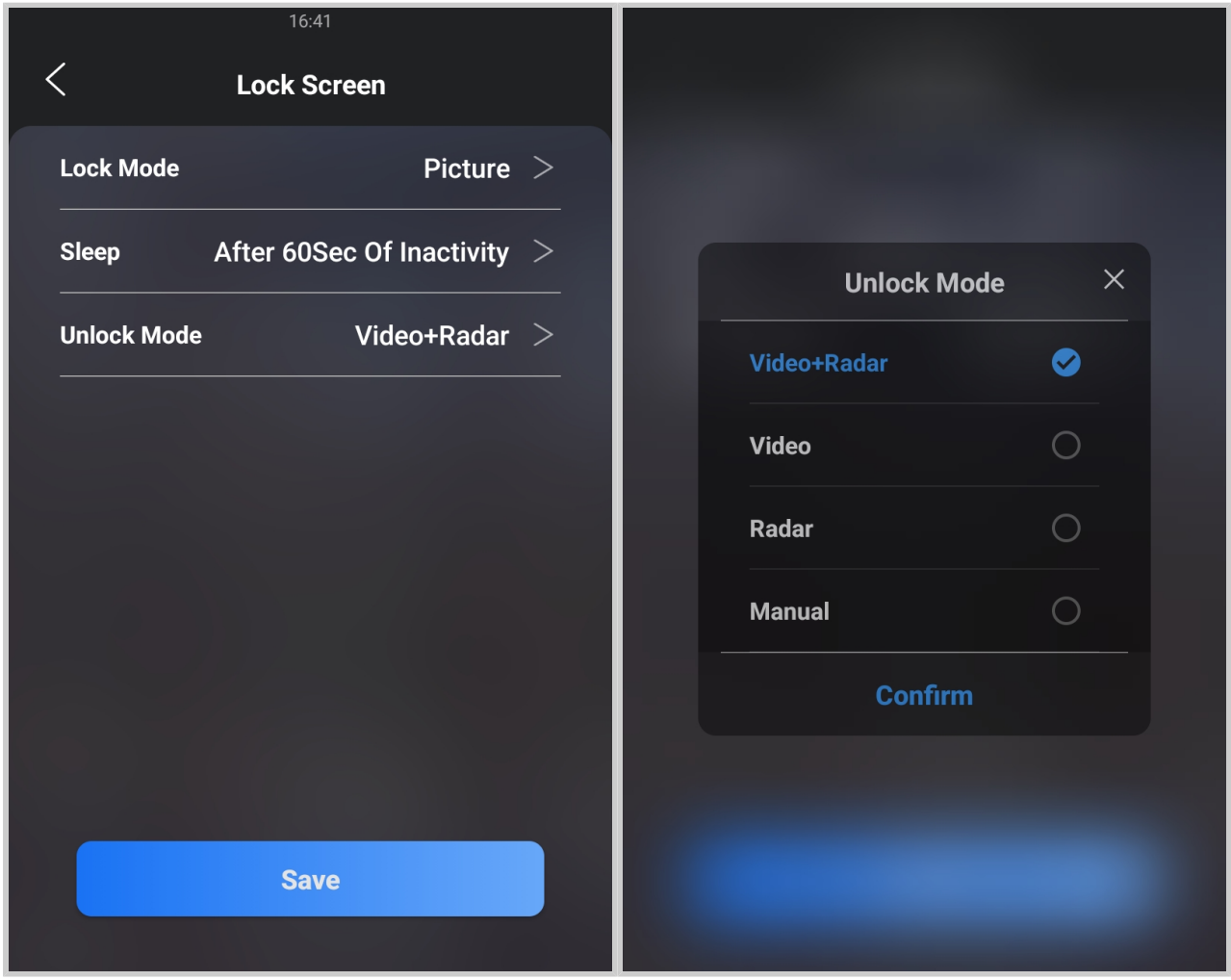
- **Screensaver Mode:**

  - **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 screensaver.
- **Screensaver Time (Sec)**: Set the screen saver start time from 5 seconds up to 180 seconds. The screensaver starts when the device detects no operation or when no one is approaching.
- **Wake Up Screensaver Mode**:
  - **Video**: Wake up the screen by video-based motion detection. Focus on analyzing visual information captured through cameras.
  - **Radar**: Wake up the screen by radar detection. It offers a longer range and better detection in poor visibility conditions.
  - **Video+Radar**: Combine the video and radar detection to wake up the screen.
  - **Manual**: Touch and wake up the screen.
- **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.

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

On the Device

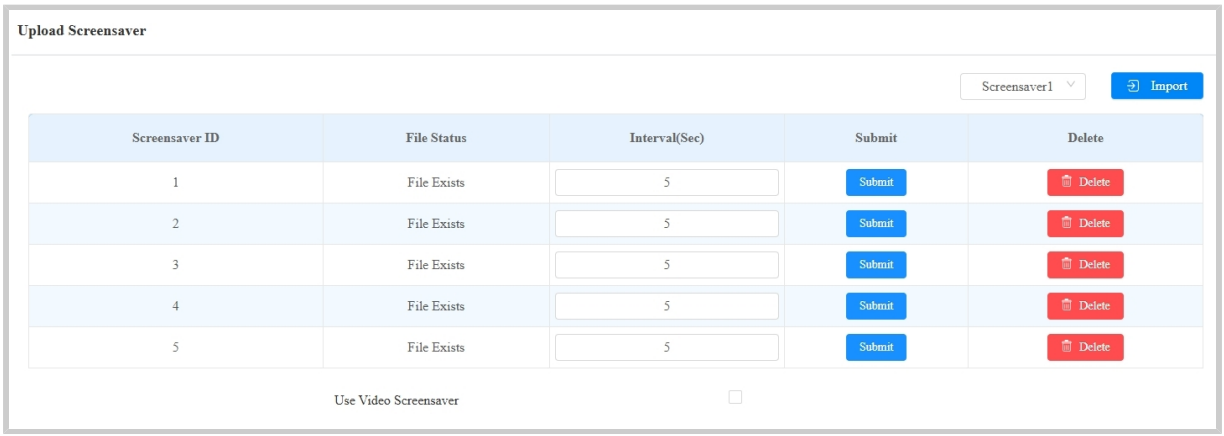
You can also configure the screensaver on the **Setting > Basic Setting > Lock Screen** screen.



Upload Screensaver

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

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



- **Use Video Screensaver**: Check to upload videos as a 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.

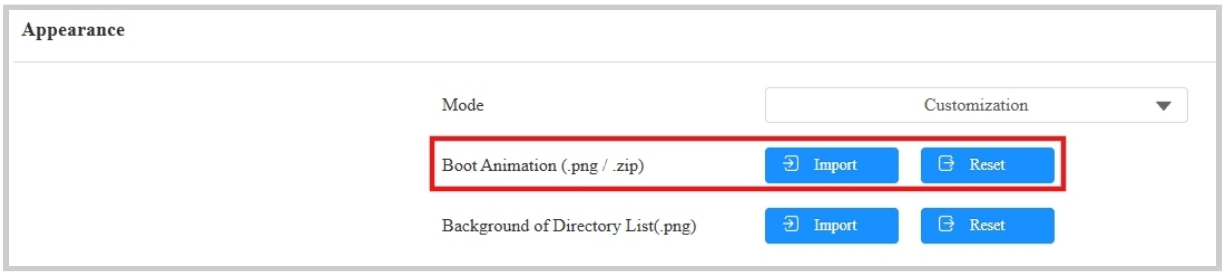
Note

- The uploaded pictures should be in JPG format with a maximum size of 2 MB.
- The recommended resolution is 800*1280.
- The previous picture with a specific ID order will be overwritten when a 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** 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 Device Directory List Background Image

You can upload a background picture that works for the directory screen. If you use the **Appearance** function, the Upload Background setting will be hidden.

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



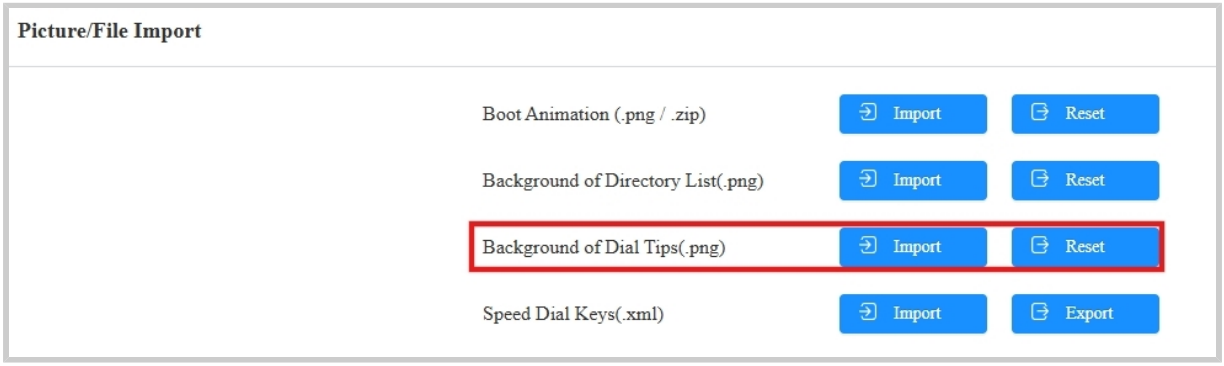
Note

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

Upload Background of Dial Tips

You can upload the background displayed on the Dial screen's time area in the **Villa** theme.

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

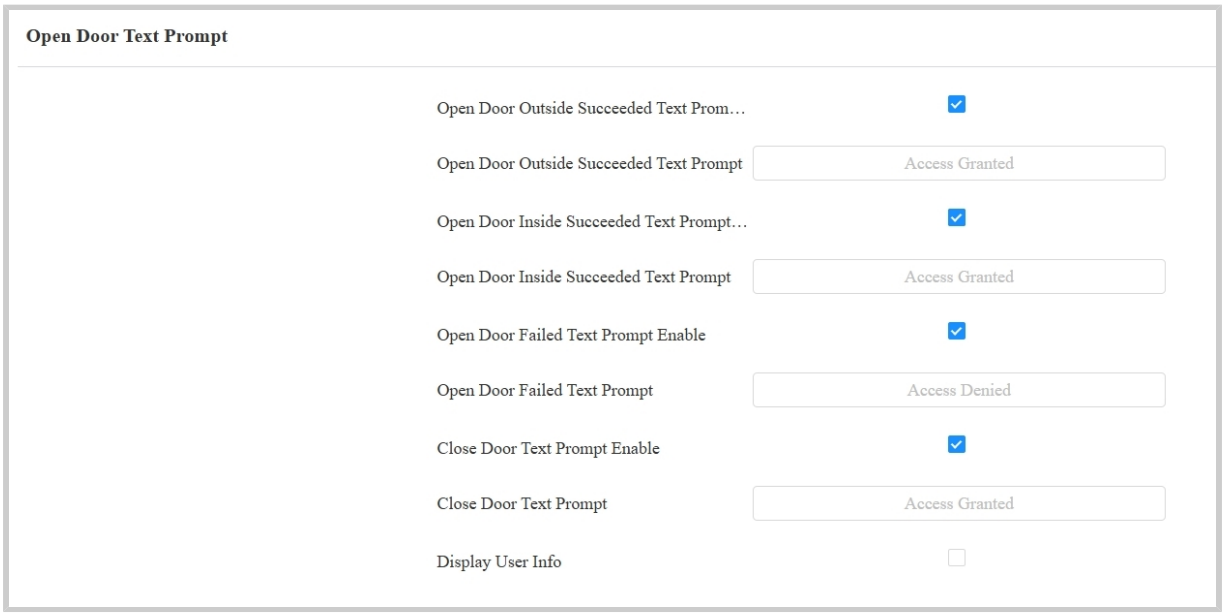


> **Note**
>
> Max picture Size: 1MB; Recommended Resolution: 800*400.

Open Door Text Prompt

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

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

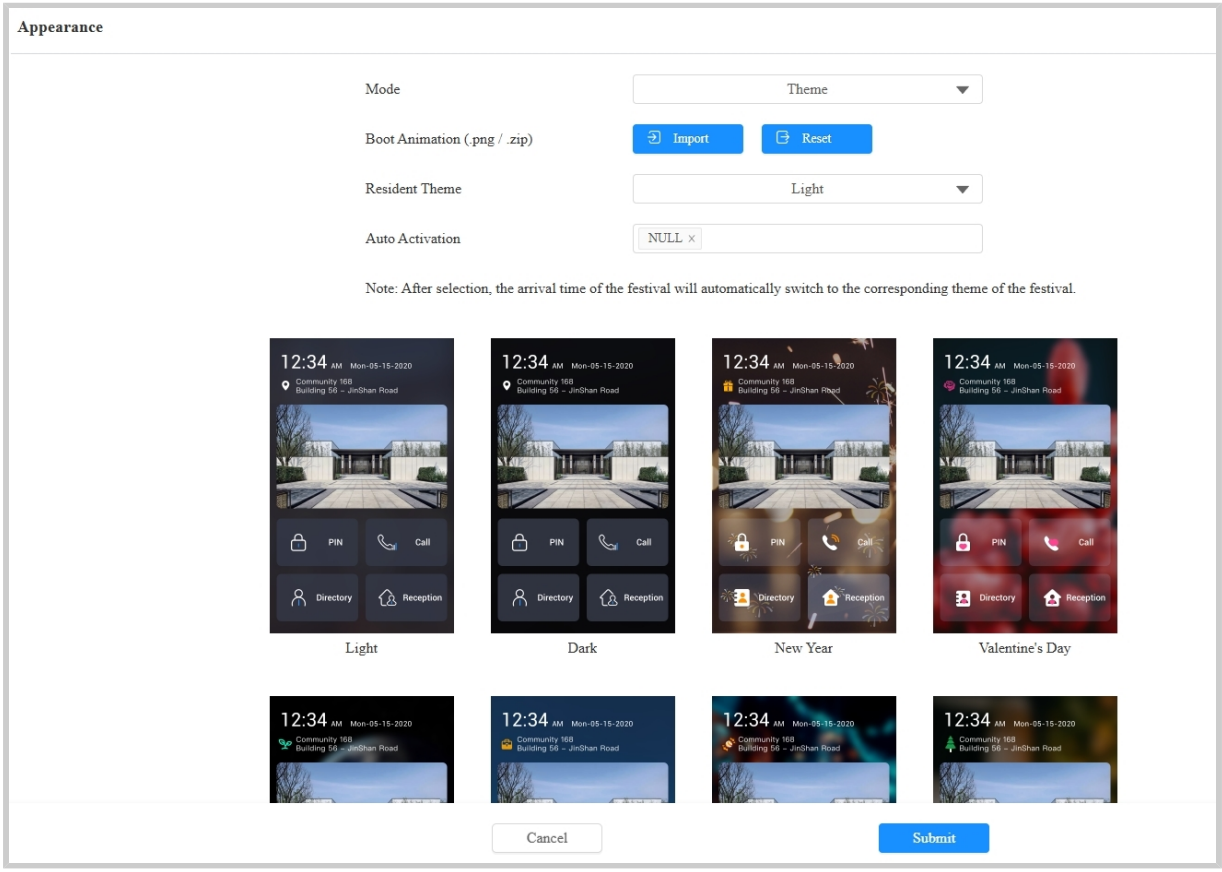


- **Open Door Outside Succeeded Text Prompt:** Display a text prompt after the door is opened by the device-supported access methods except for the exit button.
- **Open Door Inside Succeeded Text Prompt:** Display a text prompt after the door is opened by pressing an exit button(the input is triggered).
- **Open Door Failed Text Prompt:** Display a text prompt after opening the door fails.
- **Close Door Text Prompt**: The door-closing text prompt works for the relay(s) set to the **Bistable** mode. When users close the door with their credentials, the prompt will be displayed on the device's screen.
- **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" with "Stranger, Name: Unknown" will be displayed.

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.



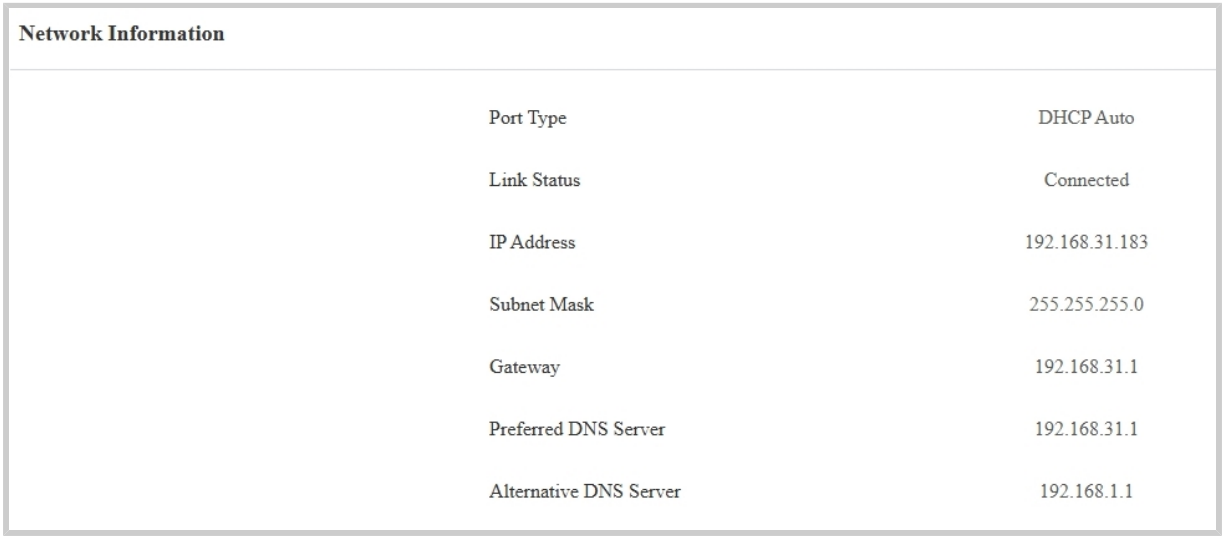
- **Mode**:
  - **Theme**: The default option. When selected, you can check the desired appearance option.
  - **Customization**: When selected, you can upload icon pictures for desired tabs, such as PIN, Call, and Directory.
- **Resident Theme**: Select the desired appearance.
- **Auto Activation**: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

Network Setting

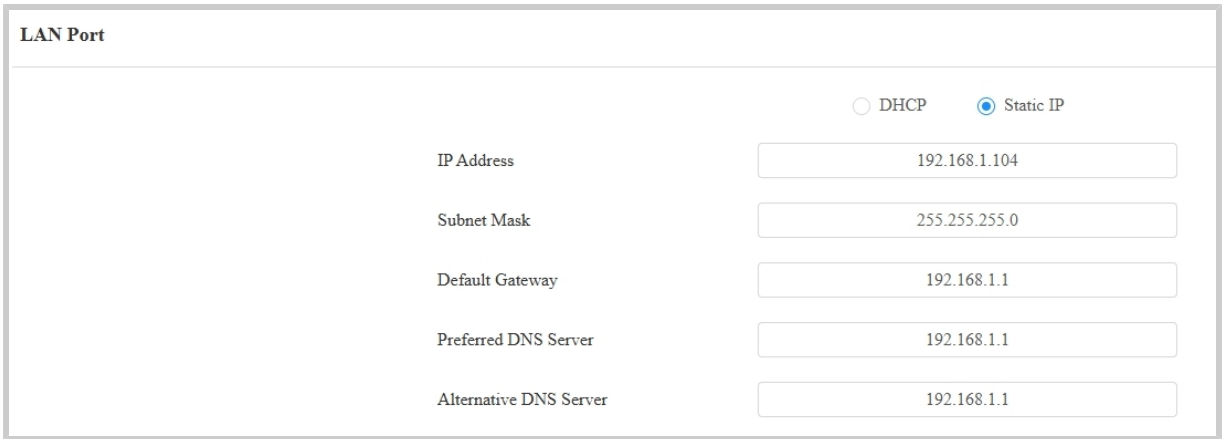
Device Network Configuration

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

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

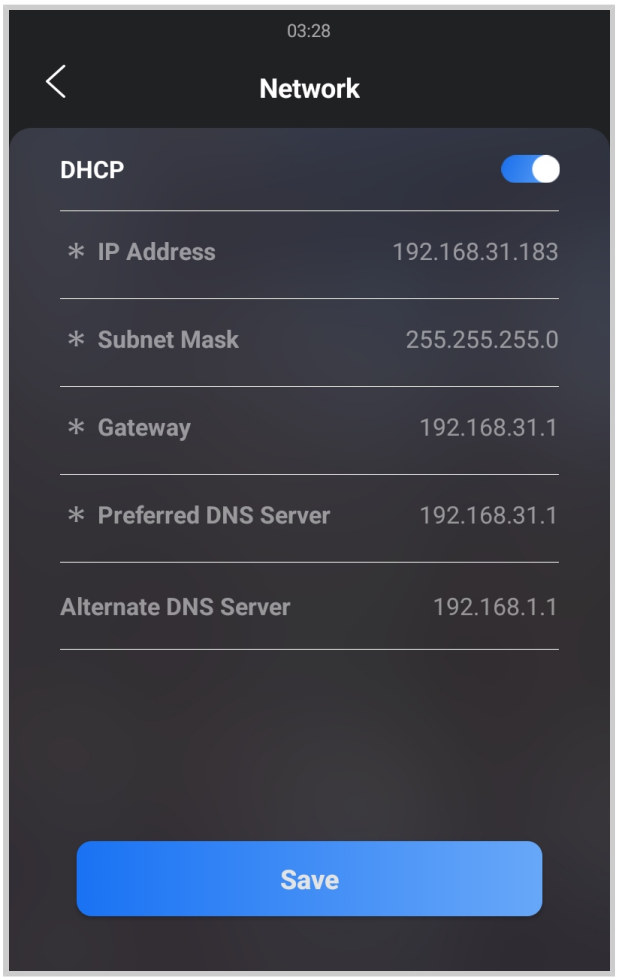


Set the network connection on the web **Network > Basic** interface.



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

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

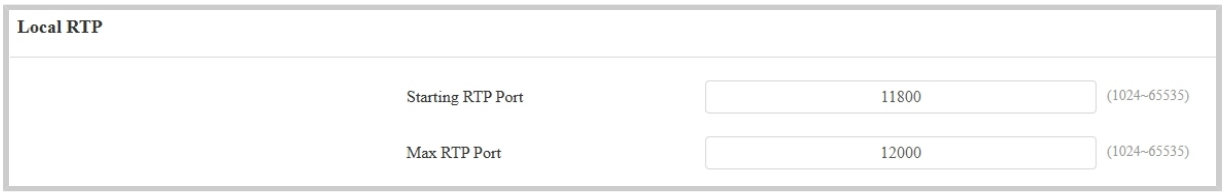


Device Local RTP Configuration

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.



- **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 Type**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None. You can also select 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/ACMS**: The device is connected to the SDMC/ACMS, a management platform designed for on-premise projects. The SDMC/ACMS 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.
- **Device Location**: Enter the location in which the device is installed and used to distinguish it from other devices.

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.

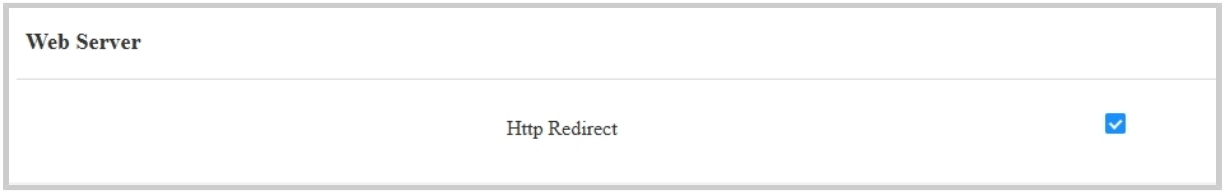


- **UDP Keep Alive Messages:** If enabled, the device will send the message to the SIP server, which will recognize whether the device is online.
- **UDP Alive Messages Interval:** Set the message-sending interval from 5-60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when the SIP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

Web HTTP Setting

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

Enable the HTTP redirect on the **Network > Advanced** interface.



- **HTTP Redirect**: It is enabled by default, which means all HTTP requests will automatically be redirected to HTTPS. If it is disabled, the device's web interface can be accessed using HTTP directly.

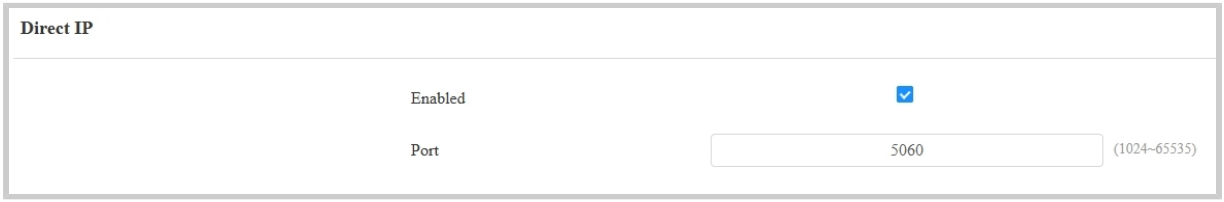
Intercom Call Configuration

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

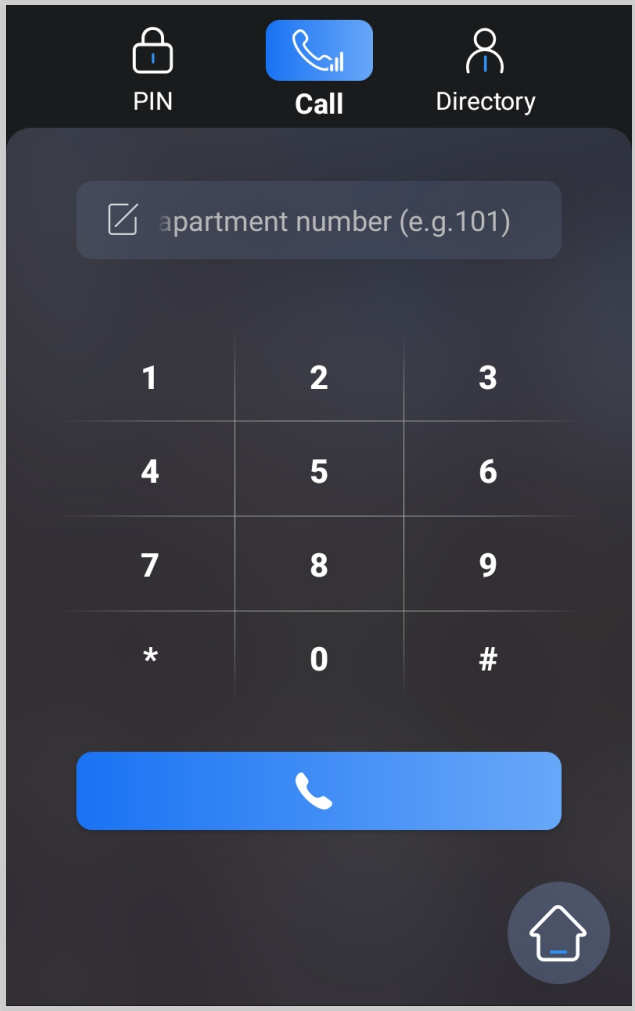
Enable IP call on the **Intercom > Basic > Direct IP** interface.



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

Make IP Calls

Make IP calls by pressing the **Dial** key on the home screen, entering the IP number such as “192✳168✳35✳123”, and pressing the Call button.



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.

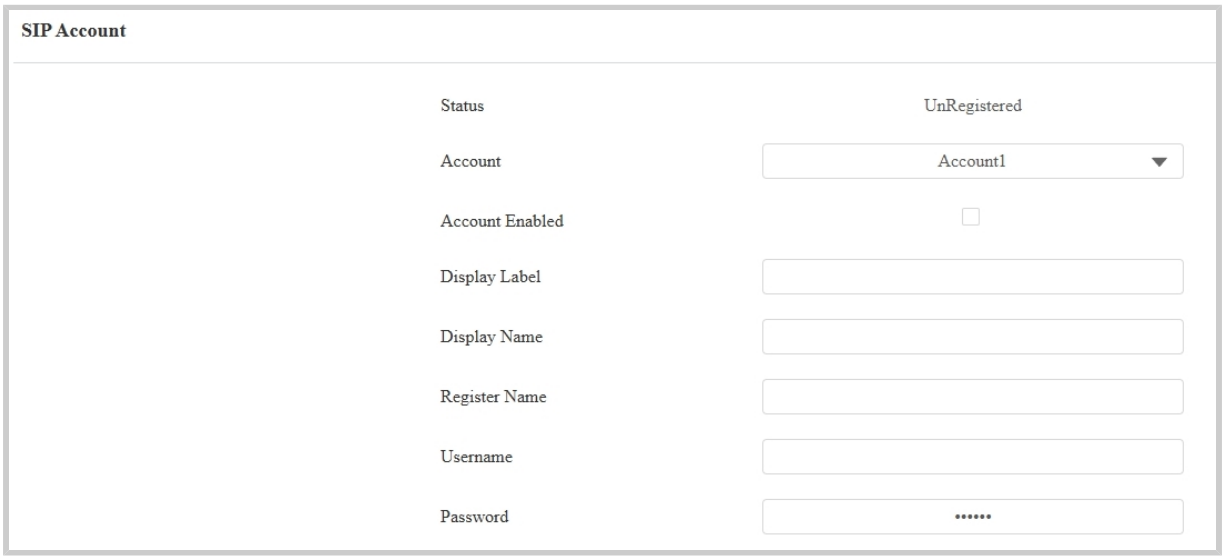
SIP Account Registration

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.



- **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

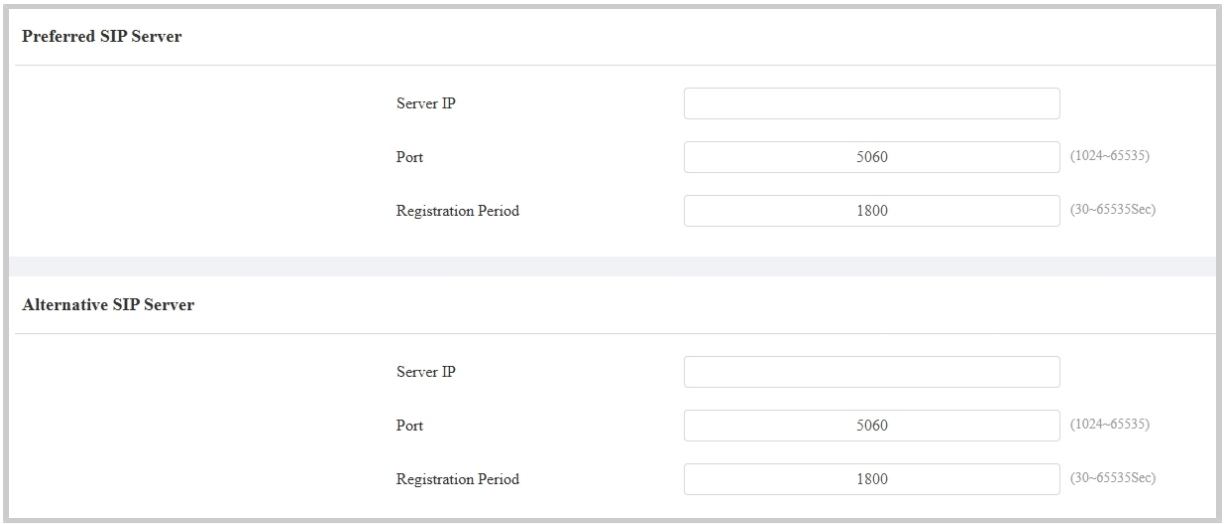
- For configuring contact call and dial plan, see here.
- When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

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

SIP Server Configuration

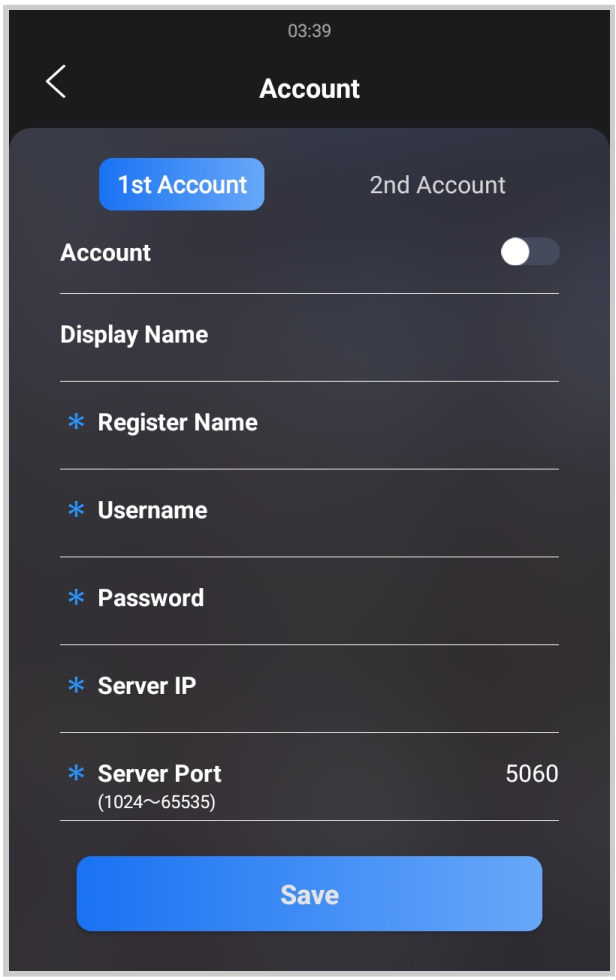
SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

Set it up on the web **Account > Basic > Preferred SIP Server** interface.



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

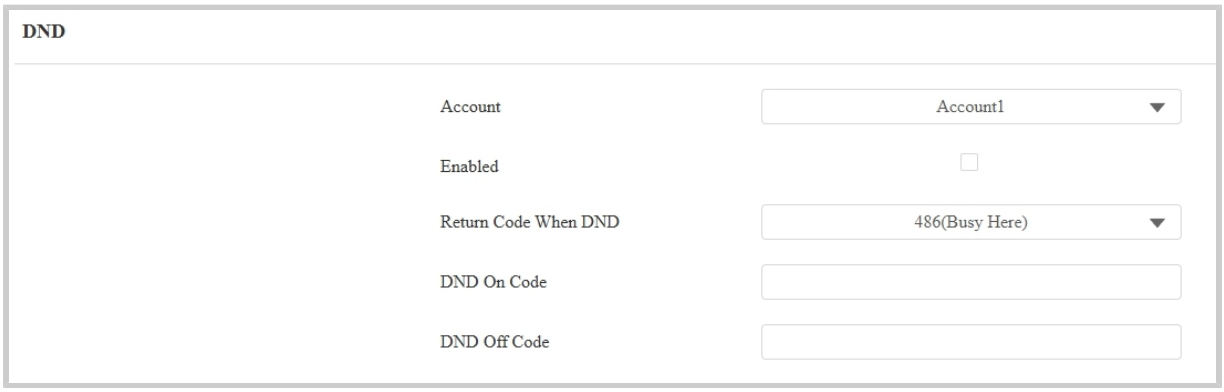
You can also register SIP accounts on the **Setting > Account** screen.



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.

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

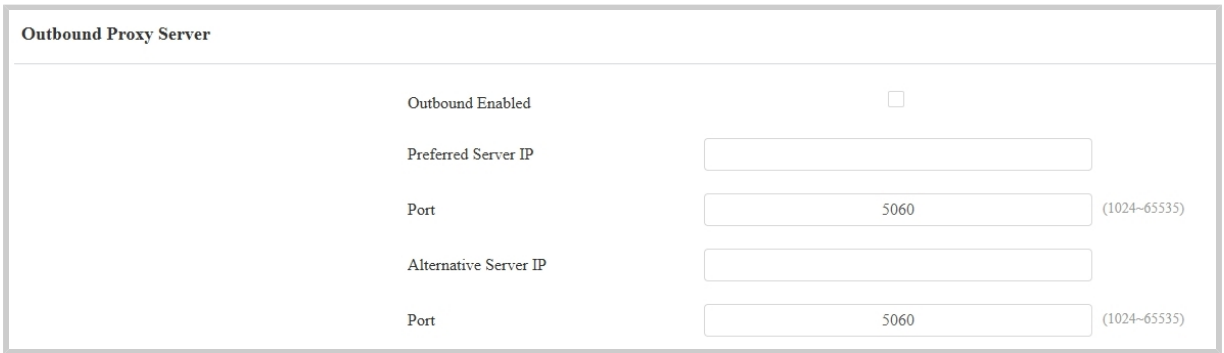


- **Account**: Select the account(s) that adopt the DND feature.
- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode
- **DND On Code**: The code used to turn on DND in the SIP server.
- **DND Off Code:** The code used to turn off DND in the SIP server.

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.



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

- **Port:** Set the proxy port for establishing a call session via the backup outbound proxy server.

Data Transmission Type

SIP messages can be transmitted in three data transmission protocols: **UDP** (**User Datagram Protocol**), **TCP** (**Transmission Control Protocol**), and **TLS** (**Transport Layer Security**). In the meantime, you can also identify the server from which the data comes.

Set up the data transmission type on the web **Account > Basic > Transport Type** interface.

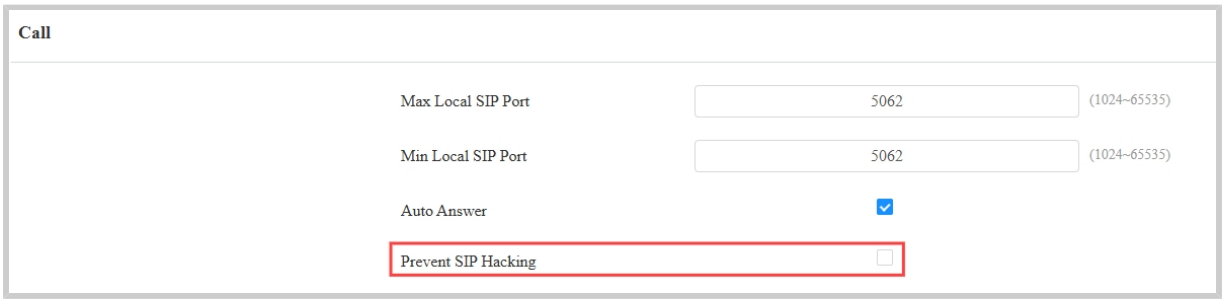


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

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.

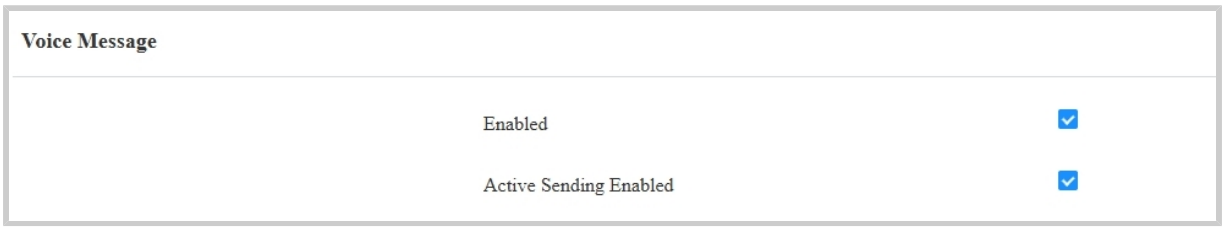


- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

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.



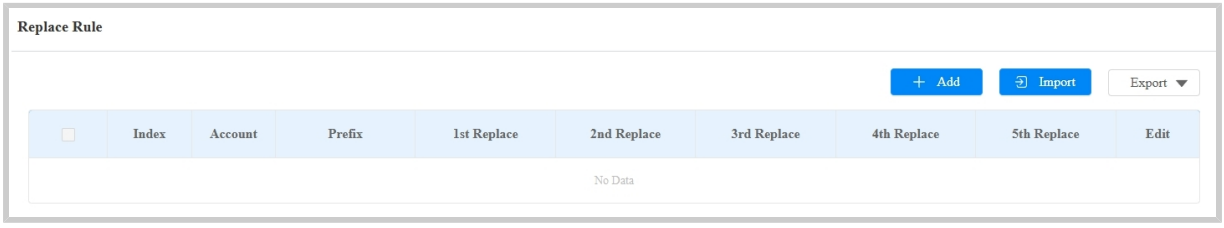
- **Active Sending Enabled**: When enabled, users can proactively leave messages to a specific contact. When disabled, the message icon on the **Directory** screen will be hidden.

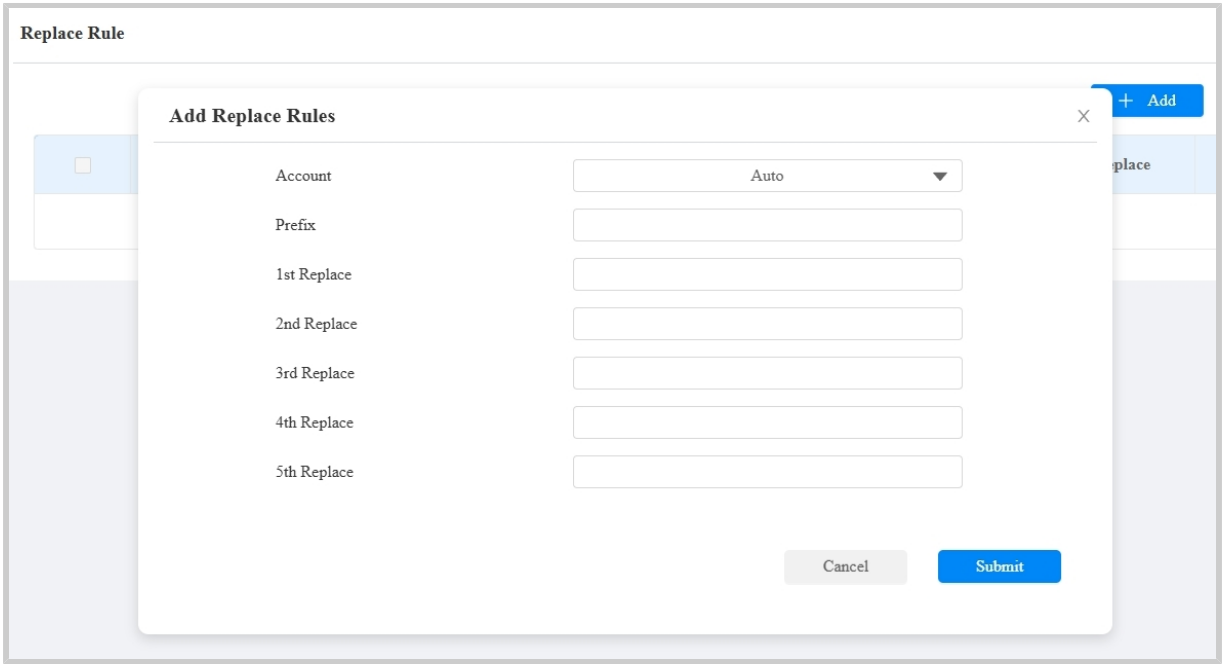
Call Settings

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**. The device supports up to 2,000 dial plan rules.

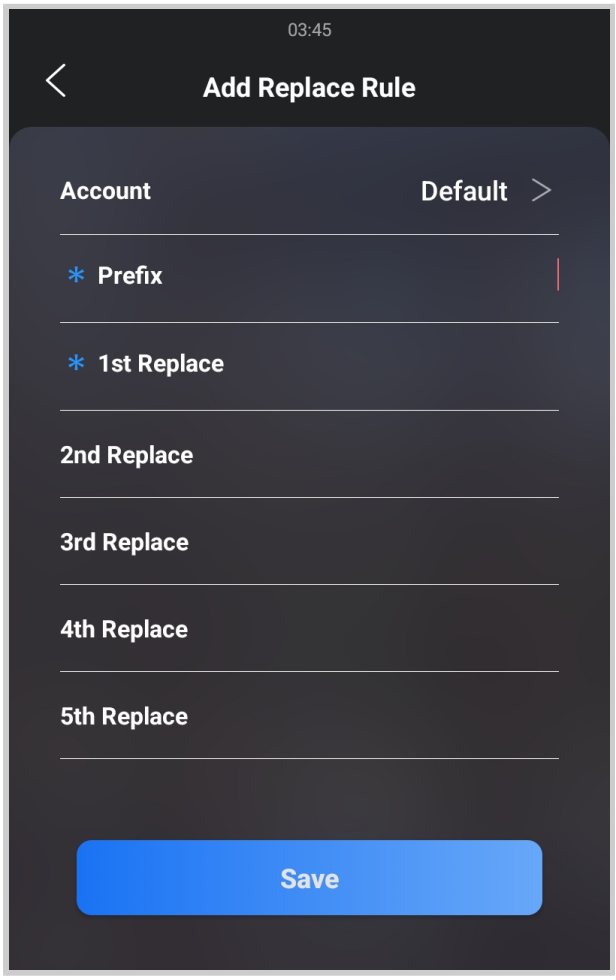




- **Account:** Select the dial-out account.
  - Auto: Dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.

- **Account 1/2:** Dial-out using the chosen account.
- **Prefix:** Specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** Specify up to 5 numbers, which can be SIP numbers or IP addresses, to be replaced by the prefix. All these numbers will be called simultaneously when the caller dials the prefix.

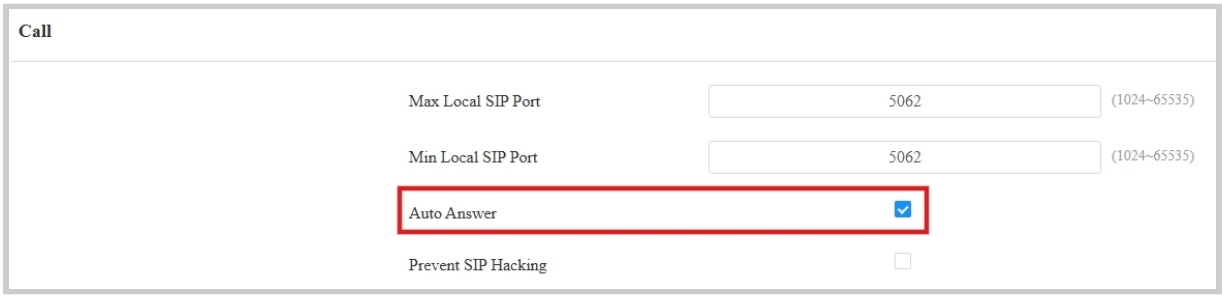
You can also set up the dial plan on the **Setting > Replace Rule** screen.



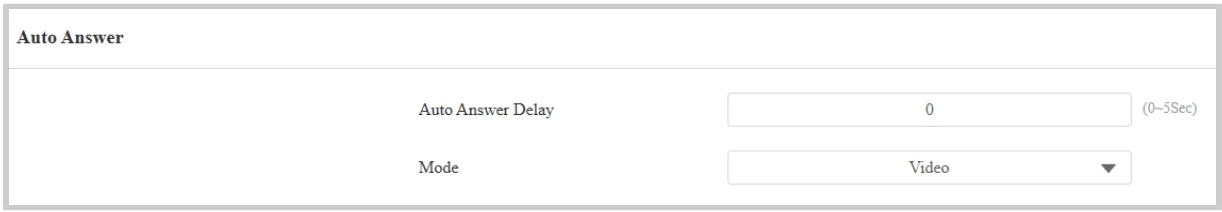
Call Auto-answer Configuration

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.



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



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

Sequence Call

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

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

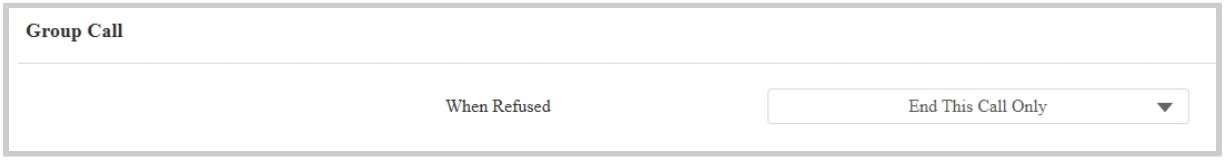


- **Time Out(Sec):** Specify the time limit for the call between two sequential call numbers. For example, if the time value is set to 10, the call that is not answered in 10 seconds will be ended automatically and transferred to the next call number in order.
- **When Refused:** Determine whether to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

Group Call

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

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

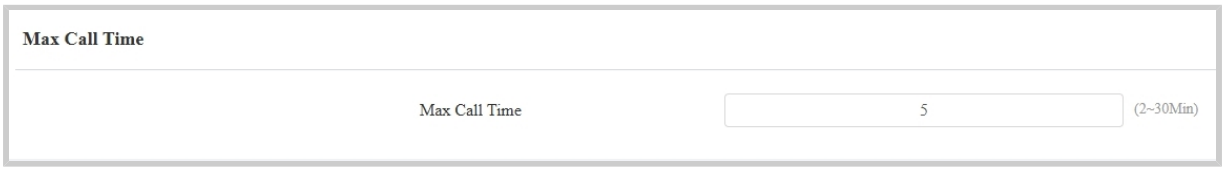


- **When Refused**:
  - **End This Call Only**: The device will continue to call other numbers.
  - **End All Calls**: The call ends.

Maximum Call Duration

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

To configure it, go to **Intercom > Call Feature > Max Call Time** interface.

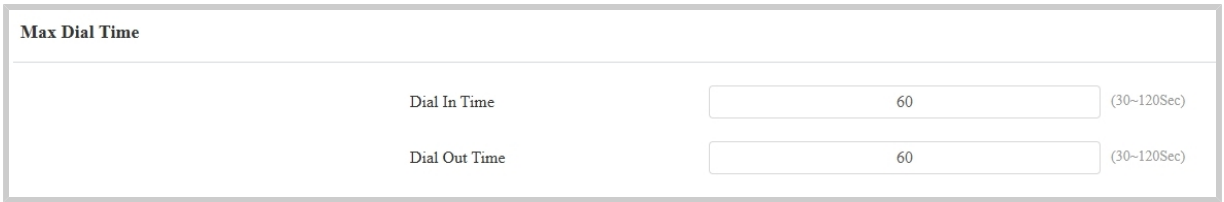


- **Max Call Time:** Specify the maximum duration of all calls. The door phone will end the call automatically when the time limit is reached.

Maximum Dial Duration

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

To configure it, go to **Intercom > Call Feature > Max Dial Time** interface.



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

- **Dial Out Time:** Specify the maximum duration of an outgoing call. The door phone will automatically end the call 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.

To set the feature, go to **Intercom > Call Feature > Hang Up After Open Door** interface.



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

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 > In Call Type** interface.



- Two-Way Video: Normal 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.

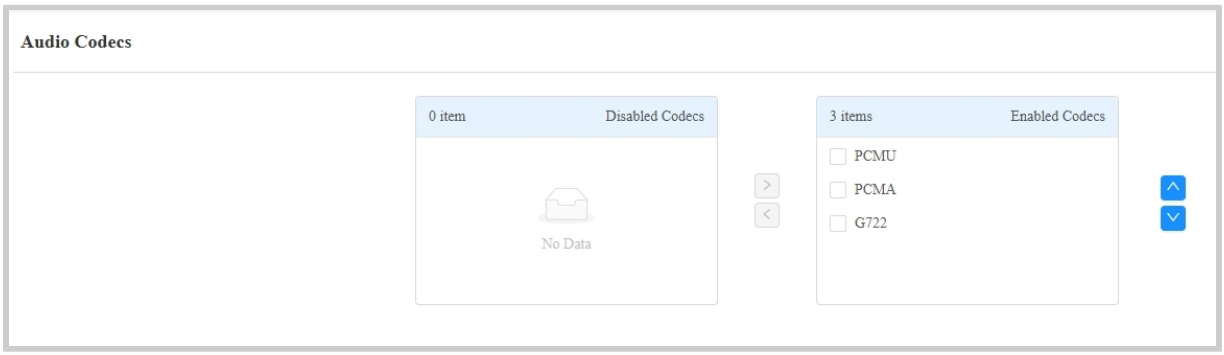
Audio and Video Codec Configuration

Audio Codec

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

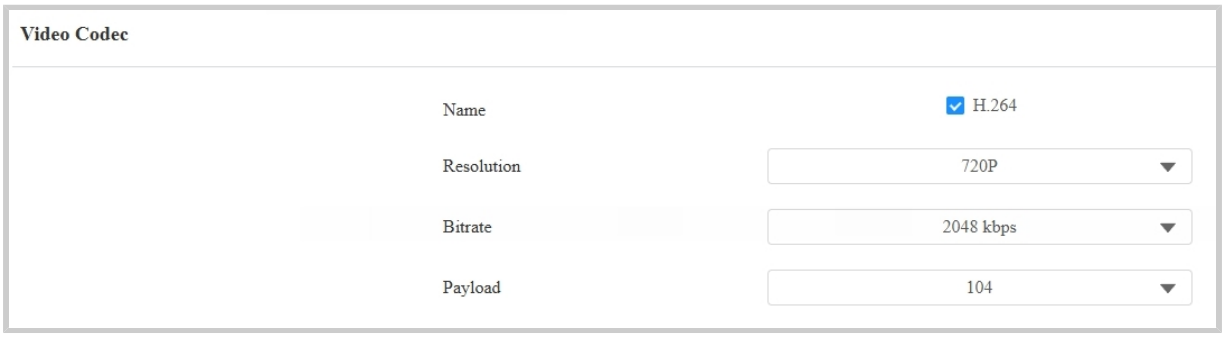


Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec

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

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



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



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

Contacts Configuration

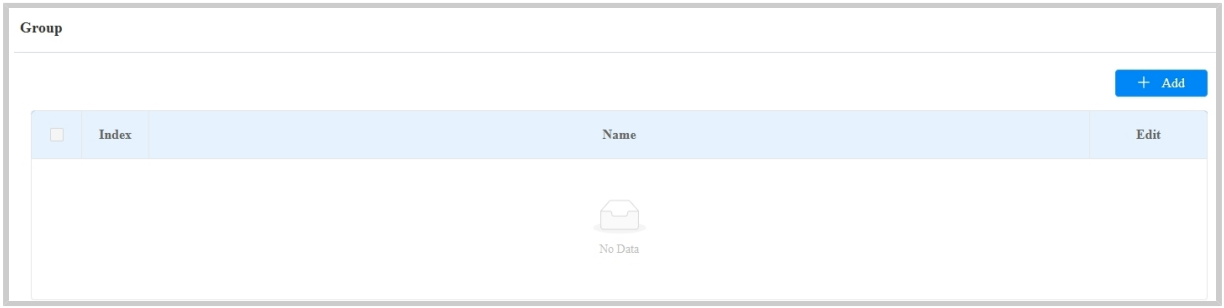
The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

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

Manage Contact Groups

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

To set it up, go to the **Directory > User > Group** interface. Click **+Add**. You can also add groups on the **Setting > User > Group** screen. You can add 5,000 groups or more.

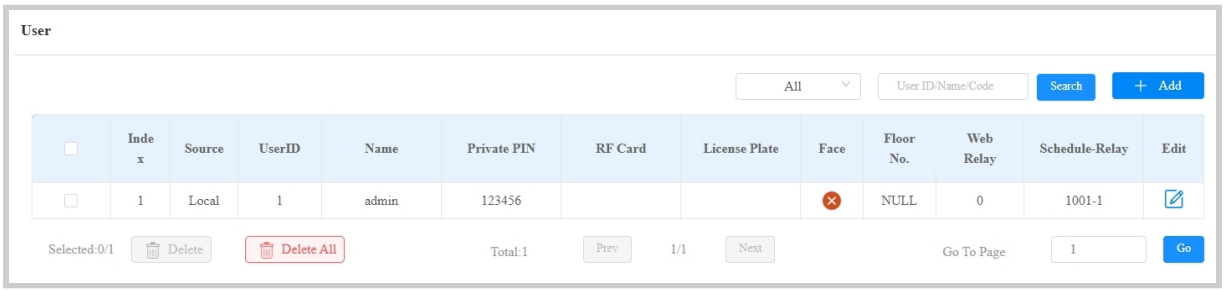


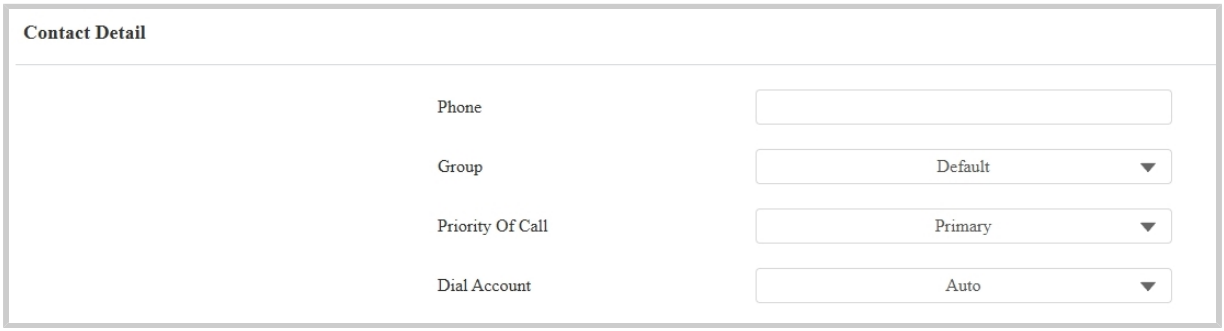


Set up Contact Details

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

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



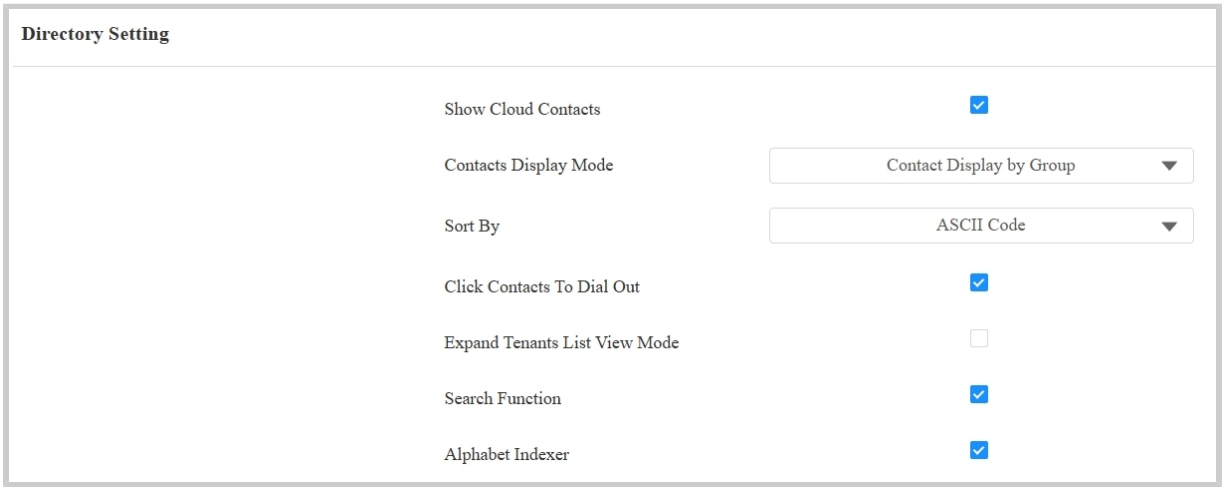


- **Phone**: The IP or SIP number.
- **Group**: Assign the contact to the Default, Hidden Contact, or a self-created group.
- **Priority of Call**: When assigning the contact to a self-created group, set the priority of the call among three options: Primary, Secondary, and Tertiary. For example, if you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

Contact List Display

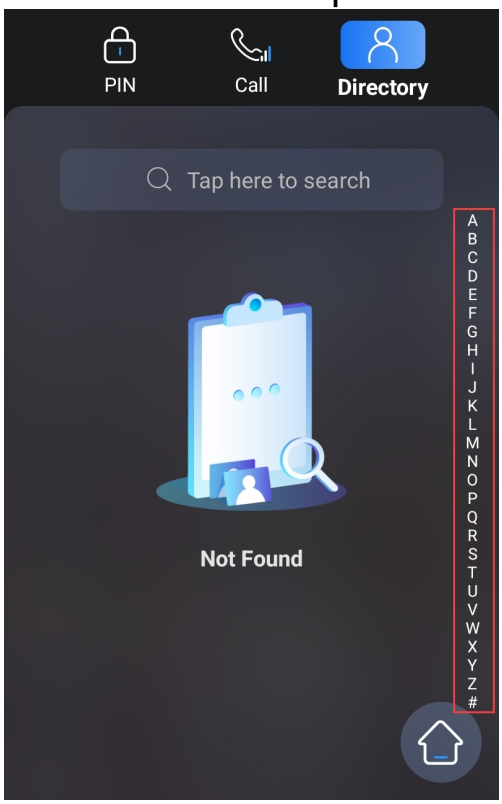
You can customize the contact list display to cater to users' operational and visual preferences.

To set it up, go to **Directory > Directory Setting** interface.



- **Show Cloud Contacts**: The contacts synchronized from the SmartPlus cloud can be displayed.
- **Contacts Display Mode**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only:** Display contact groups. Press the desired group on the device screen to make a group call.
  - **Contact Display by Group:** Display contacts by groups. Press the group, and users can see the contacts in it.
- **Sort By**:
  - **ASCII Code** lists directory by its name in the sequence of the ASCII code.
  - **Room No.** lists the directory according to their room numbers.
  - **Import** lists directory according to their order in the imported file.
- **Click Contacts 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.
- **Search Function**: Set whether to display the search box at the top of the screen.

- **Alphabet Indexer**: When enabled, users can find the desired contact with the alphabet indexer on the Directory screen.



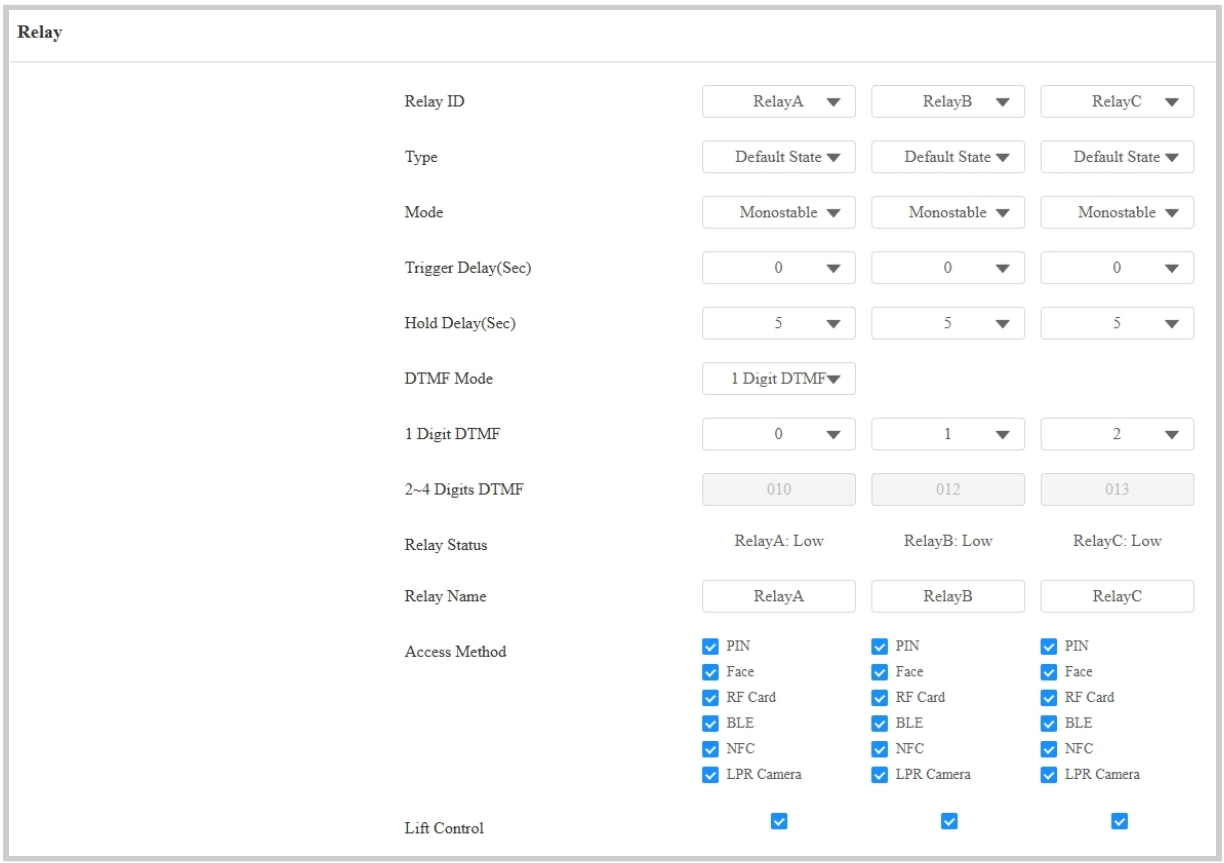
- **Cloud Call Permission Control**: This option will display when the device is connected to the Akuvox Cloud. It decides whether to link the SmartPlus user's permissions to open doors and make calls.
  - For example, when users are not authorized to open doors during a specific time, and the Cloud Call Permission Control feature is enabled, their SmartPlus App and/or indoor monitors will not receive calls from the door phone.
  - If this feature is disabled, even if users cannot open doors, they can receive calls.

Relay Setting

Local Relay

A local relay is the relay output built into the intercom device. It can directly control connected devices, such as door locks, by triggering actions based on user input or authorization.

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



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 open.

- **Invert State**: A “Low” status in the Relay Status field indicates an open door, while “High” indicates a closed one.

- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **Bistable**: The relay status resets upon triggering the relay again.

Trigger Delay (Sec): Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.

- **Hold Delay (Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.

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

- **2-4 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 open and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Access Method**: Check the method(s) to trigger the relay.
- **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.

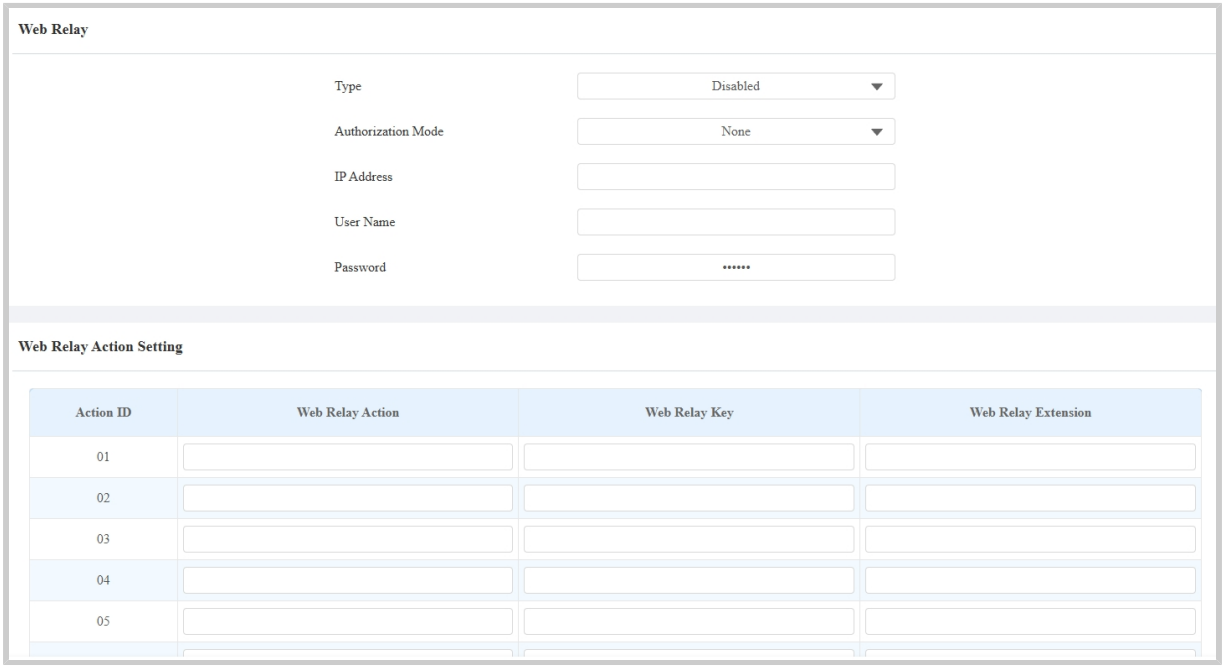
Web Relay

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 configure it, go to **Access Control > Web Relay** interface.



- **Type**: Determine the type of relay activated when employing door access methods for entry.
  - **Disabled**: Only activate the local relay.
  - **Only Web Relay**: Only activate the web relay.
  - **Both Local Relay and Web Relay**: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay.

- **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.

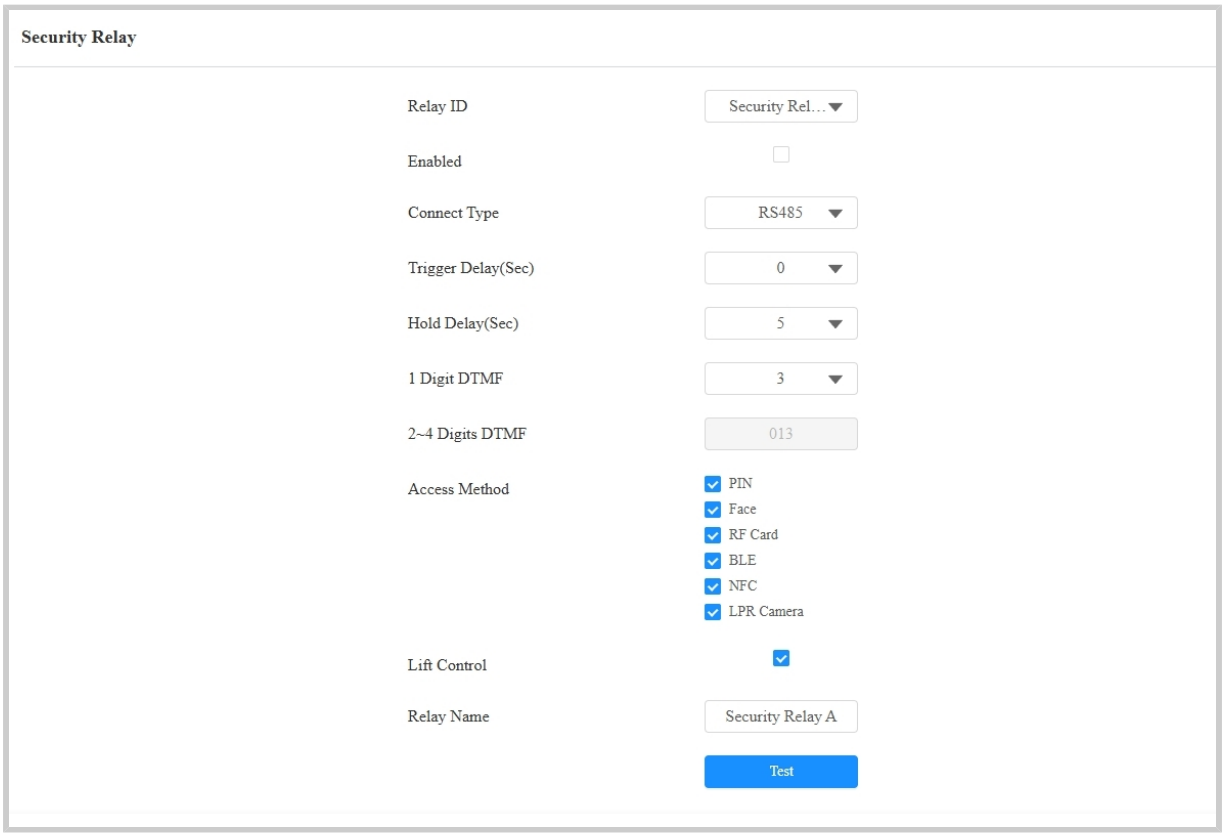
Security Relay

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.

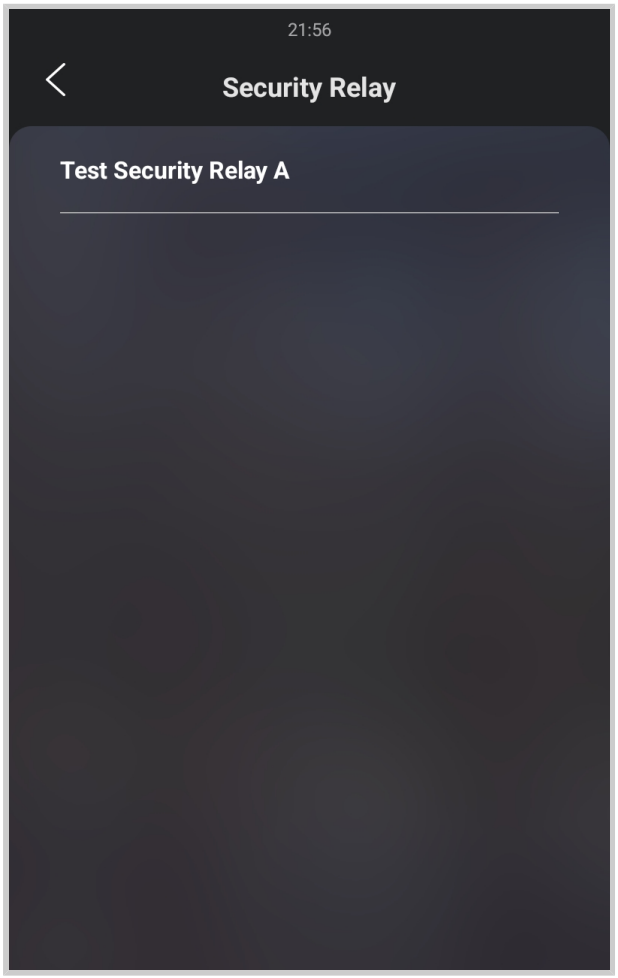
To set up the security relay, navigate to **Access Control > Relay > Security Relay** interface.



- **Connect Type**: Select the connection type between the security relay and the door phone. You can select the 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 open for 5 seconds before closing.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **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.

- **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.

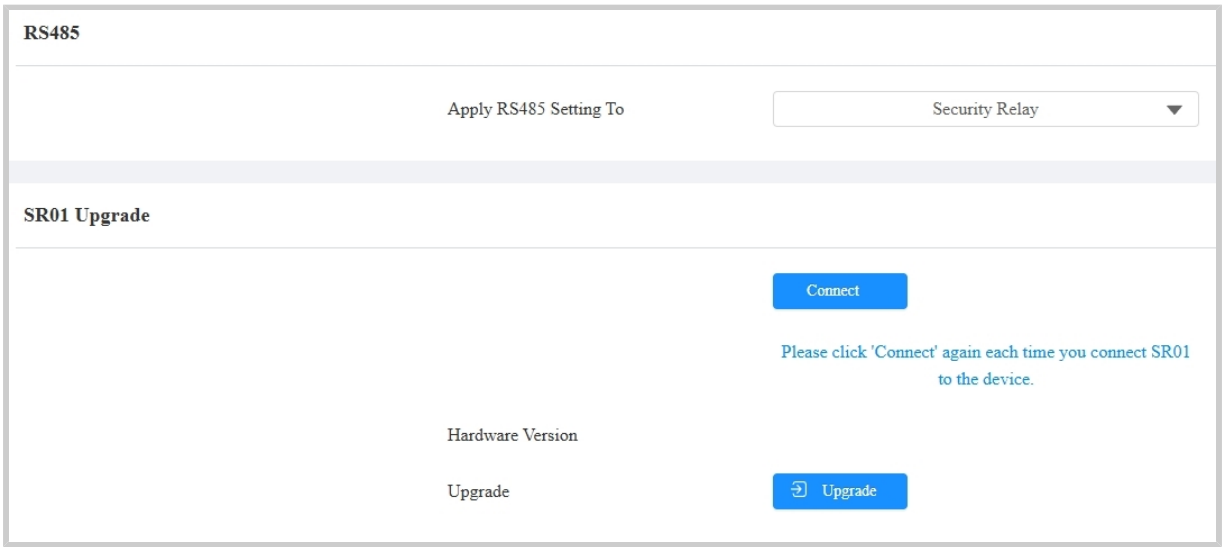
You can also test the security relay on the device by going to **Security > Security Relay**.



Upgrade SR01

You can upgrade the Akuvox SR01 on the **Device > RS485** interface.

SR01 Upgrade is available when the **Apply RS485 Setting To** option is set to **Security Relay**.



- **Connect**: Ensure a successful connection between the device and the SR01 before the upgrade.
- **Hardware Version**: The SR01 hardware version will display after a successful connection.
- **Upgrade**: Click to upload the ROM file.

> **Note**
>
> Click here to download the upgrade file.

Access Control Schedule Management

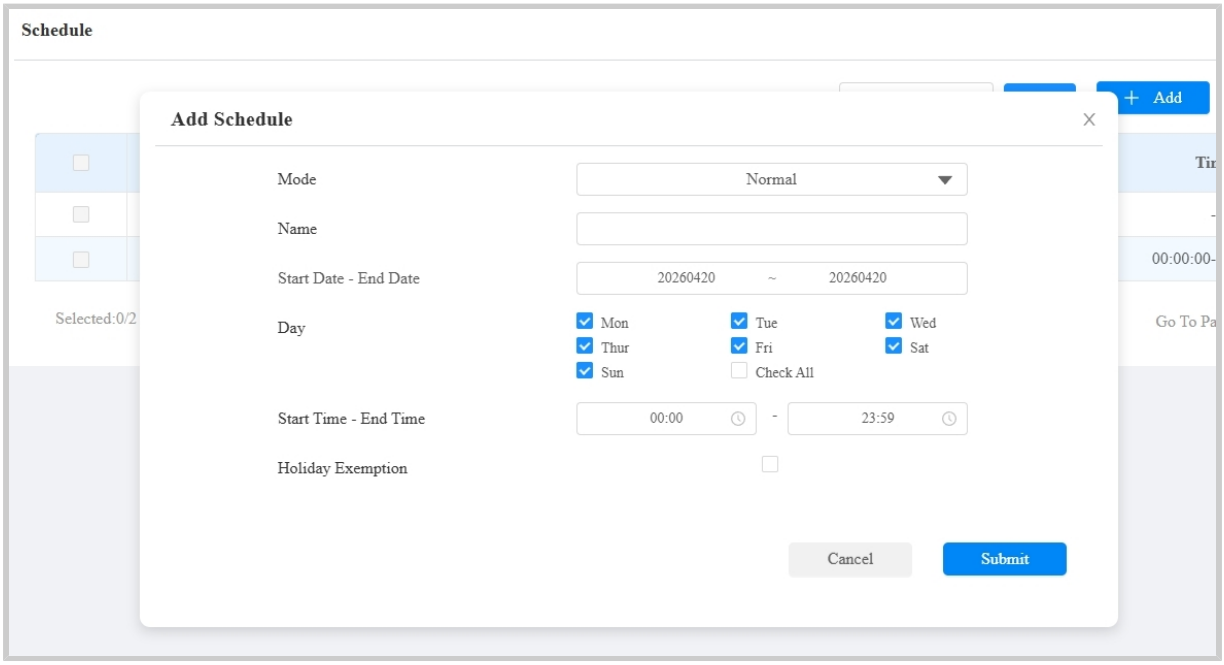
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create a Door Access Schedule

To configure the schedule, navigate to the web **Setting > Schedule** interface. Click **+Add**. You can add 500 schedules.

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





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

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

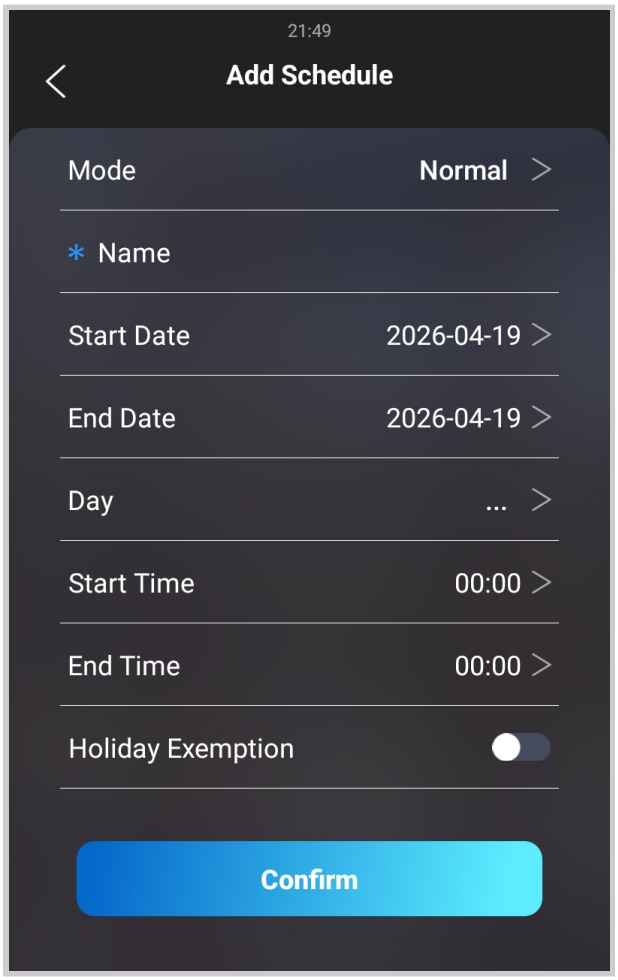
Import and Export Door Access Schedule

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.



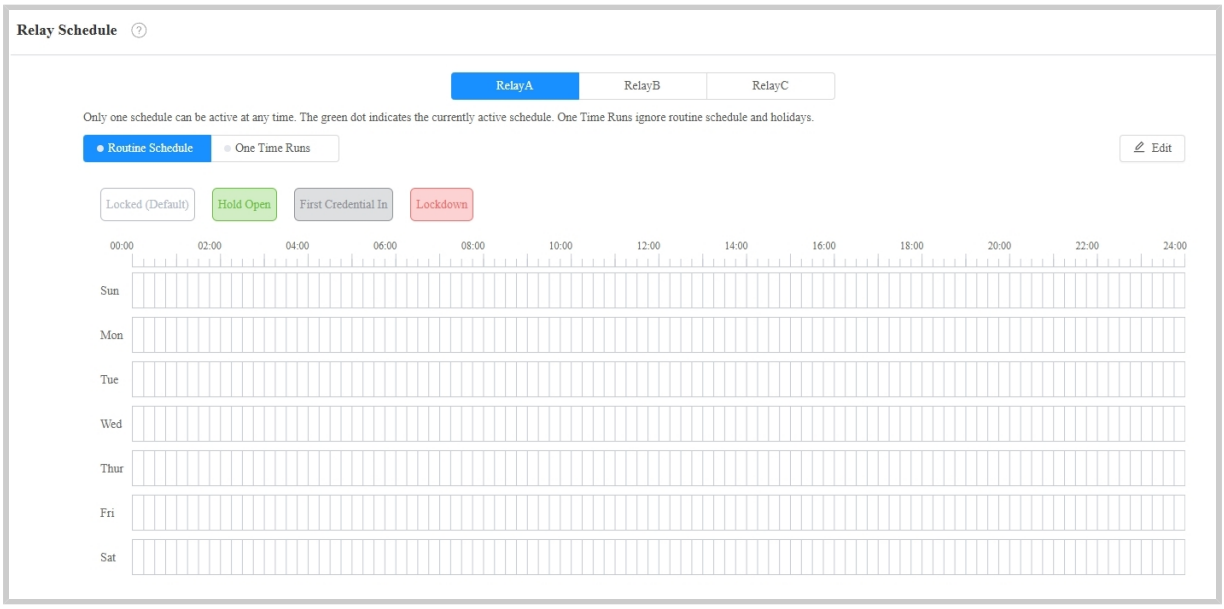
You can also create schedules on the **Setting > Basic Setting > Schedule** screen.



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

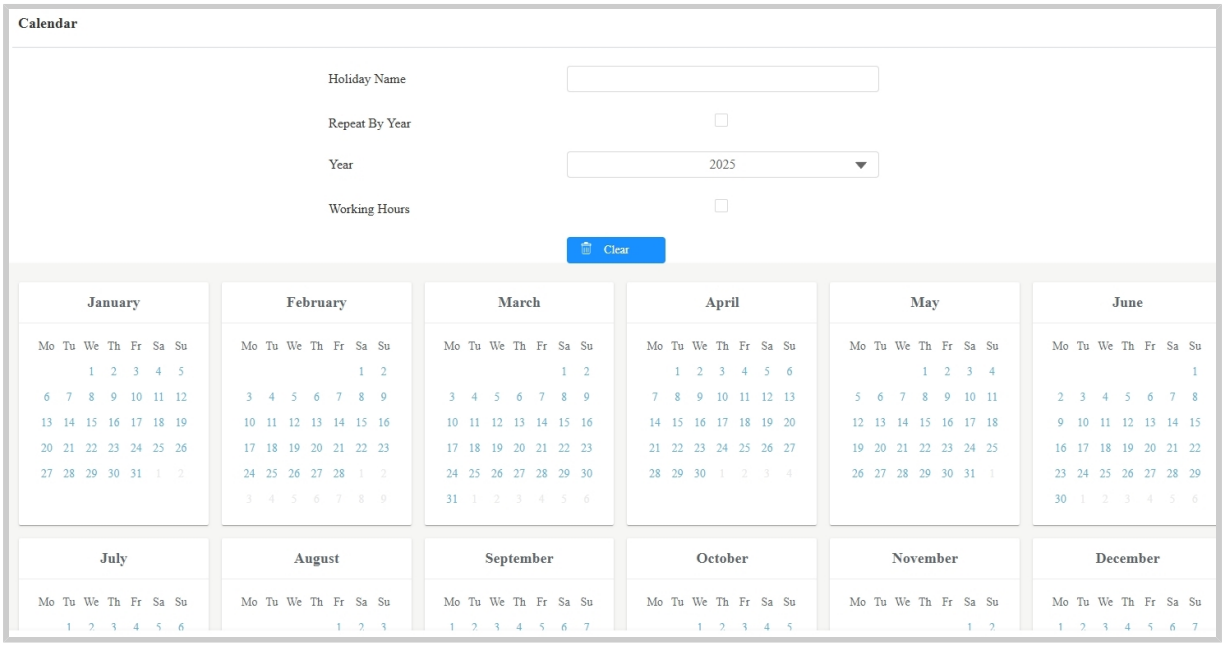
> **Note**
>
> Click here to view the detailed configuration of each schedule mode.

Holiday Schedule

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

Set it up on the **Setting > Holiday** interface. Click **+Add**. You can add 100 holiday schedules.





- **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.

Door-opening Configuration

Unlock By Public PIN

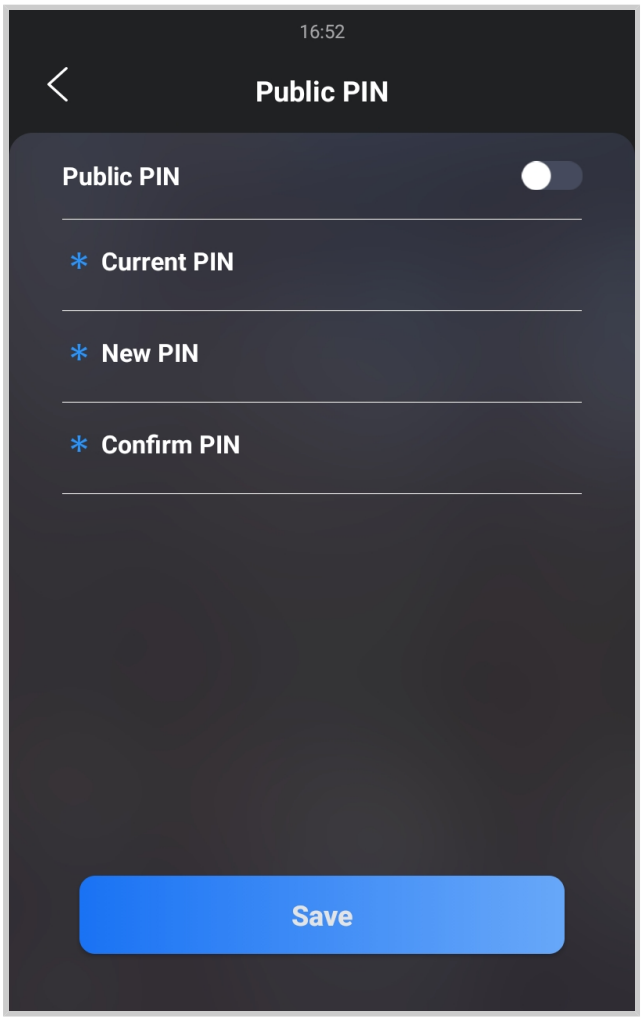
There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex. You can create and modify both the public and private PIN codes.

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



- **PIN Code**: Set the 4-8 digit code without 9 as the start. The default is 33333333.

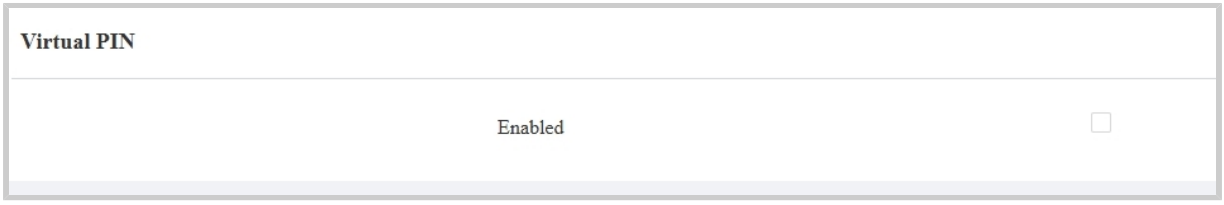
You can also set it up on the **Setting > Security > Public PIN** screen.



Virtual PIN

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

To enable the virtual PIN feature, navigate to **Access Control > PIN Setting > Virtual PIN** interface.



- **Enabled**: If enabled, users can add random digits before and after their PIN when unlocking the door, helping prevent others from seeing the real PIN.
  For example, if the PIN is 1234567, they can enter 99123456788. The device checks which stored PIN has the most matching digits and grants access to that user. If **Two-Factor Authentication** is enabled, the virtual PIN is verified only after the first authentication step is passed, such as **Face + PIN**.

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

User-specific Access Methods

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

When adding a user, you can also customize settings such as defining the door access schedule to determine when the code is valid and specifying which relay to open. You can add up to 50,000 users.

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



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

Unlock by Private PIN Code

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



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

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



- **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 RF Card/Bkey

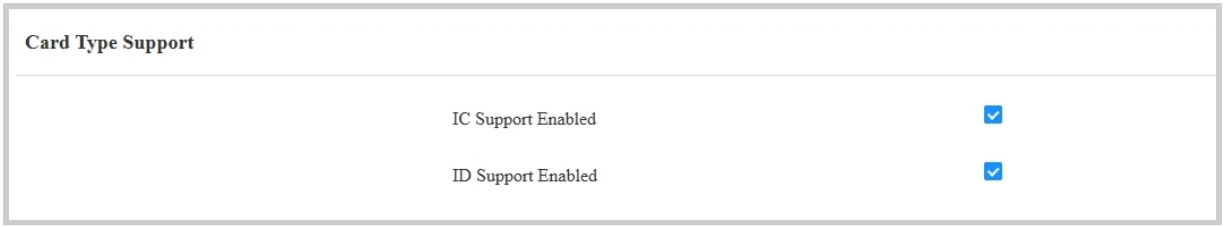
On the **Directory > User > +Add** interface, find the **RF Card & Bkey** section.



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

> **Note**
>
> - Click here to view the detailed steps of configuring Bkey.
> - RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device for access.
> - Each user can have a maximum of 5 cards added.
> - The device allows for adding 50,000 users.

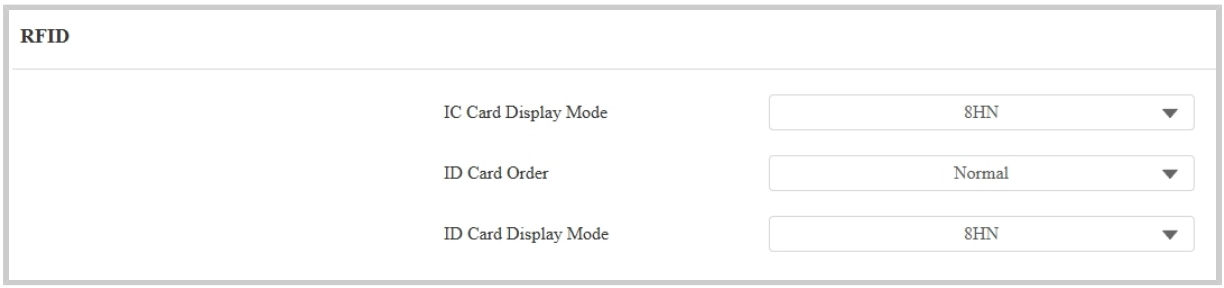
You can disable the use of cards on the **Access Control > Card Setting > Card Type Support** interface.



RF Card Code Format

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

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



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



- **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.

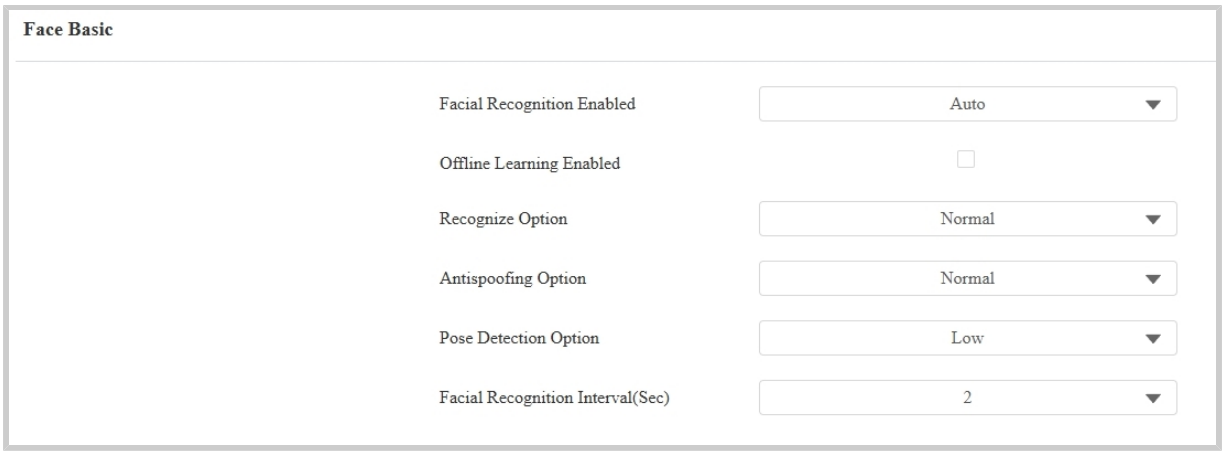


- **Photo**: Max File Size: 2M; Format: .jpg/.png/.bmp.

Facial Recognition Settings

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

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



- **Facial Recognition Enabled**:
  - **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.

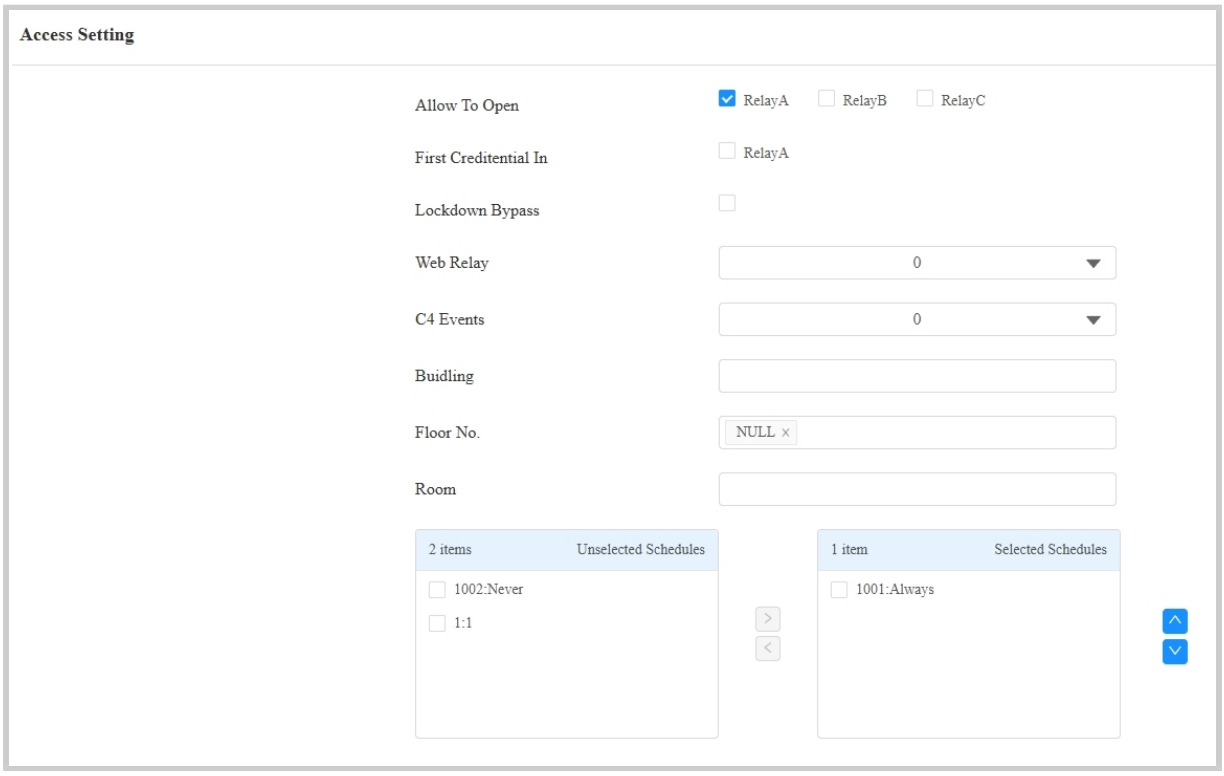
- Low: Allow slight differences from the uploaded face data, with little face coverage.
- Highest: Require the face to be identical to the uploaded one, with minimal or no covering.
- The other two levels are in between.

- **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, or High. The higher the level is, the more accurate the detection is. Users will be prompted to “please face the camera directly” when they do not face the camera.
- **Facial Recognition Interval(Sec)**: Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.

Access Setting

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

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



- **Allow To Open**: Specify the relay that can be unlocked by the user's credentials.
- **First Credential In:** This decides whether the user can keep the door open during the scheduled time after activating it.
- **Lockdown Bypass**: This decides whether the user can open the door when the door is locked during the scheduled time.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **C4 Events**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **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.

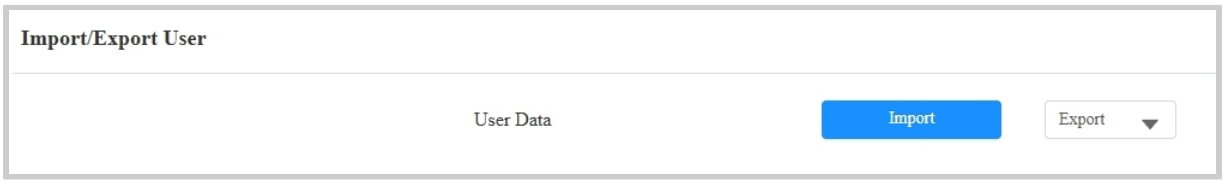
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
  - **Always**: Allows door opening without limitations on door open counts during the valid period.
  - **Never**: Prohibits door opening.

Import/Export User Data

The device supports access control user data being shared among Akuvox devices through import and export.

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

Navigate to the web **Directory > User > Import/Export User** interface. The device allows adding 50,000 users.

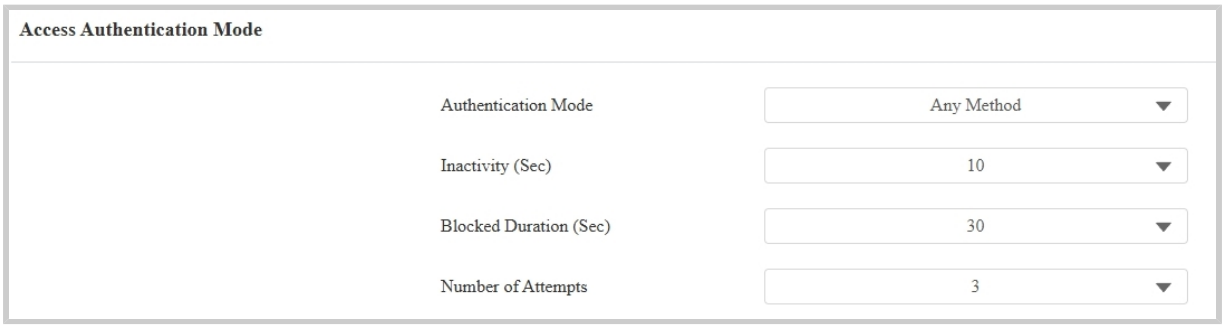


> **Note**
>
> The imported/exported file supports XML or CSV formats.

Access Authentication

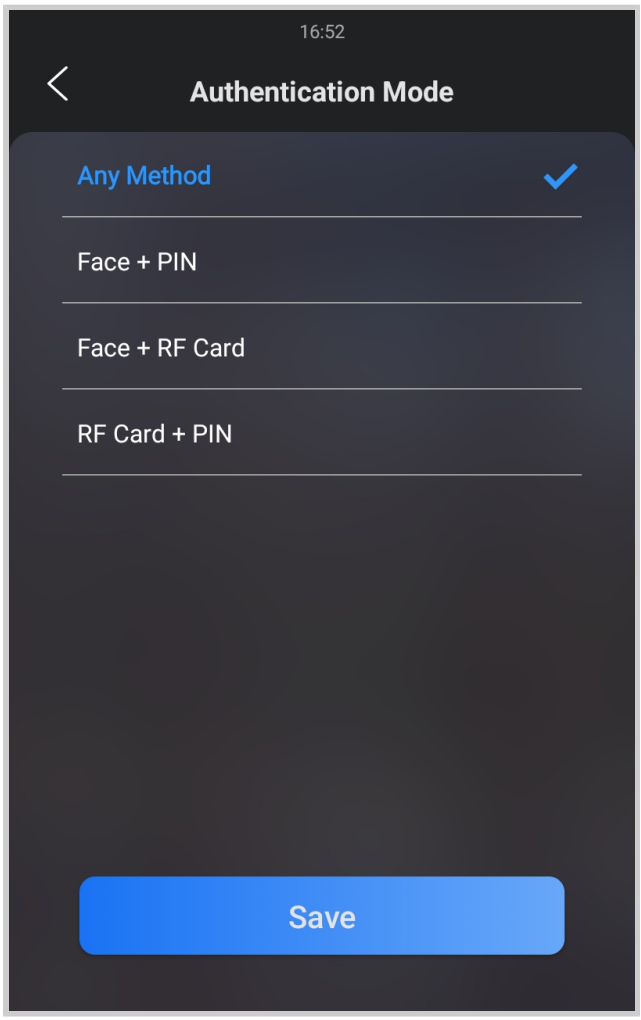
You can set up multiple access authentication modes, and set up authentication security as needed.

Set it up on the **Settings> Key/Display > Access Authentication Mode** interface. This feature applies to the **Multi-factor Authentication** theme.



- **Authentication Mode**: Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.
  - **Any Method**: Allows all access methods.
  - **Face + PIN**: Scan the face first, then enter the PIN code.
  - **Face + 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 within 10 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.

To set up authentication mode on the device, go to **Setting > Security > Authentication Mode**.



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.



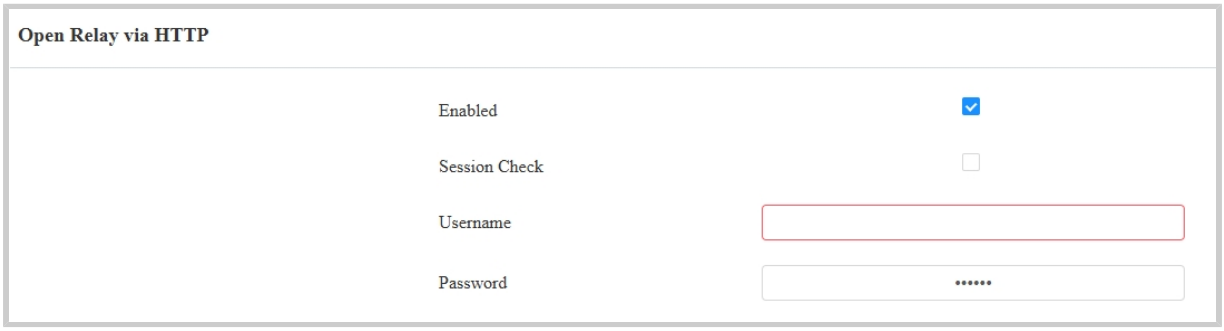
- **Enable Hands Free Mode**: If enabled, users can gain door access hands-free. If disabled, users have to wave their hands near the device to open doors.
- **RSSI Threshold**: Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Bkey Trigger Signal**: There are three ranges that determine the Bkey trigger distance, ranging from 1m to 10m.
- **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.



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

Tip

Here is an HTTP command URL example:

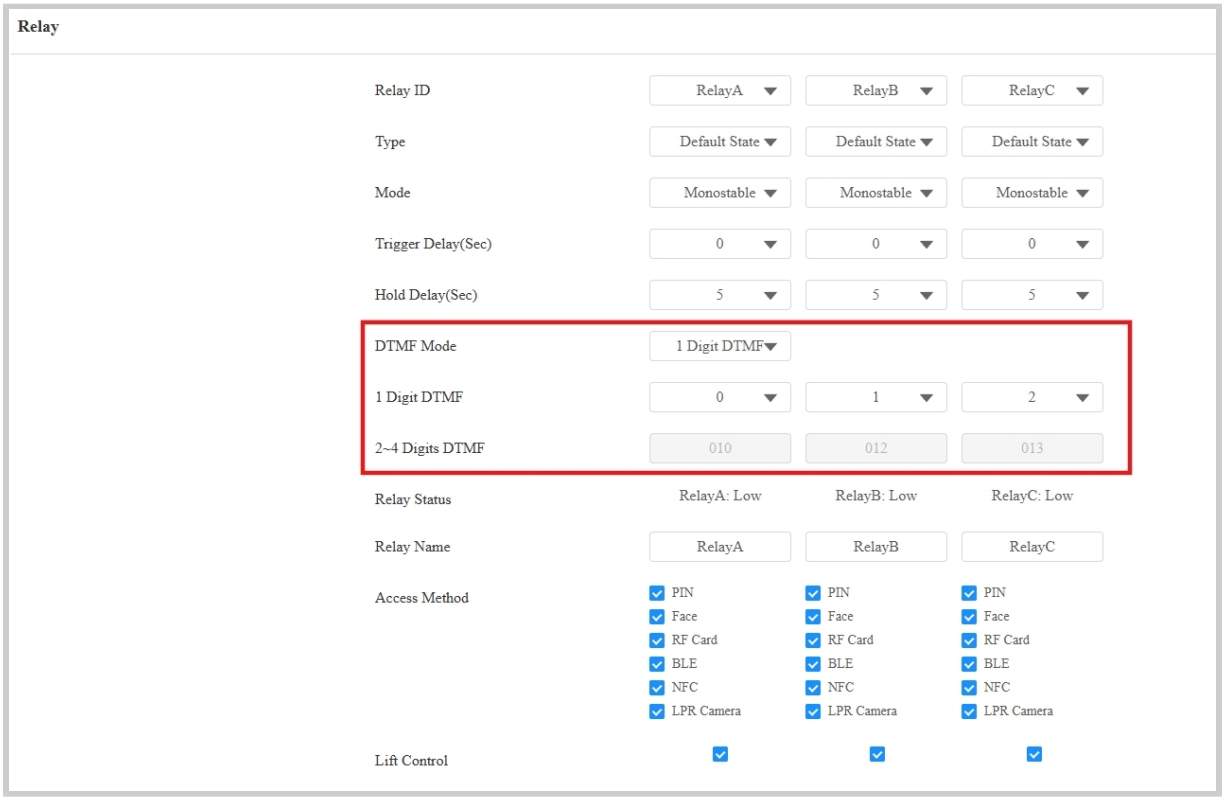


Note

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

Unlock by DTMF Code

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



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

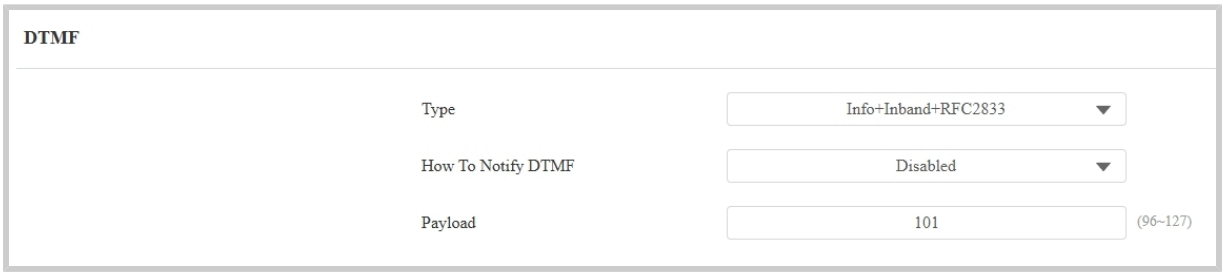
DTMF Data Transmission

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.

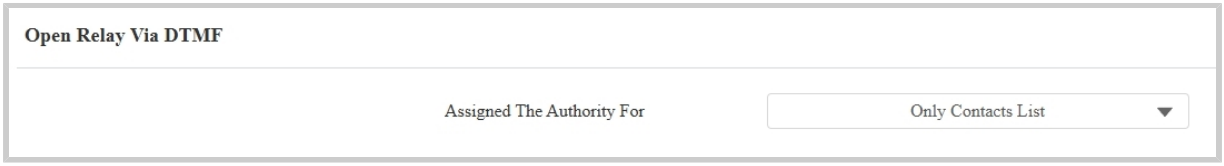


- **Type**: Select from the available options based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select Disabled, DTMF, DTMF-Relay, or Telephone-Event according to the specific type adopted by the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

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

DTMF Whitelist

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

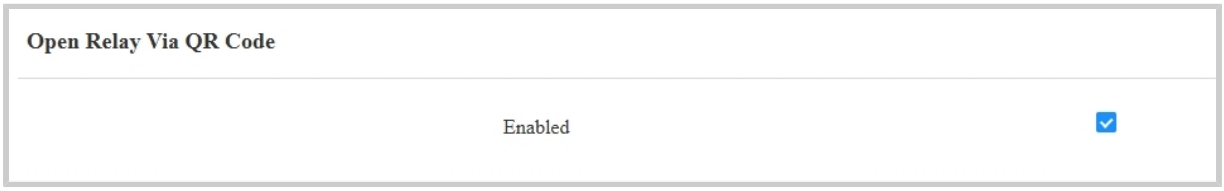


- **Assigned The Authority For**: Specify the contacts authorized to open doors via DTMF:
  - **None**: No numbers can unlock doors using DTMF.
  - **Only Contacts List**: Only numbers added to the door phone's contact list can unlock via DTMF.
  - **All Numbers**: Any numbers can unlock using DTMF.

Unlock by QR Code

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

Set it up on the **Access Control > Relay > Open Relay via QR Code** interface.



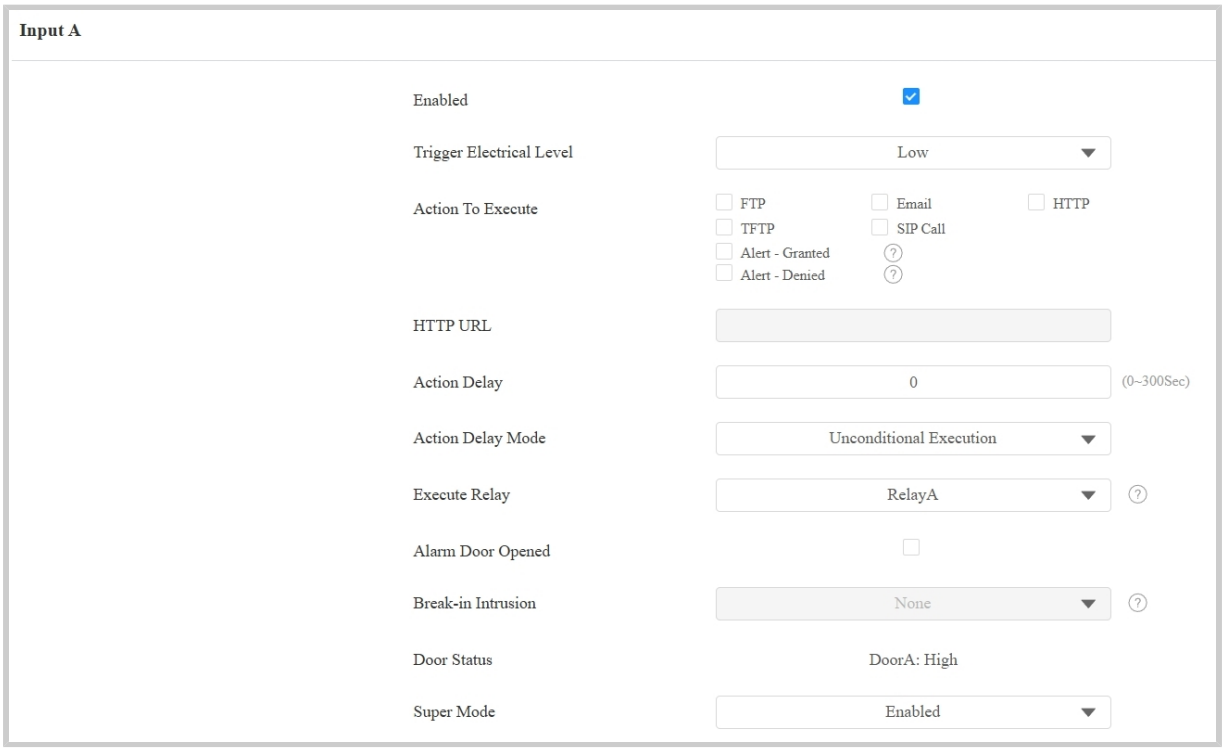
> **Note**
>
> The function should work with the Akuvox SmartPlus cloud. Please click here to view the configuration details.

Unlock by Exit Button

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

Click here to watch the instruction video.

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



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

    - **Alert-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, the 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.
- **Super Mode**: When enabled, the administrator will be able to open the door using an RF card even when the door phone breaks down or malfunctions.

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.



- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
- **DESFire**:
  - **App ID**: A 6-digit hexadecimal number
  - **File ID**: The ID of the encrypted file of the app, which can be a number from 0 to 31.
  - **Crypto**: The encryption method, either AES or DES.
  - **Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.
- **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.

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.

Enable the use of NFC and/or Felica cards on the **Access Control > Card Setting > Contactless Smart Card** interface.



Note

- The NFC feature is only for Android mobile phones.
- Click here to view how to open doors via NFC.

CEPAS Card Reading

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

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



- **CSN**: The default option. This option allows the device to read the **UID** (Unique Identifier) of the CEPAS card, which is a unique value assigned to each card.
- **CAN**: This option allows the device to read the **card number** stored on the CEPAS card, which can be used for identification or access control.

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.

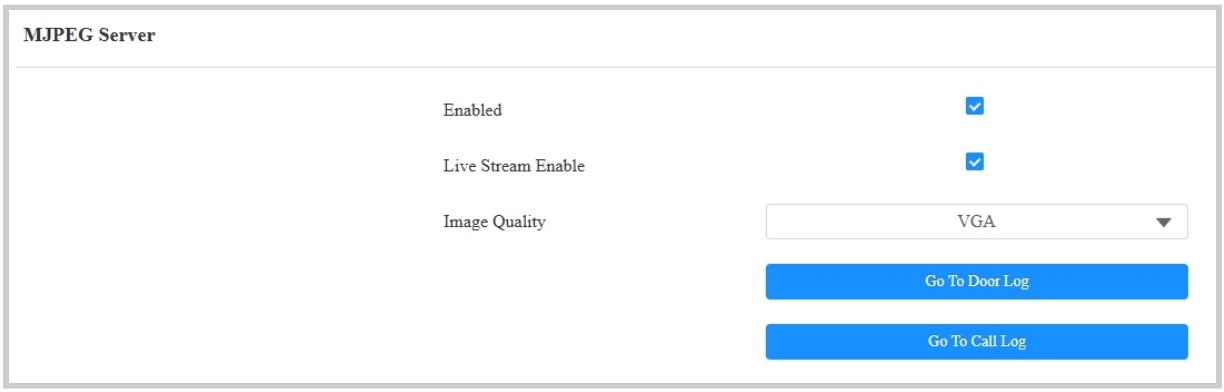
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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.

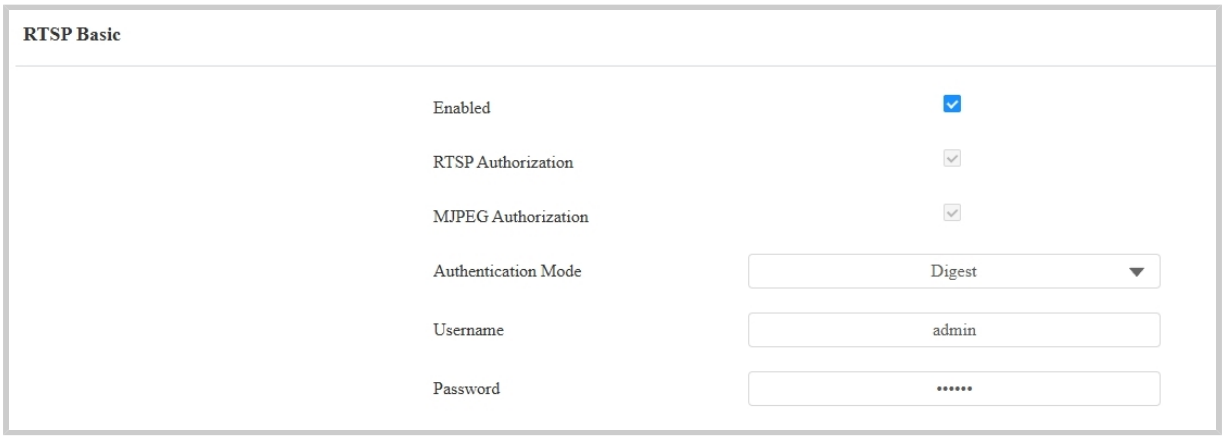


- **Live Stream Enable**: Set whether to view the video stream via URLs(*http://ip:8080/video.cgi; http://ip:8080/picture.cgi; http://ip:8080/jpeg*
  It is disabled by default.
- **Image Quality**: Specify the MJPEG image quality from the lowest QCIF(176×144 pixels) to the highest 1080P(1920×1080 pixels).
- **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.
- **Go to Call Log**: Click to redirect to the call 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.



- **MJPEG Authorization**: 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 in the web browser.

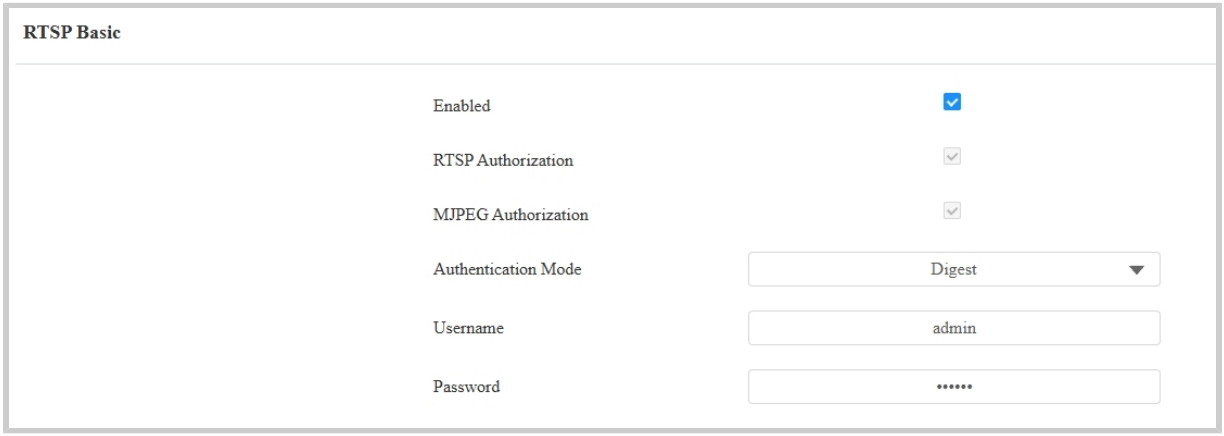
RTSP Stream Monitoring

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

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

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.

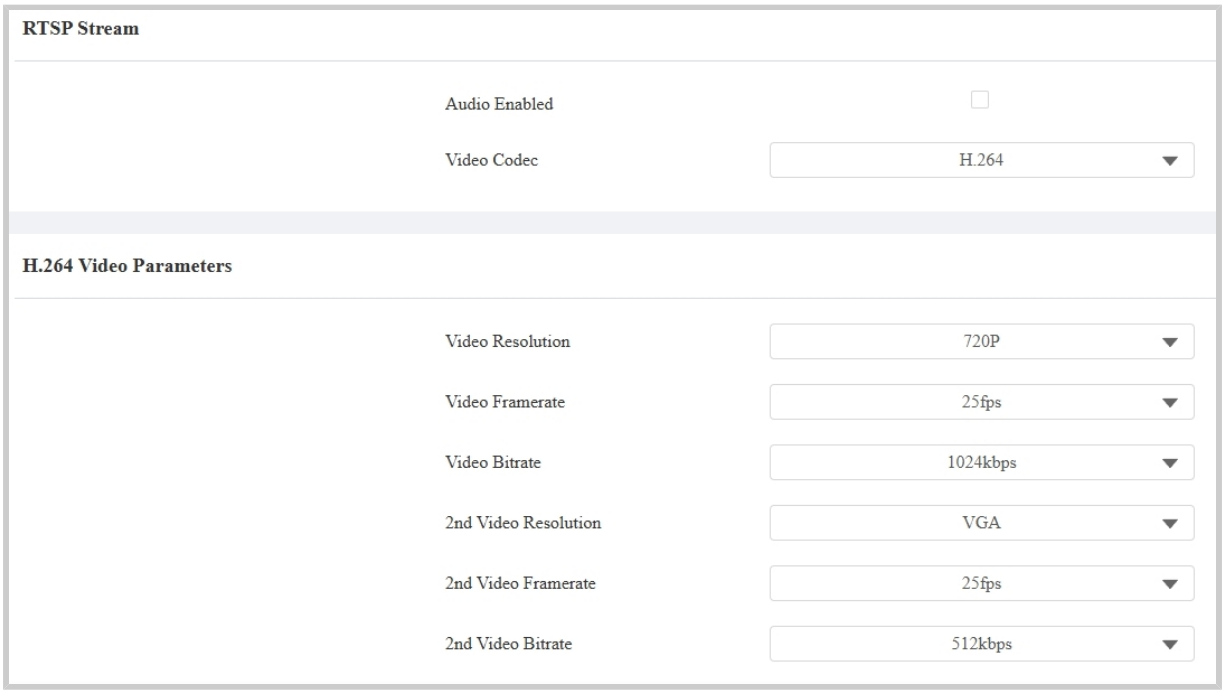


- **RTSP Authorization**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: Select between Basic and Digest. It is Digest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

RTSP Stream Setting

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

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



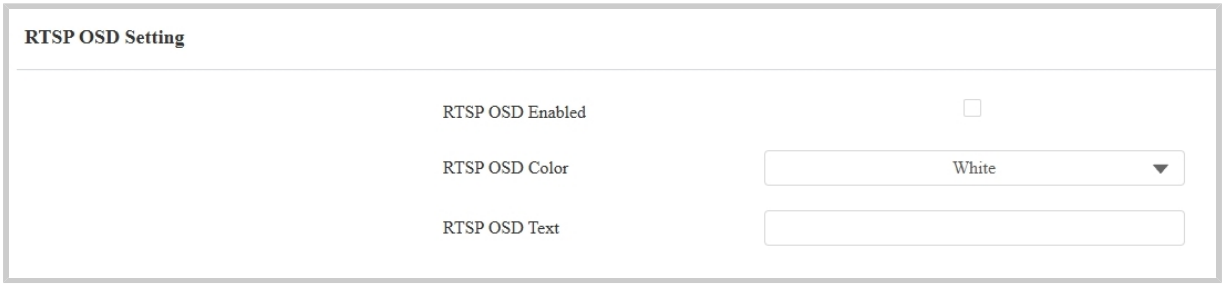
- **Audio Enabled**: When enabled, the device will send the audio stream with the video to the monitor via RTSP.
- **Video Resolution**: Specify the image resolution, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Video Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **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 720P.
- **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 2048 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. To protect the owner of the video or image.

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



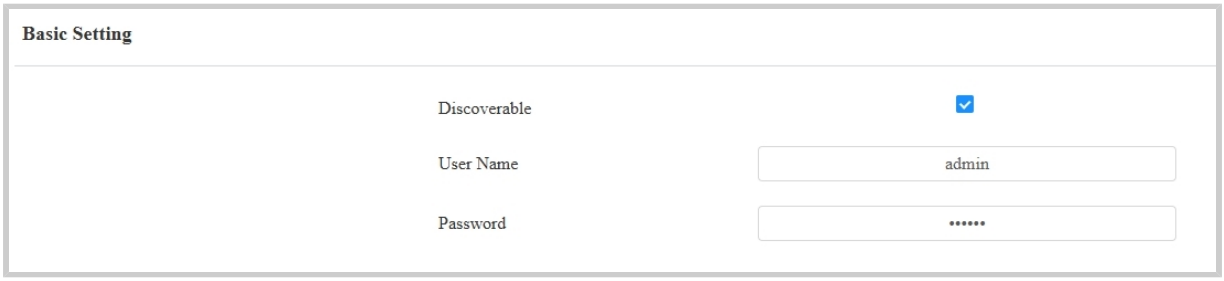
- **RTSP OSD Color**: Select the color from White, Black, Red, Green, or Blue.
- **RTSP OSD Text**: Customize the OSD content.

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.



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

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

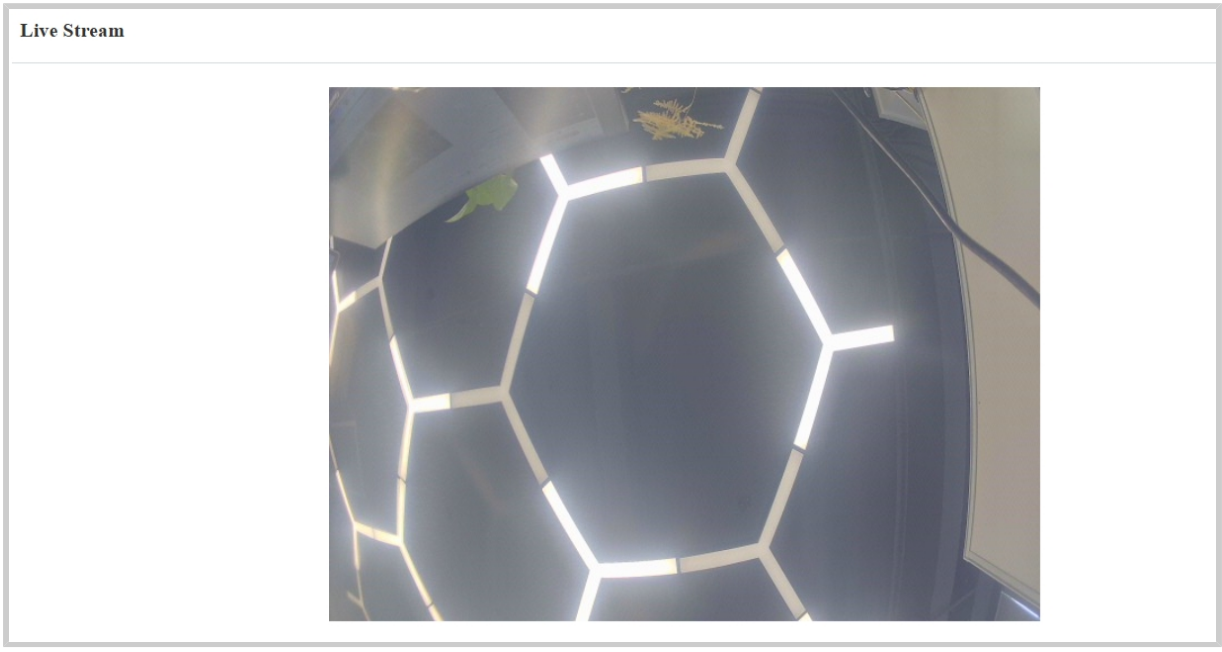
Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.



Live Stream

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

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 in the MJPEG Authorization section.



Data Transmission Type for Third-party Camera

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

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



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

Security

Tamper Alarm

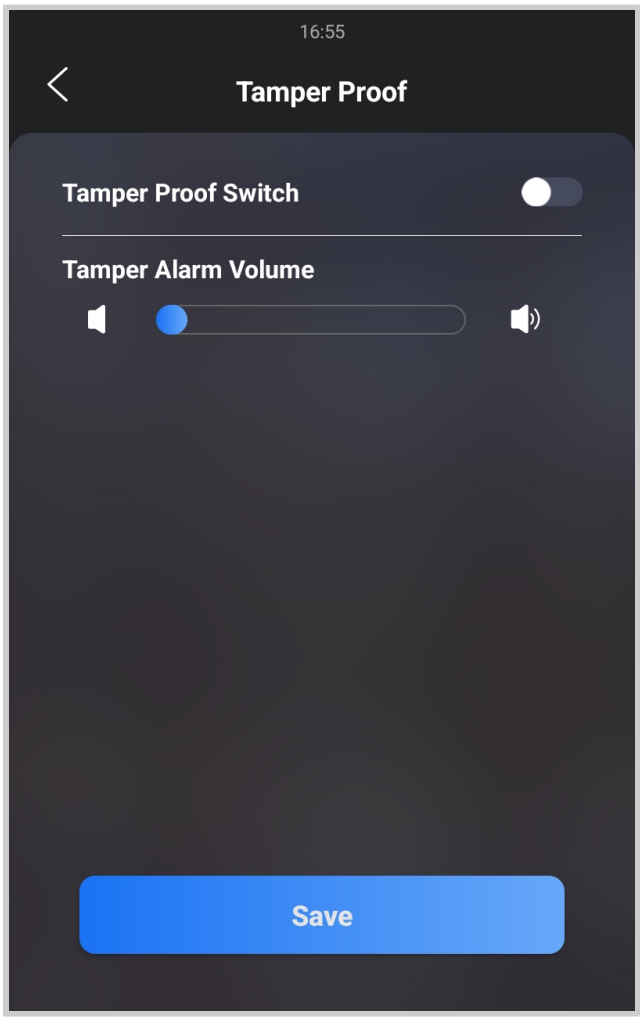
The tamper alarm function prevents anyone from removing the device without permission. Akuvox devices support two types of tamper proof: gravity detection and button status detection.

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

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



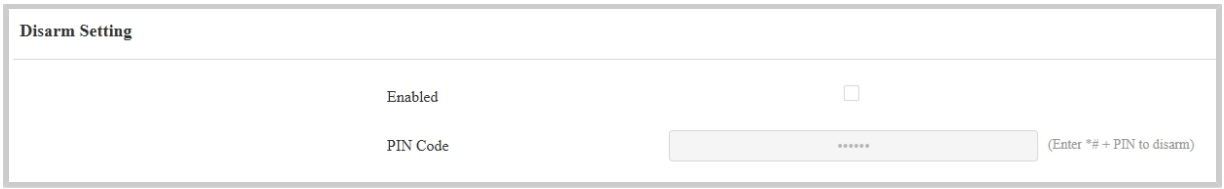
You can also set up the tamper alarm on the **Setting > Security > Tamper Proof** screen.



Disarm Setting

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

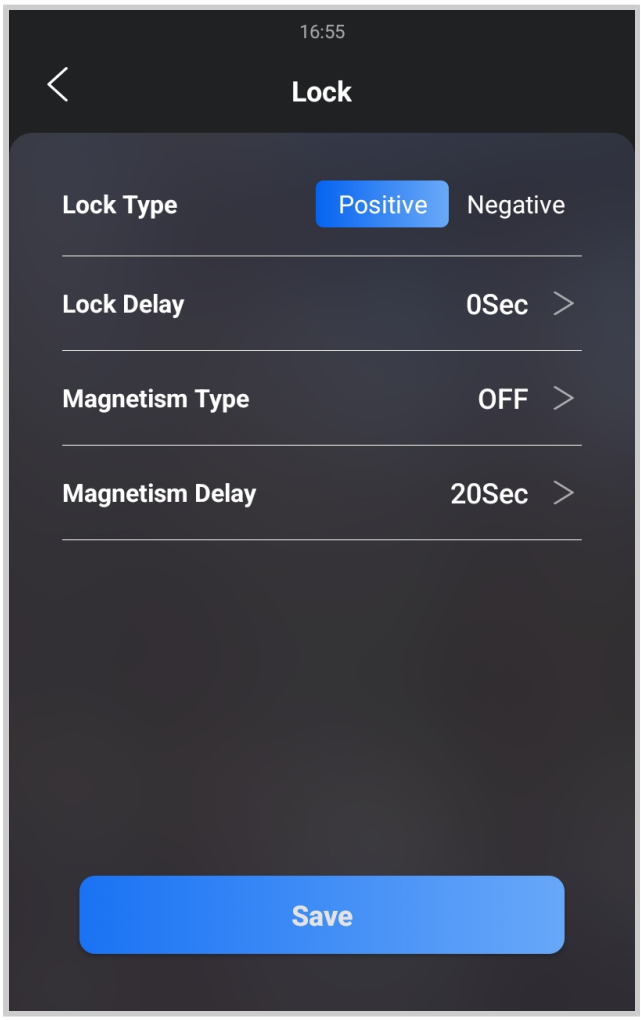
Set it up on the **System > Security > Disarm Setting** interface.



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.


16:55
Lock
Lock Type
Positive
Negative
Lock Delay
0Sec
Magnetism Type
OFF
Magnetism Delay
20Sec
Save



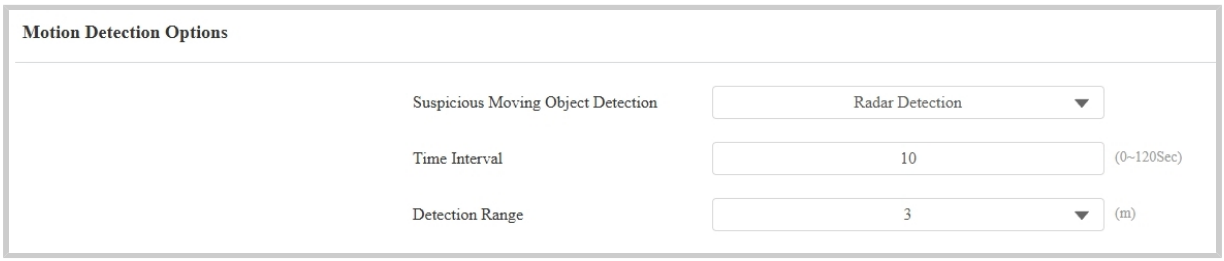
- **Lock Type**:
  - **Positive**: The lock unlocks when power is ON and locks when power is OFF. Suitable for scenarios where the door should remain locked during a power outage.
  - **Negative**: The lock unlocks when power is OFF and locks when power is ON. Commonly used in places like fire escapes 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 you 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 it is triggered. The delay range is from 10-120 seconds.

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.

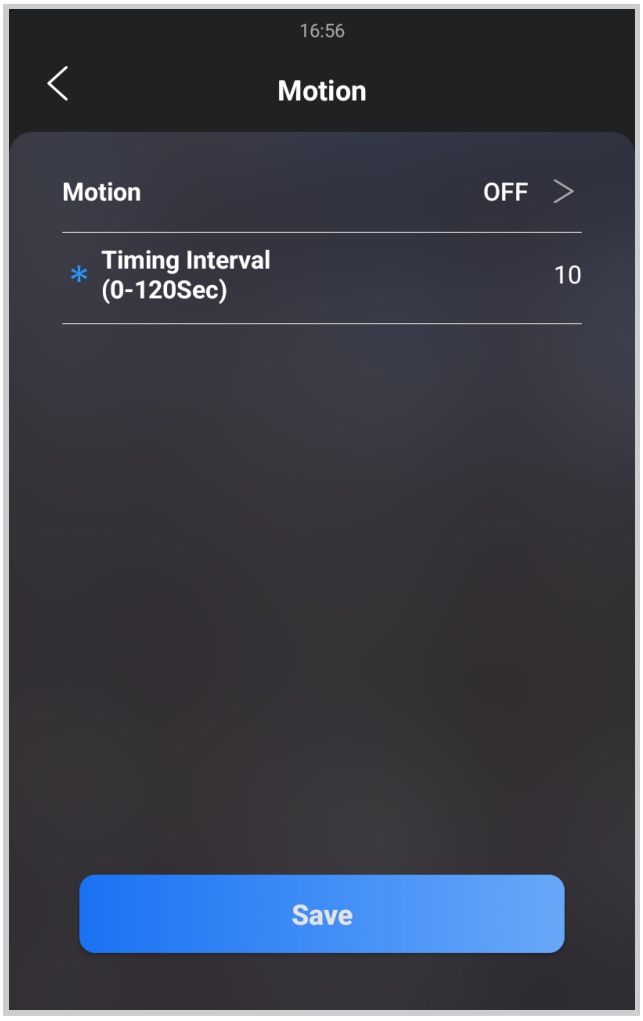
Set it up on the web **Surveillance > Motion > Motion Detection Options** interface.



- **Suspicious Moving Object Detection**:
  - **Disabled**: Turn off the motion detection function.
  - **Video Detection**: When the video camera detects moving objects, preset actions will be triggered. Focus on analyzing visual information captured through cameras.
  - **Radar Detection**: When the radar detects moving objects, preset actions will be triggered. It offers longer range and better detection in poor visibility conditions.
  - **Video + Radar**: Detect motion with the combination of the video camera and radar.
- **Timing Interval**: Determine how to delay and trigger motion detection.
  - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.

  - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
  - The default interval is 10 seconds.
- **Detection Range**: After enabling radar detection, you can select the detection range among 1, 2, and 3 meters.
- **Detection Accuracy**: The detection sensitivity. Specify this option when selecting Video Detection. The greater the value is, the more accurate the detection is. The default value is 3.
- **Detection Area**: Click and hold down the mouse button to select up to three detection areas.

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



Motion Detection Triggered Actions

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



- **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*.
- **Execute Relay**: The relay to be triggered.

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



Security Notification

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

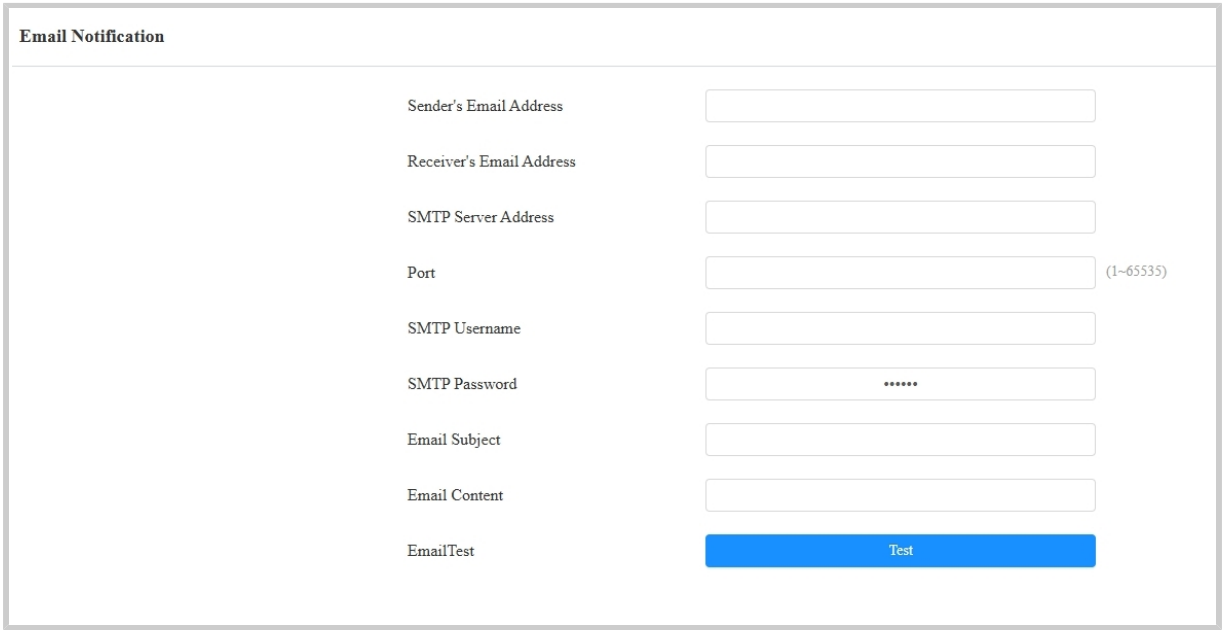
Set up notifications on the **Setting > Action** interface.

Email Notification

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

Click here to view how to set this feature up.

Find the **Email Notification** section.



- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP Username**: 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 the FTP server, you need to set up the FTP settings. The device will upload a screenshot to the specified FTP folder if it detects any unusual motion.

Click here to view the configuration steps.

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



- **FTP Server**: Set the address (URL) of the FTP server.
- **FTP Username**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.
- **FTP Path**: The folder name you created in 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.

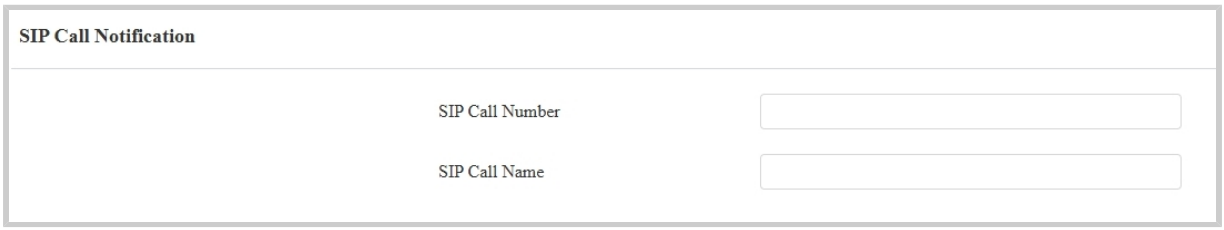
Set it up on the **TFTP Notification** section.



SIP Call Notification

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

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



Action URL

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

Akuvox Action URL:

Event	Parameter format	Example
Make Call	$remote	Http://server ip/Callnumber=$remote
Hang Up	$remote	Http://server ip/Callnumber=$remote
Relay Triggered	$relay1status	Http://server ip/relaytrigger=$relay1status
Relay Closed	$relay1status	Http://server ip/relayclose=$relay1status

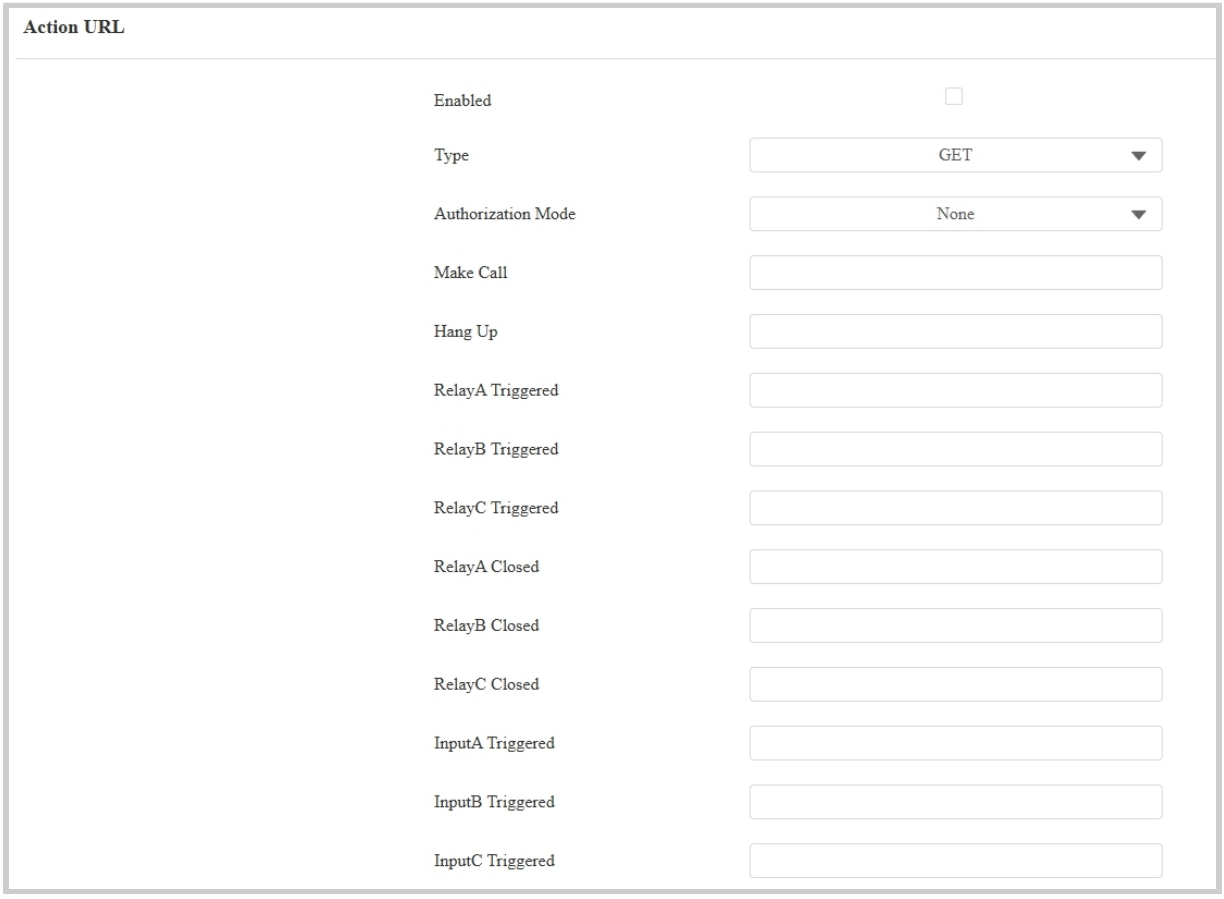
Input Triggered	$input1status	Http://server ip/inputtrigger=$input1status
Input Closed	$input1status	Http://server ip/inputclose=$input1status
Valid Code Entered	$code	Http://server ip/validcode=$code
Invalid Code Entered	$code	Http://server ip/invalidcode=$code
Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
Invalid Card Entered	$card_sn	Http://server ip/invalidcard=$card_sn
Facial Recognition	$unlocktype	Http://serverip/unlocktype=$unlocktype
QR Code	$unlocktype	Http://serverip/unlocktype=$unlocktype
Break-in Alarm	$inputstatus	Http://server ip/inputtrigger=$input1status **NOTE**: $input1-3status corresponds to Input A-C.

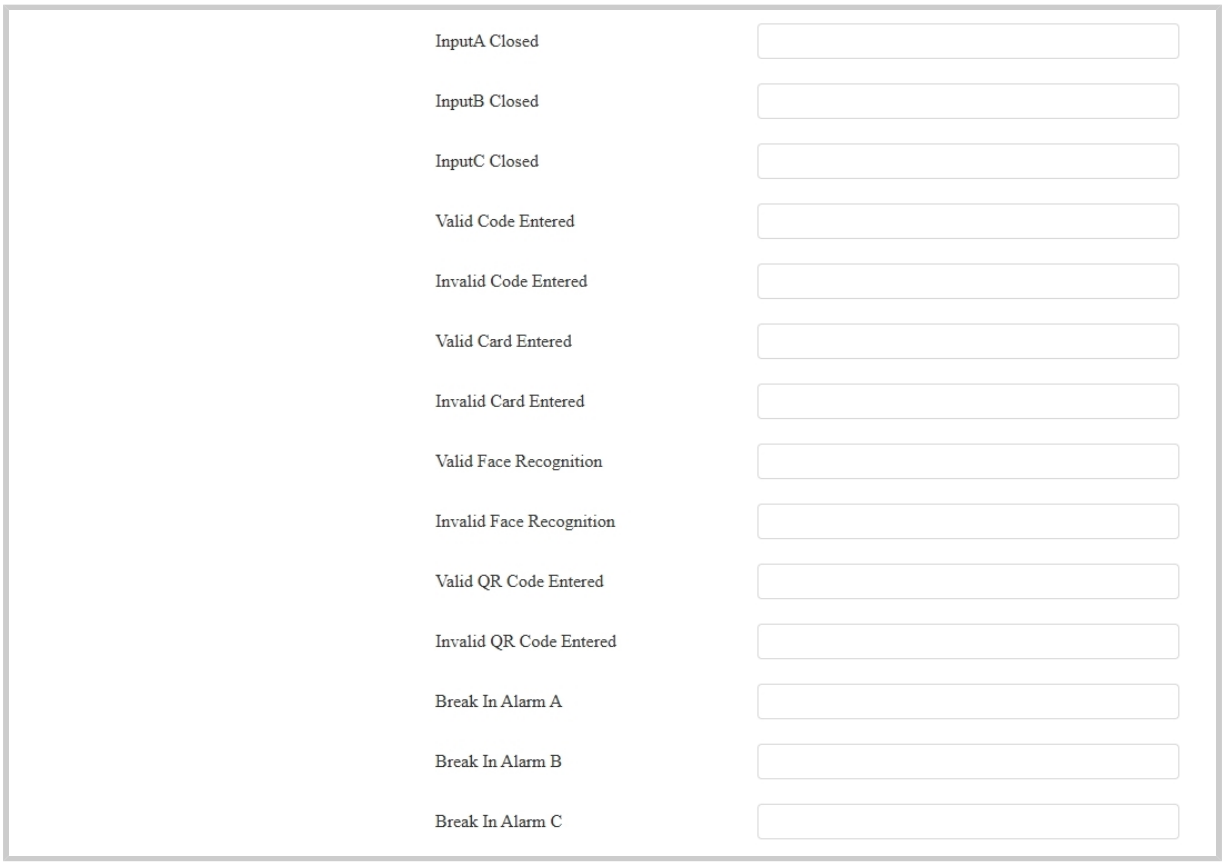
For example: http://192.168.16.118/help.xml? mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

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

Note

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





- **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.

Voice Encryption

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

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



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

User Agent

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

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



Web Interface Automatic Log-out

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

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



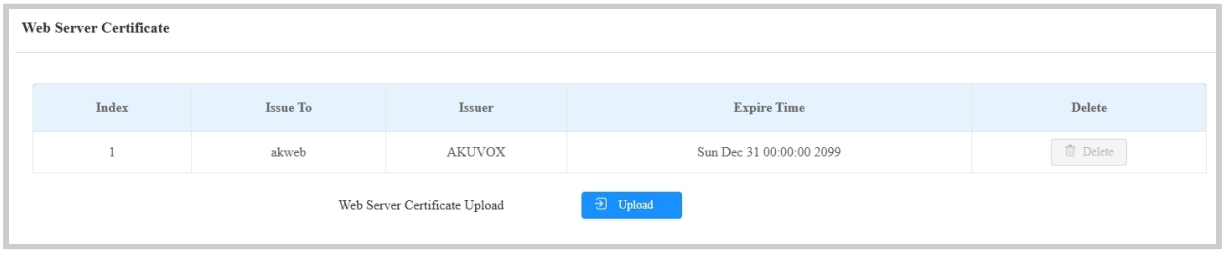
Client Certificate Setting

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.

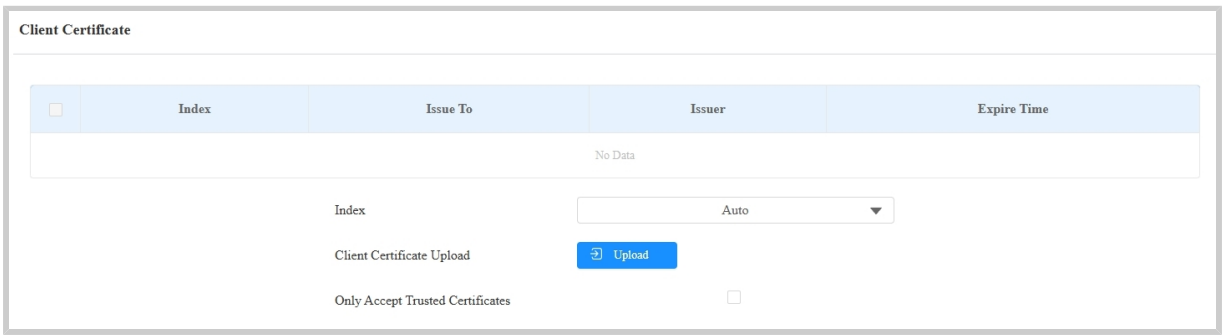
Upload a web server certificate on the **System > Certificate > Web Server Certificate** interface.



Client Certificate

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

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



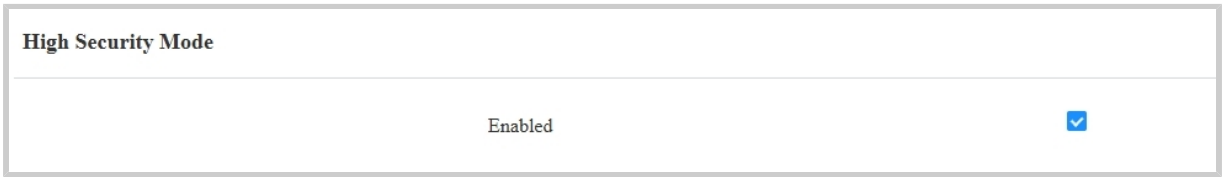
- **Index**: Select the desired value from the drop-down list of Index. If you select Auto, the uploaded certificate will be displayed in numeric order. If you select a value from 1 to 10, the uploaded certificate will be displayed according to the number.

- **Client Certificate Upload**: Locate and upload the desired certificate (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.

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.



Important Notes

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

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

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

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

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

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

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

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

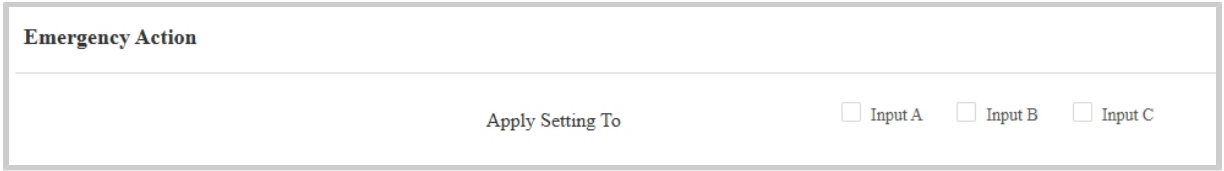
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Emergency Action

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

Click here to view the detailed configuration of this feature.

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



Real-time Monitoring

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

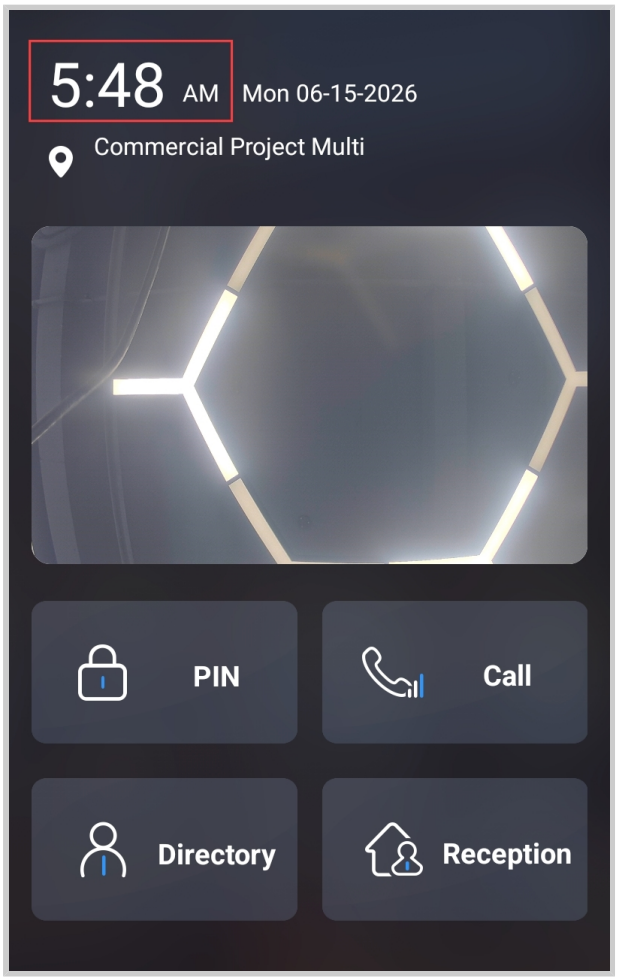
Click here to see the detailed configuration.

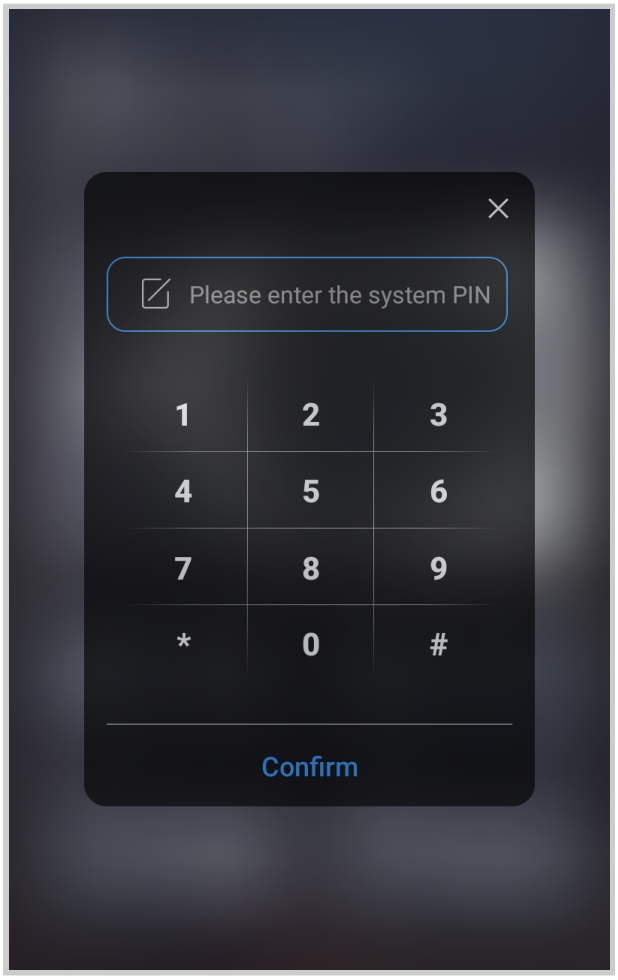
Set it up on the **System > Security > Real-time Monitoring** interface.



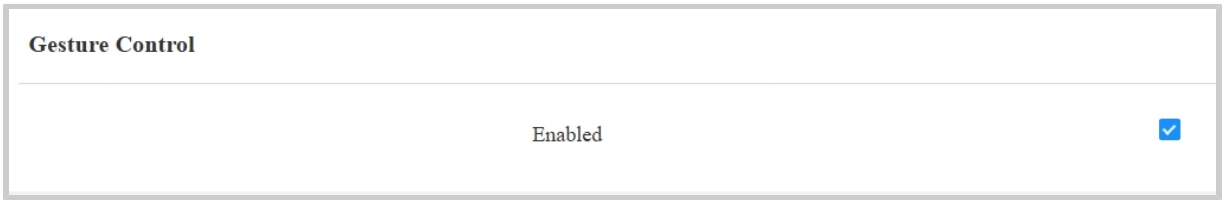
Gesture Control Setting

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.


5:48 AM
Mon 06-15-2026
Commercial Project Multi
PIN
Call
Directory
Reception



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



Note

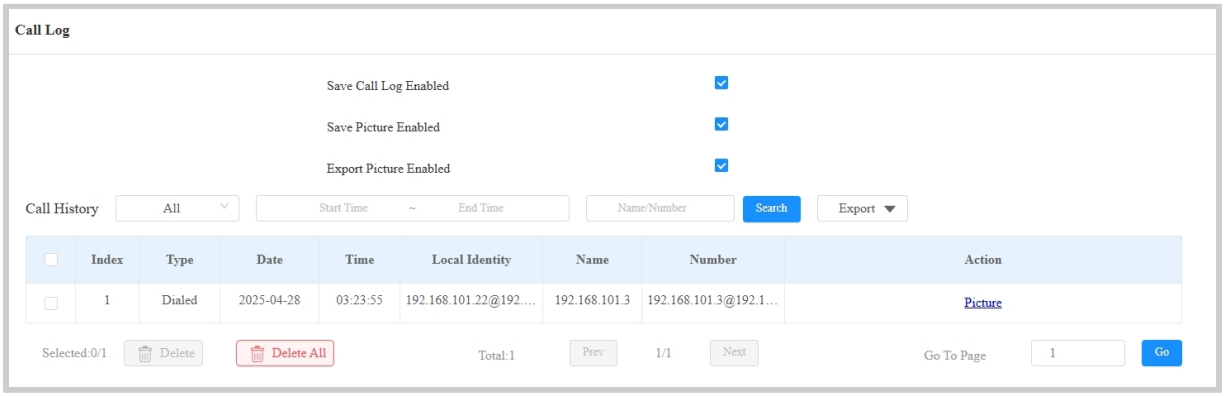
See the theme configuration in the Screen Display chapter.

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 logs can be exported in CSV format.

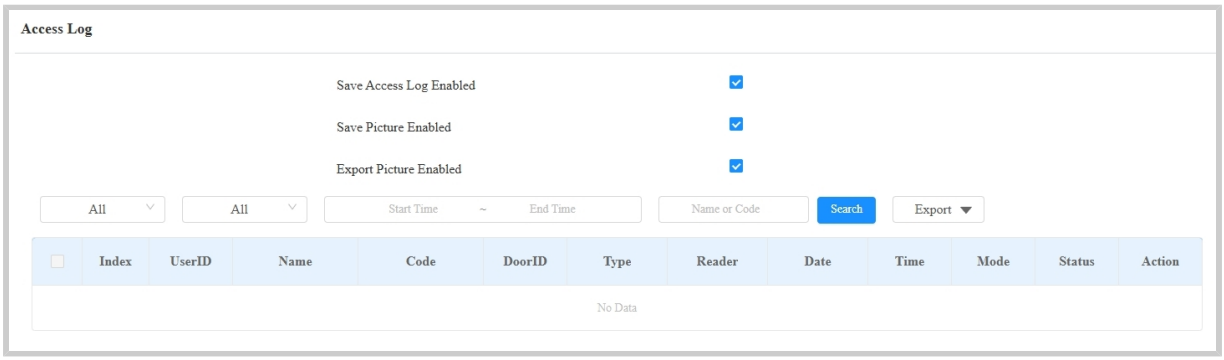


- **Call History**: Four types of call history are available: All, Dialed, Received, and Missed.
- **Time**: The specific time of the call logs you want to search, check, or export.
- **Name/Number**: Search the call log by the name or by the SIP or IP number.
- **Save Picture Enabled**: When enabled, the device will capture pictures of calls, and you can click **Picture** in the Action column to view the snapshot.

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. The logs can be exported in XML or CSV format.



- **Save Picture Enabled**: When enabled, the device will capture pictures of door-opening, and you can click Picture in the Action column to view the snapshot.
- **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.

The supported number of door logs stored and exported varies by image resolution. As the resolution increases, the number of logs that can be exported decreases.

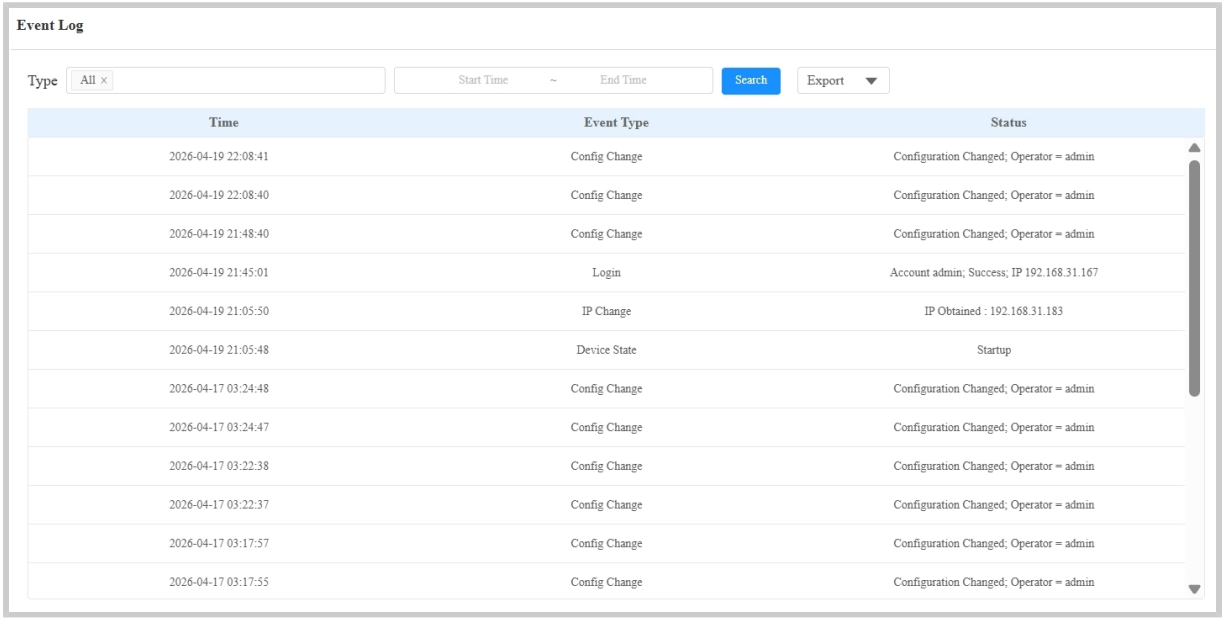
Resolution	Maximum Number of Stored Door Logs
Null, Save Picture is disabled.	15,000
QCIF	15,000
QVGA	15,000
CIF	15,000

Resolution	Maximum Number of Stored Door Logs
VGA	15,000
4CIF	10,000
720P	5,000
1080P	2,500
2K	1,250

Event Logs

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

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

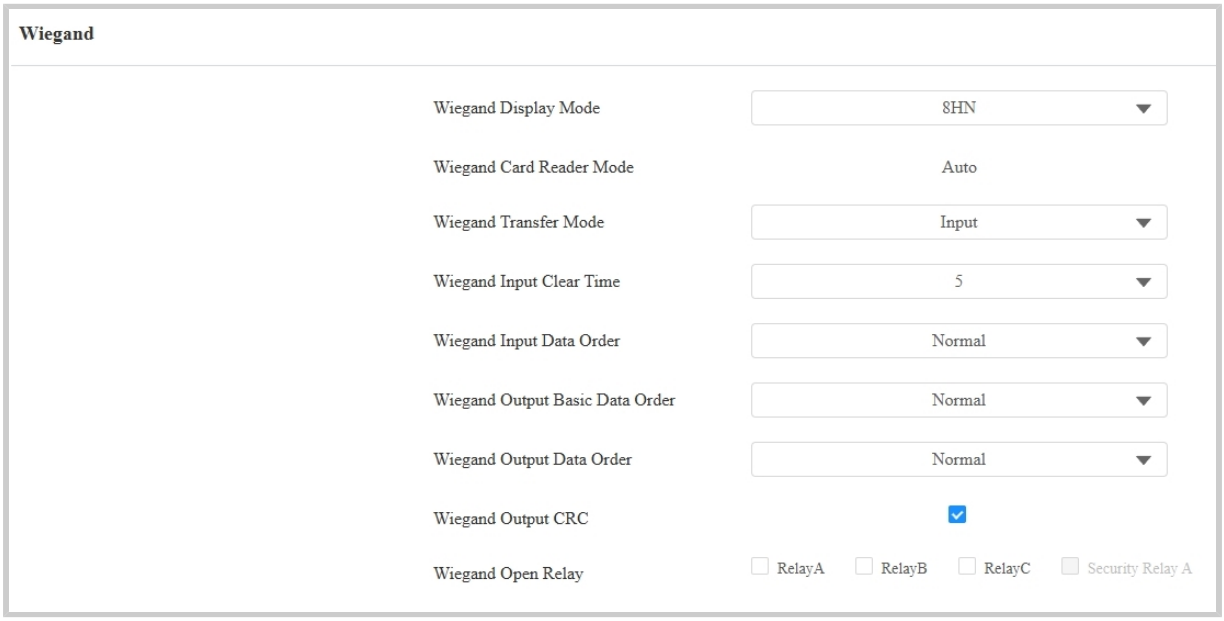


Integration with Third-party Devices

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 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 when Input is selected as the Wiegand Transfer Mode.
- **IC Card Reading Order**: This option only works when the Wiegand Transfer Mode is **Output** and **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. If users can only open the door by swiping an RF card, select the Wiegand transfer mode as Output.
  - **Convert To Card No. Output**: The device serves as a sender. If users are assigned multiple door-opening methods, select the Wiegand transfer mode as Convert To Card No. Output.
- **Wiegand Input 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**: If enabled, the door phone will conduct the RF card verification. It is not suggested to enable the feature when the door phone just serves as the signal sender while the third-party device controls door opening.

- **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.

Facility Code Setting

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

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



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

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

Wiegand Virtual Door Mode

This feature determines which relay to open when a credential is read from a Wiegand device.

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



- **Enabled**: It is enabled by default.
  - When enabled, the door phone gives priority to the relay(s) configured in **Wiegand Open Relay**.

When a user presents their credentials via Wiegand, the door phone will open the relay(s) defined in the **Wiegand Open Relay**.
If no relay is configured, the door phone will open the relay(s) assigned to the user.

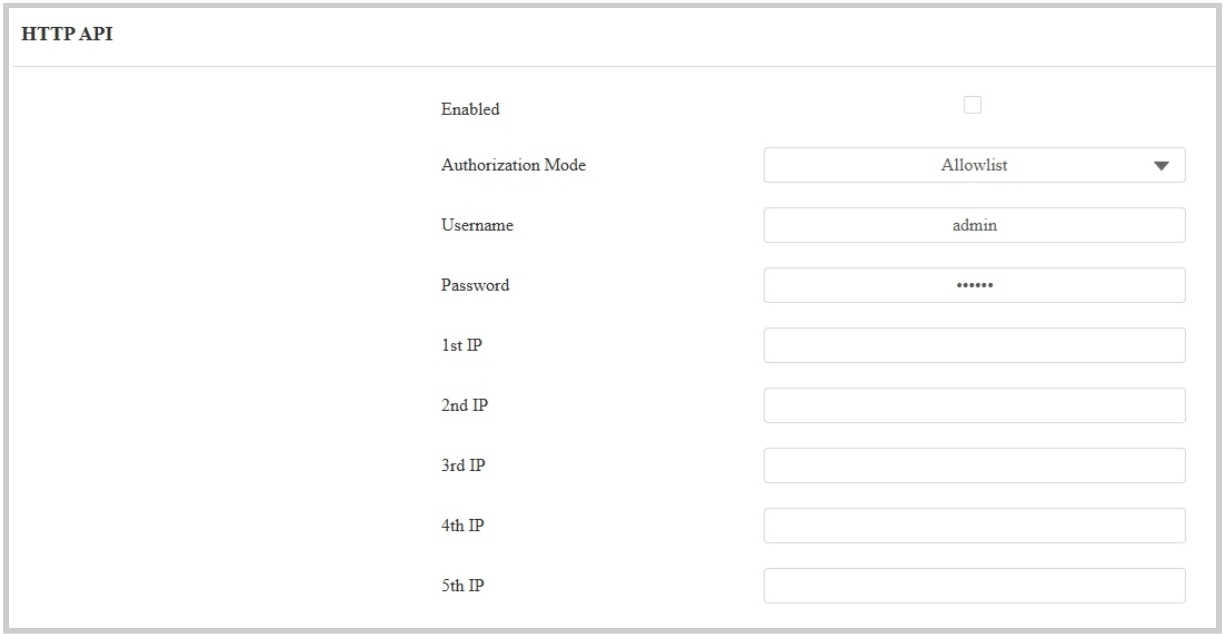
- When disabled, a relay will open only if it is allowed both in the **Wiegand Open Relay** and in the user's relay permissions.

> **Note**
>
> If two-factor authentication methods are used and one of them comes from a Wiegand device, the door phone will follow the relay opening rules set in the Wiegand settings.

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.



- **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, and Digest for authorization type, which will be explained in detail in the following chart.
- **Username**: Enter the user name when **Basic** or **Digest** authorization mode is selected. The default username is admin.
- **Password**: Enter the password when **Basic** or **Digest** authorization mode is selected. The default password is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

Please refer to the following description for the authentication mode:

Authorization Mode	Description
None	No authentication is required for HTTP API as it is only used for demo testing.
Normal	This mode is used by Akuvox developers only.
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.
Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode the username and password.

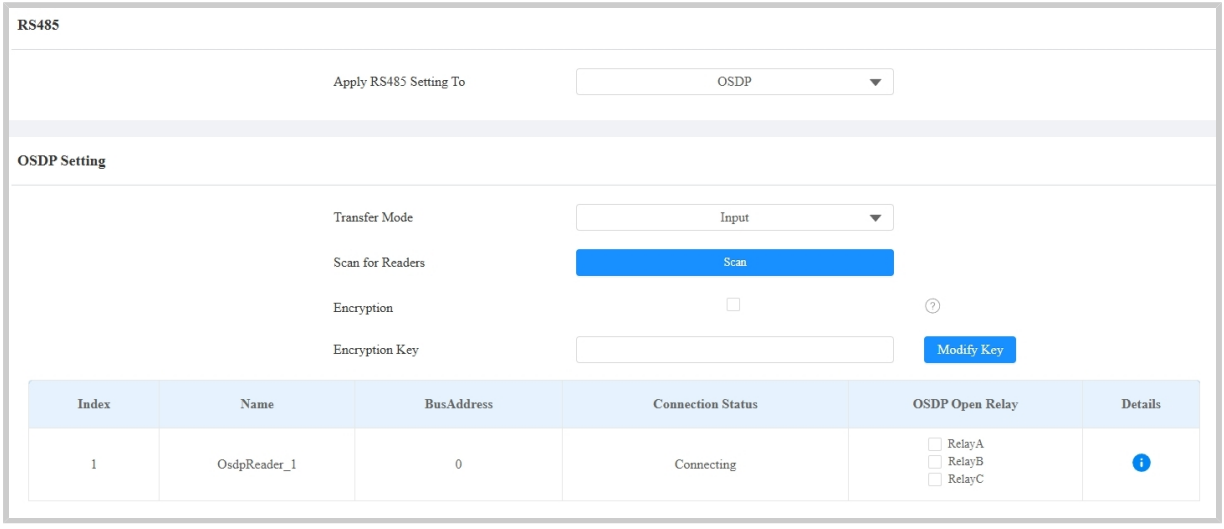
Authorization Mode	Description
Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".

Integration via RS485

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

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

To set it up, go to the **Device > RS485** interface.



- **Apply RS485 Setting To**:
  - **Disabled**: The RS485 function is disabled.
  - **Security Relay**: The default option. Select it when the device works with the security relay(SR01).

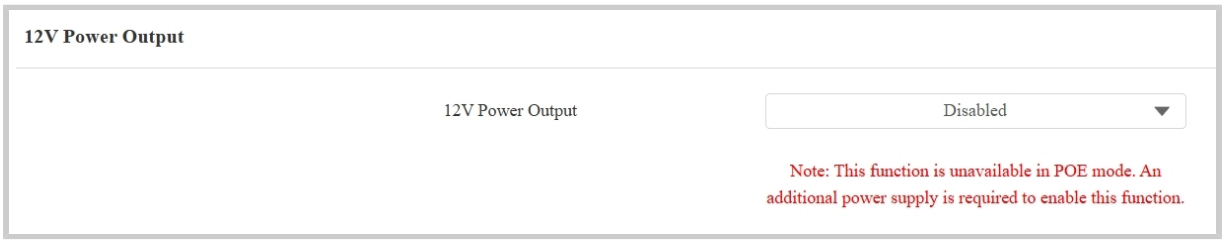
  - **OSDP**: The device is connected to an OSDP-based external device, such as a card reader.
- **Transfer Mode**: Select the RS485 working mode, **Output**, or **Input**.
  When **Output** is selected, configure the following options:
  - **Local Relay Verification**: Set whether to carry out the access credentials verification. When unchecked, door-opening failure prompts will not be given.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **Encryption Key**: 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. It must be 32 bits long and can include numbers (0-9) and letters (a-f, A-F).

  When **Input** is selected, configure the following options:
  - **Scan for Readers**: Click **Scan** to detect the connected card reader.
  - **Encryption**: Check this option when the OSDP protocol is encrypted.
  - **Encryption Key**: Fill in the key when **Encryption** is checked. If the output device is a third-party card reader, please confirm the key with the service provider.
  - **Modify Key**: Click to modify the encryption key, which must be 32 bits long and can include numbers (0-9) and letters (a-f, A-F).
  - **Connection Status**: Display whether the reader is online and connected properly.
  - **OSDP Open Relay**: Check the door to be opened.
  - **Details**: Click to view the card reader's information.

Power Output Control

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

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

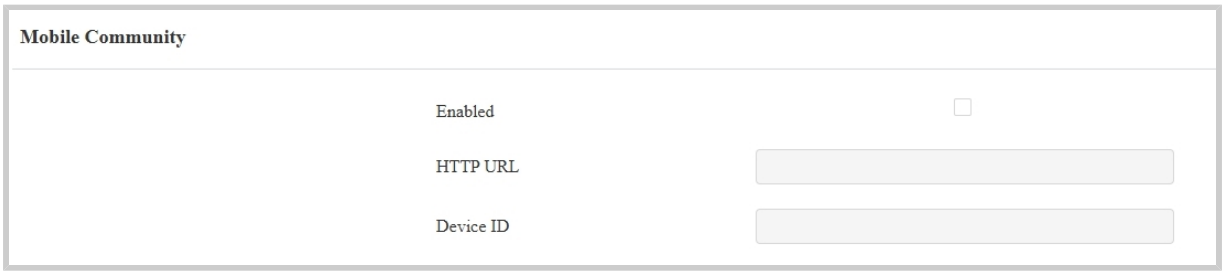


- **12V Power Output**:
  - **Disabled**: Disable the power output function.
  - **Always**: Provide continuous power to the third-party device.
  - **Triggered By Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.
    - **Time Out (Sec)**: Select the power supply time duration after the relay is triggered from 3, 5, and 10 seconds. It is 3 seconds by default. The power output is 12V, and the maximum output amperage is 0.8A.

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.



- **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 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 the switch on the **Device > Control4** interface.



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

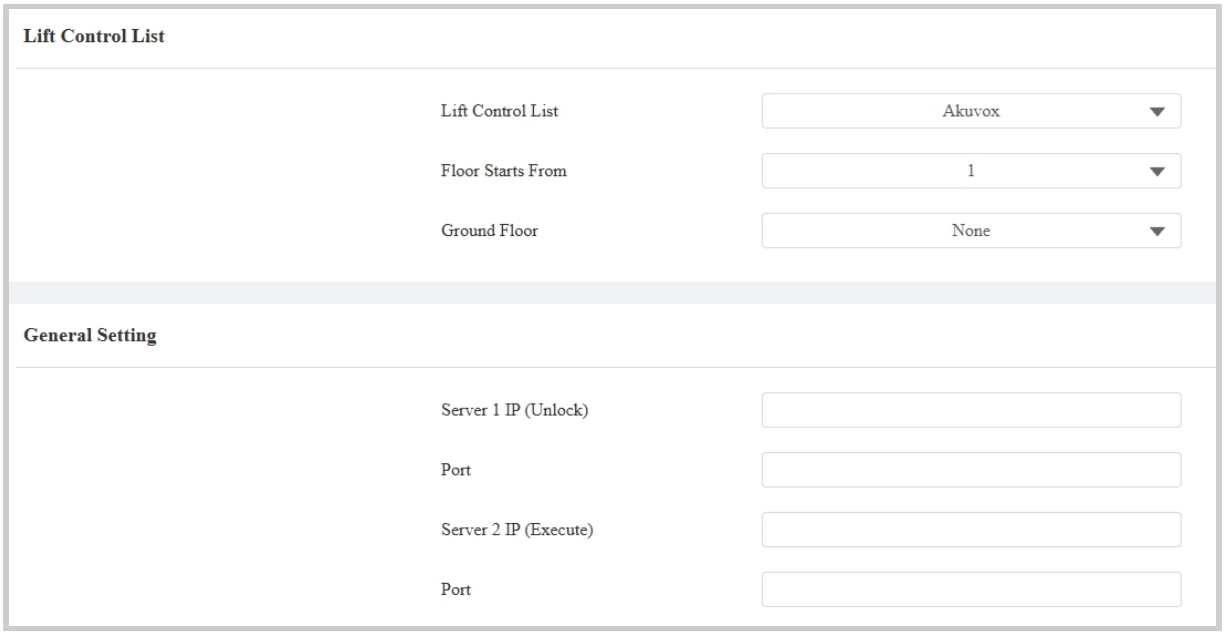
Lift Control

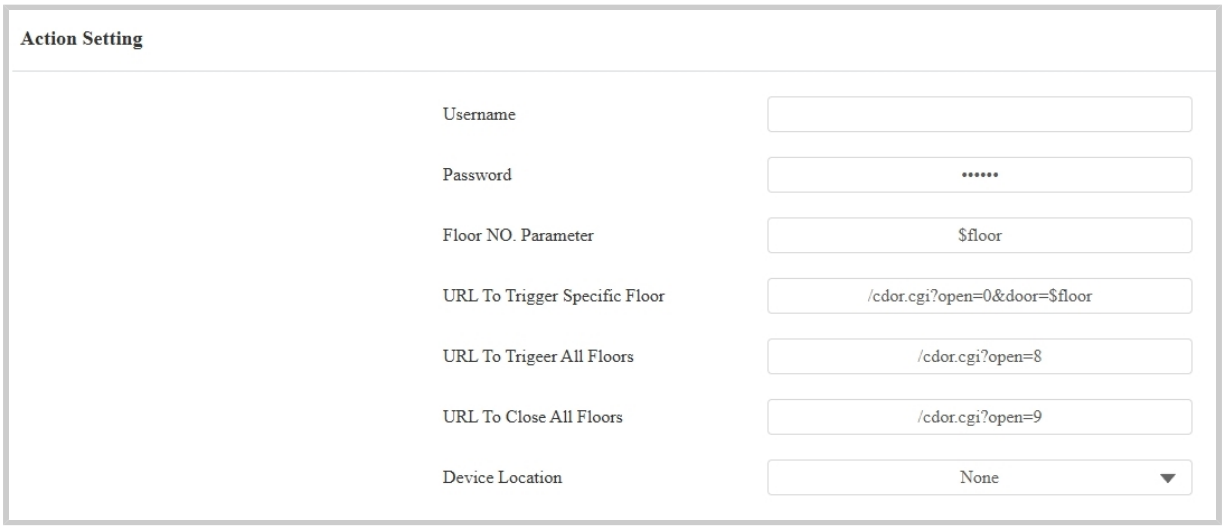
Akuvox Lift Controller

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 **Device > Lift Control** interface.





- **Lift Control List**: Select None to disable the function, and select Akuvox to integrate the door phone with the Akuvox controller.
- **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 Akuvox lift control server. It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute):** The IP address of the server that triggers lift control.
- **Port:** The server port of the lift controller server.
- **Username**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.

- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **Device Location**: Select the floor where the device is installed.

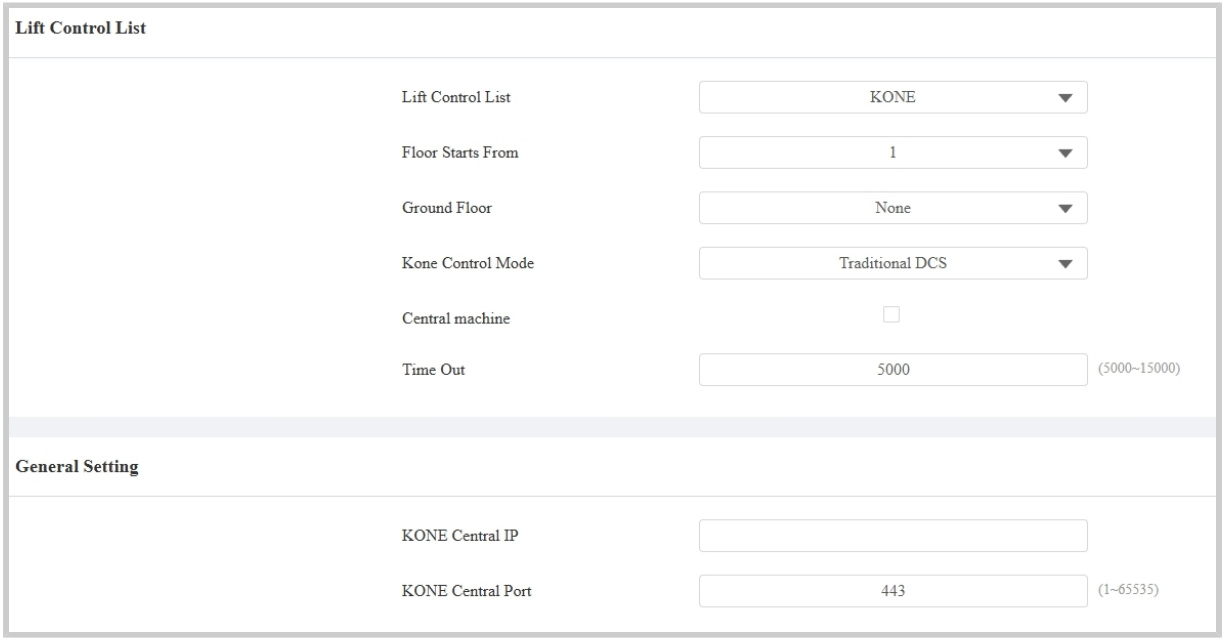
KONE Lift Controller

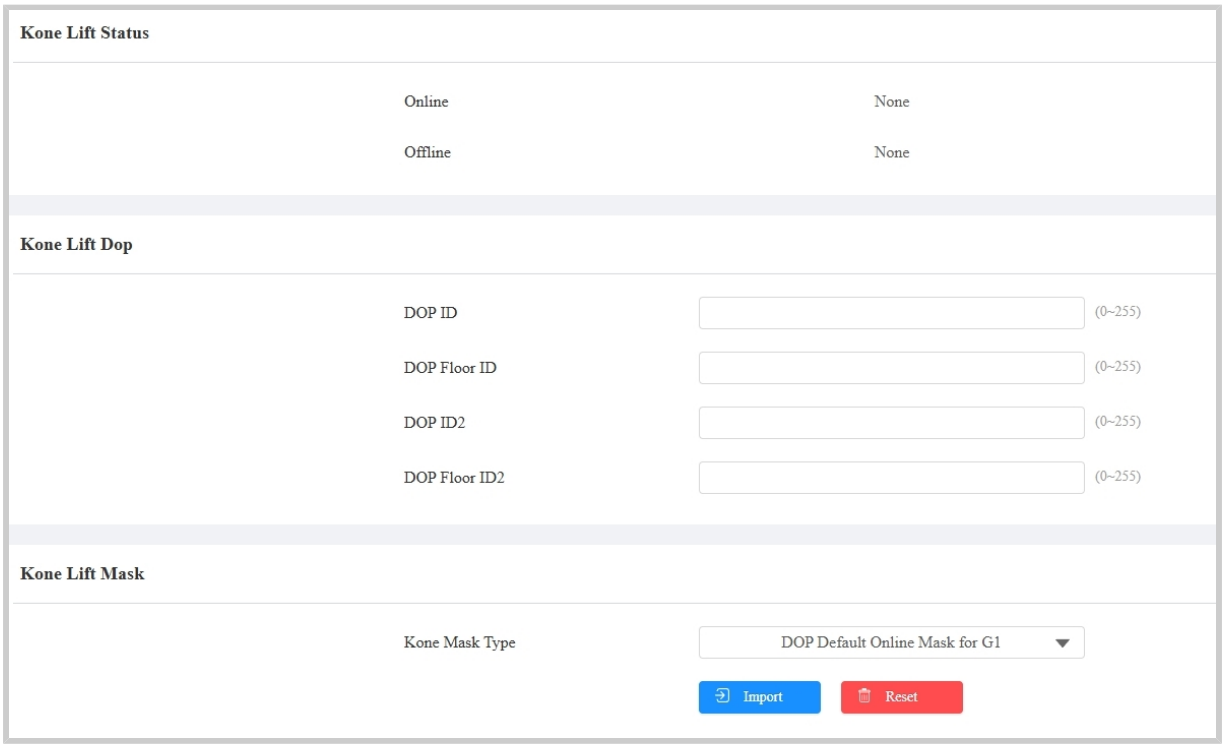
The device supports the integration with the KONE lift control panel. Users can use their credentials configured on the door phone to unlock the lift button and access the desired floor.

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.





- **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.
- **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.

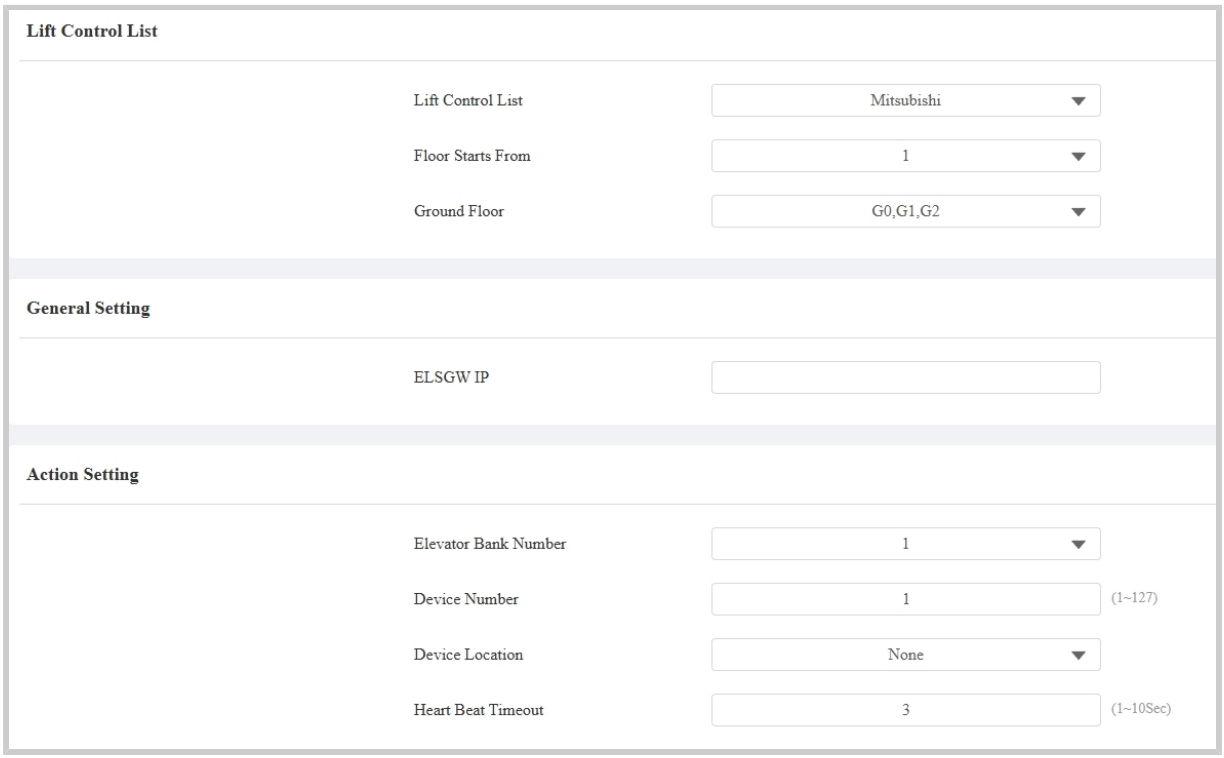
Kone Lift Dop	Kone Lift Cop	Lift Turnstile
DOP ID	COP Elevator ID	Device Terminal ID
DOP Floor ID	COP Group ID	Device Floor ID
DOP ID2	COP Elevator ID2	Device Door
DOP Floor ID2	COP Group ID2	Device Terminal ID2
		Device Floor ID2
		Device Floor ID2

- **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.

Mitsubishi Lift Controller

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

To set this feature up, go to the **Device > Lift Control** interface. Select **Mitsubishi** in the Lift Control List.



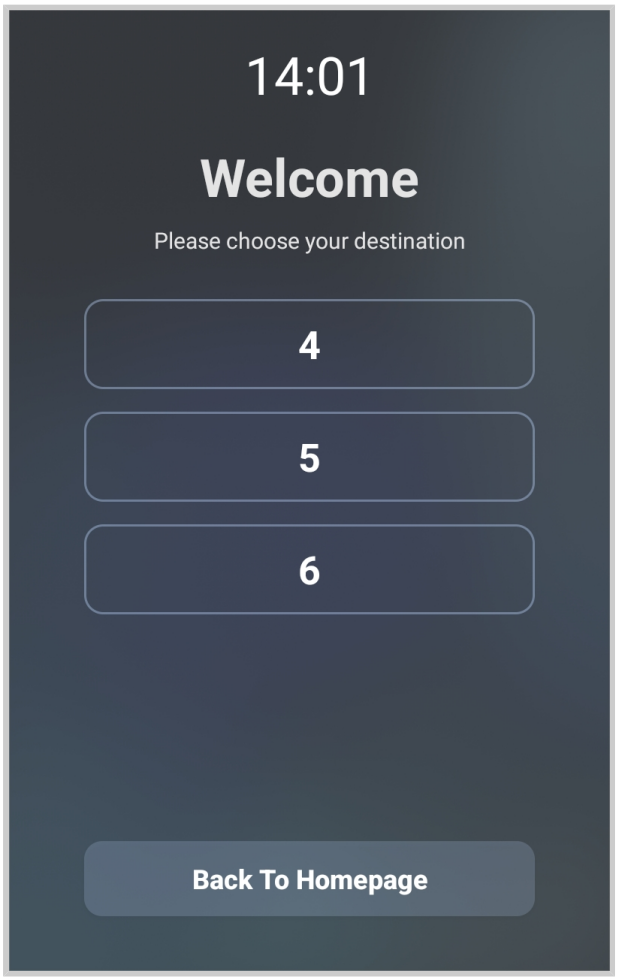
- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor.
- **Ground Floor**: If there are ground floors between the -1 and 1 floors, configure this option.
- **ELSGW IP**: The IP address of the Mitsubishi lift control server.

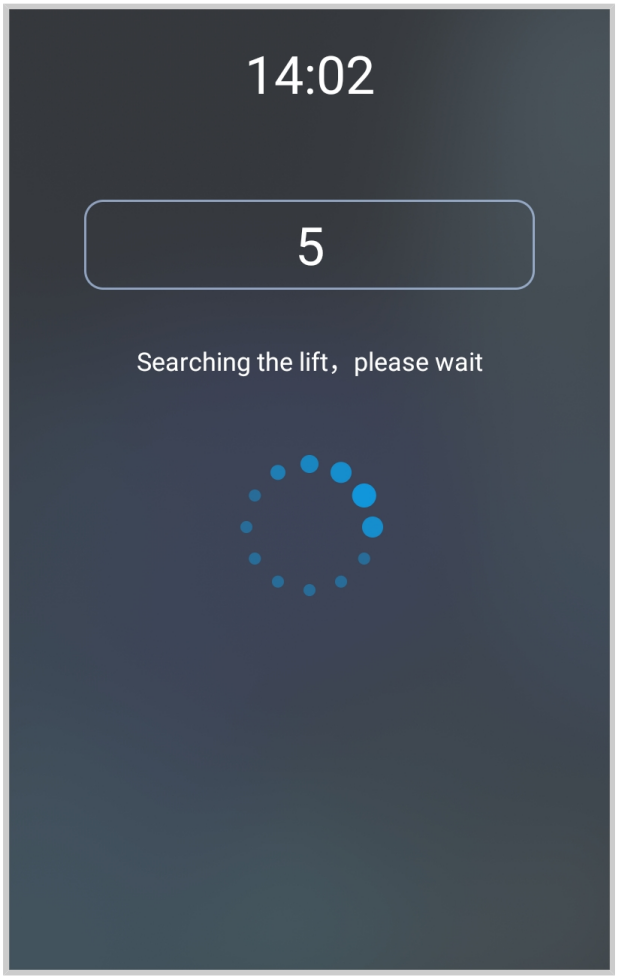
- **Elevator Bank Number**: The options are 1-4 and FFh. For example, choosing 3 selects the third group of elevators, while FFh selects all groups without specifying one.
- **Device Number**: Select a number(1~127) for the device to distinguish it from others.
- **Device Location**: Select the floor where the device is installed.
- **Heart Beat Timeout**: Specify the time interval for the device to send heartbeat packets to the lift control server. The default is 3 seconds.

> **Note**
>
> Configure local users' credentials and select their accessible floors on the **Directory > User** interface. For details, see the Door-opening Configuration chapter.

When users use their credentials, the accessible floor options will display on the device.

Users can select the desired floor number.

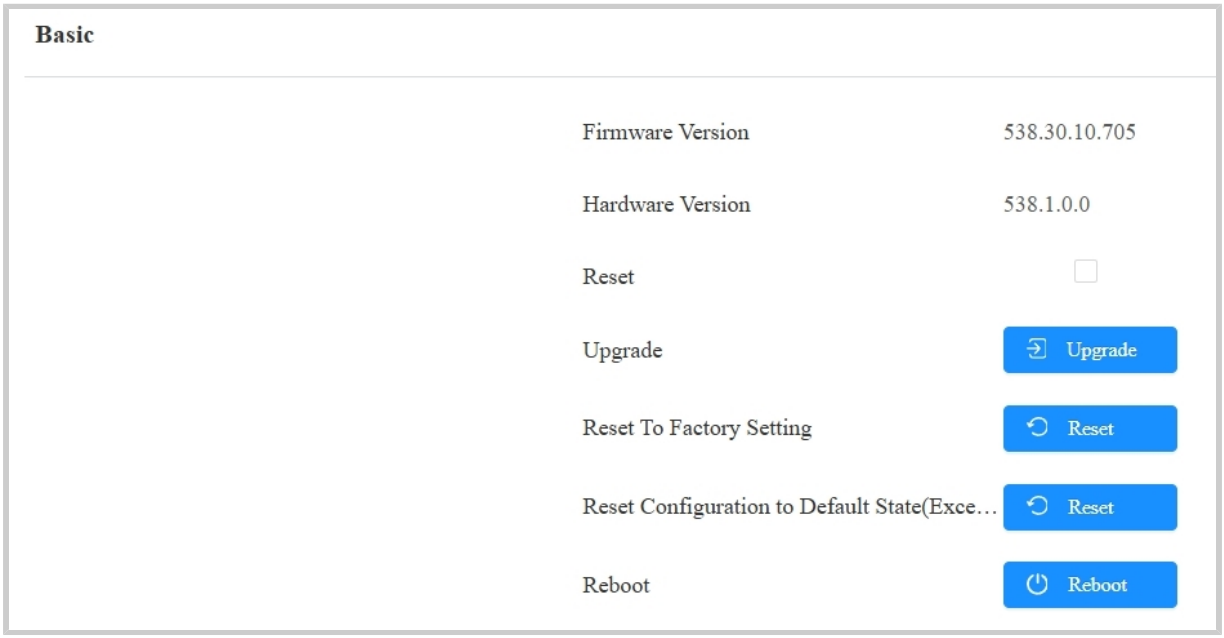

14:01
Welcome
Please choose your destination
4
5
6
Back To Homepage


14:02
5
Searching the lift，please wait

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Note

- Firmware files should be in **.zip** format for upgrade.

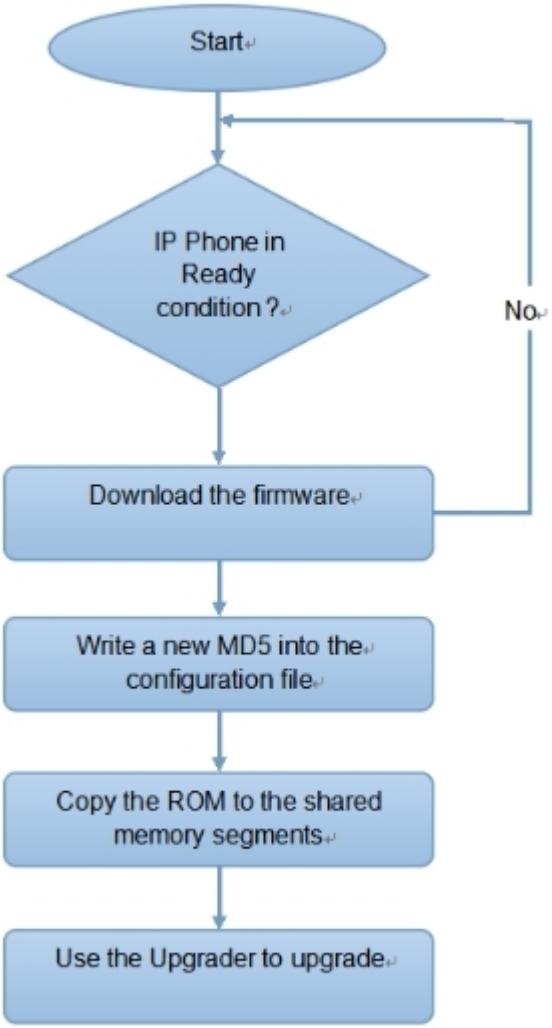
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

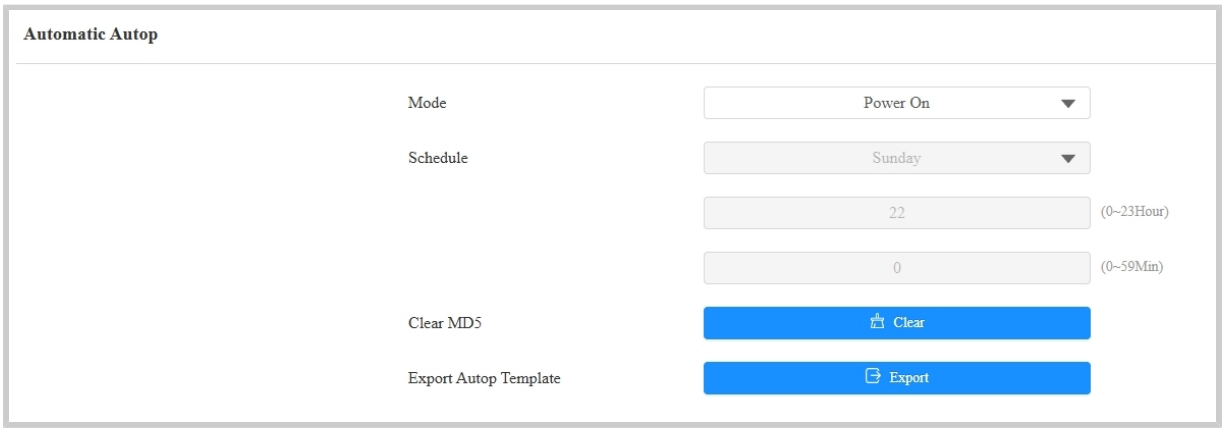
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

Akuvox provides you with different AutoP methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule.

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

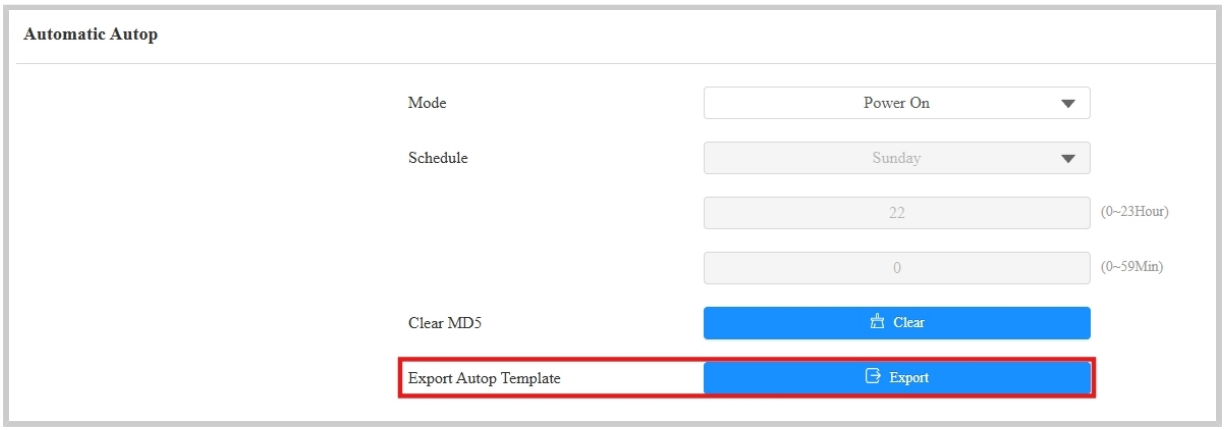


- **Mode**:
  - **Power On**: Allow the device to perform Autop every time it boots up.
  - **Repeatedly**: Allow the device to perform Autop according to the schedule.
  - **Power On + Repeatedly**: Combine Power On and Repeatedly modes, allowing the device to perform Autop every time it boots up or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

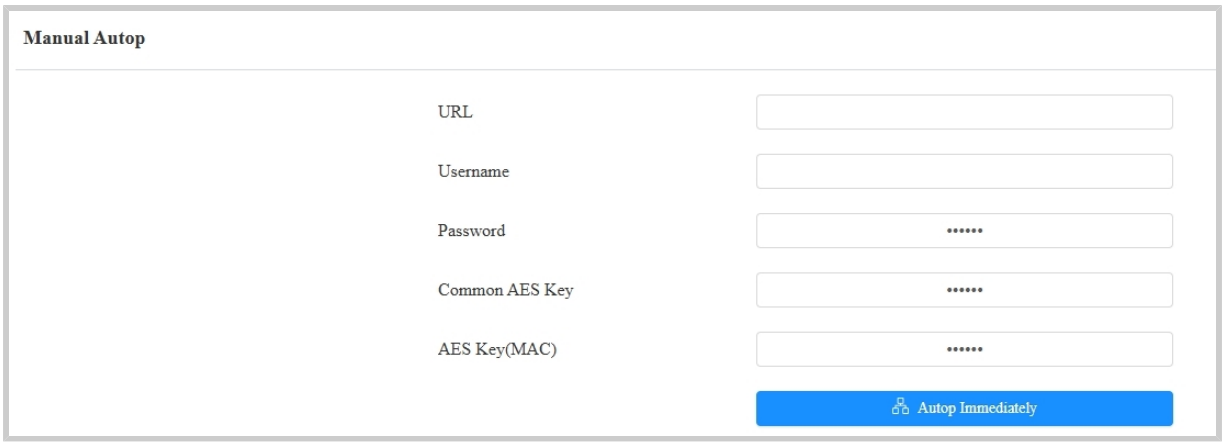
Static Provisioning

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

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



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



- **URL**: The TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **User Name**: Set up a username if the server requires a username to be accessed.
- **Password**: Set up a password if the server requires 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

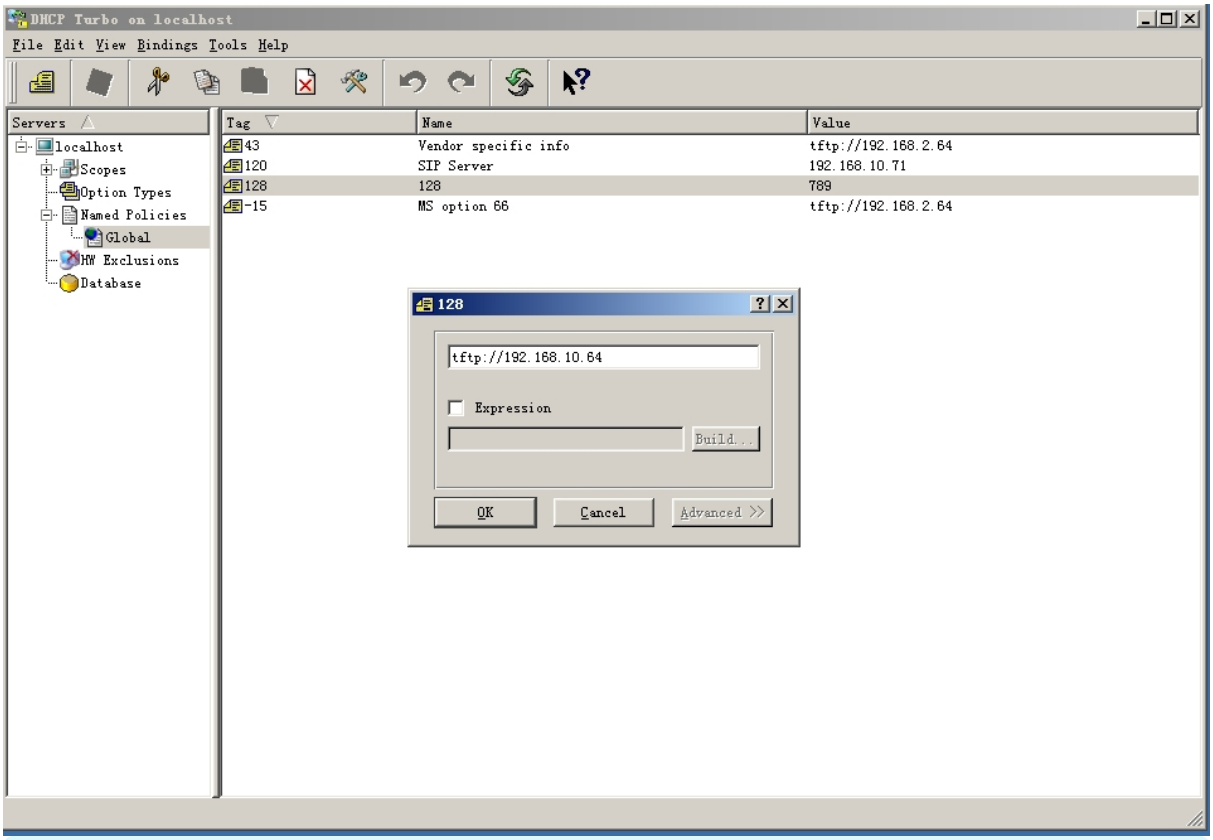
- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use 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 **CustomOption**as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.

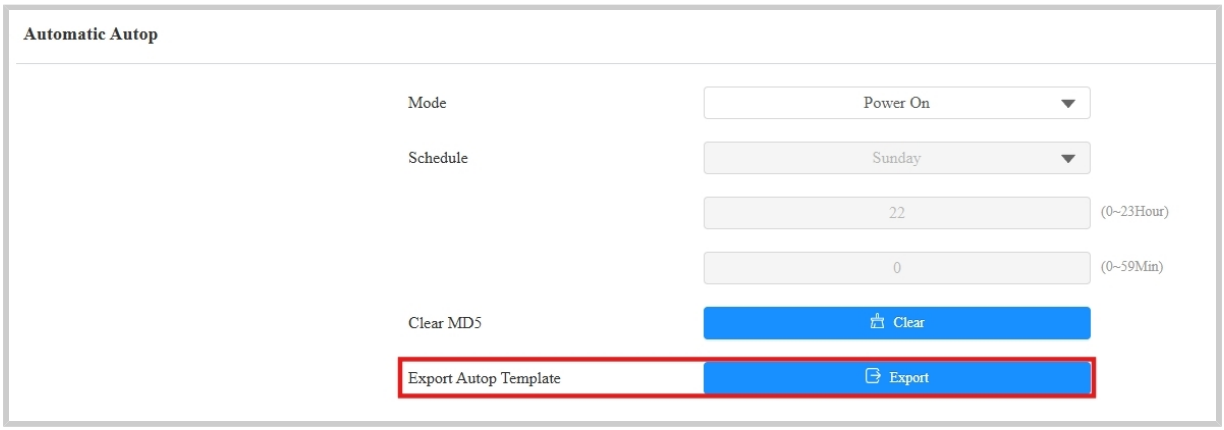


Note

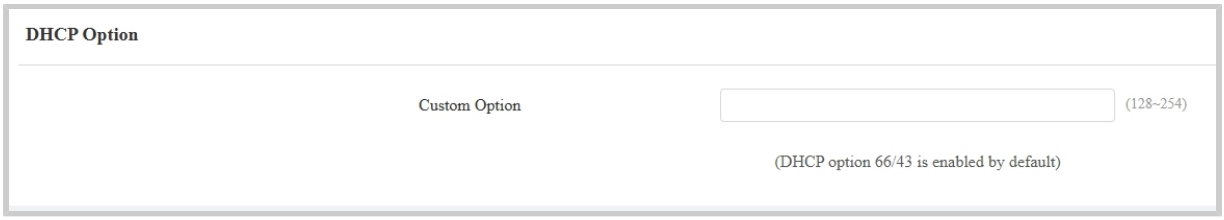
The Custom Option type must be a string. The value is the URL of the TFTP server.

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

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



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



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

PNP Configuration

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

Click here to watch the configuration video.

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

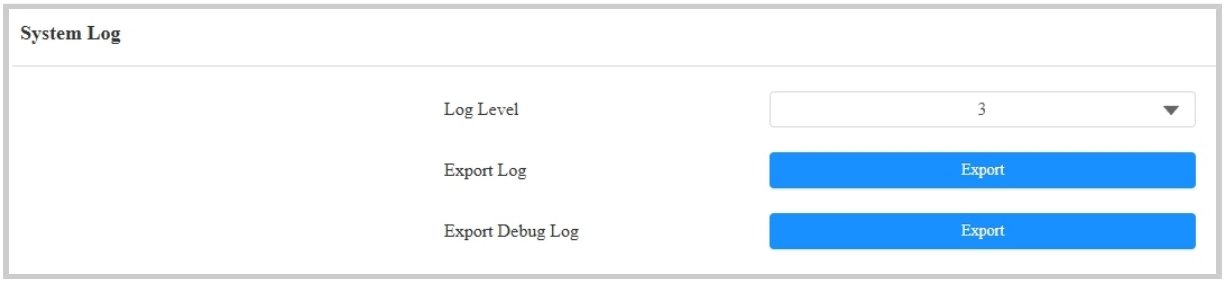


Debug

System Log for Debugging

System logs can be used for debugging purposes.

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

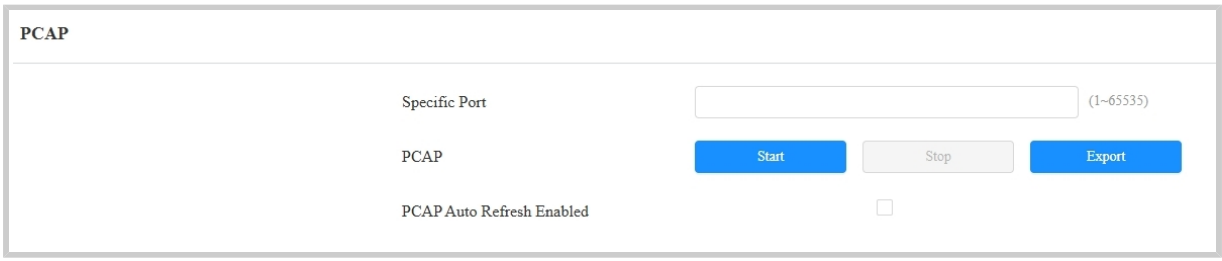


- **Log Level**: Select log levels from 1 to 7. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is **3**. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export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

PCAP for Debugging

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

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

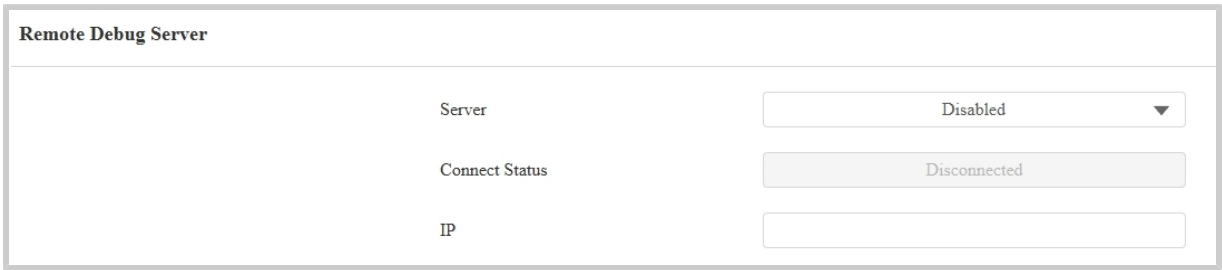


- **Specific Port**: Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: Click **Start** and **Stop** to capture a certain range of data packets before clicking the **Export** tab to export the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

Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

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



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

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.



Ping

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

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

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

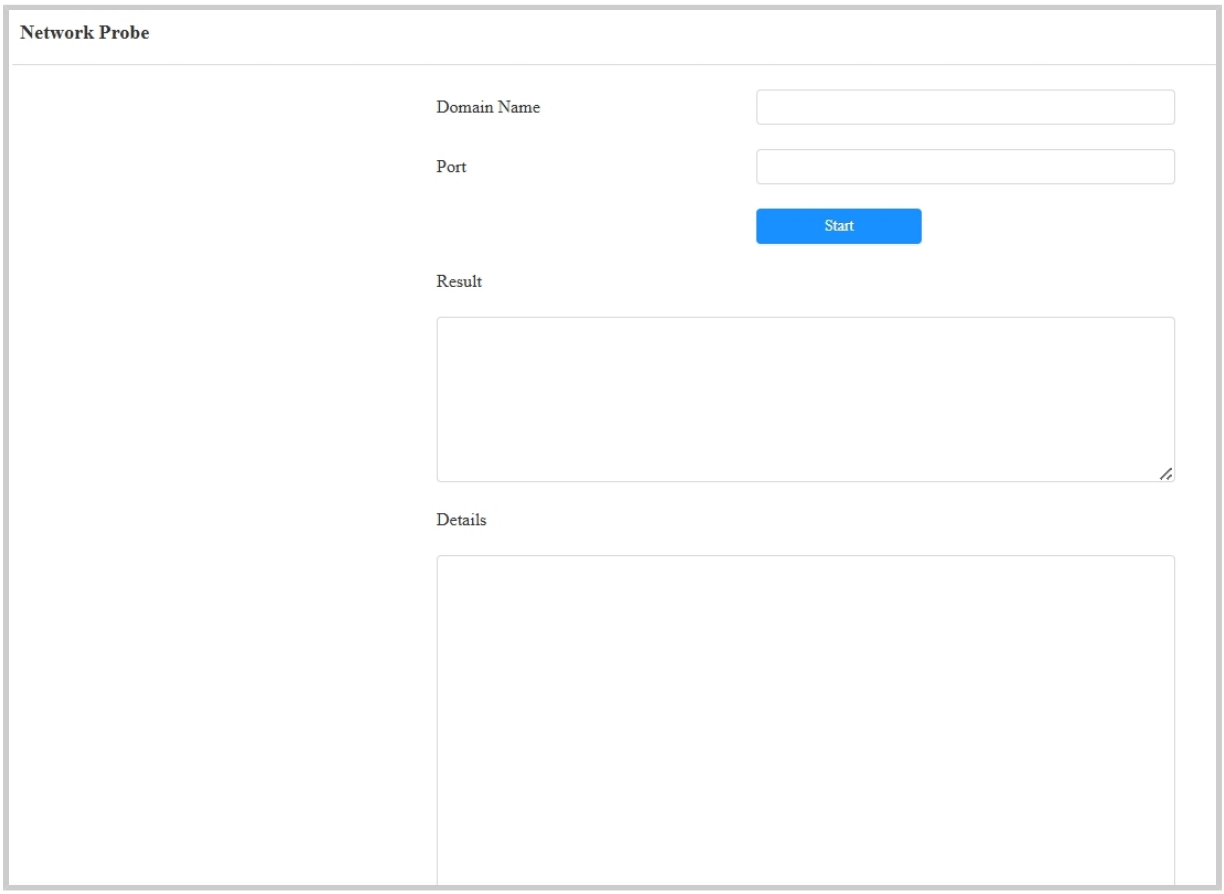


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Network Probe

This function is designed to identify and locate various network issues. When a device has trouble accessing or uploading to a domain, you can quickly pinpoint the problem by entering the domain and port into the network detection feature, enhancing problem-solving efficiency and reducing the resolution time.

To use this feature, go to the **System > Maintenance > Network Probe** interface.



- **Domain Name**: Enter the domain name or IP address.
- **Port**: Enter the port number.
- **Start**: Click to start detection after entering the domain name and port.
- **Result**: Display the detection result.
- **Details**: Display analysis of the result.

Backup

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

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



- **Config File**:
  - **Scope:** Config import/export includes configuration settings, user data (including face data), and contact-related data (such as imported contact files, contact database, and Dial Plan).
  - **Exclusions:** It does not include access logs, call logs, snapshots, or event logs.
  - **Behavior:** During Config import, only the included Config-related data is replaced. All other existing device data remains unchanged.
  - **Supported formats:** .cfg, .tgz
- **Data File**:
  - **Scope:** Data import/export includes configuration settings, user data (including face data), contact-related data (such as imported contact files, contact database, and Dial Plan), as well as access logs, call logs, snapshots, and event logs.
  - **Behavior:** During Data import, all corresponding device data will be overwritten.
  - **Supported format:** .tgz

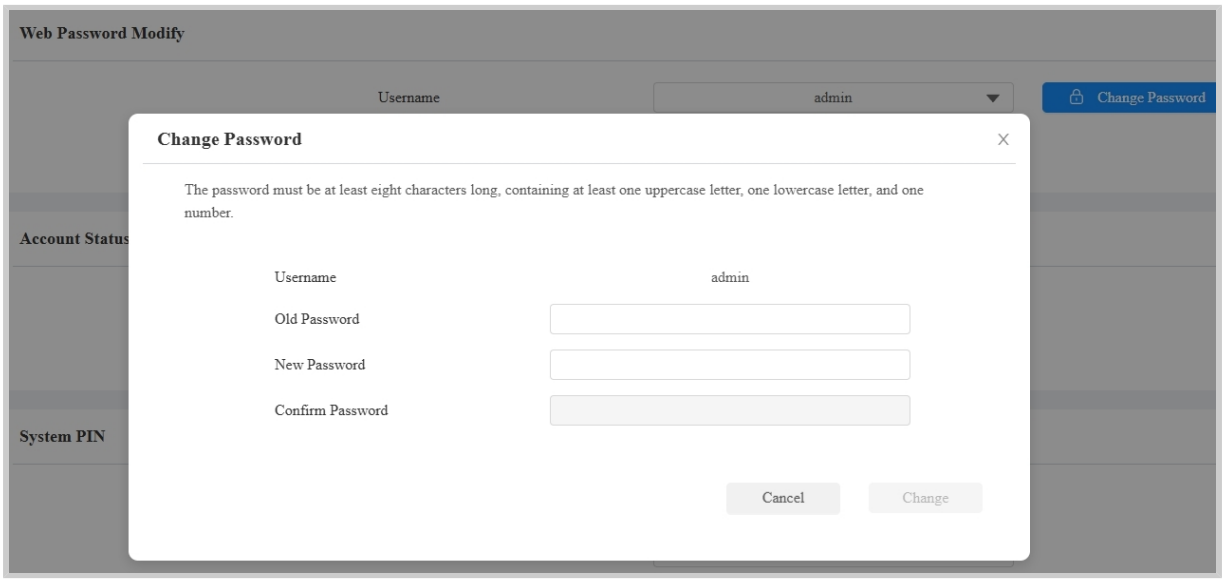
Password Modification

Modify Device Web Interface Password

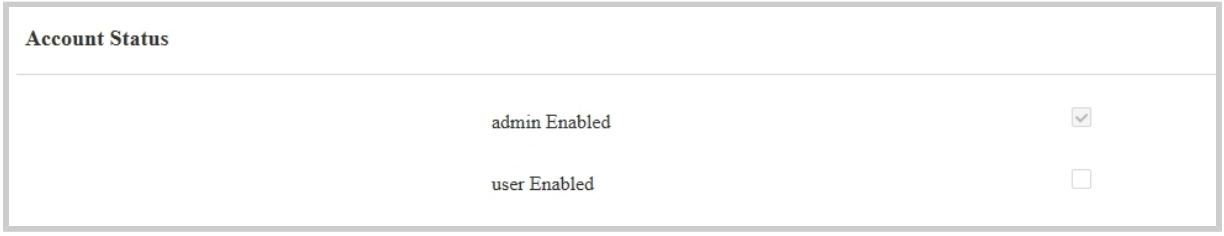
Change the web password on the **System > Security > Web Password Modify** interface.

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





You can enable/disable the user account in the **Account Status** section.



Modify Security Questions

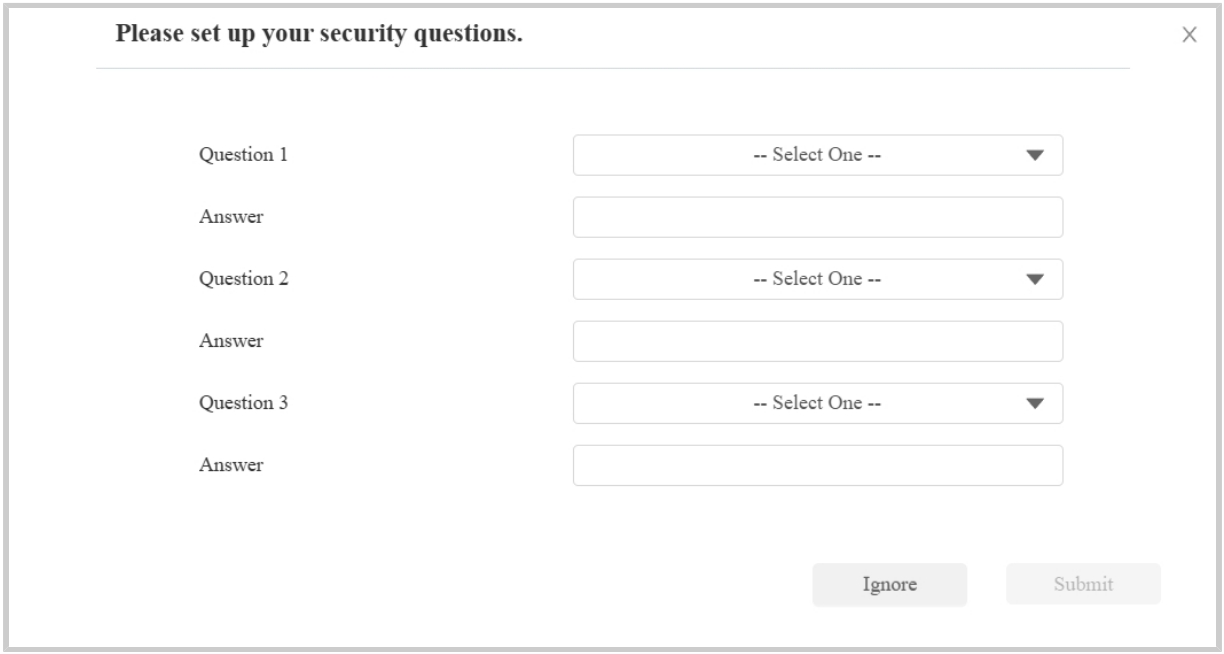
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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**.



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



Modify System Password

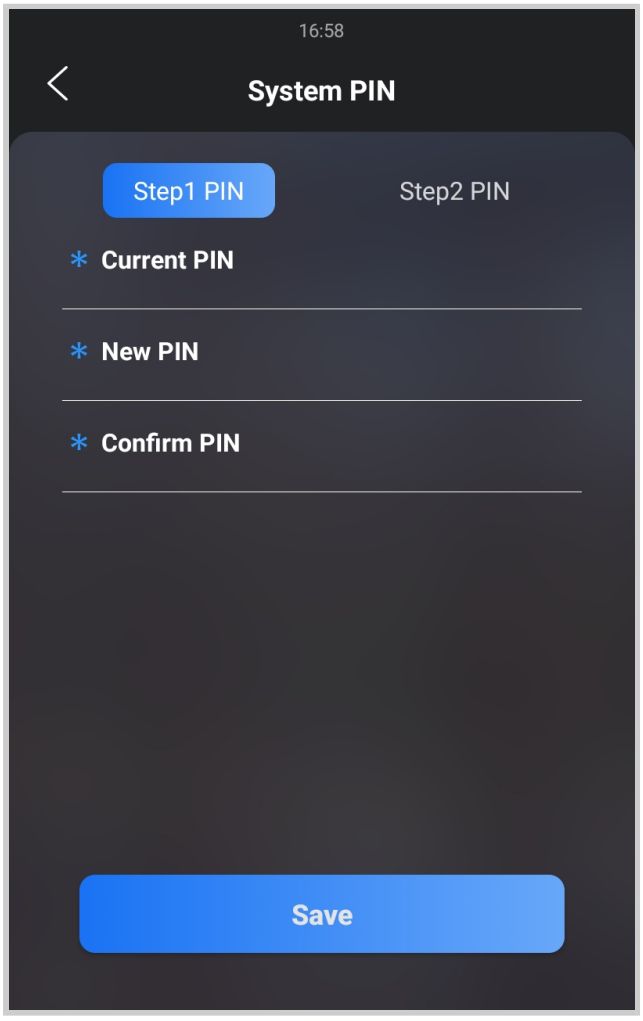
You can enter the Step1 PIN and then the Step2 PIN on the device's Dial screen to access the system settings.

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



- **Step1 PIN**: Set a 6-digit password. The default is 9999.
- **Step2 PIN**: Set a 6-digit password. The default is 3888.

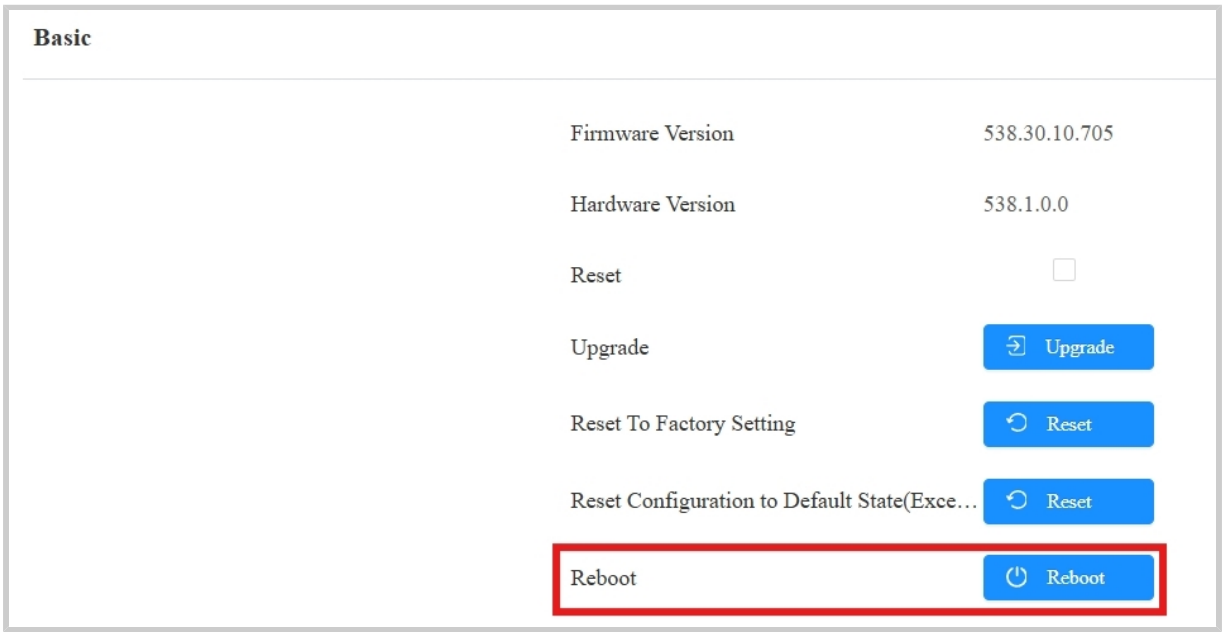
You can also set them up on the **Setting > Security > System PIN** screen.



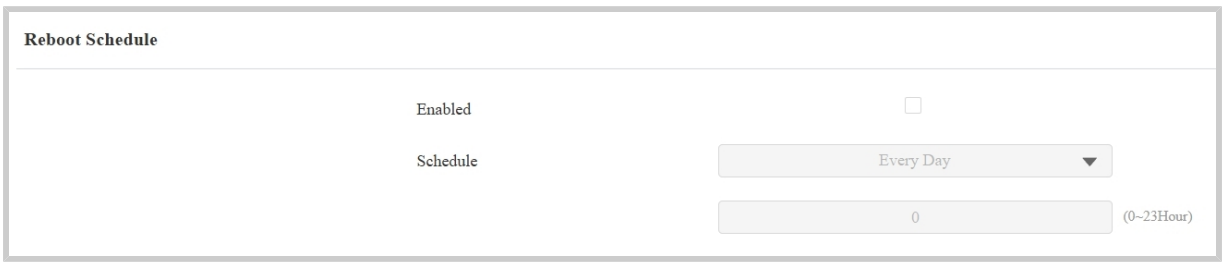
System Reboot&Reset

Reboot

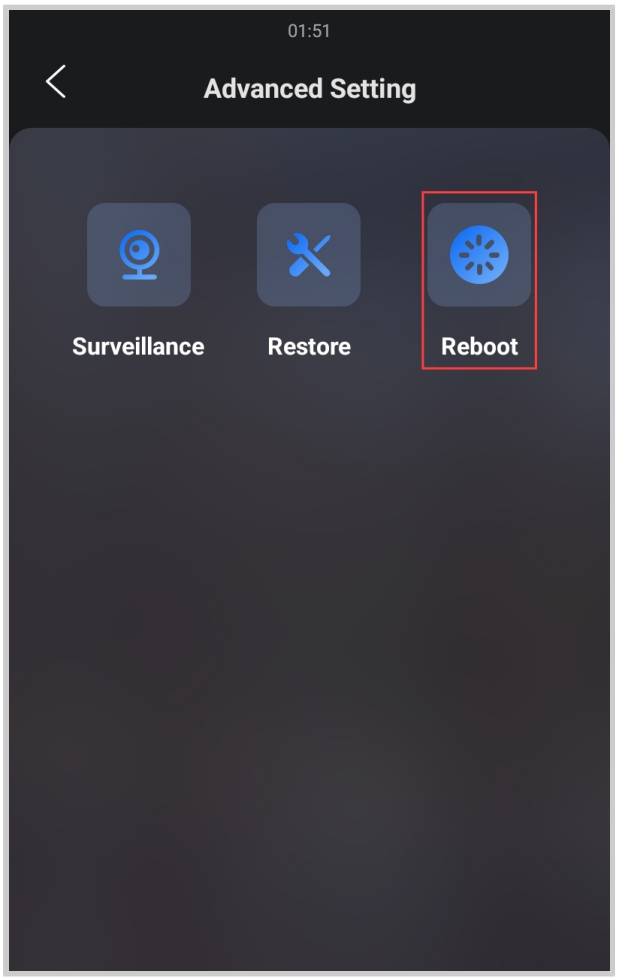
Reboot the device on the **System > Upgrade** interface. Click **Reboot**.



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



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

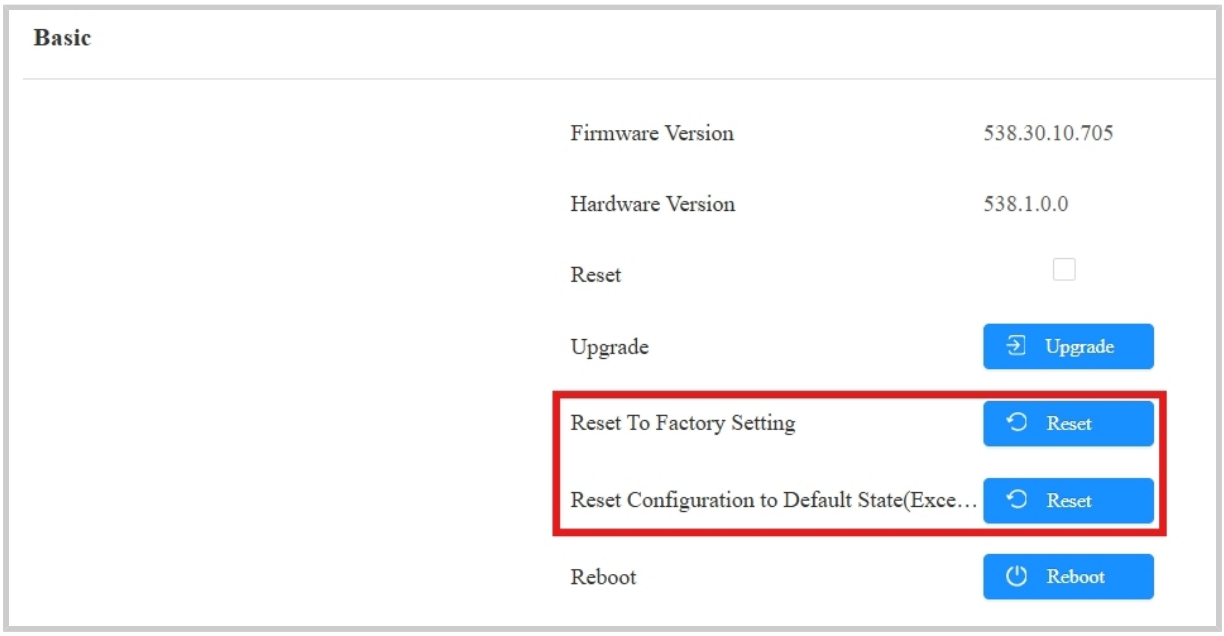


Reset

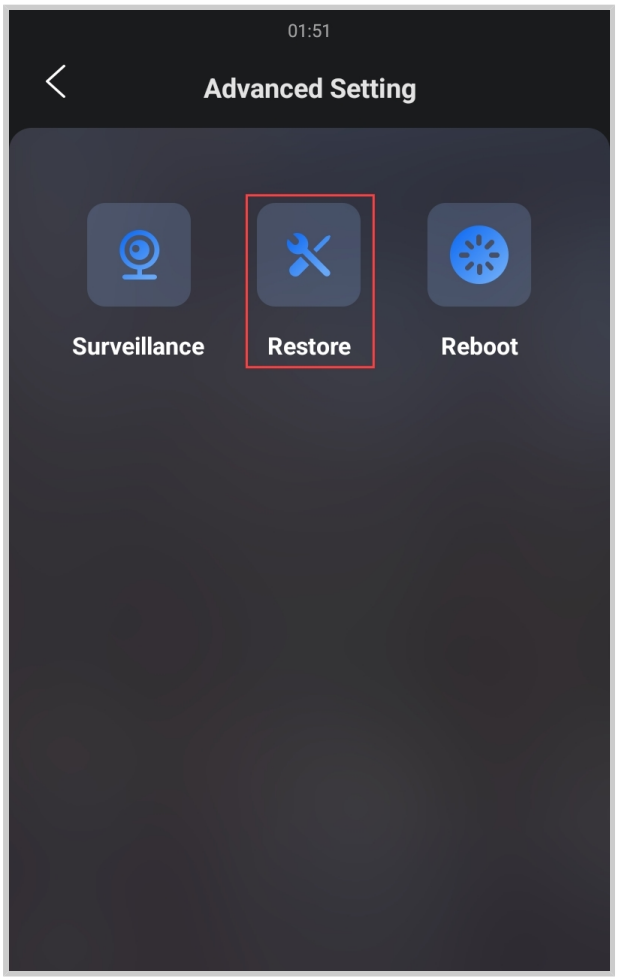
The device provides two reset options:

- **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.



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


01:51
Advanced Setting
Surveillance
Restore
Reboot

Tip

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

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

