Akuvox

Table of contents

Akuvox R29 Series Door Phone Administrator Guide

About This Manual 12

Product Overview 14

Changelog 15

Model Differences 16

Supported Card Types 17

Introduction to Configuration Menu 19

Access the Device 21

Access the Device Settings 21

Gesture Control Setting 23

Access Device Web Settings 26

Language and Time 28

Language 28

On the Web 28

On the Device 30

Time 31

On the Web 31

On the Device 31
Volume and Tone 33
Volume Configuration 33
On the Web 33
On the Device 34
Door-opening Tones 35
Guiding Tone Of Contact List 36
Upload Tones 36
Visitor-friendly Mode 37
Open Door Tone Mode 38
LED and LCD 39
Infrared LED Setting 39
On the Web 39
On the Device 40
Card Reader LED Control 43
Screen Backlight Brightness 44
LED White Light 45
Screen Display 47
Home Screen Display 47
Home Screen Display Theme 47

Villa/Office Theme 48
Building Theme 50
Speed Dial Setting in Villa/Office/Building Theme 54
PIN Keypad Display in Villa/Office/Building Theme 55
Alphanumeric Theme 56
Screensaver Settings 58
On the Web 58
On the Device 60
Upload Screensaver 61
Upload Pictures for Alphanumeric Mode Screen Display 62
Upload Background Picture in the Time-displaying Area 63
Upload Device Booting Image 64
Upload Device Logo 65
Unlock Options Display 65
Open Door Text Prompt 66
Keyboard Interface Text Prompt 68
Appearance 69
Network Setting 71
Device Network Connection 71
Device Local RTP Configuration 73

Device Deployment in Network 74
Device Web HTTP Setting 76
NAT Setting 76
LTE Wireless Connection (Optional) 77
LTE Data Usage Control 78
Intercom Call Configuration 80
IP Call Configuration 80
Make IP Calls 80
IP Call Setup 80
SIP Call Configuration 81
SIP Account Registration 81
SIP Server Configuration 83
SIP Call DND&Return Code Configuration 85
Outbound Proxy Server 86
Data Transmission Type 87
SIP Hacking Protection 87
Two-way Video Call 88
Video Transport Type 89
Call Setting 91
Quick Dial By Number Replacement 91

Quick Dial Using Configured Dial Name 92
Speed Dial 94
Import/Export the Speed Dial Contacts 98
Call Auto-answer 99
Sequence Call 100
Maximum Call Duration 101
Maximum Dial Duration 102
Hang up After Opening the Door 102
Audio & Video Codec Configuration 104
Audio Codec 104
Video Codec 105
Video Codec for IP Calls 105
Contacts Configuration 107
Manage Contact Groups 107
Set up Contact Details 109
Contacts List Display 111
Relay Settings 115
Local Relay 115
Web Relay 118
Security Relay 121

Upgrade SR01 122
Door Access Schedule Management 124
Create a Door Access Schedule 124
Import and Export Door Access Schedule 125
Door Schedule 125
Holiday Schedule 127
Holiday Schedule Import/Export 128
Door-opening Configuration 130
Unlock By Public PIN 130
User-specific Access Methods 131
Unlock by Private PIN Code 132
Unlock by RF Card/Bkey 133
Unlock by License Plate 134
Unlock by Facial Recognition 135
Access Setting 137
Import/Export User Data 139
Access Authentication Mode 139
Unlock by NFC and Felica Cards 141
Mifare Card Encryption 141
Unlock by HTTP Command 143

Unlock by DTMF Code 144
DTMF Data Transmission 145
DTMF Whitelist 147
Unlock by Exit Button 147
Unlock by QR Code 149
Unlock by Reception Tab 150
Unlock by Voice Assistant 152
Body Temperature Measurement for Door Access 155
Body Temperature Measurement Configuration 155
Ambient Temperature Configuration 159
Monitor and Image 160
MJPEG Image Capturing 160
MJPEG Authorization 161
RTSP Stream Monitoring 162
RTSP Basic Setting 163
RTSP Stream Setting 164
RTSP OSD Setting 165
Live Stream 166
ONVIF 167
Camera Exposure Adjustment 168

Data Transmission Type for Third-party Camera 169
Security 171
Tamper Alarm 171
Disarm Setting 172
Lock Security 173
Client Certificate Setting 174
Web Server Certificate 174
Client Certificate 175
Motion Detection 176
Motion Detection Schedule 178
Security Notification 180
Email Notification 180
FTP Notification 181
TFTP Notification 181
SIP Call Notification 182
Action URL 182
GDPR Setting 186
User Agent 187
Screenshots 187
Web Interface Automatic Log-out 188

Emergency Action 188
Real-time Monitoring 188
High Security Mode 189
Logs 191
Call Logs 191
Door Logs 192
Temperature Logs 193
Event Logs 194
Integration with Third-party Devices 196
Integration via Wiegand 196
Facility Code Setting 198
Wiegand Virtual Door Mode 199
Integration via HTTP API 200
Integration with Third-party Access Control Server 202
Integration via RS485 205
RS485 Virtual Door Mode 206
Power Output Control 207
Integration with Control4 208
Lift Control 209
Akuvox Lift Controller 209

KeyKing Lift Controller 211
ZKT Lift Controller 212
KONE Lift Controller 213
OSDP Setting 216
Firmware Upgrade 218
Auto-provisioning via Configuration File 219
Provisioning Principle 219
Configuration Files for Auto-provisioning 220
AutoP Schedule 221
Static Provisioning 222
DHCP Provisioning 224
Debug 227
System Log for Debugging 227
PCAP for Debugging 227
Remote Debug Server 228
Ping 229
Web Call 229
Network Probe 229
Backup 231
Password Modification 233

Modify Web Password 233
Modify Security Questions 233
Modify Device Setting Password 234
System Reboot&Reset 236
Reboot 236
Reset 237

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



R29 SERIES DOOR PHONE

Administrator Guide

Akuvox

Thank you for choosing the Akuvox R29 series door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to the 29.30.10.727 version, and it provides all the configurations for the functions and features of the R29 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



The Akuvox R29 series is an Android-based IP video door phone that combines audio and video communications, access control, and video surveillance. Its advanced Android OS, Cloud, and AI-based communication technologies allow for customization to meet your specific operational needs. The R29 series includes multiple ports for integrating external digital systems like access control and fire alarm systems, providing comprehensive control over building entrances and surroundings. It offers various secure access methods such as card, NFC, Bluetooth, QR code, voice control door access, and even body temperature measurement, ideal for residential buildings, office buildings, and complexes.

Changelog

What’s new in version 29.30.10.727:

- Support multi-factor authentication mode for the integration with the third-party access control server.
- Support configuring the data length for reading the Mifare cards .
- Support configuring the detection accuracy for waking the device from standby .

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

Model Differences

Model	R29C	R29S
Touch Screen	√	√
Relay Ports	3	3
Alarm In	X	X
RS485	√	√
Card Reader	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ
Wi-Fi	X	X
Bluetooth	√	X
Temperature Detection	X	X
Facial Recognition	√	√
LTE	X	X
USB	X	X
External SD card	X	X

R29C-B	R29C-L
√	√
3	2

R29C-B	R29C-L
X	X
√	√
13.56MHZ & 125KHZ	13.56MHZ & 125KHZ
X	X
√	√
√	X
√	√
X	√
X	X
X	X

Supported Card Types

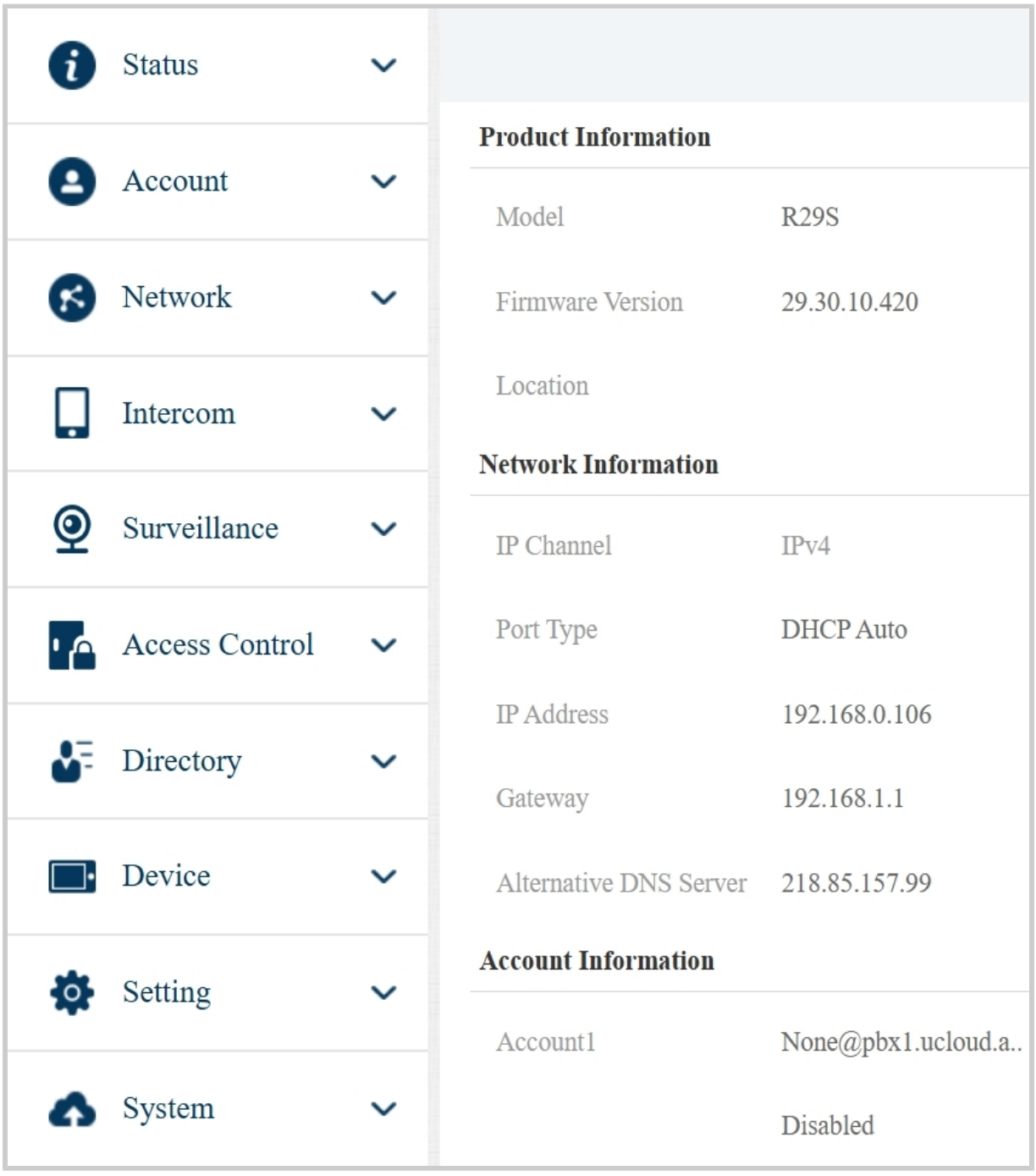
The device's firmware should be 29.30.10.332 or higher:

- Unencrypted ID Card:
  - EM4100
  - EM4200
- Unencrypted IC Card:
  - Mifare Ultralight C/EV1
  - Mifare Classic Compatible Card
  - Mifare Plus-S 2K
  - Mifare Desfire EV1 2K D21
  - Mifare Desfire EV2 D42
  - Mifare Desfire EV2 D22

  - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
  - NFC Type2 216
  - NFC Type2 215
- Felica Card
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Classic ev1 7-byte
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
  - Mifare Classic 1K
  - Mifare S50-1K Card
  - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, account information, etc.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, etc.
- **Network**: This section mainly deals with DHCP & Static IP settings, RTP port settings, device deployment, etc.
- **Intercom**: This section covers intercom call, dial plan, and voice assistant settings.
- **Surveillance**: This section is about motion detection, RTSP, MJPEG, ONVIF settings, etc.
- **Access Control**: This section is for relay, input, facial recognition, card, PIN settings, etc.
- **Directory**: This section covers user management.
- **Device**: This section includes LCD, Light, Wiegand, lift control, RS485, audio settings, etc.
- **Setting**: This section includes time, language, action, and action URL, access control schedule settings, etc.
- **System**: This section includes the device upgrade, maintenance, auto-provisioning, debugging, password modification, etc.

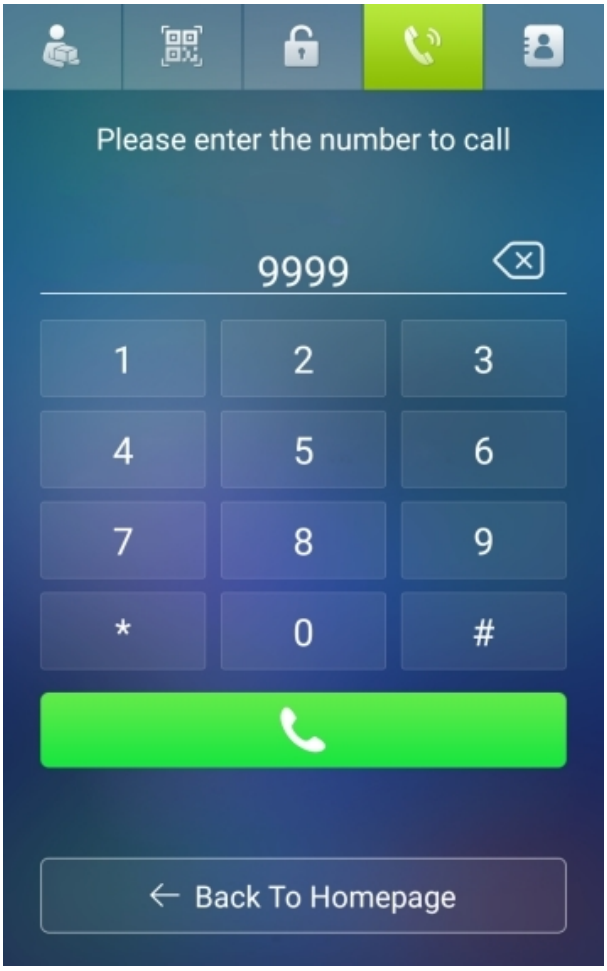

Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System
Product Information
Model
R29S
Firmware Version
29.30.10.420
Location
Network Information
IP Channel
IPv4
Port Type
DHCP Auto
IP Address
192.168.0.106
Gateway
192.168.1.1
Alternative DNS Server
218.85.157.99
Account Information
Account1
None@pbx1.ucloud.a..
Disabled

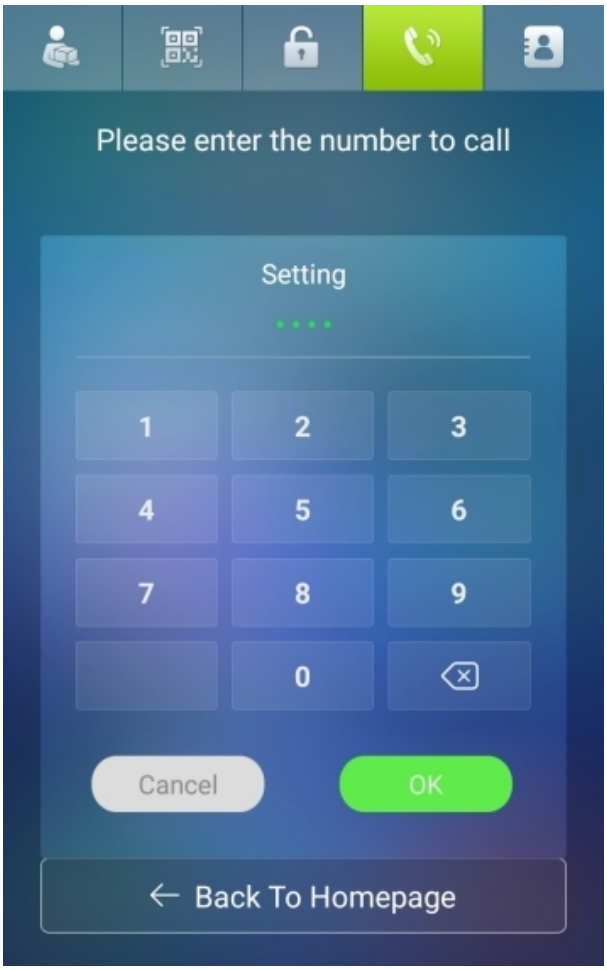
Access the Device

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

Access the Device Settings

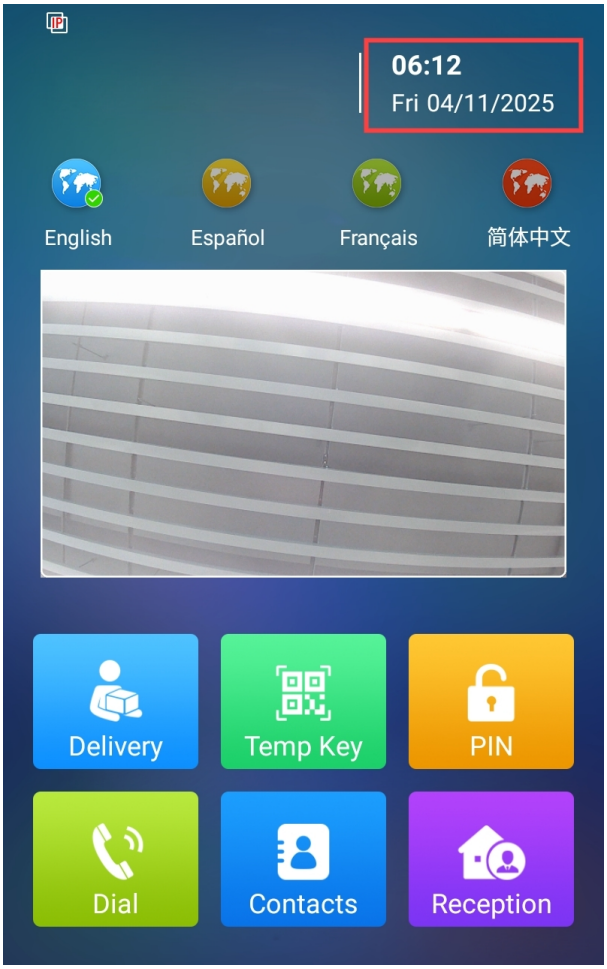
You can set up some basic settings on the device screen by pressing **9999** + **Dial key** + **3888** (password) on the **Dial** screen.

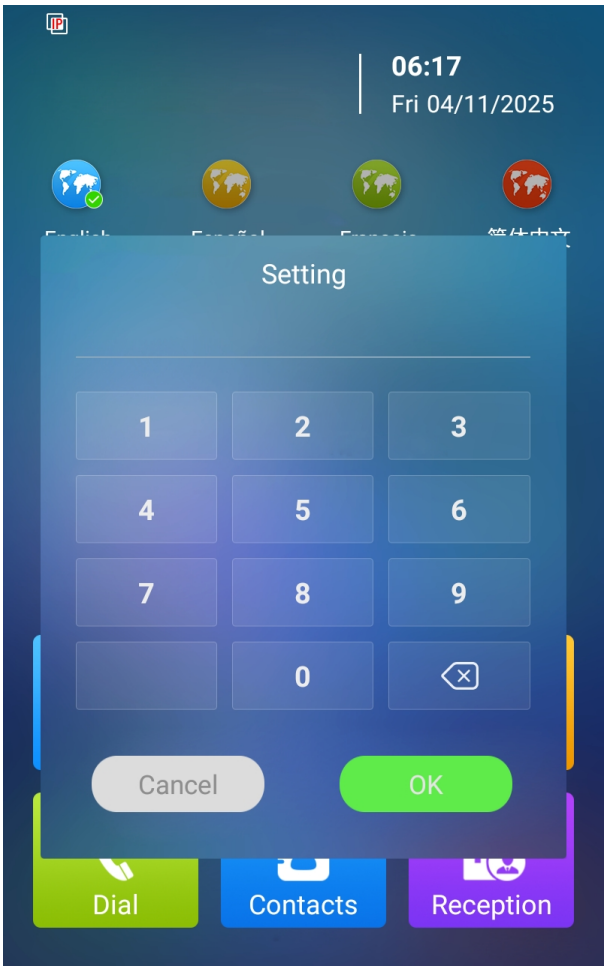

Please enter the number to call
9999
1
2
3
4
5
6
7
8
9
*
0
#
Back To Homepage



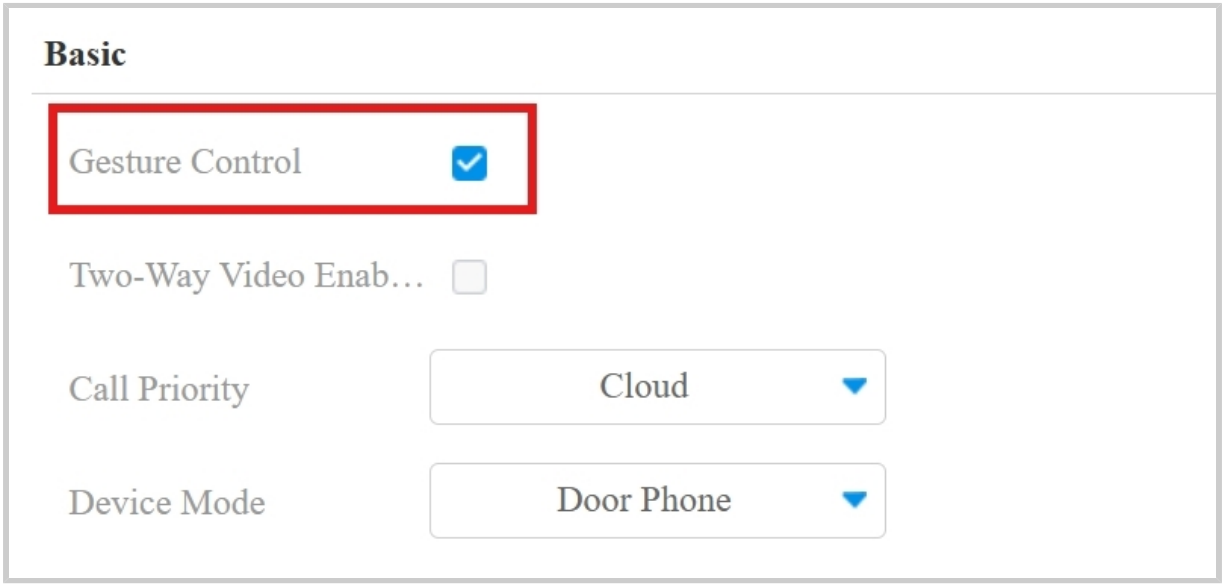
Gesture Control Setting

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.


06:12
Fri 04/11/2025
English
Español
Français
简体中文
Delivery
Temp Key
PIN
Dial
Contacts
Reception



To enable the feature, navigate to the web **Intercom > Basic** interface.

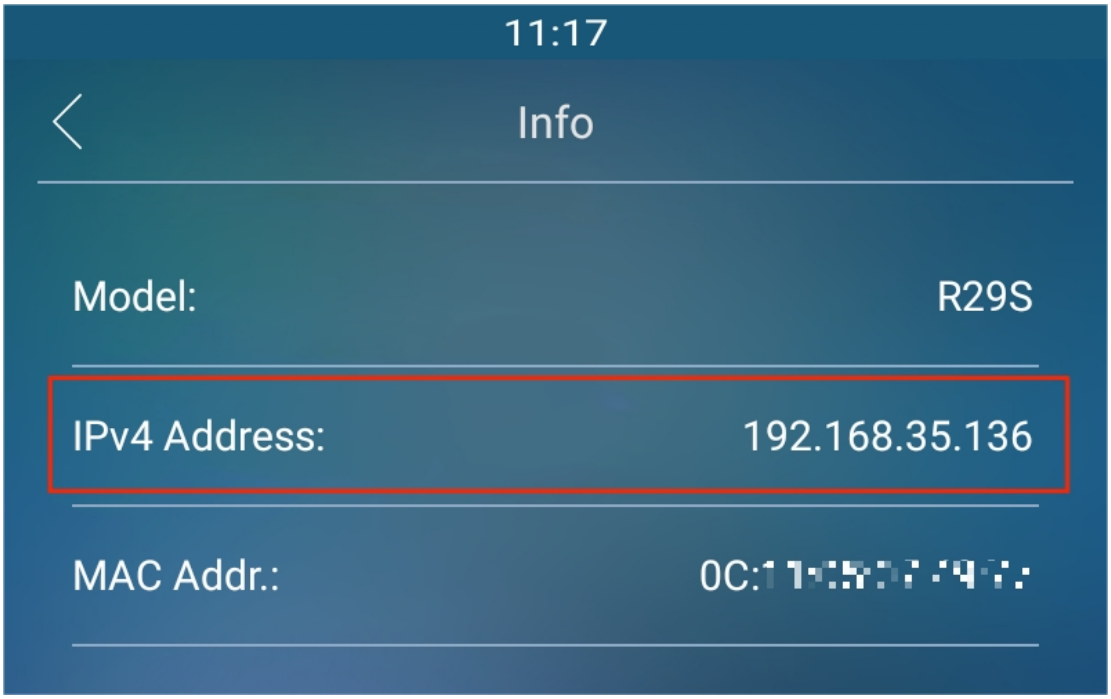


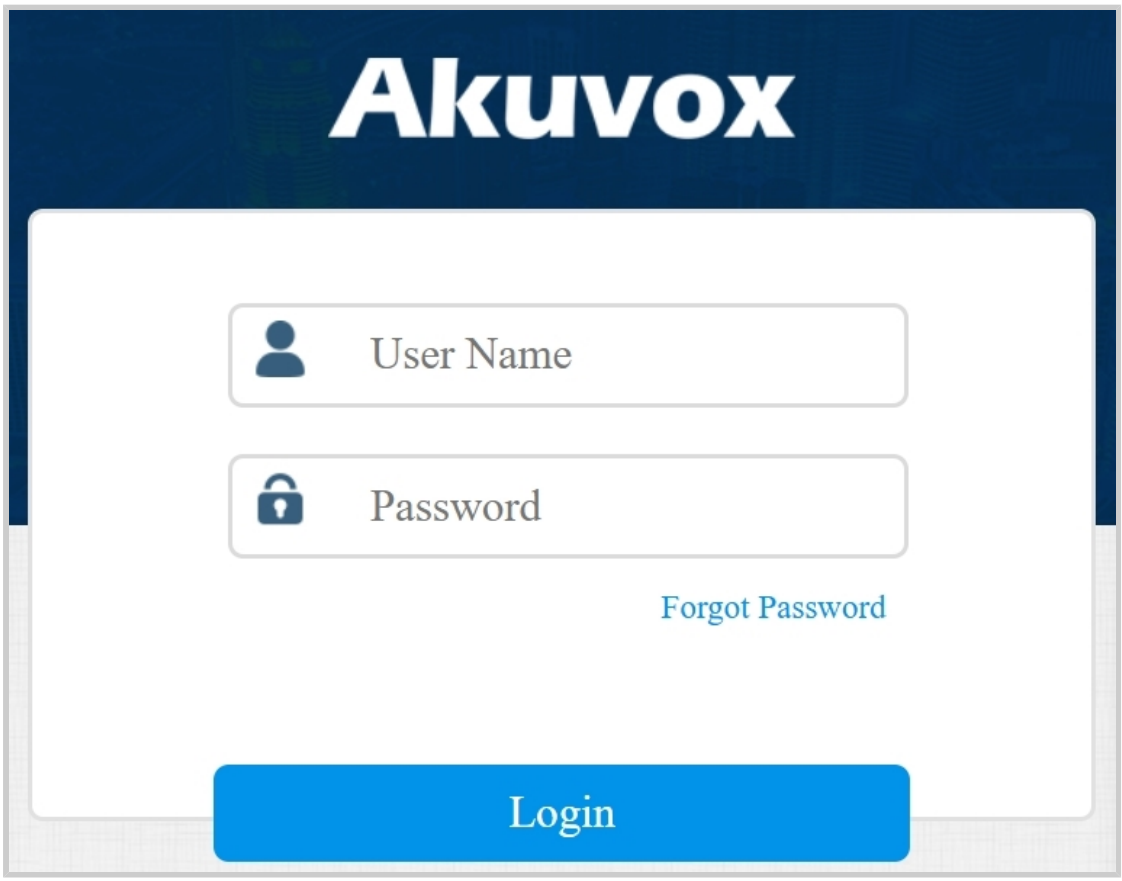
Access Device Web Settings

You can also enter the device IP address on the web browser to log in to the device web interface, where you can configure parameters, etc.

You can check the IP address on the device **Settings > Info** screen.

Or, use the IP scanner to scan the device IPs on the same LAN.





Note

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

Language and Time

Language

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

> **Note**
>
> R29Z/R29Z-L's language is Chinese by default, so there is no such option the first time it boots up.

On the Web

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

The device screen supports the following languages:

- English, Simplified Chinese, Spanish, Danish, French, Czech, Traditional Chinese, Turkish, Japanese, German, Polish, Portuguese, Hungarian, Russian, Norsk, Korean, Swedish, Ukrainian, Azerbaijani, Slovak, Hebrew, Dutch, Slovenian, Italian, Arabic, Vietnamese, and Bosnian.



Select the device web language on the **Setting > Time/Lang > Web Language** interface.

The device web supports the following languages:

- Simplified Chinese, Spanish, Danish, French, Czech, Traditional Chinese, Turkish, Japanese, German, Polish, Portuguese, Hungarian, Russian, Norwegian, Korean, Swedish, Ukrainian, Azerbaijani, Slovak, Hebrew, Dutch, Slovenian, Italian, Arabic, Vietnamese, and Bosnian.



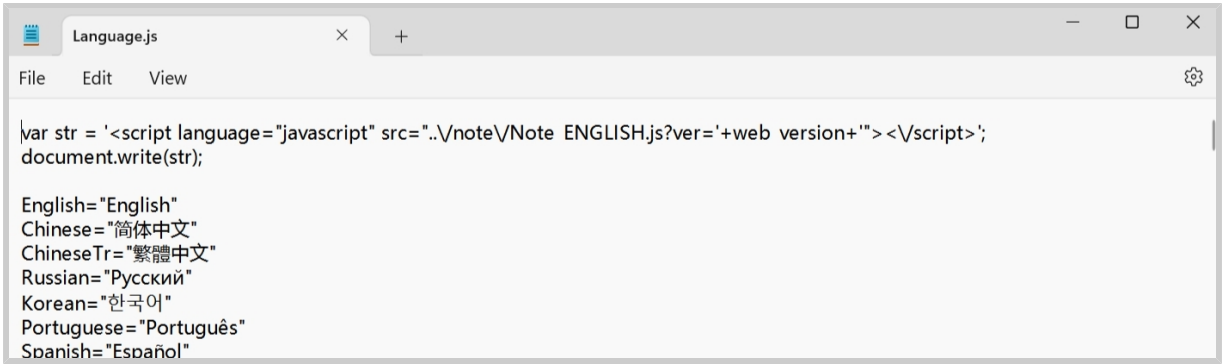
Custom Language

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

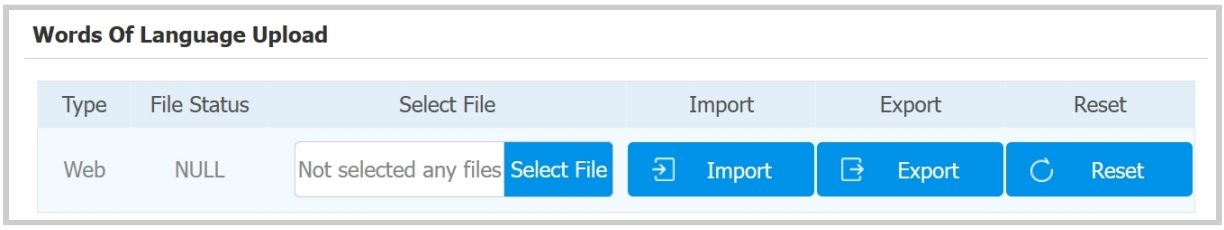
Export the .json file for editing. You may edit it with Notepad on your computer.

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

File Example:



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



Note

R29Z/R29Z-L only supports English and Chinese for LCD and web display.

On the Device

Select the LCD language on the **Setting > Language** screen.



Time

Time settings, including time zone, date and time format, and more, can be configured either on the device or the web interface.

On the Web

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.

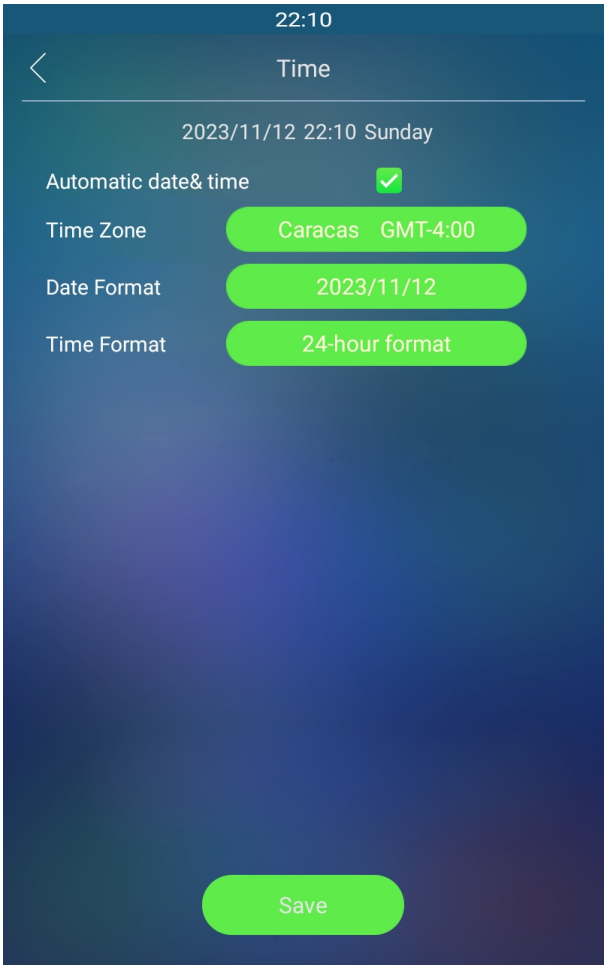
Set up time on the **Setting >Time/Lang >Time** interface.



- **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).
- **Time Visible**: Decide whether to display time on the device screen.
- **NTP Server**: The NTP server address.

On the Device

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



- **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).

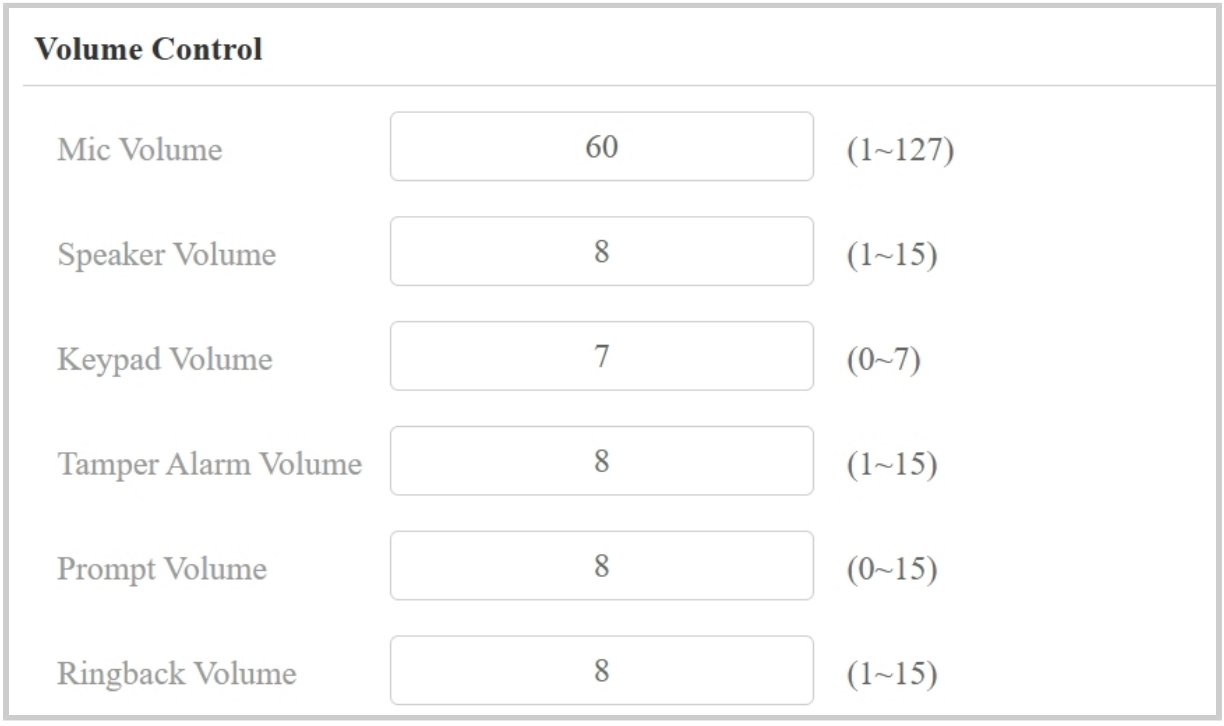
Volume and Tone

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

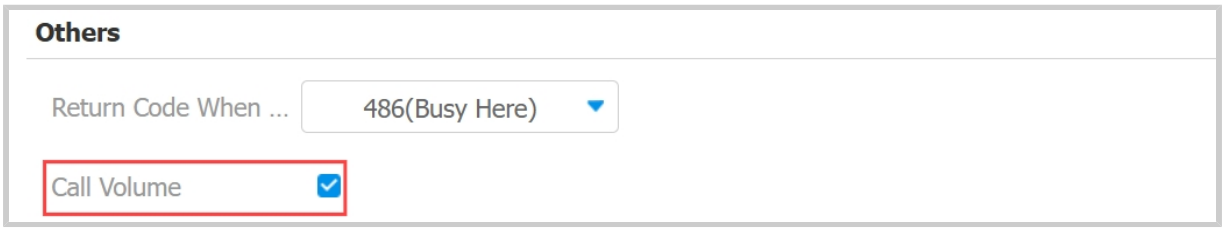
Set up volumes on the **Device > Audio** interface.



- **Mic Volume**: The default is 60.
- **Speaker Volume**: The default is 8.
- **Keypad Volume**: The icon tapping sound. The default is 7.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 8.
- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 8.

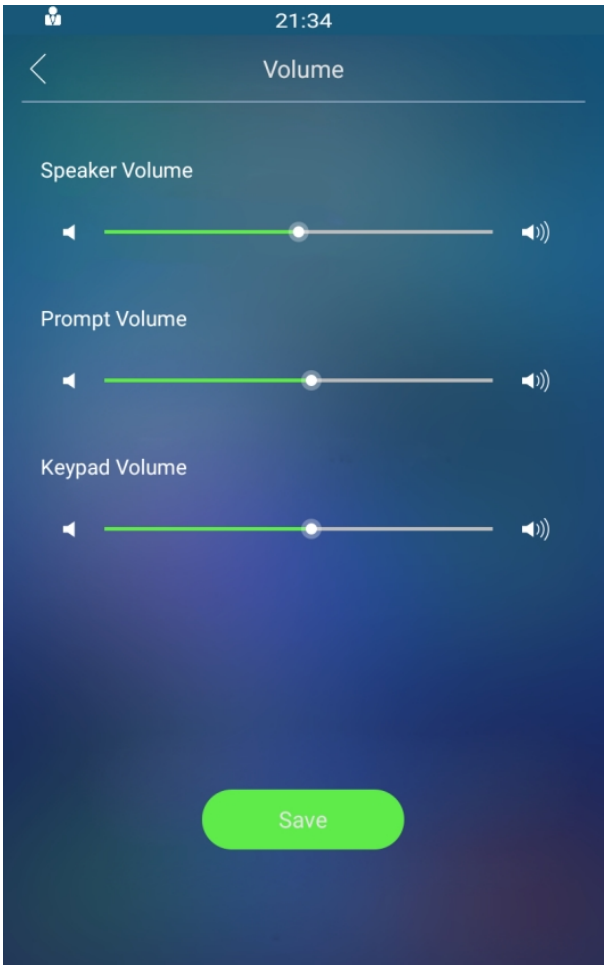
- **Ringback Volume:** The ringback is heard by someone calling the device. The default is 8.

In addition, you can set up call volume on the **Intercom > Call Feature > Others** interface. When it is enabled, users can adjust the volume when they are on calls.



On the Device

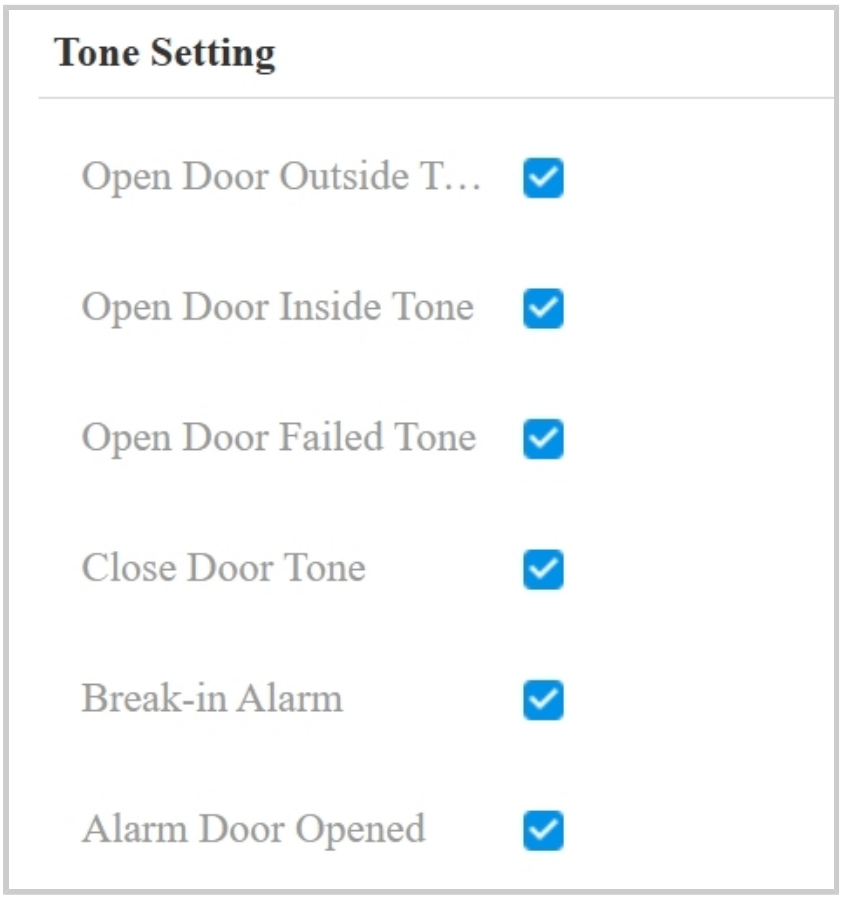
Set up the volumes on the **Setting > Volume** screen.



- **Speaker Volume**: The default is 8.
- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 8.
- **Keypad Volume**: The icon tapping sound. The default is 8.

Door-opening Tones

You can enable or disable various types of door-opening tones on the web **Device > Audio > Tone Setting** interface.



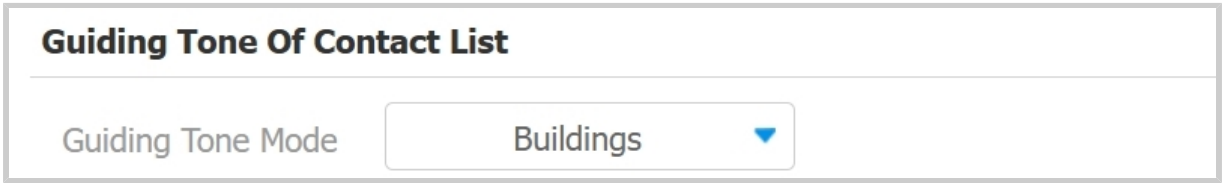
- **Open Door Outside Tone**: The relay-triggered tone. The door-opening tone can be heard when users open doors by the device-supported access methods, except for the exit button.
- **Open Door Inside Tone**: The input-triggered tone. The door-opening tone can be heard when users open doors by pressing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

- **Open Door Failed Tone**: The door-opening failure tone.
- **Close Door Tone**: The door-closing tone.
- **Break-in Alarm**: The tone can be heard when the break-in alarm is triggered. Click here to view how to set up the break-in intrusion alert.
- **Alarm Door Opened**: The tone is heard when the door-opening time exceeds a limit. The time limit can be set on the **Access Control > Input** interface.

Guiding Tone Of Contact List

You can select the guiding tone that sounds when users press Contacts on the device.

To set it up, go to the **Device > Audio > Guiding Tone of Contact List** interface.

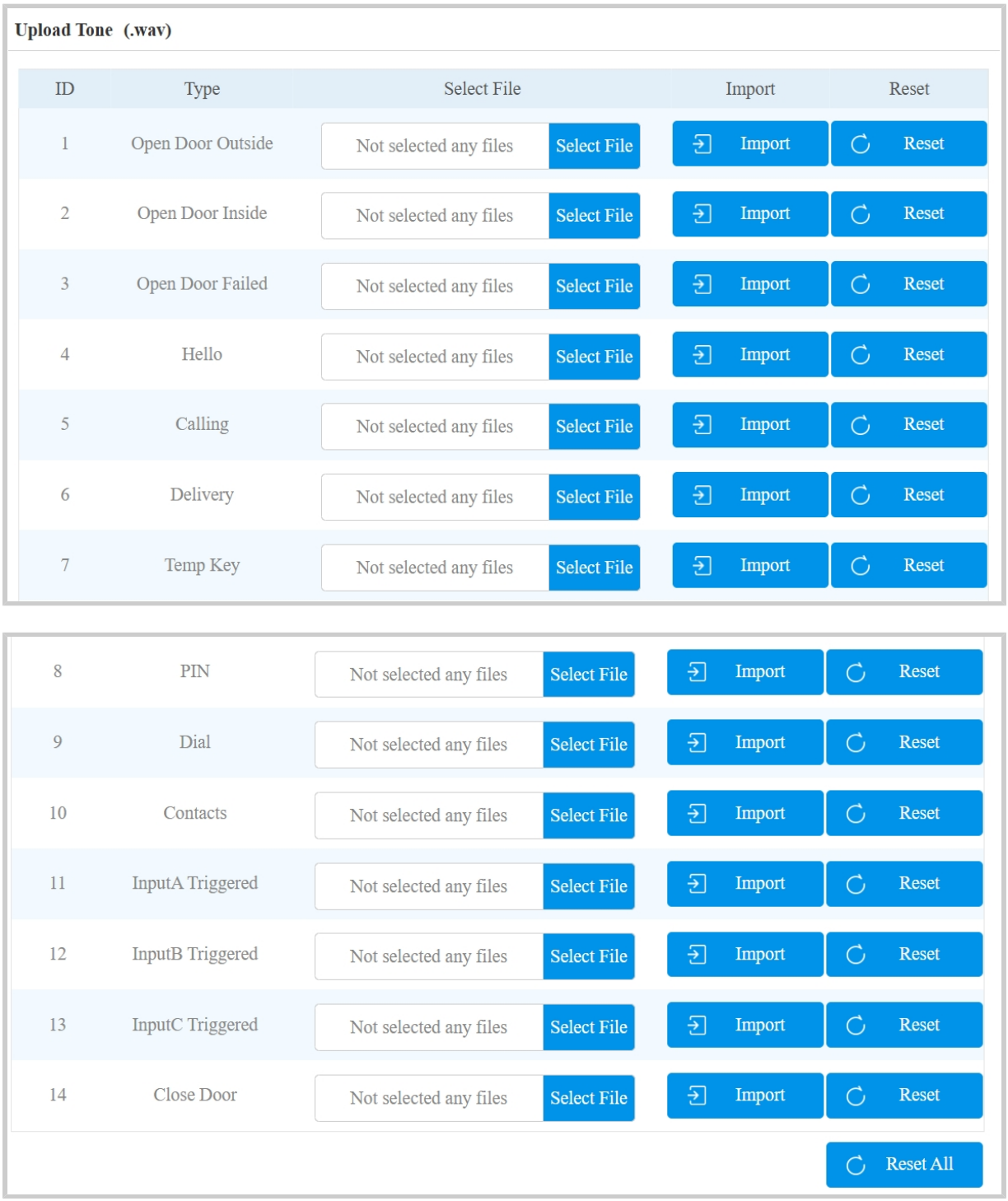


- **Buildings**: The tone is “To search, please enter the name or number. Or just slide down to search.”
- **Apartments**: The tone is “To search, please enter the name or apartment number. Or just slide down to search.”

Upload Tones

You can upload various types of tones on the **Device > Import/Export > Upload Tone** interface. The file should be in .wav format.

- Click **Select File** to choose the file from your drive and click **Import** to upload it.
- Click **Reset** to remove the file.



Visitor-friendly Mode

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

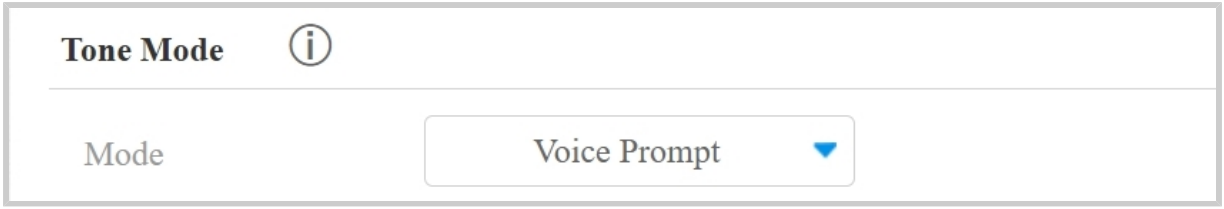
Set it up on the **Device > Audio > Visitor-friendly Mode** interface.



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

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.

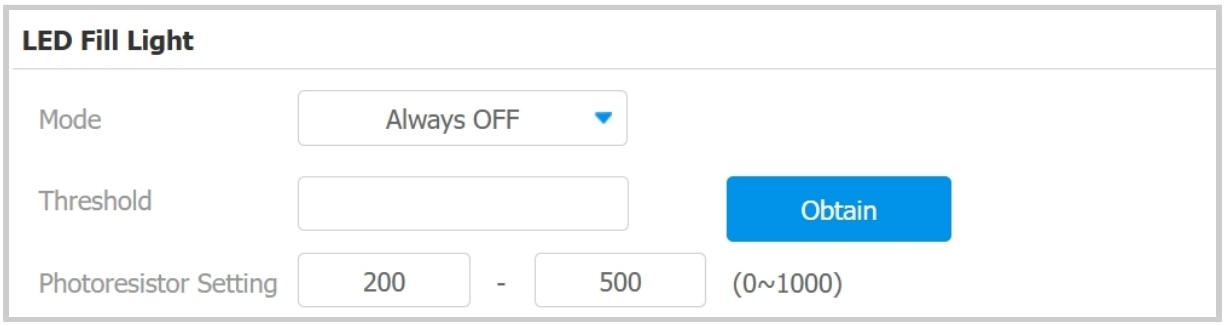
LED and LCD

Infrared LED Setting

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

On the Web

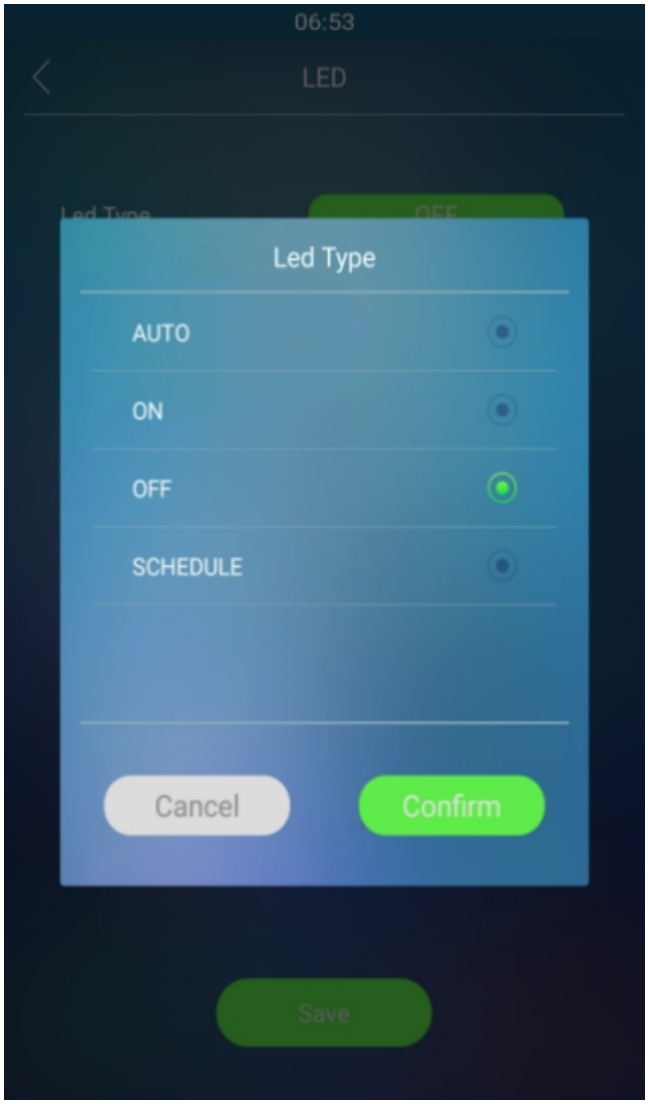
To set it up, go to the **Device > Light** interface.

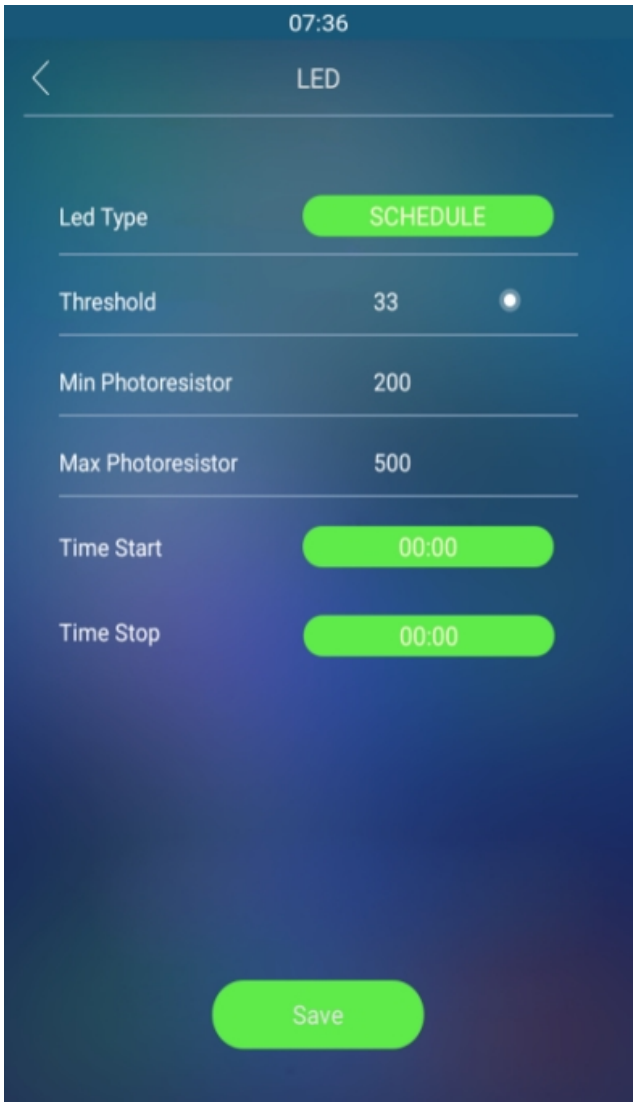


- **Mode**:
  - **Auto**: Turn on the infrared LED automatically based on the minimum and maximum photoresistor value.
  - **Always On**: Enable the infrared LED.
  - **Always Off**: Disable the infrared LED.
  - **Schedule**: Turn on the infrared LED based on the schedule. Specify the Start Time and End Time when this option is selected.
- **Threshold**: The current light intensity indicated by the photo-resistor value. Click Obtain to display the value. The photoresistor values inversely relate to light intensity: higher values indicate lower light and lower values indicate higher light.
- **Photoresistor Setting**: Set the minimum and maximum photoresistor value 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 infrared LED setting on the **Setting > LED** screen.


06:53
LED
Led Type
AUTO
ON
OFF
SCHEDULE
Cancel
Confirm
Save



- **LED Type**:
  - **Auto**: Turn on the infrared LED automatically based on the minimum and maximum photoresistor value.
  - **On**: Enable the infrared LED.
  - **Off**: Disable the infrared LED.
  - **Schedule**: Turn on the infrared LED based on the schedule. Specify the Start Time and End Time when this option is selected.

- **Threshold**: The current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is 33. You can tap the icon  several times to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is the basis of configuring the minimum and maximum photo-resistor values.
- **Min/Max Photoresistor**: Set the minimum and maximum photoresistor value to automatically control the ON-OFF of the LED fill light. The default value is 200 and 500. 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 **Device > Light > LED Control** interface.



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

Screen Backlight 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.

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



- **High Contrast**: Enable High Contrast to enhance the visibility of icons and texts on the screen.
- **Backlight Mode**:
  - **Manual**: Set the backlight brightness value manually.
  - **Auto**: The screen backlight brightness will be adjusted automatically.

Note

The backlight brightness has two automatic modes, Day and Night. They are determined by the photoresistor.

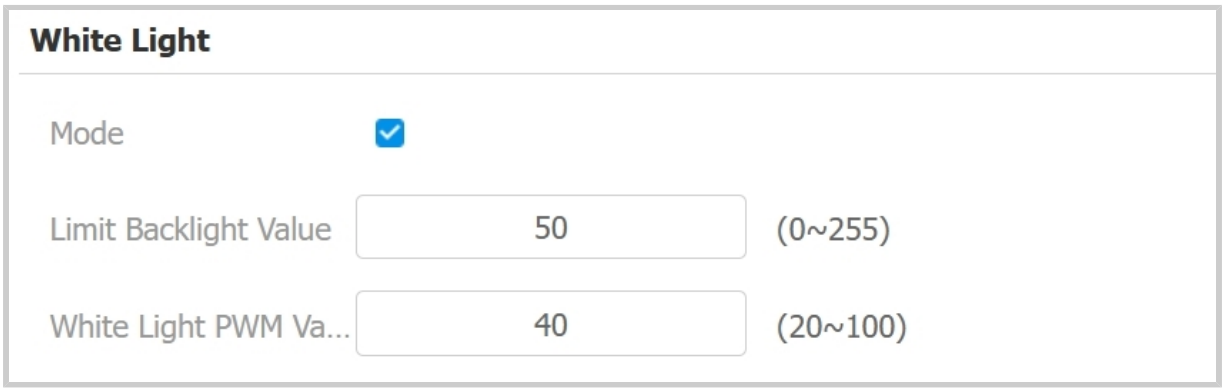
- If the current value is between the minimum and maximum photoresistor, the device is in Day mode.
- If the current value is higher than the maximum photoresistor, the device is in Night mode.

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

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.



- **Limit Backlight Value**: Set the white light value from 0-255. The default is 50.

- **White Light PWM Value**: Set the white light PWM value from 20-100. 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 brighter white light. In short, the higher the PMW value is, the brighter the light is.

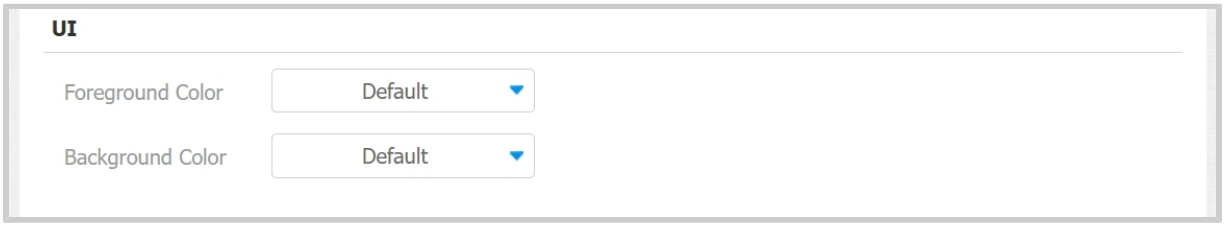
Screen Display

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

You can configure the home screen background and the foreground colors for the **Villa**, **Building**, and **Office** modes.

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



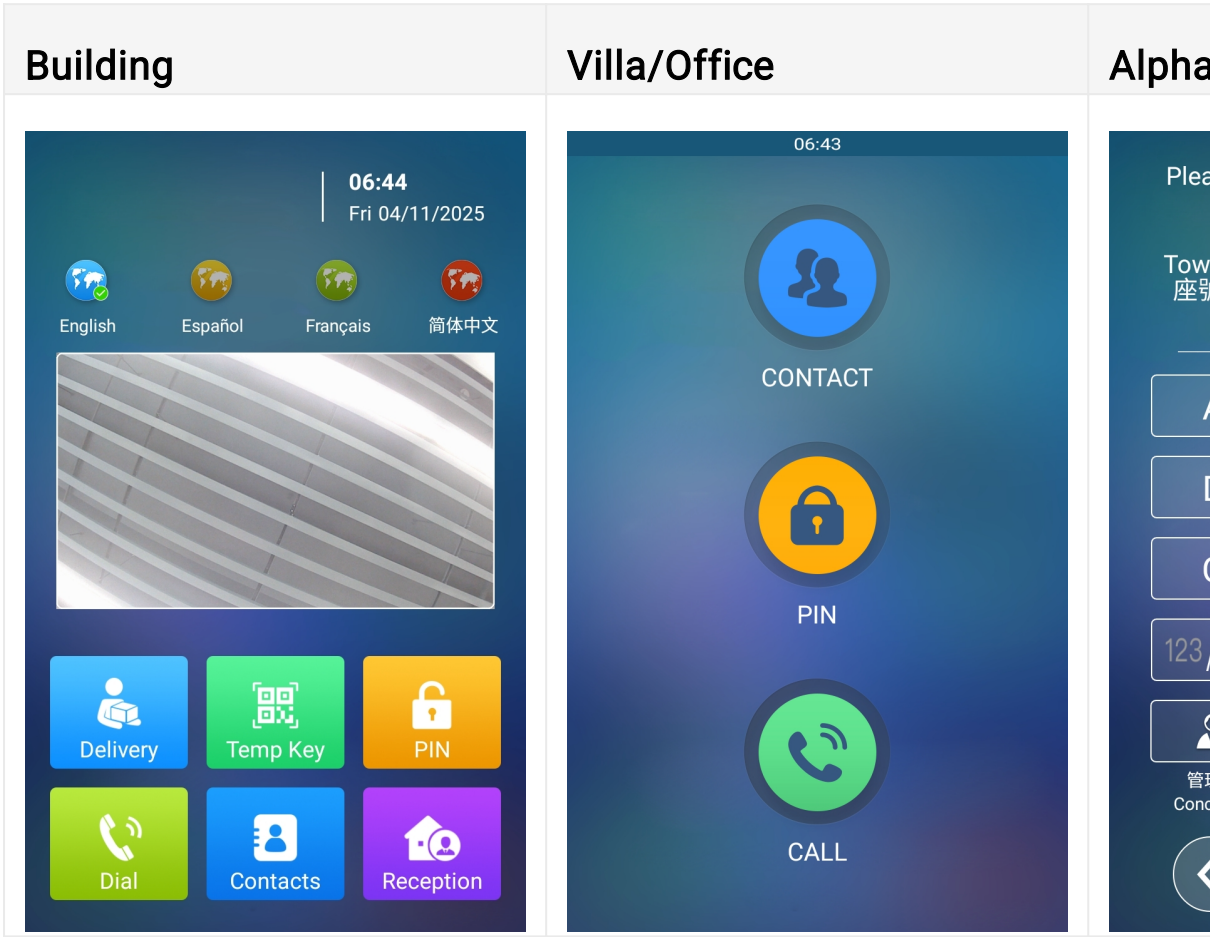
- **Foreground Color**: Select from Default, Black, White, or Custom. When Custom is selected, click Submit before setting the color manually.
- **Background Color**: Select from Default, Black, White, or Custom. When Custom is selected, click Submit before setting the color manually.

Home Screen Display Theme

The device supports four themes: Villa, Building, Office, and Alphanumeric. You can apply the desired theme to different scenarios.

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

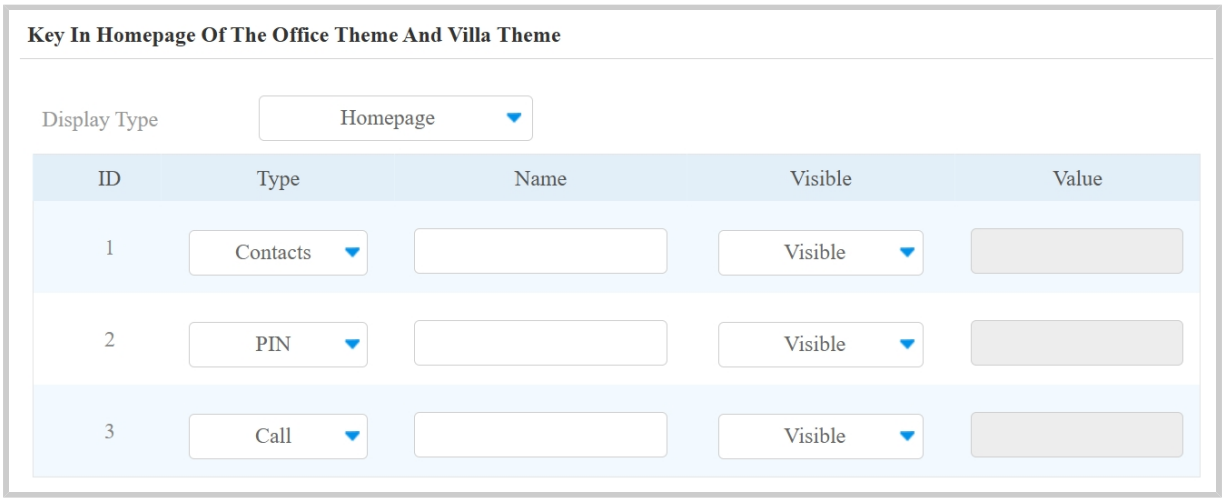




Villa/Office Theme

You can set up the key display, including the PIN, Call, and Contact tabs, in the Villa/Office theme.

Go to the **Setting > Key/Display > Key In Homepage Of The Office Theme And Villa Theme** interface.



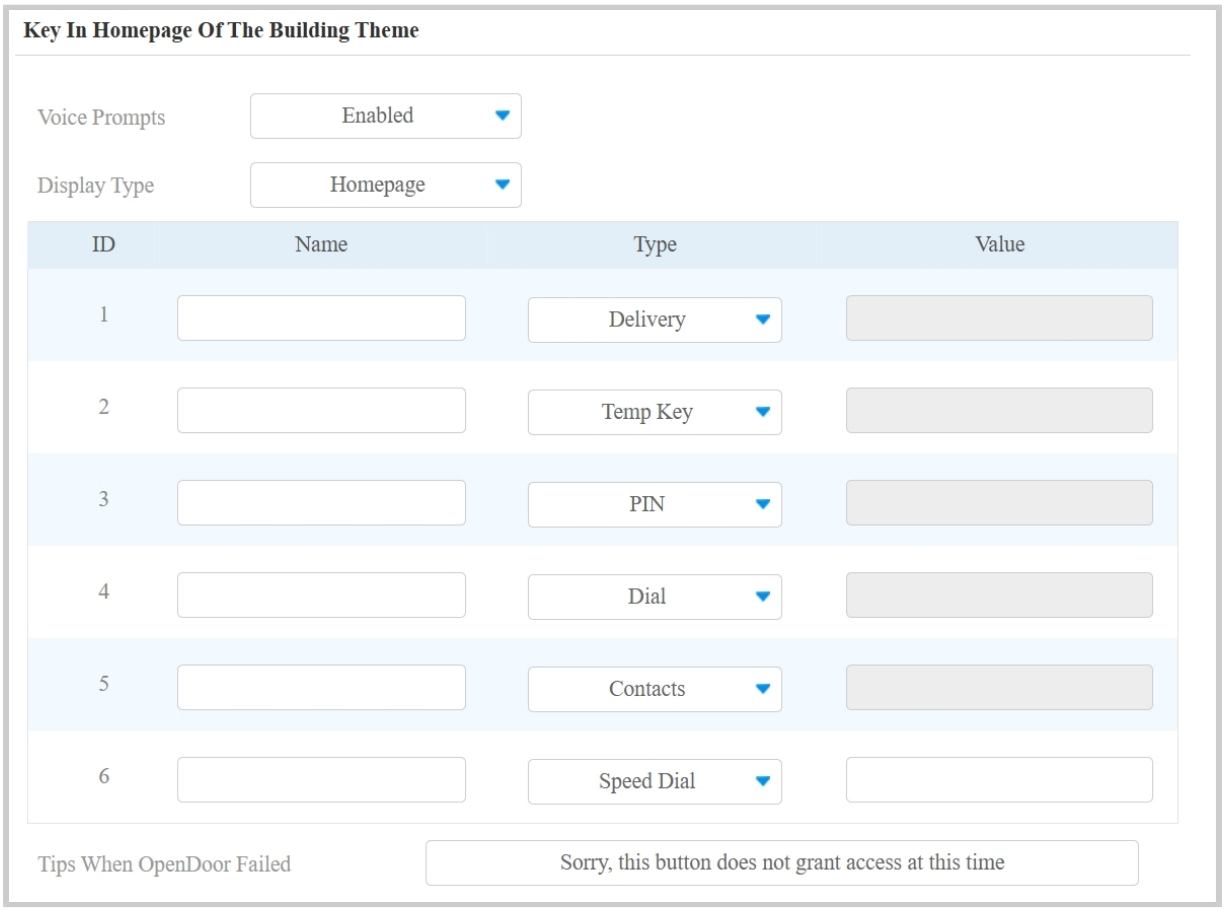
- **Display Type**: Select the homepage display type.
  - **Homepage**: The default display with three vertical round icons, Contact, PIN, and Call.
  - **Dial**: Display the Dial screen as the homepage.
  - **Contacts**: Display the Contacts screen as the homepage.
  - **Password**: Display the PIN screen as the homepage.

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

- **Type**: Select the key to be displayed from Contact, PIN, Call, and Speed Dial.
- **Name**: Name the key. The name will not change the attribute of the key.
- **Visible**: Display the key or not.
- **Value**: Enter the target number when Speed Dial is selected.

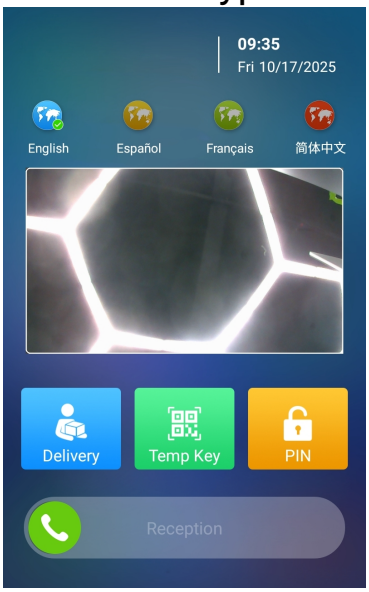
Building Theme

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



- **Voice Prompts**: The voice instruction is played when users press a key on the home screen.
- **Display Type**: Select the homepage display type.
  - **Home Page**: The default displays Delivery, Temp Key, PIN, Dial, Contact, and Speed Dial tabs and the facial recognition box.
  - **Delivery**: Display the delivery screen.
  - **Temp Key**: Display the temp key screen.
  - **PIN**: Display the PIN screen.
  - **Dial**: Display the Dial screen.
  - **Contacts**: Display the Contacts screen.

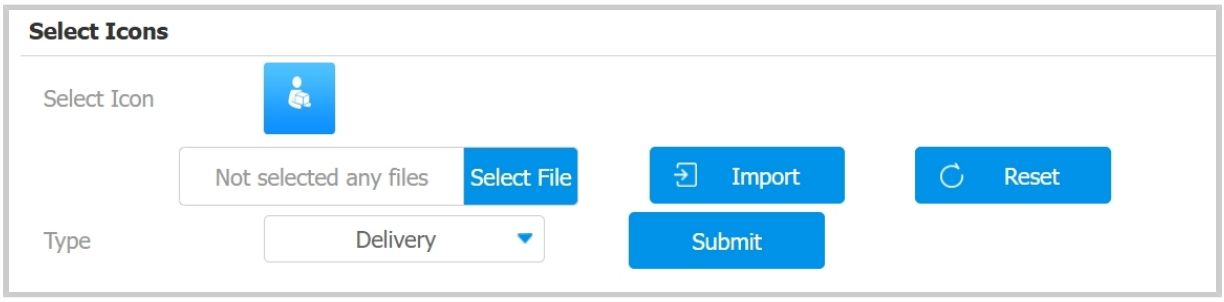
- **Slide to Dial**: Display the slide to dial icon with three function icons on the home screen. When this type is selected, the fourth icon type defaults to **Speed Dial**.



- **Name**: Name the key. The name will not change the attribute of the key.
- **Type**: Select the key type.
  - **Relay**: When Relay is selected, you can specify which relay to trigger and set up the relay schedule.
- **Value**: It is available for those features that need to be set up with numbers, such as Speed Dial.
- **Tips When OpenDoor Failed**: Customize the prompt when the door opening fails.

Besides, you can customize the icon picture for each key. Scroll to the **Select Icons** part.

- Click Select File to choose the picture from your driver and click Import to upload it.
- Click Reset to remove the picture.

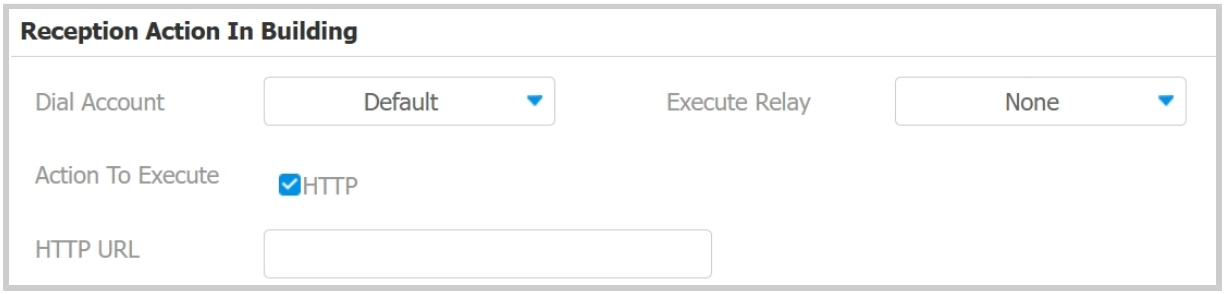


- **Type**: Select the key type.

Reception Tab Setup

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

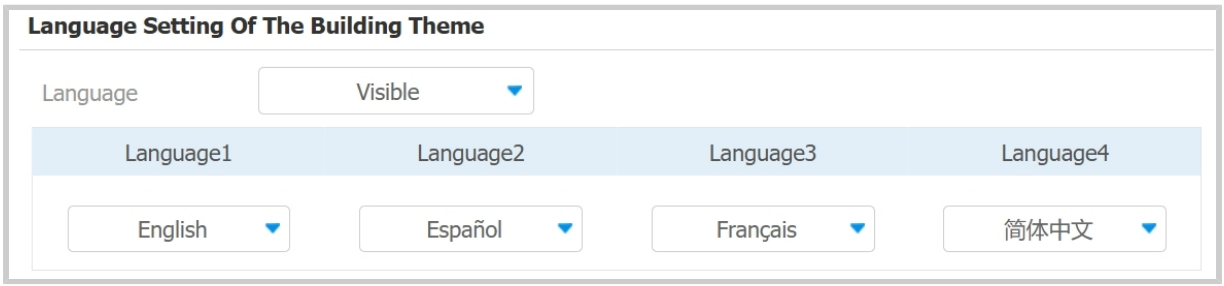
Set it up on the **Setting > Key/Display > Reception Action In Building** interface.



- **Dial Account**: Select the account to make the call. It applies to the registered account. If both accounts are registered, Account1 is used when Default is selected.
- **Execute Relay**: Select the relay to be triggered along with the call.
- **Action to Execute**: Set the action to be triggered with the call. When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
  - **HTTP URL**: Enter the HTTP URL to perform certain actions. The format of sending the message is *http://HTTP server's IP/Message content*.

Language Setting Of The Building Theme

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



- **Language**: When **Invisible** is selected, 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.

Delivery Setting Of Building Theme

The package room feature requires the device's connection to the SmartPlus Cloud.

Enable the feature on the **Setting > Key/Display > Delivery Setting of Building Theme** interface.

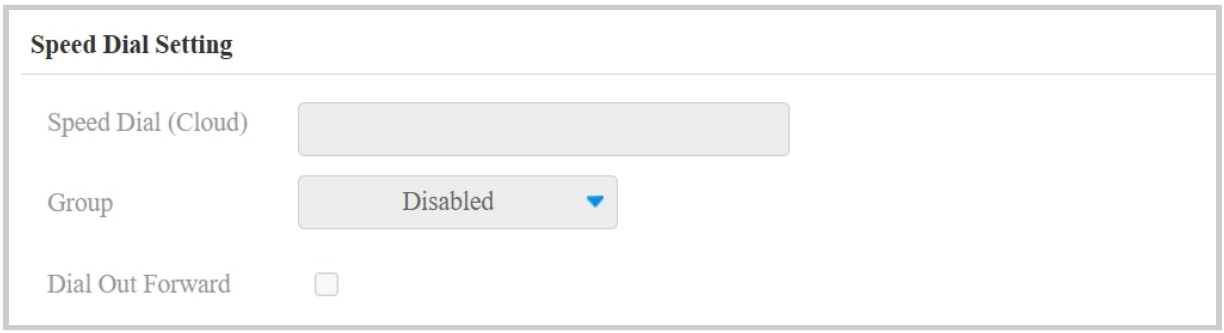


> **Note**
>
> You can click here to view the configuration steps of the package room feature.

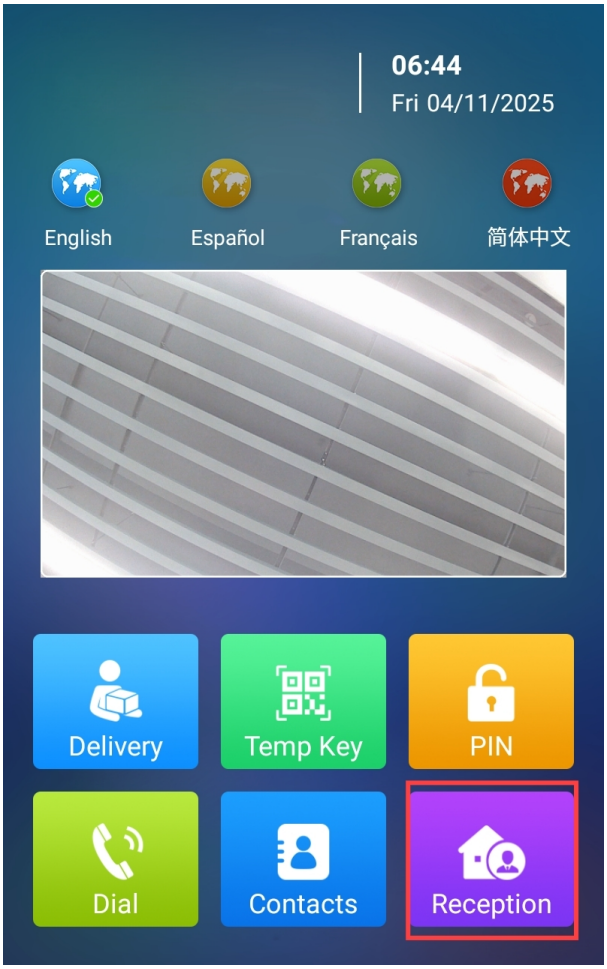
Speed Dial Setting in Villa/Office/Building Theme

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.



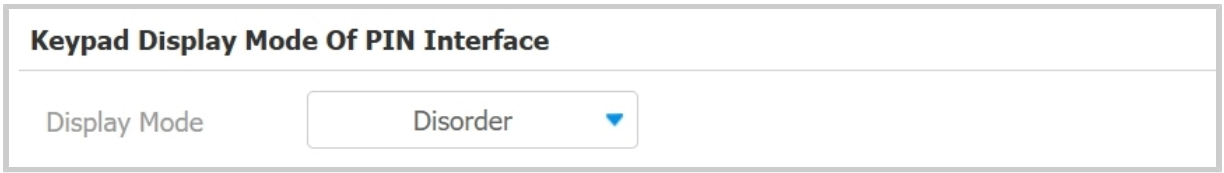
- **Speed Dial(Cloud)**: Display the number(s) configured on the SmartPlus Cloud when the device is connected to the Cloud.
- **Group**:
  - **Disabled**:
    - When the device is connected to the Cloud, Disabled means the call will be made to other devices and the SmartPlus App, based on where it is installed.
    - When the device is deployed locally, the call will be made to the number you fill in the value field of the Speed Dial(Reception) key.
  - [Cloud Group Name]: The call will be made to all contacts in the group. The Cloud group name is the APT name.
- **Dial Out Forward**: When enabled, all calls will be made to the same target number when pressing the Reception button.
  - **Mode**: When Dial Out Forward is enabled, configure the schedule when the feature is working. You can also select **Auto Disable** and decide after how many hours the feature will be turned off.



PIN Keypad Display in Villa/Office/Building Theme

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.

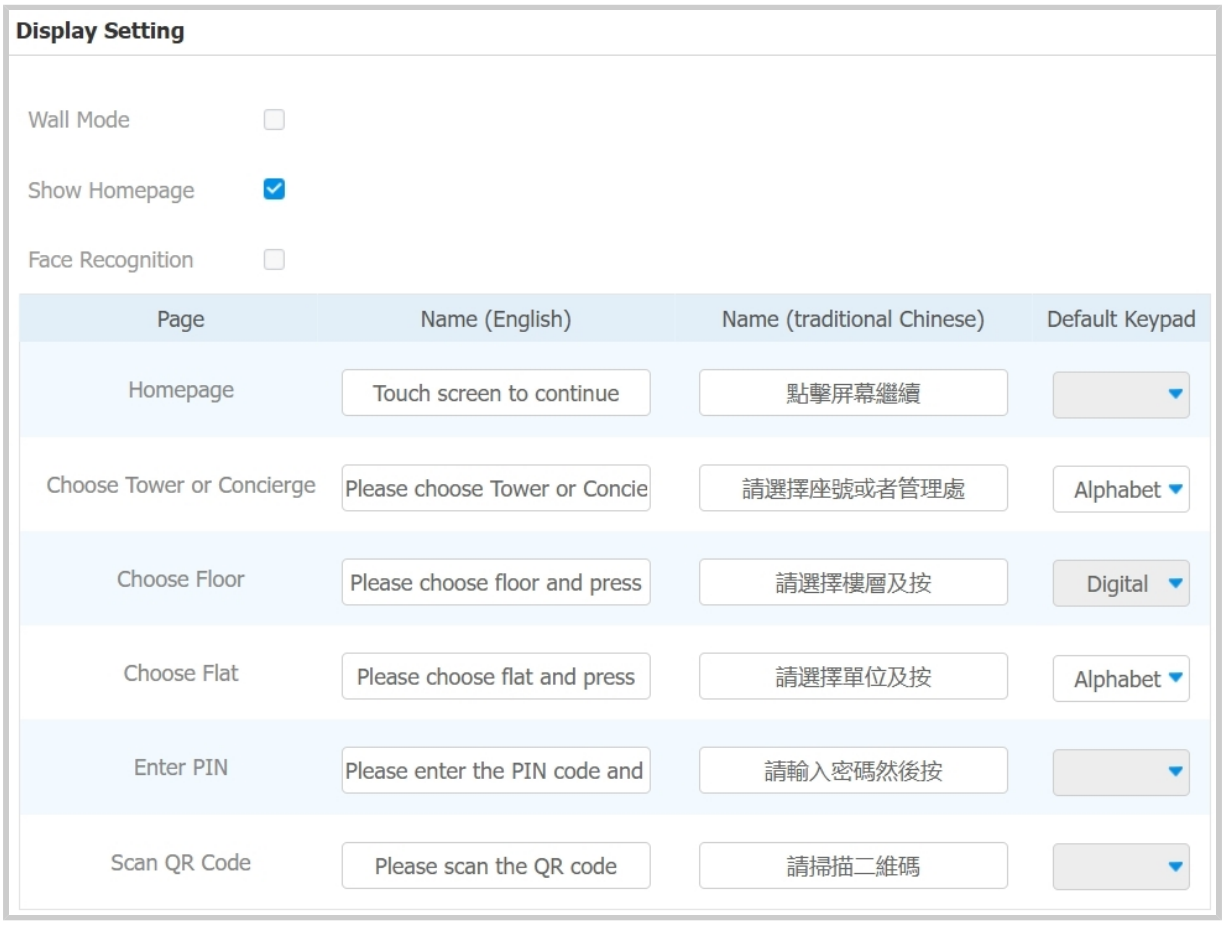
Set it up on the **Setting > Key/Display > Keypad Display Mode Of PIN Interface**.



Alphanumeric Theme

The Alphanumeric Theme is used in the apartment with a 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.
- **Homepage Visible**: 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.

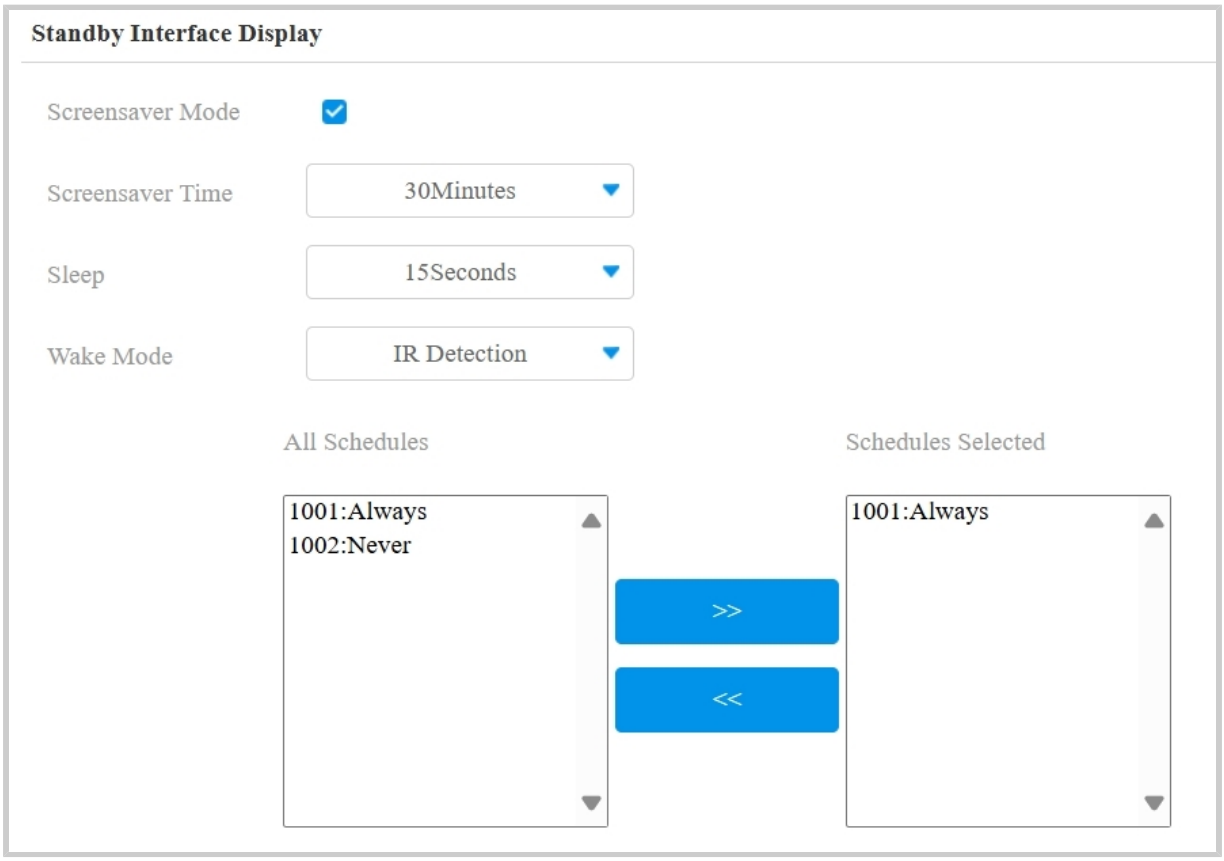
- **Name**: Change the names for the Concierge, QR Code, and PIN icons if needed.
- **Alphabet Keypad**: Select the alphabetical letters you want displayed on the keypad.
- **Digital Keypad**: Choose the numbers and alphabets to be displayed on the digital keypad.
- **Enable Items**: Choose to show or hide the following tabs on the screen: Tower, Floor, and Flat.
- **Flat Length**: Select a maximum length for flats: 1 or less, 2 or less, 3 or less, and 4 or less.
- **Tower Length**: Select a maximum length for towers: 1 or less, 2 or less, 3 or less, and 4 or less.

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 **Device > LCD > Standby Interface Display** interface.

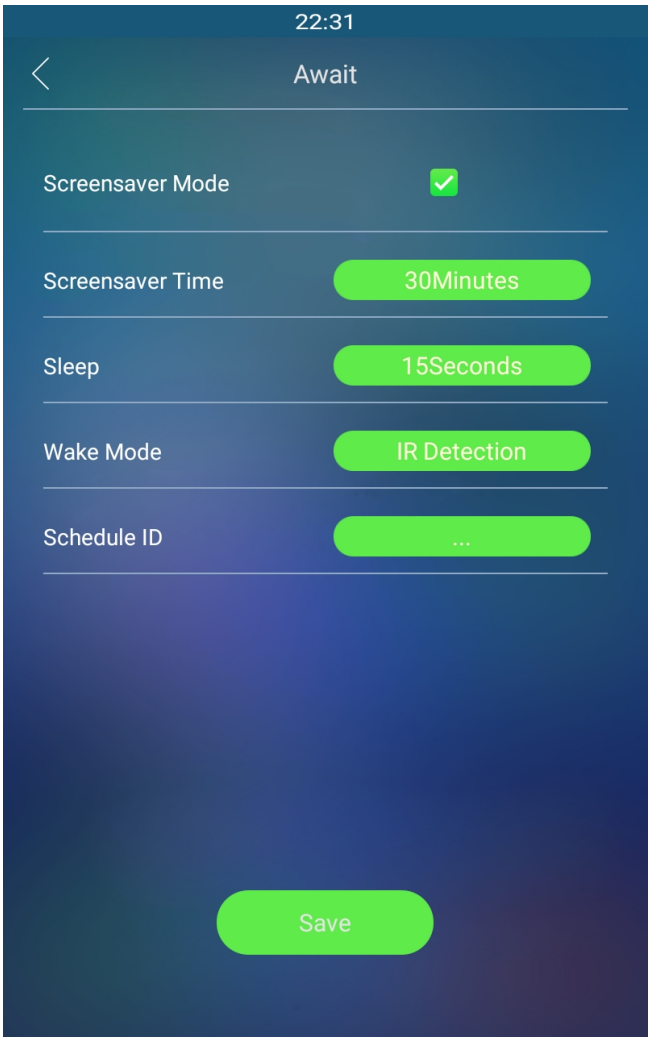


- **Screensaver Time**: The screensaver display duration ranges from 5 seconds to 2 hours. The screensaver display will start when the device goes into sleep mode.
- **Sleep**: Set the time for the device to start displaying screensavers or directly turn off. For example, if you set it to 10 seconds, the device will display a screensaver 10 seconds after no one approaches or performs no operation on the device. If the screensaver mode is disabled, the device screen will turn off directly.
- **Wake Mode**:
  - **IR Detection**: Wake up the screen by IR detection. It offers longer range and better detection in poor visibility conditions.
  - **Manual:** Wake up the screen by touching it.
  - **Video Detection**: Wake up the screen by video-based motion detection. Focus on analyzing visual information captured through cameras.

  - **Face & Video Detection**: Wake up the screen by video-based motion detection and facial detection. Simply detecting motion without detecting faces will not wake the screen.
- **Detection Accuracy**: Available only when Wake Mode is set to **Video** or **Video & Face**. Specify the sensitivity of video-based motion detection for waking the device from standby. A higher value increases the detection sensitivity, making the device more likely to wake from standby.
- **Schedule**: Select the schedule when the screensaver settings will be effective.

On the Device

Set up the screensaver on the **Setting > Await** screen.

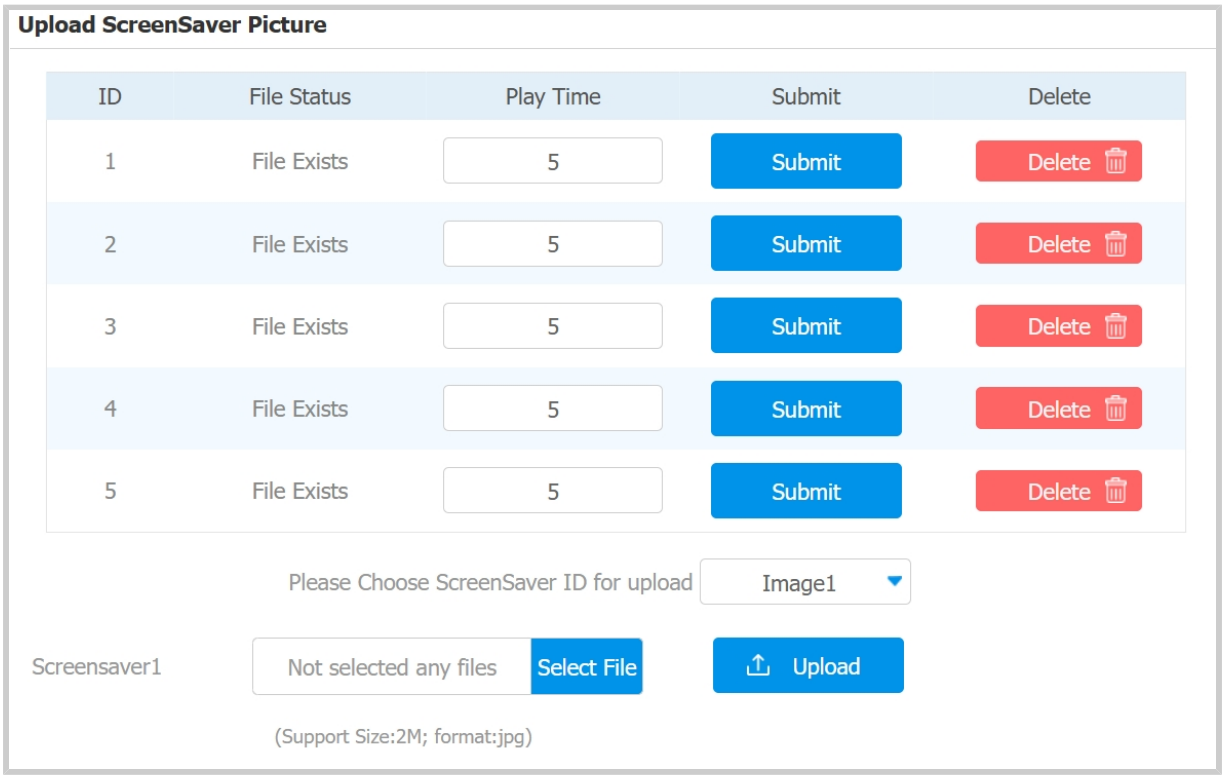


- **Screensaver Time**: The screensaver display duration, ranging from 5 seconds to 2 hours. The screensaver display will start when the device goes into sleep mode.
- **Sleep**: Set the time for the device to start displaying screensavers or directly turn off. For example, if you set it to 10 seconds, the device will display screensavers 10 seconds after no one approaches or no operation on the device. If the screensaver mode is disabled, the device screen will directly turn off.
- **Wake Mode**:
  - **IR Detection**: Wake up the screen by IR detection.
  - **Manual:** Wake up the screen by touching it.
  - **Video Detection**: Wake up the screen by video-based detection.
- **Schedule ID**: Select the schedule when the screensaver settings will be effective.

Upload Screensaver

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

Set it up on the **Device > Import/Export > Upload Screensaver Picture** interface. You can upload a maximum of 5 pictures, and each picture will be displayed in rotation according to the ID order with the specific time duration (**Play Time**) you set.



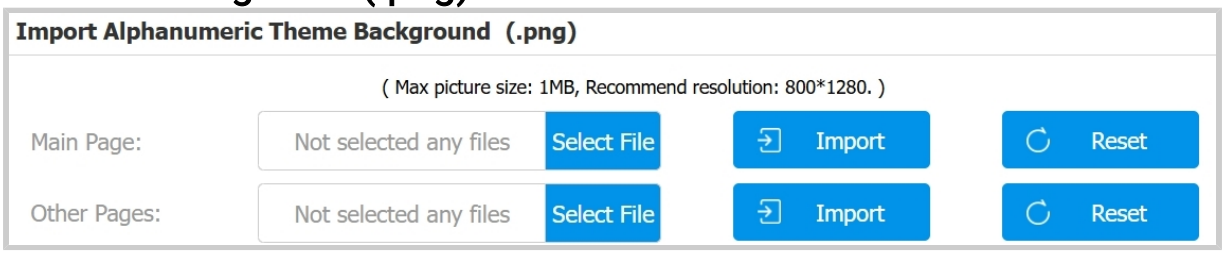
- **Play Time**: The time for playing the screensaver picture. The time ranges from 0 to 120 seconds. The picture will not be shown if the time is 0.

Note

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

Upload Pictures for Alphanumeric Mode Screen Display

Set it up on the **Device > Import/Export > Import Alphanumeric Theme Background(.png)** interface.

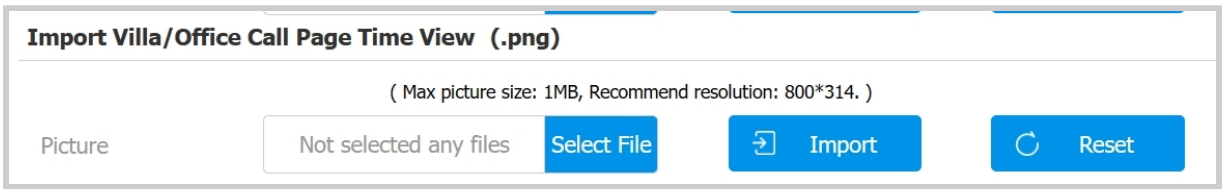


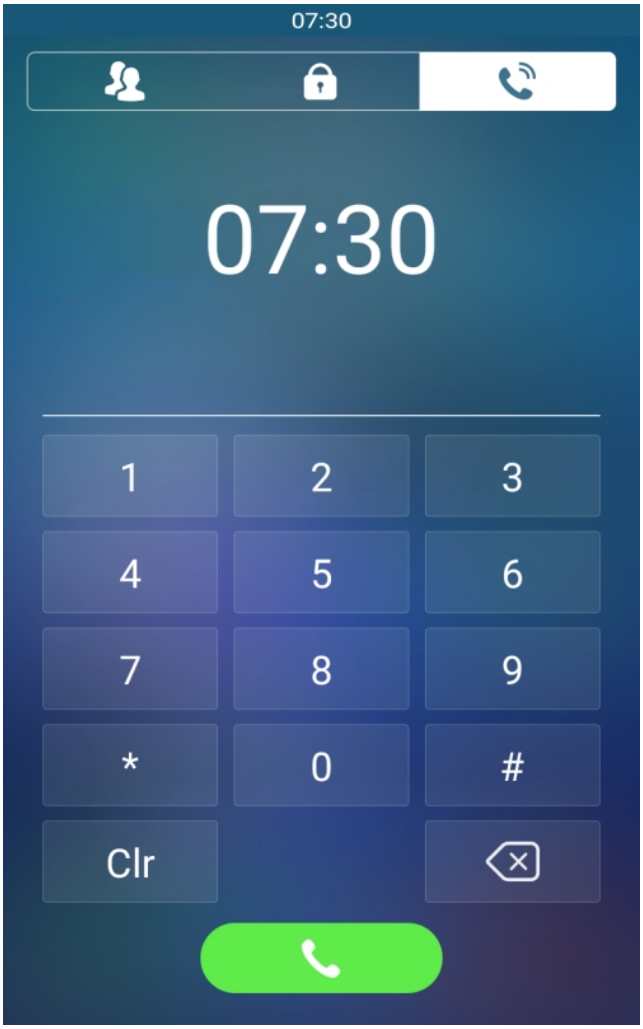
- **Main Page**: The poster display. Visitors need to tap the poster (screen) to access the home screen.
- **Other Pages**: The background images for screens other than the poster display.

> **Note**
>
> - The pictures uploaded should be in .png format; the max picture size is 1MB.
> - This function can be applied to both the home screen background and the contact screen background.
> - The recommended picture resolution is 800*1280.

Upload Background Picture in the Time-displaying Area

You can upload pictures on the web **Device > Import/Export > Import Villa/Office Call Page Time View** interface as the background for the time-displaying area on the dial screen in Villa/Office mode.





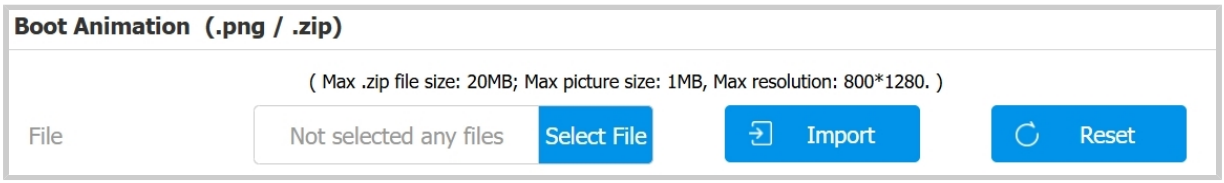
Note

- This function can only be applied in the Villa/Office mode.
- Pictures uploaded should be in .png format with 1 MB maximum.
- The ideal picture size is 800*314 in order to achieve the best effect.

Upload Device Booting Image

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

Set it up on the **Device > Import/Export > Boot Animation (.png /.zip)** interface.

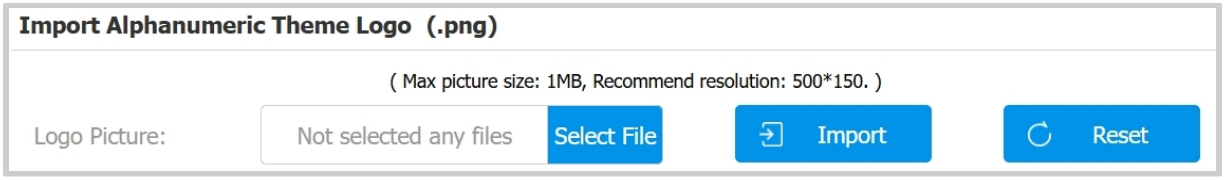


Note

- File format: .png or .zip; Max Size: 20MB for ZIP file, 1MB for PNG picture.
- The recommended resolution is 800×1280.

Upload Device Logo

Upload the logo in Alphanumeric mode on the **Device > Import/Export > Import Alphanumeric Theme Logo (.png)** interface.



Note

- File Format: .png; Max Size: 1MB.
- The recommended resolution is 500×150.

Unlock Options Display

Users can select relay(s) to be triggered when the device is connected to more than one door lock.

To display the unlock options, go to **Access Control > Relay > Unlock Options** interface.

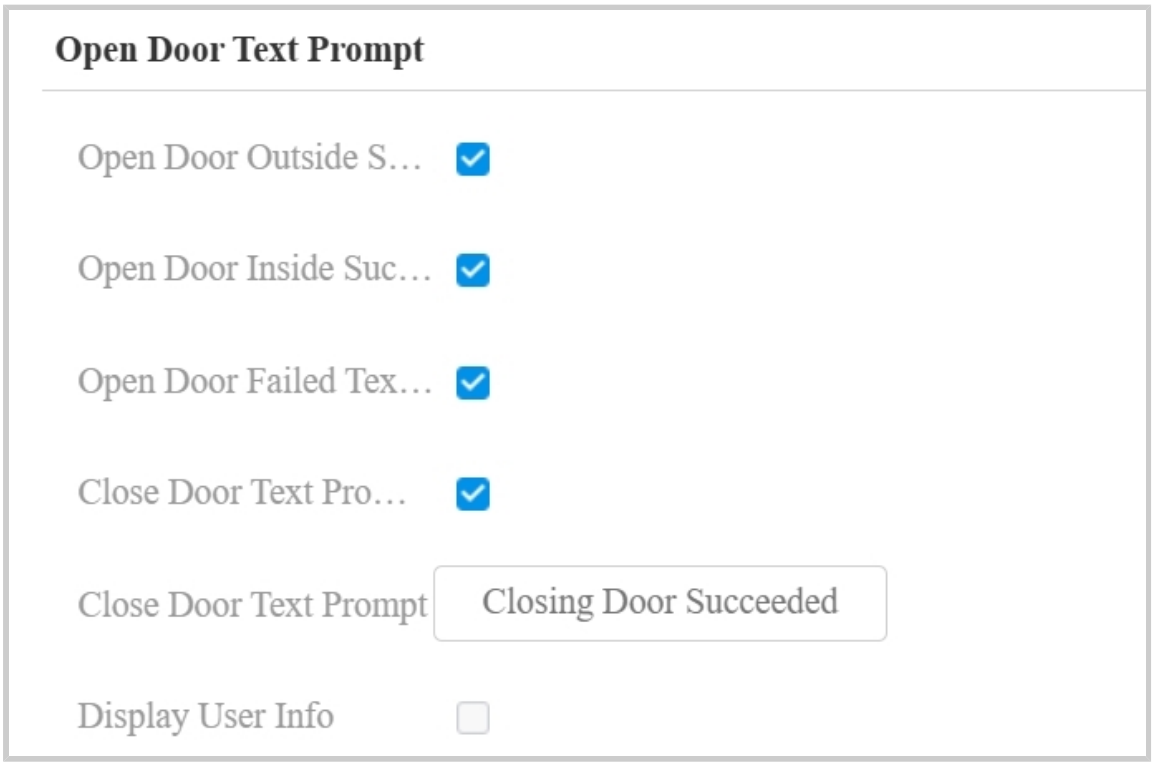


> **Note**
>
> Click here to view the detailed configuration.

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.

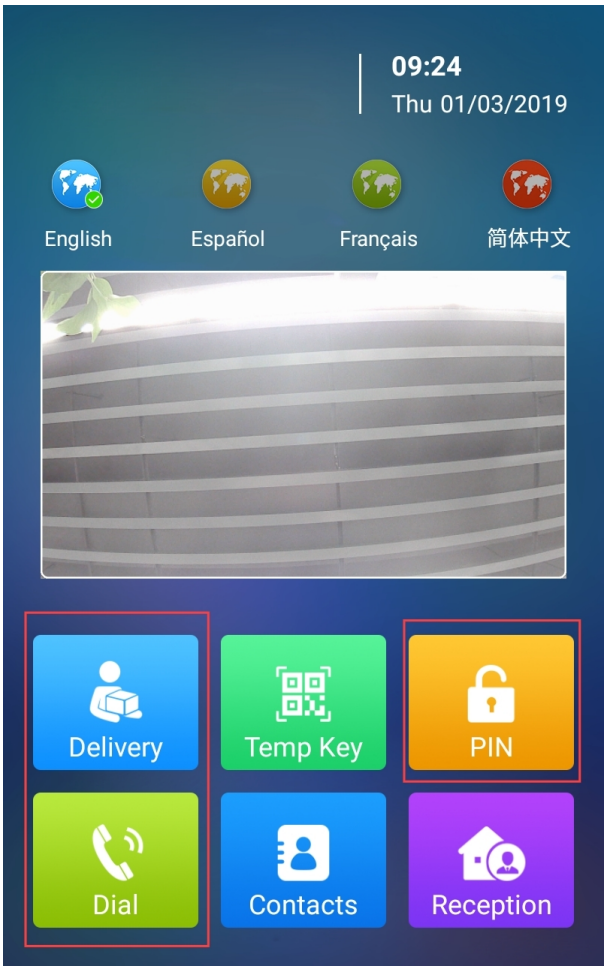
To set it up, go to the **Access Control > Relay > Open Door Text Prompt** interface.



- **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 Enable**: 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.
- **Close Door Failed Text Prompt**: The default is Closing Door Succeeded. You can customize it with up to 63 characters.
- **Display User Info**: Display the user information after users use their credentials. If opening doors succeeds, the user name will pop up on the device screen.

Keyboard Interface Text Prompt

You can customize the text prompts displayed on the device PIN entering, Delivery, and Dial screen. Users can be better instructed to enter codes or numbers.



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

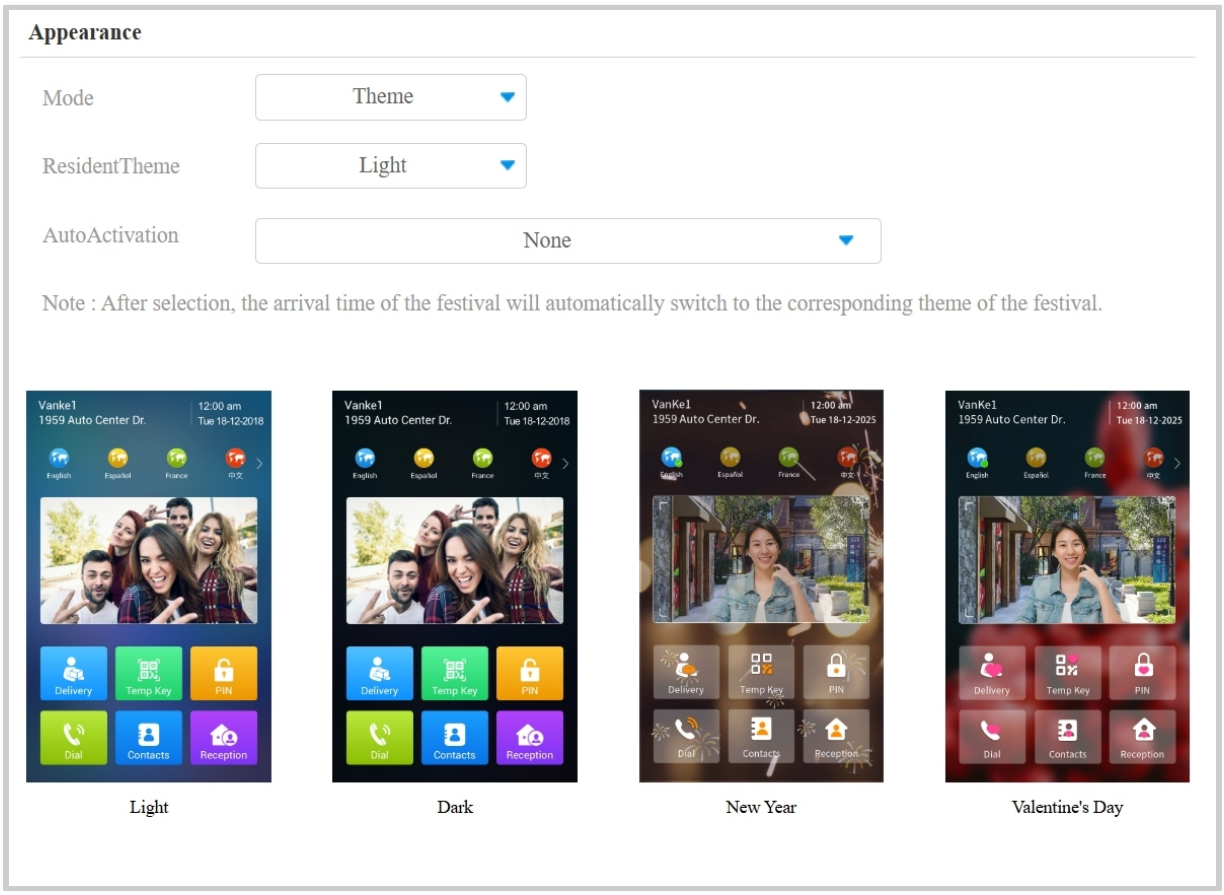


- **PIN**: The default is “Please input your PIN”.
- **Delivery**: The default is “Please enter your delivery PIN”.
- **Dial**: The default is “Please enter the number to call”.

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.

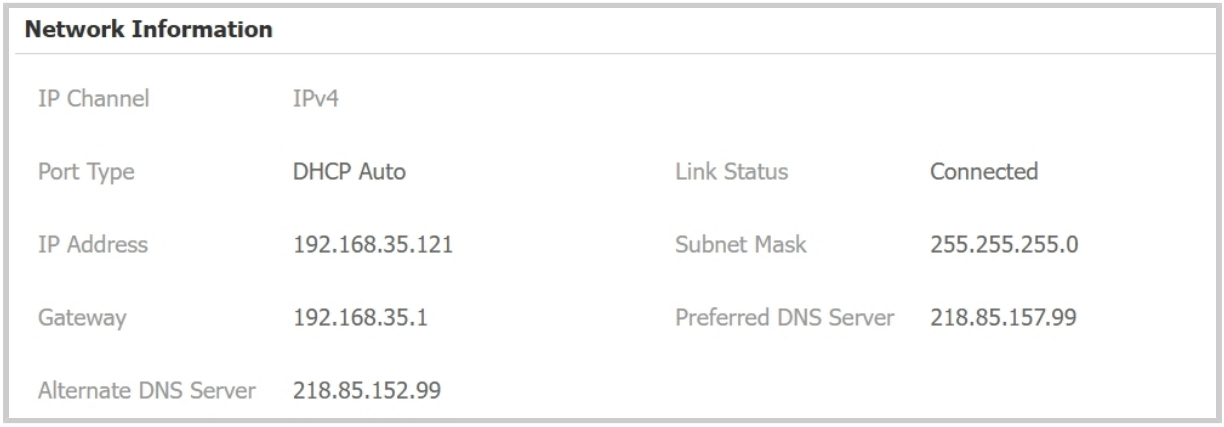
    - **Customization**: When selected, you can upload icon pictures for desired tabs, such as PIN, Call, and Tenants.
- **Resident Theme**: Select the desired appearance.
- **Auto Activation**: None by default. Select the desired festival appearance(s). The device will automatically switch to the appearance during the festival. The following festivals are supported:
    - New Year - 1.1
    - Valentine's Day - 2.14
    - Earth Day - 4.22
    - Worker‘s Day - 5.1
    - Halloween - 10.31
    - Christmas - 12.25

Network Setting

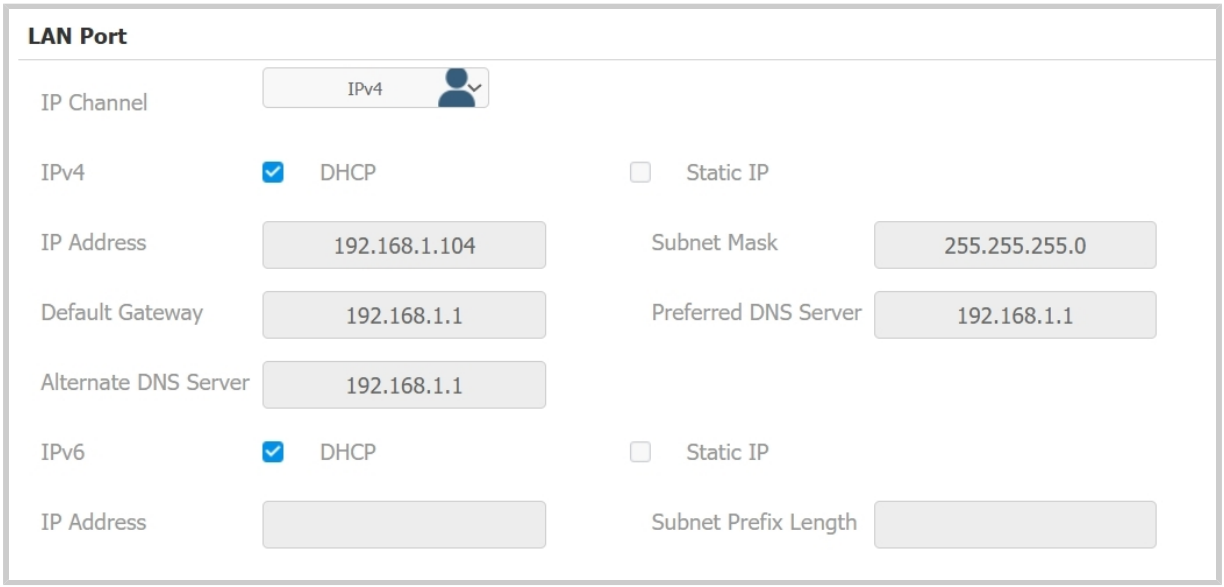
Device Network Connection

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

Check the network on the web **Status > Basic > Network information** Interface.



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



- **IP Channel**: Select the IP channel from IPv4, IPv6, and IPv4&IPv6.

- IPv4/IPv6:
  - DHCP: DHCP mode is the default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
  - Static IP: When static IP mode is selected, the IP address, subnet mask, default gateway, and DNS server address should be configured according to the 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 address, your computer should be on the same local network as the device.
- Subnet Mask: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.
- Default Gateway: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- Preferred/Alternate DNS Server: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The door phone connects to the alternate DNS server when the primary one is unavailable.
- Subnet Prefix Length: Indicate how many bits of an IP address are used to identify the network portion.

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

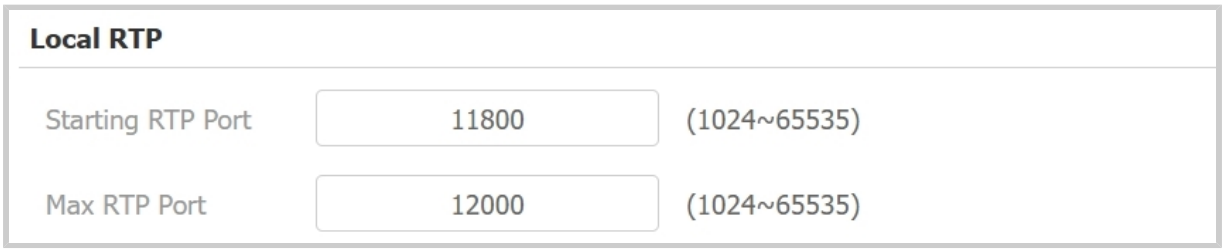


Device Local RTP Configuration

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 **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**: The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.

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

Device Web HTTP Setting

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

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



- **Protocol**: HTTP is enabled by default.

NAT Setting

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

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

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



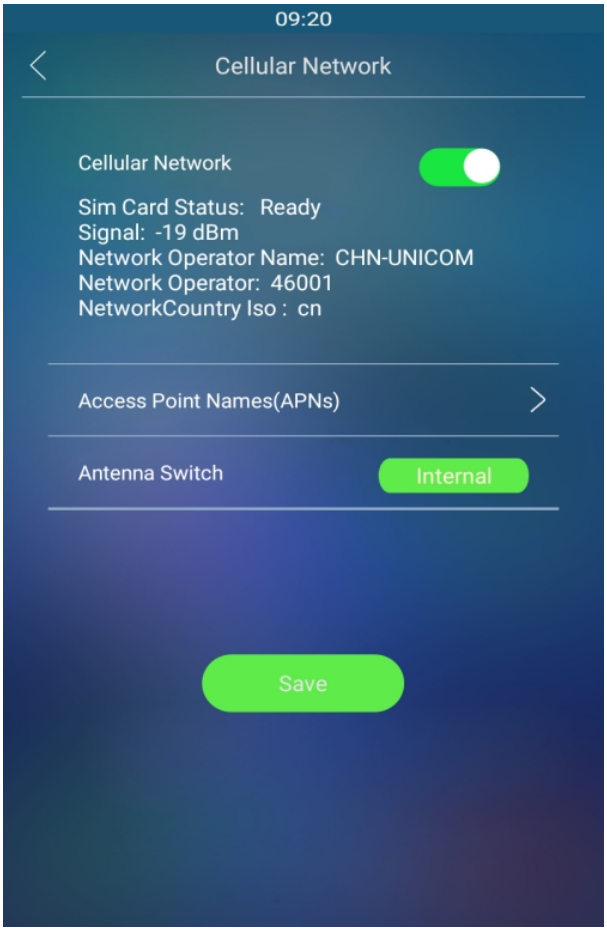
- **UDP Keep Alive Messages:** If enabled, the device will send the message to the SIP server, which will recognize whether the device is online.

- **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.

LTE Wireless Connection (Optional)

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

Only R29C-L has an LTE module, and the LTE setting can only appear after the SIM card is inserted. Set up the LTE on the device's **Settings > Cellular Network** screen.

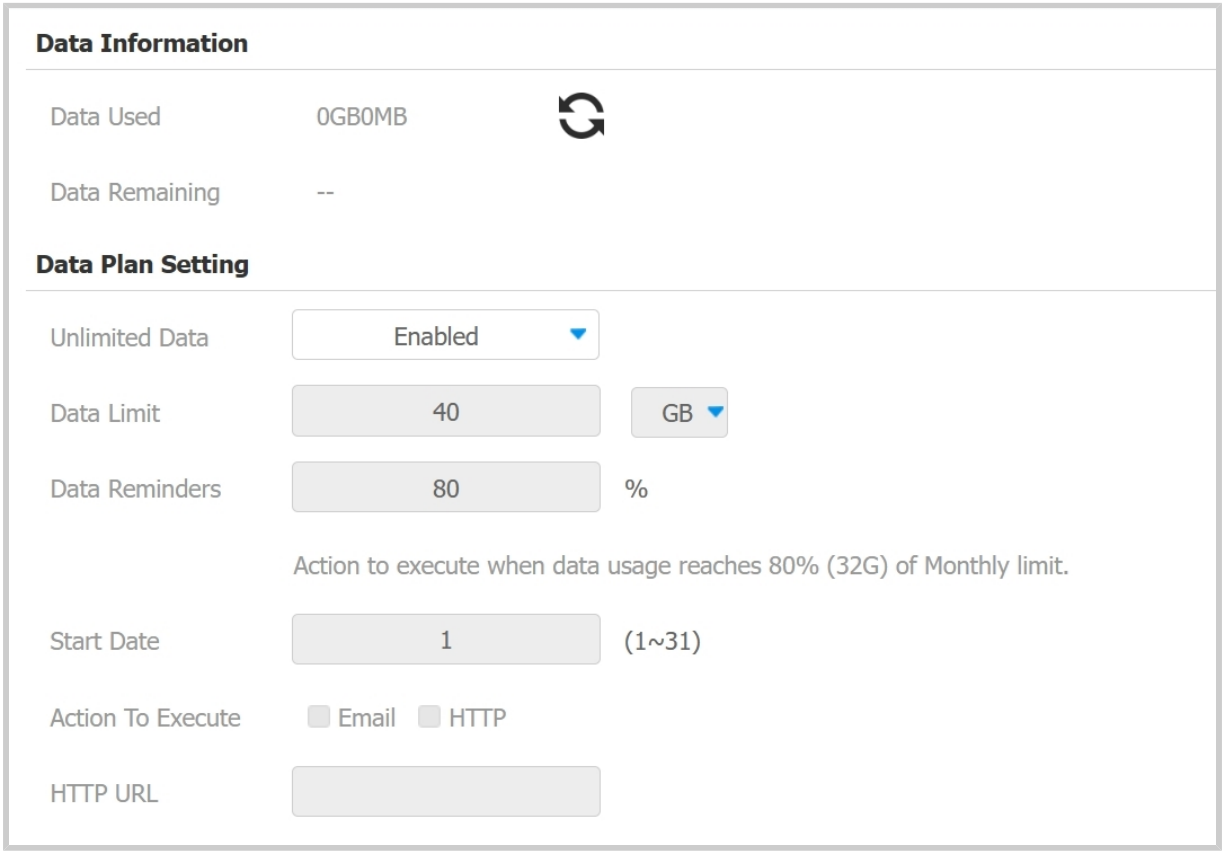


- **Cellular Network**: Move the toggle switch on and off to enable or disable the LTE function.

- **Access Point Name (APNs)**: Enter the settings from your network provider. These can be found from the network provider of your SIM Card; you may have different options for PAYG or Contract sims.
- **Antenna Switch**: Select the internal and external antenna for signal transmission. The internal antenna is a built-in antenna in the device, while the external antenna is optional and is used to reinforce the signal in a compromised network environment.

LTE Data Usage Control

LTE data usage can be checked on the device web **Network > Data Usage** interface.



- **Unlimited Data**: Enable this option if you have an unlimited data plan; otherwise, leave it disabled (default).
- **Data Limit**: Set the data limit based on the plan, either 40 GB or MB.

- **Data Reminders**: Choose a percentage to trigger notifications. For example, at the default of 80%, notifications will be sent when this threshold is reached.
- **Start Date**: Specify the start date for monitoring data usage (1-31). The default is 1. If set to 1, monitoring ends on the last day of the month. If set to 2, it ends at 23:59 on the first day of the next month. For months with fewer than 31 days, monitoring ends on the last day of that month.
- **Action To Execute**: Select Email or HTTP URL to receive notifications when data usage reaches the limit.
- **HTTP URL**: Enter the HTTP URL for notifications.

Intercom Call Configuration

IP Call Configuration

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

Make IP Calls

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

IP Call Setup

Enable IP call on the **Intercom > Call Feature > Direct IP** interface.



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

SIP Call Configuration

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

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

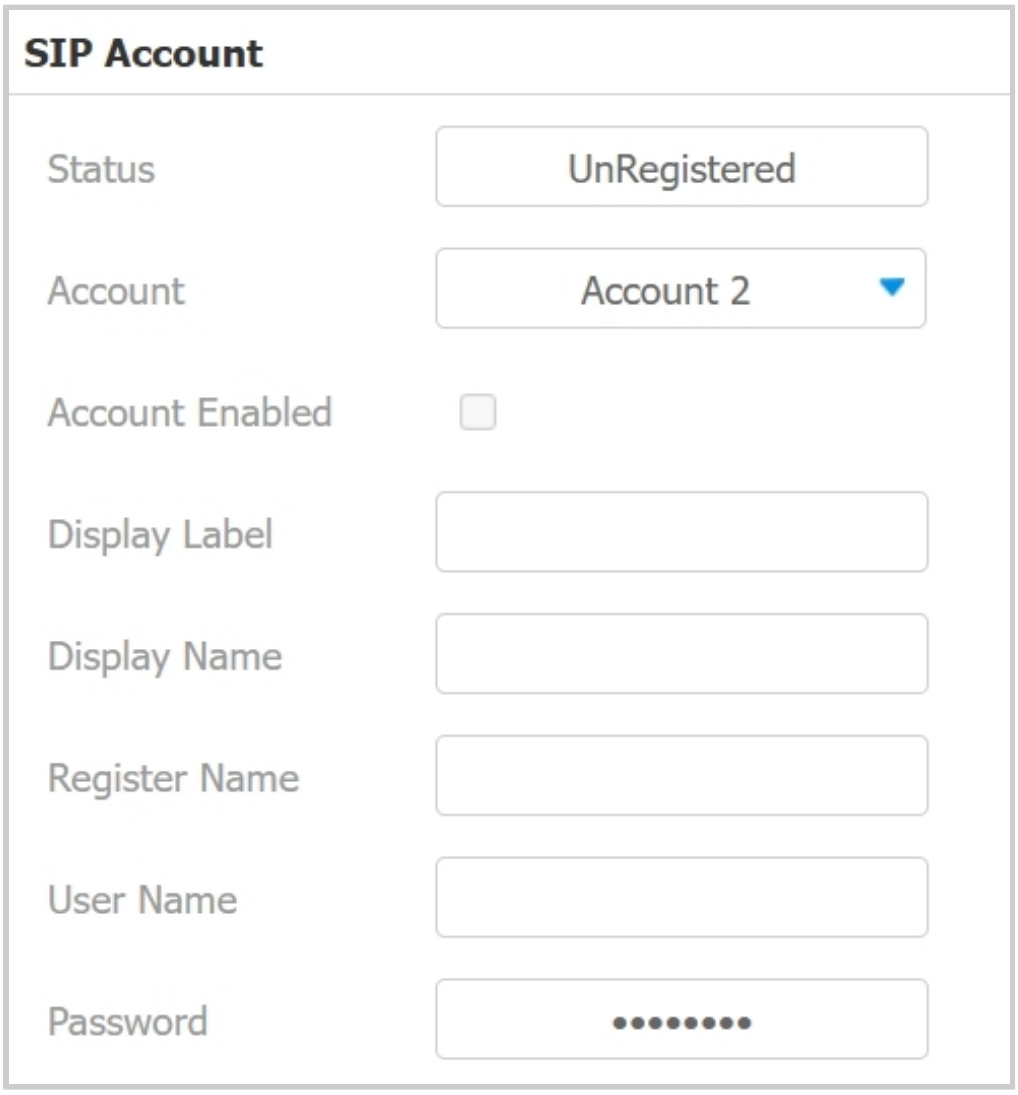
SIP Account Registration

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

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

Click here to view the SIP account registration example.

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



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

Tip

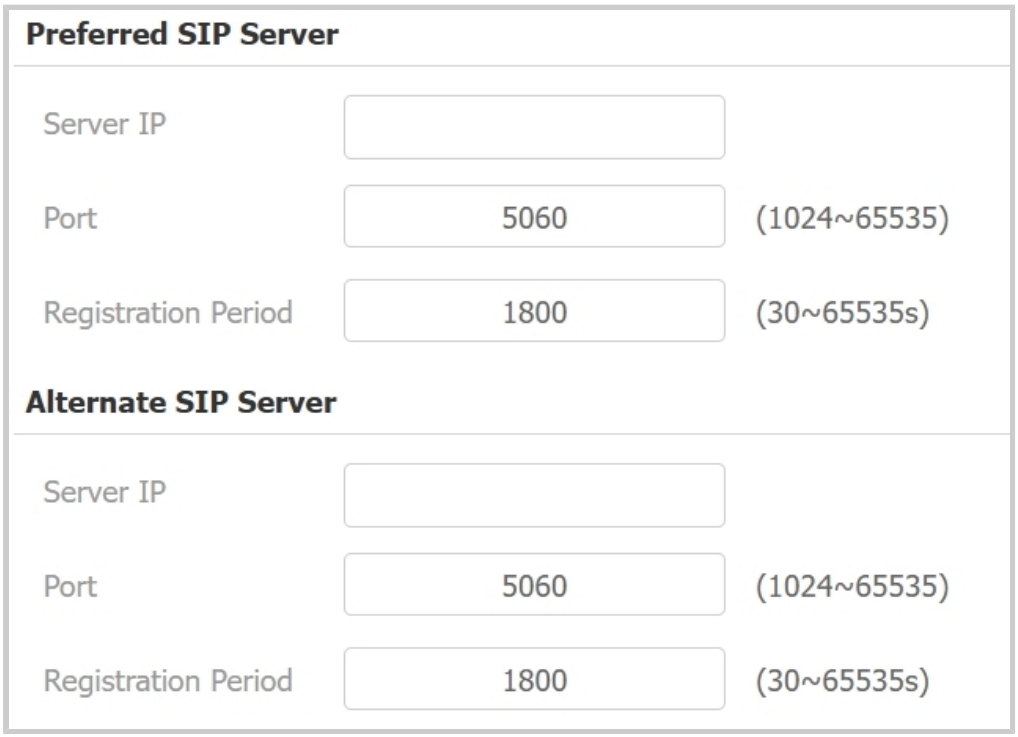
- For configuring contact call and dial plan, see here.
- When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

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

SIP Server Configuration

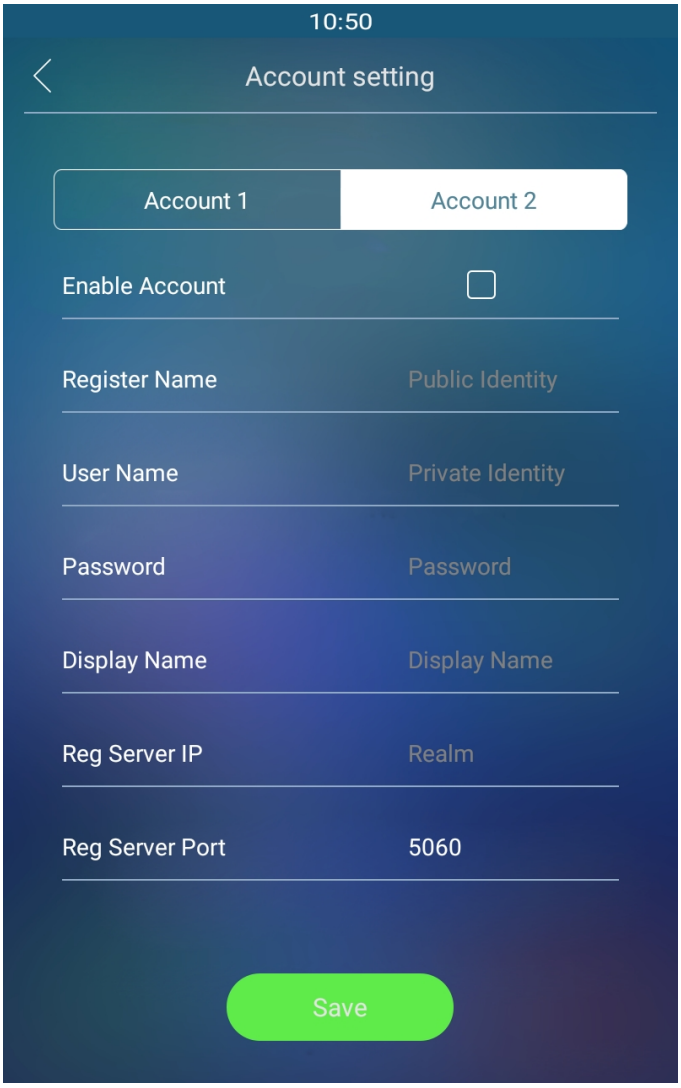
SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

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



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

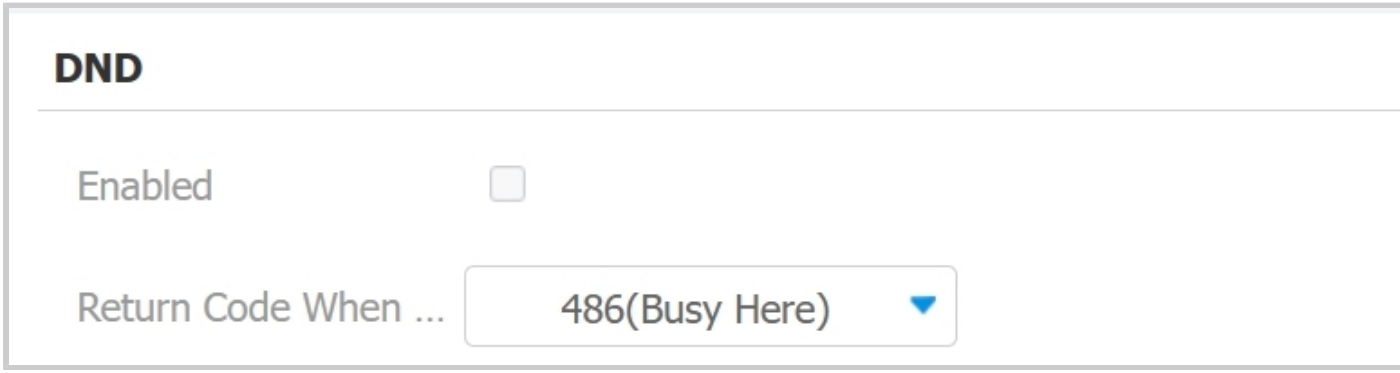
You can also register SIP accounts on the **Setting > Account** screen.



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.

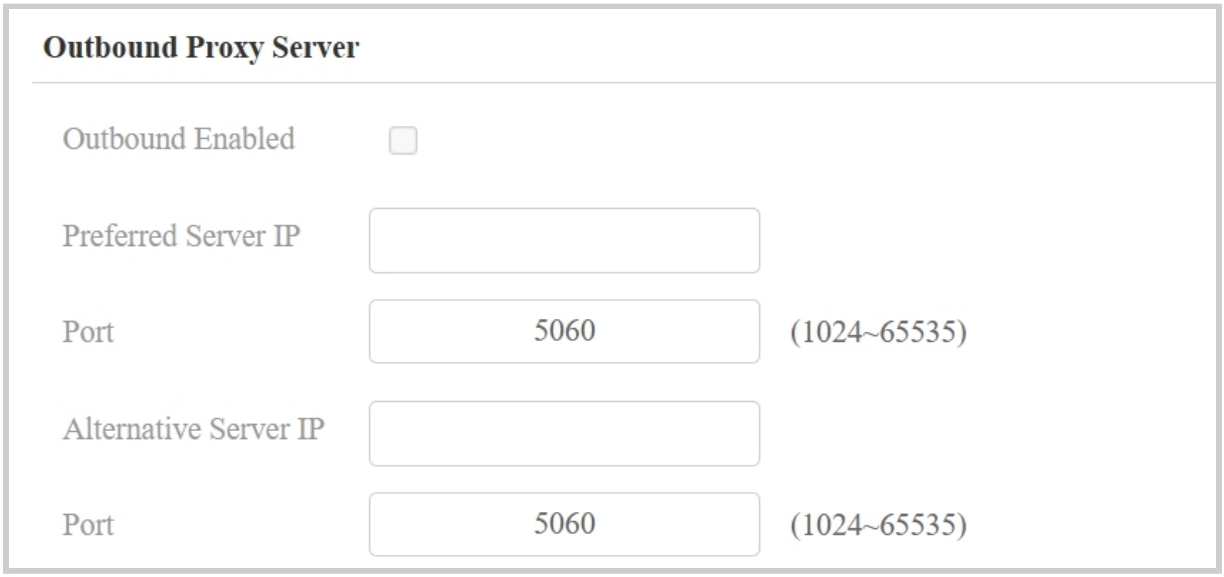


- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

Outbound Proxy Server

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

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



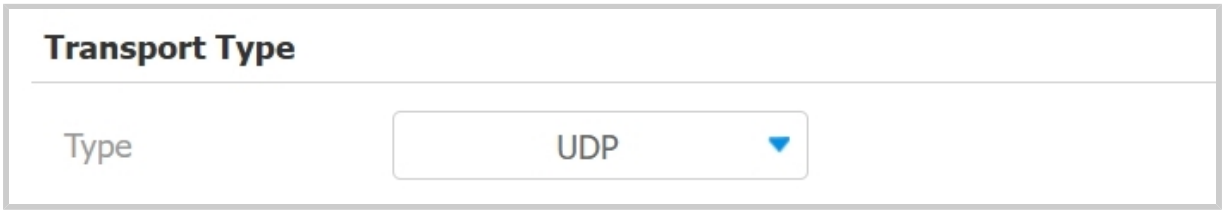
- **Preferred Server IP:** Enter the SIP proxy IP address.
- **Port:** Set the port for establishing a call session via the outbound proxy server.

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

Data Transmission Type

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

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

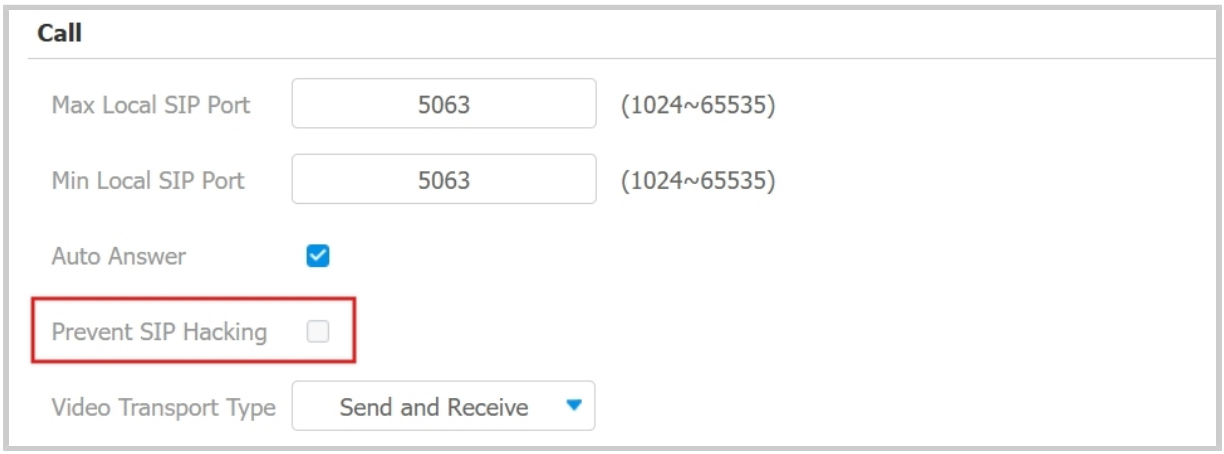


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

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.

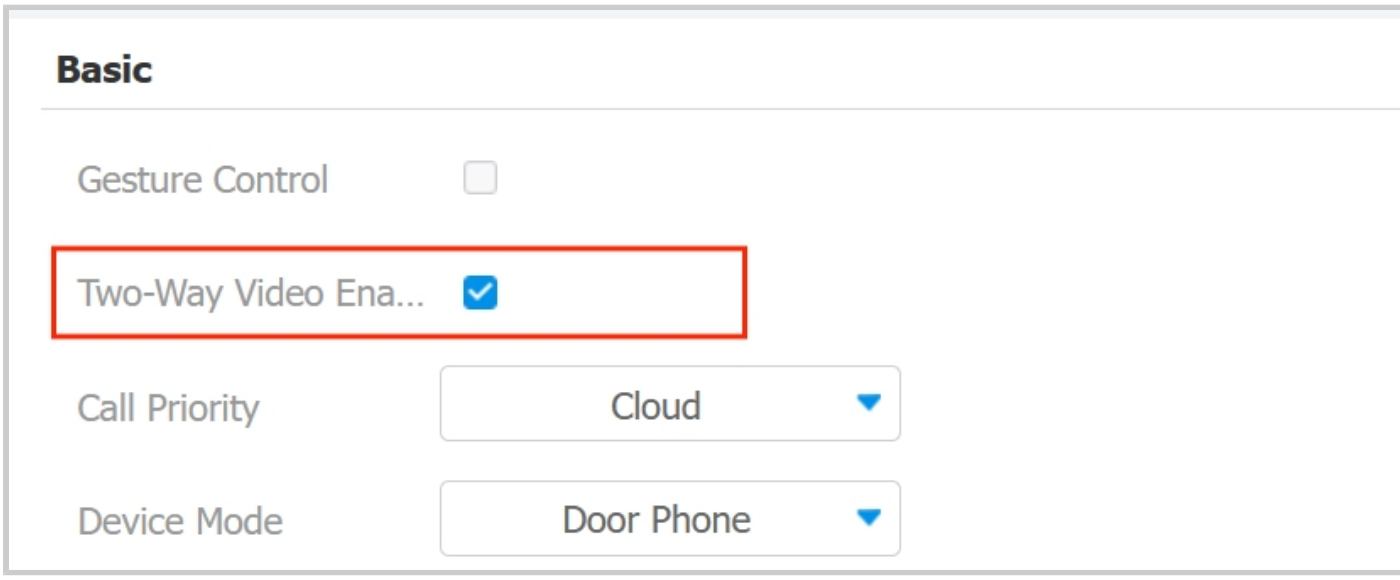
Set it up on the **Account > Advanced > Call** interface.



- **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.

Two-way Video Call

R29 allows you to have two-way video calls with the callee so that you can see the callee's video image. Set it up on the **Intercom > Basic** interface.



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

Video Transport Type

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



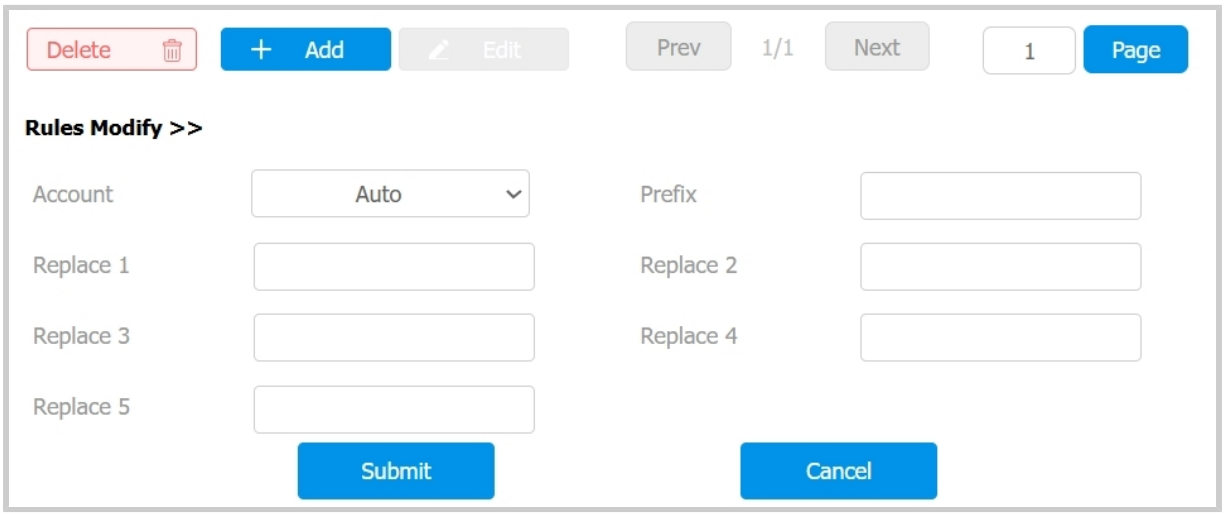
- **Video Transport Type**: It is Send and Receive by default.
  - **Inactive**: Disable the function.
  - **Send Only**: The device sends the video stream to the other party.
  - **Receive Only**: The device only receives the video stream from the other party.
  - **Send and Receive**: The device can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

Call Setting

Quick Dial By Number Replacement

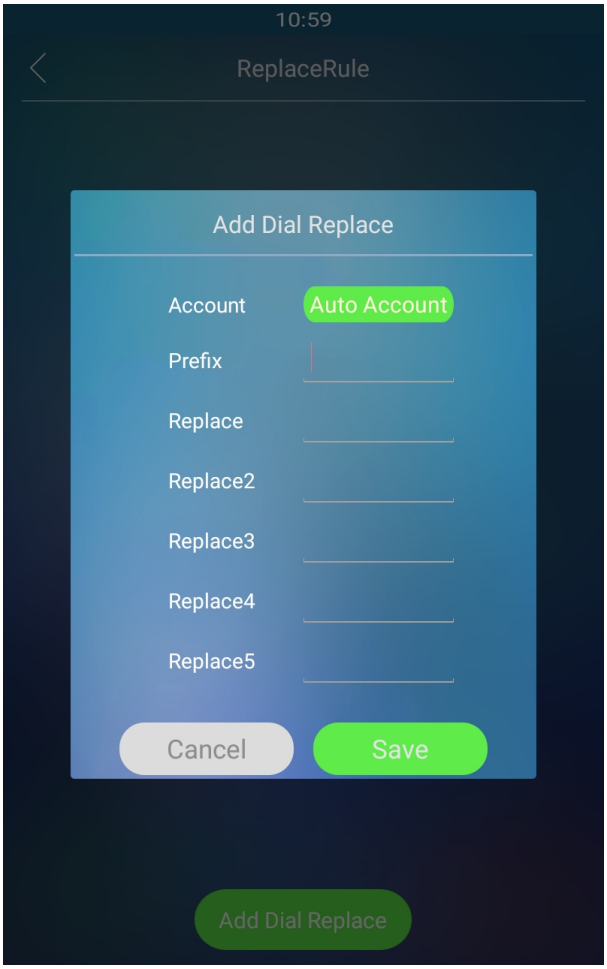
The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

Set it up on the **Intercom > Dial Plan** interface. Click **Add**. You can add up to 1,500 rules.



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

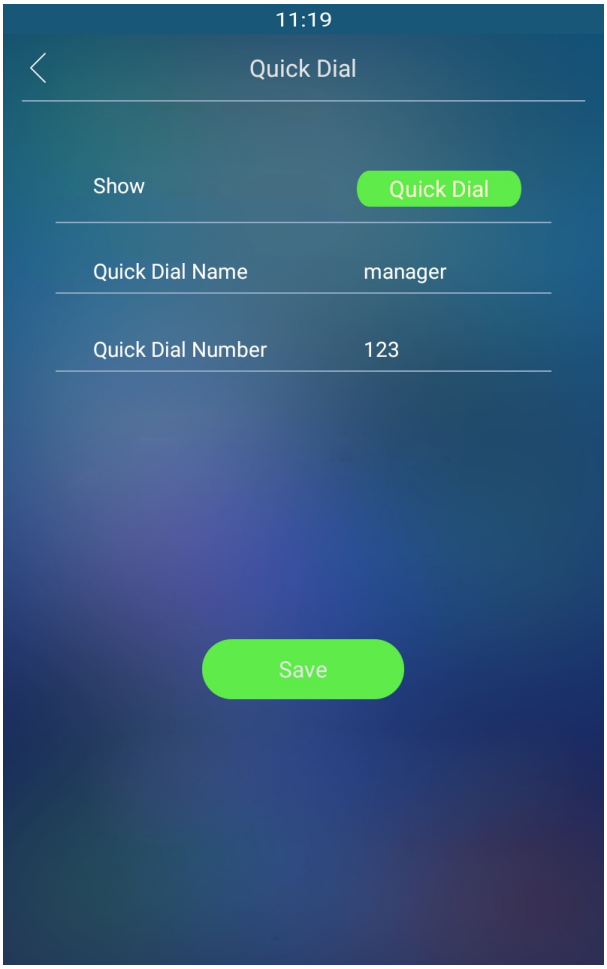
You can also set up the dial plan on the **Setting > Replace Rule** screen. Tap **Add Dial Replace**.

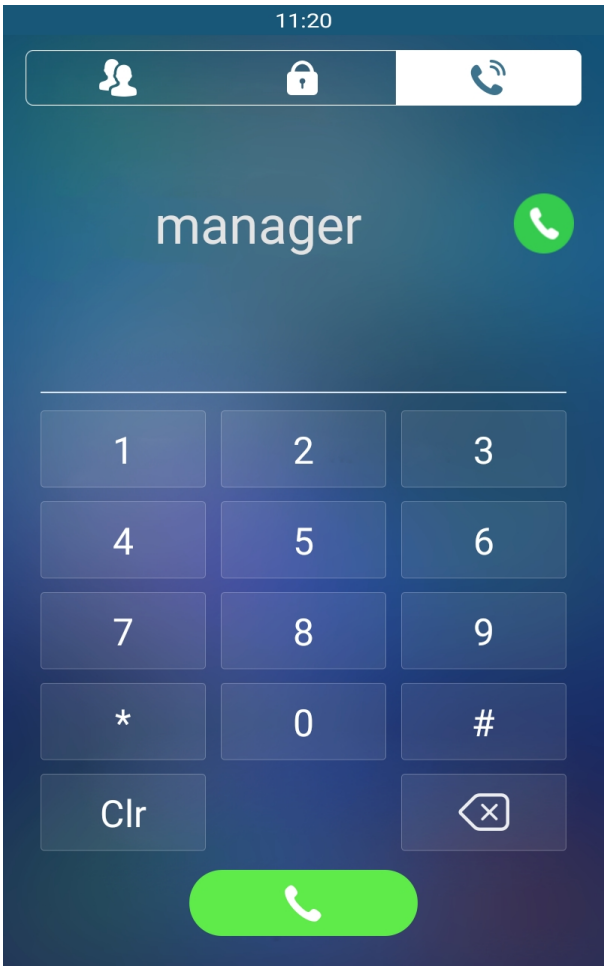


Quick Dial Using Configured Dial Name

You can create one dial name on the **Setting > Quick Dial** screen in Villa/Office mode on the device directly.

Then, users can directly tap the Quick Dial name on the Dial screen to call.


11:19
Quick Dial
Show
Quick Dial
Quick Dial Name
manager
Quick Dial Number
123
Save

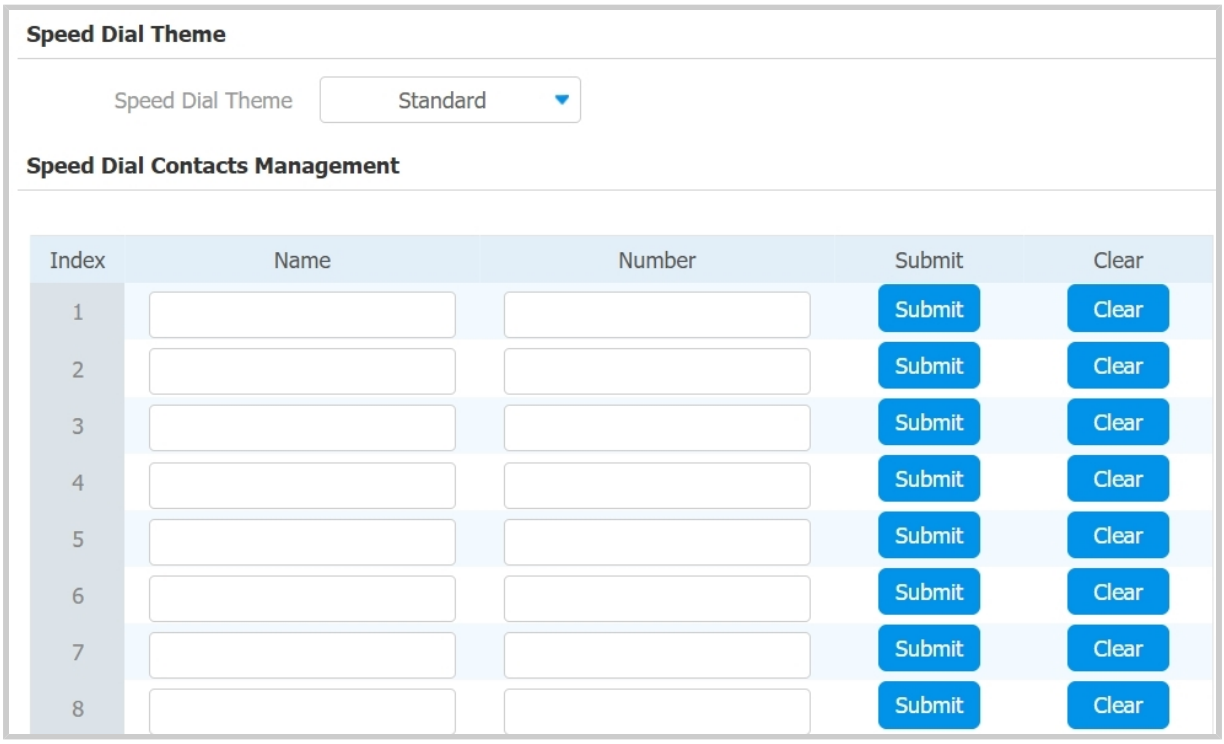


- **Show**: **Quick Dial** displays the configured Quick Dial name; **Time** displays the current time.
- **Quick Dial Name**: The name of the quick-dial contact.
- **Quick Dial Number**: The SIP number or IP address of the contact.

Speed Dial

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.

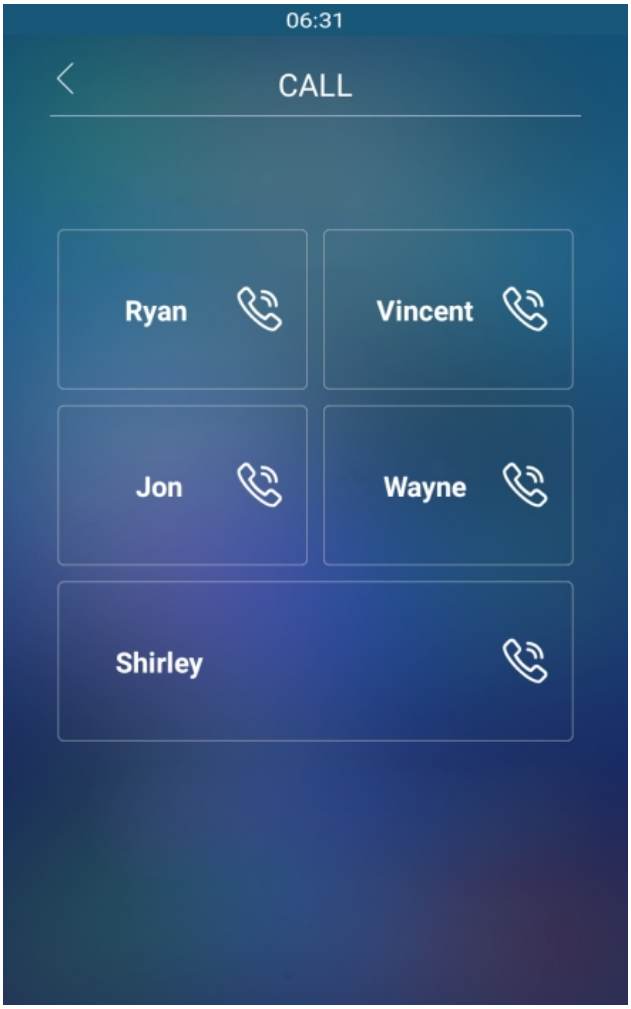
Set it up on the **Setting > Key/Display** interface. The setting is available when the **Villa** or **Office** theme is selected.

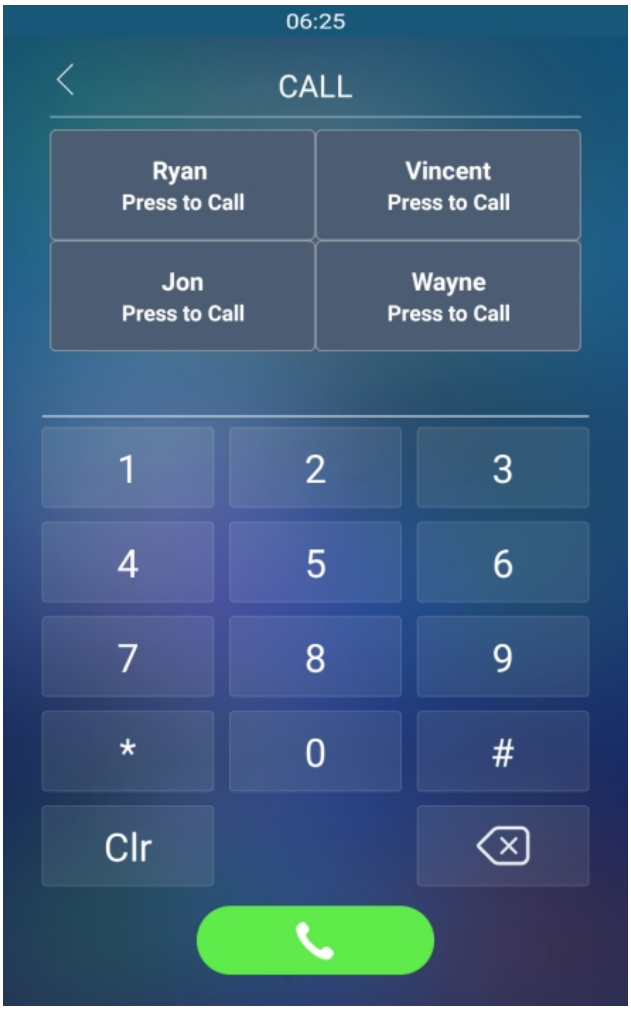


- **Speed Dial Theme:** Define layouts for speed dial buttons and the keypad on the dial screen. The 9 options are explained as follows:

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

Options	Descriptions
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.


06:31
CALL
Ryan
Vincent
Jon
Wayne
Shirley



> **Note**
>
> This function exclusively applies to Villa and Office themes.

Import/Export the Speed Dial Contacts

You can import/export the speed dial contacts for quick setup on the **Setting > Key/Display > Import/Export Speed Dial Contacts(.xml)** interface.

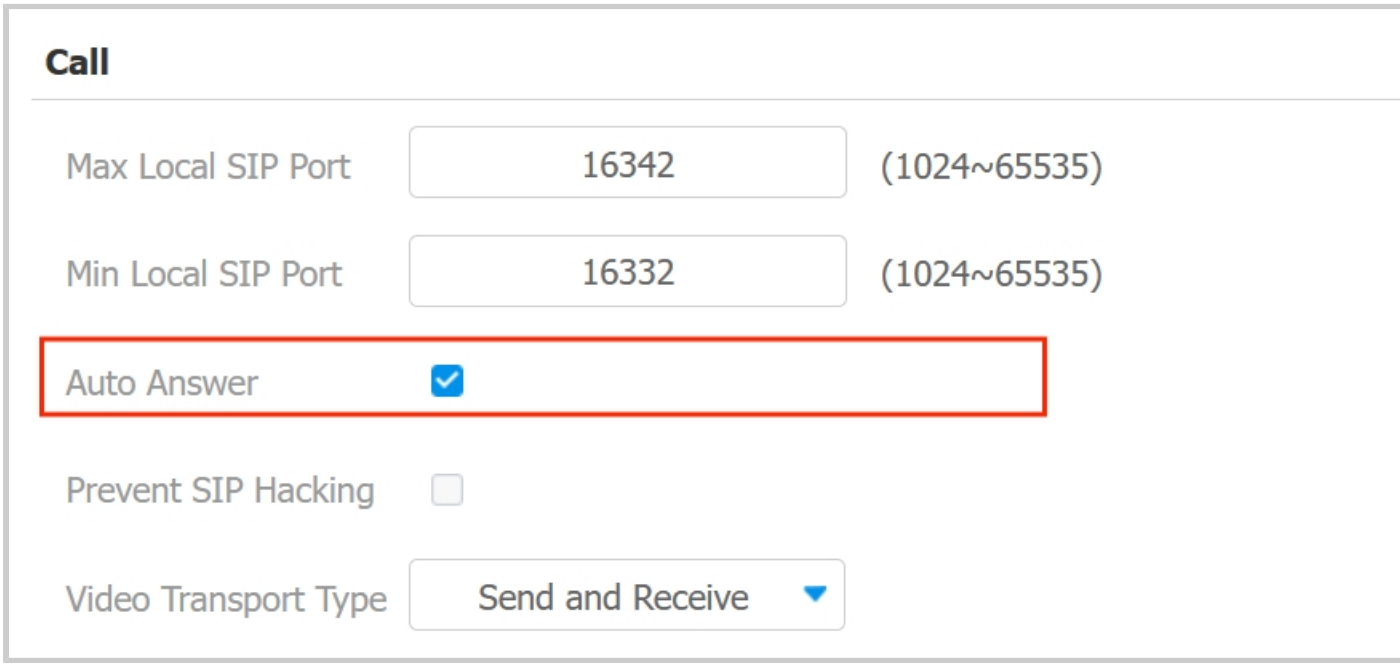
Add at least one speed dial contact before exporting the file.



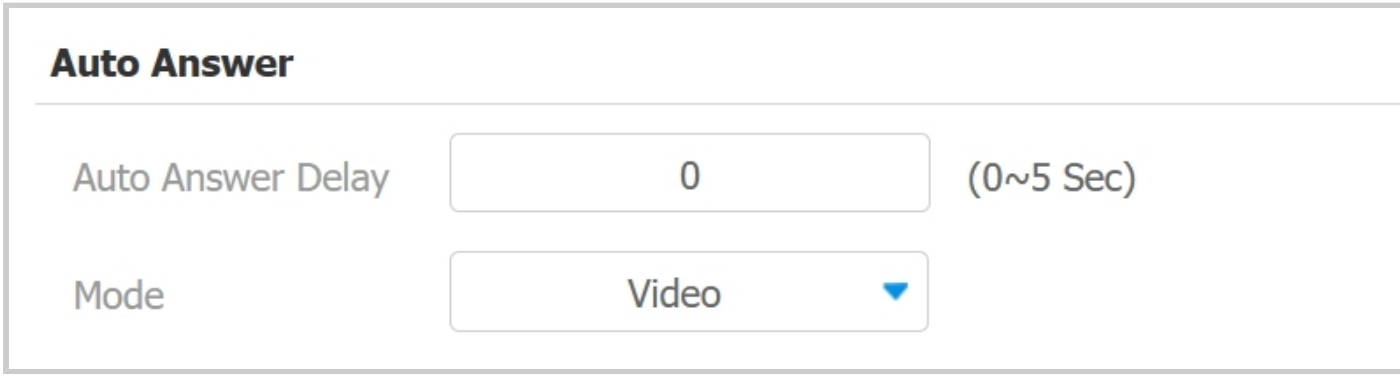
Call Auto-answer

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

To enable the Auto Answer feature, go to **Account > Advanced > Call** interface.



Once the feature is enabled, navigate to **Intercom > Call Feature > Auto Answer** interface.

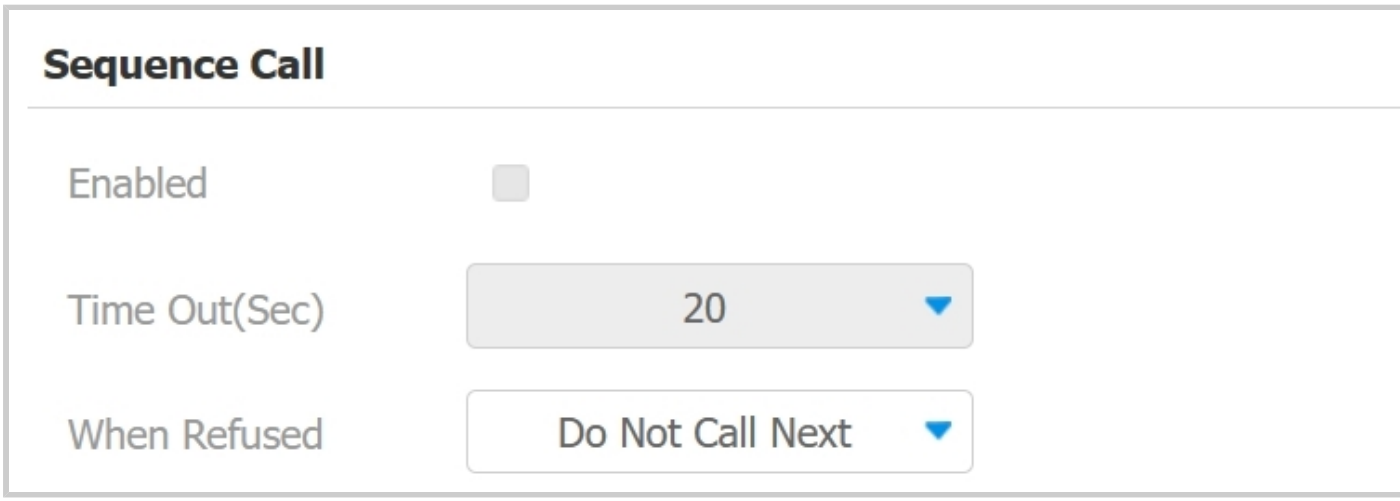


- **Auto Answer Delay:** Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode:** Determine whether to auto-answer the call as a video or audio call.

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.

To configure the sequence call, go to **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.

Maximum Call Duration

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

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

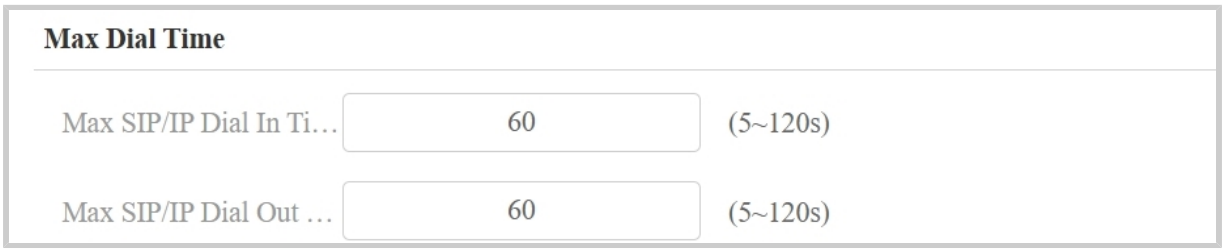


- **Max SIP/IP Call Time:** Specify the maximum duration of all calls. The door phone will end the call automatically when the time limit is reached.

Maximum Dial Duration

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

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



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

Hang up After Opening the Door

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

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



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

Audio & Video Codec Configuration

Audio Codec

The door phone supports three types of codec (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each type of codec varies in terms of sound quality. PCMU and PCMA are well-suited for traditional telephony and bandwidth-constrained environments, while G722 delivers better audio quality for more modern communication needs.

You can select the specific codec according to the actual network environment.

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

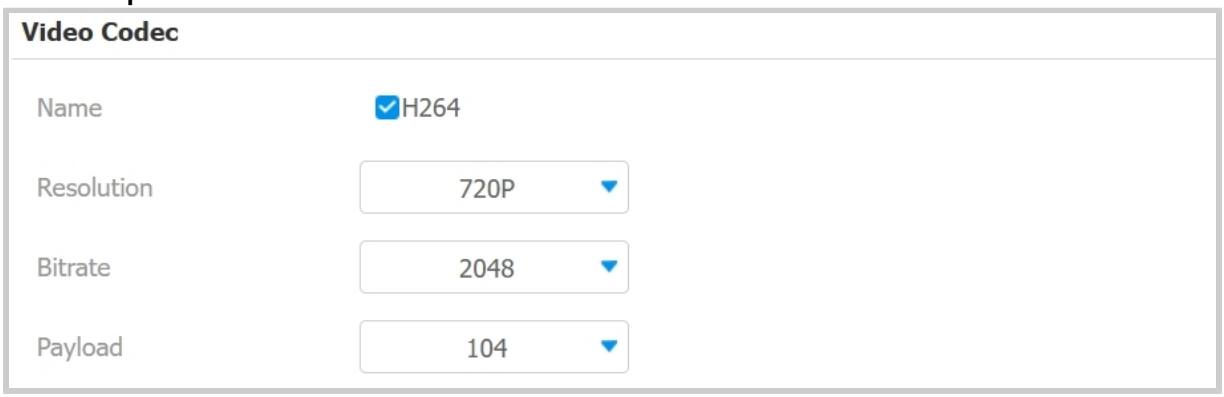


Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec

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

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

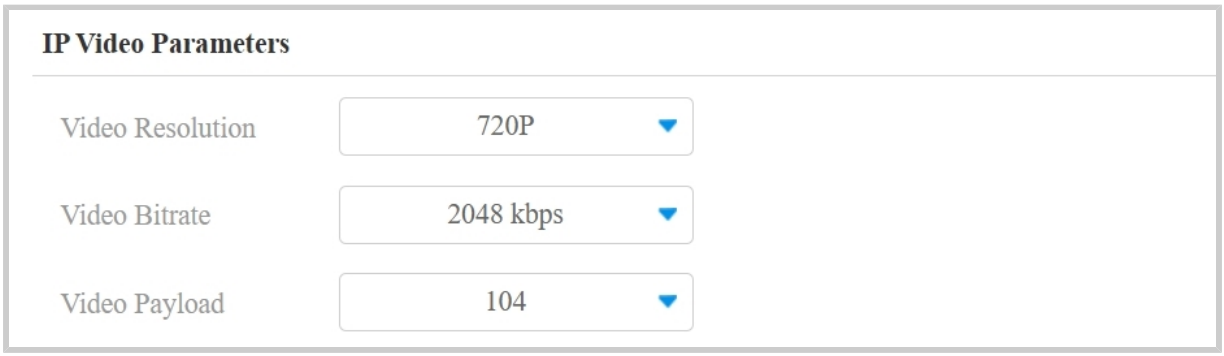


- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default resolution is 720P(720 × 480 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate,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

Video Codec for IP 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 is 720P(1280×720 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 128 to 4096 kbps. The default bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Contacts Configuration

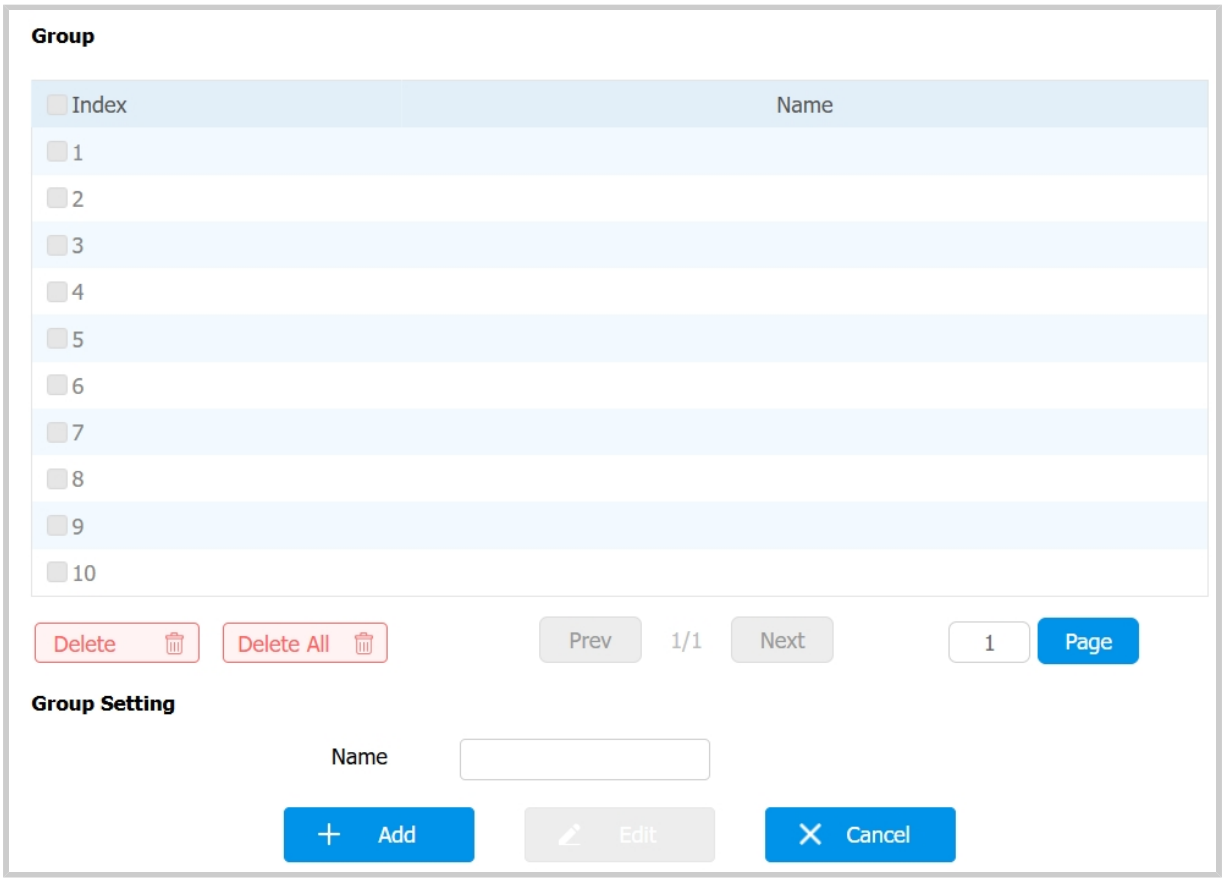
The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

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

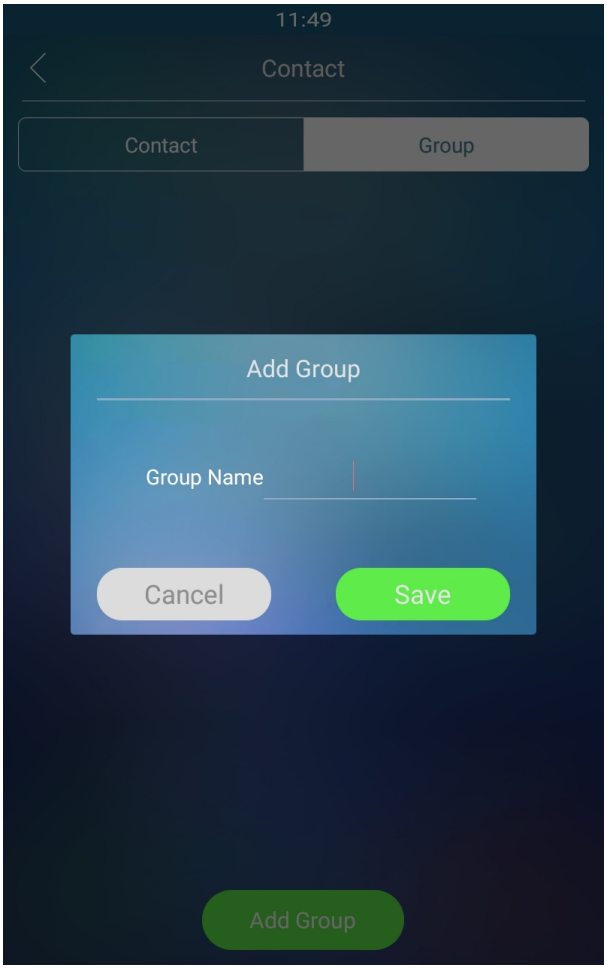
Manage Contact Groups

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. Enter the group name and click **+Add** to create a group. The device supports adding up to 500 groups.



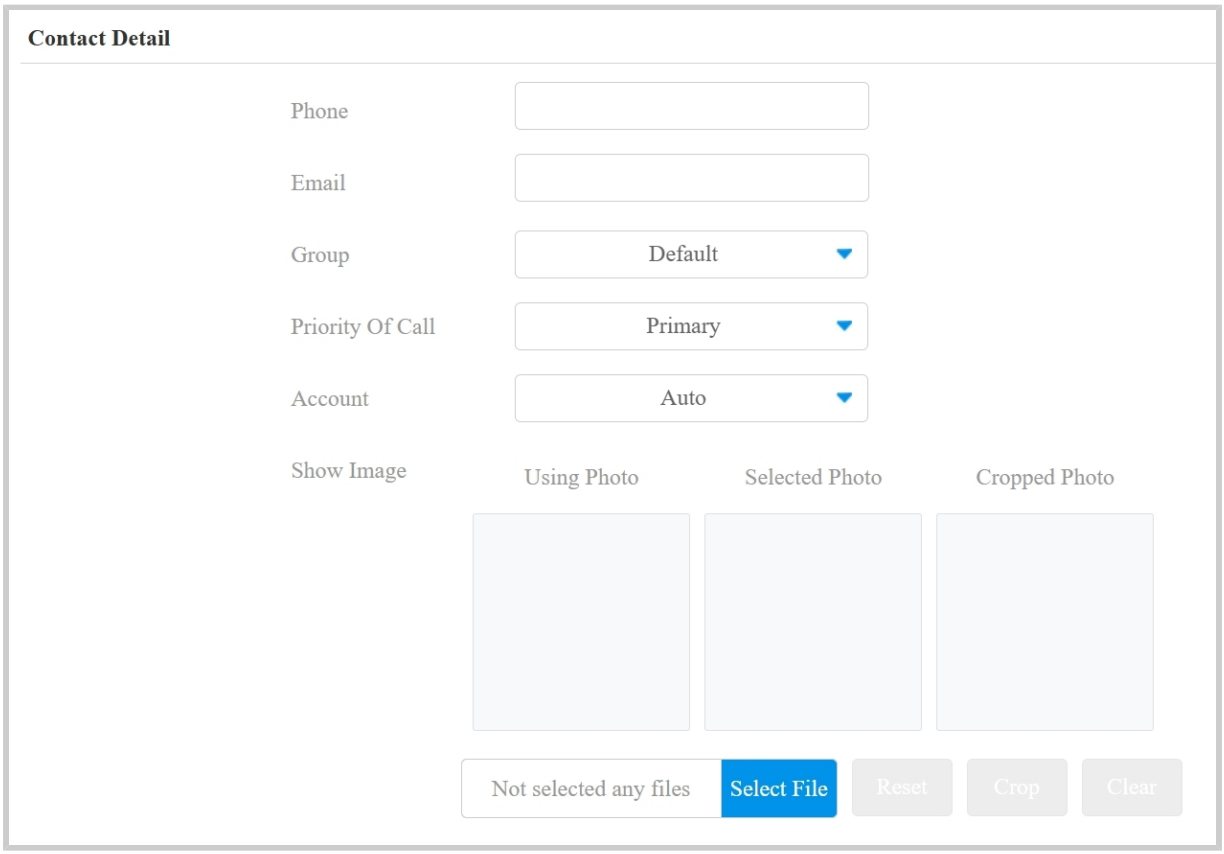
You can also add groups on the **Setting > Contact** screen. Tap **Add Group**.



Set up Contact Details

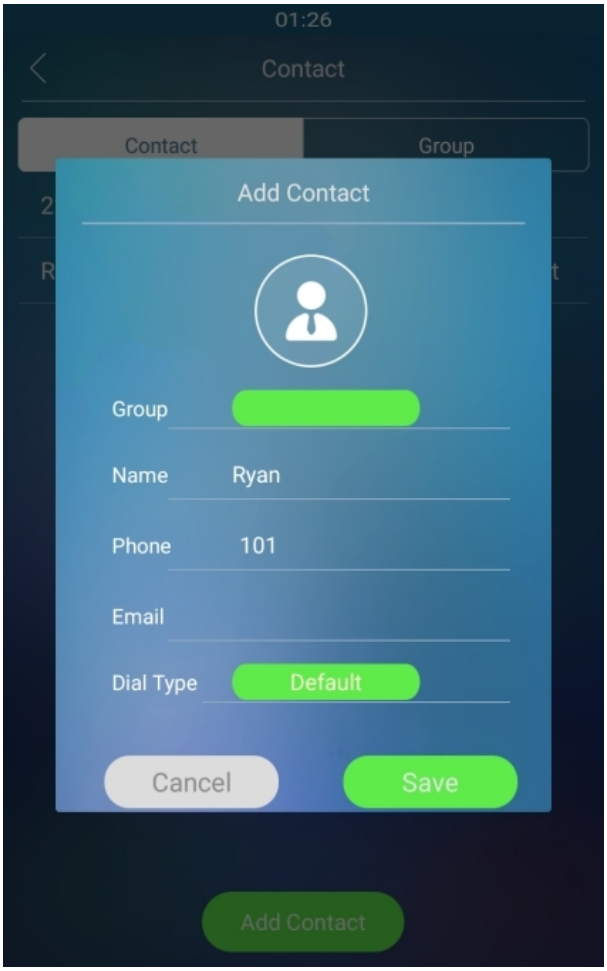
You can add users' contact information when adding or editing a user on the **Directory > User** interface. The users added will be displayed on the device's **Directory** screen.

Click **+Add** to add a user or click to modify a user. Scroll to the **Contacts Detail** section.



- **Phone**: The IP or SIP number of the contact.
- **Email**: The email address of the contact.
- **Group**: Assign the contact to the Default, Hidden Contact, or a self-created group.
  - **Priority of Call**: When assigning the contact to a self-created group. Set the priority of the call among three options: Primary, Secondary, and Tertiary. For example, if you set the priority of call for one of the contacts in a specific contact group as Primary, then the contact will be the first to be called among all the contacts in the same contact group when someone presses on the contact group for making a group call.
- **Account**: Select the account to make a call to the contact.
- **Show Image**: You can upload the contact profile photo. Click **Select File** to choose the photo from your driver and click **Import** to upload it.

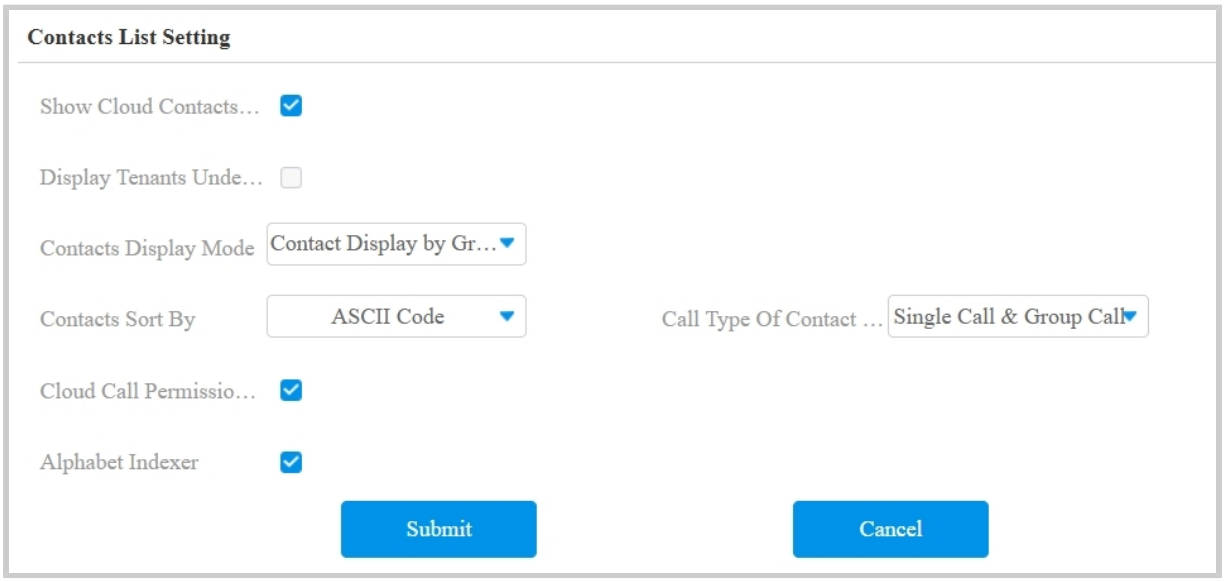
You can also add contacts on the **Setting > Contact** screen. Tap **Add Contact**.



Contacts List Display

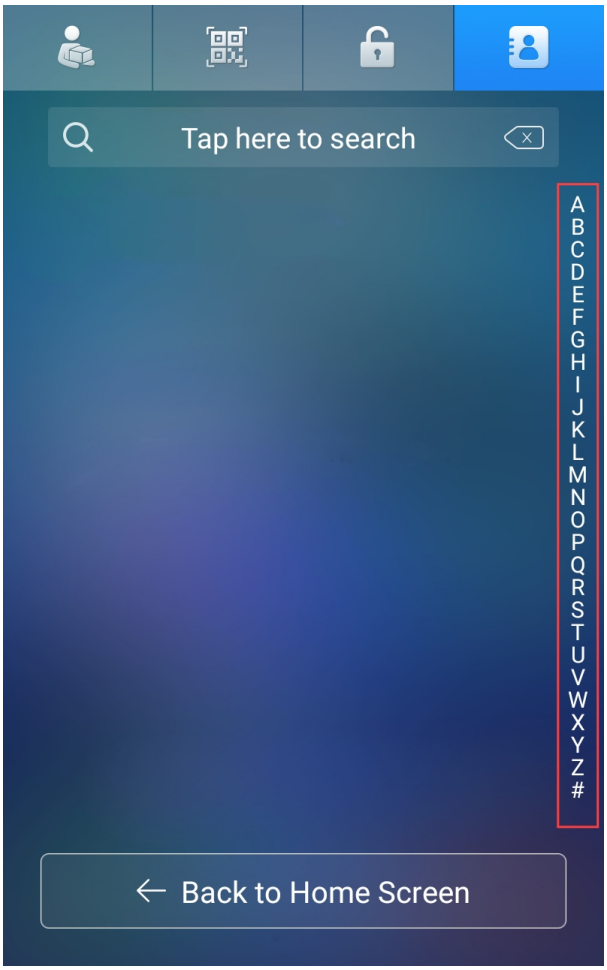
You can customize the contact list display to cater to users' operational and visual preferences.

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

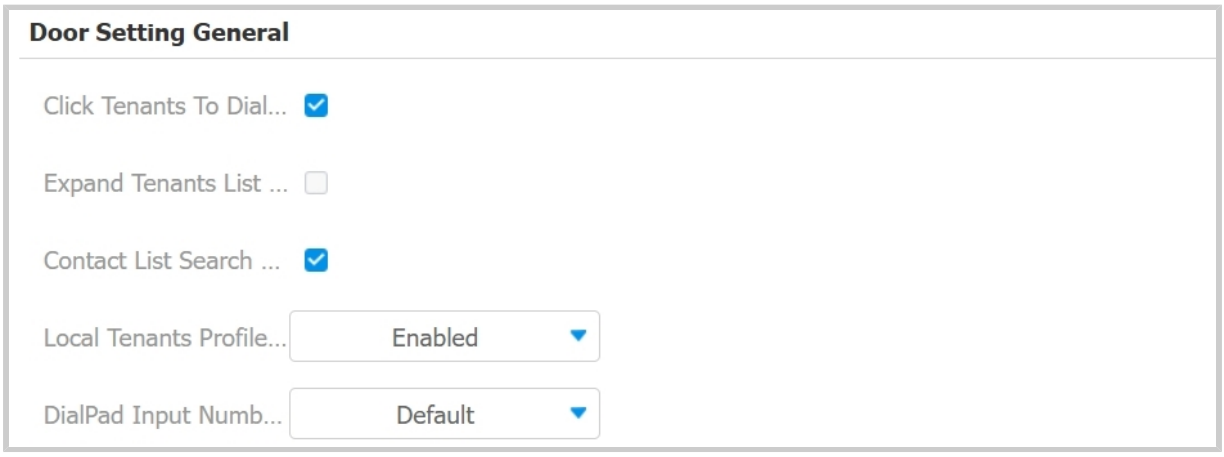


- **Show Cloud Contacts**: The contacts synchronized from the SmartPlus Cloud can be displayed.
- **Contacts Display Mode**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only**: Display contact groups. Press the desired group on the device screen to make a group call.
  - **Contact Display by Group**: Display contacts by groups. Press the group, and users can see the contacts in it.
- **Contacts Sort By**:
  - **ASCII Code** lists the tenants by their names in the sequence of the ASCII code.
  - **Room No.** lists the tenants according to their room numbers.
  - **Import** lists the tenants according to their order in the imported file.
- **Call Type of Contact Group**:
  - **Single Call & Group Call**: Users can call contacts one by one or simultaneously in a group.
  - **Only Single Call**: Users can only call contacts one by one.
  - **Only Group Call**: Users can only call contacts in a group simultaneously.

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



You can set up additional settings for contact display on the **Intercom > Basic > Door Setting General** interface.



- **Click Tenants To Dial**: Set whether to allow dialing out by pressing the contact tab.
- **Expand Tenants List View Mode**: Control the width of the contact tab. When enabled, the contact tab will be wider.
- **Contact List Search Box Visible**: Set whether to display the search box at the top of the screen.
- **Local Tenants Profile Display Mode**: Choose whether to show the contact's profile picture. **Auto** will display the default picture.
- **Dial Pad Input Number Limit**: Choose the maximum digits allowed on the dial pad (4, 6, 8, or 10 digits). **Default** means no limit.

Relay Settings

Local Relay

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

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

Relay

Relay ID	RelayA	RelayB
Relay Type	Default Status	Default Status
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	#	1
2~4 Digits DTMF	010	012
Relay Status	RelayA: Low	RelayB: Low
Relay Name	Door1	RelayB

Access Method	PIN	PIN	PIN
	Face	Face	Face
	RF Card	RF Card	RF Card
	BLE	BLE	BLE
	NFC	NFC	NFC
	LPR Camera	LPR Camera	LPR Camera
Lift Control			

- **Relay ID**: The specific relay for door access. Please note that R29Z/R29ZL has only one relay available.
- **Type**: Determine the interpretation of the Relay Status regarding the state of the door:
  - **Default State**: A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.
  - **Invert State**: A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.
- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **Bistable**: The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1-Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Access Method**: Check the method(s) to trigger the relay.
- **Lift Control**: Set whether to perform lift control when the specific relay is triggered.

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

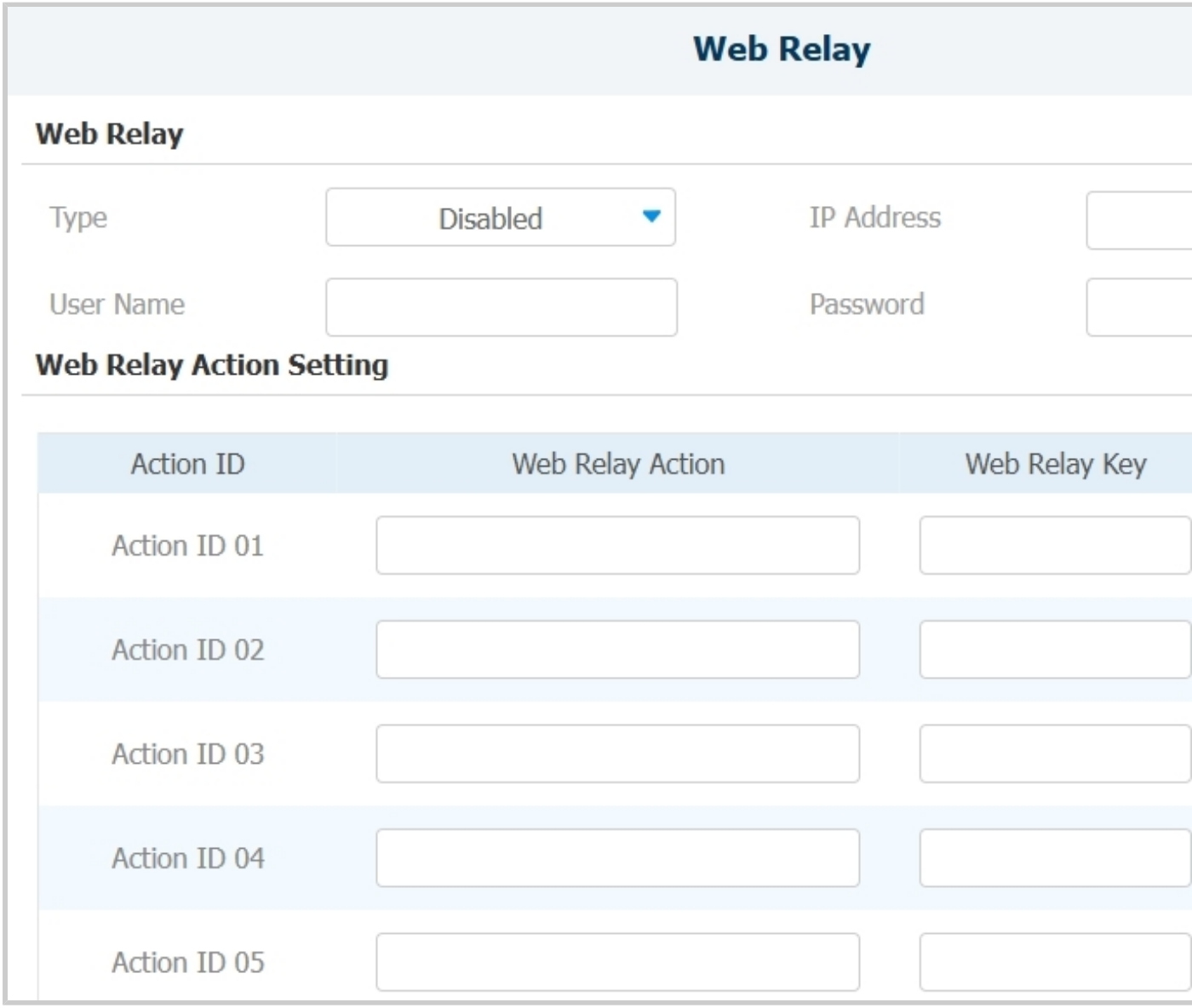
Web Relay

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



Click here to view how to set up web relay.

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



- **Type**: Determine the type of relay activated when employing door access methods for entry.
  - Disabled: Only activate the local relay.
  - Web Relay: Only activate the web relay.
  - Both: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **IP Address**: The web relay IP address provided by the web relay manufacturer.

- **User Name**: The user name provided by the web relay manufacturer.
- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.
- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

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

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

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

- Leaving it blank enables all door-opening methods.

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

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

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

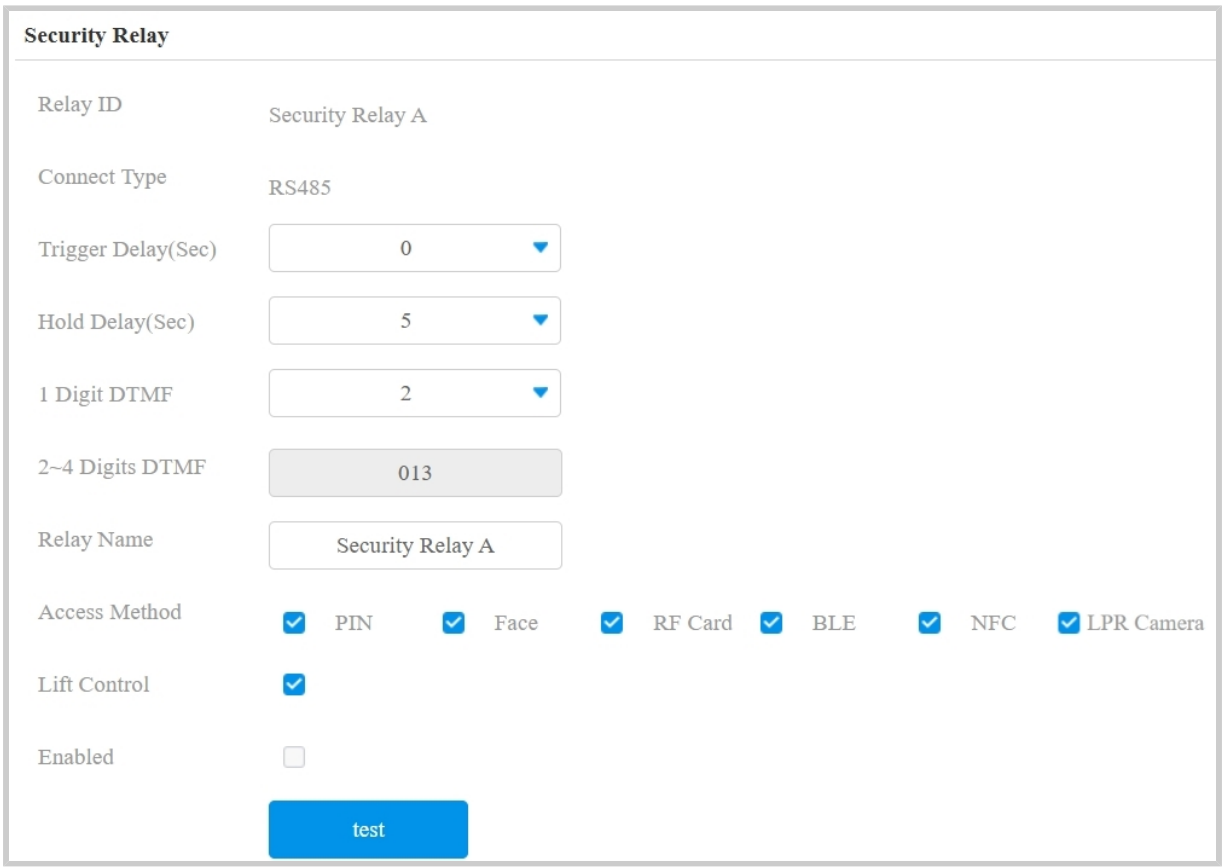
Security Relay

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.

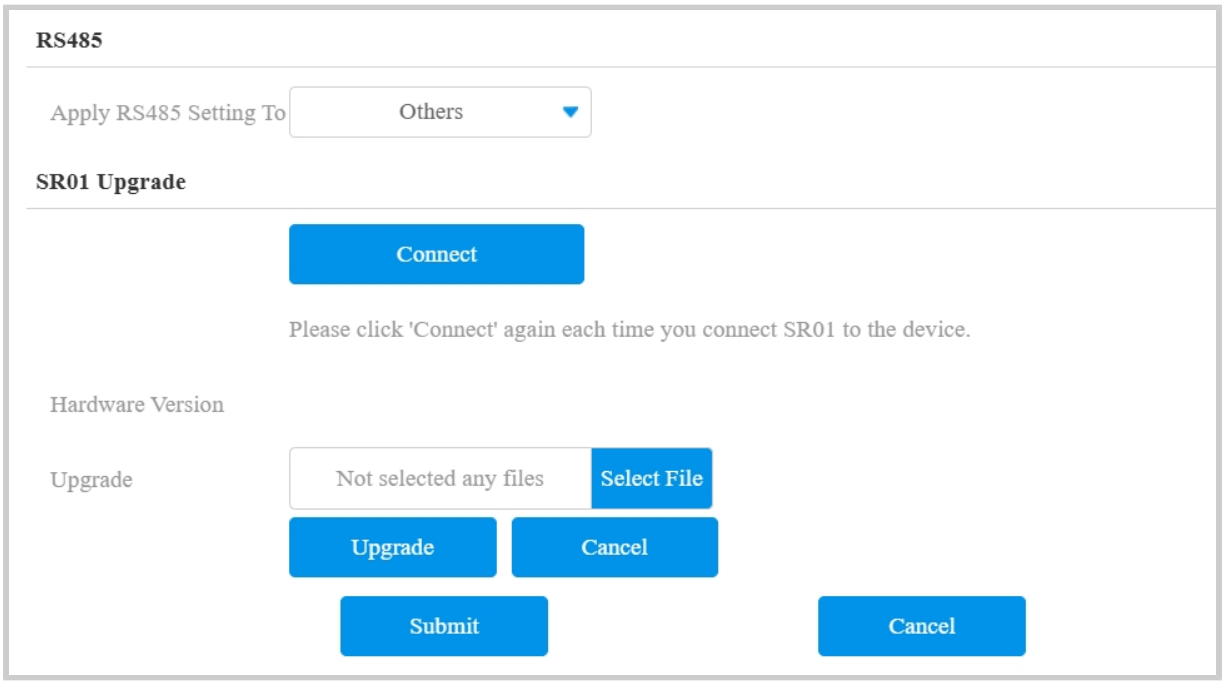


- **Connect Type**: The security relay connects to the door phone using RS485 by default.
- **Trigger Delay (Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec)**: Determine how long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

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 **Others**.



- **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.
- **Select File**: Click to upload the ROM file before clicking Upgrade.

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

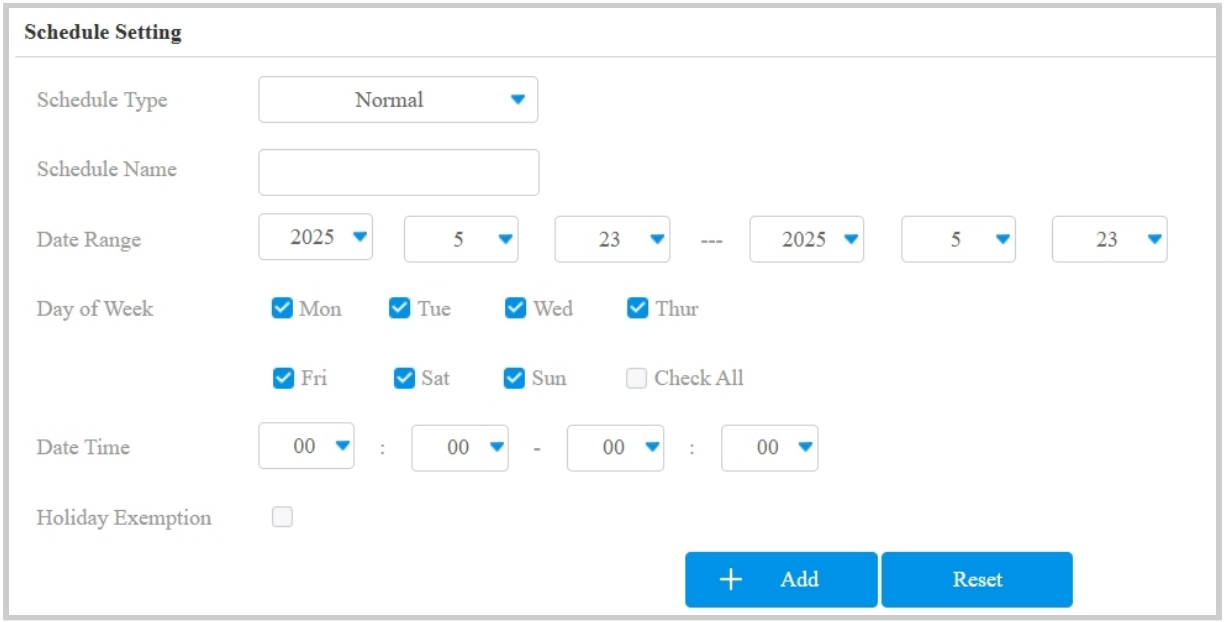
Door Access Schedule Management

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

Create a Door Access Schedule

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

To configure the schedule, navigate to the web **Setting > Schedule** interface. You can create up to 100 schedules.



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

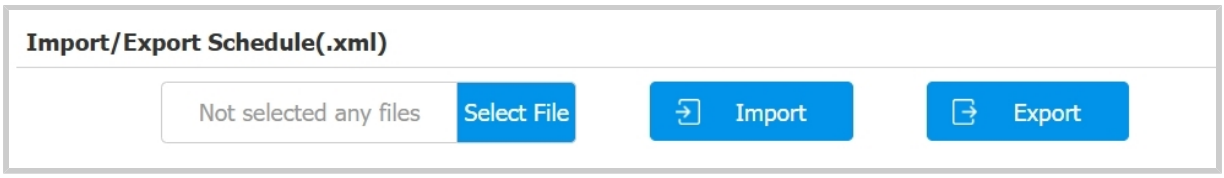
- **Holiday Exemption**: The holiday schedule has higher priority over the access schedule, which limits users from opening doors. If users want to open doors during holidays within the access schedule, you need to check this option.

> **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.

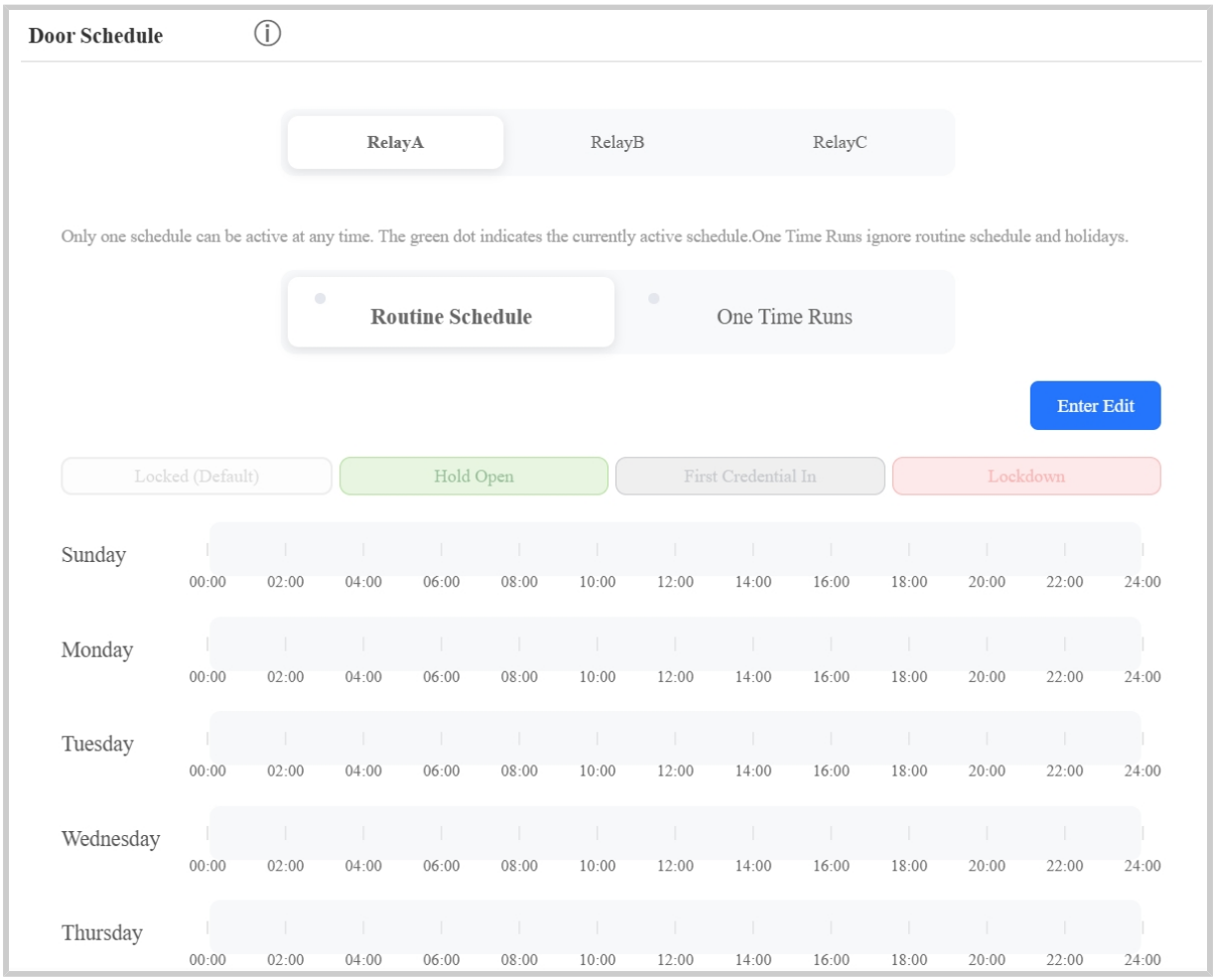
Set it up on the **Setting > Schedule** interface.



Door Schedule

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

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



- **Relay ID**: Specify the relay that applies the schedule.
  - **Security Relay A**: Only when the SR01 is enabled, will this option be available.
- **Repeat Type**:
  - **Routine Schedule**: The schedule repeats every week. Click **Enter 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.

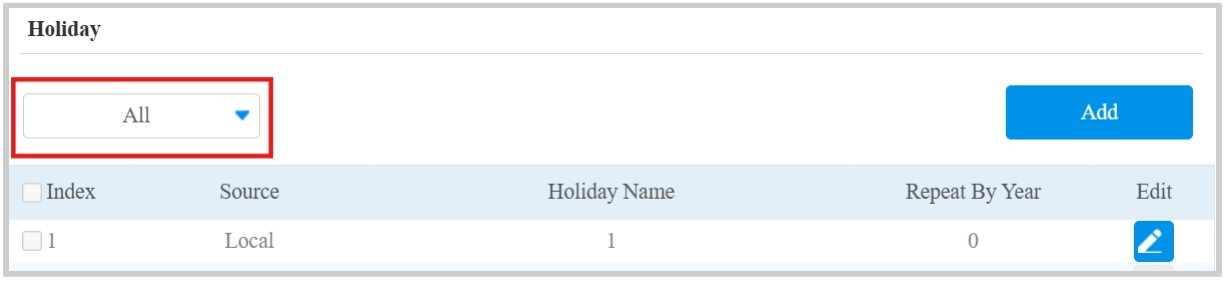
> **Note**
>
> Click here to view the detailed configuration of each schedule mode.

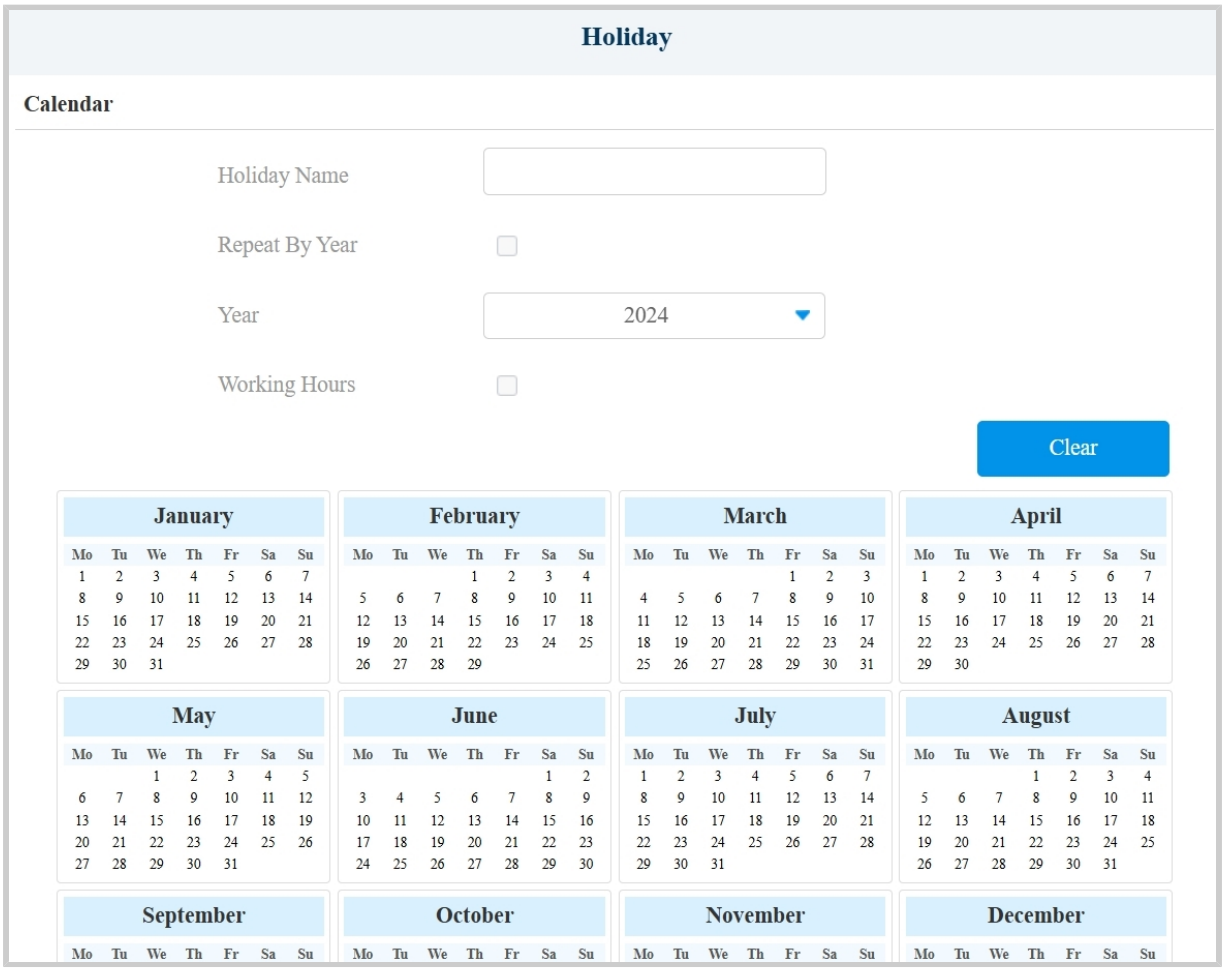
Holiday Schedule

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. You can choose to view the local holidays, SmartPlus Cloud holidays, or both.

Click **Add** to set up a local holiday schedule.



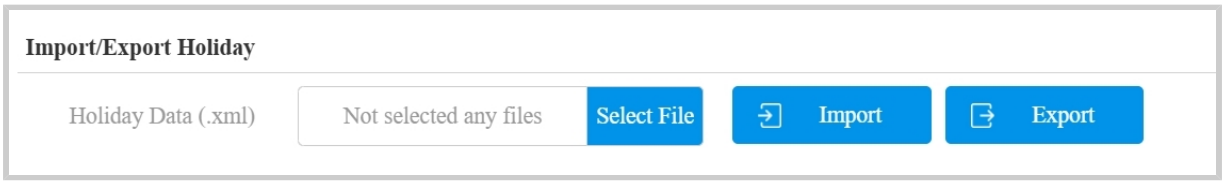


- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

Holiday Schedule Import/Export

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

The import/export file format is .xml.


Import/Export Holiday
Holiday Data (.xml)
Not selected any files
Select File
Import
Export

Door-opening Configuration

Unlock By Public PIN

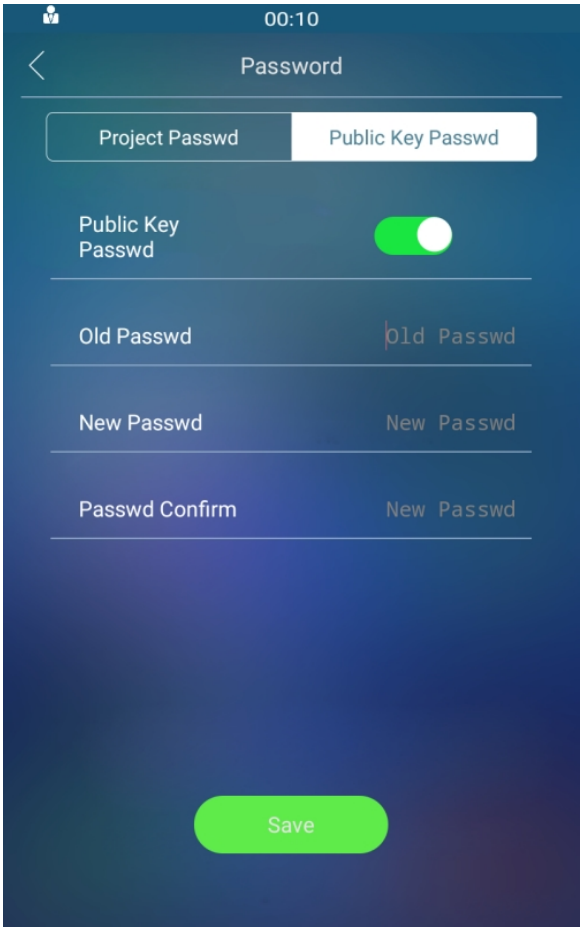
There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex. You can create and modify both the public and private PIN codes.

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



- **PIN Code**: Set the 3-8 digits code.

You can also set up the public PIN on the **Setting > Password** screen.

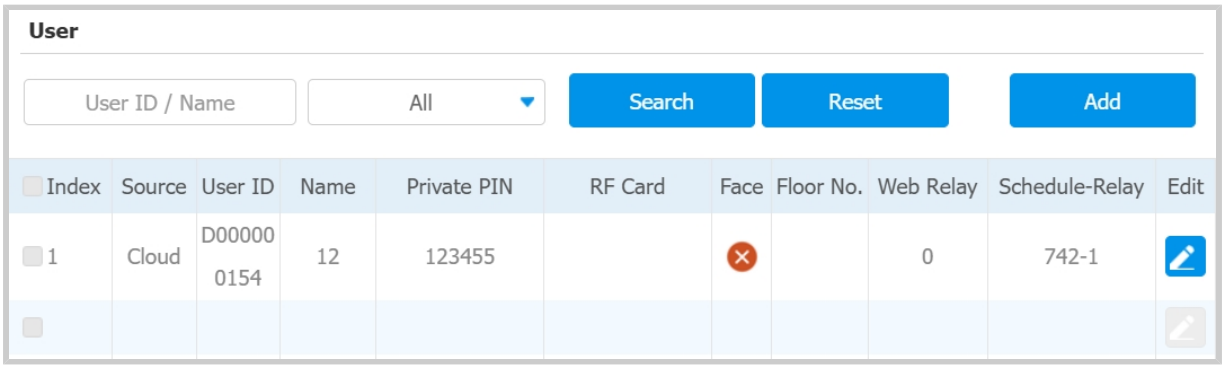


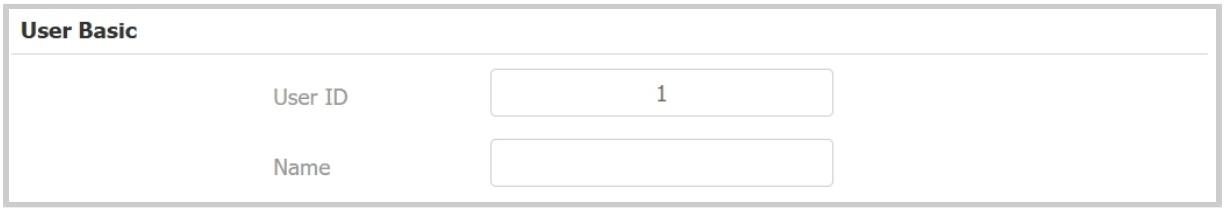
User-specific Access Methods

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

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

To add a user, go to **Directory > User** interface and Click **+Add**.





- **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 user. Each user can only be assigned a single PIN code.
  - Support entering numbers and letters saved in uppercase form.
  - DO NOT start the PIN with 9, which is invalid.

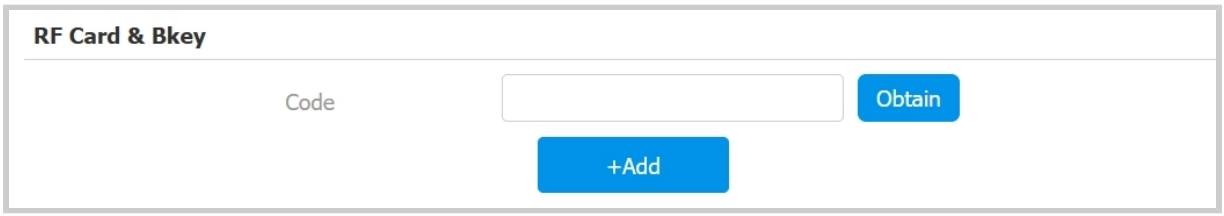
You can enable/disable the use of the private PIN and set the PIN mode on the **Intercom > PIN Setting > Private PIN** interface.



- **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 Cloud.

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 to add 20000 users.

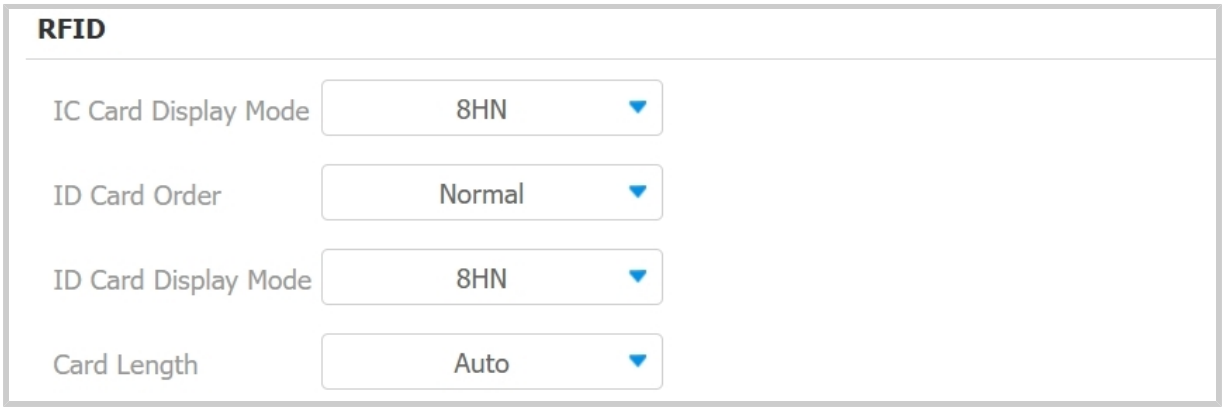
You can enable and disable the use of RF cards on the **Access Control > Card Setting** interface.



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.
- **Card Length**: Set the card reading length between Auto and 3 Bytes.

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.

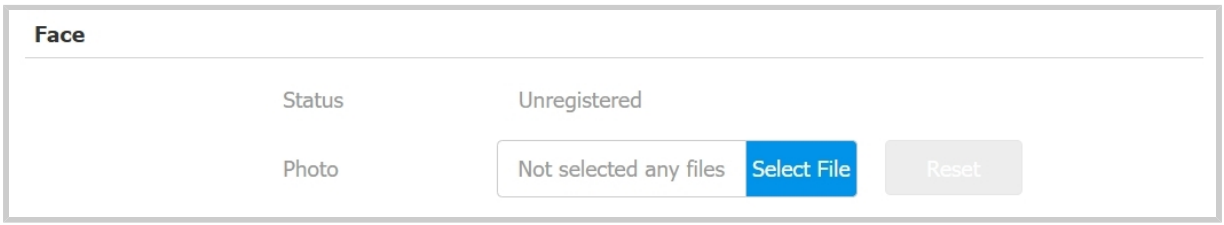
- Use the Akuvox long-range card reader ACR-CPR12 to recognize the UHF card attached to the vehicle's windshield.

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



Unlock by Facial Recognition

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

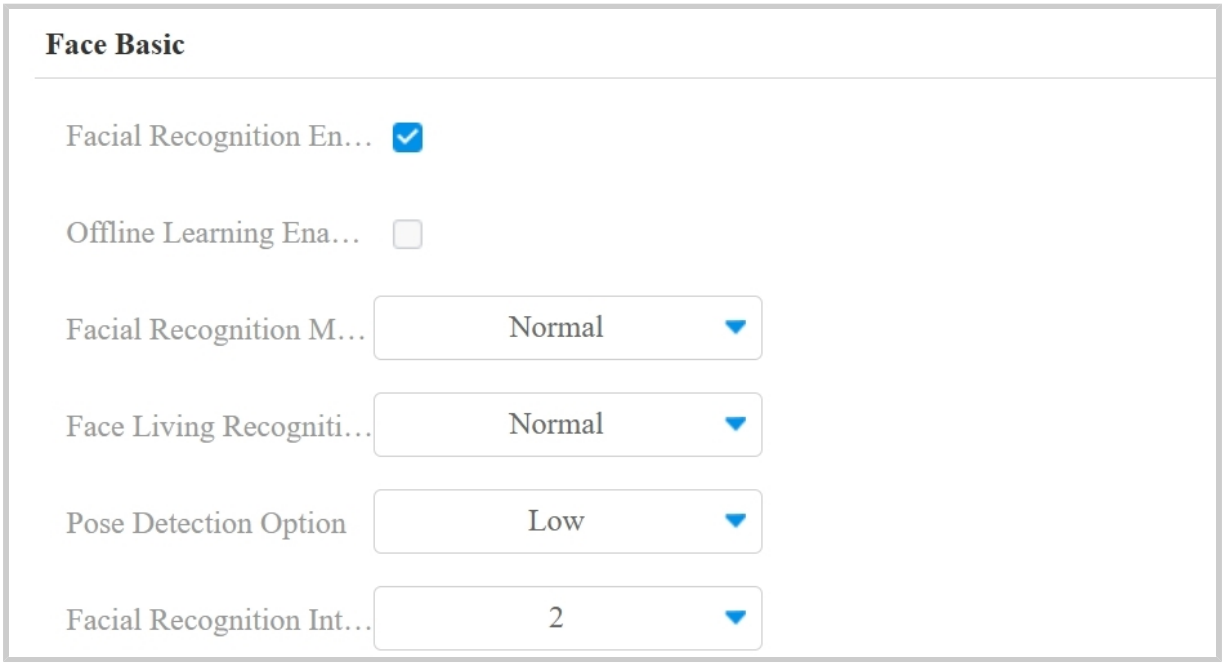


- **Status**: Indicate whether the user's face photo has been uploaded successfully.
- **Photo**: Upload a photo complying with the following requirements:
  - The photo must be in JPG, PNG, or BMP format.
  - The photo must be at least 250 x 250 pixels and no more than 2MB in size.
  - The photo must be clear and not blurred.
  - The photo should include a full face with a front view and open eyes.
  - Avoid shadows on the face or background in the photo.

Facial Recognition Settings

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

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



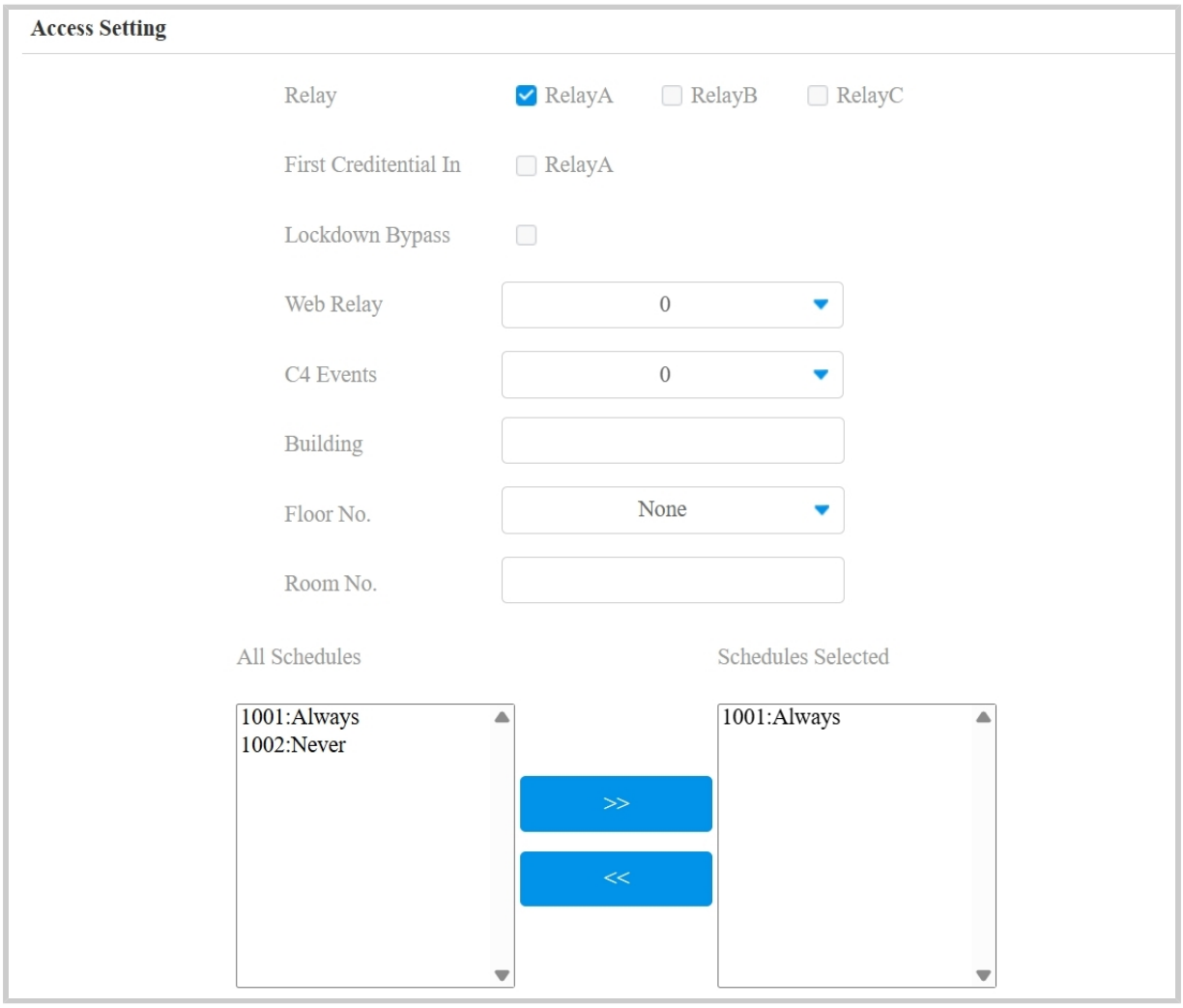
- **Face Recognition Enabled**: Enable/disable the facial recognition function.
- **Offline Learning Enabled**: Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level**: Determine how strict the facial recognition system is in comparing a person's face with uploaded face data. Each level allows a different degree of difference or face covering (**excluding the mouth area**) to pass the recognition.
  - Low: Allow slight differences from the uploaded face data, with little face coverage.
  - Highest: Require the face to be identical to the uploaded one, with minimal or no covering.
  - The other two levels are in between.
- **Face Living Recognition Matching Level**: 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**: Select the pose detection level from Close, Low, Normal, and High. The higher the level is, the more accurate the detection is. Users will be prompted to “please face the camera directly” when they do not face the camera.
- **Facial Recognition Interval**: 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.



- **Relay**: 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.

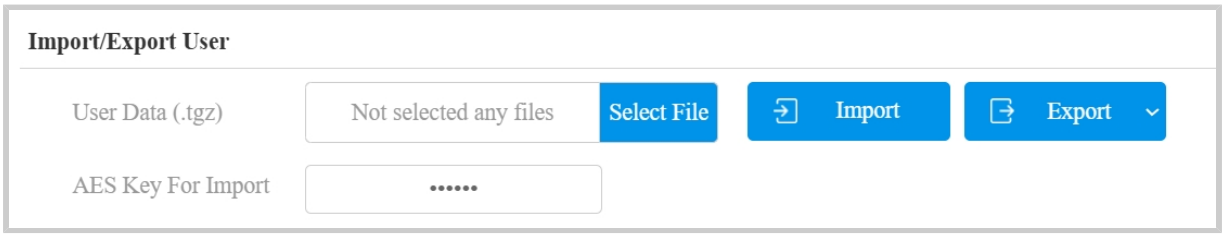
- **Building**: Specify the building the user lives in.
- **Floor No.**: Specify the accessible floor(s) to the user via the elevator.
- **Room No.**: Enter the user's room number.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) 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

You can import and export user data for quick setup on the **Directory > User > Import/Export User** interface.

The import/export file format can be .XML or .CSV.

Click here to view how to import and export user data between Akuvox door phones. The device allows to add 20,000 users.



Access Authentication Mode

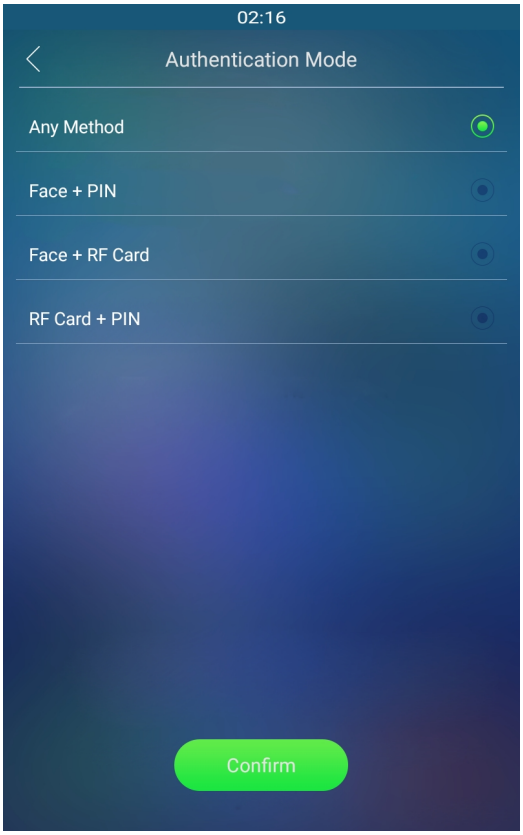
You can set up multiple access authentication modes, and set up authentication security as needed.

Set it up on the **Setting > Key/Display > Access Authentication Mode of The Building Theme** interface. This feature applies to the **Building** theme.



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

You can also set it up on the **Setting > Authentication Mode** screen.



Unlock by NFC and Felica Cards

Set the device to support NFC and Felica cards on the device before they can be used.

Go to the **Access Control > Card Setting > Contactless Smart Card** interface.



Note

- Click here to view the detailed steps of setting up the NFC function.
- Due to conflicts between NFC and Felica cards when applied simultaneously, it's necessary to disable one of them to avoid conflict.

Mifare Card Encryption

The device can read encrypted Mifare cards for greater security. When this feature is enabled, it reads the data in the cards' designated sectors and blocks, not the UID.

Click here to view the details of encrypting and reading Mifare cards.

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



- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
  - **Key Type**: The authentication key type used to read the Mifare Classic card
  - **Data Offset**: The starting byte position from which card data is read. The default is 0.
  - **Data Length**: The number of valid data bytes to read from the card. The default is 4.
  - **Code Length**: Select the code length between Auto and 7 Bytes to 4.
  - **Code Order**: Select the code order between Normal and Reversed.
- **Plus**: You can set up three choices. This means you can use three types of Mifare Plus cards. When swiping a card, as long as one of the choices matches its SL key, the card code in the block you specified will be output.
  - **Block**: Specify the block(s) to be read.
  - **SL3**: The key number within 32 bits.
- **DESFire**:
  - **App ID**: A 6-digit hexadecimal number
  - **File ID**: The ID of the encrypted file of the app, which can be a number from 0 to 31.
  - **Crypto**: The encryption method, either AES or DES.
  - **Read Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.
  - **Byte Order**: The byte reading order. The default is MSB. The device starts reading bytes after performing **Data Offset** and **Data Length**.
    - **MSB**: Most Significant Bit means the reading order is normal(from left to right).

  - **LSB**: Least Significant Bit means the reading order is reversed(from right to left).
- **Data Offset**: Define from which byte position to start reading data, with a range of 0 to 43. The default is 0.
- **Data Length**: Define the length of valid byte data, with a range of 1 to 8. The default is 4.

Unlock by HTTP Command

The door phone supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the door phone. This will trigger the relay and open the door, even if the users are away from the device.

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



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

Tip

Here is an HTTP command URL example:



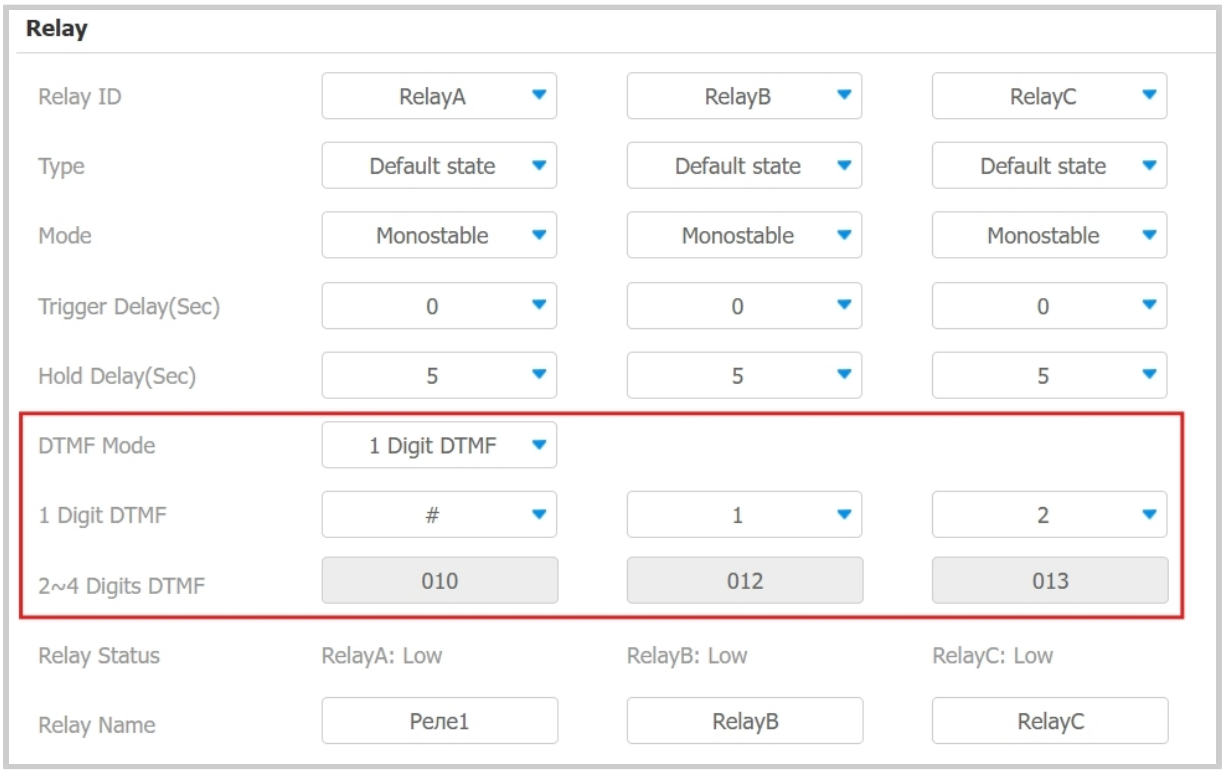
Note

The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide Opening the Door via HTTP Command for more information.

Unlock by DTMF Code

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

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



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

DTMF Data Transmission

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

DTMF Type Differences:

Inband	DTMF signals are transmitted within the same audio channel as voice data. Simple implementation but signal distortion may occur with highly compressed codecs (e.g., G.729).

RFC2833	Transmits DTMF as special event packets over RTP (Real-Time Transport Protocol), known as out-of-band transmission. Reliable and unaffected by codecs.
Info	Sends DTMF signals via SIP (Session Initiation Protocol) signaling channel. Separate from voice transmission, ensuring audio quality.
Info+Inband	Combines Info and Inband methods.
Info+RFC2833	Combines both Info and RFC2833 methods.
Info+Inband +RFC2833	All three methods are used simultaneously.

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



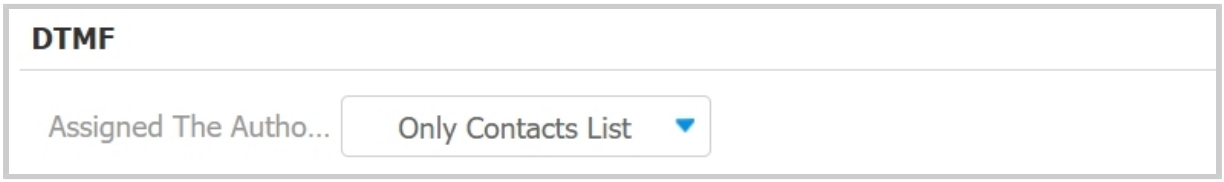
- **Type**: Select from the available options based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select Disabled, DTMF, DTMF-Relay, or Telephone-Event according to the specific type adopted by the 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 > DTMF** interface so that only the caller numbers you designated in the door phone can use the DTMF code to gain door access.



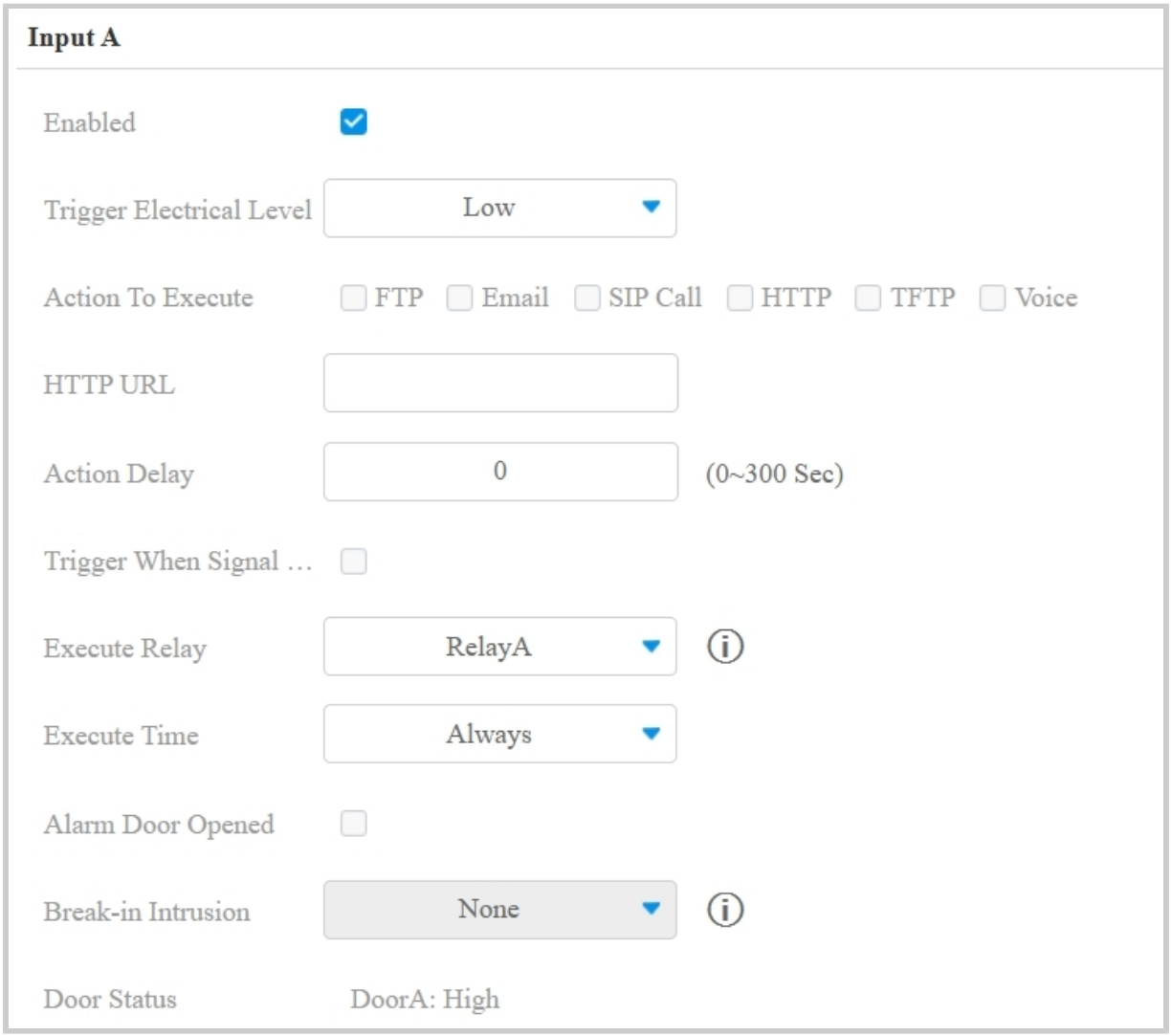
- **Assigned The Authority For**: Specify the contacts authorized to open doors via DTMF:
  - **None**: No numbers can unlock doors using DTMF.
  - **Only Contacts List**: Only numbers added to the door phone's contact list can unlock via DTMF.
  - **All Numbers**: Any numbers can unlock using DTMF.

Unlock by Exit Button

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

Click here to watch the instruction video.

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



- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - FTP: Send a screenshot to the preconfigured FTP server.
  - Email: Send a screenshot to the preconfigured Email address.
  - SIP Call: Call the preset number upon 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.
- Voice: When triggered, the door phone will play the customized prompt instead of the default one.

> **TIP:**
>
> To enable the custom audio prompt, upload the audio file at **Device>Import/Export>Upload Tone.**

- **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.
- **Trigger When Signal Is Hold**: To trigger the preconfigured action when the door remains open before the timeout.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Execute Time**: Specify whether the relay can be triggered at any time or only within a scheduled time period.
- **Alarm Door Opened**: If enabled, an alarm will be triggered when the door-opening time exceeds a limit.
  - **Door Opened Timeout**: The door-opening time limit.
- **Break-in Intrusion**: Activate an alarm when the door is forcibly or illegally opened. Once triggered, the alarm can only be turned off by checking this option. Click here to learn more about this feature. It is incompatible with the Execute Relay feature.
- **Door Status**: Display the status of the input signal.

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.

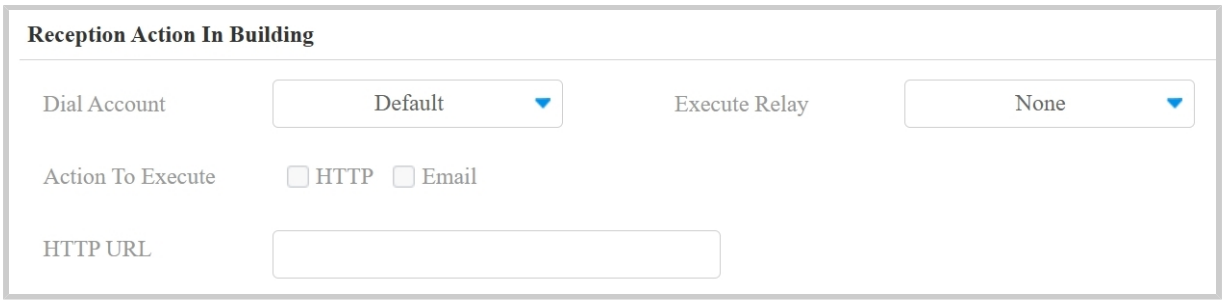


> **Note**
>
> The function should work with the Akuvox SmartPlus cloud. Please click here to view the configuration details.

Unlock by Reception Tab

The Reception button is a tab on the home screen that allows residents and visitors to contact the receptionist or the security guard of the building. They can tap this button to ask for help or access to the door.

To configure a reception tab, go to **Setting > Key/Display > Reception Action In Building** interface.

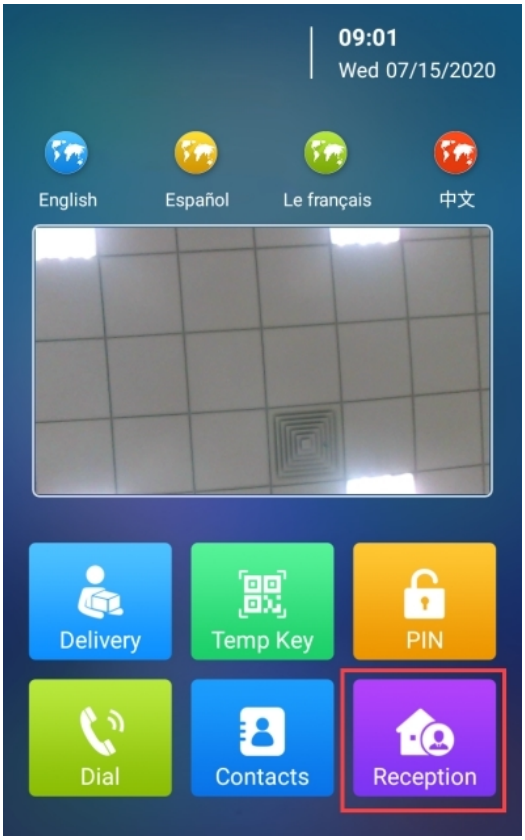


- **Dial Account**: Select the registered SIP account to make calls with receptionists or security guards. Selecting Default will use Account 1 for the calls.
- **Execute Relay**: Specify the relay(s) to be triggered by the Reception tab.

- **Action To Execute**: Set the desired actions that occur when pressing the Reception tab to open the door.
  - **Email**: Send a screenshot to the preconfigured Email address.
  - **HTTP**: When checked and the HTTP URL is entered in the box below, press the Reception tab that triggers the desired action.
- **HTTP URL**: Enter the HTTP command URL. Here is an example of relay triggering:



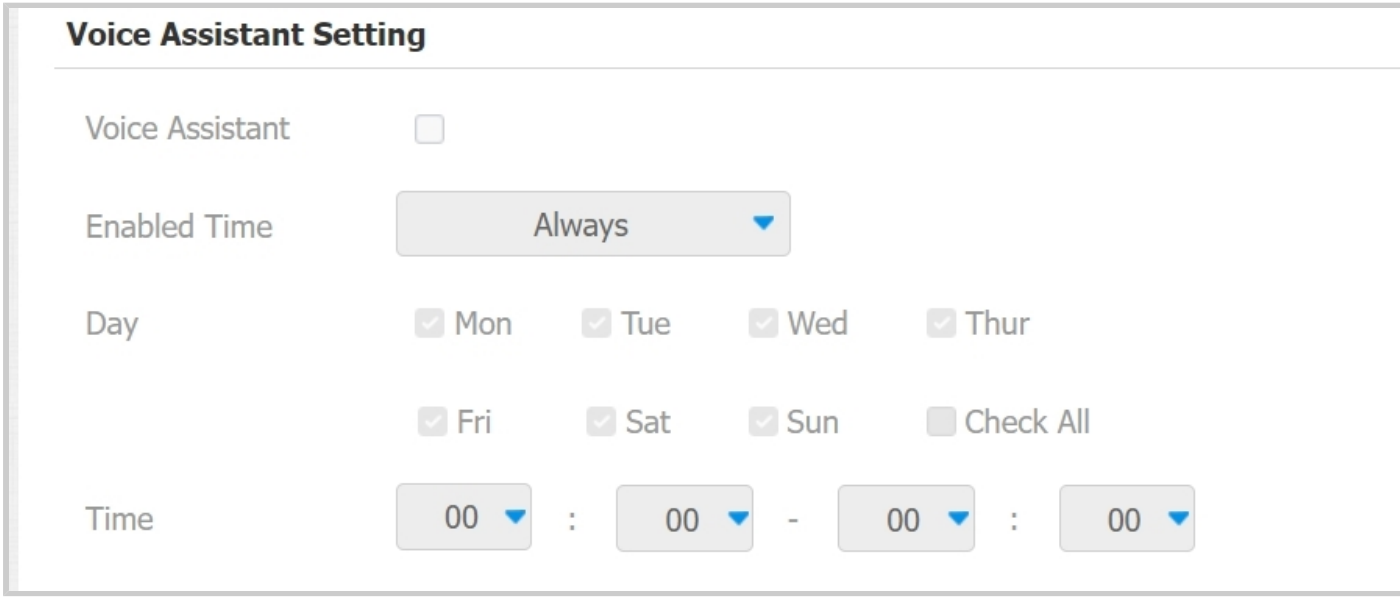
> **Note**
>
> The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide Opening the Door via HTTP Command for more information.



Unlock by Voice Assistant

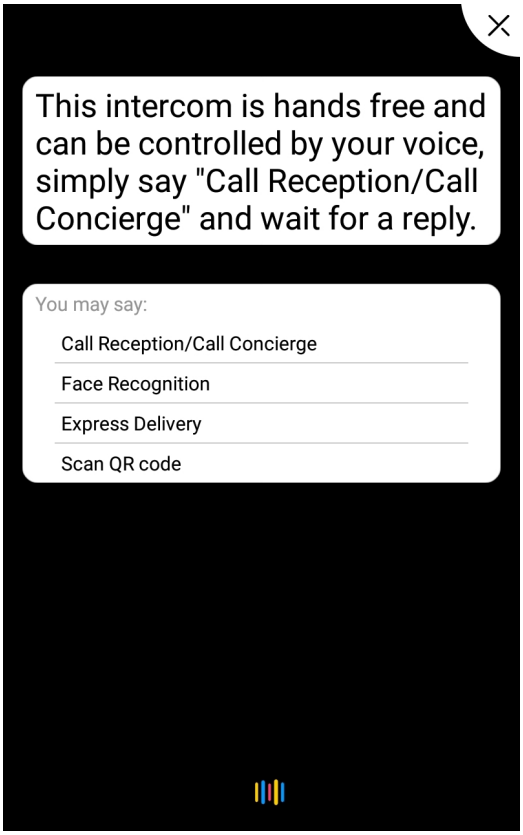
Albert is a voice assistant from Akuvox. It can help you with intercom calls, door opening, arming modes, and other functions. As for the door access control, you can choose which relay to activate by this voice assistant.

To configure the voice assistance, go to **Intercom > Basic > Voice Assistant Setting** interface.



- **Voice Assistant**: Enable/disable the voice assistant function.
- **Enabled Time**: Define the operational hours for the voice assistant.
  - Always: Voice assistant remains continuously enabled.
  - Schedule: Voice assistant operates based on the defined schedule below.
- **Day**: Select the day(s) when the voice assistant is active.
- **Time**: Set the specific period for the voice assistance to operate.

The voice assistant function on the device is shown below:


This intercom is hands free and can be controlled by your voice, simply say "Call Reception/Call Concierge" and wait for a reply.
You may say:
Call Reception/Call Concierge
Face Recognition
Express Delivery
Scan QR code

Tip:

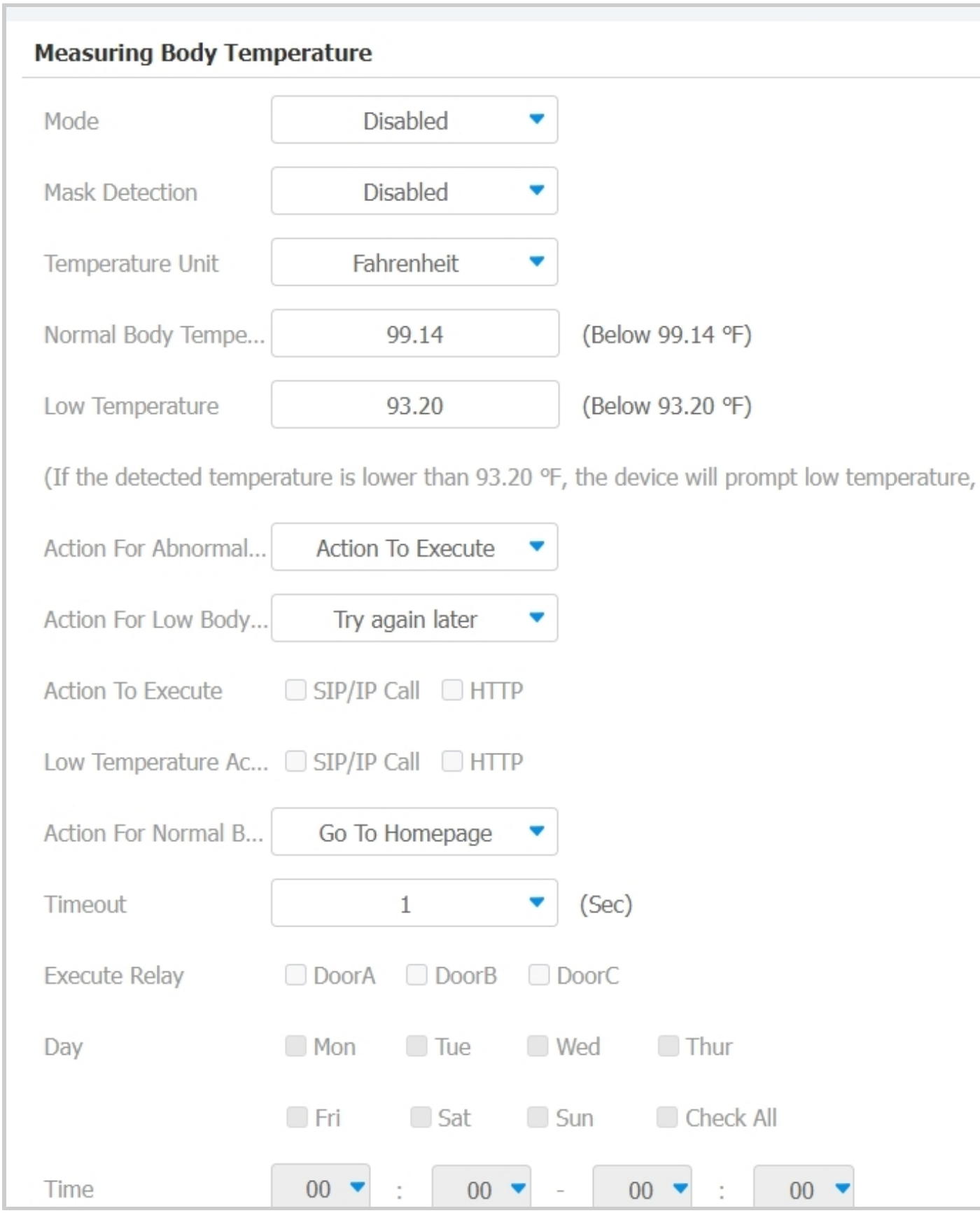
After being waken up, the voice assistant can perform the following tasks for users:

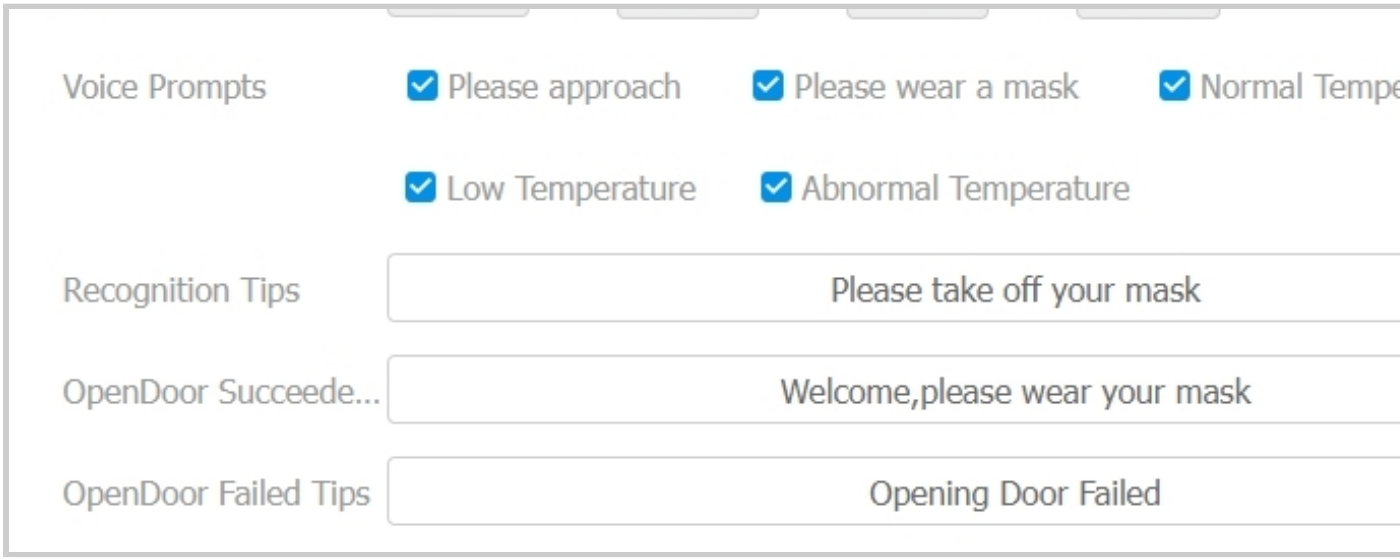
Function	Description
Call Reception/ Call Concierge	After waking up the voice assistant, say "Call Reception' or 'Call Concierge" to make a call. Configure the **reception number** before the voice assistant can automatically dial it.
Face Recognition	Say "Face Recognition" to go to the facial recognition screen.
Express Delivery	Say "Express Delivery" to access the dial screen, where users can either scan the QR code or enter the temporary PIN for door access.
Scan QR Code	Say "Scan QR Code" to utilize the QR code for door access.

Body Temperature Measurement for Door Access

Body Temperature Measurement Configuration

You can configure the body temperature measurement function on the device web **Access Control > Body Temperature > Measuring Body Temperature** interface in terms of defining the normal temperature as well as making the schedule for the validity of the function etc.


Measuring Body Temperature
Mode
Disabled
Mask Detection
Disabled
Temperature Unit
Fahrenheit
Normal Body Tempe...
99.14
(Below 99.14 °F)
Low Temperature
93.20
(Below 93.20 °F)
(If the detected temperature is lower than 93.20 °F, the device will prompt low temperature,
Action For Abnormal...
Action To Execute
Action For Low Body...
Try again later
Action To Execute
SIP/IP Call
HTTP
Low Temperature Ac...
SIP/IP Call
HTTP
Action For Normal B...
Go To Homepage
Timeout
1
(Sec)
Execute Relay
DoorA
DoorB
DoorC
Day
Mon
Tue
Wed
Thur
Fri
Sat
Sun
Check All
Time
00
:
00
-
00
:
00



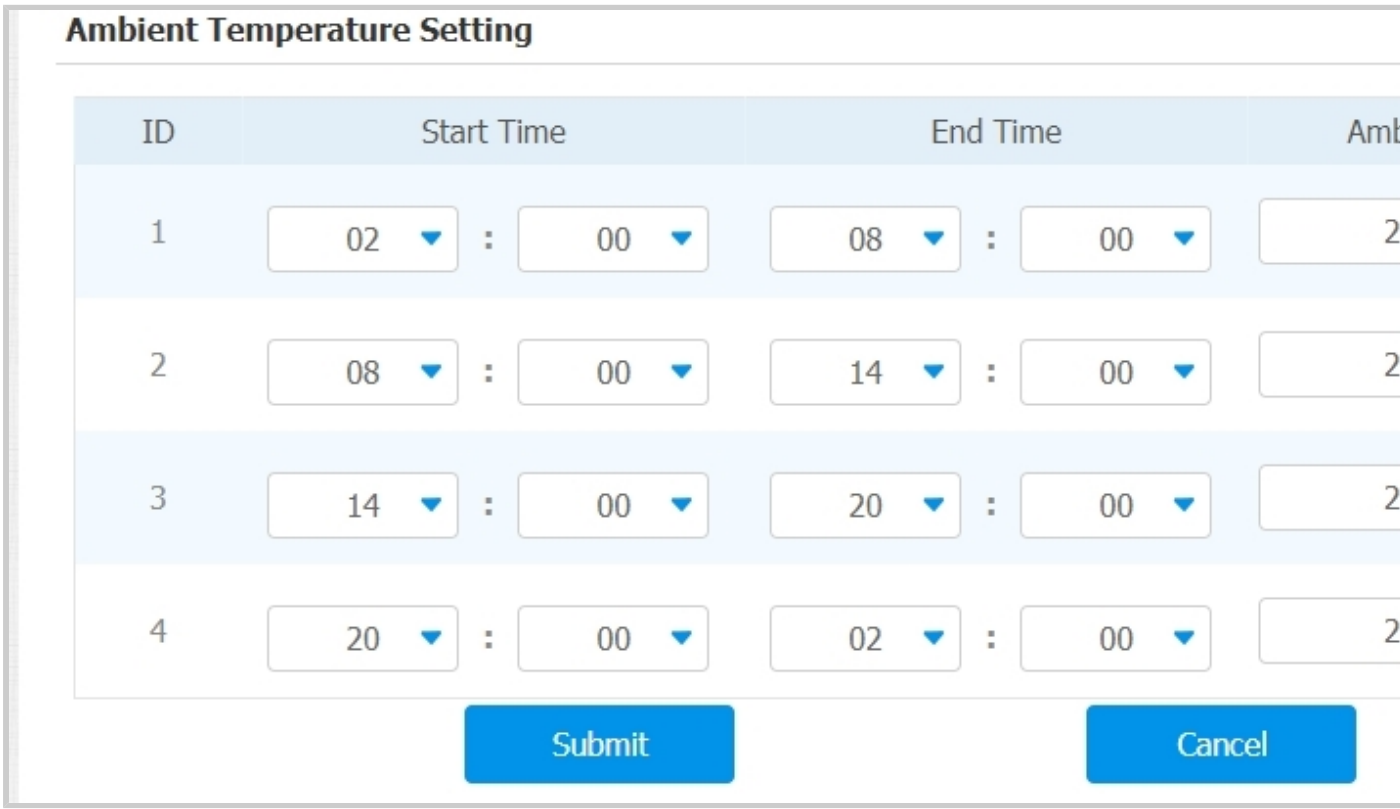
- **Mode**: Enable forehead or wrist temperature measurement, or disable the function.
  - Disabled: Turn off temperature measurement.
  - Forehead: Measure forehead temperature with a built-in module(R29C-B only).
  - Wrist: Measure wrist temperature with the additional device(R29C-B excluded).
- **Mask Detection**: Detect whether visitors are wearing masks. When enabled, the device reminds those without masks to wear one with the prompt "Please wear a mask."
- **Temperature Unit**: Select between Celsius and Fahrenheit to specify the measurement used to express temperature.
- **Normal Body Temperature**: Define the fever cut-off temperature. For example, setting it at 37.3 degrees Celsius means any temperature higher than that is considered a fever, triggering the preset action(s) for abnormal body temperature.
- **Low Temperature**: Set the lowest normal temperature. Any temperature below this value triggers the preset designated action(s).
- **Action for Abnormal Body Temperature**: Set the actions that occur when a fever is detected.
  - Action to Execute: When selected, choose the desired box in the Action to Execute field including SIP/IP Call and HTTP.

  - Go to Home Page: The door phone returns to the Home screen.
- **Action for Low Body Temperature**: Set the actions that occur when a low temperature is detected.
  - Try again later: The device prompts “Try again later” and executes the specified actions set under the Low Temperature Action field.
  - Go To Homepage: The door phone returns to the Home screen.
- **Action to Execute**: This field only appears when Action to Execute is selected for the Action for Abnormal Body Temperature.
  - SIP/IP Call: Call designated numbers, including local numbers, dial plans, SmartPlus numbers, and group ones.
  - HTTP: Send a preconfigured command to the door phone to execute the specified actions.
- **Low Temperature Action**: This field only appears when “Try again later” is selected for the Action for Low Body Temperature.
  - SIP/IP Call: Call designated numbers, including local numbers, dial plans, SmartPlus numbers, and group ones.
  - HTTP: Send a preconfigured command to the door phone to execute the specified actions.
- **Action for Normal Body Temperature**: Set the actions that occur when the temperature detected is normal.
- **Timeout**: Specify the termination time for temperature measurement in case of no operation or face detection.
- **Execute Relay**: Select the relay(s) to be triggered.
- **Day**: Select the day(s) when the relay can be triggered.
- **Time**: Set the specific period for the relay to be triggered.
- **Voice Prompts**: Select the desired voice prompts for various scenarios.
- **Recognition Tips**: Customize the prompt displayed for face verification.
- **OpenDoor Succeeded Tips**: Customize the message displayed when the relay is triggered.
- **OpenDoor Failed Tips**: Customize the message displayed when the relay fails to be triggered.

Ambient Temperature Configuration

You can adjust the temperature settings according to different time segments of the day. This can help you balance the temperature variations due to different locations and times.

To set it up, navigate to **Access Control > Body Temperature > Ambient Temperature Setting** interface.



- **Start Time/End Time**: Divide the 24 hours into four time segments.
- **Ambient Temperature**: Ambient temperature affects the sensitivity of fever detection, with increased sensitivity at higher ambient temperature.

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.

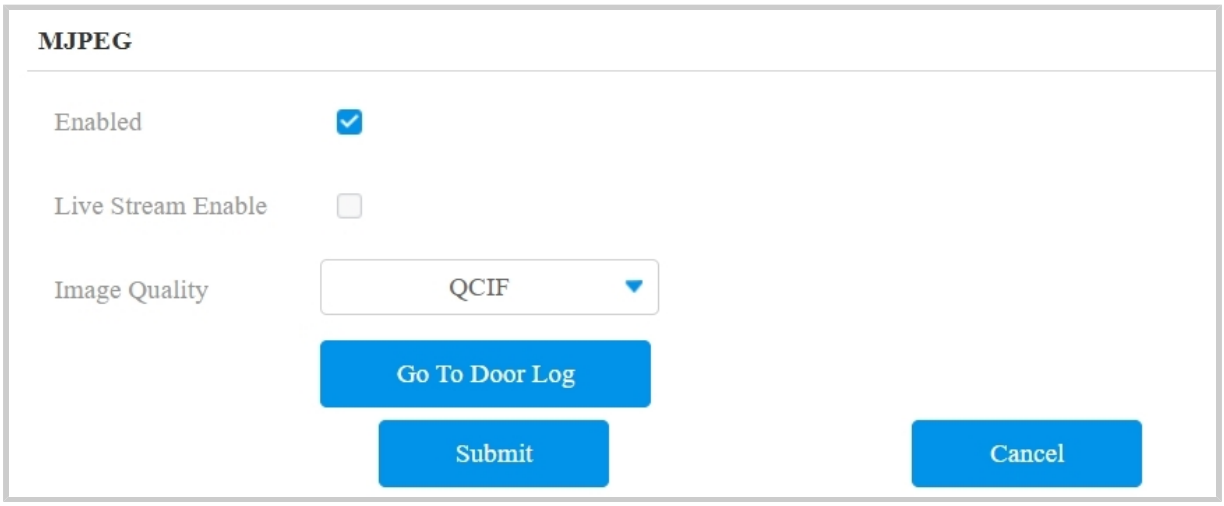
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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 **Surveillance > MJPEG** interface.

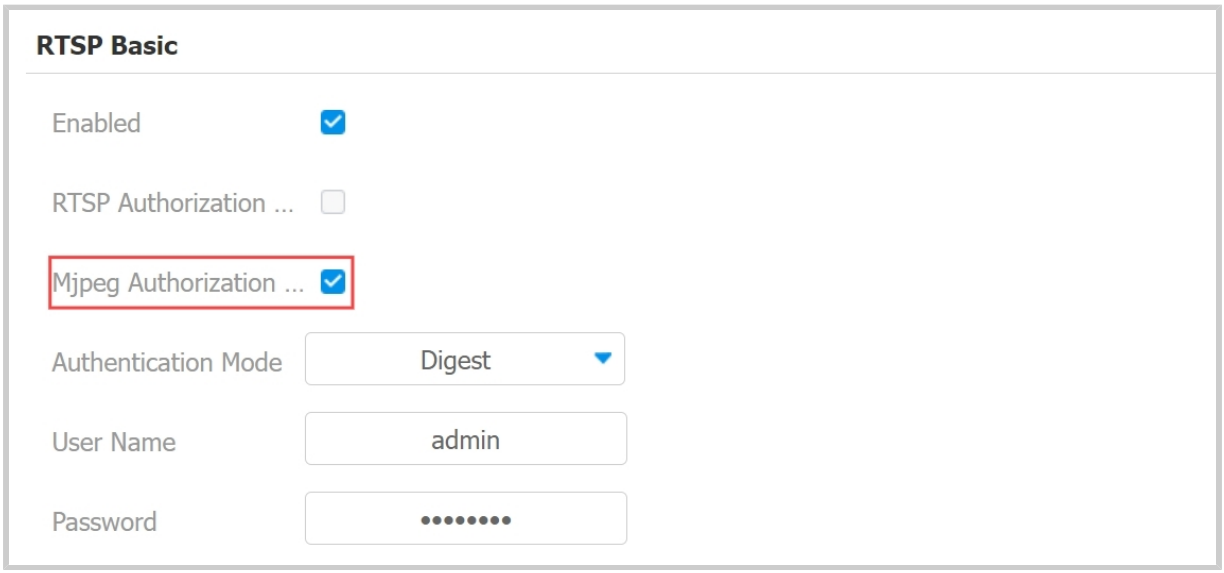


- **Live Stream Enable**: Set whether to view the video stream via URLs(*http://ip:8080/video.cgi; http://ip:8080/picture.cgi; http://ip:8080/jpeg*. It is disabled by default.
- **Image Quality**: Specify the MJPEG image quality from the lowest QCIF(176×144 pixels) to the highest 1080P(1920×1080 pixels).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

MJPEG Authorization

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

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



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

Tip

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

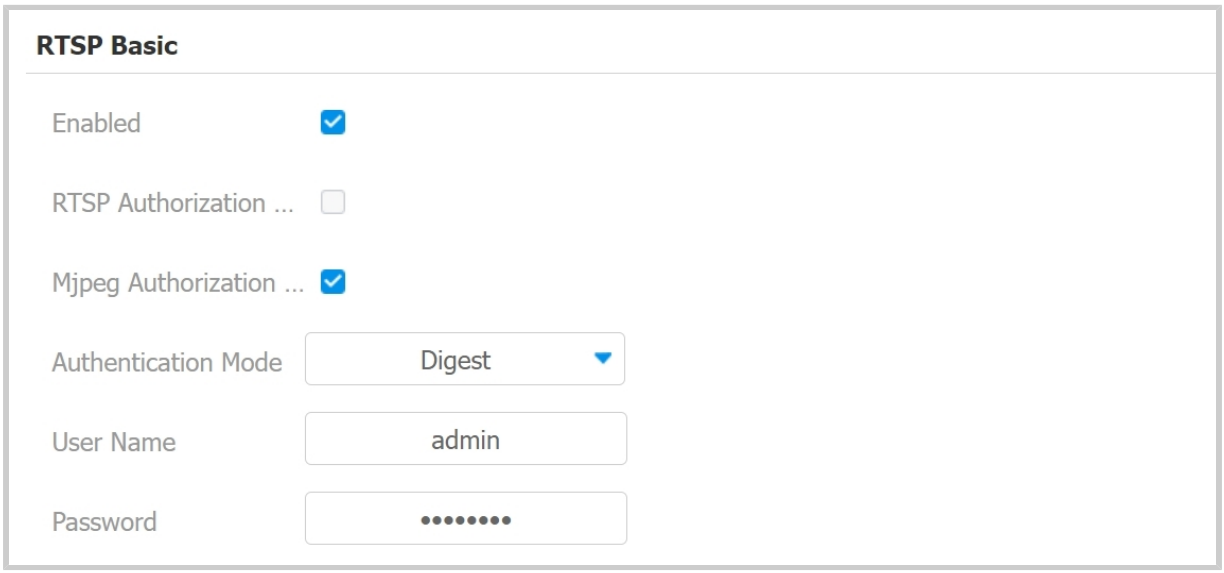
RTSP Stream Monitoring

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

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

RTSP Basic Setting

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

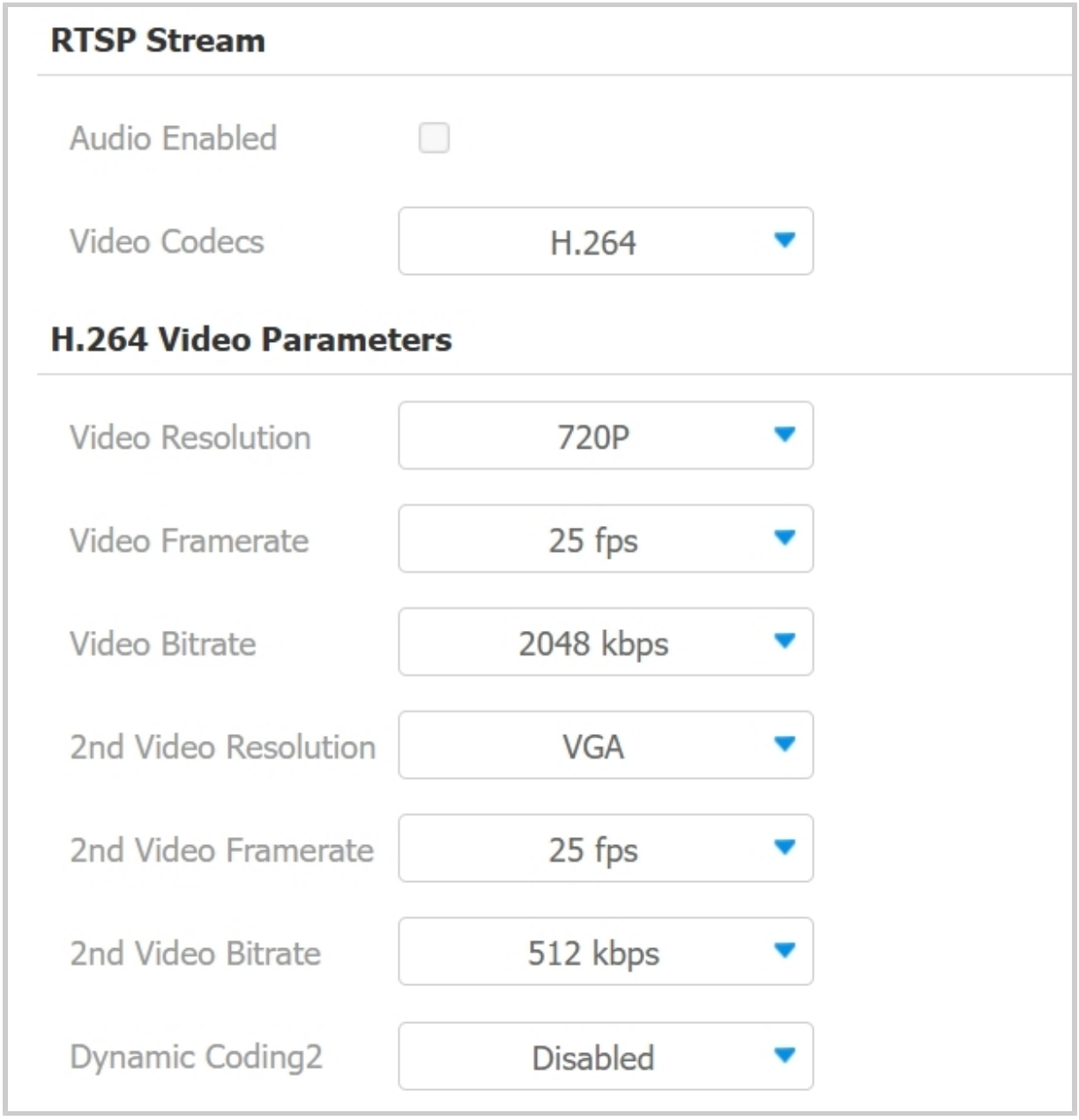


- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: Select between Basic and Digest.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

RTSP Stream Setting

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

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



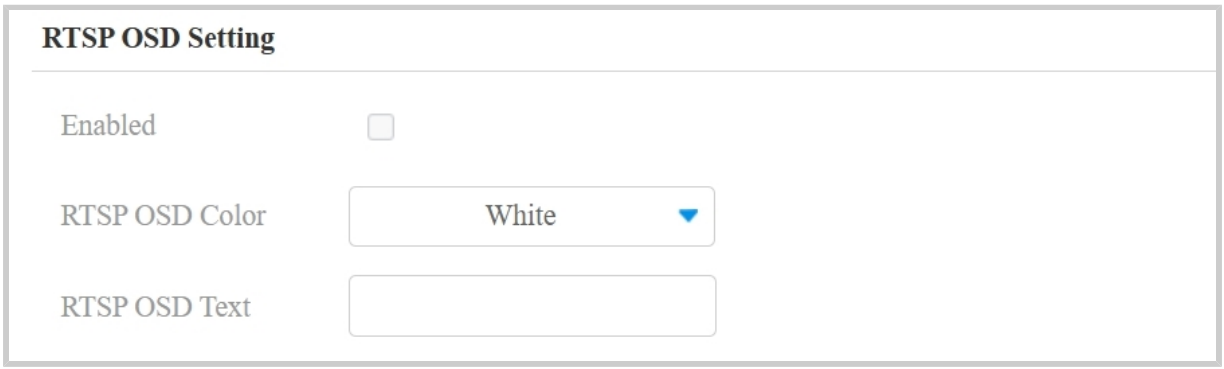
- **Audio Enabled**: Allow the door phone to send audio information to the monitor by RTSP.
- **Video Codec**: Select between H.264 and MJPEG.
- **Video Resolution**: Specify the image resolution, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 25fps.
- **Video Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048 kbps.
- **2nd Video Resolution**: Specify the image resolution for the second video stream channel.
- **2nd Video Framerate**: Set the frame rate for the second video stream channel.
- **2nd Video Bitrate**: Set the bit rate for the second video stream channel. The default is 512 kbps.
- **Dynamic Coding2**: If it is enabled, the dynamic coding will be automatically adopted for the video preview and monitoring on the SmartPlus App. The video resolution will be optimized when you use your SmartPlus app for the call preview for the incoming calls from the door phone and for the door phone monitoring.

> **Tip**
>
> To view the audio and video stream using RTSP:
>
> - First channel: rtsp://Device's IP/live/ch00_0
> - Second channel: rtsp://Device's IP/live/ch00_1

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture. It is disabled by default.

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

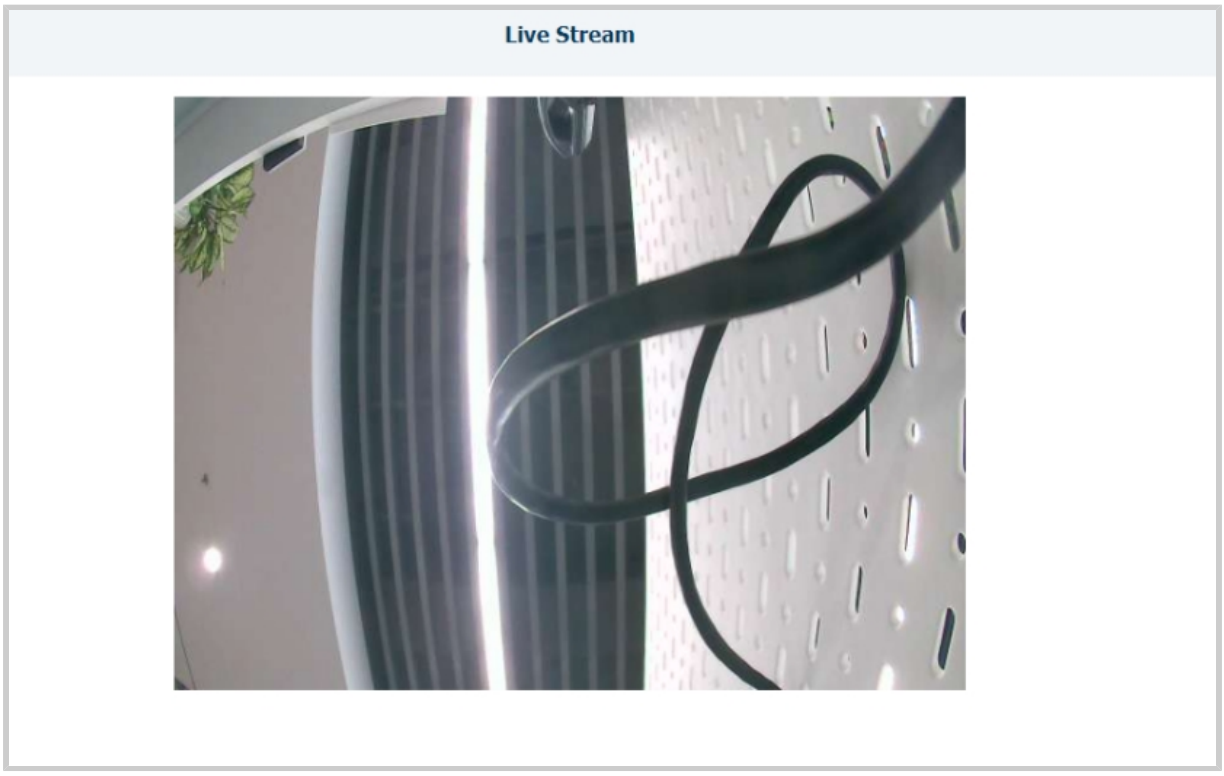


- **RTSP OSD Color**: Select the color from White, Black, Red, Green, and Blue.
- **RTSP OSD Text**: Customize the OSD content.

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

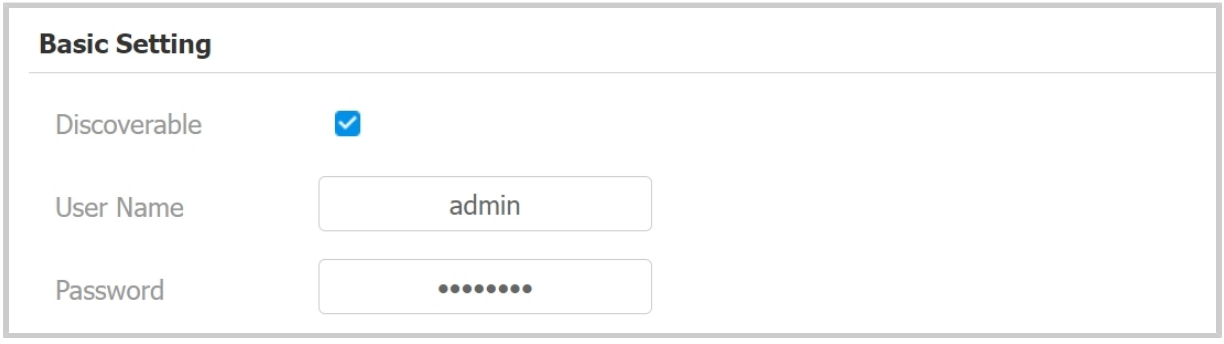


ONVIF

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 **Surveillance > ONVIF >Basic Setting** interface.



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

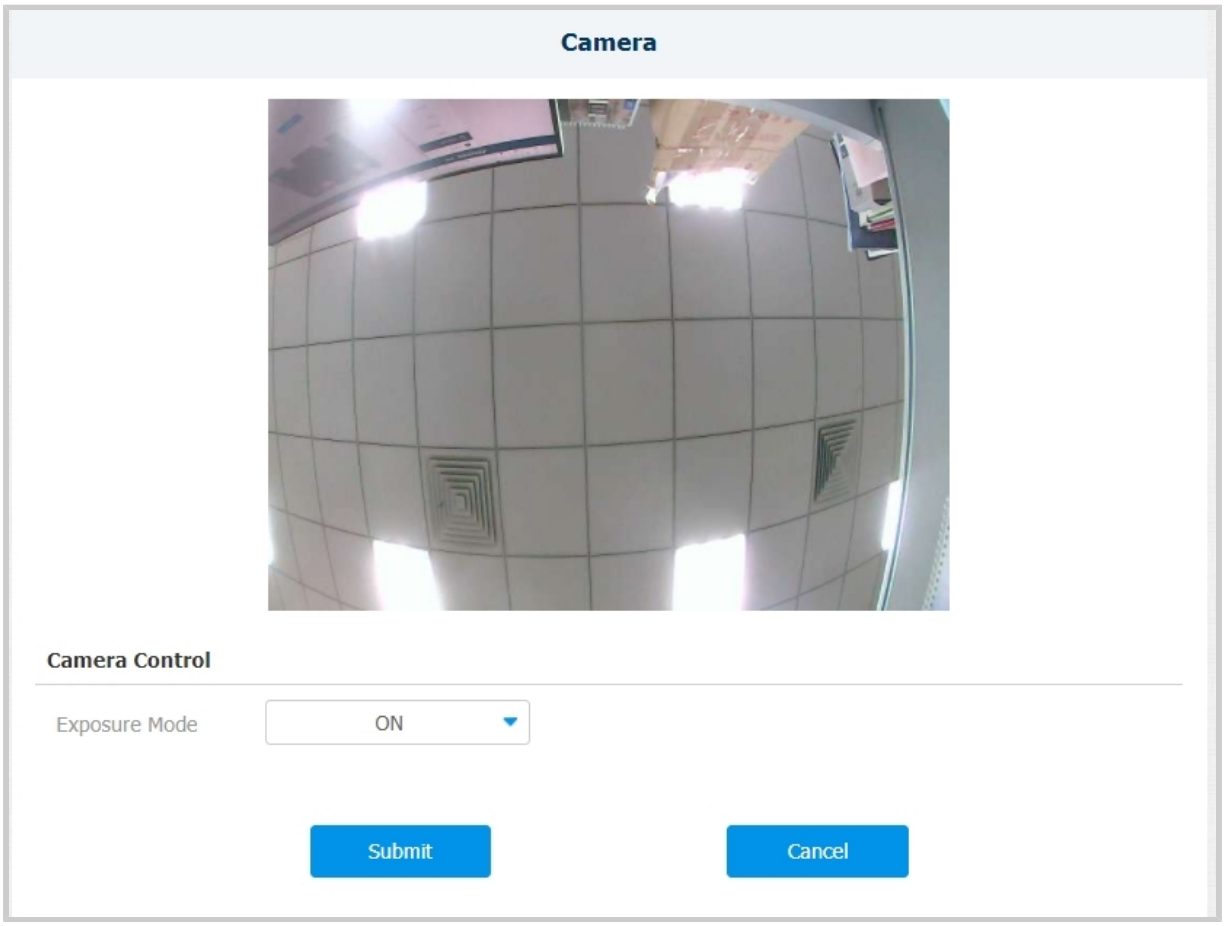
> **Tip**
>
> Once the settings are configured, to access the video stream on the third-party device, simply enter the ONVIF URL: http://Device's IP:80/onvif/device_service.

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



Camera Exposure Adjustment

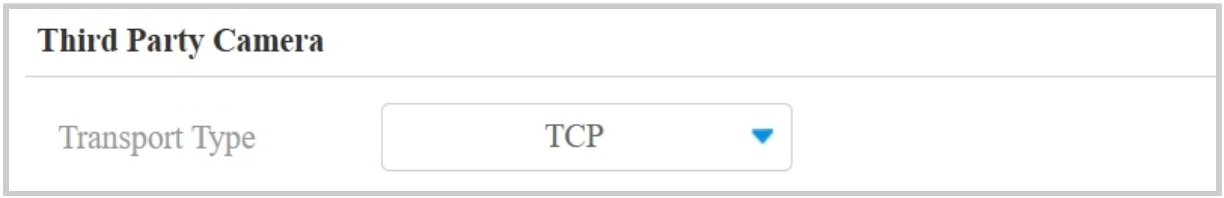
Door phone camera exposure can be turned on the web **Device > Camera** interface so that indoor monitors or third-party devices can obtain the video with improved quality.



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.

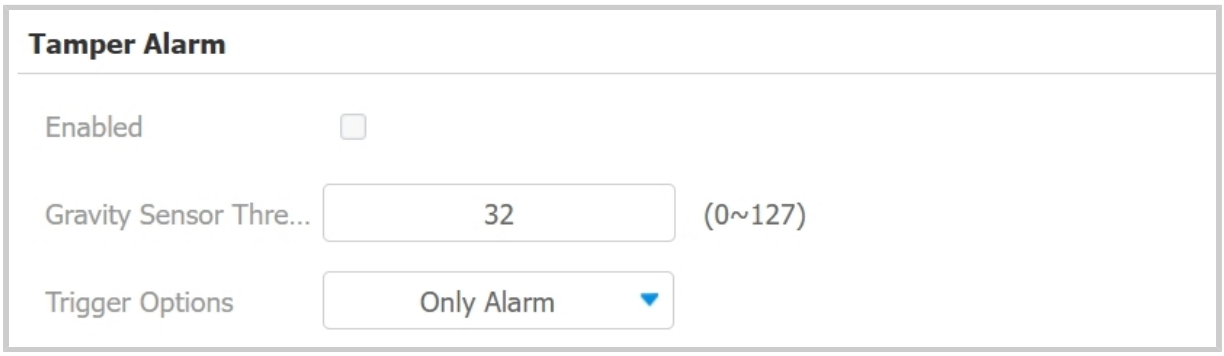
Security

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.

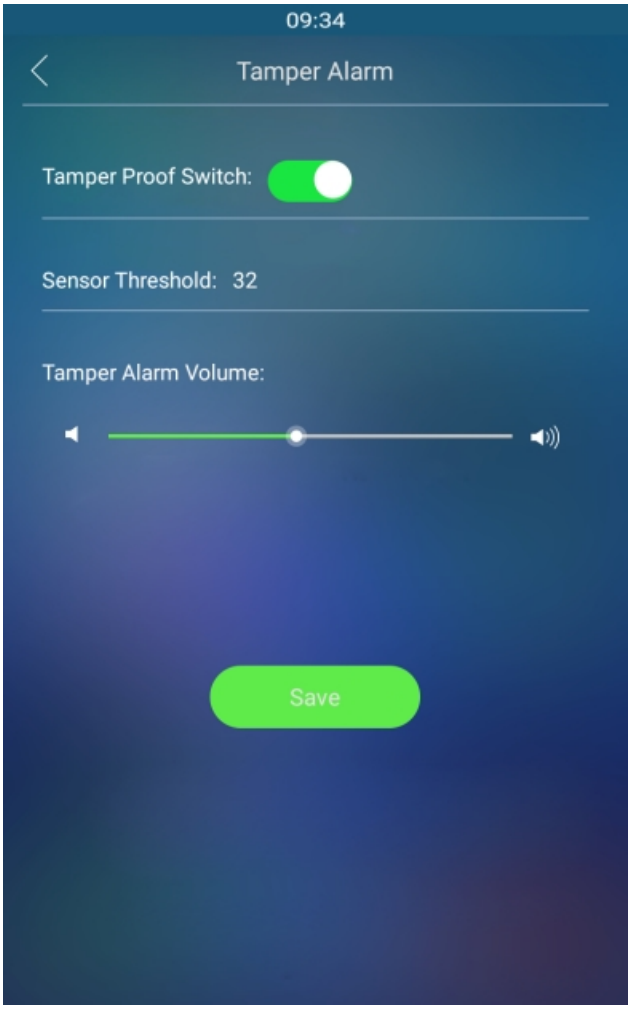
Click here to view which type is supported by the device and learn the function details.

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



- **Gravity Sensor Threshold**: Set the threshold for gravity sensory sensitivity. The lower the value is, the higher the sensitivity will be. The gravity sensor value is 32 by default.
- **Trigger Options**: Select what can be triggered when the gravity sensor is triggered.

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



Disarm Setting

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

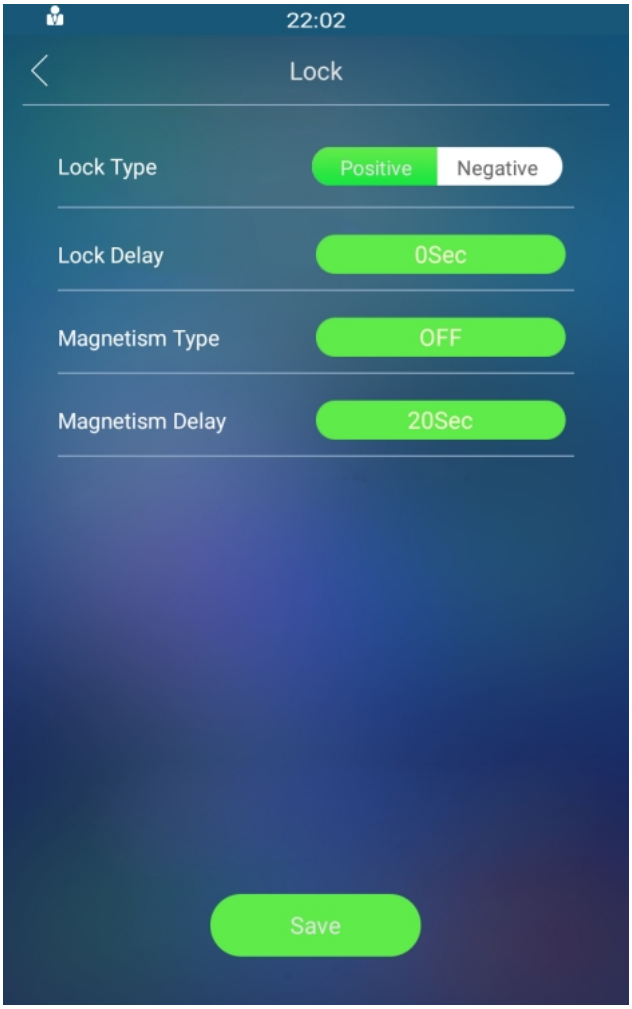
Set it up on the **System > Security > Disarm Setting** interface.



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.

Set it up on the **Setting > Lock** for the setting.



- **Lock Type**:
  - **Positive**: The lock unlocks when power is ON and locks when power is OFF. Suitable for scenarios where the door should remain locked during a power outage.

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

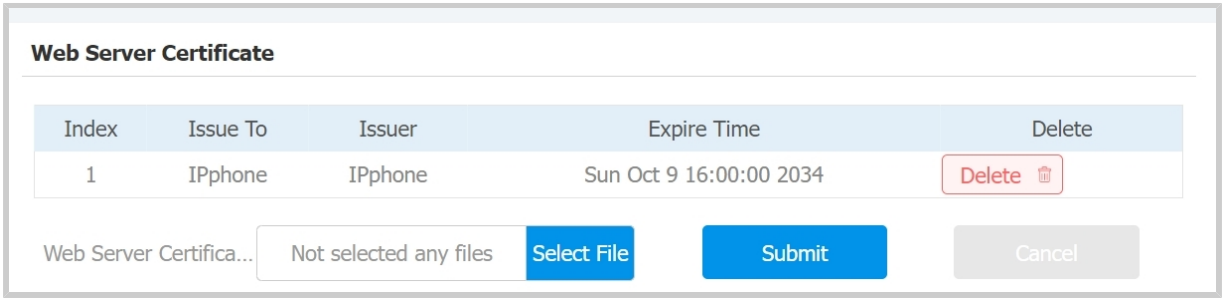
Client Certificate Setting

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

Web Server Certificate

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

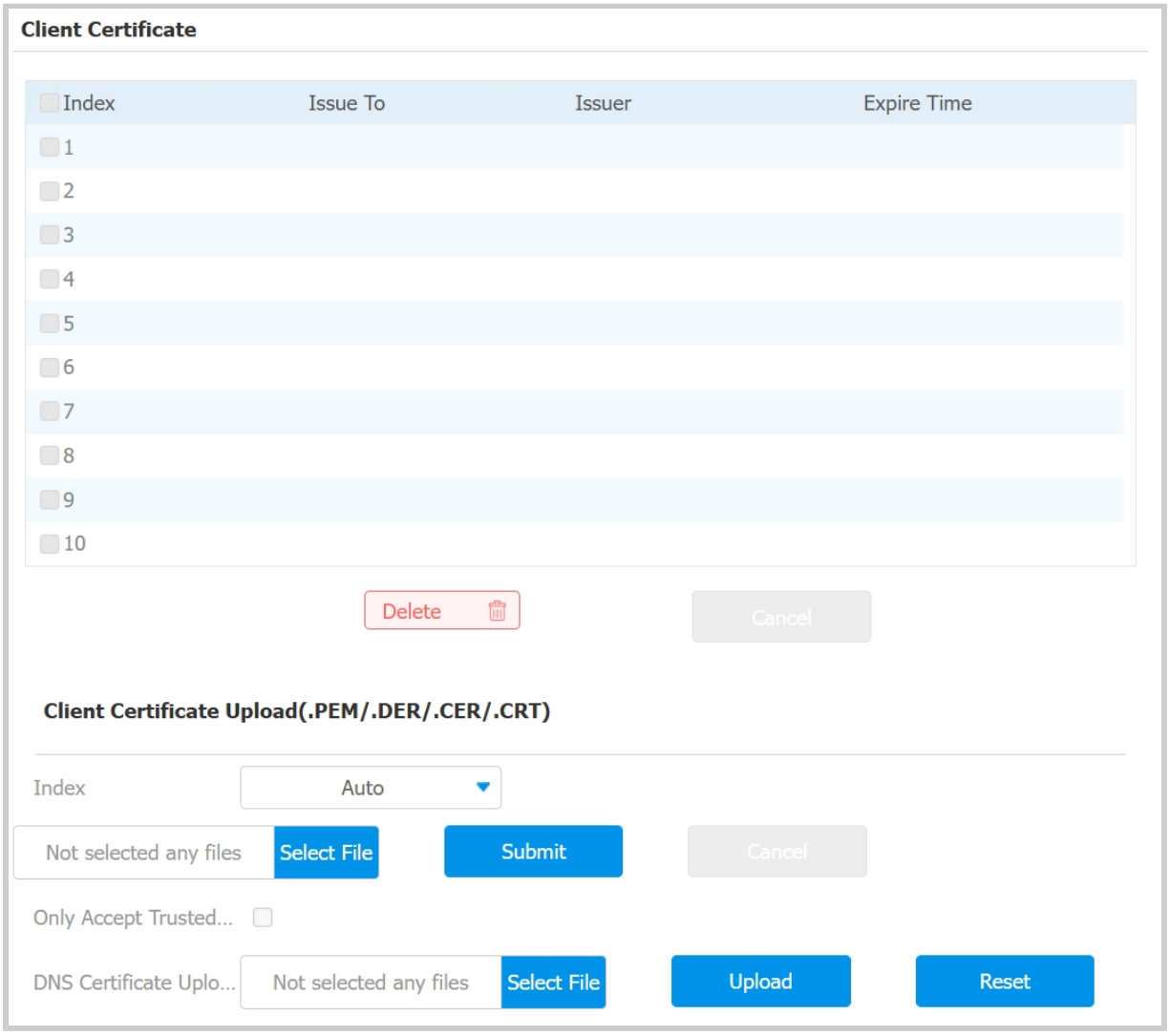
Upload the Web Server certificate on the device web **System > Certificate > Web Server Certificate** interface.



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 **System > Certificate > Client Certificate** interface.



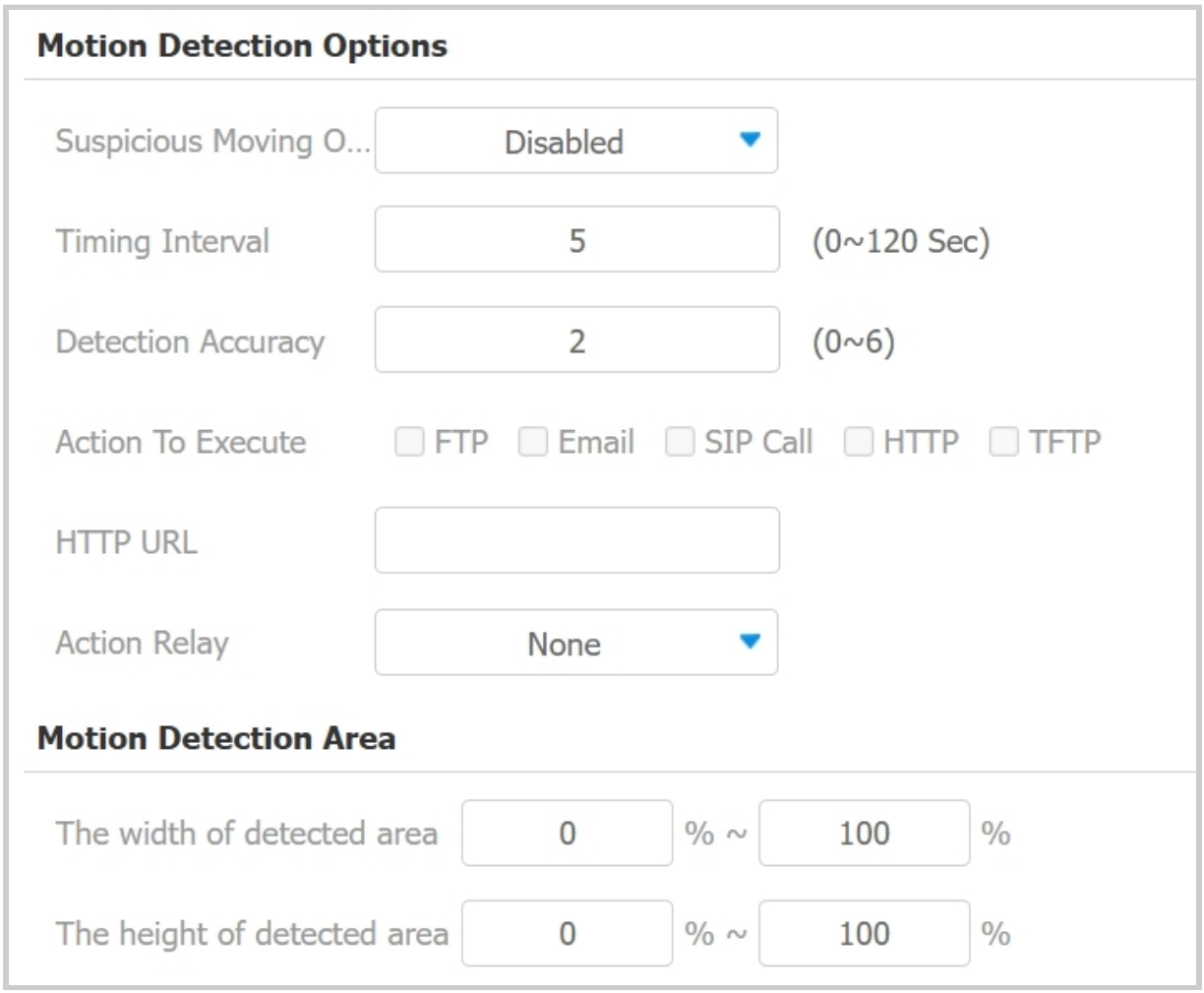
- **Index**: Select the desired value from the drop-down list of Index. If you select Auto, the uploaded certificate will be displayed in numeric order. If you select the value from 1 to 10, the uploaded certificate will be displayed according to the number.

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

Motion Detection

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

Set it up on the **Surveillance > Motion** interface.



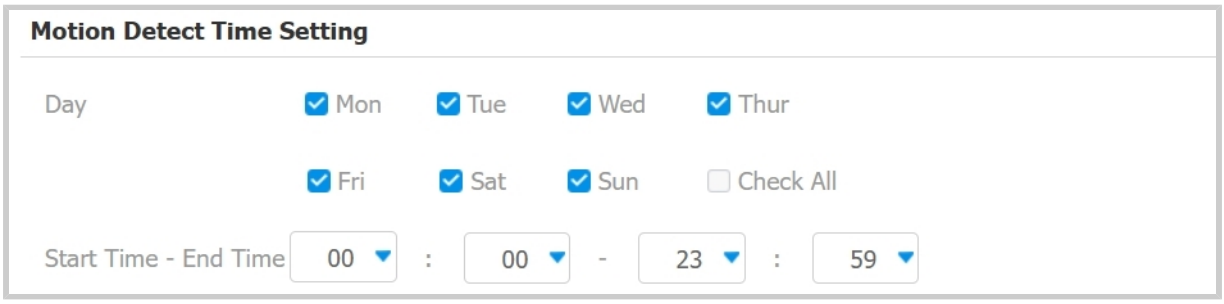
- Suspicious Moving Object Detection:
  - Disabled: Turn off the motion detection function.
  - Video Detection: When the video camera detects moving objects, preset actions will be triggered. Focus on analyzing visual information captured through cameras.
  - IR Detection: When the infrared detects moving objects, preset actions will be triggered. It offers better detection in low-light or dark conditions.
  - Pedestrian Detection: When the device detects the upper body of the passers-by, preset actions will be triggered.
- 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 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 2.
- **Action to Execute**: The notification type includes FTP, Email, SIP Call, HTTP, and TFTP.
  - FTP: The notification will be sent to the designated FTP server.
  - Email: The email will be sent to the pre-configured email address.
  - SIP Call: A call will be made to the pre-configured number.
  - HTTP: The notification will be sent to the designated server.
  - TFTP: The notification will be sent to the designated TFTP server .
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Relay**: The relay to be triggered.
- **Motion Detection Area**: Available for video and pedestrian detection. You can limit the detection area by drawing a box. You can also enter the value. Start by measuring it as a percentage from left to right, with 100% representing the entire width. You can then choose a horizontal detection range from 0% to 100% and a vertical detection range from 0% to 100%. The intersection of these selected ranges will give you the exact detection area you want, allowing for easy customization.

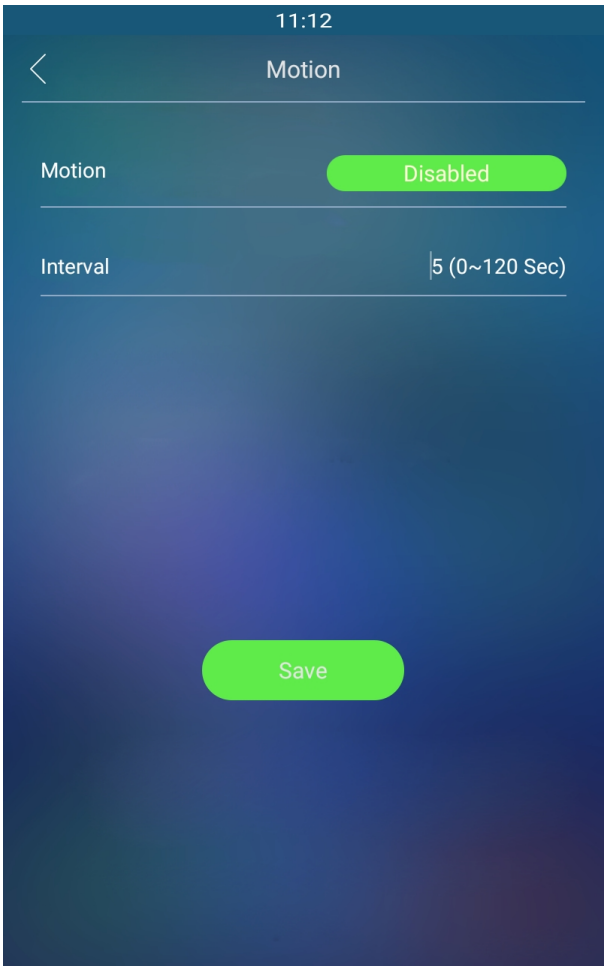
Motion Detection Schedule

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

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



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



Security Notification

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

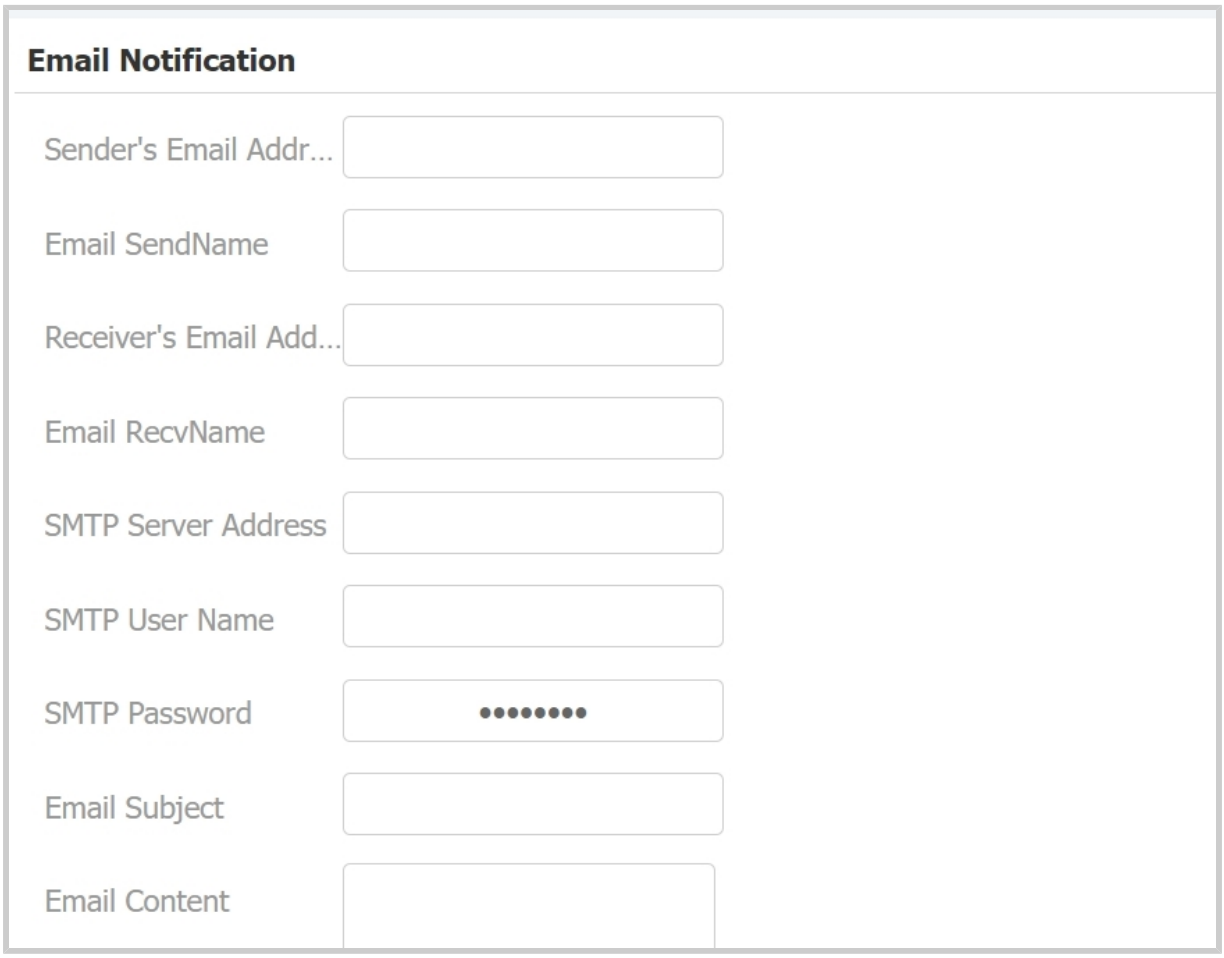
Set up notifications on the **Setting > Action** interface.

Email Notification

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

Click here to view how to set this feature up.

Find the **Email Notification** section.



- **SMTP Server Address**: The SMTP server address of the sender.

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

FTP Notification

To get notifications through FTP server, you need to set up the FTP settings. The door phone will upload a screenshot to the specified FTP folder if it senses any unusual motion.

Click here to view the configuration steps.

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



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

TFTP Notification

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

Click here to view the configuration steps.

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



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

SIP Call Notification

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

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



Action URL

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

Click here to view the action URL configuration example.

Akuvox Action URL:

No	Event	Parameter format
1	Make Call	$remote
2	Hang Up	$remote

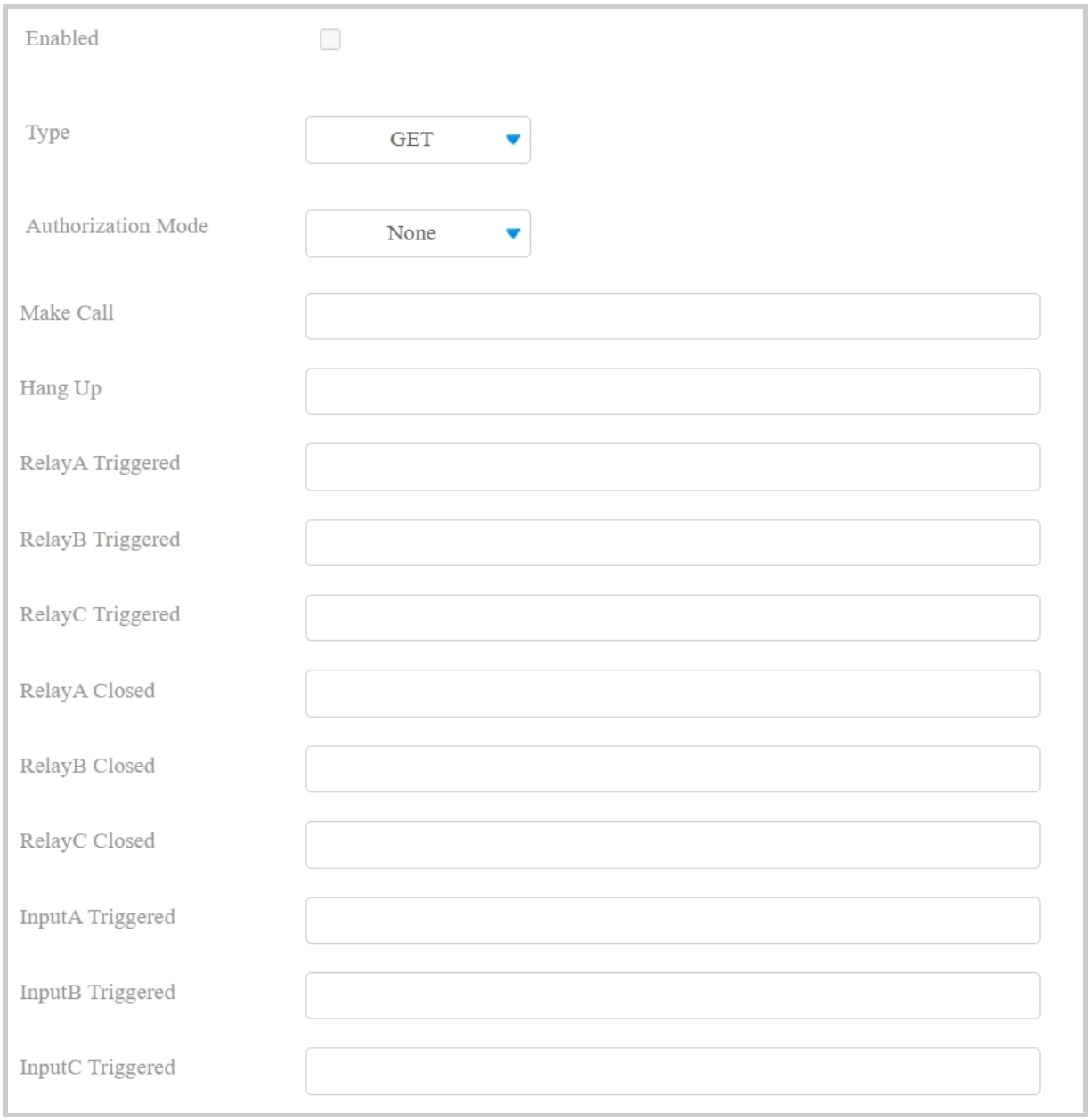
3	Relay Triggered	$relay1status
4	Relay Closed	$relay1status
5	Input Triggered	$input1status
6	Input Closed	$input1status
7	Valid Code Entered	$code
8	Invalid Code Entered	$code
9	Valid Card Entered	$card_sn
10	Invalid Card Entered	$card_sn
11	Facial Recognition	$unlocktype
12	Break-in Alarm	$input1status
13	QR Code Entered	$unlocktype

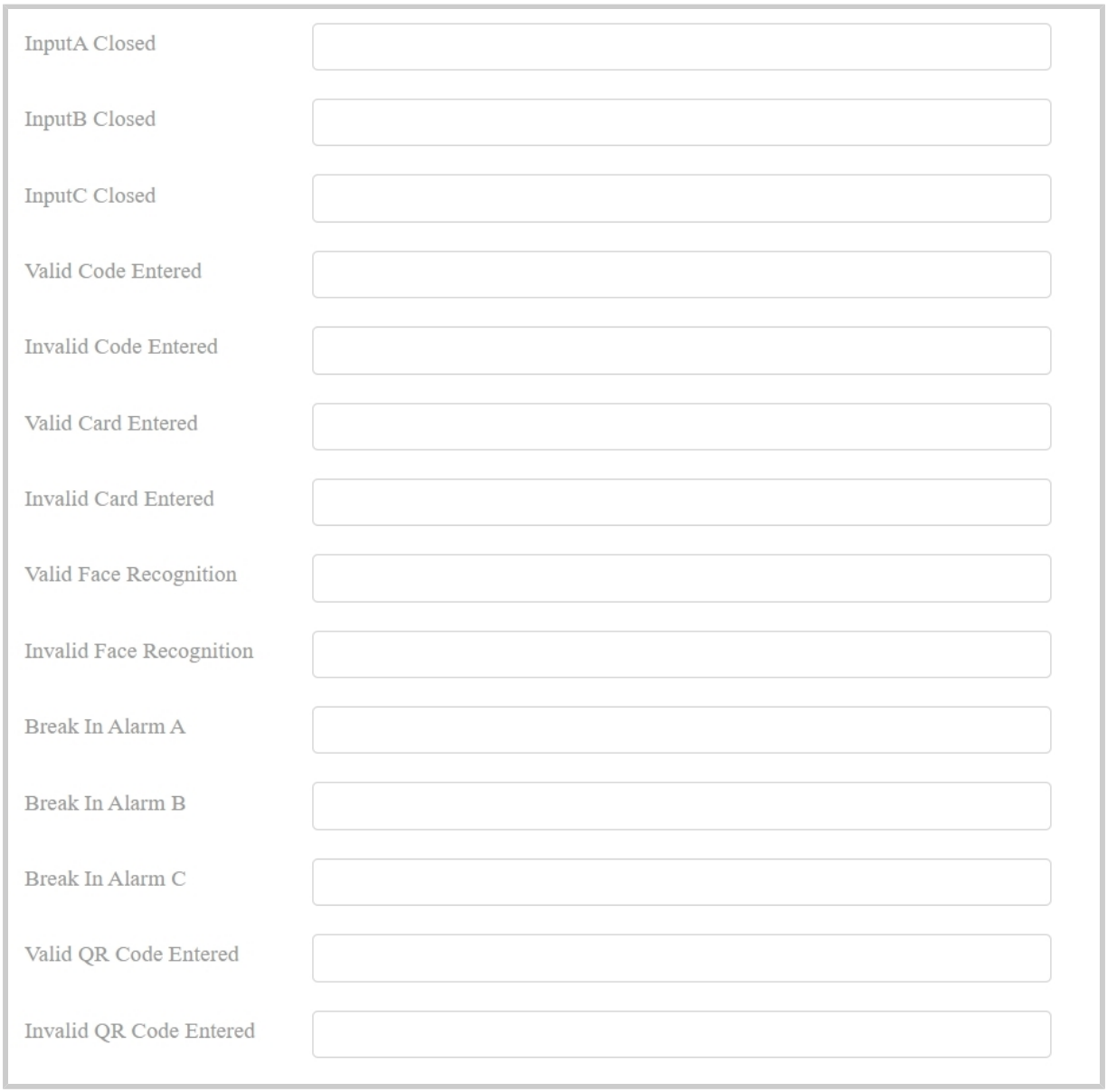
Example
Http://server ip/ Callnumber=$remote
Http://server ip/ Callnumber=$remote
Http://server ip/ relaytrigger=$relay1status
Http://server ip/relayclose=$relay1status
Http://server ip/inputtrigger=$input1status
Http://server ip/inputclose=$input1status
Http://server ip/validcode=$code

Http://server ip/invalidcode=$code
Http://server ip/validcard=$card_sn
Http://server ip/invalidcard=$card_sn
Http://server ip/unlocktype=$unlocktype
Http://server ip/inputtrigger=$input1status **NOTE**: $input1-3status corresponds to inputA-C.
Http://server ip/unlocktype=$unlocktype

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

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


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



- **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.

GDPR Setting

General Data Protection Regulation (GDPR) is a regulation in European Union's law on data protection and privacy. The GDPR feature in Akuvox door phone is to encrypts the card data you enter for better security.

Set it up on the **Access Control > Card Setting > Encrypted display of the card** interface.



- **Enabled**: If enabled, the card data will be encrypted automatically when an RF card is added.

User Agent

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

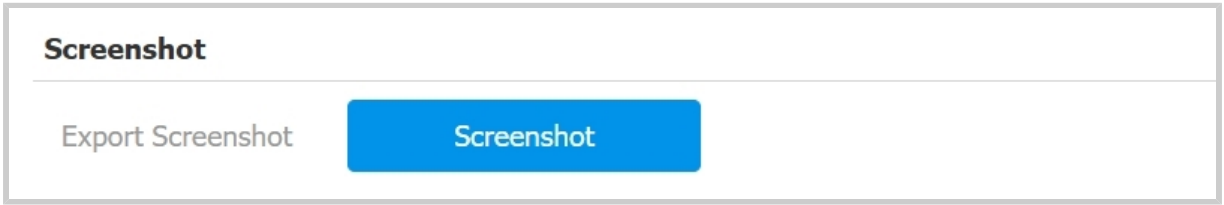
To set it up, go to the **Account > Advanced > User Agent** interface.



Screenshots

You can take a screenshot of the specific device screen to help with the troubleshooting and so on.

Take a screenshot on the **System > Maintenance > Screenshot** 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 **System > Security > Session Time Out** interface.

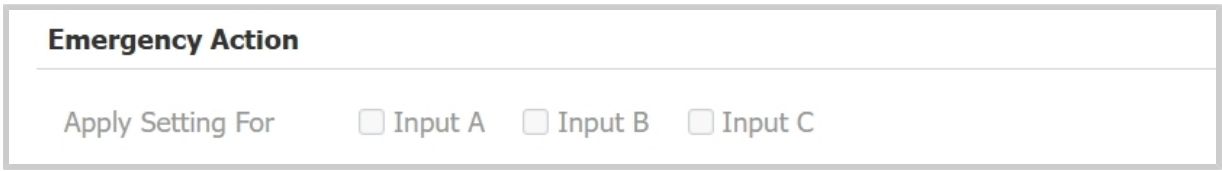


Emergency Action

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

Click here to view the detailed configuration of this feature.

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

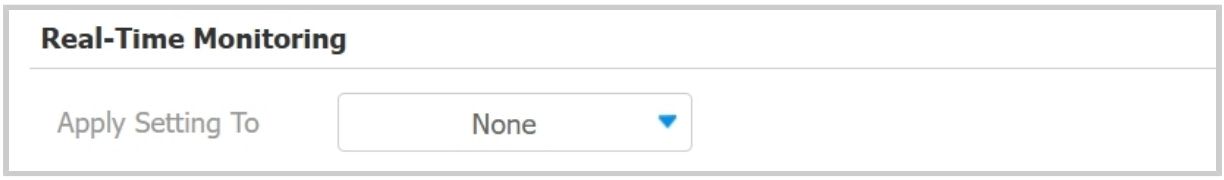


Real-time Monitoring

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

Click here to see the detailed configuration.

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



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.

Set it up on the **System > Security > High Security Mode**.



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

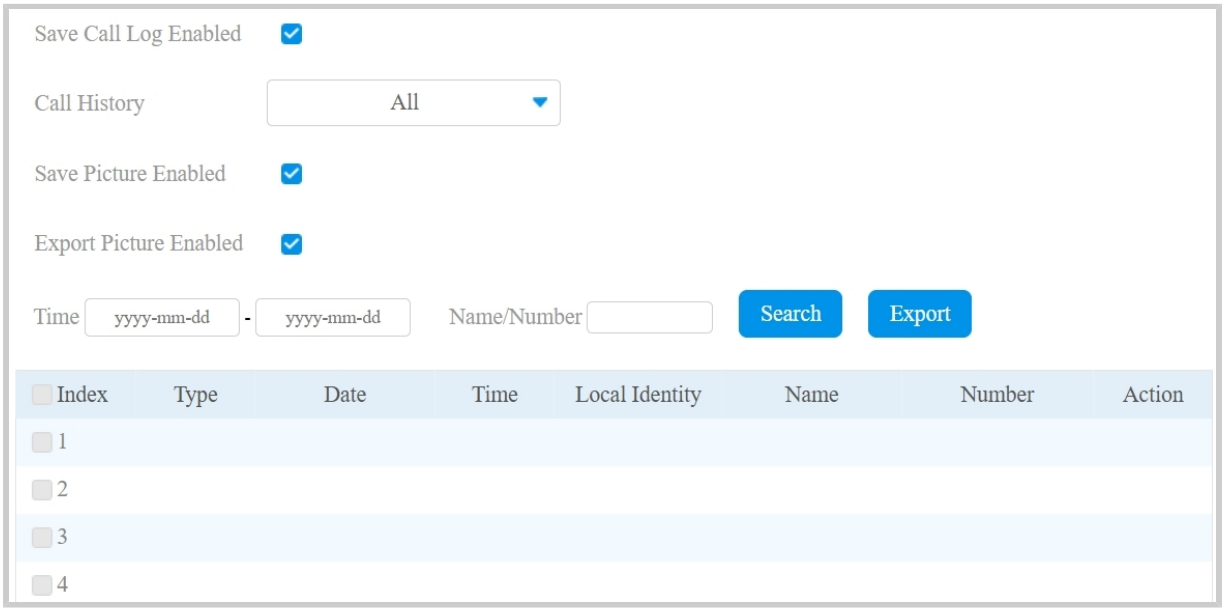
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

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 logs on the **Status > Call Log** interface. The device supports up to 600 call logs.



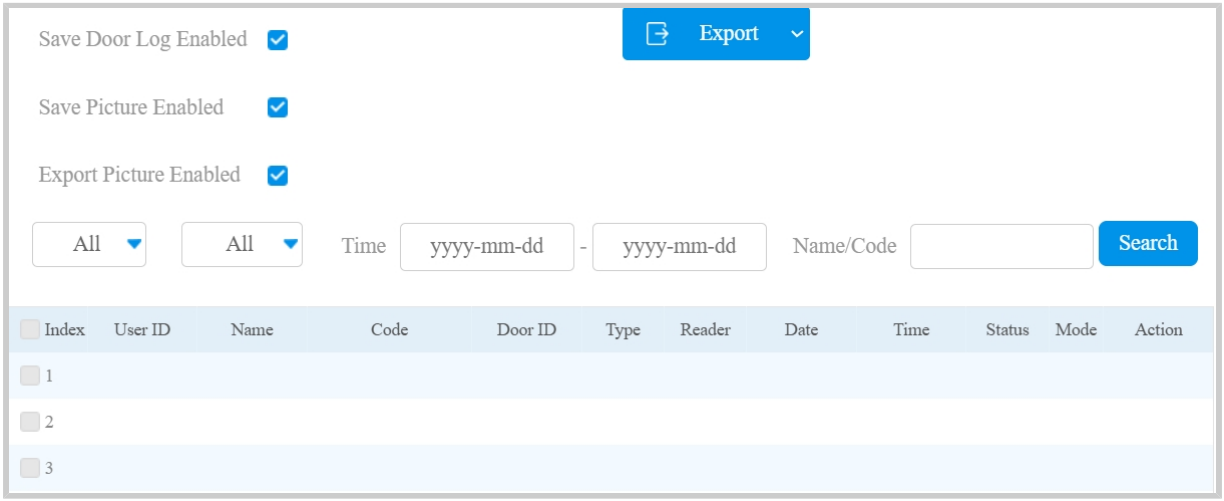
- **Call History**: Four types of call history are available: All, Dialed, Received, and Missed.
- **Time**: The specific time of the call logs you want to search, check, or export.
- **Name/Number**: Search the call log by the name or by the SIP or IP number.
- **Save Picture Enabled**: When enabled,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

- **Export Picture Enabled**: When enabled, you can export the call log file.
- **Export**: Call logs can be exported in .csv format.

Door Logs

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

Check the door log on the **Status > Access Log** interface. The device supports up to 50,000 door logs.



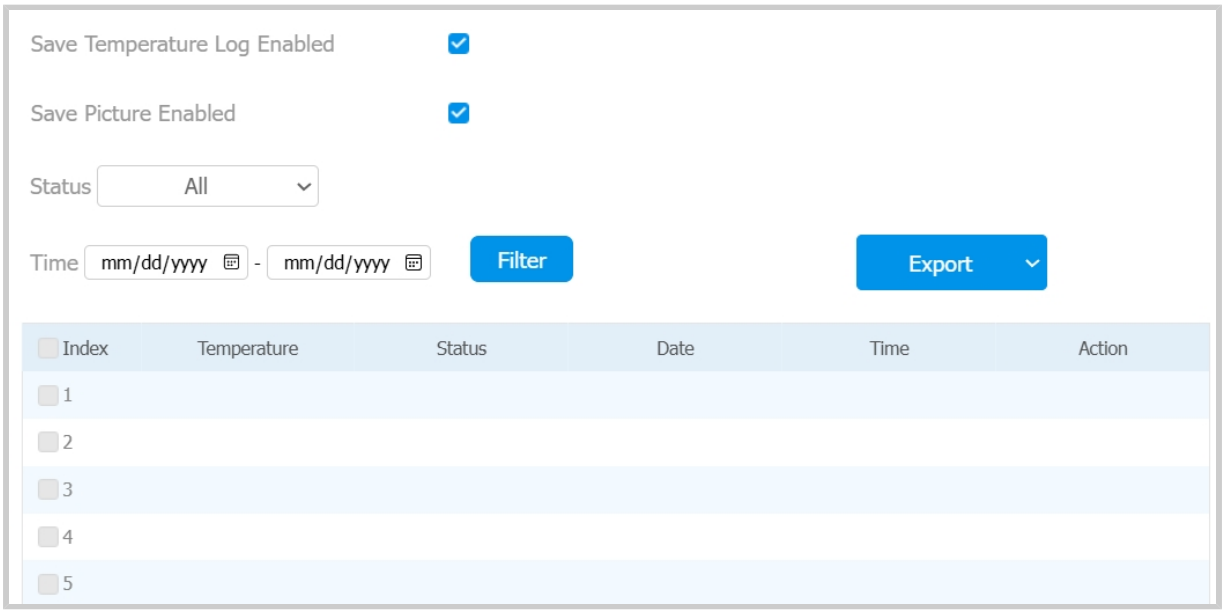
- **Save Picture Enabled**: When enabled, the device will capture pictures of door-opening, and you can click Picture in the Action column to view the snapshot.
- **Export Picture Enabled**: When enabled, you can export the door log file.
- **All**: Three types of access logs are available: All, Success,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

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

Resolution	Maximum Number of Stored Door Logs	Maximum Number of Exported Door Logs with 1.6G Export Capacity.
Null, Save Picture is disabled.	25,000	196,200
QCIF	25,000	196,200
QVGA	25,000	83,200
CIF	25,000	66,100
VGA	25,000	25,900
4CIF	20,000	20,900
720P	10,000	10,800
1080P	5,000	5,500

Temperature Logs

You can check the temperature logs on the **Status > Temperature Log** interface. The device supports up to 600 temperature logs.

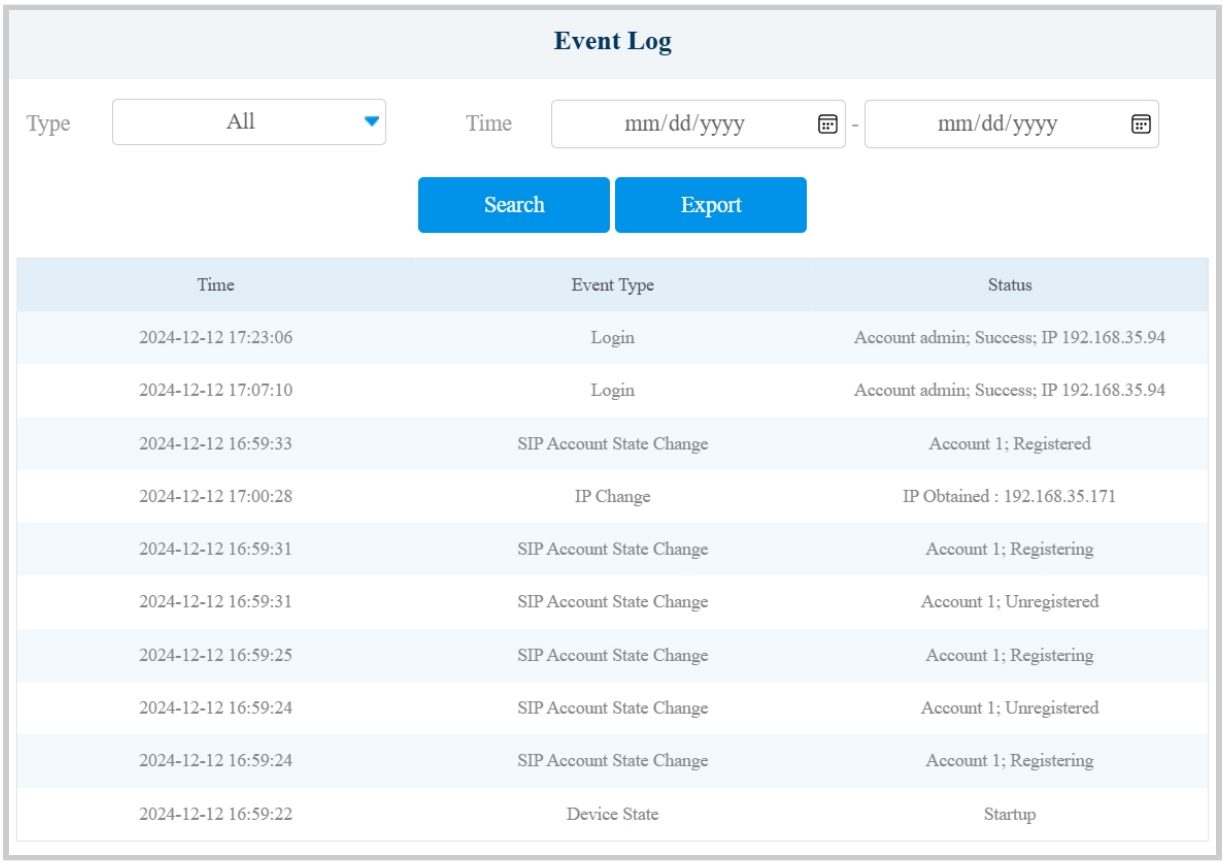


- **Save Picture Enabled**: Enable it if you want to save the temperature-measuring snapshot.
- **Export**: You can export the log in .xml or .csv format.
- **Time**: Select the specific period of the temperature log you want to search, check, or export.
- **Action**: Click to display the picture captured.

Event Logs

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

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



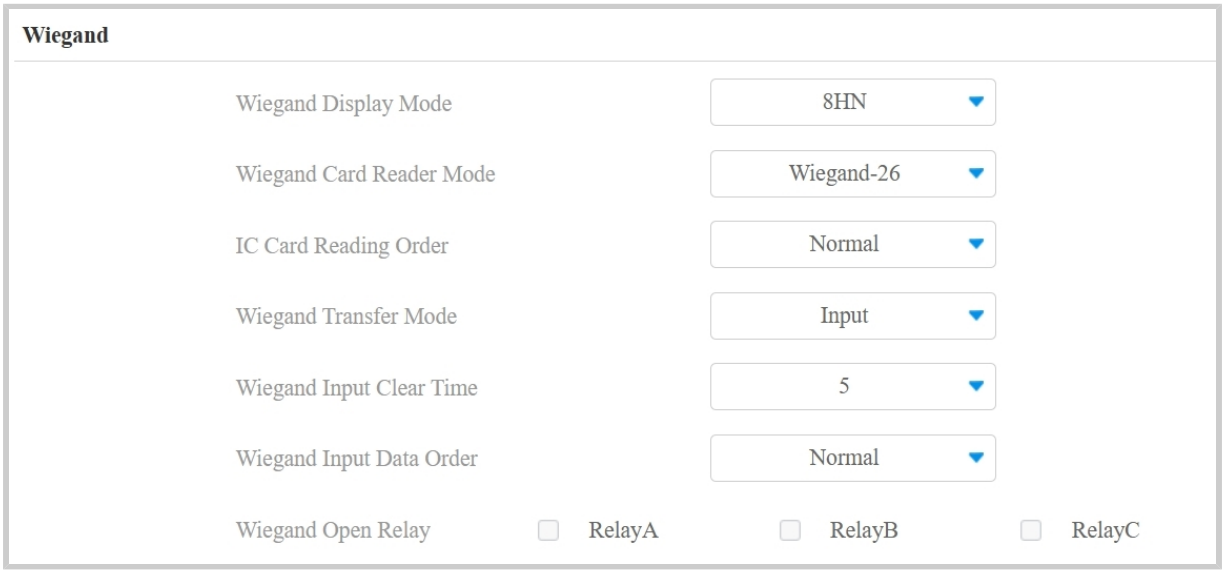
Time	Event Type	Status
2024-12-12 17:23:06	Login	Account admin; Success; IP 192.168.35.94
2024-12-12 17:07:10	Login	Account admin; Success; IP 192.168.35.94
2024-12-12 16:59:33	SIP Account State Change	Account 1; Registered
2024-12-12 17:00:28	IP Change	IP Obtained : 192.168.35.171
2024-12-12 16:59:31	SIP Account State Change	Account 1; Registering
2024-12-12 16:59:31	SIP Account State Change	Account 1; Unregistered
2024-12-12 16:59:25	SIP Account State Change	Account 1; Registering
2024-12-12 16:59:24	SIP Account State Change	Account 1; Unregistered
2024-12-12 16:59:24	SIP Account State Change	Account 1; Registering
2024-12-12 16:59:22	Device State	Startup

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 **Device > Wiegand > 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 Wiegand-26 by default.
- **IC Card Reading Order**: This option only works when Wiegand-26 is selected.
  - **Normal**: The device will read the last three bytes of the IC card. For example, if the IC card number is 840C9F50, 0C9F50 will be read.

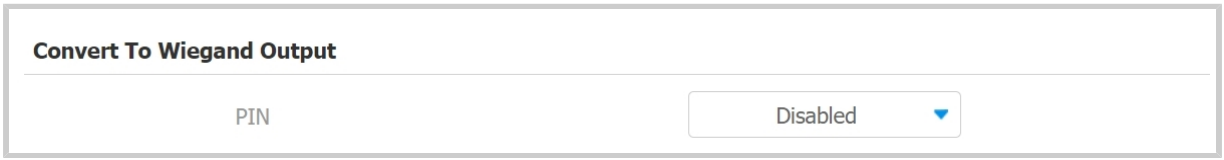
- **Reversed**: The device will read the first three bytes of the IC card. For example, if the IC card number is 840C9F50, 840C9F will be read.

- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
    - **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.
  - **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.
    - **Wiegand Output Basic Data Order**: Set the sequence of the card data before going through the Wiegand conversion and outputting the card code.
      For example, if the card data is 0x11 0x22 0x33 0x44 and the **Reversed** option is selected, the data will be 0x44 0x33 0x22 0x11.
    - **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
      For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If **Reversed** is selected, the card data is 0x55 0x44 0x33.
    - **Wiegand Output CRC**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
    - **RF Card/PIN/QR Code Verification**: 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.
  - **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 Open Relay**: Check the relay to be triggered through Wiegand.

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

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



- **8 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 8 bits, "11100001".
- **4 bits per digit**: When users press "1" on the keypad, the binary data will be transmitted in 4 bits, "0001".
- **All at once**: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode.

> **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.

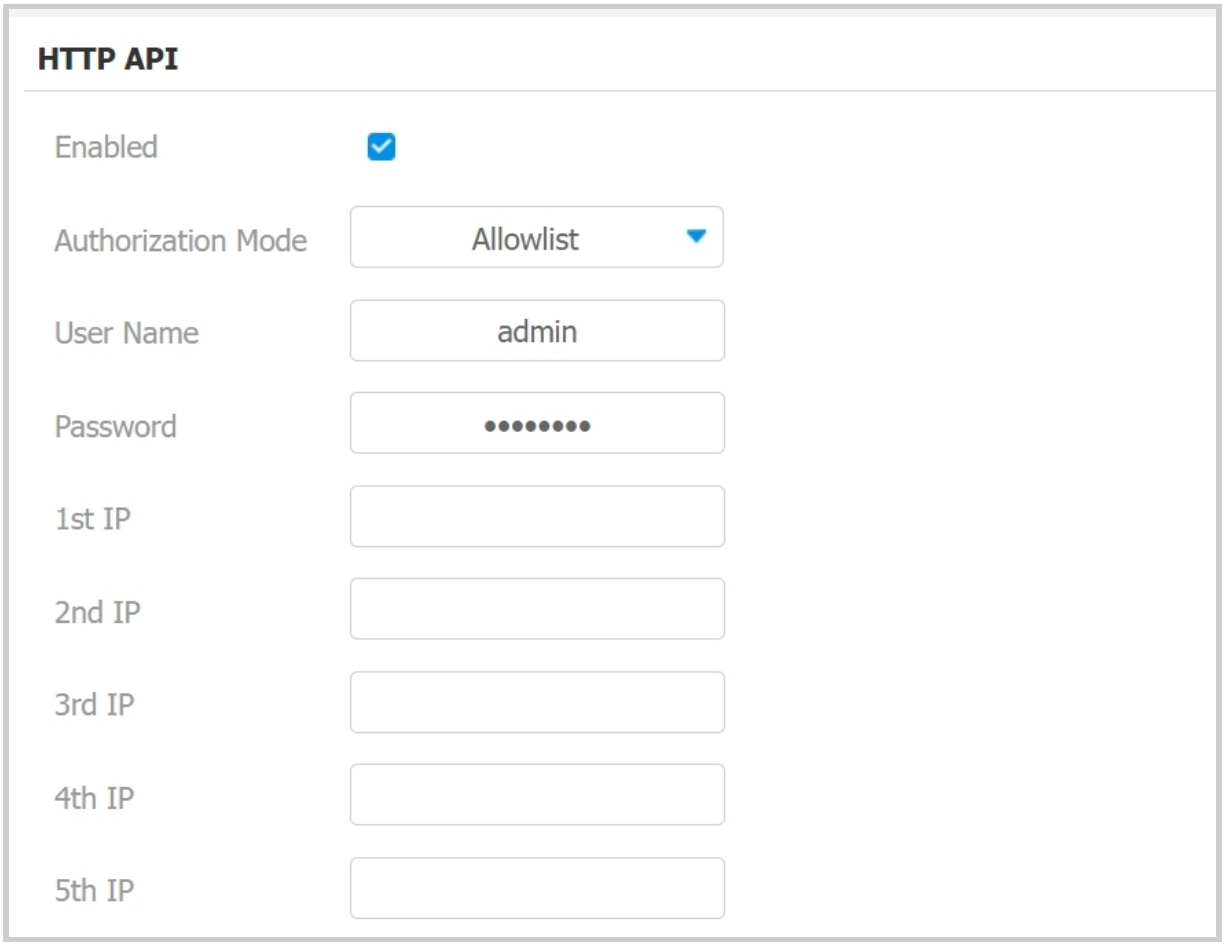
- When disabled, a relay will open only if it is allowed both in the **Wiegand Open Relay** and in the user's relay permissions.

> **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.



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

Please refer to the following description for the authentication mode:

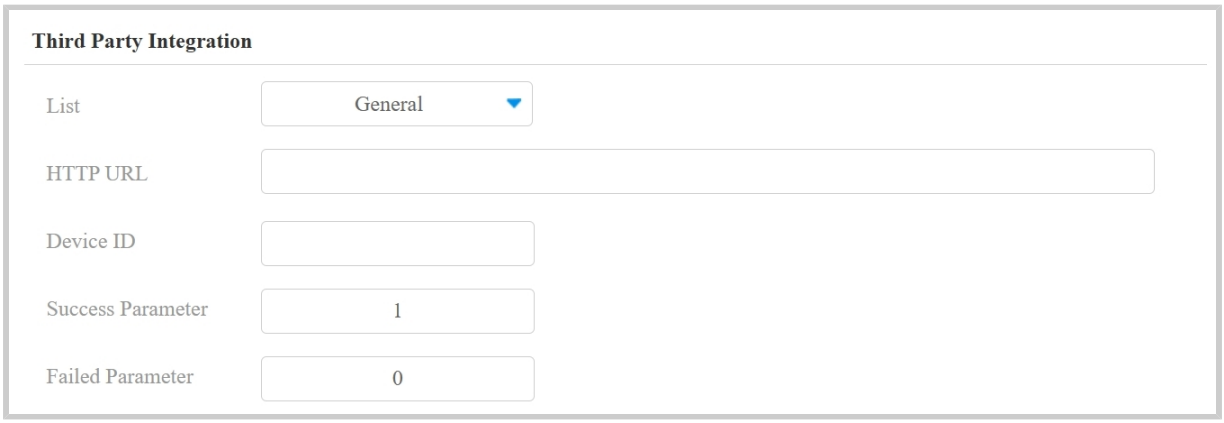
NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API, as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication.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

NO.	Authorization Mode	Description
4	Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode of username and password.
5	Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

Integration with Third-party Access Control Server

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

Set it up on the **Access Control > Relay > Third-party Integration** interface.



- **List**:
  - **None**: Disable the feature.
  - **General**: Transmit the QR code-linked HTTP URL in Akuvox's method.
    - **HTTP URL**: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before it is sent to the QR code server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode} &deviceId={DeviceID}.*
    - **Device ID**: The device ID is provided by the third-party server. It will be added to the HTTP command automatically when using a QR code for door access.
    - **Success Parameter**: Receiving this value indicates that opening the door succeeds.
    - **Failed Parameter**: Receiving this value indicates that opening the door fails.
  - **Customize**: Transmit access credential data in a customized method. When **Face** is selected, the device performs local face recognition first. If no matching face is detected, authentication fails. If a match is found, the associated **User ID** or **PIN** is submitted to the third-party server for further verification.
    - **Prompt on LCD**: Select **Default** to adopt the Akuvox door phone's door-opening prompt; Select **Return Value** to use the return value from the third-party server as the prompt.

- **Remote Verification**: Specify which access credentials will be verified by the third-party server.
  Available options depend on the configured Authentication Mode. When **Multi-Factor Authentication Mode** is enabled,

Option	Description
QR Code	The device scans the QR code and sends it directly to the third-party server. No local verification is performed.
Multi-Factor	The device first checks whether the authentication method matches the configured method. If not matched → User is prompted to use the correct method. If matched → The collected credentials are sent to the server for verification (no local verification).

- **HTTP URL**: Enter the HTTP command format provided by the third-party service provider. After a QR code scan, card swipe, face recognition, or PIN entry, the device automatically replaces variables in the URL and sends the request to the server.
  Example format:
  http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode}/{Card}/{UserID}/{Pin}/{Face}&deviceId={DeviceID}.
  If a user swipes a card, the URL will be http://192.168.35.123:8090/api/visitor/scan?codeKey={QRCode}/123456/{UserID}/{Pin}/{Face}&deviceId=1.
- **Multi-Factor HTTP URL Format**: In **Multi-Factor Authentication** mode, the example format is: *http://{Server IP}:8090/api/visitor/scan?codeKey={Token}/{Type}&deviceId={DeviceID}.*

Variable	Description
{Token}	Credential collected in the current authentication step.
{Type}	Two-factor authentication type: 1 = RF Card + PIN 3 = Face + RF Card 4 = Face + PIN

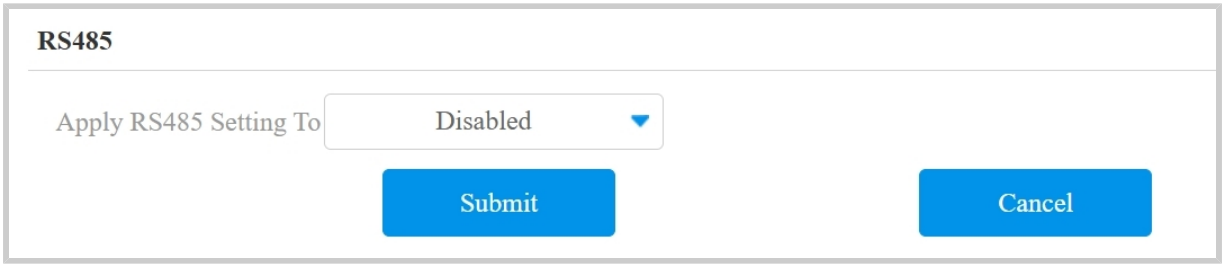
- **Device ID**: The device ID is provided by the third-party server. It will be added to the HTTP command automatically.
- **Success Parameter**: Receiving this value indicates that opening the door succeeds.
- **Failed Parameter**: Receiving this value indicates that opening the door fails.

Integration via RS485

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

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

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



- **Disabled**: The RS485 function is disabled.
- **Others**: 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.

RS485 Virtual Door Mode

This feature determines which relay to open when a credential is read from an OSDP(RS485) device.



- **Enabled**: It is enabled by default.
  - When enabled, the door phone gives priority to the relay(s) configured in **OSDP Open Relay**.
    When a user presents their credentials, the door phone will open the relay(s) defined in the **OSDP 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 **OSDP Open Relay** and in the user's relay permissions.

Power Output Control

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

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



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

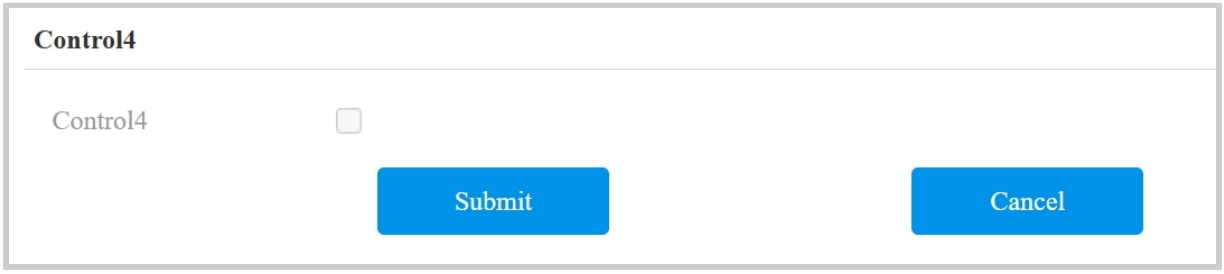
- **Time Out (Sec)**: Select the power supply time duration after the relay is triggered from 3, 5, and 10. It is 3 seconds by default.

Integration with Control4

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

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

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



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

Lift Control

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

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

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

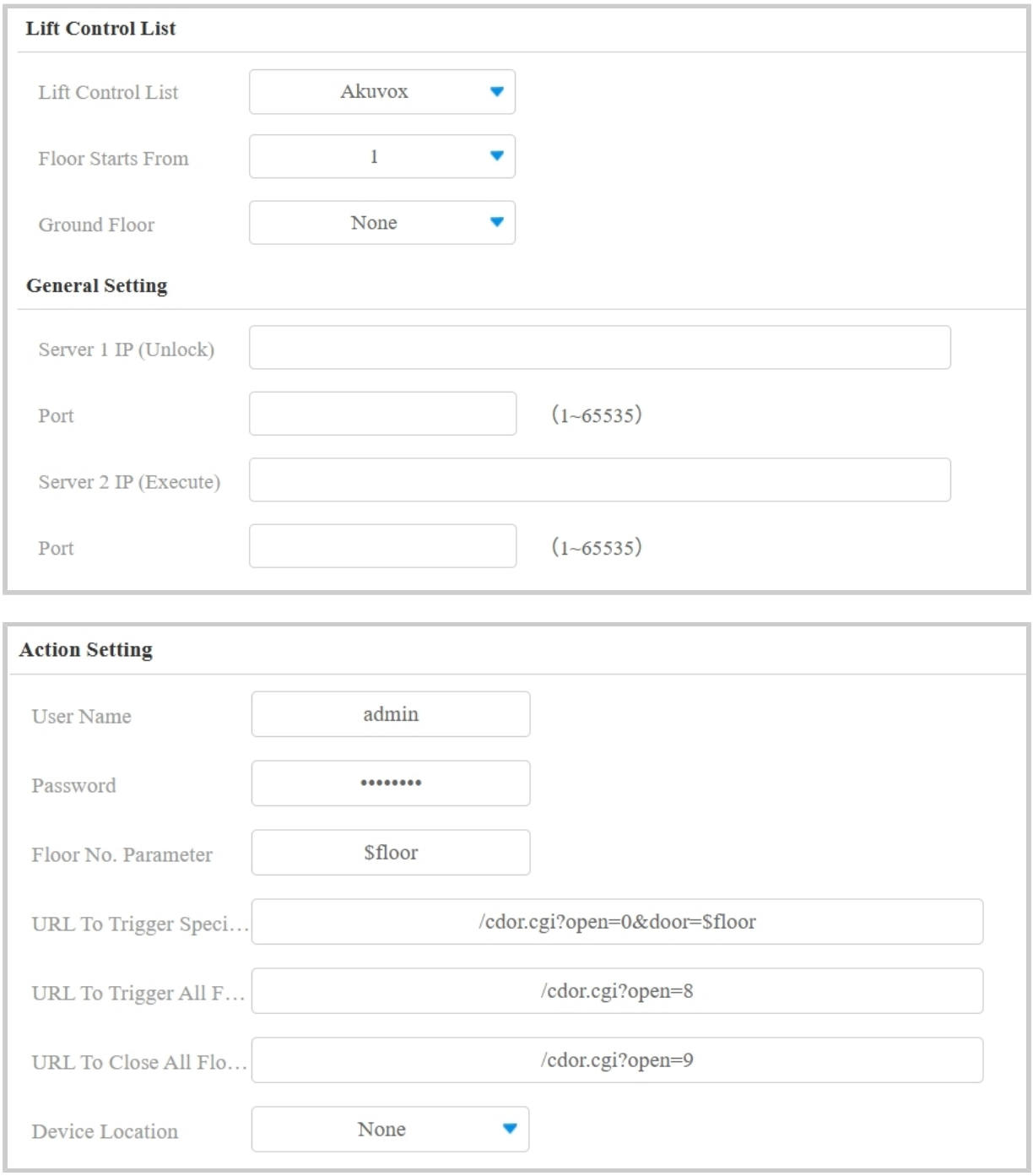


- **Lift Control List:** Select the lift controller brand.
  - None: The integration will be disabled.
  - OSDP: Integrate with OSDP lift controller.
  - Dahua: Integrate with Dahua lift controller.
  - KeyKing: Integrate with KeyKing lift controller.
  - Akuvox: Connect the device with the Akuvox EC33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

> **Note**
>
> When connecting the door phone to the lift controller via the RS485 ports, you need to select the right RS485 mode on the **Device > RS485** interface.

Akuvox Lift Controller

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

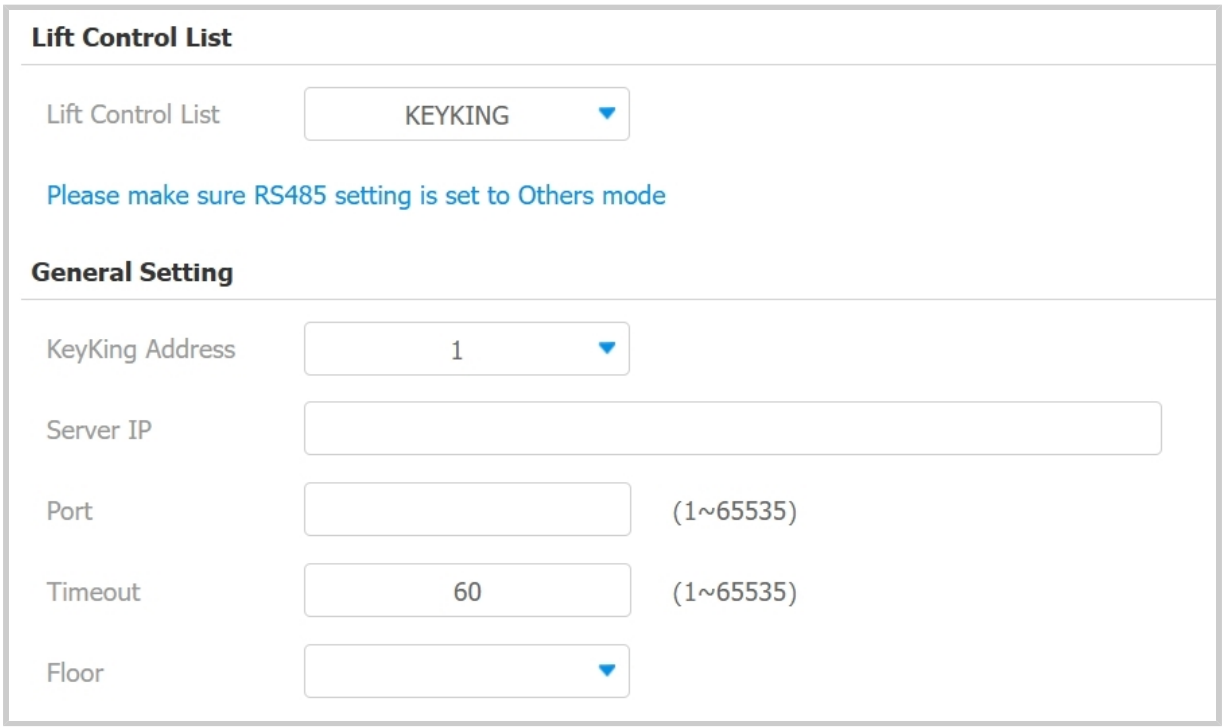


- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **Ground Floor**: If there are ground floors between the -1 and 1 floors, configure this option.

- **Server 1 IP(Unlock)**: The IP address of the lift controller that unlocks the elevator button(s). It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute)**: The IP address of the lift controller that sends the lift control commands.
- **Port**: The server port of the lift controller server.
- **User Name**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **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).
- **Device Location**: Select the floor where the device is installed.

KeyKing Lift Controller

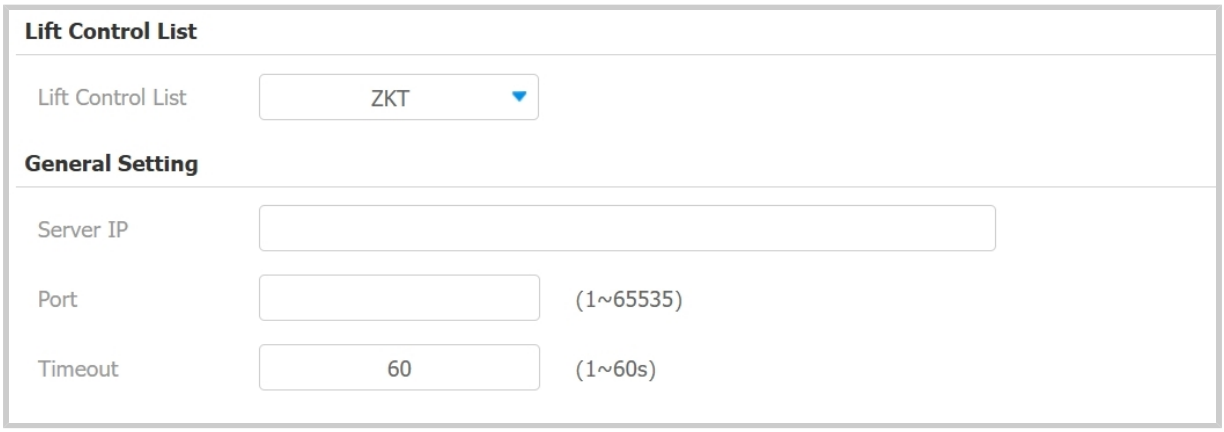
After selecting KeyKing, you need to set the KeyKing address.



- **KeyKing Address**: When the door phone works with the lift controller via RS485, select the number from 0 to 126. The binary number converted from the address number corresponds to the dip switch on the lift board. For example, if you select 5, set the dip switch to 101000.
- **Server IP**: When the door phone works with the lift controller via TCP/IP, enter the correct IP address.
- **Port**: Enter the port.
- **Timeout**: The default is 60.
- **Floor**: The lift will first go to the floor selected to pick up the user. Then, it will take the user to the designated floor based on their card or password.

ZKT Lift Controller

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



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

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.

Lift Control List

Lift Control List	KONE	
Floor Starts From	1	
Ground Floor	None	
Kone Control Mode	Traditional DCS	
Central machine	☐	
Time Out	5000	(5000~15000)

General Setting

KONE Central IP		
KONE Central Port	443	(1~65535)

Action Setting

User Name	admin	
Password	••••••••	
URL To Trigger DOP	/api/konelift/trig?DeciceType=DOP&DopID=$dop1_id&DopFloorID=$dop1_floc	

Kone Lift Dop

DOP ID		(0~1000)
DOP Floor ID		(0~255)
DOP ID2		(0~1000)
DOP Floor ID2		(0~255)

- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **Ground Floor**: If there are ground floors between the -1 and 1 floors, configure this option.
- **KONE Control Mode**: Select the option based on the lift control scenario.
  - **Traditional DCS**: The destination operating panels are on all floors, and there are no buttons on the car operating panel.
  - **Conventional**: Passengers select their destination floors on the control panel inside the lift car.
  - **Hybrid DCS**: The destination operating panels are located only on the main floors, while other floors have conventional landing signalization. Cars have a conventional operating panel.
  - **Turnstile Integration**: Passengers use their credentials at the entrance and call the lift.
- **Central Machine**:
  When the door phone is used as the central machine, configure the following options.
  - **KONE Group Control IP/IP2**: The KONE control panel's IP address. You can enter three IPs for each group, separated by ",".
  - **Kone Group Control Port**: The KONE control panel's port number.

  When the door phone is NOT used as the central machine, configure the following options.
  - **KONE Central IP**: The IP address of another door phone that is used as the central machine.
  - **KONE Central Port**: The port number of another door phone that is used as the central machine.
  - **Username**: The username of the HTTP API authentication set in the central machine.

  - **Password**: The password of the HTTP API authentication set in the central machine.
- **Time Out**: Available for Traditional DCS, Conventional, and Hybrid DCS. It is 5000ms by default; define the time for users to press the lift button.

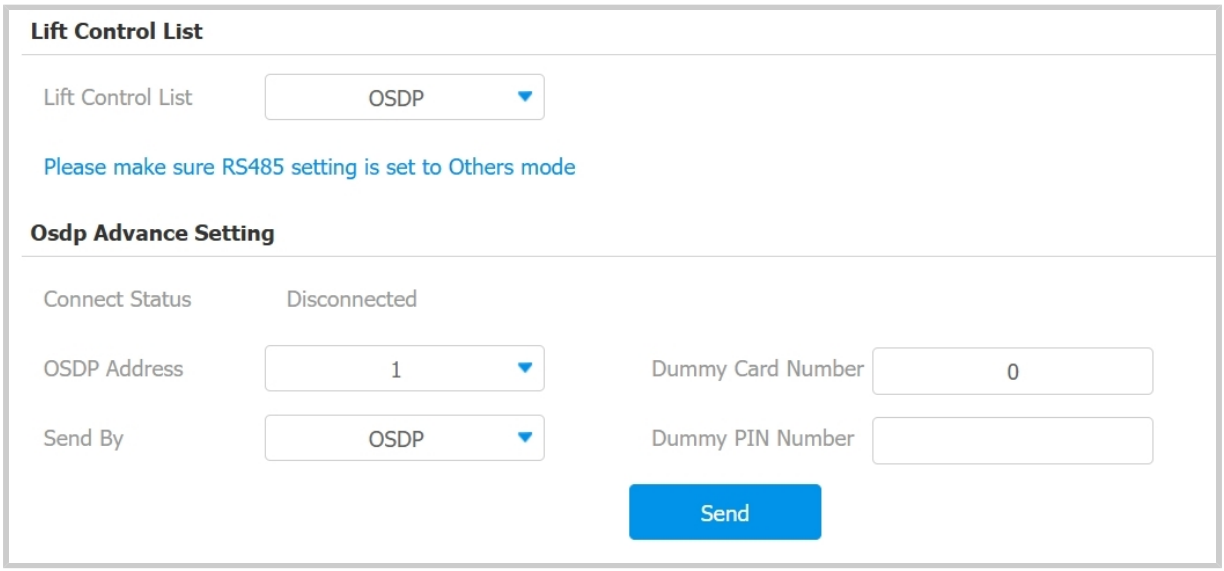
After choosing the KONE Control Mode, you need to fill in specific options. Please confirm them with the KONE service provider.

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

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

OSDP Setting

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

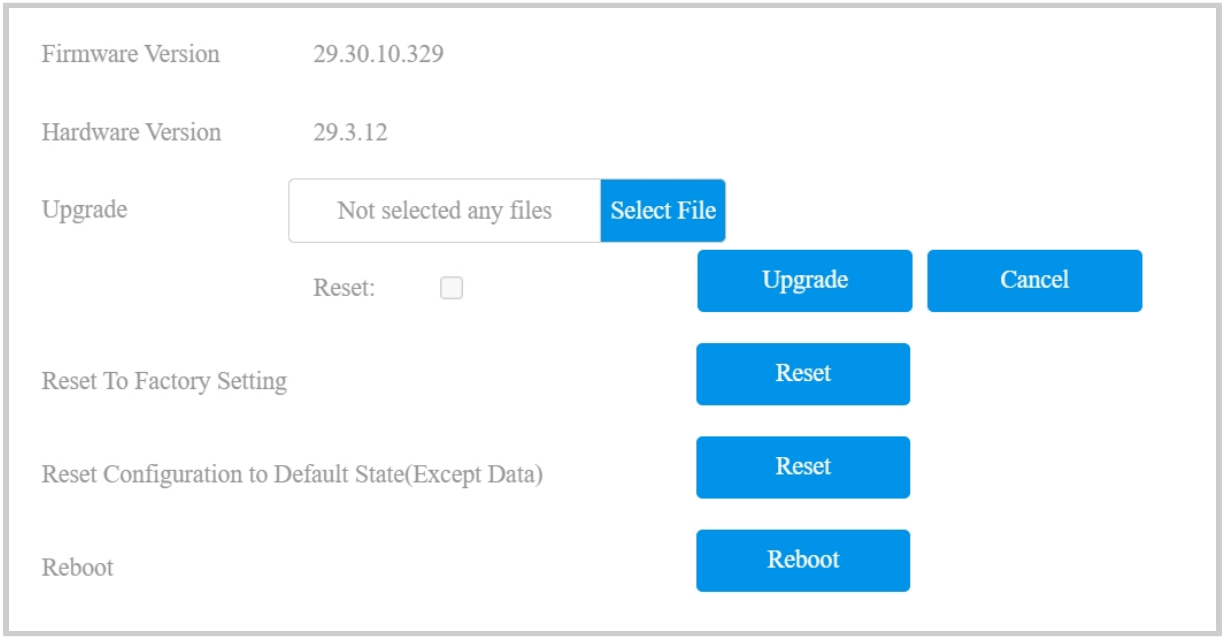


- **Connect Status**: Indicate OSDP-based communication status.
- **OSDP Address**: Obtain the specific OSDP address from the service provider.
- **Dummy Card Number**: Enter the card number to obtain authentication by third-party devices such as opening the lift door, closing the door, or other forms of door access, etc.
- **Dummy PIN Number**: Enter the PIN code to obtain authentication from third-party devices such as opening the lift door, closing the door, and so on.
- **Send by**: Select in what way you want to send out the card number among three options: OSDP, Wiegand, and None. If you select OSDP then the card number will be sent out to the third-party devices via RS485. If you select Wiegand then the card number will be sent out via Wiegand. If you select None then the card number will not be sent out but retained in the system.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Note

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

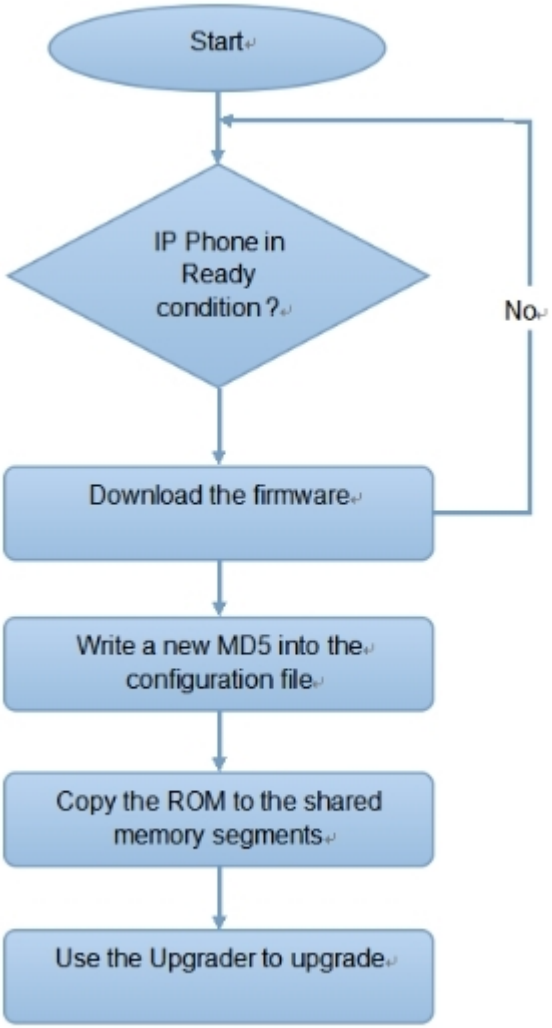
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

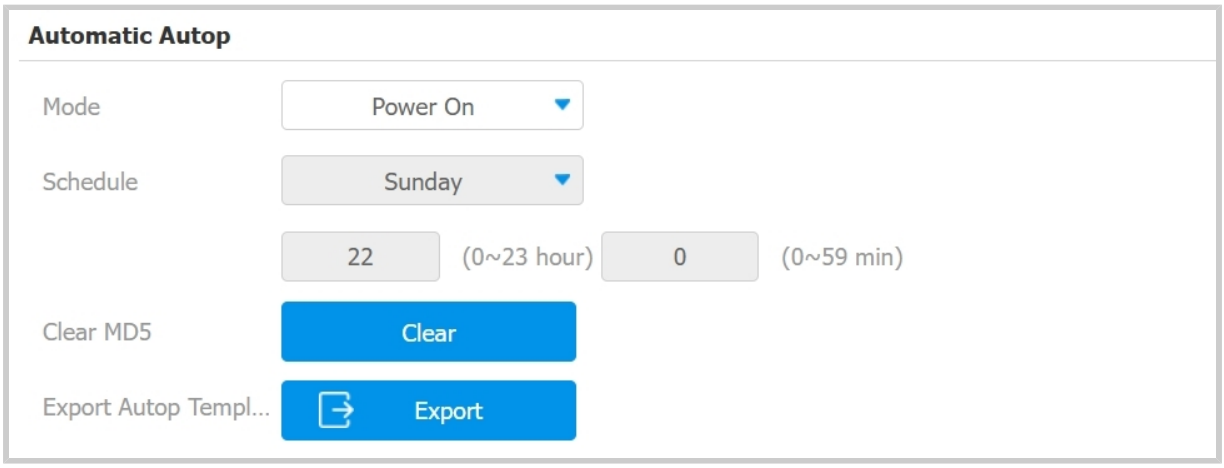
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

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

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

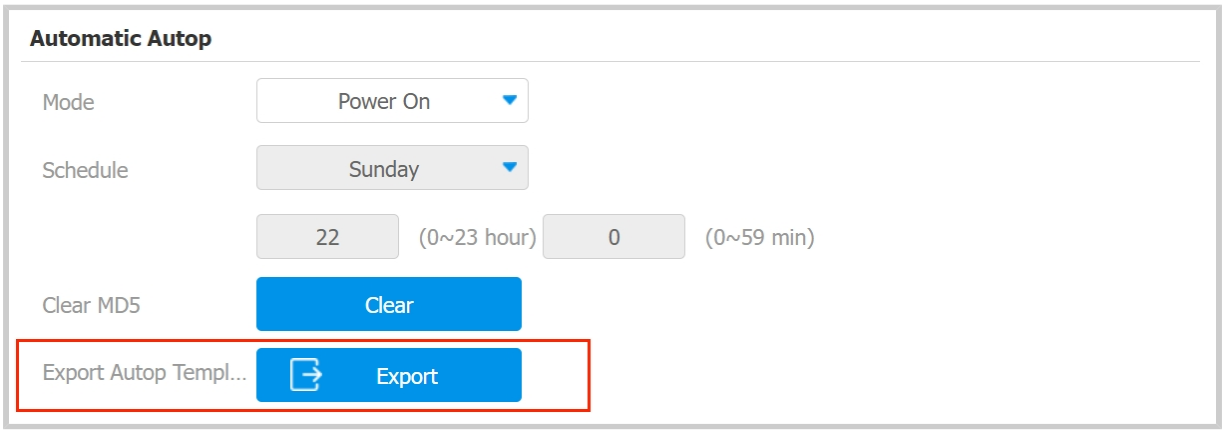


- **Mode**:
  - **Power On**: Allow the device to perform Autop every time it boots up.
  - **Repeatedly**: Allow the device to perform Autop according to the schedule.
  - **Power On + Repeatedly**: Combine Power On and Repeatedly modes, allowing the device to perform Autop every time it boots up or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

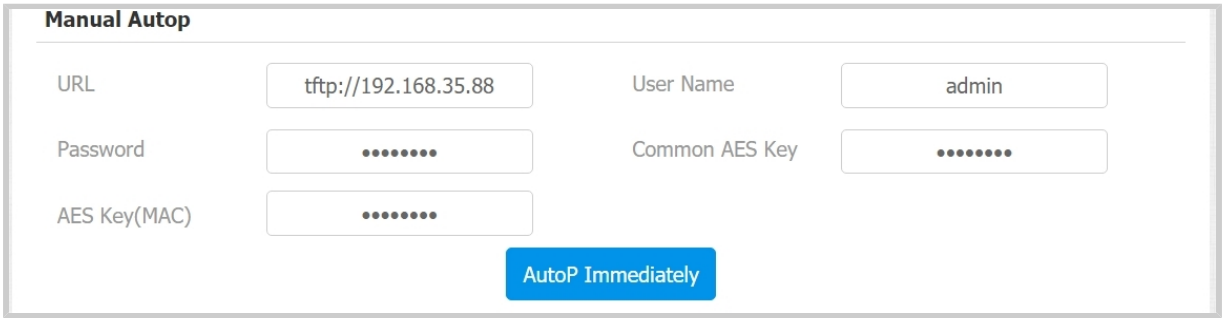
Static Provisioning

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

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



Then, set up 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 needs a username to be accessed.
- **Password**: Set up a password if the server needs a password to be accessed.
- **Common AES Key**: Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key(MAC)**: Set up the AES code for the intercom to decipher the MAC-based auto-provisioning configuration file.

Note

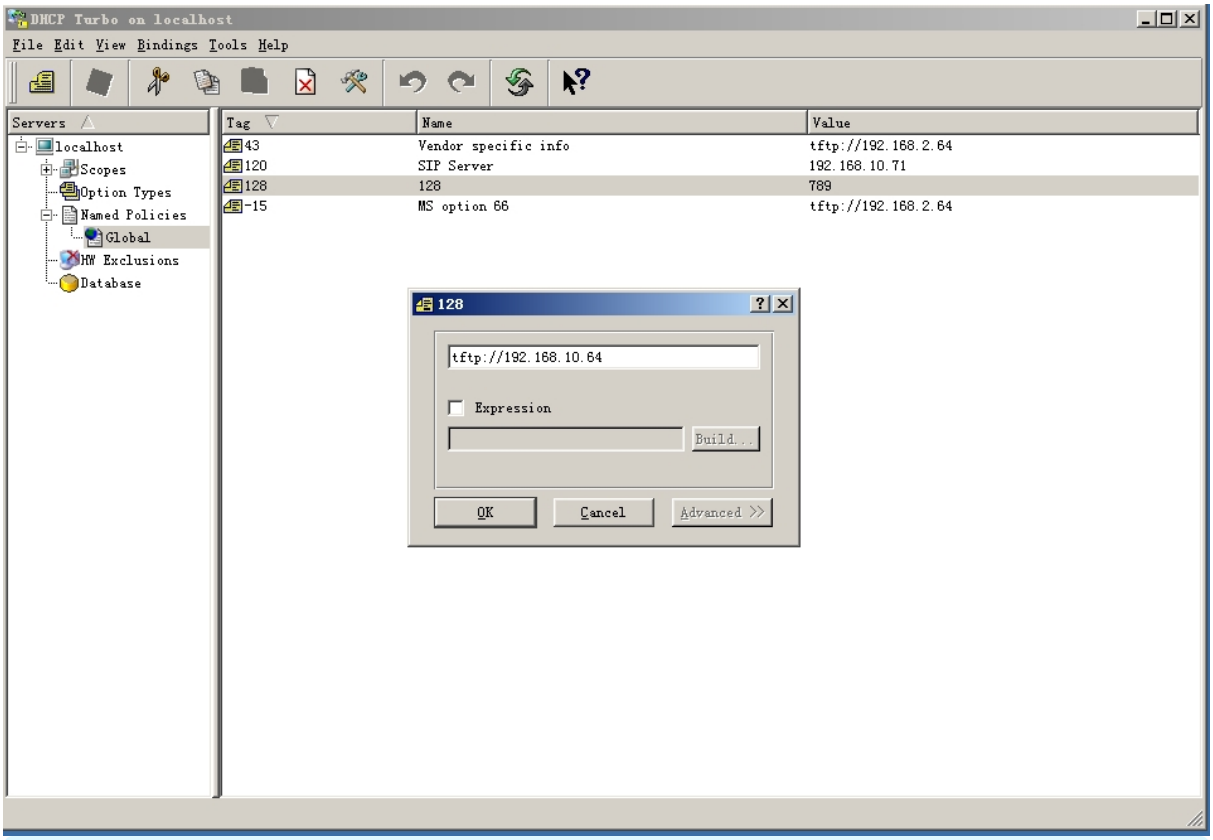
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning

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

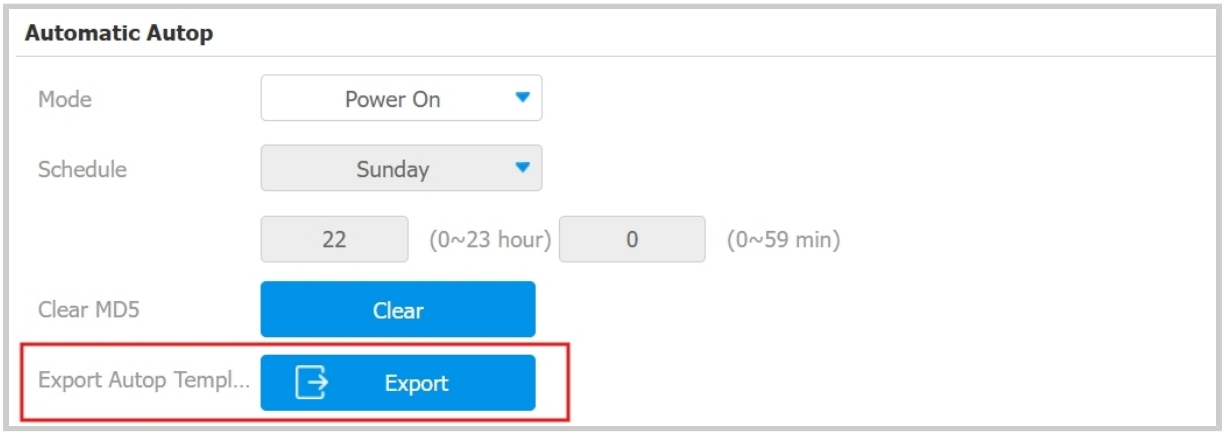


Note

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

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

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



Set it up on the **DHCP Option** section.



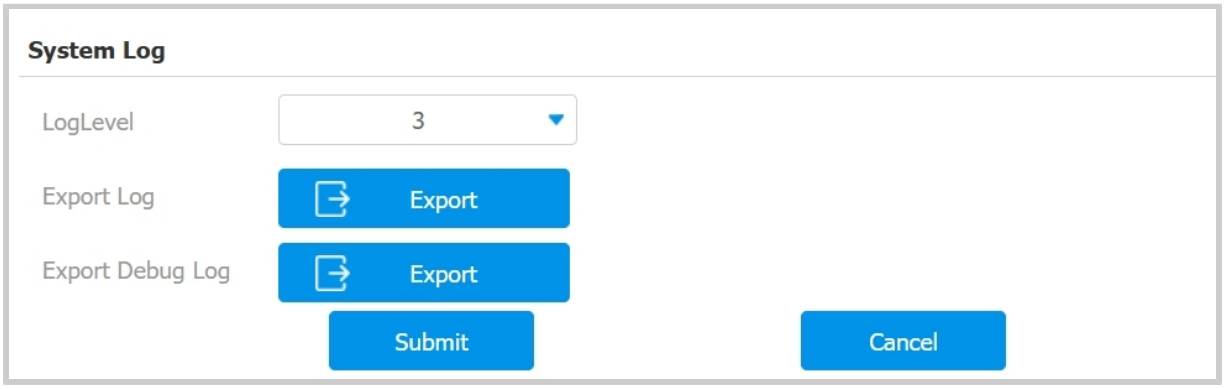
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL.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

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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

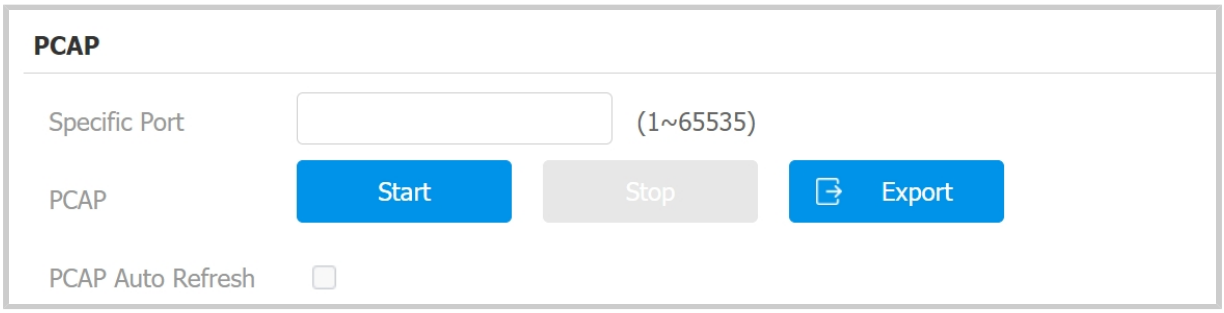


- **Log Level**: Select log levels from 1 to 7. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the Export tab to export the temporary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



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

Remote Debug Server

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

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



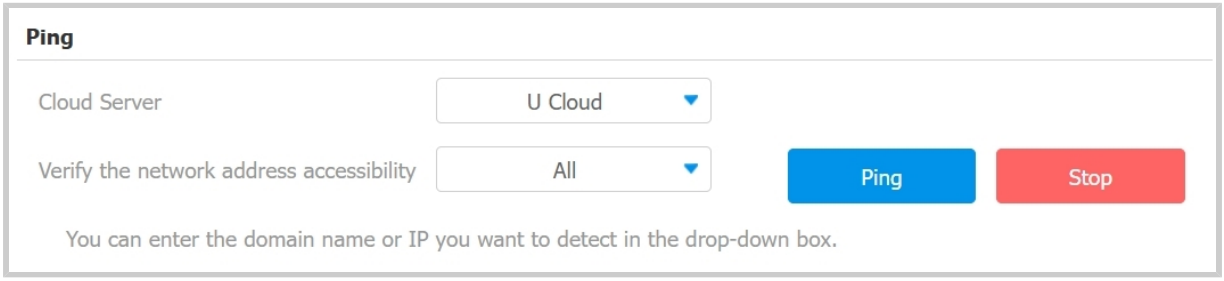
- **Connect Status**: Display the connection status between the device and the server.

- **IP**: Enter the IP address of the server.

Ping

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

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

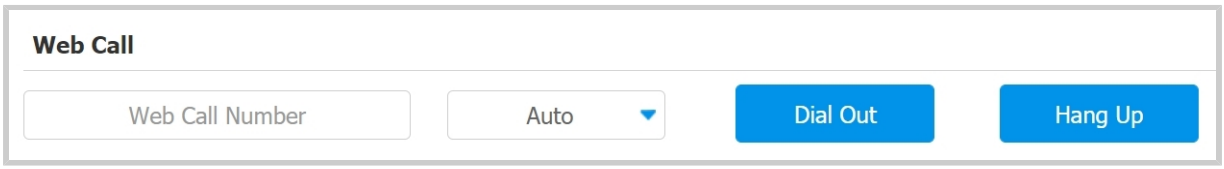


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Web Call

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

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



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.

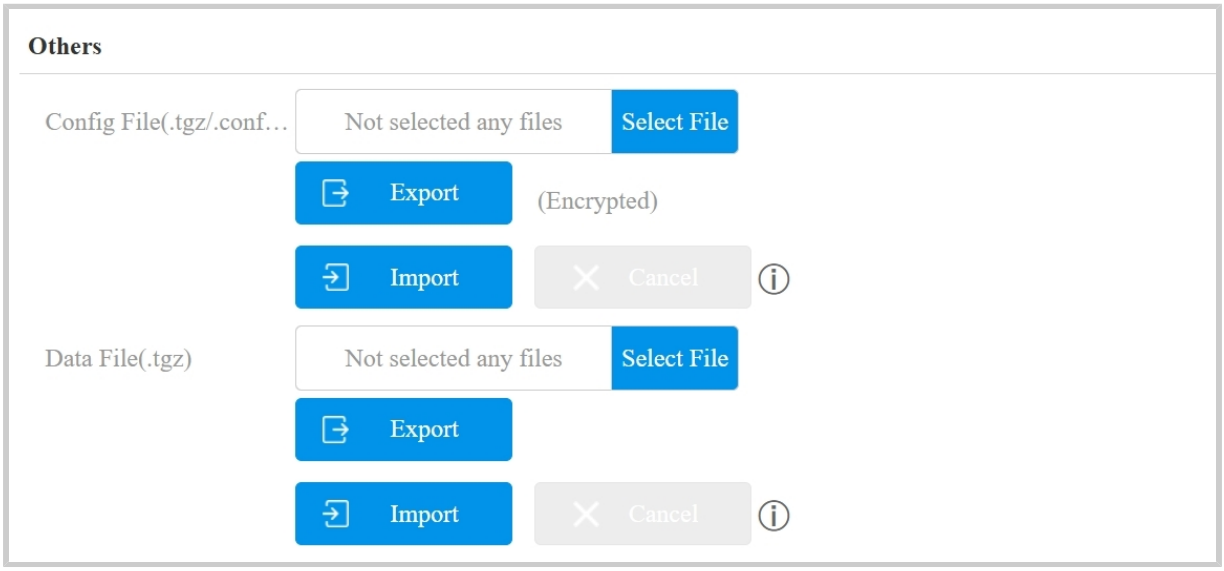


- **Domain Name**: Enter the domain name or IP address.
- **Port**: Enter the port number.
- **Start**: Click to start detection after entering the domain name and port.
- **Result**: Display the detection result.
- **Details**: Display analysis of the result.

Backup

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

Set it up on the **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, .conf
- **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

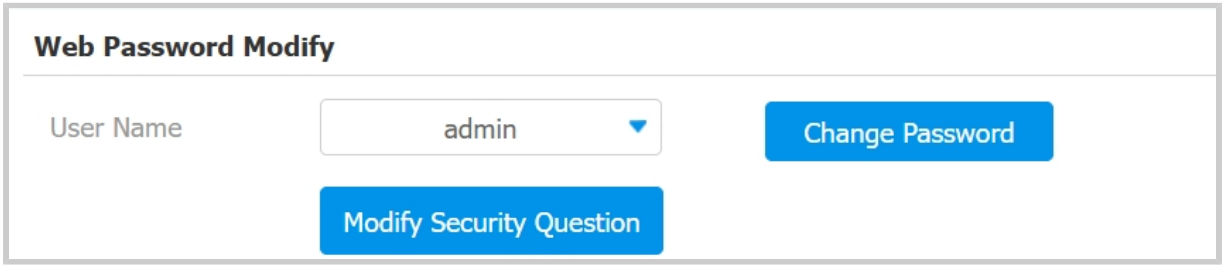
Password Modification

Modify Web Password

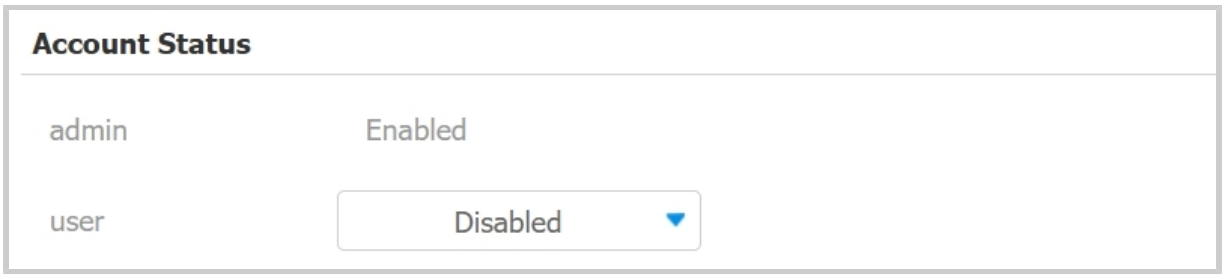
The web password is used to access the device's web settings.

To modify it, go to the **System > Security** interface.

Select Admin to change the password for the administrator account and User for the user account.



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

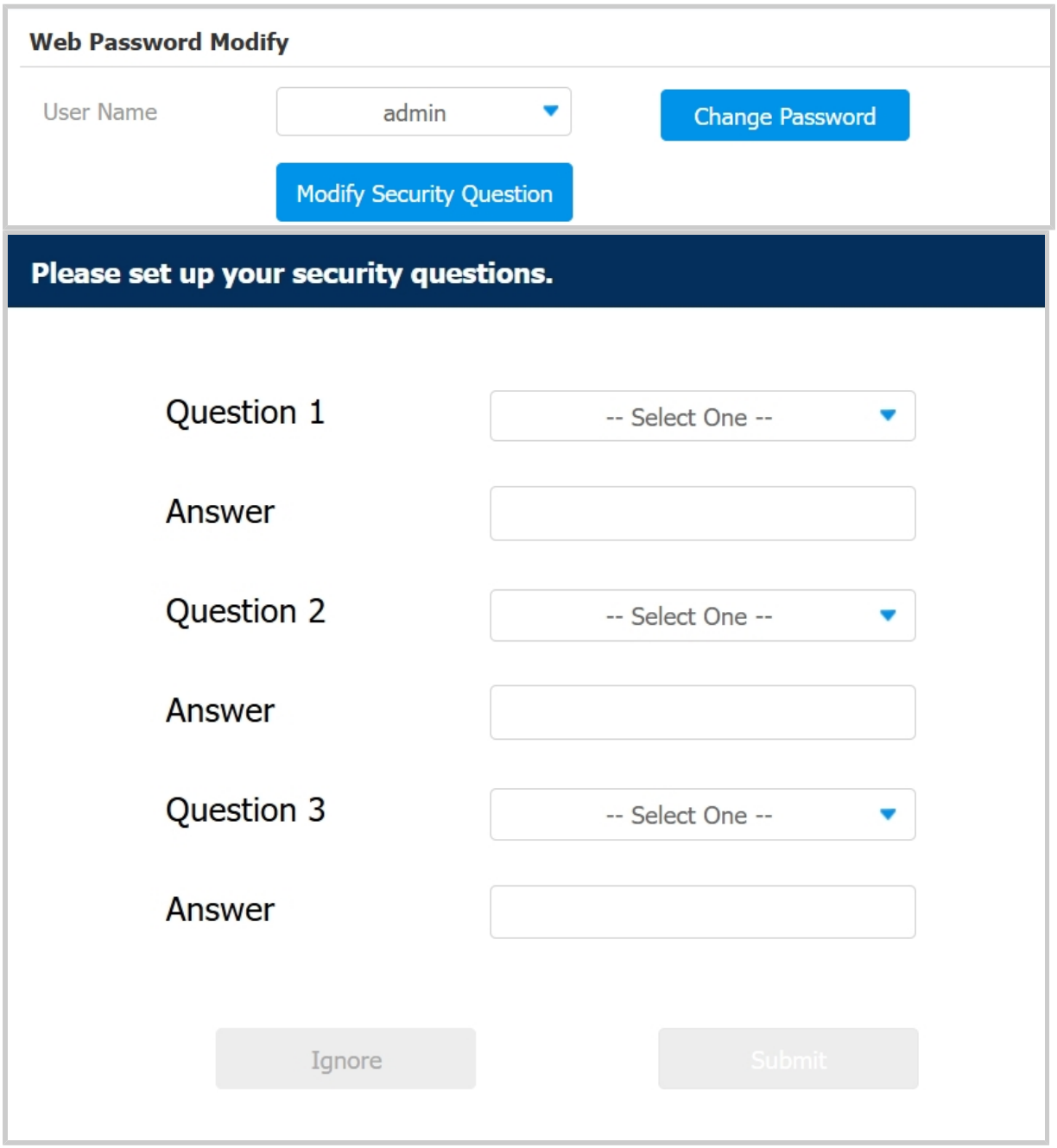


Modify Security Questions

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**.



Modify Device Setting Password

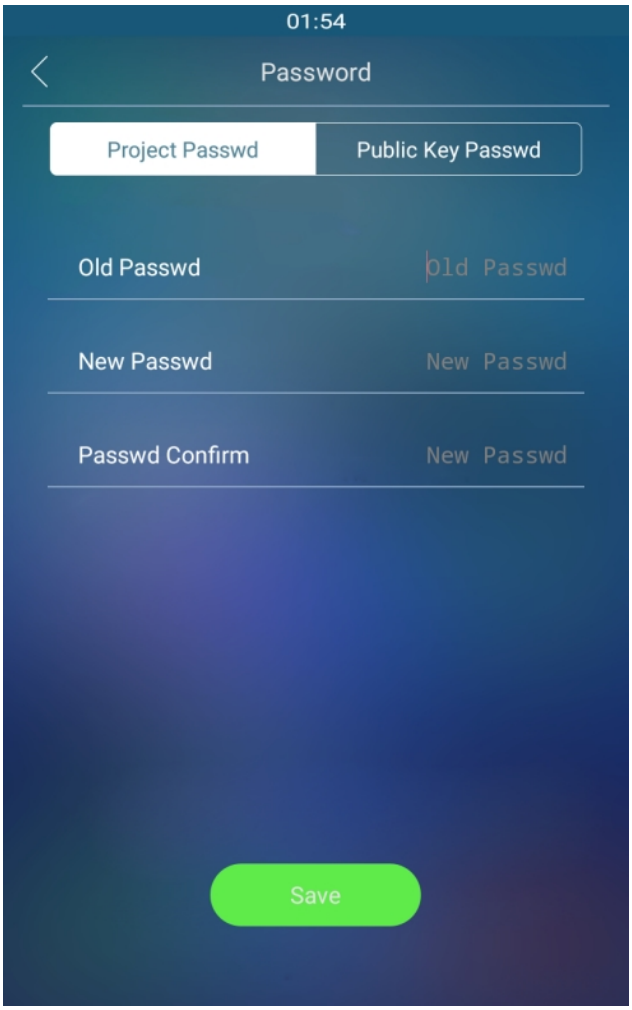
You can enter the Step1 PIN and then the Step2 PIN on the device's Dial screen to access the system settings.

Change them on the **Intercom > Basic > 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.

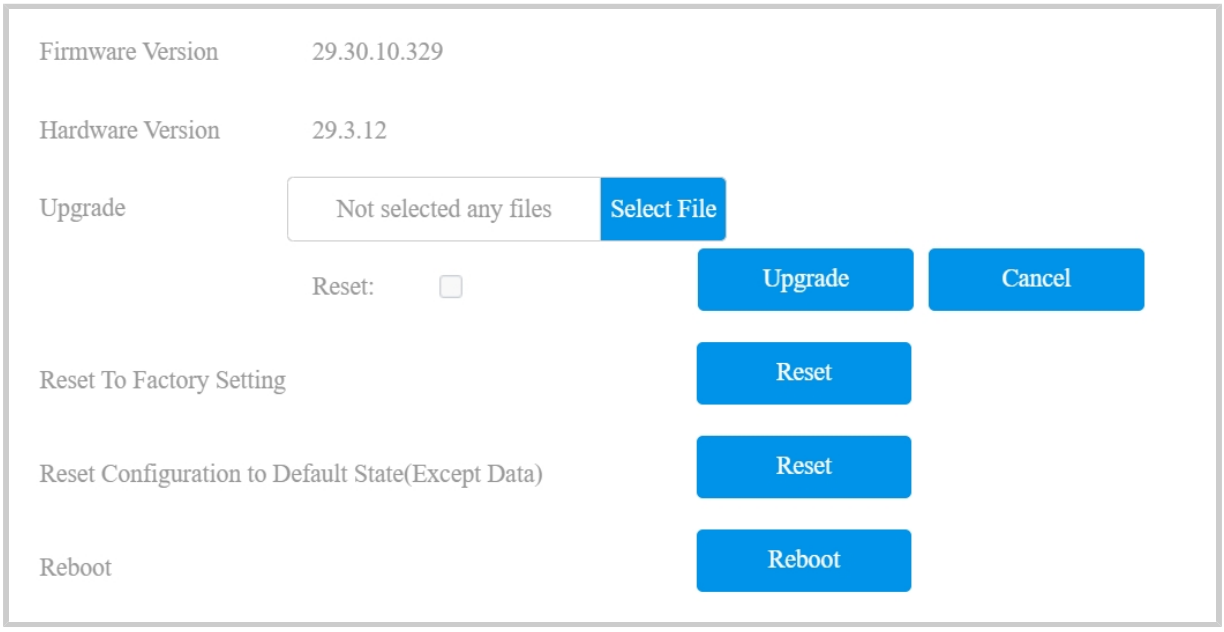
You can also change the password on the **Setting > Password** screen.



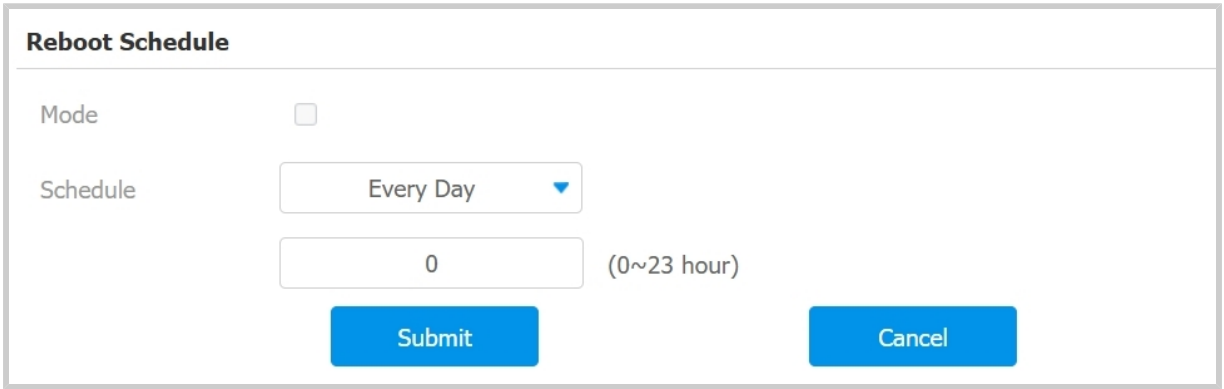
System Reboot&Reset

Reboot

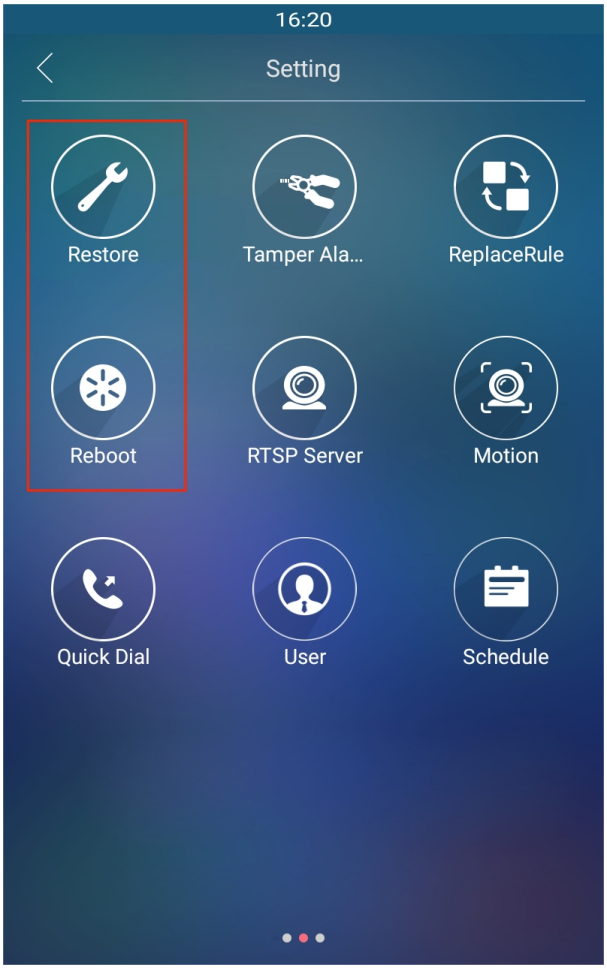
Reboot the device on the **System > Upgrade** interface.



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



You can also reboot the device on the **Setting** screen.

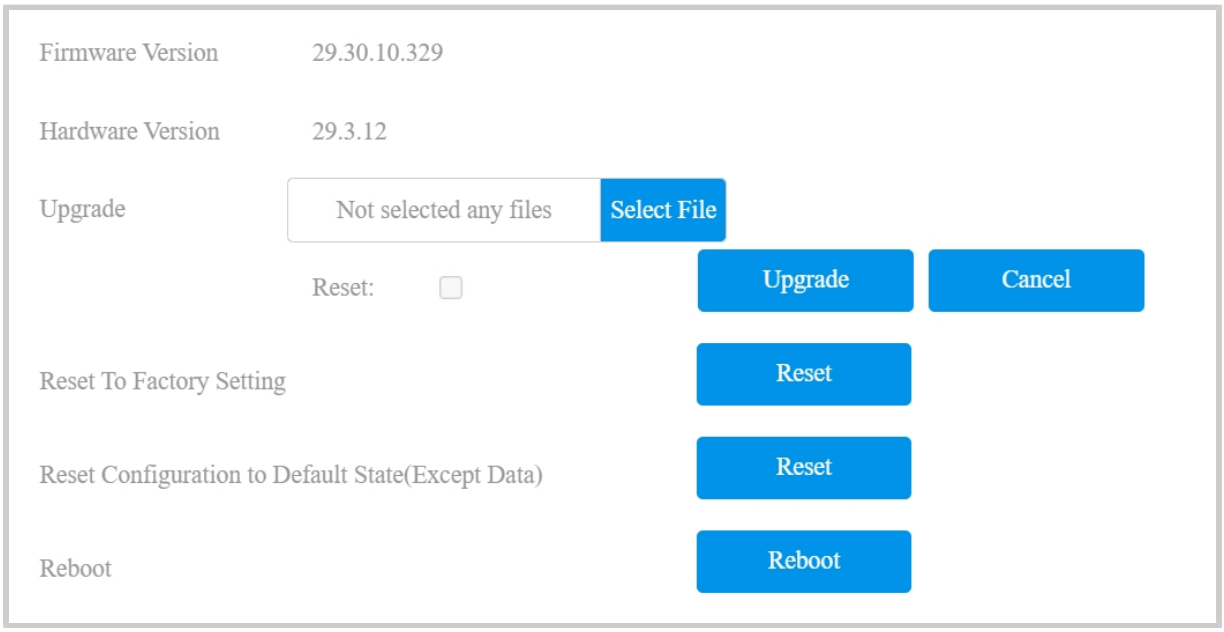


Reset

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** screen.

