Akuvox

Table of contents

Akuvox X912 Series Door Phone Administrator Guide_V2

About This Manual 10

Product Overview 13

Changelog 14

Model Differences and Specification 15

Supported Card Types 16

Access the Device 18

Access the Device Settings 18

Access the Web Settings 19

Introduction to Configuration Menu 20

Language and Time 22

Language 22

Time 22

Volume and Tone 25

Volume Configuration 25

On the Web 25

On the Device 26

Upload Tones 26
Ringback Tone Setting 28
Visitor-Friendly Mode 29
Open Door Tone Mode 29
LCD Setting 31
On the Web 31
On the Device 32
Keypad Light Setting 34
Screen Display 35
Theme Settings 35
Default (Buttons) Theme 36
Speed Dial Theme 38
Customized Text Theme 38
Gate Mode 39
Relay Key Settings 40
Dial Screen Prompt Display 41
Screensaver Configuration 41
Upload Screensaver 42
Upload Background Picture 43
Open Door Text Prompt Display 44

Door Status Display 44
Screen Displayed when Pressing Keypad 45
Network Setting 47
Device Network Configuration 47
Device Local RTP Configuration 50
Device Deployment in Network 50
Device Web HTTP Setting 52
NAT Setting 52
Intercom Call Configuration 54
IP Call & IP Call Configuration 54
Make IP Calls 54
IP Call Configuration 54
SIP Call & SIP Call Configuration 55
SIP Account Registration 55
SIP Server Configuration 57
SIP Account Selection 57
Outbound Proxy Server 58
Data Transmission Type 59
SIP Hacking Protection 59
Call Settings 61

Quick Dial by Number Replacement 61
Call Auto-answer 62
Manager Dial 63
Group Call 63
Sequence Call 64
Maximum Call Duration 66
Maximum Dial Duration 66
Two-Way Video Call 67
Hang Up After Open Door 68
Video Transport Type 68
Audio & Video Codec Configuration 70
Audio Codec 70
Video Codec 71
Video Codec for Direct IP Calls 71
Contacts Configuration 73
Manage Contact Groups 73
Set up Contact Details 74
Contact List Display 76
Relay Settings 79
Local Relay 79

Web Relay 80
Security Relay 82
Upgrade SR01 84
Door Access Schedule Management 86
Configure Door Access Schedule 86
Create Door Access Schedule 86
Import and Export Door Access Schedule 87
Relay Schedule 88
Holiday Schedule 90
Door-opening Configuration 92
Unlock by Public PIN 92
Virtual PIN 92
User-specific Access Methods 93
Unlock by Private PIN 94
Unlock by QR Code 95
Unlock by RF Card/Bkey 96
Unlock by License Plate 98
Unlock by Facial Recognition 98
Unlock by Bluetooth 101
Access Setting 103

Import/Export User Data 104
Mifare Card 105
Unlock by HTTP Command 107
Unlock by DTMF Code 108
DTMF White List 109
DTMF Data Transmission 109
Unlock by Exit Button 111
Configure Access Methods on the Device 112
Admin Card 112
Public PIN 114
Private PIN 116
RF Cards 118
Monitor and Image 121
MJPEG Image Capturing 121
RTSP Stream Monitoring 123
RTSP Stream Setting 124
RTSP Audio 125
ONVIF 125
Live Stream 126
NACK 127

Security 128
Tamper Alarm 128
Client Certificate Setting 128
Web Server Certificate 128
Client Certificate 129
Motion Detection 130
Security Notification 132
Email Notification 132
FTP Notification 133
SIP Call Notification 133
Action URL 133
Voice Encryption 137
User Agent 137
Real-Time Monitoring 137
Emergency Action 138
Web Interface Automatic Log-out 139
High Security Mode 139
Logs 141
Call Logs 141
Door Logs 141

Event Logs 142
Integration with Third-Party Device 144
Integration via Wiegand 144
Facility Code Setting 146
Integration via HTTP API 147
Power Output Control 149
Integration via RS485 149
Integration with Third-party Access Control Server 150
Lift Control 154
Lift Control 154
Firmware Upgrade 156
Auto-provisioning via Configuration File 157
Provisioning Principle 157
Configuration Files for Auto-provisioning 158
AutoP Schedule 159
Static Provisioning 160
PNP Configuration 162
Debug 164
System Log for Debugging 164
Remote Debug Server 164

PCAP for Debugging 165
Web Call 166
Ping 166
Network Probe 167
Backup 169
Password Modification 170
Modify Device Web Interface Password 170
Modify Security Questions 171
Modify System Password 172
Modify Service Password 174
System Reboot&Reset 176
Reboot 176
Reset 178

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX X912S DOOR PHONE

Administrator Guide

Akuvox

Thank you for choosing the Akuvox X912 series door phone. This manual is intended for administrators who need to properly configure the door phone. This manual is written based on the 912.30.12.216 version, and it provides all the configurations for the functions and features of the X912 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox X912 is a Linux IP video door phone with a 4-inch touch screen and physical keypad. It incorporates audio and video communications, access control, and video surveillance. Its finely tuned Linux OS, Cloud, and AI-based communication technology allow featured customization to better suit users' operation habits. X912 has multiple ports, such as RS485 and Wiegand ports, which can be used to easily integrate external digital systems, such as lift controller and fire alarm detector, helping to create a holistic control of the building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, Facial recognition NFC, Bluetooth, QR code. X912 series door phone is applicable to mid-end and upscale residential buildings, and upscale single-tenant residential buildings.

Changelog

What’s new in version 912.30.12.216:

- Support configuring the data length for reading the Mifare cards .

Click here to view the changelog of previous device versions.

Model Differences and Specification

Model	X912S	X912K
Front Panel	Stainless steel	Aluminum
Button	Numeric keypad	Physical numeric keypad
IK Rating	IK10	IK08
Touch Screen	✓	✓
Relay In	3	3
Relay Out	2	2
Alarm In	X	X
RS485	✓	✓
Card Reader	13.56MHz&125kHz,NFC	13.56MHz&125kHz,NFC
Wi-Fi	X	X
Bluetooth	✓	✓
Temperature Detection	X	X
Facial Recognition	✓	✓
LTE	X	X

Model	X912S	X912K
USB	X	X
External SD Card	X	X

Supported Card Types

The device firmware should be 912.30.11.15 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
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Classic ev1 7-byte
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
  - Mifare Classic 1K

- Mifare S50-1K Card
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

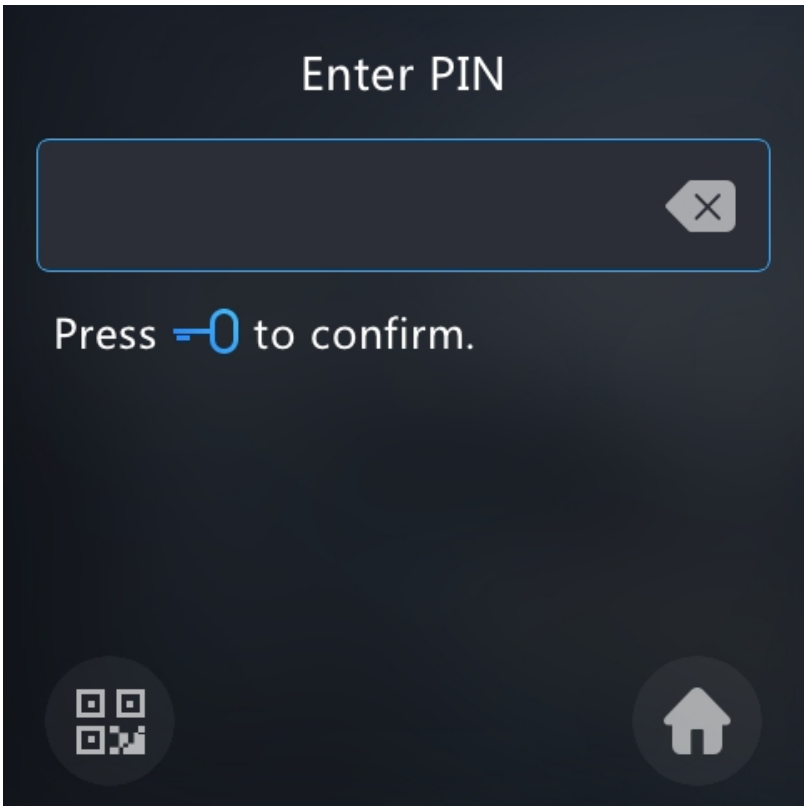
Access the Device

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

Access the Device Settings

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

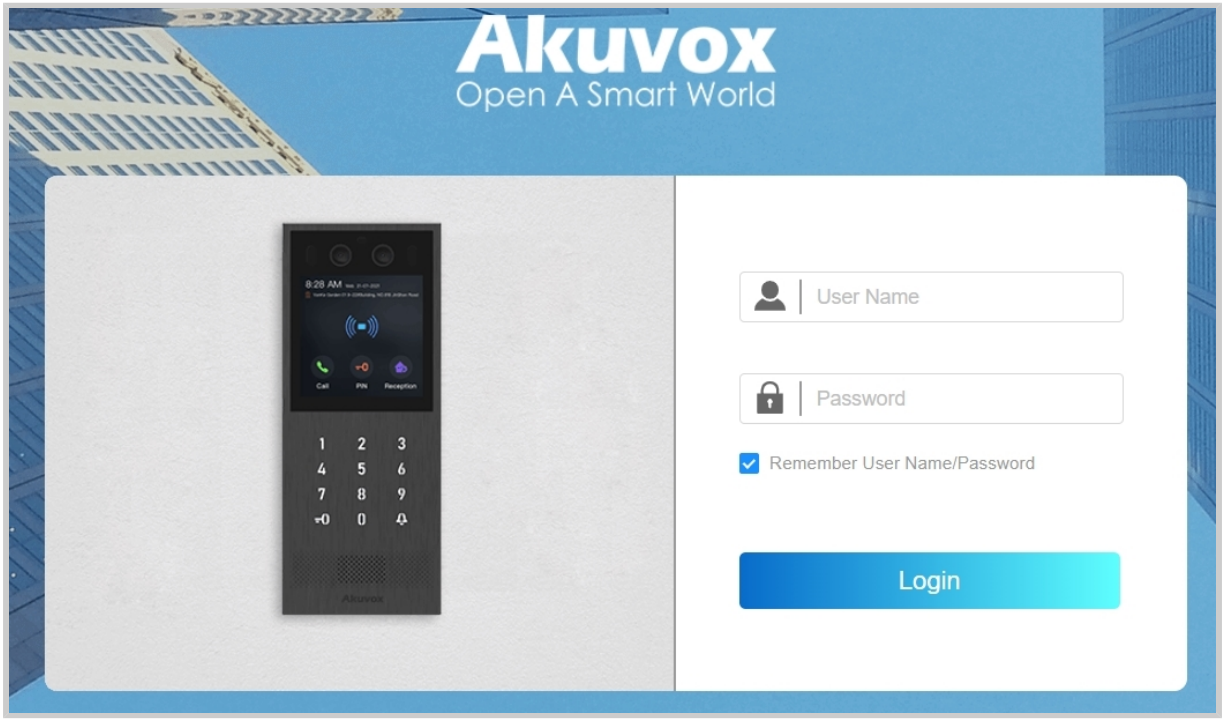
- To access the device system settings, press on the screen or the keypad, enter the default system PIN code **2396**, then press for the confirmation.
- To enter the access method settings screen, press . Enter the default PIN code **3888,** and press for confirmation.



Access the Web Settings

Use the Akuvox IP scanner tool to search for the device's IP address on the same LAN. Then use the IP address to log in to the web browser using the username and password **admin** and **admin**.

The IP address can also be checked on the device's **Admin Settings > System Information** screen.

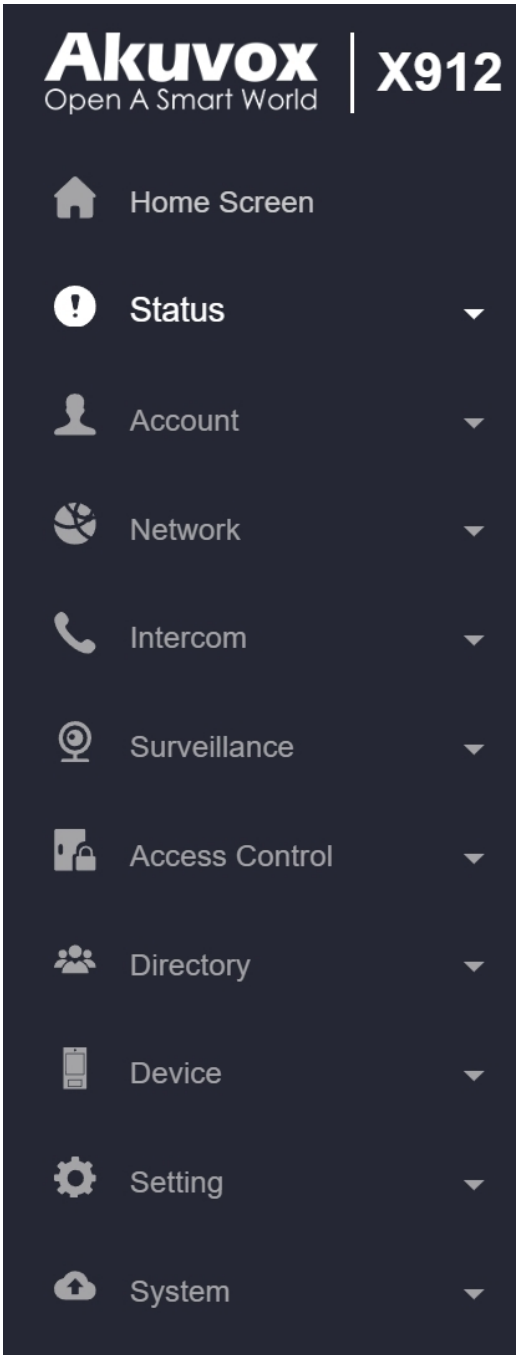


Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See 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.
- Please be case-sensitive to the user names and passwords entered.
- Your computer should be on the same network as the device.

Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, call log, door log, etc.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio and video codec, DTMF, etc.
- **Network**: This section mainly deals with DHCP and Static IP settings, RTP port settings, device deployment, etc.
- **Intercom**: This section covers intercom settings, call features, etc.
- **Surveillance**: This section covers motion detection, RTSP, MJPEG, ONVIF, live stream, etc.
- **Access Control**: This section covers access control methods setup, and input and relay control.
- **Directory**: This section involves user and contact management.
- **Device**: This section includes light, LCD, audio, lift control, and Wiegand settings.
- **Setting**: This section includes time, language, action settings, schedule for access control, screen display, and HTTP API.
- **System**: This section covers device upgrade and maintenance.


Akuvox
Open A Smart World
X912
Home Screen
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System

Language and Time

Language

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

To select the LCD language, navigate to **Setting > Time/Lang > LCD Language** interface.

The supported languages are:

- English, Simplified Chinese, Traditional Chinese, Russian, Korean, Spanish, Dutch, French, German, Hebrew, Polish, Turkish, Ukrainian, Swedish, Italian, and Brazilian Portuguese.



Switch the web language in the upper right corner.

The supported languages are:

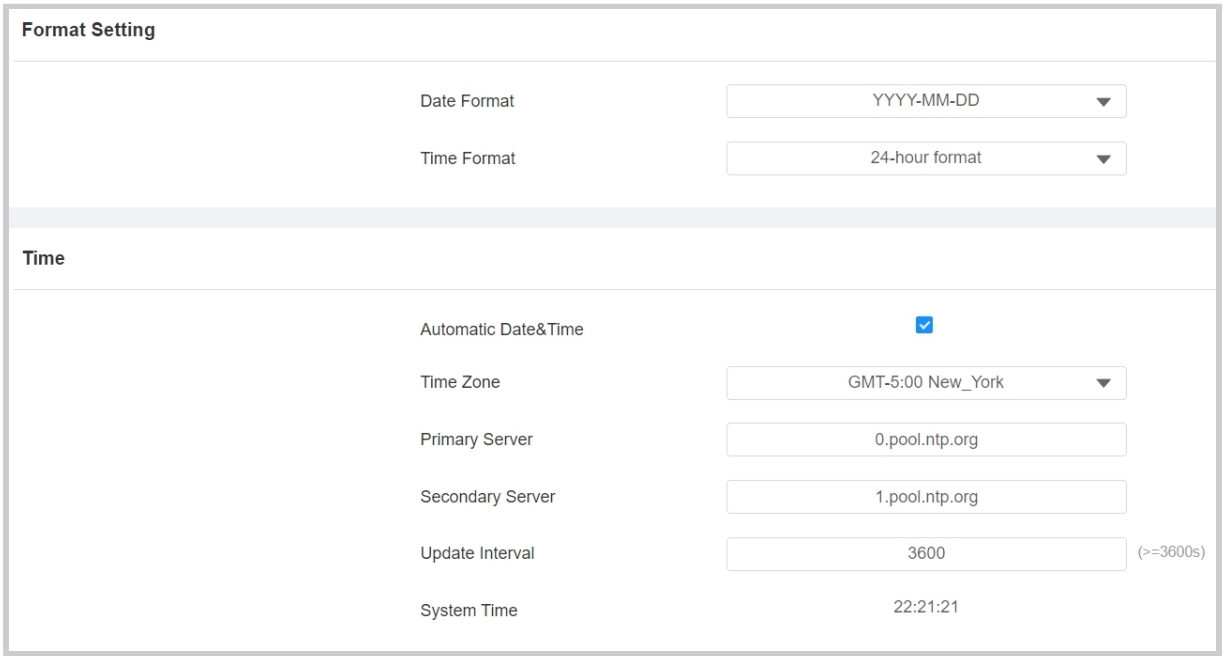
- English, Simplified Chinese, Traditional Chinese, Russian, Korean, Turkish, Spanish, Dutch, French, German, Polish, Swedish, Italian, Ukrainian, and Brazilian Portuguese.



Time

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

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



- **Date Format**: Select the date format from the provided options.
- **Time Format**: Select a 12-hour or 24-hour time format.
- **Automatic Date & Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Primary Server**: Enter the NTP server address.
- **Secondary Server**: Enter the backup server address. When the main NTP server fails, it will change to the backup server automatically.

- **Update Interval**: Set the time update interval. For example, if you set it to 3600, the device will send a request to the NTP server for the time update every 3600 seconds.
- **System Time**: Display the current device time.

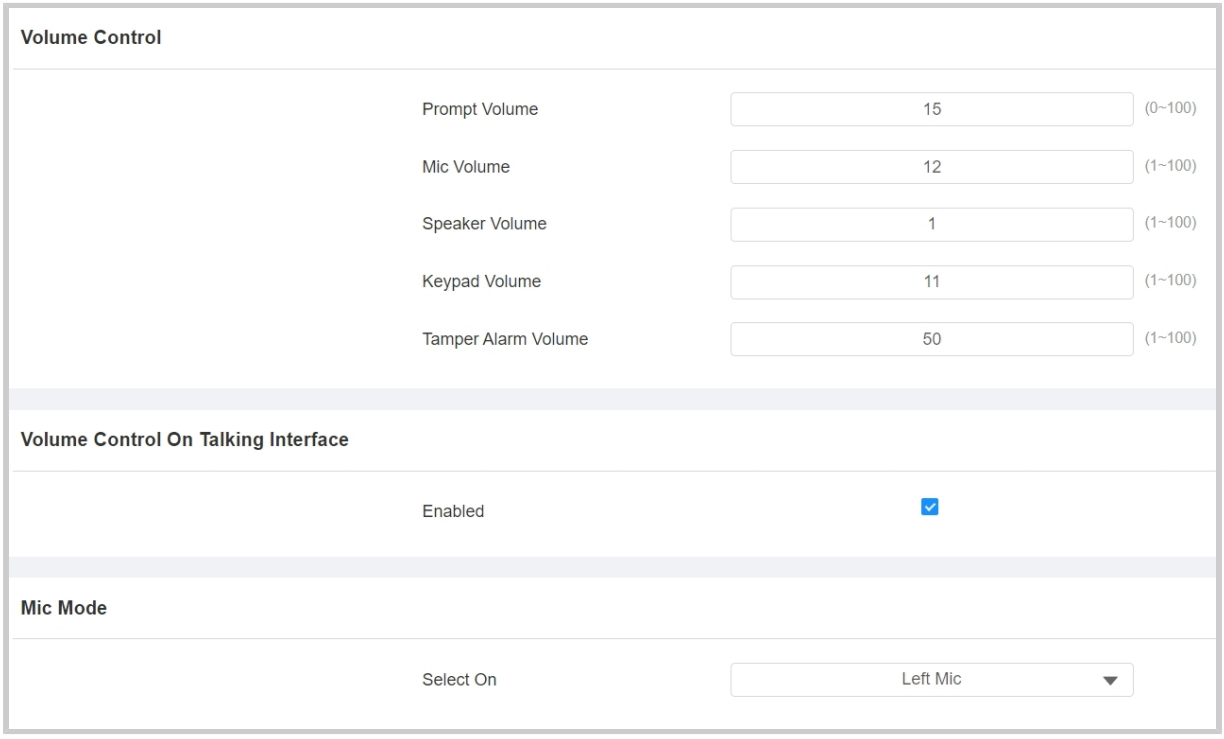
Volume and Tone

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

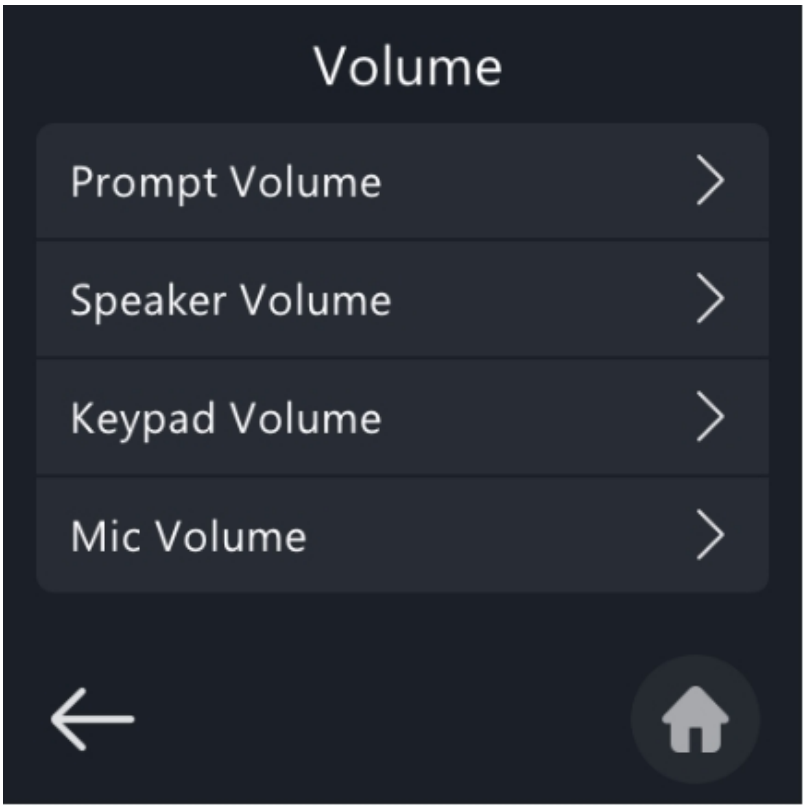


- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 50.
- **Mic Volume**: The default is 50.
- **Speaker Volume**: The default is 50.
- **Keypad Volume**: The icon tapping sound. The default is 50.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 50.

- **Volume Control On Talking Interface**: Decide whether users can control the microphone volume during a call.
- **Mic Mode**: Decide which microphone is turned on, left or right. The default is Left Mic.

On the Device

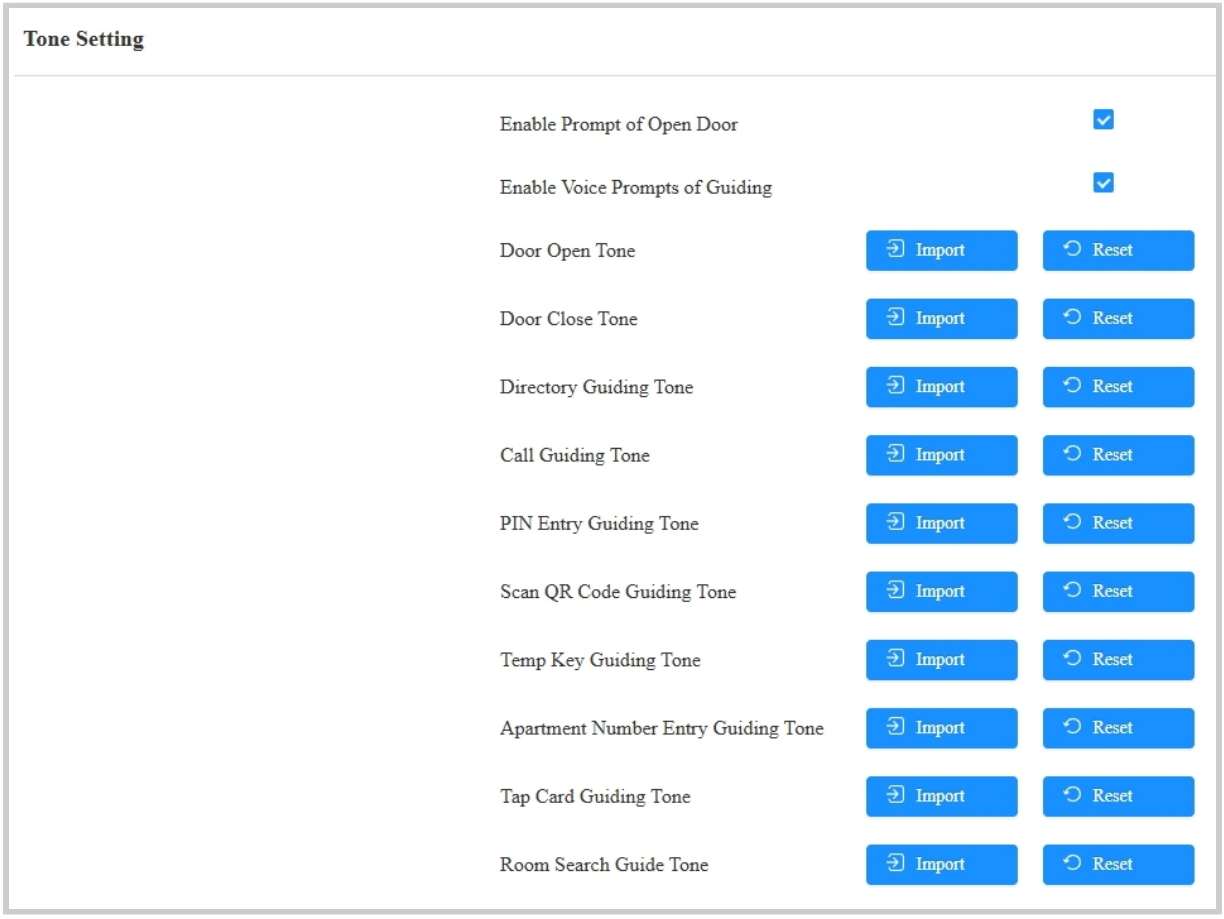
Set it up on the device **Admin Settings > Volume** interface.



- **Prompt Volume**: Include door-opening prompts, instruction tones, and ringback. The default is 50.
- **Speaker Volume**: The default is 50.
- **Keypad Volume**: The icon tapping sound. The default is 50.
- **Mic Volume**: The default is 50.

Upload Tones

You can upload various tones on the **Device > Audio > Tone Setting** interface. Click **Import** to upload the file and **Reset** to remove the file.



- **Enable Prompt of Open Door**: The door-opening success tone.
- **Enable Voice Prompt of Guiding**: The default guiding tone is “Please enter the number, then press the call button” when pressing the Call button on the screen.
- **Door Open Tone**: The door-opening success tone.
- **Door Close Tone**: The door-closing tone.
- **Directory Guiding Tone**: The voice prompt is heard when tapping the Directory button.
- **Call Guiding Tone**: The voice prompt is heard when tapping the Call button.
- **PIN Entry Guiding Tone**: The voice prompt is heard when tapping the PIN button.

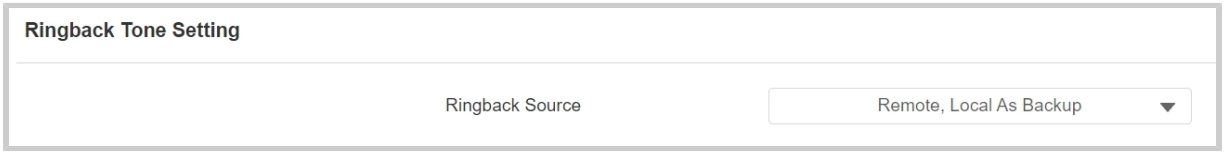
- **Scan QR Code Guiding Tone**: The voice prompt is heard when scanning the QR code.
- **Temp Key Guiding Tone**: The voice prompt is heard when entering the temporary PIN.
- **Apartment Number Entry Guiding Tone**: The voice prompt is heard when entering the apartment number.
- **Tap Card Guiding Tone**: It is applied for the “Face+RF card” dual authentication mode when opening doors. It will be heard after users scan their faces first.
- **Room Search Guide Tone**: The voice prompt is heard when users search for the target directory on the device screen.

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

Ringback Tone Setting

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

To set it up, go to the **Intercom > Call Feature > Ringback Tone Setting** interface.



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

- **Local**: The local ringtone will be played. Whether the SIP server returns 183 or not, the callee will not have any intercom preview.
- **Remote:**
  - If the SIP server returns non-183, the local ringtone will be played, and the callee will not have any intercom preview.
  - If the SIP server returns 183, the SIP server's ringtone will be played, and the callee will receive the video preview without voice.

Visitor-Friendly Mode

This feature decides whether to display prompts when opening doors fail via facial recognition, LPR camera, and/or Wiegand card reader. When enabled, no visual or auditory prompts will be given when the recognition fails. The door log will not be saved.

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



- **Type**: Disabled by default. When checked, no prompts will be given when facial recognition/LPR camera recognition/Wiegand card reader scanning fails for door opening.
- **Save Access Log Enabled**: This option displays when **LPR Camera** is checked. Enabled by default. If disabled, the device will not save the logs of door-opening failure via the LPR camera.

Open Door Tone Mode

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



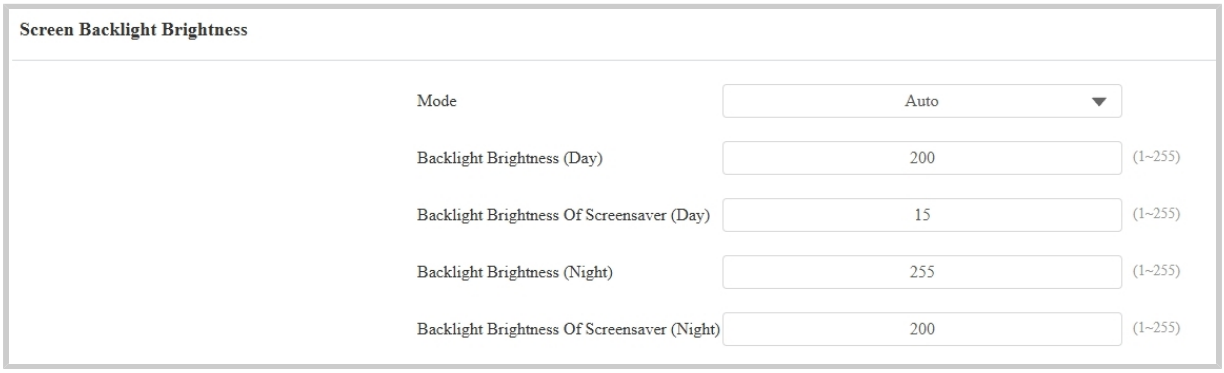
- **Voice Prompt**: Play the default prompt “Welcome, please come in” when the door is opened.
- **Sound Effect**: Play the beep sound when the door is opened.

LCD Setting

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

On the Web

To set it up, go to **Device > LCD > Screen Backlight Brightness** interface.



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

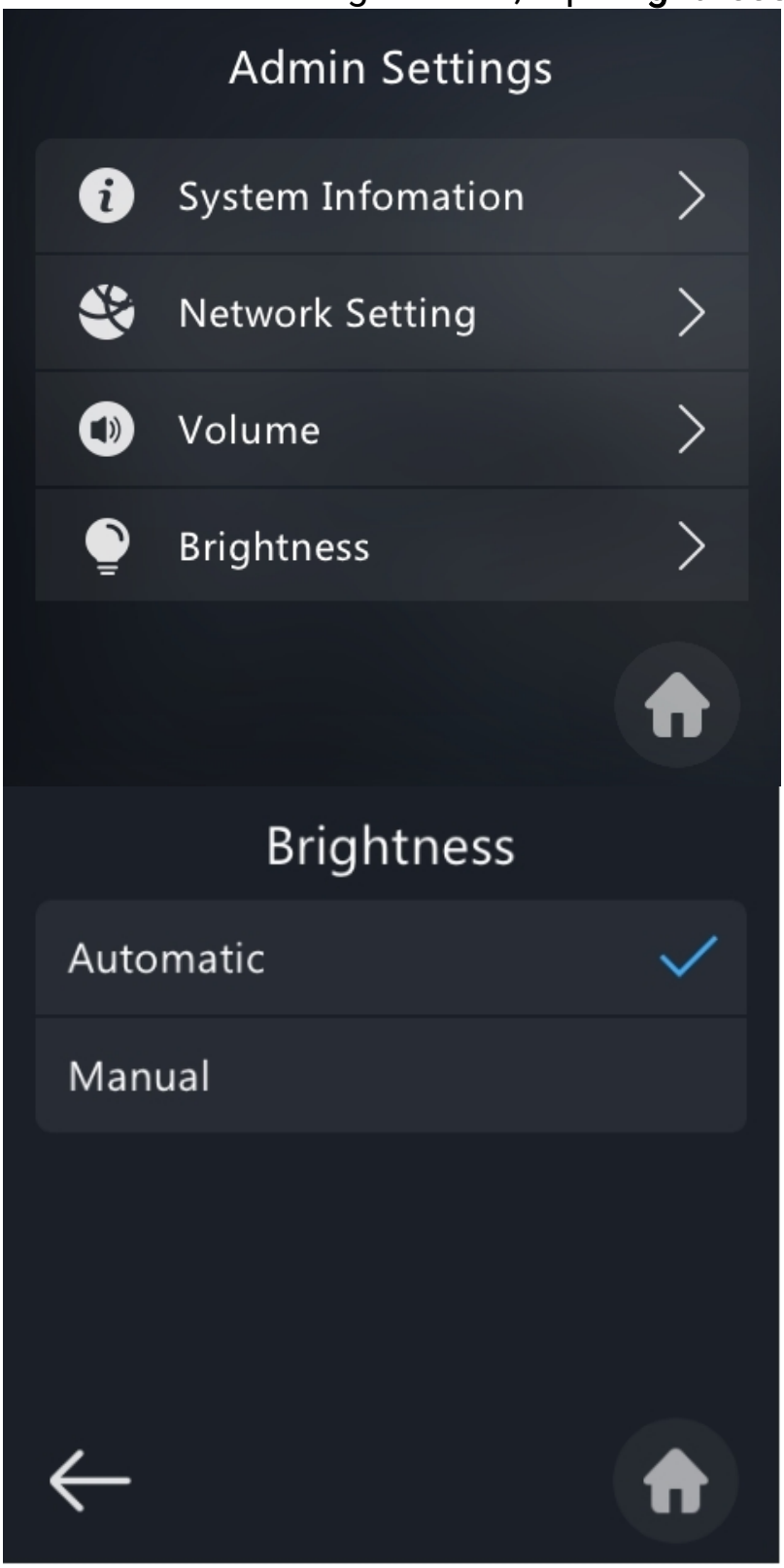
> **Note**
>
> The backlight brightness has two automatic modes, Day and Night. They are determined by the photoresistor.
>
> - If the current value is between the minimum and maximum photoresistor, the device is in Day mode.
> - If the current value is higher than the maximum photoresistor, the device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

- **Backlight Brightness (Day)**: Select the brightness value from 1-255. The default value is 200. The larger the value, the brighter the screen.

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

On the Device

On the Admin Settings screen, tap **Brightness**.



- **Automatic**: The device adjusts the brightness automatically.

- **Manual:** Set the brightness manually.

Keypad Light Setting

You can enable or disable the keypad light or set it to be turned on during a specific time.

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



- **Mode**:
  - **Auto**: The keypad light is off when the screen turns dark. The keypad lights up when pressed.
  - **Always OFF**: The keypad light stays off.
  - **Specific Time**: Set the time when the keypad light will be on.

Screen Display

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

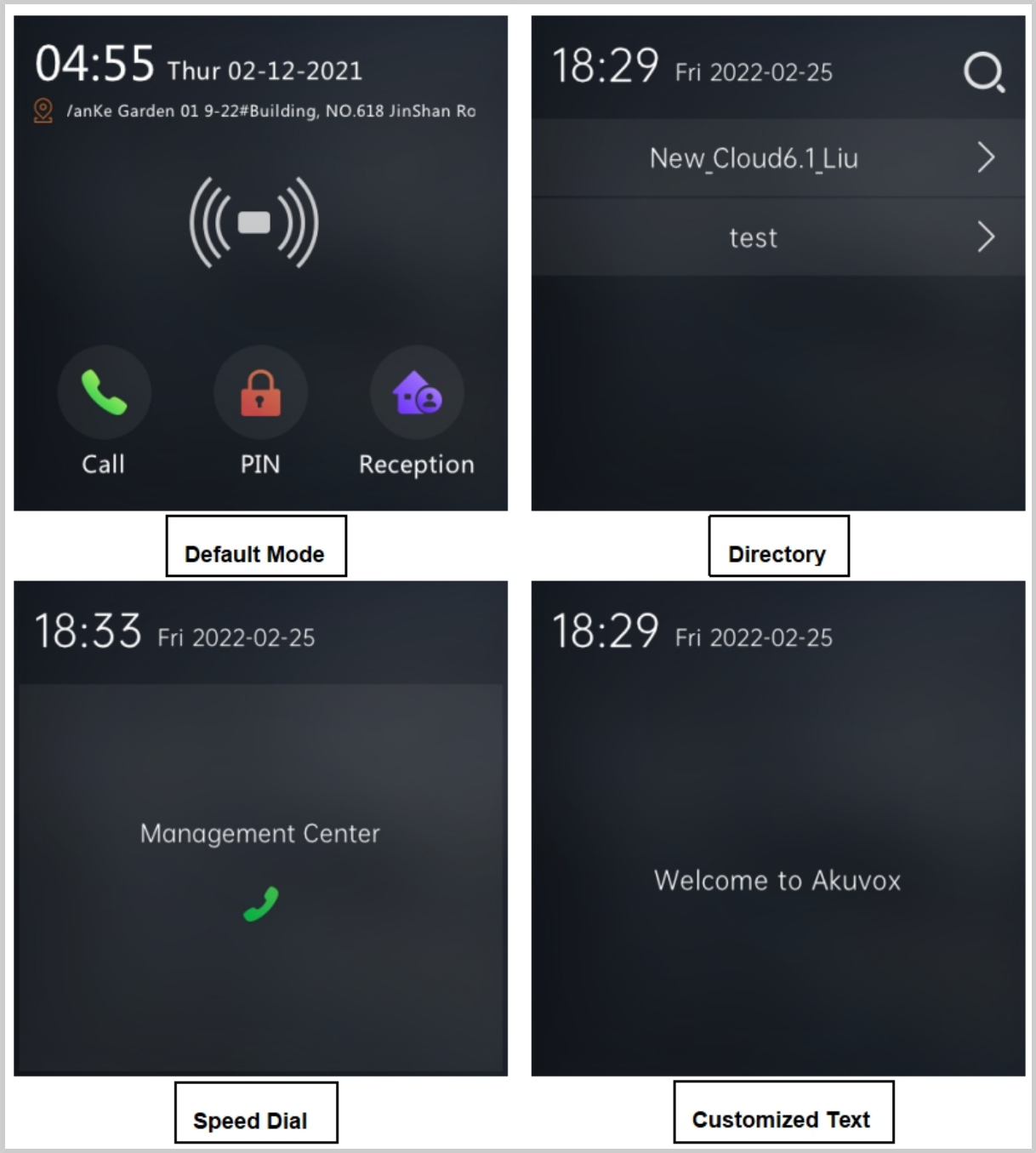
Theme Settings

X912 door phones offer you five types of screen display modes for different applications.

To set it up, navigate to **Setting > Key/Display > Theme** interface.



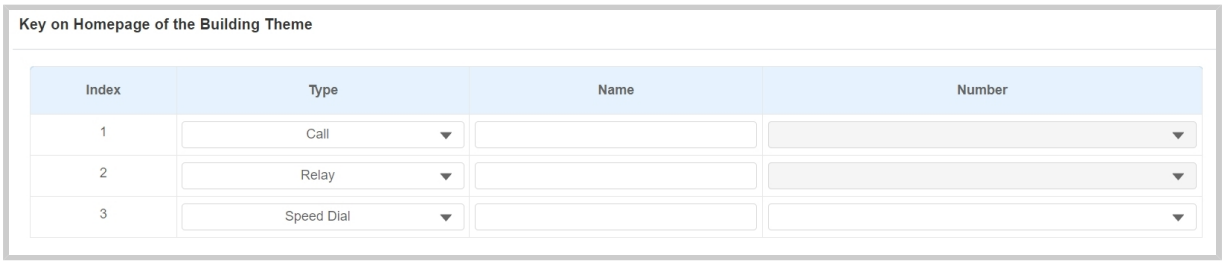
- **Theme**:
  - **Default(Buttons)**: Display Call, PIN, and Reception buttons on the home screen.
  - **Directory**: Display usernames.
  - **Speed Dial**: Display the contact for making the speed dial call.
  - **Customized Text**: Display the customized text.
  - **Gate Mode**: This mode requires using the SmartPlus Cloud service. It will display buildings and apartments in the Cloud.



Default (Buttons) Theme

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

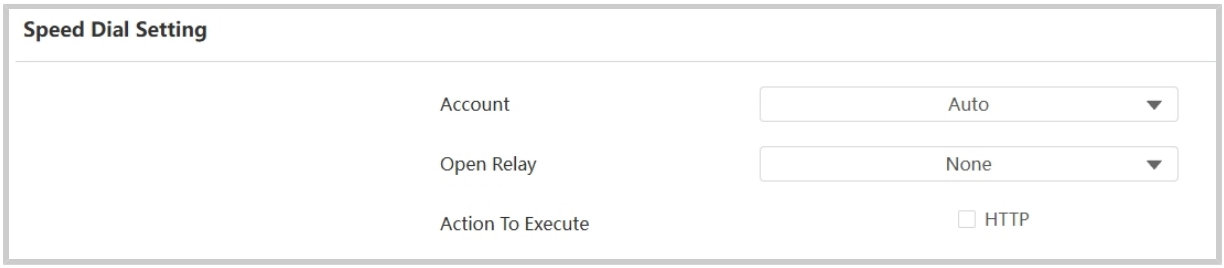
To set it up, scroll to **Key on Homepage of the Building Theme section** on the **Setting > Key/Display** interface.



- **Type**: Select the desired functional tab to be displayed in the desired area.
  - **Face**: When selected, the X912 will not automatically start facial recognition. Users must tap the **Face** icon to display the face recognition frame and initiate recognition. If **Preview Visible** is enabled under **Facial Recognition Setting**, the recognition frame remains displayed on the homepage. However, facial recognition is ONLY triggered when the **Face** icon is tapped.
- **Name**: Name the tab. Its name will not change its attribute.
- **Number**: Only available for the Speed Dial tab. Set the number to be called through speed dial.

Speed Dial Setting in Default Theme

In the Default theme, you can set up the speed dial action on the **Setting > Key/Display > Speed Dial Setting** interface.



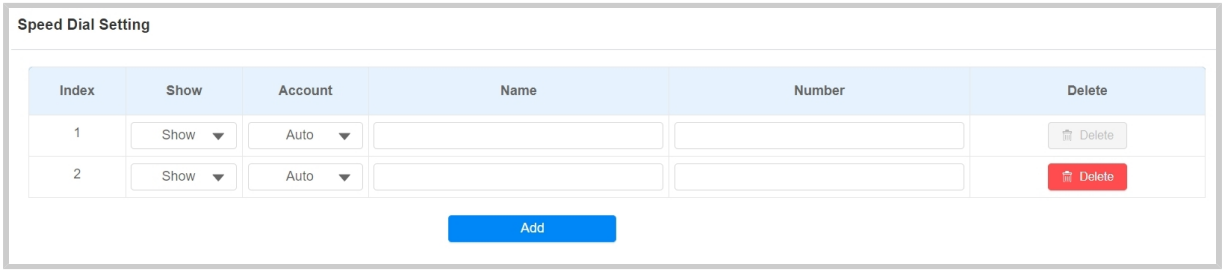
- **Account**: Select the account to make the call. It applies to the registered account. If both accounts are registered, Account1 is used when Default is selected.
- **Open Relay**: Select the relay to be triggered along with the call.

- **Action to Execute**: Set the action to be triggered with the call. When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
  - **HTTP URL**: Enter the HTTP URL to perform certain actions. The format of sending the message is *http://HTTP server's IP/Message content*.

Speed Dial Theme

You can display up to five speed dial numbers in the Speed Dial theme.

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



- **Name**: The contact's name.
- **Number**: The target SIP/IP number.

Customized Text Theme

You can customize the text to be displayed on the device home screen, such as community or company names.

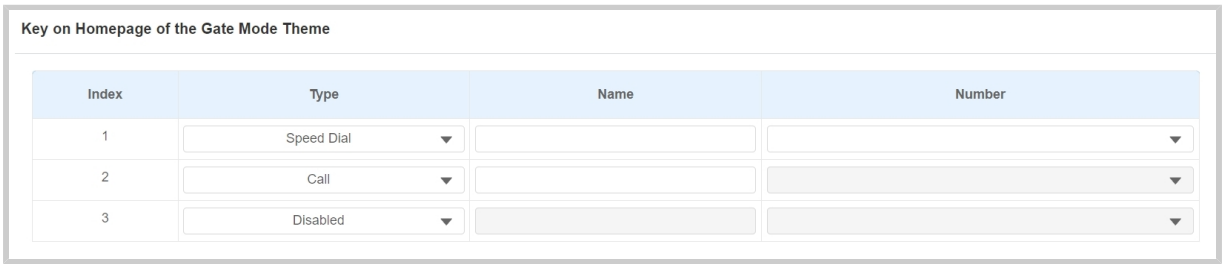
To set it up, scroll to the **Customized Text** section on the **Setting > Key/Display** interface.



- **Text**: The maximum text length is 63 characters.

Gate Mode

You can set up functional tabs to be displayed in **Key on Homepage of the Gate Mode Theme** section.

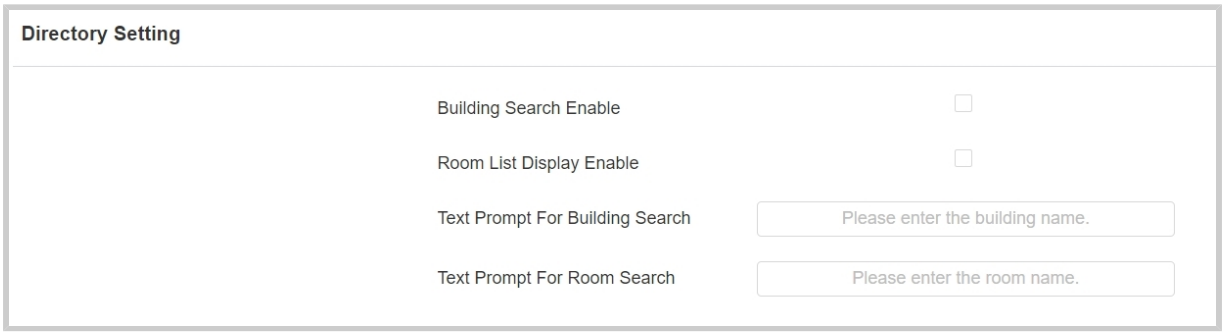


- **Type**: Select the desired functional tab to be displayed in the desired area.
- **Name**: Name the tab. Its name will not change its attribute.
- **Number**: Only available for the Speed Dial tab. Set the number to be called through speed dial.

Directory Setting

In Gate Mode, you can set up the search functions by which users can conveniently find desired buildings and rooms.

Set it up in the **Directory Setting** section.



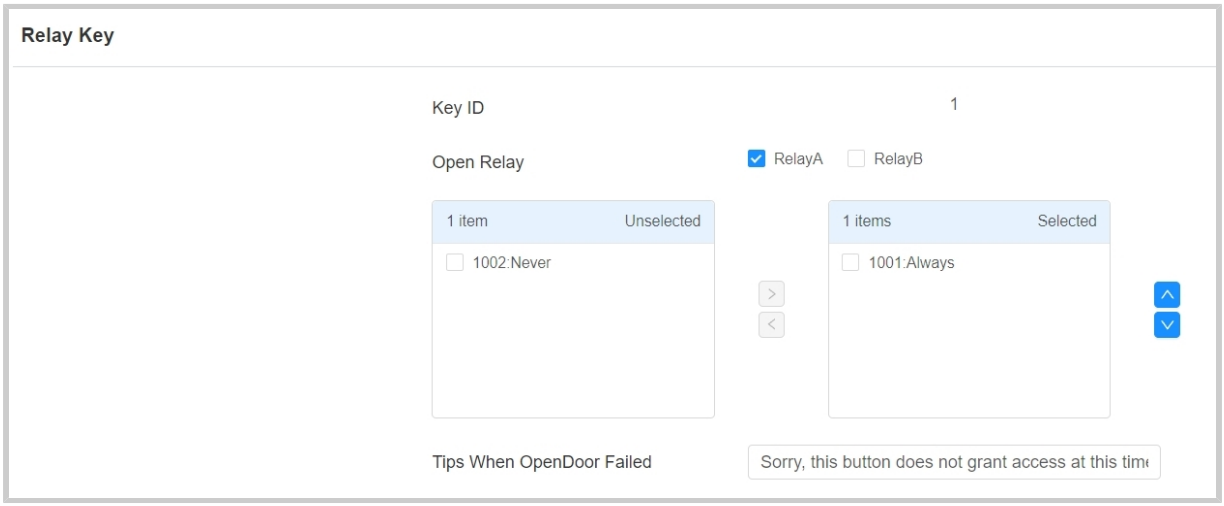
- **Building Search Enable**: When enabled, a search box will be displayed on the home screen. Users can enter the building name to find the target building.

- **Room List Display Enable**:
  - When enabled, all rooms in a building will be displayed after users select the building, and users can search for rooms.
  - When disabled, rooms will not be displayed, and users can only search for the room by entering the complete room number.
- **Text Prompt For Building Search**: Shown on the building display screen.
- **Text Prompt For Room Search**: Shown on the room display screen.

Relay Key Settings

This feature applies to the Default(Buttons) theme and Gate Mode. When the Relay tab is selected to be displayed, you can set up which relay and when it can be unlocked.

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



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

Dial Screen Prompt Display

This feature does NOT work for Gate Mode.

You can customize the prompt to be displayed on the dial screen on the **Setting > Key/Display > Prompt Of The Call Page** interface.

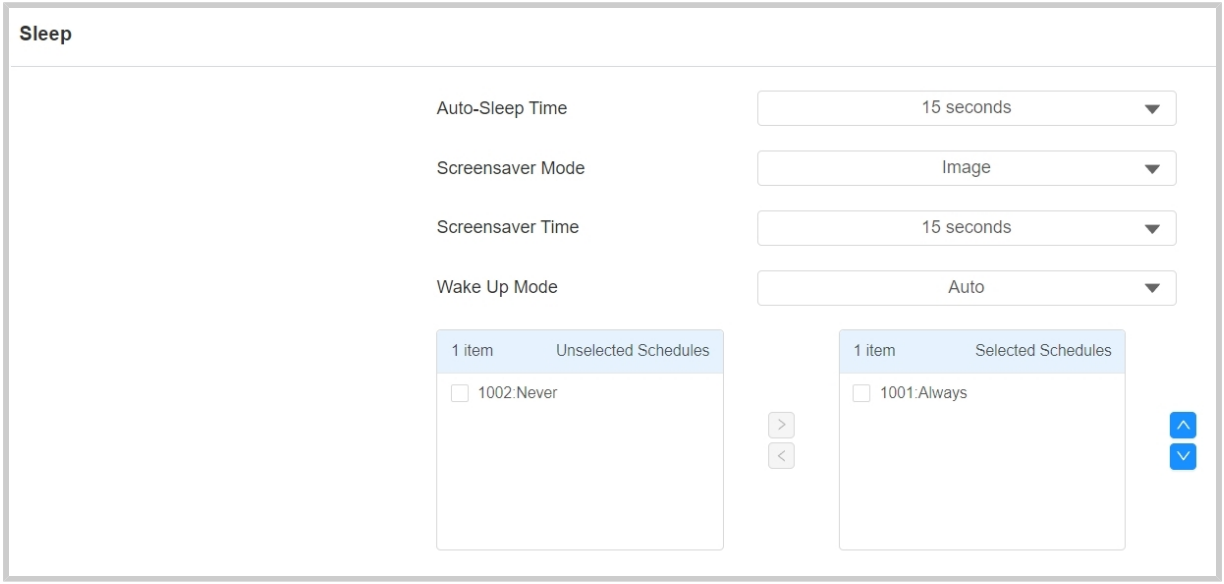


- **Text Prompt**: The maximum text length is 128 characters.

Screensaver Configuration

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

To set it up, go to **Device > LCD > Sleep**.

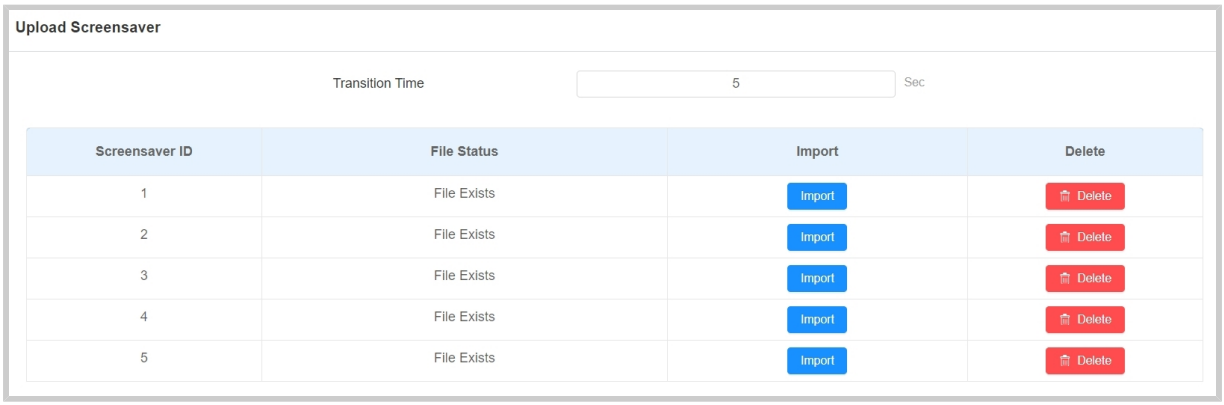


- **Auto-Sleep Time**: The interval between the screensaver and the screen off. For example, if it is set to 15 seconds, the device will go into screen saver mode when the device detects no operation or no approaching object for 15 consecutive seconds. When screen saver mode is disabled, the device screen will be turned off directly in 15 seconds. Auto-sleep time ranges from 5 seconds to 30 minutes.
- **Screensaver Mode**:
  - **Image**: Display the personalized pictures uploaded to the device.
  - **Disabled:** Disable the screen saver function.
- **Screensaver Time**: The screensaver duration ranges from 5 seconds to 30 minutes.
- **Wake Up mode**:
  - **Auto**: You can set the schedule when the screen will be automatically woken up by detecting an approaching object or operation.
  - **Manual**: Wake up the screen by touching it.
  - **Activated by Motion Detection**: This option is designed to prevent unintended activation. The screen needs to be unlocked by sliding the unlock button on the screen or by detecting a face in front of the camera. When enabled, you can set the schedule when the feature is effective. Beyond the range of the schedule, the device adopts the Auto mode.

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.

To set it up, go to the **Device > LCD > Upload Screensaver** interface. Click **Import** to upload the file and click **Delete** to remove the existing one.



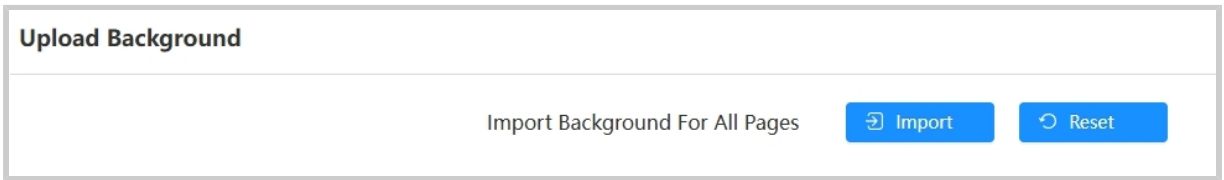
- **Transition Time**: The display time(1-120 seconds) of each screensaver picture. The default is 5 seconds.

> **Note**
>
> - Max Size: 1M, Format: .jpg, Recommended resolution: 480×480.
> - The previous picture with a specific ID order will be overwritten when picture with the same ID is uploaded.

Upload Background Picture

You can upload the background picture that works for all pages.

To set it up, go to the **Device > LCD > Upload Background** interface. Click **Import** to select the file from your local drive and click **Reset** to remove the file.

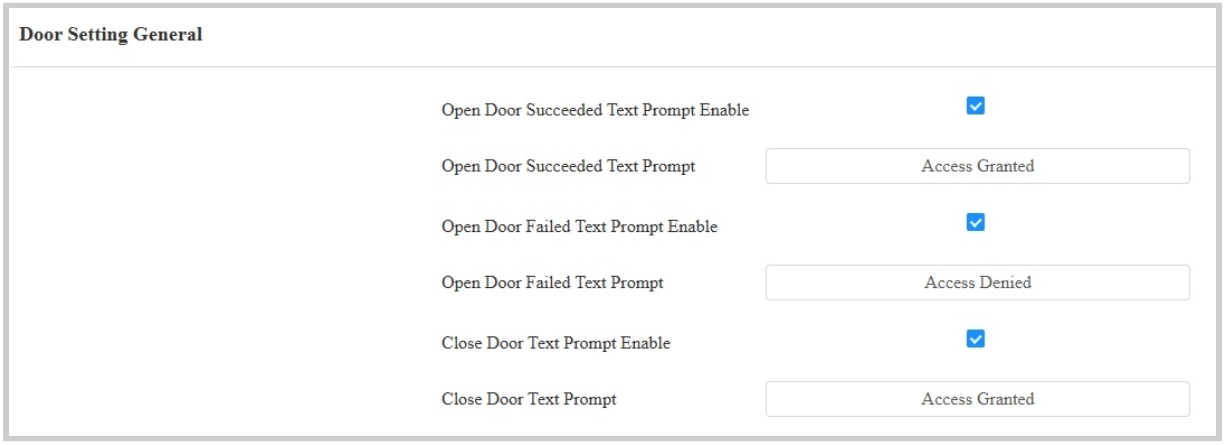


> **Note**
>
> Max Size: 2M; Format: .jpg/png; Recommended resolution: 480*480.

Open Door Text Prompt Display

You can enable the text prompt for door opening and closing, and customize the content.

To set it up, navigate to the **Access Control > Relay > Door Setting General** interface.



- **Open Door Succeeded Text Prompt**: The default is Access Granted. You can customize it with up to 63 characters.
- **Open Door Failed Text Prompt**: The default is Access Denied. You can customize it with up to 63 characters.
- **Close Door Text Prompt Enabled**: 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 Access Granted. You can customize it with up to 63 characters.

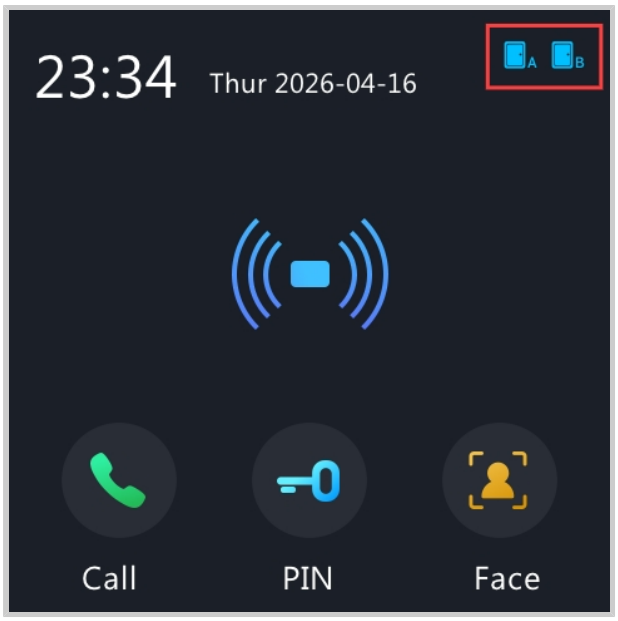
Door Status Display

This feature allows the device to show the real-time status of connected doors on the home screen, helping users quickly identify whether a door is open or closed.

To set it up, go to the **Setting > Key/Display** interface. This feature ONLY applies to the **Default(Buttons)** theme.



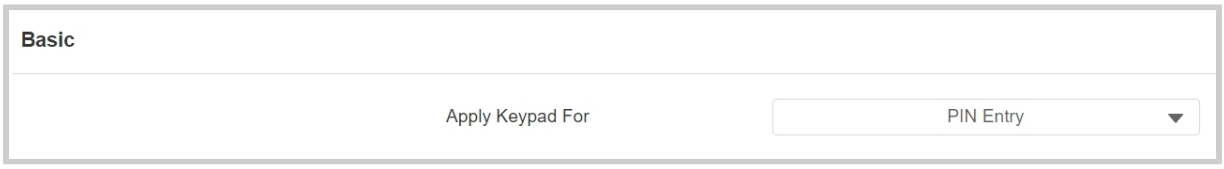
- **Icon Display**: Enable the icon display of specific relay(s). The device automatically updates the icon based on the relay output status.



Screen Displayed when Pressing Keypad

You can decide which screen to display, PIN entering or dialing screens, by selecting the keypad mode.

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



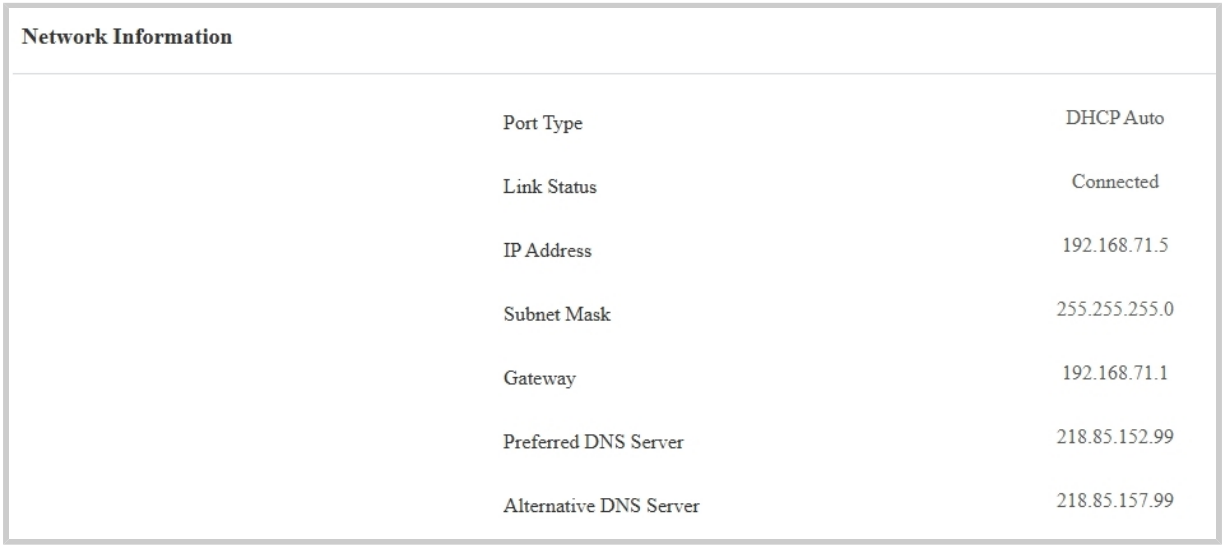
- **PIN Entry**: Enter the PIN entry screen when pressing numbers on the keypad.
- **Dial or PIN Entry**: Enter the dialing screen when pressing numbers on the keypad.

Network Setting

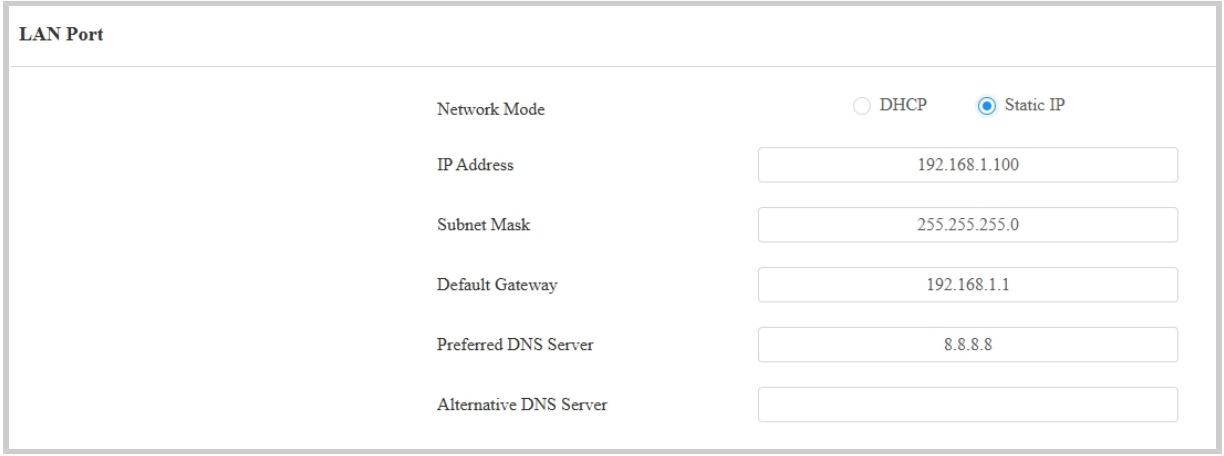
Device Network Configuration

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

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



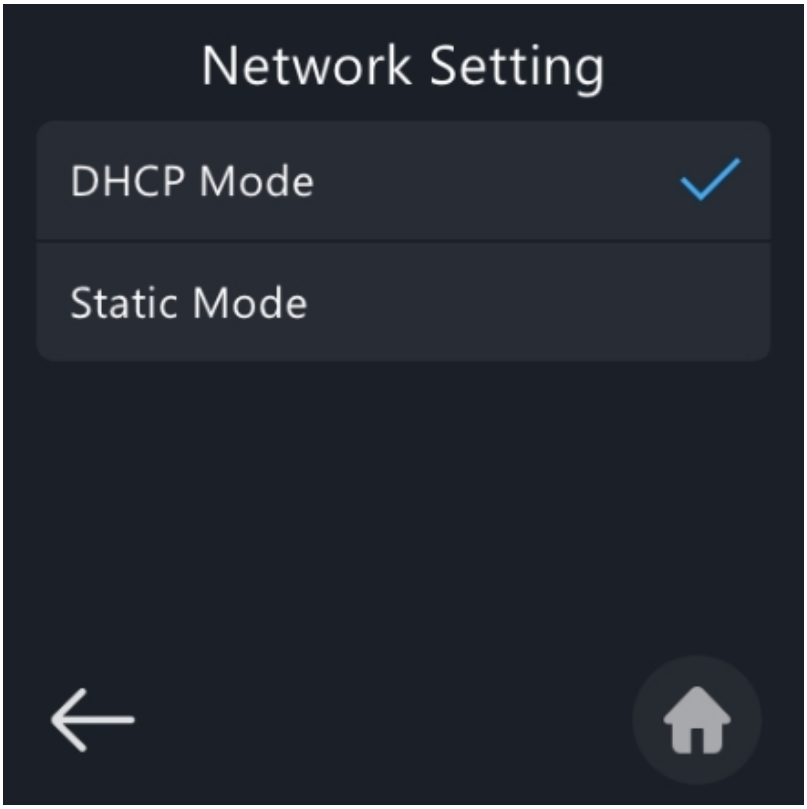
Set the network connection on the **Network > Basic** interface.

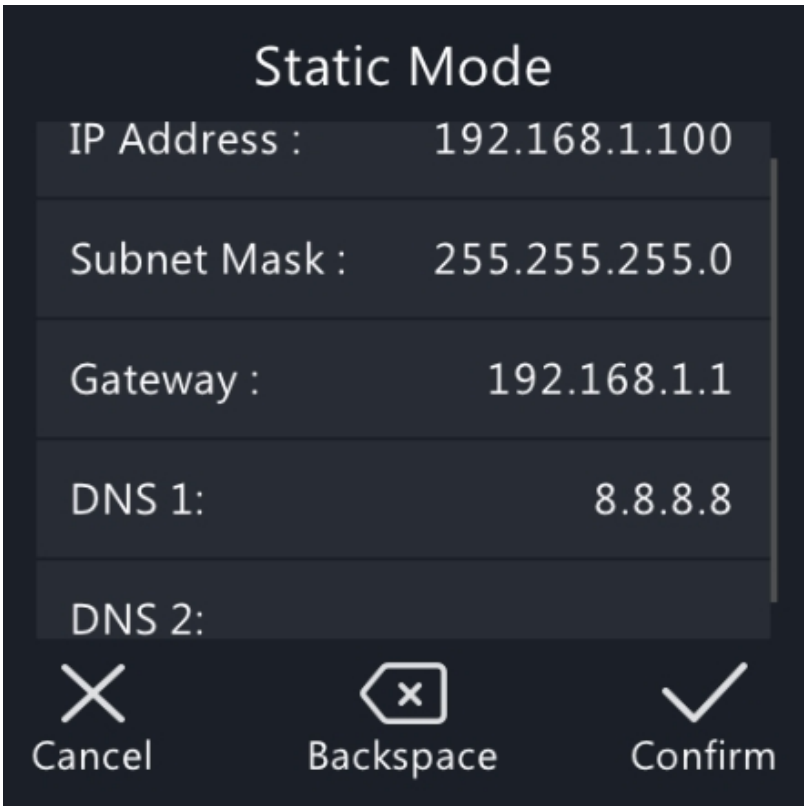


- **Network Mode**:

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

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


Network Setting
DHCP Mode
Static Mode

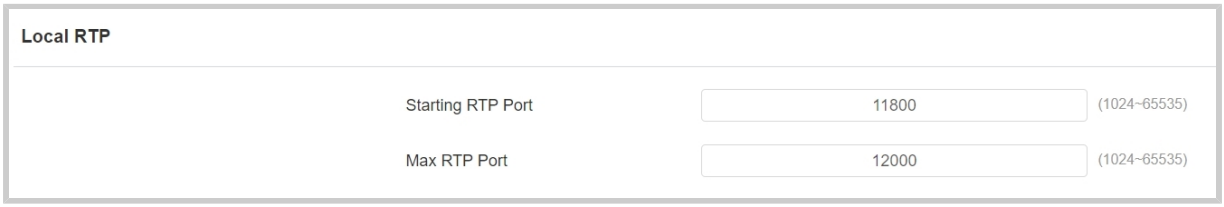

Static Mode
IP Address : 192.168.1.100
Subnet Mask : 255.255.255.0
Gateway : 192.168.1.1
DNS 1: 8.8.8.8
DNS 2:
Cancel
Backspace
Confirm

Device Local RTP Configuration

Real-time Transport Protocol(**RTP**) lets devices stream audio and video data over a network in real time.

To use RTP, devices need a range of ports. A port is like a channel for data on a network. By setting up RTP ports on your device and router, you can avoid network interference and improve audio and video quality.

To set it up, go to the **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.

To set it up, go to 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.

  - **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**: When enabled, 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**: 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**: The device extension number.

- **Device Location**: The location in which the device is installed and used.

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.



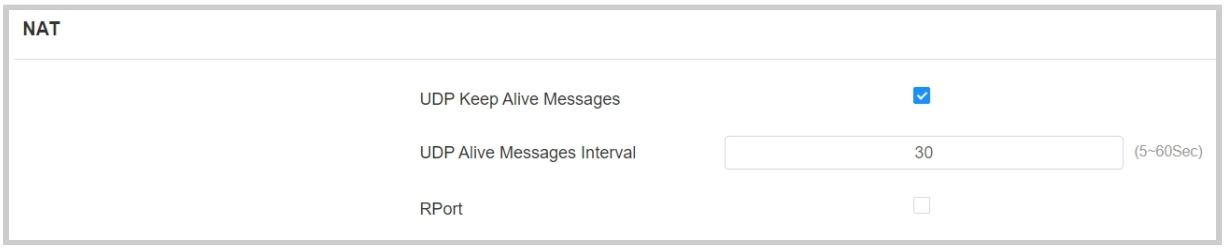
- **Protocol**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

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.

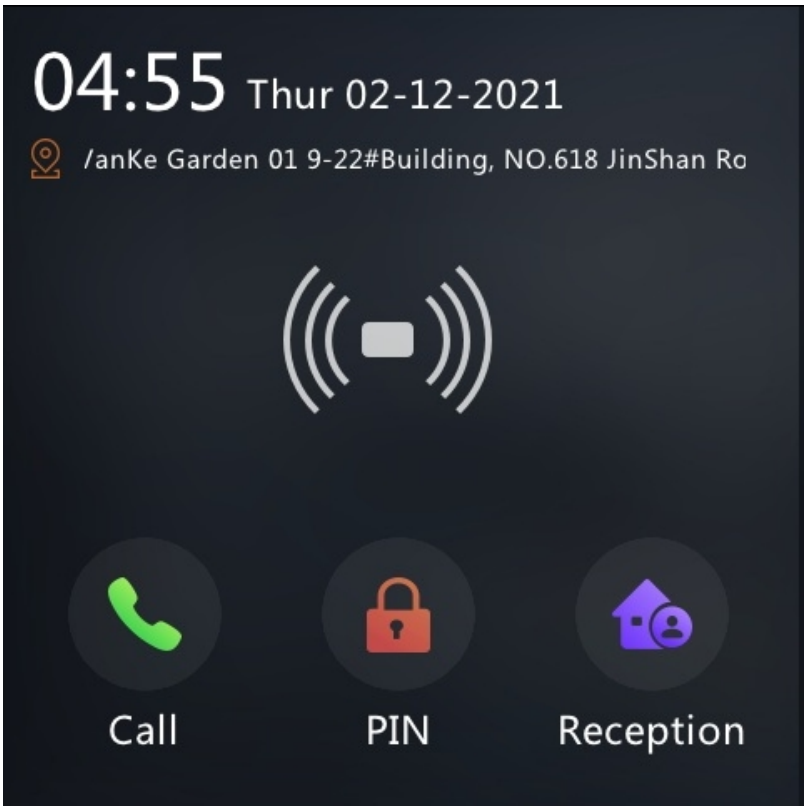
Intercom Call Configuration

IP Call & 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.

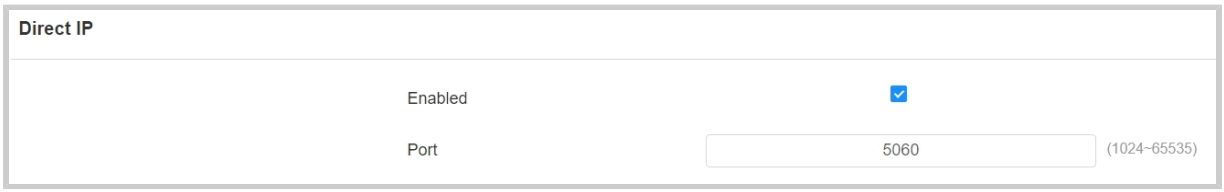
Make IP Calls

Make IP calls on the device by tapping the Call button on the home screen.



IP Call Configuration

Set the IP direct call on the device **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 & 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.

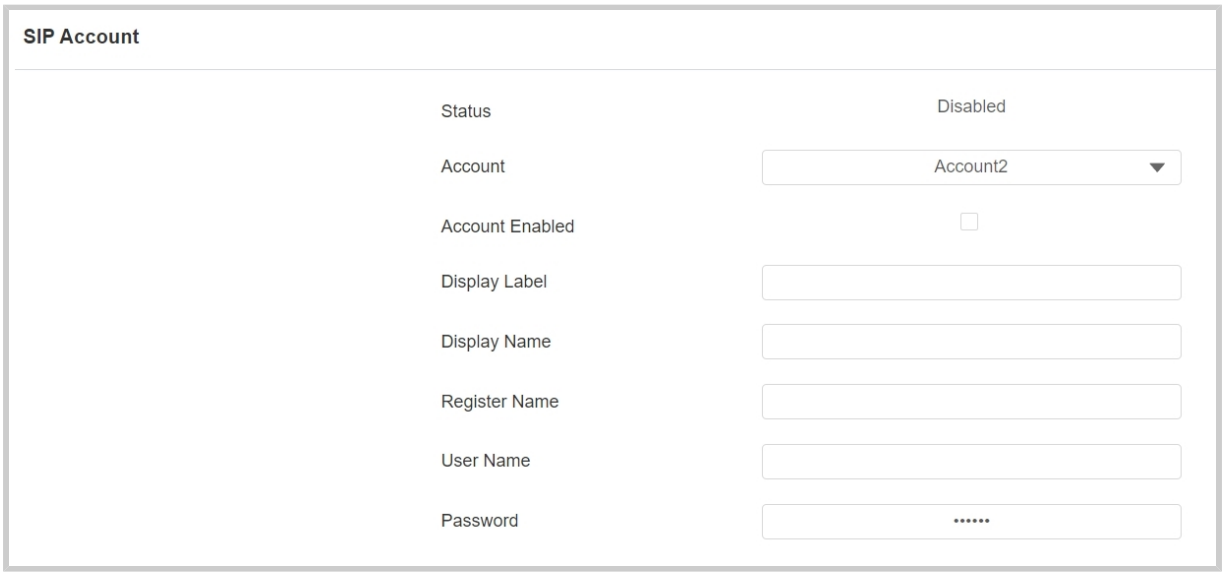
SIP Account Registration

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.

To set it up, navigate to the web **Account > Basic > SIP Account** 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.

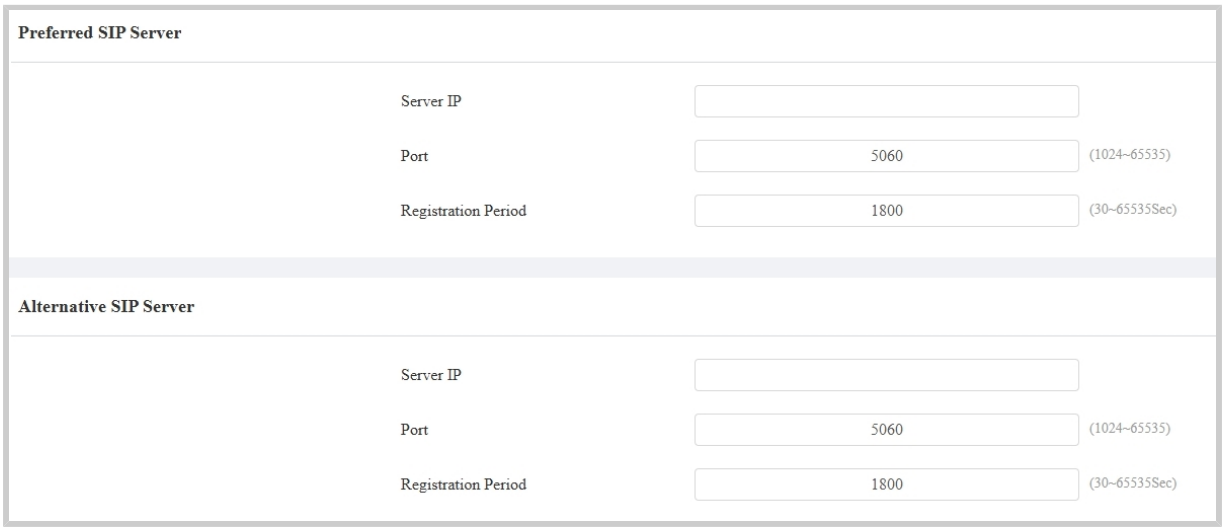
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 is to be shown on the device itself on the calling screen.
- **Register Name:** Same as the username from the PBX server.

- **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.

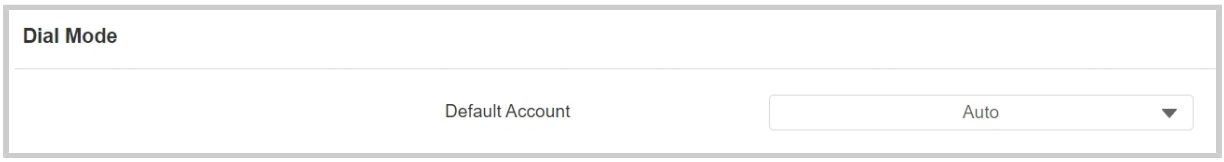


- **Server IP**: Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified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

SIP Account Selection

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

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

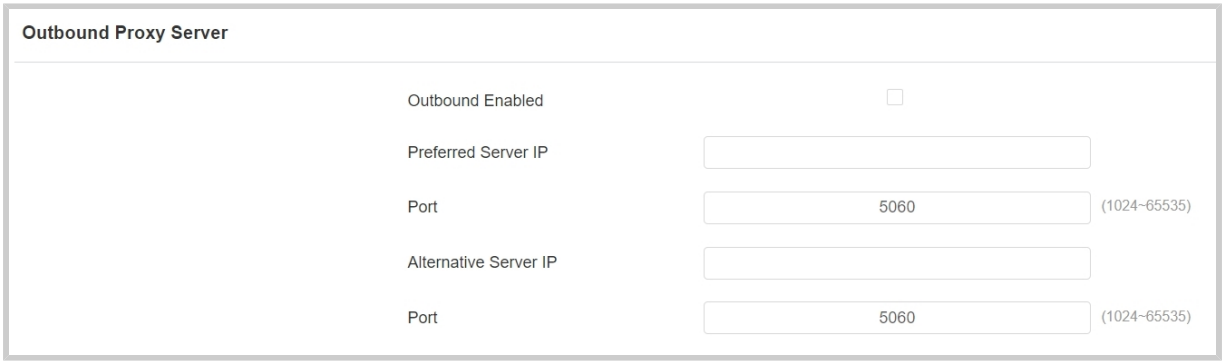


- **Default Account**:
  - **Auto**: The device will use the registered account to make SIP calls. If both are registered, Account 1 will be used by default.
  - **Account 1**: Calls can only be made to Account 1's contacts.
  - **Account 2**: Calls can only be made to Account 2's contacts.

Outbound Proxy Server

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

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



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

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

Data Transmission Type

SIP messages can be transmitted in three data transmission protocols. In the meantime, you can also identify the server from which the data comes.

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

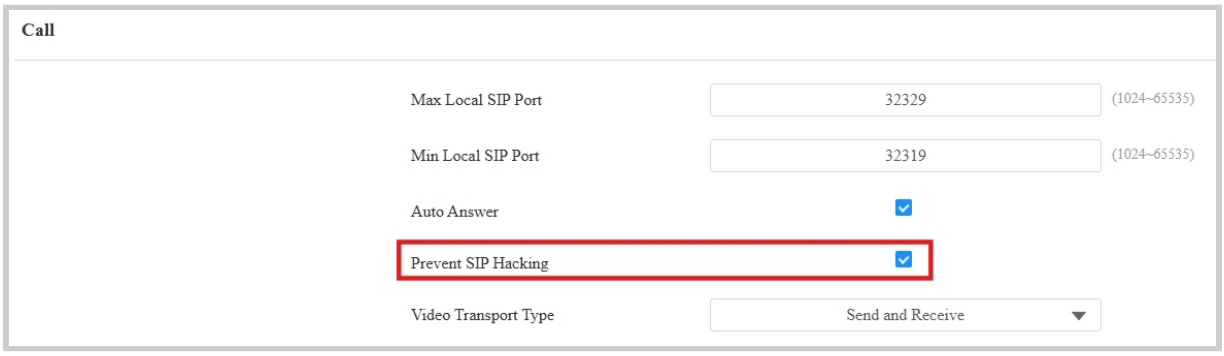


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

SIP Hacking Protection

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

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



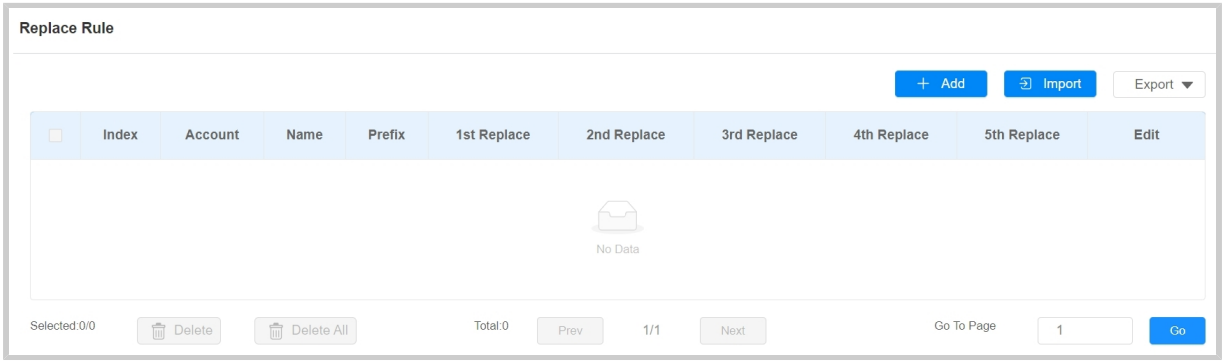
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

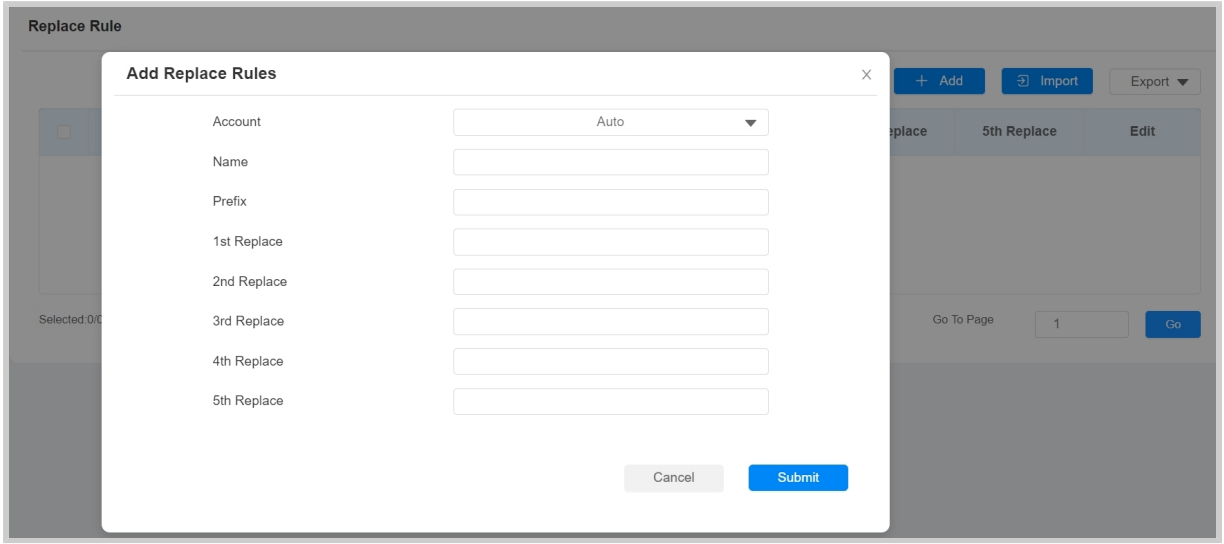
Call Settings

Quick Dial by Number Replacement

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

To set it up, go to the **Intercom > Dial Plan > Replace Rule** interface. Click **+Add**.





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

- **Account 1/2:** Dial-out using the chosen account.
- **Name:** Name the replaced number(s).
- **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.

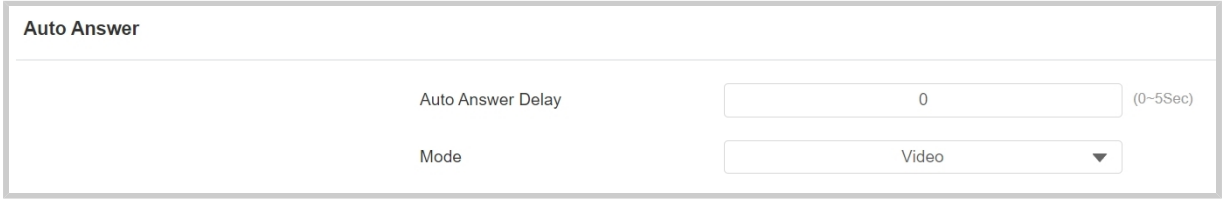
Call Auto-answer

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 call auto-answer feature, go to the **Account > Advanced > Call** interface.



To set it up, go to the **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.

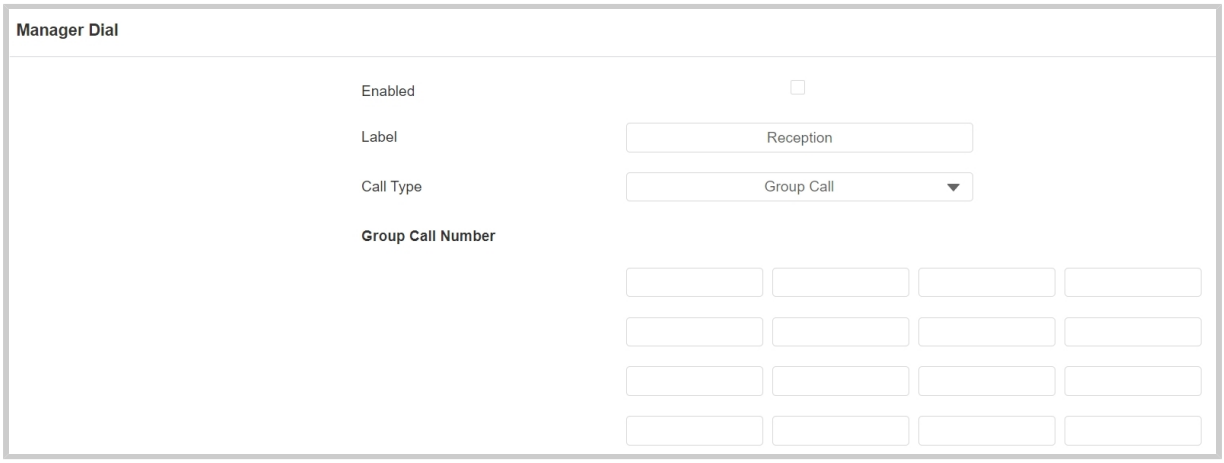
Manager Dial

Manager Dial Call includes two types of calls: Sequence call and group call. It allows quick initiation of pre-configured numbers by pressing the Management key on the door phone.

Group Call

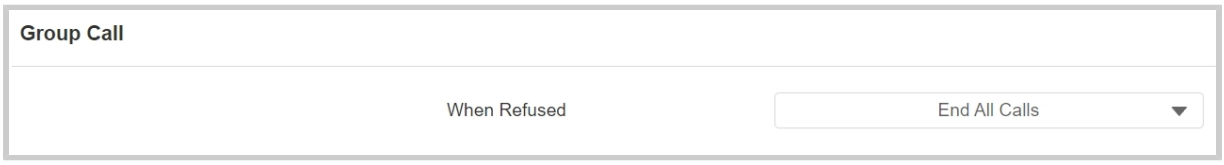
Group call is used to quickly initiate the pre-configured numbers by pressing the Dial key. You can create up to 16 group call numbers.

To set it up, go to the web **Intercom > Basic > Manager Dial** interface.



- **Label**: Set the button name to be displayed on the device.
- **Call Type**: Select between Group Call and Sequence Call.
- **Group Call Number**: If you fill in the local group call number, the local group number will be called instead of the SmartPlus group call number.

You can set up the actions when the call is refused in the **Group Call** section on the same interface.



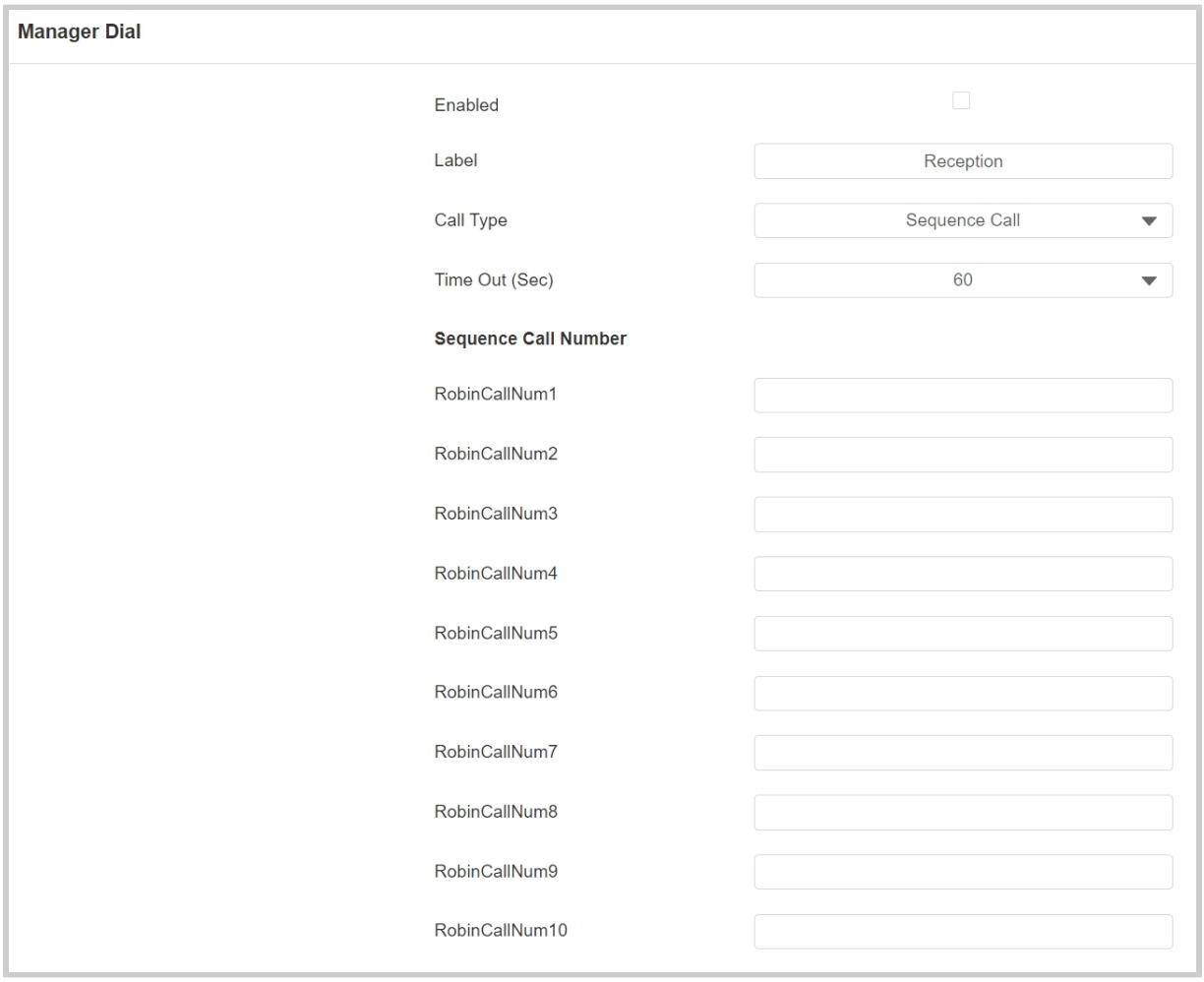
- **When Refused**:
  - **End This Call Only**: The call made to the refusing party will be terminated.
  - **End All Calls**: all calls will be terminated.

> **Note**
>
> You can refer to Configure Group Call for detailed configuration.

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. You can set up local sequence call numbers or connect the device to the Akuvox SmartPlus which provides a set of sequence call numbers for the application.

To set up the sequence call, go to **Intercom > Basic > Manager Dial** interface.



- **Label**: Set the button name to be displayed on the device.
- **Call Type**: Select between Sequence Call and Group Call.
- **Time Out(Sec)**: Determine the duration before calling the next number when the previous call is not answered.
- **Sequence Call Number(Local)**: Enter the target IP/SIP numbers.

Note

- When the device is connected to SmartPlus Cloud, local Sequence Call option will be unavailable.
- Please refer to Configure Sequence Call for detailed configuration.

Maximum Call Duration

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

To set it up, go to the web **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.

> **Note**
>
> The max call time is affected by the SIP server's max call time when users make SIP calls. The max call time should not exceed the call duration of SIP server.

Maximum Dial Duration

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

To set it up, go to the web **Intercom > Call Feature > Max Dial Time** interface.



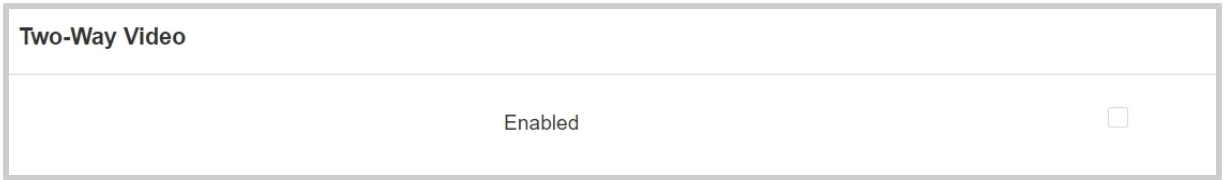
- **Max SIP/IP Dial In Time:** Specify the maximum duration of an incoming call. The door phone will automatically end the incoming call if it is not answered within the preset time.
- **Max SIP/IP Dial Out Time:** Specify the maximum duration of an outgoing call. The door phone will automatically end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

> **Note**
>
> The max dial time is affected by the SIP server's max dial time when users make SIP calls. The max call time should not exceed the dial duration of SIP server.

Two-Way Video Call

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

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



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

- The other party with a camera initiates a video cal,l and the device answers it.
- In all other cases, only audio communication is displayed.

Hang Up After Open Door

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

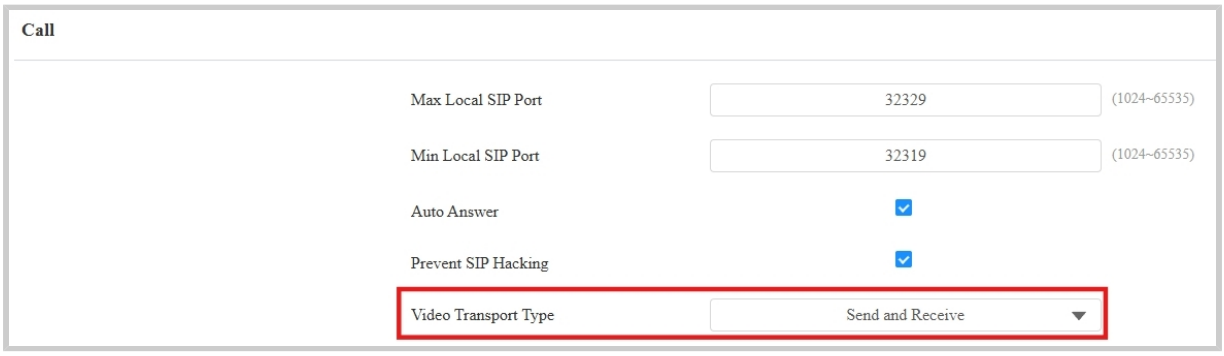
To set it up, go to the web **Intercom > Call Feature > Hang Up After Opening Door** interface.



- **Type:** Specify the door-opening 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.

Video Transport Type

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



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

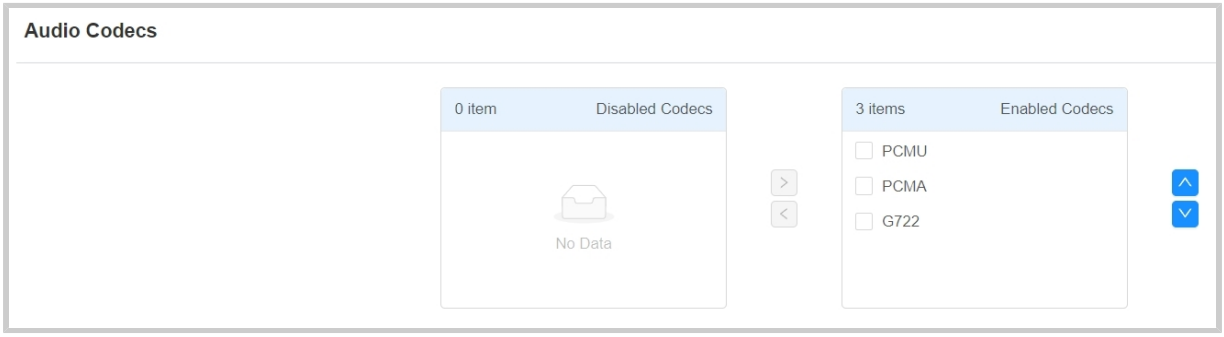
Audio & Video Codec Configuration

Audio Codec

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

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

To set it up, go to the web **Account > Advanced > Audio Codecs** interface.



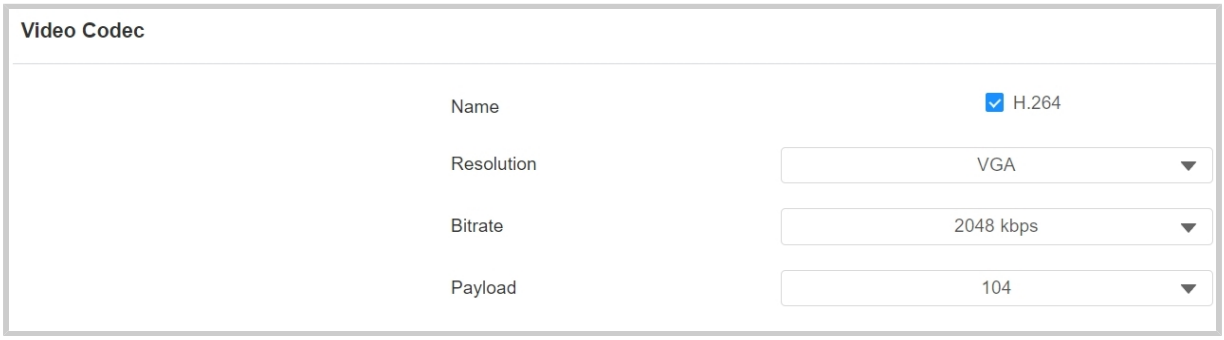
Please refer to the bandwidth consumption and sample rate for the codec types below:

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.

To set it up, go to the web **Account > Advanced > Video Codec** interface.

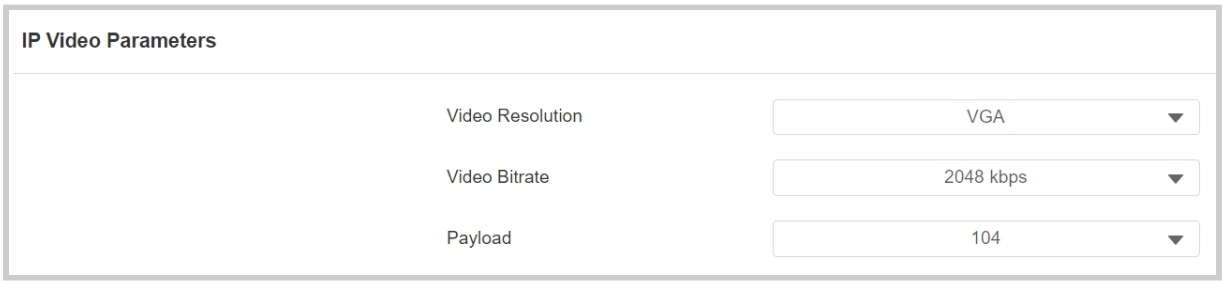


- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default code resolution is 720P(720 × 480 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate,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

Video Codec for Direct IP Calls

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

To set it up, navigate to the **Intercom > Call Feature > IP Video Parameters** interface.



- **Video Resolution**: Select the resolution from the provided options. The default resolution is 720P(720 × 480 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 64 to 2048 kbps. The default bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Contacts Configuration

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

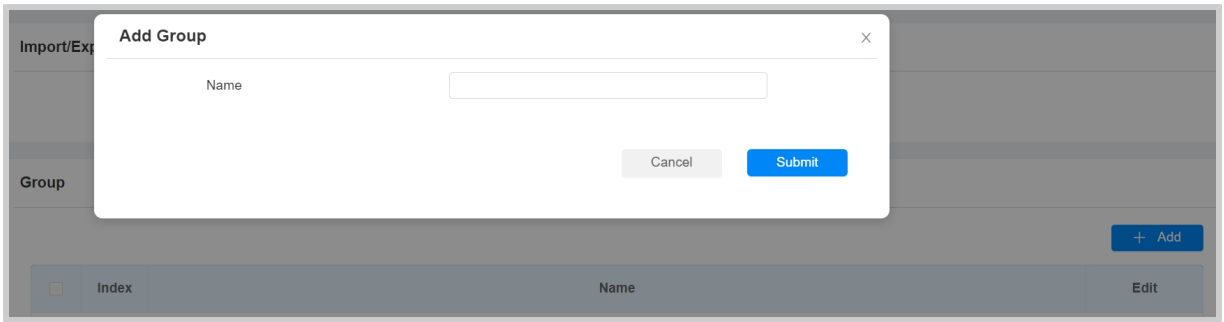
When the device is deployed on the SmartPlus Cloud, cloud contacts will display on the device web but not editable.

Manage Contact Groups

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

To set it up, navigate to the web **Directory > User > Group** interface. Click **+Add** to create a group. The device supports adding up to 1,000 groups.

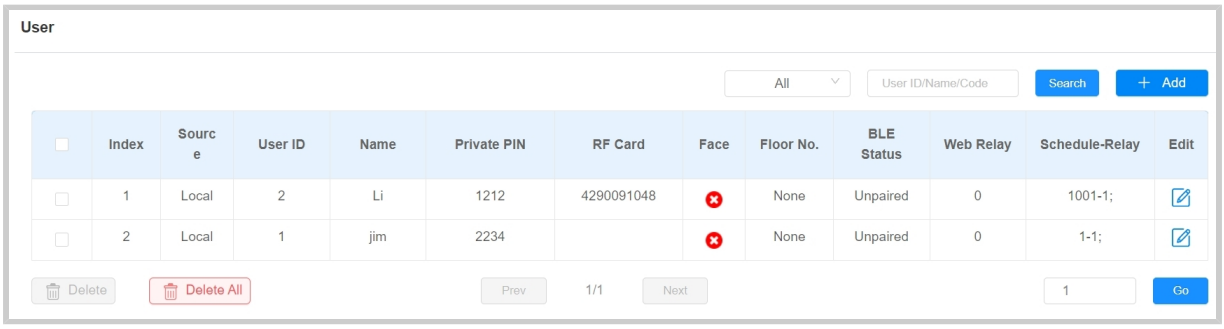


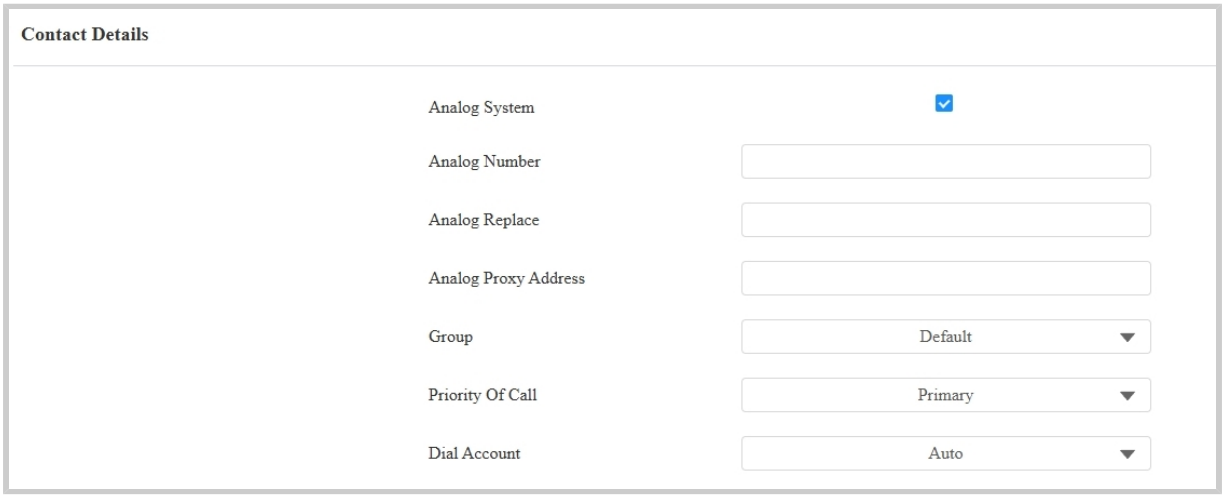


Set up Contact Details

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 Details** section.





- **Analog System**: The analog feature works with the Akuvox S532 door phone connected to the analog handset. It allows end users to call analog handsets by selecting contacts or entering numbers on the X912 door phone.
  When enabled, configure the following settings.
  - **Analog Number**: The number of the analog switch.
  - **Analog Replace**: Optional configuration. The short number replaces the analog number. Users can call the analog handset by entering the short number on the X912 door phone's keypad.
  - **Analog Proxy Address**: The IP address of the S532 in Direct mode.

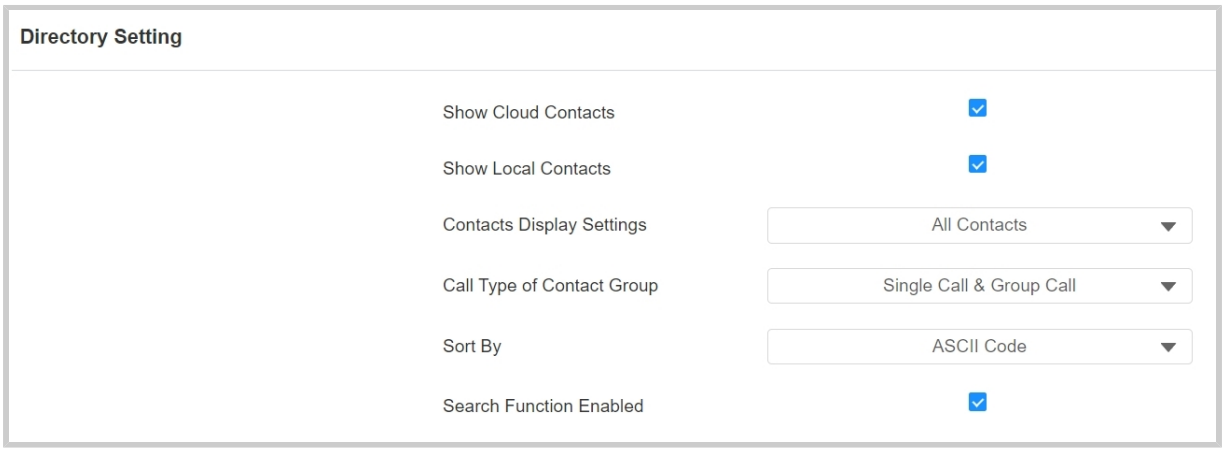
> **Note**
>
> To see detailed steps of configuring analog feature, please refer to:
> - Integration Between S532 and Third-party Analog Handsets.
> - Integration Between S532 and Akuvox Answering Units.

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

Contact List Display

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

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



- **Show Cloud Contacts**: Set whether to display the contacts configured on the cloud. This option changes by the device's deployment. If the device is deployed on the SmartPlus Cloud, it shows **Show Cloud Contacts**. If it is on SDMC, it shows **Show SDMC Contacts**.
- **Show Local Contacts**: The local contacts can be displayed on the device's home screen.
- **Contacts Display Settings**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only**: display contact groups. Press the desired group on the device screen to make a group call.
  - **Groups On Entry Page And Their Contacts On Subpage**: Display contacts by groups. Press the group, and users can see the contacts in it.
- **Call Type of Contact Group**:
  - **Single Call & Group Call**: Users can call contacts one by one or simultaneously in a group.
  - **Only Single Call Allowed**: Users can only call contacts one by one.
  - **Only Group Call Allowed**: Users can only call contacts in a group simultaneously.
- **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.
- **Search Function Enabled**: Decide whether users can search for the desired contact.
- **Cloud Call Permission Control**: This option will display when the device is connected to the SmartPlus Cloud. It decides whether to link the SmartPlus user's permissions to open doors and make calls.

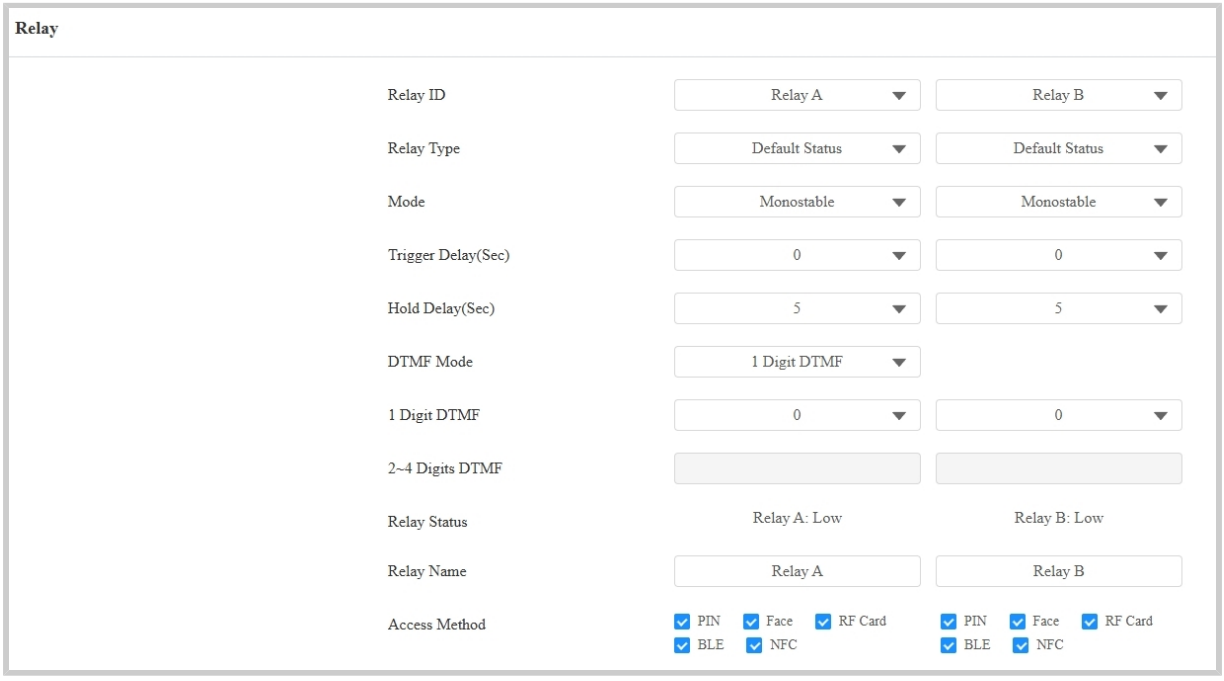
- For example, when users are not authorized to open doors during a specific time and the Cloud Call Permission Control feature is enabled, their SmartPlus App and/or indoor monitors will not receive calls from the door phone.
- If this feature is disabled, even if users cannot open doors, they can receive calls.

Relay Settings

Local Relay

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

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



- **Relay ID**: The specific relay for door access.
- **Type**: Determine the interpretation of the Relay Status regarding the state of the door:
  - **Default Status**: A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.
  - **Invert Status**: A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.
- **Mode**: Specify the conditions for automatically resetting the relay status.

  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Access Method**: Check the method(s) to trigger the relay.

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

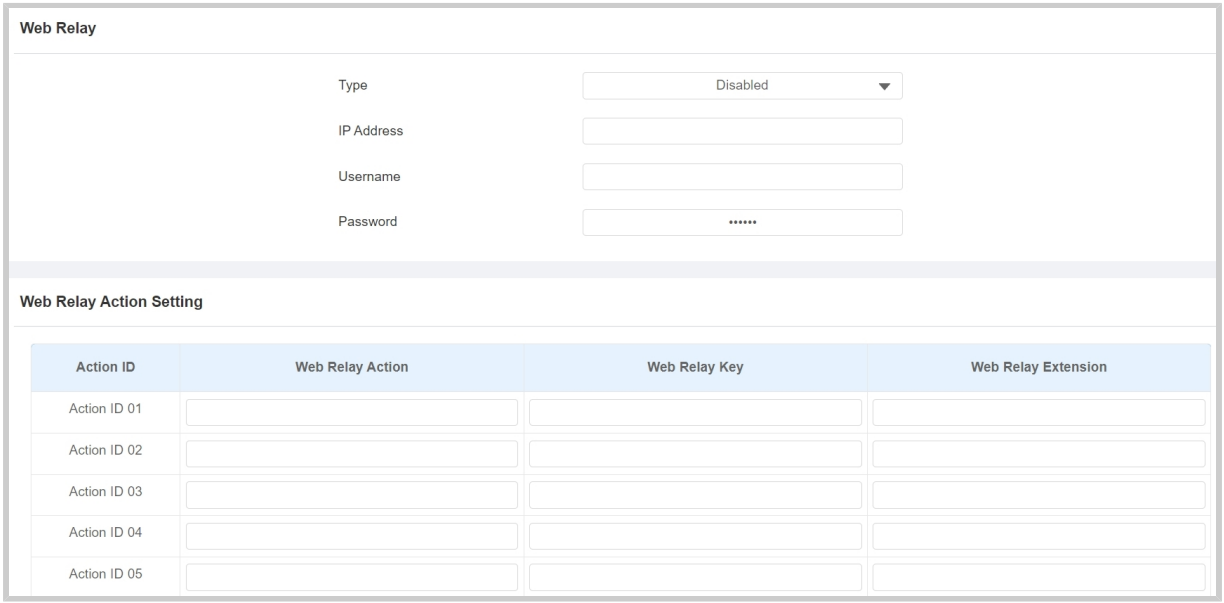
Web Relay

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**: There are three options, **Disabled, Only WebRelay**, and **Both**.
- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **Username**: The user name provided by the web relay manufacturer.

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

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

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

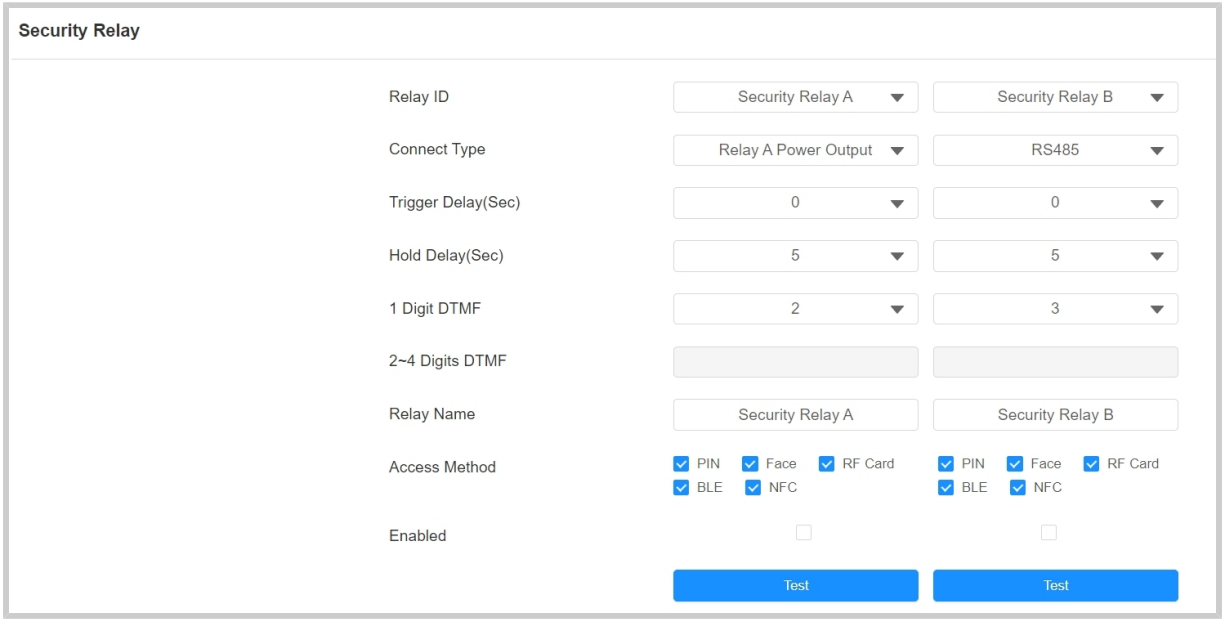
Security Relay

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 the web **Access Control > Relay > Security Relay** interface.



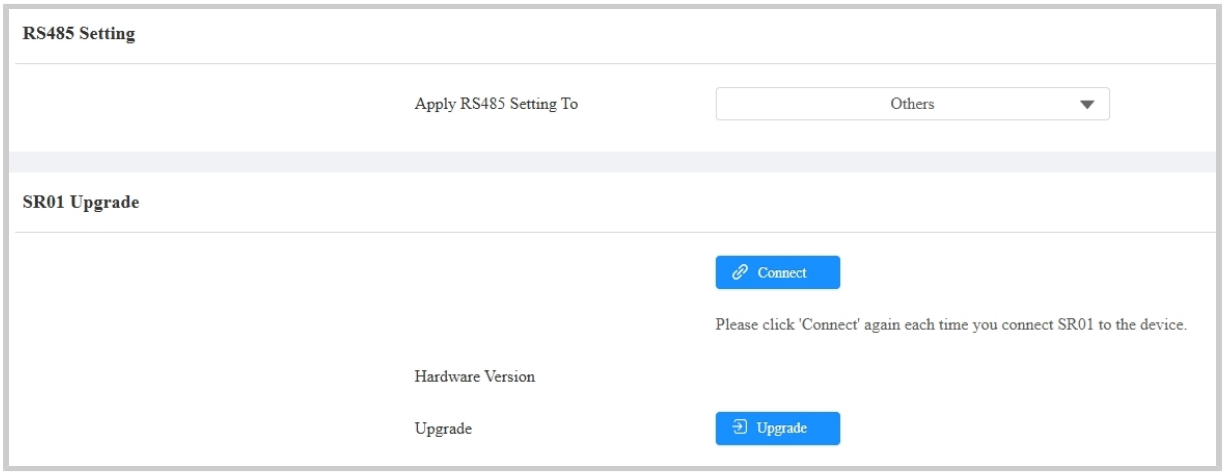
- **Relay ID**: The specific relay for connection.
- **Connect Type**: Select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.

- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name**: Name the security relay. The name can be displayed in door-opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method**: Check the method(s) to trigger the security relay.
- **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.
- **Upgrade**: Click to upload the ROM file.

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

Door Access Schedule Management

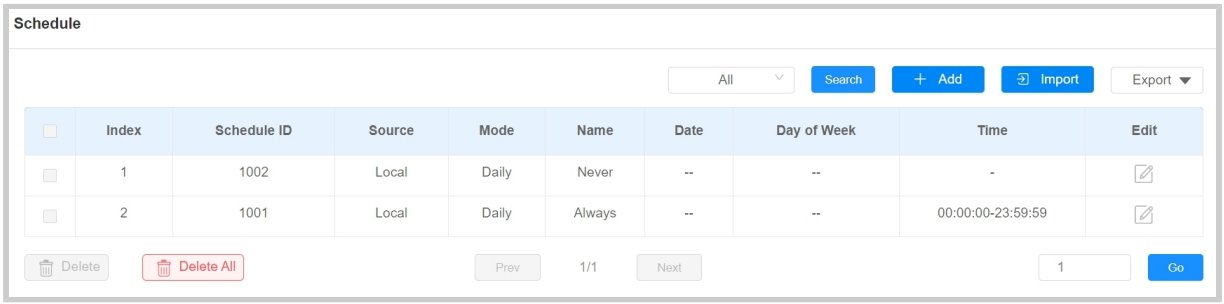
Configure Door Access Schedule

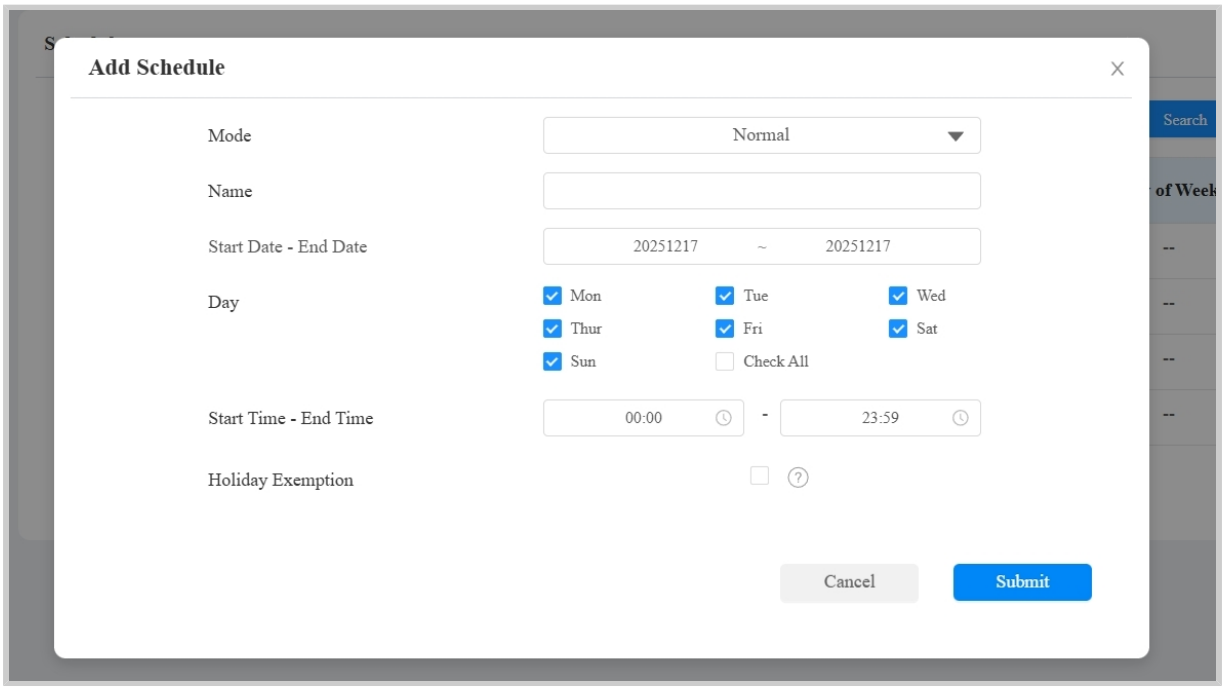
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Door Access Schedule

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

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





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

> **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.

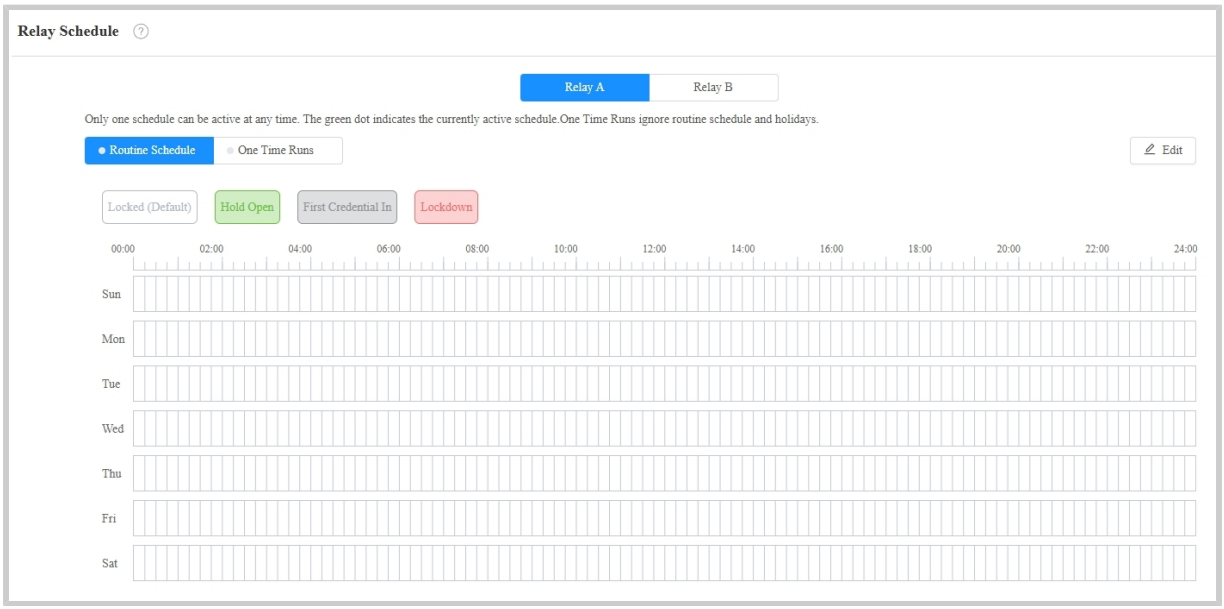
To set it up, go to the **Setting > Schedule** interface. The export/import file is in **XML** format.



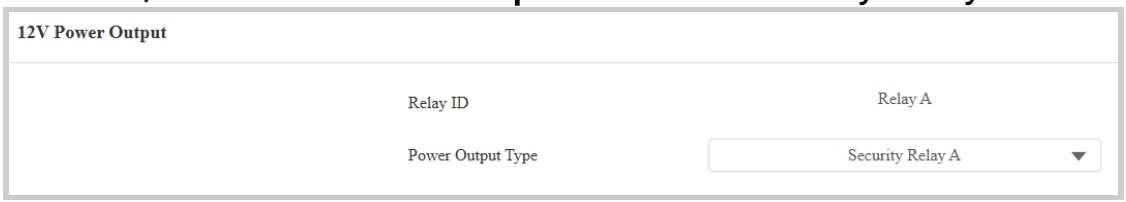
Relay Schedule

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

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



- **Relay ID**: Specify the relay that applies the schedule.
  - **Security Relay A**: Only available when the security relay is enabled, and **12V Power Output** is set to Security Relay A.



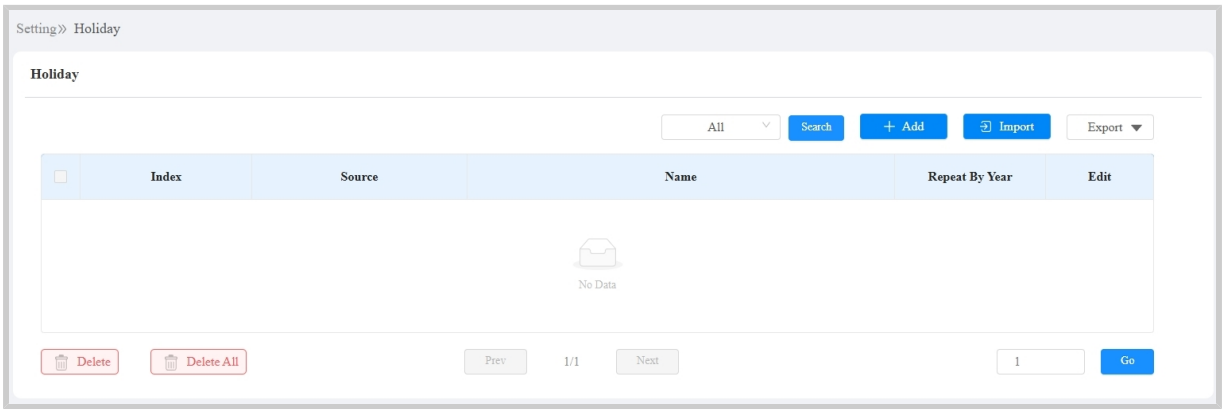
  - **Security Relay B**: Only available when the security relay is enabled.
- **Repeat Type**:
  - **Routine Schedule**: The schedule repeats every week. Click **Edit** on the right to configure.
  - **One-Time Runs**: Set the daily or weekly schedule that repeats during a defined period.
- **Schedule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

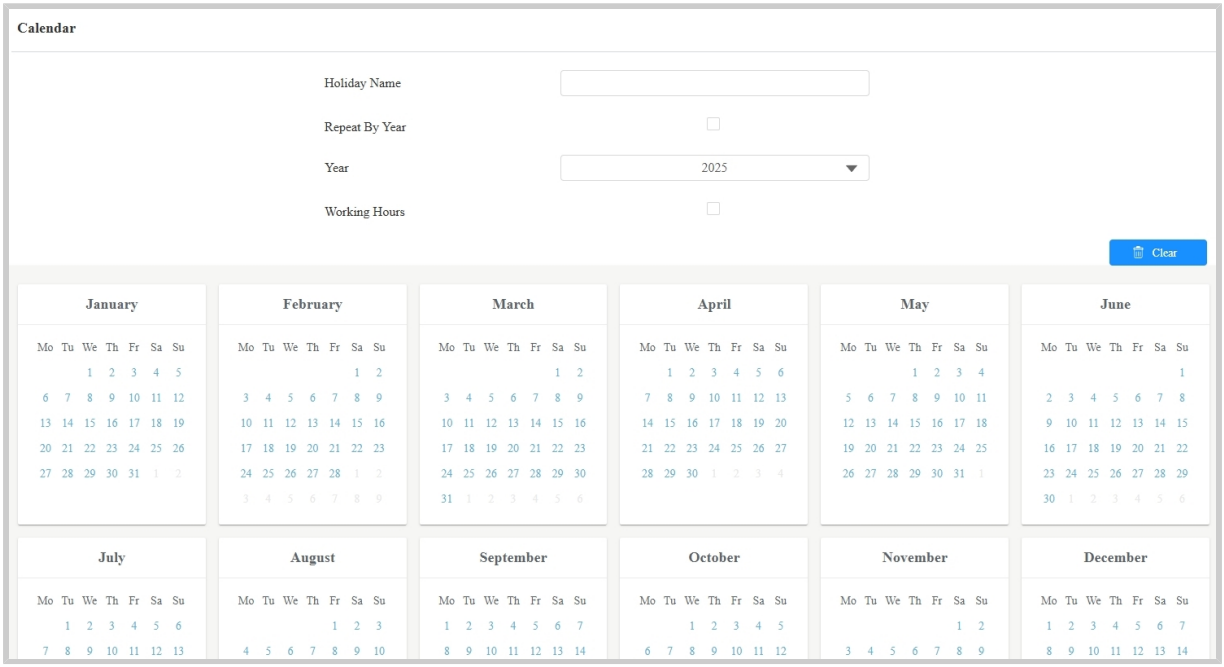
> **Note**
>
> Click here to view the detailed configuration of each schedule mode.

Holiday Schedule

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

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





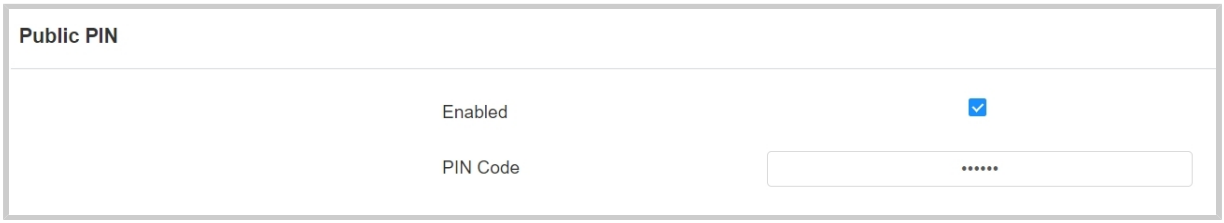
- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

Door-opening Configuration

Unlock by Public PIN

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

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

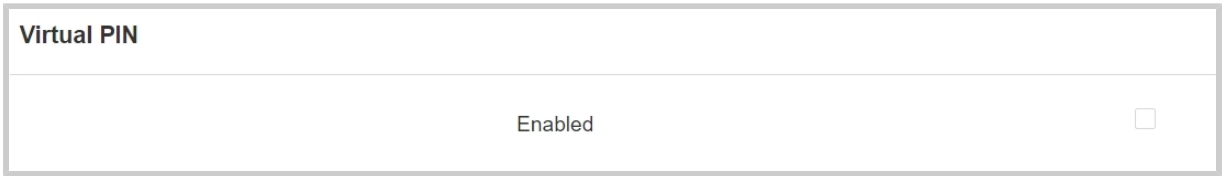


- **PIN Code**: Set a 3-8 digit PIN code accessible for universal use.

Virtual PIN

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

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



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

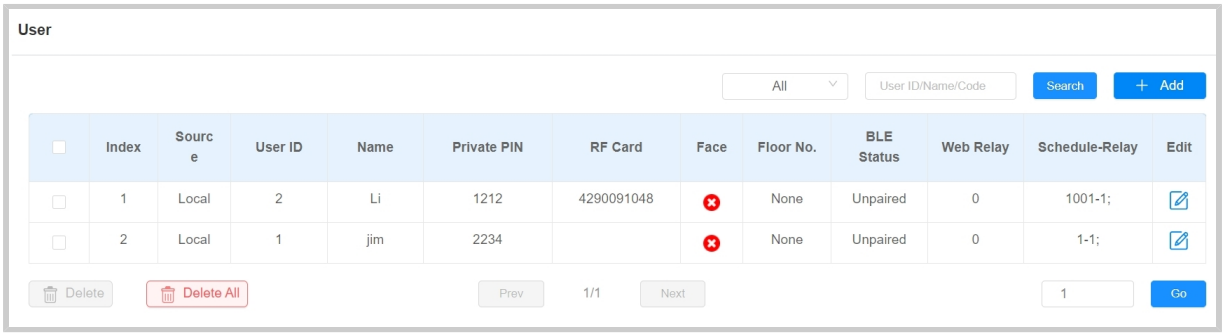
> **Note**
>
> This feature is not used for Public PIN and Apartment+PIN.

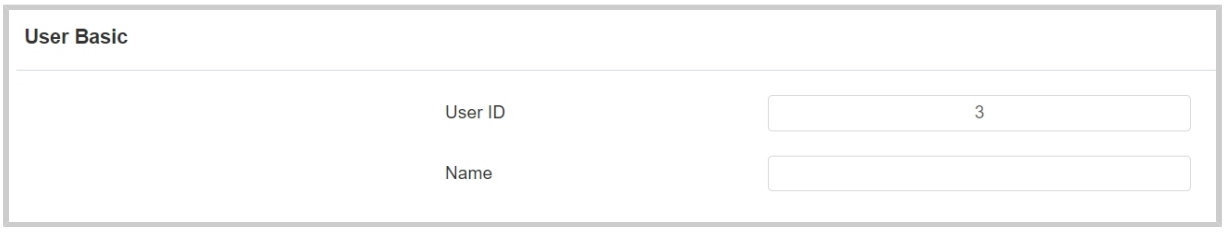
User-specific Access Methods

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

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

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





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

Unlock by Private PIN

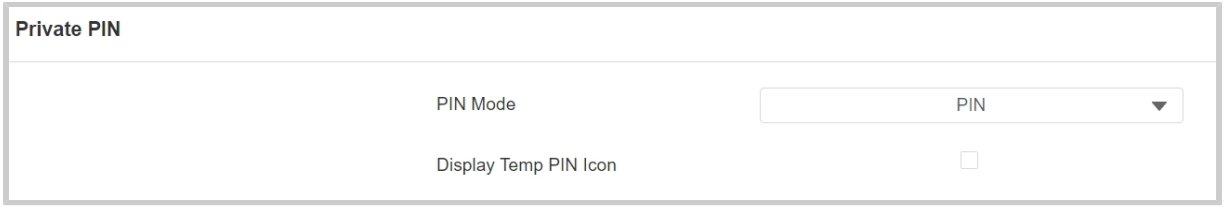
On the **Directory > User > +Add** interface, scroll to the **Private PIN** section.



- **Code**: Set a 2-8 digit PIN code solely for the use of this user. Each user can only be assigned a single PIN code.

You can set up the private PIN mode and decide whether to display the temp PIN icon on the PIN code entry screen.

Go to the **Access Control > PIN Setting > Private PIN** interface for setup.



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

- **Display Temp PIN Icon**: When enabled, the temp PIN icon will be displayed on the PIN code entry screen.

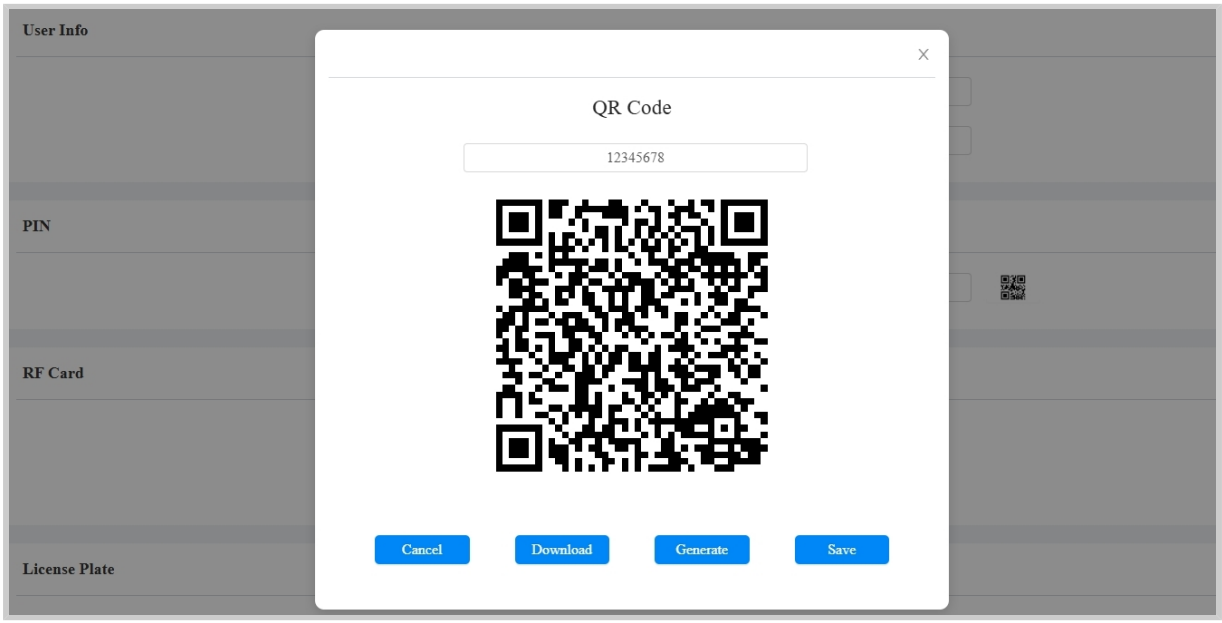
Unlock by QR Code

The device supports scanning on-premise-generated and SmartPlus Cloud-generated QR codes.

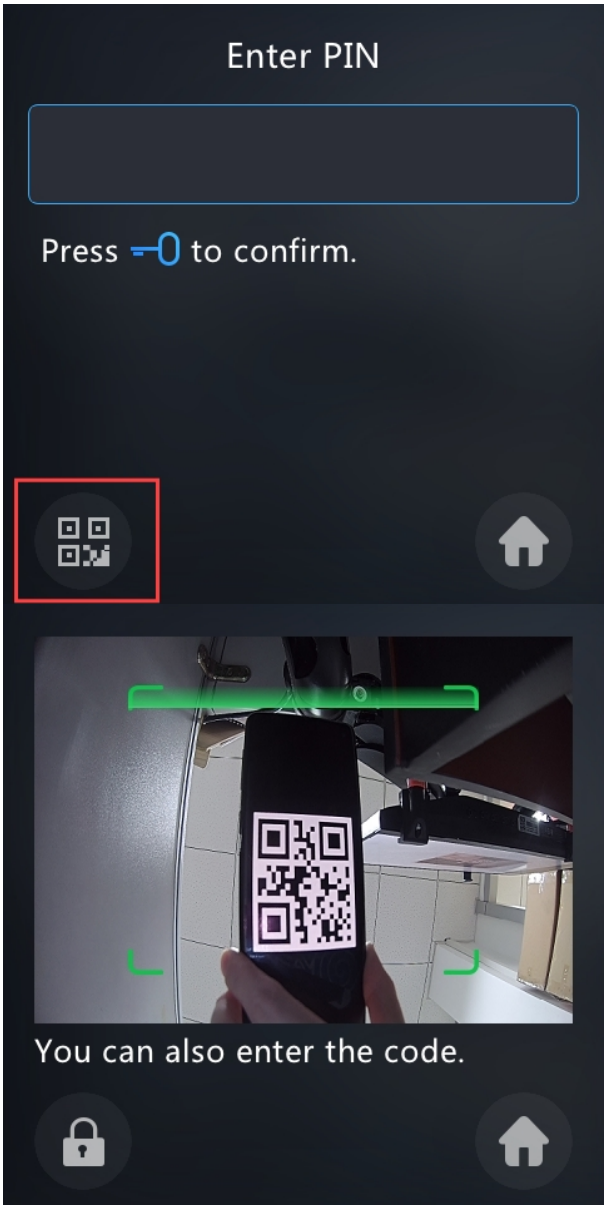
To generate a QR code on the web, go to the **Directory > User > +Add** interface, scroll to the PIN section. Click the QR code icon .



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

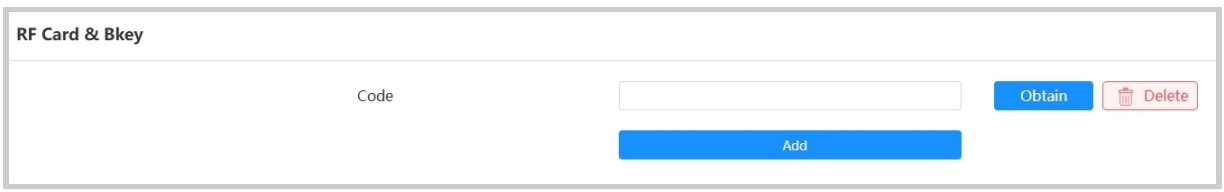


- **Cancel**: Click to return to the user editing interface. The QR code and the PIN code will not be saved.
- **Download**: Click to save the QR code to your PC.
- **Generate**: Click to generate another QR code and PIN code.
- **Save**: Click to return to the user editing interface and save the codes.



Unlock by RF Card/Bkey

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

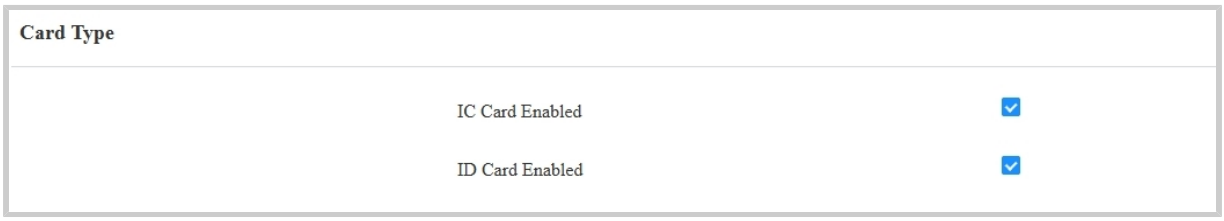


- **Code**: The card number that the card reader reads.

Note:

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

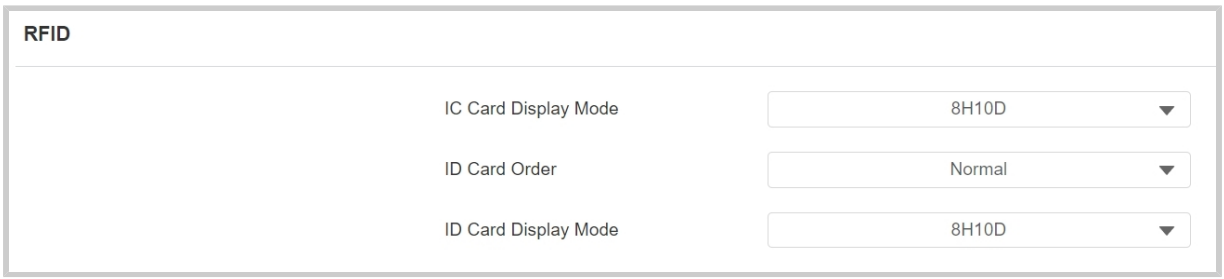
You can enable and disable the use of RF cards on the **Access Control > Card Setting** interface.



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.



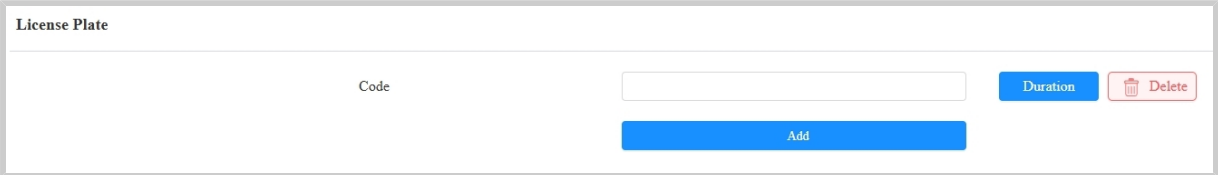
- **IC/ID Card Display Mode**: Set the card number format from the provided options.
- **ID Card Order**: Set the ID card reading mode between Normal and Reversed.

Unlock by License Plate

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

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

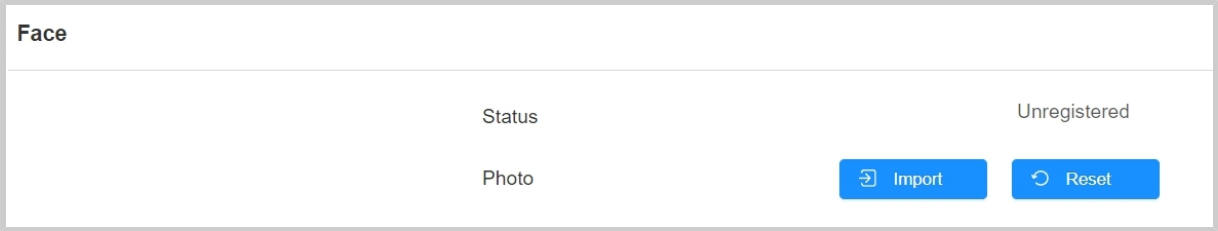
To assign the license plate to a user, find the **License Plate** part on the **Directory > User > +Add** interface.



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

Unlock by Facial Recognition

On the **Directory > User > +Add** interface, scroll to the **Face** section. Click **Import** to upload the picture and Reset to **remove** it.

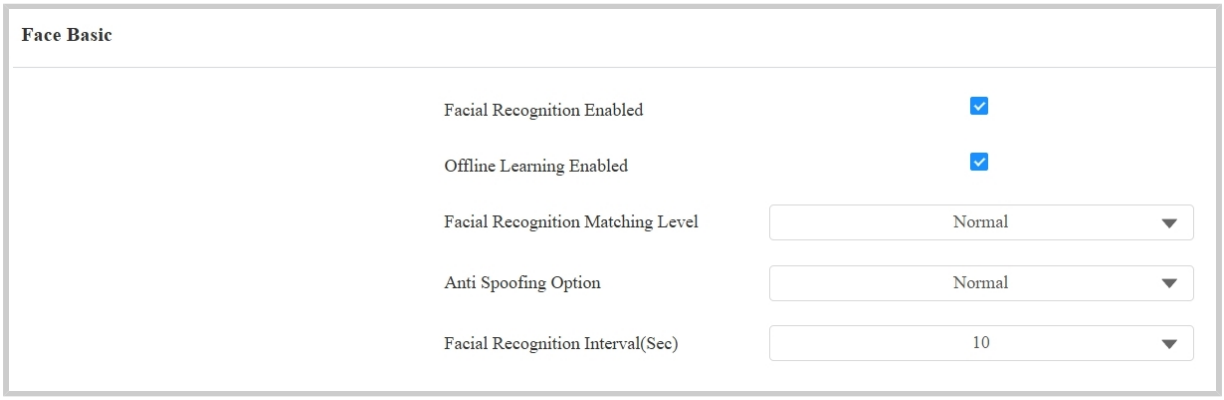


> **Note**
>
> Max File Size: 2M, Format: .jpg/.png.

Facial Recognition Settings

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

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



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

- Low: Allow slight differences from the uploaded face data, with little face coverage.

- Highest: Require the face to be identical to the uploaded one, with minimal or no covering.

- The other two levels are in between.

- **Anti-Spoofing Option**: Set how strict the system is in preventing fake faces.

- Close: Disable the facial anti-spoofing function. Facial verification can be passed using non-living substitutes for an authorized person's face, such as a photo.

- Highest: The system cannot be fooled by any non-living substitutes for an authorized person's face.

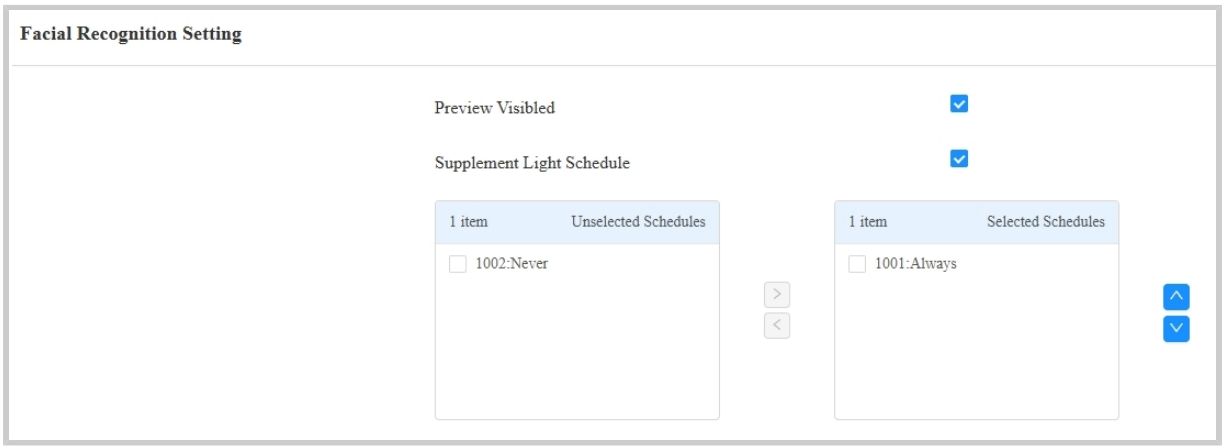
- The other three levels are in between.

- **Facial Recognition Interval**: Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.

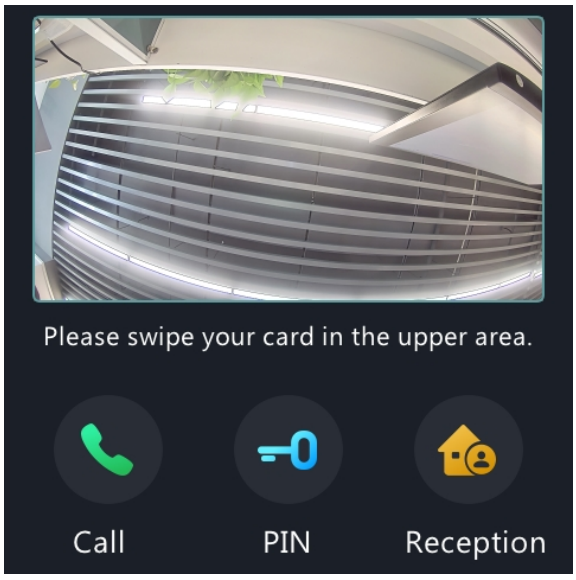
Besides, you can set up the facial recognition supplement light and preview frame on the **Setting > Key/Display > Facial Recognition Setting** interface.

The supplement light is used to make recognition easier during a specific time in a dark environment.

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



- **Preview Visible**: Disabled by default and only available in the **Default** theme. When enabled, the facial recognition frame will display on the home screen.



- **Schedule**: Enable the schedule by checking and moving it from the left to the right box. To set up a schedule, go to the **Setting > Schedule** interface.

Unlock by Bluetooth

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

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

Unlock via My MobileKey

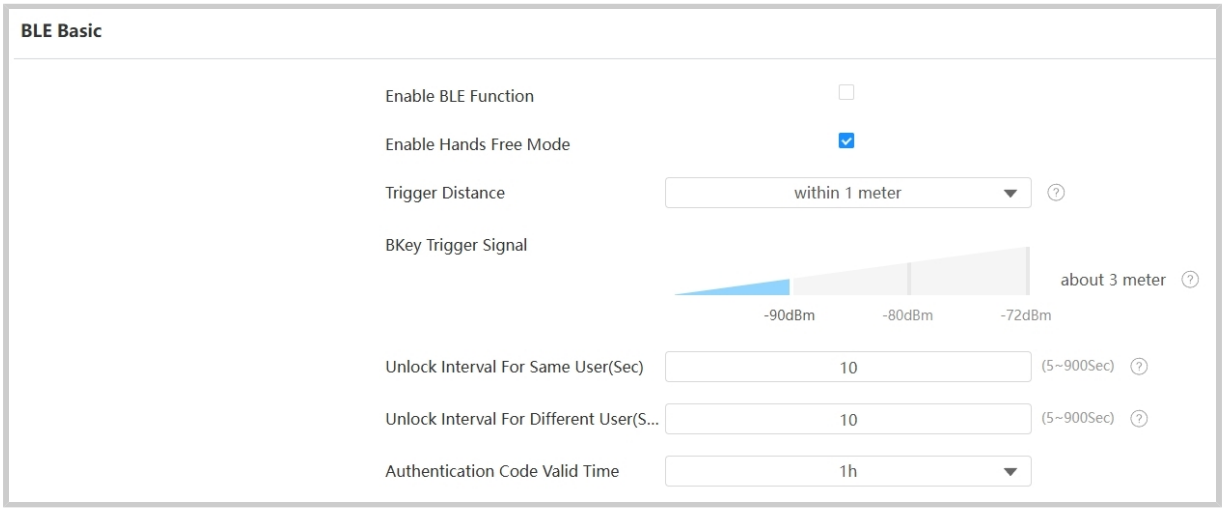
On the **Directory > User > +Add** interface, scroll to the **BLE Setting** section.



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

Bluetooth Unlock Settings

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



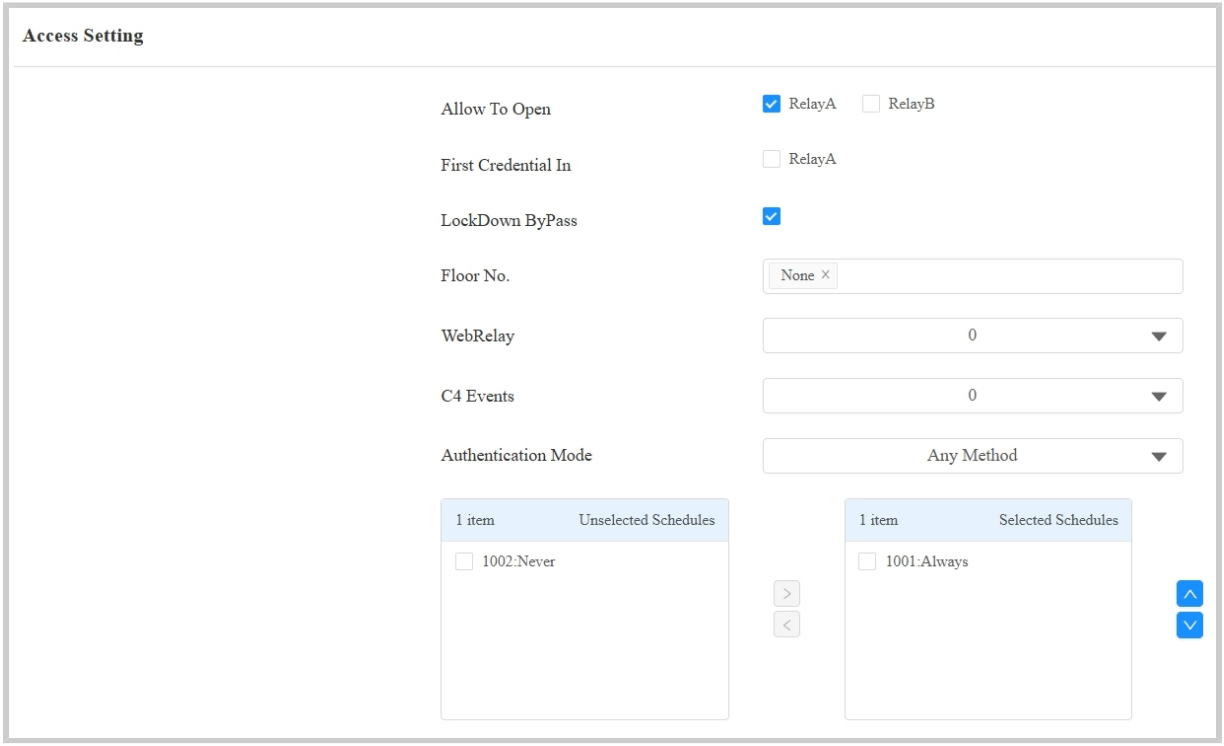
- **Enable Hands Free Mode**: If enabled, users can gain door access hands-free. If disabled, users have to wave their hands near the device to open doors.
- **Trigger Distance**: Set the triggering distance of the Bluetooth for the door access. You select Within 1 Meter, Within 2 Meters, and Within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

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

Access Setting

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

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



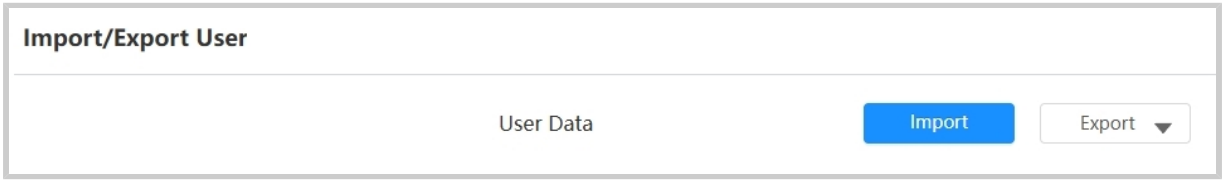
- **Allow To Open**: Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **First Credential In:** This decides whether the user can keep the door open during the scheduled time after activating it.
- **Lockdown Bypass**: This decides whether the user can open the door when the door is locked during the scheduled time.
- **Floor No.** : Specify the accessible floor(s) to the user via the elevator.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **C4 Events**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **Authentication Mode**: Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.
  - **Any Method**: Allow all access methods.
  - **Face + PIN**: Scan the face first, then enter the PIN code.
  - **Face + RF Card**: Scan the face first, then swipe the RF card.
  - **RF Card + PIN**: Swipe the RF card first, then enter the PIN code.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
  - **Always**: Allows door opening without limitations on door open counts during the valid period.
  - **Never**: Prohibits door opening.

Import/Export User Data

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

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

To set it up, go to the **Directory > User > Import/Export User** interface. The device allows adding 20,000 users.



Note

- The import file supports TGZ or CSV format.
- The export file is in XML or CSV format.

Mifare Card

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



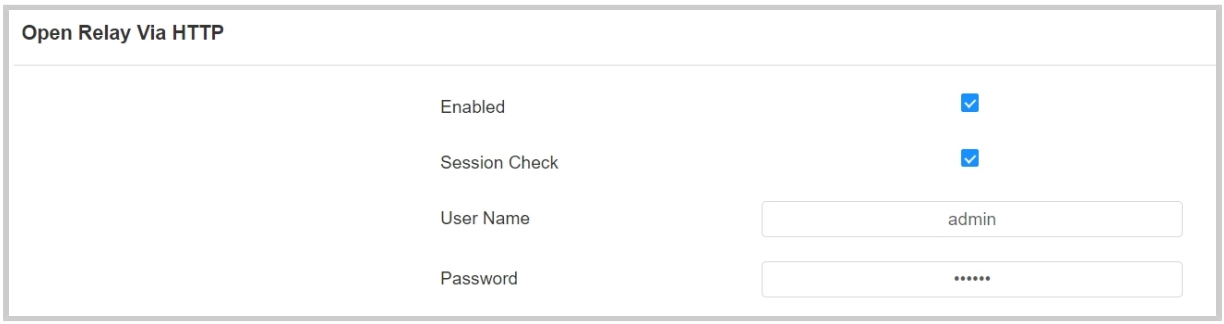
- **Type**: There are four options: **None, Classic**, **Plus**, and **DESFire**.

- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
  - **Key Type**: The authentication key type used to read the Mifare Classic card
  - **Data Offset**: The starting byte position from which card data is read. The default is 0.
  - **Data Length**: The number of valid data bytes to read from the card. The default is 4.
- **Plus**: There are three block choices. The device can read the encrypted data in SL1 and SL3.
  - **Block**: The block number where the encrypted data is located.
  - **SL3**: The key number within 32 bits.
- **DesFire**:
  - **App ID**: A 6-digit hexadecimal number
  - **File ID**: The ID of the encrypted file of the app, which can be a number from 0 to 16.
  - **Crypto**: The encryption method, either AES or DES.
  - **Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.
  - **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

You can unlock the door remotely without approaching the device physically for door entry by typing in the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for door entry.

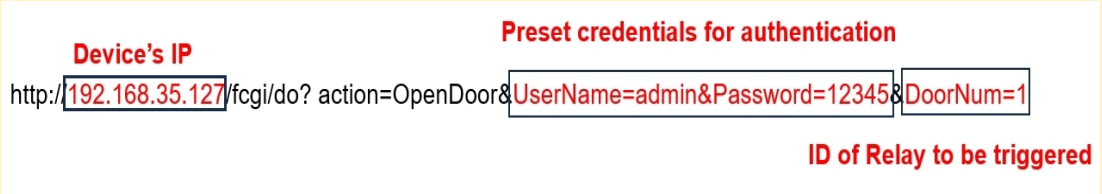
To set it up, go to **Access Control > Relay > Open Relay Via HTTP** interface.



- **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 for relay triggering.



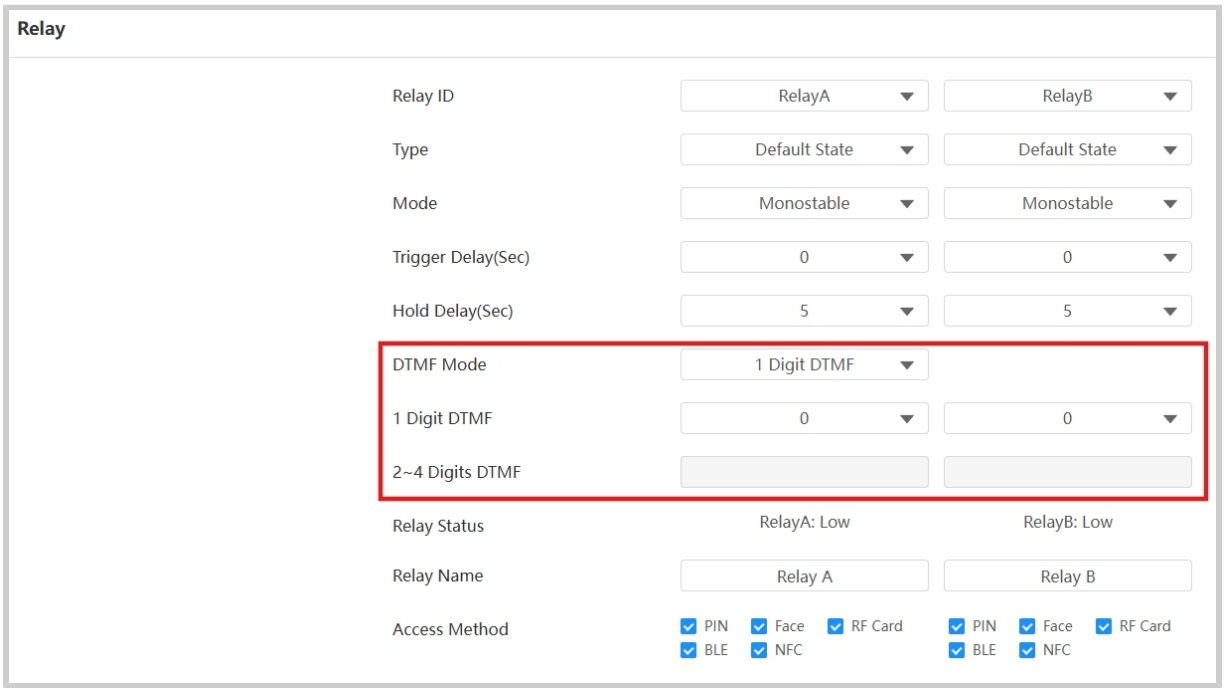
Note

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

Unlock by DTMF Code

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

To configure DTMF codes, go to **Access Control > Relay** interface.

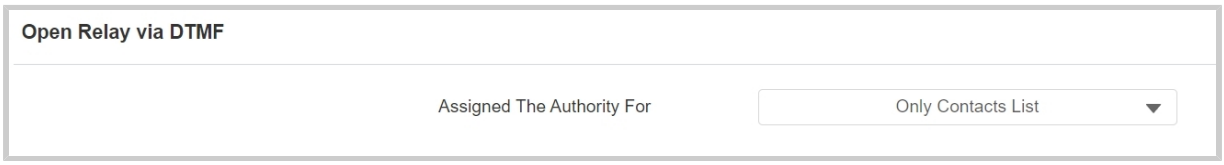


- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digit DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

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

DTMF White List

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



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

DTMF Data Transmission

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

DTMF Type Differences:

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

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

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



- **Type:** Select from the available options based on the specific DTMF transmission type of the third-party device 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.

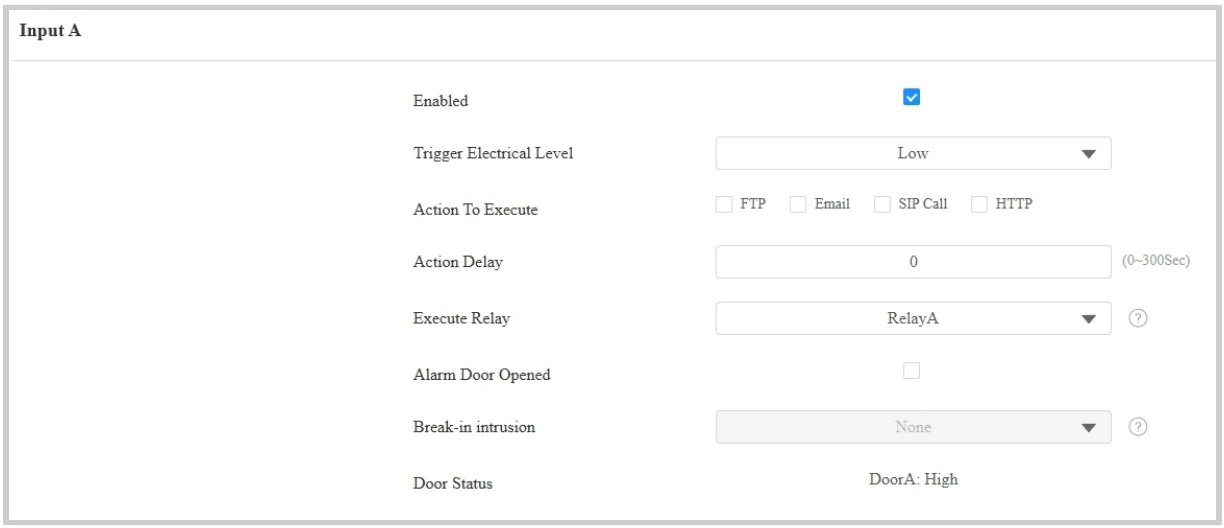
- **Payload**: Set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

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.

To set it up, navigate to the **Access Control > Input** interface.



- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at a low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - **FTP**: Send a screenshot to the preconfigured FTP server.
  - **Email**: Send a screenshot to the preconfigured Email address.
  - **SIP Call**: Call the preset number upon the trigger.
  - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.

- **HTTP URL**: Enter the HTTP URL 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.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Alarm Door Opened**: If enabled, when the door-opening time exceeds a limit, an alarm will be triggered.
  - **Door Opened Timeout**: The door-opening time limit.
- **Break-in Intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. It is incompatible with the Execute Relay feature. Click here to learn more about this feature.
- **Door Status**: Display the status of the input signal.

Configure Access Methods on the Device

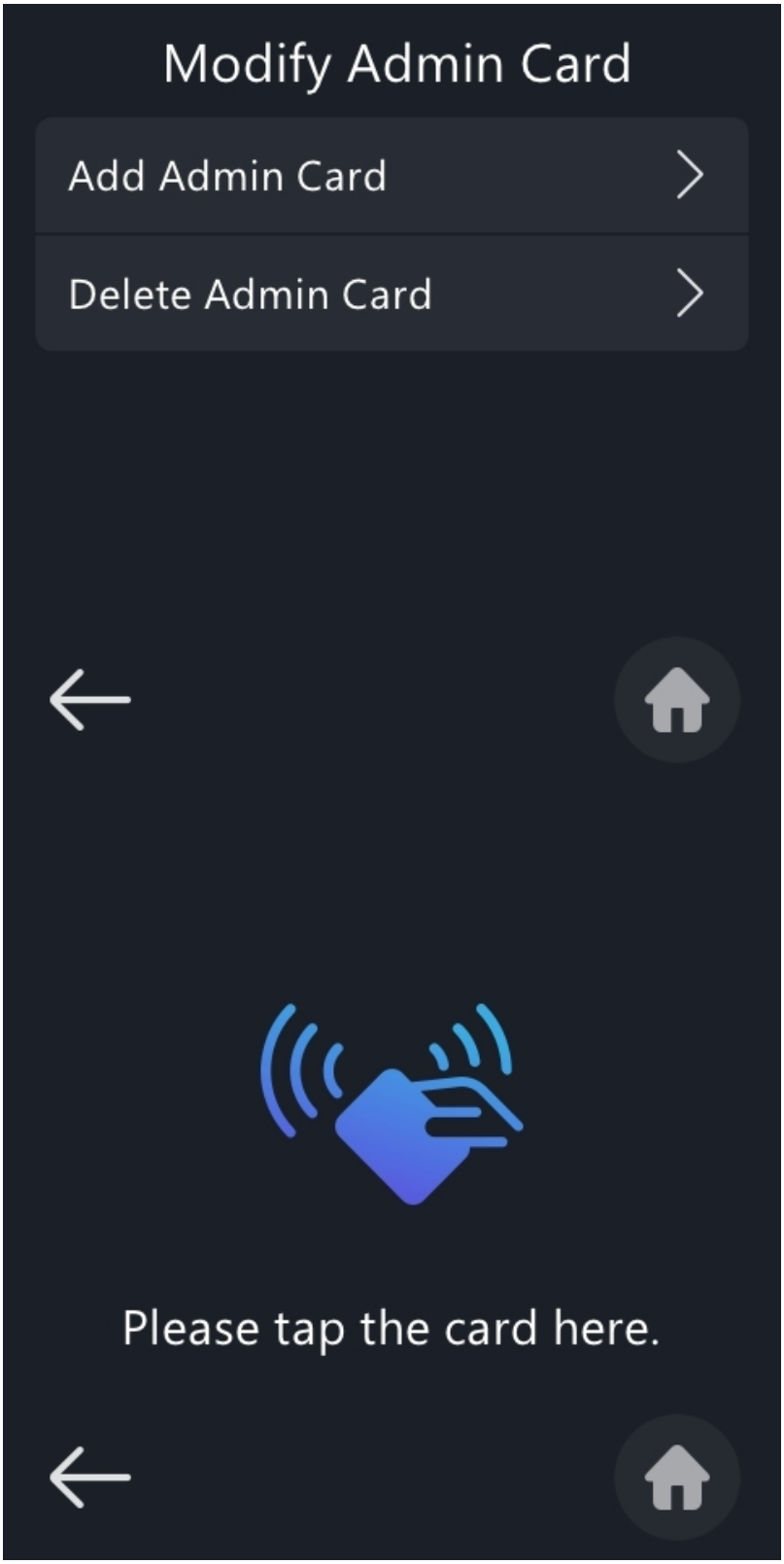
Property managers can set up the public PIN code, private PINs, and users' RF cards on the device through an admin card.

Admin Card

The admin card grants property managers permission to manage access methods on the device.

To add or delete an admin card, access the device's admin settings first by entering the system password. The default is 2396.

Navigate to the **Advanced Settings > Admin Access > Modify Admin Card** screen.

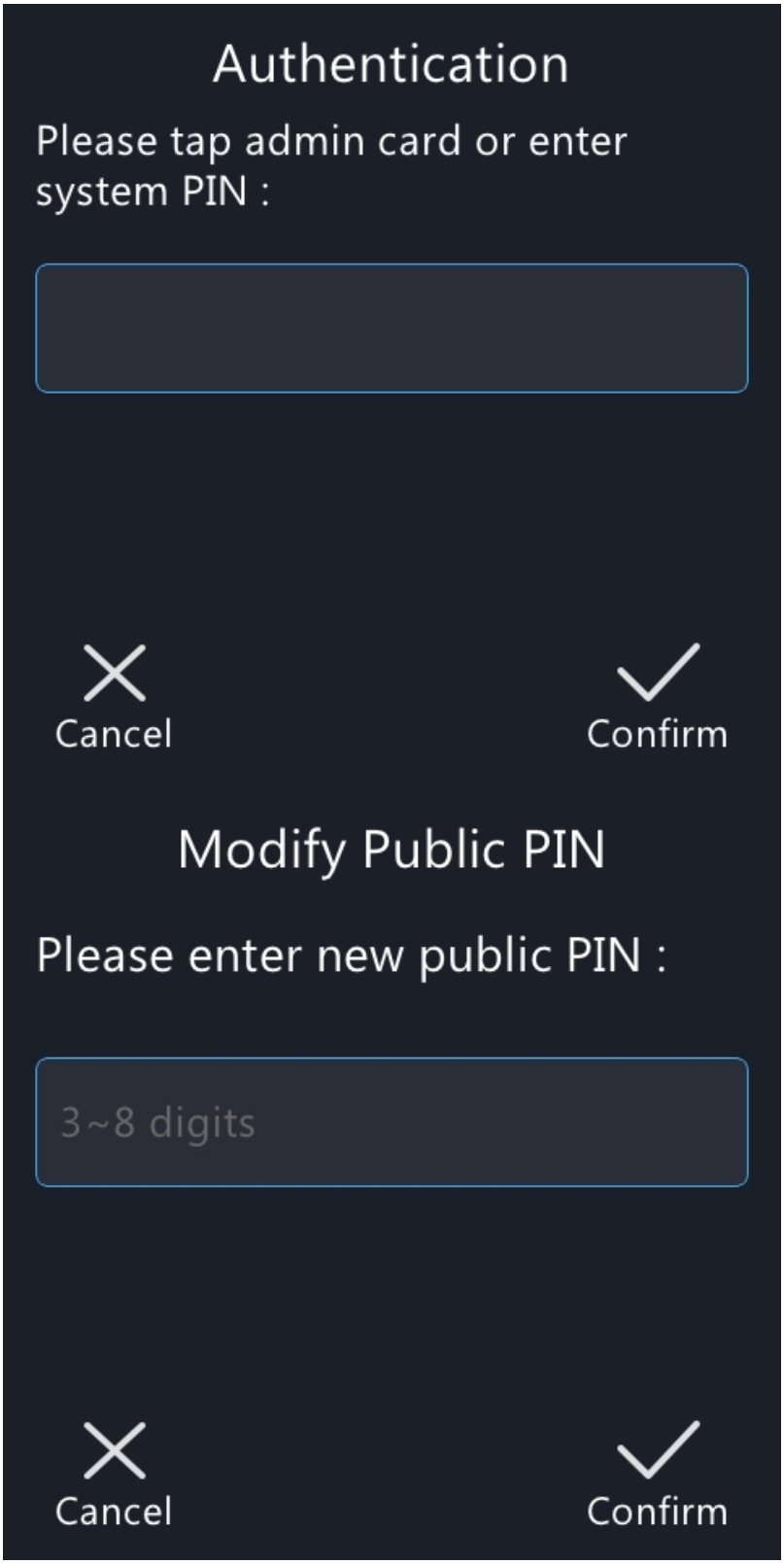

Modify Admin Card
Add Admin Card
Delete Admin Card
Please tap the card here.

Public PIN

The public PIN can be shared by residents in the same building or complex for door opening.

To set it up, go to the **Access Method Settings > Modify Public PIN** screen by entering the service password. The default is 3888.

Property managers are required to tap the admin card or enter the system PIN(2396 by default) first.

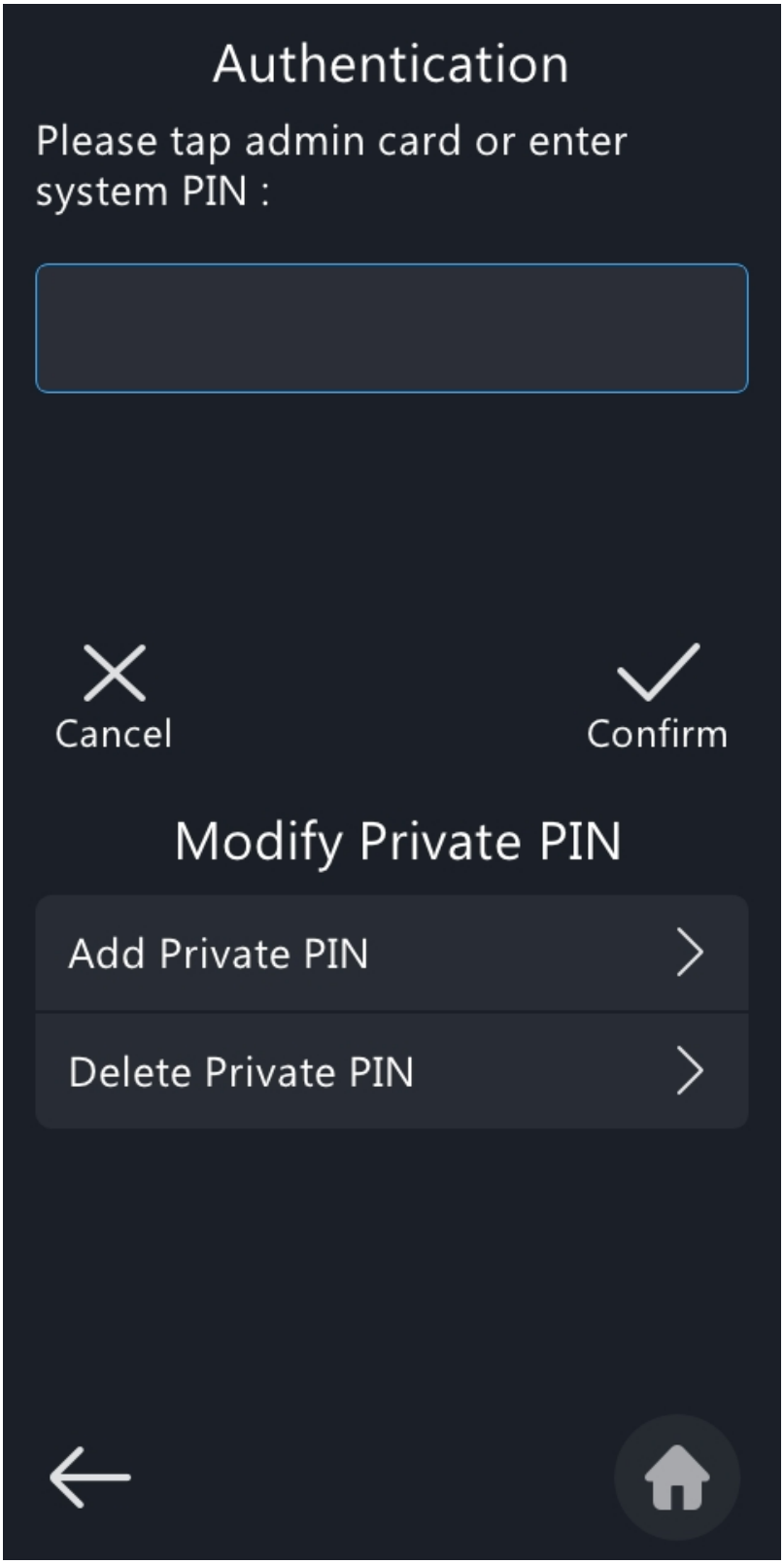

Authentication
Please tap admin card or enter system PIN :
Cancel
Confirm
Modify Public PIN
Please enter new public PIN :
3~8 digits
Cancel
Confirm

Private PIN

The private PIN is unique to each user. After adding a private PIN code, a user will be created automatically whose information can be modified on the device's web interface.

To set it up, go to the **Access Method Settings > Modify Private PIN** screen by entering the service password. The default is 3888.

Property managers are required to tap the admin card or enter the system PIN(2396 by default) before adding or deleting PINs.

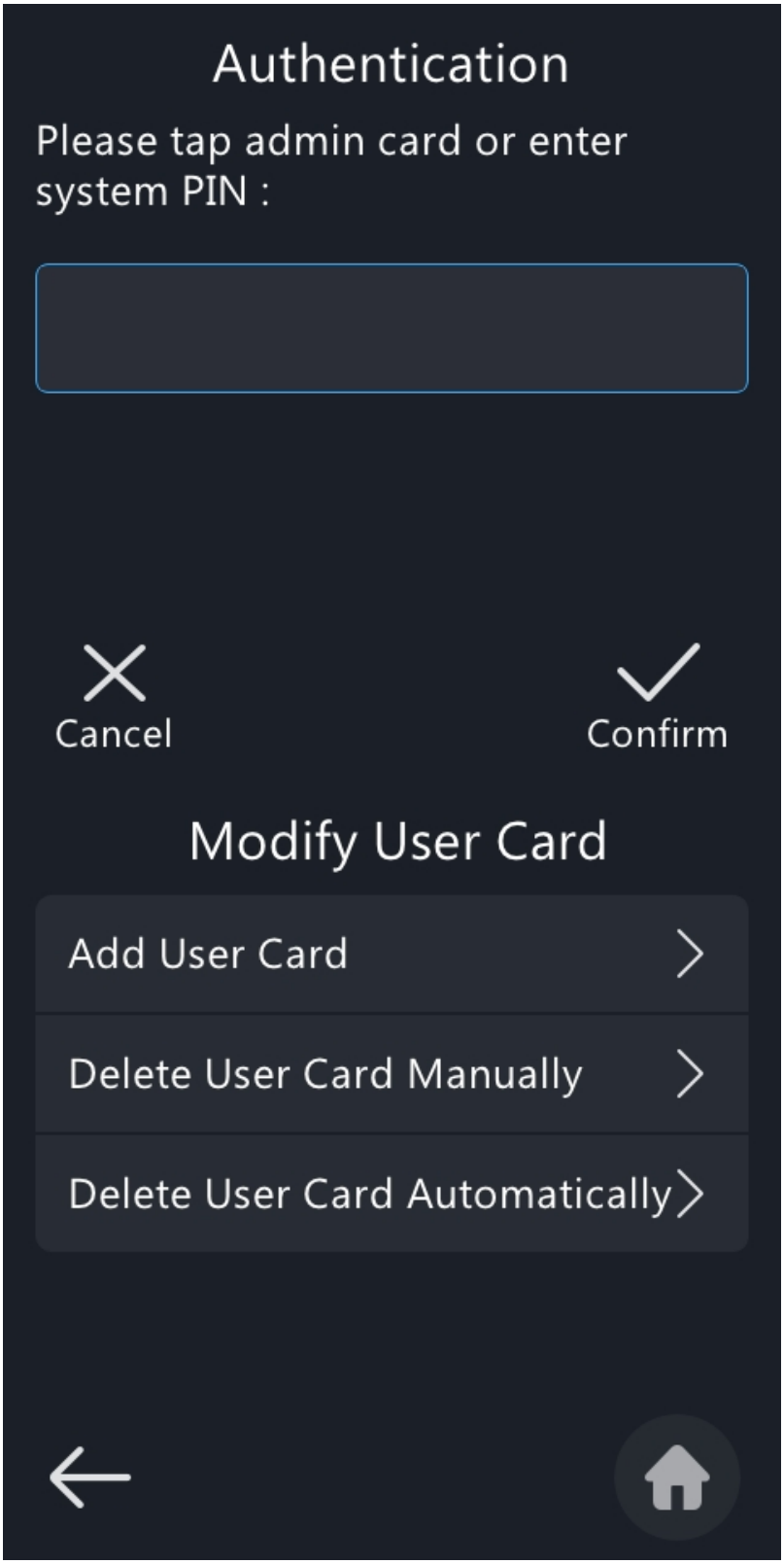

Authentication
Please tap admin card or enter system PIN :
Cancel
Confirm
Modify Private PIN
Add Private PIN
Delete Private PIN

RF Cards

The RF card is assigned to a user for door opening. After adding a card, a user will be created automatically whose information can be modified on the device's web interface.

To set it up, go to the **Access Method Settings > Modify User Card** screen by entering the service password. The default is 3888.

Property managers are required to tap the admin card or enter the system PIN(2396 by default) before adding or deleting cards.



- **Delete User Card Manually**: Delete the card by finding and tapping it in the list.

- **Delete User Card Automatically**: Delete the card by directly placing it on the card reader area.

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.

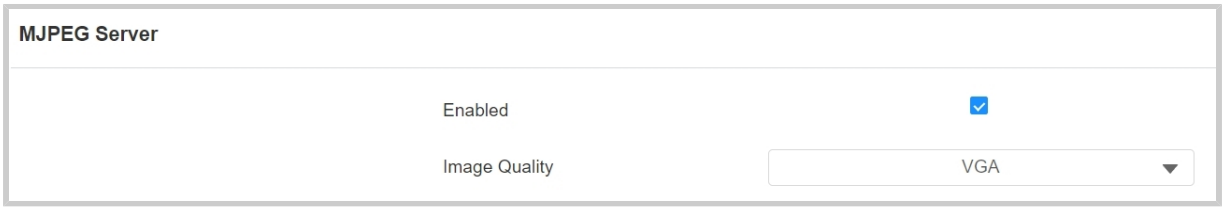
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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.

To enable the MJPEG function, go to the **Surveillance > MJPEG** interface.

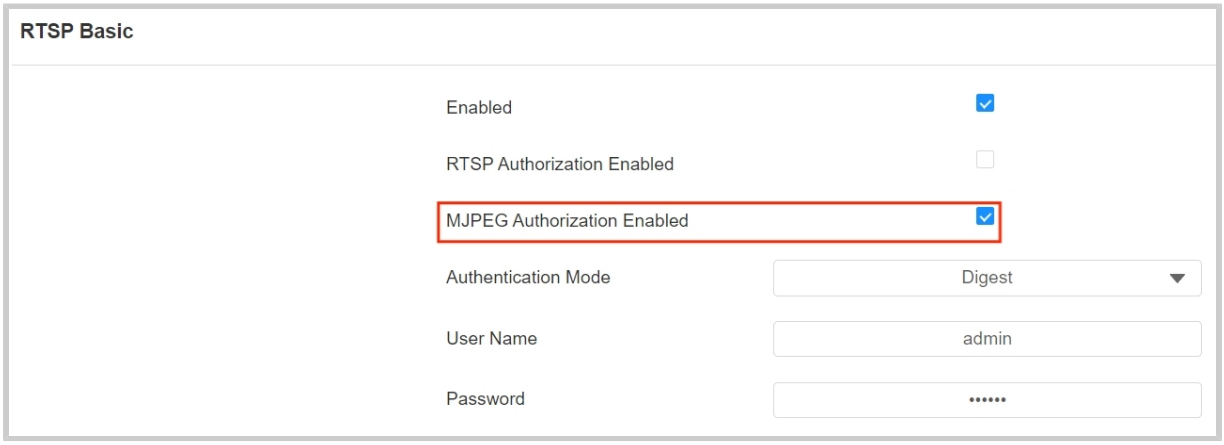


- **Enabled**: Entering the specific URL into the browser can access either an image or a video from the camera.

> **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.

- **Image Quality**: Specify the image resolution, varying from the lowest QCIF(176x144 pixels) to the highest 720P(1920x1080 pixels).

To set up MJPEG authentication, navigate to **Surveillance > RTSP > RTSP Basic** interface.



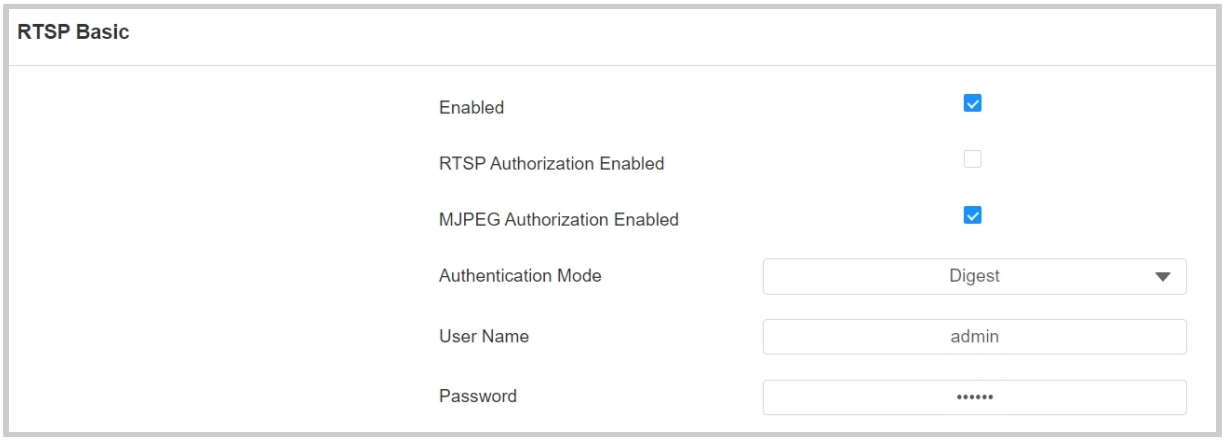
- **MJPEG Authorization Enabled**: Once enabled, accessing the door phone's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username, and RTSP Password.

RTSP Stream Monitoring

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

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

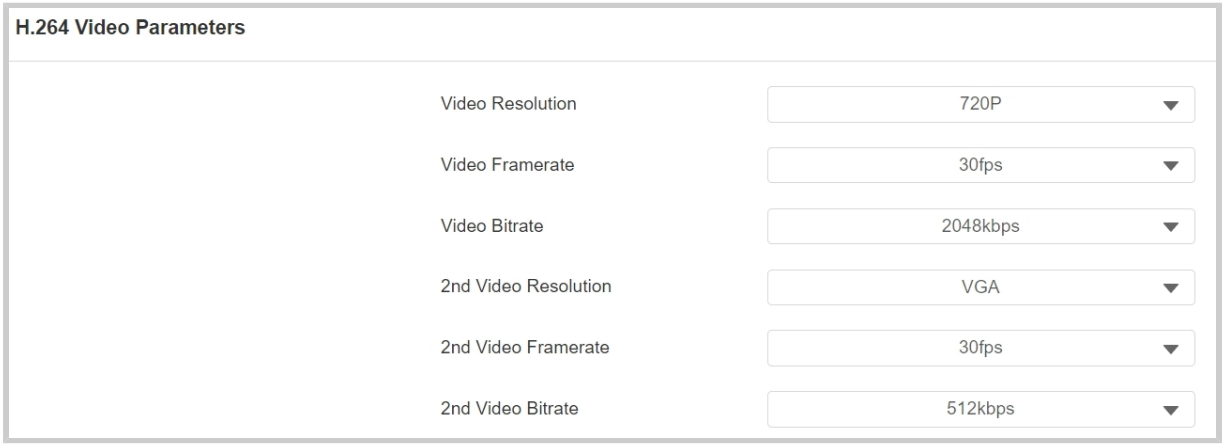
To set it up, navigate to the **Surveillance > RTSP** interface.



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

RTSP Stream Setting

The RTSP stream can use H.264 as the video codec. You can adjust the video resolution, bitrate, and other settings on the web **Surveillance > RTSP > H.264 Video Parameters** interface.



- **Video Resolution**: Specify the image resolution, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Framerate(fps)**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Video Bitrate(Kb/Sec)**: 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 Framerate(fps)**: Set the frame rate for the second video stream channel.
- **2nd Video Bitrate(Kb/Sec)**: Set the bit rate for the second video stream channel. The default is 512 kbps.

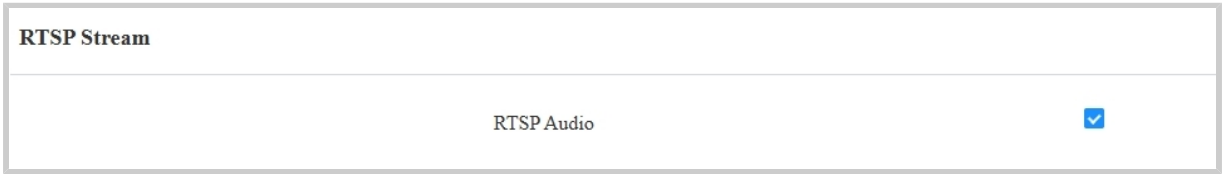
Tip

To view the audio and video stream using RTSP:

- First channel: rtsp://Device's IP/live/ch00_0
- Second channel: rtsp://Device's IP/live/ch00_1

RTSP Audio

You can set whether the RTSP stream has sound on the **Surveillance > RTSP > RTSP Stream** interface.

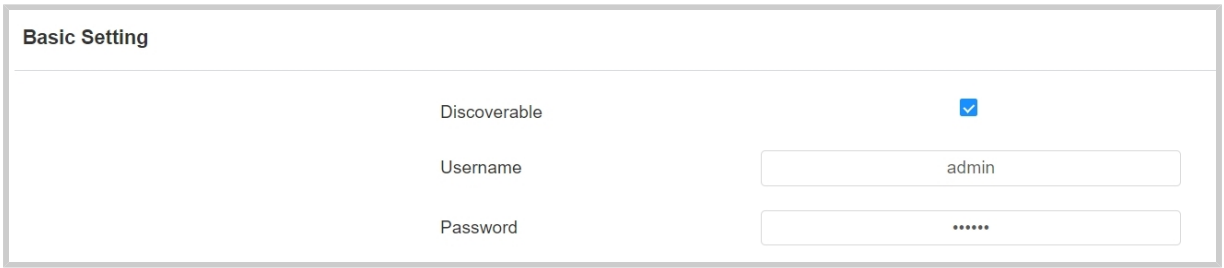


ONVIF

You can access the real-time video from the device's camera using the Akuvox indoor monitor or other third-party devices like Network Video Recorder(**NVR**). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

Click here to view an example of using the ONVIF feature: the integration with Uniview NVR System.

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



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

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

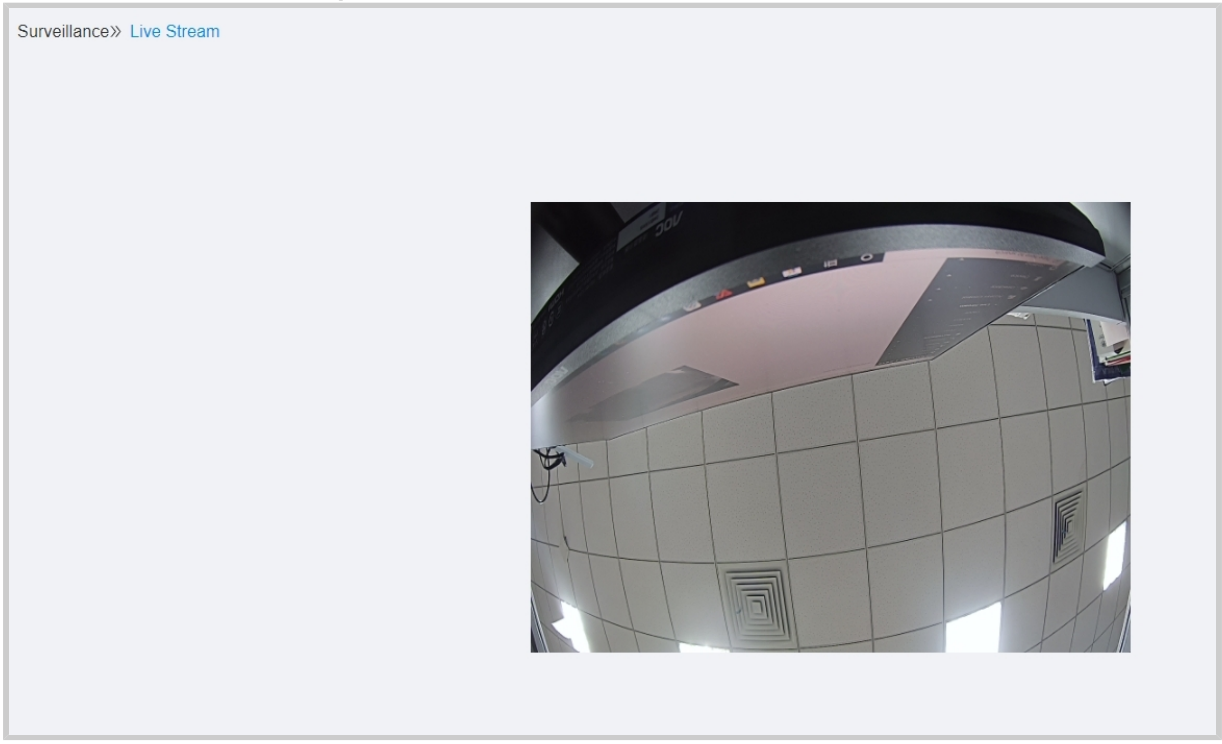
Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.



Live Stream

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

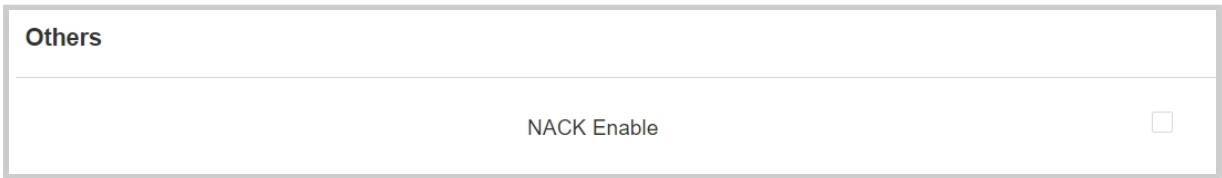
For the device, the path is **Surveillance > Live Stream** interface.



NACK

Negative Acknowledgment (**NACK**) indicates a failure or error in data transmission or processing. It is used to request retransmission or signal the failure to the sender for ensuring data integrity.

To enable NACK, navigate to the web **Intercom > Call Feature > Others** interface.



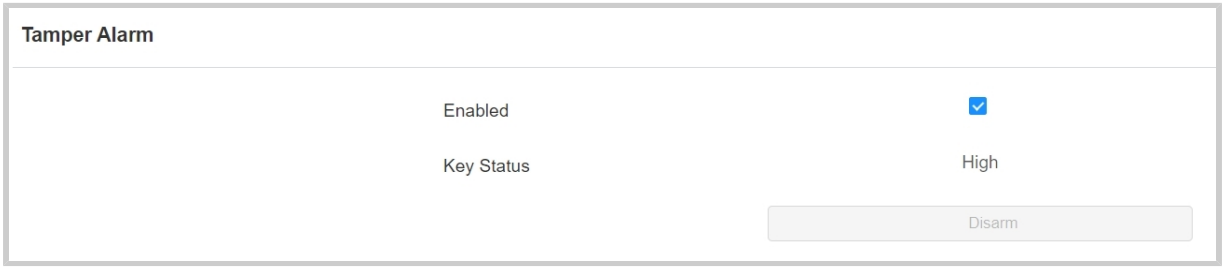
Security

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. Click **Disarm** to clear the alarm.



- **Key Status**: The tamper alarm will not be triggered unless the key status is shifted from **Low** to **High** status.

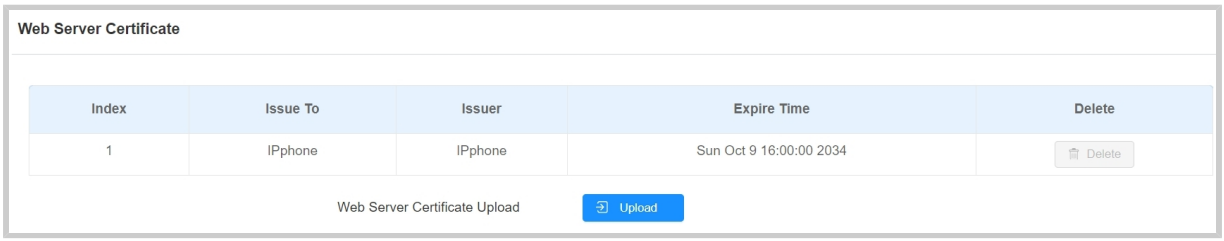
Client Certificate Setting

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.

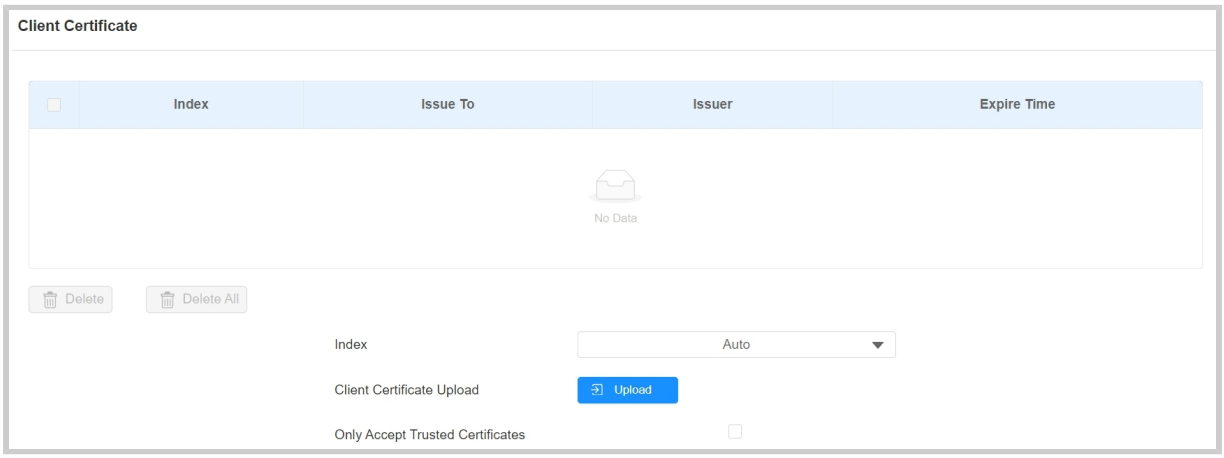
Upload the web server certificate on the web **System > Certificate** interface.



Client Certificate

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

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



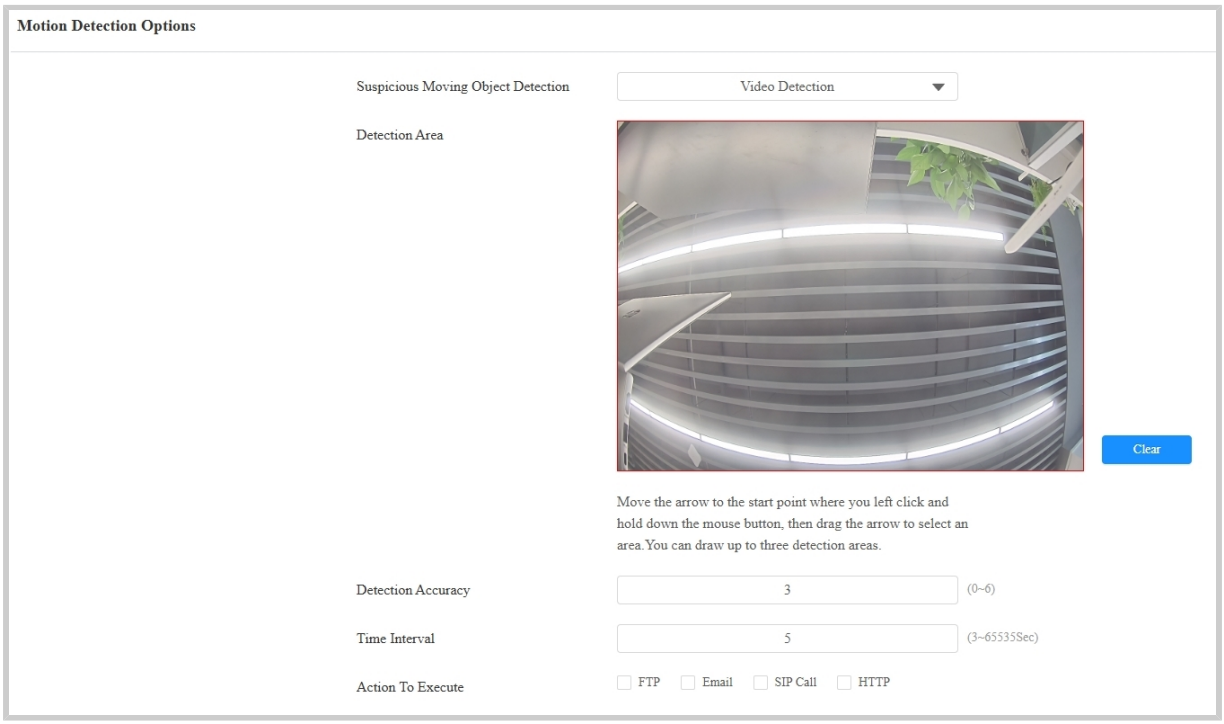
- **Index:**
  - Auto: The uploaded certificate will be displayed in numeric order.
  - 1 to 10: The uploaded certificate will be displayed according to the value selected.
- **Upload:** Click Choose File to upload the certificate.

- **Only Accept Trusted Certificates:** When enabled, as long as the authentication succeeds, the doorphone will verify the server certificate based on the client certificate list. If you select Disabled, the doorphone will not verify the server certificate, no matter whether the certificate is valid or not.

Motion Detection

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

Set up motion detection on the **Surveillance > Motion** interface.



- **Suspicious Moving Object Detection:** Select Video Detection to enable video-based motion detection during the monitoring of the suspicious moving object. Enter the username and password set in the RTSP interface before

- **Detection Area**: Click and hold the mouse button to select up to three detection areas.
- **Detection Accuracy**: The detection sensitivity. The higher the value, the greater the sensitivity. The default detection accuracy value is 3.
- **Time Interval:** Determine how to delay and trigger motion detection.
  - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.
  - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
  - The default interval is 10 seconds.
- **Action To Execute**: Set the desired actions that occur when suspicious movement is detected.
  - **FTP**: Send a screenshot to the preconfigured FTP server.
  - **Email**: Send a screenshot to the preconfigured Email address .
  - **SIP Call**: Call the preset number upon trigger.
  - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

Scroll down, and you can set the motion detection schedule.



Security Notification

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

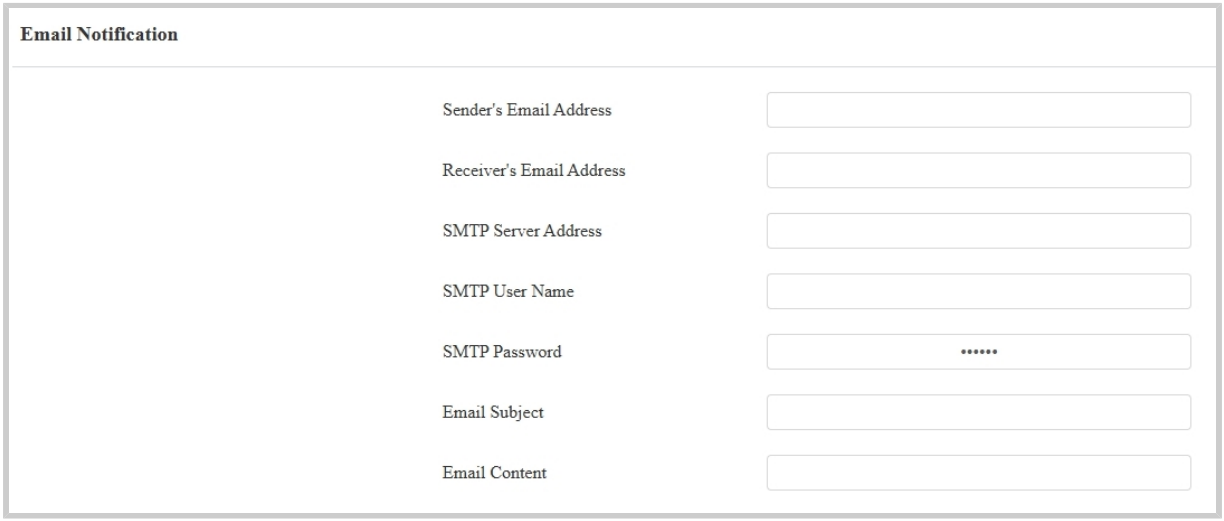
To set up security notifications, go to **Setting > Action** interface.

Email Notification

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

Click here to view how to set this feature up.

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



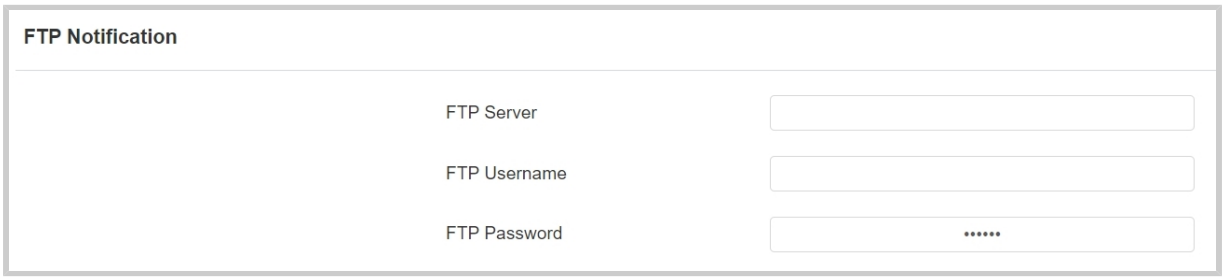
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

FTP Notification

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

Click here to view the configuration steps.

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

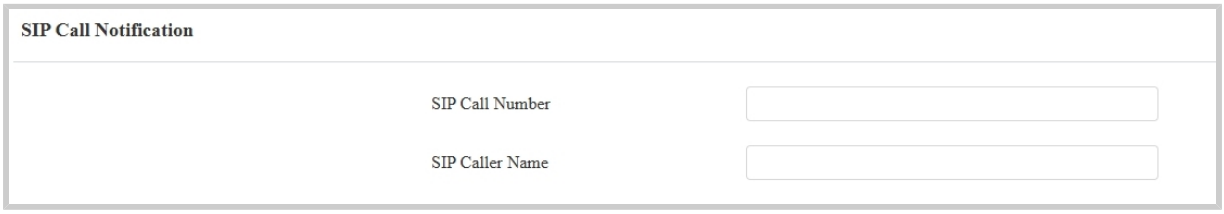


- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP Username**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

SIP Call Notification

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

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



Action URL

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

Akuvox Action URL:

No	Event	Parameter format
1	Make Call	$remote
2	Hang Up	$remote
3	Relay Triggered	$relay1status
4	Relay Closed	$relay1status
5	Input Triggered	$input1status
6	Input Closed	$input1status
7	Valid Code Entered	$code
8	Invalid Code Entered	$code
9	Valid Card Entered	$card_sn
10	Invalid Card Entered	$card_sn
11	Valid Face Recognition	$unlocktype
12	Invalid Face Recognition	$unlocktype
13	Incoming Call	$call_id $remote

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=$unlocktype
Http://server ip/unlocktype=$unlocktype
Http://server ip/callnumber=$remote:callid=call_id

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

To set it up, go to the **Setting > Action URL** interface.

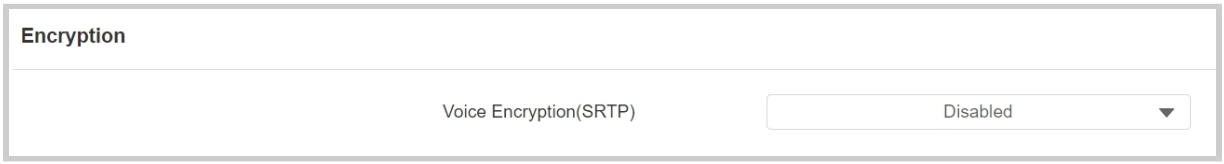
Action URL

Enabled	
Type	GET
Username	
Password	••••••
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayA Closed	
RelayB Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	
InputA Closed	
InputB Closed	
InputC Closed	
Valid Code Entered	
Invalid Code Entered	
Valid Card Entered	
Invalid Card Entered	
Valid Face Recognition	
Invalid Face Recognition	
Break In Alarm A	
Break In Alarm B	
Break In Alarm C	
Incoming Call	

Voice Encryption

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

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



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

User Agent

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

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



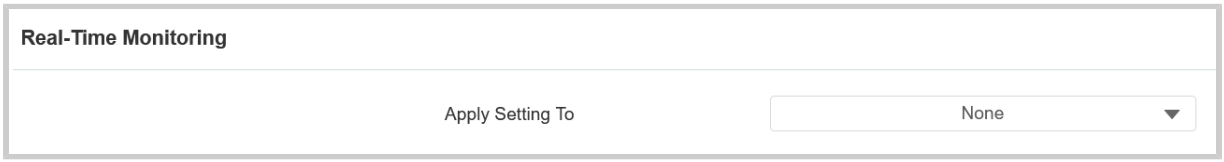
- **User Agent:** Akuvox is by default.

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.

To set it up, go to **System > Security > Real-Time Monitoring** interface.



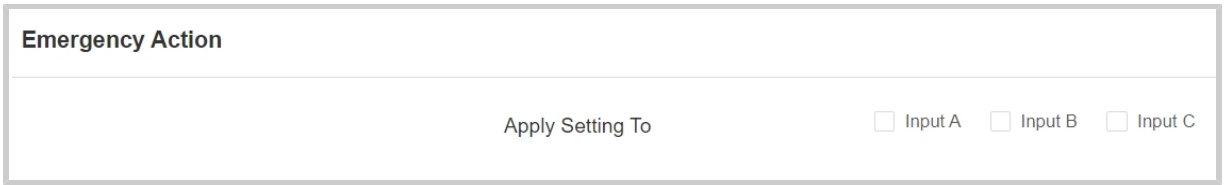
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering the input.
  - **Relay**: The door is opened by triggering the relay.

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.

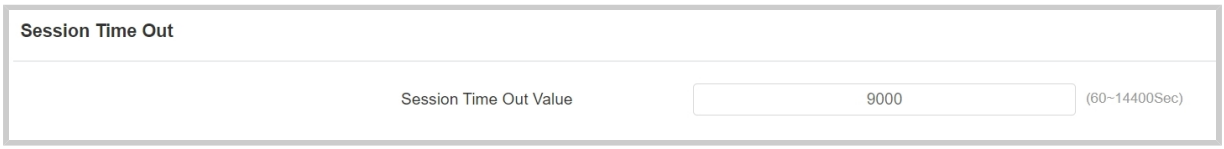
To set it up, go to **System > Security > Emergency Action** interface. Select the Input(s) to be triggered.



Web Interface Automatic Log-out

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

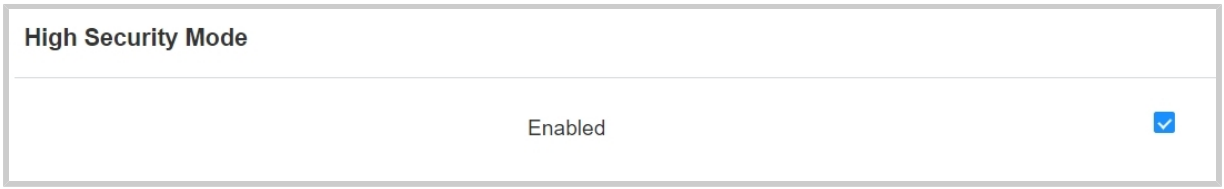
To set it up, go to **System > Security > Session Time Out** interface.



High Security Mode

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

Enable it on the **System > Security > High Security Mode** interface.



Important Notes

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

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

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

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

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

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

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

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

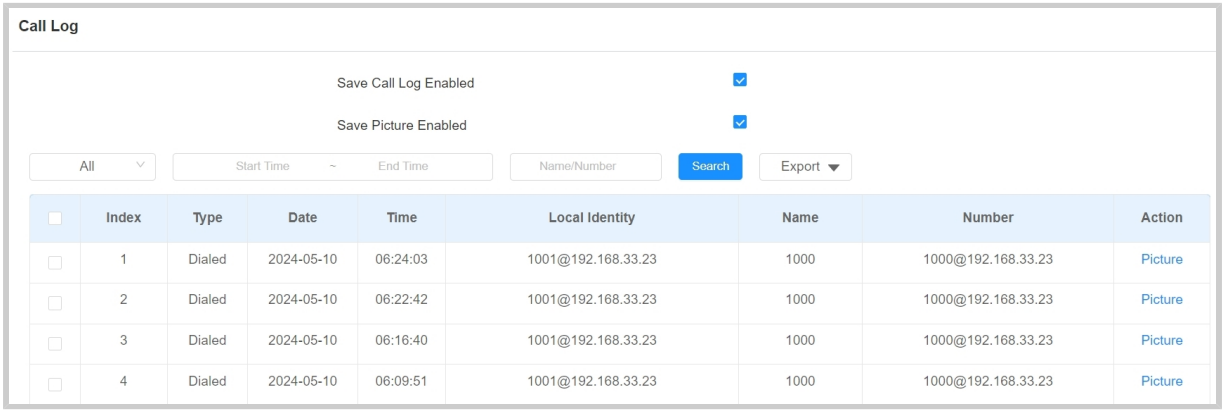
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

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

Check call logs on the web **Status > Call Log** interface. The device supports up to 1,000 call logs, which can be exported in CSV format.

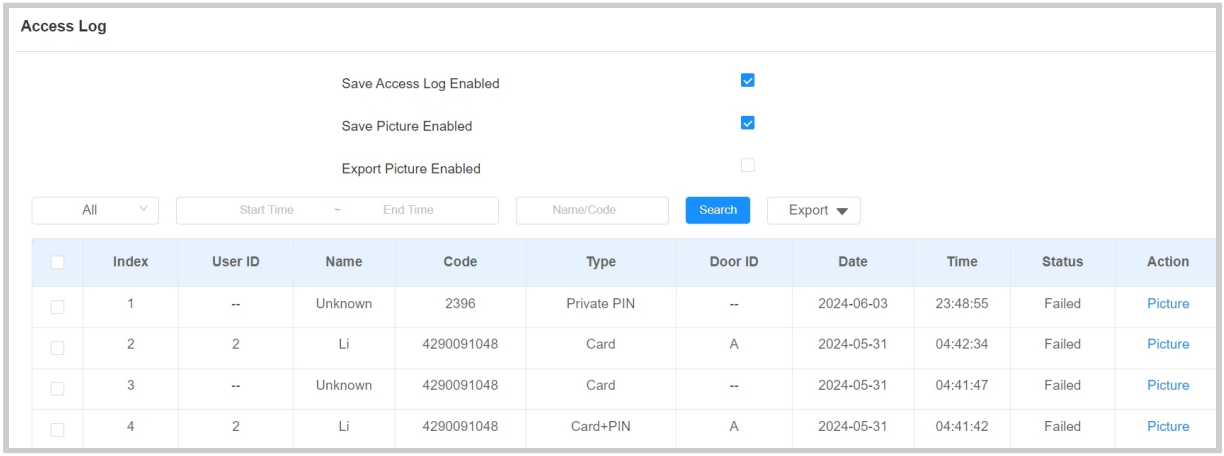


- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.
- **Picture**: Click to view the screenshots during a call.

Door Logs

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

Check door logs on the **Status > Access Log** interface. The device supports up to 5,000 door logs, which can be exported in a CSV or XML file by clicking Export.

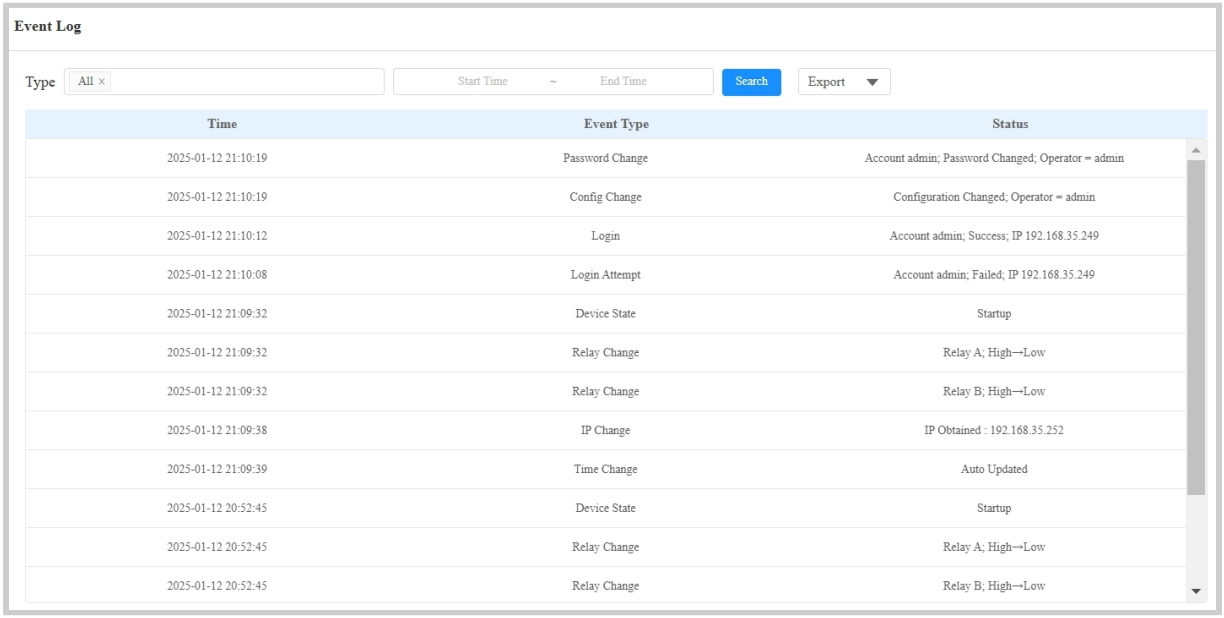


- **Save Picture Enabled**: When enabled, the device will capture pictures of the door opening, and you can click **Picture** in the Action column to view the screenshot.
- **Export Picture Enabled**: Set whether to export the captured images when exporting the door logs.
- **Status:** Display Successful and Failed door-opening records.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card code will be displayed. If the door is opened by an HTTP command, it will be empty.
- **Type:** Display the access methods.
- **Picture**: Click to view the captured image.

Event Logs

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

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

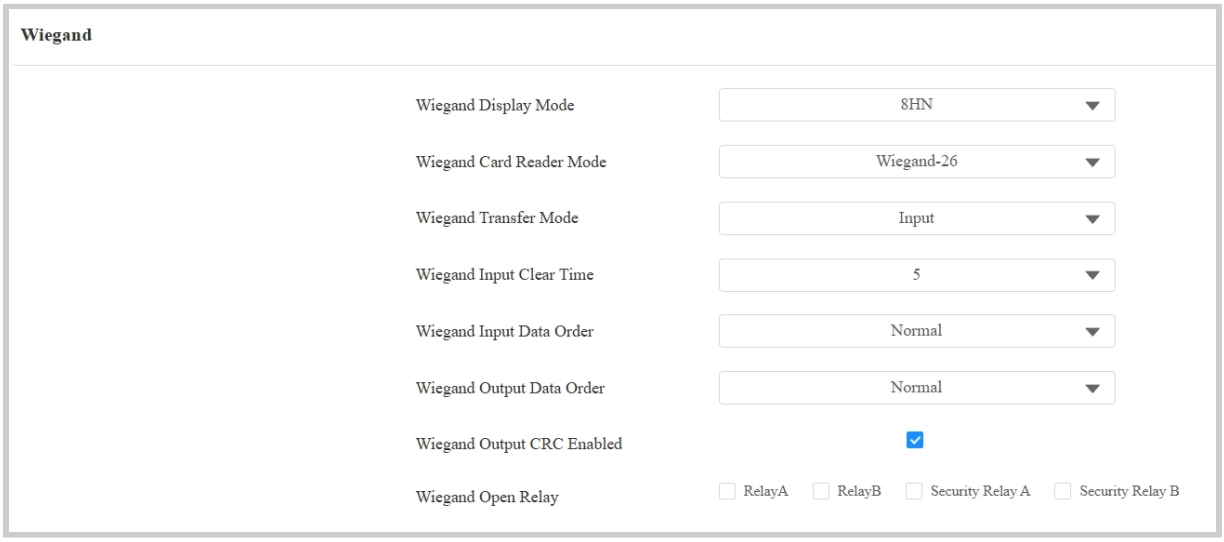


Integration with Third-Party Device

Integration via Wiegand

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

Set it up on the web **Device > Wiegand > 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.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender and can directly output the data, such as card code.
  - **Convert To Card No. Output**: The device serves as a sender and cannot directly output the data, such as the face data.

- **Wiegand Input Clear Time**: When the interval of entering passwords exceeds the time. All entered passwords will be cleared.
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
  For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If **Reversed** is selected, the card data is 0x55 0x44 0x33.
- **Wiegand Output CRC Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **RF Card Verification**: When enabled, the device will verify whether the card is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the door phone screen, but the door can still be opened. When disabled, the door phone will not perform local verification.
- **Wiegand Open Relay**: Check the relay to be triggered through Wiegand.

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 **Convert To Wiegand Output** section.



- **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.



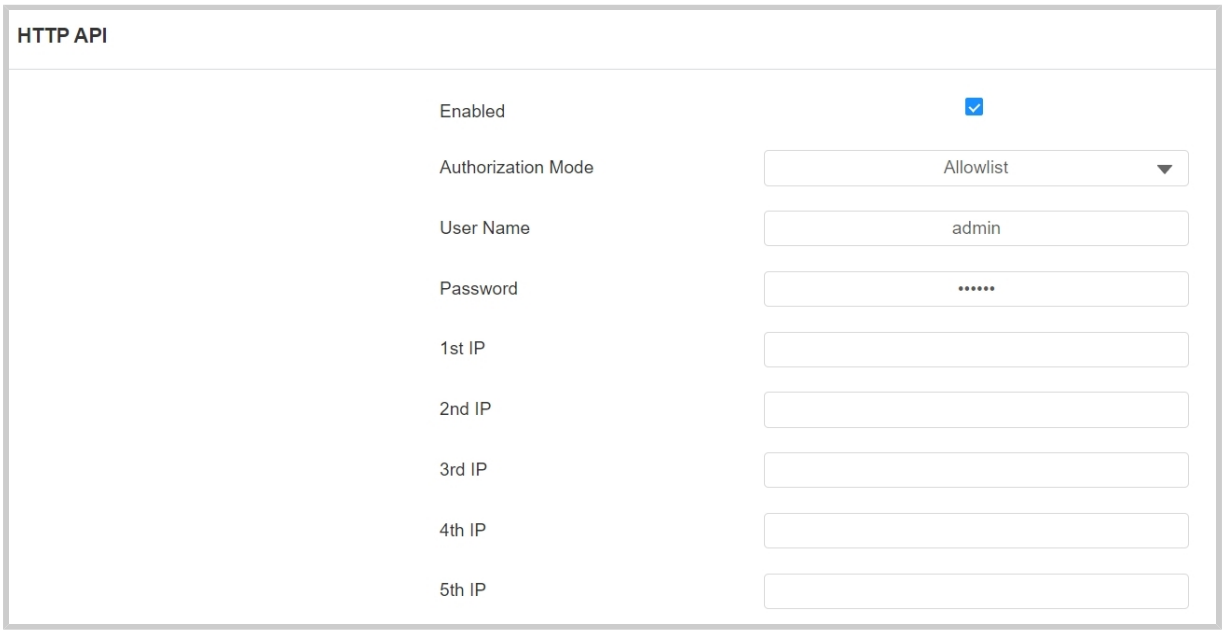
- **Facility Code**: The value ranges from 0 to 255. If filled in, the first two digits of the card number will be replaced by the code. If the code is less than 2 digits, a zero will be automatically added to the card number.

> **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.

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**: It is Digest by default. You are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode the username and password.
- **User Name**: Enter the user name for authentication. The default is admin.
- **Password**: Enter the password for authentication. The default is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

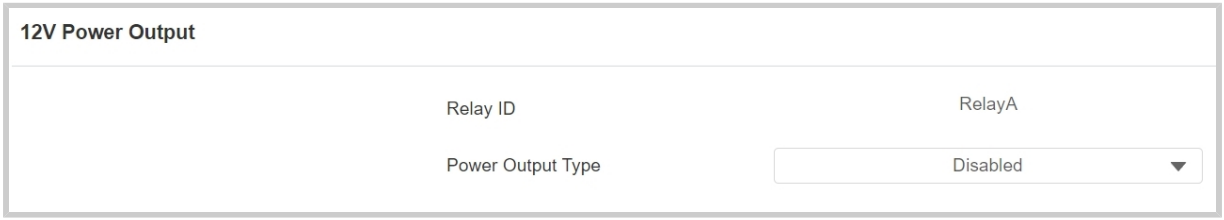
Please refer to the following description for the authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication. The allowlist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encoding method to encode of username and password.
5	Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) in Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

Power Output Control

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

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



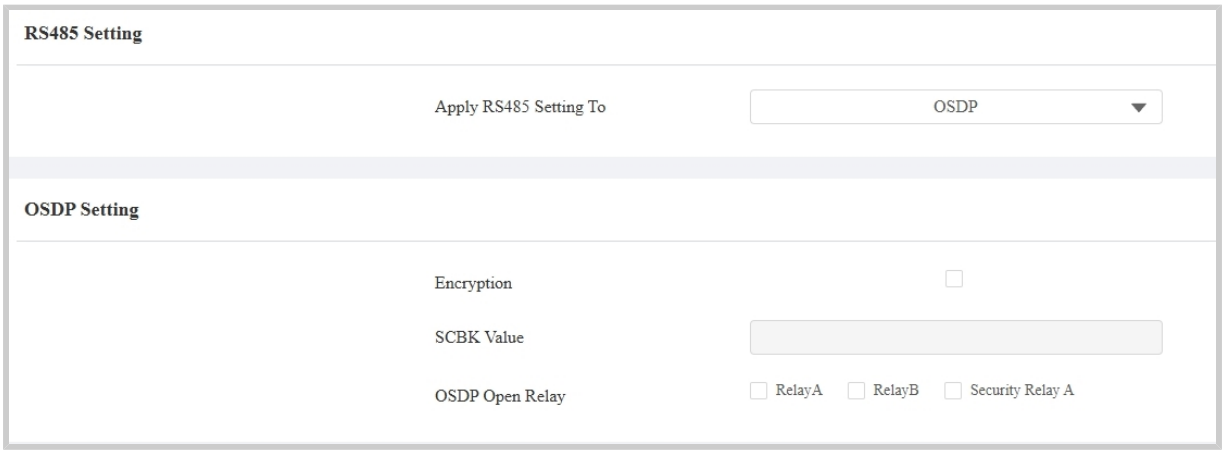
- **Power Output Type**:
  - **Always**: Provide continuous power to the third-party device.
  - **Triggered by Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.
  - **Security Relay A**: The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

Integration via RS485

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

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

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

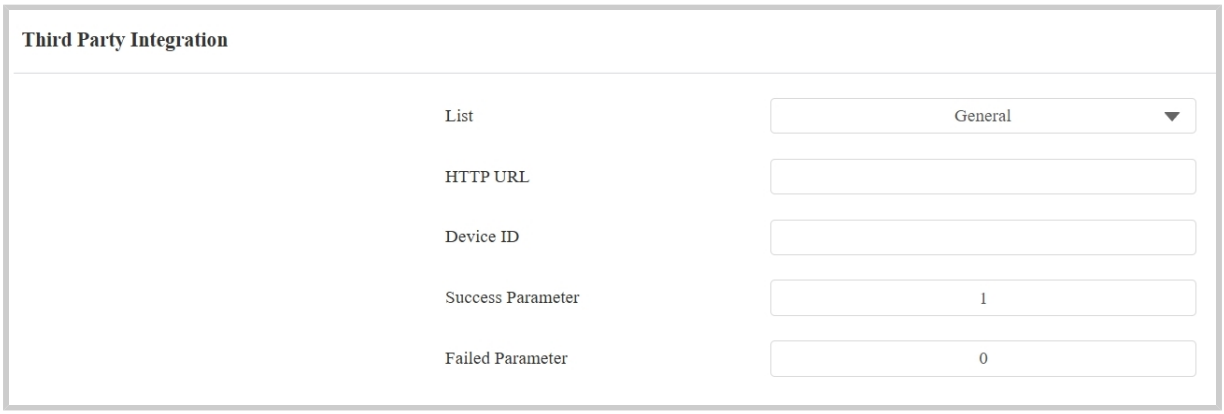


- **Disabled**: The RS485 function is disabled.
- **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **SCBK Value**: Secure Communication Key Value.
    - When it is filled, OSDP will use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

Integration with Third-party Access Control Server

The device can transmit QR codes, PIN, card data, and face data to a third-party server without doing any verification. The generation and verification of the data are conducted on the third-party server.

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



- **List**:
  - **None**: Disable the function.
  - **General**: Transmit the QR code-linked HTTP URL in Akuvox's method.
    - **HTTP URL**: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before it is sent to the QR code server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode} &deviceId={DeviceID}.*
    - **Device ID**: The device ID is provided by the third-party server. It will be added to the HTTP command automatically when using a QR code for door access.
    - **Success Parameter**: Receiving this value indicates that opening the door succeeds.
    - **Failed Parameter**: Receiving this value indicates that opening the door fails.
  - **Customize**: Transmit access credential data in a customized method. 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.
    - **Remote Verification**: Specify which access credentials will be verified by the third-party server.

Available options depend on the configured Authentication Mode. When **Two-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}&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}&deviceId=1.
- **Two-Factor HTTP URL Format**: In **Two-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.

Variable	Description
{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.

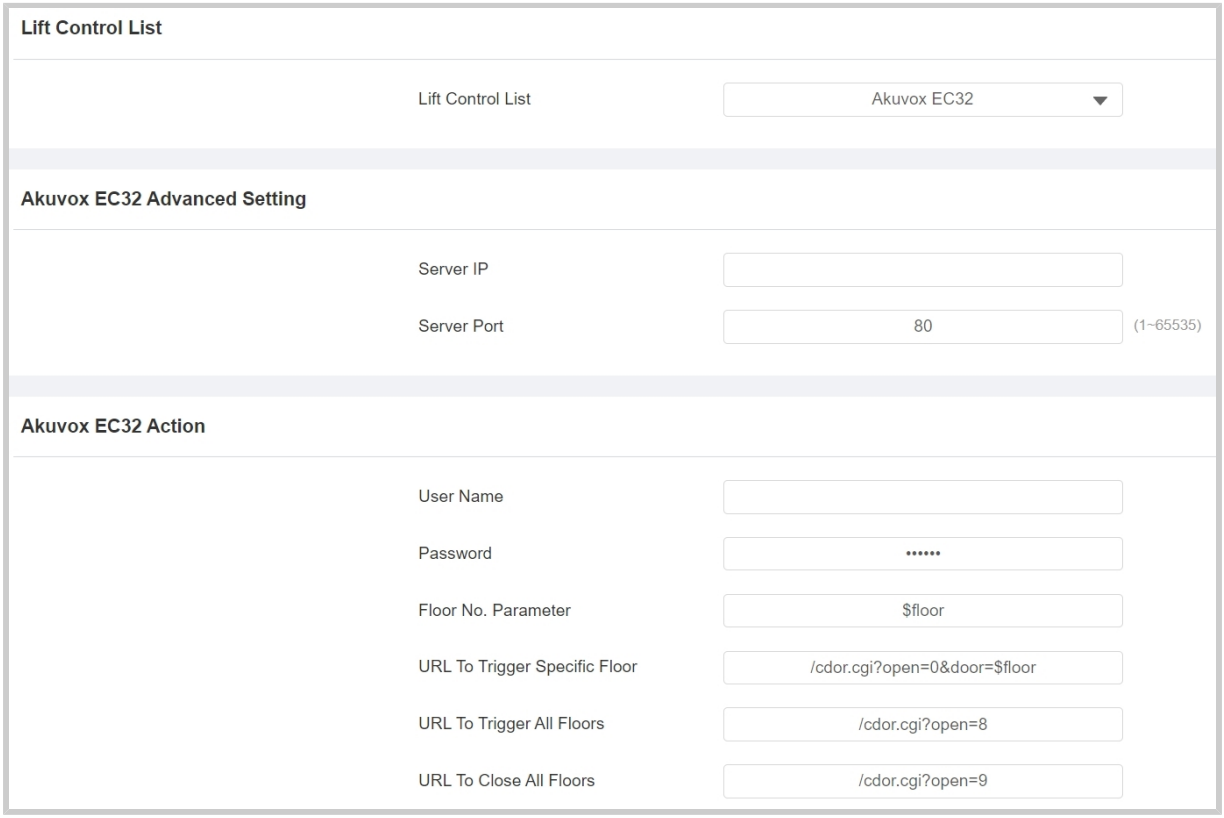
Lift Control

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.



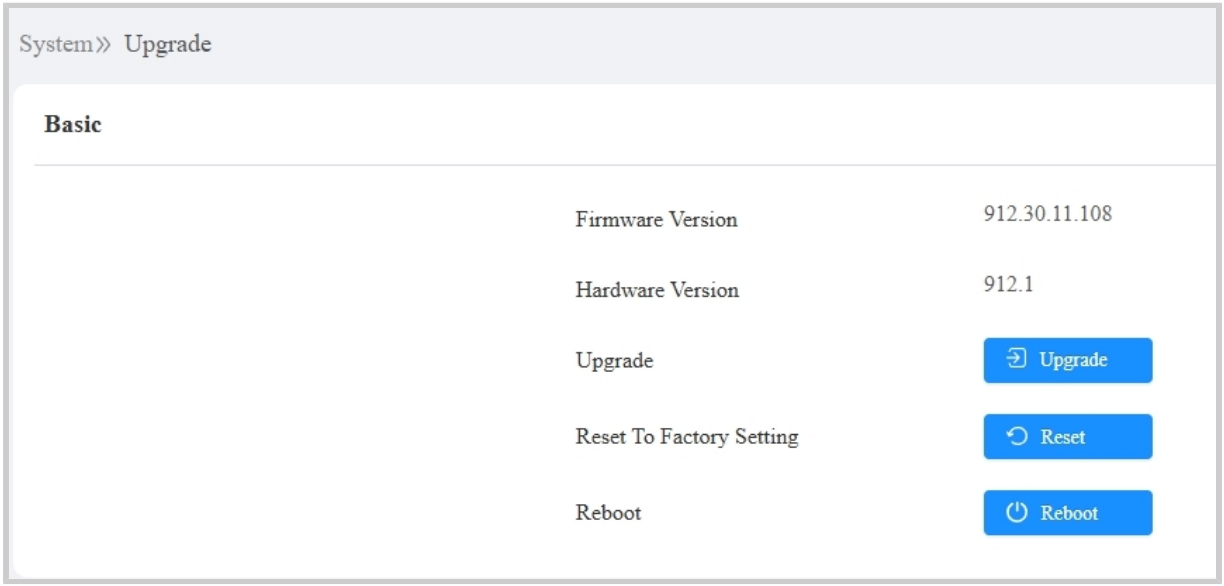
- **Lift Control List**: Select Akuvox EC32 for integration with the Akuvox lift controller.
- **Server IP:** Enter the IP address of the Akuvox lift controller.
- **Server Port:** Enter the port of the Akuvox lift controller.

- **User Name:** Enter the user name set in the lift controller.
- **Password:** Enter the password set in the lift controller.
- **Floor NO. Parameter:** The floor number parameter is provided by Akuvox. The default is **$floor**. You can define your parameter string.
- **URL To Trigger Specific Floor:** The Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string $floor at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors:** The Akuvox URL for triggering all floors.
- **URL To Close All Floors:** The Akuvox URL for closing all floors.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Note

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

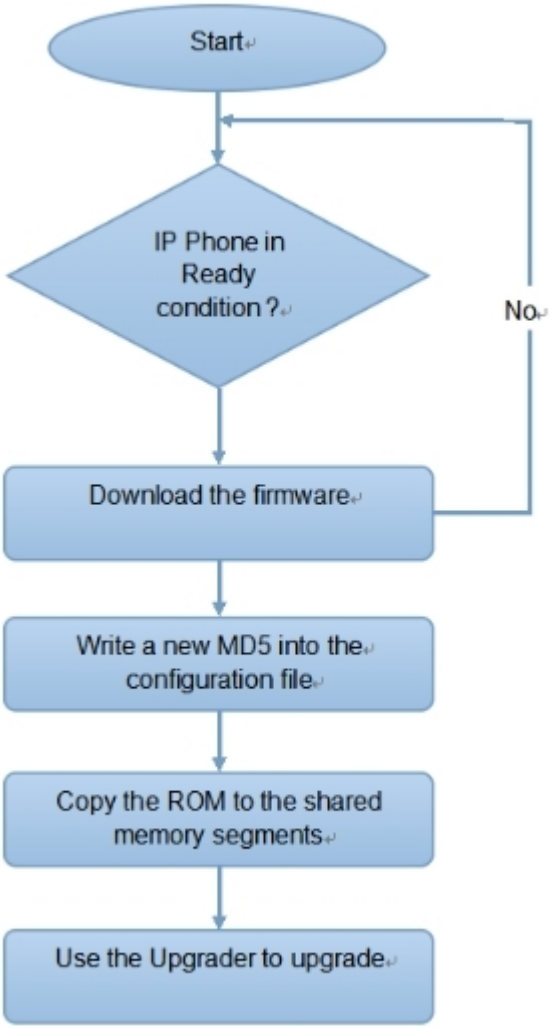
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

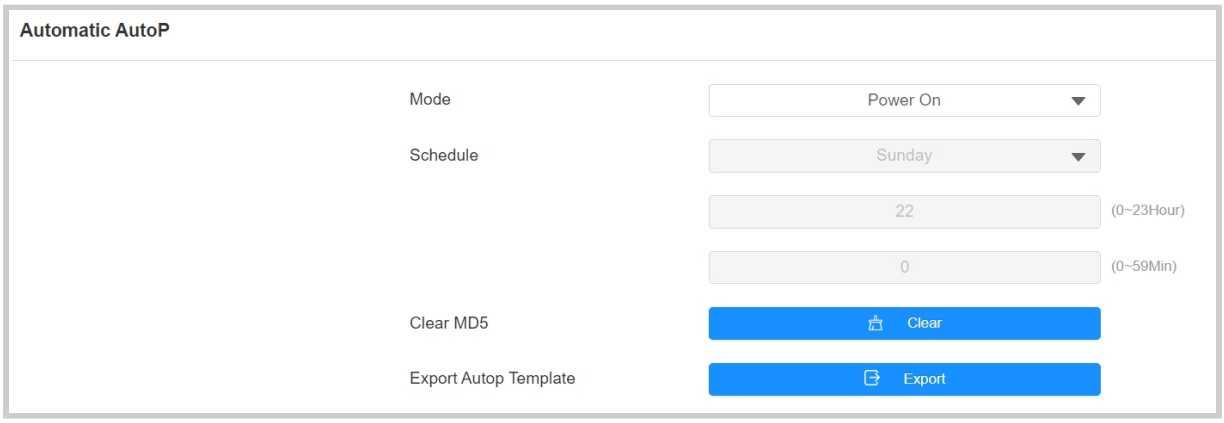
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

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

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

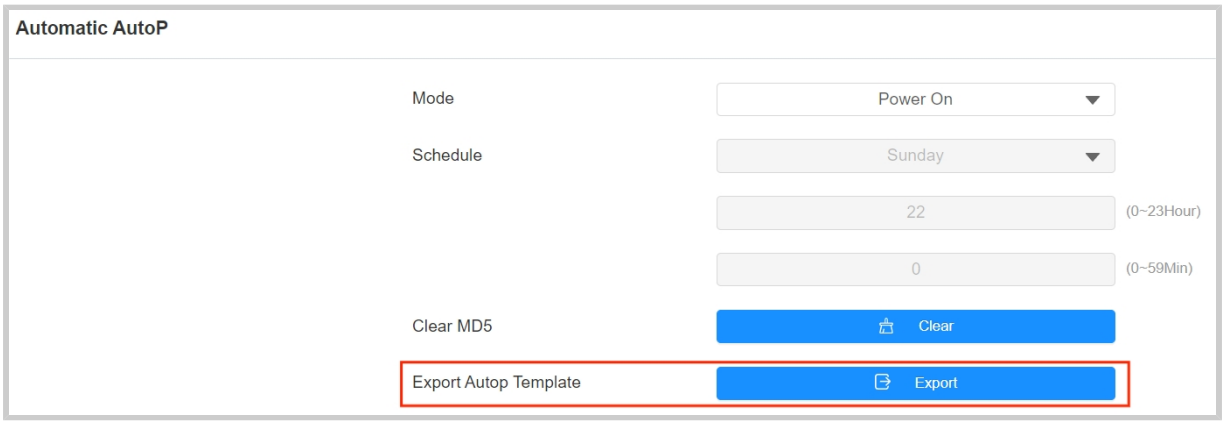


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
  - **Hourly Repeat**: The device will perform Autop every hour.

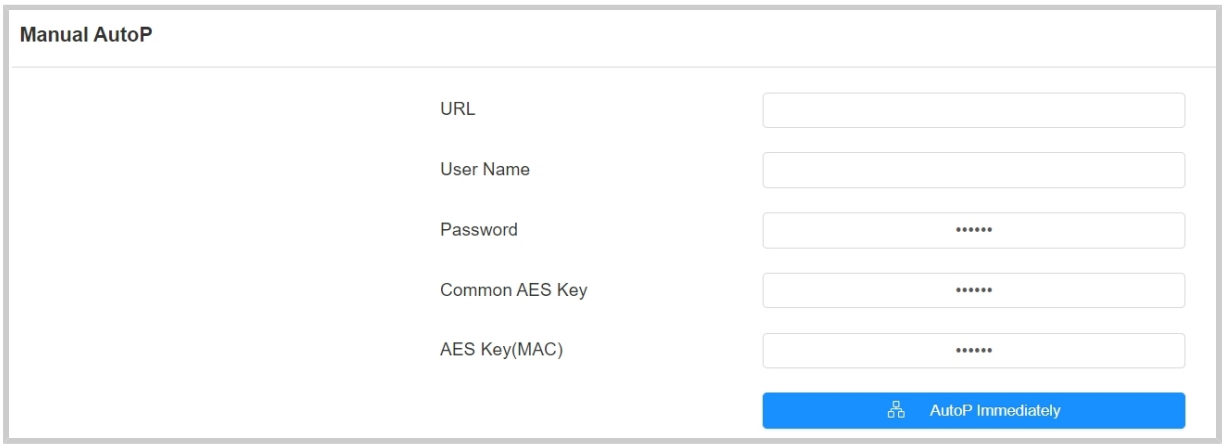
Static Provisioning

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.

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



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



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server needs a username to be accessed.
- **Password**: Enter the password if the server needs a password to be accessed.
- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop 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

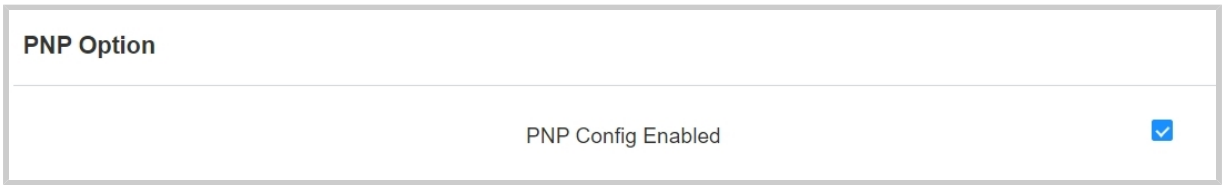
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

Click here to watch the configuration video.

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

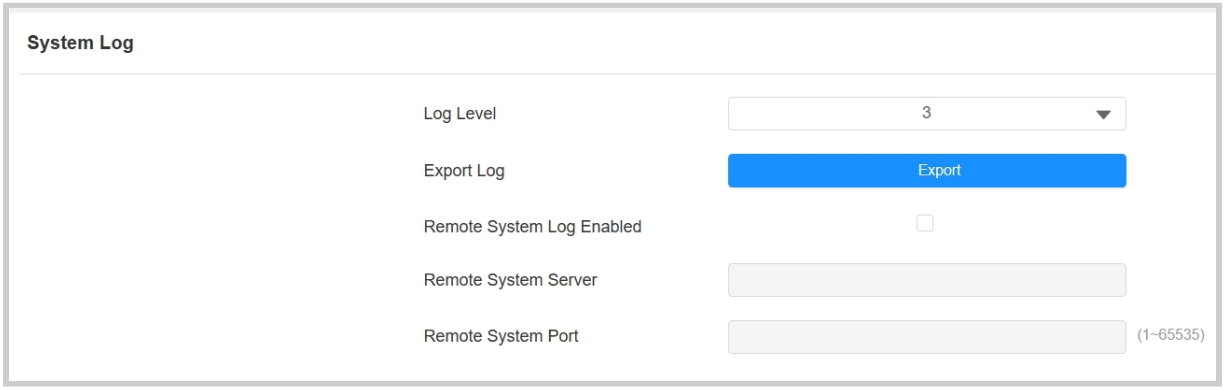

PNP Option
PNP Config Enabled

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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

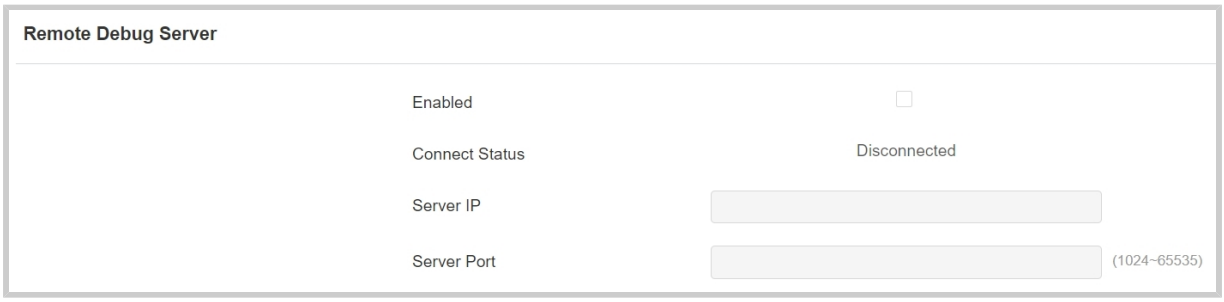


- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export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

Remote Debug Server

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

To set it up, go to the **System > Maintenance > Remote Debug Server** interface.

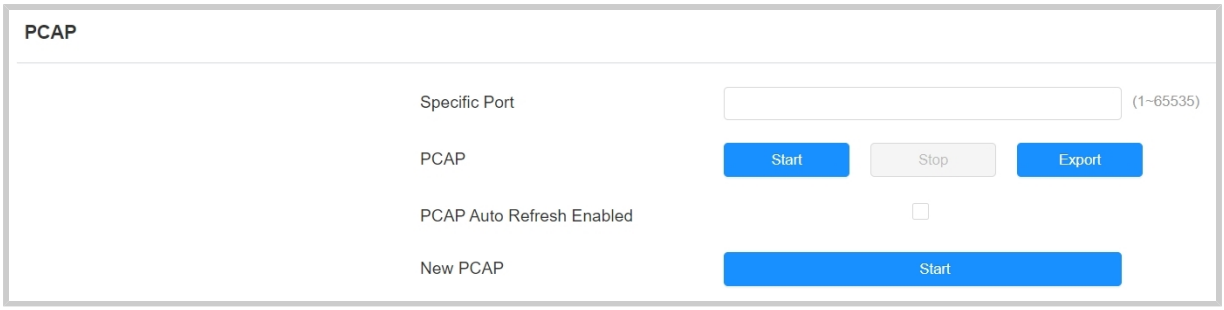


- **Connect Status**: Display the connection status between the device and the server.
- **Server IP**: Enter the IP address of the server.
- **Server Port**: Enter the port of the server.

PCAP for Debugging

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

To set it up, go to the web **System > Maintenance > PCAP** properly before using it.



- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the data packets to your Local PC.

- **PCAP Auto Refresh Enabled:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.
- **New PCAP:** Click Start to capture a bigger data package.

Web Call

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

To make a web call, navigate to **System > Maintenance > Web Call** interface.



- **Web Call (Ready)**: Enter the target IP/SIP number and select the account to dial out.

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.

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

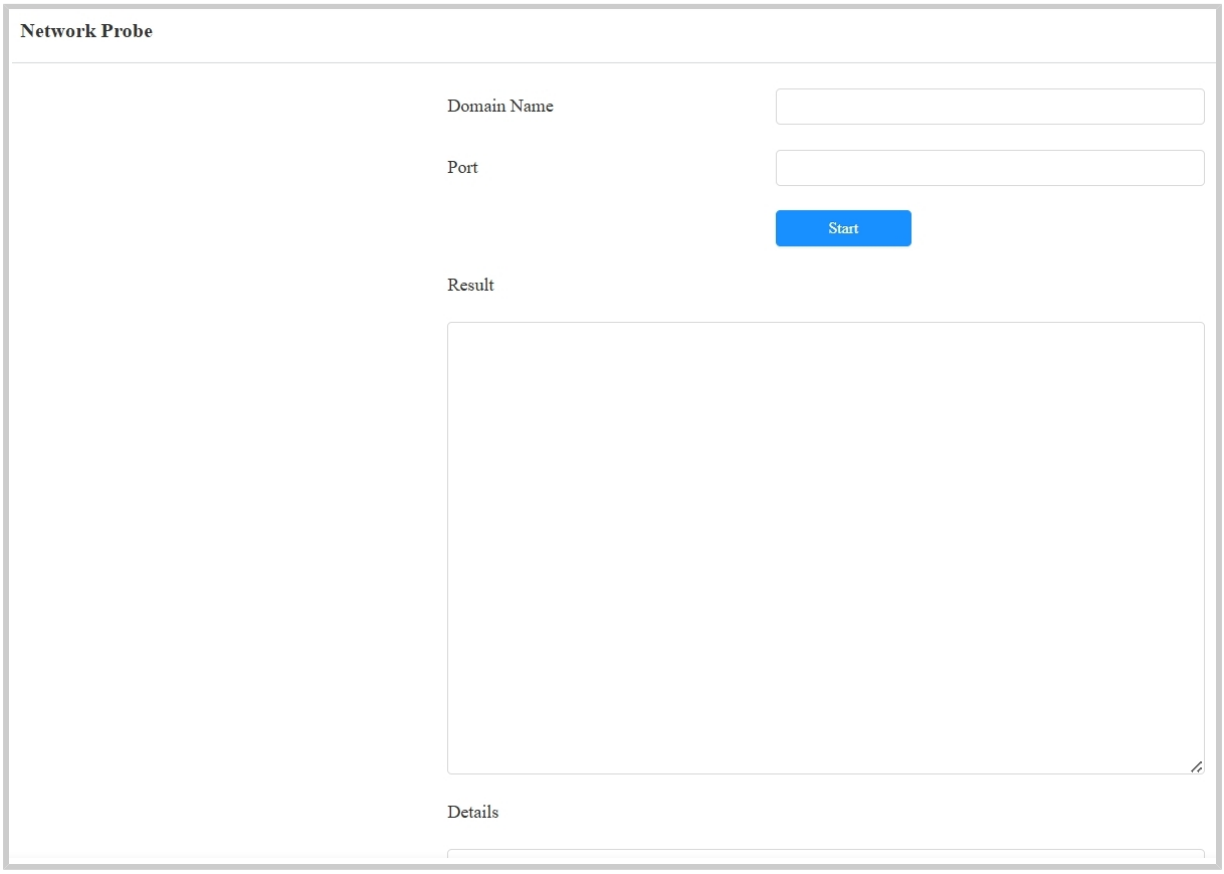


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Network Probe

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

Use this function on the **System > Maintenance** 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.

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



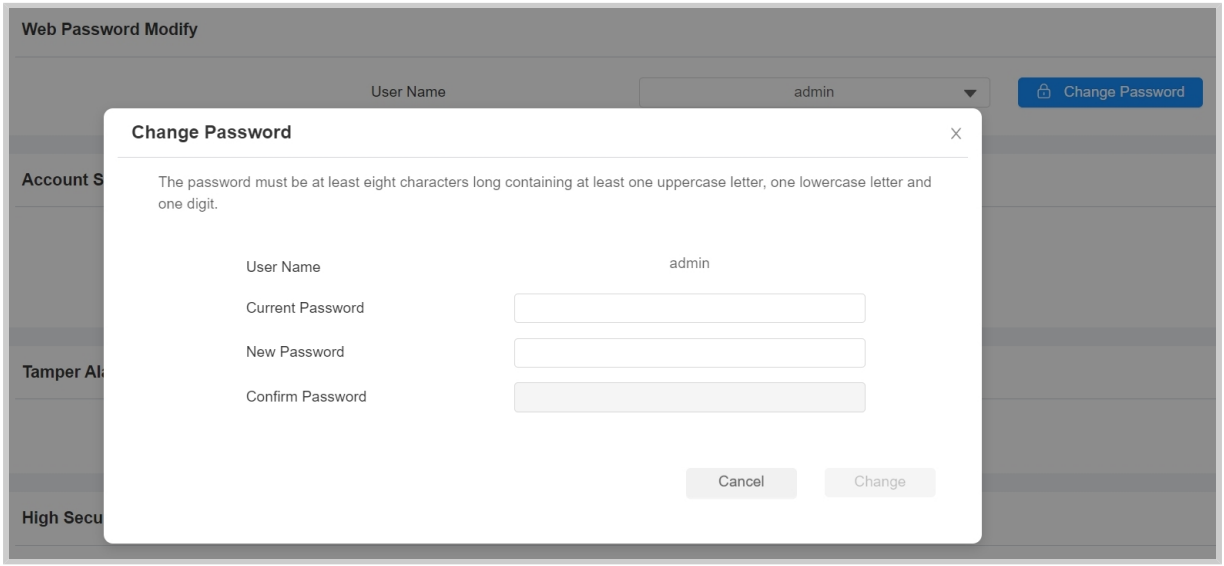
- **Config File**: Click **Export** to export configuration items as an encrypted file; click **Import** to import a configuration file to the device. The Config File includes configuration settings, user data, and contact data.

Password Modification

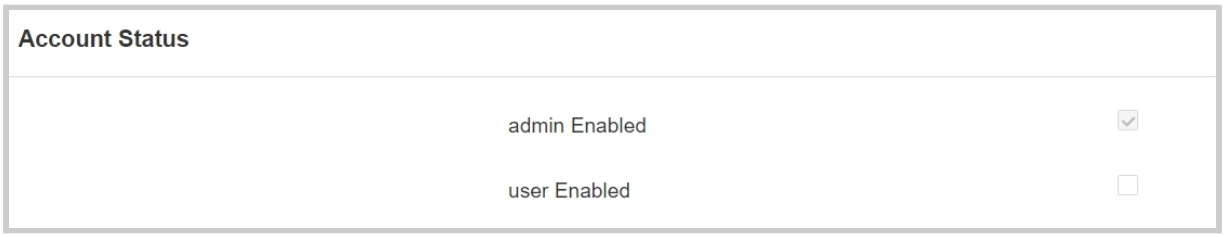
Modify Device Web Interface Password

You can modify the device web password for both the administrator account and the user account.
To set it up, go to **System > Security > Web Password Modify** interface.

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



To enable or disable the user account, scroll to the **Account Status** section.



Modify Security Questions

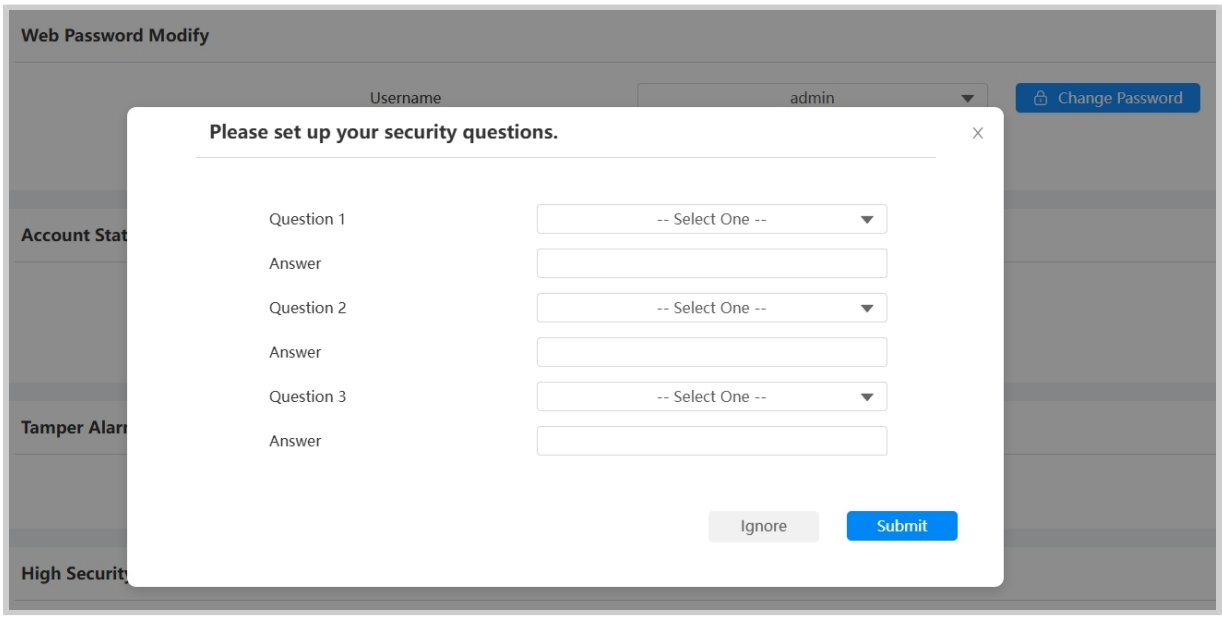
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

To set it up, go to the **System > Security > Web Password Modify** interface.



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

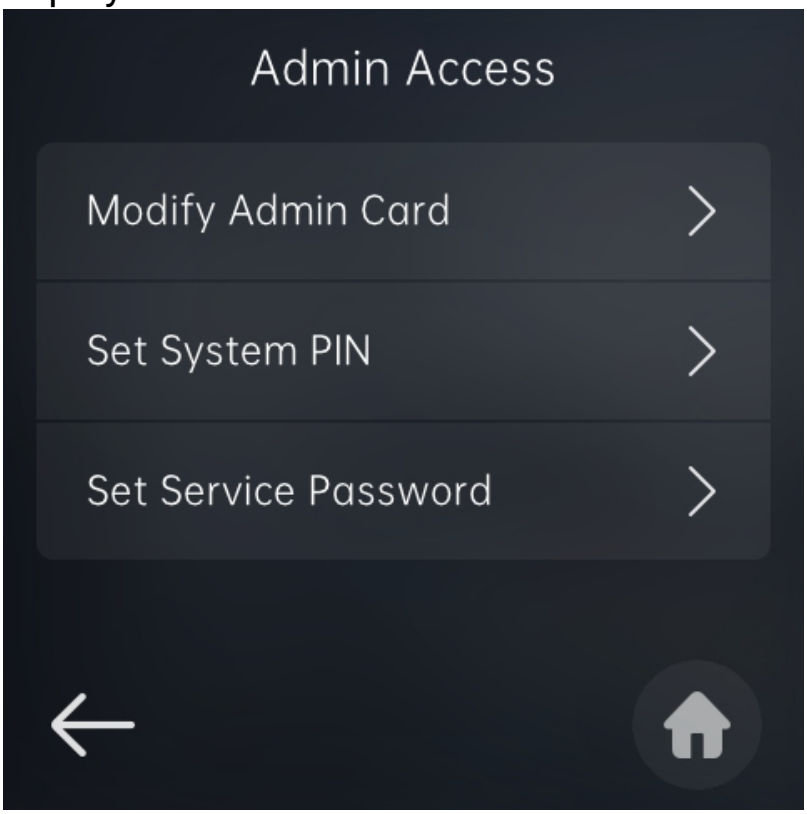


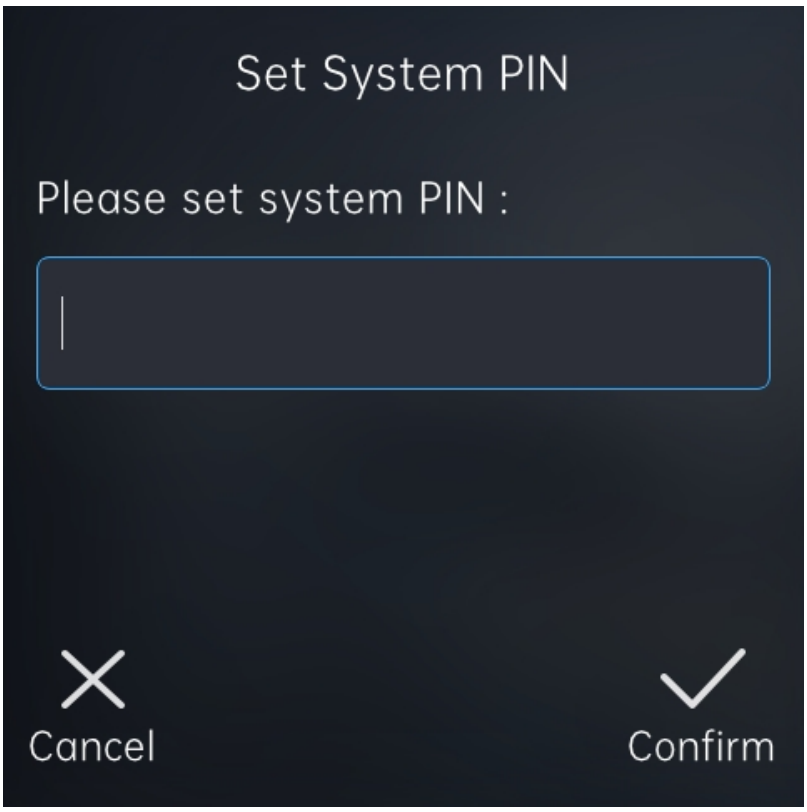
Modify System Password

The system PIN code is used to access the device‘s Admin Settings. The default is 2396.

You can modify the system PIN code directly on the device’s **Advance Settings> Admin Access > Set System PIN** screen.

Tap System PIN.



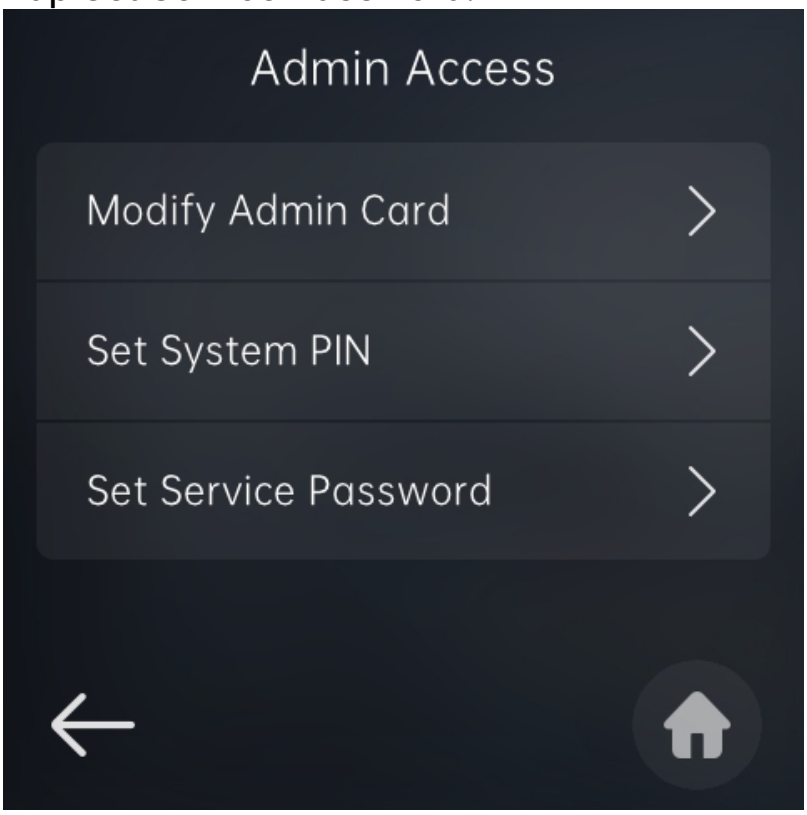


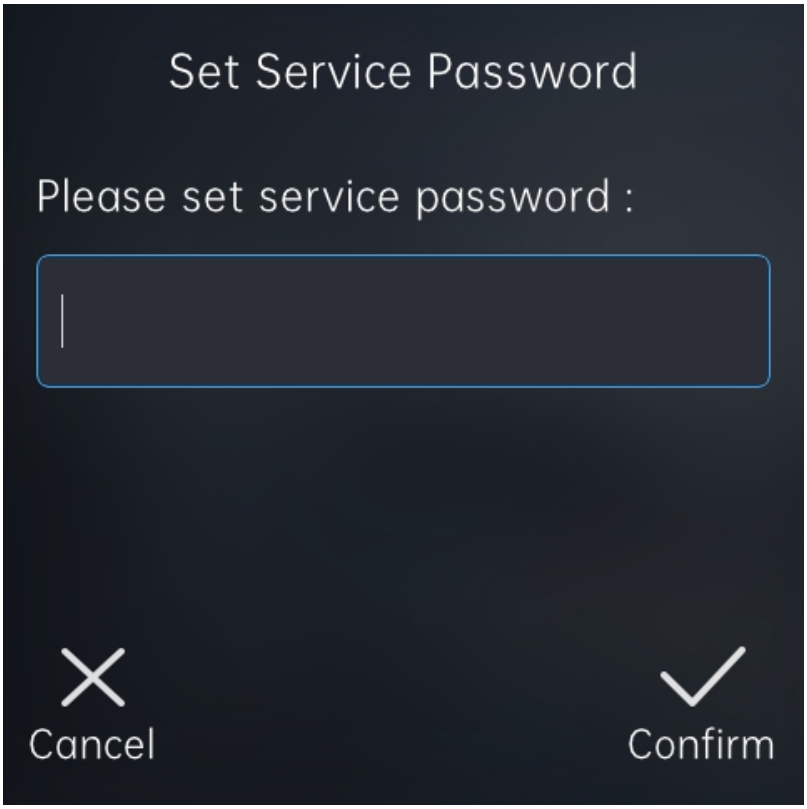
Modify Service Password

The service PIN code is used to access the device's access methods setting. The default is 3888.

You can modify the PIN code directly on the device's **Advanced Settings> Admin Access > Set Service Password** interface.

Tap Set Service Password.

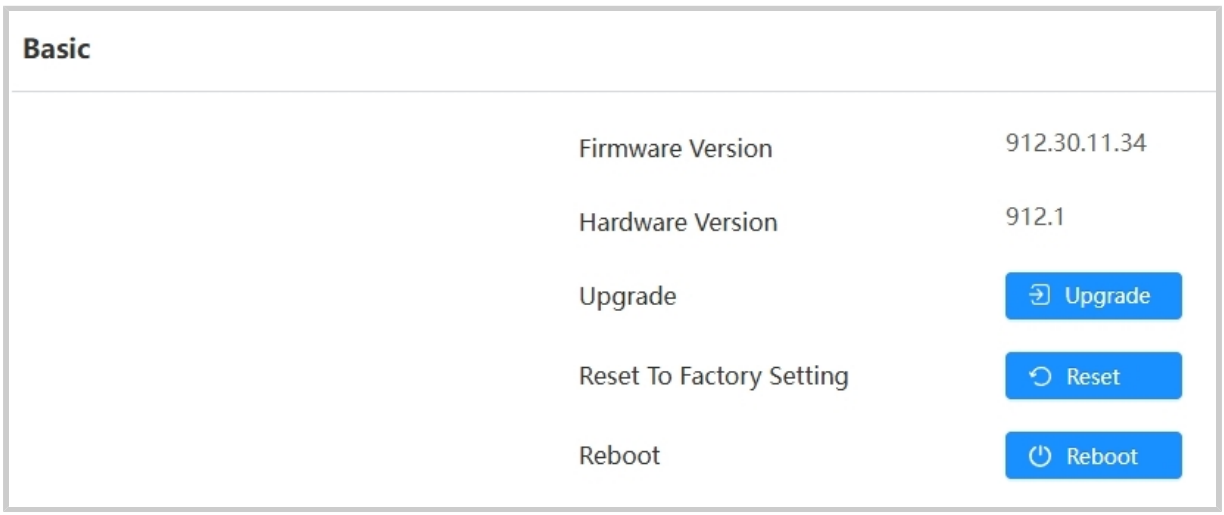



Set Service Password
Please set service password :
Cancel
Confirm

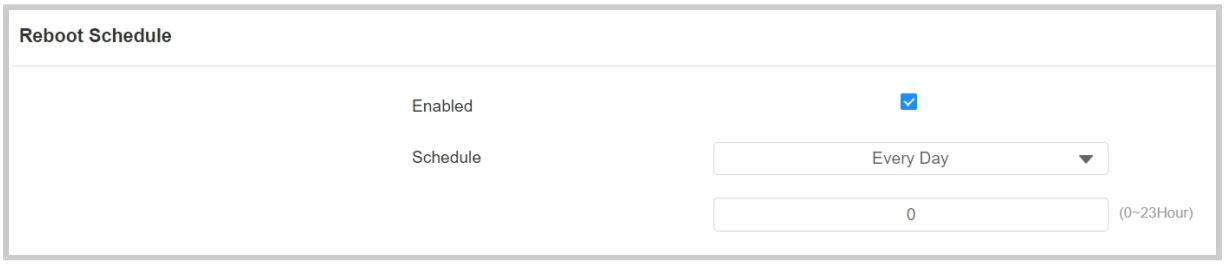
System Reboot&Reset

Reboot

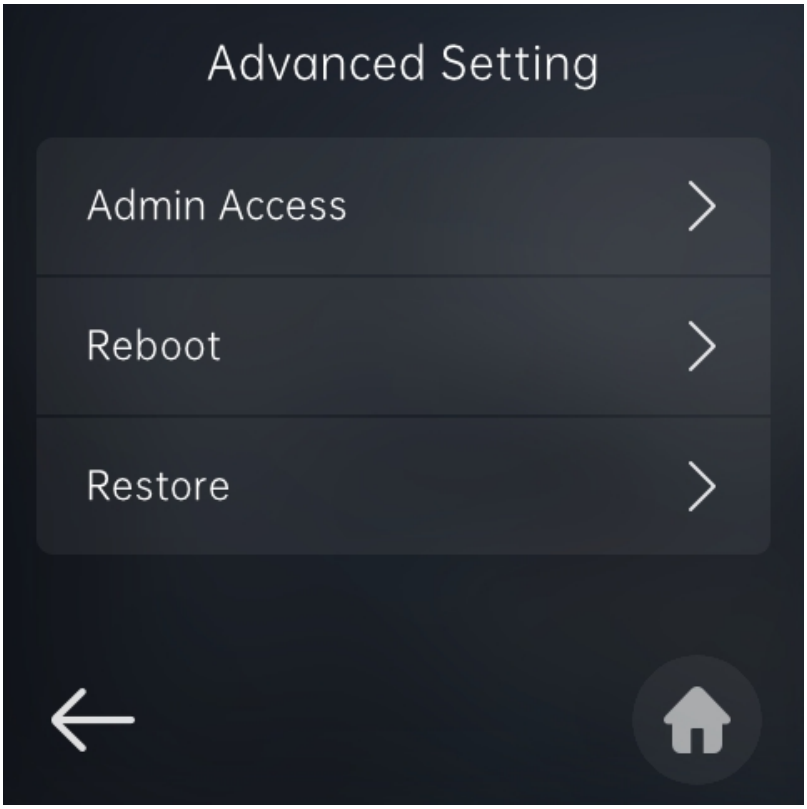
You can reboot the device on the **System > Upgrade > Basic** interface. Moreover, you can set up a schedule for the device to be restarted.



To set up the schedule, go to the **System > Auto Provisioning > Reboot Schedule** interface.



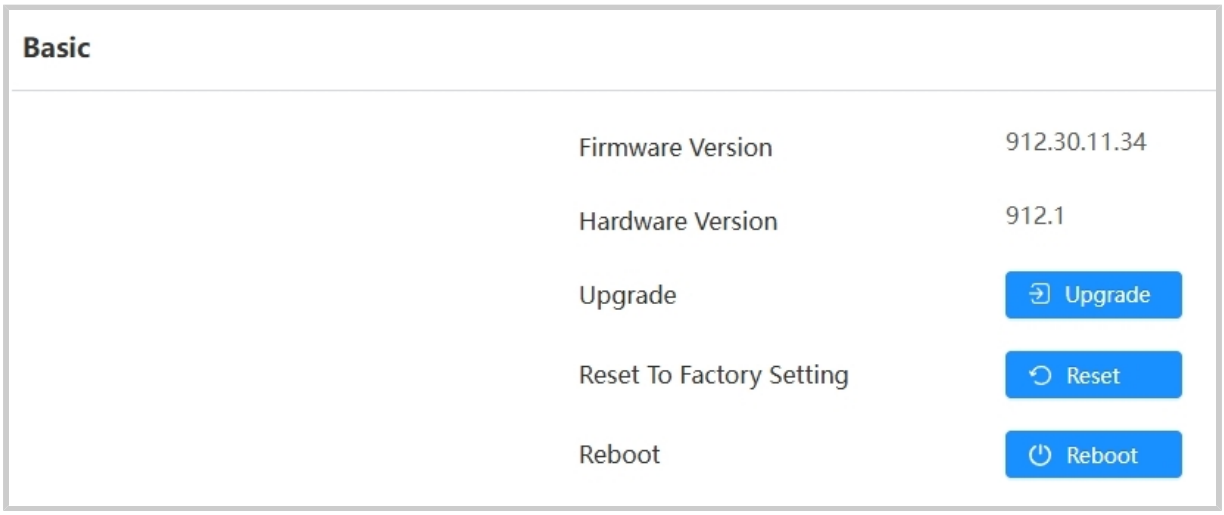
You can also reboot the device by tapping **Advanced Setting > Reboot**.


Advanced Setting
Admin Access
Reboot
Restore

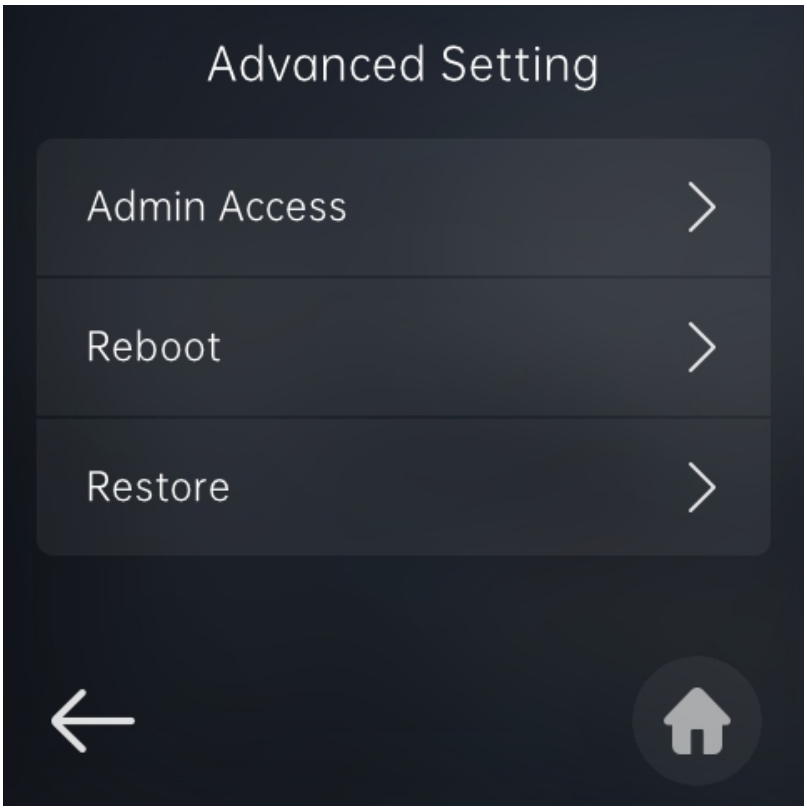

Reboot
Confirm to reboot?
Cancel
Confirm

Reset

You can reset the device on the web **System > Upgrade > Basic** interface.



You can also reset the device by tapping **Advanced Setting > Restore**.




Restore
Please confirm if you want to restore to the factory settings.
Cancel
Confirm

Tip

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

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

