Table of contents

Akuvox E18 Door Phone Administrator Guide

About This Manual 4
Product Overview 5
Changelog 6
Model Specification 7
  Supported Card Types 7
Access the Device 8
  Access the Device Settings 8
  Access the Device Web Settings 8
Introduction to Configuration Menu 10
  Introduction to Quick Start Module 10
Language and Time 12
  Language 12
    Custom Language 12
  Time 12
Volume and Tone 14
  Volume Control 14
  Upload Open Door Tone 14
  Ringback Tone 15
  Hang-up Tone 15
  Visitor-friendly Mode 15
LED and LCD 16
  Card Reader LED Control 16
  LED White Light 16
  LCD Screen Brightness 16
Screen Display 18
  Configure Screensaver 18
    Upload Screensaver 18
  Home Screen Display Mode 19
    Relay Key Settings 20
  Open Door Text Prompt Display 21
Network Setting 22
  Device Network Connection 22
  Device Deployment in Network 23
  NAT Setting 23
  Device Web HTTP Setting 24
  LTE Wireless Connection 24
Intercom Call Configuration 26
  IP Call Configuration 26
    Make IP/SIP calls 26
    IP Call Setup 26
  SIP Call&SIP Call Configuration 26
    SIP Account Registration 26
    SIP Server Configuration 27
    SIP Account Selection 28
  Outbound Proxy Server 28
  Data Transmission Type 28
  Device Local RTP 29
  SIP Hacking Protection 29
  Video Transport Type 29
Call Settings 31
  Call Auto-answer 31
  Quick Dial by Number Replacement 31
  Sequence Call 32
  Speed Dial 33
  Group Call 34
  Call the Reception Center 34
  Two-Way Video Call 35
  Maximum Call Duration 35
  Maximum Dial Duration 35
  Hang Up After Open Door 36
Audio & Video Codec Configuration 37
  Audio Codec 37
  Video Codec 37

Contacts Configuration 38
Manage Contact Groups 38
Set up Contact Details 38
Contact List Display 39
Relay Setting 40
Local Relay 40
Security Relay 41
Web Relay 41
Door Access Schedule Management 44
Create a Door Access Schedule 44
Import and Export Door Access Schedule 45
Relay Schedule 45
Holiday Schedule 45
Holiday Schedule Import/Export 46
Door-opening Configuration 47
Unlock by Public PIN 47
User-specific Access Methods 47
Unlock by Private PIN Code 48
Unlock by QR Code 48
Unlock by RF Card 49
Unlock by License Plate 50
Unlock by Facial Recognition 50
Access Setting 51
Import/Export User Data 52
Access Authentication Mode 52
Send Card Numbers to Third-Party Servers 53
Unlock by NFC 53
Mifare Card 53
Unlock by Bluetooth 54
Unlock by HTTP Command 54
Unlock by DTMF Code 54
DTMF White List 55
DTMF Data Transmission 55
Unlock by Exit Button 56
Choose Unlock Options 57
Temperature Measurement for Door Access 57
Latching PIN 58
Monitor and Image 59
MJPEG Image Capturing 59
RTSP Stream Monitoring 60
RTSP Stream Setting 60
ONVIF 61
Live Stream 61
Security 63
Tamper Alarm 63
Motion Detection 63
Security Notification 64
Email Notification 64
FTP Notification 65
TFTP Notification 65
SIP Call Notification 66
Action URL 66
Voice Encryption 67
User Agent 67
Real-Time Monitoring 68
Web Interface Automatic Log-out 68
Emergency Action 68
High Security Mode 68
Logs 70
Call Logs 70
Door Logs 70
Temperature Logs 70
Export Logs to SD Card 71
Event Logs 71
Integration with Third Party Device 73
Integration via Wiegand 73
Integration via HTTP API 74

Integration with Third-party Access Control Server 74
Power Output Control 75
Lift Control 76
Firmware Upgrade 77
Auto-provisioning 78
Provisioning Principle 78
Configuration Files for Auto-Provisioning 78
Autop Schedule 78
Static Provisioning 79
DHCP Provisioning 80
PNP Configuration 81
Debug 82
System Log for Debugging 82
PCAP for Debugging 82
Remote Debug Server 82
Web Call 83
Ping 83
Backup 84
Password Modification 85
Modify Web Interface Password 85
Modify Security Questions 86
Modify System Password 86
System Reboot&Reset 88
Reboot 88
Reset 88

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX E18C DOOR PHONE

Administrator Guide

Thank you for choosing the Akuvox E18C door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to the 18.30.11.108 version, and it provides all the configurations for the functions and features of E18C door phones. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox E18C is Linux-based with a touch screen. It incorporates audio and video communications, access control, and video surveillance. Its finely-tuned SmartPlus and AI-based communication technology allows featured customization to better suit users' operation habits. E18C multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, helping to create a holistic control of the building entrance and its surroundings and giving users a great sense of security via a variety of access such as card access, NFC, Bluetooth, QR code and newly added door access in an accompaniment with body temperature measurement. E18C door phone applies to residential buildings, office buildings, and their complex.

Changelog

What's new in version 18.30.11.108:

- Support the Parking Restrictions feature.
- Support displaying snapshots from third-party cameras in the Door Log when linked to the device.

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

Model Specification

Model	E18C
Relay Out	2
Relay In	3
RS485	✔
Card Reader	13.56MHz, 125kHz & NFC
Wi-Fi	X
Bluetooth	✔
Temperature Detection	Optional
Face Recognition	✔
LTE	Optional
USB	X
External SD Card	✔

Supported Card Types

The device's firmware should be 18.30.10.92 or higher:

- ID Card:
  - EM4100
  - EM4200
- 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

Access the Device

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

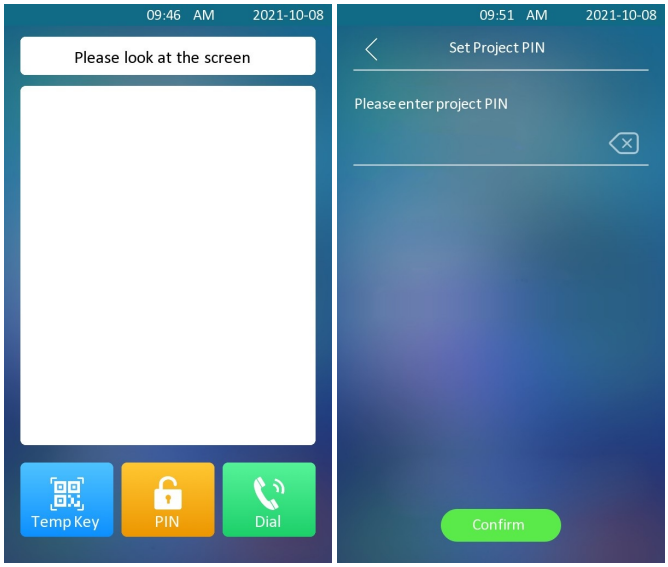
Access the Device Settings

To access the device settings, you can long-press on the initial screen for approximately five seconds, then enter the default PIN code.

Before proceeding, identify your device model and firmware version, as the default PIN varies.

The default PIN depends on your firmware version:

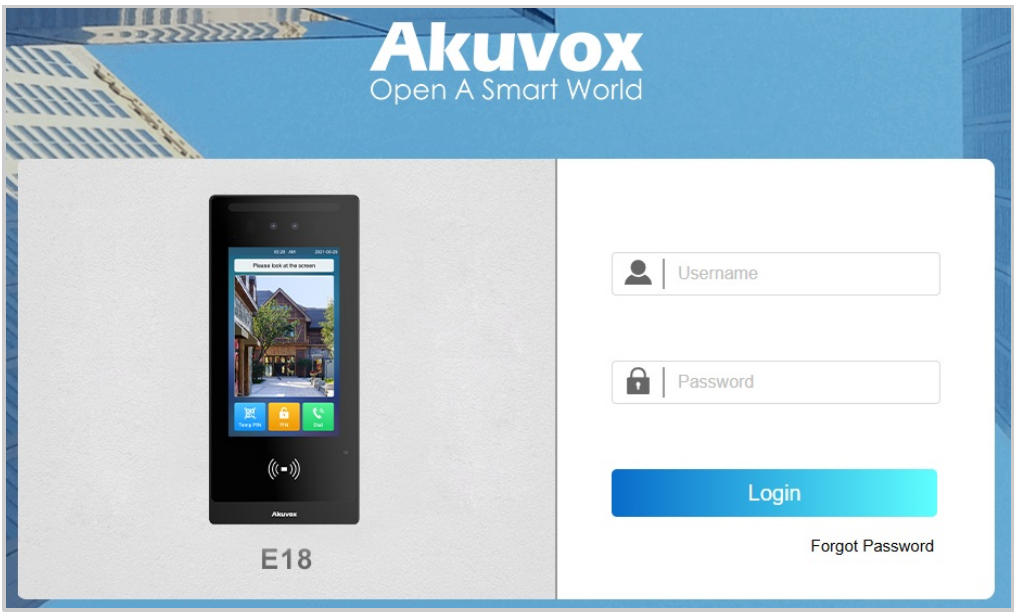
- **Firmware version 18.30.10.211 or earlier:** `admin`
- **All other versions:** `Admin321.`



Access the Device Web Settings

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

Check the device IP on the **Setting > System Info** screen or use the Akuvox IP scanner tool to search for the device's IP address in the same LAN.

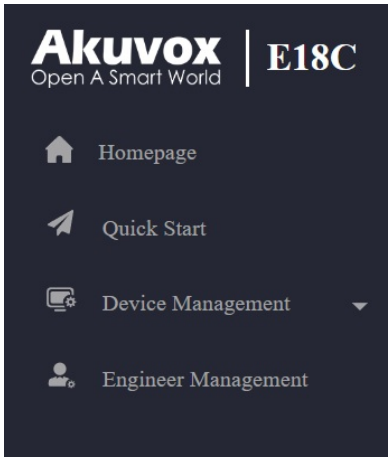


Note

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

Introduction to Configuration Menu

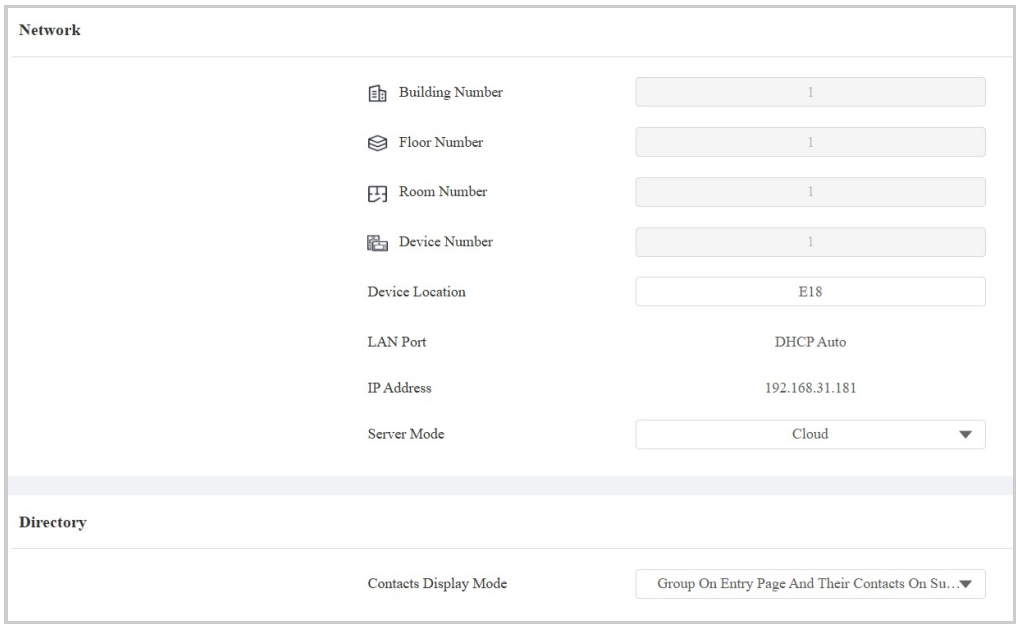
- **Quick Start**: This section provides quick access to the device's key settings, such as network, user, relay, etc.
- **Device Management**:
  - **Status**: This section gives you basic information, such as product information, network information, call log, door log, etc.
  - **Account**: This section 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 method setup, 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.
- **Engineer Management**: This section provides quick access to upgrading, maintaining, and debugging the device.



Introduction to Quick Start Module

The Quick Start module allows you to configure the device's core features on a single interface, instead of switching between different interfaces.

You can redirect to the feature detail interface by clicking **Details** in the upper-right corner.



- **Network**: Display the location information of the device.
  - **Device Location**: Enter the device's location to distinguish it from others. By default, it is [*the device name_the last 4 characters of its MAC address*] in the Self-organizing Network Solution.
  - **Server Mode**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None.
- **Auto-Discovery Contact List**: Display the contacts, such as indoor monitors, in the Self-organizing Network Solution.
  - **Show LCD Auto-Discovery Contact List**: Set whether to display these contacts on the device screen.
- **Directory**: Set the contact display mode.
  - **All Contacts**: Display all the contacts.
  - **Groups Only**: Display contact groups. Press the desired group on the device screen to make a group call.
  - **Groups On Entry Page And Their Contacts On Subpage**: Display contacts by groups. Press the group, and users can see the contacts in it.
- **Open Relay Via HTTP**:
  - **Username**: Set a username for authentication in HTTP command URLs.
  - **Password**: Set a password for authentication in HTTP command URLs.

Language and Time

Language

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

You can also select the language on the **Setting> Display & Sounds > Language** screen.

The device's LCD supports the following languages:

- English, Simplified Chinese, Russian, Korean, Dutch, French, German, Hebrew, Japanese, Turkish, Arabic, Spanish, Traditional Chinese, Kazakh, Czech, Swedish, and Ukrainian.



You can switch the device's web language in the upper-right corner.

The device web supports the following languages:

- English, Simplified Chinese, Spanish, Russian, Korean, Traditional Chinese, Dutch, French, German, Turkish, Japanese, Swedish, Italian, Czech, Ukrainian, and Kazakh.



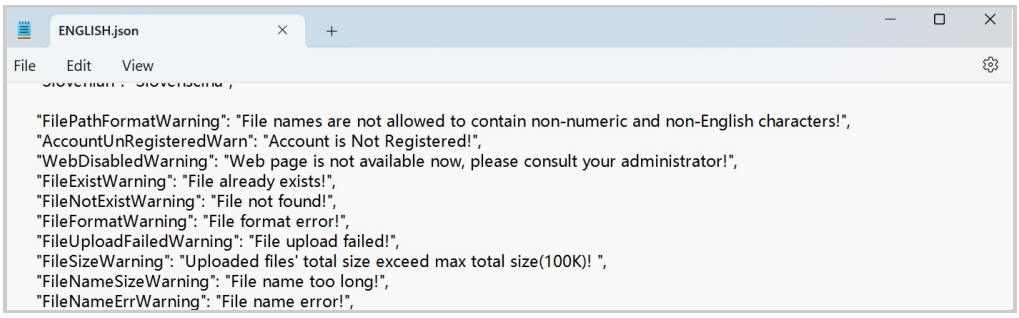
Custom Language

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

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

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

File Example:



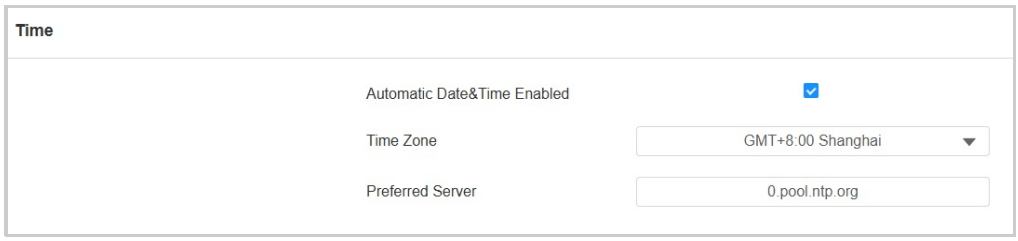
Set it up on the **Setting > Time/Lang > Words Of Language Upload** interface.



Time

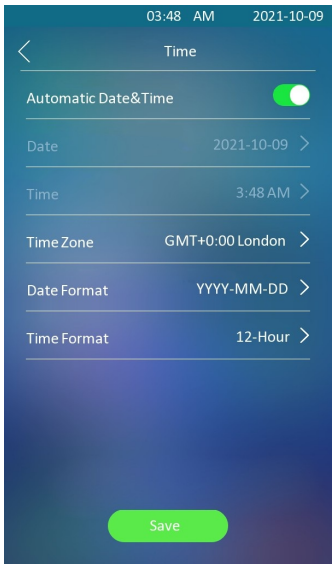
The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on your device.

To set it up, go to **Setting > Time/Lang > Time** interface.



- **Automatic Date&Time Enabled**: 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.
- **Preferred Server**: Enter the NTP server address.

You can also set up the device time on **Setting > Display & Sounds > Time** screen.

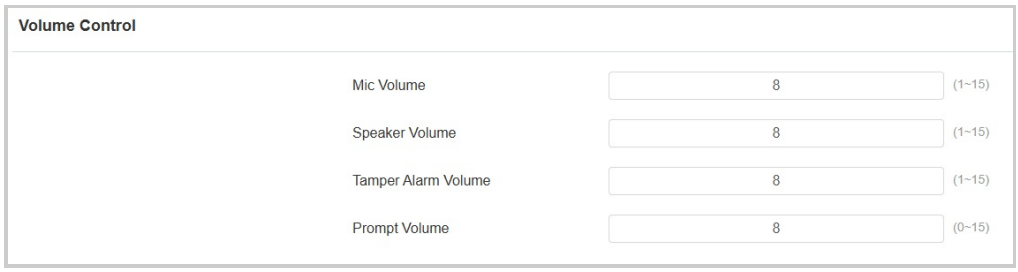


Volume and Tone

Volume and ringtone configurations include microphone volume, speaker volume, alarm volume, and more. In addition, you can upload door-opening tones to enrich the user's personalized experience.

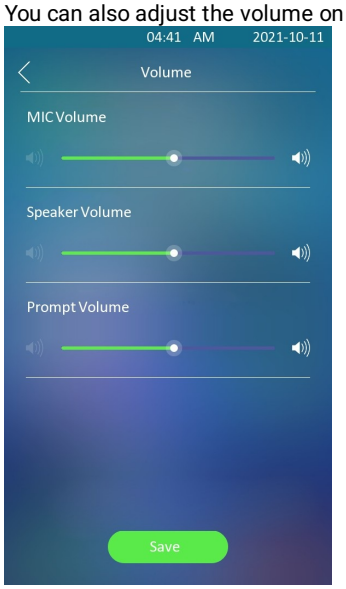
Volume Control

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



- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 8.

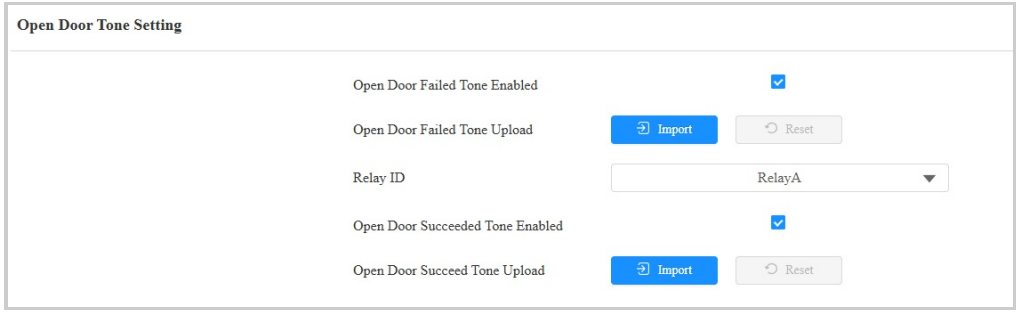
You can also adjust the volume on **Setting > Display&Sounds > Sounds** screen.



Upload Open Door Tone

You can upload the tone for open door failure and success on the device web interface.

To set it up, go to **Device > Audio > Open Door Tone Setting** interface.



- **Relay ID**: Specify which relay uses the tones.
- **Open Door Failed/Succeeded Tone Upload**: File Format: wav; Size: < 200KB; Sample rate: 16000; Bit Depth: 16 Bits. You can click Reset to remove the uploaded file.

Ringback Tone

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

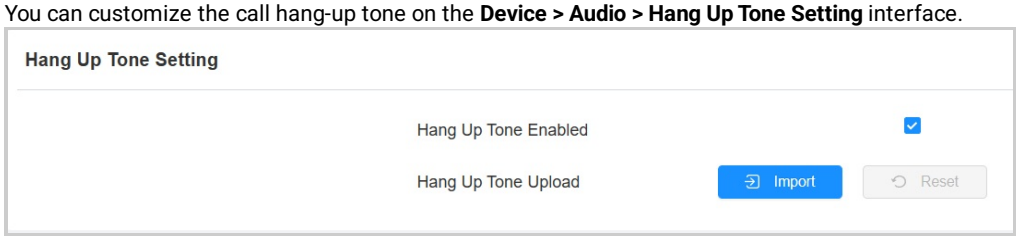
To set it up, go to the **Device > Audio > Ringback Tone Setting** interface.



- **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.

Hang-up Tone

You can customize the call hang-up tone on the **Device > Audio > Hang Up Tone Setting** interface.



- **Hang Up Tone Upload**: File Format: wav; Size: < 200KB; Sample rate: 16000; Bit Depth: 16 Bits. You can click Reset to remove the uploaded file.

Visitor-friendly Mode

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

Set it up on the **Device > Audio > Visitor-friendly Mode** interface. When enabled, no prompts are given when facial recognition fails.

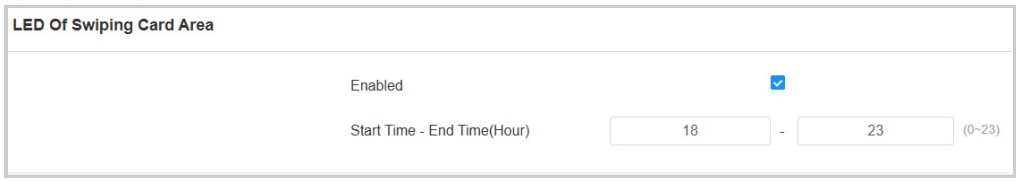


LED and LCD

Card Reader LED Control

You can enable or disable the LED lighting on the card reader area. You can also set a specific time to turn on the light.

To set it up, go to the **Device > Light > LED Of Swiping Card Area** interface.

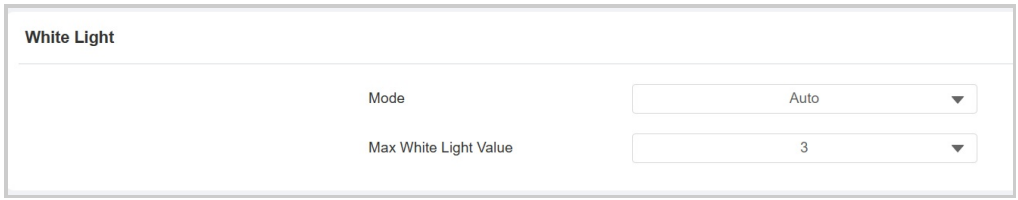


- **Start Time- End Time (Hour):** Enter the period for the LED lighting to be valid, e.g., if the period is from **18-22**, it means the LED light will stay on from **6:00 pm** to **10:00 pm** during one day (24 hours).

LED White Light

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

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



- **Mode**:
  - **Auto**: The white light will be turned on automatically for facial recognition and QR code scanning.
  - **OFF**: Disable the function.
- **Max White Light Value**: Set the white light value from 1-5, and the default white light value is **3**. The greater the value it is, the brighter the light will be.

LCD Screen Brightness

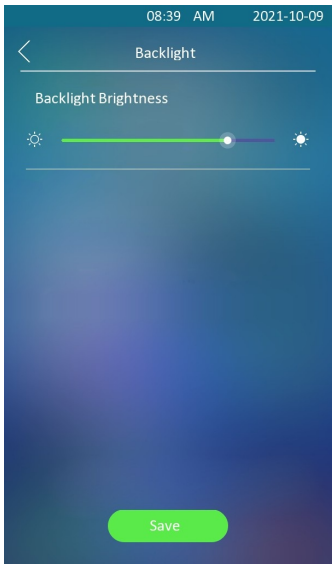
You can set up the backlight brightness so that users can better see the screen in an environment with high or low light intensity.

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



- **Backlight Brightness**: The default is 200. The higher the value, the brighter the screen is.

You can also set it up on the **Display&Sounds > Backlight** screen.


08:39 AM 2021-10-09
Backlight
Backlight Brightness
Save

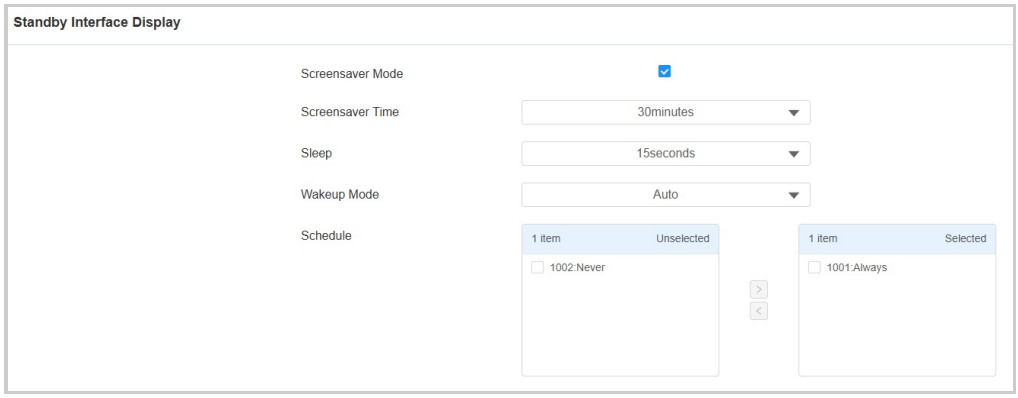
Screen Display

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

Configure Screensaver

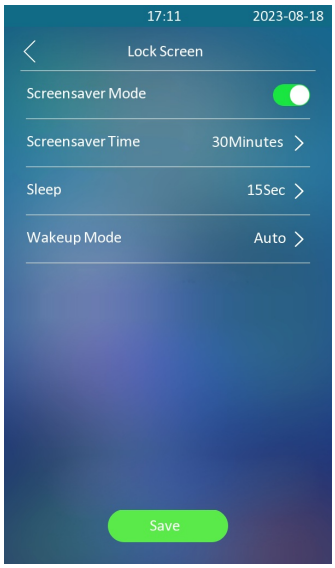
You can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction.

To set it up, go to the **Device > LCD > Standby Interface Display** interface.



- **Screensaver Time**: Set the screen saver duration time(5 seconds to 2 hours).
- **Sleep**: The time to start the screen saver mode(5 seconds to 30 minutes). 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.
- **Wakeup Mode**:
  - **Auto:** The screen will be awakened when someone approaches without it being touched.
  - **Manual:** Users need to touch and wake up the screen.
- **Schedule**: Select the schedule when the device will enter the automatic wakeup mode.

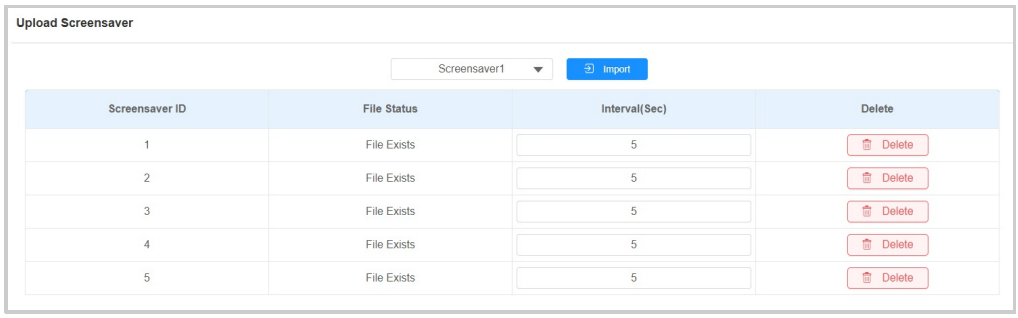
You can also set up the screen saver on **Setting > Display&Sounds > Screensaver** screen.



Upload Screensaver

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

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

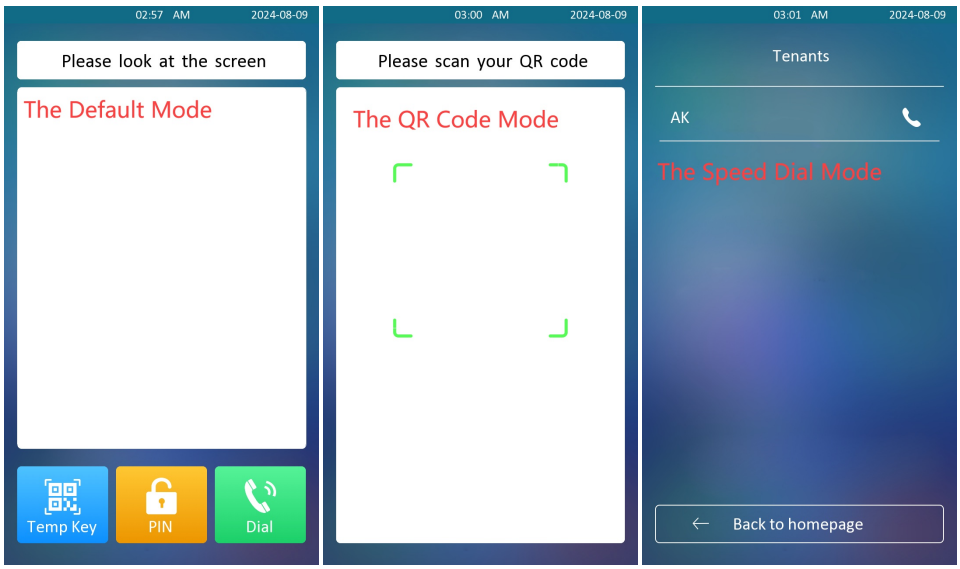


Note

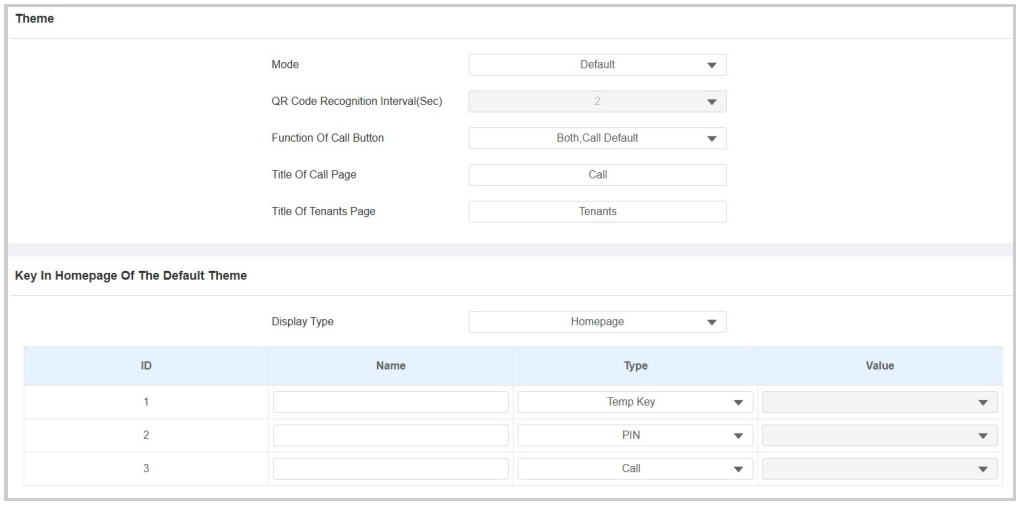
- Uploaded images should be in JPG/PNG format with no more than 2M pixels.
- The recommended resolution is 600 x 1024.
- If the uploaded image duplicates an existing image ID, the existing image will be overwritten.

Home Screen Display Mode

There are three home screen display modes: Default, QR code, and Speed Dial. To change the mode, go to **Device > LCD > Theme** interface.



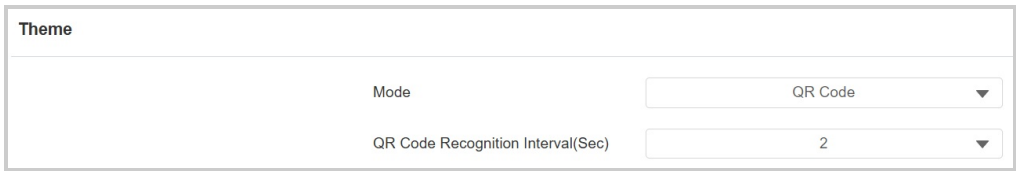
Default Mode:



- **Function of Call Button**:
  - **Both, Call Default**: The Call button will be displayed on the home screen. Tap it to see and switch between the Call screen and the Tenants screen. The Call screen will be displayed first.

  - **Both, Tenants Default**: The Call button will be displayed on the home screen. Tap it to see and switch between the Call screen and the Tenants screen. The Tenants screen will be displayed first.
  - **Only Call**: The Call button will be displayed on the home screen. Tap it to see the Call screen.
  - **Only Tenants**: The Tenants button will be displayed on the home screen. Tap it to see the Tenants screen.
- **Title of Call Page**: Customize the title shown on the upper area of the Call screen.
- **Title of Tenants Page**: Customize the title shown on the upper area of the Tenants screen.
- **Display Type**: Select the default display screen when waking up the device.
- **Name**: Name the button to be displayed on the home screen.
- **Type**: Select the button type. The button name will not change the button function.
- **Value**: Set the value when **Speed Dial** is selected as the button type.
  - When the device is deployed on-premise, select local contacts or enter the target IP/SIP numbers.
  - When the device is deployed on the SmartPlus Cloud, it follows the cloud contact display rules and cloud contacts, apartments, or groups, and devices are selectable.

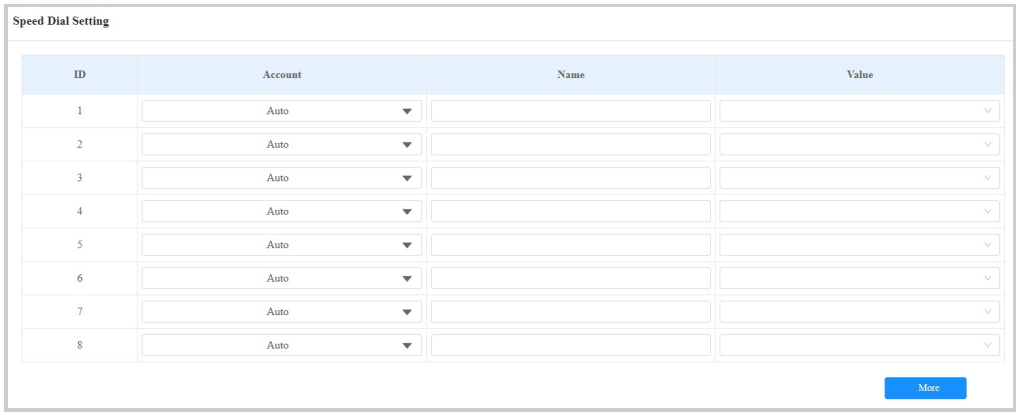
QR Code Mode:



- **QR Code Recognition Interval(Sec)**: The scanning interval between each QR code(1-8 seconds).

Speed Dial Mode:

Users can tap the specific tenant to call.

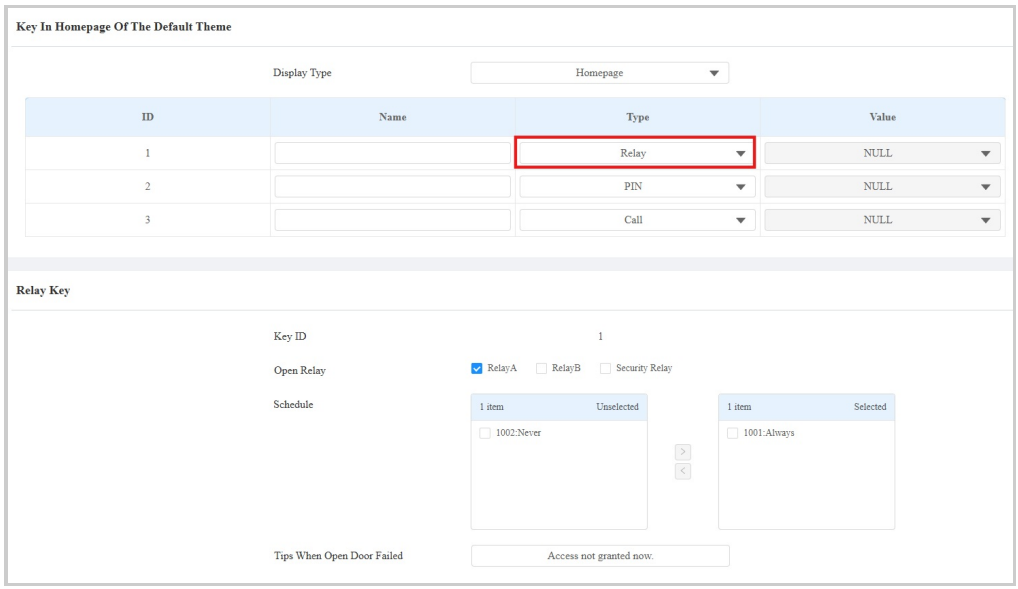


- **Account**: Select the account to make the call.
- **Name**: Name the contact.
- **Value**: Select local contacts or enter the target IP/SIP numbers.
  - When the device is deployed on the SmartPlus Cloud, it follows the cloud contact display rules and cloud contacts, apartments, or groups, and devices are selectable.
- **More**: Click to create more speed dial numbers.

Relay Key Settings

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

Scroll to the **Relay Key** section on the **Device > LCD** interface.

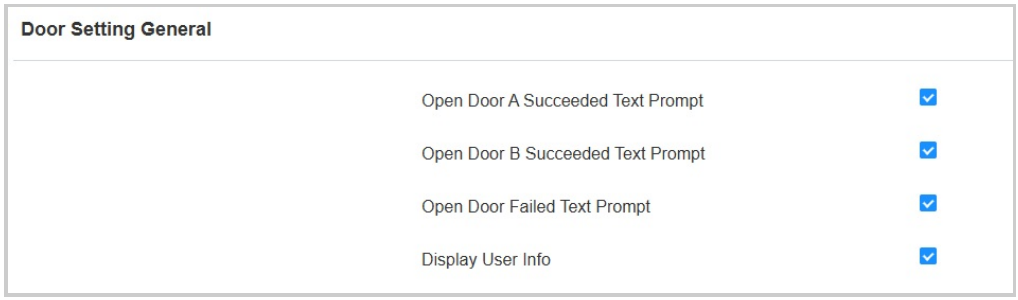


- **Key ID**: Specify which tab is set to be **Relay**.
- **Open Relay**: The relay to be triggered.
- **Schedule**: The relay can only be triggered within the schedule.
- **Tips When Open Door Failed**: The text prompt appears when the door opening fails.

Open Door Text Prompt Display

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

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



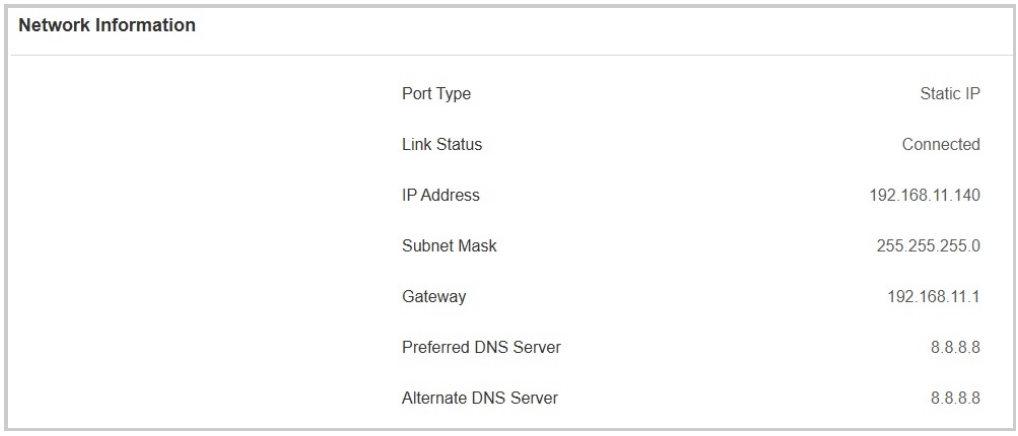
- **Display User Info**: Display the user information after facial recognition or card swiping. For example, if facial recognition succeeds, the text prompt “Access Granted” with the user ID and name will pop up on the device screen. If it fails, the text prompt “Access Denied” with “Stranger, Name: Unknown” will be displayed.

Network Setting

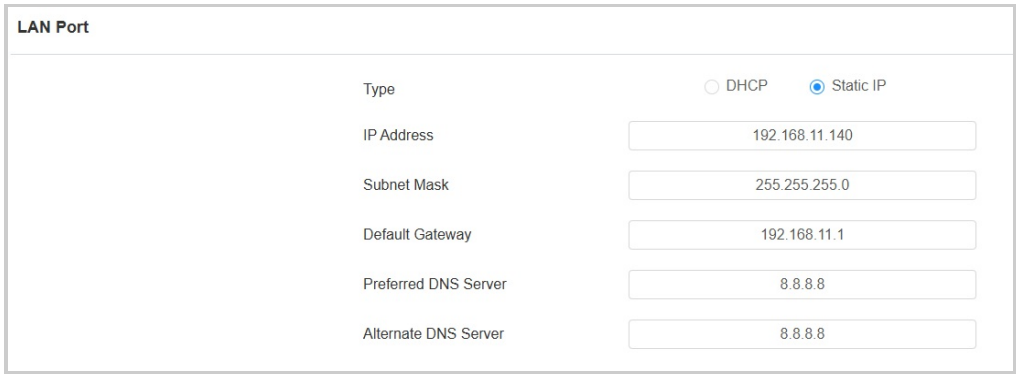
Device Network Connection

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

Check the network status on the **Status > Info** interface.

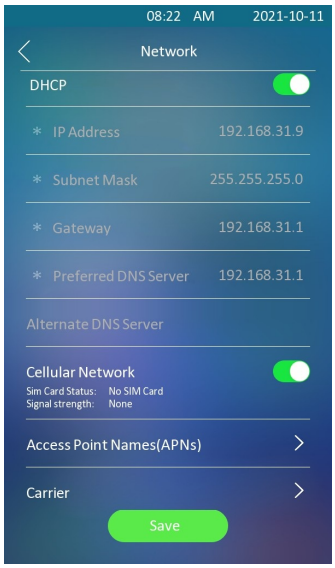


Set up the network on the **Network > Basic** interface.



- **Type**:
  - **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the access control terminal 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/Alternate DNS Server**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The door phone connects to the alternate DNS server when the primary one is unavailable.

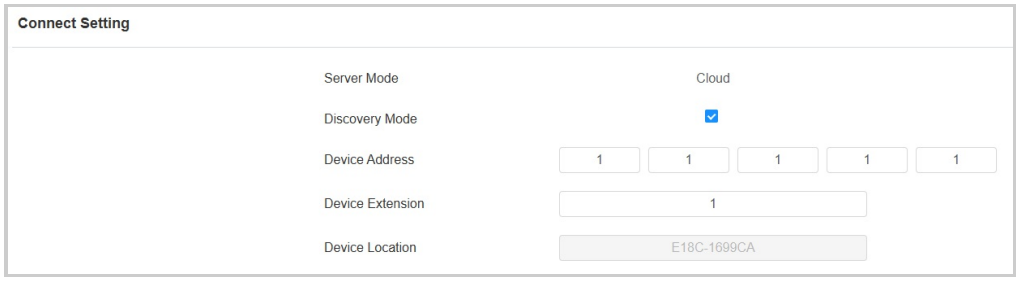
You can also set up the network on the **Setting > Network** screen.



Device 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.



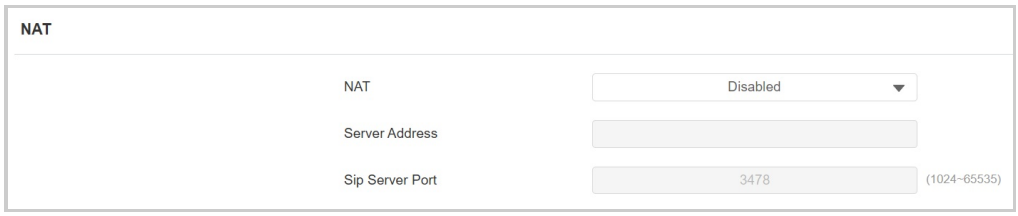
- **Server Mode**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None.
  - **None**: None is the default factory setting, indicating the device is not in any server type. Devices connect directly to each other or within a local area network (LAN) without relying on external servers.
  - **Cloud**: The device is connected to the SmartPlus Cloud, a cloud-based system simplifying property access management. The Cloud mode allows devices to interact intelligently with one another and the mobile SmartPlus App, backing up data daily and on different hosts. It suits projects requiring smart, flexible, and secure deployment and management.
  - **SDMC**: The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.
- **Discovery Mode**: Enabled by default. Available for the None server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address**: Available for the None server mode. It can be used to call the device. Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for the None server mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for the None server mode. Uneditable in Cloud and SDMC mode.

NAT Setting

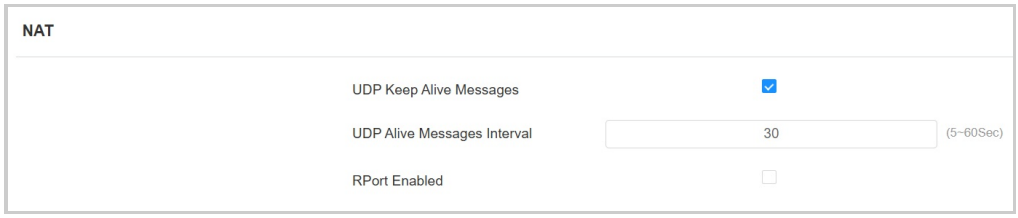
Network Address Translation(NAT) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses and hides the internal IP addresses and ports from the outside world.

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

Enabled NAT on the **Account > Basic > NAT** interface.



To set it up, go to **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 Enabled**: Enable the RPort when the SIP server is in a WAN.

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.

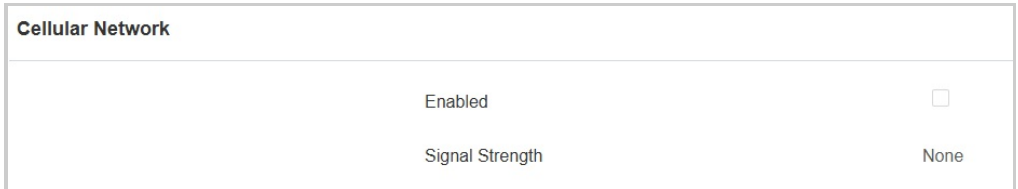


- **HTTP Redirect**: It is enabled by default, which means the device's web can be accessed using HTTP. If it is disabled, all requests will automatically switch to HTTPS.

LTE Wireless Connection

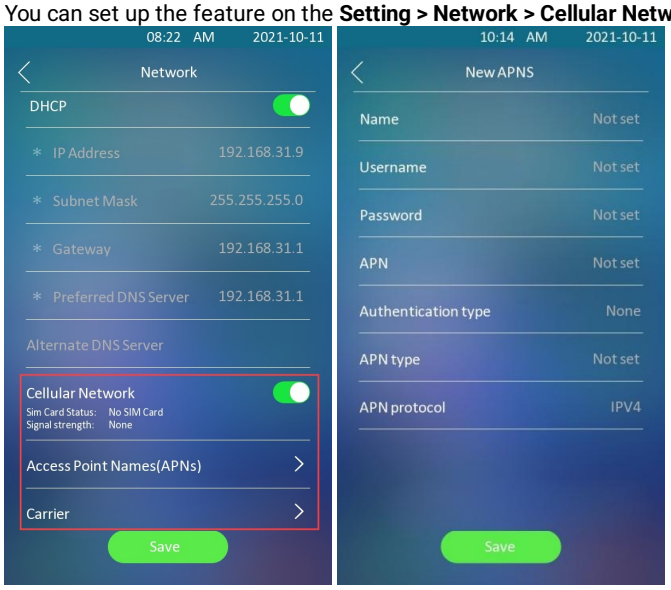
The LTE module enables cellular network connectivity for the device in areas where wired networks are unavailable, particularly beneficial for installations in older buildings.

Enable cellular network on the **Network > Advanced** interface.



- **Signal Strength**: Indicate the network connection.
  - **None**: No SIM card inserted or the SIM card is not properly inserted, unable to detect signal.
  - **Weak**: Network signal is poor, typically when the signal strength is below -100 dBm.
  - **Fair**: Network signal is average, usually when the signal strength is between -90 and -100 dBm.
  - **Good**: Network signal is good, generally when the signal strength is between -70 and -90 dBm.
  - **Excellent**: Network signal is excellent, typically when the signal strength is between -50 and -70 dBm.

You can set up the feature on the **Setting > Network > Cellular Network** screen.



- **Cellular Network**: Enable or disable the LTE function. The signal strength has four levels: Weak, Fair, Good, and Excellent.
- **Access Point Name (APNs)**: Check the Cellular Network provider for the Access Point. You can also add and delete APNs manually.
- **Carrier**: Enable or disable the network provided by the network service provider.

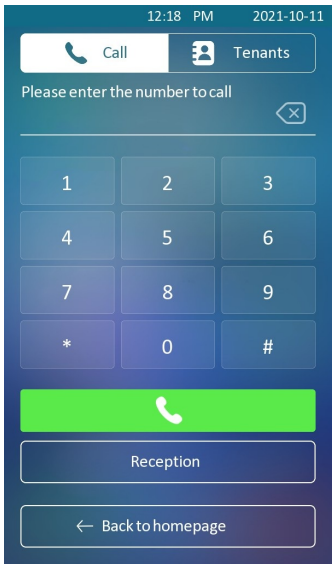
Intercom Call Configuration

IP Call Configuration

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

Make IP/SIP calls

To make a direct IP call on the device, press the Dial icon , then enter the IP or SIP number such as 192*168*35*123, and press to call out.



IP Call Setup

Set up IP call on the **Intercom > Basic > Direct IP** interface.



- **Port:** Set the port for direct IP calls. The default is 5060, with a range from 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.

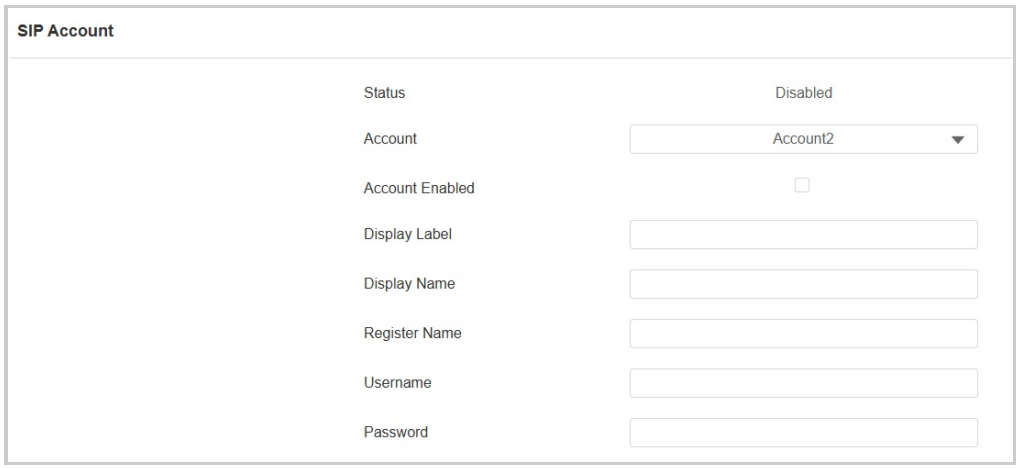
SIP Account Registration

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.

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



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

Tip

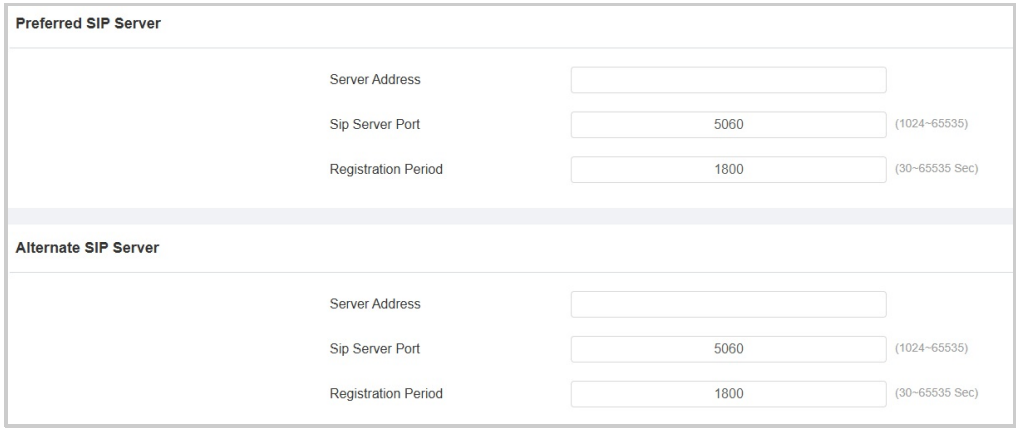
When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

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

SIP Server Configuration

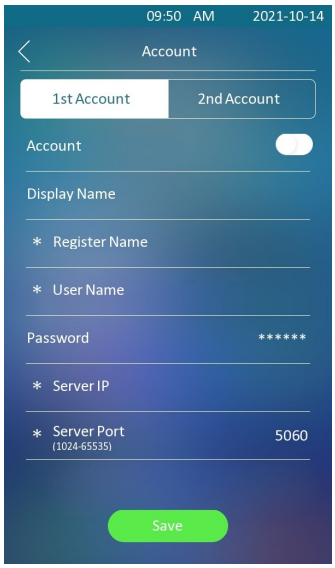
SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

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



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

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



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 Type** interface.

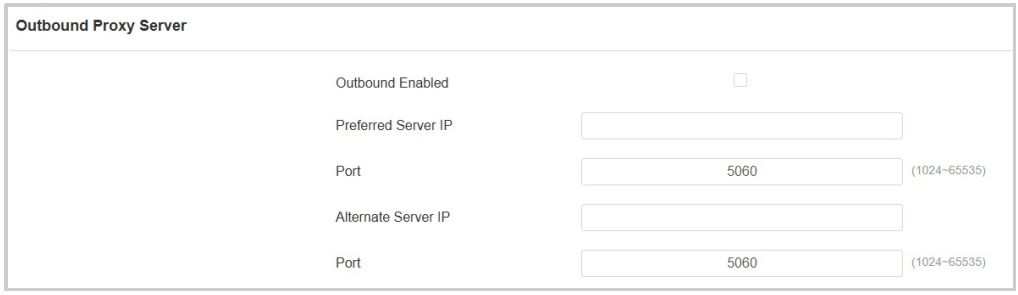


- **Default Account**:
  - **Auto**: The device will use the registered account to make SIP calls. If both are registered, Account 1 will be used by default.
  - **Account 1**: Calls can only be made to Account 1's contacts.
  - **Account 2**: Calls can only be made to Account 2's contacts.

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 **Account > Basic > Outbound Proxy Server** interface.



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

Data Transmission Type

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

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



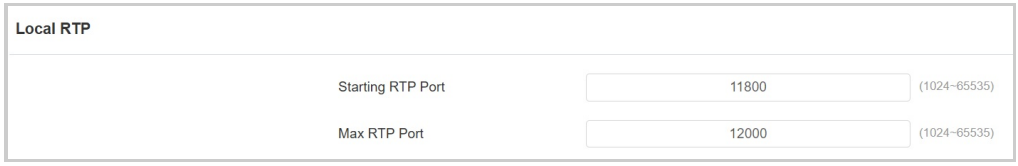
- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

Device Local RTP

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 web **Network > Advanced > Local RTP** interface.

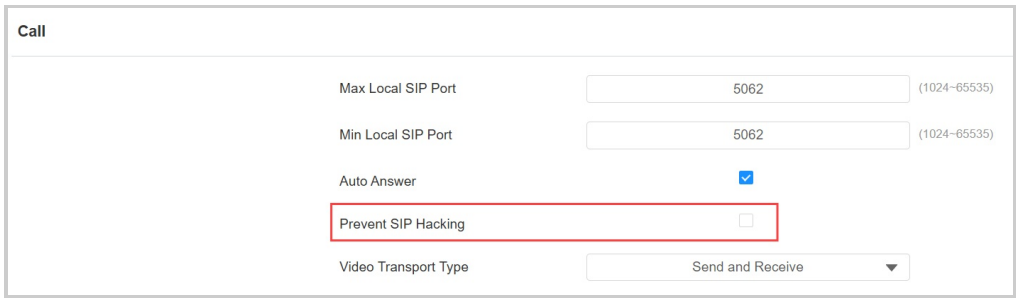


- **Starting RTP Port**: The port value to establish the start point for the exclusive data transmission range.
- **Max RTP port**: The port value to establish the endpoint for the exclusive data transmission range.

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.

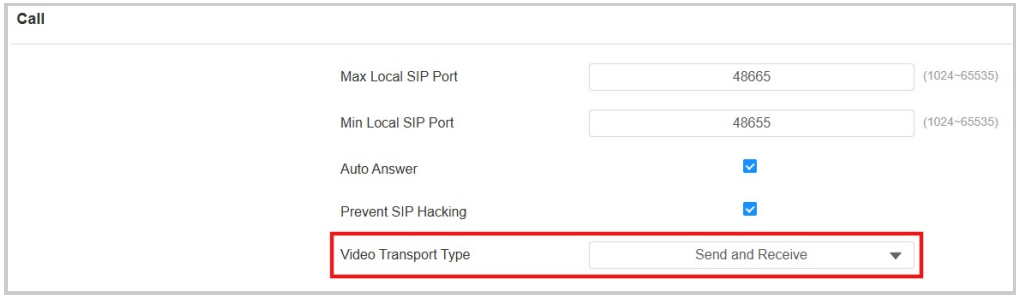
To set it up, go to the web **Account > Advanced > Call** interface.



- **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.

Video Transport Type

You can set the video transport type for SIP calls on the **Account > Advanced > Call** interface.



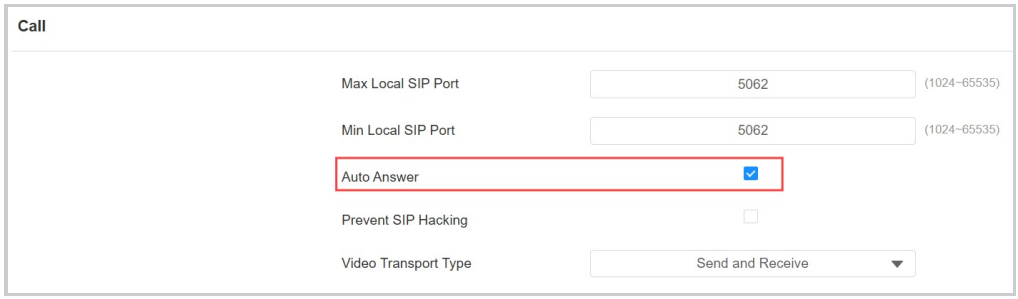
- **Video Transport Type**: It is Send and Receive by default.
  - **Inactive**: Disable the function.
  - **Send Only**: The device sends the video stream to the other party.
  - **Receive Only**: The device only receives the video stream from the other party.
  - **Send and Receive**: The device can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

Call Settings

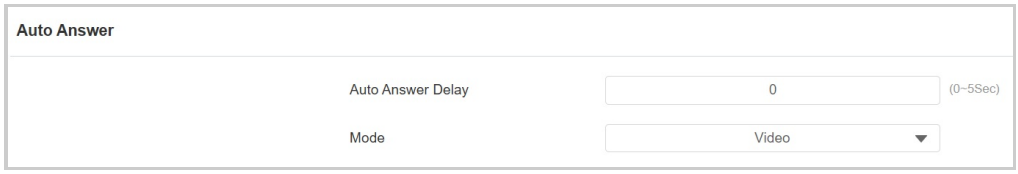
Call Auto-answer

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.



You can further set it up on the **Intercom > Call Feature > Auto Answer** interface.

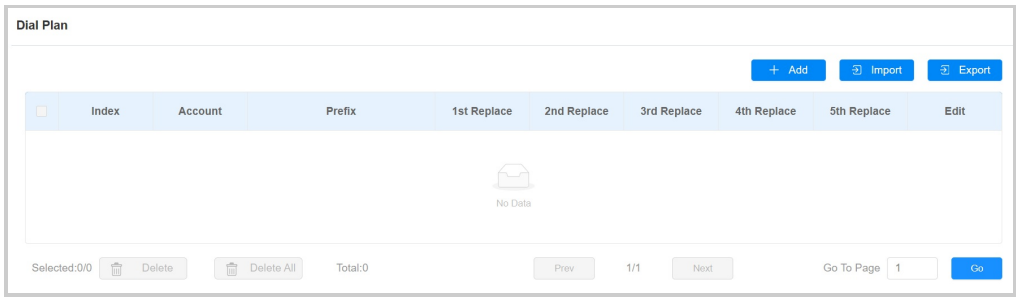


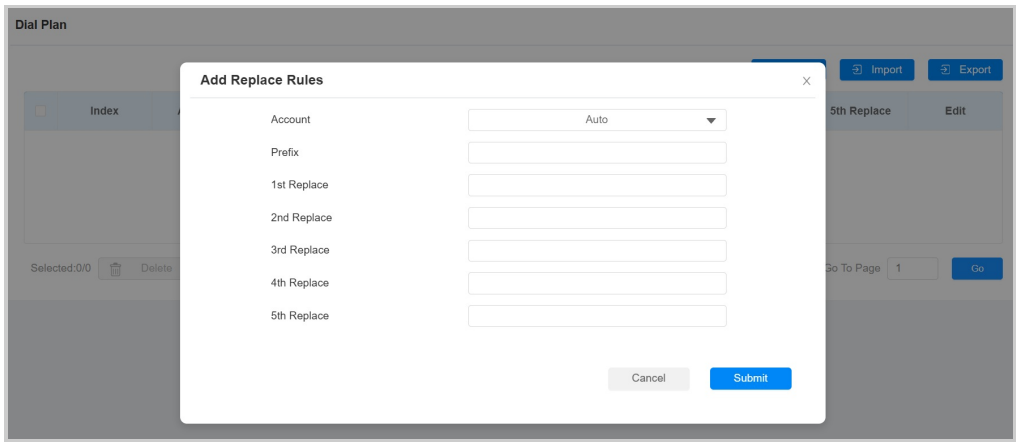
- **Auto Answer Delay**: Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode**: Determine whether to auto-answer the call as a video or audio call.

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** interface. Click **+Add**. You can add 1,000 dial plan rules.





- **Account:** Select the dial-out account.
  - **Auto:** Dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.
  - **Account 1/2:** Dial-out using the chosen account.
- **Prefix:** Specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** Specify up to 5 numbers, which can be SIP numbers or IP addresses, to be replaced by the prefix. All these numbers will be called simultaneously when the caller dials the prefix.
  When E18's version is 18.30.10.255 or higher, it supports making dial plan calls using 2 accounts. Click here to view the details.

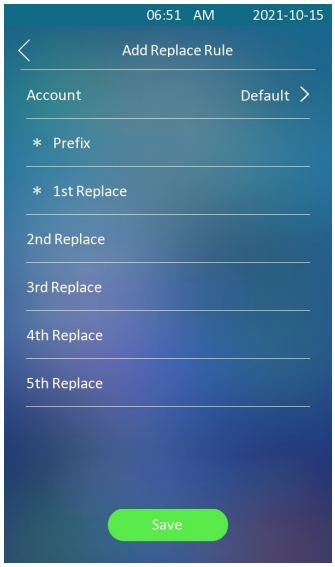
You can import/export the dial plan numbers in a batch.



Note

Max File Size:200KB; Format:.xml.

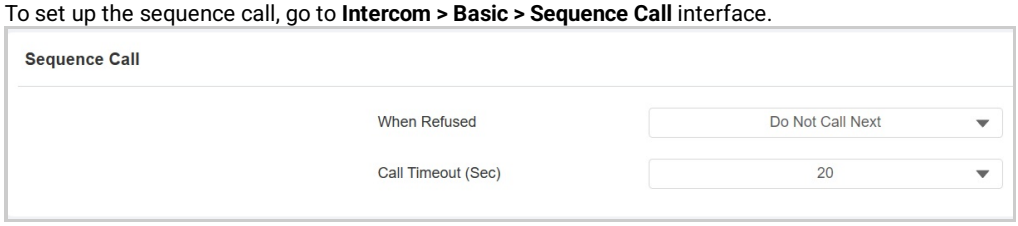
You can also configure the dial plan on the **Setting > Replace Rule** interface.



Sequence Call

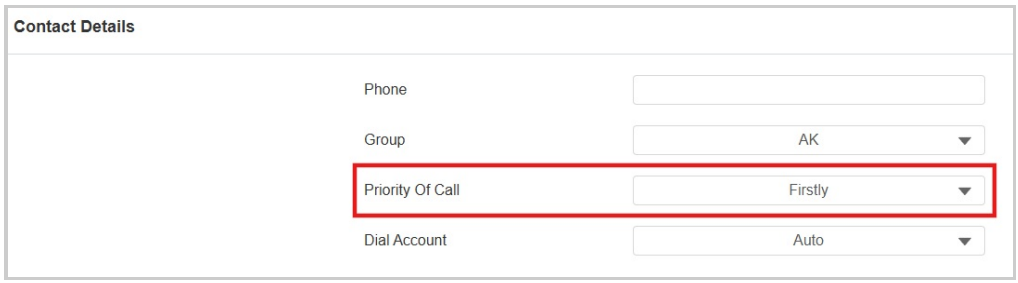
Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application. Please click here for the detailed configuration.

To set up the sequence call, go to **Intercom > Basic > Sequence Call** interface.



- **When Refused**:
  - **Do Not Call Next**: The device will stop calling.
  - **Call Next**: The device will continue to call the next number.
- **Call Timeout(Sec)**: Determine the duration before calling the next number when the previous call is not answered.

The call order for local contacts can be set on the User Add/Edit interface. The Priority of Call option can only be configured when the contact is assigned to a self-created group.



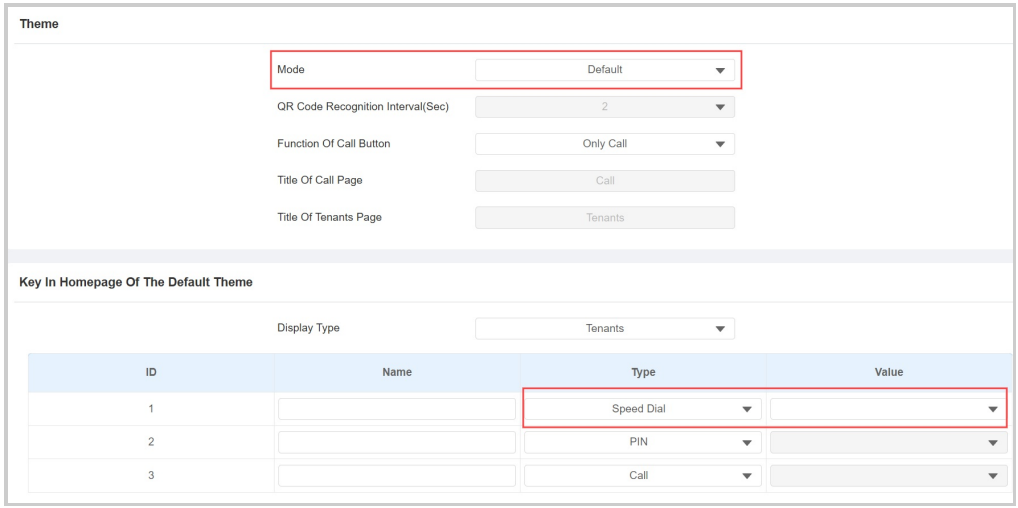
Speed Dial

Speed dial is a function that allows you to create a tab or a combination of organized tabs to be displayed on the device's dial screen. You can make calls by pressing the specific tabs to make speedy calls without entering any dial numbers.

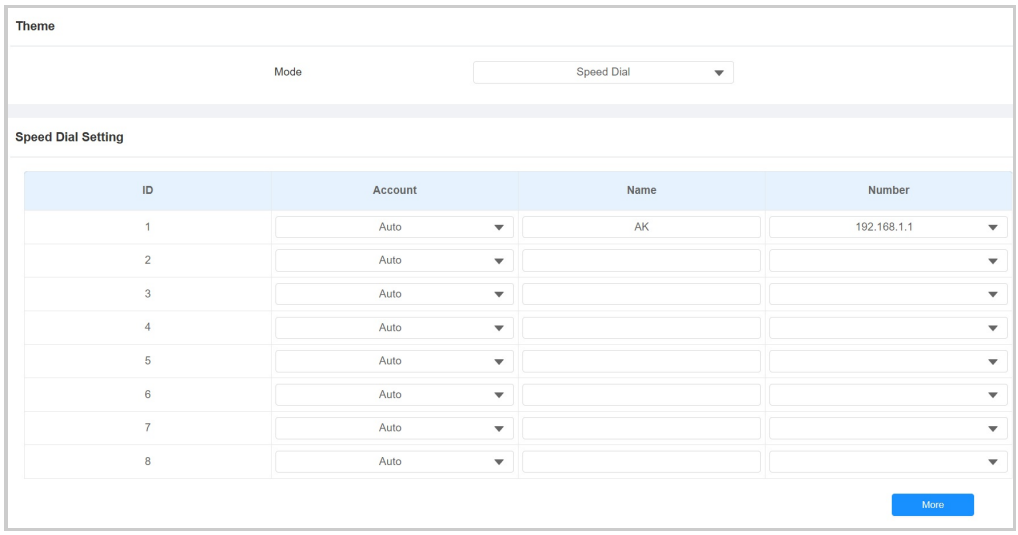
You can set up speed dial in the Default and Speed Dial home screen display mode on the **Device > LCD** interface.

Support entering multiple numbers separated by ";".

Default Mode:



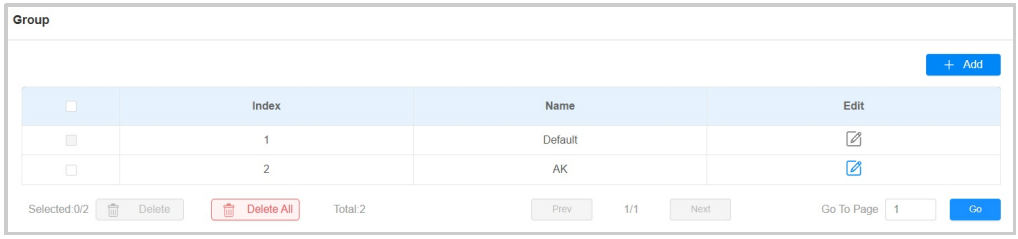
Speed Dial Mode:



Group Call

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

Set up local groups on the **Directory > User** interface. Click +Add to create a new group. You can assign users to specific groups when adding or editing users.



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



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

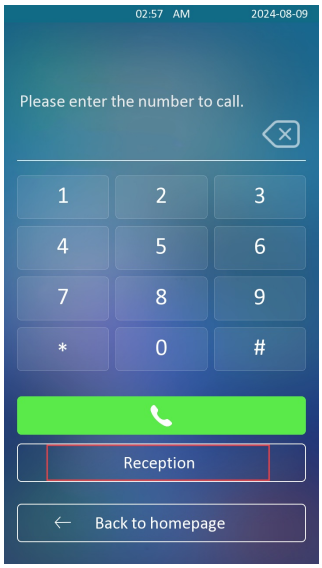
Call the Reception Center

You can configure the Reception button on the device's call screen for quick one-touch calling.

Set it up on the **Intercom > Basic > Key Setting** interface.



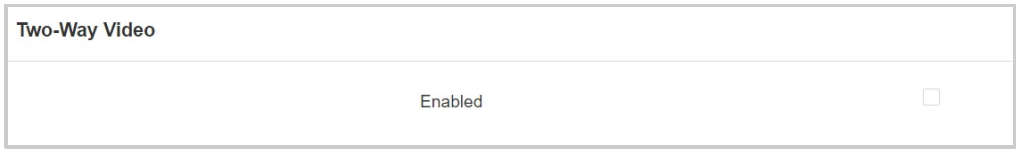
- **Name**: Name the button.
- **Number**: Enter the IP/SIP number, multiple numbers separated by ";".



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 > Two-way Video** 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 call, and the device answers it.
  - In all other cases, only audio communication is displayed.

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 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.



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

Note

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

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

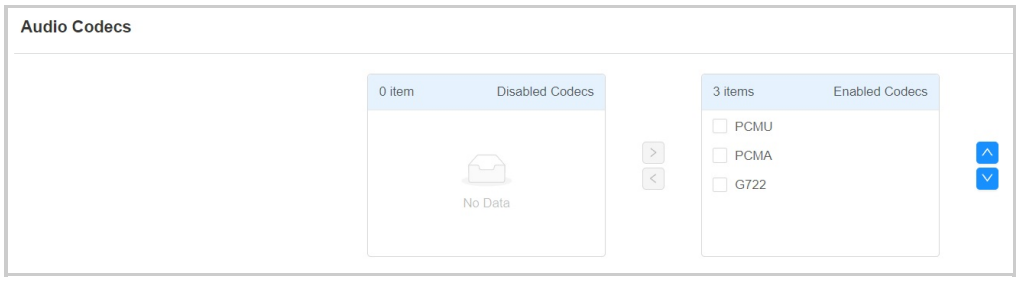
Audio & Video Codec Configuration

Audio Codec

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

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

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



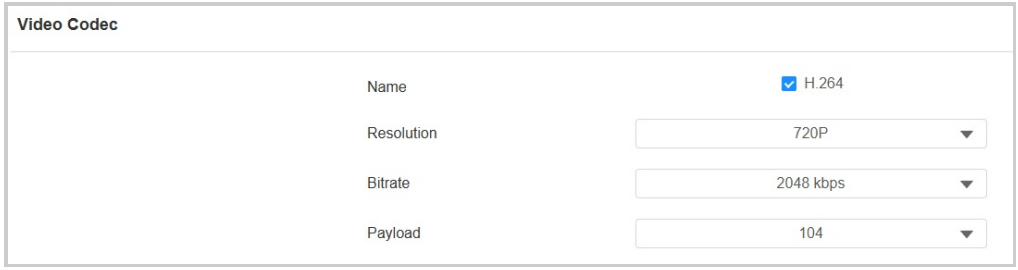
Please refer to the bandwidth consumption and sample rate for the codec types below:

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.

Set it up on the **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.

Contacts Configuration

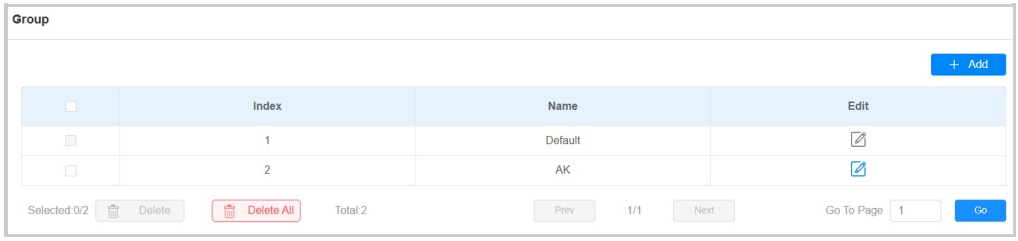
The local contact information is used to initiate SIP or IP calls to users. You can group the contact information to facilitate group calls to target users. Moreover, the contact list functions as a whitelist, allowing only listed numbers to open doors via DTMF during calls.

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

Manage Contact Groups

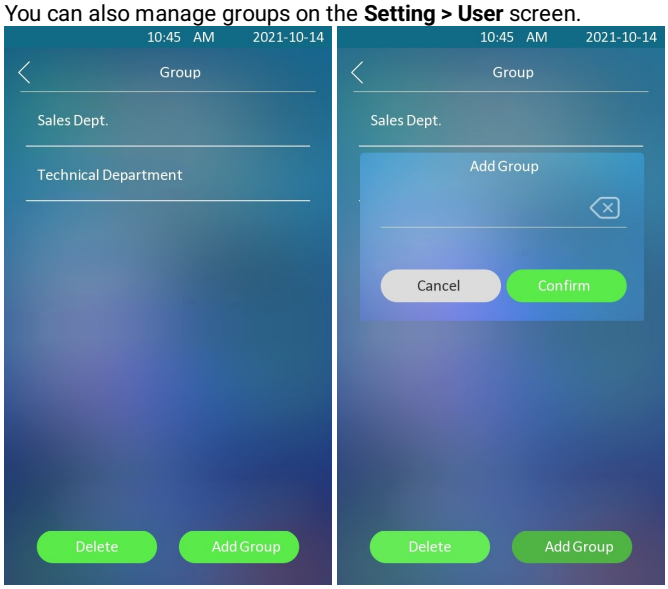
You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

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.





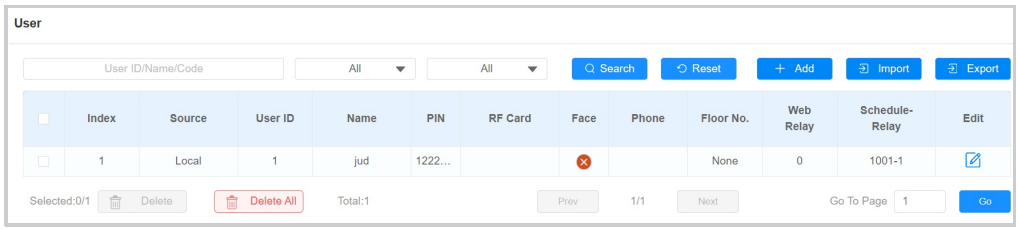
You can also manage groups on the **Setting > User** screen.

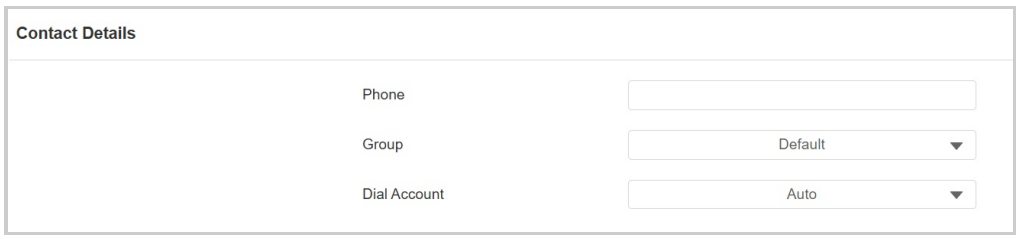


Set up Contact Details

You can add the user's contact information on the **Directory > User** interface. The user will be displayed on the device's **Directory** screen.

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



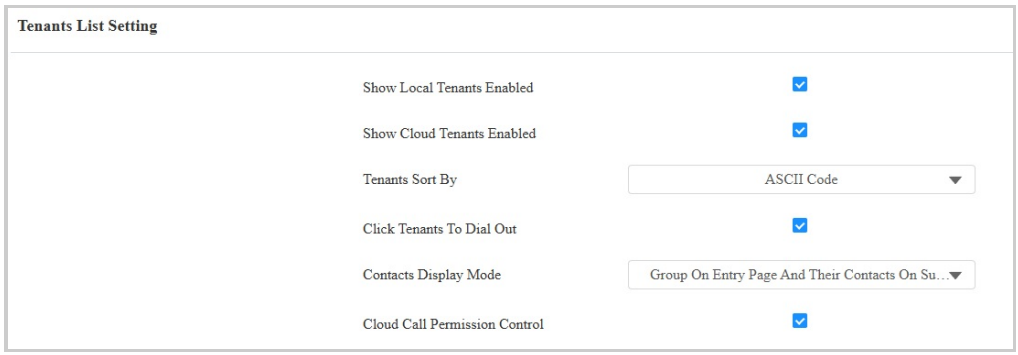


- **Phone**: The SIP or IP number.
- **Group**: Assign the contact to the Default or self-created group.
- **Priority of Call**: Set the priority of the call among three options: Primary, Secondary, and Tertiary. For example, set the priority of a call for one of the contacts in a specific contact group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



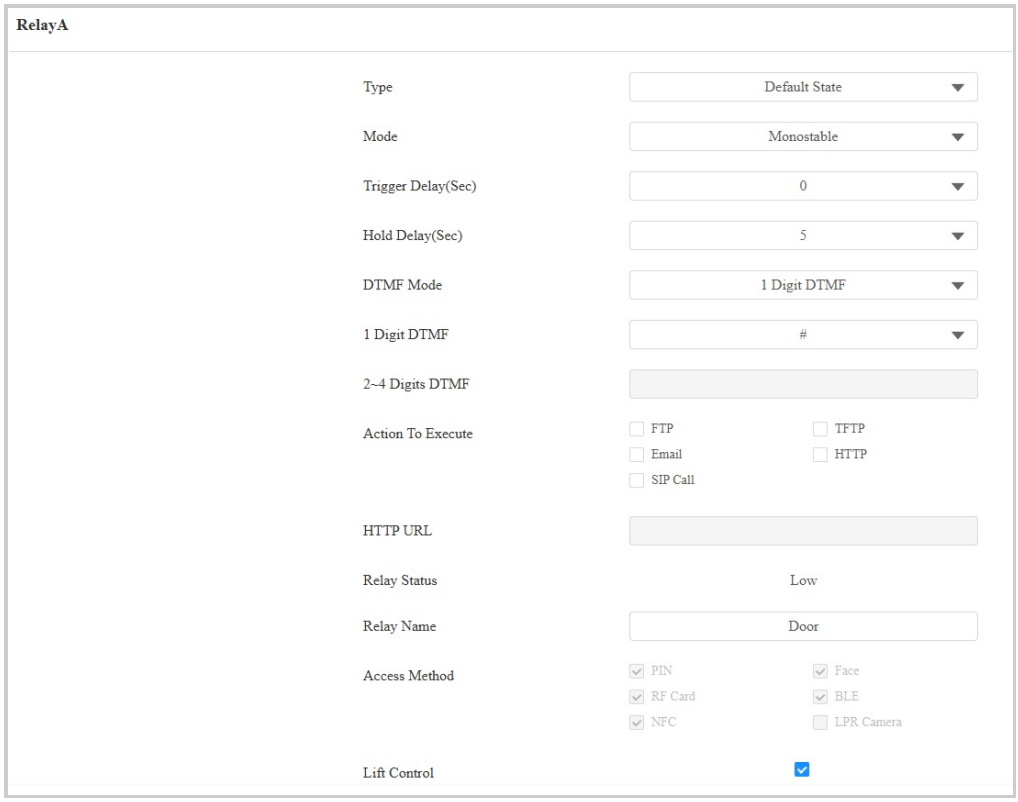
- **Show Local Tenants Enabled**: The local contacts can be displayed on the device's Tenants list.
- **Show Cloud Tenants Enabled**: The contacts configured in SmartPlus Cloud will be displayed on the device's Tenants list.
- **Tenants Sort By**:
  - **ASCII Code** lists the tenants by their names in the sequence of the ASCII code.
  - **Room No.** lists the tenants according to their room numbers.
  - **Import** lists the tenants according to their order in the imported file.
- **Click Tenants to Dial Out**: When enabled, users can directly tap a specific tenant name to call.
- **Contacts Display Mode**:
  - **All Contacts**: Display all the contacts.
  - **Groups Only**: Display contact groups. Press the desired group on the device screen to make a group call.
  - **Groups On Entry Page And Their Contacts On Subpage**: Display contacts by groups. Press the group, and users can see the contacts in it.
- **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 Setting

Local Relay

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

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



Type: Determine the interpretation of the Relay Status regarding the state of the door:

Default State: A "Low" status in the Relay Status field indicates that the door is closed, while "High" indicates that it is open.

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

- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open for 5 seconds before closing.
- **DTMF Mode**: Set the digits of the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Action To Execute**: Set the desired actions that occur when the relay 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.
  - **TFTP**: Send a screenshot to the preconfigured TFTP server.
- **HTTP URL**: Enter the HTTP URL if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Relay Status**: Indicate the states of the relay, which are normally open and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).

- **Relay Name**: Assign a distinct name for identification purposes.
- **Access Method**: Check the method(s) to trigger the relay.
- **Lift Control**: Set whether to perform lift control when the specific relay is triggered.

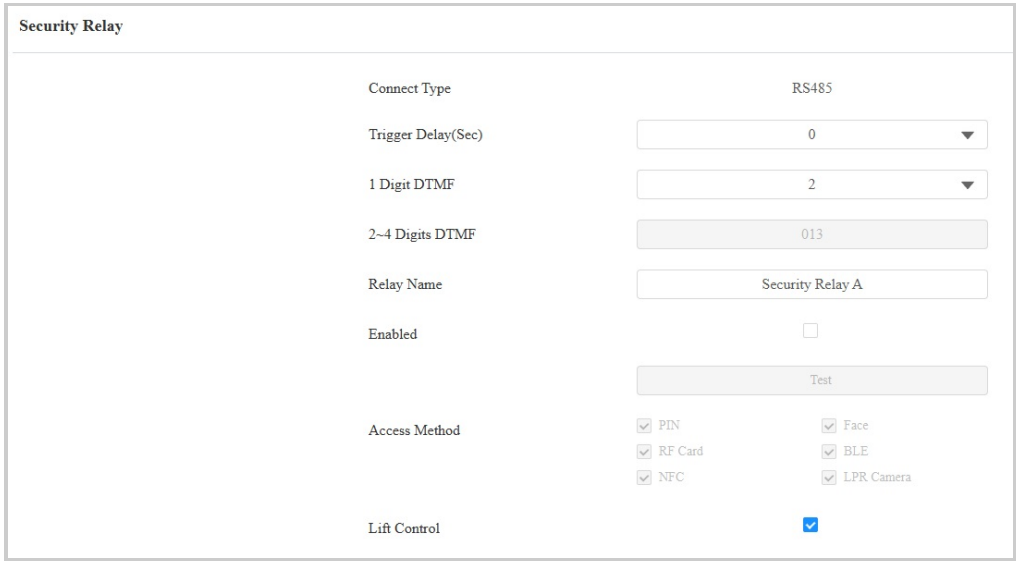
Security Relay

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



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

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



- **Connect Type**: The security relay connects to the door phone using RS485 by default.
- **Trigger Delay (Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name**: Name the security relay. The name can be displayed in door-opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method**: Check the method(s) to trigger the relay.
- **Lift Control**: Set whether to perform lift control when the specific relay is triggered.

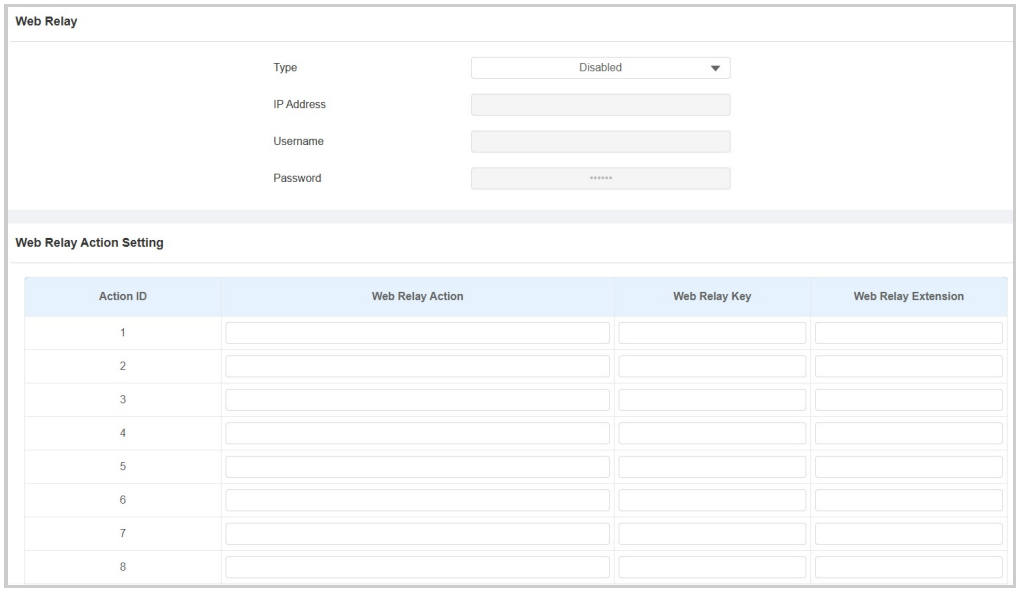
Web Relay

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



- **Type**: Determine the type of relay activated when employing door access methods for entry.

- Disabled: Only activate the local relay.

- Web Relay: Only activate the web relay.

- Local Relay+Web Relay: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay.

- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **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**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

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

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

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

- Leaving it blank enables all door-opening methods.

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

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

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

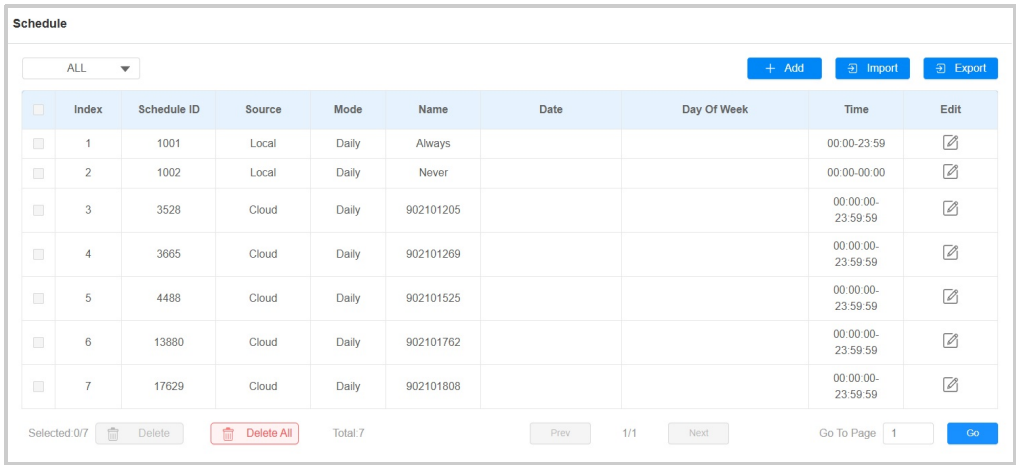
Door Access Schedule Management

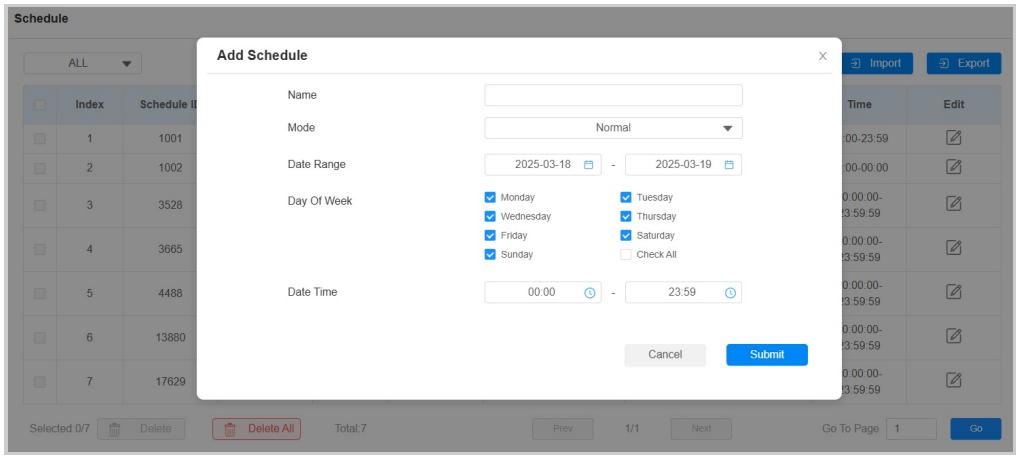
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create a Door Access Schedule

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

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

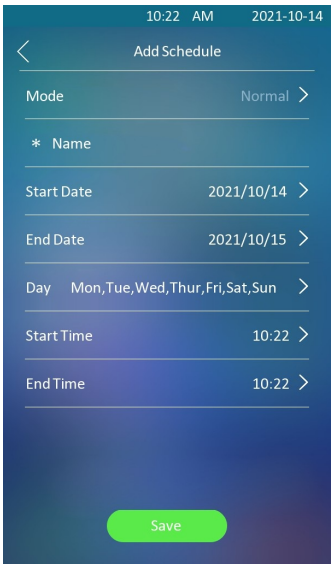




- **Name**: Name the schedule.
- **Mode**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long-term schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.

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

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



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.

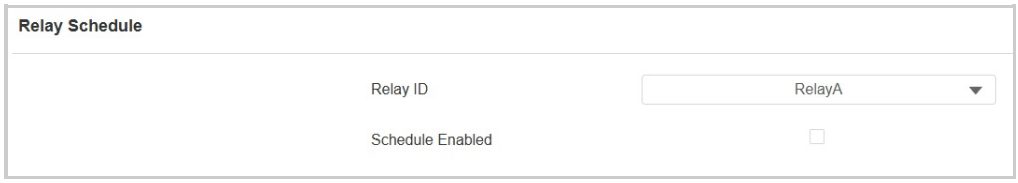
To set it up, go to the **Setting > Schedule** interface. The export/import file is in **XML** format.



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.

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

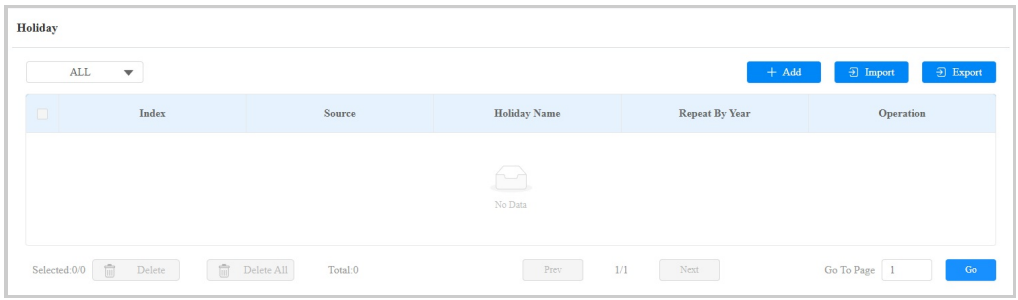


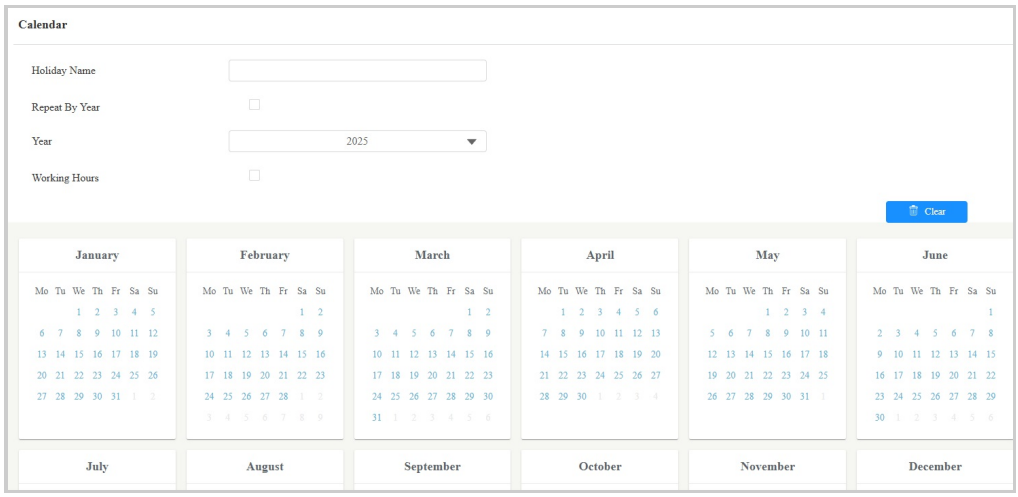
- **Relay ID**: Specify the relay you need to set up.
- **Schedule Enabled**: Assign particular door access schedules to the chosen relay. Simply move them to the Enabled Schedules box.
  For instructions on creating schedules, kindly consult the Create a Door Access Schedule section.

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 to add a schedule.





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

Holiday Schedule Import/Export

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

The import/export file format is XML.



Door-opening Configuration

Unlock by Public PIN

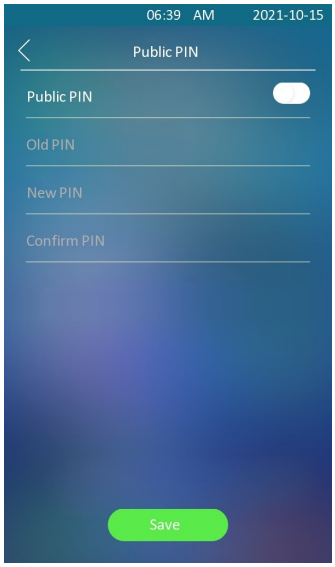
There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex. You can create and modify both the public and private PIN codes.

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



- **PIN Code**: Set a 4-8 digit PIN code accessible for universal use.

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

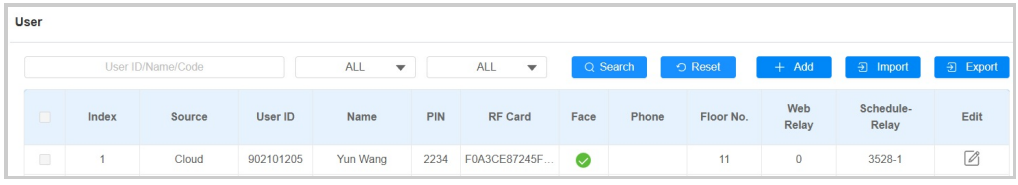


User-specific Access Methods

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

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

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





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

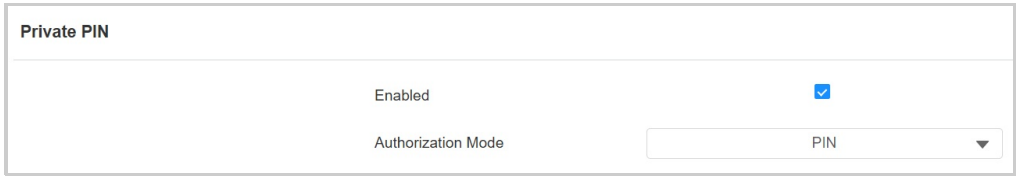
Unlock by Private PIN Code

On the **Directory > User > +Add** interface, scroll to the **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 on the **Access Control > PIN Setting > Private PIN** interface.



- **Authorization 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.

Unlock by QR Code

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

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

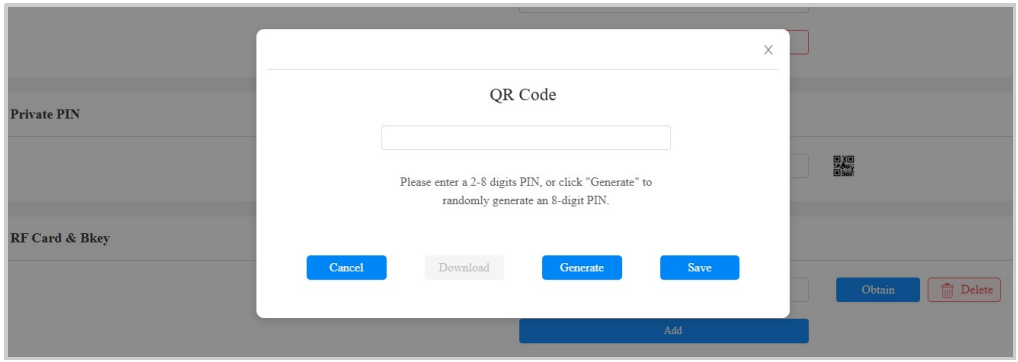
The feature can be enabled on the **Access Control > Relay > Open Relay via QR Code** interface.

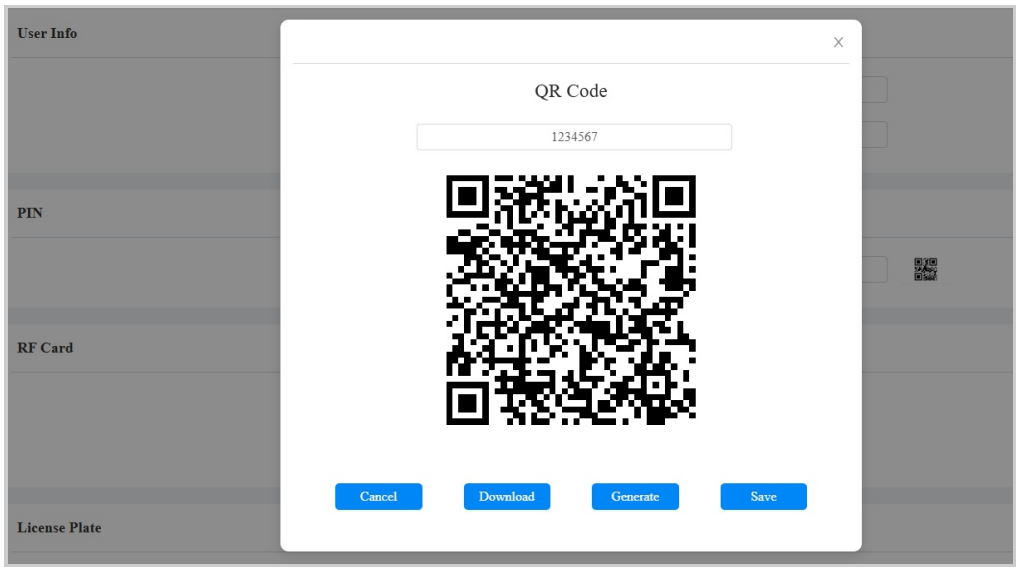


On the **Directory > User > +Add** interface, scroll to the **PIN** section. Click the QR code icon.



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 code.

Unlock by RF Card

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

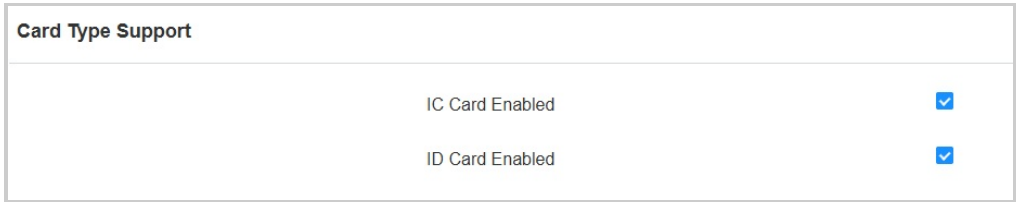


- **Code**: The card number that the card reader reads.

Note:

- 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.

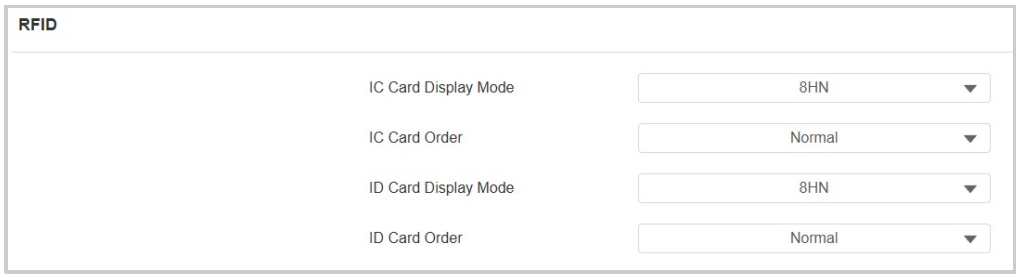
You can enable and disable the use of RF cards on the **Access Control > Card Setting** interface.



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

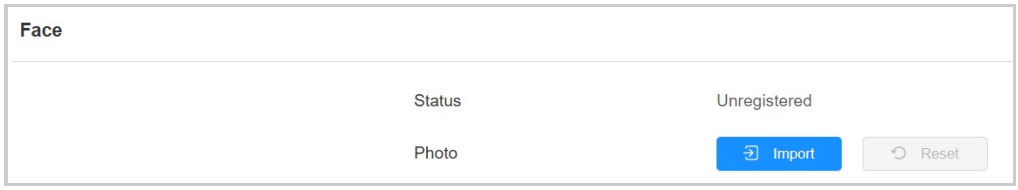
To assign the license plate to a user, find the **License Plate** part on the **Directory > User > +Add** interface.



- **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.

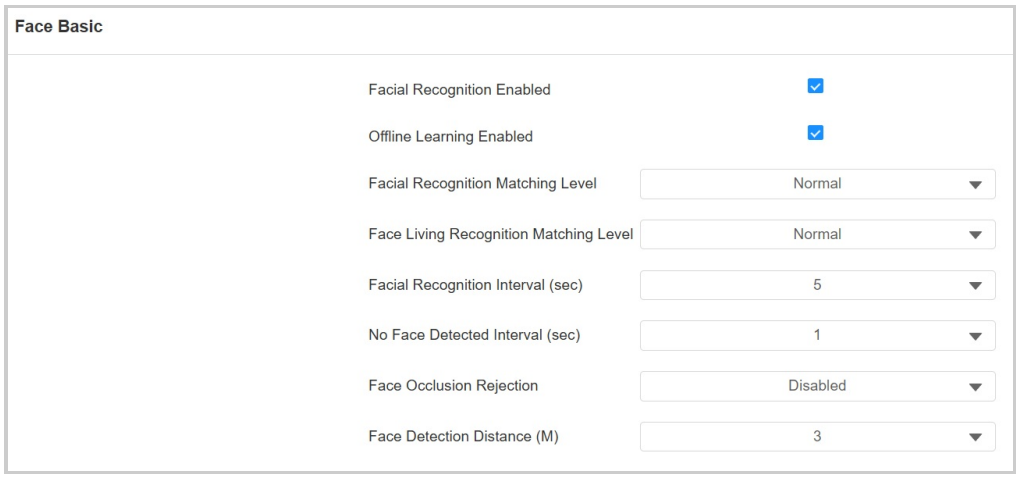


> **Note**
> Support Format: jpg, png, bmp, and jpeg; Max File Size: 2M.

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.

- **Face Living Recognition Matching Level**: Set how strict the system is in preventing fake faces.

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

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

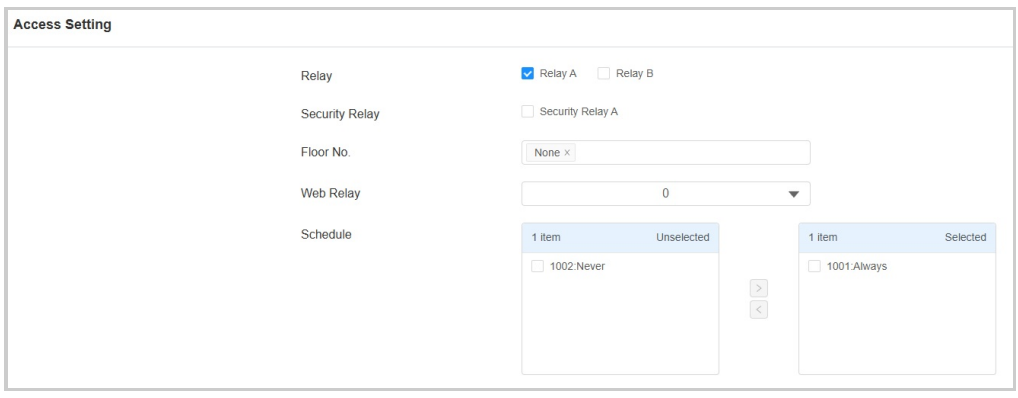
- The other three levels are in between.

- **Facial Recognition Interval(Sec)**: Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.
- **No Face Detected Interval(Sec)**: Adjust the time interval between each detection, ranging from 1 to 8 seconds.
- **Face Occlusion Rejection**: When enabled, if the user is detected to be wearing a mask, he/she will not be able to pass the face recognition.
- **Face Detection Distance(M)**: Adjust the detection distance, ranging from 1 to 3 meters.

Access Setting

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

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



- **Relay**: Specify the relay to be opened.
- **Security Relay**: When the device is connected to a security relay. You can check the option to permit users to trigger the security relay.
- **Floor No.** : Specify the accessible floor(s) to the user via the elevator.

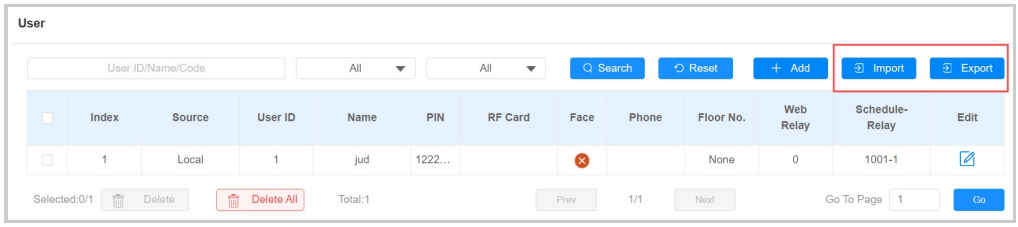
- **Web Relay**: Specify the ID of the web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
  - **Always**: Allows door opening without limitations on door open counts during the valid period.
  - **Never**: Prohibits door opening.

Import/Export User Data

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

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

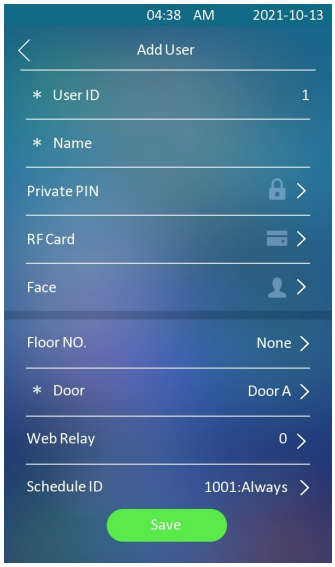
To set it up, go to the **Directory > User** interface.



Note

- The imported/exported file is in TGZ format.
- The device supports 20,000 users.

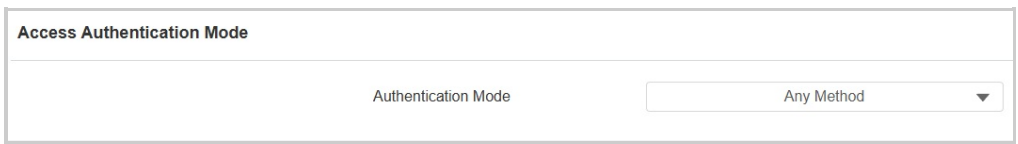
You can also manage users on the **Setting > User** screen.



Access Authentication Mode

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

To set it up, go to **Access Control > Relay > Access Authentication Mode** interface.



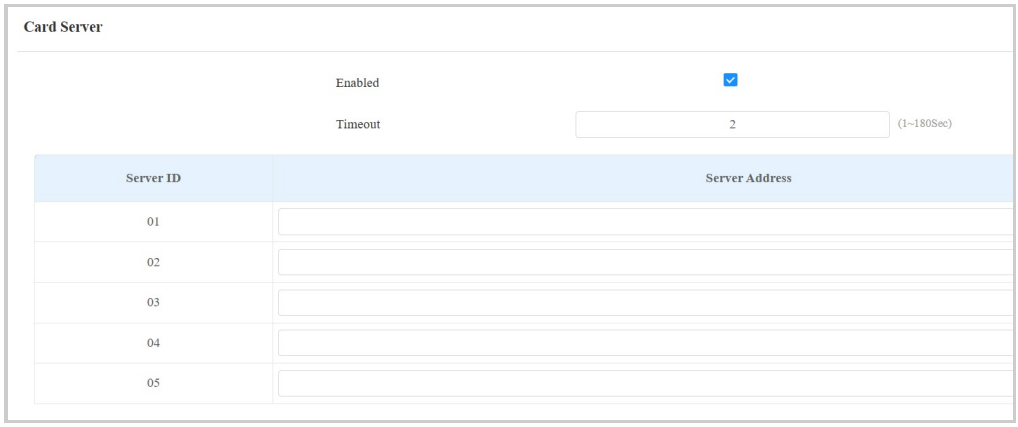
- **Authentication Mode**: Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.
  - **Any Method**: Allow all access methods.

- **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.

Send Card Numbers to Third-Party Servers

The device supports sending card numbers to third-party servers when users swipe cards.

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



- **Enabled**: The feature is disabled by default.
- **Timeout**: Define the timeout of sending the card number(1~180 seconds).
  - For example, if it is set to 5 seconds, when the first server does not respond in 5 seconds, the device will try the next server.
  - This process continues through up to five servers until one of them responds.
  - If all five servers fail to respond, the device will repeat the cycle, with a maximum of three attempts in total.
- **Server Address**: Support up to 5 addresses in HTTP/HTTPS format with a maximum of 256 characters and no restrictions on special characters.

Unlock by NFC

NFC (Near Field Communication) is a popular way for door access. It uses radio waves for data transmission interaction. The device can be unlocked by NFC. You can keep the mobile phone closer to the device for door access.

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



Note

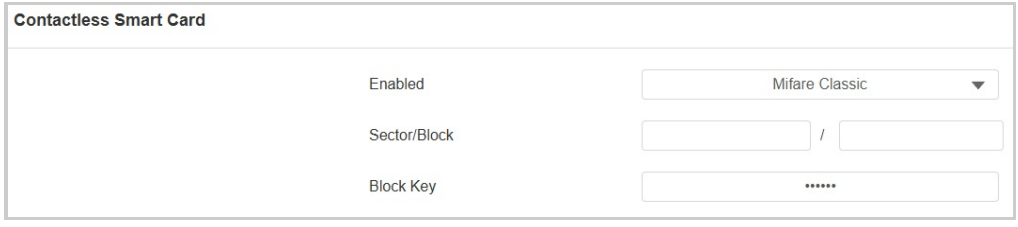
Click **here** to view how to set up door opening by NFC.

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 > Contactless Smart Card** interface.



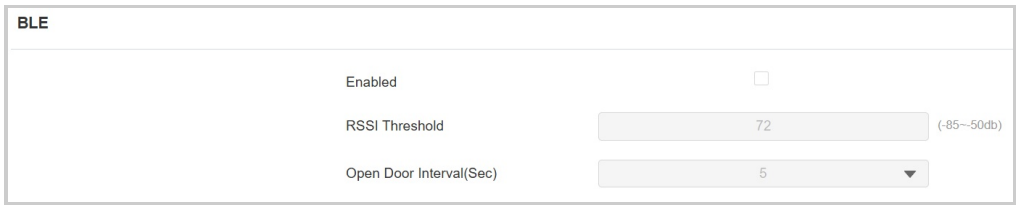
- **Mifare Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
- **Mifare 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.

Unlock by Bluetooth

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

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

To set up the Bluetooth unlocking, go to the **Access Control > BLE** interface.



- **RSSI Threshold**: Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Open Door Interval (Sec)**: Set the time interval between consecutive Bluetooth door access attempts.

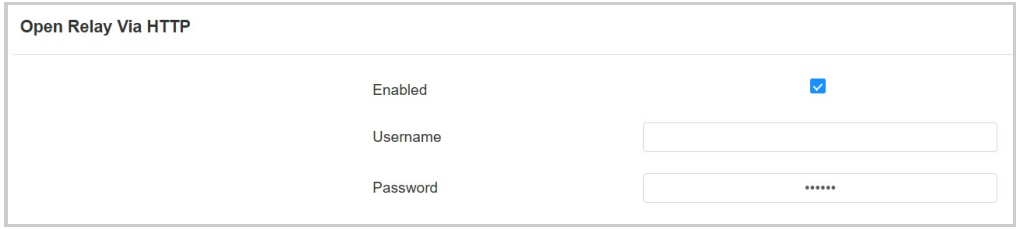
Note

Click **here** to view how to set up door opening via Bluetooth.

Unlock by HTTP Command

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

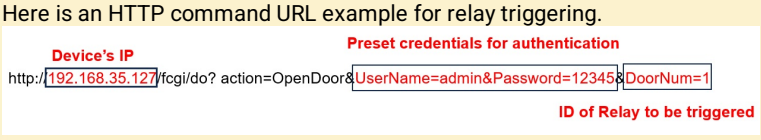
To set it up, go to **Access Control > Relay > Open Relay Via HTTP** interface.



- **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.



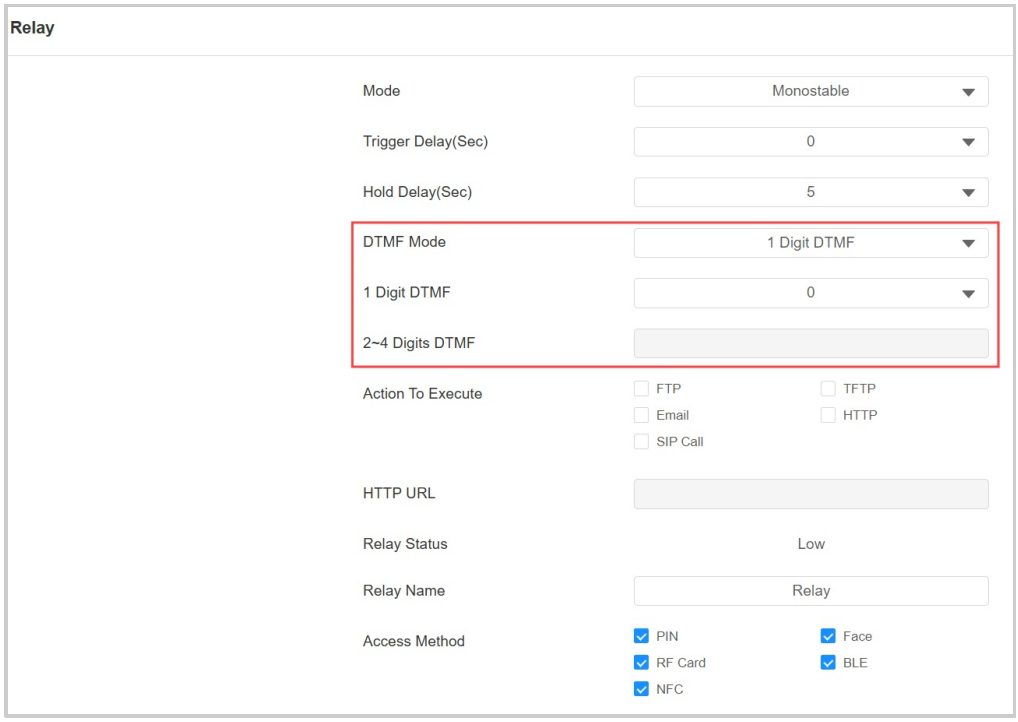
Note

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.



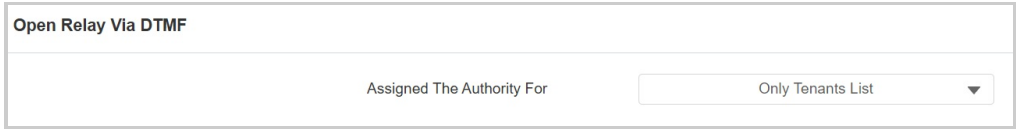
- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

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 Tenants 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.

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



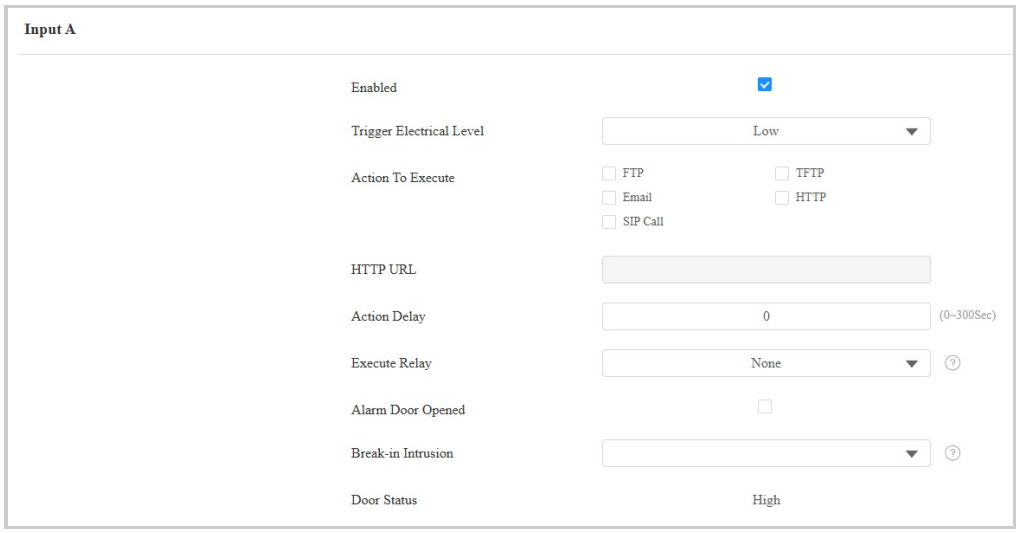
- **Type:** Select from the available options based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, or **Telephone-Event** according to the specific type adopted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

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.
  - **TFTP**: Send a screenshot to the preconfigured TFTP 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 message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.
- **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.

Choose Unlock Options

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

Click here to view the feature details.

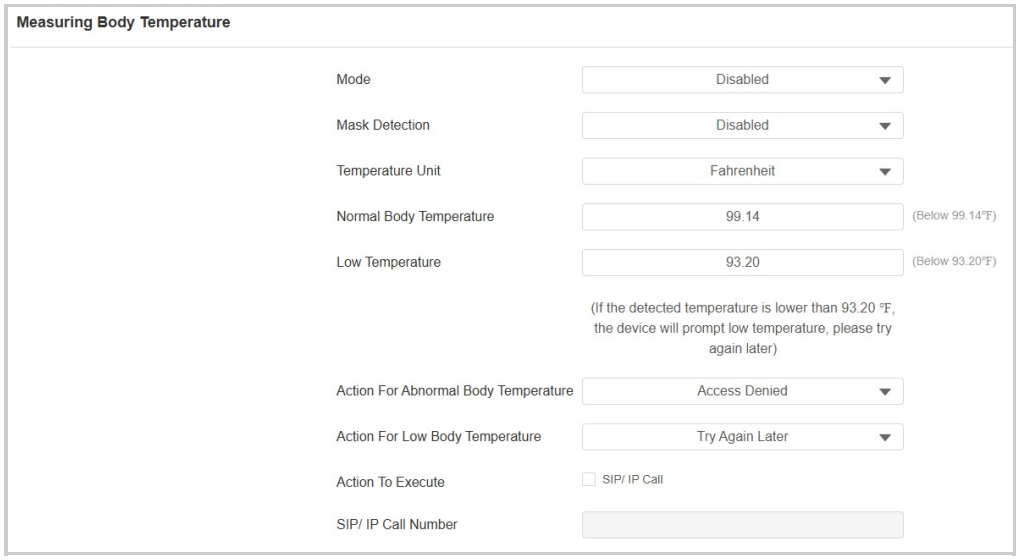
To display the unlock options, go to **Access Control > Relay > Unlock Options** interface.



Temperature Measurement for Door Access

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

> **Note**
> ONLY E18C with the extra module installed supports temperature measurement.



- **Mode**: Enable forehead or wrist temperature measurement, or disable the function.

- Disabled: Turn off temperature measurement.

- Forehead: Measure forehead temperature with a built-in module.

- Wrist: Measure wrist temperature with the additional device.

- **Mask Detection**: Detect whether visitors are wearing masks. When enabled, the device reminds those without masks to wear one with the prompt "Please wear a mask."
- **Temperature Unit**: Select between Celsius and Fahrenheit to specify the measurement used to express temperature.

- **Normal Body Temperature**: Define the fever cut-off temperature. For example, setting it at 37.3 degrees Celsius means any temperature higher than that is considered a fever, triggering the preset action(s) for abnormal body temperature.
- **Low Temperature**: Set the lowest normal temperature. Any temperature below this value triggers the preset designated action(s).
- **Action for Abnormal Body Temperature**: Set the actions that occur when a fever is detected.

- Access Denied: The user will not be allowed to open the door.

- Just for Reminder: The door can be opened, and a prompt of abnormal temperature will pop up on the device.

- **Action for Low Body Temperature**: Set the actions that occur when a low temperature is detected.

- Try again later: The device prompts “Try again later”.

- Just for Reminder: The door can be opened, and a prompt of low temperature will pop up on the device.

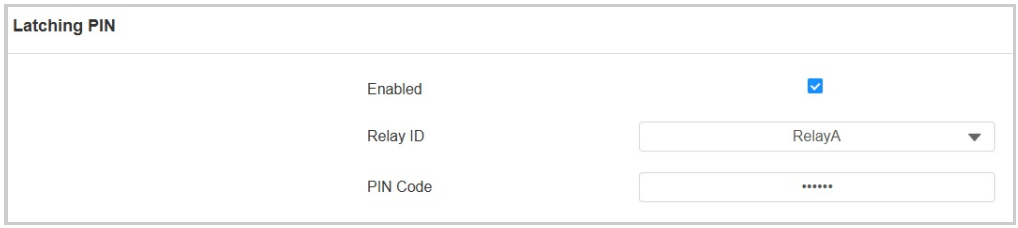
- **Action to Execute**: This field only appears when Access Denied is selected for the Action for Abnormal Body Temperature.

- SIP/IP Call: Call designated numbers, including local numbers, dial plans, SmartPlus numbers, and group ones.

Latching PIN

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

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



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

Note

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

Monitor and Image

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

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

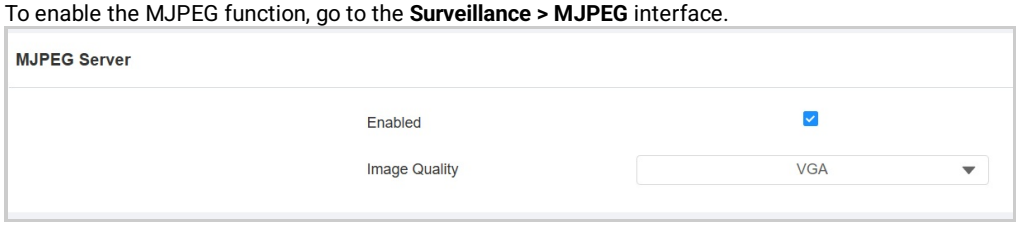
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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

MJPEG 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.



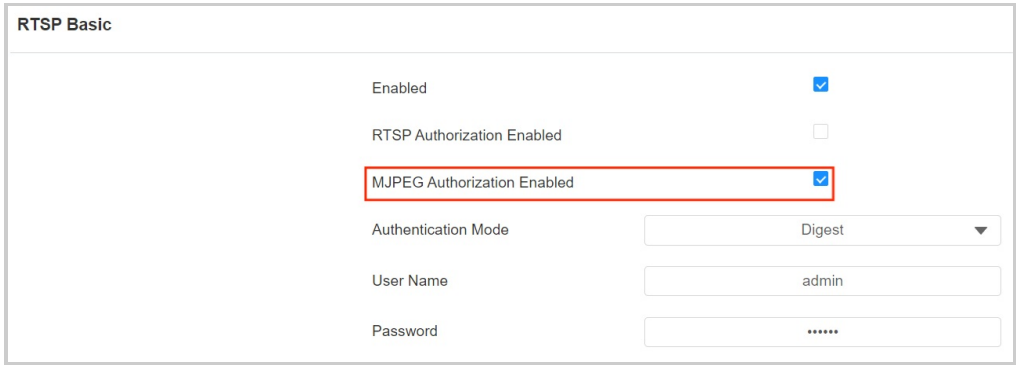
- **Enabled**: Entering the specific URL into the browser can access either an image or a video from the camera.

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.

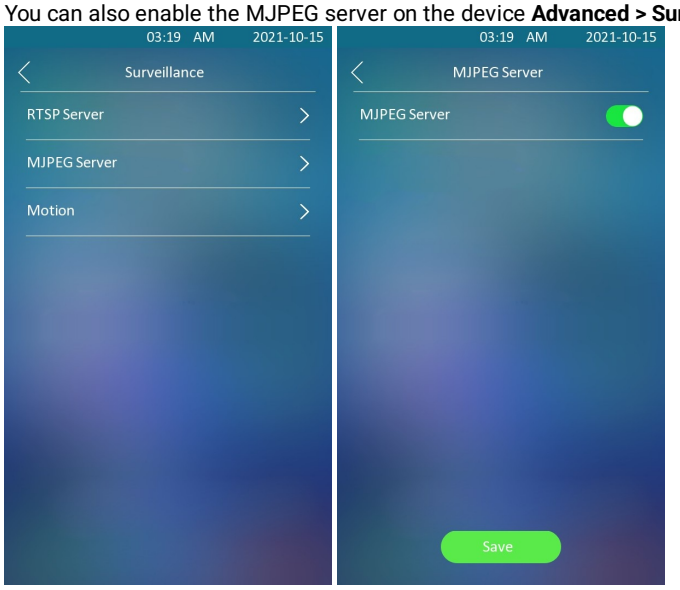
- **Image Quality**: Specify the image resolution, varying from the lowest QCIF(176x144 pixels) to the highest 1080P(1920x1080 pixels). The default is VGA(640×480 pixels).

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



- **MJPEG Authorization Enabled**: It is enabled by default. 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.

You can also enable the MJPEG server on the device **Advanced > Surveillance > MJPEG Server** screen.

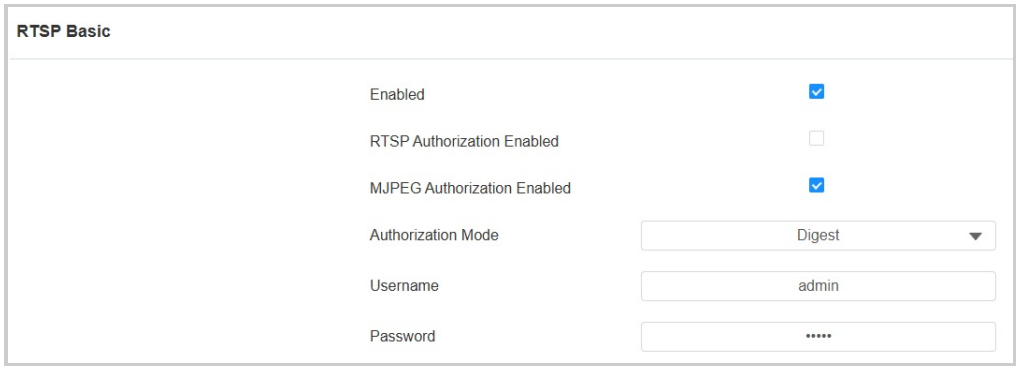


RTSP Stream Monitoring

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.

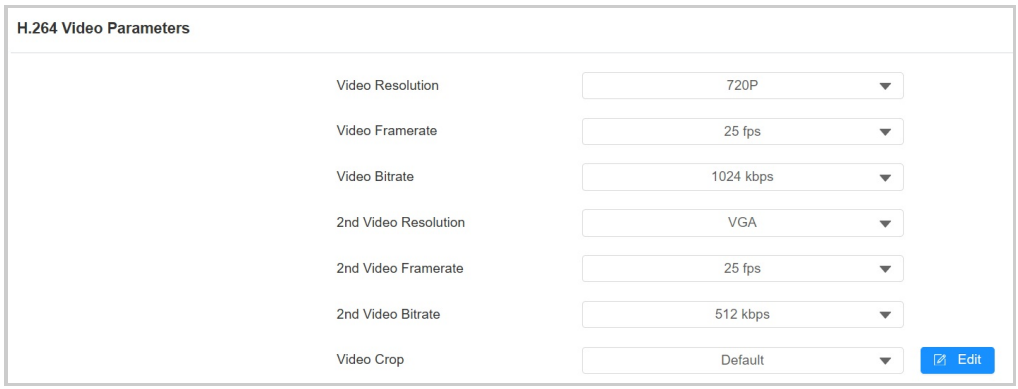
To set it up, navigate to the **Surveillance > RTSP > RTSP Basic** interface.



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

RTSP Stream Setting

The RTSP stream can use 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). The default is 720P.
- **Video Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default frame rate is 25fps.
- **Video Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048 kbps.
- **2nd Video Resolution**: Specify the image resolution for the second video stream channel. The default is VGA.
- **2nd Video Framerate**: Set the frame rate for the second video stream channel.
- **2nd Video Bitrate**: Set the bit rate for the second video stream channel. The default is 512 kbps.
- **Video Crop**:
  - **Default**: The video stream in the RTSP feed or during a call will be enlarged equally to fill the entire screen. If the video is taller than the screen, the excess height will be cropped off from the top and bottom, focusing on the middle part of the video.
  - **Original**: The RTSP stream or video during the call will display the original video without any cropping.

Tip

To view the audio and video stream using RTSP:

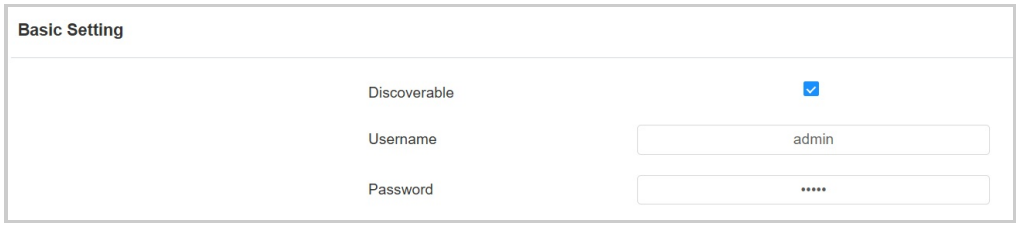
- First channel: rtsp://Device's IP/live/ch00_0
- Second channel: rtsp://Device's IP/live/ch00_1

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.

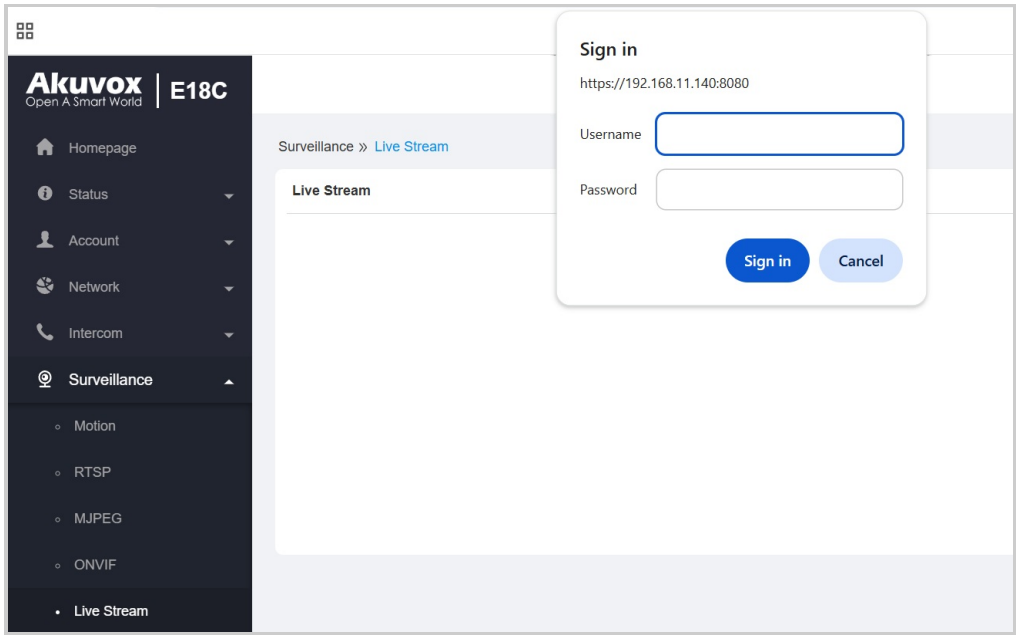
Tip

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.

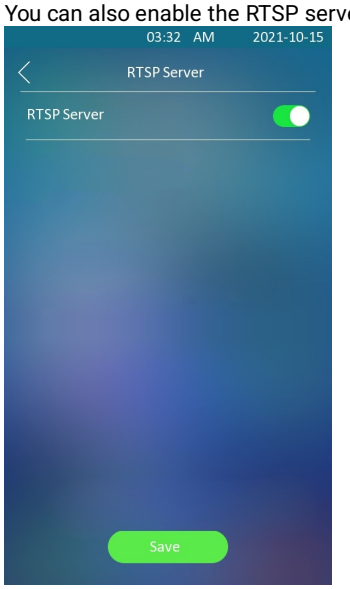
Live Stream

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

View the live stream on the **Surveillance > Live Stream** interface. If MJPEG authorization is enabled, you are required to enter the username and password for authentication set on the RTSP Basic section.



You can also enable the RTSP server on the device's **Advanced > Surveillance > RTSP Server** screen.



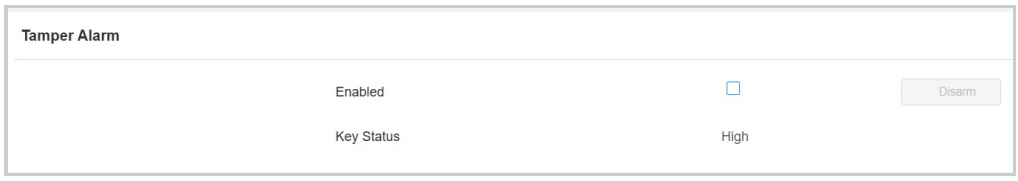
Security

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.

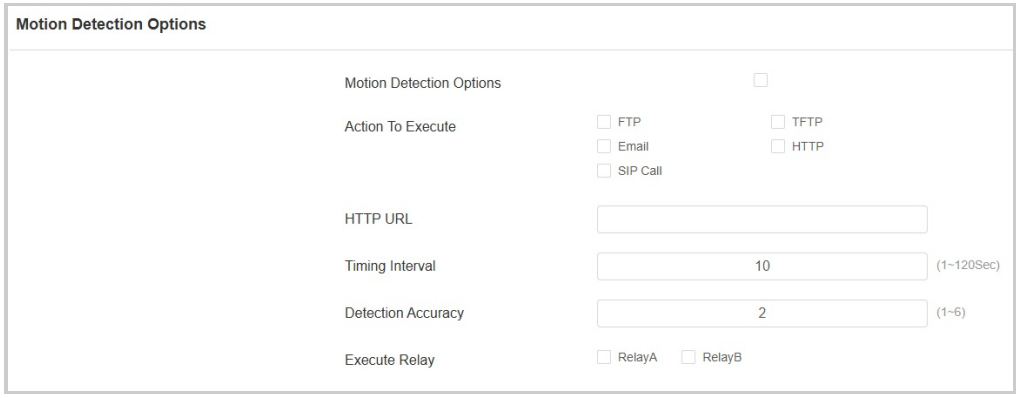
Set it up on the **System > Security > Tamper Alarm** interface. Click **Disarm** to clear the alarm.



Motion Detection

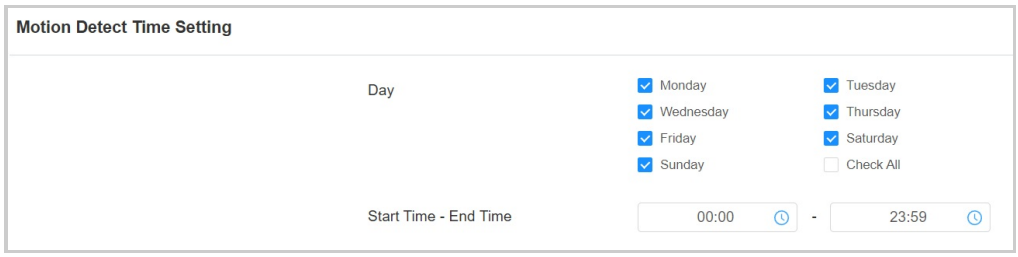
Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved, and activates the system to perform the appropriate action.

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



- **Action To Execute**: Set the desired actions that occur when suspicious movement is detected.
  - **FTP**: Send a screenshot to the preconfigured FTP server.
  - **TFTP**: Send a screenshot to the preconfigured TFTP 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 message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Time Interval:** Determine how to delay and trigger motion detection.
  - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.
  - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
  - The default interval is 10 seconds.
- **Detection Accuracy**: The detection sensitivity. The default detection accuracy value is 2.
- **Execute Relay**: If enabled, the relay will be triggered when unusual motion is detected.

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



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



Security Notification

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

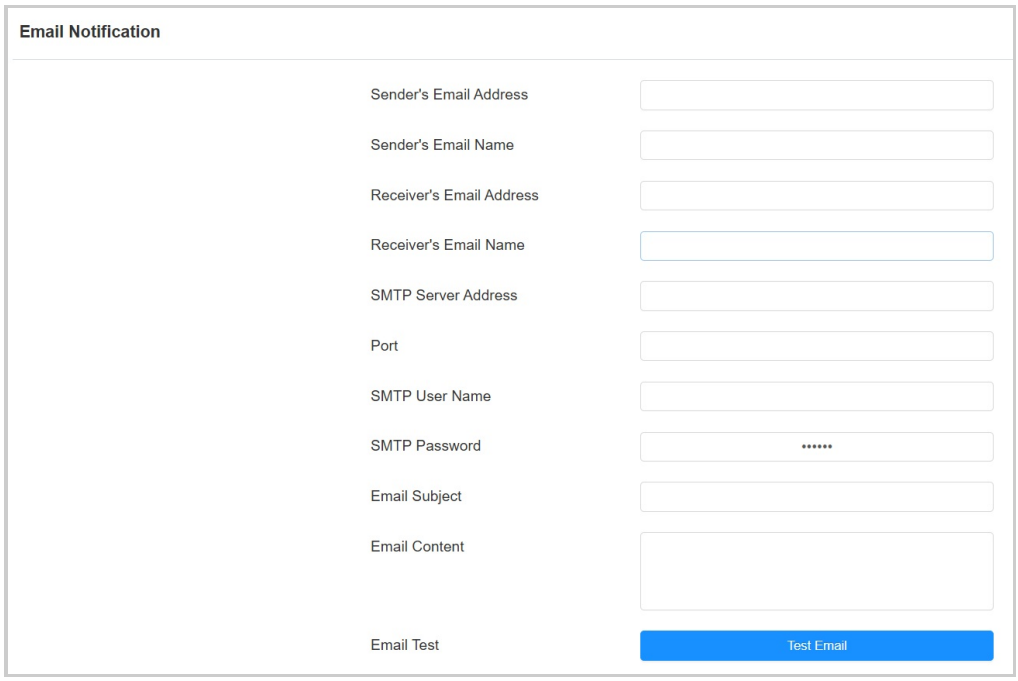
To set up security notifications, go to **Setting > Action** interface.

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.



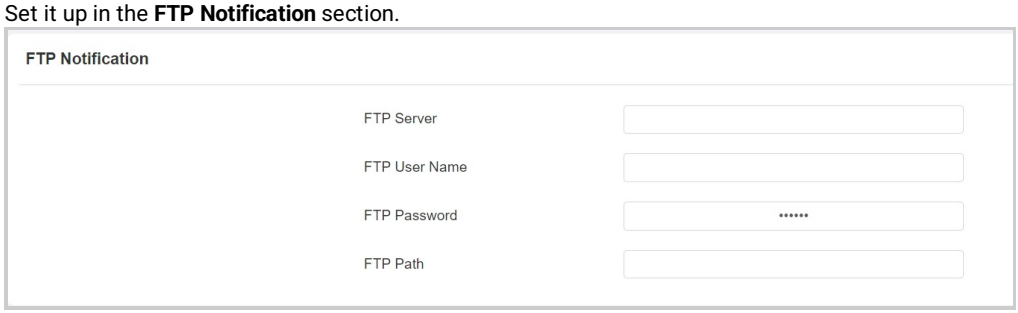
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

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 User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.
- **FTP Path**: Enter the folder name you created on the FTP server.

TFTP Notification

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

Click here to view the configuration steps.

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

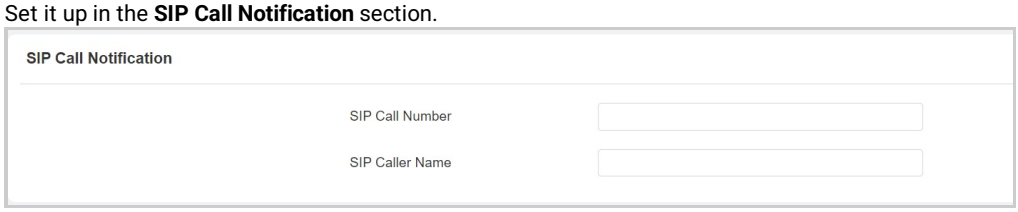


- **TFTP Server**: Enter the address (URL) of the TFTP server.

SIP Call Notification

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

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



Action URL

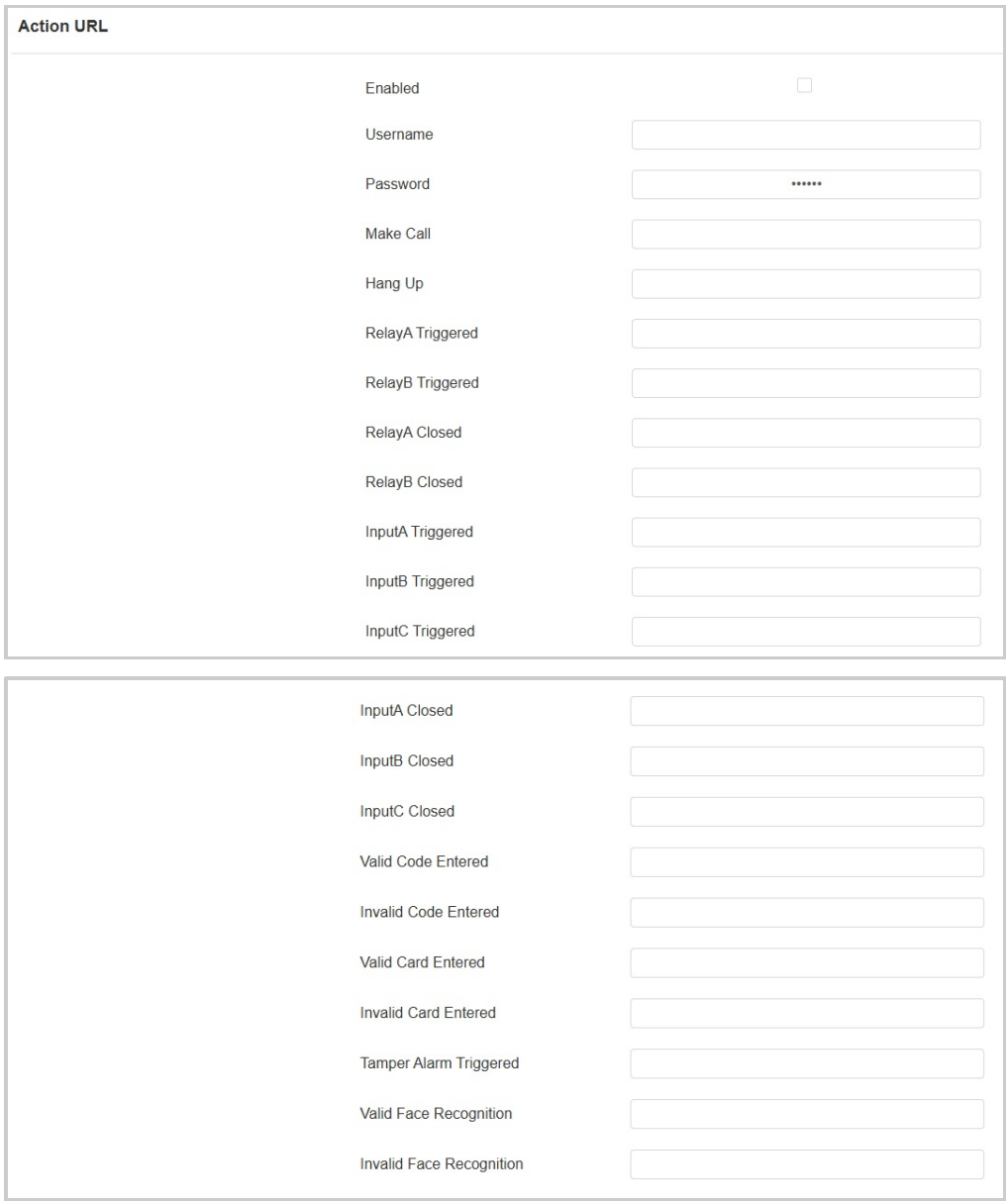
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/ Callnumber=$remote
2	Hang Up	$remote	Http://server ip/ Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Relay Closed	$relay1status	Http://server ip/relayclose=$relay1status
5	Input Triggered	$input1status	Http://server ip/inputtrigger=$input1status
6	Input Closed	$input1status	Http://server ip/inputclose=$input1status
7	Valid Code Entered	$code	Http://server ip/validcode=$code
8	Invalid Code Entered	$code	Http://server ip/invalidcode=$code
9	Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
10	Invalid Card Entered	$card_sn	Http://server ip/invalidcard=$card_sn
11	Tamper Alarm Triggered	$alarmstatus	http://server ip/tampertri=$alarmstatus
12	Valid Face Recognition	$unlocktype	http://serverip/unlocktype=$unlocktype:floor=$floor:webrelay=$webrelay:userid=$userid

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

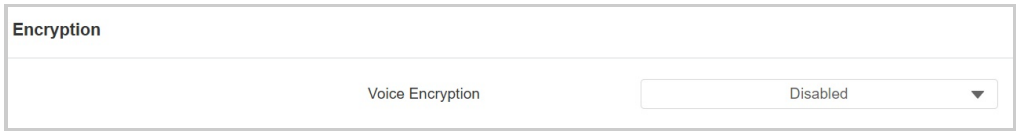
To set it up, go to the **Setting > Action URL** interface. You can set the username and password for authentication.



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.

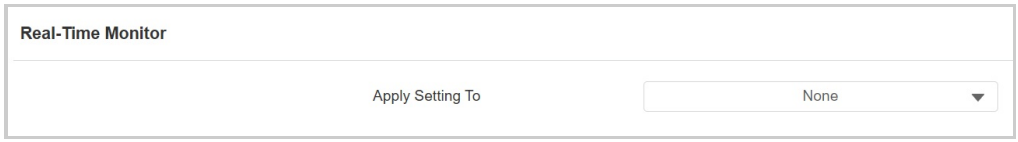


- **User Agent:** Akuvox is by default.

Real-Time Monitoring

When the device is connected to SmartPlus Cloud or ACMS, the door status can be displayed on the SmartPlus platform or ACMS.

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



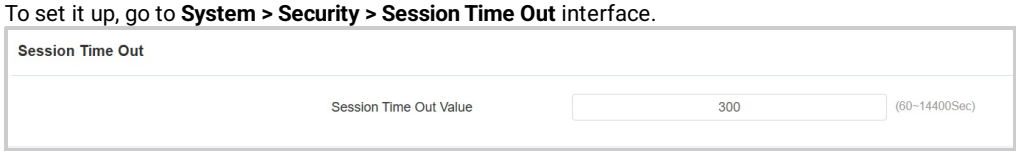
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering the input.
  - **Relay**: The door is opened by triggering the relay.

> **Note**
> Click **here** to see the detailed configuration steps.

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.

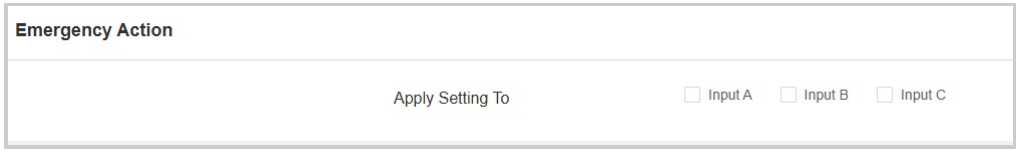


Emergency Action

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. Check the Input to be triggered.



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.

Turn on/off high security mode on the **System > Security** 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

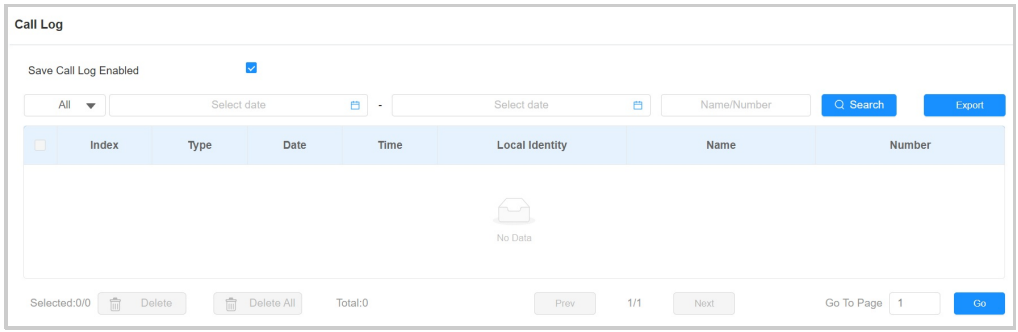
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

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 2,000 call logs, which can be exported in a CSV file by clicking Export.

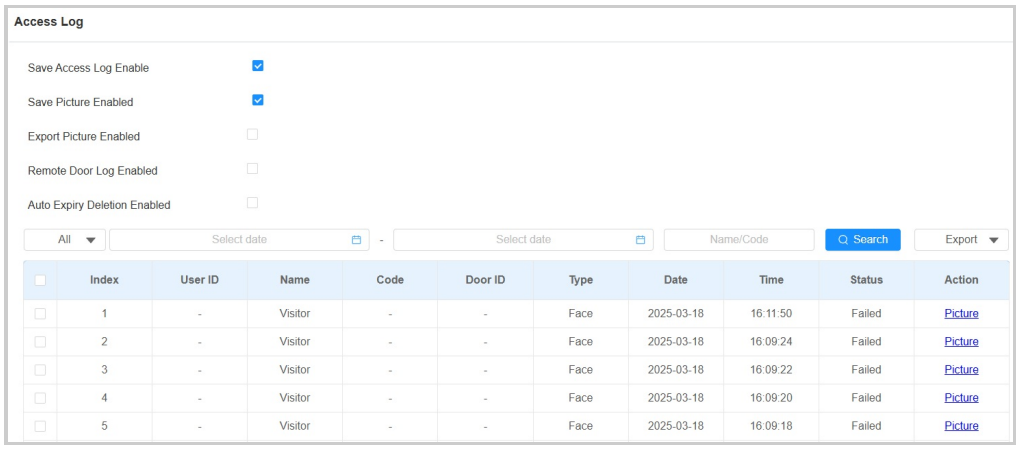


- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.

Door Logs

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

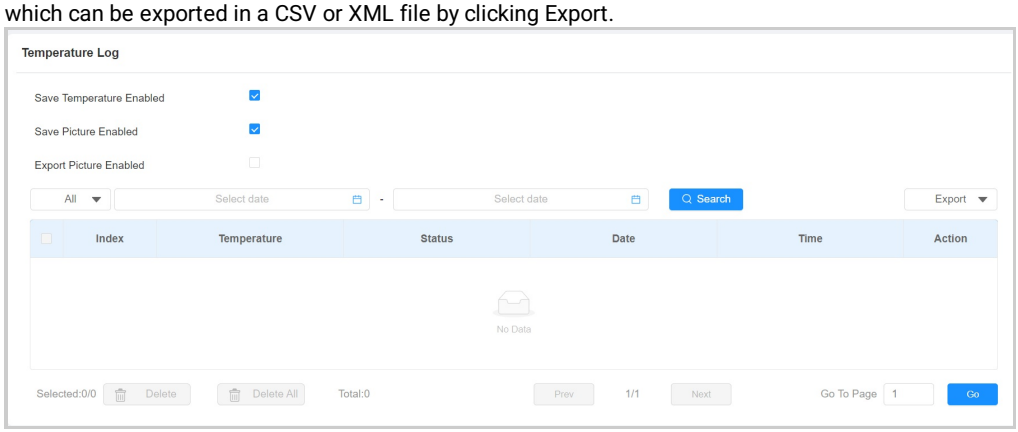
Check door logs on the **Status > Access Log** interface. The device supports 50,000 door logs, which can be exported in a CSV or XML file by clicking Export.



- **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.
- **Remote Door Log Enabled**: Set the remote server to store the door logs.
- **Auto Expiry Deletion Enabled**: Set whether to delete logs automatically when they exist for a certain days.
  - **Expiry Time**: Specify how long the logs can be retained. It ranges from 0 to 90 days.
- **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.

Temperature Logs

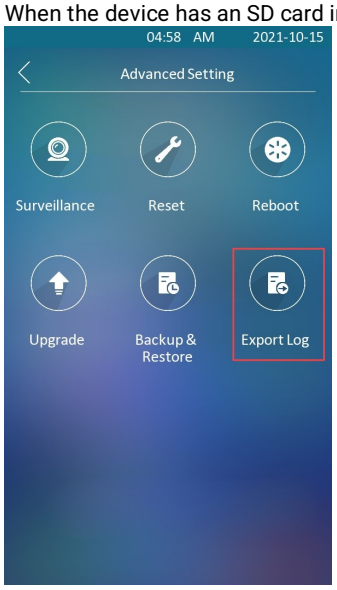
To check the temperature log, go to **Status > Temperature Log** interface. The device supports 50,000 temperature logs, which can be exported in a CSV or XML file by clicking Export.



- **Save Picture Enabled**: When enabled, the device will capture pictures of the temperature detection, 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 temperature logs.

Export Logs to SD Card

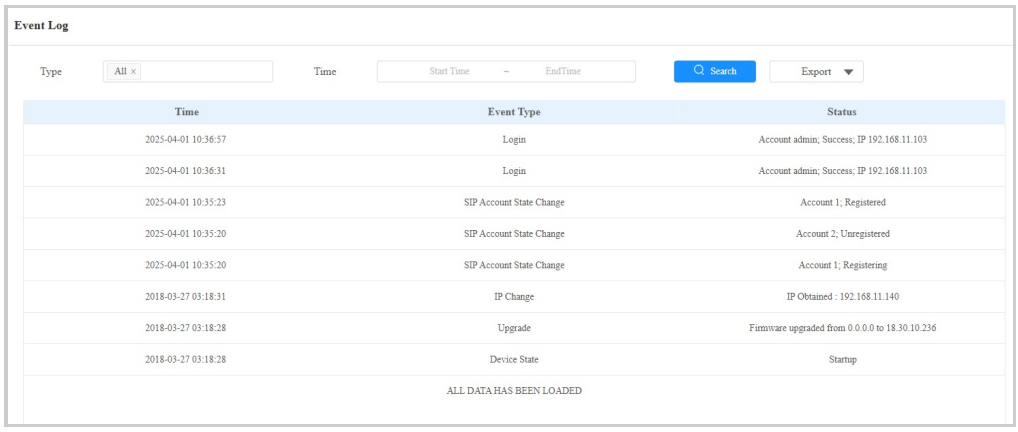
When the device has an SD card inserted, you can export logs to it on the **Advanced > Export Log** screen.



Event Logs

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

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

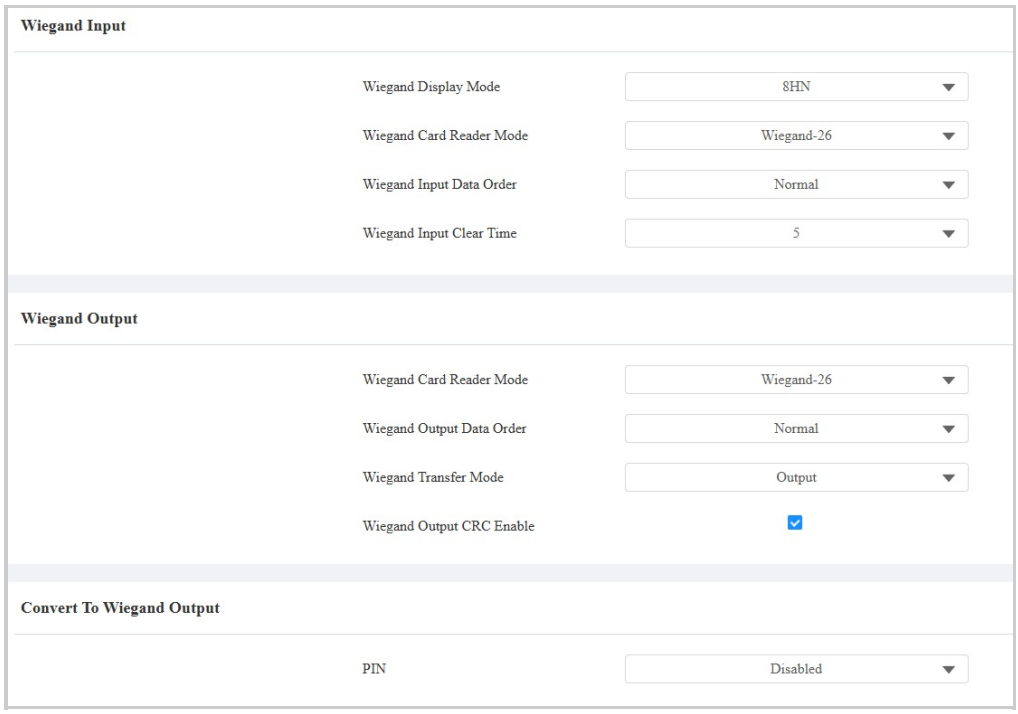

Event Log
Type
All ×
Time
Start Time
~
EndTime
Search
Export
Time
Event Type
Status
2025-04-01 10:36:57
Login
Account admin; Success; IP 192.168.11.103
2025-04-01 10:36:31
Login
Account admin; Success; IP 192.168.11.103
2025-04-01 10:35:23
SIP Account State Change
Account 1; Registered
2025-04-01 10:35:20
SIP Account State Change
Account 2; Unregistered
2025-04-01 10:35:20
SIP Account State Change
Account 1; Registering
2018-03-27 03:18:31
IP Change
IP Obtained : 192.168.11.140
2018-03-27 03:18:28
Upgrade
Firmware upgraded from 0.0.0.0 to 18.30.10.236
2018-03-27 03:18:28
Device State
Startup
ALL DATA HAS BEEN LOADED

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 Input**: The device serves as a relay controller.
  - **Wiegand Display Mode**: Select the Wiegand card code format from the provided options: 8H10D, 6H3D5D, 6H8D, 8HN, 8HR, RAW, 8HR10D, and 6H3D5D-R.
  - **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device. It is automatically configured.
  - **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 Input Clear Time**: When the interval of entering passwords via Wiegand exceeds the time. All entered passwords will be cleared. The default is 5 seconds.
- **Wiegand Output**:
  - **Wiegand Card Reader Mode**: The transmission format should be identical between the door phone and the third-party device. It is automatically configured.
  - **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 Transfer Mode**:
    - **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 Output CRC Enable**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **Convert To Wiegand Output**: Available when **Output** is Wiegand Transfer Mode. This option determines the output PIN format.
  - Disabled: Turn off the feature.
  - 8 bits per digit: When users press "1" on the keypad, the binary data will be transmitted in 8 bits, "11100001".
  - 4 bits per digit: When users press "1" on the keypad, the binary data will be transmitted in 4 bits, "0001".
  - All at once: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode. For example, “123456” will be converted to “01e240” in Wiegand 26.

Note

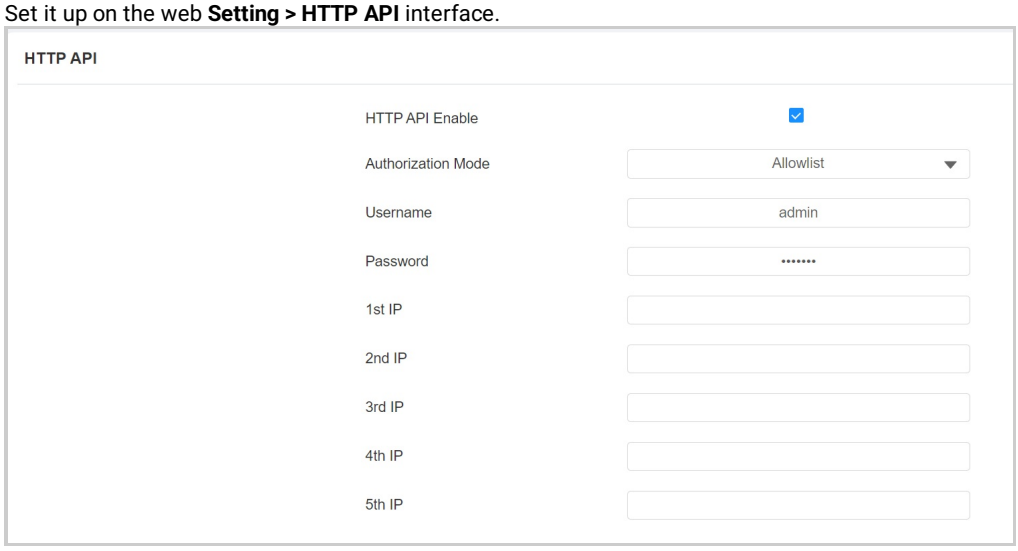
Click here to view more information on Wiegand settings including:

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

Integration via HTTP API

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

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



- **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	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.
3	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.
4	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".
5	Token	This mode is used by Akuvox developers only.

Integration with Third-party Access Control Server

The device can transmit access credentials 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.

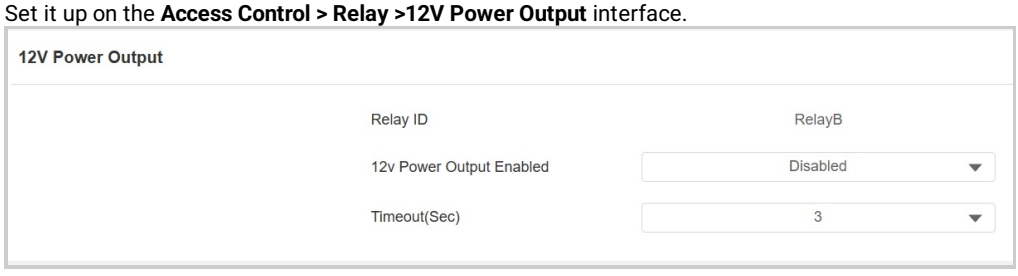


- **List**:
  - **None**: Disable the function.
  - **General**: Transmit the QR code-linked HTTP URL in Akuvox's method.
    - **HTTP URL**: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information 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.
  - **Customize**: Transmit QR code, RF card, and PIN data in a customized method.
    - **Prompt on LCD**: Select **Default** to adopt the Akuvox door phone's door-opening prompt; Select **Return Value** to use the return value from the third-party server as the prompt.
    - **Remote Verification**: Check the access method to be verified by the third-party server.
    - **HTTP URL**: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, swiping the card, or entering the PIN, the HTTP command will carry the credential data automatically before it is sent to the server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode}/{CardCode}/{Pin}&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, RF card, or PIN for door access.
  - **HAOSEN**: Choose to integrate with the HAOSEN server.
    - **Remote Verification**: Check the access method(s) to be verified by the third-party server.
    - **Verification URL**: Enter the URL provided by the third-party service provider. It is used to verify the face image, QR code, and card code. For example, *http://{Server IP}:8001/openapi/xw/checkcustomer*.
    - **Access Log URL**: Enter the URL provided by the third-party service provider. It is used to send the access log to the third-party server. For example, *http://{Server IP}:8001/openapi/xw/access*.
    - **Heart Beat URL**: The address is used to receive the heartbeat packet. The packet is sent every minute, and when the integration settings change. For example, *https://{Server IP}:3538/openapi/xw/heartBeat.*
    - **Device ID**: This ID should match the ID assigned to the device in the third-party system.

Power Output Control

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

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



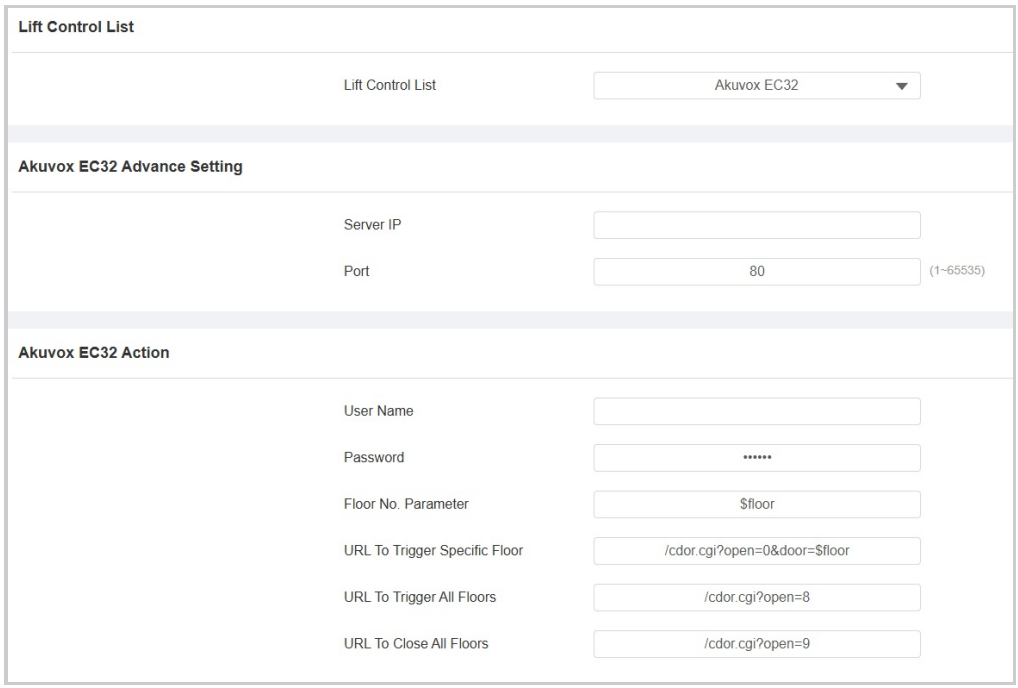
- **12V Power Output**:
  - **Disabled**: Disable the power output function.
  - **Always**: Provide continuous power to the third-party device.
  - **Triggered By Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted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

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**:
  - **OSDP**: The integration communication between the door phone and the third-party device is via OSDP protocol.
  - **Akuvox**: Integrate the door phone with the Akuvox lift controller.
  - **KEYKING**: Integrate the door phone with the KEYKING lift controller.

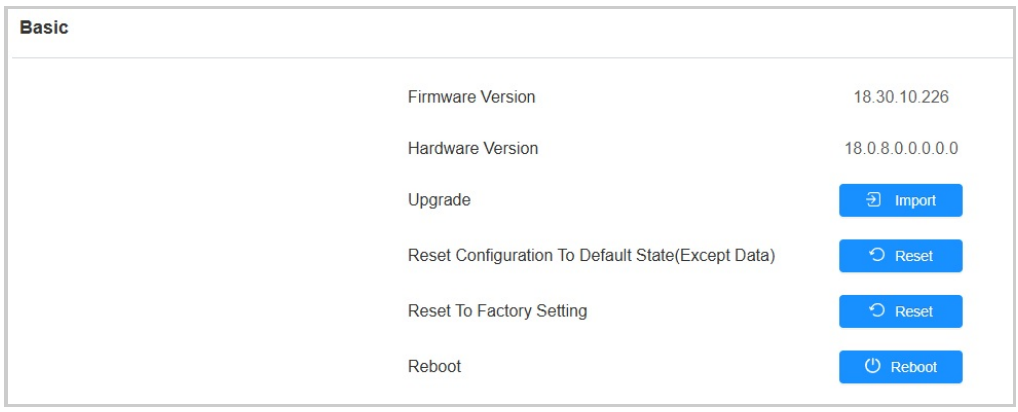
When **Akuvox** is selected, set up the following options:

- **Server IP**: The IP address of the Akuvox lift control server.
- **Port**: The server port of the lift controller server.
- **Username**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Note

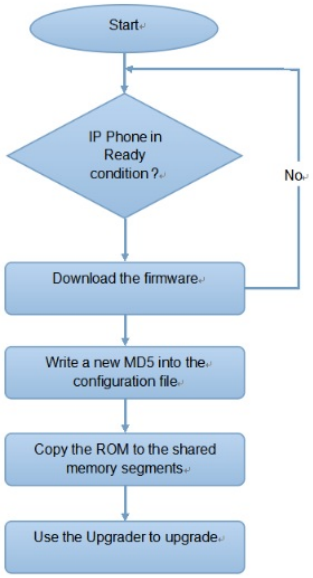
- Firmware files should be **.rom** format for upgrade.
- When the device has an SD card inserted, you can add a .rom file at the root directory and change the file name to update.rom. Then, tap **Advanced > Upgrade** on the device screen for upgrading.
- Click **here** to download the latest firmware and check new features.

Auto-provisioning

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

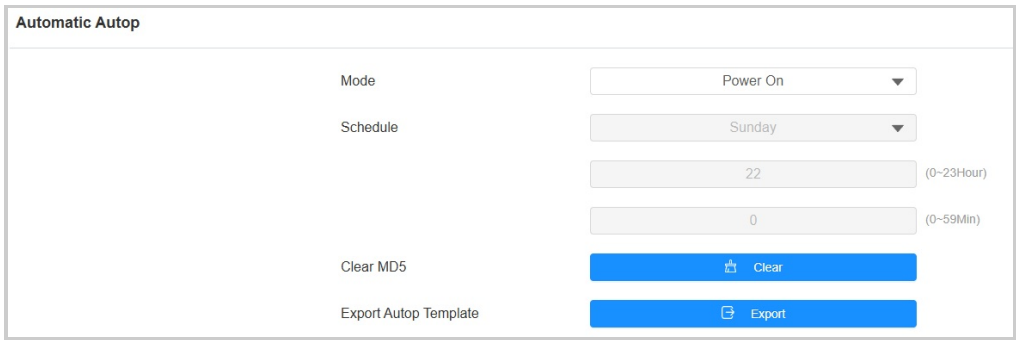
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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 up the schedule, go to the web **System > Auto Provisioning** interface.

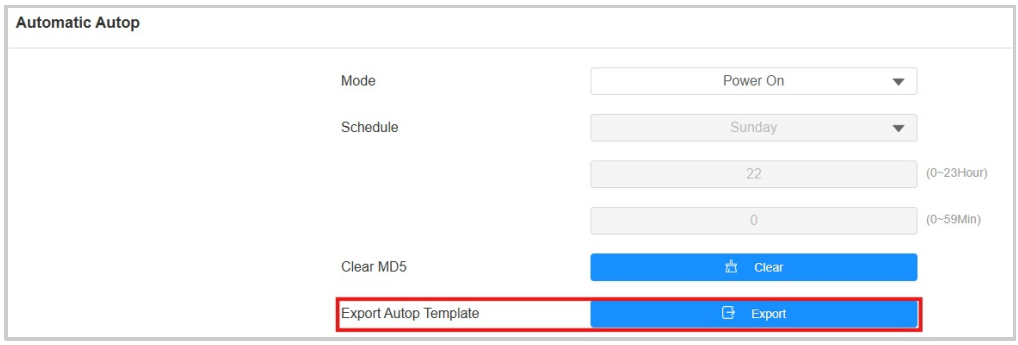


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode which will enable the device to perform Autop every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

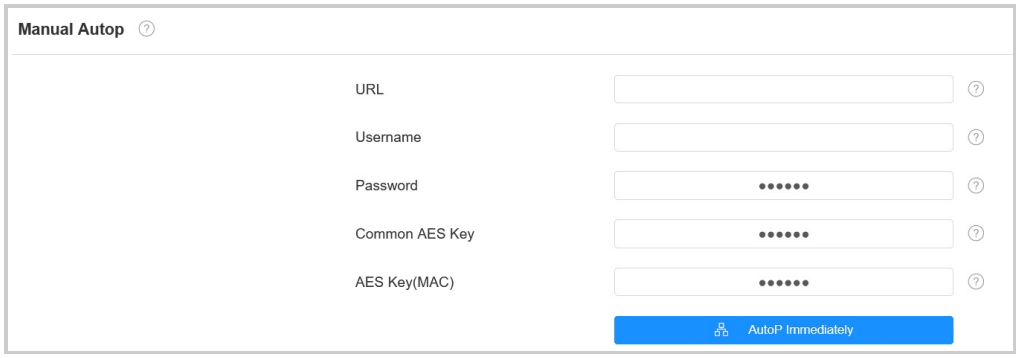
Static Provisioning

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 download the template, go to the web **System > Auto Provisioning** interface.



Then, scroll to the Manual Autop part.



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server requires a username to be accessed.
- **Password**: Enter the password if the server requires 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

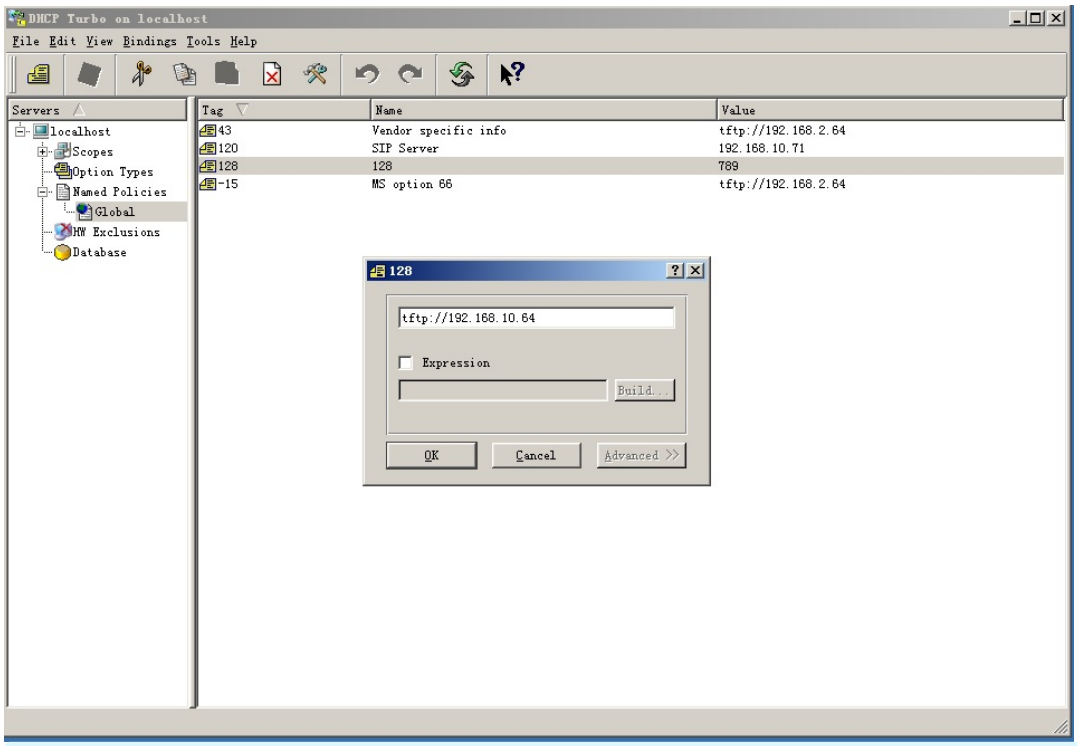
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

DHCP Provisioning

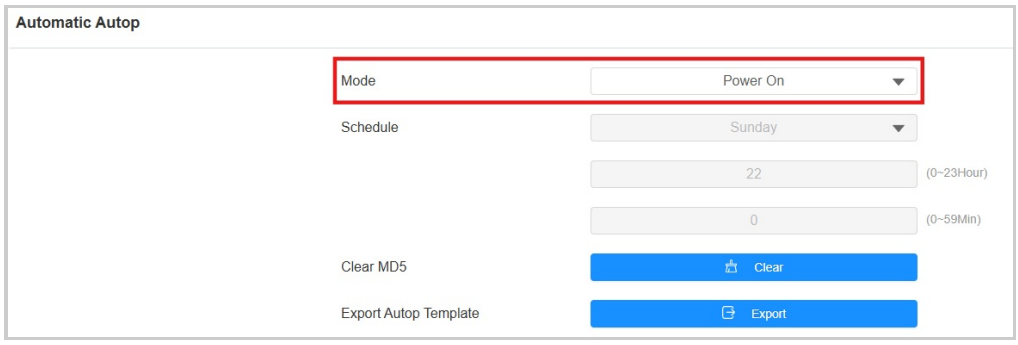
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **CustomOption**as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option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



Note

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

To set up DHCP Autop with **Power On** mode, go to the web **System > Auto Provisioning** interface.



To set up the DHCP Option, scroll to the **DHCP Option** section.



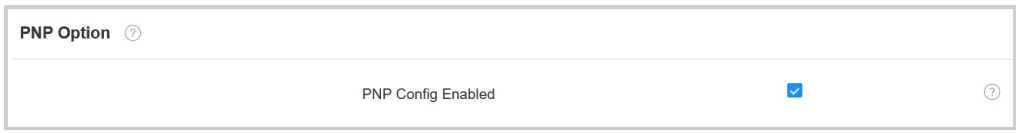
- **Custom Option**: Enter the DHCP code that matches with corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done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

PNP Configuration

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

Click here to watch the configuration video.

To enable the function, go to the web **System > Auto Provisioning** interface.

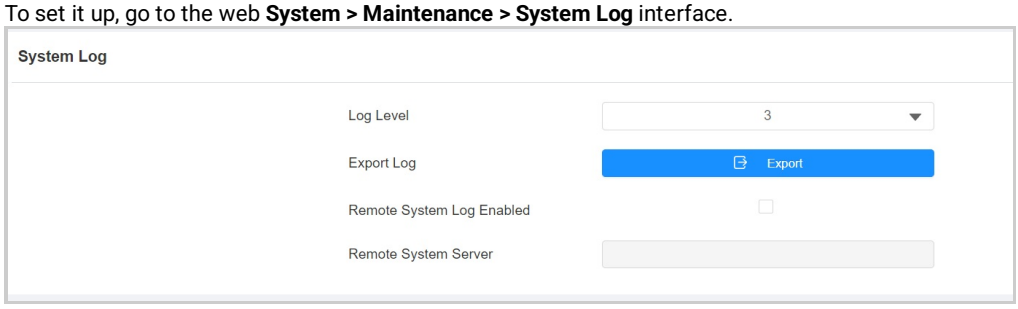


Debug

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.

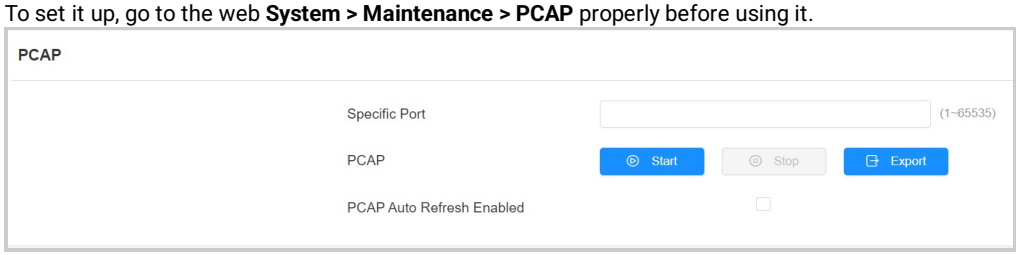


- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export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

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.

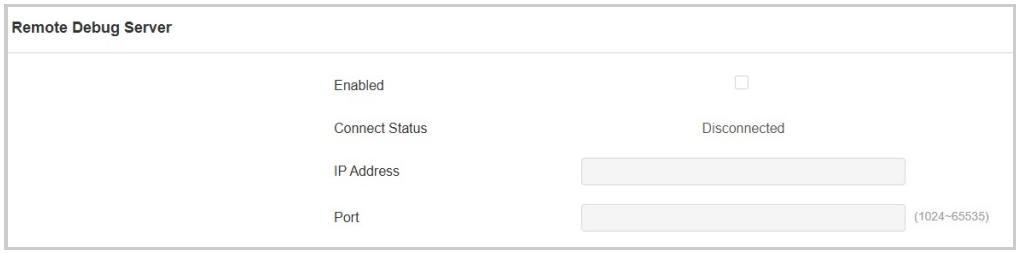


- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the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

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.



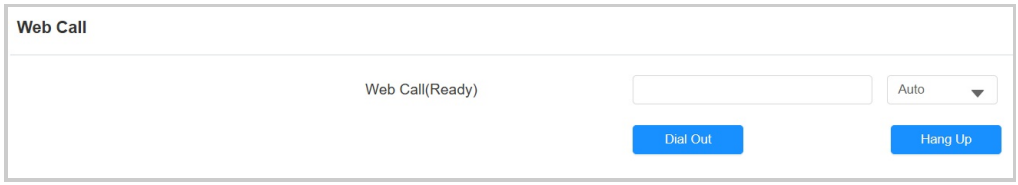
- **Connect Status**: Display the connection status between the device and the server.

- **IP Address**: Enter the server's IP address.
- **Port**: Enter the port of the server.

Web Call

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

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.

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

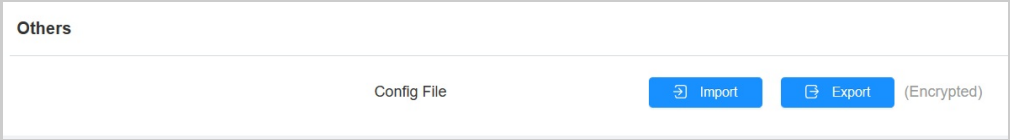


- **Cloud Server**: The server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Backup

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

Export the file on the **System > Maintenance > Others** interface. The supported file format is TGZ/CONF/CFG.



Note

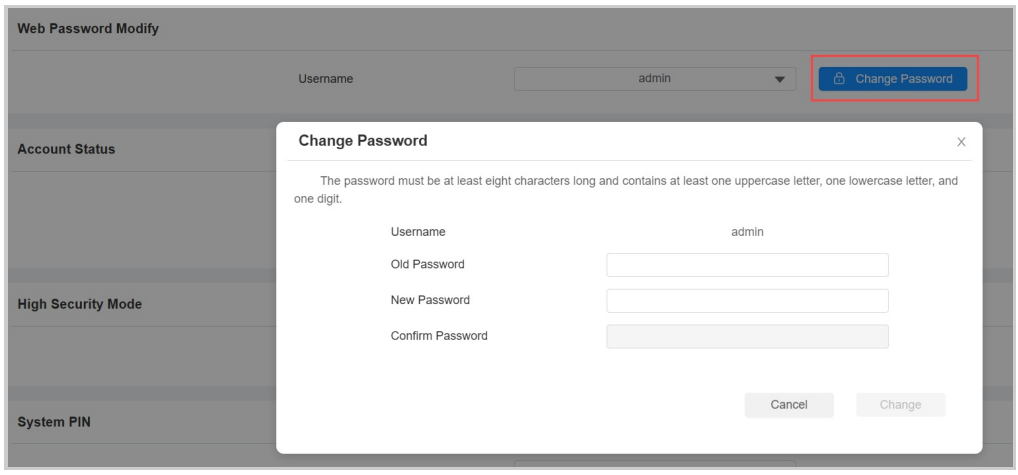
- If the device has an SD card inserted, you can also use it for backup.
- Tap **Advanced > Backup & Restore** on the device screen and choose to backup All Data or Only User Data:
  - All Data: Include user, group schedule data, and configuration data exclusive of all types of logs.
  - Only User Data: Include user and schedule data.
- SDHC and SDXC SD cards with FAT32 format are supported.

Password Modification

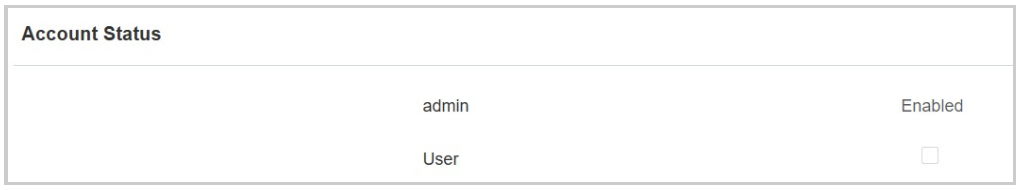
Modify Web Interface Password

Navigate to the web **System > Security > Web Password Modify** interface.

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



To enable or disable the user account, scroll to the **Account Status** section. The default password for the user account is **user**.



Modify Security Questions

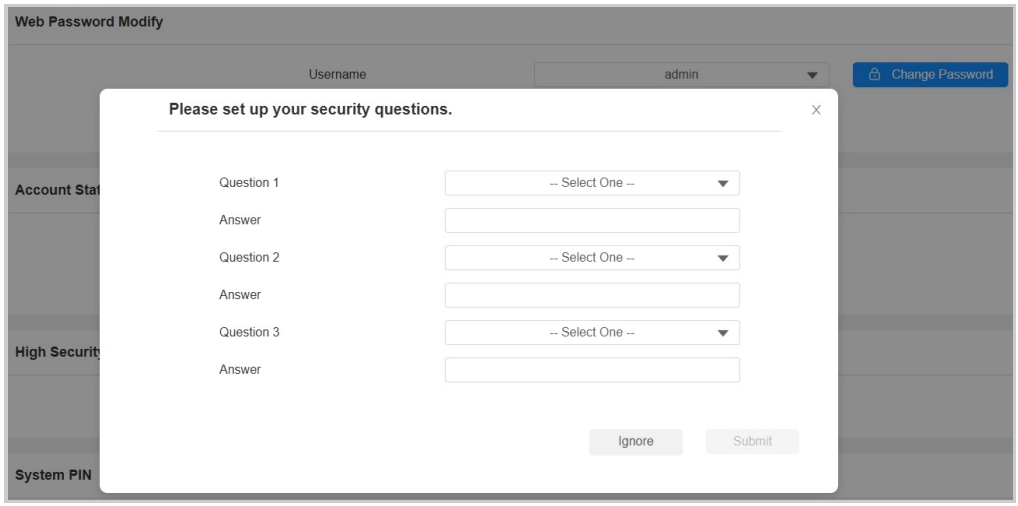
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

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



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



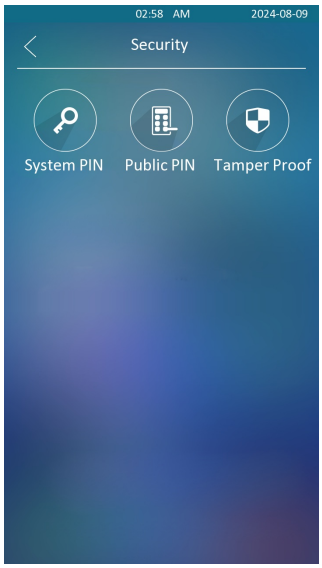
Modify System Password

The system PIN code is used to access the device's settings. The default is "Admin321.".

To set it up, go to **System > Security > System PIN** interface.



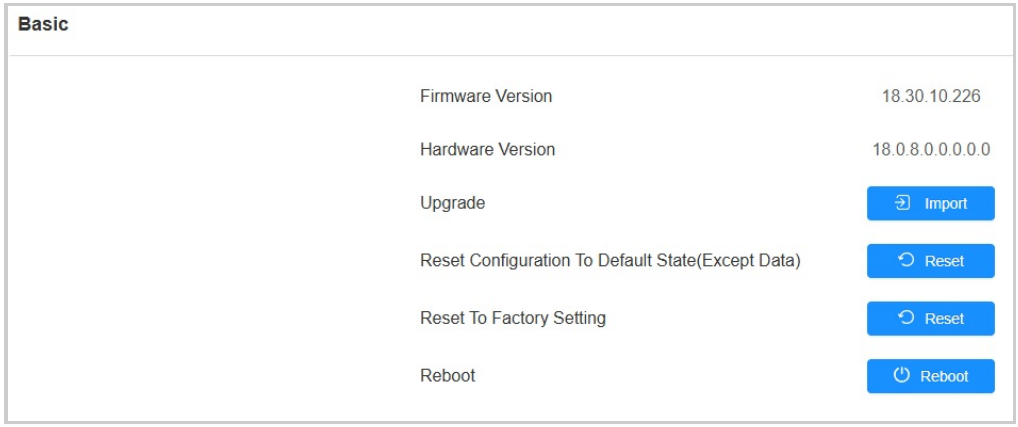
You can also change the password on the **Setting > Security** screen.


02:58 AM
2024-08-09
Security
System PIN
Public PIN
Tamper Proof

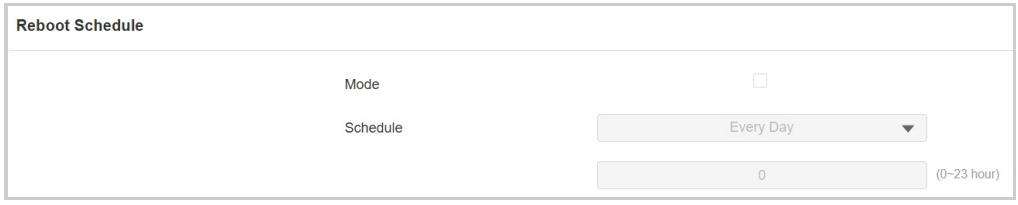
System Reboot&Reset

Reboot

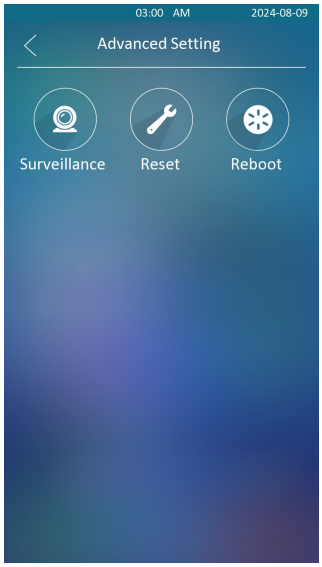
You can reboot the device on the **System > Upgrade > Basic** interface. Moreover, you can set up a schedule for the device to be restarted.



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



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

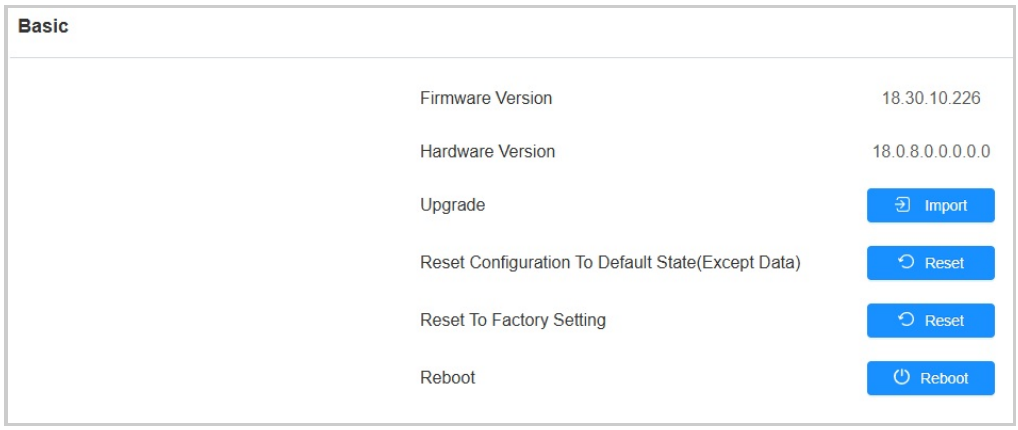


Reset

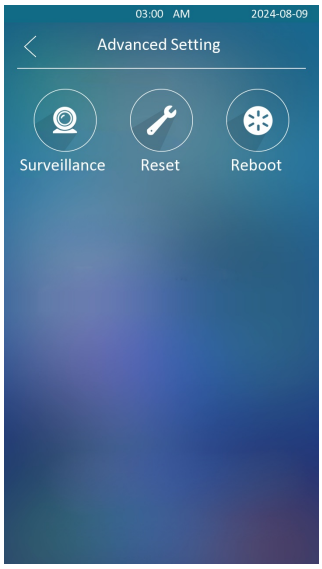
The device provides two reset options:

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

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



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



Tip

The device can be reset by pressing a physical button.

1. Remove the back cover of the door phone.
2. Power on the device.
3. Hold the white button until the backlight and white fill light in the card reader area light up simultaneously for 1 second.

- When the device screen does not light up, hold the white button for about 3-5 seconds.
- When the device is in a normal working state, hold the white button for about 8-10 seconds.

Then, the device will go into factory reset and reboot.

