Table of contents

Akuvox X910 Series Door Phone Administrator Guide

About This Manual 5
Product Overview 7
Changelog 8
Model Specification 9
Supported Card Types 10
Access the Device 12
Obtain Device IP Address 12
Access the Device Setting 13
Introduction to Configuration Menu 14
Language and Time 16
Language 16
Custom Language 16
Time 17
LED Setting 19
LED Fill Light 19
LED Setting on Card Reader Area 20
LED Light Status 20
White Light Setting 21
Volume and Tone 22
Volumes 22
Upload Tone Files 22
Ringback Tone 23
Network Connection 25
Network Status 25
Device Network Configuration 25
Device Deployment in Network 26
Device Web HTTP Setting 28
Device Local RTP Setting 28
SNMP Setting 29
NAT Setting 29
TR069 30
Intercom Call Configuration 32
IP Call Configuration 32
SIP Call Configuration 32
SIP Account Registration 32

SIP Server Configuration 33
Outbound Proxy Server 34
Data Transmission Type 35
SIP Hacking Protection 35
Video Transport Type Selection 36
Call Settings 37
Call Auto-answer 37
Sequence Call 37
Group Call 39
Do Not Disturb 39
Push To Hang Up 40
Multicast 40
Maximum Call Duration 41
Maximum Dial Duration 42
Hang up After Opening Doors 43
Audio & Video Codec Configuration 44
Audio Codec 44
Video Codec 44
Video Codec for IP Calls 45
Relay Settings 47
Local Relay 47
Security Relay 48
Web Relay 49
Access Control Schedule Management 52
Configure Door Access Schedule 52
Create Door Access Schedule 52
Import and Export Door Access Schedule 53
Relay Schedule 53
Holiday Schedule 54
Door-opening Configuration 56
User-specific Access Methods 56
Unlock by RF Card/Bkey 57
Unlock by License Plate 58
Unlock by Bluetooth 58
Unlock By QR Code 61
Access Setting 62
Import/Export User Data 63
Cloud Call Permission Control 64
Unlock by Contactless Smart Card 64
Unlock by Mifare Card 65

Unlock by HTTP Command 65
Unlock by DTMF Code 66
DTMF White List 67
DTMF Data Transmission 68
Unlock by Exit Button 69
Monitor and Image 71
MJPEG Authorization 71
MJPEG Video Stream 72
RTSP Stream Monitoring 73
RTSP Basic Setting 73
RTSP Stream Setting 73
RTSP OSD Setting 75
ONVIF 76
Video Record 77
Live Stream 78
NACK 78
Data Transmission Type for Third-party Camera 79
SD Card for Storing Videos 79
Camera Mode 80
Package Detection 82
Security 84
Tamper Alarm 84
Client Certificate Setting 84
Web Server Certificate 84
Client Certificate 85
Motion Detection 85
Security Notification 87
Email Notification 88
FTP Notification 88
SIP Call Notification 89
Action URL 89
Voice Encryption 91
User Agent 92
Real-Time Monitoring 92
Emergency Action 93
Web Interface Automatic Log-out 93
High Security Mode 93
Logs 95
Call Logs 95
Door Logs 95

Event Logs 96
Integration with Third Party Device 98
Integration via Wiegand 98
Integration via HTTP API 99
Integration via RS485 101
Power Output Control 102
Lift Control 104
Firmware Upgrade 106
Auto-provisioning via Configuration File 107
Provisioning Principle 107
Configuration Files for Auto-provisioning 108
AutoP Schedule 109
Static Provisioning 110
DHCP Provisioning 111
PNP Configuration 113
Debug 114
System Log for Debugging 114
Remote Debug Server 114
PCAP for Debugging 115
Ping 116
Web Call 116
Backup 117
Backup via SD Card 117
Password Modification 118
Modify Security Questions 118
System Reboot&Reset 120
Reboot 120
Reset 120

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

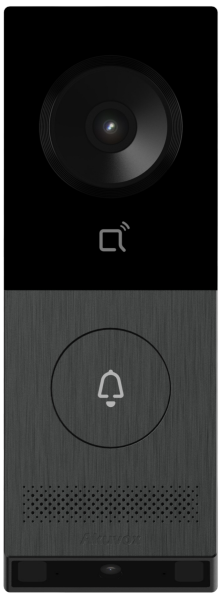


AKUVOX X910 DOOR PHONE

Administrator Guide

Thank you for choosing the Akuvox X910 door phone. This manual is intended for administrators who need to configure the door phone properly. This manual applies to firmware version 2910.30.11.35, and it provides all the configurations for the functions and features of the door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



The X910 door phone is designed to integrate with Akuvox indoor monitors, SmartPlus Cloud services, and smart home systems. It functions as a smart intercom, enabling features like audio/video communication, surveillance, and access control. Key benefits include quick deployment, reduced maintenance costs, improved mobile communication, enhanced security against package theft, and seamless smart home integration, providing residents with a convenient and secure living experience.

Changelog

What's new in version 2910.30.11.33:

- Support the integration with Control4.

What's new in version 2910.30.11.35:

- Support adjusting the ringback volume.

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

Model Specification

Model	X910
Operation System	Linux
Cameras	2
Fill Light	✔
Motion Detection	✔, Radar Detection
IC Card Reader	✔, 13.56MHz
ID Card Reader	X
NFC	✔
Bluetooth	✔, 5.0 and higher
RJ45 Port	1. Support PoE or PoE+
Wiegand	1
RS485	1
Relay	2, DC 30V 2A
Input	2
SD Card Slot	1
Power Supply	PoE or PoE+, or 12~24 VDC power adapter
Power Output Port	Provide power(12V/600mA) when PoE+ powers the device.
Tamper Proof	✔

Ethernet Indicator Light	1
Reset Button	✔
Microphone	1
Speaker	1

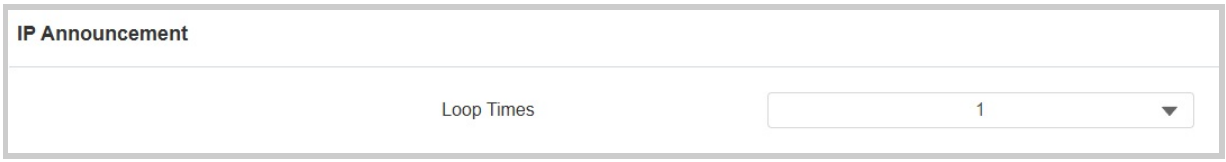
Supported Card Types

- IC Cards:
    - Mifare Ultralight C/EV1
    - Mifare Classic Compatible Card
    - Mifare Plus-S 2K
    - Mifare Desfire EV1 2K D21
    - Mifare Desfire EV2 D42
    - Mifare Desfire EV2 D22
    - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
    - NFC Type2 216
    - NFC Type2 215
- Felica Card
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
    - Mifare Classic 1K
    - Mifare S50-1K Card
    - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

Access the Device

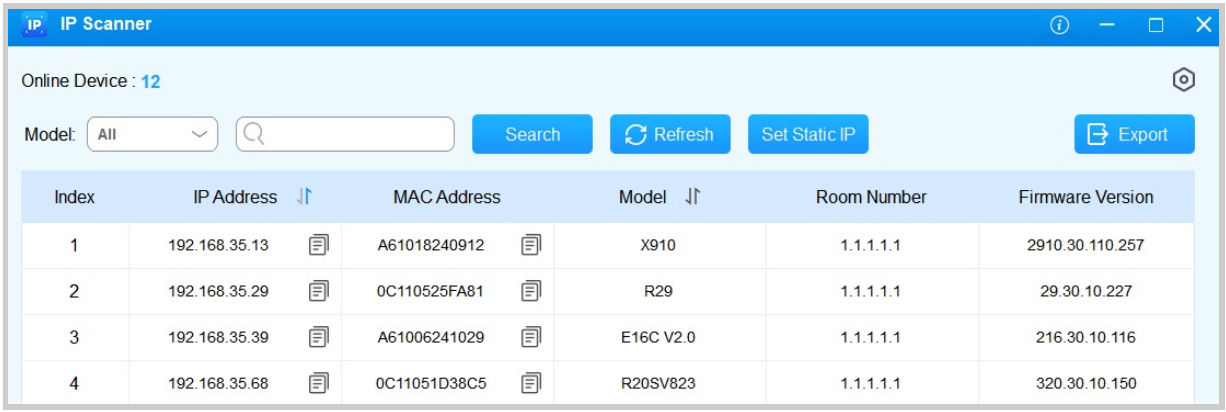
Obtain Device IP Address

Check the device IP address by holding the push button for 5 to 10 seconds. You can set up the IP announcement loop times on the **Device > Audio > IP Announcement** interface.



- **Loop Times:** Set the IP announcement loop times.

Or, search the device IP with the IP scanner on the same network. Click **Refresh** to update the list



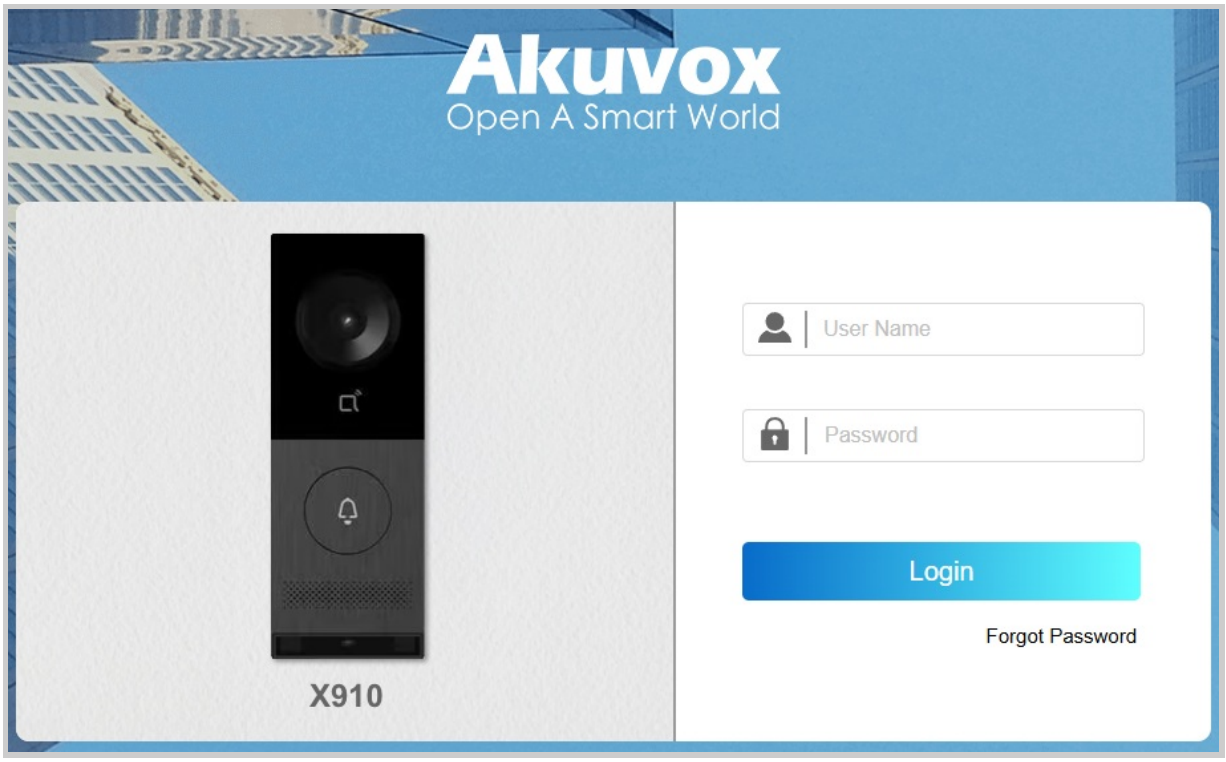
Note

- 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
- Your computer should be on the same local network as the device.

Access the Device Setting

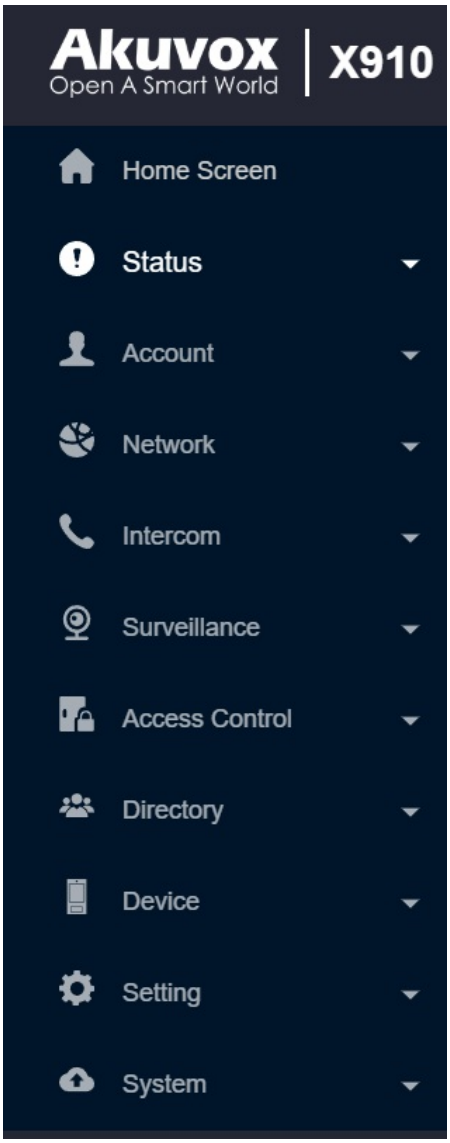
You can enter the device IP address on the web browser to log in to the device web interface where you can configure and adjust parameters, etc.

The initial username and password are **admin** and please be case-sensitive to the username and password entered.



Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, etc.
- **Network:** This section mainly deals with DHCP & static IP settings, RTP port settings, device deployment, etc.
- **Intercom:** This section covers intercom settings, call logs, etc.
- **Surveillance:** This section covers motion detection, RTSP, MJPEG, ONVIF, and live streaming.
- **Access Control:** This section covers input control, relay, card settings, private PIN code, Wiegand connection, etc.
- **Directory**: This section includes the management of users.
- **Device:** This section includes LED, audio, and SD card settings.
- **Setting:** This section includes time & language, action settings, door settings, and schedule for access control.
- **System:** This section includes device upgrade and maintenance, auto-provisioning, security settings, certification upload, etc.


Akuvox
Open A Smart World
X910
Home Screen
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System

Language and Time

Language

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

The device supports the following web languages:

- English, Simplified Chinese, and Spanish.



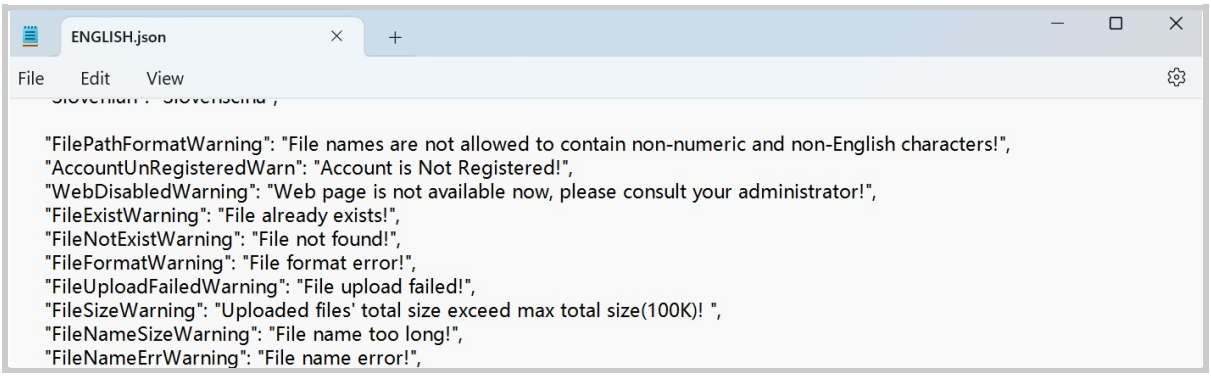
Custom Language

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

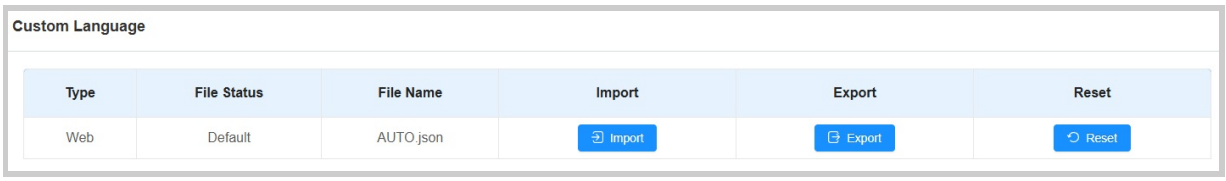
Export the .json file for editing. You may edit it with the notepad on your computer.

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

File Example:



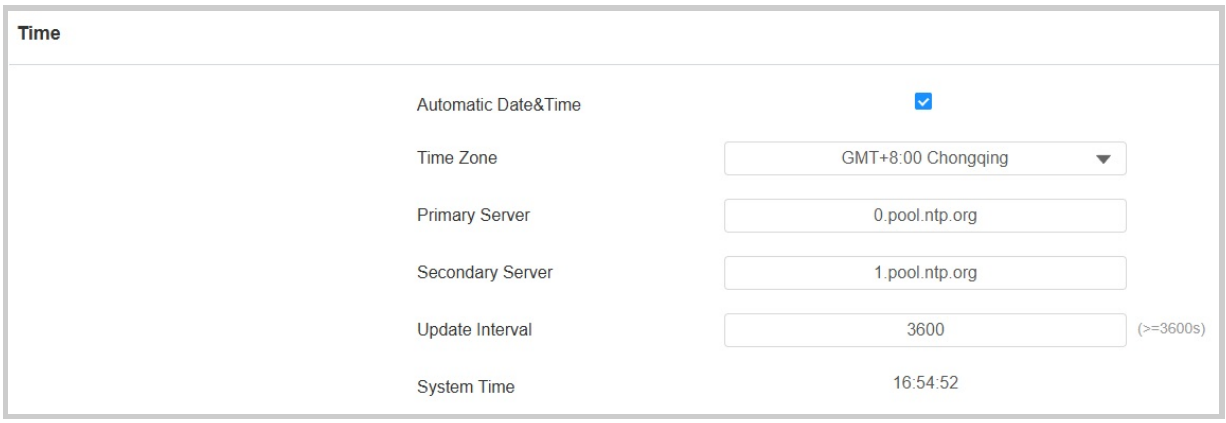
To set it up, navigate to **Setting > Time/Lang > Custom Language** interface.



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.

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



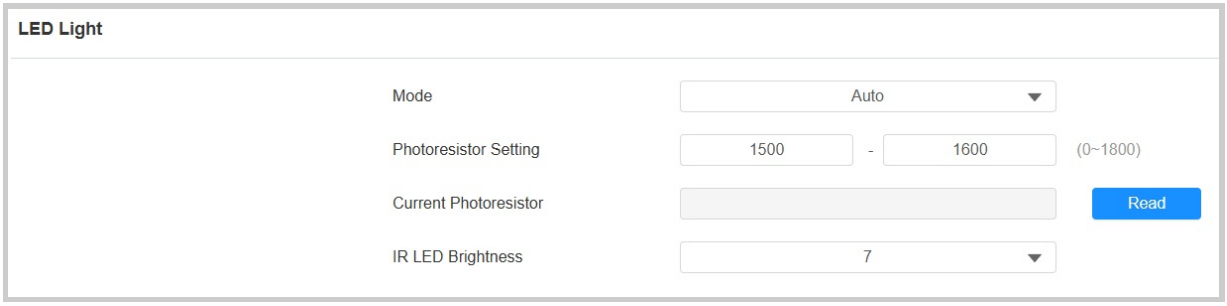
- **Automatic Date&Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Time Zone**: Select the specific time zone based on where the device is used. The default time zone is GMT+0:00.
- **Primary Server**: Enter the primary NTP server address for updating the time. The default NTP server address is 0.pool.ntp.org.
- **Secondary Server**: Enter the backup NTP server address when the primary one fails.
- **Update Interval**: Set the time between each update request to the NTP server.
- **System Time**: Display the current system time.

LED Setting

LED Fill Light

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

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



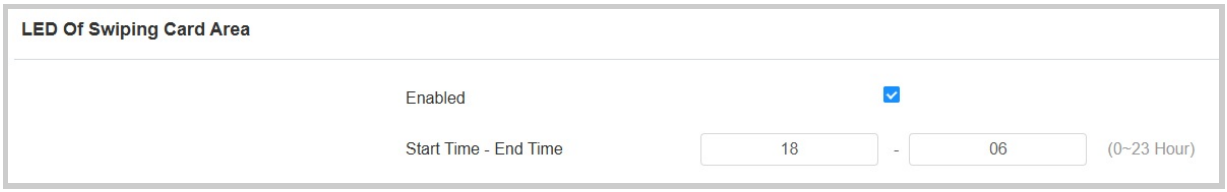
- **Mode**:
  - **Auto**: The device adjusts the LED mode automatically based on the photoresistor value. The higher the value is, the darker the environment is. The device will enable the infrared fill light and switch on the black-and-white filter mode.
  - **Always Off**: Turn off the infrared fill light. The device is in colored mode.
  - **Always On**: Turn on the infrared fill light. The device is in black-and-white mode.
  - **Specific Time**: Set the specific time to enable the infrared fill light. Beyond this time, the device will enable/disable the infrared fill light automatically based on the photoresistor value.
- **Photoresistor Setting**: Set the minimum and maximum photoresistor values to automatically control the ON-OFF of the infrared LED light. If the photoresistor value is less than the minimum threshold, turn it off. If the photoresistor value is greater than the maximum threshold, turn it on.

- **Current Photoresistor**: Click **Read** to obtain the current photoresistor value. The photoresistor values inversely relate to light intensity: higher values indicate weaker light and lower values indicate stronger light.
- **IR LED Brightness**: Set the brightness of the infrared light. The default is 7.

LED Setting on Card Reader Area

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

Set it up on the **Device > Light > Light of Swiping Card Area** interface.

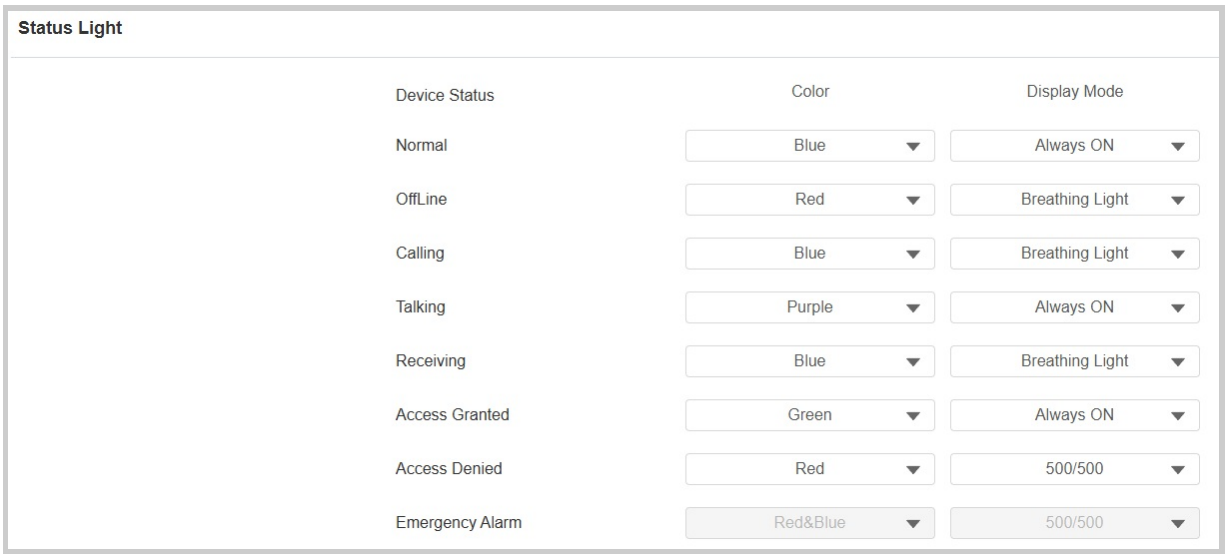


- **Enabled**: When enabled, specify the time to keep the card reader light on.

LED Light Status

The LED display adjustment indicates the light changes of the call button in different states. The LED status allows users to verify the device's current mode.

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

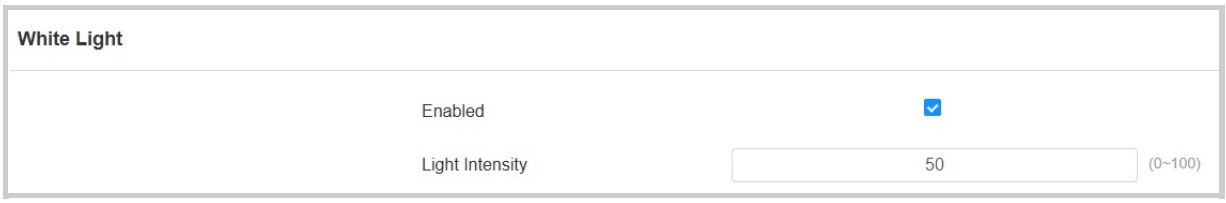


- **Device Status:** The indicator light can indicate 8 statuses.
- **Color:** Select from Blue, Red, Green, Cyan, Yellow, White, and Purple. The light color of the Emergency Alarm status cannot be changed.
- **Display Mode:** Set different flashing frequencies. The display mode of the Emergency Alarm status cannot be changed.

White Light Setting

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

Set it up on the **Device > Light > White Light** interface. It is enabled by default.



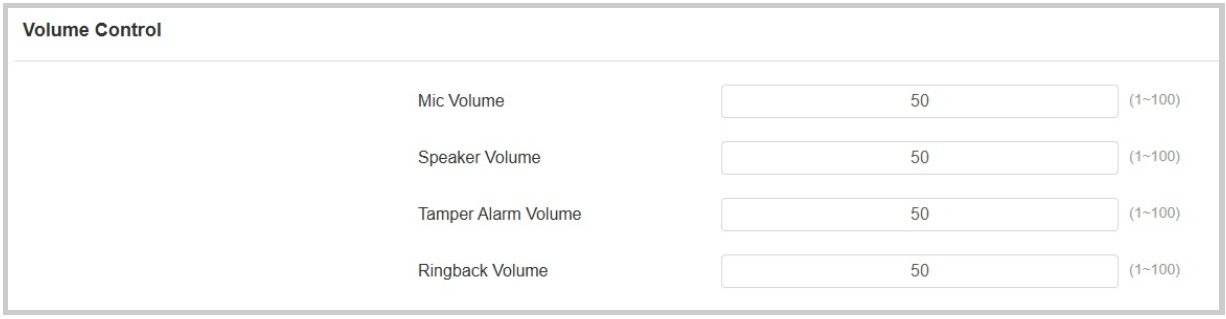
- **Light Intensity**: Set the white light value from 0-100. The default is 50. The greater the value is, the brighter the light will be.

Volume and Tone

Volume and tone configuration include various volume controls. Moreover, you can upload tones to enrich the user experience.

Volumes

To set up volumes, go to the web **Device > Audio** interface.

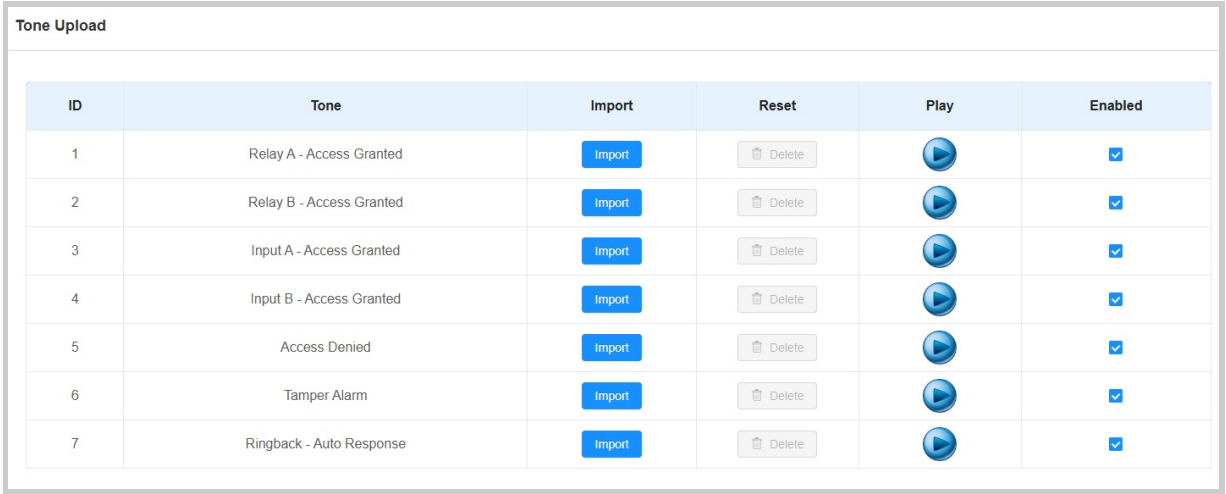


- **Tamper Alarm Volume**: Set the volume when the tamper alarm is triggered.

Upload Tone Files

You can customize ringback, door-opening, and emergency alarm tones.

Upload files on the **Device > Audio > Tone Upload** interface.



- **Ringback**: The tone can be heard when someone calls the device.

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

Ringback Tone

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

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

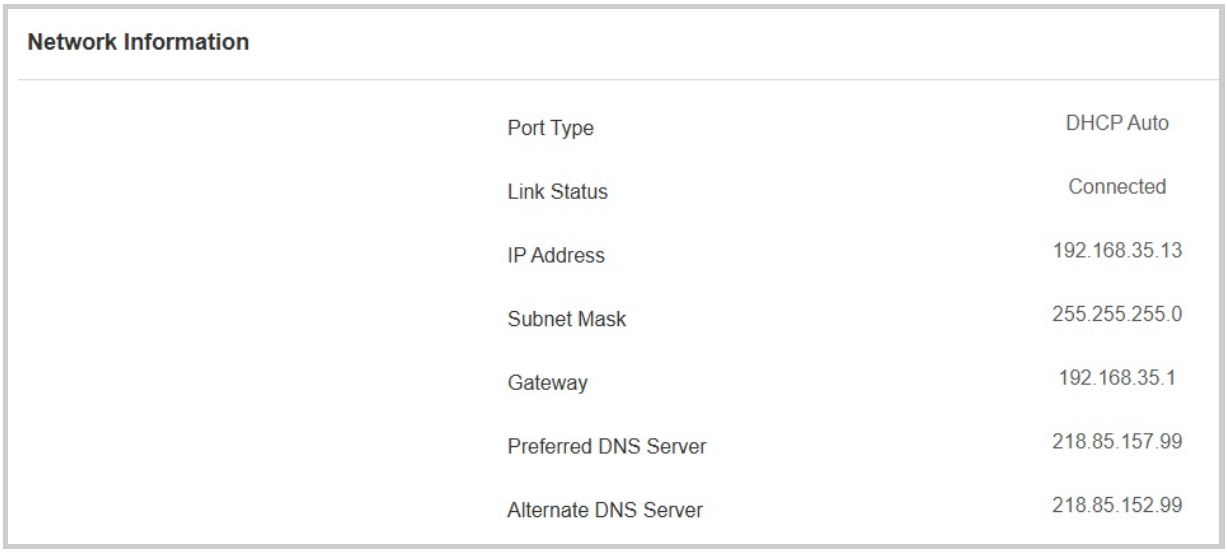


- **Ringback Source**:
  - **Remote, Local As Backup**: The local ringtone will be played.
    - When the door phone calls another device, for example, an Akuvox indoor monitor, and the SIP server returns non-183, the indoor monitor will not have any intercom preview.
    - If the SIP server returns 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.
- **Auto Response**: When disabled, the device will use the default ringback tone. When enabled, you can upload the customized tone.

Network Connection

Network Status

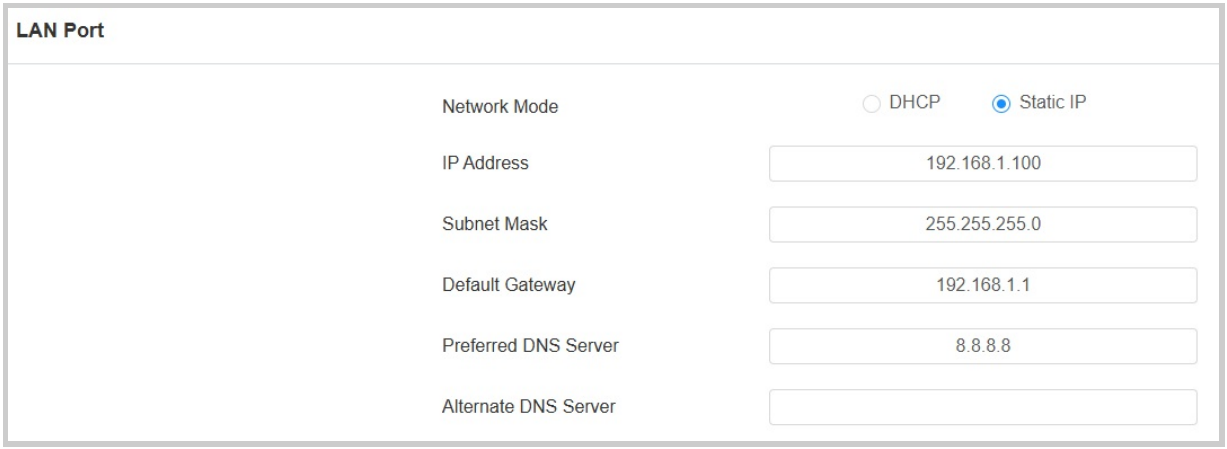
Check the network status on the web **Status > Info > Network Information** interface.



Device Network Configuration

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

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



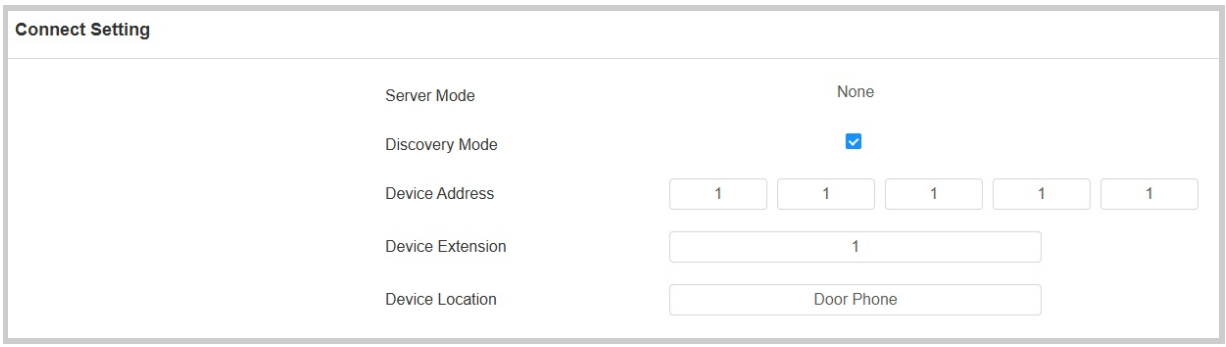
- **Network Mode**:

    - **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
    - **Static IP**: When static IP mode is selected, the IP address, subnet mask, default gateway, and DNS server address should be configured according to the network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings, your computer should be on the same local network as the device.
- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.
- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **Preferred/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.

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, navigate to the web **Network > Advanced > Connect Setting** interface.



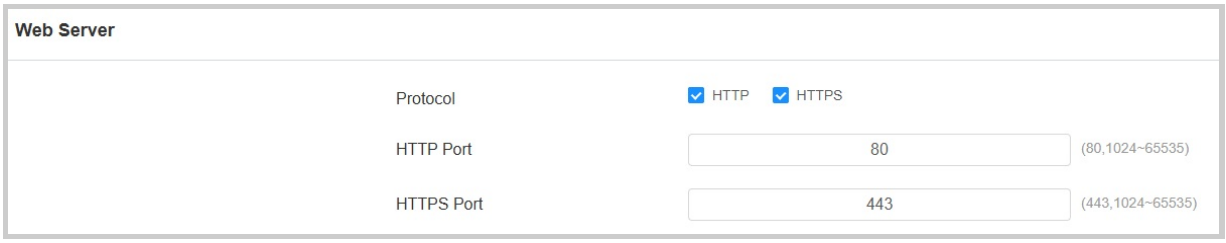
- **Server Mode**: It is automatically set up according to the device connection with a specific server in the network, such as SDMC, Cloud, or None.
  - **None**: None is the default factory setting indicating the device is not in any server type. Devices connect directly to each other or within a local 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 **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address**: Available for None server mode. Uneditable in Cloud and SDMC mode. It can be used to call the device. Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for None server mode. Uneditable in Cloud and SDMC mode. The device extension number ranges from 0 to 10.

- **Device Location**: The location in which the device is installed and used. Available for None server mode.

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.



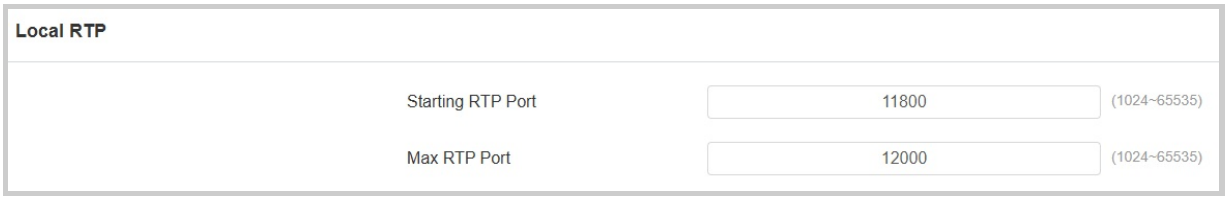
- **HTTP/HTTPS Enabled**: HTTP and HTTPS are enabled by default.
- **HTTP/HTTPS Port**: Specify the web server port for accessing the device web interface via HTTP/HTTPS.

Device Local RTP Setting

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

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

To set it up, go to the **Network > Advanced > Local RTP** interface.

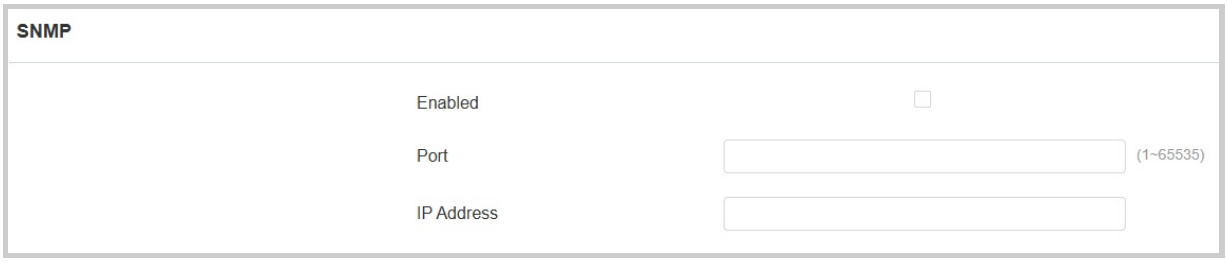


- **Starting RTP Port**: Set the port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: Set the port value to establish the endpoint for the exclusive data transmission range.

SNMP Setting

Simple Network Management Protocol**(SNMP)** is a protocol for managing IP network devices. It allows network administrators to monitor devices and receive alerts for attention-worthy conditions. SNMP provides variables describing system configuration, organized in hierarchies and described by Management Information Bases (MIBs).

To set it up, go to **Network > Advanced** interface.



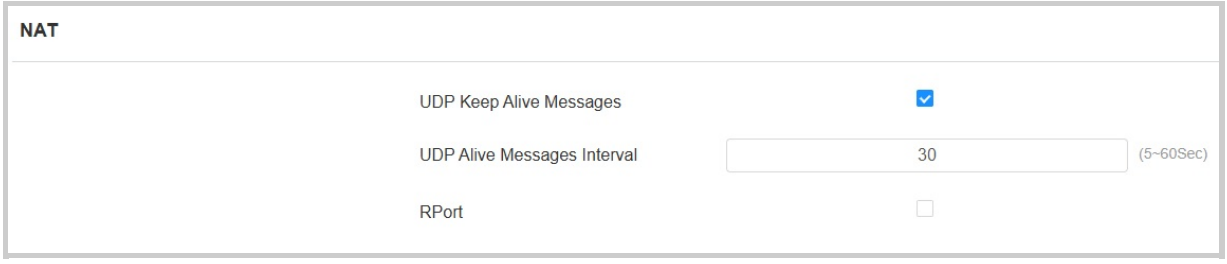
- **Port**: Set a specific port for the data transmission from 1024-65535.
- **IP Address**: Enter the third-party IP address.

NAT Setting

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

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

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

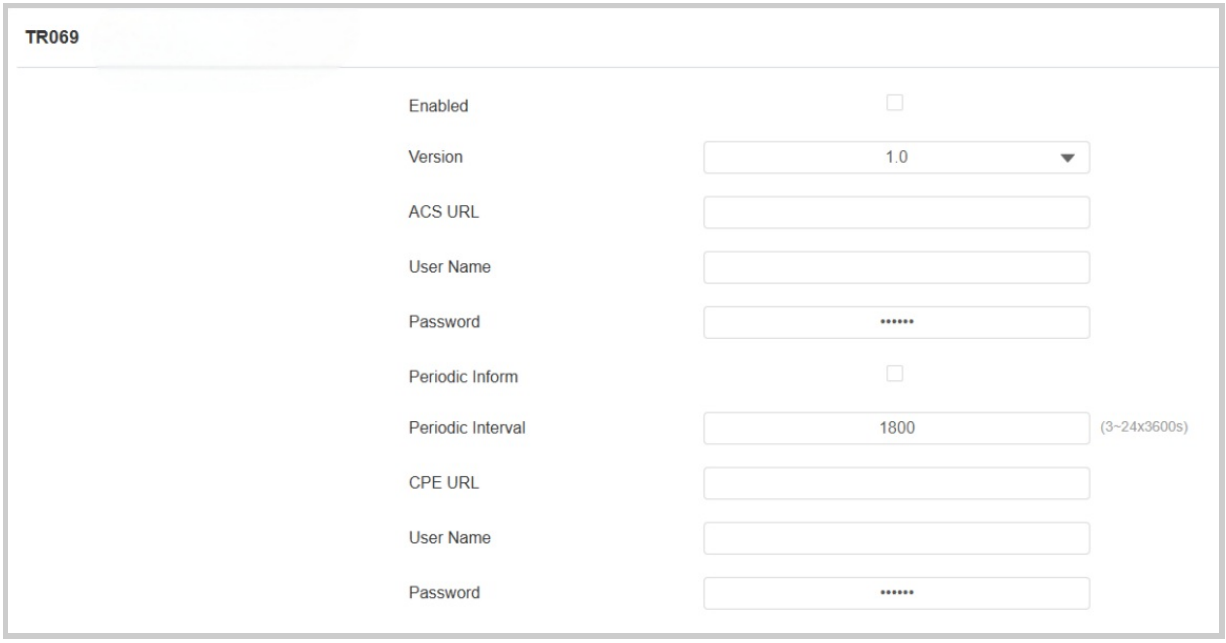


- **UDP Keep Alive Messages Enabled:** If enabled, the device will send the message to the SIP server, which will recognize whether the device is online.
- **UDP Alive Messages Interval:** Set the message-sending interval from 5-60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when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

TR069

TR-069 (Technical Report 069) provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. For door phones, the administrators can manage all the devices on a common TR-069 Platform. IP phones can be easily and securely configured on the TR-069 platform to make mass deployment more efficient.

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



- **Version**: Select the TR069 version.
- **ACS URL**: Set the URL of the ACS server, for example, http://192.168.1.47:8080/openacs/acs.
- **User Name**: Set the ACS server username for authentication.
- **Password**: Set the ACS server password for authentication.
- **Periodic Inform**: Allow the device to send requests to the ACS server for automatic configuration and update.

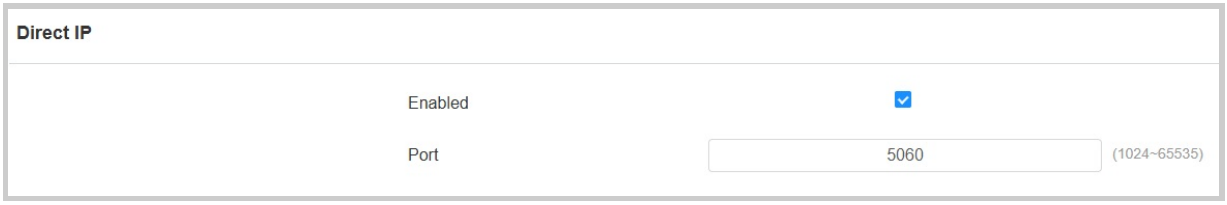
- **Periodic Interval**: Set the time interval for the device to send the request to the ACS server for the automatic configuration and update.
- **CPE URL**: Set the device URL, for example, http://192.168.1.48:8882/.
- **User Name**: Set the device authentication username.
- **Password**: Set the device authentication password.

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.

Enable direct IP 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 Configuration

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

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

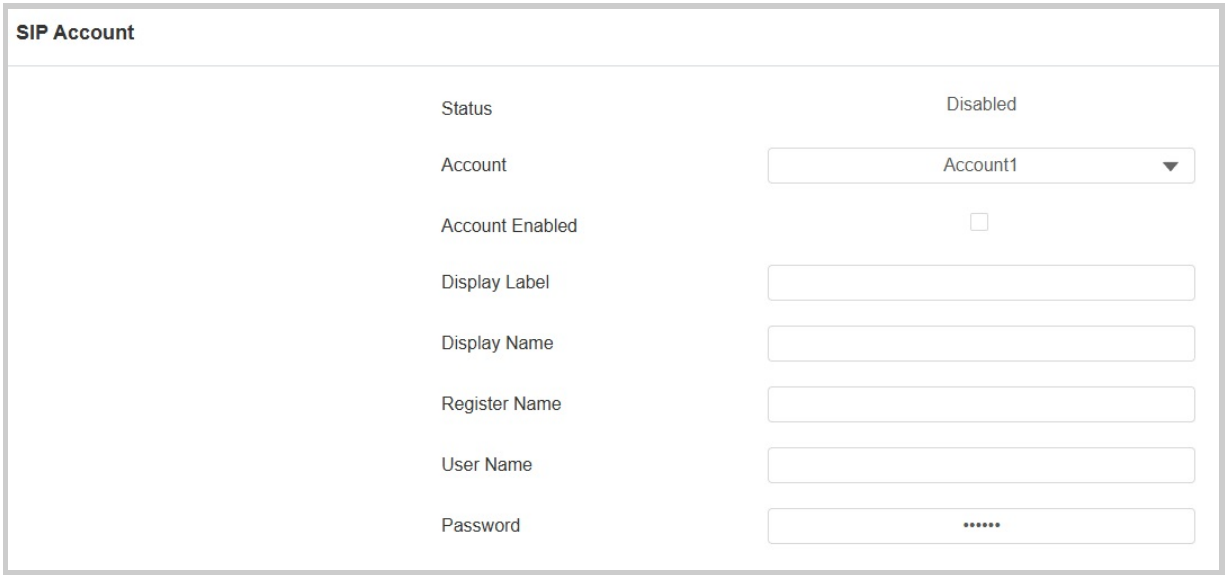
SIP Account Registration

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

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

Click here to view the SIP account registration example.

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



- **Status:** Indicate whether the SIP account is registered or not.
- **Account 1/Account 2:** The door phone supports 2 SIP accounts.
    - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.
    - The system switches to Account 2 if Account 1 is not registered.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 is to be shown on the device itself on the calling screen.
- **Register Name:** Same as the username from the PBX server.
- **User Name:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

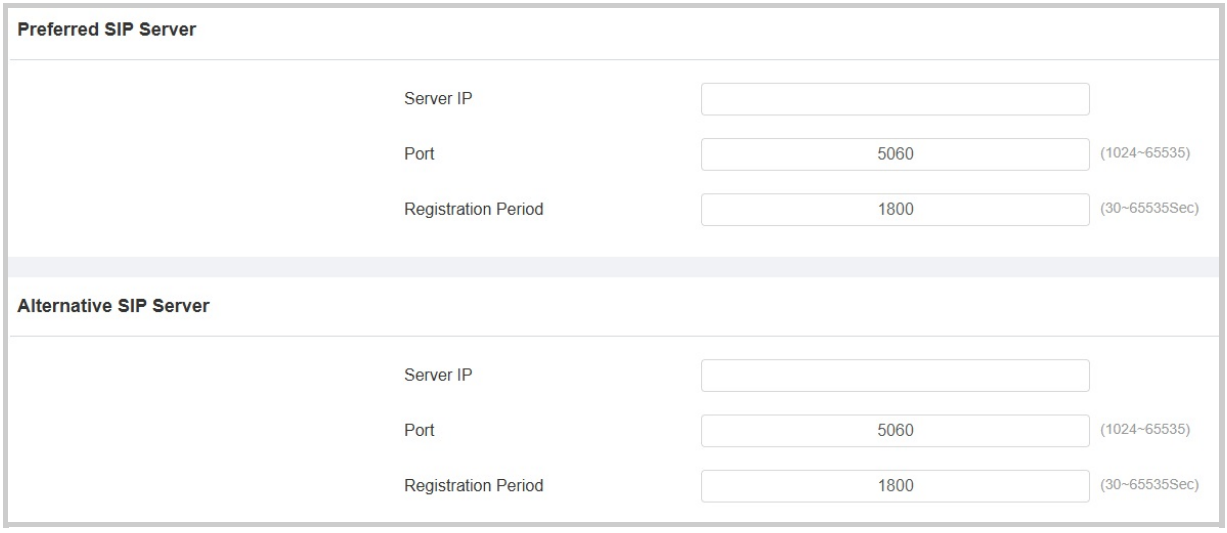
Tip

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

SIP Server Configuration

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

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

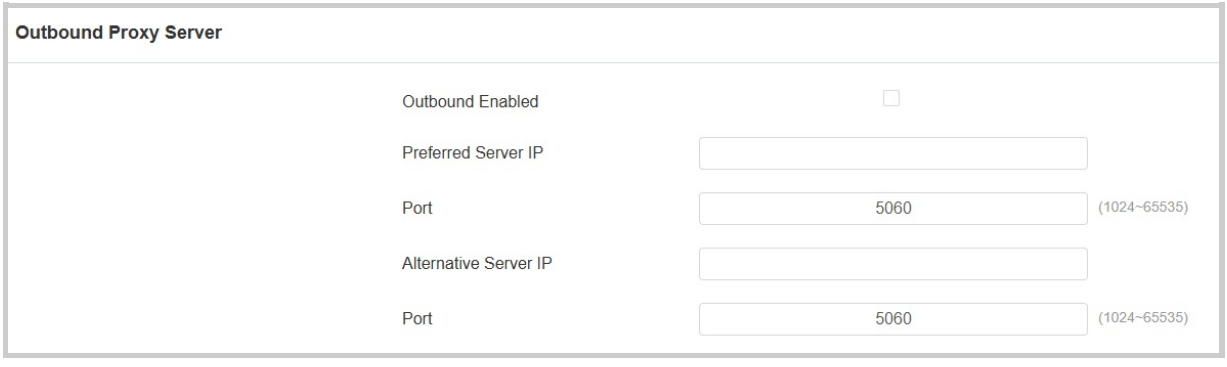


- **Server IP**: Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified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

Outbound Proxy Server

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

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



- **Preferred Server IP:** Enter the SIP proxy server's IP address.
- **Port:** Set the port 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 the web **Account > Basic > Transport Type** interface.

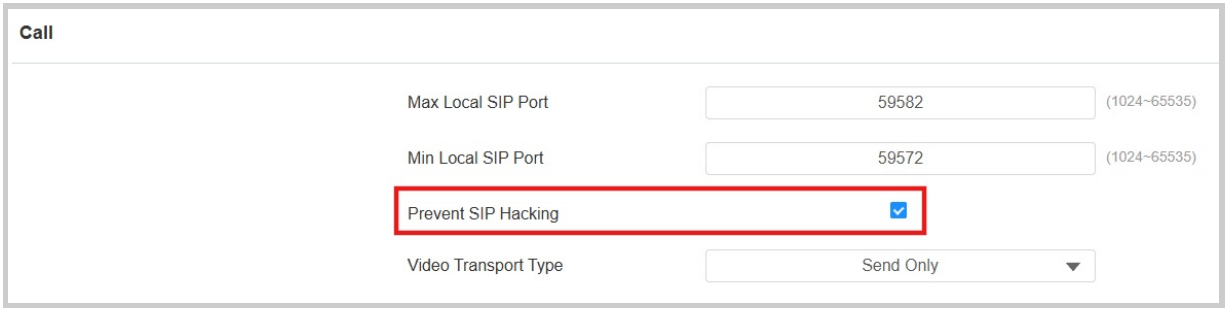


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

SIP Hacking Protection

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

To enable it, go to **Account > Advanced > Call** interface.

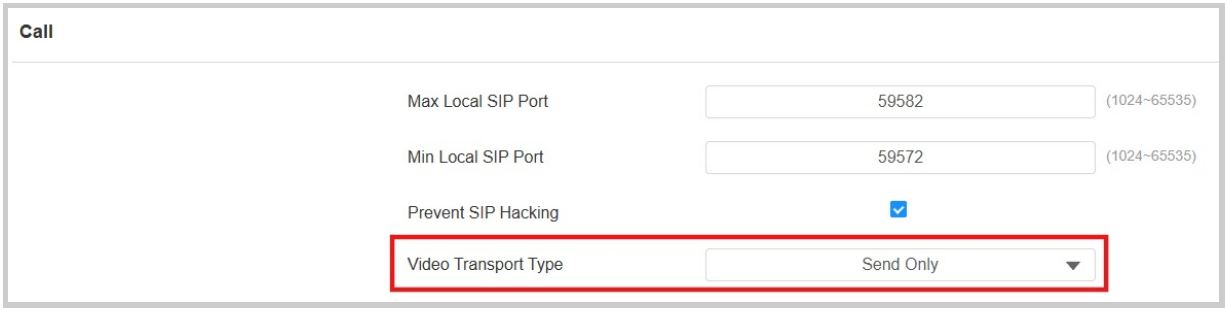


- **Prevent SIP Hacking**: Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Video Transport Type Selection

The video transport type controls how videos are viewed and shared between intercom devices during a call preview.

To choose the video transport type, go to the **Account > Advanced > Call** interface. This setting applies to SIP calls.



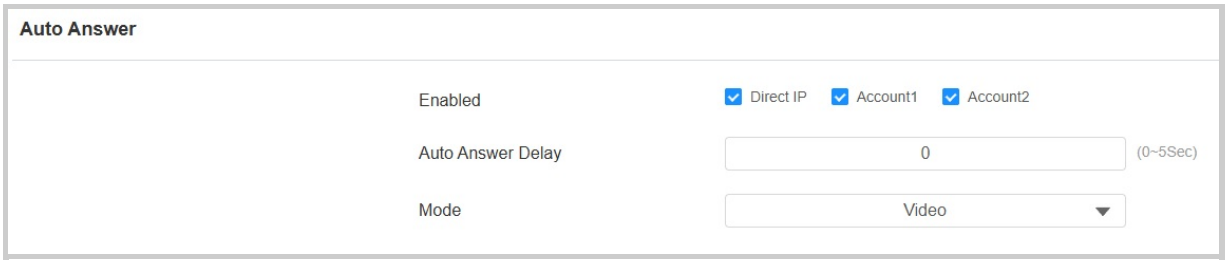
- **Video Transport Type**:
  - **Inactive**: No video transmission is taking place.
  - **Send Only**: The device will only send video data, but not receive any.
  - **Receive Only**: The device will only receive video data, but not send any.
  - **Send and Receive**: The device will both send and receive video data.

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.

Enable the feature on the **Intercom > Call Feature > Auto Answer** interface.

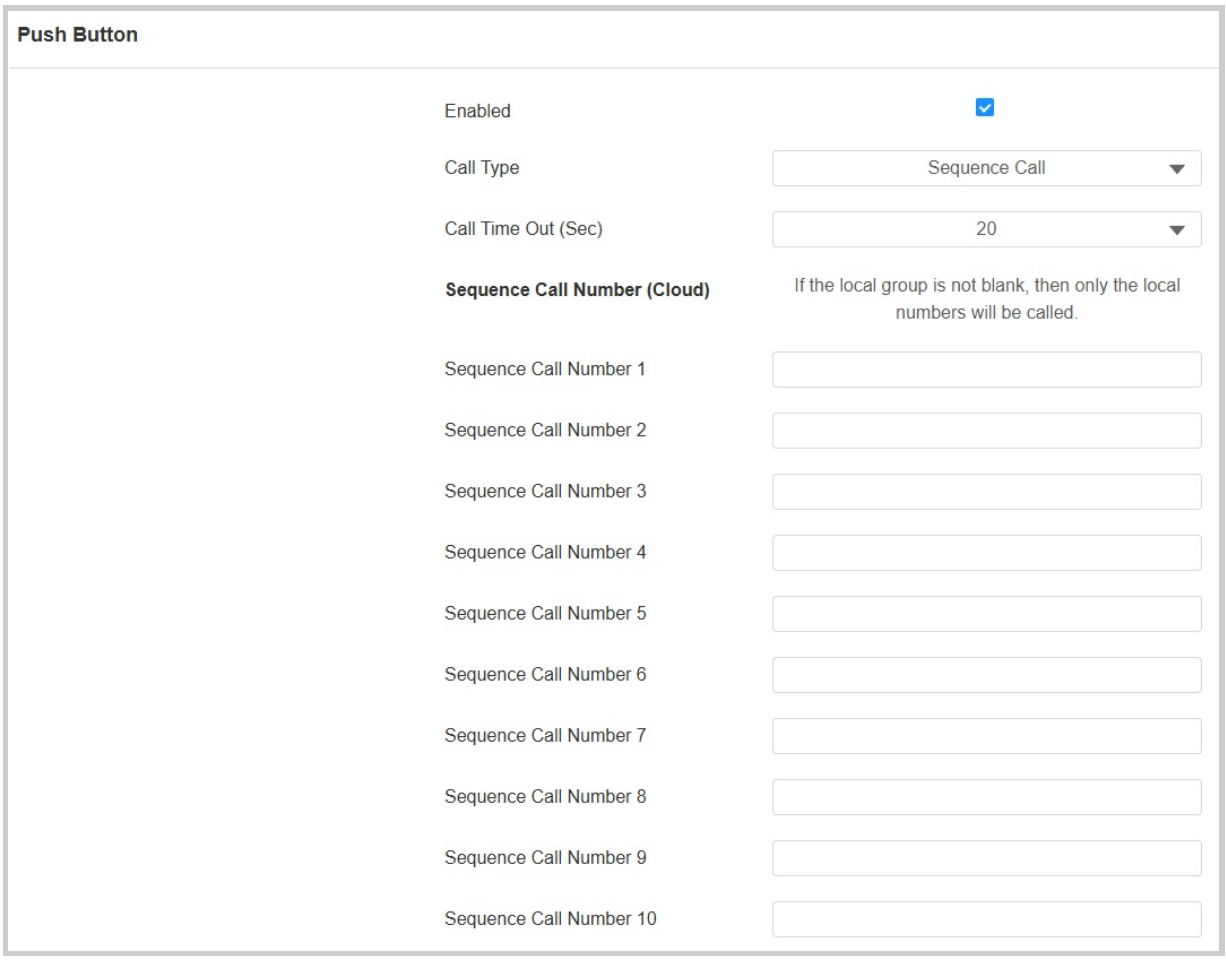


- **Enabled**: Enabled for all options by default. Specify that the auto-answer feature works for IP calls and/or SIP calls from account1/2.
- **Auto Answer Delay**: Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode:** Determine whether to auto-answer the call as a video or audio call.

Sequence Call

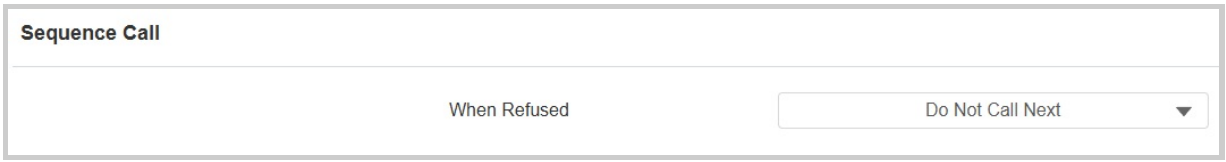
Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application. Please click here for the detailed configuration.

You can set up local sequence call numbers on the **Intercom > Basic > Push Button** interface.



- **Call Type**: Select Sequence Call.
- **Call Timeout(Sec)**: Determine the duration before calling the next number when the previous call is not answered.
- **Sequence Call Number**: Enter the target IP/SIP numbers.

Scroll to the **Sequence Call** section to configure the action when the sequence call is refused.



- **When Refused**:
  - **Do Not Call Next**: The device will stop calling.
  - **Call Next**: The device will continue to call the next number.

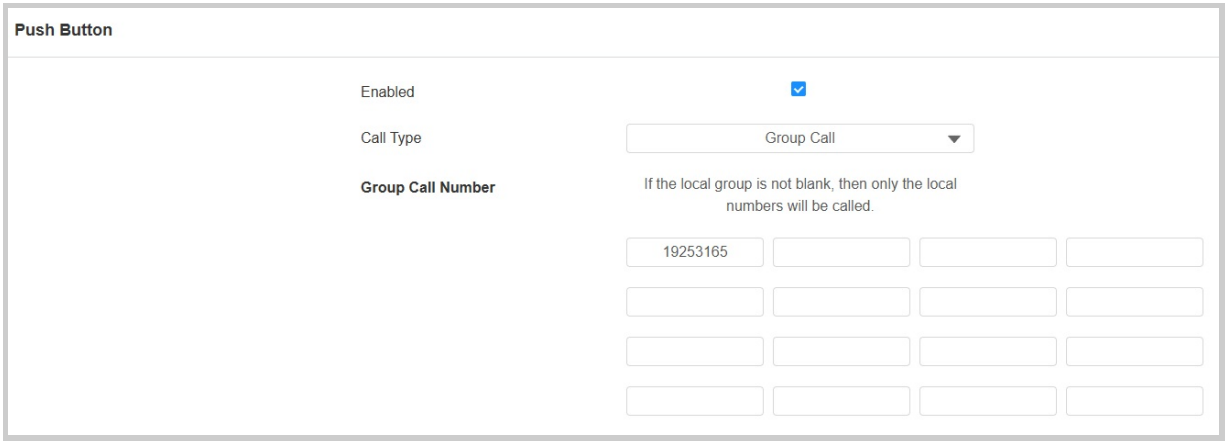
Note

When the device is connected to SmartPlus Cloud, local Sequence Call option will be unavailable.

Group Call

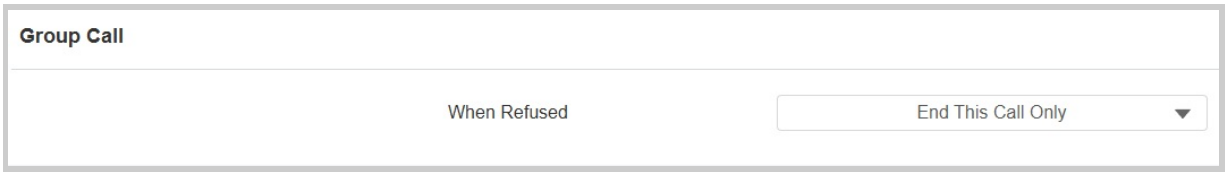
This feature allows users to call a group of contacts by a single press. The device supports local and SmartPlus-featured group calls. To learn about the detailed configuration, please click here.

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



- **Call Type**: Select Group Call.
- **Group Call Number**: Enter the target IP/SIP numbers.

Scroll to the **Group Call** section to configure the action when the group call is refused.

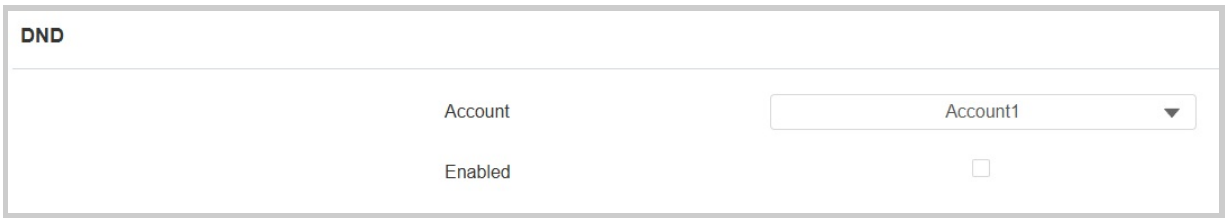


- **When Refused:**
  - **End This Call Only**: The device will continue to call other numbers.
  - **End All Calls**: The device will stop calling.

Do Not Disturb

The Do Not Disturb(**DND**) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus.

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



- **Account**: Choose the account to apply this feature.

Push To Hang Up

Users can hang up the call on the door phone by pressing the push button. To enable the feature, navigate to **Intercom > Basic** > **Push Button Action** interface.

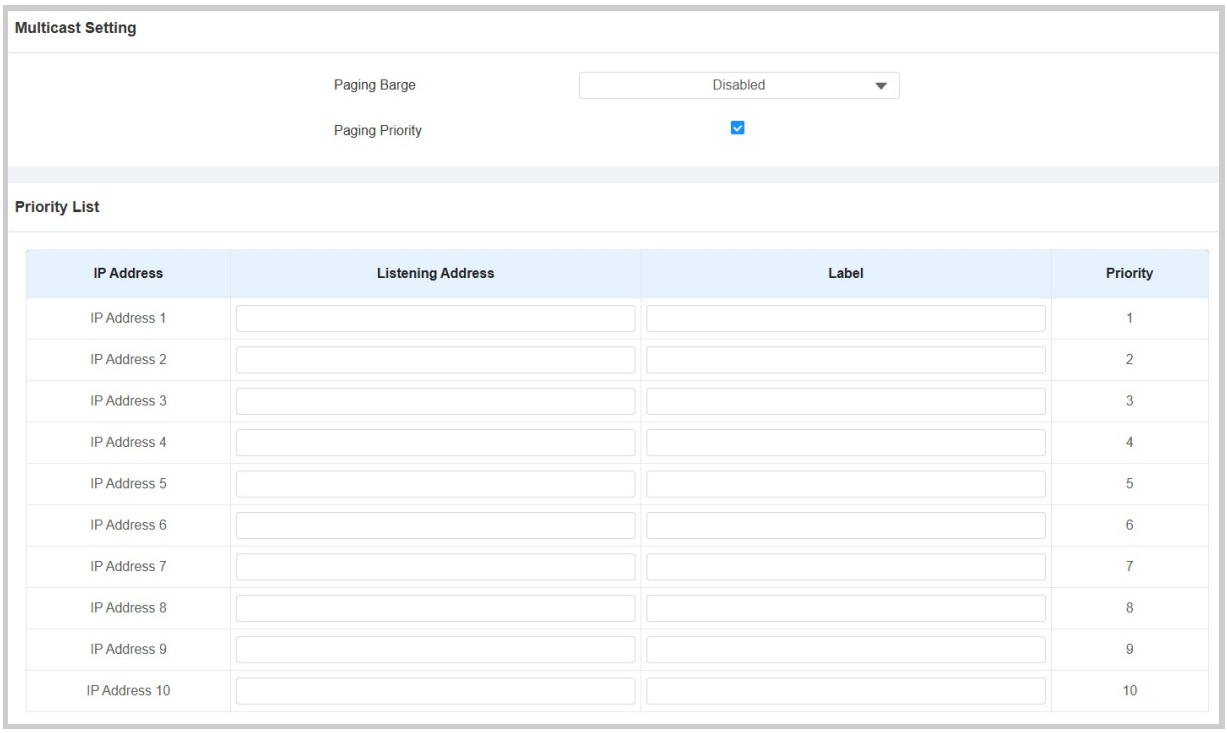


- **Action to Execute**: Specify the action to be carried out by pressing the push button.
  - **FTP**: Send a notification to the preconfigured FTP server.
  - **Email**: Send a notification to the preconfigured Email address.
  - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
    - **HTTP URL**: The format is http://HTTP server's IP/Message content.

Multicast

Multicast is a one-to-many communication within a range. The door phone can act as a listener and receive audio from the broadcasting source.

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



- **Paging Barge:** Determine how many multicast groups have higher priority than SIP calls. If disabled, SIP calls will have higher priority.
- **Paging Priority:** Decide whether to make a multicast in order of priority.
- **Listening Address:** Enter the IP address. The listen address should be the same as the multicast address. The listening port and the multicast port cannot be the same for each IP address. Multicast IP address is from 224.0.0.0 to 239.255.255.255.

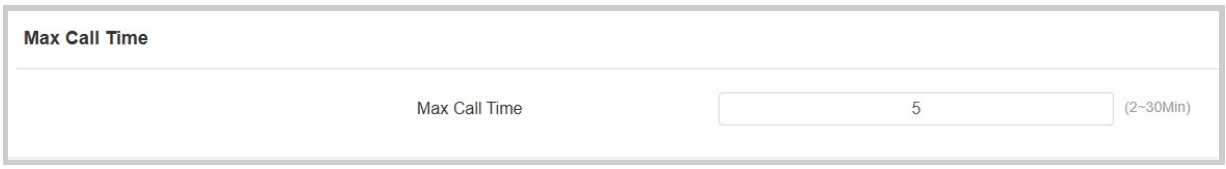
> **Note**
>
> Please contact Akuvox tech team for valid multicast address.

- **Label**: Name the multicast group.

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 up call time duration, navigate to the web **Intercom > Call Feature > Max Call Time** interface.



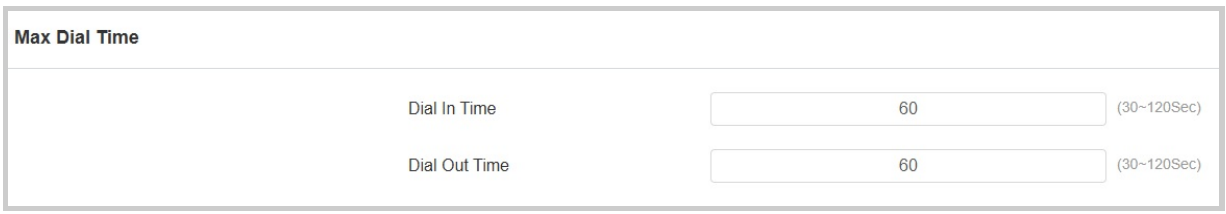
- **Max Call Time:** Specify the maximum duration of all calls. The door phone will end the call automatically when the time limit is reached.

> **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, navigate to **Intercom > Call Feature > Max Dial Time** interface.



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

Hang up After Opening Doors

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

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



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

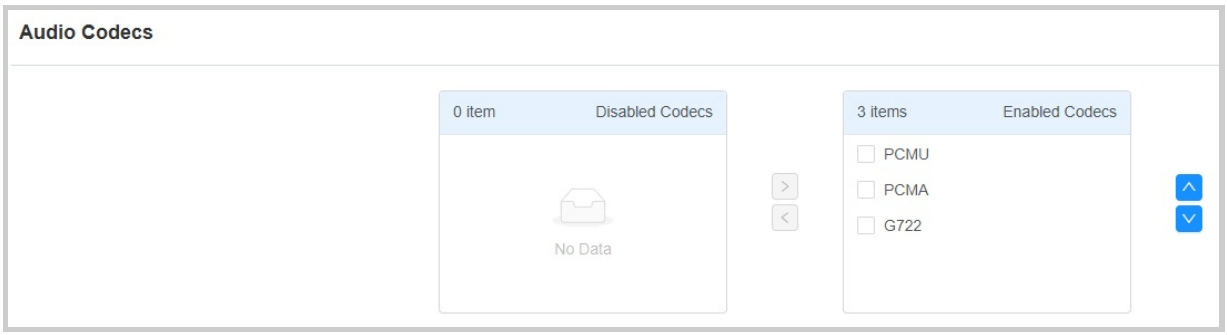
Audio & Video Codec Configuration

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 codec varies in terms of sound quality. PCMU and PCMA are well-suited for traditional telephony and bandwidth-constrained environments, while G722 delivers better audio quality for more modern communication needs.

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

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



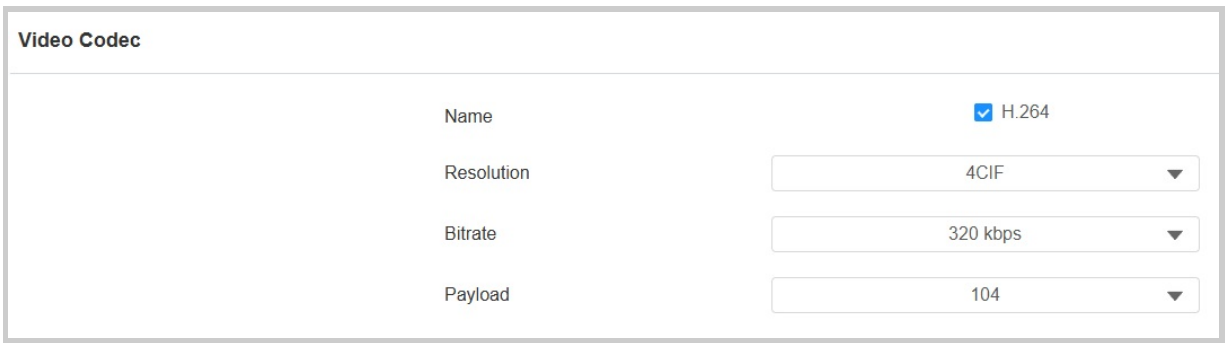
Please refer to the bandwidth consumption and sample rate for the three codec types below:

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

Video Codec

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

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

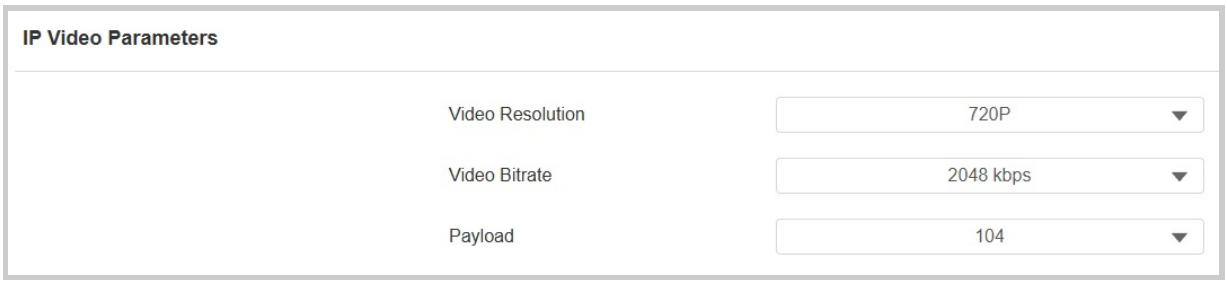


- **Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Resolution**: Select the resolution from the provided options. The default code resolution is 4CIF(704×576 pixels).
- **Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data is transmitted every second, and the clearer the video will be. The default code bitrate is 2048.
- **Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for IP Calls

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

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



- **Video Resolution**: Select the resolution from the provided options. The default is 720P(1280×720 pixels).
- **Video Bitrate**: The video stream bitrate ranges from 64 to 2048 kbps. The default bitrate is 2048.

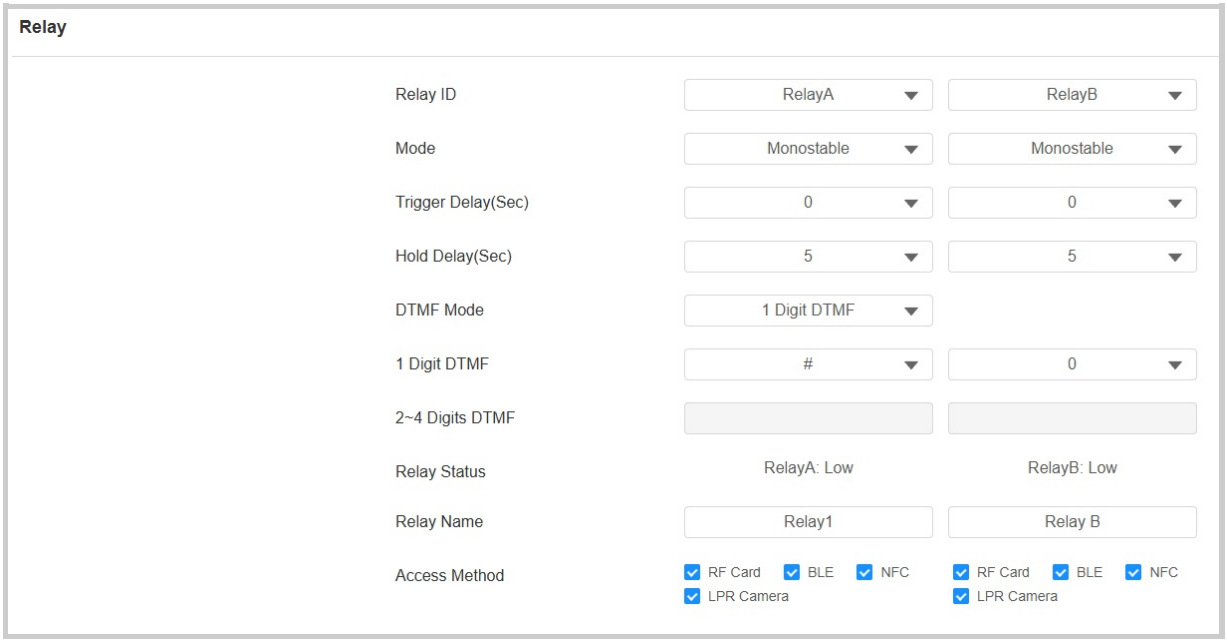
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Relay Settings

Local Relay

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

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



- **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.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.
- **Access Method**: Select the method(s) to trigger the relay.

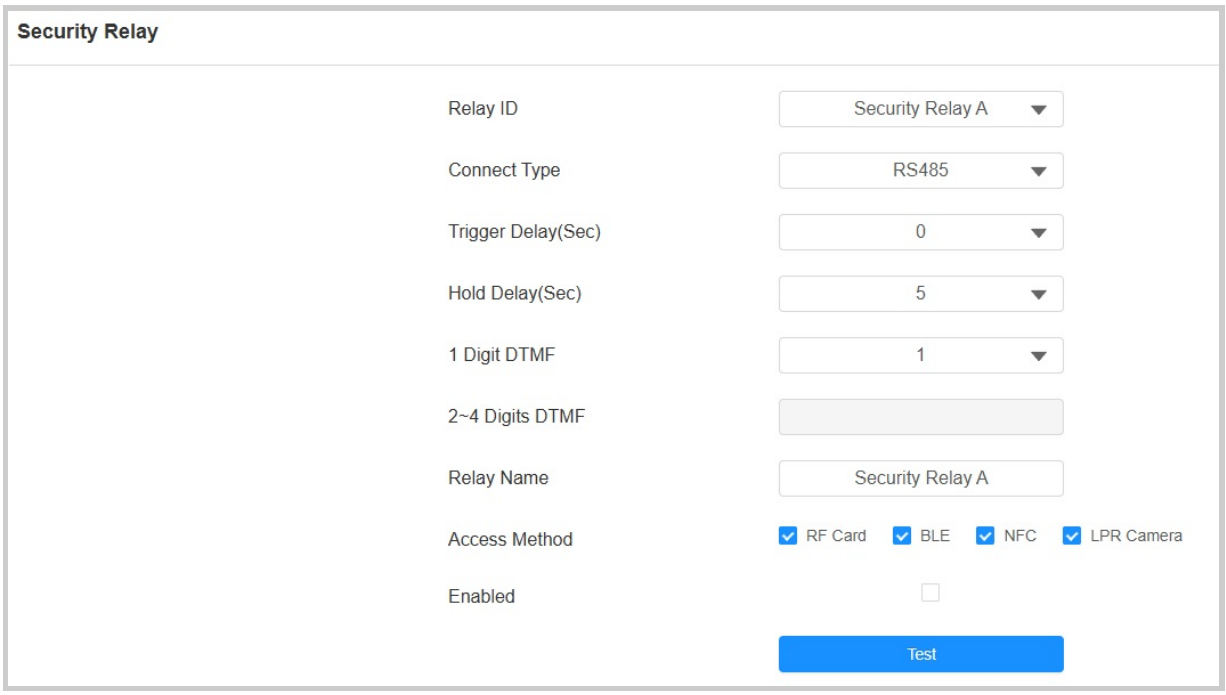
Security Relay

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**: Indicate the connection type between the security relay and the door phone. It is RS485 by default.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open for 5 seconds before closing.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-digit.
- **2~4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **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**: Select the method(s) to trigger the relay.
- **Test**: Click to send the signal to the SR01. When the door phone and SR01 are pairing, click Test to finish the matching.

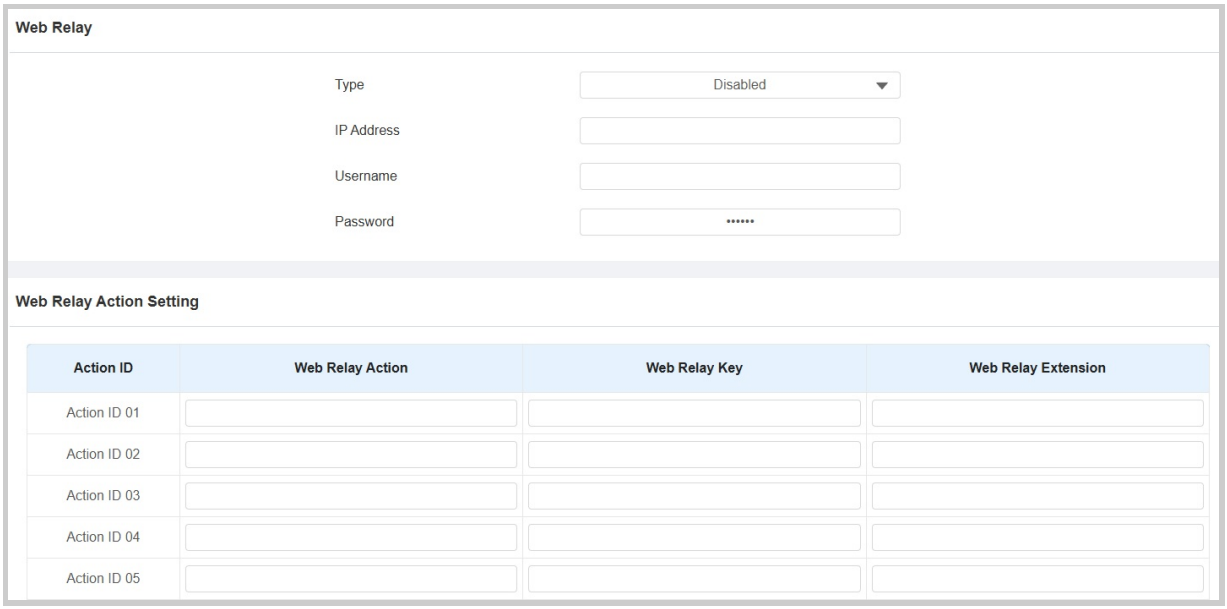
Web Relay

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, navigate to **Access Control > Web Relay** interface.



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

Access Control Schedule Management

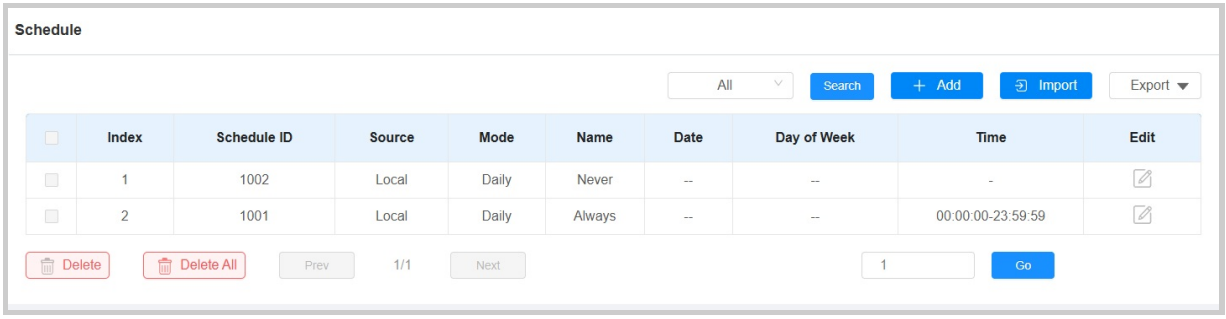
Configure Door Access Schedule

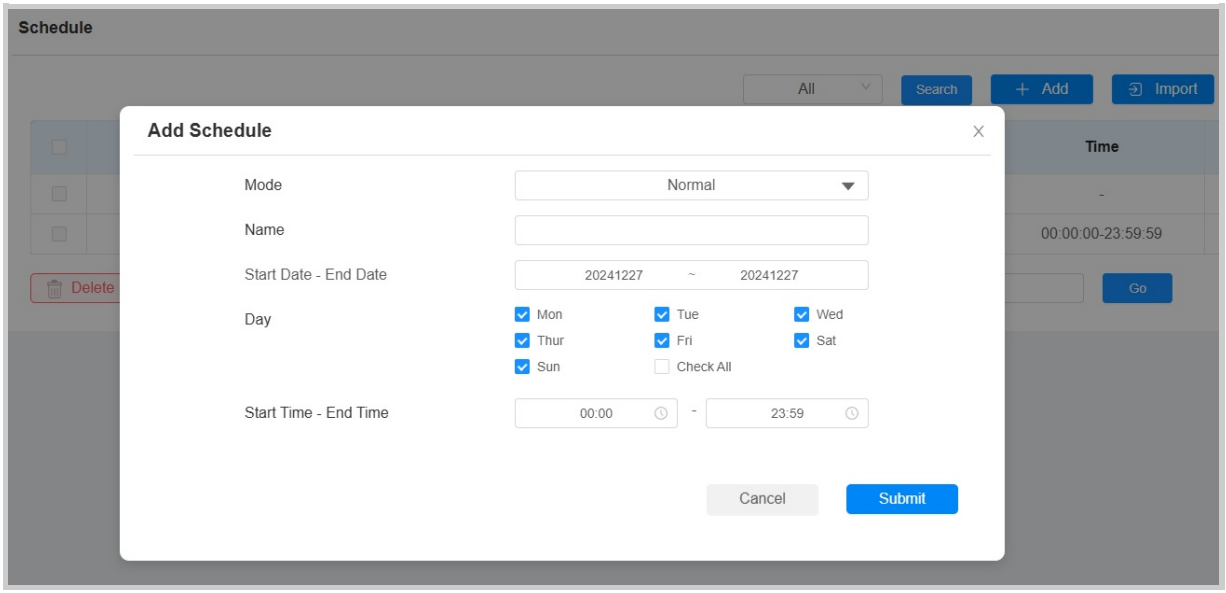
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Door Access Schedule

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

To set it up, navigate to the web **Setting > Schedule** interface. Click **+Add**.





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

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.

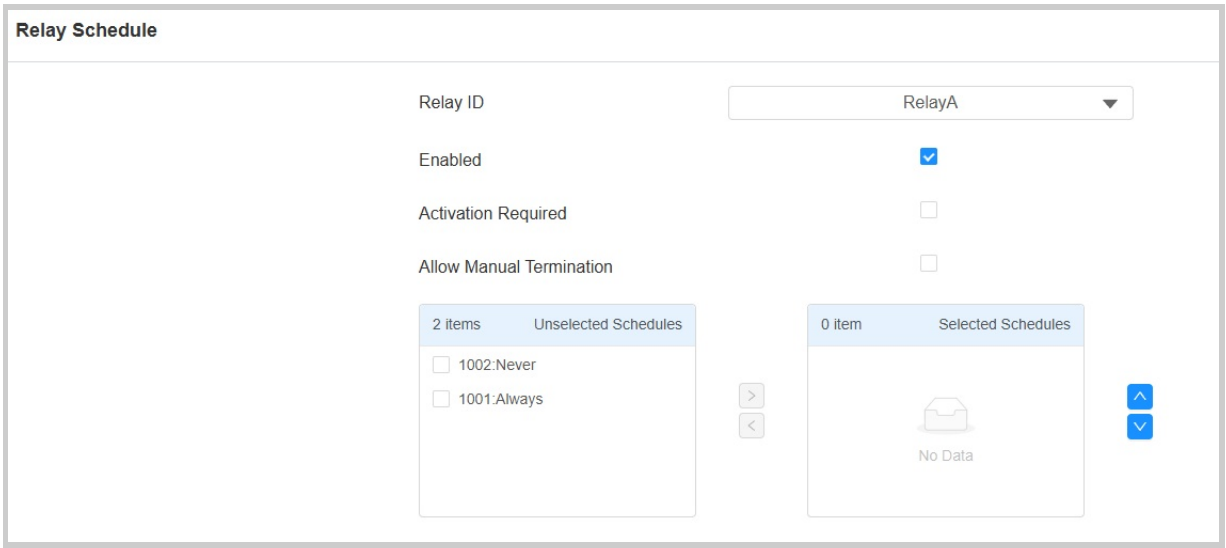
To set it up, go to the **Setting > Schedule** interface. The import/export file is in an XML file, supporting up to 100 schedules.



Relay Schedule

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

To set up a relay schedule, navigate to the **Access Control > Relay > Relay Schedule** interface.



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

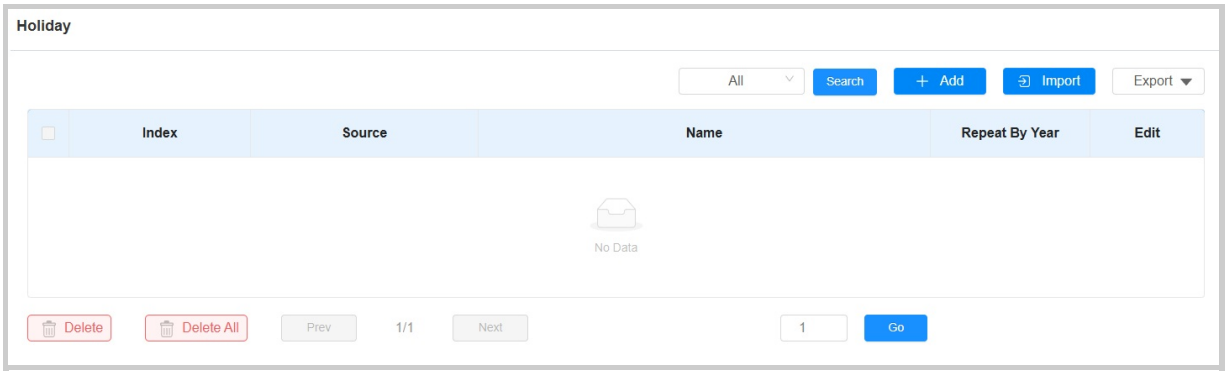
> **Note**
>
> Click **here** to view the details of the Activation Required feature

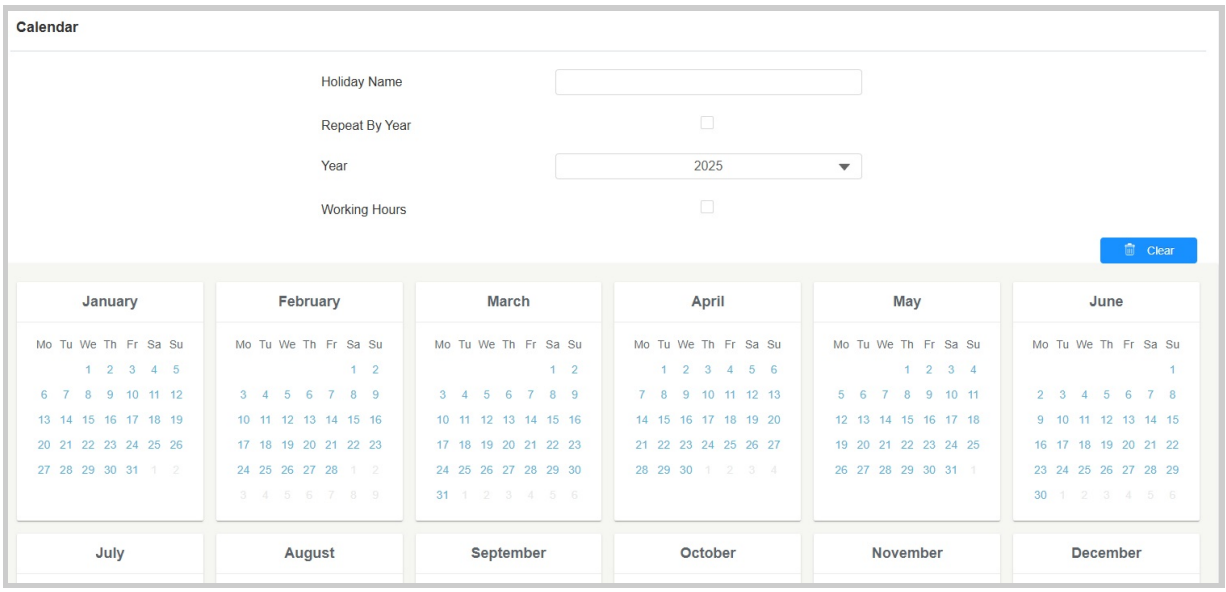
For instructions on creating schedules, kindly consult the Create Door Access Schedule section.

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.





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

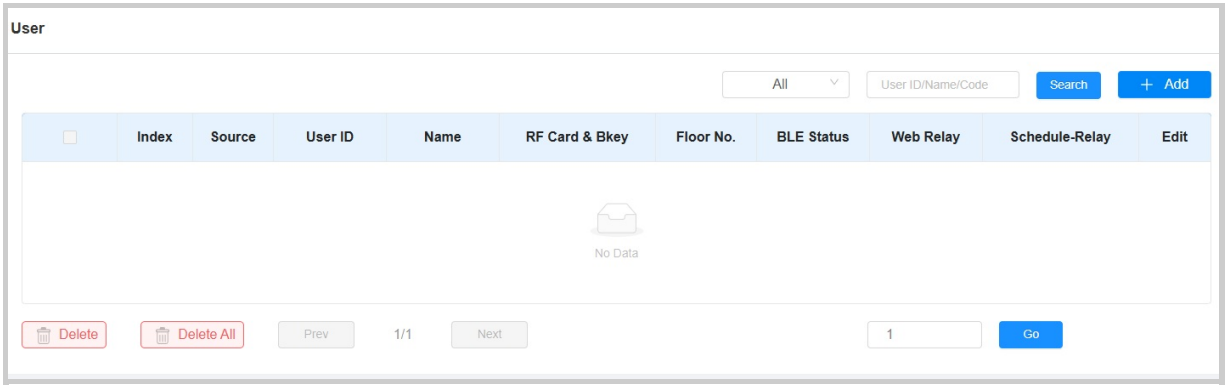
Door-opening Configuration

User-specific Access Methods

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

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

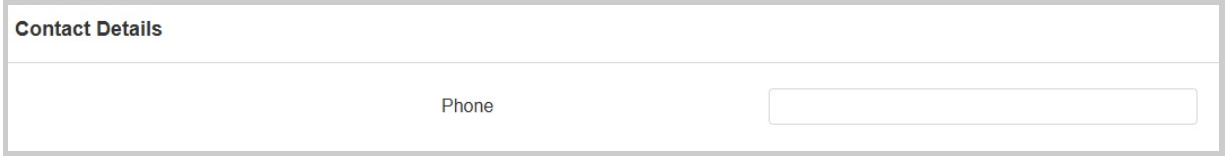
To add a user, go to **Directory > User** interface and click **+Add**.





- **User ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.
- **Role**: Specify the user's identity, as a general user or an administrator.

Then scroll to the **Contact Details** part to set up the user's contact.



- **Phone**: The IP or SIP number.

Unlock by RF Card/Bkey

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

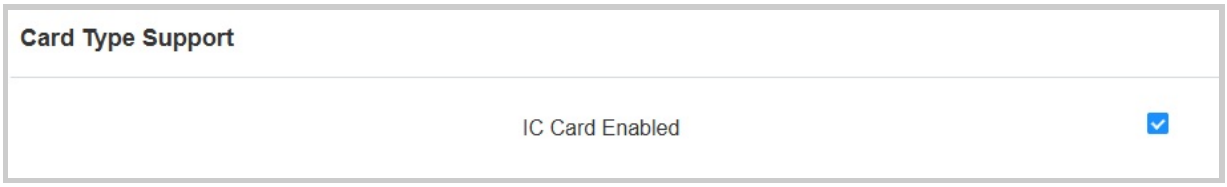


- **Code**: The card number that the card reader reads.

Note:

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

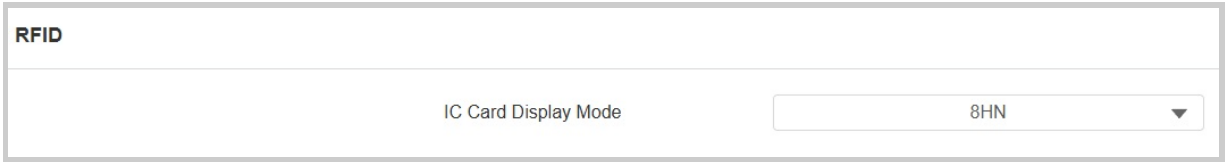
You can enable and disable the use of RF cards on the **Access Control > Card Setting** interface.



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 Card Display Mode**: Set the card number format from the provided options.

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 Bluetooth

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

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

Unlock via My MobileKey

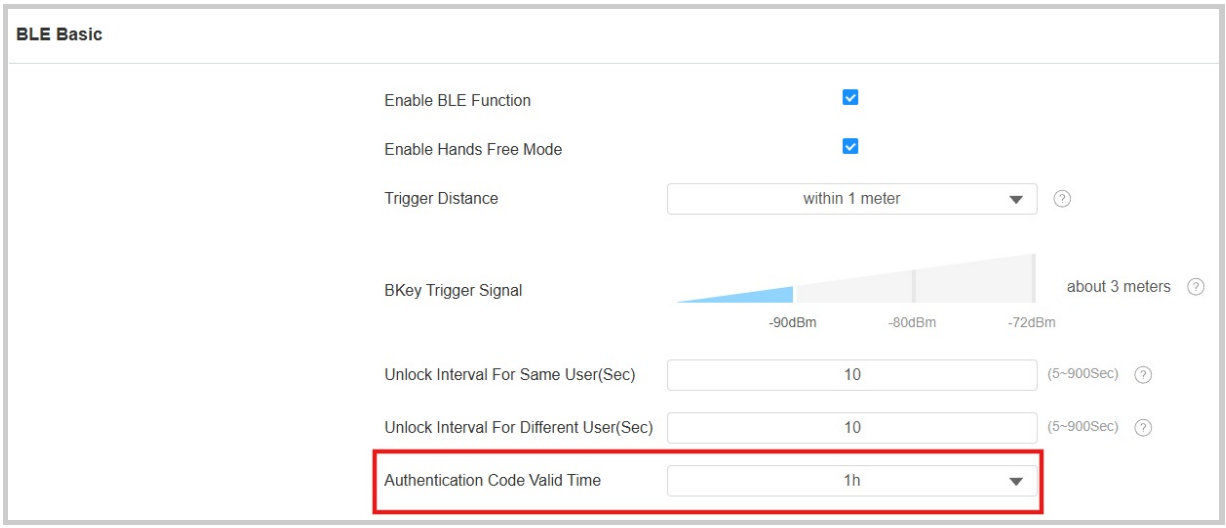
On the **Directory > User > +Add** interface, scroll to the **BLE Setting** section.



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

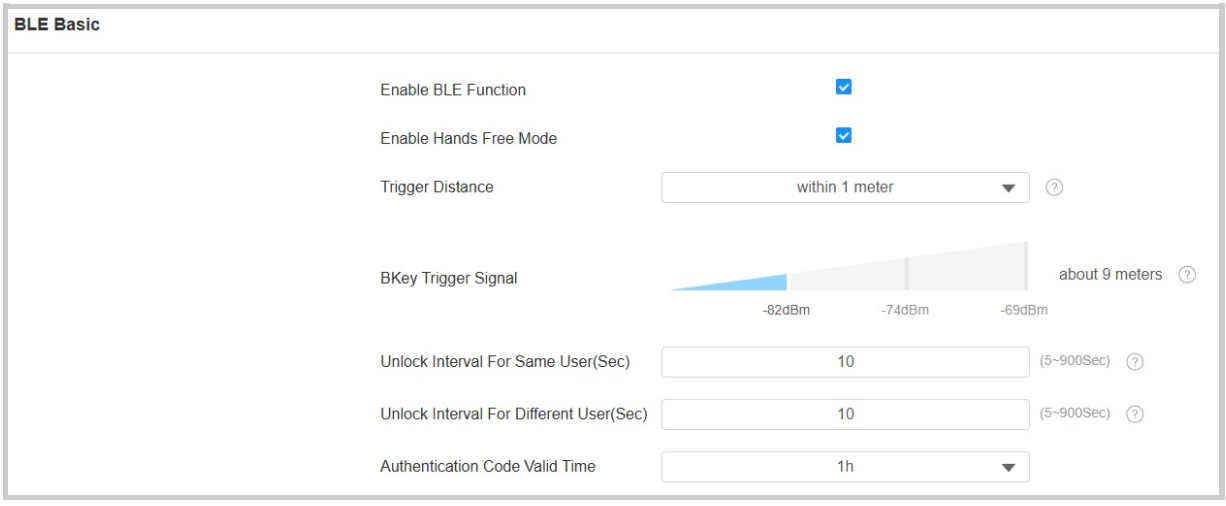
You can set up the pairing valid time within which users need to finish the pairing.

To set it up, go to **Access Control > BLE > BLE** interface.



Bluetooth Settings

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



- **Enable Hands Free Mode**: If enabled, users can gain door access hands-free. If disabled, users have to wave their hands near the device to open doors.
- **Trigger Distance**: Set the triggering distance of the Bluetooth for the door access. You select Within 1 Meter, Within 2 Meters, and Within 3 Meters. The trigger distance is 3 meters maximum.
- **Bkey Trigger Signal**: There are three ranges that determine the Bkey trigger distance, ranging from 1 meter to 9 meters.
- **Unlock Interval For Same User(Sec)**: Set the time interval between consecutive Bluetooth door access attempts for the same user.
- **Unlock Interval For Different Users(Sec)**: Set the time interval between consecutive Bluetooth door access attempts for different users.

Note

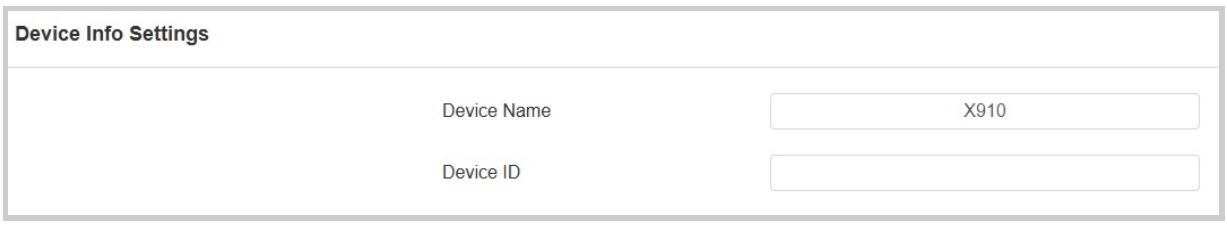
To learn about detailed configuration steps of different Bluetooth-based access methods, you can click the following articles.

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

Device Info Settings

You can customize the device name and ID for convenient Bluetooth pairing.

To set it up, go to **Access Control > BLE > Device Info Settings** interface.

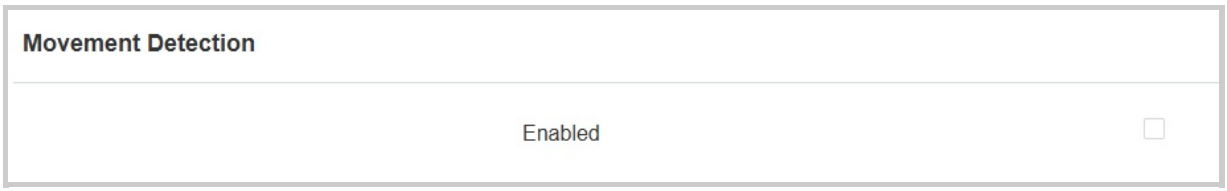


- **Device Name**: Limited to 1-63 numbers or characters.
- **Device ID**: Limited to 1-12 numbers or characters.

Bluetooth Movement Detection

This feature only works for Bluetooth-based door opening via the My Mobilekey App. When enabled, users cannot open the door without shaking their mobile phones.

Enable the function on the **Access Control > BLE > Movement Detection** interface.

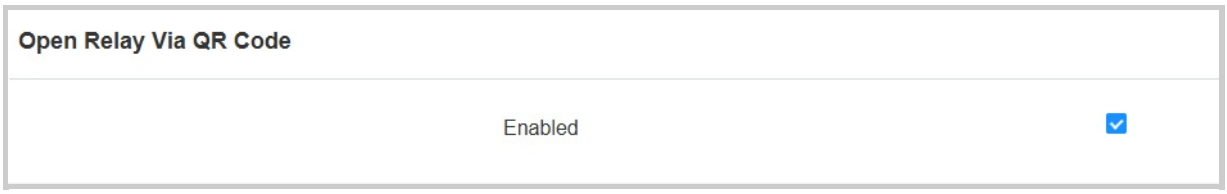


Unlock By QR Code

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. It is enabled by default.



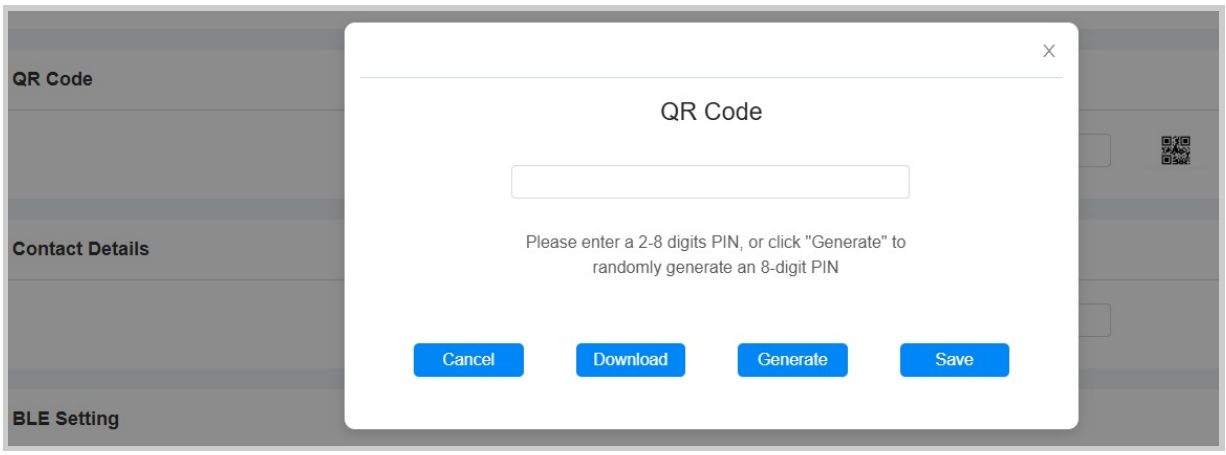
Generate QR Codes on the Web

On the **Directory > User > +Add** interface, scroll to the **QR Code** section.

Click the QR code icon .



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

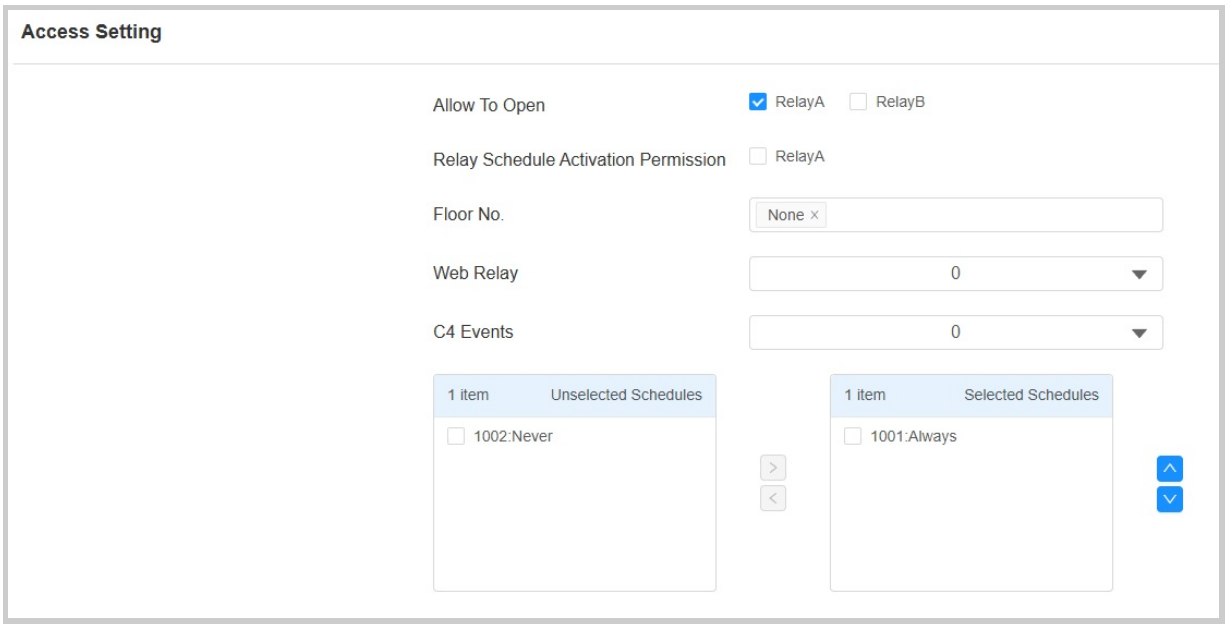


- **Cancel**: Click to return to the user editing interface. The QR code and the PIN code will not be saved.
- **Download**: Click to save the QR code to your PC.
- **Generate**: Click to generate another QR code and PIN code.
- **Save**: Click to return to the user editing interface and save the code.

Access Setting

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

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



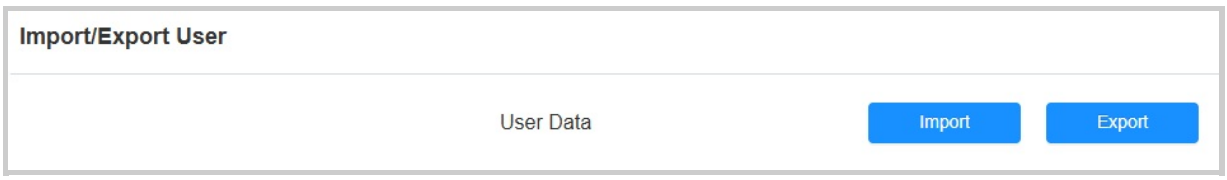
- **Allow to Open**: Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **Relay Schedule Activation Permission**: This decides whether the user can keep the relay open during the scheduled time after activating it.
- **Floor No.**: Specify the floor(s) that are accessible 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.
- **C4 Events**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
    - **Always**: Allows door opening without limitations on door open counts during the valid period.
    - **Never**: Prohibits door opening.

Import/Export User Data

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

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

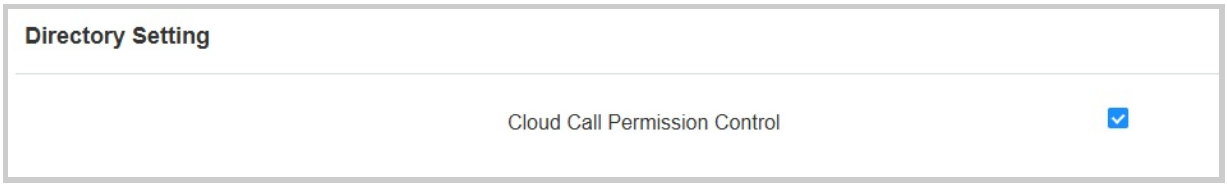
Navigate to the web **Directory > User > Import/Export User** interface. The import file should be in TGZ format. The device supports 5,000 local users.



Cloud Call Permission Control

This option works 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.

Enable/disable it on the **Directory > Directory Setting** interface. It is enabled by default.



- 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.
- When this feature is disabled, even if users cannot open doors, they can receive the call.

Unlock by Contactless Smart Card

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

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



Note

- The NFC feature is not available on iPhones.
- Click **here** to view the detailed configuration of opening doors via NFC.

Unlock by 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 > Mifare Card Encryption** interface.

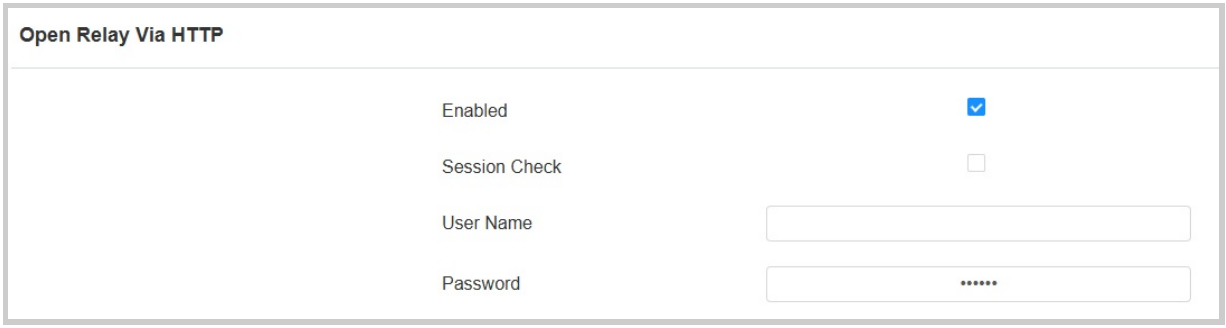


- **Mifare**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
- **Plus**: You can set up three choices. This means you can use three types of Mifare Plus cards. When swiping a card, as long as one of the choices matches its SL key, the card code in the block you specified will be output.
  - **Block**: Specify the block(s) to be read.
  - **SL3**: The key number within 32 bits.
- **DESFire**:
  - **App ID**: A 6-digit hexadecimal number
  - **File ID**: The ID of the encrypted file of the app, which can be a number from 0 to 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 HTTP Command

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

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



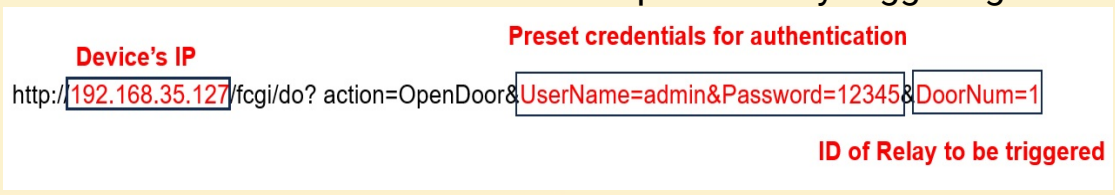
- **Username**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a password for authentication in HTTP command URLs.

Note

Click **here** to view the detailed configuration of opening doors via HTTP commands.

Tip:

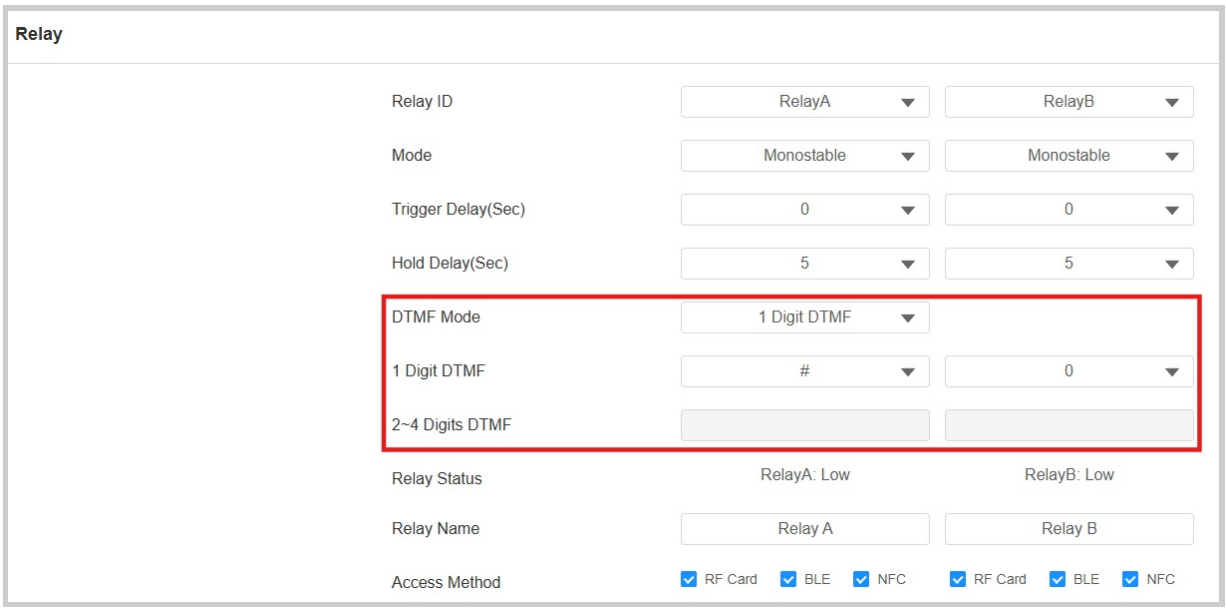
Here is an HTTP command URL example for relay triggering.



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.

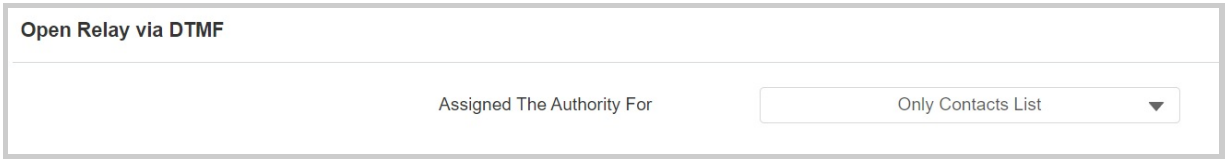


- **DTMF Mode**: Set the number of digits for the DTMF code.
- **1 Digit DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2-4 Digits DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

> **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 Contacts List**: Doors can be opened by contact numbers added to the door phone's user 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.

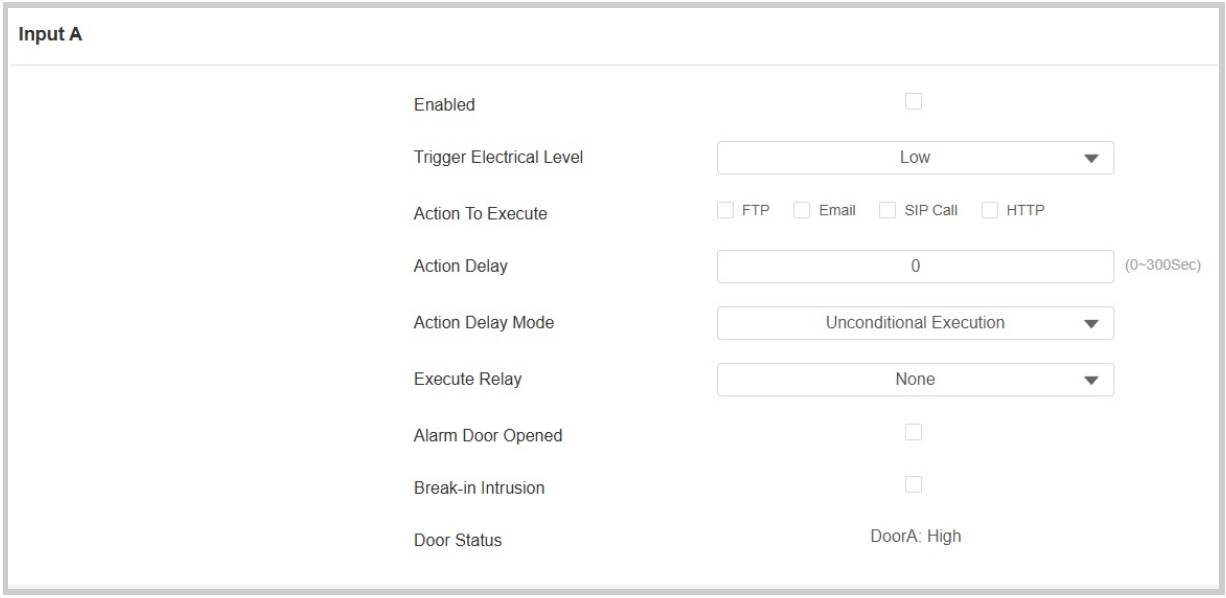
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, or **Telephone-Event** according to the specific type adopted by the third-party device. You are required to set it up only when the third-party device to be matched with adopts **Info** mode.
- **Payload**: Set the payload according to 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, go to **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 notification to the preconfigured FTP server.
    - **Email**: Send a notification 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.
- **Action Delay Mode**:
    - **Unconditional Execution**: The action will be carried out when the input is triggered.
    - **Execute If Input Still Triggered**: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Alarm Door Opened**: If enabled, when the door-opening time exceeds a limit, an alarm will be triggered.
    - **Door Opened Timeout**: The door-opening time limit.
- **Break-in Intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. Click here to learn more information about this feature.
- **Door Status**: Display the status of the input signal.

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.

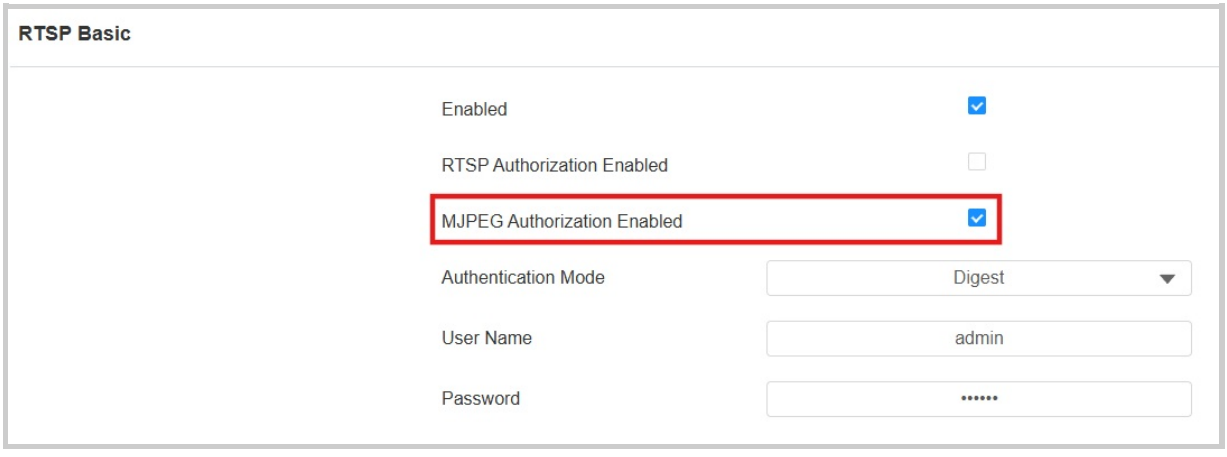
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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 Authorization

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

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



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

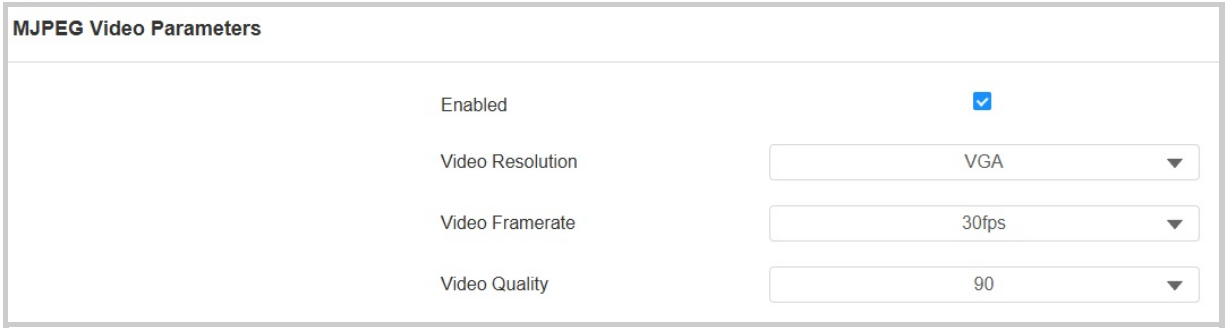
Tip

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

MJPEG Video Stream

You can take a monitoring image and view video streams in MJPEG format with the device.

To set it up, go to the **Surveillance > RTSP > MJPEG Video Parameters** interface.



- **Video Resolution**: Specify the video resolution from the lowest QCIF(176×144 pixels) to the highest 1080P(640×480 pixels).
- **Video Framerate**: It is 30 fps by default.
- **Video Quality**: It is 90 by default.

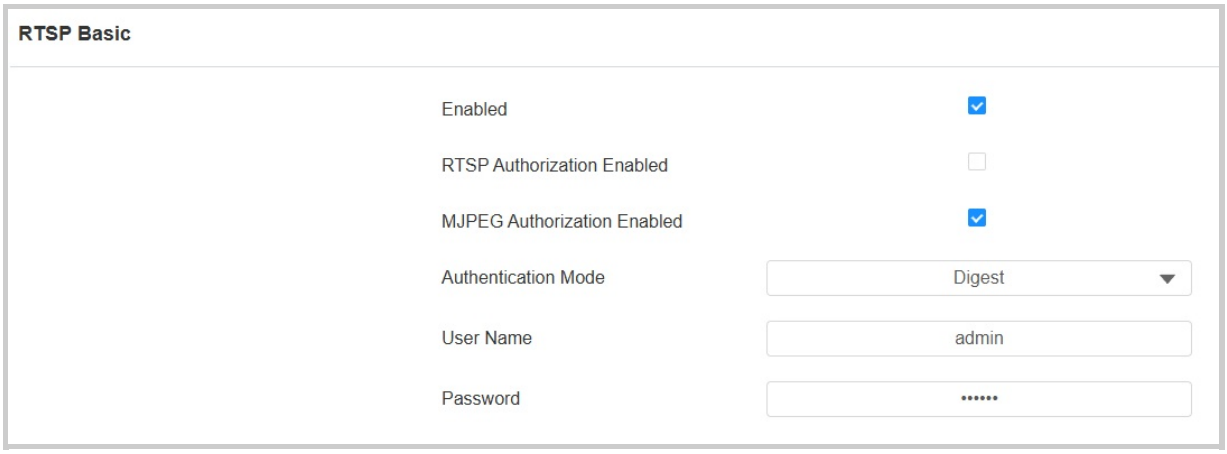
RTSP Stream Monitoring

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

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

RTSP Basic Setting

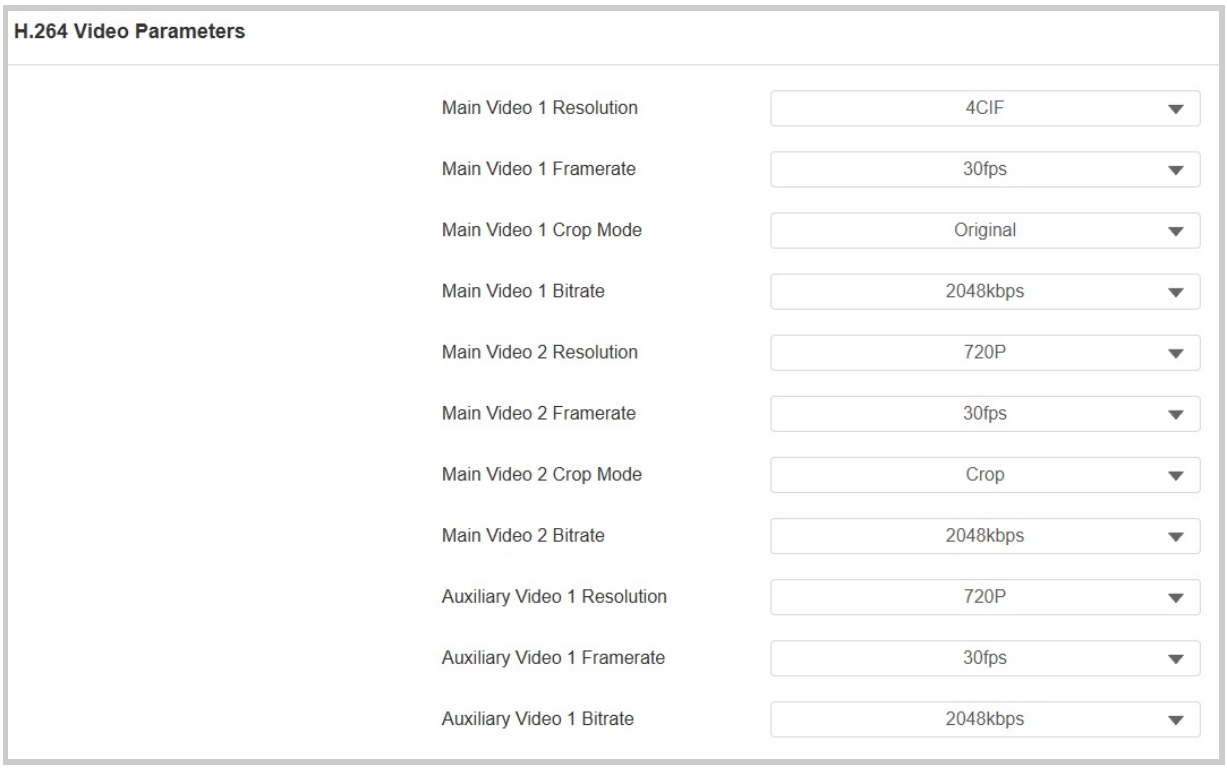
You are required to set up the **RTSP** function on the web **Surveillance > RTSP > RTSP Basic** interface in terms of RTSP Authorization, authentication, password, etc., before you are able to use the function.



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

RTSP Stream Setting

The RTSP stream can use 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.



- **Main Video 1 Resolution**: Specify the image resolution for the first video stream channel of the main camera, varying from the lowest QCIF(176×144 pixels) to the highest 2K(2560×1440 pixels). The default is 4CIF.
- **Main Video 2 Resolution**: Specify the image resolution for the second video stream channel of the main camera, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Main Video 1/2 Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Main Video 1/2 Crop Mode**:
    - **Crop**: The transmitted video frame is cropped to eliminate vignettes.
    - **Original**: The original video frame is transmitted without cropping.
- **Main Video Video 1/2 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.

- **Auxiliary Video 1 Resolution**: Specify the image resolution for the first and second video stream channels of the auxiliary camera at the bottom of the device, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Auxiliary Video 1 Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Auxiliary Video 1 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.

Tip

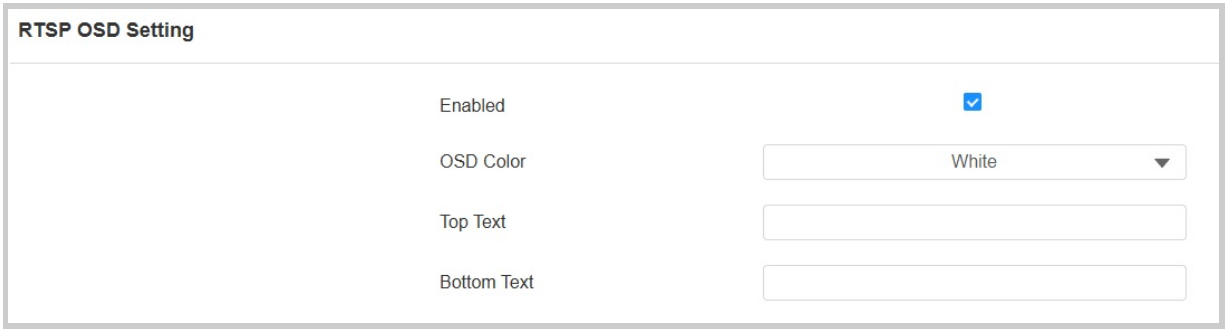
To view the audio and video stream using RTSP:

- First channel: rtsp://Device's IP/live/ch00_0
- Second channel: rtsp://Device's IP/live/ch00_1
- The auxiliary camera at the device bottom: rtsp://Device's IP/live/ch00_2

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture.

Set it up on the web **Surveillance > RTSP > RTSP OSD Setting** interface. It is disabled by default.



- **OSD Color**: There are five color options, White, Black, Red, Green, and Blue, for RTSP watermark text.
- **Top Text**: Customize the watermark text displayed at the top.

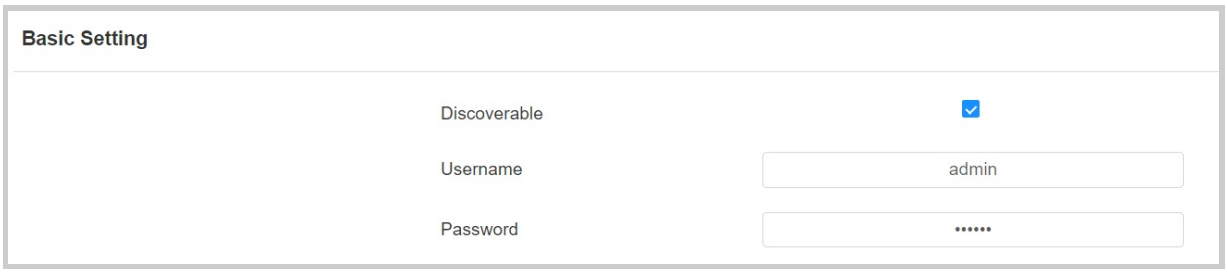
- **Bottom Text**: Customize the watermark text displayed at the bottom.

ONVIF

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

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

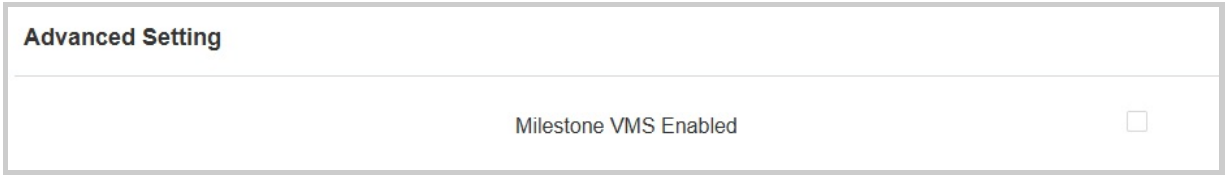
To set it up, go to the web **Surveillance> ONVIF** interface.



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

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

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

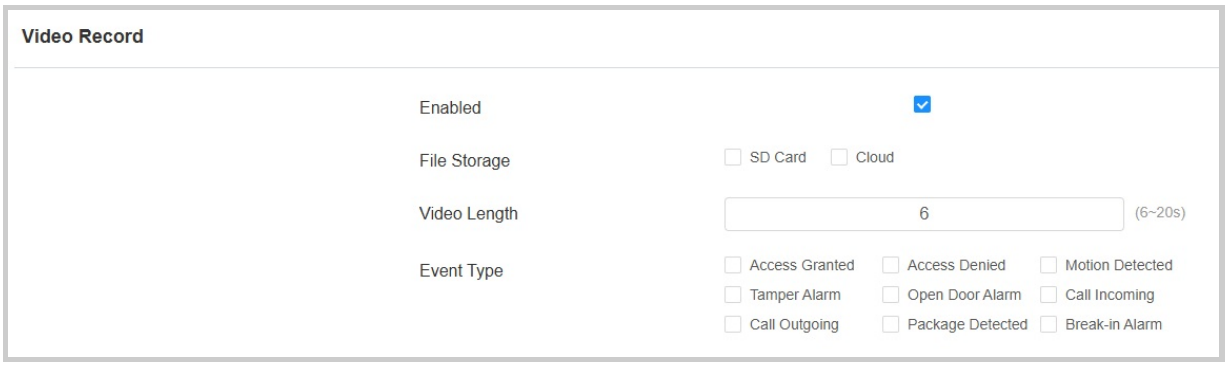


Video Record

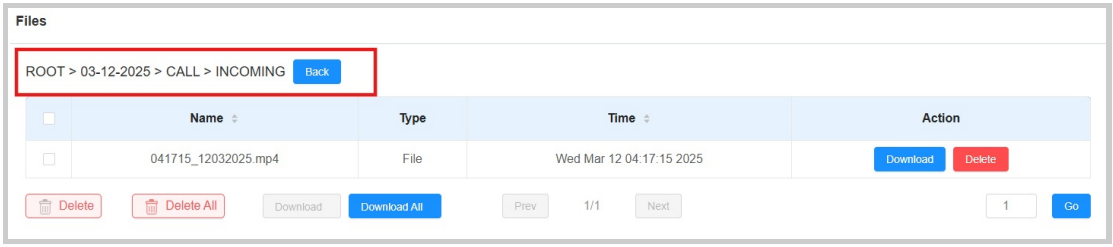
The video record feature enables the device to record videos automatically when specific events happen.

Except for package detection, the X910 only uses the main camera to record videos.

Set it up on the **Surveillance > Video Record** interface.



- **File Storage**: Store the videos in the SD Card or the SmartPlus Cloud. Only when the device has an SD card inserted or is connected to the SmartPlus Cloud will these two options display. When videos are stored in the SD card, the storage path is **date/event/event details**.



- **Video Length**: The video recording length.
- **Event Type**: Specify the event that will trigger video recording.

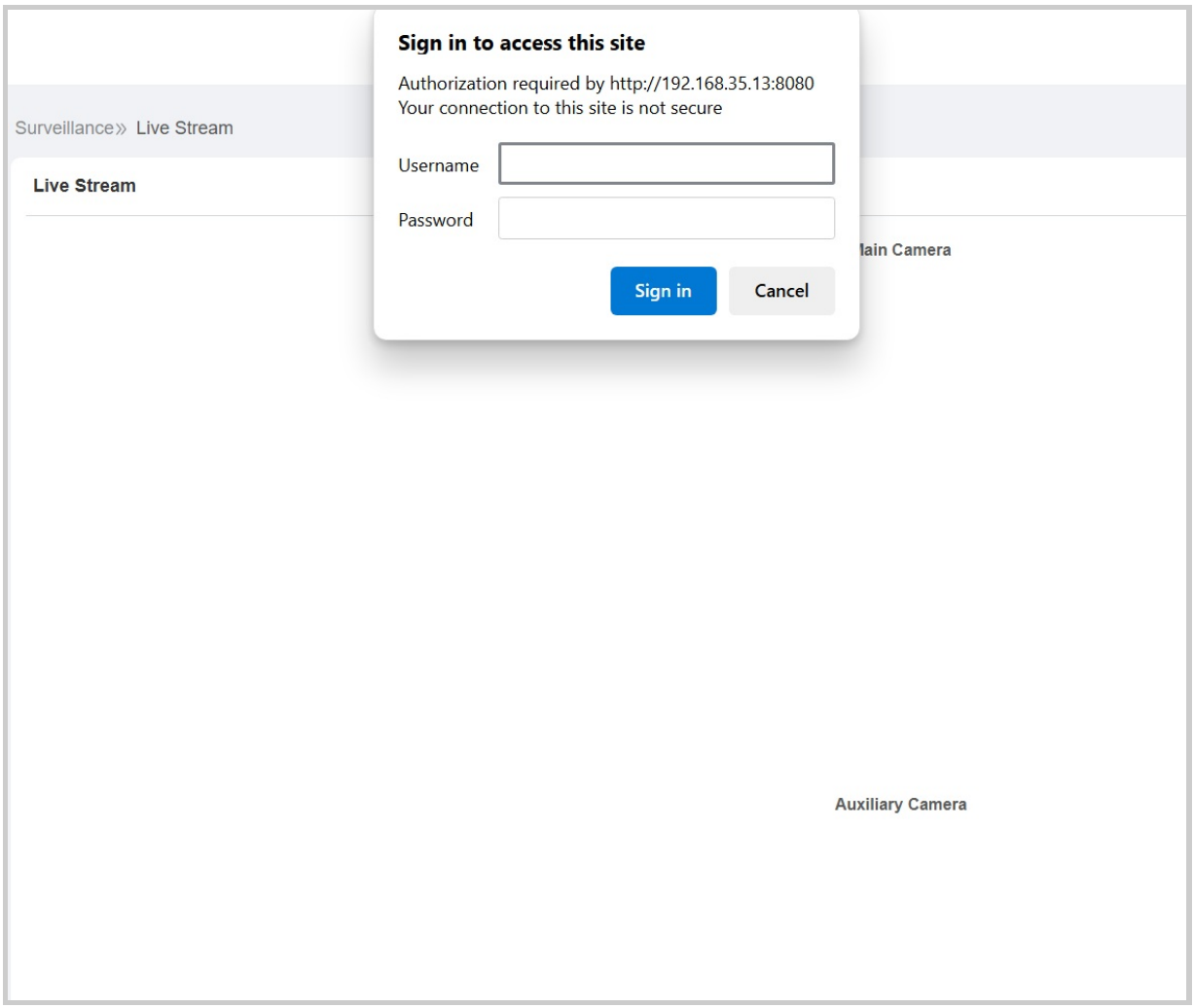
Note

- When the videos are stored in the SD card, all event types are supported.
- When the videos are stored on the SmartPlus Cloud, specific event types(Access Granted/Denied; Motion Detected; Call Incoming/Outgoing) are supported.
- Click **here** to view how to set up the feature on the SmartPlus Cloud.

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.

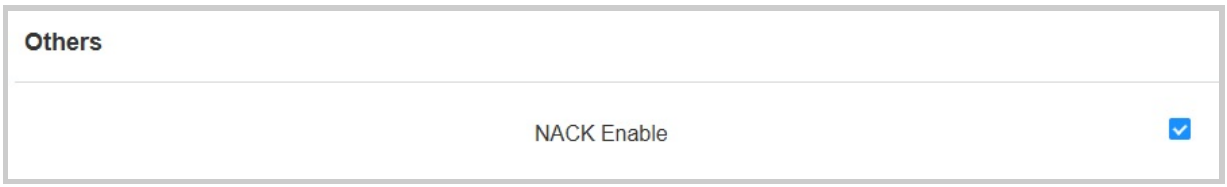
View the video stream on the **Surveillance > Live Stream** interface. If you have enabled MJPEG authorization, you need to enter the user name and password set in the RTSP Basic section for viewing the stream.



NACK

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

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



Data Transmission Type for Third-party Camera

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

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

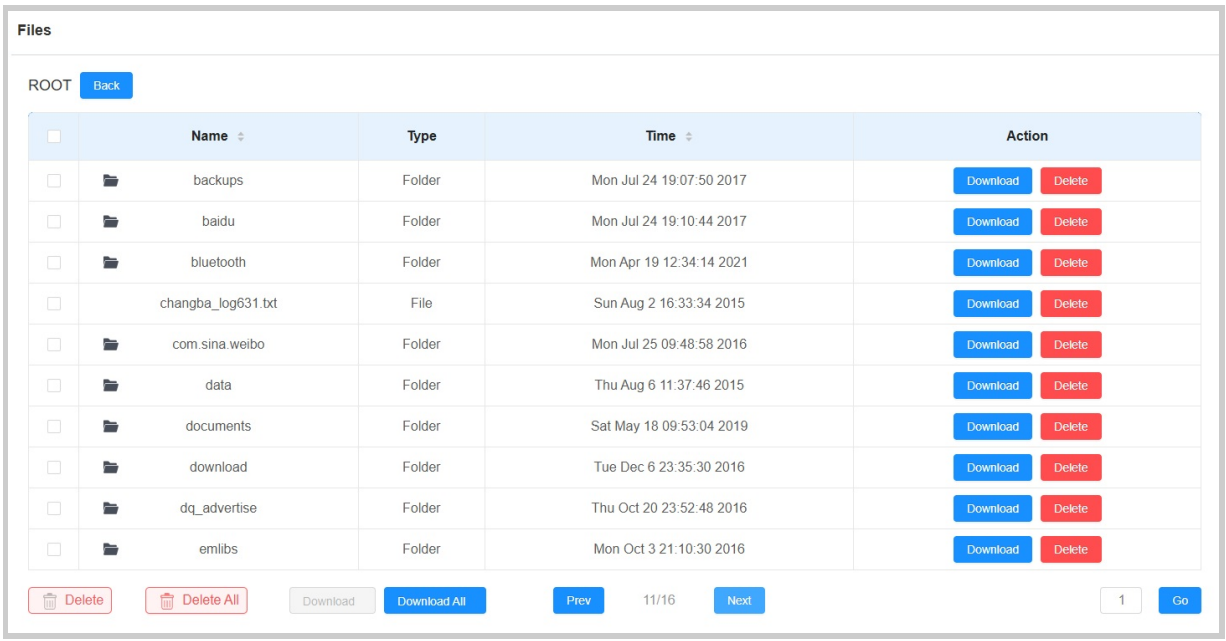


- **UDP**: An unreliable but very efficient transport layer protocol.
- **TCP**: A less efficient but reliable transport layer protocol. It is the default transport protocol.

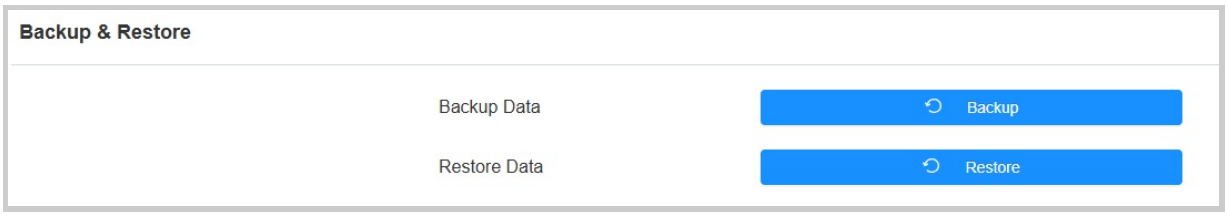
SD Card for Storing Videos

The device can be inserted into an SD card to store motion and call videos.

To check the videos, go to **Device > SD Card** interface. When there is not enough space in the SD card to record the next video, the system automatically deletes the oldest video.



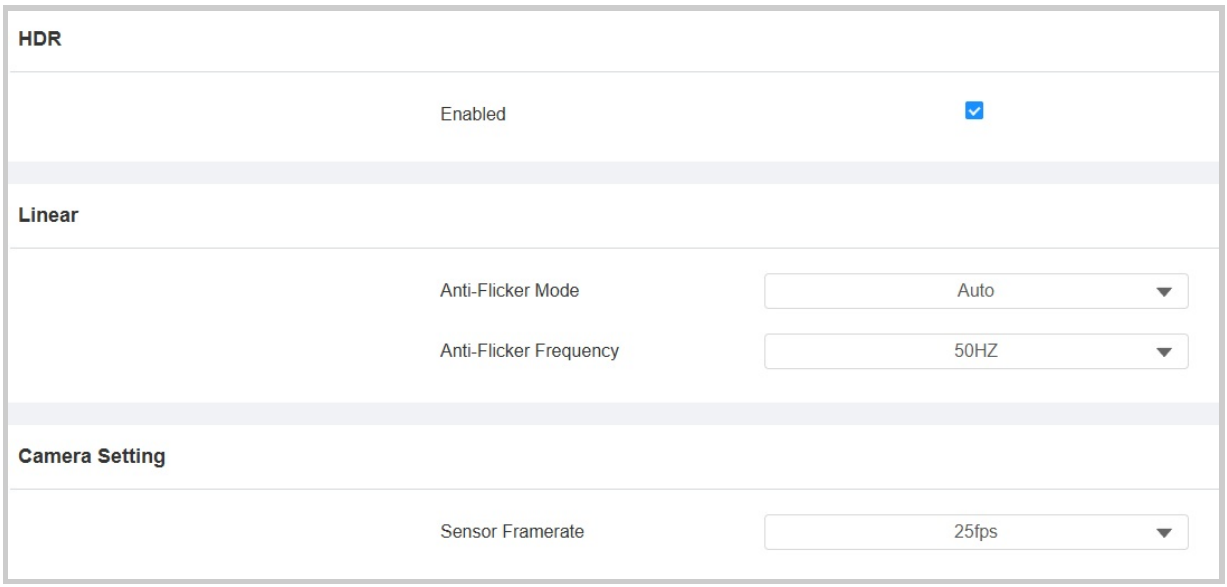
You can backup the door phone's configuration data to the SD card and restore it from the SD card.



Camera Mode

- High Dynamic Range (HDR) is a technology used in photography, videography, and display devices to enhance image quality by capturing a wider range of brightness and color.
- Linear refers to a straightforward representation of brightness in images. Linear images are commonly used in controlled lighting environments, such as indoor scenes, where consistent brightness is present.

You can set the camera mode between HDR and Linear on the **Device > Camera** interface. It is HDR by default.

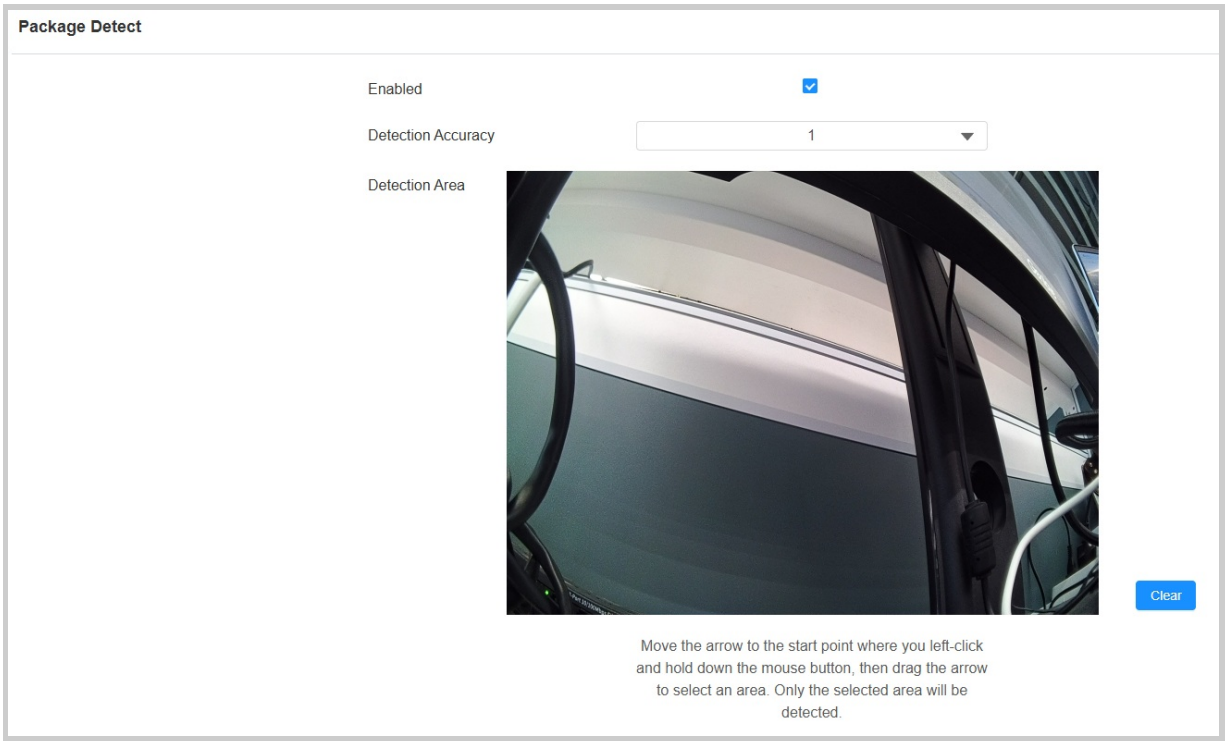


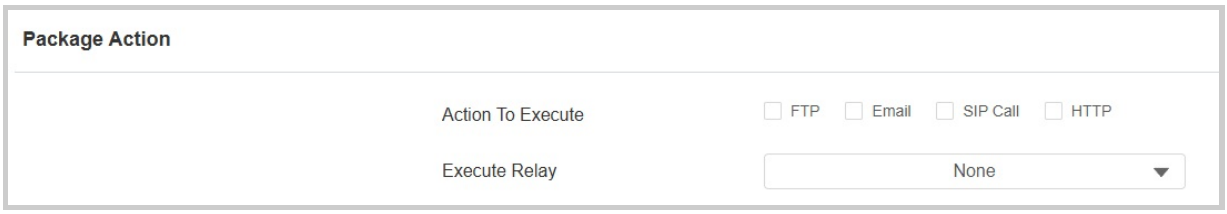
- **Anti-Flicker Mode**: The anti-flicker feature reduces or eliminates flickering in images or videos caused by varying light sources.
  - **Auto**: The device will switch automatically between 50Hz and 60Hz anti-flicker frequency.
  - **Manual**: Select the anti-flicker frequency manually.
  - **Off**: Disable the anti-flicker function.
- **Anti-Flicker Frequency**: Select the anti-flicker frequency between 50Hz and 60Hz.
- **Sensor Framerate**: Adjust the camera frame rate.
  - **30fps**: Better for applications needing higher smoothness.
  - **25fps**: Suitable for standard video recording and playback, especially under a 50Hz power frequency to minimize flicker.

Package Detection

The door phone can send notifications or open doors when its auxiliary camera(at the device's bottom) detects packages.

Set this feature on the **Surveillance > Package** interface. It is disabled by default.





- **Detection Area**: You can click and hold the mouse button to select up to three detection areas. When packages are detected within these three areas, the preset actions will be carried out.
- **Detection Accuracy**: Select the accuracy level between 1 and 2. Higher value indicates a higher accuracy. The default is 1.
- **Action to Execute**: Set the desired actions that occur when package detection 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 and enter the URL.

- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Execute Relay**: Specify the relay to be triggered.

You can set the schedule that determines when the feature is effective on the **Package Detect Time Setting** part.



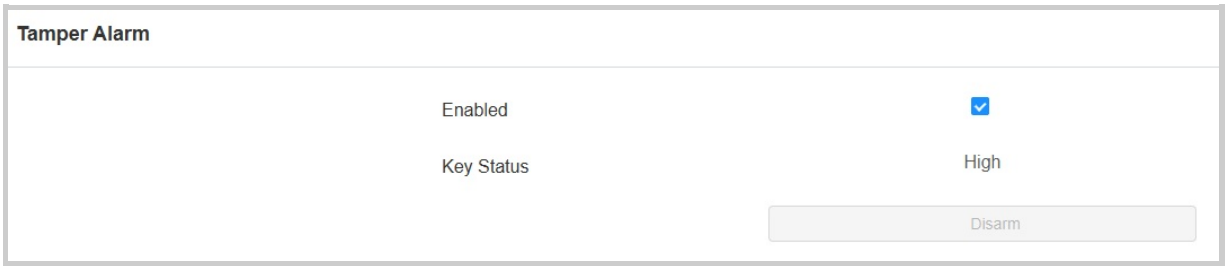
Security

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.

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



- **Disarm**: Click Disarm to clear the arming.

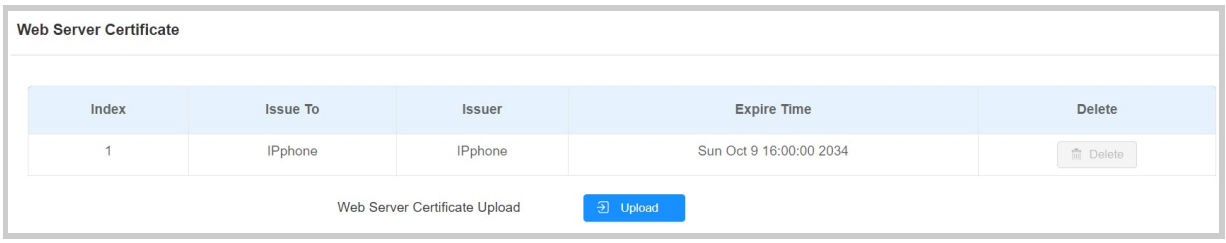
Client Certificate Setting

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

Web Server Certificate

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

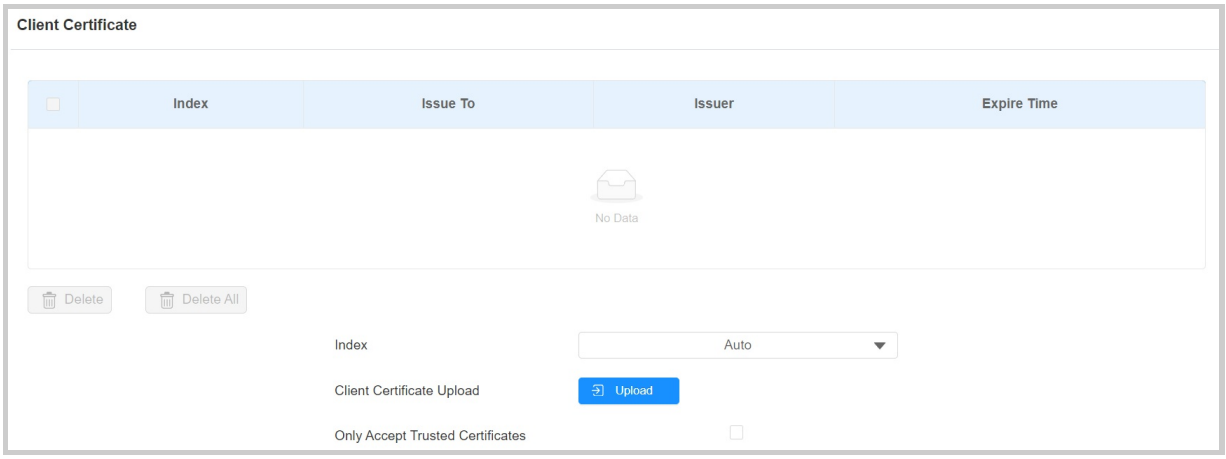
Upload Web Server Certificate on the web **System > Certificate** interface.



Client Certificate

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

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

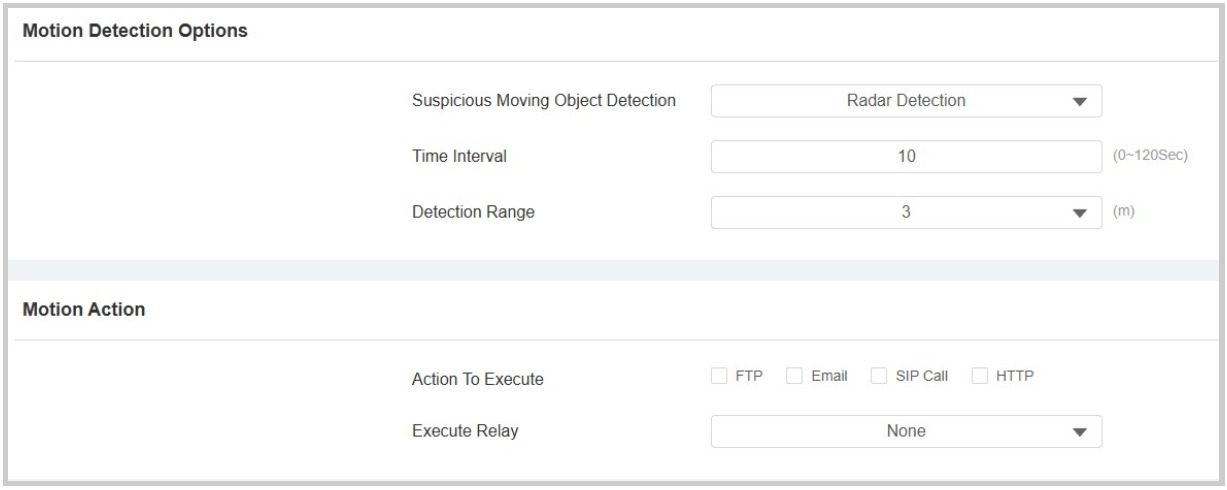


- **Index:**
  - Auto: The uploaded certificate will be displayed in numeric order.
  - 1 to 10: the uploaded certificate will be displayed according to the value selected.
- **Upload:** Click Choose File to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, as long as the authentication succeeds, the doorphone will verify the server certificate based on the client certificate list. If select Disabled, the doorphone will not verify the server certificate no matter whether the certificate is valid or not.

Motion Detection

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

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



- **Suspicious Object Movement Detection:** The feature uses the main camera for detection.
    - **Disabled**: Turn off the feature.
    - **Video Detection**: When the video camera detects moving objects, preset actions will be triggered. Focus on analyzing visual information captured through cameras.
    - **Radar Detection**: When the radar detects moving objects, preset actions will be triggered. It offers longer-range and better detection in poor visibility conditions.
    - **Video + Radar**: Detect motion with the combination of the video camera and radar.
    - **Pedestrian Detection**: When the device detects the upper body of the passers-by, preset actions will be triggered.
    - **Pedestrian + Radar**: Combine the pedestrian and radar detection.
- **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**: Not available for radar detection. The detection sensitivity. The higher the value, the greater the sensitivity. The default detection accuracy value is 3.
- **Detection Range**: Set the distance within which radar detection is triggered. The range includes 1, 2, and 3 meters.
- **Detection Area**: Click and hold the mouse button to select up to three detection areas. When motion is detected within these areas, preset actions will be carried out.
- **Action To Execute**: Set the desired actions that occur when suspicious movement is detected.
    - FTP: Send a screenshot to the preconfigured FTP server.
    - Email: Send a screenshot to the preconfigured Email address.
    - SIP Call: Call the preset number upon 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.
- **Execute Relay**: A relay can be unlocked with motion detection.

Scroll down and you can set the motion detection schedule.



Security Notification

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

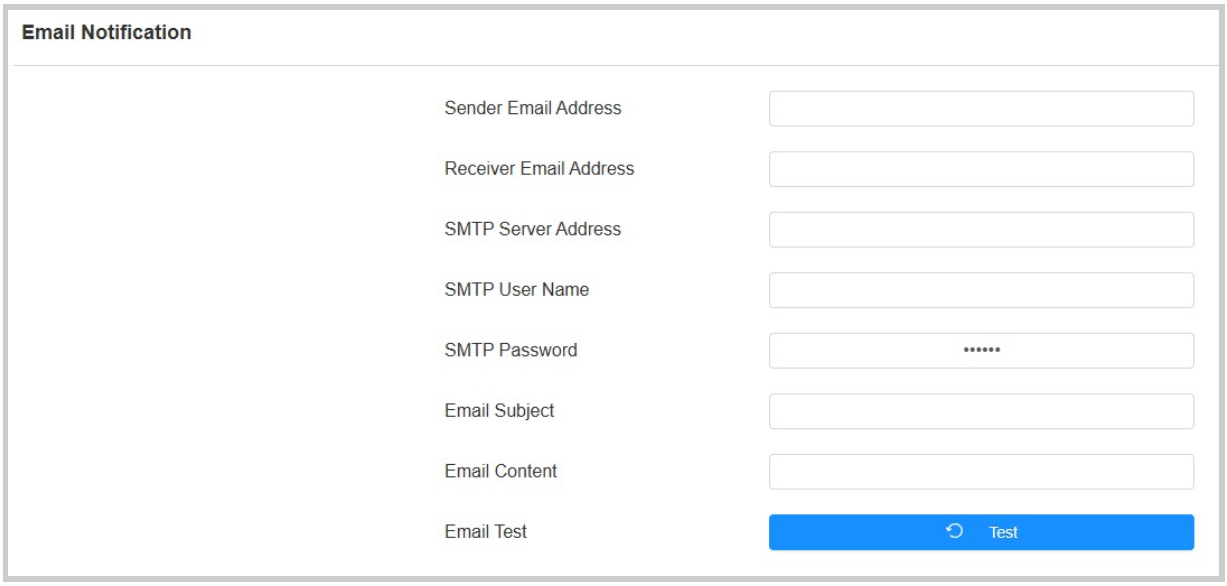
To set up security notifications, go to **Setting > Action** interface.

Email Notification

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

Click here to view how to set this feature up.

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



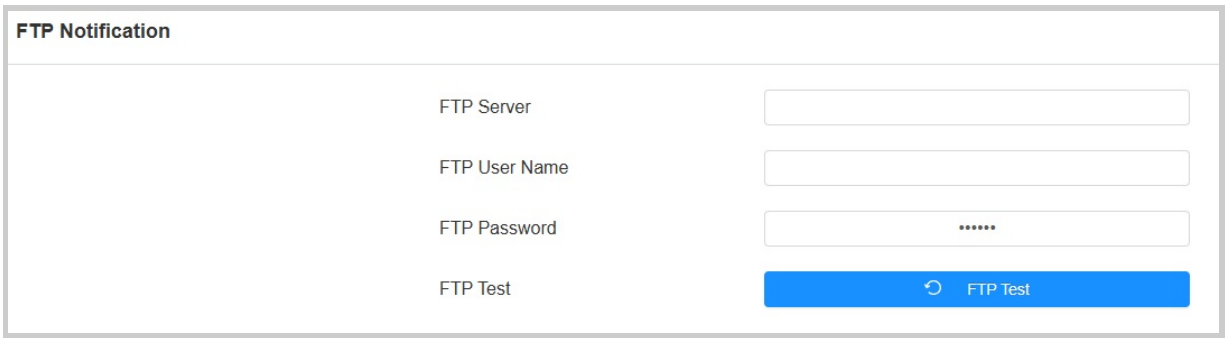
- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP Username**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

FTP Notification

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

Click here to view the configuration steps.

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

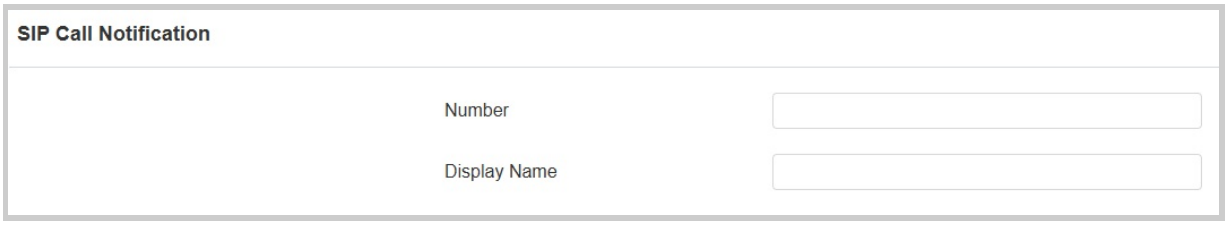


- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP Username**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

SIP Call Notification

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

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



- **Display Name**: The name of the device displayed in the notification.

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	Break-in Alarm	$input1status	Http://server ip/inputtrigger=$input1status **NOTE**: $input1/2status corresponds to inputA/B.

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.



- **Enabled**: When enabled, you can select the schedule within which the action URL can be performed.
- **Type**: Select the request type between GET and POST.

Voice Encryption

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

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



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

User Agent

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

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

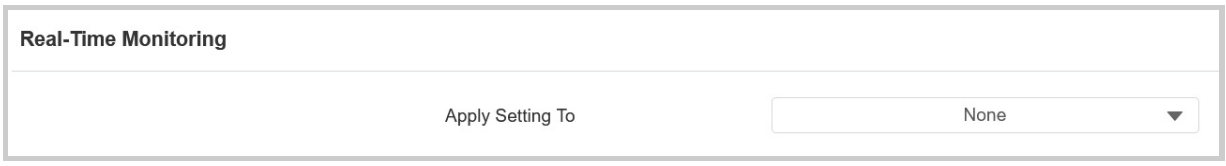


- **User Agent:** Akuvox is by default.

Real-Time Monitoring

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

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



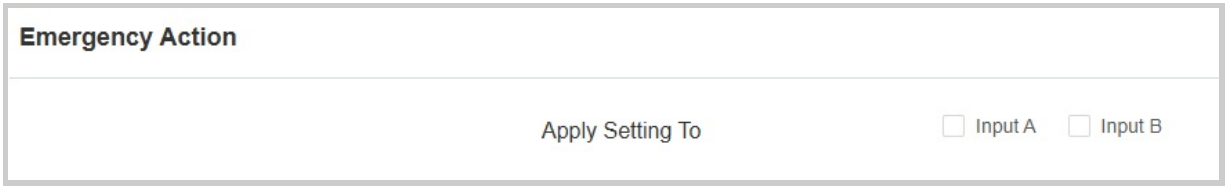
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering input.
  - **Relay**: The door is opened by triggering the relay.

Emergency Action

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

Click here to view the detailed configuration of this feature.

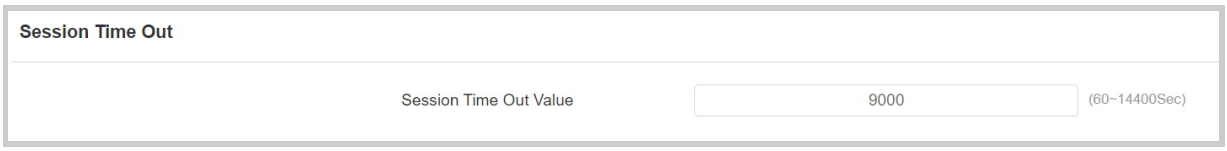
To set it up, go to **System > Security > Emergency Action** interface. Select the Input(s) to be triggered.



Web Interface Automatic Log-out

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

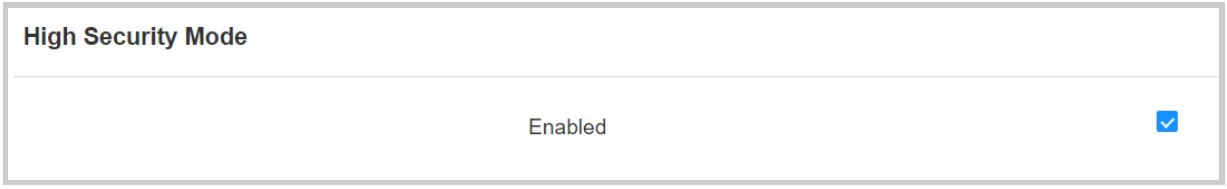
To set it up, go to **System > Security > Session Time Out** interface.



High Security Mode

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

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



Important Notes

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

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

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

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

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

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

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

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

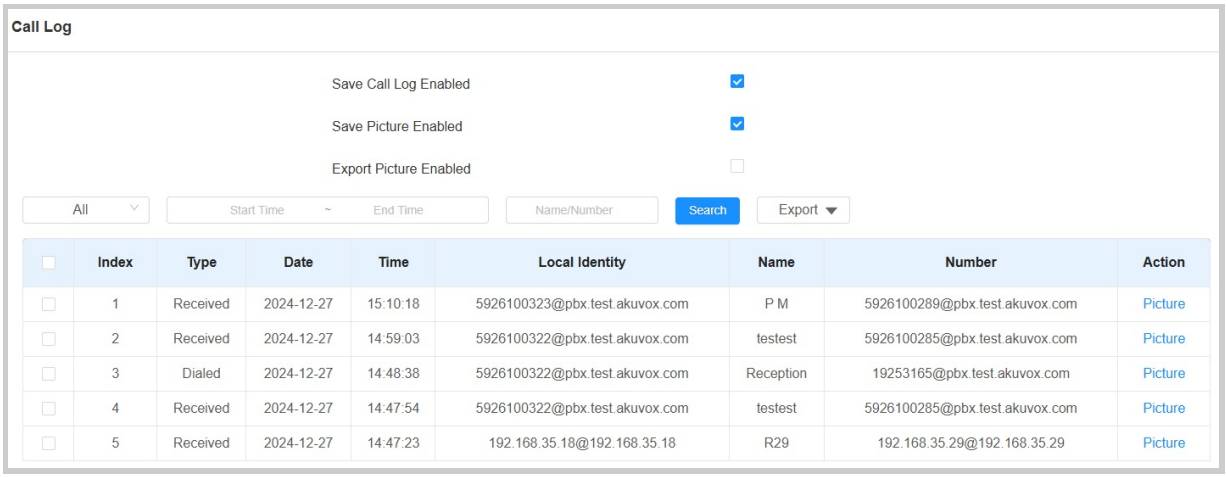
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

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

Check call logs on the web **Status > Call Log** interface. You can export call logs in a CSV file by clicking **Export**. The device supports up to 1,000 call logs.



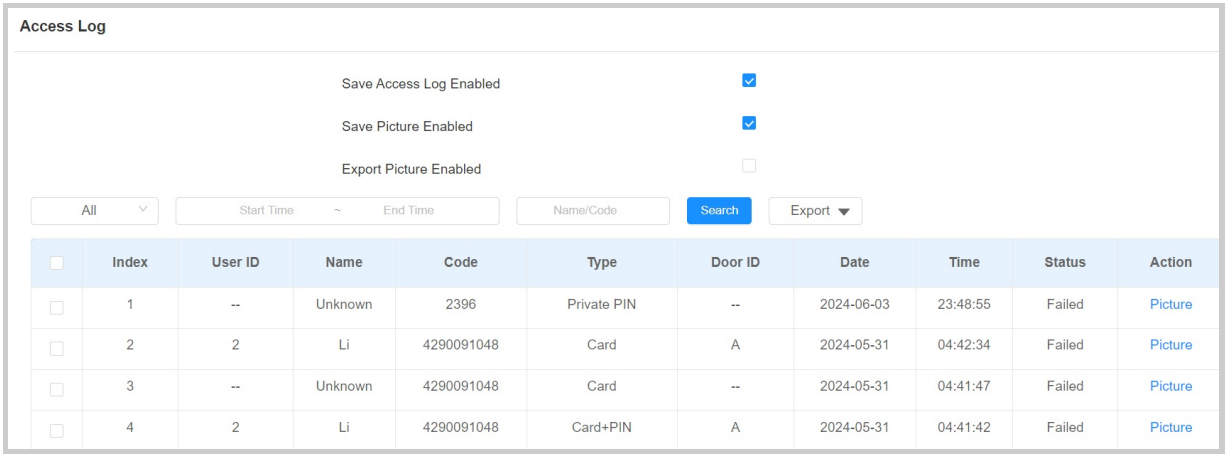
Index	Type	Date	Time	Local Identity	Name	Number	Action
1	Received	2024-12-27	15:10:18	5926100323@pbx.test.akuvox.com	P M	5926100289@pbx.test.akuvox.com	Picture
2	Received	2024-12-27	14:59:03	5926100322@pbx.test.akuvox.com	testest	5926100285@pbx.test.akuvox.com	Picture
3	Dialed	2024-12-27	14:48:38	5926100322@pbx.test.akuvox.com	Reception	19253165@pbx.test.akuvox.com	Picture
4	Received	2024-12-27	14:47:54	5926100322@pbx.test.akuvox.com	testest	5926100285@pbx.test.akuvox.com	Picture
5	Received	2024-12-27	14:47:23	192.168.35.18@192.168.35.18	R29	192.168.35.29@192.168.35.29	Picture

- **Save Picture Enabled**: When enabled, the device will capture pictures of calls, and you can click Picture in the Action column to view the screenshot.
- **Export Picture Enabled**: Set whether to export the captured images when exporting the call logs.
- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.
- **Picture**: Click to view the snapshot during a call.

Door Logs

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

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



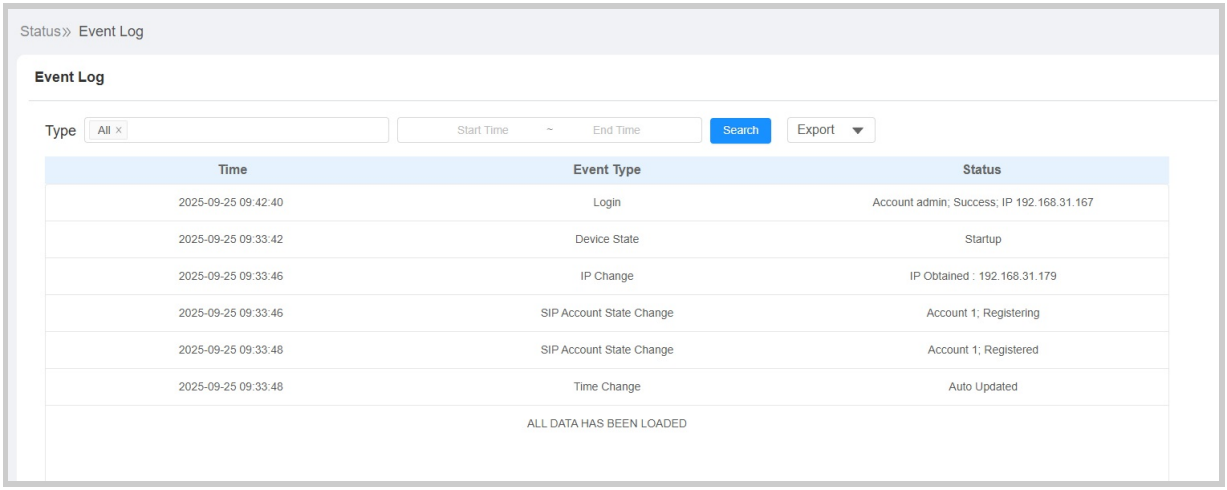
Index	User ID	Name	Code	Type	Door ID	Date	Time	Status	Action
1	--	Unknown	2396	Private PIN	--	2024-06-03	23:48:55	Failed	Picture
2	2	Li	4290091048	Card	A	2024-05-31	04:42:34	Failed	Picture
3	--	Unknown	4290091048	Card	--	2024-05-31	04:41:47	Failed	Picture
4	2	Li	4290091048	Card+PIN	A	2024-05-31	04:41:42	Failed	Picture

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

Event Logs

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

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

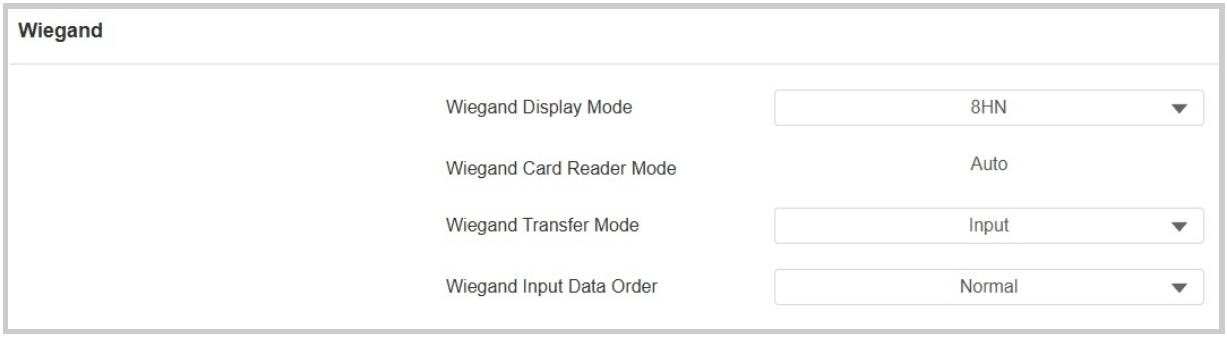


Integration with Third Party Device

Integration via Wiegand

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

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



- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: It is automatically configured when **Input** is the Wiegand Transfer Mode. If Output is the Wiegand Transfer Mode, the transmission format should be identical between the door phone and the third-party device.
- **Wiegand Transfer Mode**:
    - **Input**: The device serves as a receiver.
    - **Output**: The device serves as a sender and can directly output the data, such as card code.
    - **Convert To Card No. Output**: The device serves as a sender and cannot directly output data, such as the face data.
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
  For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If **Reversed** is selected, the card data is 0x55 0x44 0x33.

- **Wiegand Output Basic Data Order**: Set the sequence of the card data before going through Wiegand conversion and outputting the card code.
  For example, if the card data is 0x11 0x22 0x33 0x44 and the **Reversed** option is selected, the data will be 0x44 0x33 0x22 0x11.
- **Wiegand Output CRC Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.

Note

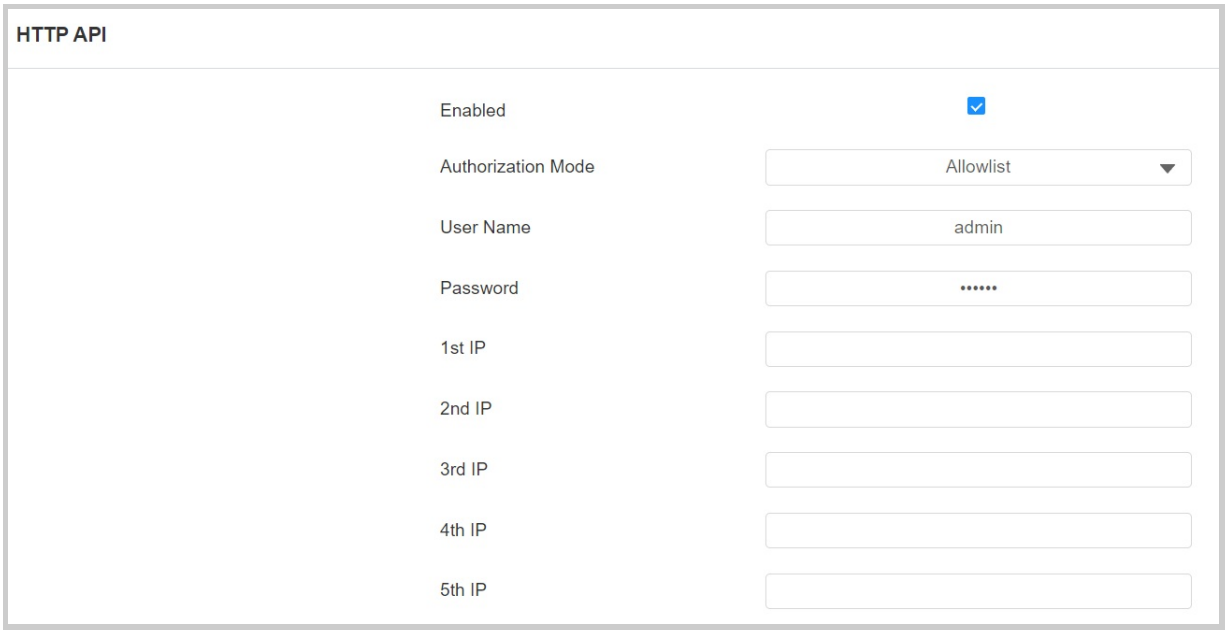
Click **here** to view more information on Wiegand settings including:

- 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 encode method to encode the username and password.
- **User Name**: Enter the user name for authentication. The default is admin.
- **Password**: Enter the password for authentication. The default is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

Please refer to the following description for the authentication mode:

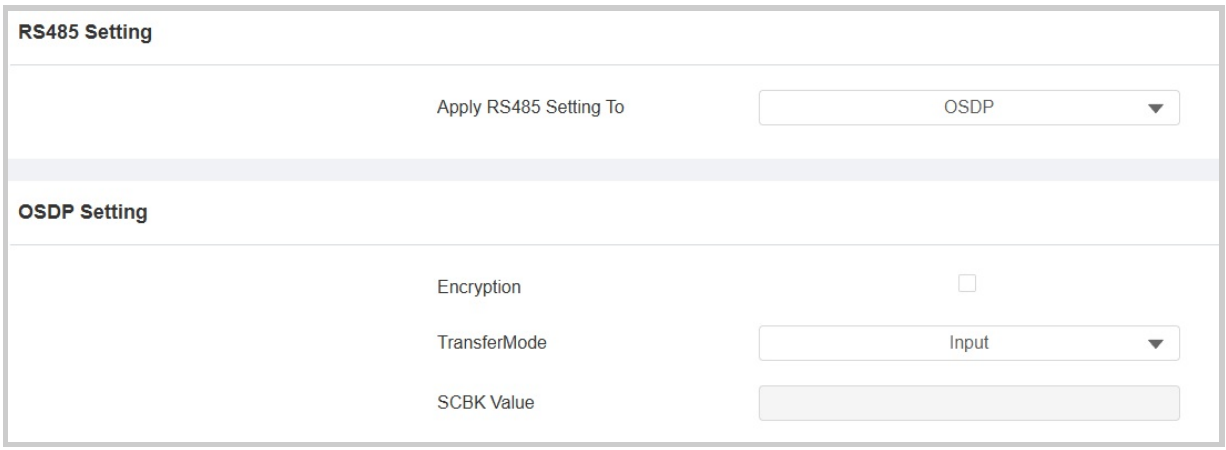
NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication.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

Integration via RS485

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

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

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

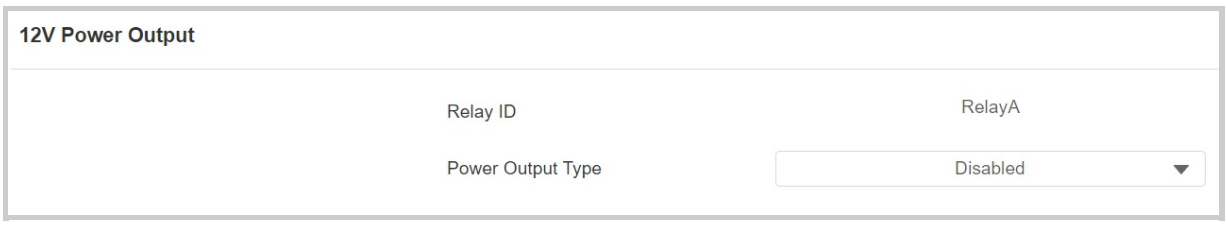


- **Apply RS485 Setting To**:
  - **Disabled**: The RS485 function is disabled.
  - **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Security Relay**: The device is connected to Akuvox Security Relay, SR01.
- **Encryption**: Check this option when the protocol is encrypted.
- **Transfer Mode**: Select the RS485 working mode, Output, or Input.
- **SCBK Value**: Secure Communication Key Value.
  - When it is filled, OSDP will use this value for encryption, employing a customized protocol for communication.
  - When it is left empty, OSDP will use the default encrypted protocol for communication.

Power Output Control

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

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



- **Power Output Type**:
  - **Always**: Provide continuous power to the third-party device.

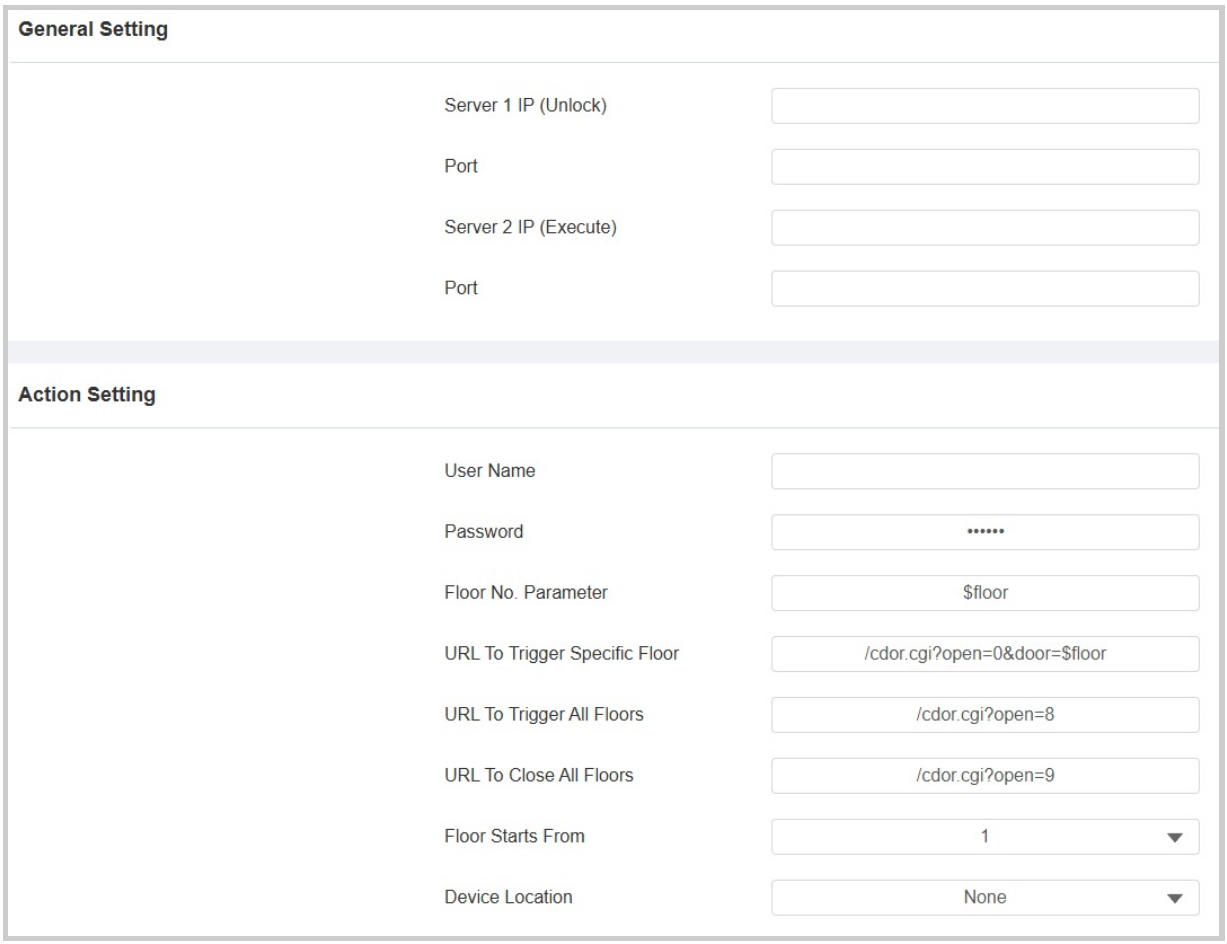
- **Triggered by Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.

Lift Control

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

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

To set it up, go to the **Device > Lift Control** interface. Select **Akuvox** for integration with the Akuvox EC33 lift controller.



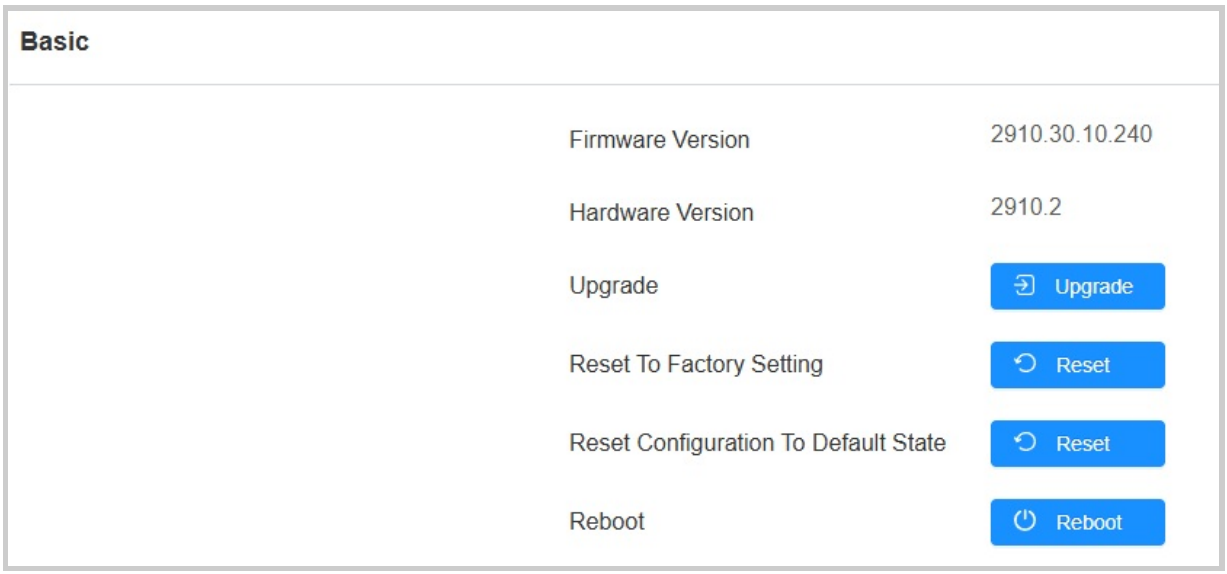
- **Server 1 IP(Unlock)**: The IP address of the lift controller that unlocks the elevator button(s). It supports up to 10 server addresses separated by ";".

- **Server 2 IP(Execute)**: The IP address of the lift controller that sends the lift control commands.
- **Port**: The server port of the lift controller server.
- **User Name**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **Device Location**: Select the floor where the device is installed.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

To upgrade the device, go to **System > Upgrade** interface.



Note

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

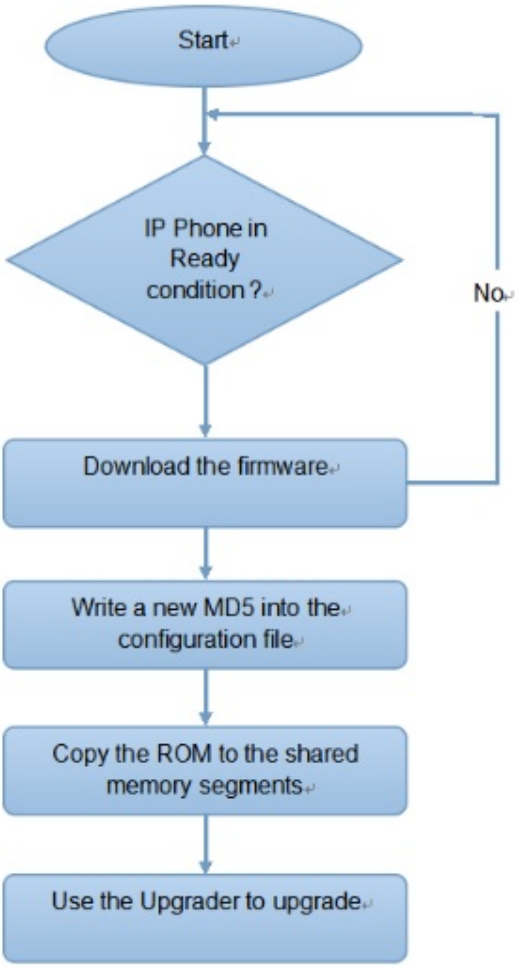
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

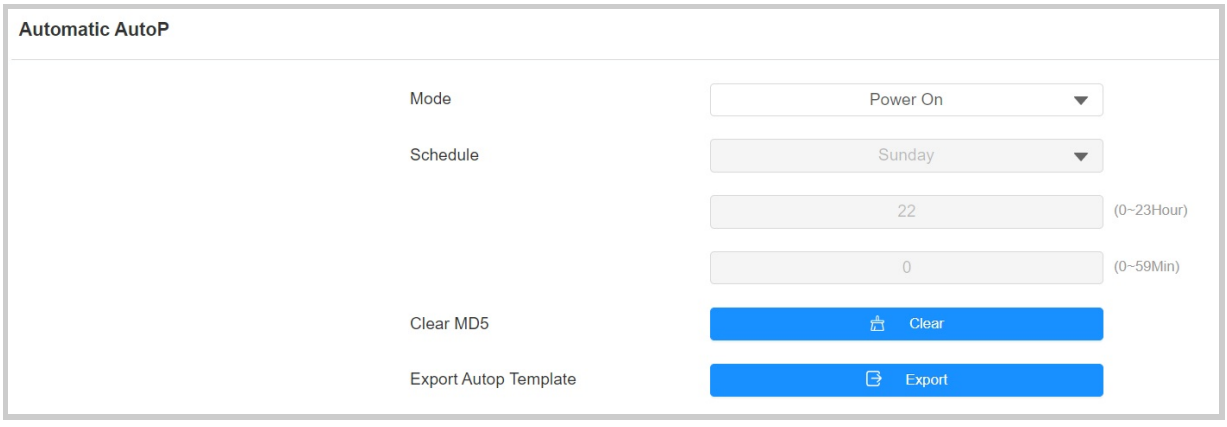
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

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

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



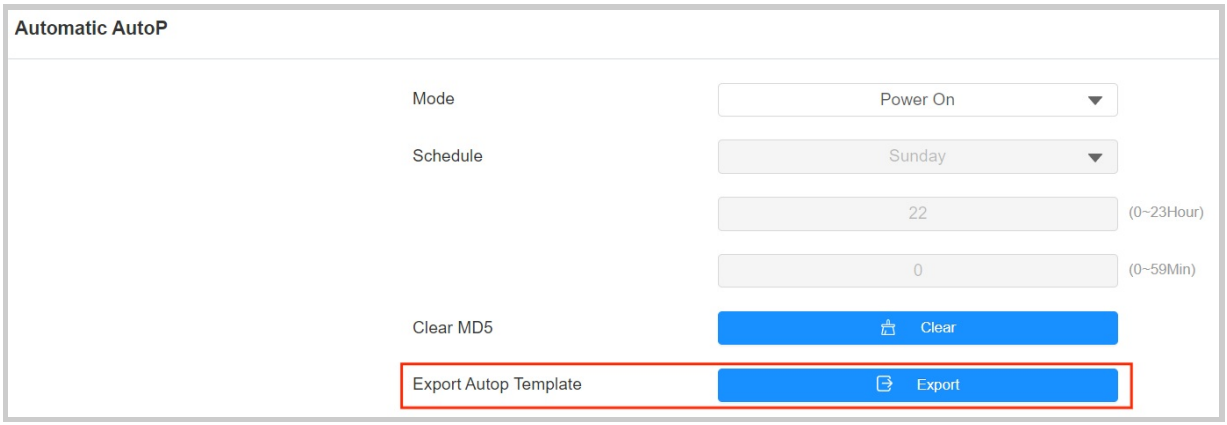
- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.

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

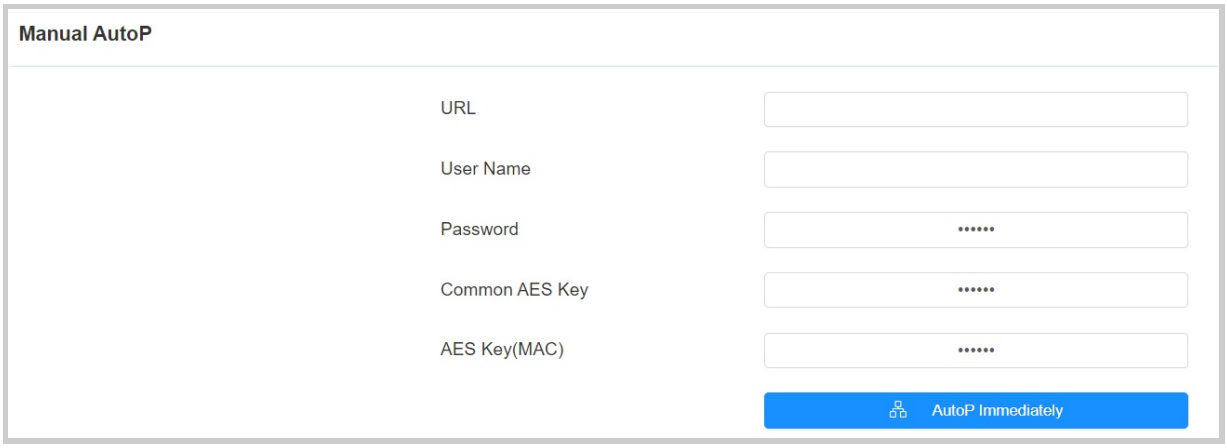
Static Provisioning

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

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



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



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

Note

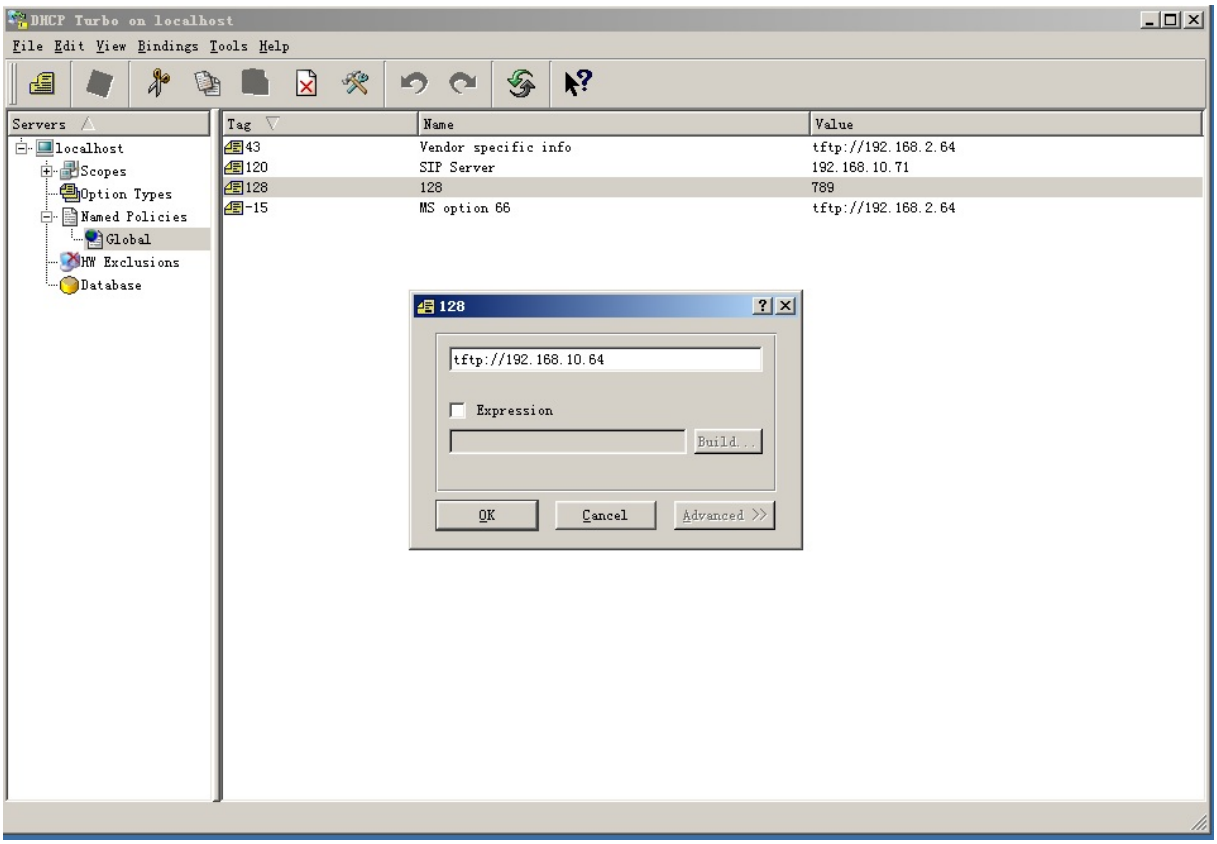
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning

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

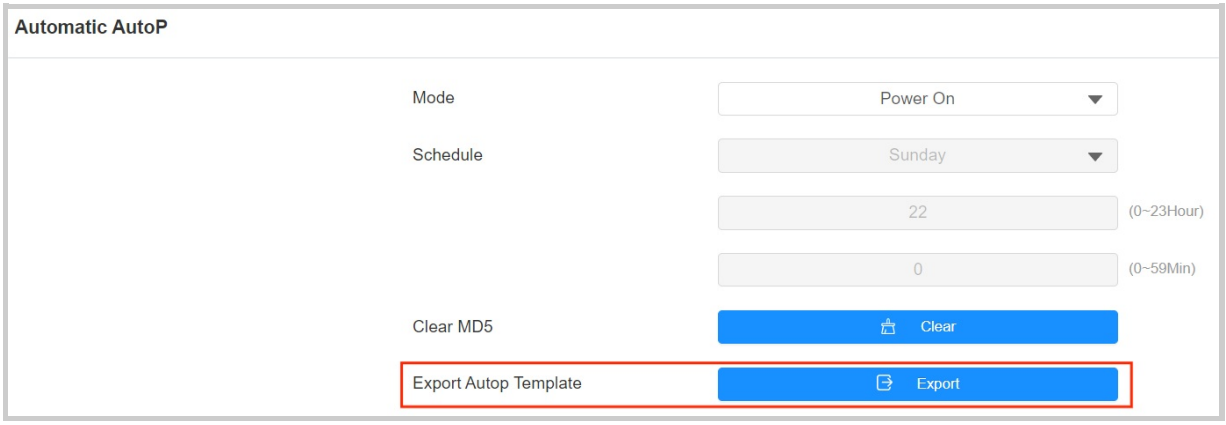


Note

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

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

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



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



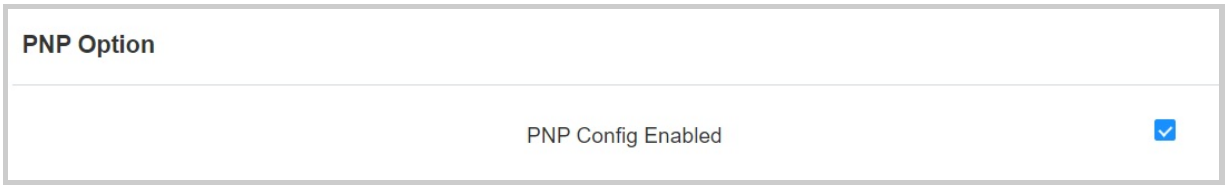
- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL.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

PNP Configuration

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

Click here to watch the configuration video.

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

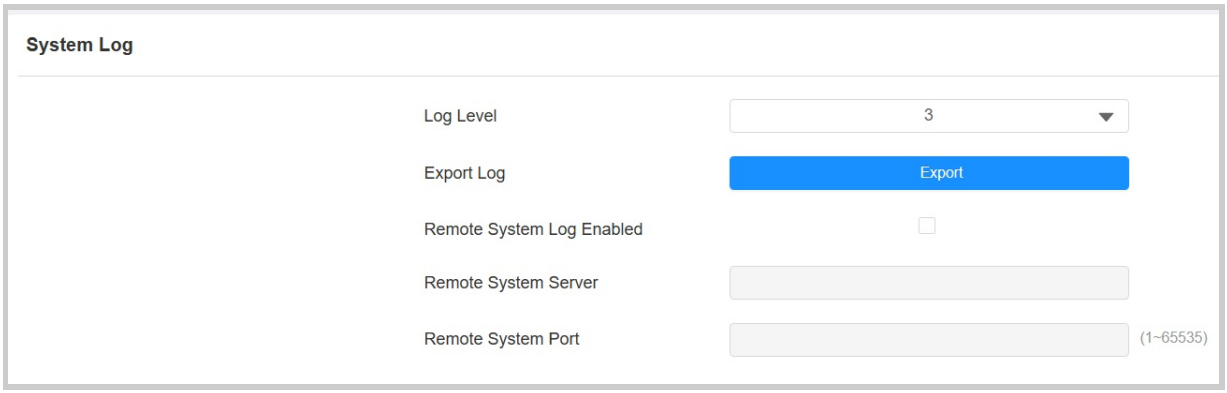


Debug

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.

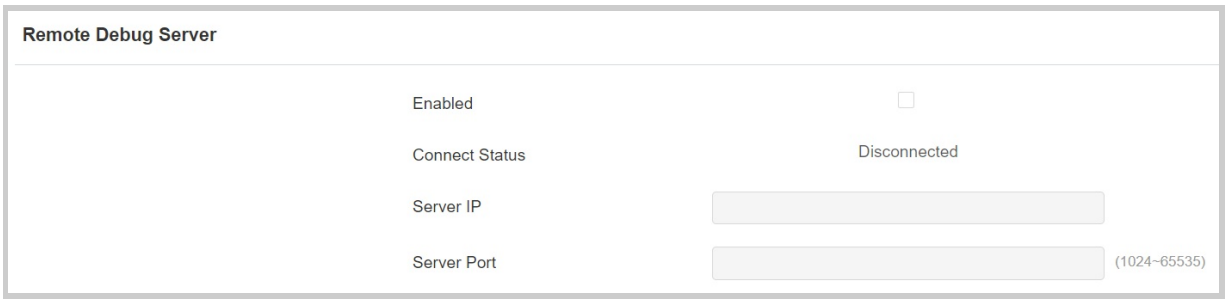


- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export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

Remote Debug Server

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

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

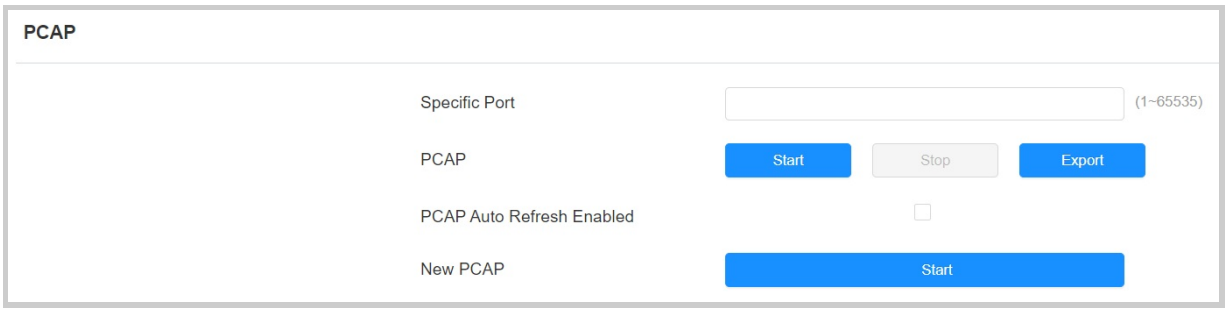


- **Connect Status**: Display the connection status between the device and the server.
- **Server IP**: Enter the IP address of the server.
- **Server Port**: Enter the port of the server.

PCAP for Debugging

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

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



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

Ping

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

To set it up, go to **System > Maintenance > Ping** interface.

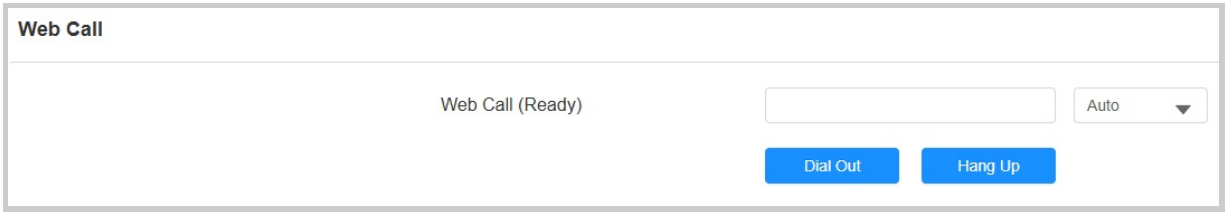


- **Cloud Server**: Select the server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Web Call

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

Make a web call on **System > Maintenance > Web Call** interface.



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

Backup

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

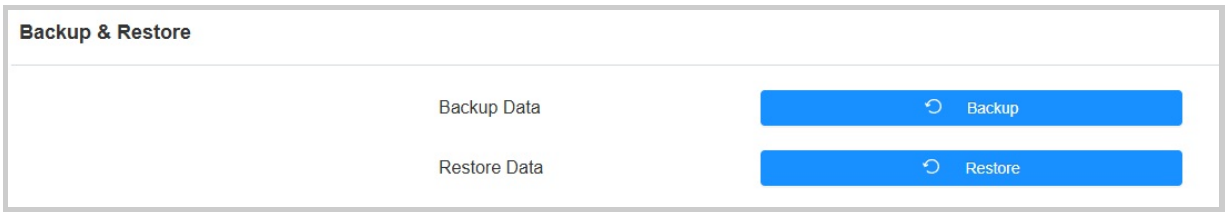
Export the file on the **System > Maintenance** interface. The imported file should be in the .tgz/.conf/.cfg format.



Backup via SD Card

The device supports inserting an SD card for backing up and restoring data.

To use this feature, go to **Device > SD Card** interface. The tested SD card capacity is 64GB.



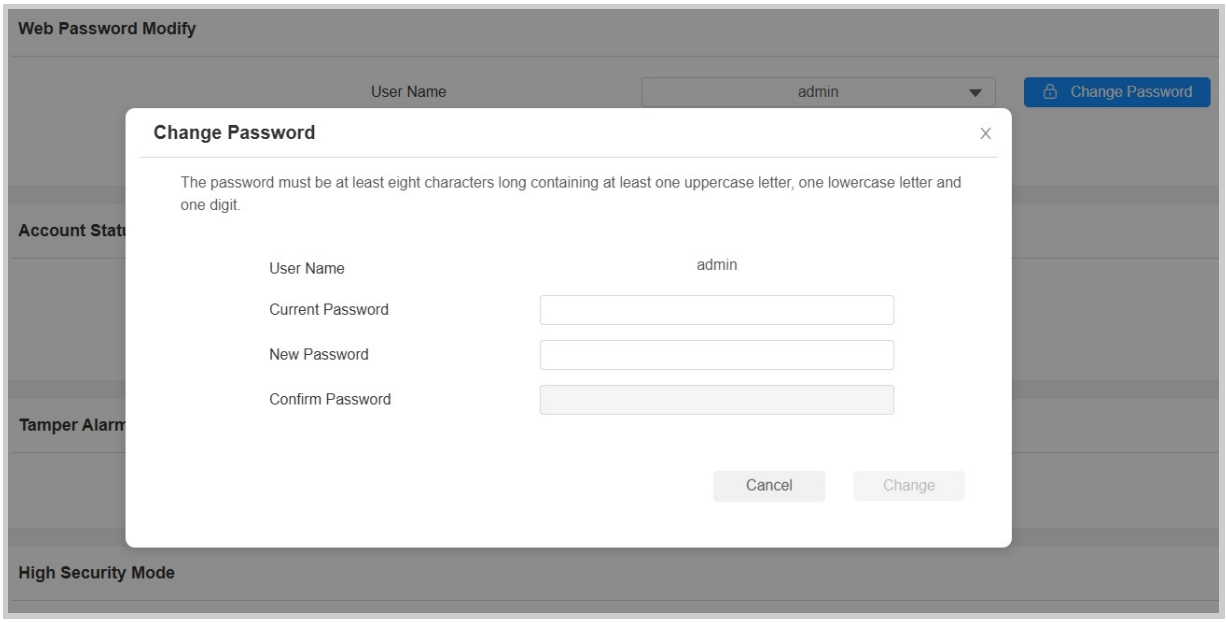
Password Modification

You can modify the device web password for both the administrator account and the user account.

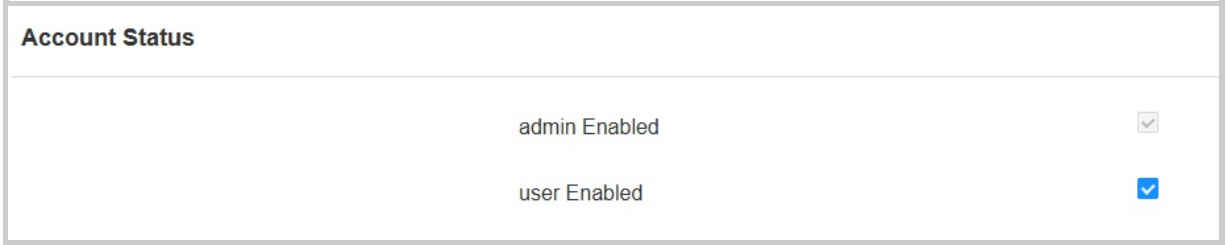
To set it up, go to **System > Security > Web Password Modify** interface.



Click **Change Password** to modify the password. The new password cannot contain “&,=',,%”.



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

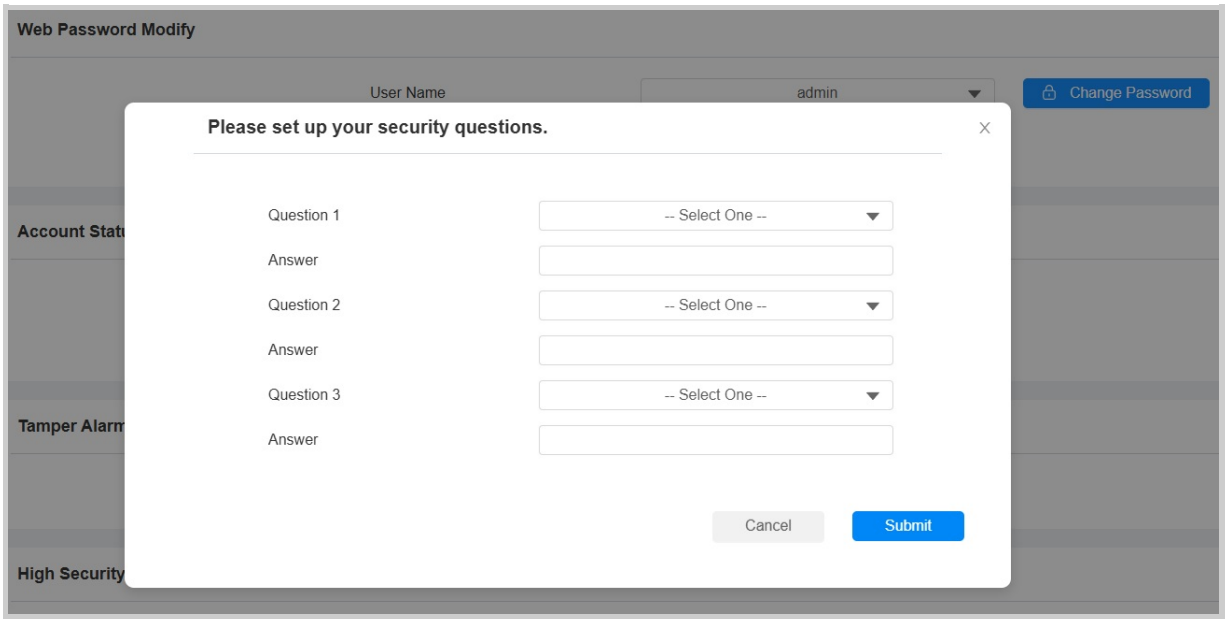
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

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



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

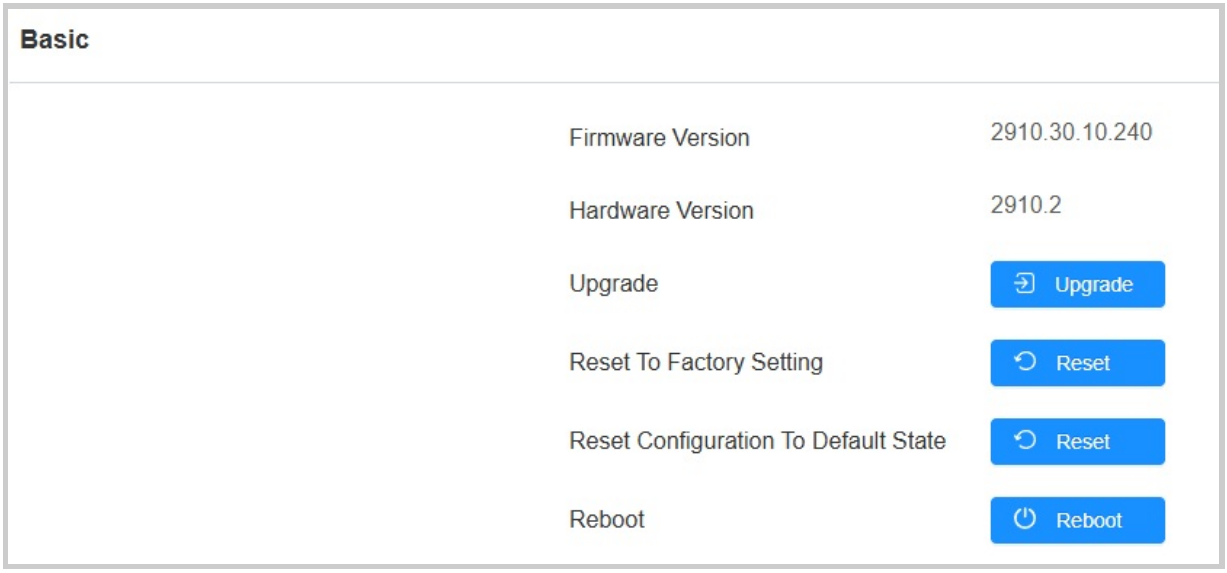


System Reboot&Reset

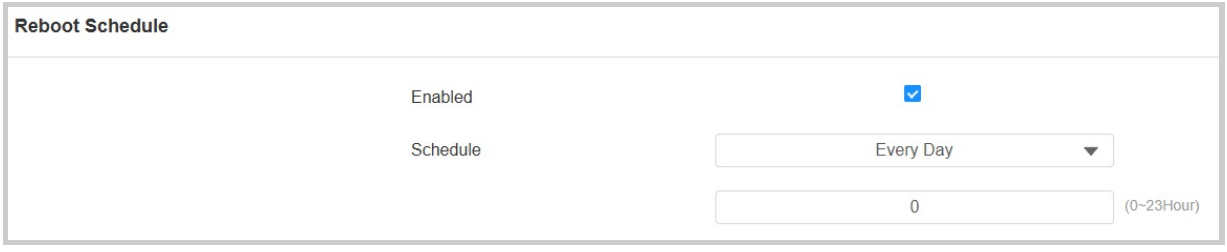
Reboot

If you want to restart the device system, you can operate it on the device web. Moreover, you can set up a schedule for the device to be restarted.

Navigate to the **System > Upgrade** interface.



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

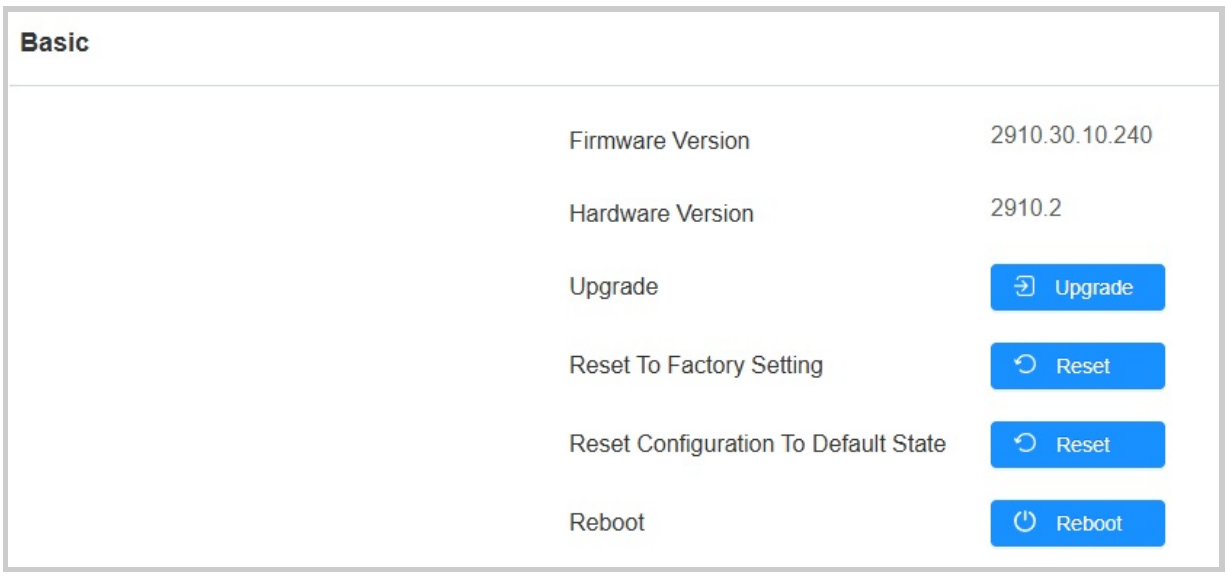


Reset

The device provides two reset options:

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

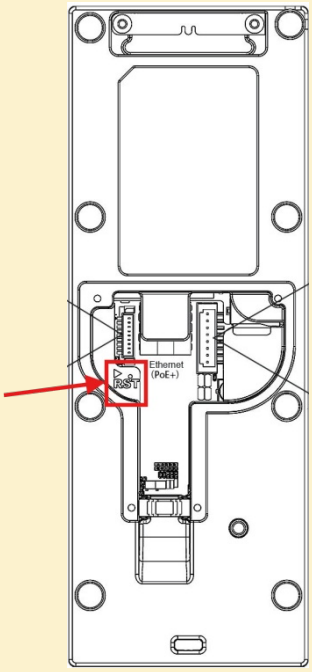
Reset the device on the web **System > Upgrade** interface.



Tip

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

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



Powered by Document360