

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



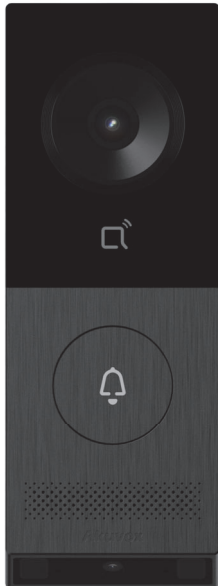
AKUVOX X910S

Door Phone

Administrator Guide

Thank you for choosing the Akuvox X910S door phone. This manual is intended for administrators who need to configure the door phone properly. This manual applies to firmware version 2910.30.10.240 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 x910S 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.

Model Specification

Model	X910S
Operation System	Linux
Cameras	2
Fill Light	✓
Motion Detection	✓, Radar Detection
IC Card Reader	✓, 13.56MHz
ID Card Reader	X
NFC	✓
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)

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 | X910S

Open A Smart World



Home Screen



Status



Account



Network



Intercom



Surveillance



Access Control



Directory



Device



Setting



System



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.

IP Announcement

Loop Times

1

- **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

IP Scanner						
Online Device : 12						
Model:	All		Search	Refresh	Set Static IP	Export
Index	IP Address	MAC Address	Model	Room Number	Firmware Version	
1	192.168.35.13	A61018240912	X910	1.1.1.1.1	2910.30.110.257	
2	192.168.35.29	0C110525FA81	R29	1.1.1.1.1	29.30.10.227	
3	192.168.35.39	A61006241029	E16C V2.0	1.1.1.1.1	216.30.10.116	
4	192.168.35.68	0C11051D38C5	R20SV823	1.1.1.1.1	320.30.10.150	

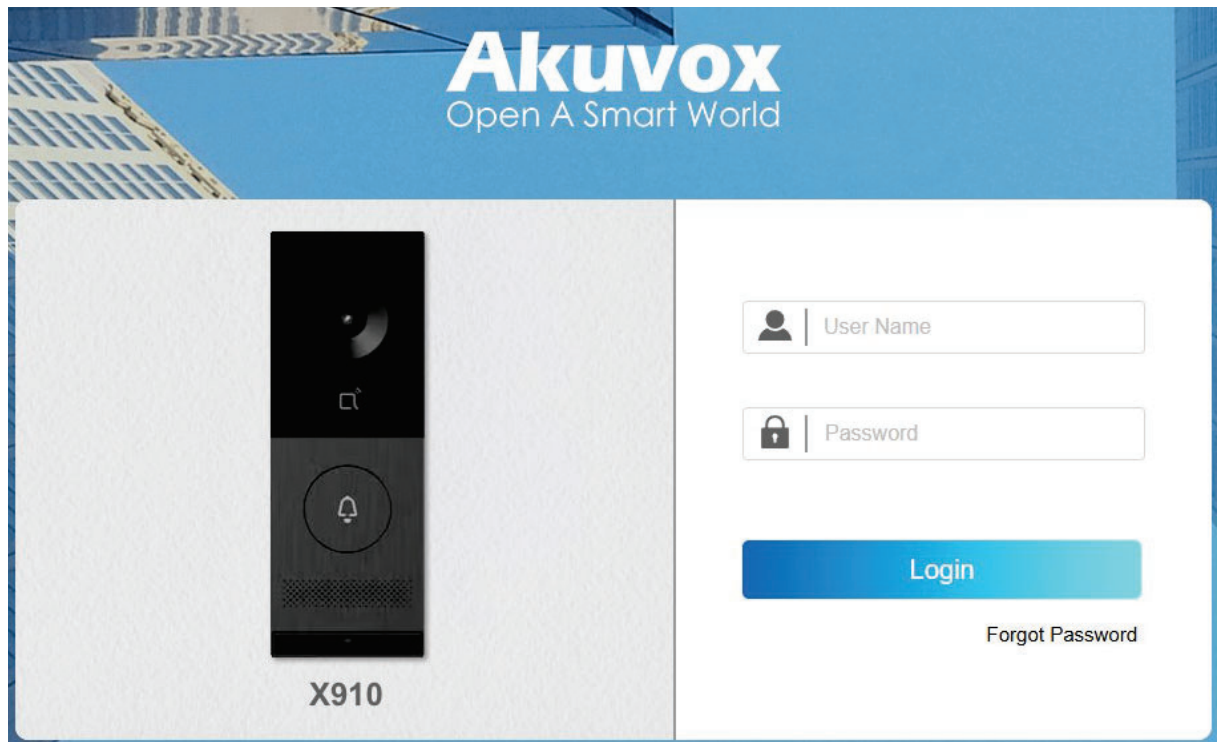
Note

- 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.



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.



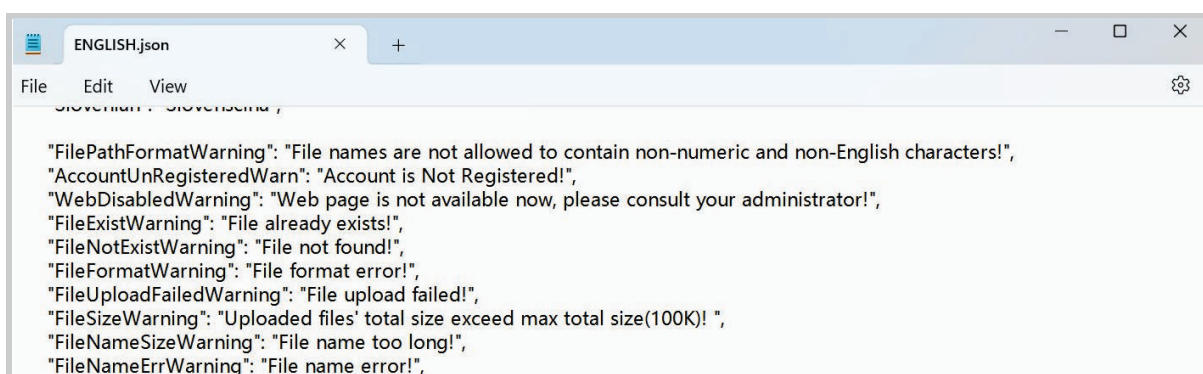
Custom Language

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.

Custom Language

Type	File Status	File Name	Import	Export	Reset
Web	Default	AUTO.json	<button>Import</button>	<button>Export</button>	<button>Reset</button>

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.

Time

Automatic Date&Time	<input checked="" type="checkbox"/>
Time Zone	GMT+8:00 Chongqing ▼
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>=3600s)
System Time	16:54:52

- **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 NPT 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.

LED Light

Mode	<div>Auto ▼</div>		
Photoresistor Setting	<div>1500</div>	-	<div>1600</div> (0~1800)
Current Photoresistor	<div></div>		<div>Read</div>
IR LED Brightness	<div>7 ▼</div>		

- **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.

LED Of Swiping Card Area

Enabled



Start Time - End Time

18

-

06

(0~23 Hour)

- **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.

Status Light

Device Status	Color	Display Mode
Normal	Blue	Always ON
OffLine	Red	Breathing Light
Calling	Blue	Breathing Light
Talking	Purple	Always ON
Receiving	Blue	Breathing Light
Access Granted	Green	Always ON
Access Denied	Red	500/500
Emergency Alarm	Red&Blue	500/500

- **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.

White Light

Enabled



Light Intensity

50

(0~100)

- **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.

Volume Control

Mic Volume	<input type="text" value="50"/>	(1~100)
Speaker Volume	<input type="text" value="50"/>	(1~100)
Tamper Alarm Volume	<input type="text" value="50"/>	(1~100)

- **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.

Tone Upload

ID	Tone	Import	Reset	Play	Enabled
1	Relay A - Access Granted	import	Delete	Play	<input checked="" type="checkbox"/>
2	Relay B - Access Granted	import	Delete	Play	<input checked="" type="checkbox"/>
3	Input A - Access Granted	import	Delete	Play	<input checked="" type="checkbox"/>
4	Input B - Access Granted	import	Delete	Play	<input checked="" type="checkbox"/>
5	Access Denied	import	Delete	Play	<input checked="" type="checkbox"/>
6	Tamper Alarm	import	Delete	Play	<input checked="" type="checkbox"/>
7	Ringback - Auto Response	import	Delete	Play	<input checked="" type="checkbox"/>

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

Note

File Format: .wav; Size: < 200Kb; Sample Rate: 16k; Bits: 16.

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 Tone Setting

Ringback Source

Remote, Local As Backup ▼

Auto Response



- **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.

Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.35.13
Subnet Mask	255.255.255.0
Gateway	192.168.35.1
Preferred DNS Server	218.85.157.99
Alternate DNS Server	218.85.152.99

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.

LAN Port

Network Mode	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text" value="192.168.1.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Alternate DNS Server	<input type="text"/>

- **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.

Connect Setting

Server Mode	None
Discovery Mode	<input checked="" type="checkbox"/>
Device Address	<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="Door Phone"/>

- **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** is the default factory setting, indicating the device is not in any server type.
- **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.

Web Server

Protocol	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> HTTPS
HTTP Port	<input type="text" value="80"/>	(80,1024~65535)
HTTPS Port	<input type="text" value="443"/>	(443,1024~65535)

- **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.

Local RTP

Starting RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

- **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.

SNMP

Enabled	<input type="checkbox"/>
Port	<input type="text" value=""/> (1~65535)
IP Address	<input type="text" value=""/>

- **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.

NAT

UDP Keep Alive Messages	<input checked="" type="checkbox"/>
UDP Alive Messages Interval	<input type="text" value="30"/> (5~60Sec)
RPort	<input type="checkbox"/>

- **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.

TR069

Enabled

☐

Version

1.0

ACS URL

User Name

Password

Periodic Inform

☐

Periodic Interval

1800

(3~24x3600s)

CPE URL

User Name

Password

- **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.

Direct IP

Enabled	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1024~65535)

- **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**.

SIP Account

Status	Disabled
Account	Account1 ▼
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password" value="*****"/>

- **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.

Preferred SIP Server

Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535Sec)

Alternative SIP Server

Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535Sec)

- **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.

Outbound Proxy Server

Outbound Enabled	<input type="checkbox"/>	
Preferred Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)
Alternative Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)

- **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.

Transport Type

Type

UDP ▼

- **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.

Call

Max Local SIP Port	<input type="text" value="24194"/>	(1024~65535)
Min Local SIP Port	<input type="text" value="24184"/>	(1024~65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input checked="" type="checkbox"/>	
Video Transport Type	<input type="text" value="Send Only"/>	▼

- **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.

Call

Max Local SIP Port	<input type="text" value="24194"/>	(1024~65535)
Min Local SIP Port	<input type="text" value="24184"/>	(1024~65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input checked="" type="checkbox"/>	
Video Transport Type	<input type="text" value="Send Only"/>	▼

- **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 **Account > Advanced > Call** interface.

Call

Max Local SIP Port	<input type="text" value="24194"/>	(1024~65535)
Min Local SIP Port	<input type="text" value="24184"/>	(1024~65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input checked="" type="checkbox"/>	
Video Transport Type	<input type="text" value="Send Only"/>	▼

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

Auto Answer

Auto Answer Delay	<input type="text" value="0"/>	(0~5Sec)
Mode	<input type="text" value="Video"/>	▼

- **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.

Push Button

Enabled	<input checked="" type="checkbox"/>
Call Type	Sequence Call ▼
Call Time Out (Sec)	20 ▼
Sequence Call Number (Cloud)	If the local group is not blank, then only the local numbers will be called.
Sequence Call Number 1	<input type="text"/>
Sequence Call Number 2	<input type="text"/>
Sequence Call Number 3	<input type="text"/>
Sequence Call Number 4	<input type="text"/>
Sequence Call Number 5	<input type="text"/>
Sequence Call Number 6	<input type="text"/>
Sequence Call Number 7	<input type="text"/>
Sequence Call Number 8	<input type="text"/>
Sequence Call Number 9	<input type="text"/>
Sequence Call Number 10	<input type="text"/>

- **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.

Sequence Call

When Refused	Do Not Call Next ▼
--------------	--------------------

- **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.

Push Button

Enabled	<input checked="" type="checkbox"/>																
Call Type	Group Call ▼																
Group Call Number	<p>If the local group is not blank, then only the local numbers will be called.</p> <table> <tr> <td>19253165</td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	19253165															
19253165																	

- **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.

Group Call

When Refused

End This Call Only ▼

- **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.

DND

Account Account1 ▼

Enabled ☐

- **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.

Push Button Action

Push To Hang Up ☒

Action To Execute ☐ FTP ☐ Email ☐ HTTP

- **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.

Multicast Setting

Paging Barge

Disabled

Paging Priority

☒

Priority List

IP Address	Listening Address	Label	Priority
IP Address 1			1
IP Address 2			2
IP Address 3			3
IP Address 4			4
IP Address 5			5
IP Address 6			6
IP Address 7			7
IP Address 8			8
IP Address 9			9
IP Address 10			10

- **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

Max Call Time

5

(2~30Min)

- **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.

Max Dial Time

Dial In Time

60

(30~120Sec)

Dial Out Time

60

(30~120Sec)

- **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.

Hang Up After Opening Door

Enabled



Type

Only DTMF



Time Out (Sec)

5

(0~15Sec)

- **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.

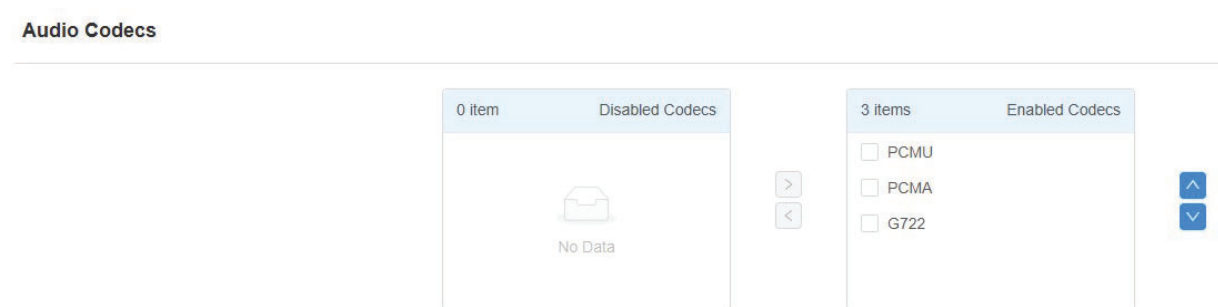
Audio & Video Codec Configuration

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.

Video Codec

Name	<input checked="" type="checkbox"/> H.264
Resolution	4CIF ▼
Bitrate	320 kbps ▼
Payload	104 ▼

- **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.

IP Video Parameters

Video Resolution	720P ▼
Video Bitrate	2048 kbps ▼
Payload	104 ▼

- **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.

Relay

Relay ID	RelayA ▼	RelayB ▼
Mode	Monostable ▼	Monostable ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼
DTMF Mode	1 Digit DTMF ▼	
1 Digit DTMF	# ▼	0 ▼
2~4 Digits DTMF		
Relay Status	RelayA: Low	RelayB: Low
Relay Name	Relay A	Relay B
Access Method	<input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC <input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC	

- **Mode:** Specify the conditions for automatically resetting the relay status.
 - **Monostable:** The relay status resets automatically within the relay delay time after activation.
 - **Bistable:** The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec):** Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode:** Set the digits of the DTMF code.

- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status:** Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name:** Assign a distinct name for identification purposes.
- **Access Method:** 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.

Security Relay

Relay ID	Security Relay A ▼
Connect Type	RS485 ▼
Trigger Delay(Sec)	0 ▼
Hold Delay(Sec)	5 ▼
1 Digit DTMF	1 ▼
2~4 Digits DTMF	
Relay Name	Security Relay A
Access Method	<input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC
Enabled	<input type="checkbox"/>
<button>Test</button>	

- **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 to be opened for 5 seconds before closing.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name:** Name the security relay. The name can be displayed in door-opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method:** 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.

Web Relay

Type	Disabled ▼
IP Address	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 02	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 03	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 04	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 05	<input type="text"/>	<input type="text"/>	<input type="text"/>

- **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**.

Schedule

All

Search

+ Add

Import

Export

<input type="checkbox"/>	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
<input type="checkbox"/>	1	1002	Local	Daily	Never	--	--	-	
<input type="checkbox"/>	2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	

Delete

Delete All

Prev

1/1

Next

1

Go

Schedule

All

Search

+ Add

🔍 Import

Time

00:00:00-23:59:59

Go

Add Schedule

Mode

Normal

Name

Start Date - End Date

20241227 ~ 20241227

Day

☒ Mon

☒ Tue

☒ Wed

☒ Thur

☒ Fri

☒ Sat

☒ Sun

☐ Check All

Start Time - End Time

00:00 - 23:59

Cancel

Submit

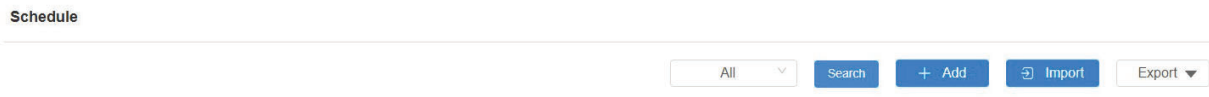
- **Mode:**

- **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.

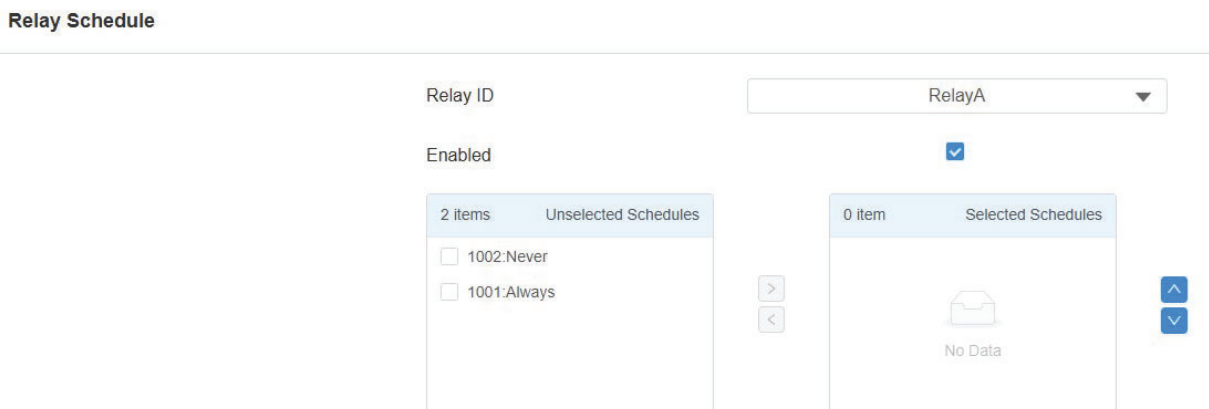
To set it up, go to the **Setting > Schedule** interface. The import/export file is in an XML file, supporting up to 100 schedules.



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.

For instructions on creating schedules, kindly consult the [Create Door Access Schedule](#) section.

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

All User ID/Name/Code Search + Add

<input type="checkbox"/>	Index	Source	User ID	Name	RF Card & Bkey	Floor No.	BLE Status	Web Relay	Schedule-Relay	Edit
 No Data										

 Delete
 Delete All
Prev
1/1
Next
1
Go

User Basic

User ID	<input type="text"/>
Name	<input type="text"/>
Role	General User ▼

- **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.

Contact Details

Phone	<input type="text"/>
-------	----------------------

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

Unlock by RF Card/Bkey

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

RF Card & Bkey

Code	<input type="text"/>	<button>Obtain</button>	<button>Delete</button>
<button>Add</button>			

- **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.

Card Type Support

IC Card Enabled	<input checked="" type="checkbox"/>
-----------------	-------------------------------------

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.

RFID

IC Card Display Mode	<input type="text" value="8HN"/>
----------------------	----------------------------------

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

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.

BLE Setting

Authentication Code	<input type="text"/>	<button>Generate</button>	<button>Delete</button>
Status	Unpaired		
Pairing Valid Until	N/A		

- **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.

BLE Basic

Enable BLE Function	<input checked="" type="checkbox"/>
Enable Hands Free Mode	<input checked="" type="checkbox"/>
Trigger Distance	within 1 meter ?
BKey Trigger Signal	
Unlock Interval For Same User(Sec)	10 (5~900Sec) ?
Unlock Interval For Different User(Sec)	10 (5~900Sec) ?
Authentication Code Valid Time	1h ?

Bluetooth Settings

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

BLE Basic

Enable BLE Function ☒

Enable Hands Free Mode ☒

Trigger Distance ?

BKey Trigger Signal ?

Unlock Interval For Same User(Sec) (5~900Sec) ?

Unlock Interval For Different User(Sec) (5~900Sec) ?

Authentication Code Valid Time

- **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 Info Settings

Device Name

X910

Device ID

- **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.

Movement Detection

Enabled



Unlock By QR Code

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

Click the QR code icon .

QR Code

Code



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.

Access Setting

- **Allow to Open:** Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **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.
- **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.

Import/Export User

User Data

Import

Export

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.

Contactless Smart Card

Enabled

NFC

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 Card Encryption

Type

None ▼

- **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.

Open Relay Via HTTP

Enabled	<input checked="" type="checkbox"/>
Session Check	<input type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="password"/>

- **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.

Device's IP
`http://192.168.35.127/fcgi/do? action=OpenDoor&`

Preset credentials for authentication
`UserName=admin&Password=123456`

ID of Relay to be triggered
`DoorNum=1`

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.

Relay

Relay ID	RelayA	RelayB
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	#	0
2~4 Digits DTMF		
Relay Status	RelayA: Low	RelayB: Low
Relay Name	Relay A	Relay B
Access Method	<input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC <input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC	

- **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.

DTMF

Type	Info+Inband+RFC2833 ▼
How To Notify DTMF	Disabled ▼
Payload	101 (96~127)

- **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.

Input A

Enabled	<input type="checkbox"/>
Trigger Electrical Level	Low ▼
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> Email <input type="checkbox"/> SIP Call <input type="checkbox"/> HTTP
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution ▼
Execute Relay	None ▼
Alarm Door Opened	<input type="checkbox"/>
Break-in Intrusion	<input type="checkbox"/>
Door Status	DoorA: High

- **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.

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input checked="" type="checkbox"/>
Authentication Mode	<div>Digest ▼</div>
User Name	<div>admin</div>
Password	<div>*****</div>

- **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.

MJPEG Video Parameters

Enabled	<input checked="" type="checkbox"/>
Video Resolution	VGA ▼
Video Framerate	30fps ▼
Video Quality	90 ▼

- **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.