

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX S532 DOOR PHONE

Administrator Guide

Thank you for choosing Akuvox S532 series door phones. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to version 532.30.1.19, and it provides all the configurations for the functions and features of the Akuvox door phone. Please visit Akuvox web or consult technical support for any new information or the latest firmware.

Product Overview



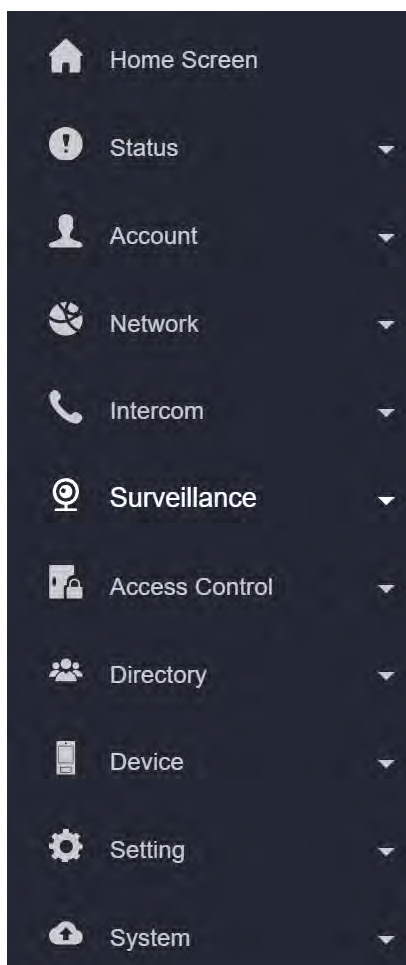
- 2.8" LCD
- Aluminum Body
- **Linux OS**
- Numeric keypad
- Multiple access control (RFID, NFC, Bluetooth)
- **IP to Analog audio/video output (optional)**
- **IK08 & IP66**

Model Specification

S532	
Camera	x 1
IR LEDs	✓
Card Reader	✓
Touch Screen	X
Ethernet	x 1, PoE+(802.3at)
Wiegand	x 1
RS485	x 1
Relay	x 2
Input	x 4
Analog Audio	Optional
Analog Video	Optional
TF Card Slot	x 1
Line Out	x 1
Power In	x 1, 12V/2A
MIC	x 1
Speaker	x 1
BLE	✓

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 setting, RTP port setting, device deployment, etc.
- **Intercom:** this section includes LCD setting, call features, multicast, etc.
- **Surveillance:** the section covers motion detection, RTSP setting, ONVIF setting, etc.
- **Access Control:** this section covers relay setting, card setting, PIN setting, etc.
- **Directory:** this section is for user management.
- **Device:** this section covers LCD, light, wiegand, audio, and lift control settings.
- **Setting:** this section covers time and language, action, schedule and HTTP API settings.
- **System:** this section is for upgrading, maintenance, auto-provisioning, etc.



Access the Device

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

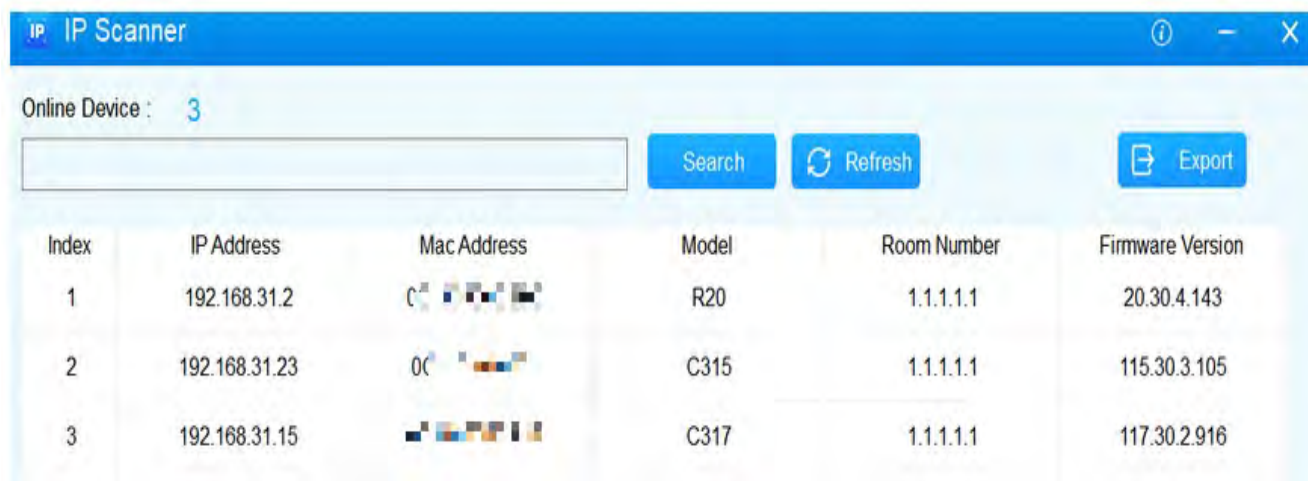
Access the Device Setting on the Device

To access the device setting, press *2396# to enter the advanced setting screen. It provides some advanced permissions like editing network, resetting, and admin password modification to administrators, including **System Information**, **Admin Setting**, and **System Setting**.

Access the Device Setting on the Web Interface

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

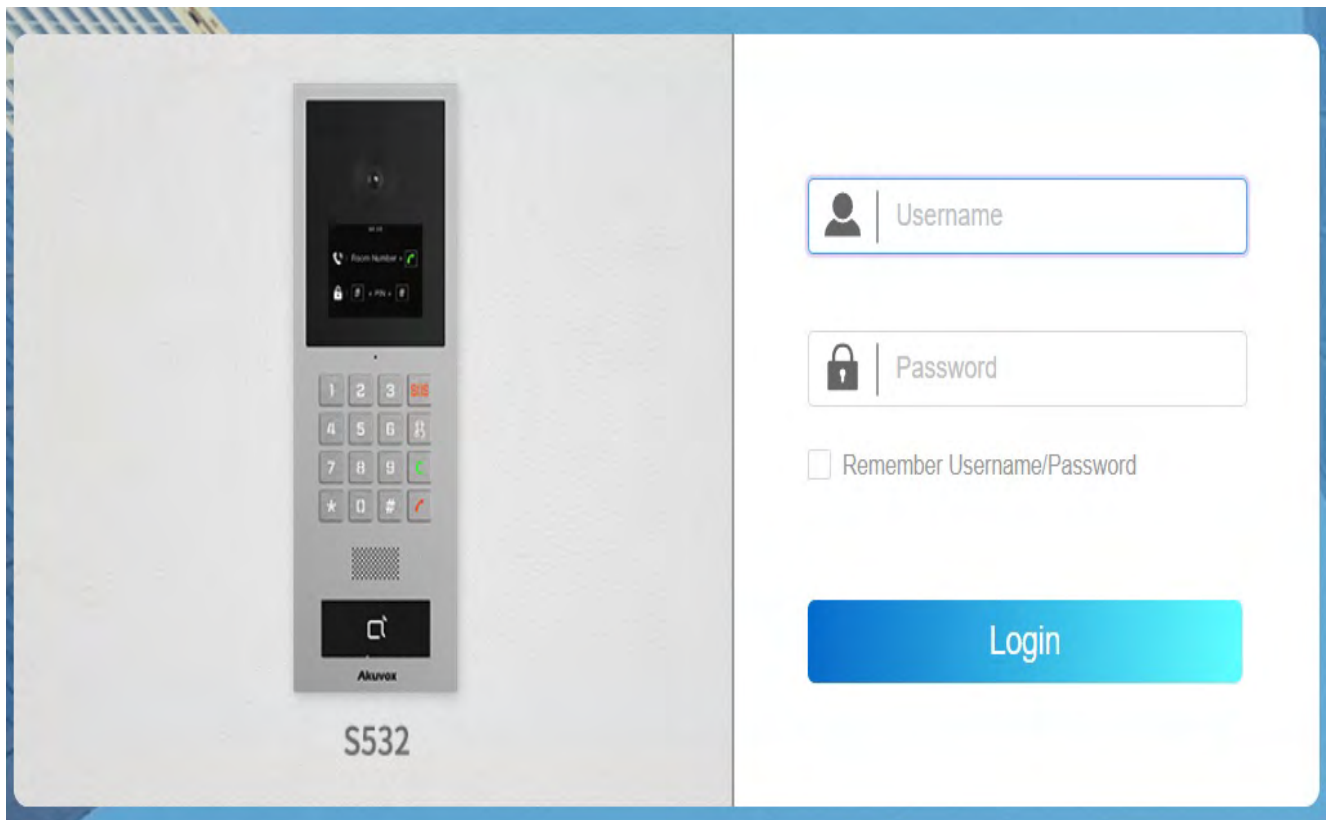
You can check the IP address on the device **System Information** screen or you can search the device IP by the IP scanner in the same LAN network.



The screenshot shows a window titled "IP Scanner" with a search bar and buttons for "Search", "Refresh", and "Export". Below the search bar is a table with the following data:

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.31.2	08:00:27:12:34:56	R20	1.1.1.1	20.30.4.143
2	192.168.31.23	08:00:27:12:34:57	C315	1.1.1.1	115.30.3.105
3	192.168.31.15	08:00:27:12:34:58	C317	1.1.1.1	117.30.2.916

The initial user name and password are both **admin** and please be case-sensitive to the user names and passwords entered.



Note:

- Download IP scanner:
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- See the detailed guide:
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Google Chrome browser is strongly recommended.

Language and Time Setting

Language Setting

To set up the language, navigate to the web **Setting > Time/Lang** interface. Currently, only English is supported.

LCD Language

Mode

English ▼

You can select the web language in the upper right corner.

Akuvox
Open A Smart World

S532

English ▼
 Log Out

You can customize the web and device language by exporting the file and importing it after modification.

To customize the language, navigate to the web **Setting > Time/Lang** interface.

Custom Language

Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	Import	Export	Reset
LCD	Default	strings.xml	Import	Export	Reset

Note

- The uploaded file for customizing web language should be in .json format.
- The uploaded file for customizing LCD language should be in .xml format.

Time Setting

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

To configure time, navigate to the web **Setting > Time/Lang** interface.

Time

Automatic Date&Time	☒
Time Zone	GMT+0:00 GMT ▼
Date Format	2023-12-12 ▼
Time Format	24 Hour ▼
NTP Server	0.pool.ntp.org
Update Interval	3600 (≥3600s)
System Time	02:32:13

- **Automatic Date & Time:** When enabled, the device's date and time are automatically set up and synchronized with the default time zone and the NTP server (Network Time Protocol).
- **NTP Server:** The NTP server address.
- **Update Interval:** The interval between two consecutive NTP requests.

LED & LCD Setting

Infrared LED Setting

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

To set up the LED, navigate to the web **Device > Light > LED Setting** interface.

LED Setting

Mode	Auto ▼		
Photoresistor Setting	1670	-	1710 (0~1800)
IR LED Brightness	7 ▼		

- **Mode:** Select from **Auto**, **Always ON**, **Always OFF**, and **Schedule**.
- **Photoresistor Setting:** Set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the ON-OFF of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off.
- **IR LED Brightness:** Adjust the IR LED brightness from level 0 to 10.

LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce electrical power consumption.

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

LED Of Swiping Card Area

Enabled



Start Time - End Time

18

-

23

(0~23 Hour)

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

LED Setting on Keypad

You can enable or disable the LED lighting on the keypad area as needed on the web interface. You can also set the timing for the exact time during which the LED light can be disabled to reduce electrical power consumption.

To set it up, navigate to the web **Device > Light > LED Of Keypad Area** interface.

LED Of Keypad Area

Enabled



Start Time - End Time

18

-

23

(0~23 Hour)

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

Configure Screensaver

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

Navigate to the web **Device > LCD** interface.

Sleep

Auto-Sleep Time	15 seconds ▼
Screensaver Mode	Image ▼
Screensaver Time	15 seconds ▼
Wake Up Mode	Auto ▼

- **Auto-Sleep Time:** It ranges from 5 seconds to 30 minutes. If you set it as 10 sec, the device will go into screen saver mode in 10 sec when there is no operation on the device or no one is detected approaching.
- **Screensaver Mode:** **Image** displays the default picture or the picture uploaded.
- **Screensaver Time:** The screensaver duration after the device goes into sleep mode. Screensaver duration ranges from 5 seconds to 30 minutes. The default is 15 seconds.
- **Wake Up Mode:** When **Auto** is selected, the screen will be awakened when someone approaches without it being touched upon. When **Manual** is selected, touch and wake up the screen.

Upload Screensaver

You can upload screen-saver pictures to the device for publicity purposes or a greater visual experience.

Navigate to the web **Device > LCD** interface.

Upload Screensaver

Transition Time

5

Sec

Screensaver ID	File Status	Import	Delete
1	File Exists	Import	Delete
2	File Exists	Import	Delete
3	File Exists	Import	Delete
4	File Exists	Import	Delete

- **Transition Time:** The time interval switching between two pictures.

Note

The file should be in .jpg format with a 1M max size.

Screen Backlight Brightness

You can adjust the backlight brightness for the screen and screen saver.

Navigate to the web **Device > LCD** interface.

Screen Backlight Brightness

Mode	Auto	
Backlight Brightness (Day)	200	(1~255)
Backlight Brightness Of Screensaver (Day)	100	(1~255)
Backlight Brightness (Night)	100	(1~255)
Backlight Brightness Of Screensaver (Night)	50	(1~255)
Backlight Brightness (High)	255	(1~255)
Backlight Brightness Of Screensaver (High)	255	(1~255)

- **Mode:** When **Auto** is selected, the screen backlight brightness will be adjusted automatically.

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

-If the current photoresistor is lower than the preset minimum photoresistor, the device is in **High** mode.

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

-If the current value is higher than the maximum photoresistor, the device is in **Night** mode.

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

- **Backlight Brightness (Night):** The backlight at night with a value ranging from 1-255.
- **Backlight Brightness Of Screensaver (Night):** The backlight for the screensaver at night with the value ranging from 1-255.
- **Backlight Brightness (High):** The backlight with a value ranging from 1-255.
- **Backlight Brightness Of Screensaver (High):** The backlight for the screensaver with a value ranging from 1-255.

LCD Heat Control

To ensure the normal operation of the door phone in low-temperature environments, you can heat up the device's LCD screen according to your heat control setting.

Navigate to **Intercom > Basic** interface.

LCD Heat Control

Enabled

☐ ?

Heat Threshold

(-40~30°C)

Current Temperature

- **Enabled:** This function cannot be used in Low Power Mode. You need to use POE+ to ensure a sufficient power supply.
- **Threshold:** When the device temperature reaches the threshold, the device will start heating up.
- **Current Temperature:** Click **Read** to acquire the device's current temperature.

Volume and Tone Configuration

Volume and tone configurations include microphone volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

Navigate to the web **Device > Audio** interface.

Volume Control

Prompt Volume	8	(1~15)
Mic Volume	8	(1~15)
Mic Volume(Proxy)	8	(1~15)
Speaker Volume	8	(1~15)
Analog Volume	8	(1~15)
Keypad Volume	8	(1~15)
Tamper Alarm Volume	8	(1~15)

- **Mic Volume(Proxy):** The mic volume of the analog switch.
- **Analog Volume:** The volume of the analog switch during a call.

Upload Tone Files

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

Navigate to the web **Device > Audio** interface.

Tone Upload

ID	Tone	Import	Reset	Play	Enabled
1	Access Granted	Import	 Reset		☒
2	Access Granted(Input)	Import	 Reset		☒
3	Access Denied	Import	 Reset		☒

Network Setting

Network Status

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

Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.100
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternative DNS Server	8.8.8.8

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 up the network, navigate to the web **Network > Basic** interface.

LAN Port

Network Mode	☐ DHCP ☒ Static IP
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS Server	8.8.8.8
Alternative DNS Server	

- **DHCP:** DHCP mode is the default network connection. If the DHCP mode is turned on, the door phone 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(es) have to be manually configured according to the actual network environment.
- **IP Address:** The IP address when the static IP mode is selected.
- **Subnet Mask:** The subnet mask according to the actual network environment.
- **Default Gateway:** The correct gateway according to the IP address.
- **Preferred/Alternate DNS:** The preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary one. The door phone will connect to the alternate server when the primary server is unavailable.

You can also configure the network on the device. Press *2396# on the device keypad and tap 3 and 1 to enter the network setting screen.

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

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

Connect Setting

Connect Type	Cloud
Discovery Mode	☒
Device Address	1 1 1 1 1
Device Extension	1
Device Location	S532

- **Server Mode:** It is automatically set up according to the actual device connection with a specific server in the network such as SDMC, Cloud, or None. None is the default factory setting indicating the device is not in any server type.
- **Discovery Mode:** When enabled, the device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.

- **Device Address**: Specify the device address by entering device location information from the left to the right: Community, Unit, Stair, Floor, and Room in sequence.
- **Device Extension**: The device extension number.
- **Device Location**: The location in which the device is installed and used.

Device Local RTP Configuration

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

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

To configure RTP, navigate to the web **Network > Advanced** interface.

Local RTP		
Starting RTP Port	11800	(1024~65535)
Max RTP Port	12000	(1024~65535)

- **Starting RTP Port**: The port value for establishing the start point for the exclusive data transmission range.
- **Max RTP Port**: The port value for establishing 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 configure SNMP, navigate to the web **Network > Advanced** interface.

SNMP

Enabled	☐	
Port		(1024~65535)
Trusted IP		
SNMP Trap IP		
Username		(8~16 digits)
Password		(8~16 digits)
DES		(8~16 digits)

- **Port:** The SNMP server's port.
- **Trusted IP:** The allowed SNMP server address. It can be an IP address or any valid URL domain name.

VLAN Setting

A Virtual Local Area Network (VLAN) is a logical group of nodes from the same IP domain, regardless of their physical network segment. It separates the layer 2 broadcast domain via switches or routers, sending tagged packets only to ports with matching VLAN IDs. Utilizing VLANs enhances security by limiting ARP attacks to specific hosts and improves network performance by minimizing unnecessary broadcast frames, thereby conserving bandwidth for increased efficiency.

To configure VLAN, navigate to the web **Network > Advanced** interface.

VLAN

Enabled	☐	
VID	1	(1~4094)
Priority	0	

- **VID:** The VLAN ID for the designated port.
- **Priority:** The VLAN priority for the designated port.

QoS Setting

Quality of Service(QoS) is a network's ability to provide better service for specific network communications by utilizing various technologies. It serves as a security mechanism in networks, addressing issues like network latency and congestion. Ensuring QoS is crucial for networks with limited capacity, particularly for multimedia applications such as VoIP and IPTV. These applications often require a consistent transmission rate and are sensitive to delays.

To configure QoS, navigate to the web **Network > Advanced** interface.

QoS

Sip QoS	40	(0~63)
Voice QoS	40	(0~63)
RTSP Signaling QoS	40	(0~63)
RTSP Media QoS	40	(0~63)

TR069 Setting

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.

To configure it, navigate to the web **Network > Advanced** interface.

TR069

Enabled	☐
Version	1.0
ACS URL	
Username	
Password	*****
Periodic Inform	☐
Periodic Interval	1800 (3~24x3600s)
CPE URL	
Username	
Password	*****

- **Version:** Select the supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE URL:** The URL address for ACS or CPE. ACS is short for auto-configuration servers on the server side, and CPE is short for customer-premise equipment as client-side devices.
- **Periodic Interval:** The interval for periodic notifications.

Device Web HTTP Setting

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

To configure it, navigate to the web **Network > Advanced** interface.

Web Server

Allow HTTP	☒
Allow HTTPS	☒
HTTP Port	80 (80,1024~65535)

- **HTTP Port:** The port for the HTTP access method. 80 is the default port.

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 configure NAT, navigate to the web **Account > Basic** interface.

NAT

STUN Enabled	☐
STUN Server IP	
Port	3478 (1024~65535)

- **Port:** The default is 3478.

Intercom Call Configuration

IP Call & IP Call Configuration

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

Navigate to the web **Intercom > Call Feature > Direct IP** interface.

Direct IP

Enabled



Dtmf Type

RFC2833



Port

5060

(1~65535)

- **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 & 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.

To configure the SIP account, navigate to the web **Account > Basic** interface.

SIP Account

Status	Disabled
Account	Account1 ▼
Account Enabled	☐
Display Label	
Display Name	
Register Name	
Username	
Password	*****

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

Tip

For configuring contact call and dial plan, see [here](#).

- **Account Enabled:** Check to activate the registered SIP account.
- **Display Label:** The device label to be shown on the device screen.
- **Display Name:** The device's name to be shown on the device being called to.
- **User Name:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

SIP Server Configuration

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

To configure SIP server, go to the web **Account > Basic** interface.

Preferred SIP Server		
Server IP		
Port	5060	(1024~65535)
Registration Period	1800	(30~65535Sec)

Alternative SIP Server		
Server IP		
Port	5060	(1024~65535)
Registration Period	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 Configuration

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

To configure the outbound proxy server, go to the device web **Account > Basic > Outbound Proxy Server** interface.

Outbound Proxy Server

Outbound Enabled	☐
Preferred Server IP	
Port	5060 (1024~65535)
Alternative Server IP	
Port	5060 (1024~65535)

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

Data Transmission Type Configuration

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

To configure the data transmission type, navigate to the web **Account > Basic** interface.

Transport Type

Type	UDP
------	----------------------------------

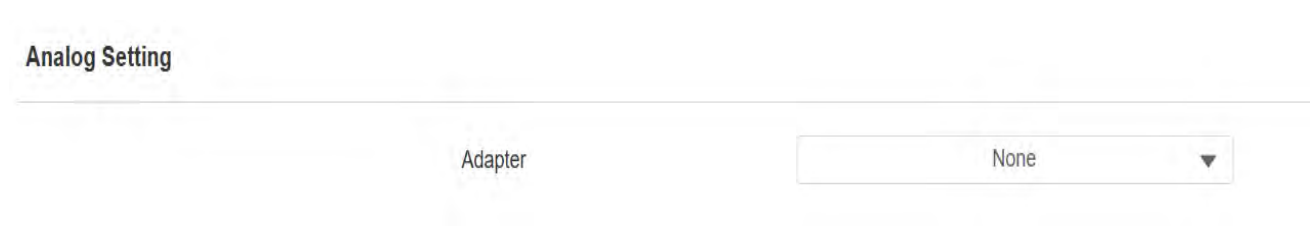
- **UDP**: An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP**: A less efficient but reliable transport layer protocol.

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

Analog Setting

Users can use an analog switch to answer calls made to the door phone after it is connected to the door phone.

Navigate to the web **Intercom > Basic > Analog Setting** interface.



Analog Setting

Adapter None ▼

- **Adapter:** The brand of the analog switch that the door phone is connected to. You can select from **Vizit, Cyfral, Eltis, Metakom, and Lascomex**.

Contacts Configuration

Manage Contact Groups

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

Navigate to the web **Directory > User > Group** interface. Click **+Add** to add a group. The device supports adding up to 1000 groups.

Group

+ Add

☐	Index	Name	Edit
☐	1	Akuvox	

Selected:0/1

 Delete

 Delete All

Total:1

Prev

1/1

Next

Go To Page

1

Go

User Basic

User ID

1

Name

Contact Details

Analog System



Analog Number

Analog Replace

Analog Mode

Direct



Group

Default



Priority of Call

Primary



- **Analog System:** When enabled, configure the analog number and users can call the analog switch.
- **Analog Number:** The number of the analog switch.
- **Analog Replace:** Optional configuration. The short number replaces the analog number. Users can call the analog switch by entering the short number on the door phone's keypad.
- **Analog Mode:** **Direct** means the analog switch is connected to the door phone through wires. **Proxy** means the analog switch is not connected to the door phone through wires and when this option is selected, the analog proxy address needs to be filled in.
- **Analog Proxy Address:** The proxy IP address.
- **Group:** Put the user in the desired contact group.
- **Priority of Call:** Set the priority of the call among three options: Primary, Secondary, and Tertiary. For example, if you set the priority of call for one of the contacts in a specific contact group as Primary, then the contact will be the first to be called among all the contacts in the same contact group when someone presses on the contact group for making a group call.
- **Dial Account:** The account to make the call.

Tip

To see detailed steps of configuring analog feature, please refer to [Integration Between S532 and Analog Handsets](#).

Contact List Display Setting

You can customize the contact list display on the device screen.

Navigate to **Directory > Directory Setting** interface.

Directory Setting

Show Cloud Contacts

☒

Contacts Display Mode

All Contacts ▼

Sort By

ASCII Code ▼

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

Call Setting

DND Configuration

The Do Not Disturb(DND) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

To configure DND, navigate to the web **Intercom > Call Feature** interface.

DND

Account	Account1 ▼
Enabled	☐
Return Code When DND	486(Busy Here) ▼
DND On Code	
DND Off Code	

- **Account:** The account to apply the DND feature.
- **Return Code When DND:** Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.
- **DND On Code:** The code used to turn on DND in the SIP server.
- **DND Off Code:** The code used to turn off DND in the SIP server.

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 configure call time duration, navigate to the web **Intercom > Call Feature** interface.

Max Call Time

Max SIP/IP Call Time	5	(2~30Min)
----------------------	---	-----------

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

Maximum Dial Duration

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

To configure maximum dial duration, navigate to the web **Intercom > Call Feature** interface.

Max Dial Time		
Max SIP/IP Dial In Time	60	(30~120Sec)
Max SIP/IP Dial Out Time	60	(30~120Sec)

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

Auto-answer Configuration

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

To configure auto-answer, navigate to the web **Intercom > Call Feature** interface.

Auto Answer		
Enabled	☒ Direct IP ☒ Account1 ☒ Account2	
Auto Answer Delay	0	(0~5Sec)
Mode	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.

Hang Up After Opening the Door

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

To configure it, navigate to the web **Intercom > Call Feature** interface.

Hang Up After Opening Door

Enabled	☐
Type	DTMF or HTTP ▼
Time Out (Sec)	5 (0~15Sec)

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

Prevent SIP Hacking

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 configure SIP hacking, navigate to the web **Account > Advanced** interface.

Call

Max Local SIP Port	5062	(1024-65535)
Min Local SIP Port	5062	(1024-65535)
Prevent SIP Hacking	☐	

- **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.

Speed Dial

Group Call

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

To configure the group call, navigate to the web **Intercom > Basic** interface.

Speed Dial

Call Type	Group Call																
When Refused	End This Call Only																
Group Call Number	<table> <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> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>																
No Answer Event	☐																
Trigger Relay	☐ RelayA ☐ RelayB																
Action to Execute	☐ FTP ☐ Email ☐ HTTP																

- **Call Type:** Group Call or Sequence Call.
- **When Refused:**

- **End This Call Only:** The call made to the refusing party will be terminated.
- **End All Calls:** all calls will be terminated.
- **Group Call Number:** If you fill in the local group call number, the local group number will be called instead of the SmartPlus group call number.
- **No Answer Event:** When the call is not answered, actions will be triggered.
- **Trigger Relay:** Relay to be triggered when the call is not answered.
- **Action to Execute:** Action to be triggered when the call is not answered.

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.

To configure the sequence call, navigate to the web **Intercom > Basic** interface.

Speed Dial

Call Type	Sequence Call ▼
Time Out (Sec)	60 ▼
When Refused	Do Not Call Next ▼
Sequence Call Number	
RobinCallNum1	
RobinCallNum2	
RobinCallNum3	
RobinCallNum4	
RobinCallNum5	
RobinCallNum6	
RobinCallNum7	
RobinCallNum8	
RobinCallNum9	
RobinCallNum10	
No Answer Event	☐
Trigger Relay	☐ RelayA ☐ RelayB
Action to Execute	☐ FTP ☐ Email ☐ HTTP

- **Call Type:** Group Call or Sequence Call.
- **Time Out(Sec):** Set the call timeout before calling the next called party when the first called party does not receive the call within the timeout.
- **When Refused:**
 - **Do Not Call Next:** the sequence call will be terminated if the call is rejected by the called party.

- **Call Next:** the sequence call will be continued to the next called party if it is rejected by the called party.
- **No Answer Event:** when the call is not answered, actions will be triggered.
- **Trigger Relay:** relay(s) to be triggered when the call is not answered.
- **Action to Execute:** action(s) to be triggered when the call is not answered.

Dial Plan

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

To configure dial plan, navigate to the web **Intercom > Dial Plan** interface. Click **Add**.

Replace Rule

+ Add
📄 Import
Export ▼

☐	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
No Data									

Selected: 0/0
🗑 Delete
🗑 Delete All

Total: 0
Prev
1/1
Next

Go To Page

Go

Add Replace Rules

Account

Auto

Prefix

1st Replace

2nd Replace

3rd Replace

4th Replace

5th Replace

Cancel

Submit

- **Account:** Select the dial-out account.
 - **Auto:** Dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.
 - **Account 1/2:** Dial-out using the chosen account.
- **Prefix:** Specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** Specify up to 5 numbers, which can be SIP number or IP address, to be replaced by the prefix. All these numbers will be called simultaneously when the caller dials the prefix.

Multicast

The Multicast function allows one-to-many broadcasting for different purposes. For example, it enables the indoor monitor to announce messages from the kitchen to other rooms, or to broadcast notifications from the management office to multiple locations. In these scenarios, indoor monitors can either listen to or send audio broadcasts.

To configure multicast, navigate 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:** Multicast or how many multicast calls are higher priority than SIP call, if you disable Paging Priority, SIP call will have higher priority.
- **Paging Priority:** Multicast calls are called in order of priority or not.
- **Listening Address:** The multicast IP address to be listened to. The multicast IP address needs to be the same as the listened part 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.

Web Call

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

To configure web call, navigate to the web **System > Maintenance > Web Call** interface. Select the registered SIP account to make the web call.

Web Call

Web Call(Ready)

Auto ▼

Dial Out

Hang Up

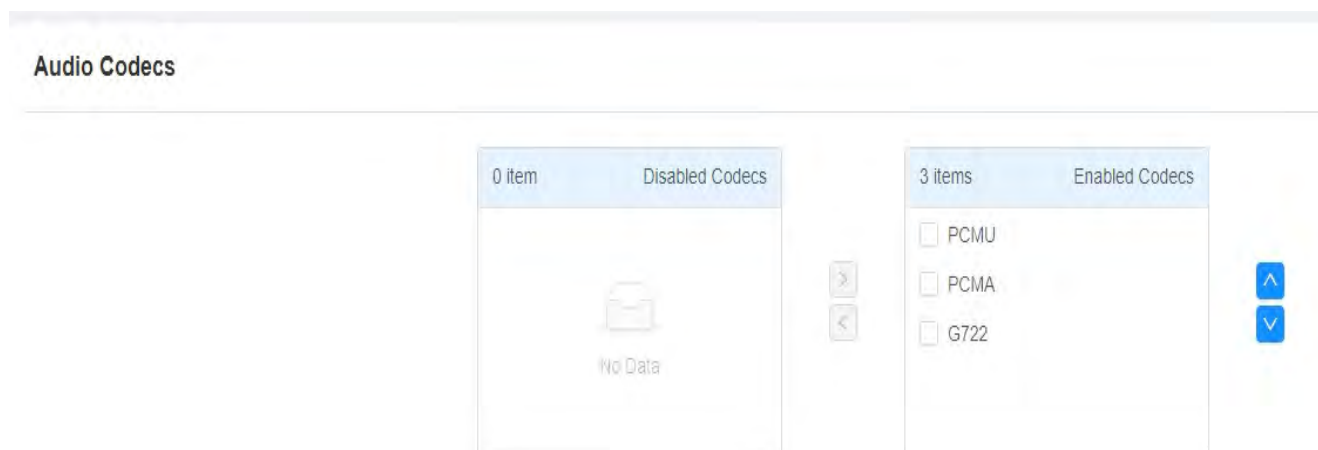
- **Web Call(Ready):** The target SIP/IP number.

Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

The door phone supports three types of codec (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To configure the audio codec, navigate to the web **Account > Advanced** 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 Configuration

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 configure the video codec, navigate to the web **Account > Advanced** interface.

Video Codec

Name	☒ H.264
Resolution	4CIF ▼
Bitrate	2048 kbps ▼
Payload	104 ▼
RateControl	VBR ▼
Profile	BP ▼

- **Name:** Check to enable the H264 video codec format for the door phone video stream.
- **Resolution:** The code resolution for the video quality has these options: **CIF**, **VGA**, **4CIF**, and **720P**. The default code resolution is 4CIF.
- **Bitrate:** The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the data transmitted every second the greater in amount, therefore, 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 Configuration for IP Direct Calls

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

Navigate to the **Intercom > Call Feature** interface.

Direct IP

Enabled	☒
Dtmf Type	RFC2833
Port	5060 (1~65535)
Video Resolution	720P
Video Bitrate	512 kbps
Video Payload	104

- **Video Resolution:** The code resolution for the video quality has these options: **CIF, VGA, 4CIF, 720P, and 1080P**. The default is 720P.
- **Video Bitrate:** The video stream bitrate ranges from 128 to 2048 kbps. The default code bitrate is 2048.
- **Video Payload:** The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Configure 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 door phone and other intercom devices for third-party integration.

To configure DTMF data transmission, navigate to the web **Account > Advanced > DTMF** interface.

DTMF

Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)

- **Type:** Select from the following options: **Inband, RFC2833, Info, Info+Inband, Info+RFC2833, Info+Inband+RFC2833** 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.

Relay Setting

Relay Switch Setting

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

Relay

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

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

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

Note

External devices connected to the relay require separate power adapter.

Security Relay Setting

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.



To configure the security relay, navigate to the web **Access Control > Relay** interface.

Security Relay

Relay ID	Security Relay A ▼	Security Relay B ▼
Connect Type	Relay A Power Output ▼	RS485 ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼
1 Digit DTMF	2 ▼	2 ▼
2~4 Digits DTMF	013	013
Relay Name	Security Relay A	Security Relay B
Enabled	☐	☐
	Test	Test

- **Connect Type:** Select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Trigger Delay (Sec):** Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name:** Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.

Web Relay Setting

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.



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

Web Relay

Type	Disabled ▼
IP Address	
Username	
Password	*****

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01			
Action ID 02			
Action ID 03			
Action ID 04			

- **Type:** There are three options, **Disabled**, **Only WebRelay**, and **Both Local Relay and Web Relay**.
- **IP Address:** The web relay IP address provided by the web relay manufacturer.

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

Note

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

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

Door Access Schedule Management

Configure Door Access Schedule

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

Create Door Access Schedule

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

To configure the schedule, navigate to the web **Setting > Schedule** interface. Click **+Add** to create a schedule.

Schedule									
					All ▾	Search	+ Add	Import	Export ▾
	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
☐	1	1002	Local	Daily	Never	--	--	-	
☐	2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	
Selected: 0/0 Delete Delete All Total: 2 Prev 1/1 Next Go To Page 1 Go									

To create a daily schedule:

Add Schedule

Mode

Daily ▾

Name

Start Time - End Time

00:00

-

23:59

Cancel

Submit

To create a weekly schedule:

Add Schedule



Mode	Weekly
Name	
Day	☒ Mon ☒ Tue ☒ Wed ☒ Thur ☒ Fri ☒ Sat ☒ Sun ☐ Check All
Start Time - End Time	00:00 - 23:59

Cancel

Submit

To create a longer period schedule:

Add Schedule



Mode	Normal
Name	
Start Date - End Date	20231212 ~ 20231212
Day	☒ Mon ☒ Tue ☒ Wed ☒ Thur ☒ Fri ☒ Sat ☒ Sun ☐ Check All
Start Time - End Time	00:00 - 23:59

Cancel

Submit

Edit the Door Access Schedule

Navigate to the web **Setting > Schedule** interface.

Tick the box of the local schedule to edit or delete. The access control schedule synchronized from the SmartPlus cannot be edited or deleted.

Schedule

All

Search

+ Add

Import

Export

☒	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
☒	1	1	Local	Normal	Schedule	20231212-20231212	Sun Mon Tue Wed Thur Fri Sat	00:00-23:59	
☐	2	1002	Local	Daily	Never	--	--	-	
☐	3	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	

Selected: 1/0

Delete

Delete All

Total: 3

Prev

1/1

Next

Go To Page

1

Go

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.

Navigate to the web **Setting > Schedule** interface.

Schedule

										All ▾	Search	+ Add	Import	Export ▾
Note It only supports a .xml format file for importing and exporting the schedule.														

Door Unlock Configuration

Configure PIN Code for Door Unlock

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

Configure Public PIN

Navigate to the web **Access Control > PIN Setting** interface.

Public Key

Enabled	☒
PIN Code	***** (5~8 digits)
Relay	☒ RelayA ☒ RelayB

- **PIN Code:** Set a 3-8 digits PIN code accessible for universal use.
- **Relay:** The relay to be triggered.

Configure Private PIN

On the web interface, you can create the PIN code and customize additional settings, such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

Navigate to the web **Directory > User** interface. Click Add to configure the private PIN.

User Basic

User ID

2

Name

Private PIN

Code

- **User ID:** The unique identification number assigned to the user.
- **Name:** The name of this user.
- **Code:** Set a 2-8 digit PIN code solely for the use of this user. Each user can only be assigned a single PIN code.

Scroll down and select the door access schedule for private PIN code door access.

Access Setting

Allow To Open

☒ Relay A ☐ Relay B

Floor No.

None x

Web Relay

0

2 items Unselected Schedules

- ☐ 1:Schedule
- ☐ 1002:Never

1 item Selected Schedules

- ☐ 1001:Always

- **Allow To Open:** Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **Floor NO.:** Specify the accessible floor(s) to the user via the [elevator](#).

- **Web Relay:** Specify the ID of web relay action commands that you've configured on the [Web Relay](#) interface. A default value of 0 indicates that the web relay will not be triggered.
- **Schedule:** Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the right box to the left 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.

Note

This step applies to door access by RF card and facial recognition as they are identical in configuration.

Configure RF Card for Door Unlock

Configure RF Card

Navigate to the web **Directory > User** interface. Click Add to configure the RF card. Place the card on the card reader area and click Obtain to add the card.

User Basic	
User ID	2
Name	

Private PIN	
Code	

RF Card	
Code	Obtain Delete
Add	

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

Note

- RF cards with 13.56 MHz and 125 KHz can be applied to the door phone for door access.
- Each user can have a maximum of 5 cards added.
- The device allows to add 10000 users.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the door phone for access.
- You can also add admin cards on the device. Press *2396#, on the keypad. Then, tap 2 and 1 to enter the card setting screen where you can add or delete an RF card.

Configure 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 configure the RF card code, navigate to the web **Access Control > Card Setting** interface.

RFID

IC Card Display Mode	8HN ▼
ID Card Order	Normal ▼
ID Card Display Mode	8HN ▼

- **IC/ID Card Display Mode:** Set the card number format from available options. The default format in the door phone is 8HN.
- **ID Card Order:** Select normal or reversed display of ID card number.

Mifare Card Encryption

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

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

Mifare Card Encryption

Type	Classic ▼	
Sector/Block	0	/ 0
Block Key	*****	

- **Type:** There are three options, **None**, **Classic**, and **Plus**.
- **Classic:**
 - **Sector/Block:** Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
 - **Block Key:** Set a password to access the data stored in the predefined sector/block.

Mifare Card Encryption

Type	Plus ▼
First Choice	
Block(1~128)	*****
SL1	*****
SL3	*****
Second Choice	
Block(1~128)	*****
SL1	*****
SL3	*****
Third Choice	
Block(1~128)	*****
SL1	*****
SL3	*****

- **Plus:** There are three block choices. The device can read the encrypted data in SL1 and SL3.
 - **Block:** The block number where the encrypted data is located.
 - **SL1:** The key number within 24 bits.
 - **SL3:** The key number within 32 bits.

NFC Card Setting

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

To configure NFC, navigate to the web **Access Control > Card Setting** interface. Enable the card type before using the card to open the door.

Card Type

Enabled ☒ IC Card ☒ ID Card ☒ NFC

Configure Open Relay via HTTP for Door Unlock

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 configure it, navigate to the web **Access Control > Relay > Open Relay Via HTTP** interface.

Open Relay Via HTTP

Enabled ☒

Username

Password

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

Tip

Here is an HTTP command URL example:

Door phone's IP **Preset credentials for authentication**
 http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1
ID of Relay to be triggered

Configure Exit Button for Door Unlock

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.

Navigate to the web **Access Control > Input** interface.

Input A

Enabled	☒
Trigger Electrical Level	Low ▼
Action to Execute	☐ FTP ☐ Email ☐ SIP Call ☐ HTTP
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution ▼
Execute Relay	None ▼
Door Status	DoorA: High

- **Enabled:** To use a specific input interface.
- **Trigger Electrical Level:** Set the input interface to trigger at low or high electrical level.
- **Action to Execute:** Set the desired actions that occur when the specific Input interface is triggered.
 - **FTP:** Send a screenshot to the preconfigured [FTP server](#).
 - **Email:** Send a screenshot to the preconfigured [Email address](#).
 - **SIP Call:** Call the [preset number](#) upon 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](#).
- **Action Delay:** Specify whether the relay can be triggered at any time or only within a scheduled period.
- **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.

Configure Bluetooth for Door Unlock

The Bluetooth-enabled SmartPlus app enables users to enter the door hands-free. They can either open the door with the app in their pockets or wave their phones towards the door phone as they get closer to the door.

To configure Bluetooth unlock, navigate to the web **Access Control > BLE** interface.

BLE Basic

Enable BLE Function

☐

Enable Hands Free Mode

☐

Trigger Distance

Within 1 meter ▼

RSSI Threshold

-72

(-85~-50db)

Open Door Interval(Sec)

5 ▼

- **Enable Hands Free Mode:** If enabled, users can gain door access hands-free. If disabled, users have to wave their hands in front of the door phone to open doors.
- **Trigger Distance:** Set the triggering distance of the Bluetooth for the door access. You select About 1 meter, Within 1 meter, and More than 2 meters. The trigger distance is 3 meters maximum.
- **RSSI Threshold:** Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Open Door Interval:** Set the time interval between consecutive Bluetooth door access attempts.

Configure Open Relay via DTMF for Door Unlock

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 ID	Relay A	Relay B
Relay Type	Default Status	Default Status
Mode	Monostable	Monostable
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	#	1
2-4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	Relay1	RelayB
Open Relay	Open	Open

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

Note

To open the door with DTMF, the intercom devices that send and receive the unlock command must use the same mode and code. Otherwise, the DTMF unlock may fail. See [here](#) for the detailed DTMF configuration steps.

DTMF Whitelist

To configure the DTMF whitelist, navigate to the web **Access Control > Relay > Open Relay** via **DTMF** interface.

Open Relay via DTMF

Assigned The Authority For

Only Contacts List ▼

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

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.

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.

RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

To configure RTSP, navigate to the web **Surveillance > RTSP** interface.

RTSP Basic

Enabled



RTSP Authorization Enabled



MJPEG Authorization Enabled



Authentication Mode

Basic ▼

Username

admin

Password

- **RTSP Authorization Enabled:** When you enable the RTSP authorization, you are required to configure RTSP Authentication Mode, RTSP Username, and Password for authorization.
- **Authentication Mode:** There are two options, Basic and Digest. **Basic** is the default authentication type.
- **Username:** Set the username for authentication.
- **Password:** Set the password for authentication.

RTSP Stream Setting

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

To configure the RTSP stream, navigate to the web **Surveillance > RTSP** interface.

RTSP Stream

RTSP Audio	☒
RTSP Video Enabled	☒
RTSP Video2	☒
RTSP Video Port	554 (554 1024~49151)
Video Codec	H.264

- **RTSP Audio:** Allow the door phone to send audio information to the monitor by RTSP.
- **RTSP Video Enabled:** The door phone can send the video information to the monitor. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **RTSP Video 2:** Akuvox door phones support 2 RTSP streams, you can enable the second one
- **RTSP Video Port:** Choose a suitable audio codec for RTSP audio.
- **Video Codec:** Choose a suitable video codec for RTSP video.

H.264 Video Parameters

Video Resolution	4CIF ▼
Video Framerate	30 ▼
Video Bitrate	2048kbps ▼
2nd Video Resolution	VGA ▼
2nd Video Framerate	25fps ▼
2nd Video Bitrate	512kbps ▼

- **Video Resolution:** There are the following options, QVGA, CIF, VGA, 4CIF, 720P, and 1080P. The default video resolution is **720P**. The video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than 720P.
- **Video Framerate:** 30fps is the video frame rate by default.
- **Video Bitrate:** There are the following options, 128kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps. Select it according to the network environment. The default video bitrate is 2048 kbps.
- **2nd Video Resolution:** The video resolution for the second video stream channel. The default video solution is VGA.
- **2nd Video Framerate:** The video framerate for the second video stream channel. 25 fps is by default for the second video stream channel.
- **2nd Video Bitrate:** There are the following options, 128kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps for the second video stream channel. The second video stream channel is 512 kbps by default.

MJPEG Image Capturing

You can take a monitoring image in Mjpeg format with the device. To do this, you need to turn on the Mjpeg function and choose the image quality.

Navigate to the web **Surveillance > RTSP** interface to enable this feature and configure the parameters.

RTSP Basic

Enabled	☒
RTSP Authorization Enabled	☐
MJPEG Authorization Enabled	☒
Authentication Mode	Basic ▼
Username	admin
Password	*****

MJPEG Video Parameter

Video Resolution	720P ▼
Video Framerate	30 fps ▼
Video Quality	90 ▼

- **MJPEG Authorization Enabled:** When enabled, you are required to configure the Authentication Mode, RTSP Username, and Password for authorization.
- **Username:** Set the username for authentication.
- **Password:** Set the password for authentication.

You can capture the image from the door phone using the following three types of URL formats:

[http:// deviceip:8080/picture.cgi](http://deviceip:8080/picture.cgi)

<http://deviceip:8080/picture.jpg>

<http://deviceip:8080/jpeg.cgi>

- **Authentication Mode:** There are two options, Basic and Digest. **Basic** is the default authentication type.
- **Video Resolution:** There are the following options, QVGA, CIF, VGA, 4CIF, 720P, and 1080P. The default video resolution is **720P**. The video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than 720P.
- **Video Framerate:** There are three options, 10 fps, 15 fps, and 30 fps. 30 fps is the video frame rate by default.

- **Video Quality:** It ranges from 50 to 90.

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.

To configure ONVIF, navigate to the web **Surveillance > ONVIF** interface.

Basic Setting

Discoverable	☒
Username	admin
Password	*****

- **Discoverable:** When enabled, the video from the door phone camera can be searched by other devices.
- **Username:** Customize the username for authentication. It is admin by default.
- **Password:** Customize the password for authentication. It is admin by default.

After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream. For example: http://IP address:80/onvif/device_service

Live Stream

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

To view the real-time video, navigate to the web **Surveillance > Live Stream** interface.

Surveillance» Live Stream



Security

Tamper Alarm Setting

The tamper alarm function prevents anyone from removing the devices without permission. It does this by setting off the tamper alarm and making calls to a designated location when the device detects a change in its gravity value from the original one.

To configure a tamper alarm, navigate to the web **System > Security > Tamper Alarm** interface.

Tamper Alarm	
Enabled	☐

Disarm Setting

You can set the disarm code on the web **System > Security** interface.

Disarm Setting	
Enabled	☐
PIN Code	(Enter * + PIN + # to disarm)

Virtual PIN

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

To configure the virtual PIN, navigate to the web **Access Control > PIN Setting** interface.

Virtual Key	
Enabled	☐

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

Note

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

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.

To upload the certificate, navigate to the web **System > Certificate** interface.

Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	 Delete

Web Server Certificate Upload

 Upload

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.

To upload the certificate, navigate to the web **System > Certificate** interface.

Client Certificate

Index	Issue To	Issuer	Expire Time
 No Data			

 Delete

 Delete All

Index

Auto ▼

Client Certificate Upload

 Upload

Only Accept Trusted Certificates



- **Index:** Select the desired value from the drop-down list of Index. If you select Auto, the uploaded certificate will be displayed in numeric order. If you select the value from 1 to 10, the uploaded certificate will be displayed according to the number.
- **Client Certificate Upload:** Locate and upload the desired certificate (*.pem only).
- **Only Accept Trusted Certificates:** When enabled, as long as the authentication is successful, the phone will verify the server certificate based on the client certificate list. When disabled, the phone will not verify the server certificate no matter whether the certificate is valid or not.

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.

To configure motion detection, navigate to the web **Surveillance > Motion** interface.

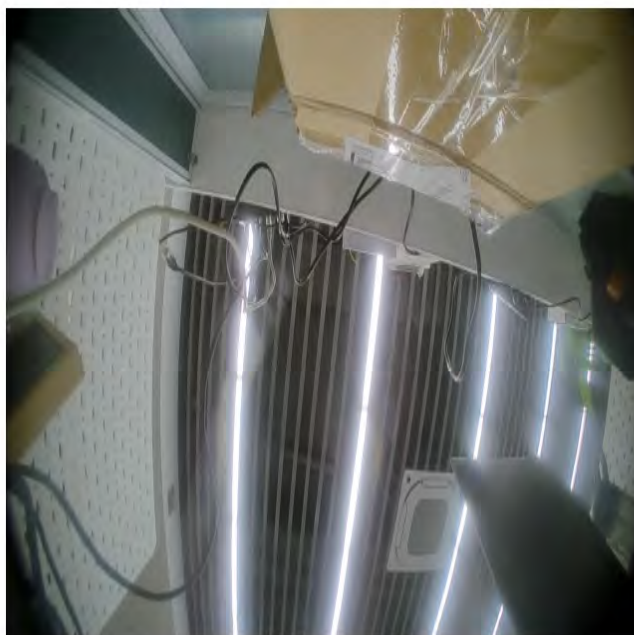
Motion Detection Options

Suspicious Moving Object Detection Video Detection ▼

Time Interval 10 (0~120Sec)

Detection Accuracy 3 (0~6)

Detection Area



Clear

Move the arrow to the start point, left click and hold down the mouse button, then drag the arrow to select an area. You can draw up to three detection area.

Motion Action

Action to Execute

☐ FTP ☐ Email ☐ SIP Call ☐ HTTP

You will need to set up the corresponding configurations in [Setting-Action](#).

Execute Relay

Relay A ▼

- **Suspicious Moving Object Detection:** There are four options, Disabled, Video Detection, Radar Detection, and Video + Radar. **Video Detection** focuses on analyzing visual information captured through cameras. **Radar Detection** offers longer-ranged and better detection in poor visibility conditions.
- **Detection Range:** After enabling radar detection, you can select the detection range among 1, 2, and 3 meters.

- **Time Interval:** The absolute triggering interval is 3 seconds. If you select a number greater than 3 seconds, then it requires a second triggering interval to trigger the alarm. For example, if you select 3 seconds, then the alarm will be triggered when a moving object is detected one time from 0 to 3 seconds (triggered any time from 0 to 3 seconds). However, for example, if you select 5 seconds (greater than 3), then the alarm will not be triggered until a moving object is detected for the second time from 3 to 5 seconds (triggered any time from 3 to 5 seconds). The default interval is 10 seconds.
- **Detection Range:** This option appears when radar detection is selected. It ranges from 1 to 3 meters.
- **Detection Accuracy:** The detection accuracy for the detection sensitivity. The higher the value, the greater the sensitivity. The default detection accuracy value is 3.
- **Detection Area :** Click and hold down the mouse button to select up to three detection areas.
- **Action to Execute:** The notification type includes FTP, Email, SIP Call, and HTTP.
 - FTP: the notification will be sent to the designated server.
 - Email: the email will be sent to the pre-configured email address.
 - SIP Call: a call will be made to the pre-configured number.
 - HTTP: the notification will be sent to the designated server.
- **Execute Relay:** The relay to be triggered.

Scroll down and you can set the motion detection schedule.

Motion Detect Time Setting

Day	☒ Mon	☒ Tue	☒ Wed
	☒ Thur	☒ Fri	☒ Sat
	☒ Sun	☐ Check All	

Start Time - End Time	00:00	-	23:59	
-----------------------	-------	---	-------	--

Security Notification Setting

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

Email Notification Setting

Set up email notification to receive screenshots of unusual motion from the door phone.

Navigate to the web **Setting > Action** interface.

Email Notification

Sender's Email Address

Receiver's Email Address

SMTP Server Address

SMTP User Name

SMTP Password

Email Subject

Email Content

Email Test

Test

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

FTP Notification Setting

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.

Navigate to the web **Setting > Action** interface.

FTP Notification

FTP Server	
FTP User Name	
FTP Password	
FTP Test	FTP Test

- **FTP Path:** The folder name you created in the FTP server.

SIP Call Notification

You can enter the SIP number to receive the notification.

SIP Call Notification

SIP Call Number	
SIP Caller Name	

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	\$relay1 status	Http://server ip/ relaytrigger=\$relay1 status
4	Relay Closed	\$relay1 status	Http://server ip/ relayclose=\$relay1 status
5	Input Triggered	\$input1 status	Http://server ip/ inputtrigger=\$input1 status
6	Input Closed	\$input1 status	Http://server ip/ inputclose=\$input1 status
7	Valid Code Entered	\$code	Http://server ip/ validcode=\$code
8	Invalid Code Entered	\$code	Http://server ip/ invalidcode=\$code
9	Valid Card Entered	\$card_sn	Http://server ip/ validcard=\$card_sn
10	Invalid Card Entered	\$card_sn	Http://server ip/ invalidcard=\$card_sn
11	Tamper Alarm Triggered	\$alarm status	Http://server ip/tampertrigger=\$alarm status

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

[mac=\\$mac:ip=\\$ip:model=\\$model:firmware=\\$firmware:card_sn=\\$card_sn](http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

Navigate to the web **Setting > Action URL** interface.

Action URL

Enabled

☐

Make Call

Hang Up

RelayA Triggered

RelayB Triggered

RelayA Closed

RelayB Closed

InputA Triggered

InputB Triggered

InputC Triggered

InputD Triggered

InputA Closed

InputB Closed

InputC Closed

InputD Closed

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

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.

Navigate to the web **System > Security** interface.

Session Time Out

Session Time Out Value

300

(60~14400Sec)

- **Session Time Out Value:** The automatic web interface log-out time ranges from 60 seconds to 14400 seconds. The default value is 300.

Low Power Mode

It displays the device's power mode. When the device is powered by POE, it displays POE+Mode. When it is powered by the 12-volt power supply, it displays Low Power Mode.

To see the power mode on the **System > Security > Low Power Mode Warning** interface.

Low Power Mode Warning

Enabled



Power Mode

POE+ Mode

Logs

Call Logs

If you want to check on the calls inclusive of the dial-out calls, received calls, and missed calls in a certain period of time, you can check and search the call log on the device web interface and export the call log from the device if needed.

Navigate to the web **Status > Call Log** interface.

Call Log

Save Call Log Enabled ☒

All ▾

Start Time ~ End Time

Name/Number

Search

Export ▾

☐	Index	Type	Date	Time	Local Identity	Name	Number
No Data							

Selected:0/0

Delete

Delete All

Total:0

Prev

1/1

Next

Go To Page

1

Go

- **All:** Four types of call history are available: All, Dialed, Received, and Missed.
- **Start Time-End Time:** The specific time of the call logs you want to search, check, or export.
- **Name/Number:** Search the call log by the name or by the SIP or IP number.
- **Export:** Call logs can be exported in .csv format.

Door Logs

If you want to search and check on the various types of door access history, you can search and check the door logs on the device's web.

Navigate to the web **Status > Access Log** interface.

Access Log

Save Access Log Enabled ☒

~

☐	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status
☐	1	1	Judy	123456	A	PIN	2023-12-12	09:34:31	Success
☐	2	--	Visitor	123456	--	PIN	2023-12-12	09:34:13	Failed

Selected:0/2

 Total:2

 1/1

 Go To Page

- **All:** Three types of access logs are available, All, Success, and Failed.
- **Start Time-End Time:** The specific time of the call logs you want to search, check, or export.
- **Name/Code:** Search the door log by the name or by the PIN code.
- **Export:** Door logs can be exported in .csv or .xml format.

Backup

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

Navigate to the web **System > Maintenance** interface.

Others

Config File

 Import

 Export

(Encrypted)

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Navigate to the web **System > Maintenance** interface.

System Log

Log Level	3 ▼
Export Log	Export
Remote System Log Enabled	☐
Remote System Server	

- **Log Level:** The log level ranges 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:** The remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.

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.

Navigate to the web **System > Maintenance** interface.

Remote Debug Server

Enabled ☐

Connect Status

Disconnected

IP

- **IP:** The remote debug server IP.

PCAP for Debugging

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

Navigate to the web **System > Maintenance** interface.

PCAP

Specific Port

 (1~65535)

PCAP

Start

Stop

Export

PCAP Auto Refresh Enabled

☐

- **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:** When enabled, the PCAP will continue to capture data packets even after the data packets reach its 1M maximum capacity. When disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capacity of 1MB.

Ping

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

Navigate to the web **System > Maintenance > Ping** interface.

Ping

Cloud Server

U Cloud ▼

Verify the network address accessibility

All ▼

Ping

Stop

You can enter the domain name or IP you want to detect in the drop-down box.

- **Cloud Server:** The server to be verified.
- **Verify the network address accessibility:** The service type.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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

Basic

Firmware Version	532.30.1.19
Hardware Version	532.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

UpgradeX

(Format: .rom)

No file selected

Select File

 Reset

☐ Reset After Upgrade

Cancel

Install

Note

Firmware files should be in .rom format for upgrade.

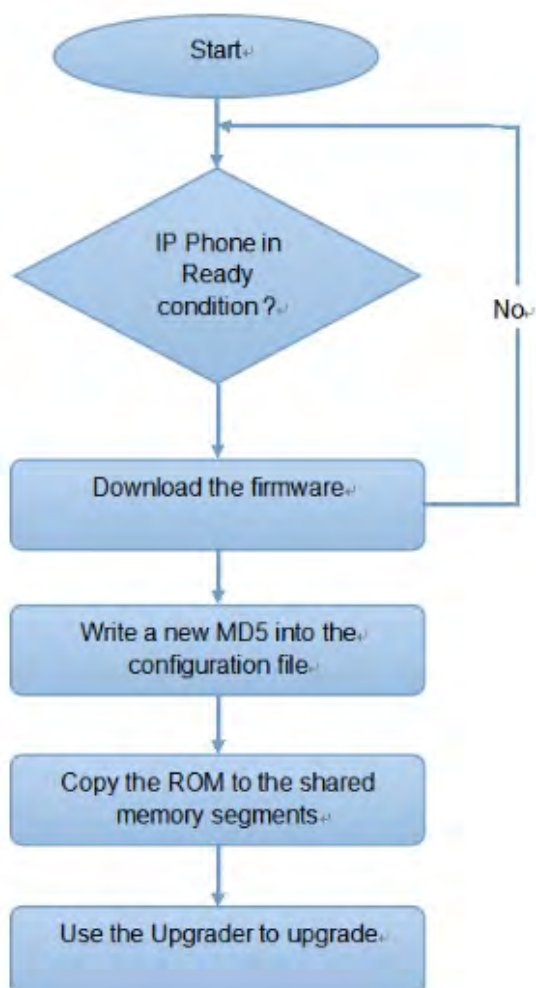
Auto-provisioning via Configuration File

You can configure and upgrade the door phone on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

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 have two formats for auto-provisioning. One is the general configuration files used for the general provisioning and the other one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown below:

- **General configuration provisioning:** a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files are used for auto-provisioning on a specific device, as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

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 configure it, navigate to the web **System > Auto Provisioning > Automatic AutoP** interface.

Automatic AutoP

Mode	Power On ▼
Schedule	Sunday ▼
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	 Clear
Export AutoP Template	 Export

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

Static Provisioning Configuration

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

Download the Autop template on the **System > Auto Provisioning > Automatic Autop**, and set up the Autop server on the **System > Auto Provisioning > Manual Autop** interface.

Automatic AutoP

Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

Manual AutoP

URL	
Username	
Password	
Common AES Key	
AES Key(MAC)	
	AutoP Immediately

- **URL:** The TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username:** Set up a username if the server needs a username to be accessed.
- **Password:** Set up a password if the server needs a password to be accessed.
- **Common AES Key:** Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key(MAC):** Set up the AES code for the intercom to decipher the MAC-based auto-provisioning configuration file.

Note

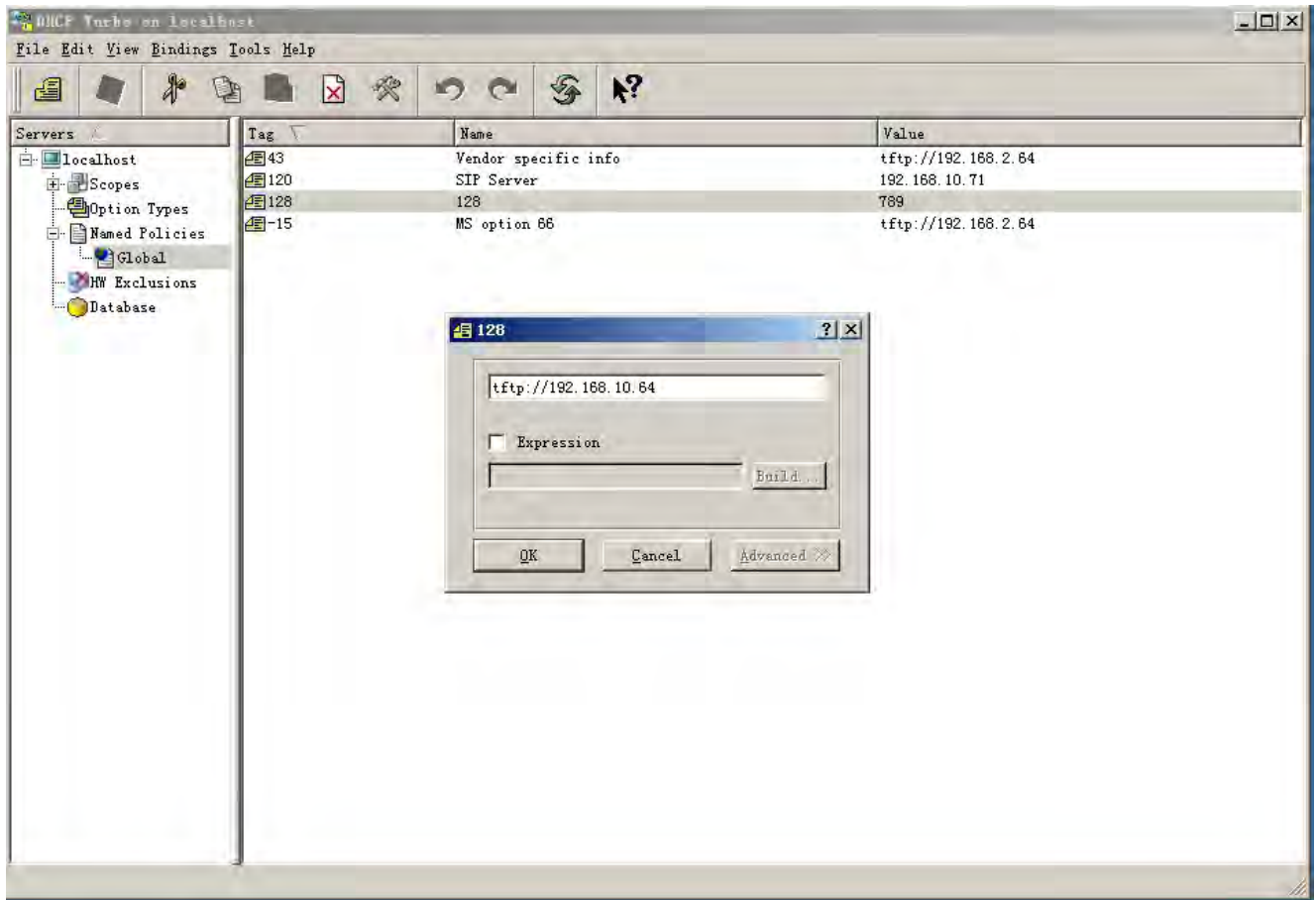
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning Configuration

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 TFTP server.

To set up DHCP Autop with Power On mode and export Autop Template to edit the configuration on the same interface, navigate to the web **System > Auto Provisioning** interface.

Automatic AutoP

Mode	Power On ▼
Schedule	Sunday ▼
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

Then, set up the DHCP Option.

DHCP Option

Enabled



Custom Option

(128~254)

(DHCP option 66/43 is enabled by default)

- **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.

Note

The general configuration file for the in-batch provisioning is with the format `cfg` taking R29 as an example, `r000000000029.cfg` (10 zeros in total while the MAC-based configuration file for the specific device provisioning is with the format `MAC_Address` of the device. `cfg`, for example, `0C110504AE5B.cfg`.

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.

To configure PNP, navigate to the web **System > Auto Provisioning > PNP Option** interface.

PNP Option

PNP Config Enabled



Integration with Third Party Device

Integration via Wiegand

You can integrate the device with Wiegand.

Navigate to the web **Device > Wiegand** interface.

Wiegand

Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	Auto
Wiegand Transfer Mode	Input ▼
Wiegand Input Data Order	Normal ▼
Wiegand Open Relay	☐ RelayA ☐ RelayB

- **Wiegand Display Mode:** Select Wiegand Card code format among 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.
- **Wiegand Card Reader Mode:** The transmission format should be identical between the door phone and the device to be integrated. It is automatically configured.
- **Wiegand Transfer Mode:** There are three options, Input, Output, and Convert to Card No.Output Wiegand. If the door phone is used as a receiver, then set it as **Input**. Select **Output** if you want to make the door phone the sender. Select **Convert to Card No.Output Wiegand** if you want Wiegand output to be converted to a card number before sending it from the door phone to a receiver.
- **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 and vice versa.
- **Wiegand Open Relay:** The relay to be triggered.

Integration via HTTP API

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

To configure HTTP API, navigate to the web **Setting > HTTP API** interface.

HTTP API

Enabled	☒
Authorization Mode	Digest ▼
Username	admin
Password	
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

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

Please refer to the following description for the Authentication mode:

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

Power Output Control

The device can serve as a power supply for the external relays.

To configure it, navigate to the web **Access Control > Relay** interface.

12V Power Output

Relay ID

Relay A

12V Power Output

Disabled

▼

?

- **12V Power Output:** when **Always** is selected, the device can provide continuous power to the third-party device. When **Triggered By Open Relay** is selected, the device can 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. When **Security Relay A** is selected, the device can work with the security relay.

Lift Control

The door phones can be connected to the Akuvox lift controller for the lift control. You can summon the lift to go down to the ground floor when you are granted access through various types of access methods on the door phone.

To configure it, navigate to the web **Device > Lift Control** interface.

Lift Control List

Lift Control List

Akuvox ▼

General Setting

Server 1 IP (Unlock)

Port

Server 2 IP (Execute)

Port

Action Setting

Username

admin

Password

.....

Floor No. Parameter

\$floor

URL To Trigger Specific Floor

/cdor.cgi?open=0&door=\$floor

URL To Trigger All Floors

/cdor.cgi?open=8

URL To Close All Floors

/cdor.cgi?open=9

Floor Starts From

1 ▼

Device Location

None ▼

- **Lift Control List:** Select None to disable the function, and select Akuvox to integrate the door phone with the Akuvox controller.
- **Server 1 IP(Unlock):** The IP address of the Akuvox lift control server. It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute):** The IP address of the server that triggers lift control.
- **Port:** The server port of the lift controller server.

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

Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature.

To enable it on the web **Surveillance > ONVIF > Advanced Setting** interface.

Advanced Setting

Milestone Enable

Disabled ▼

Password Modification

Accounts Management

You can add administrator and user accounts and configure their passwords for logging into the device web interface.

Navigate to the web **System > Security > Account Management** interface. Click +Add to create an account.

Account Management

+ Add

Index	Type	Username	Access Rights	Action
1	Admin	admin	Full Access	Delete

Modify Device Web Interface Password

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

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

Web Password Modify

Username

admin

Change Password

Change Password

×

The password must be at least eight characters long containing at least one uppercase letter, one lowercase letter and one number.

Username

admin

Current Password

New Password

Confirm Password

Cancel

Change

Modify System Password

The system PIN code is used to access the device system. You can modify the system PIN code on the device and web interface.

Press *2396# on the device keypad and press 2 to enter the **Admin Code Setting** screen.

Navigate to the web **System > Security > Admin Code Setting** interface.

Admin Code Setting

Admin Code

2396

Modify Setting Password

The setting PIN code is used to access the settings that include public PIN, private PIN, and user card code modification. You can modify the setting PIN code on the device.

Press *2396# on the device keypad and press 2 and then 3 to enter the **Service Code Setting** screen.

System Reboot & Reset

Reboot

To reboot the device on the web **System > Upgrade** interface.

Basic

Firmware Version	532.30.1.19
Hardware Version	532.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

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

Reboot Schedule

Enabled	☒
Schedule	Every Day ▼ 0 (0~23Hour)

Reset

Reset on the Web Interface

You can select **Reset To Factory Setting** if you want to reset the device (deleting both configuration data and user data such as RF cards, face data, and so on). Or, select **Reset Configuration to Default State (Except Data) Reset**, if you want to reset the device (retaining the user data).

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

Basic

Firmware Version	532.30.1.19
Hardware Version	532.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

Reset on the Device

Press *2396# on the device keypad and press 3 and 2 to enter the restore screen. Then, swipe the admin card or enter the admin code to reset the device. The default code is 2396.



FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.