

Table of contents

Akuvox A15 Access Control Terminal Administrator Guide

About This Manual	9
Product Overview	11
Model Specification	12
Access the Device	13
Initial Setup	13
Access the Device Settings	15
Access the Device's Web Settings	16
Search for Your Desired Settings	20
Introduction to the Configuration Menu	21
Language and Time	23
Language	23
Custom Language	23
Time	24
Volume and Tone	26
Volume Control	26
Voice Prompts Upload	27

Ringback Tone Setting	29
LED Settings	30
Infrared LED Setting	30
LED White Light	31
Screen Display	33
Home Screen Display	33
In Default Theme	33
In Multi-factor Authentication Mode	35
Configure Screensaver	37
Upload Screensaver	39
Open Door Text Prompt Display	41
Unlock Options Display	41
Network Settings	43
Device Deployment in Network	45
NAT Setting	46
Device Web HTTP Setting	47
Device Local RTP Configuration	47
SNMP Setting	48
Intercom Call Configuration	49
IP Call Configuration	49

SIP Call Configuration	49
SIP Account Registration	50
SIP Server Configuration	51
SIP Account Selection	52
Outbound Proxy Server	52
Data Transmission Type	53
SIP Hacking Prevention	54
Call Settings	55
Call Auto-answer	55
Group Call	56
Sequence Call	56
Maximum Dial Duration	58
Maximum Call Duration	58
Hang up After Opening Doors	59
Video Transport Type	60
Audio & Video Codec Configuration	61
Audio Codec	61
Video Codec	62
Video Codec for IP Calls	62
Relay Settings	64

Local Relay	64
Security Relay	66
Web Relay	68
Access Control Schedule Management	71
Create Door Access Schedule	71
Import and Export Door Access Schedule	72
Relay Schedule	72
Holiday Schedule	73
Holiday Schedule Import/Export	75
Door-opening Configuration	76
Unlock by Public PIN Code	76
User-specific Access Methods	76
Unlock by Private PIN	77
Unlock by QR Code	77
Unlock by RF Card	79
Unlock by License Plate	80
Unlock by Facial Recognition	81
Unlock by Bluetooth	83
Access Setting	84
Import/Export User Data	86

Unlock by NFC	86
Mifare Card	87
Unlock by DTMF Code	88
DTMF White List	89
DTMF Data Transmission	89
Unlock by HTTP Commands	91
Unlock by Exit Button	92
Monitor and Image	94
MJPEG Image Capturing	94
RTSP Stream Monitoring	96
RTSP Stream Setting	96
ONVIF	98
Live Stream	99
Camera Mode	99
Data Transmission Type for Third-party Camera	100
Security	102
Tamper Alarm	102
Disarm Setting	103
Account Management	104
Client Certificate Setting	106

Web Server Certificate	106
Client Certificate	106
Motion Detection	108
Security Notification	109
Email Notification	110
FTP Notification	111
SIP Call Notification	111
Action URL	112
Voice Encryption	115
User Agent	116
Real-Time Monitoring	116
Emergency Action	117
Web Interface Automatic Log-out	117
High Security Mode	117
Logs	120
Call Logs	120
Door Logs	120
Event Logs	121
Integration with Third-Party Device	123
Integration via Wiegand	123

Integration via HTTP API	125
Power Output Control	127
Integration via RS485	128
Integration with Third-party Access Control Server	130
Lift Control	134
Firmware Upgrade	136
Auto-provisioning via Configuration File	137
Provisioning Principle	137
Configuration Files for Auto-provisioning	138
AutoP Schedule	139
Static Provisioning	139
DHCP Provisioning	141
PNP Configuration	143
Debug	145
System Log for Debugging	145
PCAP for Debugging	145
Remote Debug Server	146
Ping	147
Web Call	147
Backup	148

Password Modification	149
Modify Web Interface Password	149
Modify Security Questions	149
Modify Administrator Credentials	150
System Reboot & Reset	152
Reboot	152
Reset	153

About This Manual



WWW.AKUVOX.COM

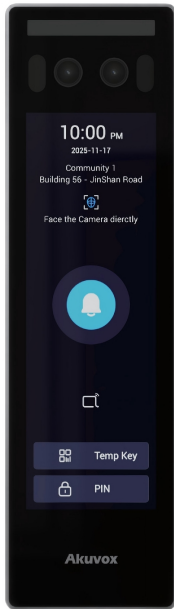


AKUVOX A15 ACCESS CONTROL

Administrator Guide

Thank you for choosing the Akuvox A15 access control device. This manual is intended for administrators who need to properly configure the device. This manual applies to version 1115.30.10.408, and it provides all the configurations for the functions and features of the A15. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



Akuvox A15S is an ultra-slim access control device that integrates a door controller and card reader into one compact device, helping reduce installation complexity and overall deployment costs. Designed for space-constrained access control scenarios, it provides a convenient solution for managing entry access.

Supporting multiple authentication methods, including face recognition, PIN codes, QR codes, Bluetooth, NFC, and RFID cards, A15S offers flexible and secure access options to meet different user requirements.

Model Specification

Model	A15
Touch Screen	✓
Relay Port	x2
Input Port	x4
Power Supply	PoE or 12VDC 2A
Power Output	12VDC 0.5A(max.) if PoE+ input 12VDC 1A(max.) if DC input
Wiegand	✓
RS485	✓
Power Output	✓
Reset Button	✓
Bluetooth	✓
Wi-Fi	X
Microphone	x1
Speaker	x1

Access the Device

Access the device's system settings either on the device or on its interface.

Initial Setup

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

During the initial setup, you will be guided to select the device language, set up admin credentials(PIN and/or card), and select the time zone.

The admin credentials are used to access the device's system settings. Select at least one method and configure it.

- **PIN:** 6 to 8 digits.

<

Step 1/2

Set Administrator Credentials

Set up at least one method (one or both):

• Password

• Card



PIN



Card

Next

<

Admin PIN

* Admin PIN

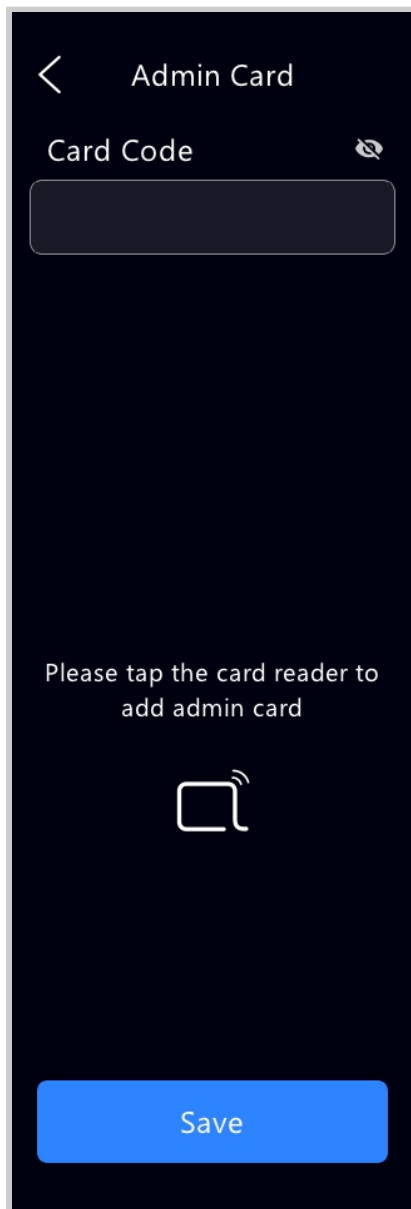
* Confirm PIN

Please enter the confirm PIN.

Save

www.akuvox.com

14

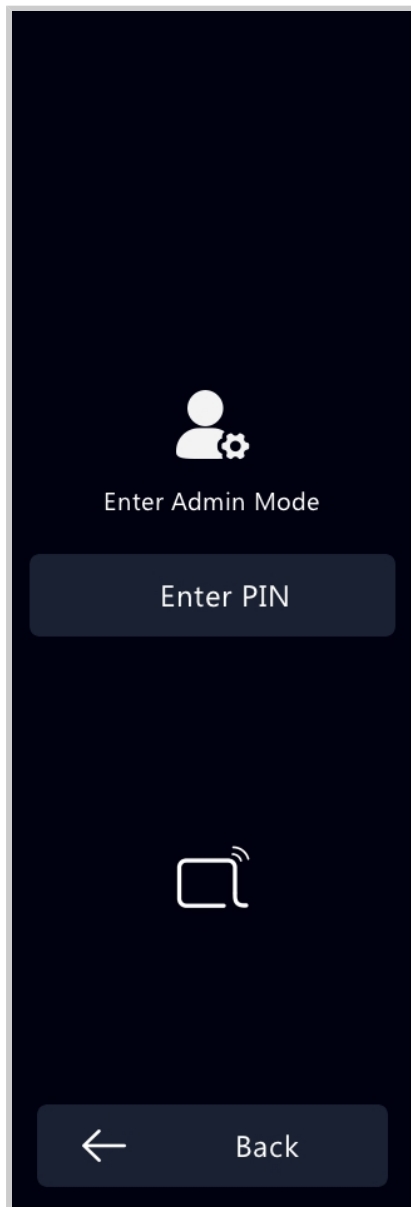


Tip

See the [Password Modification](#) chapter for modifying admin credentials.

Access the Device Settings

Long-press on any spot of the home screen for approximately five seconds, then enter the admin PIN or swipe the admin card.



Access the Device's Web Settings

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



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

<

System Info

Basic

Network

DHCP Mode

DHCP >

IP

192.168.31.197

Subnet Mask

255.255.255.0

Gateway

192.168.31.1

Preferred DNS Server

192.168.31.1

Alternative DNS Server

Note

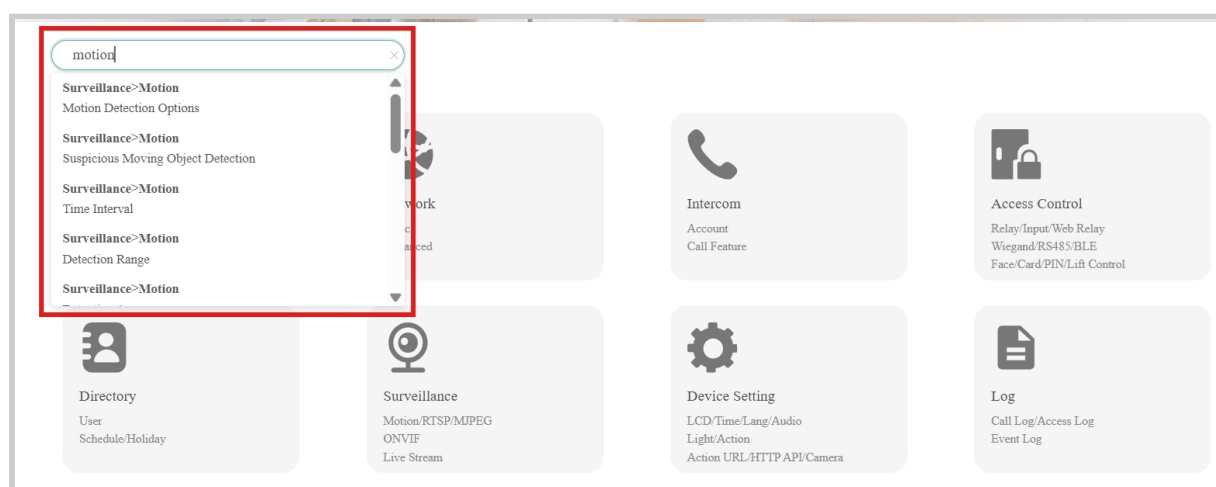
- Download IP scanner:
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- See the detailed guide:
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Google Chrome browser is strongly recommended.
- The initial username and password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

Search for Your Desired Settings

The device supports searching for features on its web interface.

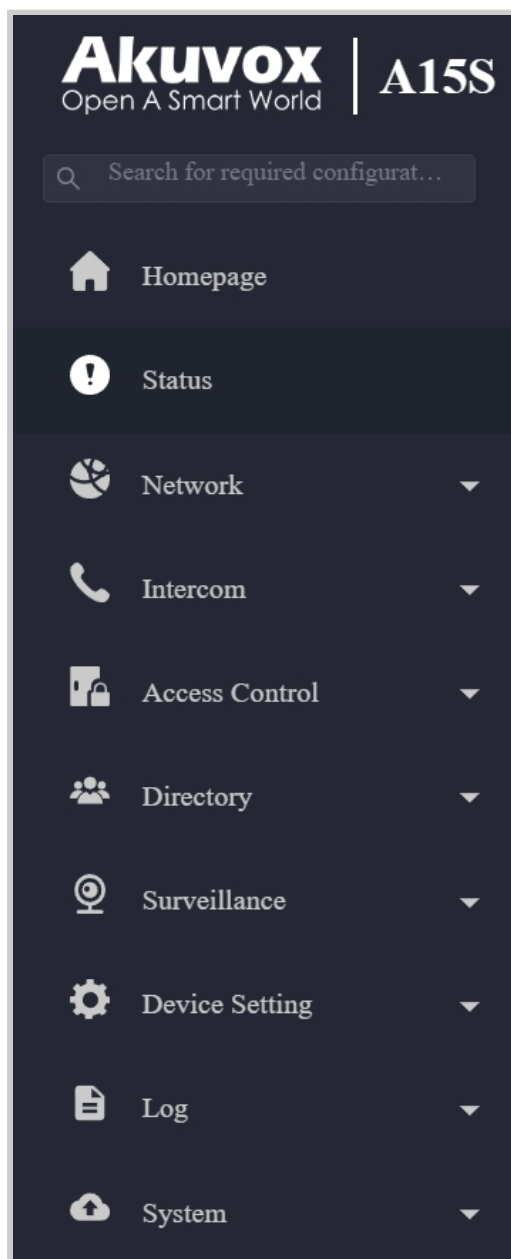
For example, if you want to search for motion detection, enter the value in the search box.

Then, select the desired option to redirect to the configuration interface.



Introduction to the Configuration Menu

- **Status:** This section gives you basic information, such as product information, network information, account information, etc.
- **Network:** This section mainly deals with DHCP & Static IP settings, RTP port settings, device deployment, etc.
- **Intercom:** This section concerns the account settings and call features.
- **Access Control:** This section covers input control, relay, card settings, facial recognition, private PIN codes, Wiegand connection, etc.
- **Directory:** This section involves user management.
- **Surveillance:** This section covers motion detection, RTSP, MJPEG, ONVIF, live stream, etc.
- **Device Setting:** This section includes light settings, tab and button display, LCD settings, and audio settings.
- **Log:** This section includes call logs, access logs, and event logs.
- **System:** This section includes firmware upgrade, automatic auto-provisioning, device maintenance, etc.



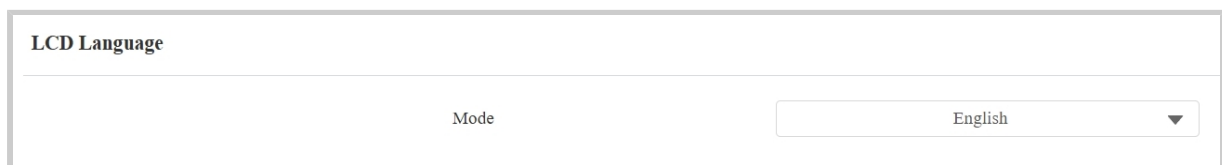
Language and Time

Language

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

The device's LCD supports the following languages:

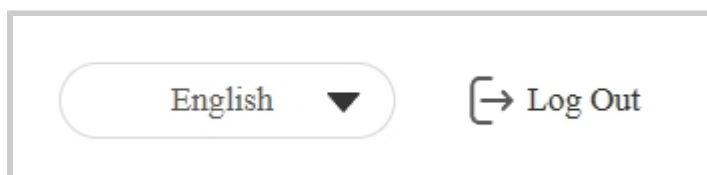
- English, Simplified Chinese, Traditional Chinese, Czech, Portuguese, Spanish, Italian, Dutch, French, German, Hebrew, Polish, and Arabic.



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

The device web supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Czech, Portuguese, Spanish, Italian, Dutch, French, German, Hebrew, Polish, and Arabic.



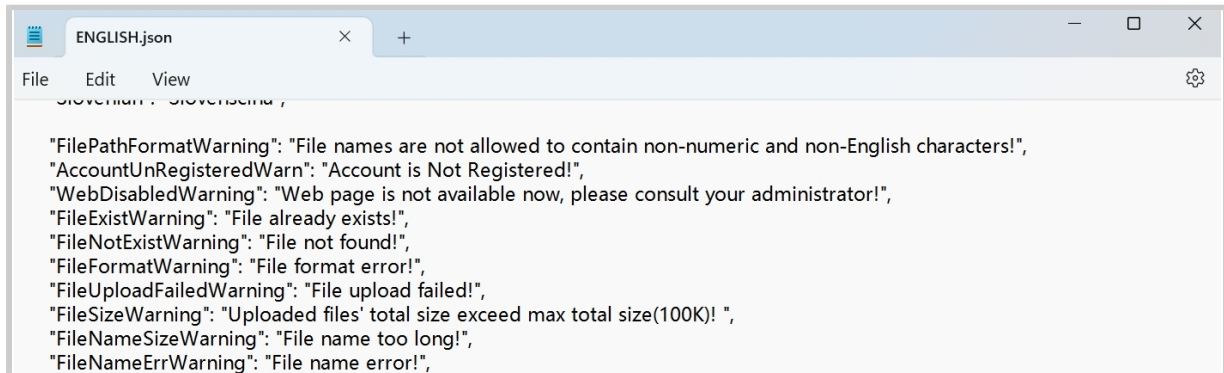
Custom Language

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

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

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

File Example:



Set it up on the **Device Setting > Time/Lang > Custom Language** 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

Time

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

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

Time	
Automatic Date&Time	☒
Time Zone	GMT+0:00 GMT ▼
Date Format	2026-07-03 ▼
Time Format	24 Hour ▼
NTP Server	0.pool.ntp.org
Update Interval	3600 (≥3600Sec)
System Time	02:52:17

- **Automatic Date&Time:** The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **NTP Server:** The NTP server address for updating the time. The default NTP server address is 0.pool.ntp.org.
- **Update Interval:** Set the time update interval. For example, if you set it to 3600 seconds, the device will send a request to the NTP server for the time update every 3600 seconds.
- **System Time:** Display the current device time.

Volume and Tone

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

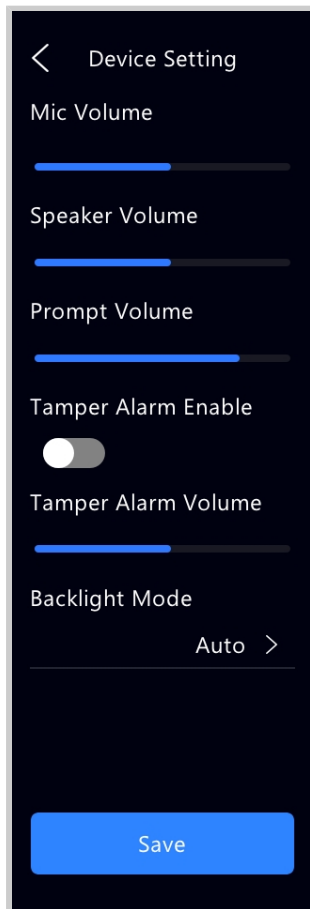
Volume Control

Set up volumes on the **Device Setting > Audio** interface. Click **Test** to play the audio at the current volume.

Volume Control			
Mic Volume	8	(1~15)	
Speaker Volume	8	(1~15)	<button>Test</button>
Tamper Alarm Volume	8	(1~15)	<button>Test</button>
Prompt Volume	12	(0~15)	<button>Test</button>
Key Pressed Volume	8	(0~15)	<button>Test</button>

- **Mic Volume:** The microphone volume. The default is 8.
- **Speaker Volume:** The speaker volume. The default is 8.
- **Tamper Alarm Volume:** Set the volume when the tamper alarm is triggered. The default is 8.
- **Prompt Volume:** Various prompts, including door-opening success and failure prompts. The default is 12.
- **Key Pressed Volume:** The icon tapping sound. The default is 8.

You can also adjust volumes on the **Setting > Device Setting** screen.



Voice Prompts Upload

You can customize and upload various voice prompts to the device.

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

ID	Tone	Import	Reset	Play	Enabled
1	Greetings	Import	Reset	Play	☒
2	Relay A - Access Granted	Import	Reset	Play	☒
3	Relay B - Access Granted	Import	Reset	Play	☒
4	Input A - Access Granted	Import	Reset	Play	☒
5	Input B - Access Granted	Import	Reset	Play	☒
6	Input C - Access Granted	Import	Reset	Play	☒
7	Input D - Access Granted	Import	Reset	Play	☒
8	Access Denied	Import	Reset	Play	☒
9	Close Door	Import	Reset	Play	☒
10	Pin Page	Import	Reset	Play	☒
11	APT+PIN	Import	Reset	Play	☒
12	Calling	Import	Reset	Play	☒
13	QR Code	Import	Reset	Play	☒

- **Access Granted(Input):** The tone is played when the door is opened by pressing an exit button connected to the device's input.
- **Close Door:** The door-closing tone works for relay(s) set to **Bistable** mode.
- **PIN Page:** The tone is played when entering the PIN screen.
- **APT+PIN:** The tone is played when entering the Apartment number and PIN code for door access.
- **Calling:** The tone is played when entering the Call screen.
- **QR Code:** The tone is played when entering the temporary QR code scanning screen.

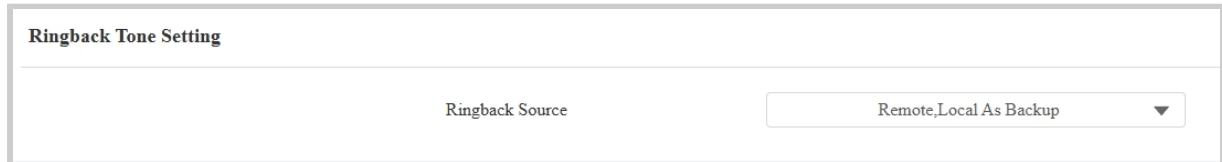
Note

File Format: wav; Size: < 200KB; Sample Rate: 16000; Bit Depth: 16 Bits.

Ringback Tone Setting

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

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



Ringback Tone Setting

Ringback Source

Remote, Local As Backup ▼

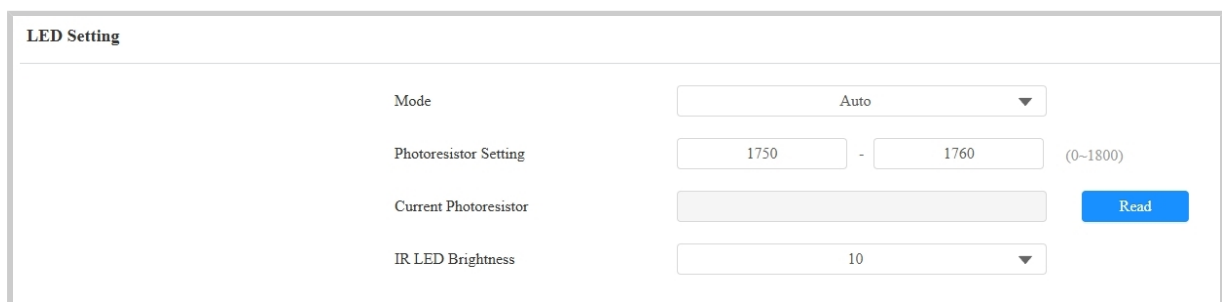
- **Ringback Source:**
 - **Remote, Local As Backup:** The local ringtone will be played.
 - When the device calls another device, for example, an Akuvox indoor monitor, and the SIP server returns non-183, the indoor monitor will not have any intercom preview.
 - If the SIP server returns 183, the indoor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

LED Settings

Infrared LED Setting

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

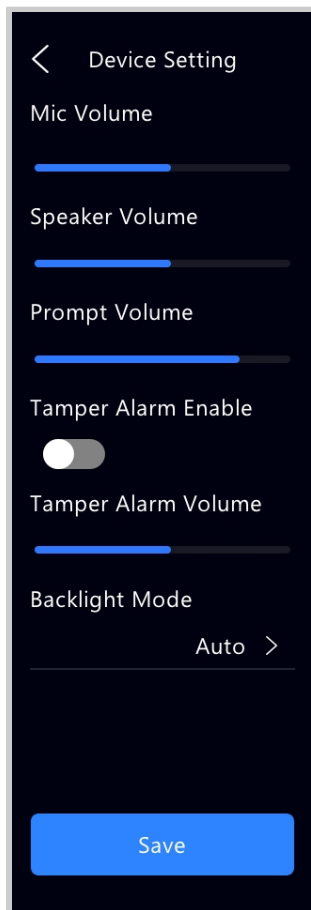
Set it up on the web **Device Setting > Light** interface.



The screenshot shows the 'LED Setting' web interface. It contains four rows of settings: 'Mode' with a dropdown menu set to 'Auto'; 'Photoresistor Setting' with two input fields containing '1750' and '1760', separated by a hyphen, with '(0-1800)' to the right; 'Current Photoresistor' with a greyed-out input field and a blue 'Read' button to its right; and 'IR LED Brightness' with a dropdown menu set to '10'.

- **Mode:**
 - **Auto:** Turn on the infrared LED automatically based on the minimum and maximum photoresistor value.
 - **Always On:** Enable the infrared LED.
 - **Always Off:** Disable the infrared LED.
 - **Schedule:** Turn on the infrared LED based on the schedule. Specify the Start Time and End Time when this option is selected. Beyond the schedule, the device adopts Auto mode.
- **Photoresistor Setting:** Set the minimum and maximum photoresistor value to automatically control the ON-OFF of the LED fill light. The higher the value, the brighter the light is. If the photoresistor value is less than the minimum threshold, turn on the fill light. If it is greater than the maximum threshold, turn it off.
- **Current Photoresistor:** Click **Read** to obtain the current photoresistor value.
- **IR LED Brightness:** Adjust the IR LED brightness from level 0 to 10. The default is 10. The higher the level is, the brighter it is.

You can also select the Backlight Mode on the **Setting > Device Setting** screen.



LED White Light

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

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

White Light	
Mode	Auto ▼
Max White Light Value	3 ▼
<button>Test</button>	

- **Mode:** Select **Auto** or **OFF**. If you select **Auto**, the white light will turn on only when all conditions are met: face recognition or QR code scanning is in progress, night mode is detected, and motion is detected by radar.
- **Max White Light Value:** Set brightness level. Higher values increase brightness. Clicking **Test** turns on the light at the current level for 3 seconds.

Screen Display

Home Screen Display

The device supports the **Default** and **Multi-factor Authentication** modes. To change the mode, go to **Device Setting > LCD > Theme** interface.

Preview

Home Page

Screensaver

Homepage Interface

Theme

Default

☒ Speed Dial

Change Reset

Access Methods

☒ Face
 ☒ RF Card
 ☒ PIN
 ☒ Temp Key

PIN

Change Reset

Button Name

PIN

PIN Display Mode ?

Normal

Temp Key

Change Reset

In Default Theme

You can upload custom icon images or restore the default icons for **Speed Dial**, **Temp Key**, and **PIN** at any time.

Click **Change** to upload and click **Reset** to restore.

Preview

Home Page

Screensaver



Homepage Interface

Theme

Default

☒ Speed Dial



Change

Reset

Access Methods

☒ Face
 ☒ RF Card
 ☒ PIN
 ☒ Temp Key

PIN



Change

Reset

Button Name

PIN

PIN Display Mode ?

Normal

Temp Key



Change

Reset

Button Name

Temp Key

☒ Background



Change

Reset

- **Icon Change:** Max file size: 200KB; Format: .jpg,.png,.bmp,.jpeg; Recommended resolution for Speed Dial icon: 120x120; for other icons: 80x80.

- **Speed Dial:** Enable/disable the **Speed Dial** icon on the home screen for making calls. See the [Call Settings](#) chapter for the speed dial number configuration.
- **Access Methods:** Specify which access methods are available on the home screen. When an access method is disabled, its icon is hidden, and the corresponding authentication method becomes unavailable.
- **PIN:**
 - **Button Name:** Customize the button name if needed. The name does not change the button attribute.
 - **PIN Display Mode:** Available when the PIN access method is enabled.
 - **Normal:** Digits are displayed in standard order.
 - **Disorder:** Digits are displayed in a random order.
- **Temp Key:**
 - **Button Name:** Customize the button name if needed. The name does not change the button attribute.
- **Background:** Customize the home screen background. The background image is visible when **Face** authentication is disabled on the home screen.
 - Max size: 200KB; Format: .jpg,.png,.bmp,.jpeg; Recommended resolution: 320x960.

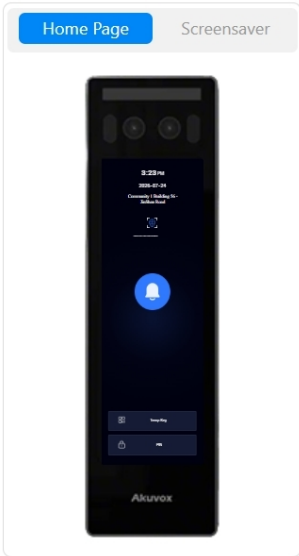
In Multi-factor Authentication Mode

In this mode, only the selected authentication methods are displayed on the home screen. Authentication options and related settings are automatically adjusted according to the selected mode.

For **Speed Dial** and **Temp Key** tabs, you can upload custom icon images or restore the default icons at any time.

Preview

Home Page Screensaver



Homepage Interface

Theme

Multi-factor Authentication ▼

☒ **Speed Dial**



[Change](#)
[Reset](#)

Authentication Mode

Face+PIN ▼

☐ **Entry Restriction**

PIN



[Change](#)
[Reset](#)

Button Name

PIN

PIN Display Mode ?

Normal ▼

Temp Key



[Change](#)
[Reset](#)

Button Name

Temp Key

☒ **Background**



[Change](#)
[Reset](#)

- **Icon Change:** Max file size: 200KB; Format: .jpg,.png,.bmp,.jpeg; Recommended resolution for Speed Dial icon: 120x120; for other icons: 80x80.

- **Speed Dial:** Enable/disable the **Speed Dial** icon on the home screen for making calls. See the [Call Settings](#) chapter for the speed dial number configuration.
- **Authentication Mode:** Select the two-factor authentication method: Face + PIN, Face + RF Card, or RF Card + PIN. The first authentication method must be completed successfully before proceeding to the second one.
- **Entry Restriction:** Enable or disable repeated access restrictions for the same user.
When enabled, a user must wait for the configured restriction period before unlocking the door again. This restriction applies only to the same user. Other authorized users can still unlock the door normally.
- **PIN:**
 - **Button Name:** Customize the button name if needed. The name does not change the button attribute.
 - **PIN Display Mode:** Available when the PIN access method is enabled.
 - **Normal:** Digits are displayed in standard order.
 - **Disorder:** Digits are displayed in a random order.
- **Temp Key:**
 - **Button Name:** Customize the button name if needed. The name does not change the button attribute.
- **Background:** Customize the home screen background. The background image is visible when **Face** authentication is disabled on the home screen.
 - Max size: 200KB; Format: .jpg,.png,.bmp,.jpeg; Recommended resolution: 320x960.

Configure Screensaver

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

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

Standby Interface

Screensaver

✓

Akuvox

Open A Smart World

✕

Akuvox

Open A Smart World

✕

Akuvox

Open A Smart World

✕

Akuvox

Open A Smart World

✕

✕

Screensaver Interval(Sec)

5 Seconds

Screensaver Time

30 Seconds

Sleep

15 Seconds

Wake Up Mode

Auto

Schedule

1001:Always ✕

- **Standby Interface:** Set whether to enable the screensaver.
- **Screensaver Interval(Sec):** The interval of switching between screensavers(1 to 120 seconds). The default is 5 seconds.
- **Screensaver Time:** Set the screensaver duration time(5 seconds to 30 minutes, or Forever).
- **Sleep:** The time to start the screensaver mode(5 seconds to 30 minutes). The default is 15 seconds. For example, if it is set to 15 seconds, the device will go into screensaver mode when it detects no operation or no approaching object for 15 consecutive seconds. When screensaver mode is disabled, the device screen will be turned off directly in 15 seconds.

- **Wake Up Mode:**
 - **Auto:** The screen will be woken up when someone approaches without it being touched.
 - **Schedule:** Select the schedule when the screen can be woken up automatically. Outside the time, it needs to be woken up manually. Configure the schedule on the **Directory > Schedule** interface.
 - **Manual:** Users need to touch and wake up the screen.

Upload Screensaver

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

Set it up on the web **Device > LCD** interface. Click the add icon **+**.

Standby Interface

Screensaver

✓

✕

✕

✕

✕

Screensaver Interval(Sec)

5 Seconds

Screensaver Time

30 Seconds

Sleep

15 Seconds

Wake Up Mode

Auto

Schedule

1001:Always ✕

Note

- Uploaded images should be in JPG format with no more than 2M pixels.
- The recommended resolution is 320×960.
- If the uploaded image duplicates an existing image ID, the existing image will be overwritten.

Open Door Text Prompt Display

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

To set it up, navigate to the **Access Control > Relay > Open Door Text Prompt** interface.

Open Door Text Prompt	
Open Door Outside Succeeded Text Prompt	☒
Open Door Inside Succeeded Text Prompt	☒
Open Door Failed Text Prompt	☒
Display User Info	☒

- **Open Door Outside Succeeded Text Prompt:** Display a text prompt after the door is opened by the device-supported access methods except for the exit button. The default prompt is "Access Granted". You can customize the prompt with a maximum of 63 characters.
- **Open Door Inside Succeeded Text Prompt:** Display a text prompt after the door is opened by pressing an exit button(the input is triggered). The default prompt is "Access Granted". You can customize the prompt with a maximum of 63 characters.
- **Open Door Failed Text Prompt:** Display a text prompt after opening the door fails. The default prompt is "Access Denied". You can customize the prompt with a maximum of 63 characters.
- **Display User Info:** Display the user information after facial recognition or RF card swiping. For example, if facial recognition succeeds, the text prompt "Access Granted" with the user ID and name will pop up on the device screen. If it fails, the text prompt "Access Denied" will be displayed.

Unlock Options Display

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

Click [here](#) to view the feature details.

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

Unlock Options	
Unlock Options	Visible ▼

Network Settings

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

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

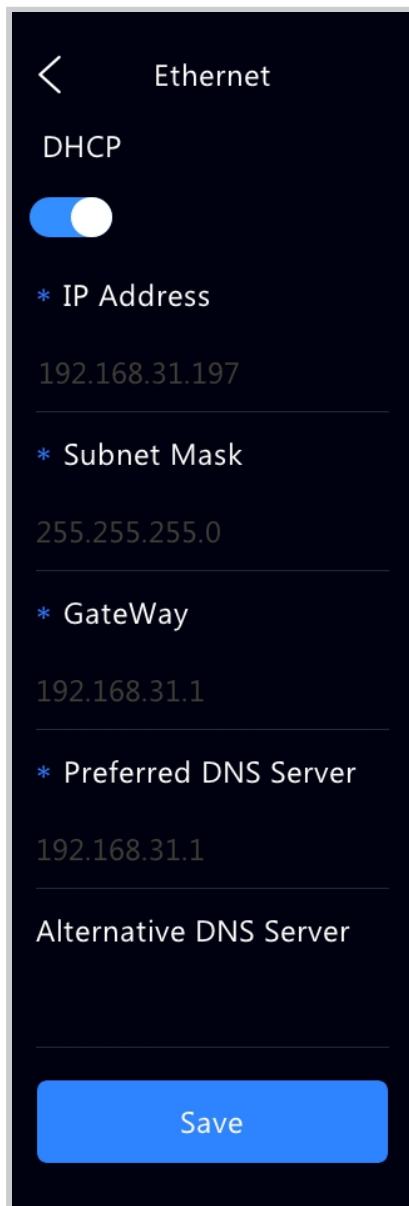
The screenshot shows the 'LAN Port' configuration page. At the top, there's a title 'LAN Port'. Below it, the 'Network Mode' is set to 'Static IP' (indicated by a blue dot), with 'DHCP' as an unselected option. Below the mode selection, there are six input fields for network configuration:

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

- **Preferred/Alternative DNS Server:** Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The device connects to the alternate DNS server when the primary one is unavailable.

You can also set up the network on the **Settings> Ethernet** 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 > Connect Setting** interface.

Connect Setting					
Connect Type	None				
Device Address	1	1	1	1	1
Device Extension	1				
Device Location	Access Control				

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

- **Device Extension:** Available for the None server mode. The device extension number ranges from 0 to 10.
- **Device Location:** The location where the device is installed and used.

NAT Setting

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

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

To enable NAT, go to **Intercom > Account > NAT** interface.

NAT	
STUN Enabled	☐
STUN Server IP	
Port	3478 (1024~65535)
UDP Keep Alive Messages	☒
UDP Alive Messages Interval	30 (5~60Sec)
RPort	☐

- **STUN Server IP:** Enter the server address when the device is in a Wide Area Network(WAN).
- **Port:** The server port.
- **UDP Keep Alive Messages:** If enabled, the device will send the message to the SIP server, which will recognize whether the device is online.
- **UDP Alive Messages Interval:** Set the message-sending interval from 5-60 seconds. The default is 30 seconds.
- **RPort:** Enable the RPort when the SIP server is in a WAN.

Device Web HTTP Setting

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

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

Web Server		
Protocol	☒ HTTP	☒ HTTPS
HTTP Port	80	(80,1024~65535)
HTTPS Port	443	(443,1024~65535)

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

Device Local RTP Configuration

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

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

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

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

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

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

SNMP Setting

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

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

SNMP	
Enabled	☐
Port	(1024–65535)
Trusted IP	

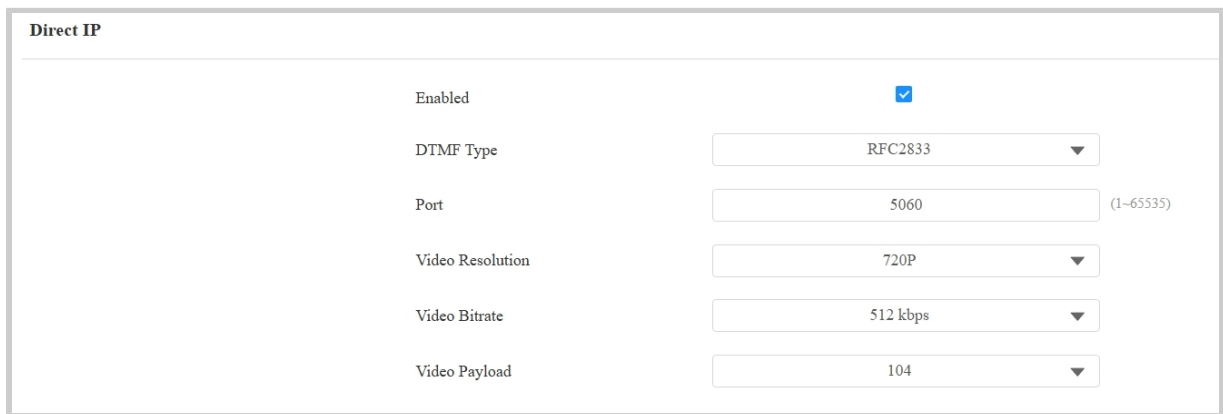
- **Port:** Set a specific port for the data transmission from 1024-65535.
- **Trusted IP:** The allowed SNMP server address. It can be an IP address or any valid URL domain name.

Intercom Call Configuration

IP Call Configuration

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

Enable or disable the direct IP call function on the **Intercom > Call Feature > Direct IP** interface.



Direct IP	
Enabled	☒
DTMF Type	RFC2833
Port	5060 (1-65535)
Video Resolution	720P
Video Bitrate	512 kbps
Video Payload	104

- **Port:** Set the port for direct IP calls. The default is 5060, with a range from 1-65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

SIP Call Configuration

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

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

SIP Account Registration

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

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

Click [here](#) to view the SIP account registration example.

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

The screenshot shows the 'Intercom > Account' interface. At the top, there are two tabs: 'Account1' (selected) and 'Account2'. Below the tabs, the title 'SIP Account' is displayed. The interface contains a table with two columns: 'Status' and 'Disabled'. The 'Status' column has a row for 'Account Enabled' with a checkbox. The 'Disabled' column has a row for 'Disabled' with a checkbox. Below the table, there are six input fields: 'Display Label', 'Display Name', 'Register Name', 'Username', and 'Password' (masked with asterisks).

Status	Disabled
Account Enabled	☐
Display Label	
Display Name	
Register Name	
Username	
Password	

- **Account 1/Account 2:** The device 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.
- **Status:** Indicate whether the SIP account is registered or not.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 is to be shown on the calling device's screen.
- **Register Name:** Same as the username from the PBX server.

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

Note

- To add the device to the cloud, select its **Device Type** as **Door Phone**. Selecting **Access Control** will disable all the device's intercom features.
- When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

SIP Server Configuration

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

To set it up, go to the web **Intercom > Account** 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)

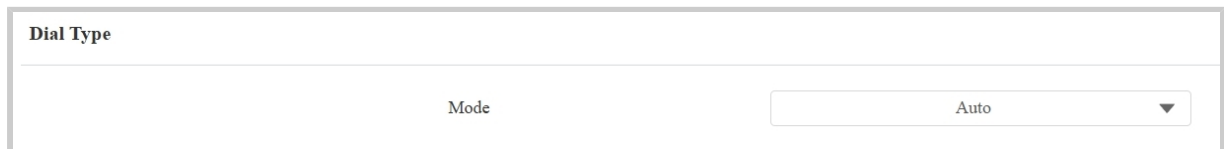
- **Server IP:** Enter the server's IP address or its domain name.
- **Port:** Specify the SIP server port for data transmission.

- **Registration Period:** Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified period.

SIP Account Selection

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

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



The screenshot shows a web interface titled "Dial Type". Below the title is a horizontal bar with the label "Mode" on the left and a dropdown menu on the right. The dropdown menu is currently set to "Auto" and has a downward arrow icon.

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

Outbound Proxy Server

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

To set it up, go to the **Intercom > Account > 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 server's 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 server malfunctions.
- **Port:** Set the proxy port for establishing a call session via the backup outbound proxy server.

Data Transmission Type

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

Select the data transmission type on the **Intercom > Account > Transport Type** interface.

Transport Type

Type

UDP ▼

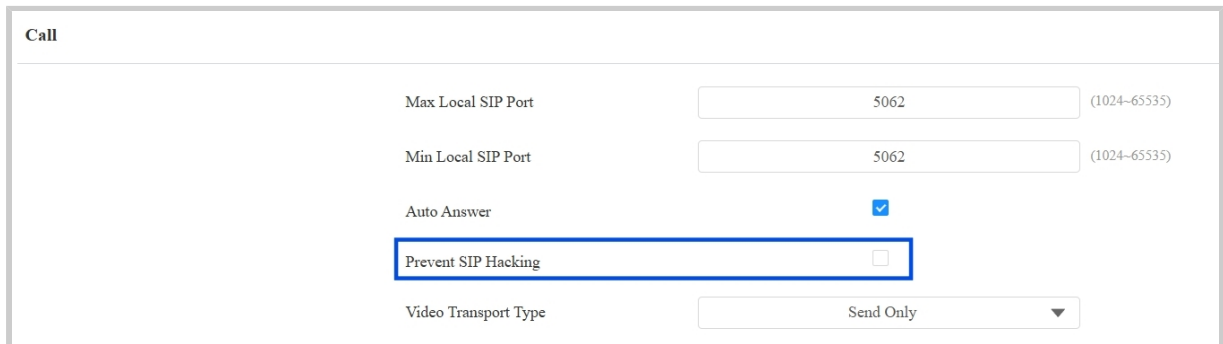
- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

- **DNS-SRV:** A DNS service record defines the location of servers. This record includes the hostname and port number of the server, as well as the priority and weight values that determine the order and frequency of using the server.

SIP Hacking Prevention

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.

Enable SIP hacking prevention on the **Intercom > Account > Call** interface.



Call	
Max Local SIP Port	5062 (1024-65535)
Min Local SIP Port	5062 (1024-65535)
Auto Answer	☒
Prevent SIP Hacking	☐
Video Transport Type	Send Only ▼

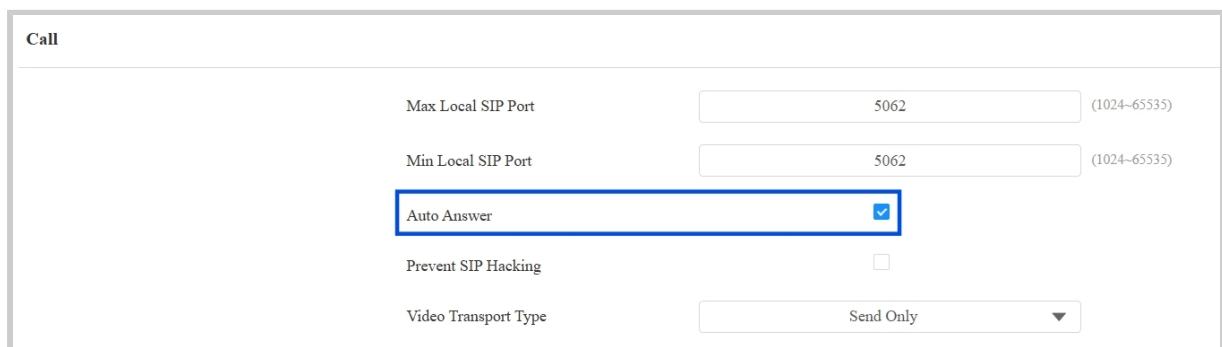
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Settings

Call Auto-answer

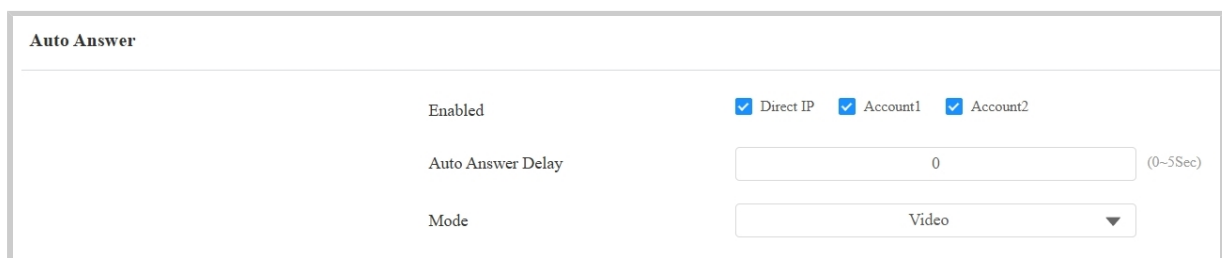
Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To enable the call auto-answer feature, go to the **Intercom > Account** interface.



Call	
Max Local SIP Port	5062 (1024-65535)
Min Local SIP Port	5062 (1024-65535)
Auto Answer	☒
Prevent SIP Hacking	☐
Video Transport Type	Send Only ▼

To set it up, go to the **Intercom > Call Feature > Auto Answer** 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 device will answer the call automatically after 5 seconds.
- **Mode:** Determine whether to auto-answer the call as a video or audio call.

Group Call

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

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

The screenshot shows the 'Speed Dial' configuration window. It contains the following fields:

- Call Type:** A dropdown menu with 'Group Call' selected.
- When Refused:** A dropdown menu with 'End This Call Only' selected.
- Label:** A text input field containing 'Reception'.
- Group Call Number (Local):** A 4x4 grid of 16 small input boxes for entering phone numbers.

- **Call Type:** Select Group Call.
- **When Refused:**
 - **End All Calls:** The device will stop calling.
 - **End This Call Only:** The device will continue to call the next number.
- **Label:** The text displayed on the device screen when the device calls the destination numbers. The default is "Reception".
- **Group Call Number(Local):** Enter the target numbers.

Sequence Call

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

You can also set up the local sequence call numbers on the **Intercom > Call Feature** interface.

Speed Dial

Call Type	Sequence Call ▼
Time Out (Sec)	20 ▼
When Refused	Do Not Call Next ▼
Label	Reception
Sequence Call Number	
Sequence Call Number 1	
Sequence Call Number 2	
Sequence Call Number 3	
Sequence Call Number 4	
Sequence Call Number 5	
Sequence Call Number 6	
Sequence Call Number 7	
Sequence Call Number 8	
Sequence Call Number 9	
Sequence Call Number 10	

- **Call Type:** Select Sequence Call.
- **Timeout(Sec):** Determine the duration before calling the next number when the previous call is not answered.
- **When Refused:** Determine whether to call the next if a call was rejected by the previously called party.
 - **Do Not Call Next:** The sequence call will stop when the call is refused.
 - **Call Next:** The device will call the next number in order when the call is refused.
- **Label:** The text displayed on the device screen when the device calls the destination numbers. The default is "Reception".
- **Sequence Call Number:** Enter the target numbers.

Maximum Dial Duration

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

To set it up, go to the **Intercom > Call Feature > Max Dial Time** 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 device 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 device will automatically end the call it dialed out if there is no answer from the recipient within the preset time.

Note

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

Maximum Call Duration

The device allows you to set up the call time duration for 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 device will terminate the call automatically.

To set it up, go to the **Intercom > Call Feature > Max Call Time** 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 device will end the call automatically when the time limit is reached.

Note

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

Hang up After Opening Doors

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

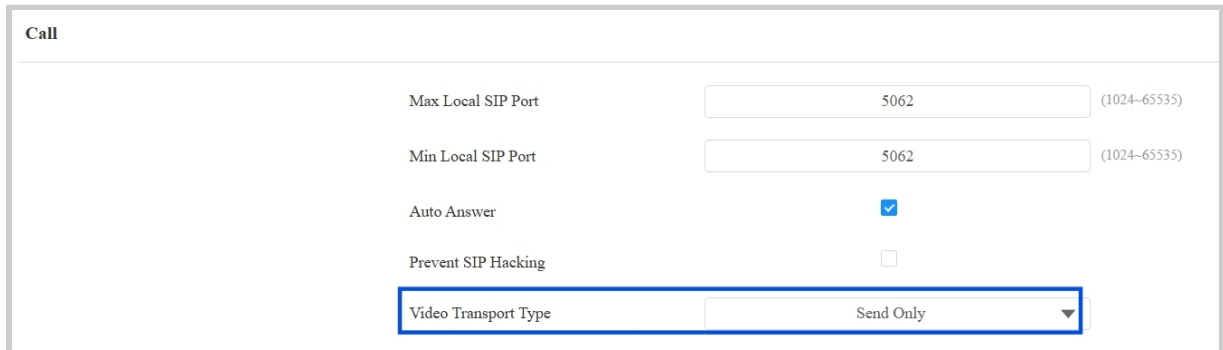
To set it up, go to the **Intercom > Call Feature > Hang Up After Open Door** interface.

Hang Up After Opening Door	
Enabled	☒
Type	Only DTMF ▼
Time Out (Sec)	5 (0~15Sec)

- **Type:** Specify the door-opening method. If this specific method is used to release the door during a call, the device will end the call when the preset hang-up time is reached.
- **Timeout(Sec):** Specify the hang-up time limit. The device will automatically terminate the call when the specific time is reached after the door is opened.

Video Transport Type

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



Call

Max Local SIP Port	5062	(1024-65535)
Min Local SIP Port	5062	(1024-65535)
Auto Answer	☒	
Prevent SIP Hacking	☐	
Video Transport Type	Send Only	

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

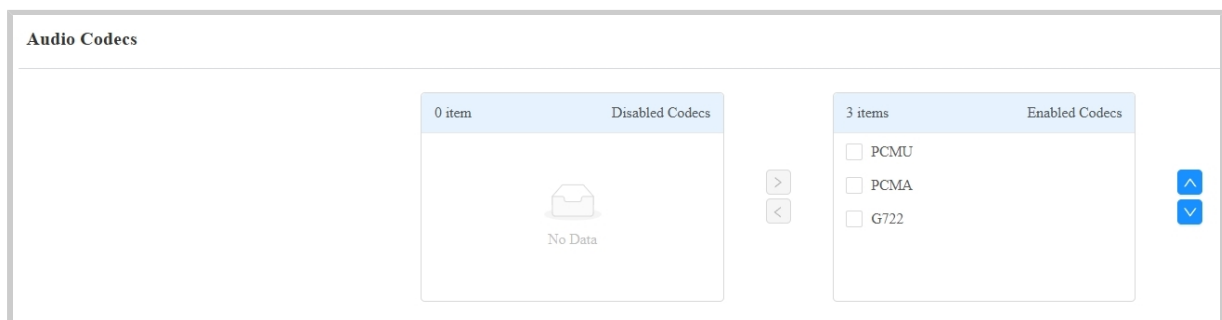
Audio & Video Codec Configuration

Audio Codec

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

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

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



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

Video Codec

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

Set it up on the web **Intercom > Account** interface.

Video Codec	
Name	☒ H.264
Resolution	720P ▼
Bitrate	320 kbps ▼
Payload	104 ▼

- **Name:** Check to enable the H264 video codec format for the device video stream.
- **Resolution:** Select the resolution from the provided options. The default resolution is 720P(1280×720 pixels).
- **Bitrate:** The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data is transmitted every second, and the clearer the video will be. The default code bitrate is 320.
- **Payload:** The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for IP Calls

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

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

Direct IP	
Enabled	☒
DTMF Type	RFC2833
Port	5060 (1-65535)
Video Resolution	720P
Video Bitrate	512 kbps
Video Payload	104

- **Video Resolution:** Select the resolution from the provided options. The default resolution is 720P(1280×720 pixels).
- **Video Bitrate:** The video stream bitrate ranges from 128 to 2048 kbps. The default bitrate is 512.
- **Video Payload:** The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Relay Settings

Local Relay

A local relay is the relay output built into the intercom device. It can directly control connected devices, such as door locks, by triggering actions based on user input or authorization.

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

Relay ID	RelayA	RelayB
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 Digit DTMF	0 ▼	1 ▼
2~4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	RelayA	RelayB
Door Sensor	None ▼	None ▼ ?
Alarm Door Opened	☐	☐ ?
Door Opened Timeout	60	60 (1~300Sec)
Break-in intrusion	☐	☐ ?
Access Method	☒ PIN ☒ Face ☒ RF Card ☒ BLE ☒ NFC ☒ LPR Camera	☒ PIN ☒ Face ☒ RF Card ☒ BLE ☒ NFC ☒ LPR Camera
	Test	Test

- **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 open.
 - **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 open for 5 seconds before closing.
- **DTMF Mode:** Set the digits of the DTMF code.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **2~4 Digits DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status:** Indicate the states of the relay, which are normally open and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name:** Assign a distinct name for identification purposes.
- **Door Sensor:** Specify which input interface is connected to a door sensor.
- **Alarm Door Opened:** If enabled, when the door-opening time exceeds a limit, an alarm will be triggered.
 - **Door Opened Timeout:** The door-opening time limit.
- **Break-in Intrusion:** Activate an alarm when the door is forcibly or illegally opened. Click [here](#) to learn more about this feature.
- **Access Method:** Check the method(s) to trigger the relay.

- **Test:** Click **Test** to trigger the relay manually.

Security Relay

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



Click [here](#) to view how to set up the security relay.

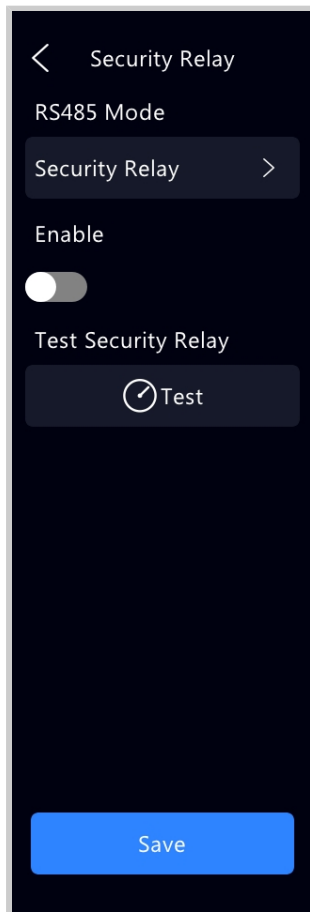
To set up the security relay, go to **Access Control > Relay > Security Relay** interface.

Security Relay

Relay ID	Security Relay		
Connect Type	RS485 ▼		
Trigger Delay(Sec)	0 ▼		
Hold Delay(Sec)	5 ▼		
1 Digit DTMF	2 ▼		
2~4 Digits DTMF	012		
Relay Name	Security Relay		
Access Method	☒ PIN ☒ BLE	☒ Face ☒ NFC	☒ RF Card ☒ LPR Camera
Enabled	☐		
Test			

- **Connect Type:** The connection type is RS485 by default. To use SR01, the RS485 mode should be set to **Security Relay** on the **Access Control > RS485** interface.
- **Trigger Delay(Sec):** Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open for 5 seconds before closing.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name:** Name the security relay. The name can be displayed in the door-opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Access Method:** Check the access method that can trigger the security relay.
- **Test:** Click to send the signal to the SR01. When the device and SR01 are pairing, click **Test** to finish the matching.

You can also enable the security relay on the **Setting > Security > Security Relay** screen.



Web Relay

A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.



Click [here](#) to view how to set up web relay.

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

Web Relay

Type

Disabled ▼

Authorization Mode

None ▼

IP Address

Username

Password

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
01			
02			
03			
04			
05			
06			

- **Type:** Determine the type of relay activated when employing door access methods for entry.
 - **Disabled:** Only activate the local relay.
 - **Only Web Relay:** Only activate the web relay.

- **Both Local Relay and Web Relay:** Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay.
- **IP Address:** The web relay IP address provided by the web relay manufacturer.
- **Username:** The username provided by the web relay manufacturer.
- **Password:** The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.
- **Web Relay Action:** Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

NOTE

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

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

Access Control Schedule Management

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

Create Door Access Schedule

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

Set it up on the web **Directory > Schedule** interface. You can add 100 local schedules.

The screenshot shows the 'Schedule' management interface. At the top, there are buttons for 'Search', '+ Add', 'Import', and 'Export'. Below these is a table with the following columns: Index, Schedule ID, Source, Mode, Name, Date, Day of Week, Time, and Edit. The table contains two rows of data:

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	

Below the table, there are buttons for 'Delete' and 'Delete All', a 'Total: 2' indicator, and pagination controls including 'Prev', '1/1', 'Next', 'Go To Page 1', and a 'Go' button.

The screenshot shows the 'Add Schedule' modal form overlaid on the 'Schedule' interface. The modal has a title bar with a close button. The form contains the following fields and options:

- Mode:** A dropdown menu set to 'Normal'.
- Name:** A text input field.
- Start Date - End Date:** A date range selector showing '2026/03 ~ 2026/03'.
- Day:** A section with checkboxes for days of the week: Mon, Tue, Wed, Thur, Fri, Sat, Sun. There is also a 'Check All' checkbox.
- Start Time - End Time:** A time range selector showing '00:00 - 23:59'.
- Holiday Exemption:** A checkbox.

At the bottom of the modal are 'Cancel' and 'Submit' buttons.

- **Mode:**

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

Import and Export Door Access Schedule

In addition to creating door access a schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency.

To set it up, go to the **Directory > Schedule** interface. The import file should be in **XML** format.

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	

Relay Schedule

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

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

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

Note

Click [here](#) to view the detailed configuration of each schedule mode.

Holiday Schedule

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

Set it up on the **Directory > Holiday** interface. You can choose to view the local holidays, SmartPlus Cloud holidays, or both.

Click **+Add** to set up a local holiday schedule.

Holiday

All
Search
+ Add
Import
Export

	Index	Source	Name	Repeat By Year	Edit
No Data					

Selected: 0/0
Delete
Delete All
Total: 0
Prev
1/1
Next
Go To Page: 1
Go

Calendar

Holiday Name
Repeat By Year
Year: 2026
Working Hours
Clear

January

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

February

Mo	Tu	We	Th	Fr	Sa	Su
					1	
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	
2	3	4	5	6	7	8

March

Mo	Tu	We	Th	Fr	Sa	Su
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

April

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

May

Mo	Tu	We	Th	Fr	Sa	Su
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

June

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

July

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

August

Mo	Tu	We	Th	Fr	Sa	Su
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

September

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

October

Mo	Tu	We	Th	Fr	Sa	Su
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

November

Mo	Tu	We	Th	Fr	Sa	Su
					1	
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

December

Mo	Tu	We	Th	Fr	Sa	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

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

Holiday Schedule Import/Export

You can import or export holiday schedules for quick setup on the **Directory > Holiday > Import/Export Holiday** interface.

The import/export file format is .xml.

Holiday

All

Search

+ Add

Import

Export

☐	Index	Source	Name	Repeat By Year	Edit
No Data					

Selected:0/0

Delete

Delete All

Total:0

Prev

1/1

Next

Go To Page 1

Go

Door-opening Configuration

Unlock by Public PIN Code

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.

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

Public Key	
Enabled	☒
PIN Code	***** (5~8 digits)

- **PIN Code:** Set 5 to 8 digits for opening doors. The default is 33333333.

User-specific Access Methods

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

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

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

User Basic	
User ID	1
Name	

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

Unlock by Private PIN

Users can open doors by entering their private PINs on the keypad.

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

Private PIN	
Code	

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

You can enable/disable the use of the private PIN code on the web **Access Control > PIN Setting > Private PIN** interface. It is enabled by default.

Private PIN	
Enabled	☒

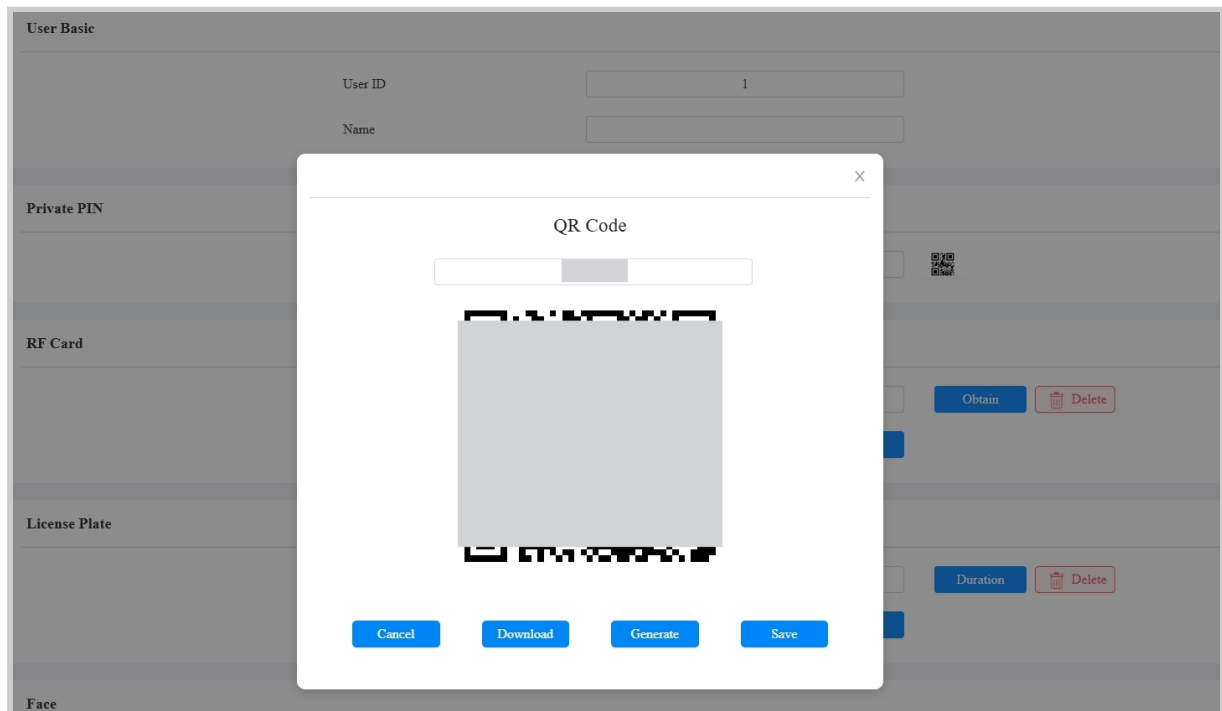
Unlock by QR Code

The device supports scanning on-premise-generated and [SmartPlus Cloud-generated QR codes](#).

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

Private PIN	
Code	

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



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

You enable or disable the use of QR code on the **Access Control > Relay > Open Relay Methods** interface.

It is enabled by default.

Relay Methods

Via HTTP
Enabled
☐

Via QR Code
Enabled
☒

Via DTMF
Enabled
☒

Assigned The Authority For

Only Contacts List

Unlock by RF Card

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

RF Card

Code

Obtain

Delete

Add

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

Note:

- Each user can have a maximum of 5 cards added.
- The device allows adding 5,000 users.
- RF cards operating at 13.56 MHz frequencies are compatible with the device for access.

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

Card Type

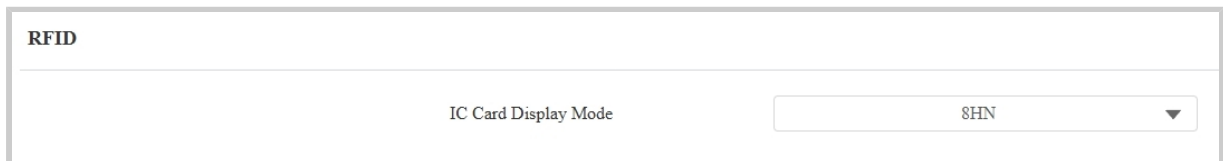
Enabled

☒ IC Card
☒ NFC

RF Card Code Format

To integrate the RF card door access with the third-party intercom system, you need to match the RF card code format with the one used by the third-party system.

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



The screenshot shows the 'RFID' interface. At the top, there is a header 'RFID'. Below it, there is a label 'IC Card Display Mode' and a dropdown menu. The dropdown menu is currently set to 'SHN'.

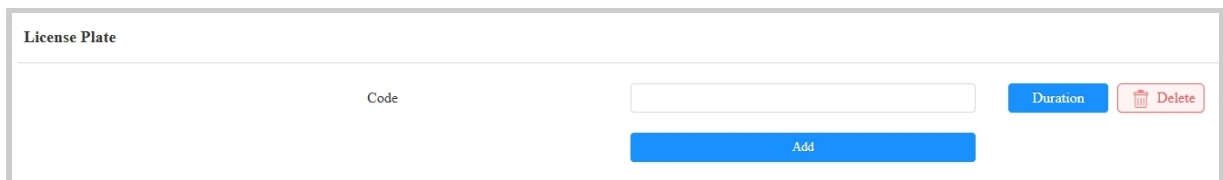
- **IC Card Display Mode:** Set the card number format from the provided options.

Unlock by License Plate

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

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

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



The screenshot shows the 'License Plate' interface. At the top, there is a header 'License Plate'. Below it, there is a label 'Code' and an input field. To the right of the input field, there are two buttons: 'Duration' and 'Delete'. Below the input field, there is a blue 'Add' button.

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

Unlock by Facial Recognition

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

- **Import:** Click to upload the face picture.
- **Obtain:** Click to start enrolling a face on the device side.
- **Reset:** Click to remove the registered face image.

Note

Support Format: jpg, png. Size: a maximum of 2 MB.

Facial Recognition Settings

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

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

- **Facial Recognition Enabled:** Enable/disable the facial recognition function.
- **Offline Learning Enabled:** Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level:** Determine how strict the facial recognition system is in comparing a person's face with uploaded face data. Each level allows a different degree of difference or face covering (**excluding the mouth area**) to pass the recognition.
 - Low: Allow slight differences from the uploaded face data, with little face coverage.
 - Highest: Require the face to be identical to the uploaded one, with minimal or no covering.
 - The other two levels are in between.
- **Anti-Spoofing Option:** Set how strict the system is in preventing fake faces.
 - Close: Disable the facial anti-spoofing function. Facial verification can be passed using non-living substitutes for an authorized person's face, such as a photo.
 - Highest: The system cannot be fooled by any non-living substitutes for an authorized person's face.
 - The other three levels are in between.
- **Facial Recognition Interval(Sec):** Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.
- **Visitor Friendly Mode:** Set whether to give auditory or visual prompts when recognition fails. Disabled by default.
- **No Face Detected Interval(Sec):** Adjust the time interval between each detection, ranging from 1 to 8 seconds.
- **Face Detection Distance(M):** Adjust the detection distance, ranging from 1 to 3 meters.

Unlock by Bluetooth

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

Note

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

Unlock via My MobileKey

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

BLE Setting	
Authentication Code	Generate Delete
Status	Unpaired
Pairing Valid Until	N/A

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

Bluetooth Unlock Settings

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

BLE Basic

Enable BLE Function

☒

Enable Hands Free Mode

☒

RSSI Threshold

(-85~-50db)

Unlock Interval For Same User (Sec)

(5~900Sec) ?

Unlock Interval For Different Users (Sec)

(5~900Sec) ?

- **Enable Hands Free Mode:** If enabled, users can gain door access hands-free. If disabled, users have to wave their hands near the device to open doors.
- **RSSI Threshold:** Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Unlock Interval For Same User(Sec):** Set the time interval between consecutive Bluetooth door access attempts for the same user.
- **Unlock Interval For Different Users(Sec):** Set the time interval between consecutive Bluetooth door access attempts for different users.

Note

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

- [Unlock by Bluetooth via My MobileKey App.](#)
- [Unlock by Bluetooth via SmartPlus App.](#)

Access Setting

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

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

The screenshot shows the 'Access Setting' configuration page. It features several toggle and selection options: 'Allow To Open' is set to 'Relay A', 'First Credential In' is set to 'Relay A', 'LockDown ByPass' is disabled, 'Floor No.' is set to 'None', and 'Web Relay' is set to '0'. At the bottom, there are two panels for managing schedules. The 'Unselected Schedules' panel lists '1002:Never', while the 'Selected Schedules' panel lists '1001:Always'. Arrows indicate the ability to move schedules between these panels.

- **Allow To Open:** Enable the door to be opened.
- **First Credential In:** This decides whether the user can keep the door open during **the scheduled time** after activating it.
- **Lockdown Bypass:** This decides whether the user can open the door when the door is locked during **the scheduled time**.
- **Floor No. :** Specify the accessible floor(s) to the user via the elevator.
- **Web Relay:** Specify the ID of the web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **Schedule:** Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:
 - **Always:** Allows door opening without limitations on door open counts during the valid period.
 - **Never:** Prohibits door opening.

Import/Export User Data

The device supports access control user data being shared among Akuvox devices through import and export.

Click [here](#) to view how to import and export user data between Akuvox devices.

To set it up, go to the **Directory > User** interface. The device supports up to 5,000 users.

Import/Export User	
User Data	Import Export ▼

- **Import:** The supported format is TGZ.
- **Export:** The supported format is CSV or XML.

Unlock by NFC

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

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

Card Type	
Enabled	☒ IC Card ☒ NFC

Note

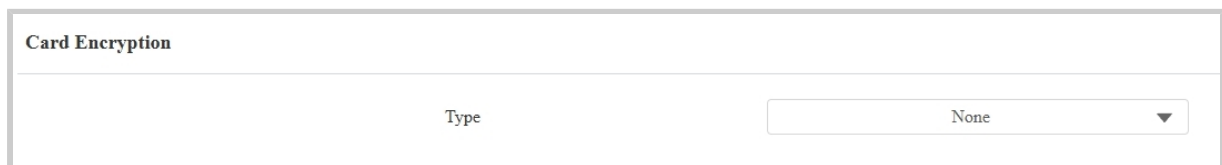
- The NFC feature is not available on iPhones.
- Click [here](#) to view how to open doors via NFC.

Mifare Card

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

Click [here](#) to view the details of encrypting and reading Mifare cards.

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



The screenshot shows a web interface titled "Card Encryption". Below the title is a form with a label "Type" and a dropdown menu. The dropdown menu is currently set to "None" and has a downward arrow icon.

- **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.
- **Plus:** You can set up three choices. This means you can use three types of Mifare Plus cards. When swiping a card, as long as one of the choices matches its SL key, the card code in the block you specified will be output.
 - **Block:** Specify the block(s) to be read.
 - **SL1:** The key number within 32 bits.
 - **SL3:** The key number within 32 bits.
- **DESFire:**
 - **App ID:** A 6-digit hexadecimal number
 - **File ID:** The ID of the encrypted file of the app, which can be a number from 0 to 16.
 - **Crypto:** The encryption method.
 - **Key:** The file key.

- **Key Index:** The index number for the key, which can be a number from 0 to 11.

Unlock by DTMF Code

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

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

Relay ID	RelayA	RelayB
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 Digit DTMF	0 ▼	1 ▼
2-4 Digits DTMF	010	012
Relay Status	Relay A: Low	Relay B: Low
Relay Name	RelayA	RelayB
Door Sensor	None ▼	None ▼
Alarm Door Opened	☐	☐
Door Opened Timeout	60	60 (1~300Sec)
Break-in intrusion	☐	☐

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

Note

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

DTMF White List

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

The screenshot shows the 'Relay Methods' configuration page. It contains three main sections, each with a title, a status, and a checkbox:

- Via HTTP**: Status is 'Enabled', checkbox is unchecked.
- Via QR Code**: Status is 'Enabled', checkbox is checked.
- Via DTMF**: Status is 'Enabled', checkbox is checked. Below this, there is a label 'Assigned The Authority For' and a dropdown menu currently set to 'Only Contacts List'.

- **Assigned The Authority For:** Specify the contacts authorized to open doors via DTMF:
 - **Only Contacts List:** Doors can be opened by numbers added to the device's contact list and pressing the push button.
 - **All Numbers:** Any numbers can unlock using DTMF.

DTMF Data Transmission

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

DTMF Type Differences:

Inband	DTMF signals are transmitted within the same audio channel as voice data. Simple implementation but signal distortion may occur with highly compressed codecs (e.g., G.729).
RFC2833	Transmits DTMF as special event packets over RTP (Real-Time Transport Protocol), known as out-of-band transmission. Reliable and unaffected by codecs.
Info	Sends DTMF signals via SIP (Session Initiation Protocol) signaling channel. Separate from voice transmission, ensuring audio quality.
Info+Inband	Combines Info and Inband methods.
Info+RFC2833	Combines both Info and RFC2833 methods.
Info+Inband+RFC2833	All three methods are used simultaneously.

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

DTMF

Type

Info+Inband+RFC2833 ▼

How To Notify DTMF

Disabled ▼

Payload

101 (96-127)

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

Unlock by HTTP Commands

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

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

The screenshot shows the 'Relay Methods' configuration page. A dashed box highlights the 'Via HTTP' section, which contains the following settings:

Via HTTP	
Enabled	☒
Session Check	☐
Username	
Password	

- **Session Check:** Enable to enhance data transmission security.
- **Username:** Set a username for authentication in HTTP command URLs.
- **Password:** Set a password for authentication in HTTP command URLs.

Tip

Here is an HTTP command URL example for relay triggering.

Device's IP
Preset credentials for authentication
 http://192.168.35.127/fcgi/do? action=OpenDoor&UserName=admin&Password=123458DoorNum=1
ID of Relay to be triggered

Note

The HTTP format for relay triggering varies depending on whether the device's high secure mode is enabled. Please refer to this how-to guide [Opening the Door via HTTP Command](#) for more information.

Unlock by Exit Button

When users need to open the door from inside by pressing the Exit button, you need to set up the Input terminal that matches the Exit button to activate the relay for the door access.

Click [here](#) to watch the instruction video.

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

Input	Input A	Input B	Input C	Input D
Input ID				
Enabled	☒	☒	☒	☒
Trigger Electrical Level	Low	Low	Low	Low
Action to Execute	☐ FTP ☐ SIP Call ☐ Email ☐ HTTP	☐ FTP ☐ SIP Call ☐ Email ☐ HTTP	☐ FTP ☐ SIP Call ☐ Email ☐ HTTP	☐ FTP ☐ SIP Call ☐ Email ☐ HTTP
HTTP URL				
Action Delay	0	0	0	0 (0-300Sec)
Action Delay Mode	Unconditional Execution	Unconditional Execution	Unconditional Execution	Unconditional Execution
Door Sensor Associated Relay	None	None	None	None
Execute Relay	None	None	None	None
Door Status	High	High	High	High

- **Enabled:** To use a specific input interface.
- **Trigger Electrical Level:** Set the input interface to trigger at a low or high electrical level.
- **Action To Execute:** Set the desired actions that occur when the specific Input interface is triggered.
 - **FTP:** Send a screenshot to the preconfigured [FTP server](#).
 - **Email:** Send a screenshot to the preconfigured [Email address](#) .
 - **SIP Call:** Call the preset [number](#) upon the trigger.
 - **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL:** Enter the HTTP message if selecting HTTP as the action to execute. The format is [http://HTTP server's IP/Message content](#).
- **Action Delay:** Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode:**
 - **Unconditional Execution:** The action will be carried out when the input is triggered.
 - **Execute If Input Still Triggered:** The action will be carried out when the input stays triggered. For example, if the door stays open after triggering the input, an action such as an email will be sent to notify the receiver.
- **Door Sensor Associated Relay:** This indicates the Relay bound to the Input when the Input is configured as a **Door Sensor**. Displays **None** when the Input is not associated with any Relay.
- **Execute Relay:** Specify the relay to be activated on input trigger. This is incompatible with the break-in intrusion feature. The same input cannot work for both the door sensor and push exit button.
- **Door Status:** Display the status of the input signal.

Monitor and Image

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

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

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

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

MJPEG Image Capturing

MJPEG function is enabled by default. You can choose the image quality on the **Surveillance > MJPEG** interface.

MJPEG Server	
Image Quality	4CIF ▼

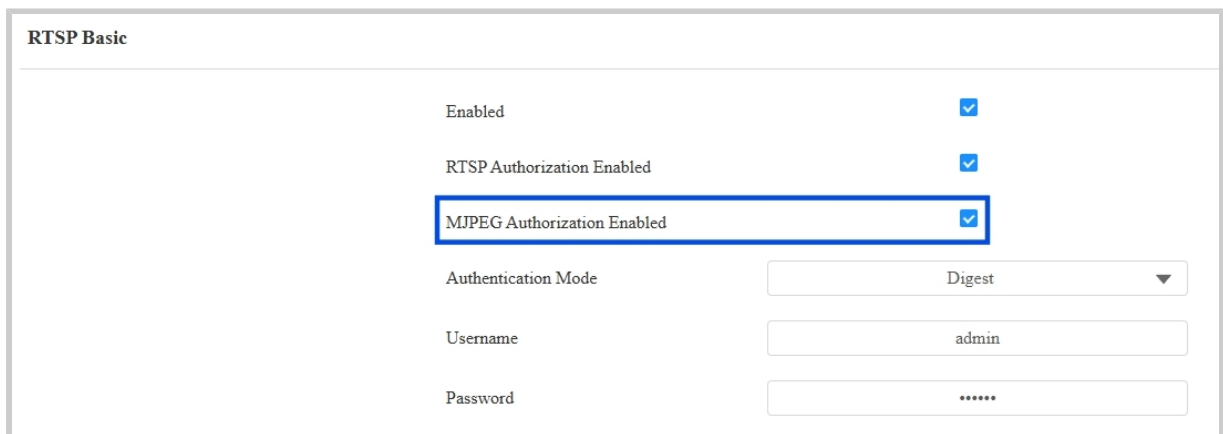
Entering the specific URL into the browser can access either an image or a video from the camera.

Tip

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

- **Image Quality:** Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 720P(1280 × 720 pixels). The default is 4CIF(704×576 pixels).

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



RTSP Basic

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

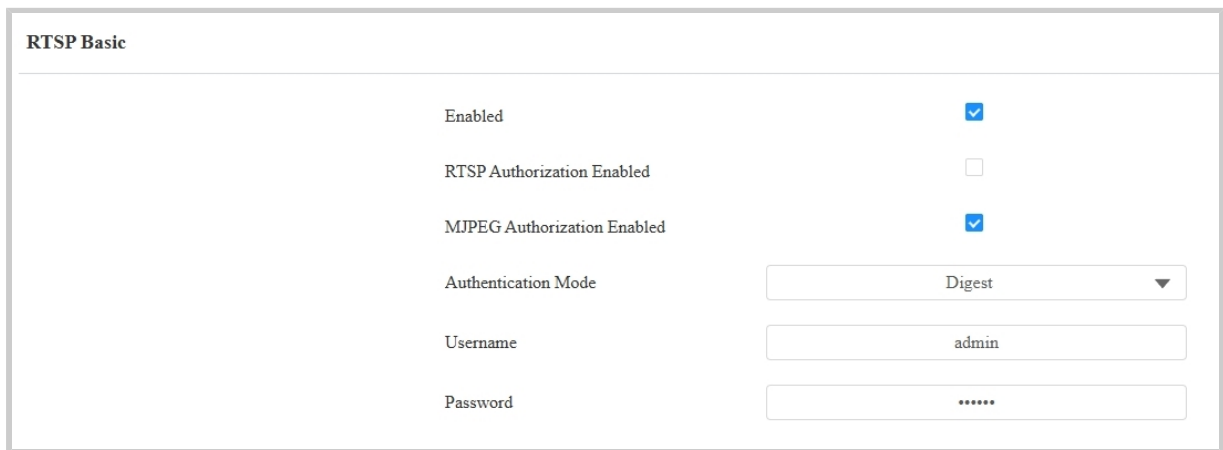
- **MJPEG Authorization Enabled:** Once enabled, accessing the device's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username, and RTSP Password.

RTSP Stream Monitoring

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

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

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



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

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

RTSP Stream Setting

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

H.264 Video Parameters	
Video Resolution	720P ▼
Video Framerate	25fps ▼
Video Bitrate	2048kbps ▼
2nd Video Resolution	VGA ▼
2nd Video Framerate	25fps ▼
2nd Video Bitrate	2048kbps ▼

- **Video Resolution:** Specify the image resolution, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Video Framerate:** Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 25fps.
- **Video Bitrate:** The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048 kbps.
- **2nd Video Resolution:** Specify the image resolution for the second video stream channel.
- **2nd Video Framerate:** Set the frame rate for the second video stream channel.
- **2nd Video Bitrate:** Set the bit rate for the second video stream channel.

Tip

To view the audio and video stream using RTSP:

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

ONVIF

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

Click [here](#) to view an example of using the ONVIF feature: the integration with Uniview NVR System.

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

Basic Setting	
Discoverable	☒
Username	admin
Password	*****

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

Tip

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

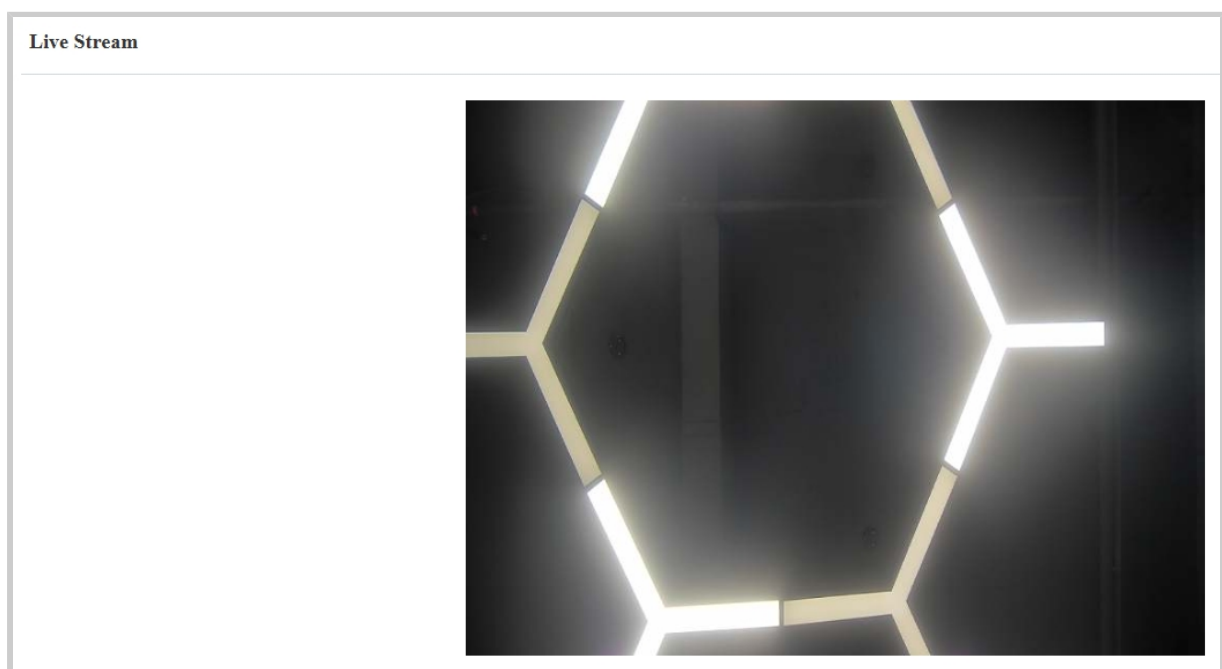
Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.

Advanced Setting	
Milestone	☐

Live Stream

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

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



Camera Mode

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

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

Camera Mode	
Mode	HDR ▼
Anti-Flicker	
Anti-Flicker Mode	Auto ▼
Anti-Flicker Frequency	50HZ ▼
Framerate	
Sensor Framerate	25fps ▼

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

Data Transmission Type for Third-party Camera

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

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

Third Party Camera	
Transport Type	TCP ▼

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

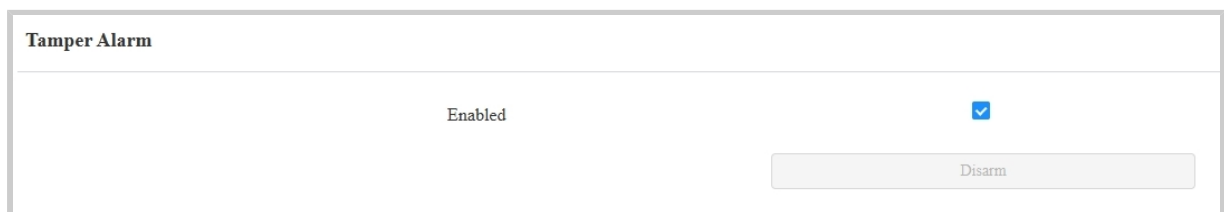
Security

Tamper Alarm

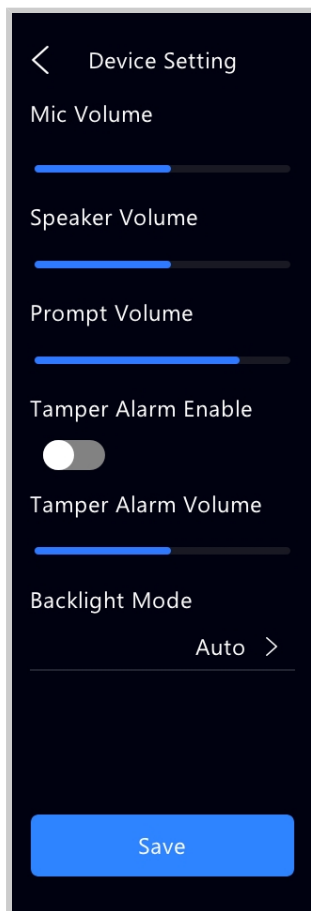
The tamper alarm function prevents anyone from removing the device without permission. Akuvox devices support two types of tamper proof: gravity detection and button status detection.

Click [here](#) to view which type is supported by the device and learn the function details.

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



You can also enable/disable Tamper Alarm on the **Setting > Device Setting** screen.

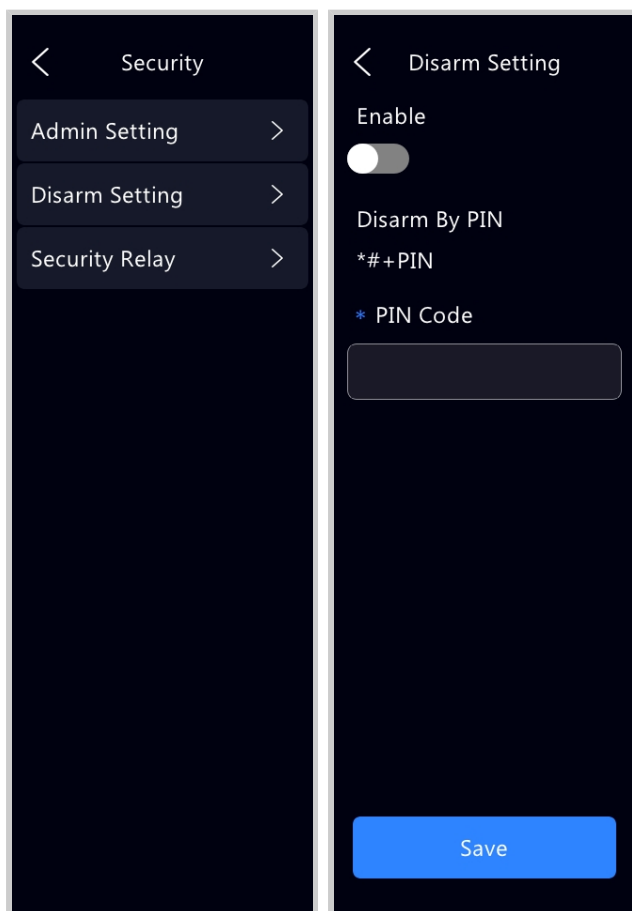


Disarm Setting

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

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

You can also set up the code on the **Setting > Security > Disarm Setting** screen.



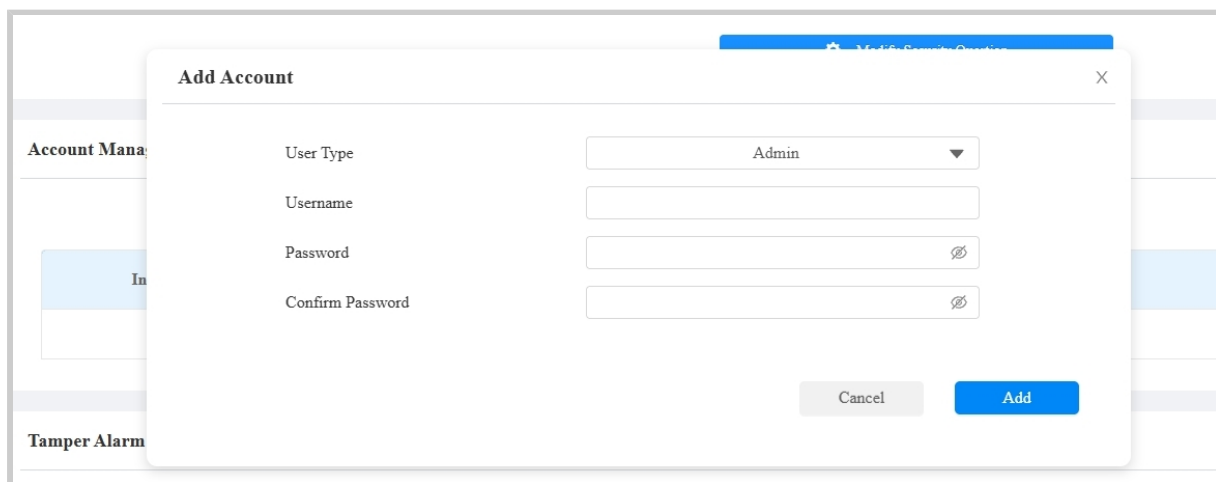
Account Management

You can add user accounts to access the device's web interface and assign different access permissions to control the settings available to each account.

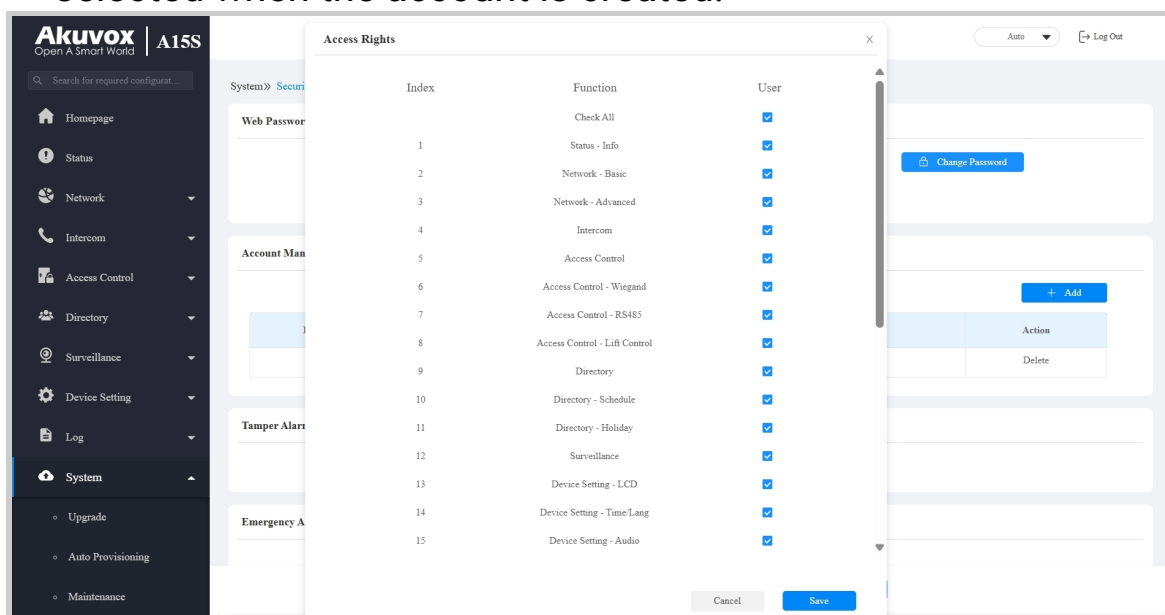
To set it up, go to the **System > Security > Account Management** interface. The default admin account cannot be deleted.

Click **+Add** to create a new account.

Account Management				
				+ Add
Index	Type	Username	Access Rights	Action
1	Admin	admin	Full Access	Delete



- **User Type:** The account type.
 - **Admin:** The Admin account has full access to the device's web settings.
 - **User:** The user account can only access the settings that are selected when the account is created.



- **Username:** The username used to log in to the device's web interface.
- **Password:** The password used to log in to the device's web interface.

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 device. Please upload the certificates in accepted formats.

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

Web Server Certificate				
Upload		 Upload		
Index	Issue To	Issuer	Expire Time	Delete
1	akweb	AKUVOX	Sun Dec 31 00:00:00 2099	 Delete

Client Certificate

Configure the TLS settings and certificates used for secure SIP communication. You can specify the TLS version, configure server certificate verification, and manage the certificates required for SIP TLS connections.

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

SIP TLS Certificate

TLS Version

TLS 1.2

CA Certificate

Verify SIP Server CA Certificate

☐

?

Index

Auto

Upload

Upload

	Index	Issue To	Issuer	Expire Time
No Data				

Delete

Delete All

Client Certificate

Upload

Upload

Index	Issue To	Issuer	Expire Time	Delete
1	akpbx	cloud.akuvov.com	Sun Sep 10 03:21:52 2049	Delete

- **TLS Version:** TLS 1.2 provides stronger security with modern encryption algorithms and is recommended for secure communication. TLS 1.0 is an outdated protocol with known vulnerabilities and should be avoided unless required for legacy compatibility.
- **Verify SIP Server CA Certificate:** When enabled, the device verifies the SIP server certificate using the uploaded CA certificate before establishing a TLS connection. The connection will be rejected if the certificate is not trusted.
- **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 a value from 1 to 10, the uploaded certificate will be displayed according to the number.
- **CA Certificate Upload:** Supported formats: .pem, .der, .cer, .crt.
- **Client Certificate Upload:** Supported formats: .pem, .cer, .crt.

Motion Detection

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

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

Motion Detection Options	
Suspicious Moving Object Detection	Radar Detection ▼
Time Interval	10 (0-120Sec)
Detection Range	3 (m) ▼

- **Suspicious Moving Object Detection:** The feature uses the main camera for detection.
 - **Disabled:** Turn off the feature.
 - **Video Detection:** When the video camera detects moving objects, preset actions will be triggered. Focus on analyzing visual information captured through cameras.
 - **Radar Detection:** When the radar detects moving objects, preset actions will be triggered. It offers longer range and better detection in poor visibility conditions.
 - **Video + Radar:** Detect motion with the combination of the video camera and radar.
- **Time Interval:** Determine how to delay and trigger motion detection.
 - Timing Interval between 1–3 seconds: Only need 1 detection during this interval to trigger actions.
 - Timing Interval > 3 seconds (e.g., 10 seconds): To perform actions, require a second detection within the final 3 seconds of the interval (e.g., between 7–10 seconds for a 10-second interval) after the first detection.
 - The default interval is 10 seconds.

- **Detection Accuracy:** Not available for radar detection. The detection sensitivity. The higher the value, the greater the sensitivity. The default detection accuracy value is 3.
- **Detection Range:** Set the distance within which radar detection is triggered. The range includes 1, 2, and 3 meters.
- **Detection Area:** Click and hold the mouse button to select up to three detection areas. When motion is detected within these areas, preset actions will be carried out.
- **Action To Execute:** Set the desired actions that occur when suspicious movement is detected.
 - **FTP:** Send a screenshot to the preconfigured [FTP server](#).
 - **Email:** Send a screenshot to the preconfigured [Email address](#) .
 - **SIP Call:** Call the preset [number](#) upon the trigger.
 - **HTTP:** When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
 - **HTTP URL:** Enter the HTTP message if selecting HTTP as the action to execute. The format is [http://HTTP server's IP/Message content](#).
 - **Execute Relay:** A relay can be unlocked with motion detection.

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

Motion Detect Time Setting

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

Security Notification

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

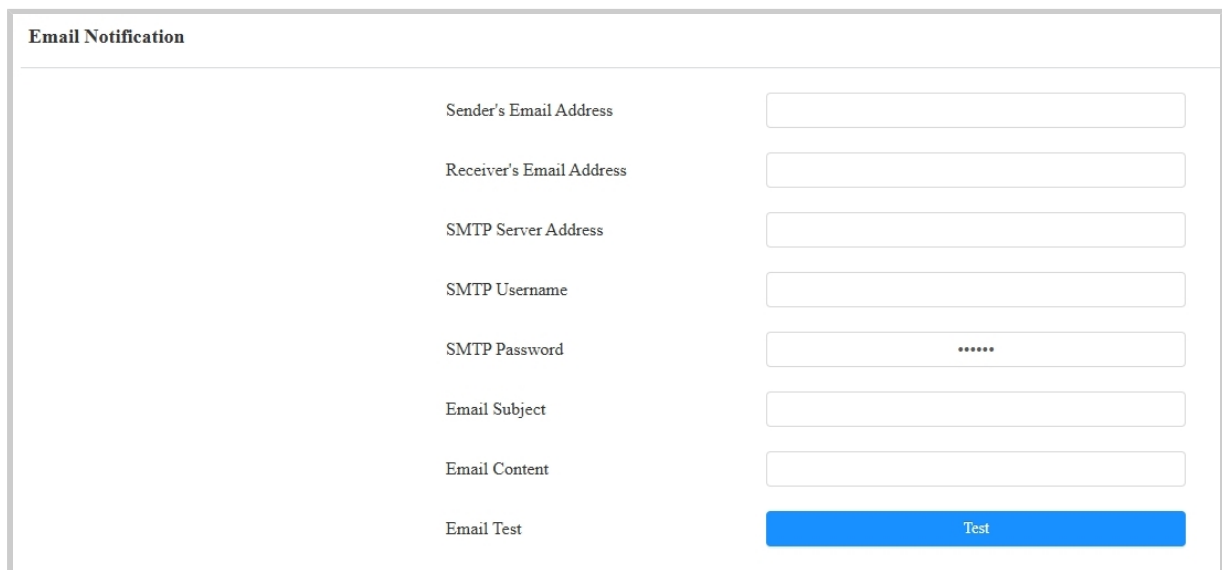
To set up security notifications, go to **Device Setting > Action** interface.

Email Notification

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

Click [here](#) to view how to set this feature up.

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



The screenshot shows a web interface titled "Email Notification". It contains several input fields for configuration: "Sender's Email Address", "Receiver's Email Address", "SMTP Server Address", "SMTP Username", "SMTP Password" (masked with asterisks), "Email Subject", and "Email Content". At the bottom, there is an "Email Test" label and a blue button labeled "Test".

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

FTP Notification

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

Click [here](#) to view the configuration steps.

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

FTP Notification

FTP Server	
FTP Username	
FTP Password	*****
FTP Test	FTP Test

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

SIP Call Notification

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

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

SIP Call Notification

SIP Call Number	
SIP Caller Name	

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

Action URL

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

Akuvox Action URL:

Event	Parameter format	Example
Make Call	\$remote	Http://server ip/Callnumber=\$remote
Hang Up	\$remote	Http://server ip/Callnumber=\$remote
Valid Code Entered	\$code	Http://server ip/validcode=\$code
Invalid Code Entered	\$code	Http://server ip/invalidcode=\$code
Valid Card Entered	\$card_sn	Http://server ip/validcard=\$card_sn
Invalid Card Entered	\$card_sn	Http://server ip/invalidcard=\$card_sn
Tamper Alarm	\$alarmstatus	Http://server ip/tampertri=\$alarmstatus
Relay Triggered	\$relay1status	Http://server ip/ relaytrigger=\$relay1status
Relay Closed	\$relay1status	Http://server ip/relayclose=\$relay1status

Input Triggered	\$input1status	Http://server ip/inputtrigger=\$input1status
Input Closed	\$input1status	Http://server ip/inputclose=\$input1status
Break-in Alarm	\$input1status	Http://server ip/inputtrigger=\$input1status
Facial Recognition	\$unlocktype	Http://serverip/unlocktype=\$unlocktype

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

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

Action URL

Enabled

☐

Type

GET

▼

Authorization Mode

None

▼

Make Call

Hang Up

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

Tamper Alarm

RelayA Triggered

RelayA Closed

RelayB Triggered

RelayB Closed

InputA Triggered

InputA Closed

Break In Alarm A	
InputB Triggered	
InputB Closed	
Break In Alarm B	
InputC Triggered	
InputC Closed	
Break In Alarm C	
InputD Triggered	
InputD Closed	
Break In Alarm D	
Valid Face Recognition	
Invalid Face Recognition	

Voice Encryption

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

Set it up on the web **Intercom > Account** interface.

Encryption

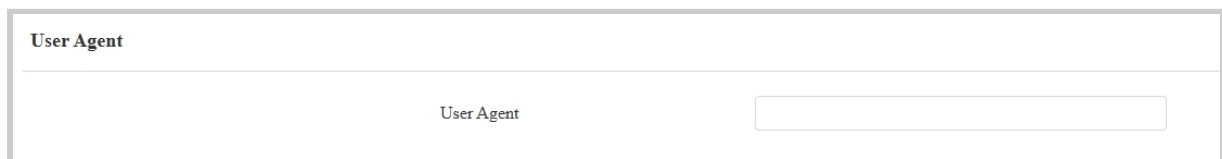
Voice Encryption(SRTP)
Disabled

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

User Agent

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

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

The screenshot shows a web interface for 'User Agent' configuration. At the top, there is a header 'User Agent'. Below it, there is a label 'User Agent' and an empty text input field.

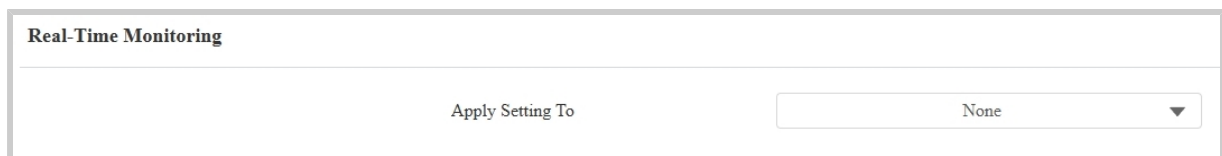
- **User Agent:** Akuvox is by default.

Real-Time Monitoring

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

Click [here](#) to see the detailed configuration.

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

The screenshot shows a web interface for 'Real-Time Monitoring' configuration. At the top, there is a header 'Real-Time Monitoring'. Below it, there is a label 'Apply Setting To' and a dropdown menu with 'None' selected.

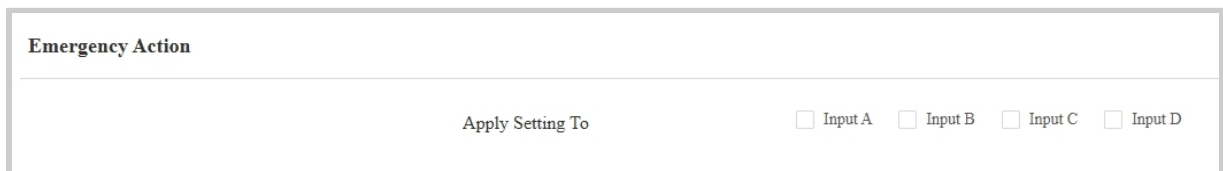
- **Apply Setting To:**
 - **None:** Not display door status.
 - **Input:** The door is opened by triggering input.
 - **Relay:** The door is opened by triggering the relay.

Emergency Action

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

Click [here](#) to view the detailed configuration of this feature.

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

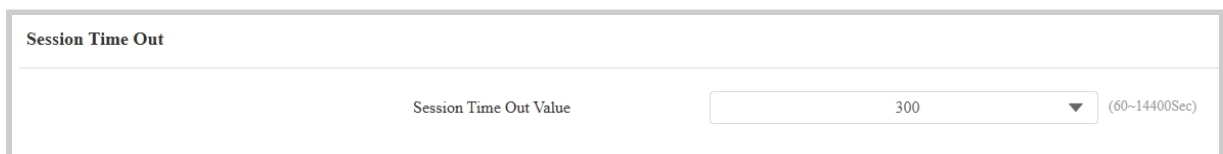


The screenshot shows the 'Emergency Action' configuration interface. It has a title bar 'Emergency Action'. Below the title bar, there is a label 'Apply Setting To' followed by four checkboxes: 'Input A', 'Input B', 'Input C', and 'Input D'. All checkboxes are currently unchecked.

Web Interface Automatic Log-out

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

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



The screenshot shows the 'Session Time Out' configuration interface. It has a title bar 'Session Time Out'. Below the title bar, there is a label 'Session Time Out Value' followed by a dropdown menu showing '300' and a range '(60~14400Sec)'.

High Security Mode

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

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

High Security Mode
Enabled ☒

Important Notes

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

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

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

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

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

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

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

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

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

Logs

Call Logs

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

Check call logs on the web **Log > Call Log** interface. The device can store 500 call logs.

- **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

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

Check door logs on the web **Log > Access Log** interface. The device can store 5,000 door logs.

The screenshot shows the 'Access Log' interface. At the top, there are three settings: 'Save Access Log Enabled' (checked), 'Save Picture Enabled' (checked), and 'Export Picture Enabled' (unchecked). Below these are filters for 'All' (selected), 'All' (selected), 'Start Time ~ End Time', and 'Name/Code'. There are 'Search' and 'Export' buttons. Below the filters is a table with columns: Index, User ID, Name, Code, Reader, Door ID, Type, and Date. The table is currently empty, showing 'No Data'. At the bottom, there are buttons for 'Delete' and 'Delete All', and a 'Go To Page' dropdown set to '1'.

- **Export Picture Enabled:** When enabled, you can export door logs with images.

Event Logs

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

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

Event Log			
Type	All x	Time	Start Time ~ End Time
			Search Export
Time	Event Type	Status	
2026-07-27 02:15:39	Login	Account admin; Success; IP 192.168.31.167	
2026-07-27 02:15:36	Login Attempt	Account admin; Failed; IP 192.168.31.167	
2026-07-27 01:59:44	Login	Account admin; Success; IP 192.168.31.167	
2026-07-27 01:45:44	Login	Account admin; Success; IP 192.168.31.167	
2026-07-27 01:14:40	IP Change	IP Changed from 169.254.210.214 to 192.168.31.197	
2026-07-27 01:14:34	IP Change	IP Connection Lost	
2026-07-27 01:13:30	IP Change	IP Obtained : 169.254.210.214	
2026-07-27 01:13:19	Device State	Startup	
2026-07-24 12:29:43	IP Change	IP Changed from 192.168.31.197 to 169.254.210.75	
2026-07-24 12:29:40	IP Change	IP Connection Lost	
2026-07-24 10:27:01	Login	Account admin; Success; IP 192.168.31.167	
2026-07-24 08:58:50	Login	Account admin; Success; IP 192.168.31.167	

Integration with Third-Party Device

Integration via Wiegand

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

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

The screenshot shows the 'Wiegand' configuration page. It contains the following settings:

- Wiegand Display Mode:** A dropdown menu currently set to '8HN'.
- Wiegand Card Reader Mode:** A dropdown menu currently set to 'Auto'.
- Wiegand Transfer Mode:** A dropdown menu currently set to 'Input'.
- Wiegand Input Data Order:** A dropdown menu currently set to 'Normal'.
- Wiegand Input Clear Time:** A dropdown menu currently set to '5'.
- Wiegand Open Relay:** Three checkboxes labeled 'Relay A', 'Relay B', and 'Security Relay', all of which are currently unchecked.

- **Wiegand Display Mode:** Select the Wiegand card code format from the following options: 8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26), 8HR10D, and RAW.
- **Wiegand Card Reader Mode:** The transmission format should be identical between the A15 and the third-party device.
- **Wiegand Transfer Mode:**
 - **Input:** The device serves as a receiver.
 - **Output:** The device serves as a sender and can directly output the data, such as the card code.
 - **Convert To Card No. Output:** The device serves as a sender and cannot directly output the data, such as the face data and fingerprint data.
- **Wiegand Input Data Order:** Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.

- **Wiegand Output Basic Data Order:** Set the sequence of the card data before going through Wiegand conversion and outputting the card code.
For example, if the card data is 0x11 0x22 0x33 0x44 and the **Reversed** option is selected, the data will be 0x44 0x33 0x22 0x11.
- **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If **Reversed** is selected, the card data is 0x55 0x44 0x33.
- **Wiegand Output CRC Enabled:** It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **Wiegand Input Clear Time:** When the interval between entering passwords exceeds this time. All entered passwords will be cleared.
- **RF Card Verification:** Available when **Output** or **Convert to Card No. Output** is selected. When enabled, the device will verify whether the card code is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the device screen. When disabled, the device will not perform local verification.
- **PIN/QR Code Verification:** Available when **Output** is selected as Wiegand Transfer Mode. When enabled, the device will verify whether the credential is assigned to a user. If it is not, a prompt "Opening Door Failed" will pop up on the device screen. When disabled, the device will not perform local verification.
- **Wiegand Open Relay:** Check the relay to be triggered through Wiegand.

Note

Click [here](#) to view more information on Wiegand settings, including:

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

When the device is in **Wiegand Output** mode, you can set the Wiegand PIN code output format that determines how data is transmitted. The format should be consistent with that of the third-party device.

Convert To Wiegand Output	
PIN Output	Disabled ▼

- **8 bits per digit:** When users press "1" on the keypad, the binary data will be transmitted in 8 bits, "11100001".
- **4 bits per digit:** When users press "1" on the keypad, the binary data will be transmitted in 4 bits, "0001".
- **All at once:** After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode. For example, "123456" will be converted to "01e240" in Wiegand 26.

Integration via HTTP API

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

To set it up, go to the web **Device Setting > HTTP API** interface.

HTTP API

Enabled

☒

Authorization Mode

Allowlist ▼

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 an HTTP 403 forbidden status.
- **Authorization Mode:** Select one of the following options: None, Allowlist, Basic, Digest, and Token for authorization type, which will be explained in detail in the following chart.
- **Username:** Enter the username 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 **Allowlist** authorization is selected for the integration.

Please refer to the following description for the authentication mode:

Authorization Mode	Description
None	No authentication is required. This mode is intended for testing only and is not recommended in production environments.
Allowlist	Authenticates requests based on the source IP address. Add the IP address of the third-party device to the allowlist before sending requests. Recommended for trusted LAN environments.
Basic	Authenticates requests using a username and password. The credentials must be Base64-encoded and included in the Authorization header.
Digest	Authenticates requests using HTTP Digest authentication. Only the MD5 algorithm is supported.
Token	Reserved for Akuvox internal development and testing.

Power Output Control

The device can serve as a power supply for the external relays. Click [here](#) to view power output requirements.

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

12V Power Output	
12V Power Output	Disabled ▼ ?
Time Out (Sec)	3 ▼

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

Integration via RS485

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

Click [here](#) to view the detailed configuration of the OSDP feature.

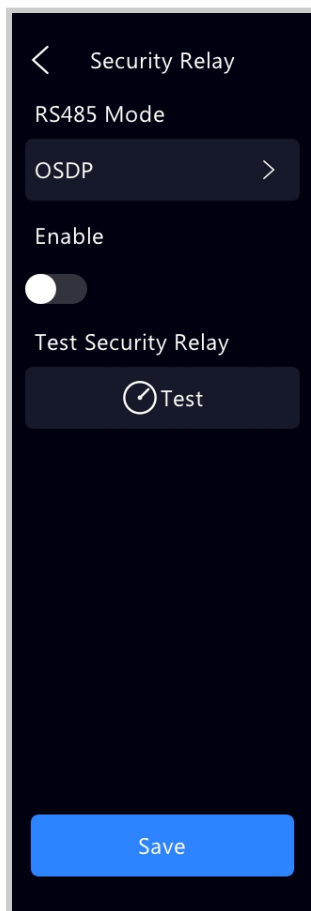
To make the connection effective, you need to set up the RS485 on the **Access Control > RS485** interface.

RS485 Setting	
Apply RS485 Setting To	OSDP ▼
OSDP Setting	
Encryption	☐
Baud Rate	9600 ▼
Transfer Mode	Input ▼
SCBK Value	
OSDP Open Relay	☐ Relay A ☐ Relay B

- **Disabled:** The RS485 function is disabled.

- **OSDP:** The device is connected to an OSDP-based external device such as a card reader.
 - **Encryption:** Check this option when the protocol is encrypted.
 - **Baud Rate:** Set the baud rate for data transmission during communication. The default is 9600, supported by Akuvox devices.
 - **Transfer Mode:** Select the RS485 working mode: Output, or Input.
 - **Local Relay Verification:** When Output is selected, set whether to carry out the access credentials verification. When unchecked, door-opening failure prompts will not be given.
 - **SCBK Value:** Secure Communication Key Value.
 - When it is filled, OSDP will use this value for encryption, employing a customized protocol for communication.
 - When it is left empty, OSDP will use the default encrypted protocol for communication.
 - **Address:** The RS485 address to distinguish this device from others.
- **Security Relay:** Select this option when the device works with the SR01.

You can also select the RS485 Mode on the **Setting > Security > Security Relay** screen.



Integration with Third-party Access Control Server

The device can transmit credential data to a third-party server without doing any verification. The generation and verification of the data are conducted on the third-party server.

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

Third Party Integration

List	Customize ▼
Prompt On LCD	Return Value ▼
Remote Verification	☒ QR Code ☒ Card ☒ PIN ☒ Face
HTTP URL	
Device ID	
Success Parameter	1
Failed Parameter	0

- **None:** Disable the function.
- **General:** Transmit the QR code-linked HTTP URL in Akuvox's method.
 - **HTTP URL:** Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before it is sent to the QR code server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode}&deviceId={DeviceID}*.
 - **Device ID:** The device ID is provided by the third-party server. It will be added to the HTTP command automatically when using a QR code for door access.
 - **Success Parameter:** Receiving this value indicates that opening the door succeeds.
 - **Failed Parameter:** Receiving this value indicates that opening the door fails.
- **Customize:** Transmit access credential data in a customized method. When **Face** is selected, the device performs local face recognition first. If no matching face is detected, authentication fails. If a match is found, the associated **User ID** or **PIN** is submitted to the third-party server for further verification.

- **Remote Verification:** Specify which access credentials will be verified by the third-party server. In all cases, the specified credential is forwarded to the server as-is, with no local verification performed on the device.

Available options depend on the [configured device](#)

[theme](#) :

Theme	Available Options
Default	QR Code, Card, PIN, Face
Multi-factor Authentication	QR Code, Multi-Factor

When the **Multi-factor Authentication** theme is selected, the **Remote Verification** options behave as follows:

Option	Description
QR Code	The device scans the QR code and sends it directly to the third-party server.
Multi-Factor	The device first checks whether the authentication method matches the configured method. If not matched → User is prompted to use the correct method. If matched → The collected credentials are sent to the server for verification.

- **HTTP URL:** Enter the HTTP command format provided by the third-party service provider. After a QR code scan, card swipe, PIN entry, or face recognition, the device automatically replaces variables in the URL and sends the request to the server.

Example format:

http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode}/{Card}/{UserID}/{Pin}&deviceId={DeviceID}.

If a user swipes a card, the URL will be

http://192.168.35.123:8090/api/visitor/scan?
codeKey={QRCode}/123456/{UserID}/{Pin}&deviceId=1.

In the **Multi-factor Authentication** theme, the available placeholders depend on the **Authentication Mode** selected.

Variable	Description
{Token}	Credential collected in the current authentication step.
{Type}	Two-factor authentication type: 1 = RF Card + PIN 3 = Face + RF Card 4 = Face + PIN

- **Device ID:** The device ID is provided by the third-party server. It will be added to the HTTP command automatically.
- **Success Parameter:** Receiving this value indicates that opening the door succeeds.
- **Failed Parameter:** Receiving this value indicates that opening the door fails.

Lift Control

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

Click [here](#) to watch a demonstration video of configuring the lift control feature.

To set it up, go to the web **Access Control > 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 ▼

Ground Floor

▼

Device Location

None ▼

- **Lift Control List:** Select None to disable the function, and select Akuvox to integrate the device with the Akuvox controller.
- **Server 1 IP(Unlock):** The IP address of the lift controller that unlocks the elevator button(s). It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute):** The IP address of the lift controller that sends the lift control commands.
- **Port:** The server port of the lift controller server.
- **Username:** The username of the lift controller for authentication.
- **Password:** The password of the lift controller for 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 the first floor, matched with relay#1 (first floor).
- **Ground Floor:** If there are ground floors between the -1 and 1 floors, configure this option.
- **Device Location:** Select the floor where the device is installed.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Upgrade the firmware on the web **System > Upgrade** interface. If you want to reset the device after the upgrade, check the Reset box.

Basic	
Firmware Version	1115.30.10.408
Hardware Version	1115.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

Note

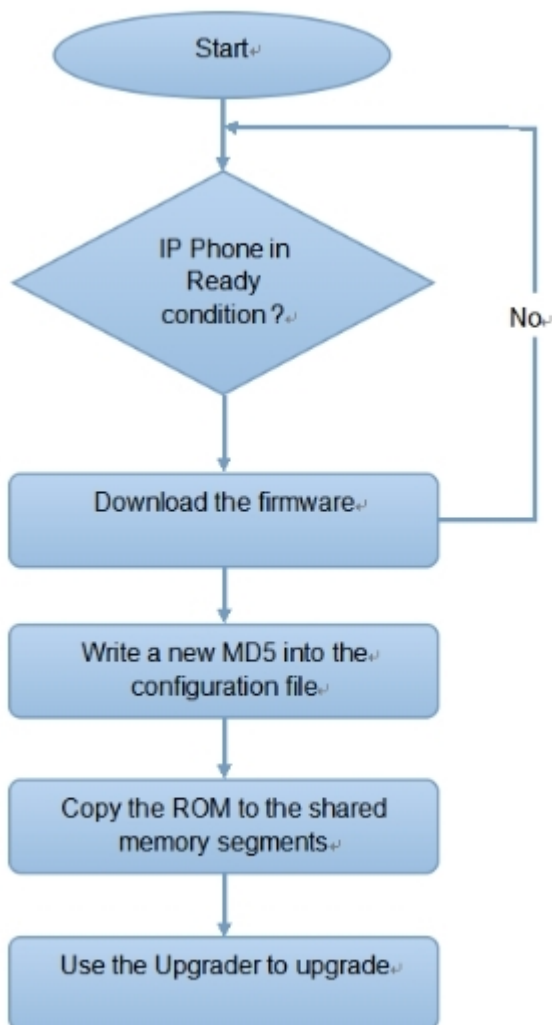
Firmware files should be in .rom format for upgrade.

Auto-provisioning via Configuration File

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

Differences:

- **General Configuration Provisioning:**

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

- **MAC-Based Configuration Provisioning:**

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

Note

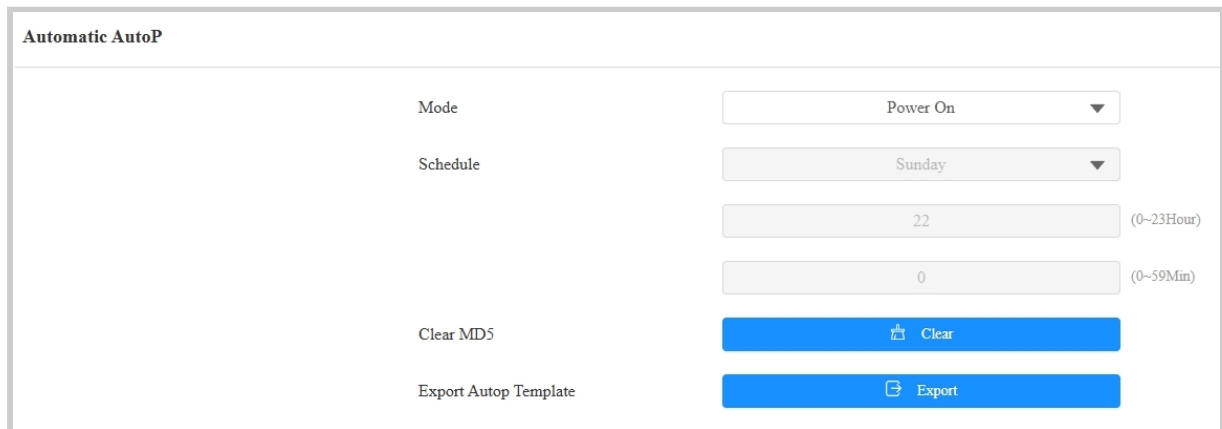
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

You may click [here](#) to see the detailed format and steps.

AutoP Schedule

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

Set it up on the web **System > Auto Provisioning > Automatic AutoP** interface.



The screenshot shows the 'Automatic AutoP' configuration page. It features a table with two columns: configuration options and their corresponding controls. The options include 'Mode', 'Schedule', 'Clear MD5', and 'Export Autop Template'. The controls consist of dropdown menus for 'Mode' (set to 'Power On') and 'Schedule' (set to 'Sunday'), input fields for time (set to '22' and '0') with ranges '(0~23Hour)' and '(0~59Min)', and blue buttons with icons for 'Clear' and 'Export'.

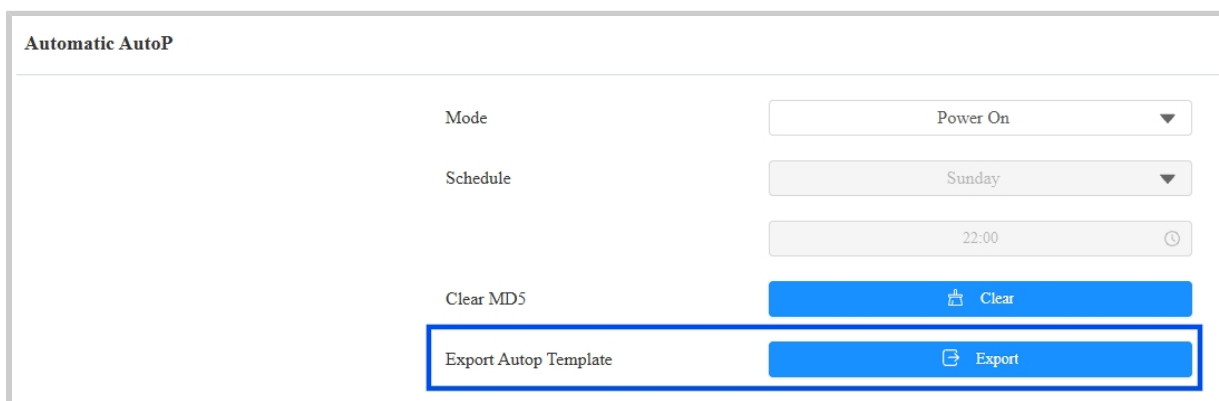
Automatic AutoP	
Mode	Power On ▼
Schedule	Sunday ▼
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

- **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

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.

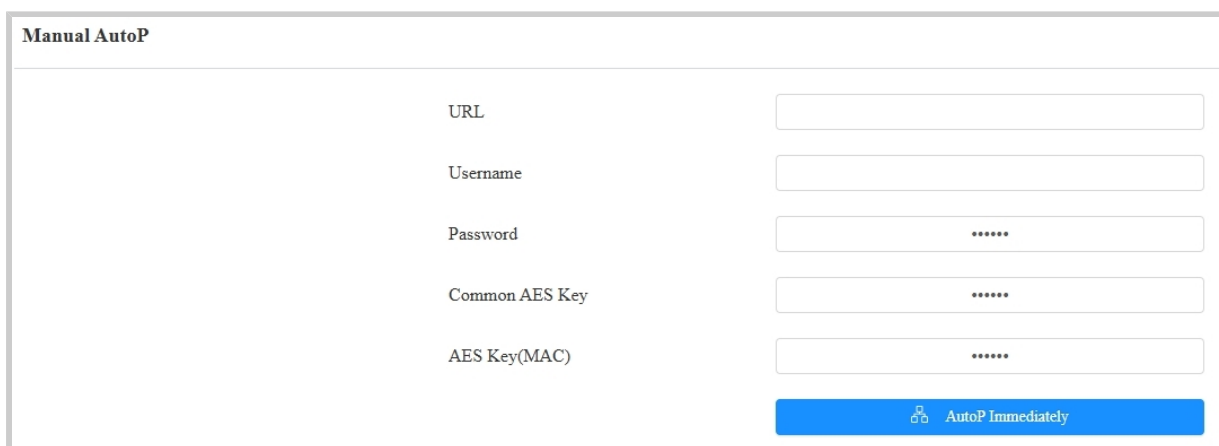
Download the Autop template on the **System > Auto Provisioning > Automatic AutoP** interface.



The screenshot shows the 'Automatic AutoP' configuration page. It features a table with two columns: a label column and a value column. The labels are 'Mode', 'Schedule', 'Clear MD5', and 'Export Autop Template'. The values are 'Power On' (in a dropdown), 'Sunday' (in a dropdown), '22:00' (with a clock icon), and a blue button labeled 'Clear' with a trash icon. Below these is another blue button labeled 'Export' with a document icon. The 'Export Autop Template' row is highlighted with a blue border.

Automatic AutoP	
Mode	Power On ▼
Schedule	Sunday ▼
	22:00 ⌚
Clear MD5	Clear
Export Autop Template	Export

Set the AutoP server on **System > Auto Provisioning > Manual AutoP** interface.



The screenshot shows the 'Manual AutoP' configuration page. It features a table with two columns: a label column and a value column. The labels are 'URL', 'Username', 'Password', 'Common AES Key', and 'AES Key(MAC)'. The values are empty text boxes, except for 'Password', 'Common AES Key', and 'AES Key(MAC)' which contain six asterisks. At the bottom right is a blue button labeled 'AutoP Immediately' with a play icon.

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

- **URL:** The TFTP, HTTP, HTTPS, or FTP server address for provisioning.
- **Username:** Set up a username if the server requires a username to access.

- **Password:** Set up a password if the server requires a password to access.
- **Common AES Key:** Set up an 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

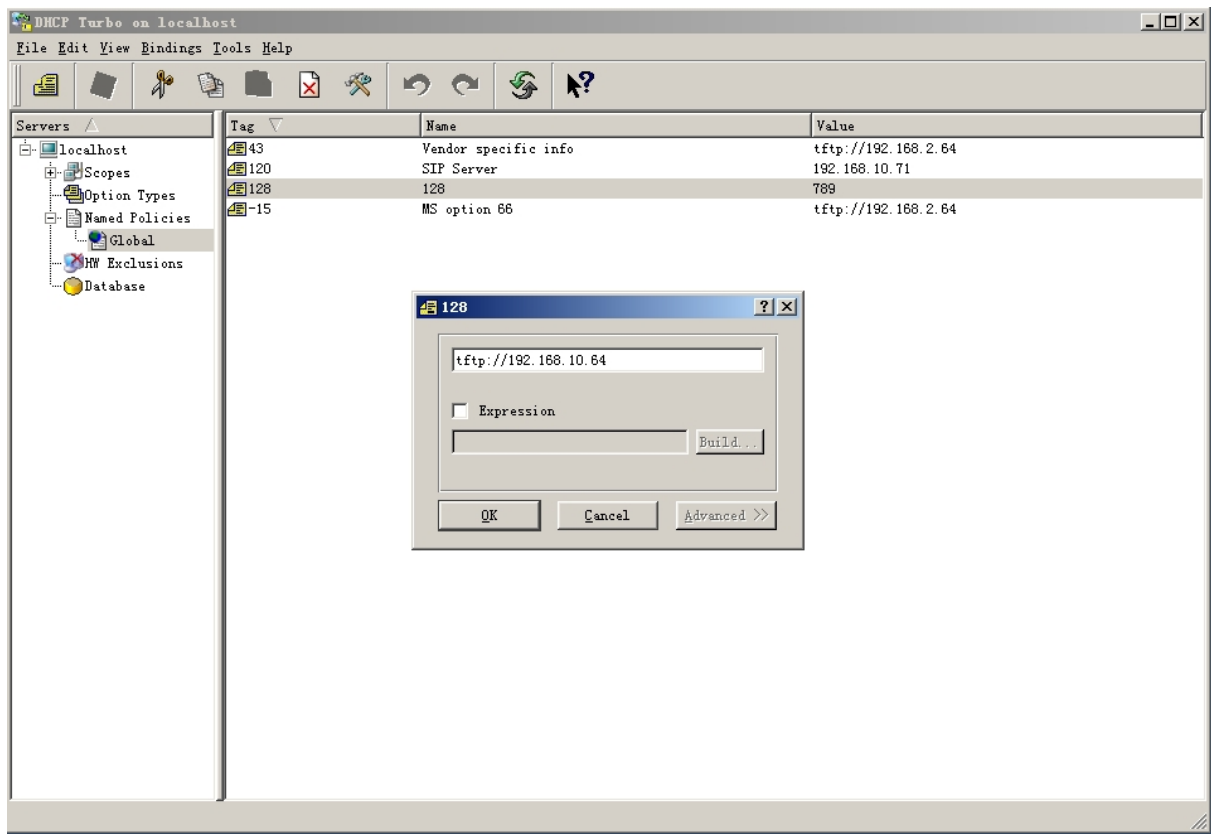
- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/(use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

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 **CustomOptions** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.



Note

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

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

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

Automatic AutoP

Mode

Power On

Schedule

Sunday

22:00

Clear MD5

Clear

Export AutoP Template

Export

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

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.

PNP Configuration

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

Click [here](#) to watch the configuration video.

Enable/disable it on the web **System > Auto Provisioning > PNP Option** interface.

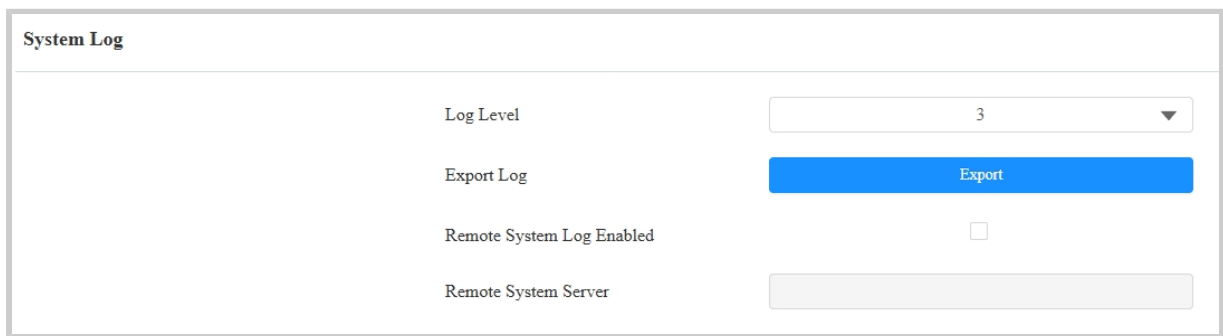
PNP Option
PNP Config Enabled ☒

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Set it up on the web **System > Maintenance > System Log** interface.



The screenshot shows the 'System Log' configuration page. It has a title bar 'System Log' and a main content area with four settings:

Setting	Value / Control
Log Level	3 (dropdown menu)
Export Log	Export (blue button)
Remote System Log Enabled	☐
Remote System Server	(empty text field)

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

PCAP for Debugging

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

Set it up on the web **System > Maintenance > PCAP** 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 Enabled:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.

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.

Set it up on the **System > Maintenance > Remote Debug Server** interface.

Remote Debug Server

Enabled

☐

Connect Status

Disconnected

IP

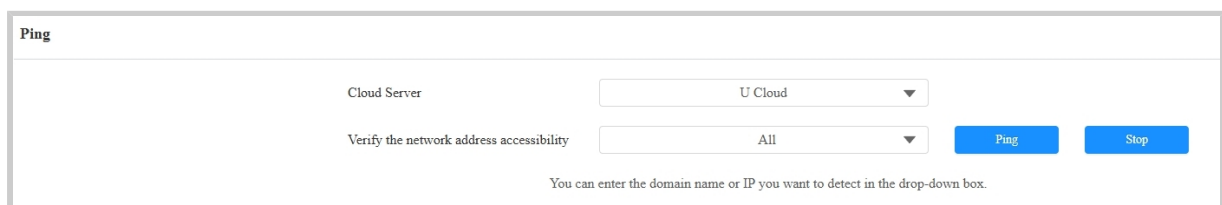
- **Connect Status:** Display the connection status between the device and the server.
- **IP:** Enter the IP address of the server.

Ping

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

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

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



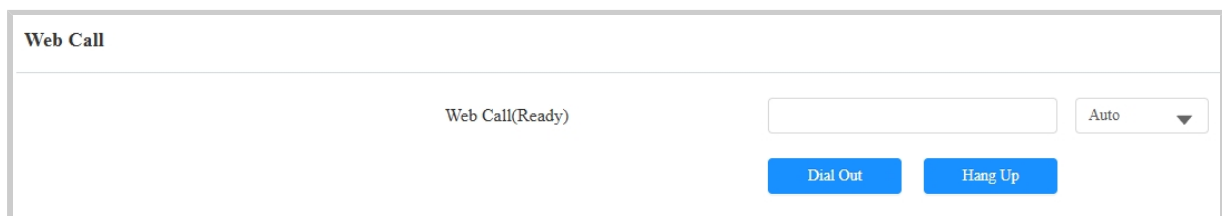
The screenshot shows the 'Ping' interface. At the top, there's a title 'Ping'. Below it, there are two dropdown menus. The first is labeled 'Cloud Server' and has 'U Cloud' selected. The second is labeled 'Verify the network address accessibility' and has 'All' selected. To the right of these dropdowns are two blue buttons: 'Ping' and 'Stop'. Below the buttons, there is a small text note: '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 includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Web Call

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

To set it up, go to the web **System > Maintenance > Web Call** interface. Select the registered SIP account, enter the IP/SIP number, and click **Dial Out** to make the call.

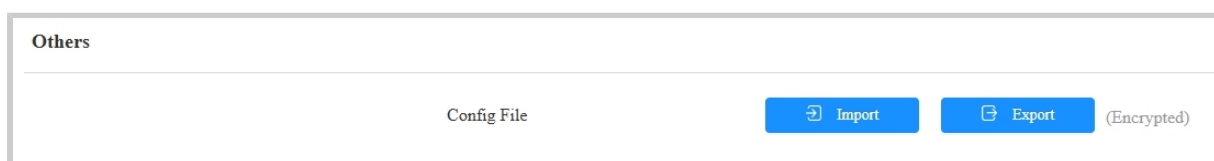


The screenshot shows the 'Web Call' interface. At the top, there's a title 'Web Call'. Below it, there's a text label 'Web Call(Ready)'. To the right of this label is a text input field and a dropdown menu with 'Auto' selected. Below these elements are two blue buttons: 'Dial Out' and 'Hang Up'.

Backup

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

Set it up on the web **System > Maintenance > Others** interface. The import file should be in .tgz/.conf/.cfg format.



- **Config File:** Click **Export** to export configuration items as an encrypted file; click **Import** to import a configuration file to the device. The Config File is used to back up and restore device **configuration settings** only. It does not include user data and contact data.

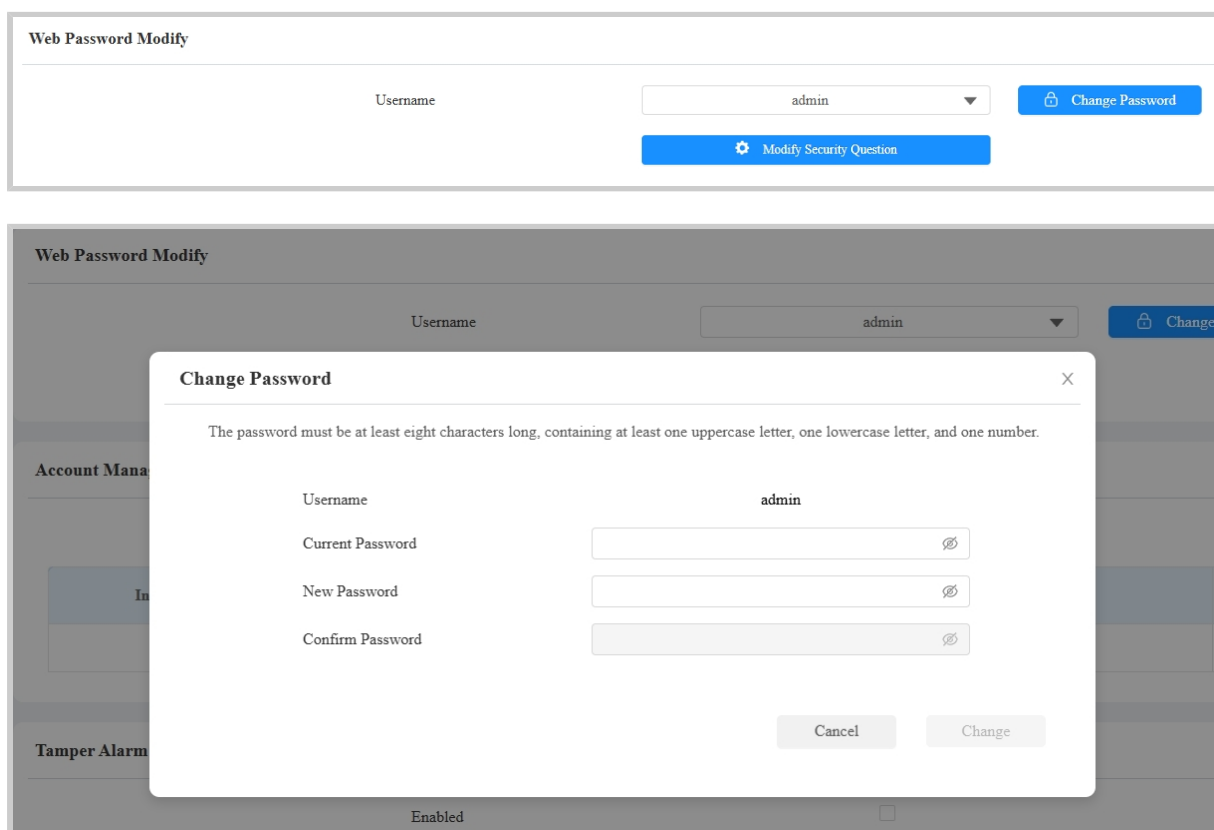
Password Modification

Modify Web Interface Password

You can modify the device web interface login password for both administrator and user accounts.

Go to the **System > Security > Web Password Modify** interface. Select admin for the administrator account and select user for the user account.

Click **Change Password** to modify the password.



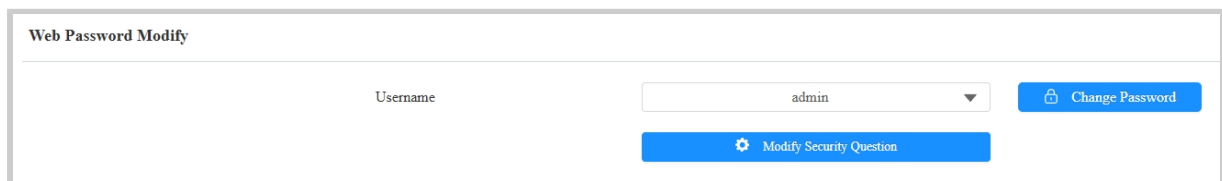
The screenshot displays the 'Web Password Modify' interface. At the top, there is a header 'Web Password Modify'. Below it, a form shows 'Username' with a dropdown menu currently set to 'admin'. To the right of the dropdown is a blue button labeled 'Change Password' with a lock icon. Below the dropdown is another blue button labeled 'Modify Security Question' with a gear icon. A modal dialog titled 'Change Password' is open in the foreground. The dialog contains a message: 'The password must be at least eight characters long, containing at least one uppercase letter, one lowercase letter, and one number.' Below this message, there are three input fields: 'Current Password', 'New Password', and 'Confirm Password'. Each field has a password strength indicator icon to its right. The 'Username' field in the dialog is also set to 'admin'. At the bottom of the dialog are two buttons: 'Cancel' and 'Change'. The background of the interface is dimmed, showing other sections like 'Account Mana', 'In', and 'Tamper Alarm'.

Modify Security Questions

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

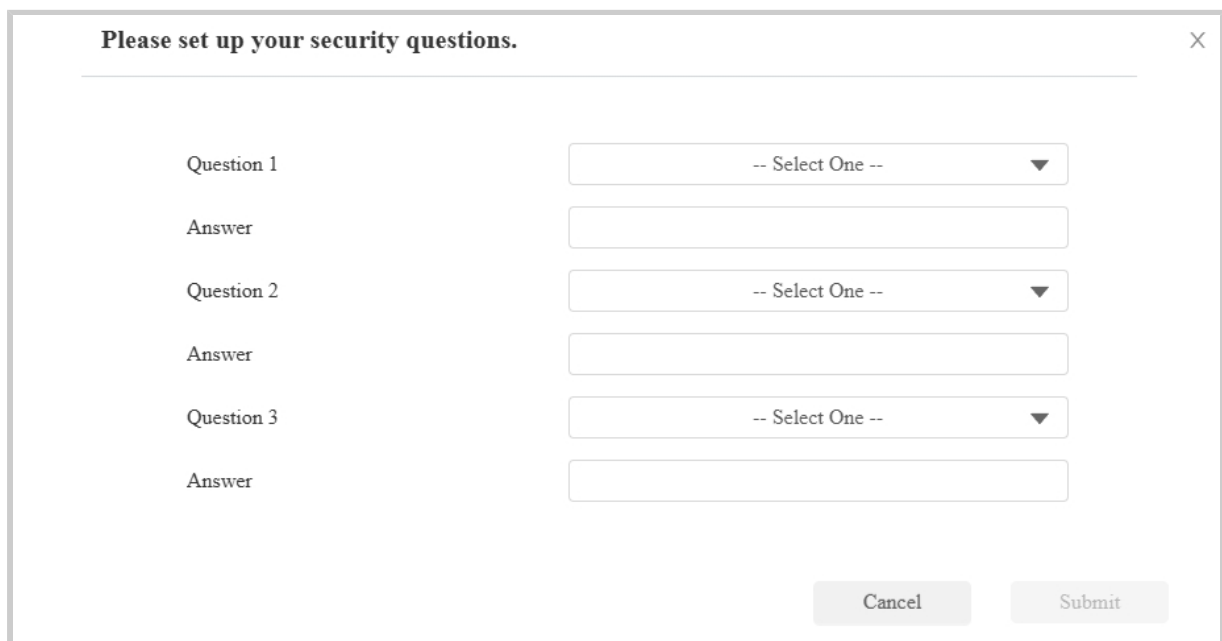
If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

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



The screenshot shows the 'Web Password Modify' interface. It features a 'Username' field with 'admin' selected in a dropdown menu. To the right of the dropdown is a blue button with a lock icon and the text 'Change Password'. Below the dropdown is another blue button with a gear icon and the text 'Modify Security Question'.

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

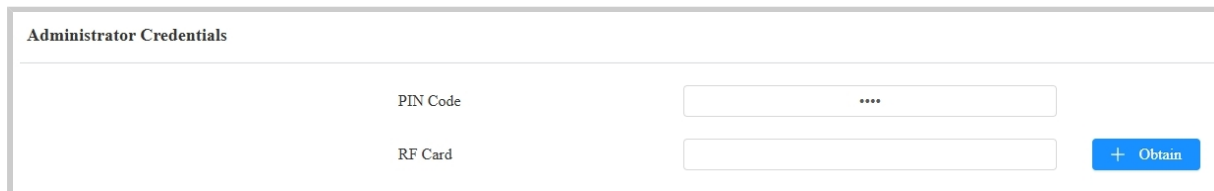


The screenshot shows a dialog box titled 'Please set up your security questions.' with a close button (X) in the top right corner. The dialog contains three sets of questions, each with a dropdown menu for the question and a text input field for the answer. The questions are labeled 'Question 1', 'Question 2', and 'Question 3'. The dropdown menus are currently set to '-- Select One --'. At the bottom right of the dialog are two buttons: 'Cancel' and 'Submit'.

Modify Administrator Credentials

The administrator credentials are used to access the device's system settings. You can set both (PIN and RF Card) or choose one.

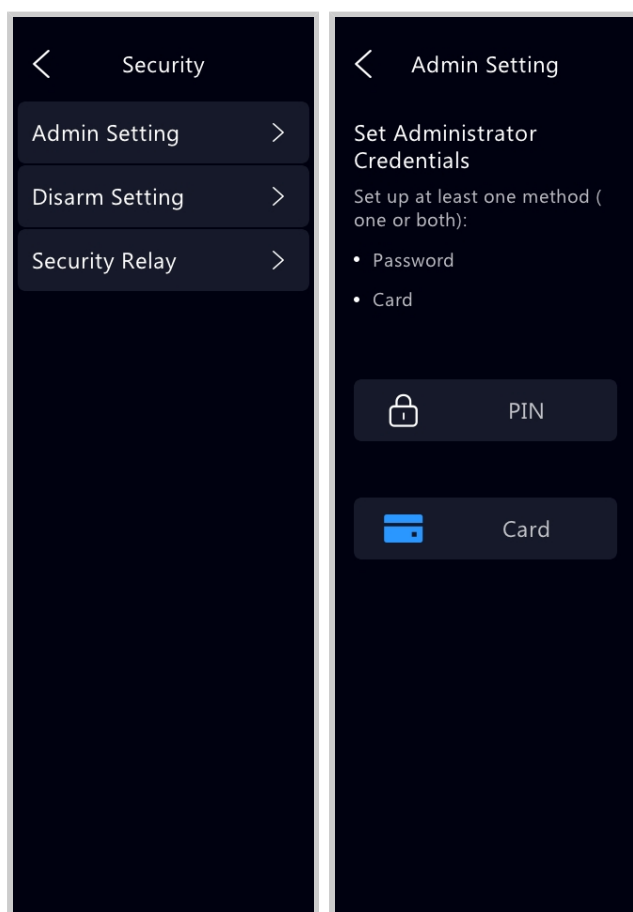
To set it up, go to the **System > Security > Administrator Credentials** interface.



The interface is titled "Administrator Credentials". It contains two input fields: "PIN Code" with a masked value "****" and "RF Card". A blue button labeled "+ Obtain" is positioned to the right of the RF Card field.

- **PIN Code:** Set the 6 to 8 digits.
- **RF Card:** Click **Obtain** while placing the card on the device.

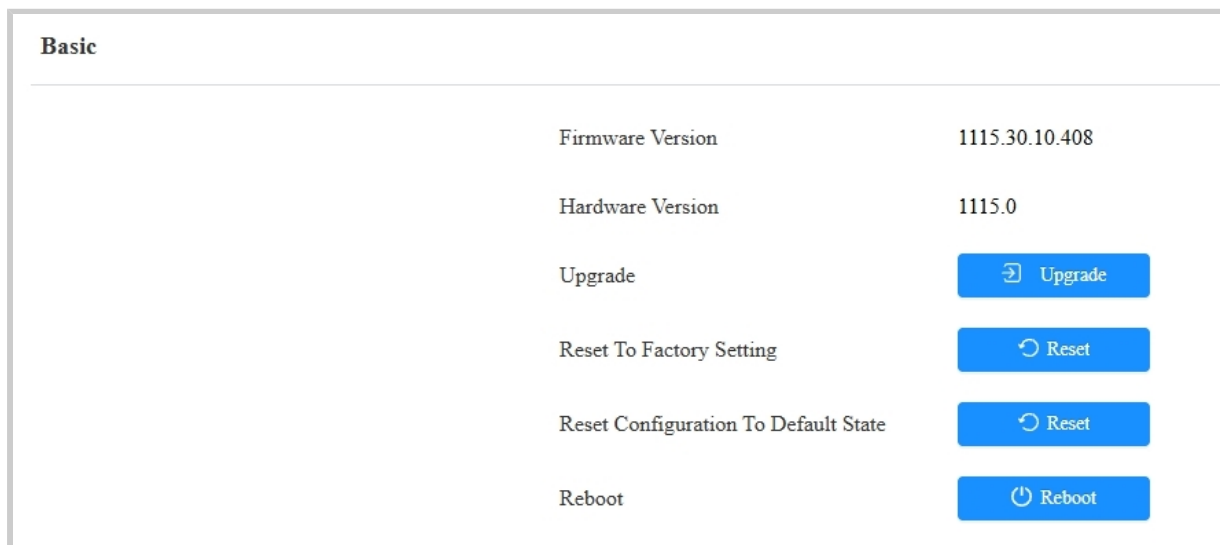
You can also modify the credentials on the **Setting > Security > Admin Setting** screen.



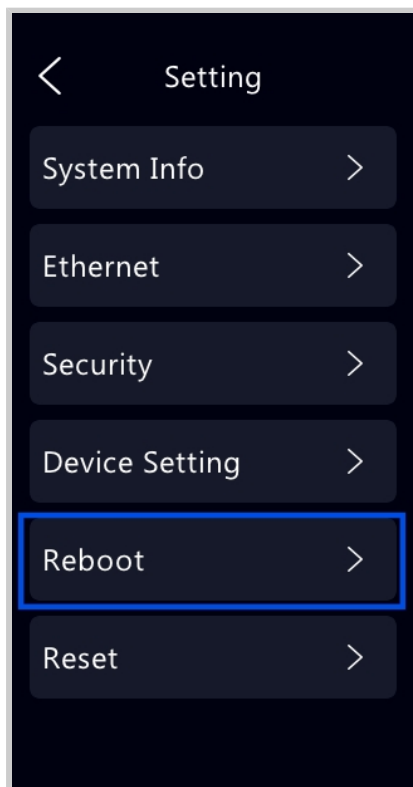
System Reboot & Reset

Reboot

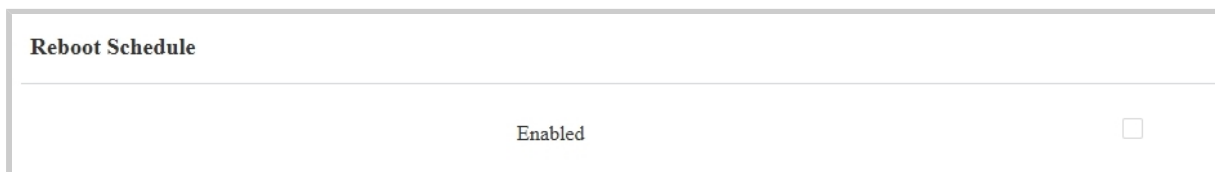
Reboot the device on the web **System > Upgrade** interface.



Or, reboot it on the **Setting** screen.



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



Reset

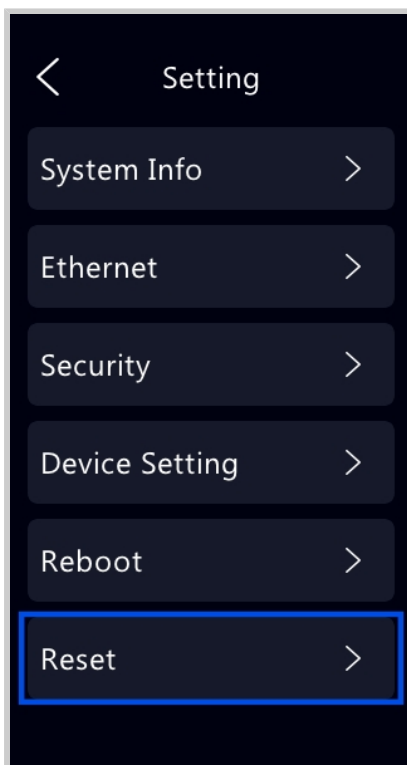
The device provides two reset options:

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

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

Basic	
Firmware Version	1115.30.10.408
Hardware Version	1115.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reset Configuration To Default State	 Reset
Reboot	 Reboot

Or, reset it on the **Setting** screen.



Tip

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

- Press the button and hold it for about 3 seconds.
- The backlight of the card reader area and the fill light will light up, and the device will go into factory reset and reboot.

