Table of Contents

Akuvox A08 Access Control Terminal Administrator Guide

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX A08 ACCESS CONTROL

Administrator Guide

Thank you for choosing the Akuvox A08 access control terminal. This manual is intended for administrators who need to properly configure the access control terminal. This manual is written based on firmware version 108.30.11.22, and it provides all the configurations for the functions and features of the A08 access control terminal. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox A08 series integrates a door controller and card reader into a single device, significantly reducing costs for building operators. It provides versatile credentials such as PIN codes, QR scanning, wave-to-unlock via Bluetooth, and mobile access via NFC and RFID cards.

Changelog

What’s new in version 108.30.11.22:

- Support configuring Floor Starts From, Ground Floor, and Device Location in Lift Control settings.

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

Model Specifications and Differences

Model	A08S	A08K
Front Panel	Toughened Glass	Toughened Glass
Frame	Aluminum Alloy	Aluminum Alloy
RFID Card Reader	13.56MHz & 125kHz	13.56MHz & 125kHz
Relay Out	x1	x1
Inputs	x2	x2
Wiegand	✔	✔
RS485	✔	✔
Speaker	8Ω / 0.5W	8Ω / 0.5W
Tamper Proof Alarm	✔	✔
Ethernet Port	RJ45, 10/100Mbps adaptive	RJ45, 10/100Mbps adaptive
Power Output	12V 600mA	12V 600mA
Power Supply	12V DC connector (if not using PoE)	12V DC connector (if not using PoE)
QR Code Unlock	✔	X
Bluetooth Unlock	✔	X

Supported Card Types

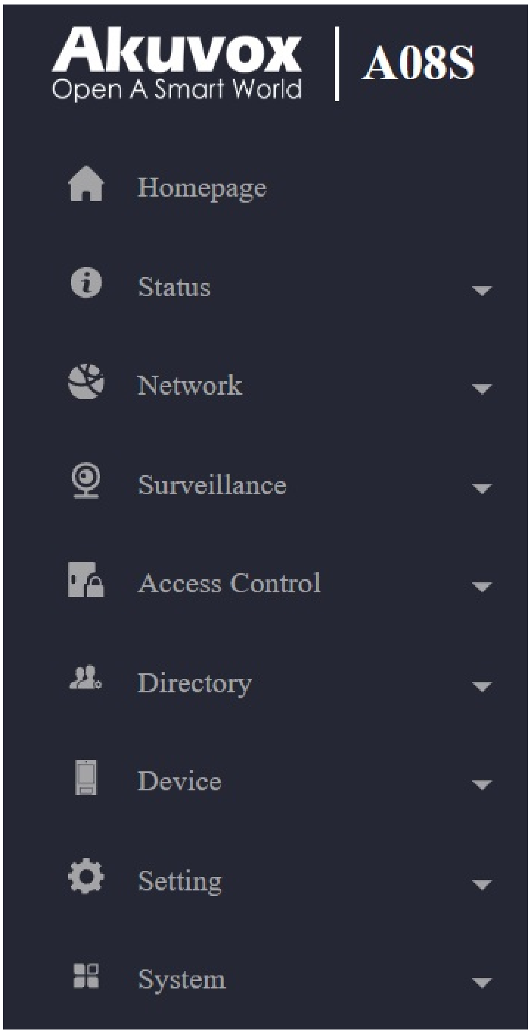
The device's firmware should be 108.30.10.149 or higher:

- ID Card:
    - EM4100
    - EM4200
    - HID-Prox
        - Only A08 with the HID-HF module supports reading the HID Prox cards, and the firmware version should be 108.30.10.121 or higher.
    - HID-iClass
        - Only A08 with the HID-LF module supports reading the HID iClass cards, and the firmware version should be 108.30.10.18/108.230.1.11 or higher.
- IC Card:
    - Mifare Ultralight C/EV1
    - Mifare Classic Compatible Card
    - Mifare Plus-S 2K
    - Mifare Desfire EV1 2K D21
    - Mifare Desfire EV2 D42
    - Mifare Desfire EV2 D22
    - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
    - NFC Type2 216
    - NFC Type2 215
- Felica Card
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
    - Mifare Classic 1K
    - Mifare S50-1K Card
    - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

- HID-iClass Clamshell Card
    - Only A08 with the HID-LF module supports reading the HID iClass cards, and the firmware version should be 108.30.10.18/108.230.1.11 or higher.
- HID-PROXCARD-II Card
    - Only A08 with the HID-HF module supports reading the HID Prox cards, and the firmware version should be 108.30.10.121 or higher.

Introduction to Configuration Menu

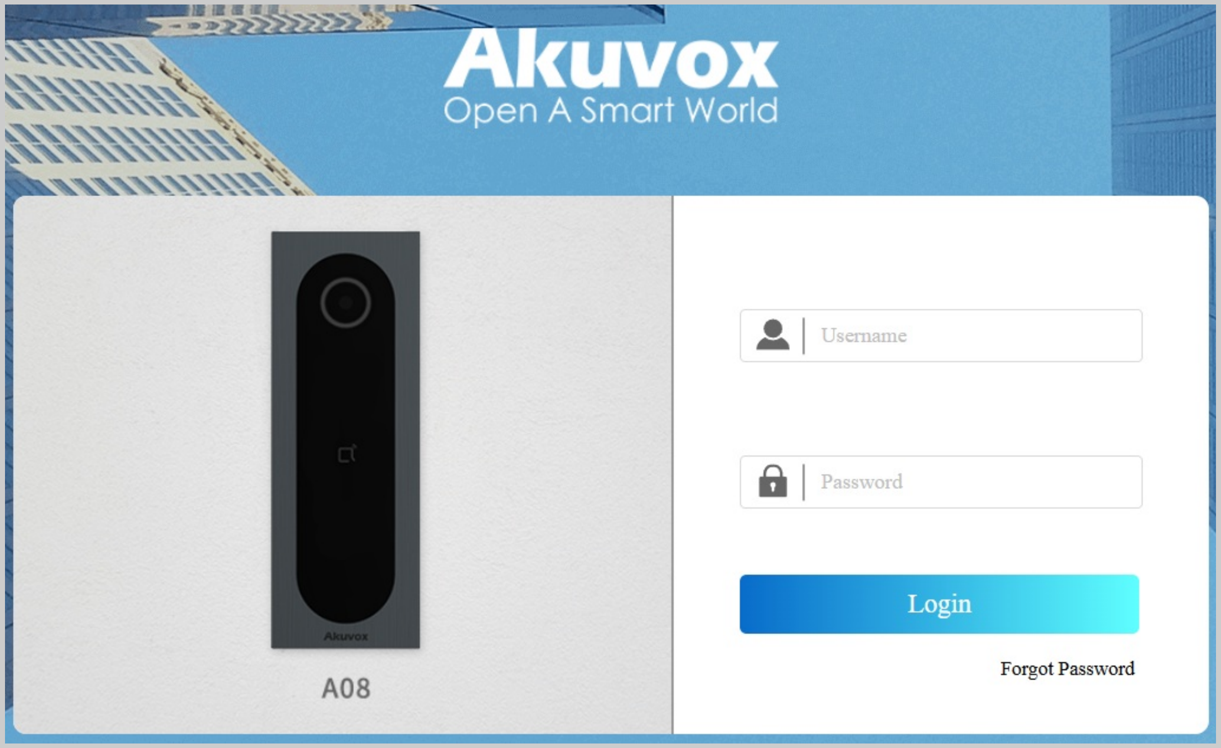
- **Status**: This section gives you basic information such as product information, network information, and access logs.
- **Network**: This section covers LAN port settings.
- **Surveillance**: This section is for third-party camera setup.
- **Access Control**: This section covers relays, inputs, web relays, card settings, Bluetooth settings, and more.
- **Directory**: This section is for user management.
- **Device**: This section includes light, Wiegand, lift control, and audio settings.
- **Setting**: This section deals with time and language settings, relay schedule, action, HTTP API settings, etc.
- **System**: This section covers device firmware upgrade, maintenance, auto-provisioning, and security.



Akuvox
Open A Smart World
A08S
Homepage
Status
Network
Surveillance
Access Control
Directory
Device
Setting
System

Access the Device

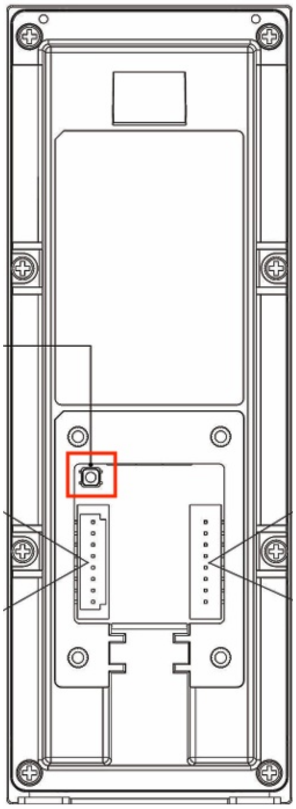
Before configuring A08, please make sure the device is installed correctly and connected to a normal network. Using the Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to log into the web browser. The initial username and password are **admin**.



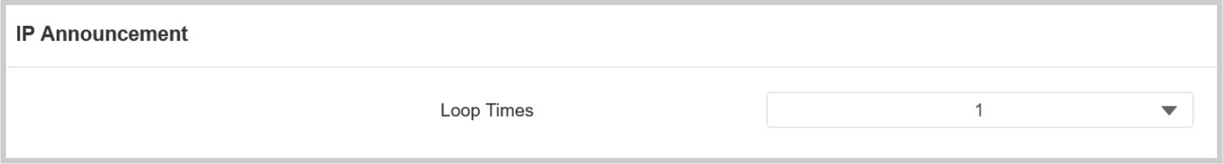
Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See 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.

You can also obtain the IP address by pressing the **Reset** button at the back of the device once. The device will announce the IP address automatically.



You can set up the loop times of the IP announcement on the **Device > Audio > IP Announcement** interface.



IP Announcement

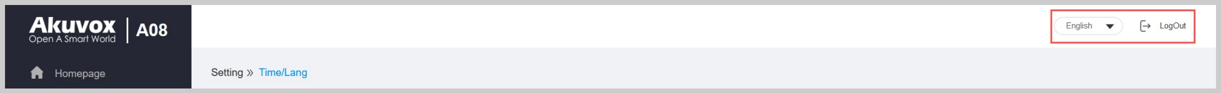
Loop Times: 1

Language and Time

Language

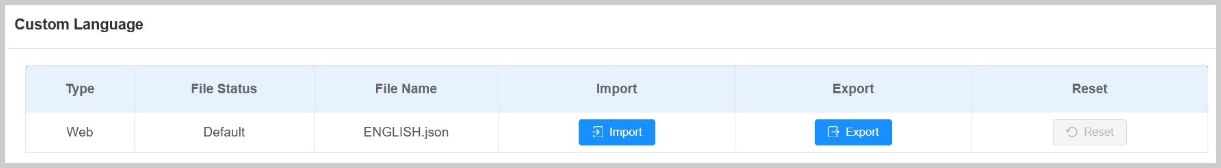
You can switch the web language in the upper right corner.

The device supports English, Simplified Chinese, and Spanish.



You can customize interface text including configuration names and prompt text.

To set it up, go to **Setting > Time/Lang** interface. Export and edit the .json file. Then import the file to the device.



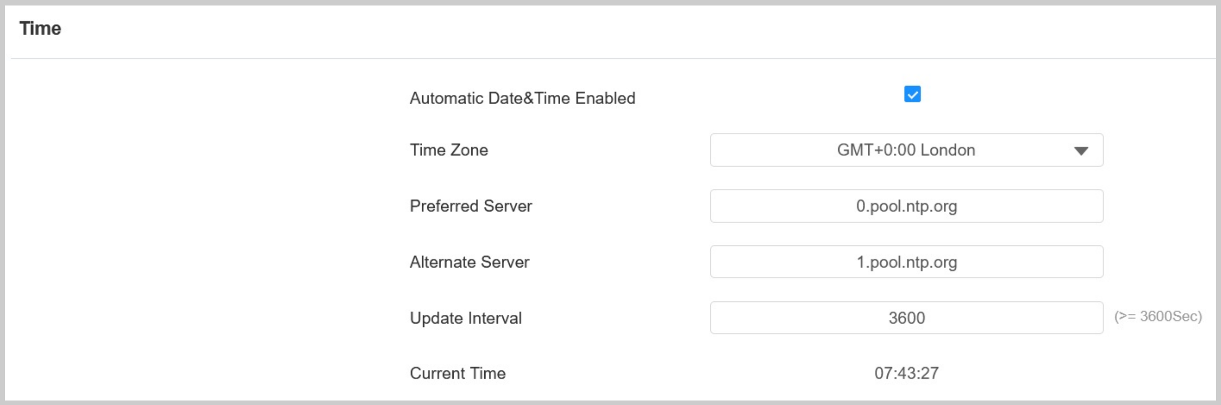
Custom Language

Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	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 up time, go to **Setting > Time/Lang** interface.



Time

Automatic Date&Time Enabled	☑
Time Zone	GMT+0:00 London
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600Sec)
Current Time	07:43:27

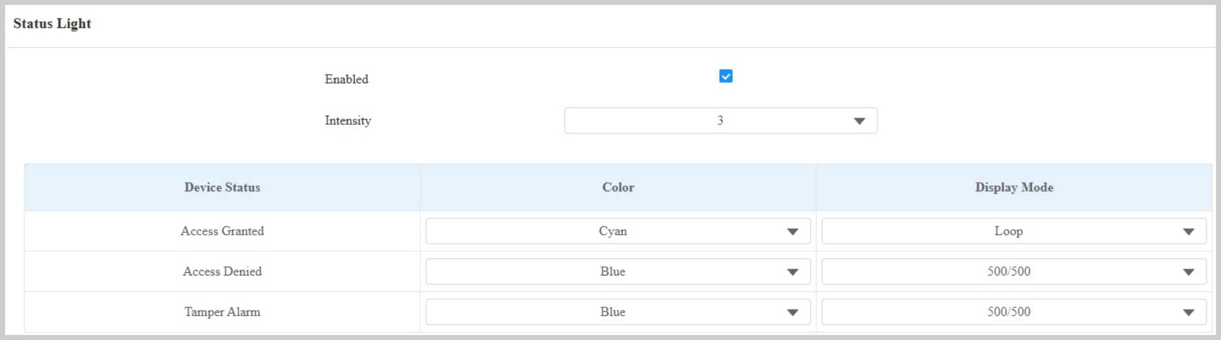
- **Automatic Date&Time Enabled**: Set whether the device updates the time automatically via the Network Time Protocol(NTP) server.
- **Date/Time**: Set the date and time for the device manually when you disable the automatic date and time service.
- **Time Zone**: Select the specific time zone based on where the device is used. The default time zone is GMT+0:00.
- **Preferred Server**: Enter the primary NTP server address for updating the time. The default NTP server address is 0.pool.ntp.org.
- **Alternate Server**: Enter the backup NTP server address when the primary one fails.
- **Update Interval**: Set the time update interval. For example, if you set it as 3600s, the device will send a request to the NTP server for the time update every 3600 seconds.
- **Current Time**: Display the current device time.

LED Setting

Status Light

You can turn on or off the status light and adjust its brightness.

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



Status Light

Enabled ☑

Intensity 3

Device Status	Color	Display Mode
Access Granted	Cyan	Loop
Access Denied	Blue	500/500
Tamper Alarm	Blue	500/500

- **Intensity**: The level ranges from 1-5. The higher the value is, the brighter it is.
- **Color**: Three colors are available, Cyan, Blue, and Green.
- **Display Mode**: Set the different flashing frequencies.

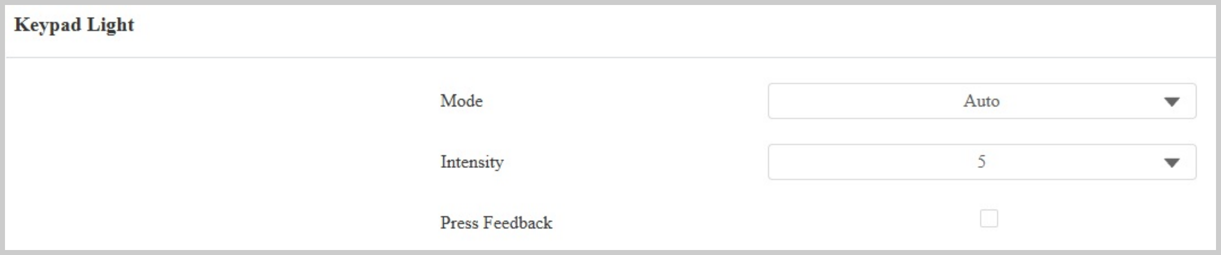
Status Light Description:

LED Color	LED Status	Description
Cyan	Light on briefly	The device starts up.
	The light circle rotates once.	Door-opening succeeds.
Blue	Flashing briefly	Door-opening fails.
	Flashing continuously	The tamper alarm is triggered.

Keypad Light

You can set up the keypad light. For example, keep the light on, and users can locate the device conveniently in a dark environment.

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



Keypad Light

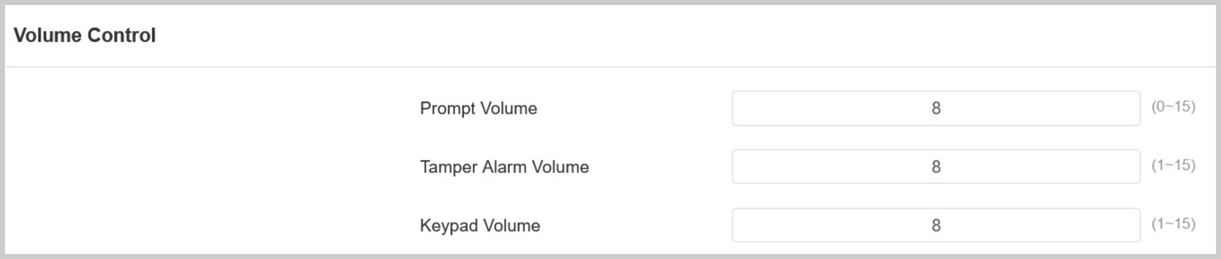
Mode	Auto
Intensity	5
Press Feedback	□

- **Mode**:
  - **Auto**: The keypad lights up when users approach or touch it.
  - **On**: Turn on the keypad light all the time.
  - **Schedule**: When enabled, select the schedule when the keypad light will stay on.
- **Intensity**: Adjust the brightness of the keypad light. The higher the value is, the brighter the light is.
- **Press Feedback**: When enabled, the keypad light flashes each time the user taps a key.

Volume and Tone

Volume and tone configuration include keypad volume, prompt volume, tamper alarm volume, and open-door tone configuration.

To set it up, go to **Device > Audio > Volume Control** interface.



Volume Control

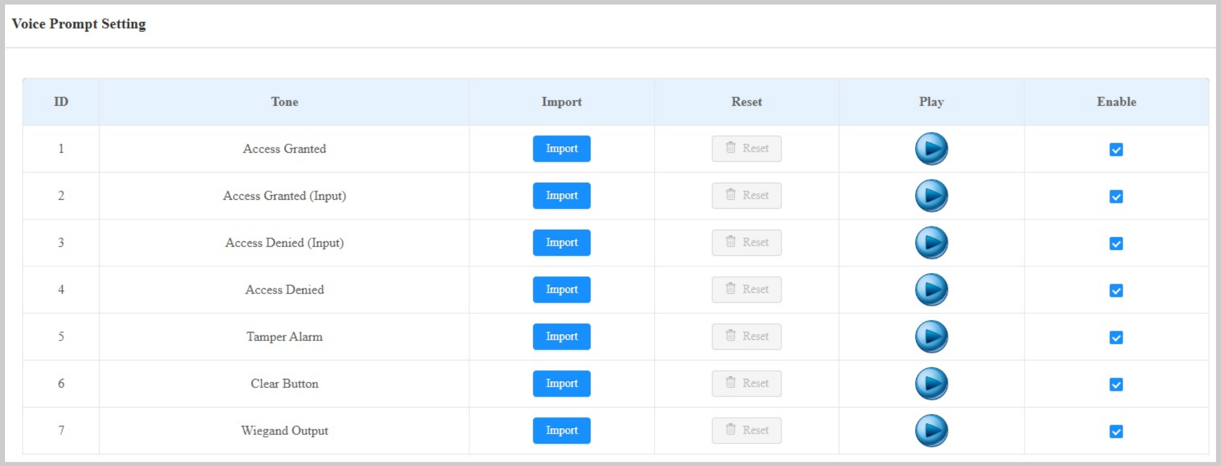
Prompt Volume	8	(0~15)
Tamper Alarm Volume	8	(1~15)
Keypad Volume	8	(1~15)

- **Prompt Volume**: Set the voice prompt volume. The default volume is 8.
- **Tamper Alarm Volume**: Set the volume when the tamper alarm is triggered. The default volume is 8.
- **Keypad Volume**: Set the volume when pressing the keypad. The default volume is 8.

Voice Prompts Upload

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

To set it up, go to **Device > Audio > Voice Prompt Setting** interface.



Voice Prompt Setting

ID	Tone	Import	Reset	Play	Enable
1	Access Granted	Import	Reset	▶	☑
2	Access Granted (Input)	Import	Reset	▶	☑
3	Access Denied (Input)	Import	Reset	▶	☑
4	Access Denied	Import	Reset	▶	☑
5	Tamper Alarm	Import	Reset	▶	☑
6	Clear Button	Import	Reset	▶	☑
7	Wiegand Output	Import	Reset	▶	☑

- **Clear Button**: The prompt is played when users press ☒ button.

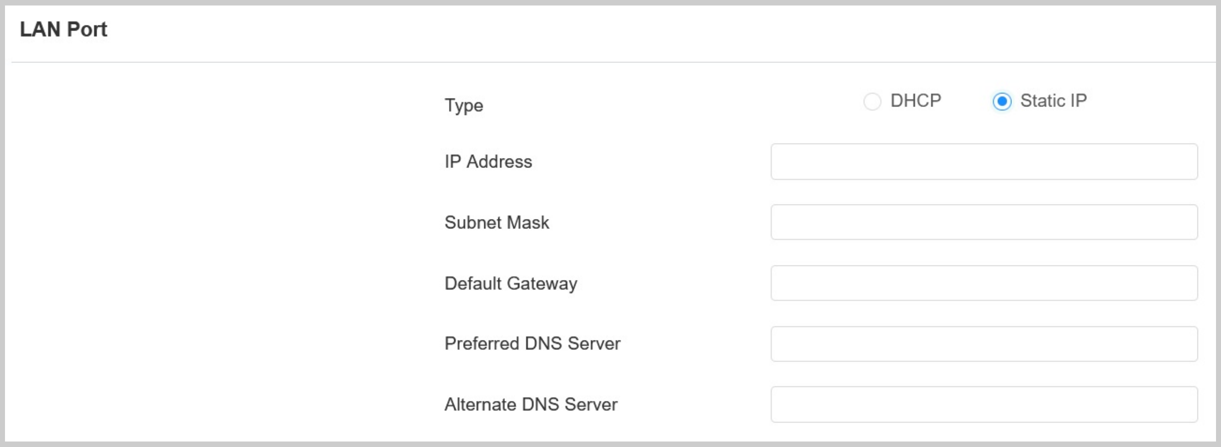
- **Wiegand Output**: The prompt is played when the QR code scanned or PIN code entered is output via Wiegand.

> **Note**
>
> File Format: WAV; Size: < 200KB; Sample Rate: 16000; Bits: 16.

Network Setting

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

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



LAN Port

Type ○ DHCP ● Static IP

IP Address

Subnet Mask

Default Gateway

Preferred DNS Server

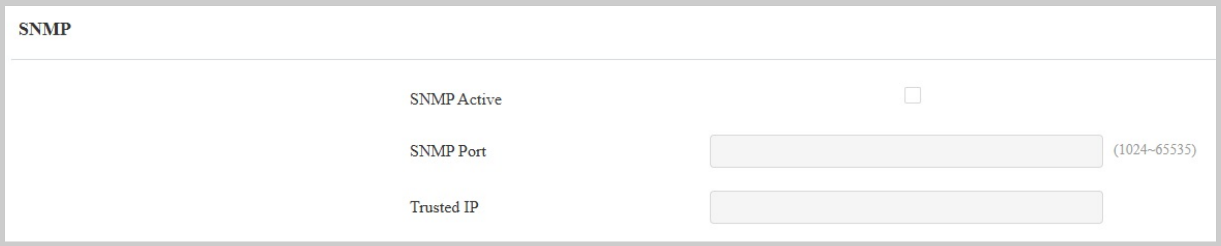
Alternate DNS Server

- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the access control terminal will be assigned by the DHCP server with 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.
- **Subnet Mask**: Set up the subnet mask according to the actual network environment.
- **Default Gateway**: Set up the correct gateway according to the IP address.
- **Preferred/Alternate DNS Server**: Set up the preferred or alternate Domain Name Server(DNS) server according to the actual network environment. The preferred DNS server is the primary server while the alternate DNS server is the secondary one. The secondary server is for backup.

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** interface.



SNMP

SNMP Active □

SNMP Port (1024~65535)

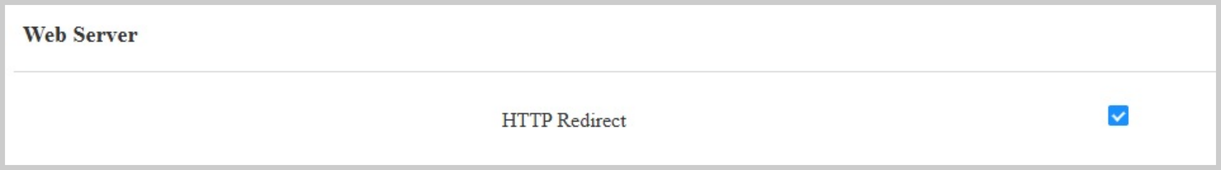
Trusted IP

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

Web HTTP Setting

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

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



Web Server

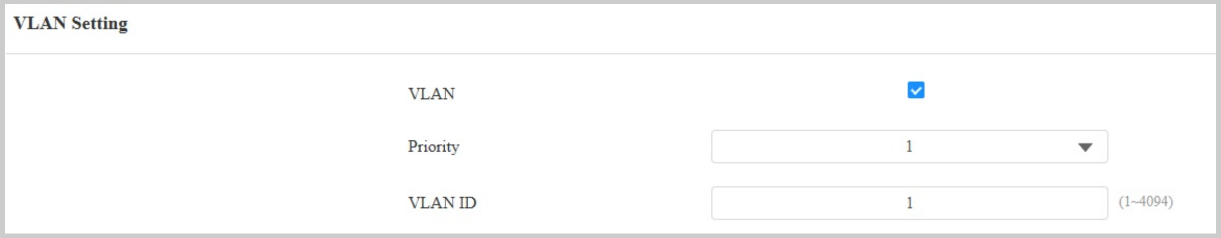
HTTP Redirect ☑

- **HTTP Redirec**t: When enabled, the device’s web settings can be accessed via HTTP protocol. When disabled, it will be redirected to the HTTPS. This setting is also effective for the HTTP API feature.

VLAN Setting

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

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



VLAN Setting

VLAN ☑

Priority: 1

VLAN ID: 1 (1~4094)

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

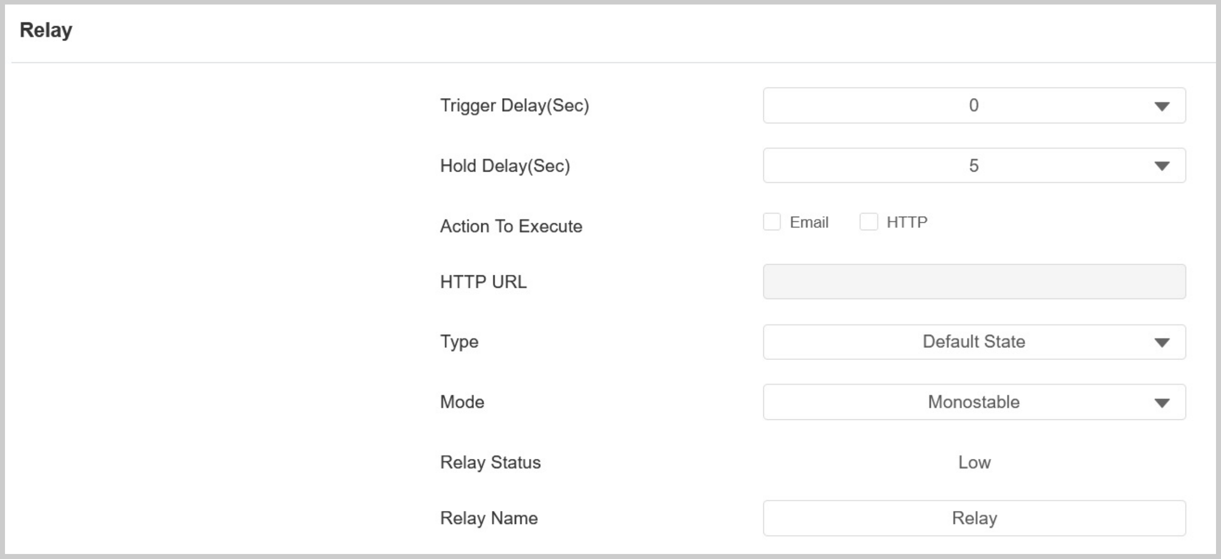
Relay Setting

You can configure the relay switch(es) for door access on the web interface.

Local Relay

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

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



Relay

Trigger Delay(Sec)	0
Hold Delay(Sec)	5
Action To Execute	□ Email □ HTTP
HTTP URL	
Type	Default State
Mode	Monostable
Relay Status	Low
Relay Name	Relay

- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **Action to Execute**: Check the action to be executed when the relay is triggered.

  - **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.
  - **Email**: Send a screenshot to the preconfigured Email address.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Type**: Determine the interpretation of the Relay Status regarding the state of the door:
  - **Default State**: A "Low" status in the Relay Status field indicates that the door is closed, while "High" indicates that it is opened.
  - **Invert State**: 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.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name**: Assign a distinct name for identification purposes.

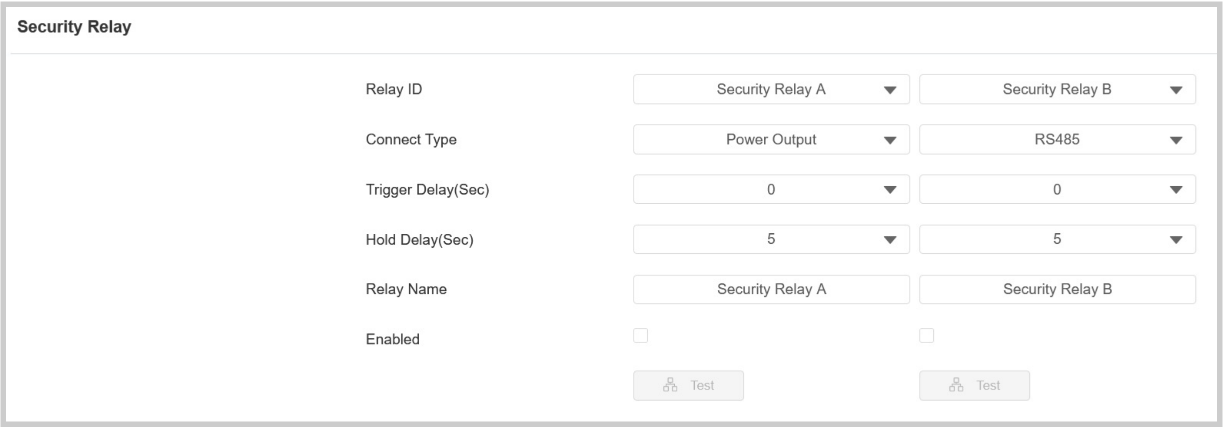
> **Note**
>
> External devices connected to the relay require separate power adapters.

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



Security Relay

Relay ID	Security Relay A ▼	Security Relay B ▼
Connect Type	Power Output ▼	RS485 ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼
Relay Name	Security Relay A	Security Relay B
Enabled	□	□
	Test	Test

- **Relay ID**: The specific relay for door access.
- **Connect Type**: The security relay connects to the device using Power Output or RS485.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.

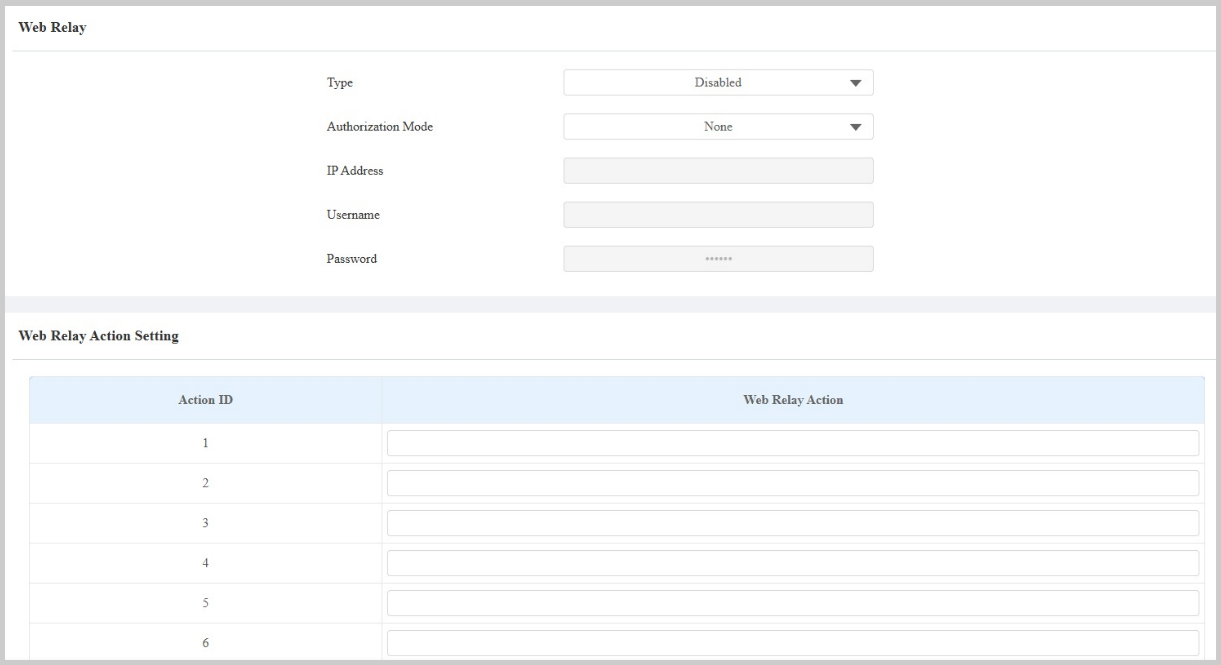
- **Relay Name**: Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Enabled**: When using the SR01 via RS485, you need to set the RS485 mode to **Others** on the **Device > RS485** interface.

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
1	
2	
3	
4	
5	
6	

- **Type**: Determine the type of relay activated when employing door access methods for entry.
  - **Disabled**: Only activate the local relay.
  - **Web Relay**: Only activate the web relay.
  - **Local Relay+Web Relay**: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **Authorization Mode**: Select the Authorization Mode between **None** and **Digest**. When Digest is selected, the username and password are used for authentication.
- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **Username**: The user name provided by the web relay manufacturer.
- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.
- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

NOTE

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

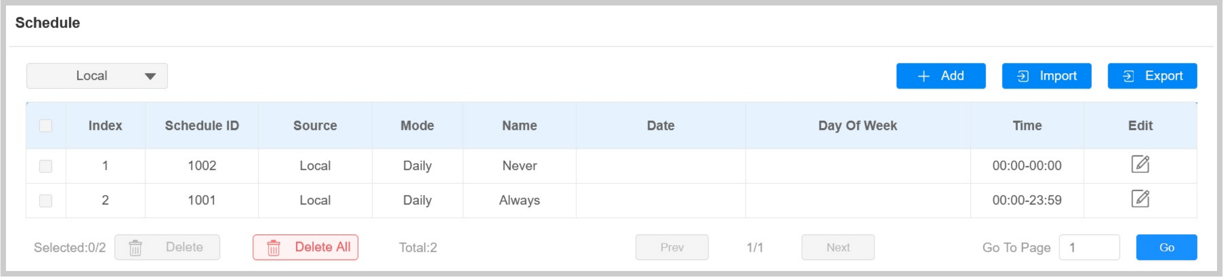
Access Control Schedule Management

Door Access Schedule

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

Create Door Access Schedule

To create a door access schedule, go to the **Setting > Schedule** interface.



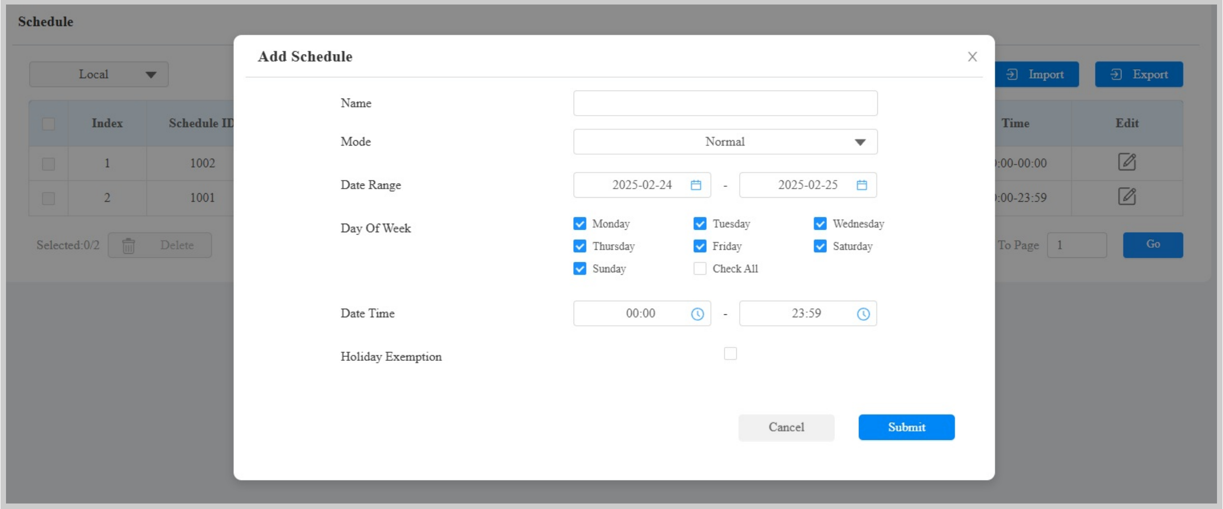
Schedule

Local ▾ + Add | Import | Export

□	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
□	1	1002	Local	Daily	Never			00:00-00:00	✎
□	2	1001	Local	Daily	Always			00:00-23:59	✎

Selected:0/2 Delete Delete All Total:2 Prev 1/1 Next Go To Page 1 Go

Click **+Add** to create a schedule.



Add Schedule

Name:

Mode: Normal ▾

Date Range: 2025-02-24 - 2025-02-25

Day Of Week: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday □ Check All

Date Time: 00:00 - 23:59

Holiday Exemption: □

Cancel Submit

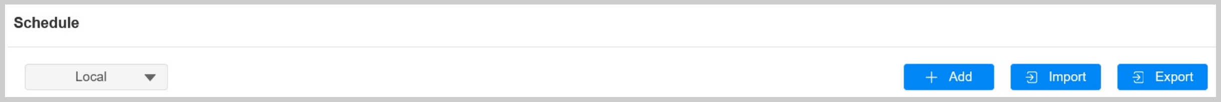
- **Name**: Name the schedule.
- **Mode**:

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

You can create door access schedules one by one or in bulk. You can export the current schedule file, edit it or add more schedules following the format, and import the new file to the desired devices. This helps you manage your door access schedules easily.

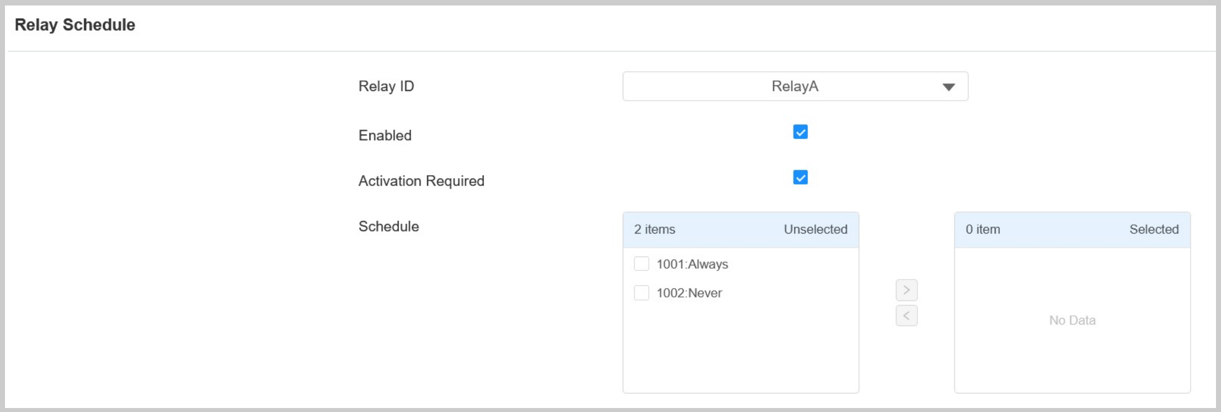
To set it up, go to the **Setting > Schedule** interface. The export file is in **TGZ** format. The import file should be in **XML** format.



Relay Schedule

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

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


Relay Schedule

Relay ID: RelayA

Enabled: ☑

Activation Required: ☑

Schedule:

2 items	Unselected
□ 1001:Always	
□ 1002:Never	

0 item	Selected
No Data	

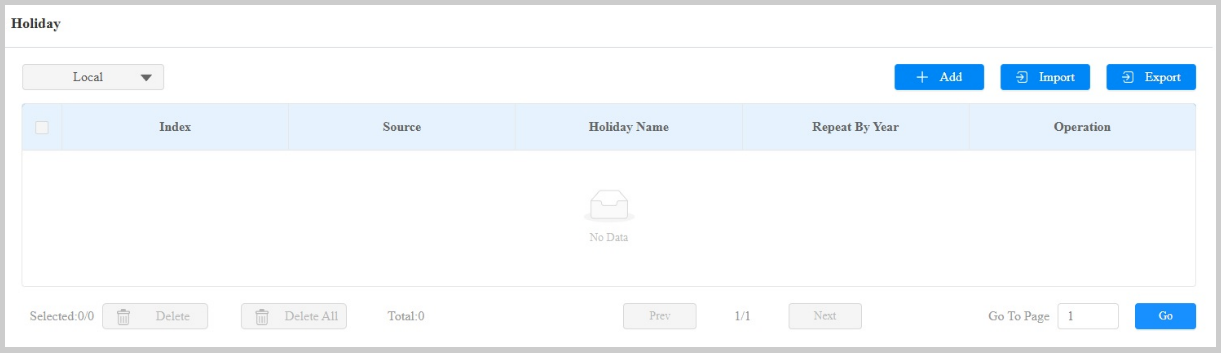
- **Relay ID**: Specify the relay you need to set up.
- **Activation Required**: It means only after the relay is triggered successfully for the first time, can it be triggered by device-supported access methods within the schedule.
- **Schedule:** Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

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

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.

To set it up, go to **Setting > Holiday** interface. Click **+Add**.

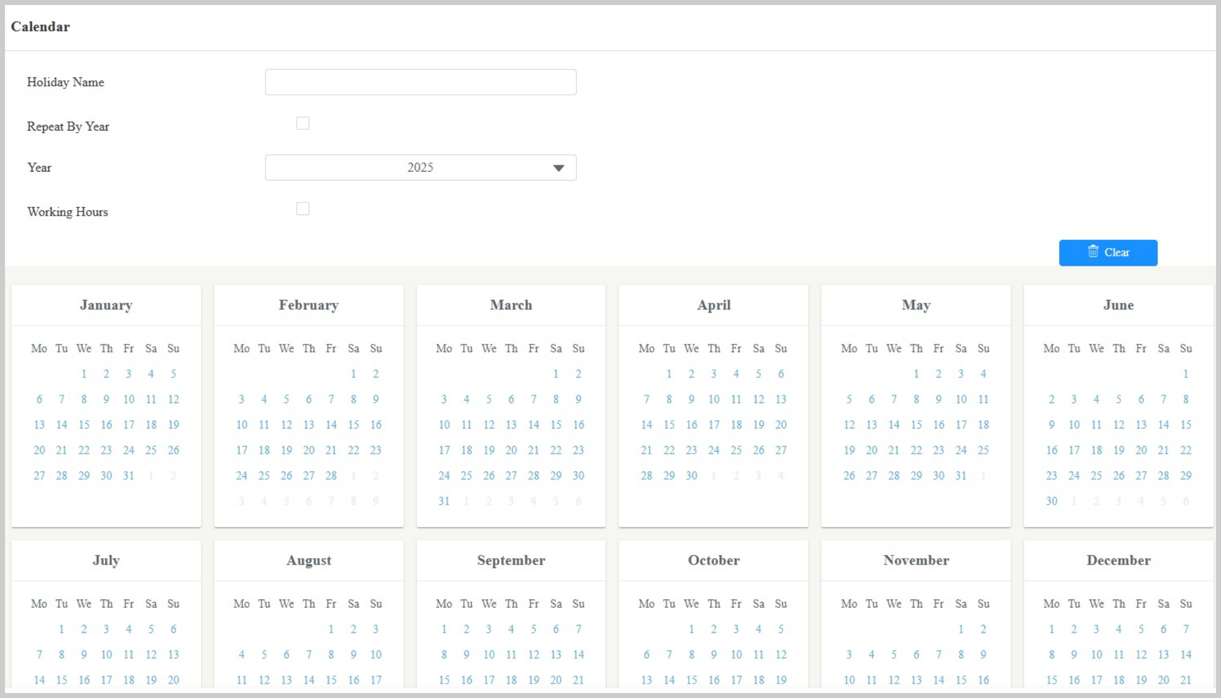


Holiday

□	Index	Source	Holiday Name	Repeat By Year	Operation

No Data

Selected:0/0 Total:0 1/1 Go To Page 1



Calendar

Holiday Name	
Repeat By Year	□
Year	2025
Working Hours	□

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	1	2

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	1	2
3	4	5	6	7	8	9

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	1	2	3	4	5	6

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	1	2	3	4

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	1

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	1	2	3	4	5	6

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

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

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

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

November

Mo	Tu	We	Th	Fr	Sa	Su
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16

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

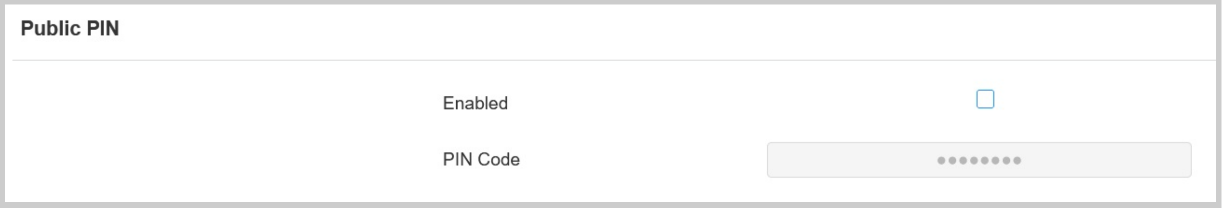
- **Holiday Name**: Enter the holiday name.
- **Repeat By Year**: Repeat the schedule every year.
- **Year**: Set the year and date of the holiday.
- **Working Hours**: When enabled, specify the time when authorized users can open doors.

Door-opening Configuration

Unlock by Public PIN

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

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



Public PIN

Enabled	□
PIN Code	••••••••

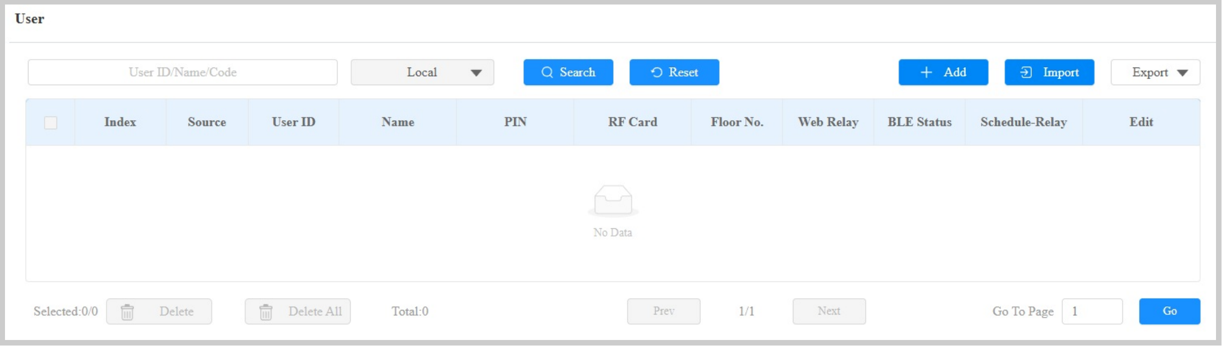
- **PIN Code**: Set a 3-8 digit PIN code accessible for universal use.

User-specific Access Methods

The private PIN code, RF card, QR code, and Bluetooth setting 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.

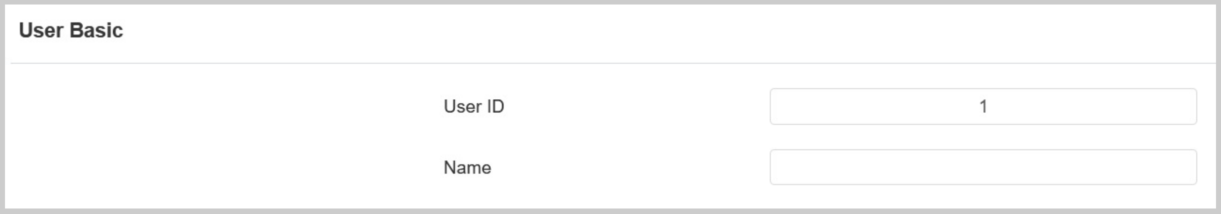
To add a user, go to **Directory > User** interface and Click **+Add**.



User

□	Index	Source	User ID	Name	PIN	RF Card	Floor No.	Web Relay	BLE Status	Schedule-Relay	Edit

No Data



User Basic

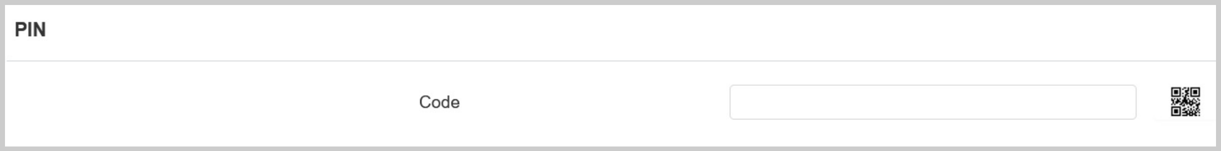
User ID 1

Name

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

Unlock by Private PIN Code

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



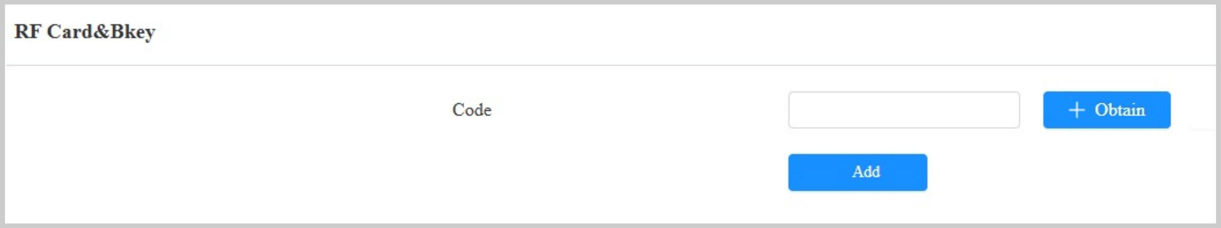
PIN

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.

Unlock by RF Card/Bkey

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



RF Card&Bkey

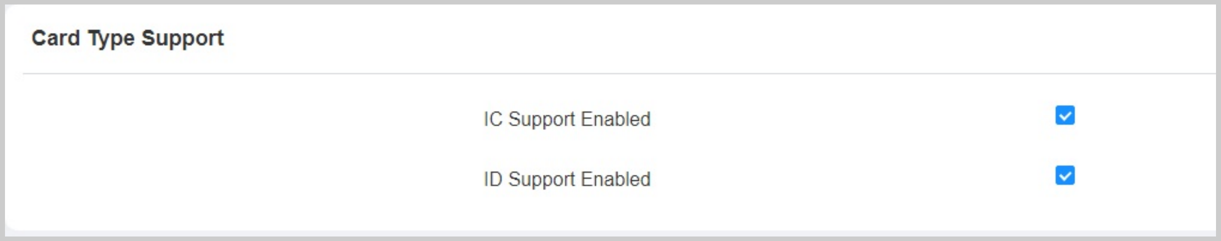
Code

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

Note:

- Click here to view the detailed steps of configuring Bkey.
- Each user can have a maximum of 5 cards added.
- The device allows to add 20,000 users.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the device for access.

You can set whether the device can read RF cards on the **Access Control > Card Setting** interface.

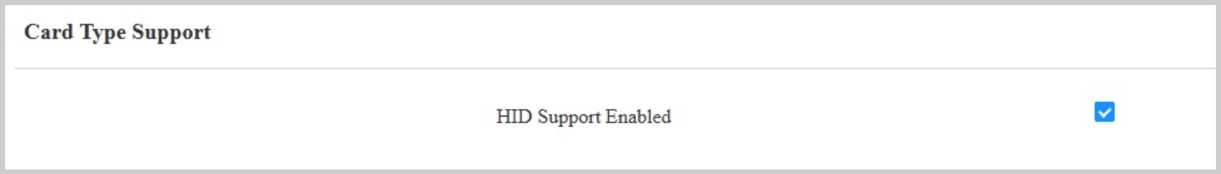


Card Type Support

IC Support Enabled ☑

ID Support Enabled ☑

A08 HID version supports reading HID cards, you can enable/disable this feature.



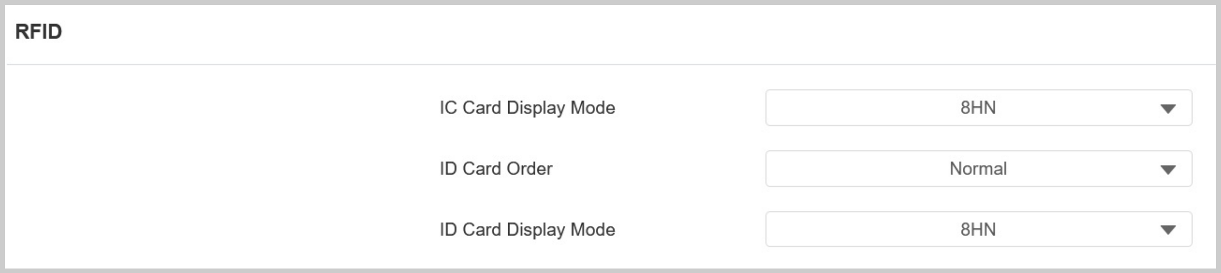
Card Type Support

HID Support Enabled ☑

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.

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



RFID

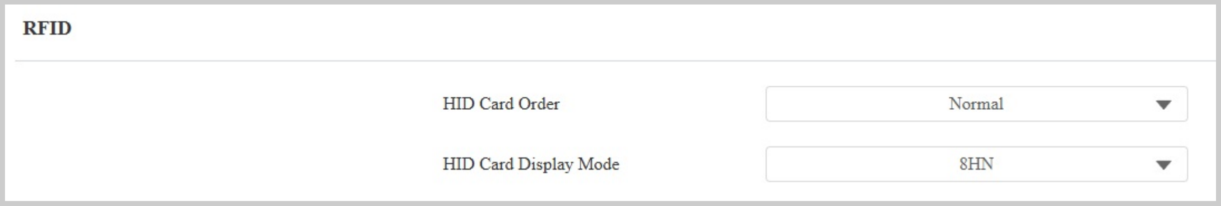
IC Card Display Mode: 8HN

ID Card Order: Normal

ID Card Display Mode: 8HN

- **IC/ID Card Display Mode**: Set the card number format from the provided options. The default format in the device is 8HN.
- **ID Card Order**: Set the ID card reading mode between Normal and Reversed.

A08 HID supports reading HID cards, you can set up the HID card order and display mode.



RFID

HID Card Order: Normal

HID Card Display Mode: 8HN

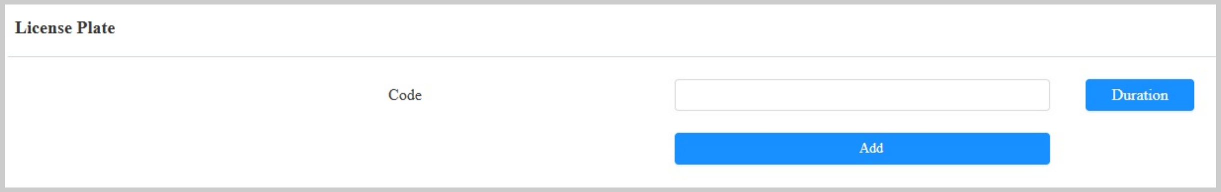
- **HID Card Order**: Set the card reading mode between Normal and Reversed.
- **HID Card Display Mode**: Set the card number format from the provided options. The default format in the device is 8HN.

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.



License Plate

Code:

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

Unlock by Bluetooth

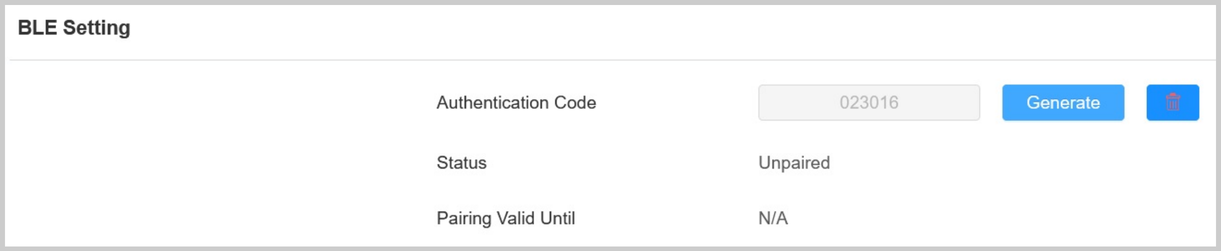
A08 supports opening the door via Bluetooth-enabled My MobileKey or SmartPlus App. Users can either open the door with the apps in their pockets or wave their phones towards the device as they get closer to the door.

Note

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

Unlock via My MobileKey

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



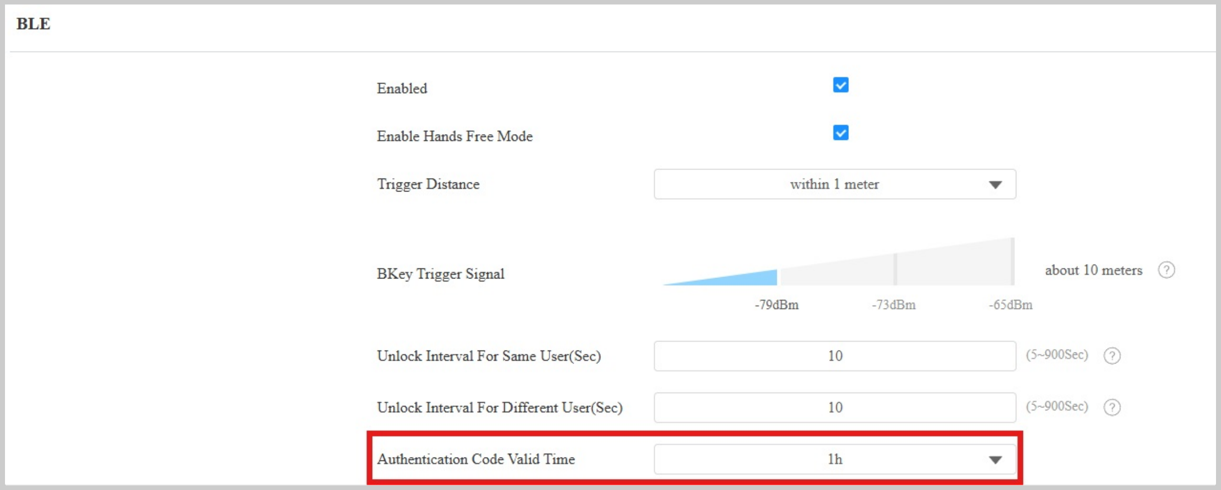
BLE Setting

Authentication Code	023016	Generate
Status	Unpaired	
Pairing Valid Until	N/A	

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

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

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



BLE

Enabled	☑	
Enable Hands Free Mode	☑	
Trigger Distance	within 1 meter	
BKey Trigger Signal	-79dBm -73dBm -65dBm	about 10 meters
Unlock Interval For Same User(Sec)	10	(5~900Sec)
Unlock Interval For Different User(Sec)	10	(5~900Sec)
Authentication Code Valid Time	1h	

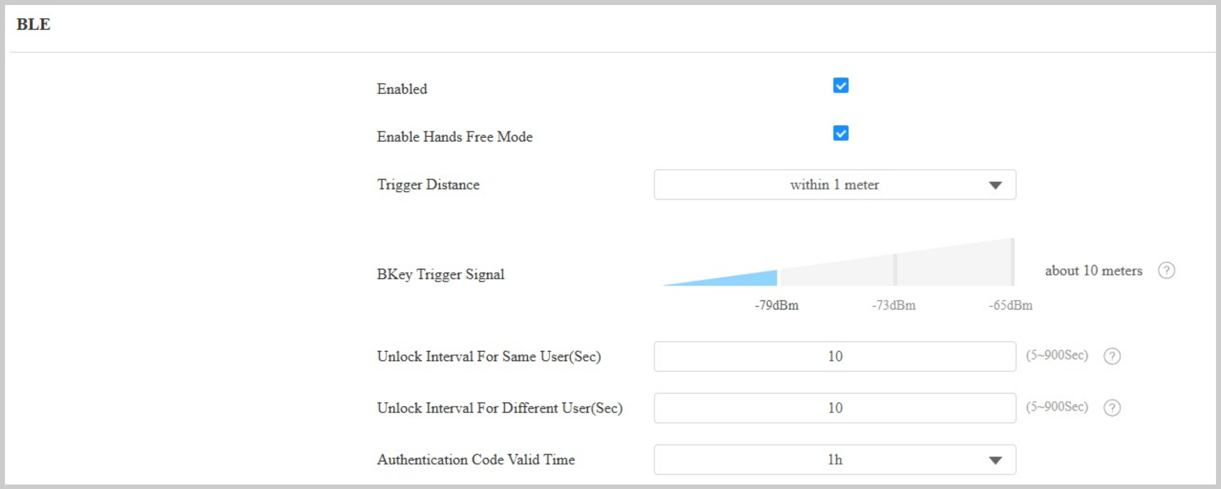
- **Authentication Code Valid Time**: Set the time from 15 minutes to 24 hours, or Forever.

Note

- Only A08S supports this feature.

Bluetooth Settings

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



BLE

Enabled ☑

Enable Hands Free Mode ☑

Trigger Distance: within 1 meter

BKey Trigger Signal: about 10 meters

Unlock Interval For Same User(Sec): 10 (5~900Sec)

Unlock Interval For Different User(Sec): 10 (5~900Sec)

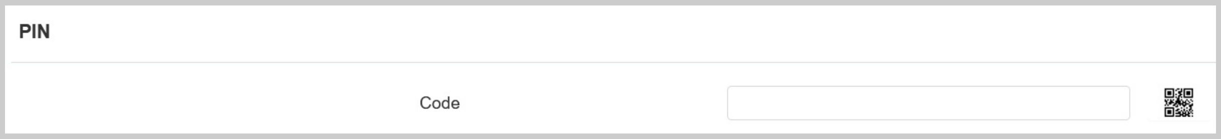
Authentication Code Valid Time: 1h

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

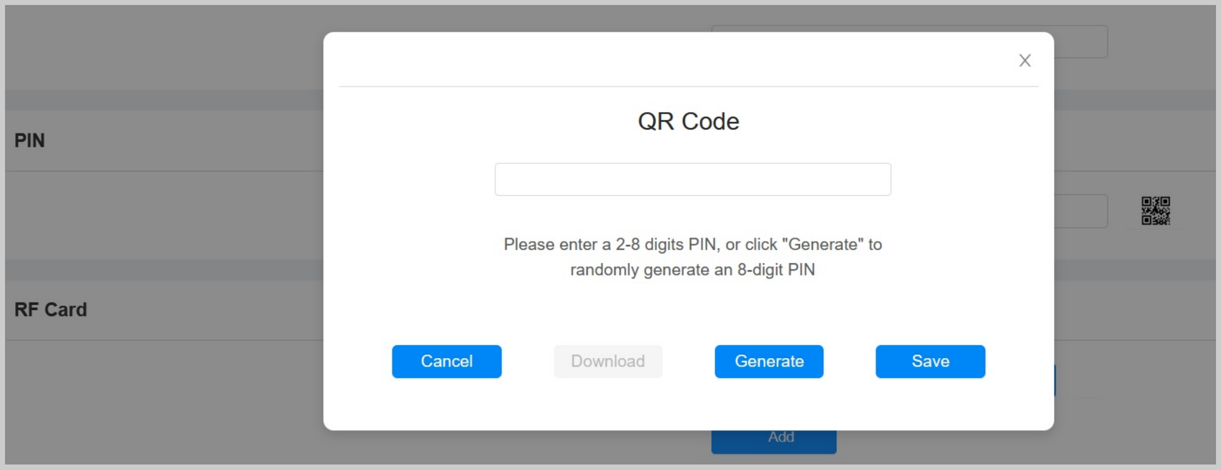
> **Note**
>
> To learn about detailed configuration steps of different Bluetooth-based access methods, you can click the following articles.
>
> - Unlock by Bluetooth via My MobileKey App.
> - Unlock by Bluetooth via SmartPlus App.
> - Open the Door via Bkey.

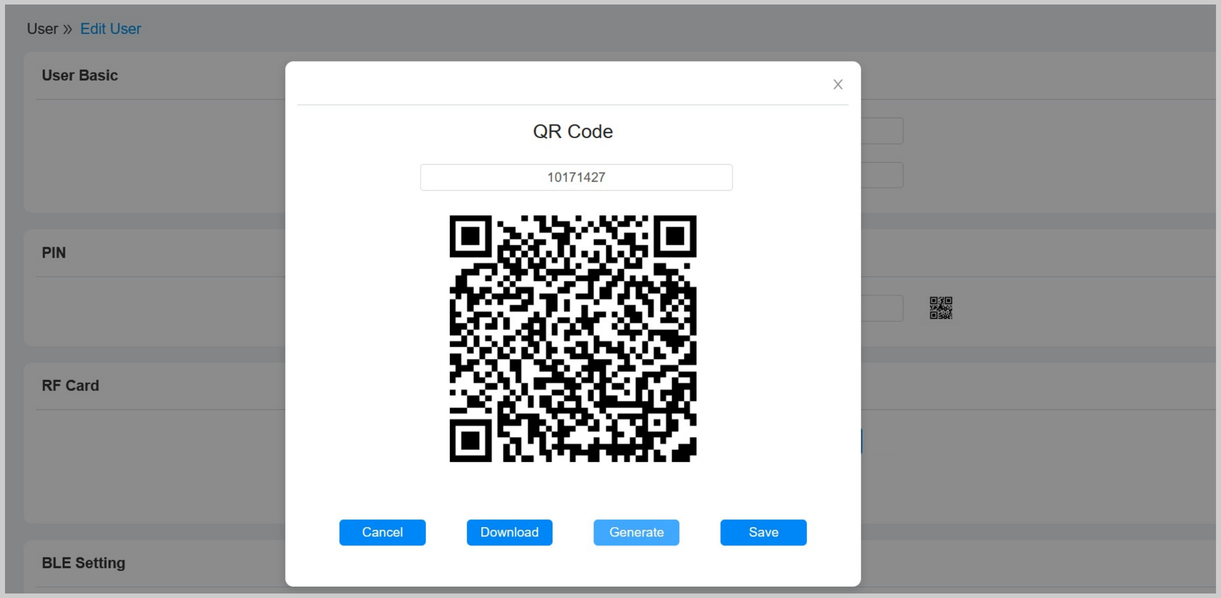
Unlock by QR Code

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



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


PIN
RF Card
QR Code
×
Please enter a 2-8 digits PIN, or click "Generate" to randomly generate an 8-digit PIN
Cancel
Download
Generate
Save
Add

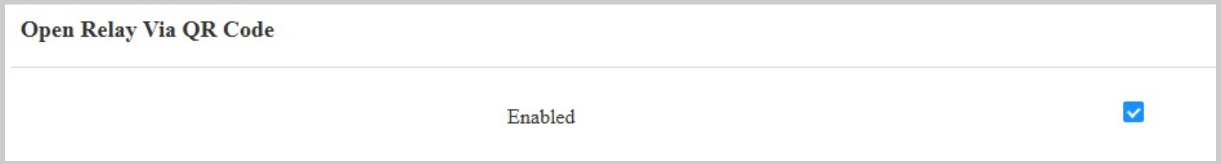


QR Code: 10171427

- **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.

> **Note**
>
> Only A08S supports this feature.

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

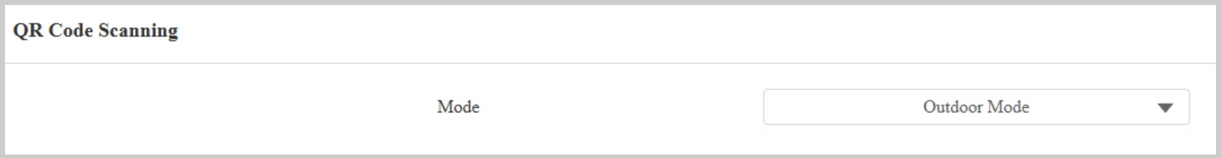


Open Relay Via QR Code

Enabled ☑

Besides, you can select the QR code scanning environment so that the device can better recognize the QR code.

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



QR Code Scanning

Mode: Outdoor Mode

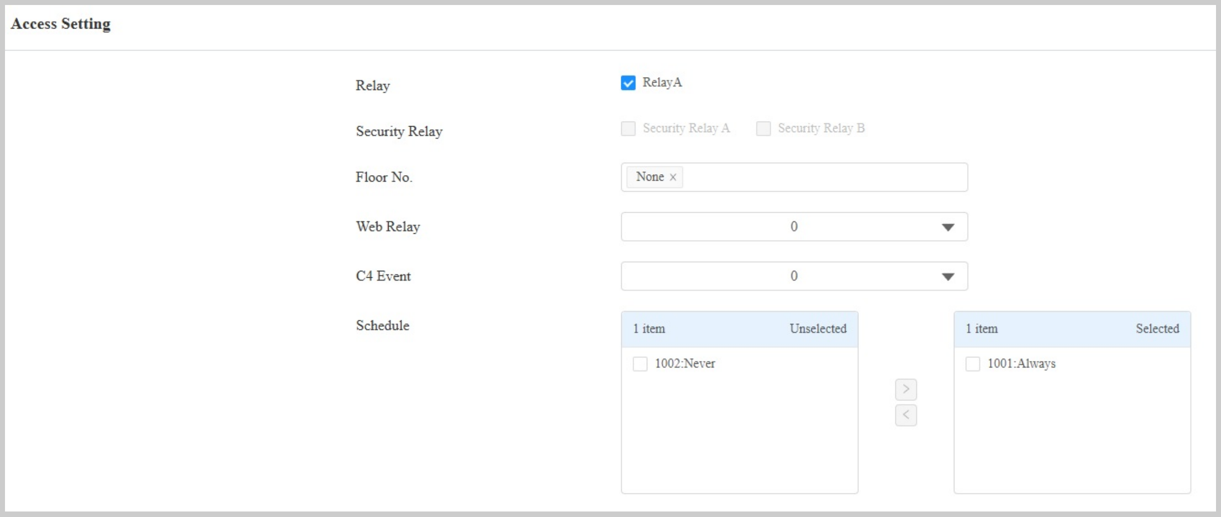
- **Outdoor Mode**: The device is installed outdoors.

- **Indoor Mode**: The device is installed indoors.

Access Setting

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

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



Access Setting

Relay: ☑ RelayA

Security Relay: □ Security Relay A □ Security Relay B

Floor No.: None ×

Web Relay: 0

C4 Event: 0

Schedule:

1 item Unselected
□ 1002:Never

1 item Selected
□ 1001:Always

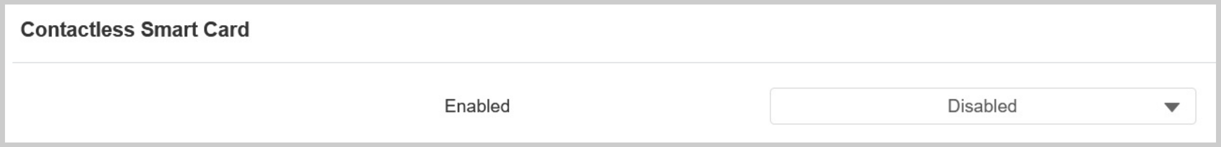
- **Relay**: Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **Security Relay**: Select the security relay that you've configured on the Security Relay interface.
- **Floor No.** : Specify the accessible floor(s) to the user via the elevator.
- **Web Relay**: Specify the ID of web relay action commands that you've configured on the Web Relay interface. A default value of 0 indicates that the web relay will not be triggered.
- **C4 Event**: When the device integrates with C4 devices, select the C4 event(s). When users use their credentials, the events will be triggered. You may refer to the manual Akuvox Integration with Control4 to learn the integration steps.
- **Schedule**: Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:

- **Always**: Allows door opening without limitations on door open counts during the valid period.
- **Never**: Prohibits door opening.

Contactless Smart Card

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

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



Contactless Smart Card

Enabled: Disabled

- **Enabled**: Select from Disabled, NFC, Felica, and NFC & Felica.

Note

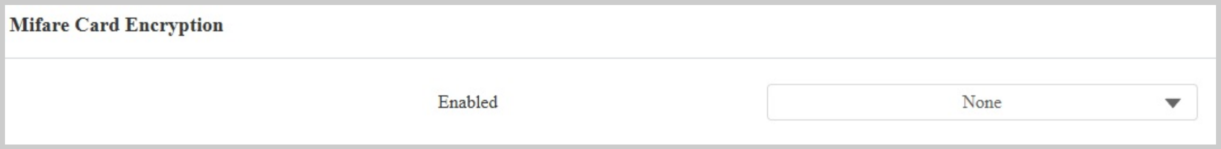
- The NFC feature is not available on iPhones.
- Click **here** to view how to open doors via NFC.

Mifare Card Encryption

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** interface.



Mifare Card Encryption

Enabled: None

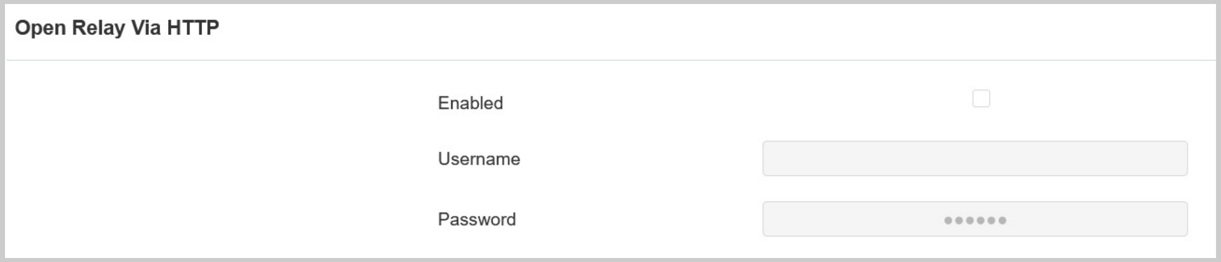
- **Mifare**:

  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
- **Mifare DESFire**:
  - **App ID**: A 6-digit hexadecimal number
  - **File ID**: The ID of the encrypted file of the app, which can be a number from 0 to 31.
  - **Crypto**: The encryption method, either AES or DES.
  - **Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.
- **Plus**: You can set up three choices. This means you can use three types of Mifare Plus cards. When swiping a card, as long as one of the choices matches its SL key, the card code in the block you specified will be output.
  - **Block**: Specify the block(s) to be read.
  - **SL3**: The key number within 32 bits.

Unlock by HTTP Command

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

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



Open Relay Via HTTP

Enabled □

Username

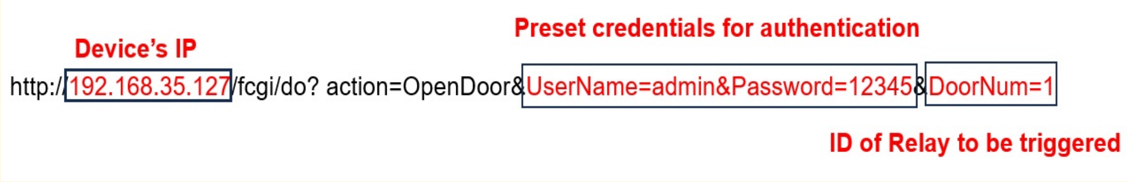
Password ••••••

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

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

Tip:

Here is an HTTP command URL example for relay triggering.



Preset credentials for authentication

Device's IP

```
http://192.168.35.127/fcgi/do? action=OpenDoor&UserName=admin&Password=12345&DoorNum=1
```

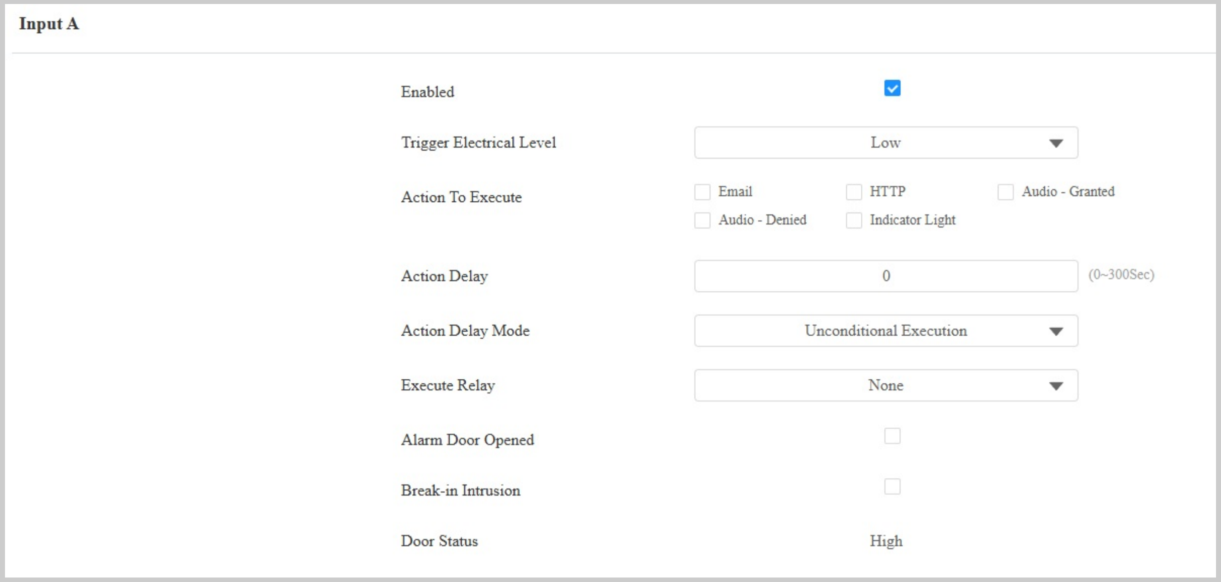
ID of Relay to be triggered

Unlock by Exit Button

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

Click here to watch the instruction video.

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



Input A

Enabled	☑
Trigger Electrical Level	Low
Action To Execute	□ Email □ HTTP □ Audio - Granted □ Audio - Denied □ Indicator Light
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution
Execute Relay	None
Alarm Door Opened	□
Break-in Intrusion	□
Door Status	High

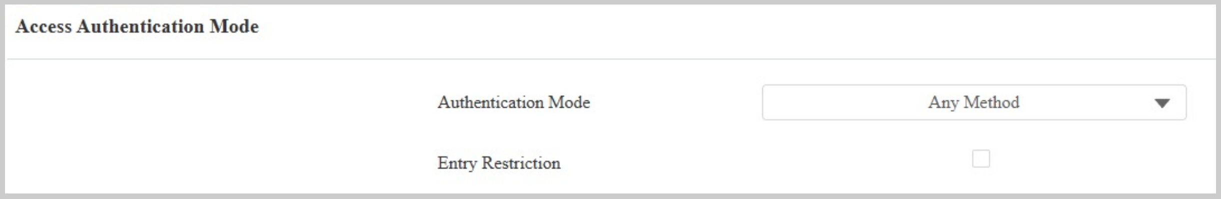
- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
  - **Email**: Send a screenshot to the preconfigured Email address.

  - **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
  - **Audio-Granted**: The device will announce “Access Granted” when the door is opened.
  - **Audio-Denied**: The device will announce “Access Denied” when opening the door fails.
  - **Indicator Light**: The indicator light will be on when the input is triggered.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server’s IP/Message content.
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.
- **Action Delay Mode**:
  - **Unconditional Execution**: The action will be carried out when the input is triggered.
  - **Execute If Input Still Triggered**: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Alarm Door Opened**: If enabled, when the door-opening time exceeds a limit, an alarm will be triggered.
  - **Door Opened Timeout**: Set the time limit for the door to stay open.
- **Break-in Intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. Click here to learn more information about this feature.
- **Door Status**: Display the status of the input signal.

Access Authentication Mode

The device allows dual authentication for door access, using the combination of PIN code and RF card. When the mode is set up, users must unlock the door in the order of the chosen methods.

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



Access Authentication Mode

Authentication Mode: Any Method

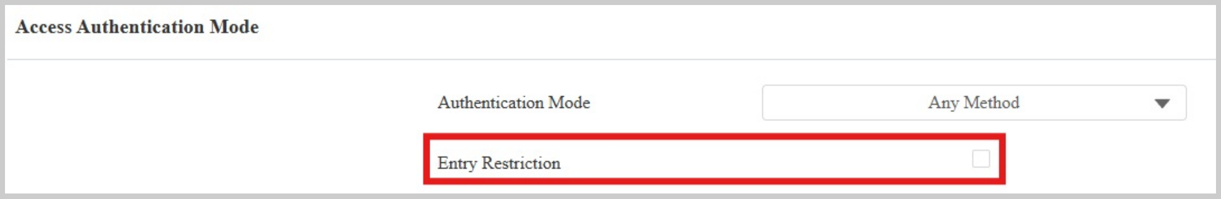
Entry Restriction: □

- **Authentication Mode**: Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.
    - **Any Method**: Allow all access methods.
    - **PIN + RF Card**: Enter the PIN code first, then swipe the RF card.
    - **RF Card + PIN**: Swipe the RF card first, then enter the PIN code.

Entry Restriction

You can limit users from opening the door repeatedly for a short time.

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



Access Authentication Mode

Authentication Mode: Any Method

Entry Restriction: □

- **Restriction Time(Sec)**: Specify the time within which the same user cannot open the door twice. For example, if it is set to 1800 seconds, the user cannot open the door again until 30 minutes later.

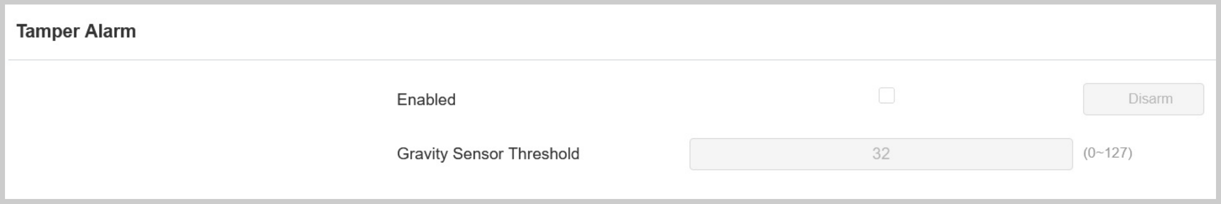
Security

Tamper Alarm

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

Click here to view which type is supported by the device and learn the function details.

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



Tamper Alarm

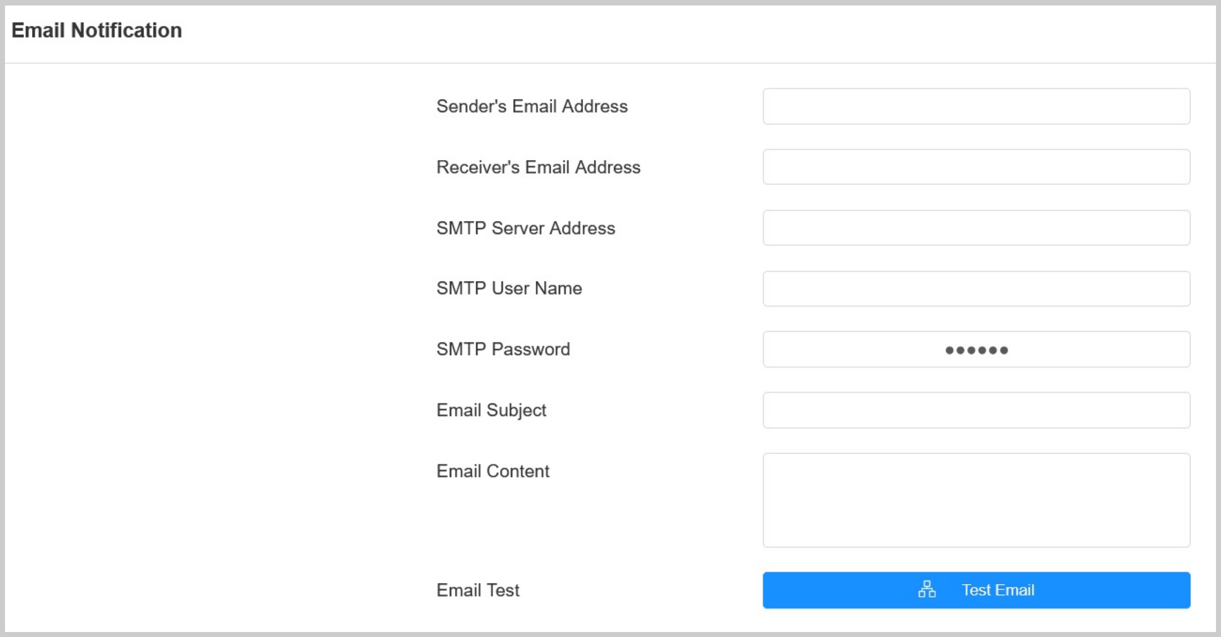
Enabled	□	Disarm
Gravity Sensor Threshold	32	(0~127)

- **Gravity Sensor Threshold**: The threshold for gravity sensory sensitivity. The lower the value is, the more sensitive the sensor will be. It is 32 by default.

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.

Set up security notifications on the **Setting > Action** interface.



Email Notification

Sender's Email Address	
Receiver's Email Address	
SMTP Server Address	
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	
Email Test	Test Email

- **SMTP Server Address**: The sender's SMTP server address.
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.
- **Email Test**: Used to test whether the email can be sent and received.

Action URL

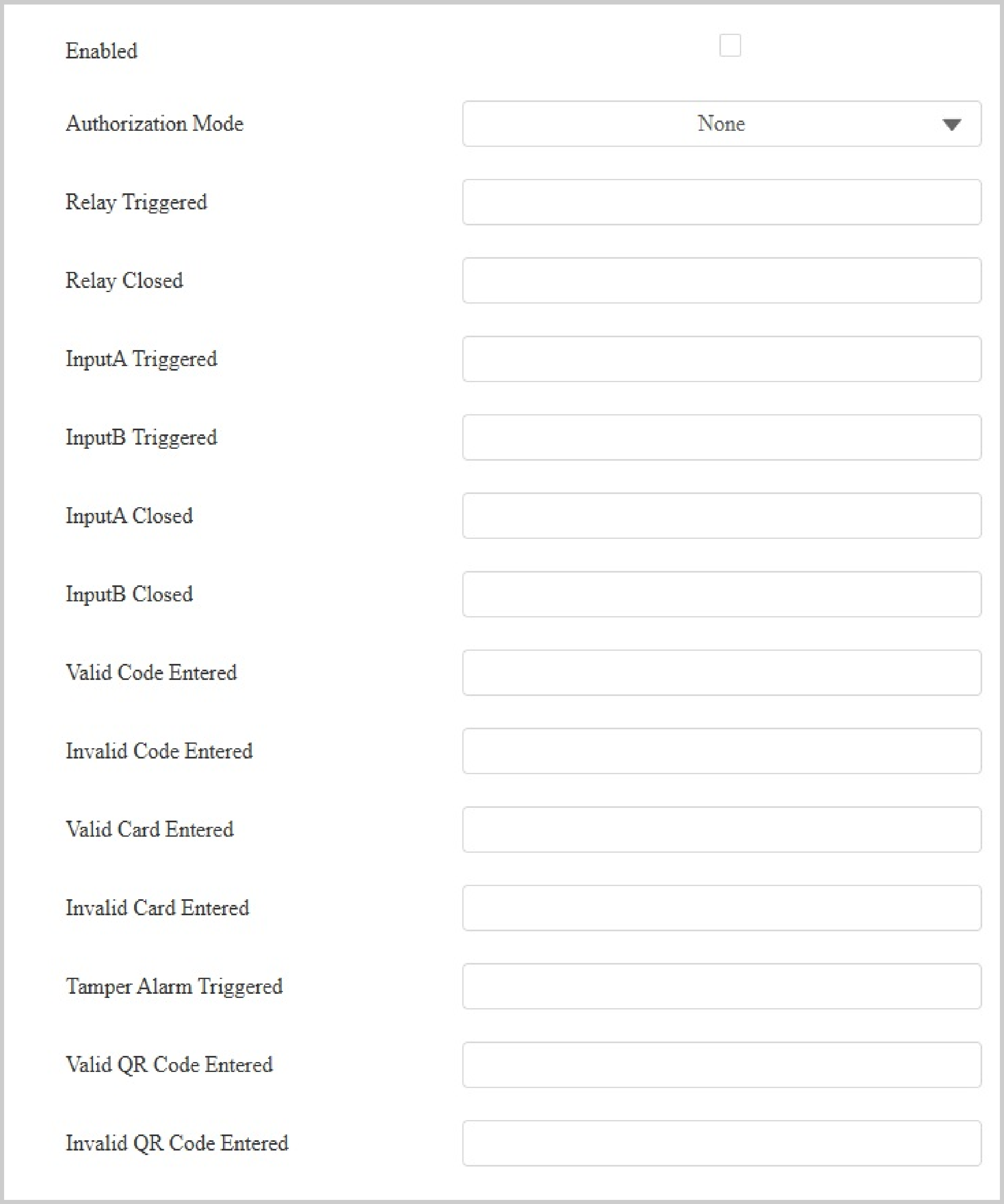
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
2	Relay Closed	$relay1status	Http://server ip/relayclose=$relay1status
3	Input Triggered	$input1status	Http://server ip/inputtrigger=$input1status
4	Input Closed	$input1status	Http://server ip/inputclose=$input1status
5	Valid Code Entered	$code	Http://server ip/validcode=$code
6	Invalid Code Entered	$code	Http://server ip/invalidcode=$code
7	Valid Card Entered	$card_sn	Http://server ip/validcard=$card_sn
8	Invalid Card Entered	$card_sn	Http://server ip/invalidcard=$card_sn
9	Tamper Alarm Triggered	$alarm status	Http://server ip/tampertrigger=$alarm status
10	Valid QR Code Entered	$unlocktype	Http://server ip/unlocktype=$unlocktype
11	Invalid QR Code Entered	$unlocktype	Http://server ip/unlocktype=$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 **Setting > Action URL** interface.



Enabled	□
Authorization Mode	None ▼
Relay Triggered	
Relay Closed	
InputA Triggered	
InputB Triggered	
InputA Closed	
InputB Closed	
Valid Code Entered	
Invalid Code Entered	
Valid Card Entered	
Invalid Card Entered	
Tamper Alarm Triggered	
Valid QR Code Entered	
Invalid QR Code Entered	

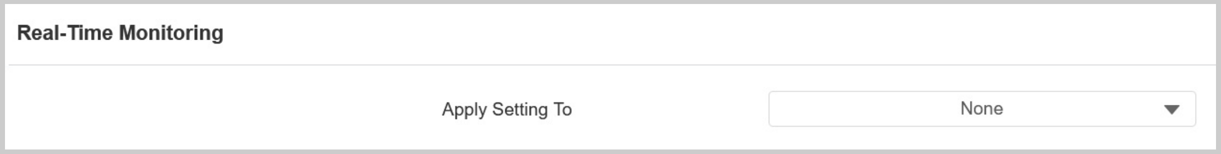
- **Authorization Mode**: When **Digest** is selected, you can set the username and password for authentication.

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.



Real-Time Monitoring

Apply Setting To: None

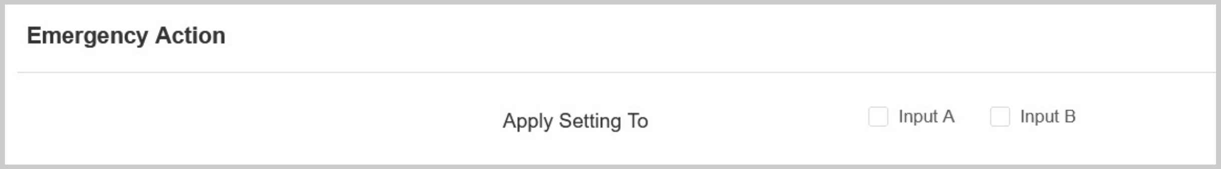
- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: the door is opened by triggering input.
  - **Relay**: the door is opened by triggering the relay.

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.



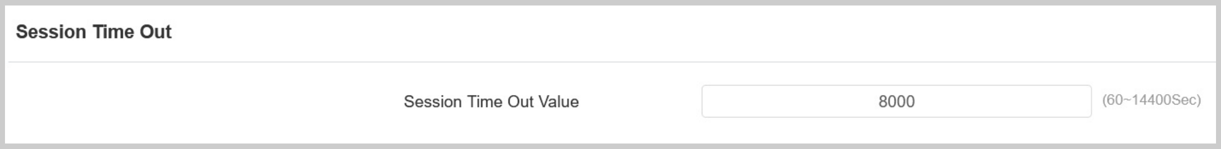
Emergency Action

Apply Setting To: □ Input A □ Input B

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.



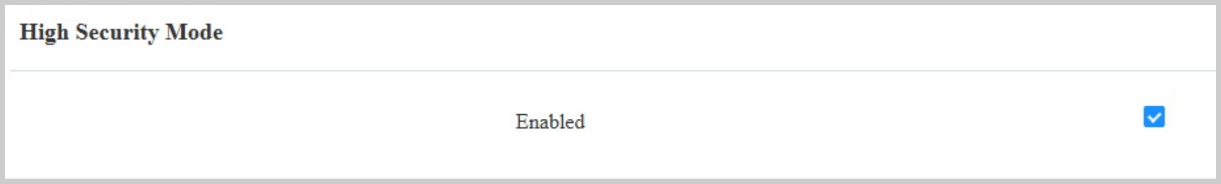
Session Time Out

Session Time Out Value 8000 (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/disable the high-security mode on the **System > Security** 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:

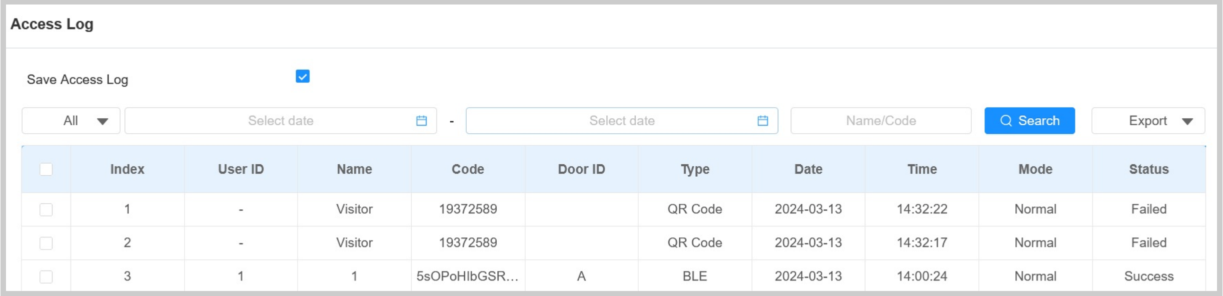
- http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

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

Access Logs

You can search and check door logs on the device web **Status > Access Log** interface. You can export the access logs in a CSV or XML file.



Access Log

Save Access Log ☑

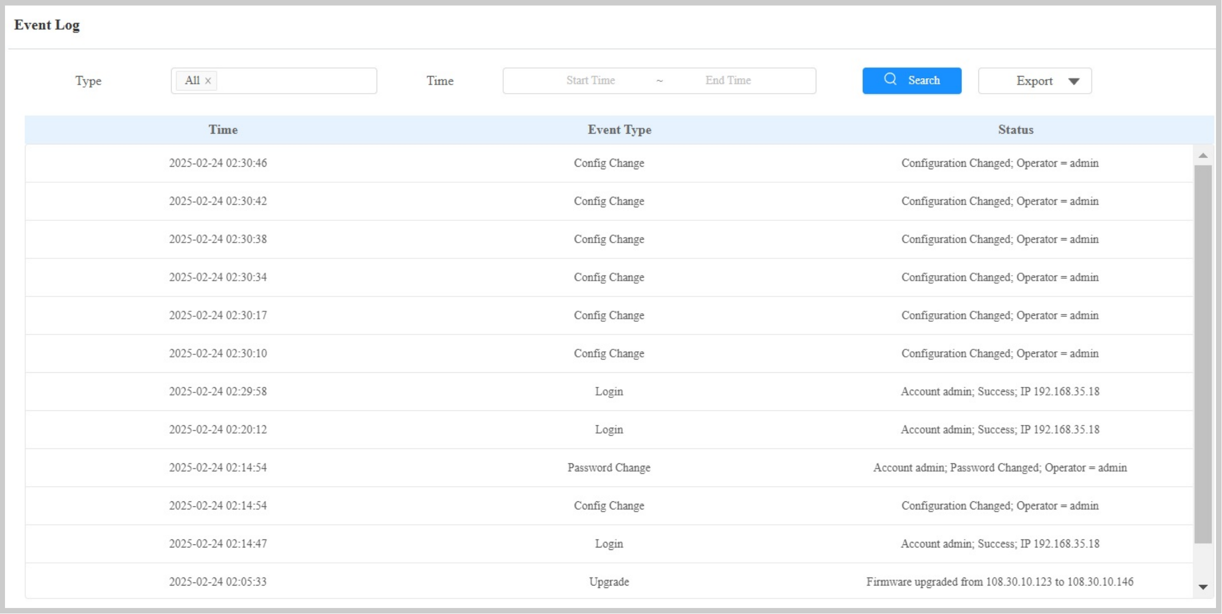
□	Index	User ID	Name	Code	Door ID	Type	Date	Time	Mode	Status
□	1	-	Visitor	19372589		QR Code	2024-03-13	14:32:22	Normal	Failed
□	2	-	Visitor	19372589		QR Code	2024-03-13	14:32:17	Normal	Failed
□	3	1	1	5sOPoHlbGSR...	A	BLE	2024-03-13	14:00:24	Normal	Success

- **Save Access Log**: Decide whether to save the door-opening records.
- **Status**: **Success** and **Failed** options represent successful door accesses and failed door accesses respectively.
- **Time**: Select the specific period of the door logs you want to search, check, or export.
- **Name/Code**: Search the log by the username or the PIN code.
- **Door ID**: Display the door name.
- **Type**: Display the access type such as QR code.

Event Logs

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

Check event logs on the **Status > Event Log** interface. You can export the event logs in a CSV file.



Event Log

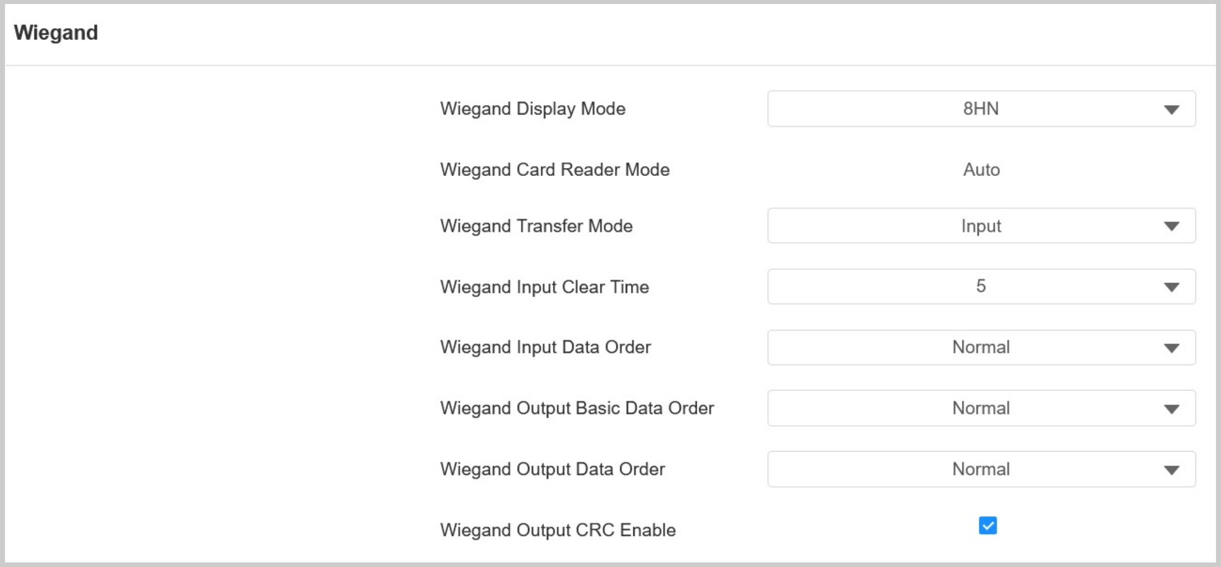
Time	Event Type	Status
2025-02-24 02:30:46	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:30:42	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:30:38	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:30:34	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:30:17	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:30:10	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:29:58	Login	Account admin; Success; IP 192.168.35.18
2025-02-24 02:20:12	Login	Account admin; Success; IP 192.168.35.18
2025-02-24 02:14:54	Password Change	Account admin; Password Changed; Operator = admin
2025-02-24 02:14:54	Config Change	Configuration Changed; Operator = admin
2025-02-24 02:14:47	Login	Account admin; Success; IP 192.168.35.18
2025-02-24 02:05:33	Upgrade	Firmware upgraded from 108.30.10.123 to 108.30.10.146

Integration with Third-party Devices

Integration via Wiegand

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

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



Wiegand

Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Auto
Wiegand Transfer Mode	Input
Wiegand Input Clear Time	5
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output CRC Enable	☑

- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the access control terminal and the third-party device. It is automatically configured when the Wiegand Transfer Mode is **Input**.
- **Wiegand Transfer Mode**:
  - **Input**: A08 serves as a receiver.
  - **Output**: A08 serves as a sender.
- **Wiegand Input Clear Time**: When the interval of entering passwords exceeds the time. All entered passwords will be cleared.
- **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 Wiegand output data.
    - **Normal**: The data is displayed as received.
    - **Reversed**: The order of the data bits is reversed.
- **Wiegand Output Data Order:** Determine the sequence of the card number.
    - **Normal**: The card number is displayed as received.
    - **Reversed**: The order of the card number is reversed.
- **Wiegand Output CRC Enable**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **Wiegand PIN Code Output**: Available when **Output** is selected as Wiegand Transfer Mode. This option determines the output PIN format.
    - Disabled: Turn off the feature.
    - 8 bits per digit: When users press "1" on the keypad, the binary data will be transmitted in 8 bits "11100001".
    - 4 bits per digit: When users press "1" on the keypad, the binary data will be transmitted in 4 bits "0001".
    - All at once: After users enter the whole PIN code, the data will be transmitted according to the Wiegand card reader mode. For example, “123456” will be converted to “01e240” in Wiegand 26.
- **RF Card Verification**: Available when **Output** is selected as Wiegand Transfer Mode. When enabled, the device will verify whether the card code is assigned to a user. If it is not, the device will announce "Opening Door Failed". 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, the device will announce "Opening Door Failed". When disabled, the device will not perform local verification.

Note

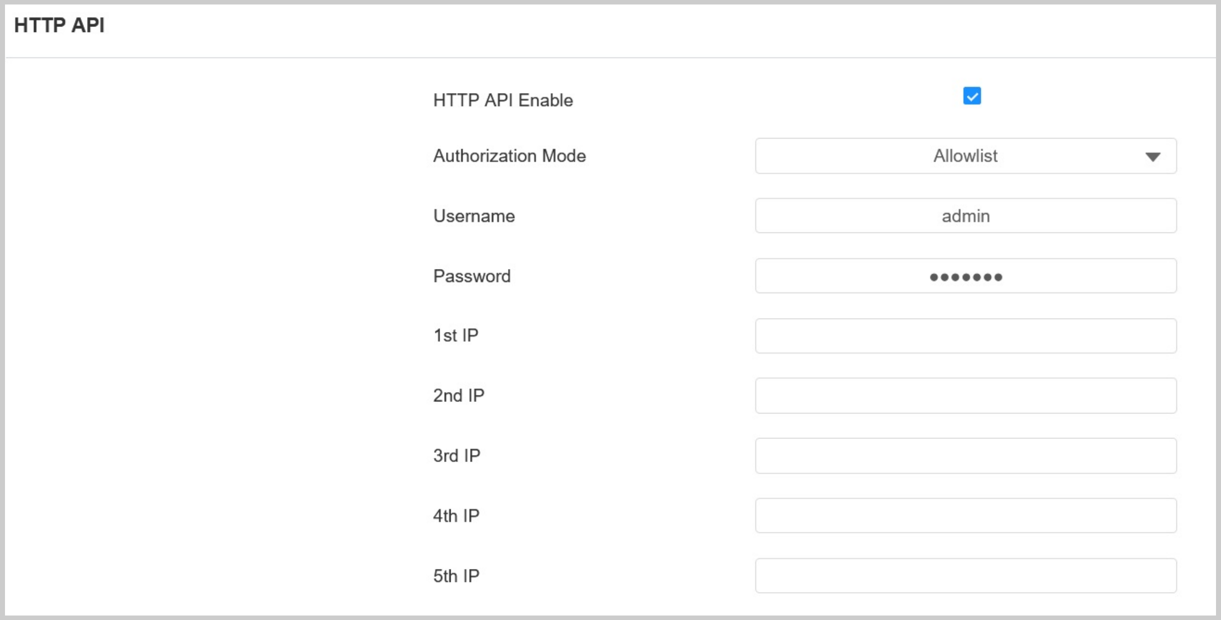
Click here to view more information on Wiegand settings including:

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

Integration via HTTP API

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

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



HTTP API

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

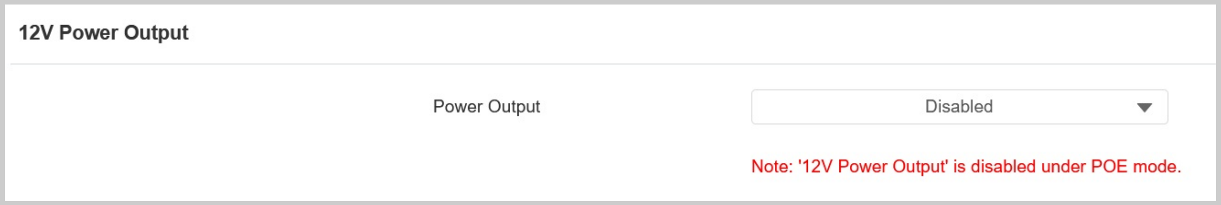
Please refer to the following description for the Authentication mode:

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

Power Output Control

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

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



12V Power Output

Power Output: Disabled

Note: '12V Power Output' is disabled under POE mode.

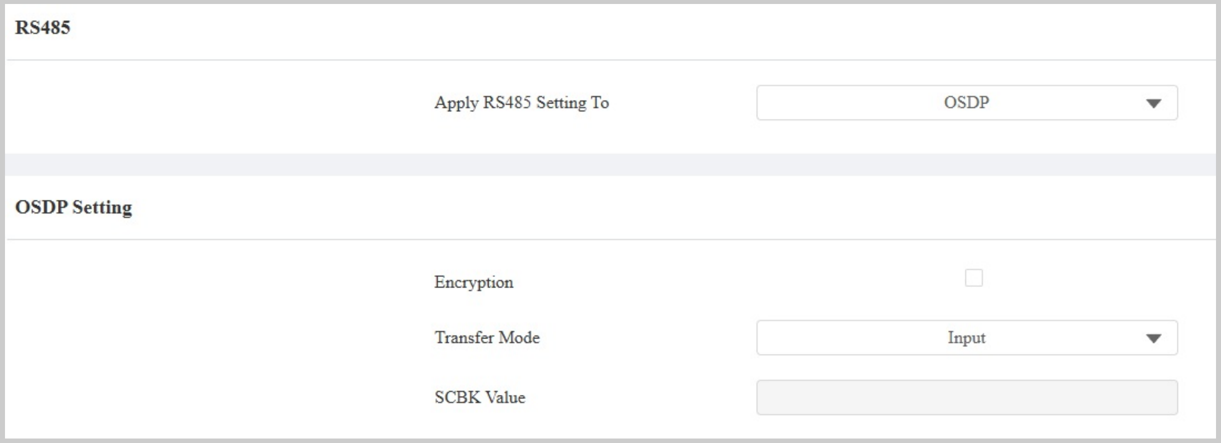
- **Power Output**:
  - **Always**: The device can provide continuous power to the third-party device.
  - **Triggered By Open Relay**: The device can provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.
  - **Security Relay A**: The device can work with the security relay.

Integration via RS485

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

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

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



RS485

Apply RS485 Setting To: OSDP

OSDP Setting

Encryption: □

Transfer Mode: Input

SCBK Value:

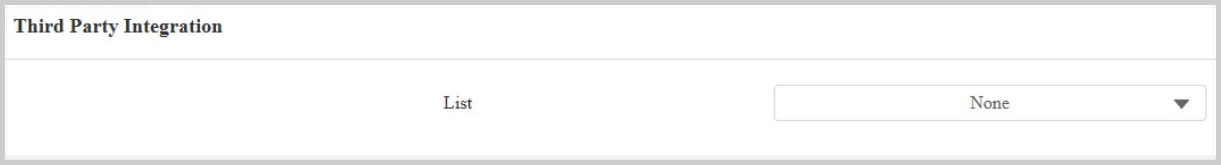
- **Disable**: The RS485 function is disabled.
- **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Encryption**: Check this option when the protocol is encrypted.
  - **Transfer Mode**: Select the RS485 working mode, Output, or Input.
  - **SCBK Value**: Secure Communication Key Value.

        - When it is filled, OSDP will use this value for encryption, employing a customized protocol for communication.
        - When it is left empty, OSDP will use the default encrypted protocol for communication.
- **Security Relay**: Select this option when the device works with the SR01.

Integration with Third-party Access Control Server

The device can transmit QR code and card 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: None

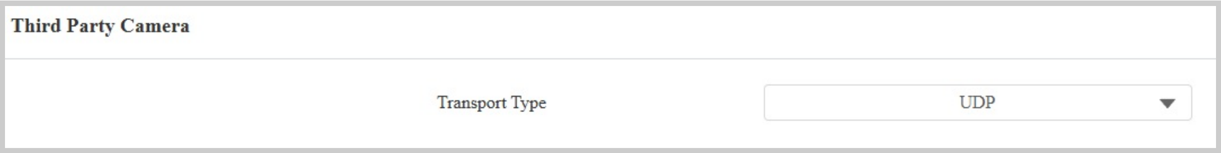
- **List**:
    - **None**: Disable the function.
    - **General**: Transmit the QR code-linked HTTP URL in Akuvox’s method.
        - HTTP URL: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before it is sent to the QR code server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={QRCode}&deviceId={DeviceID}.*
        - Device ID: The device ID is provided by the third-party server. It will be added to the HTTP command automatically when using a QR code for door access.
        - Success Parameter: Receiving this value indicates opening the door succeeds.

    - Failed Parameter: Receiving this value indicates opening the door fails.
- **Customize**: Transmit QR code and RF card data in a customized method.
    - Remote Verification: Check the access method to be verified by the third-party server.
    - HTTP URL: Enter the HTTP command format provided by the third-party service provider. After scanning the QR code or swiping the card, 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 or CardCode}&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 or RF card for door access.
    - Success Parameter: Receiving this value indicates opening the door succeeds.
    - Failed Parameter: Receiving this value indicates opening the door fails.

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 > Camera** interface.



Third Party Camera

Transport Type: UDP

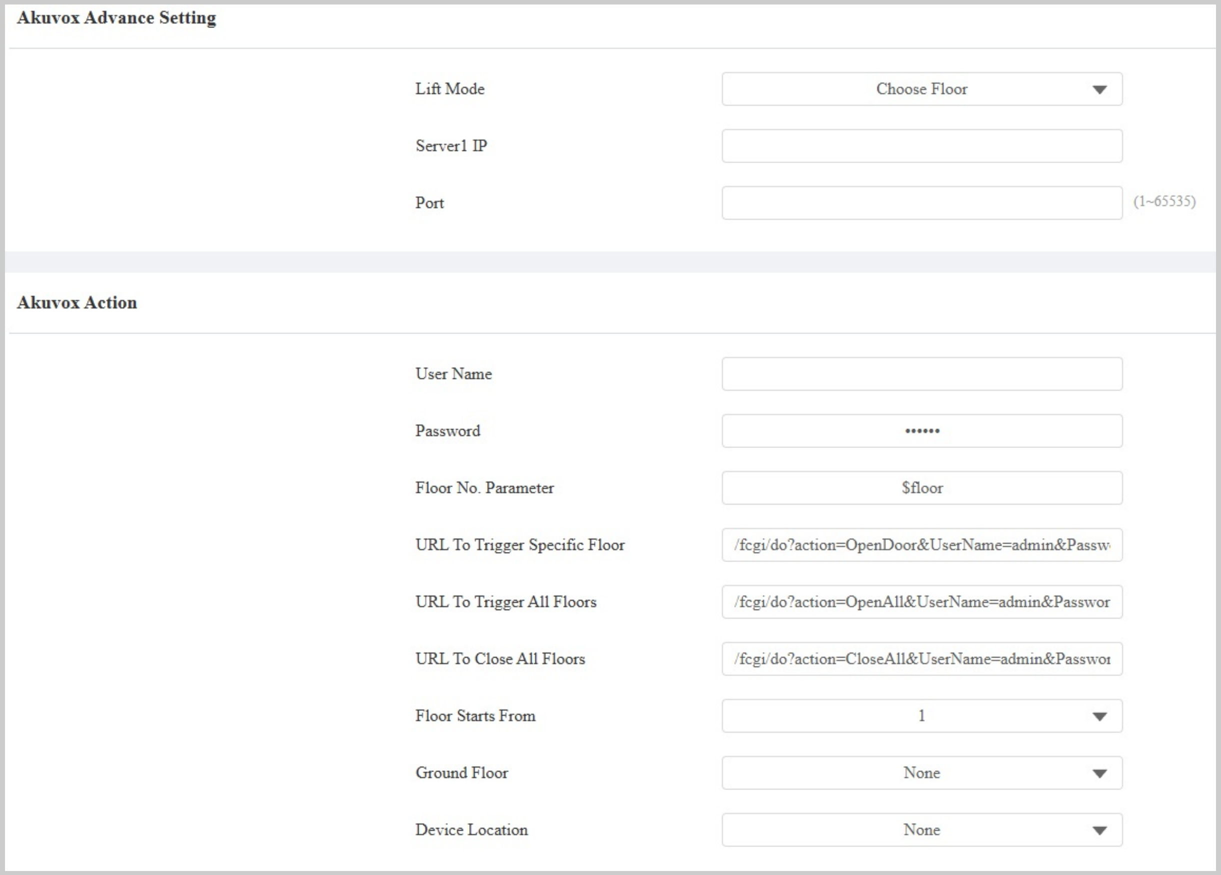
- **UDP**: An unreliable but very efficient transport layer protocol.
- **TCP**: A less efficient but reliable transport layer protocol. It is the default transport protocol.

Lift Control

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

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

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



Akuvox Advance Setting

Lift Mode	Choose Floor
Server1 IP	
Port	(1~65535)

Akuvox Action

User Name	
Password	••••••
Floor No. Parameter	$floor
URL To Trigger Specific Floor	/fcgi/do?action=OpenDoor&UserName=admin&Passw
URL To Trigger All Floors	/fcgi/do?action=OpenAll&UserName=admin&Passwor
URL To Close All Floors	/fcgi/do?action=CloseAll&UserName=admin&Passwor
Floor Starts From	1
Ground Floor	None
Device Location	None

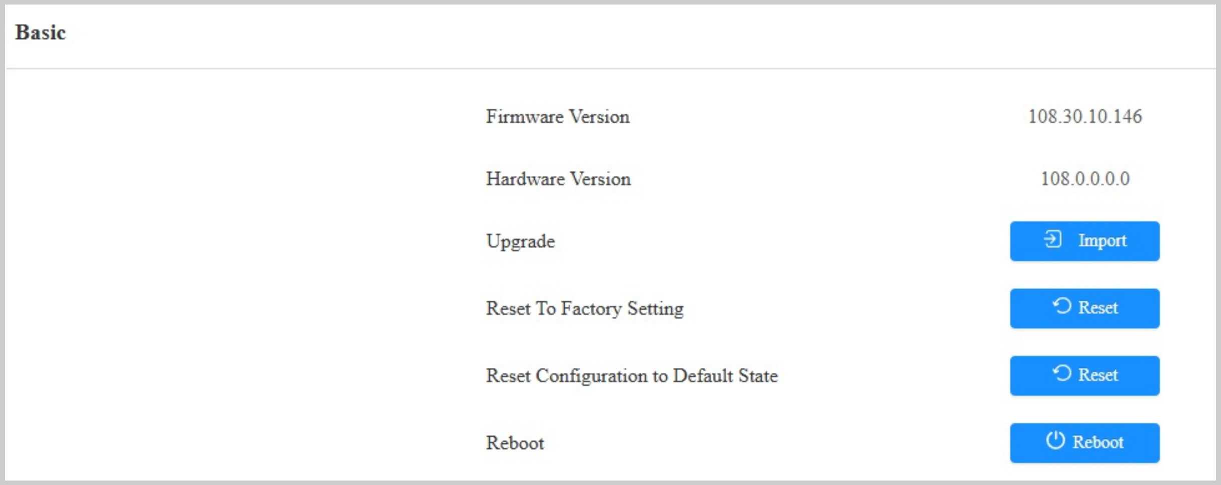
- **Lift Control List**: Select None to disable the function, and select **Akuvox** to integrate the device with the Akuvox lift controller.
- **Lift Mode:**
    - **Choose Floor**: Users can choose the floor they want to access when they use their credentials on the device.

  - **Direct Access:** Users will be directly sent to the target floor when they use their credentials on the device.
- **Server1 IP**: The IP address of the lift controller that unlocks the elevator button(s).
- **Port**: The port of the lift controller.
- **Server2 IP**: Available when **Direct Access** is selected. The IP address of the lift controller that sends the lift control commands.
- **Port**: The port of the lift controller.
- **User Name**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is “$floor”. You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string “$floor” at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **Floor Starts From**: Set the floor from which the floor count starts(-10 ~ 128). For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **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.

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



Basic

Firmware Version	108.30.10.146
Hardware Version	108.0.0.0.0
Upgrade	Import
Reset To Factory Setting	Reset
Reset Configuration to Default State	Reset
Reboot	Reboot

Note

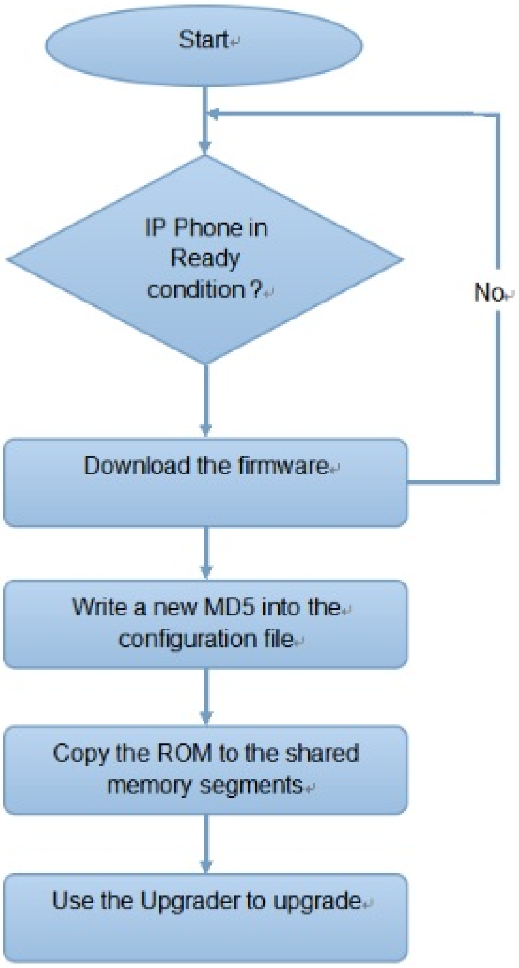
Firmware files should be in **.rom** format for upgrade.

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:


Start
IP Phone in Ready condition ?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments
Use the Upgrader to upgrade

Introduction to the Configuration Files for Auto-Provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

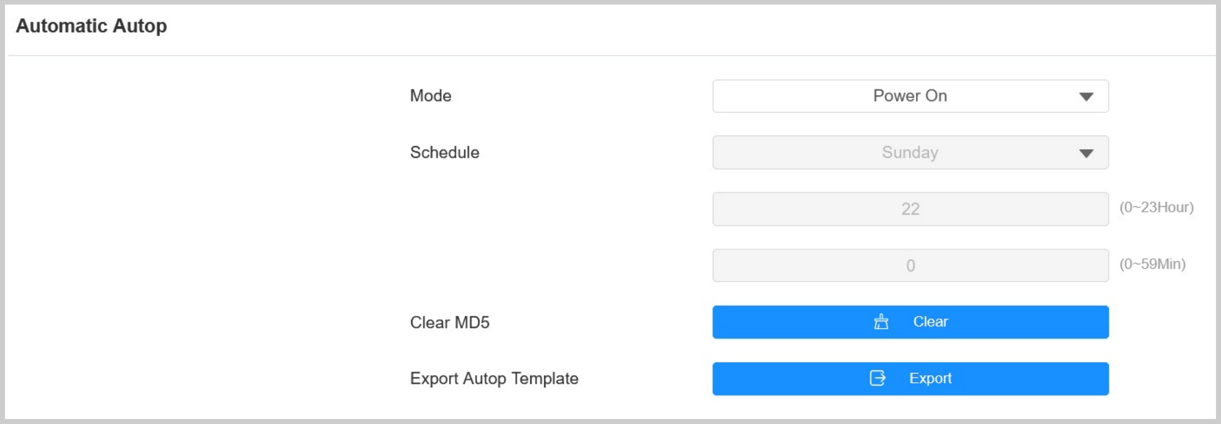
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

Autop Schedule

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

To set it up, go to **System > Auto Provisioning > Automatic Autop** interface.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

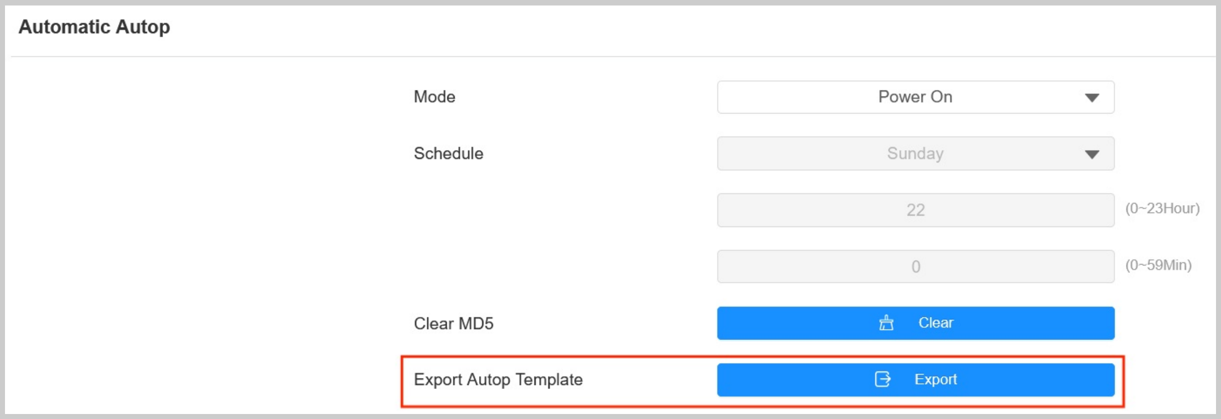
Export Autop Template: Export

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

Static Provisioning

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

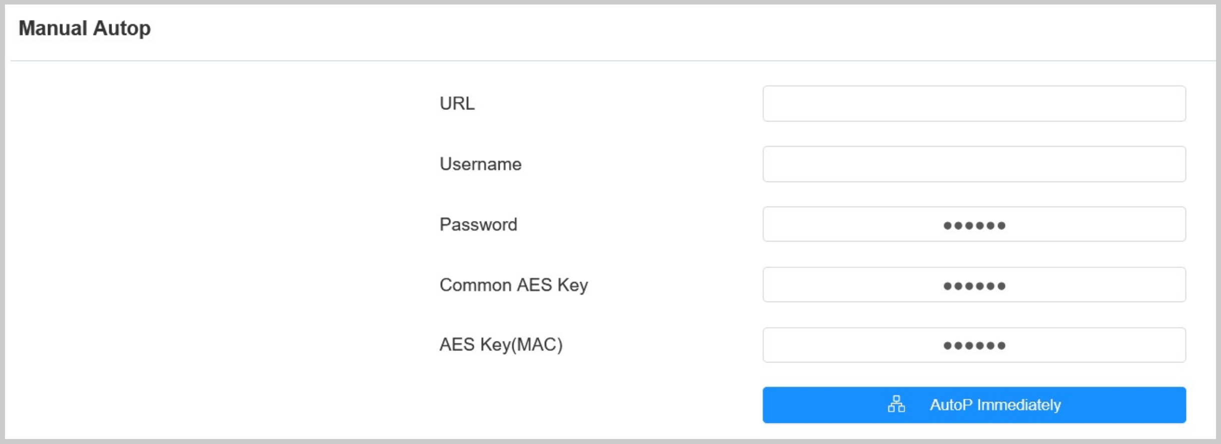
To set it up, download the template on
System > Auto Provisioning > Automatic Autop first.



Automatic Autop

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

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



Manual Autop

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

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

Note

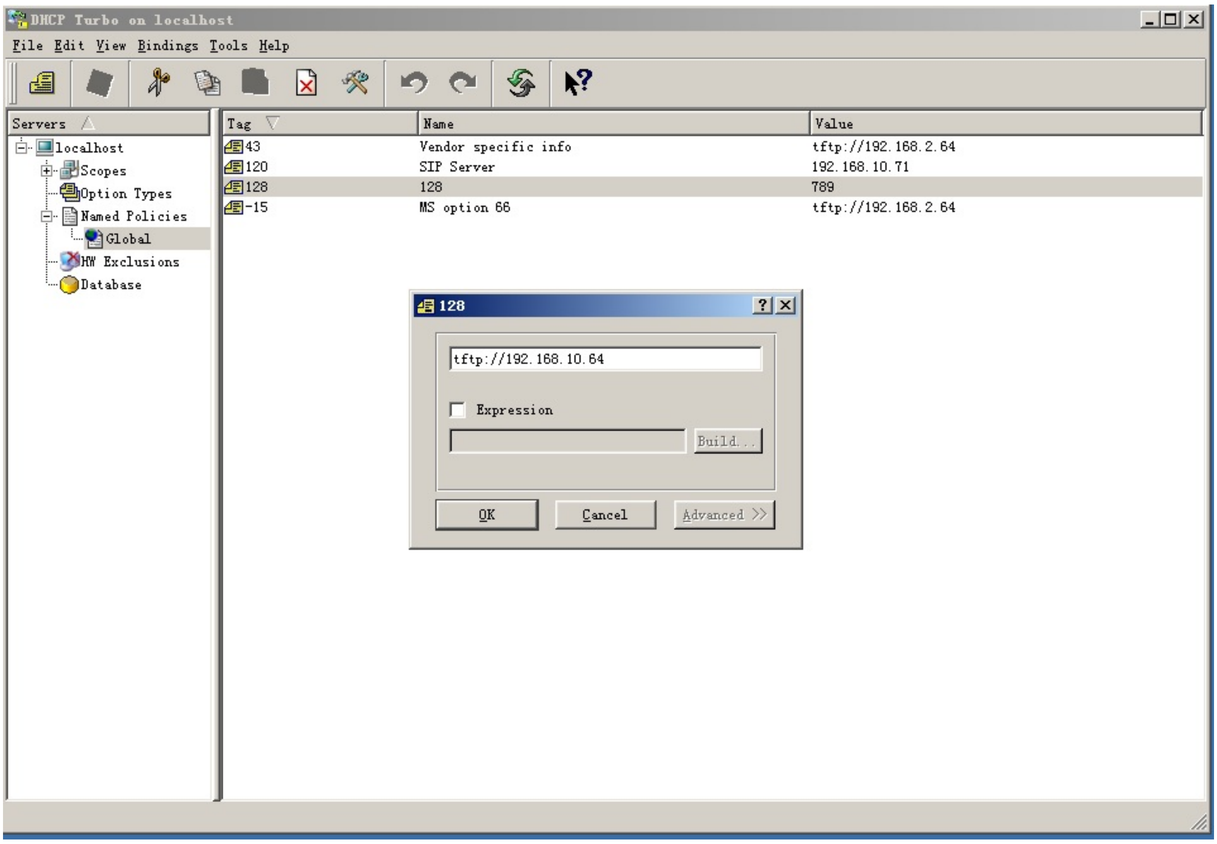
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

Tip

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

DHCP Provisioning

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



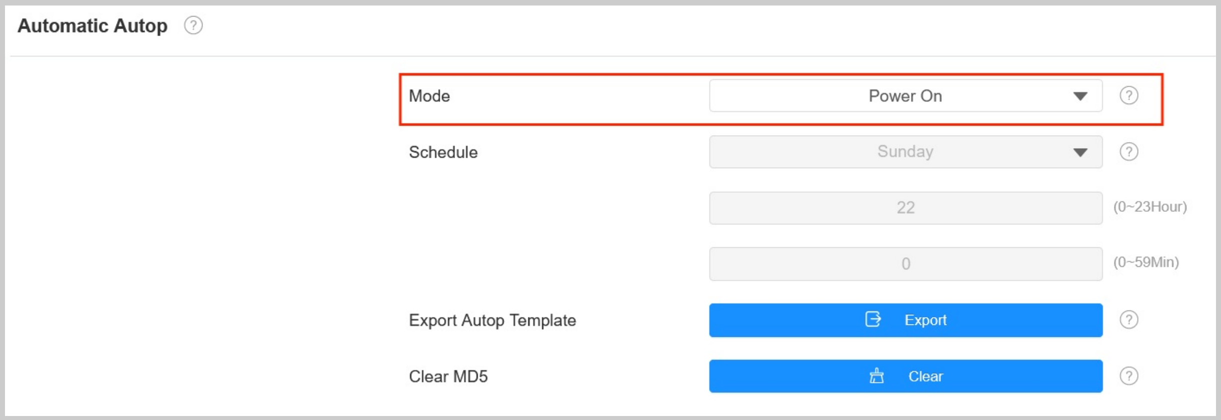
Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

tftp://192.168.10.64

Note

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

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


Automatic Autop

Mode: Power On

Schedule: Sunday

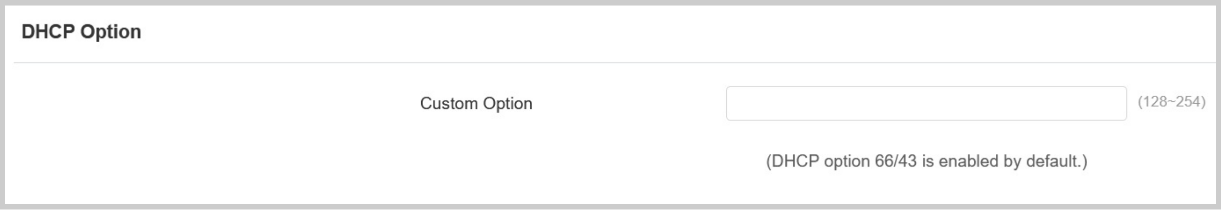
22 (0~23Hour)

0 (0~59Min)

Export Autop Template: Export

Clear MD5: Clear

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



DHCP Option

Custom Option (128~254)

(DHCP option 66/43 is enabled by default.)

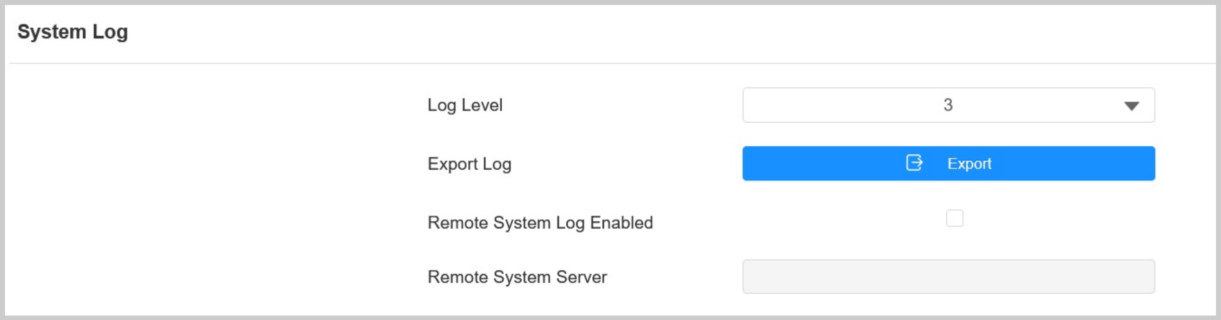
- **Custom Option**: Enter the DHCP code that matches with corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done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

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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



System Log

Log Level: 3

Export Log: Export

Remote System Log Enabled: □

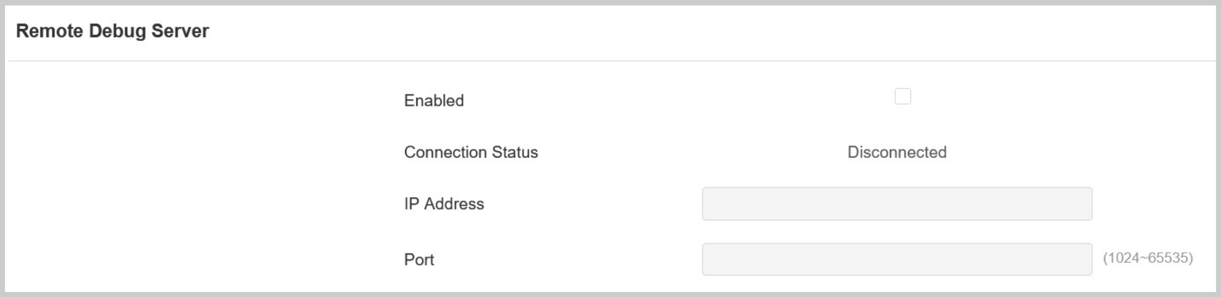
Remote System Server:

- **Log Level**: Log levels range from 1 to 7. 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 the temporary debug log file to a local PC.
- **Remote System Server**: Set the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.

Remote Debug Server

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

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



Remote Debug Server

Enabled □

Connection Status Disconnected

IP Address

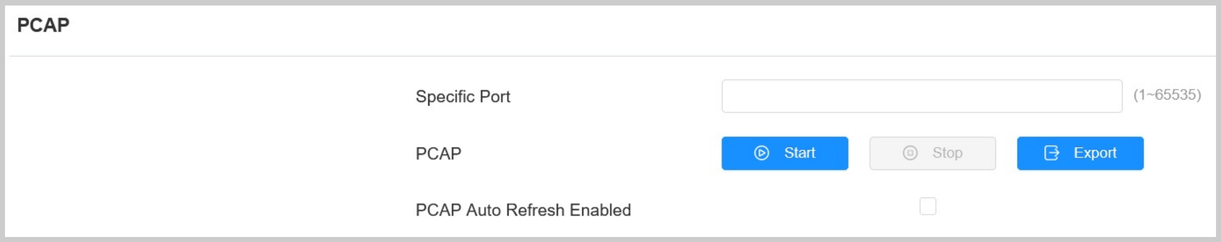
Port (1024~65535)

- **Connection Status**: Display the remote debug server connection status.
- **IP Address**: Set the remote debug server IP address. Please ask the Akuvox technical team for the server IP address.
- **Port**: Set the remote debug server port.

PCAP for Debugging

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

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



PCAP

Specific Port (1~65535)

PCAP

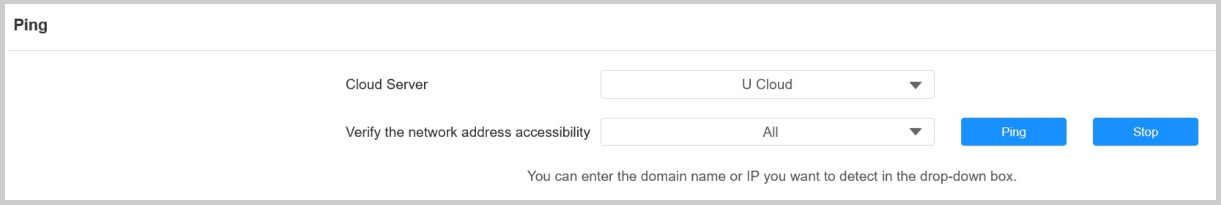
PCAP Auto Refresh Enabled □

- **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**: When enabled, the PCAP will continue to capture data packets even after the data packets reach their 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets captured reach the maximum capturing capacity of 1MB.

Ping

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

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



Ping

Cloud Server: U Cloud

Verify the network address accessibility: All

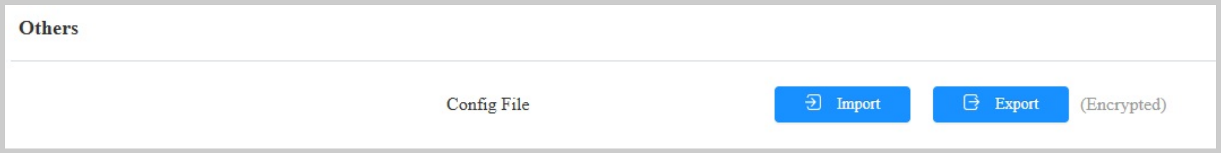
You can enter the domain name or IP you want to detect in the drop-down box.

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

Backup

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

Export the configuration files on the **System > Maintenance** interface. The supported import file format is TGZ, CONF, and CFG.



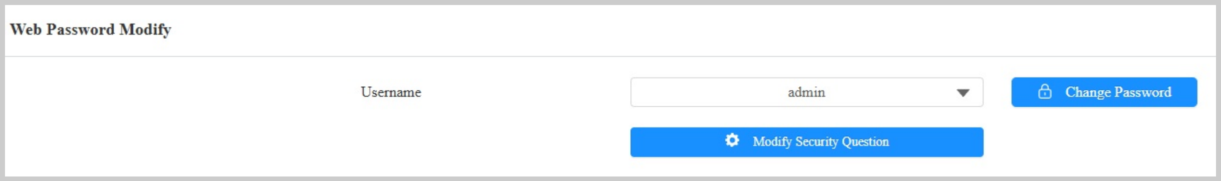
Others

Config File

Password Modification

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

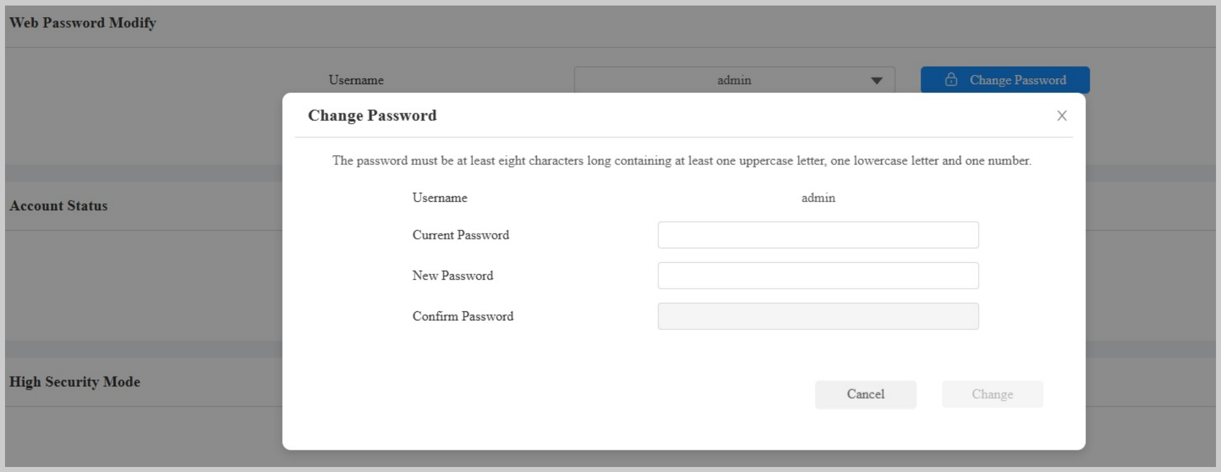
To set it up, go to **System > Security > Web Password Modify** interface.



Web Password Modify

Username: admin

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



Change Password

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

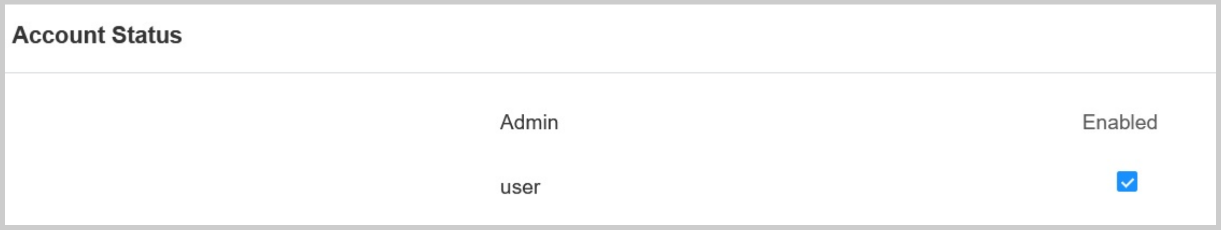
Username: admin

Current Password

New Password

Confirm Password

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



Account Status

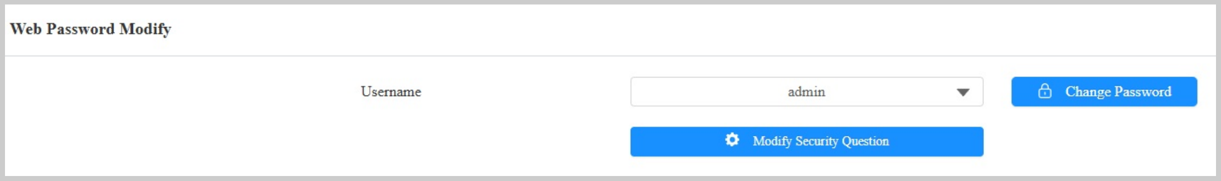
Admin	Enabled
user	☑

Modify Security Questions

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

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

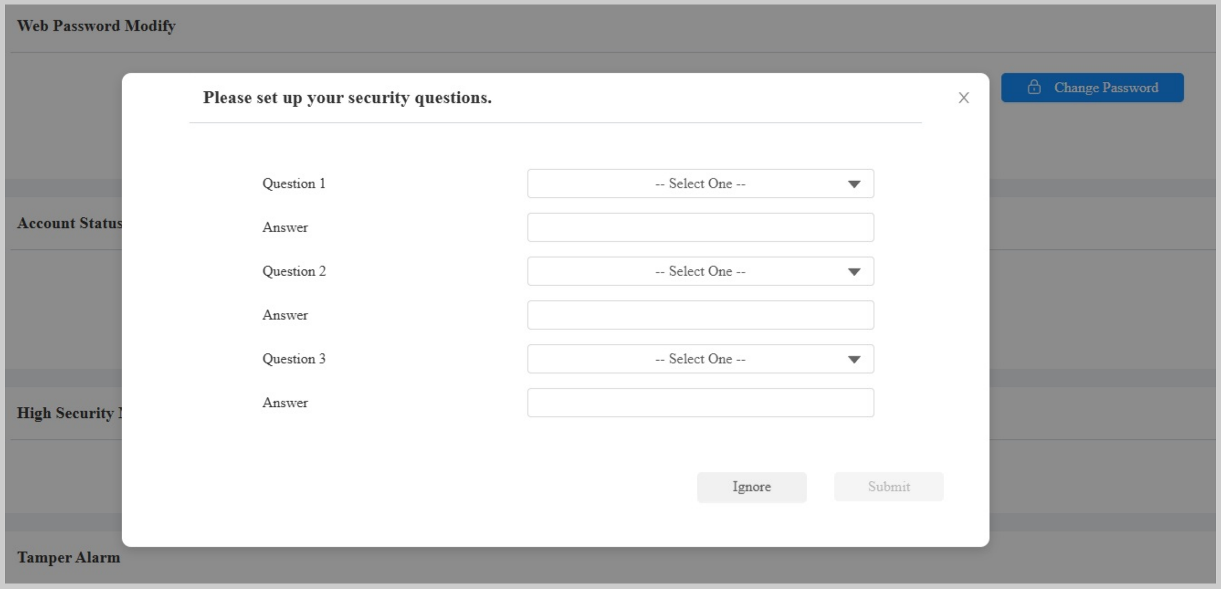
Set it up on the **System > Security** interface.



Web Password Modify

Username: admin

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



Web Password Modify

Please set up your security questions.

Question 1: -- Select One --

Answer:

Question 2: -- Select One --

Answer:

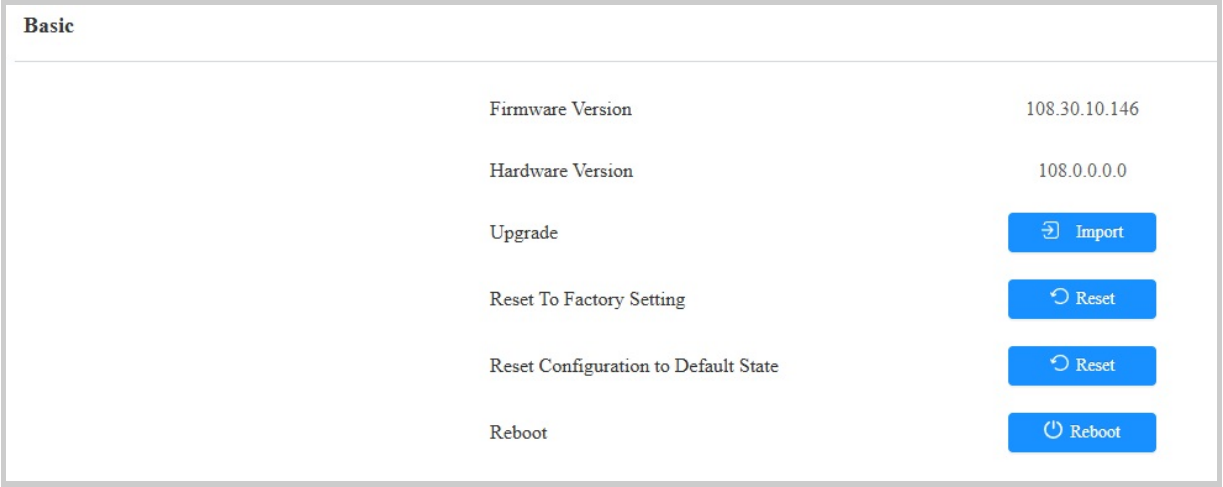
Question 3: -- Select One --

Answer:

System Reboot and Reset

Reboot

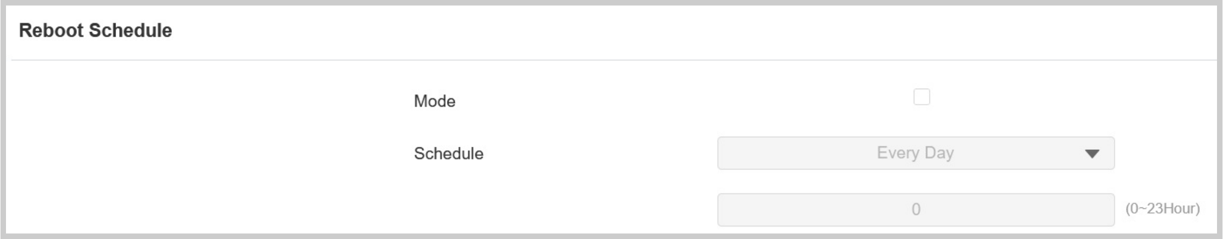
Reboot the device on the web **System > Upgrade** interface.



Basic

Firmware Version	108.30.10.146
Hardware Version	108.0.0.0.0
Upgrade	Import
Reset To Factory Setting	Reset
Reset Configuration to Default State	Reset
Reboot	Reboot

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



Reboot Schedule

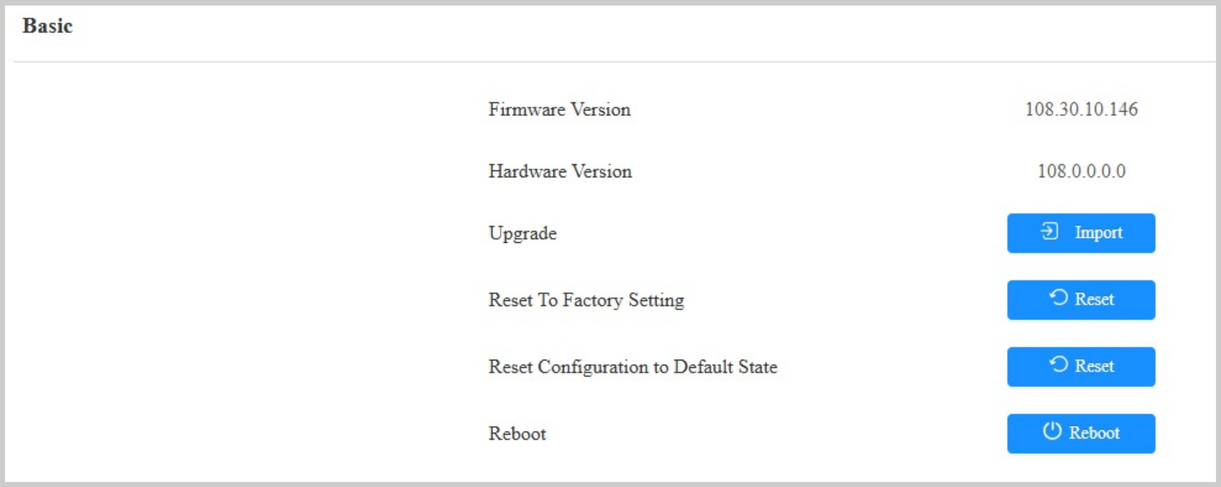
Mode	□	
Schedule	Every Day	
	0	(0~23Hour)

Reset

The device provides two reset options:

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

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



Basic

Firmware Version	108.30.10.146
Hardware Version	108.0.0.0.0
Upgrade	Import
Reset To Factory Setting	Reset
Reset Configuration to Default State	Reset
Reboot	Reboot

You can also reset the device by long pressing the **Reset** button on the back of the device.