Akuvox

Table of contents

Akuvox A01 Access Control Terminal Administrator Guide

About This Manual 6

Product Overview 9

Changelog 10

Model Specification 11

Supported Card Types 11

Introduction to Configuration Menu 13

Access the Device 15

Time and Language 17

Time 17

Language 18

LED Setting 19

LED Setting on Card Reader Area 19

Light Blink Control 19

Volume and Tone 21

Upload Open Door Tone 21

Open Door Tone Mode 22

Network Setting 23
SNMP Setting 24
Device Web HTTP Setting 24
Relay Settings 26
Local Relay 26
Security Relay 27
Web Relay 29
Relay Keep Active While Card Present 31
Door Access Schedule Management 33
Door Access Schedule 33
Create Door Access Schedule 33
Import and Export Door Access Schedule 34
Relay Schedule 34
Holiday Schedule 35
Door-opening Configuration 37
User-specific Access Methods 37
Unlock by Private PIN Code 38
Unlock by RF Card 38
Unlock by License Plate 39
Access Setting 40

Import and Export User Data 42
NFC and Felica Card Setting 42
Mifare Card 43
CEPAS Card Reading 44
Unlock by HTTP Command 45
Unlock by Exit Button 45
Security 48
Tamper Alarm 48
Security Notification 48
Email Notification 48
Action URL 49
Real-Time Monitoring 52
Emergency Action 52
Web Interface Automatic Log-out 52
High Security Mode 53
Anti-passback Mode 54
Lift Control 55
Logs 57
Access Log 57
Event Log 58

Debug 59
System Log for Debugging 59
Remote Debug Server 59
PCAP for Debugging 60
Ping 61
Backup 62
Firmware Upgrade 63
Auto-provisioning via Configuration File 64
Provisioning Principle 64
Introduction to the Configuration Files for Auto-Provisioning 65
Autop Schedule 66
Static Provisioning 66
DHCP Provisioning 68
Integration with Third-Party Device 71
Integration via Wiegand 71
Integration via HTTP API 72
Third-Party Integration 74
Power Output Control 76
Password Modification 77
Modify Security Questions 78

System Reboot and Reset 80
Reboot 80
Reset 80

About This Manual

Akuvox

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX A01 ACCESS CONTROL

Administrator Guide

Akuvox

Thank you for choosing the Akuvox A01 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 101.30.11.124, and it provides all the configurations for the functions and features of the A01 access control terminal. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox Access control terminal A01s incorporate a door controller and an RIFD reader in one standalone device, thus saving your solution costs. It is equipped with a card reader (125kHz and 13.5MHz) which is currently capable of handling a majority of cards in wide use. It is designed to provide you with greater flexibility and security than traditional access control systems. A01 access control terminal applies to residential buildings, office buildings, and their complex.

Changelog

What's new in version 101.30.11.121:

- Support configuring the data length for reading the Mifare cards .
- Optimized the integration with a third-party access control server .

What's new in version 101.30.11.124:

- Support setting the relay hold time for the Relay Keep Active while Card Present feature .

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

Model Specification

Model	A01
RFID card reader	13.56MHz & 125KHz
Relay out	1
Inputs	2
Wiegand	✓
Speaker	1
Tamper-proof alarm	✓
Ethernet port	RJ45, 10/100Mbps adaptive 802.3af power-over-Ethernet/12V DC connector (if not using PoE)
Wi-Fi	X
Bluetooth	X

Supported Card Types

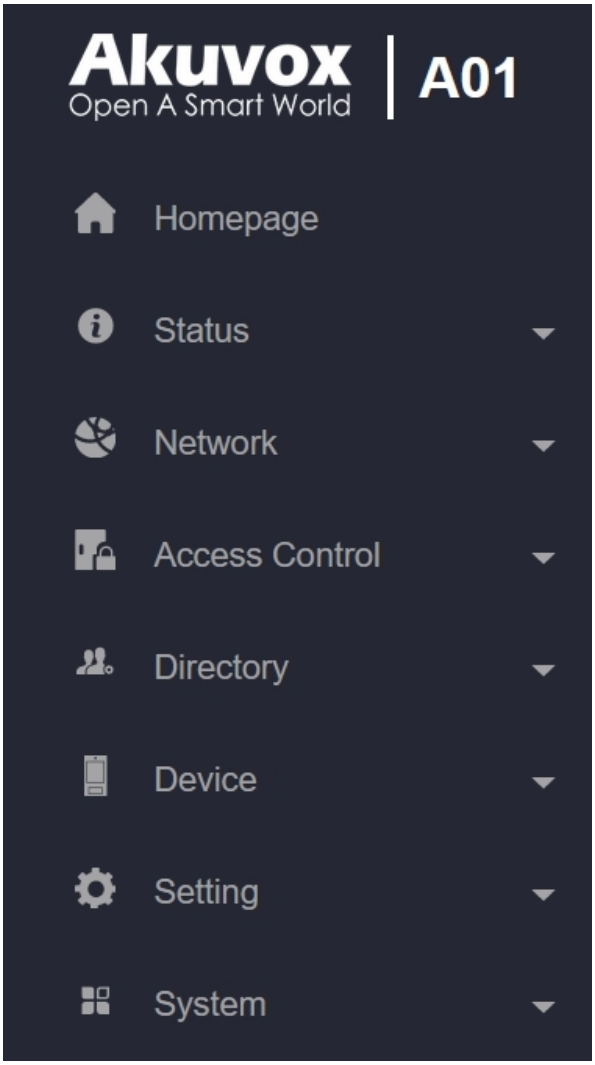
The device's firmware should be 101.30.10.127 or higher:

- Unencrypted ID Card:
  - EM4100
  - EM4200
- Unencrypted 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)

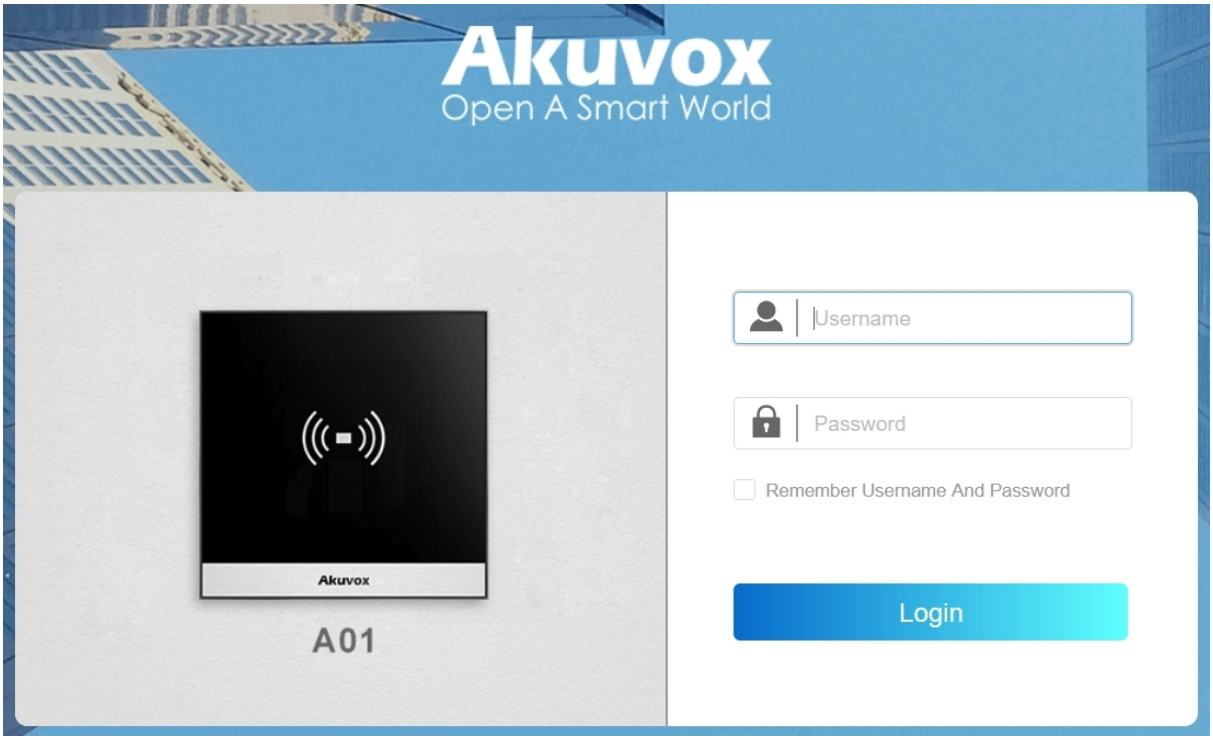
Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, and access log management.
- **Network**: This section covers LAN port settings.
- **Access Control**: This section covers relay, input, web relay, card settings, keypad settings, etc.
- **Directory**: This section includes access schedule management and user management.
- **Device**: This section includes light, Wiegand, lift control, and audio settings.
- **Setting**: This section deals with relay schedule, security notification settings, web relay, time, action, and HTTP API settings.
- **System**: This section covers firmware upgrade, device reset, reboot, configuration file auto-provisioning, system log and PCAP, password modification as well as device backup.


Akuvox
Open A Smart World
A01
Homepage
Status
Network
Access Control
Directory
Device
Setting
System

Access the Device

Before configuring Akuvox A01, please make sure the device is installed correctly and connects 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 in to the web browser by user name and password **admin** and **admin**.

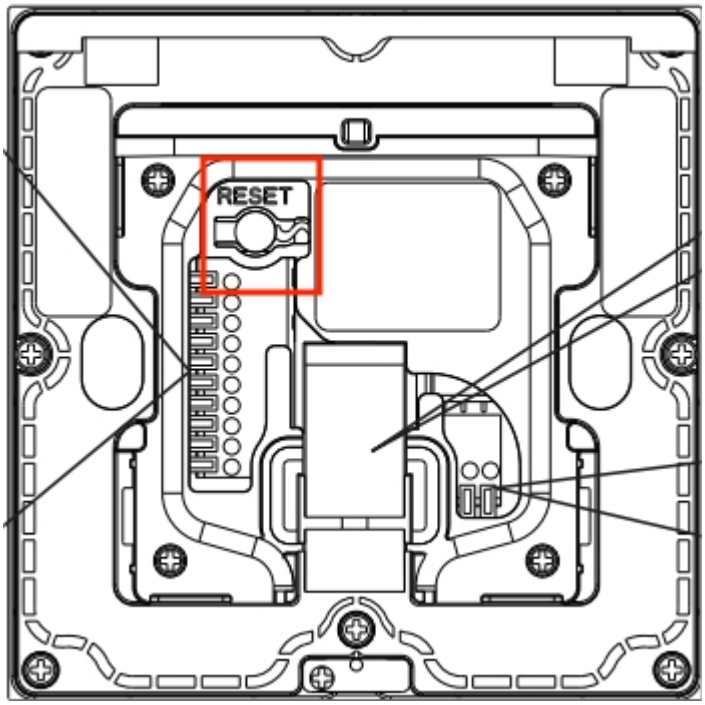


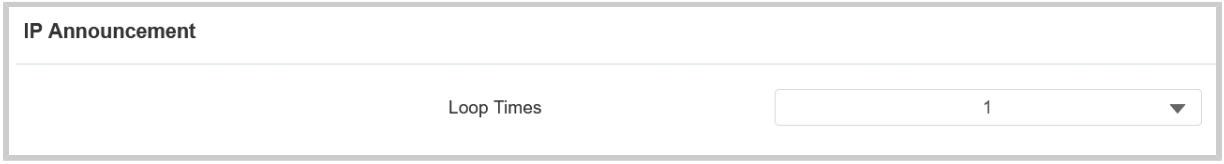
Note

- 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.
- Please be case-sensitive to the user names and passwords entered.

You can also obtain the IP by pressing the **Reset** button on the device's back. The device will announce the IP address.

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



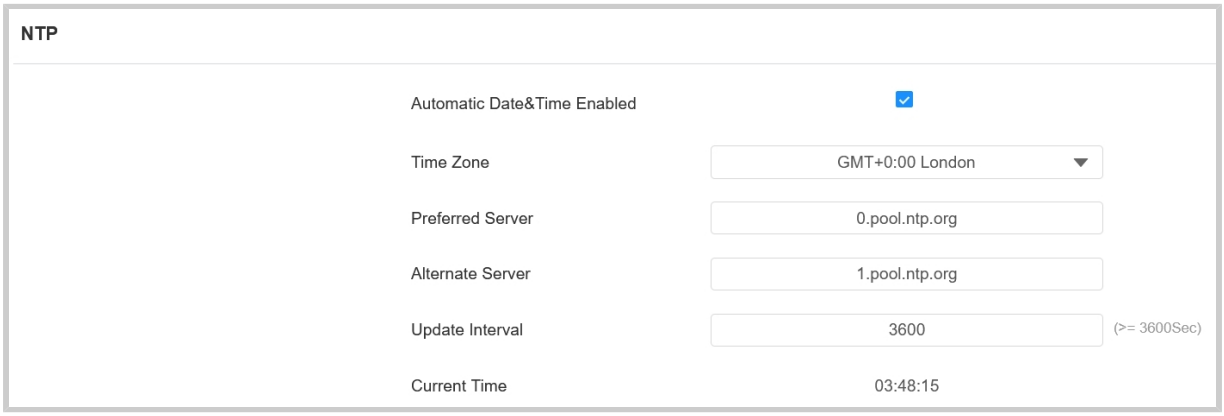


Time and Language

Time

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

Set up time on the **Setting > Time** interface.



- **Automatic Date&Time Enabled**: If enabled, the device will update the time automatically via the NTP server (**Network Time Protocol**). Disable it if you want to set up the time manually.
- **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 to update the time with. The default NTP server address is 0.pool.ntp.org
- **Alternate Server**: Enter the NTP server address for backup.
- **Update Interval**: Set the time update interval. For example, if you set it as 3600, the device will send a request to the NTP server for the time update once every 3600 seconds.

- **Current Time**: Display the current device time.

Language

You can switch the web language by selecting the language in the upper-right corner.

The following languages are supported: English, Simplified Chinese, Traditional Chinese, Spanish, Italian, Dutch, French, German, and Korean.



LED Setting

LED Setting on Card Reader Area

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

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



- **Backlight Intensity**: Adjust the backlight intensity; the bigger the value, the brighter the backlight.
- **Start Time - End Time (Hour)**: Select the time span for the LED lighting to be valid, e.g., if the time span is from 18-22, it means the LED light will stay on during the time span from 6:00 pm to 10:00 pm in one day (24 hours).
- **LED Always On When Relay Triggered**: Disabled by default. If enabled, the LED stays on when the relay is kept activated. Its brightness follows the Backlight Intensity setting.

Light Blink Control

You can disable all light blinking effects for a scheduled time, including network connection, door opening, and TOF trigger indications.

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

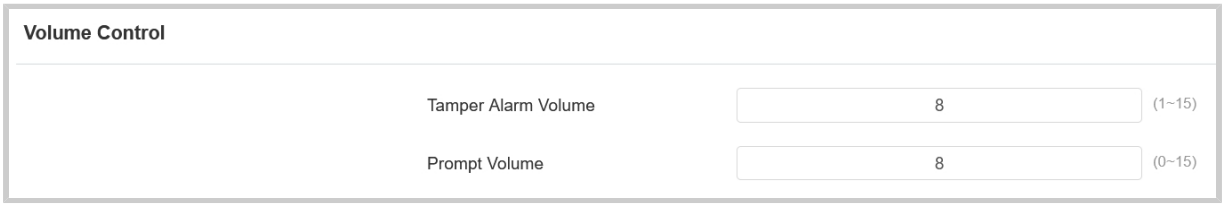


- **Disable Blinking**: The feature is disabled by default.
- **Effective Schedule**: Apply the schedule to the feature by moving it from the left to the right box.

Volume and Tone

Volume and tone configuration include tamper alarm and prompt volume. Besides, you can upload door-opening ringtones.

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

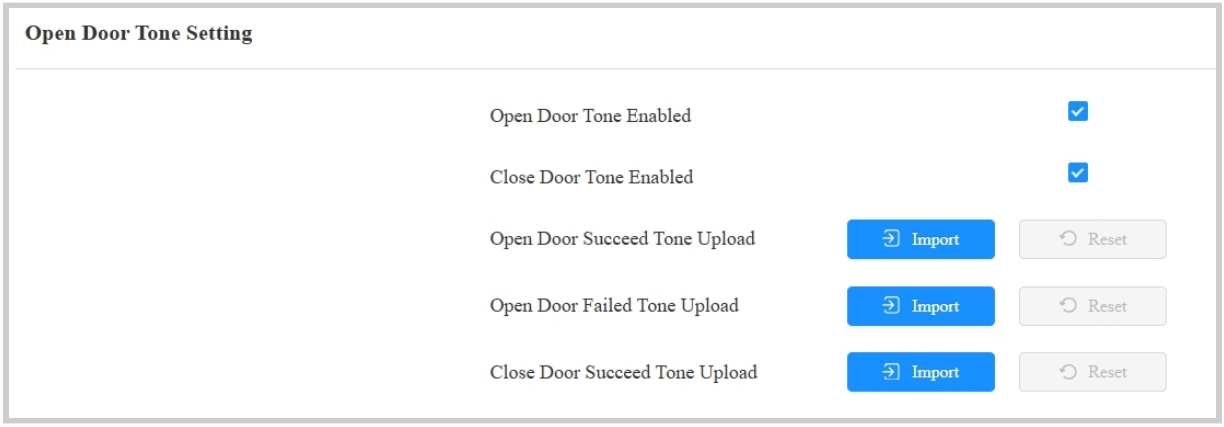


- **Tamper Alarm**: Set the volume when the tamper alarm is triggered. The default volume is 8.
- **Prompt Volume**: Set the voice prompt volume. The default volume is 8.

Upload Open Door Tone

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

To upload the tones, go to **Device > Audio > Open Door Tone Setting** interface. Enable the open door tone before uploading the file.

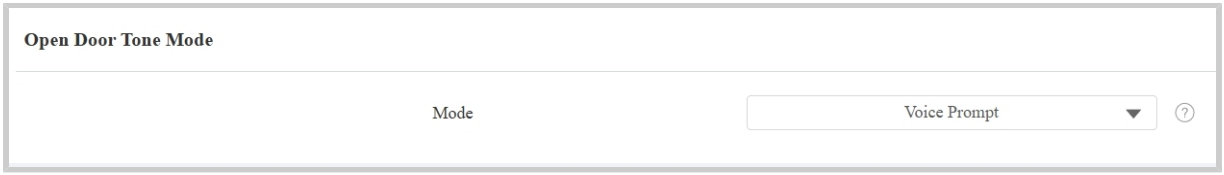


- **Close Door Tone Enabled**: The door-closing tone works for the relay(s) set to the Bistable mode. When users close the door with their credentials, the prompt will be played.

> **Note**
>
> File Format: wav, size: < 200KB, pcm(sample rate: 16000, bits: 16, mono)/pcma/pcmu

Open Door Tone Mode

You can decide the door-opening tone mode on the **Device > Audio** interface.

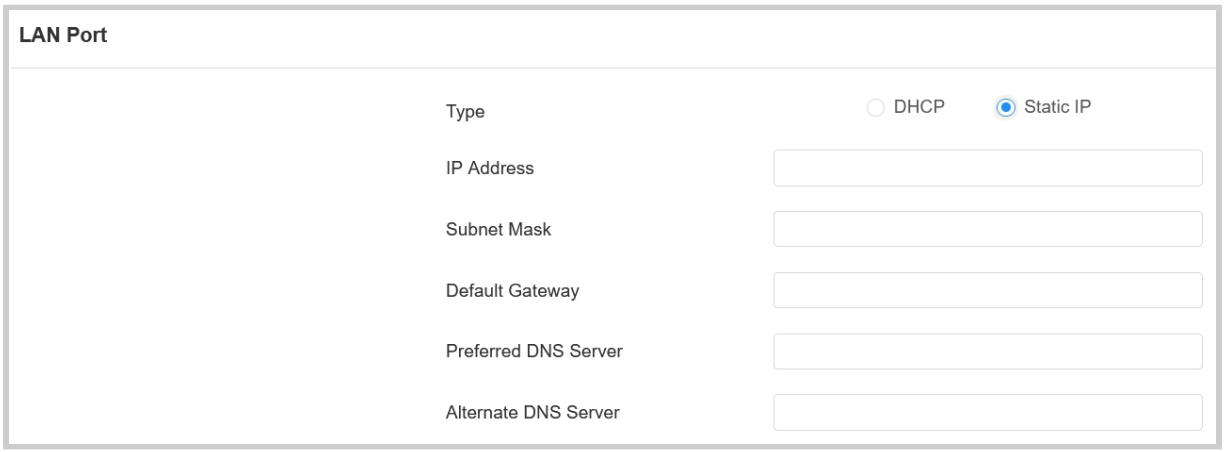


- **Voice Prompt**: Play the default prompt “Welcome, please come in” when the door is opened.
- **Sound Effect**: Play the Beep sound when the door is opened.

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.



- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, then 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 have to be manually configured according to the actual network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings with the IP, your computer should be on the same local network as the device.
- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.

- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **Preferred/Alternate DNS Server**: Set up the preferred or alternate Domain Name System(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 **Network > Advanced** interface.



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

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** interface.



- **HTTP Redirect**: It is enabled by default, which means all HTTP requests will automatically be redirected to HTTPS. If it is disabled, the device's web interface can be accessed using HTTP directly.

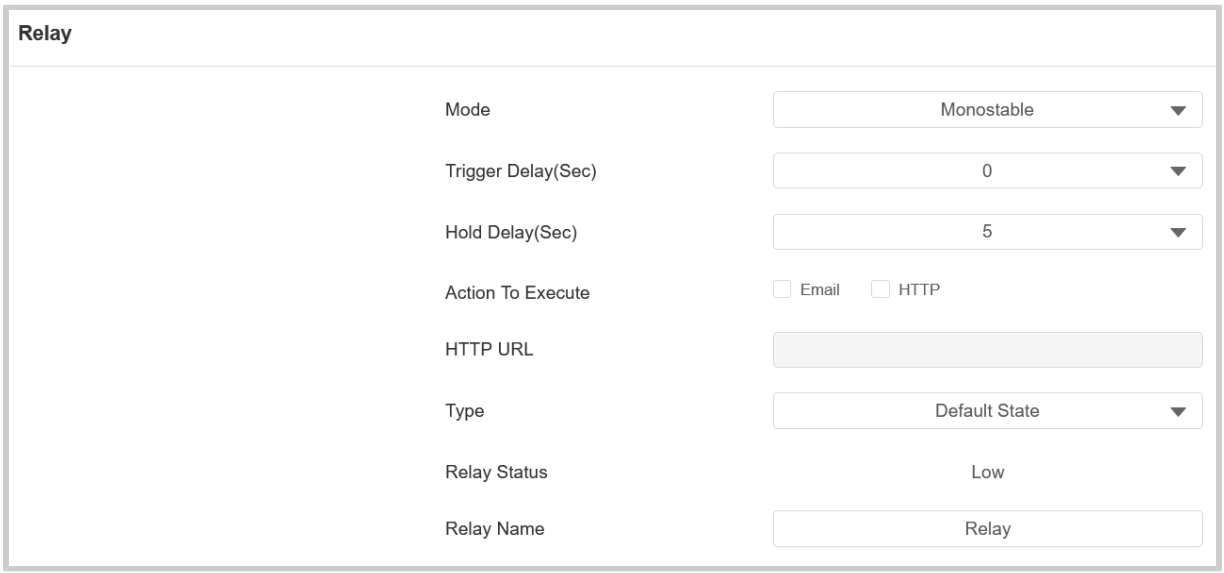
Relay Settings

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.



- **Mode**: Specify the conditions for automatically resetting the relay status.
  - **Monostable**: The relay status resets automatically within the relay delay time after activation.
  - **Bistable**: The relay status resets upon triggering the relay again.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.

- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **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.
- **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.

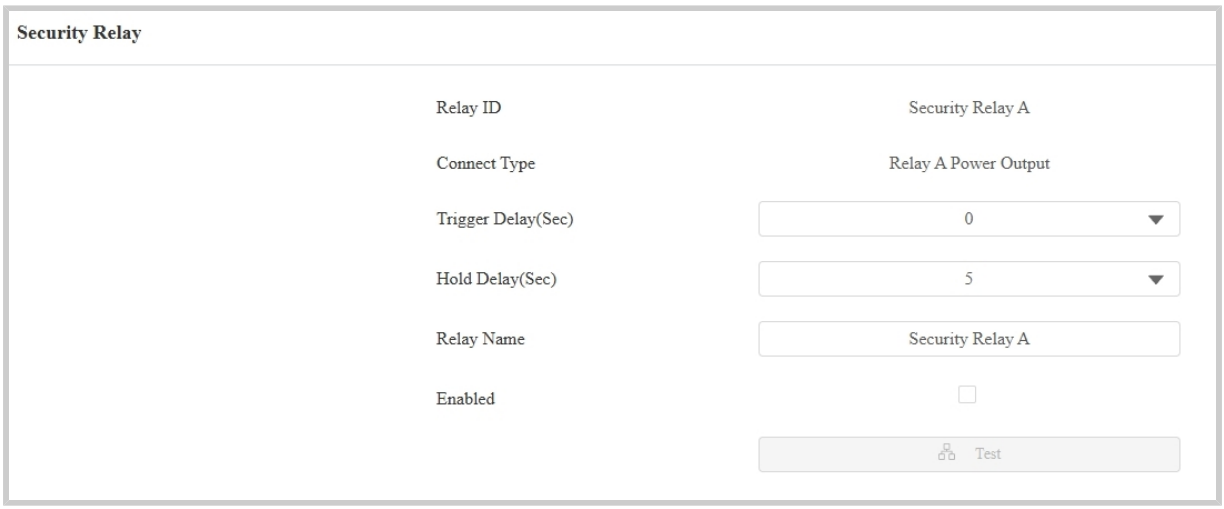
Security Relay

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.



- **Relay ID**: The specific relay for door access.
- **Connect Type**: The security relay connects to the device using Power Output by default.
- **Trigger Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.

- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **Relay Name**: Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.

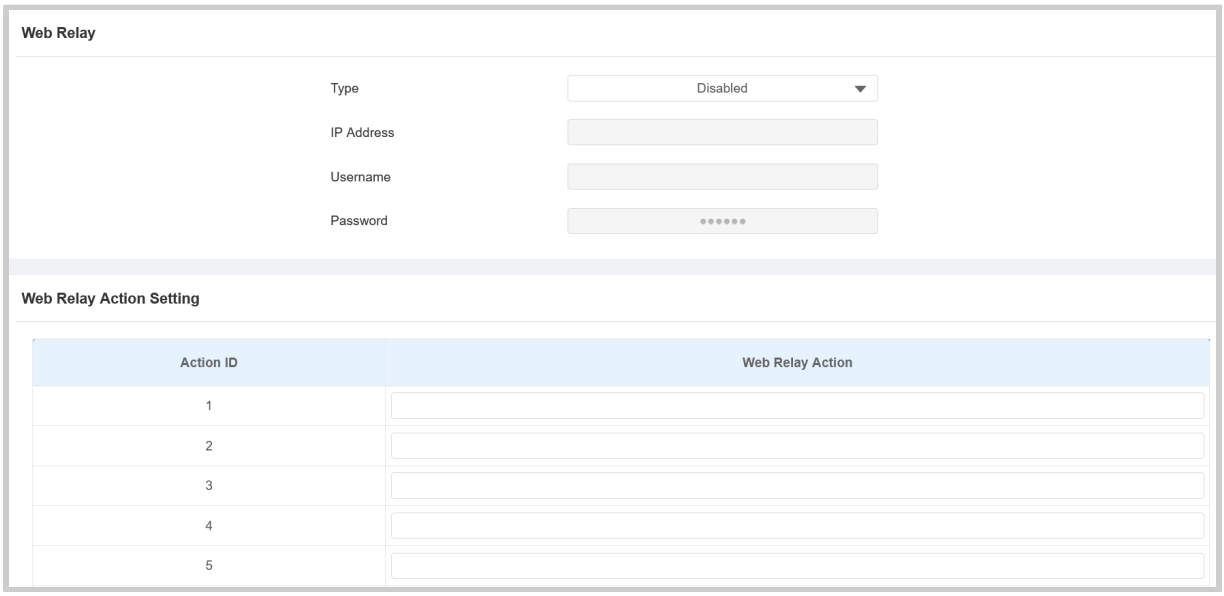
Web Relay

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.



- **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.
- **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.

Relay Keep Active While Card Present

Enable this feature to keep the relay triggered continuously while a valid card stays within its reader's detection range. The relay will deactivate automatically when the card is moved away.

> **Note**
>
> - Upon detecting a valid card, the device generates a **Card Present** Access Log and activates the relay.
> - While continuously reading the card, the relay remains active. No additional Access Logs are generated.
> - Upon detecting the card leaving the reading area, the device generates a **Card Removed** Access Log.

Set up this feature on the **Access Control > Relay > Relay Keep Active While Card Present** interface.



- **Enabled**: Turn on/off the feature.
- **Open Relay**: Check the relay to be triggered.

- **Hold Delay(Sec)**: The time the relay remains active after the card is removed.

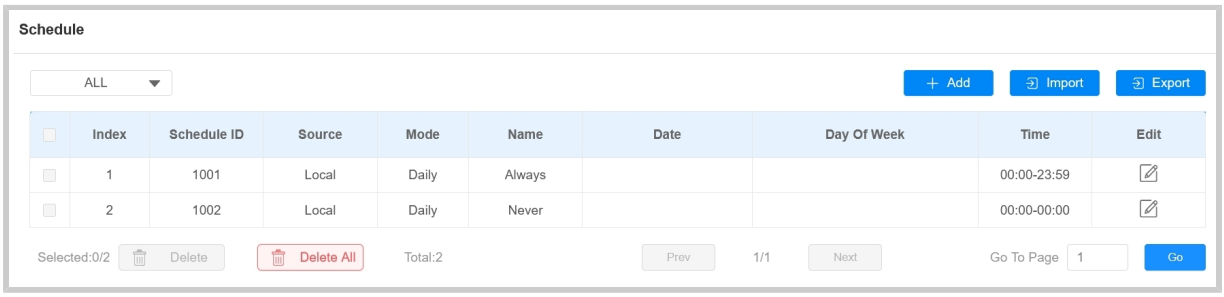
Door Access Schedule Management

Door Access Schedule

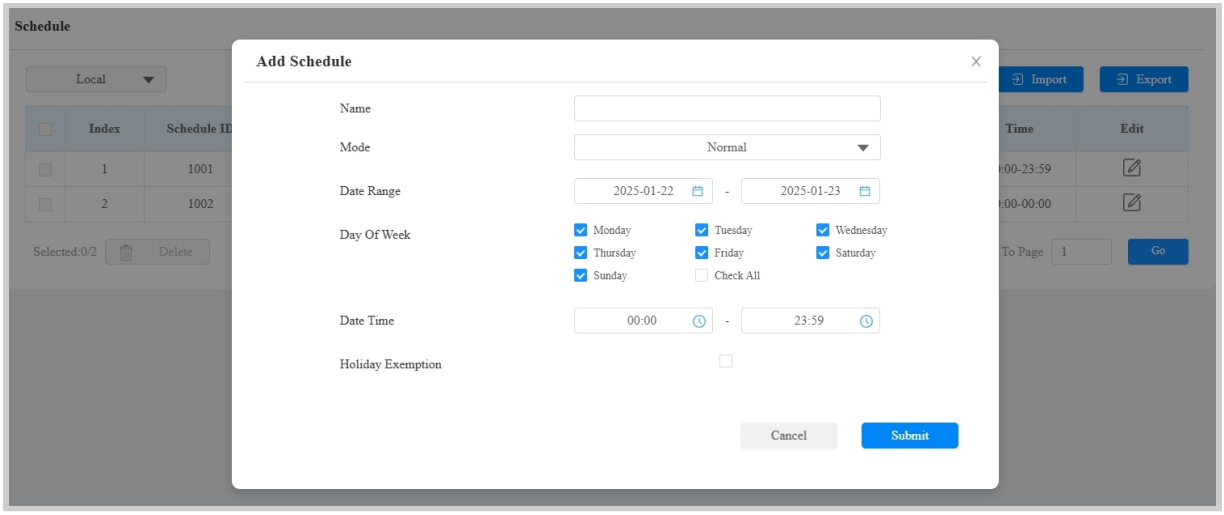
A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Door Access Schedule

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



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



- **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.



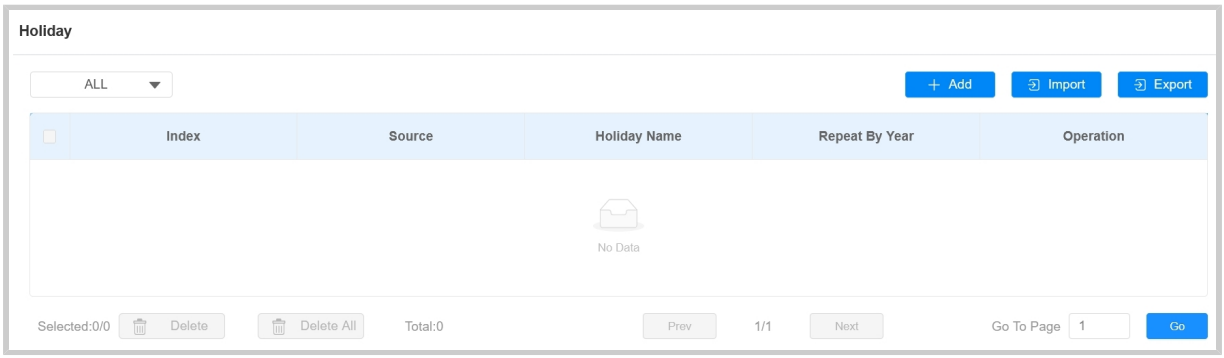
- **Repeat Type**:
  - **Routine Schedule**: The schedule repeats every week. Click **Edit** on the right to configure.
  - **One-Time Runs**: Set the daily or weekly schedule that repeats during a defined period.
- **Schedule Mode:**
  - **Hold Open**: The door remains open during the scheduled time.
  - **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.

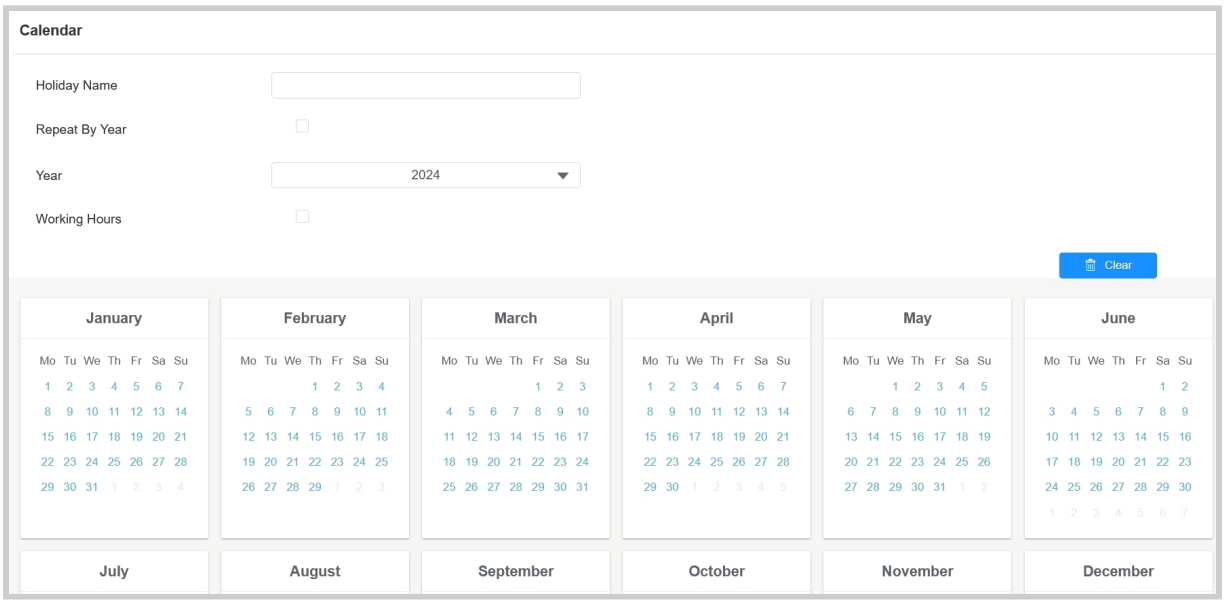
> **Note**
>
> Click here to view the detailed configuration of each schedule mode.

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 web **Setting > Holiday** interface. Click **+Add** to add a holiday and click **+Clear** to clear the selection of all dates.





You can also import and export schedule files on the same interface. The file exported is in **TGZ** format. The imported file should be in **XML** format.



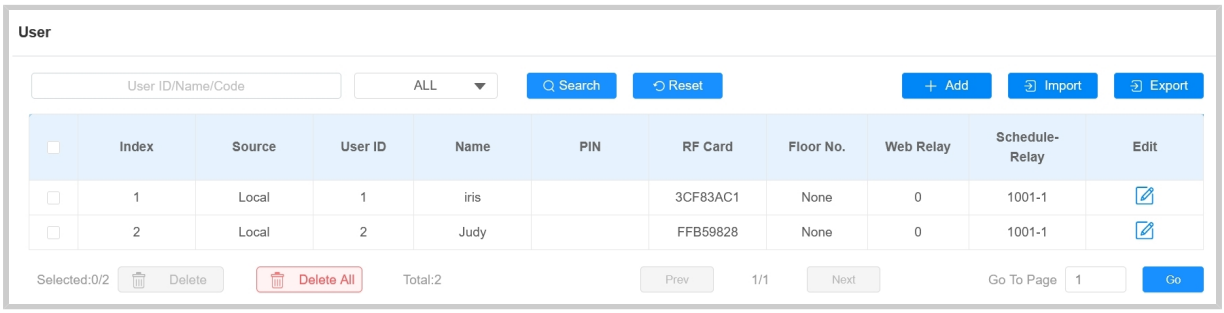
Door-opening Configuration

User-specific Access Methods

The private PIN code and RF card 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 ID**: The unique identification number assigned to the user.
- **Name**: The name of this user.
- **Role**: Define the user as a General User or an Administrator. The Admin card can be used to add a user card. Please refer to Configure Admin Cards and User Cards for detailed configuration.

Unlock by Private PIN Code

The device can be connected to an external keypad. Users can open doors by entering their private PINs on the keypad.

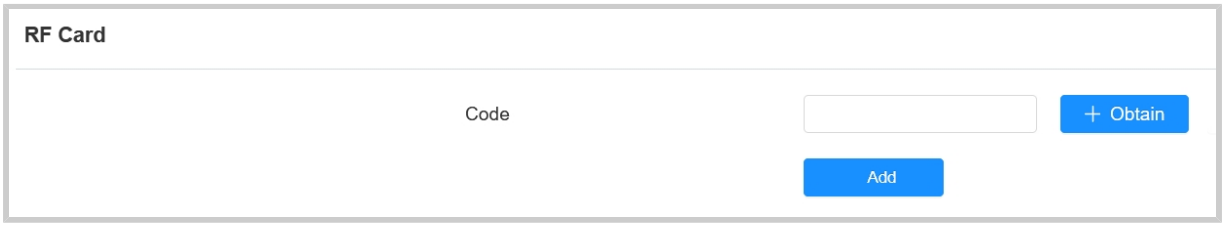
On the **Directory > User > +Add** interface, scroll to the **PIN** section.



- **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

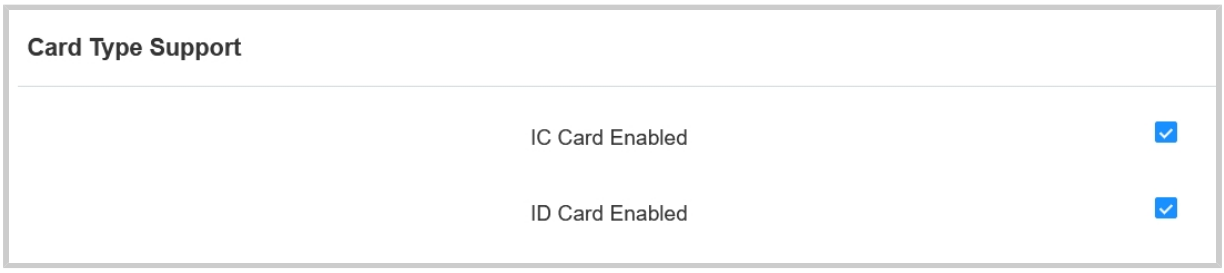
On the **Directory > User > +Add** interface, scroll to the **RF Card** section.



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

> **Note:**
>
> - 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.

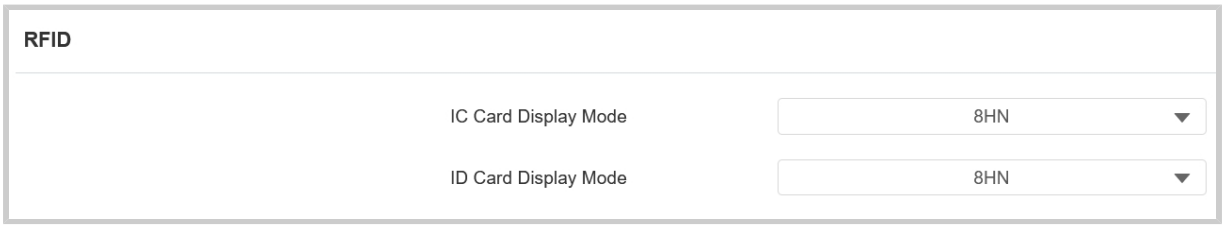
You can enable or disable the use of RF cards on the **Access Control > Card Setting** interface.



RF Card Code Format

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

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



- **IC/ID 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.

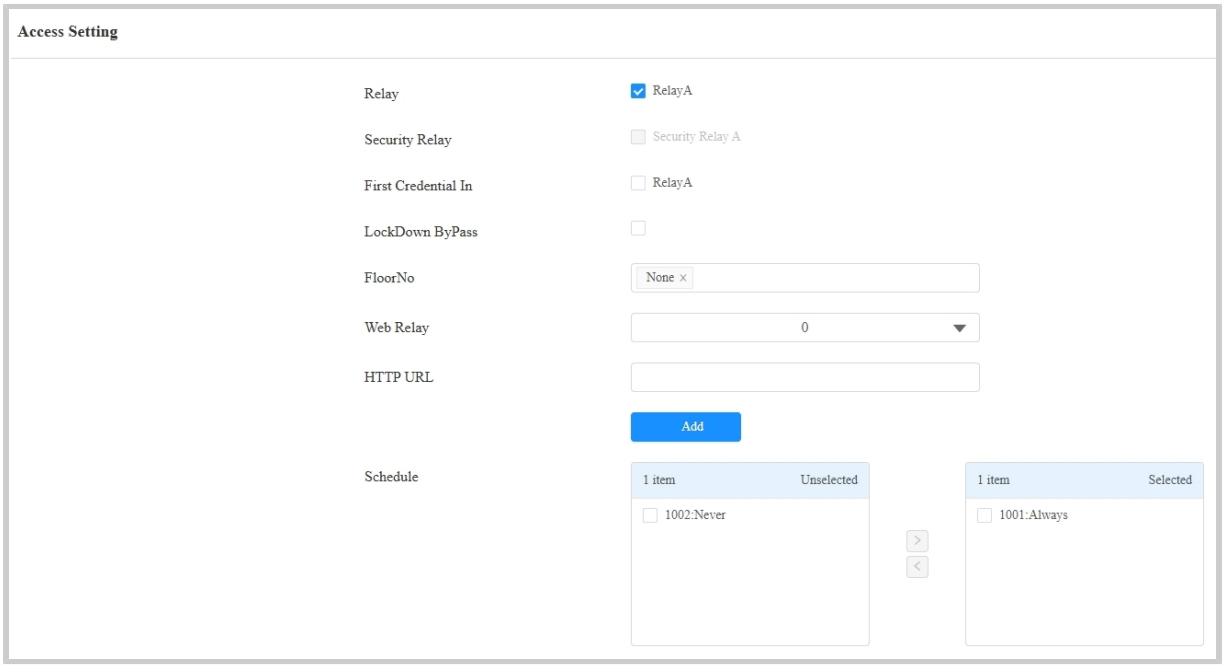


- **Add**: A user can have up to 5 license plates.
- **Duration**: Enable/disable Long-term Vehicle. It is enabled by default. If disabled, specify when the vehicle can enter or exit the parking lot.

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.

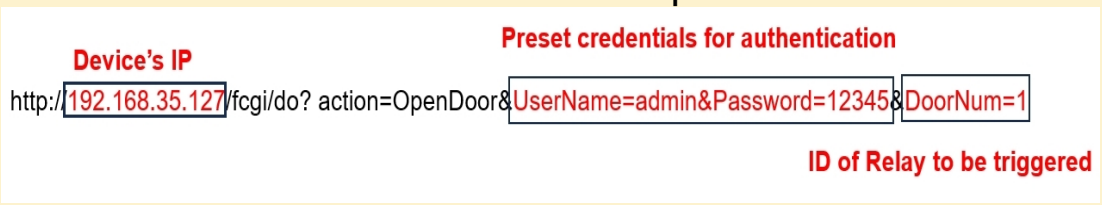


- **Relay**: Check the relay to be unlocked using the door opening methods assigned to the user.

- **Security Relay**: Select the security relay that you've configured on the Security Relay interface.
- **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 floor(s) that are accessible 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.
- **HTTP URL**: Specify the HTTP URL sent to another Akuvox device for door opening. You can add up to 10 commands.
- **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.

Tip

Here is an HTTP command URL example:



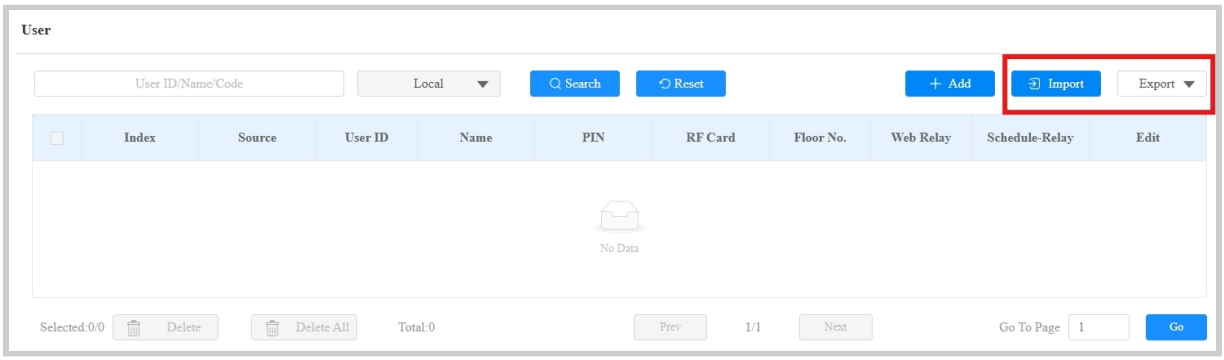
Note

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

Import and Export User Data

You can import and export user data for quick setup on the **Directory > User** interface.

The import/export file format can be .XML or .CSV.



NFC and Felica Card Setting

Set the device to support NFC and Felica cards on the device before they can be used.

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



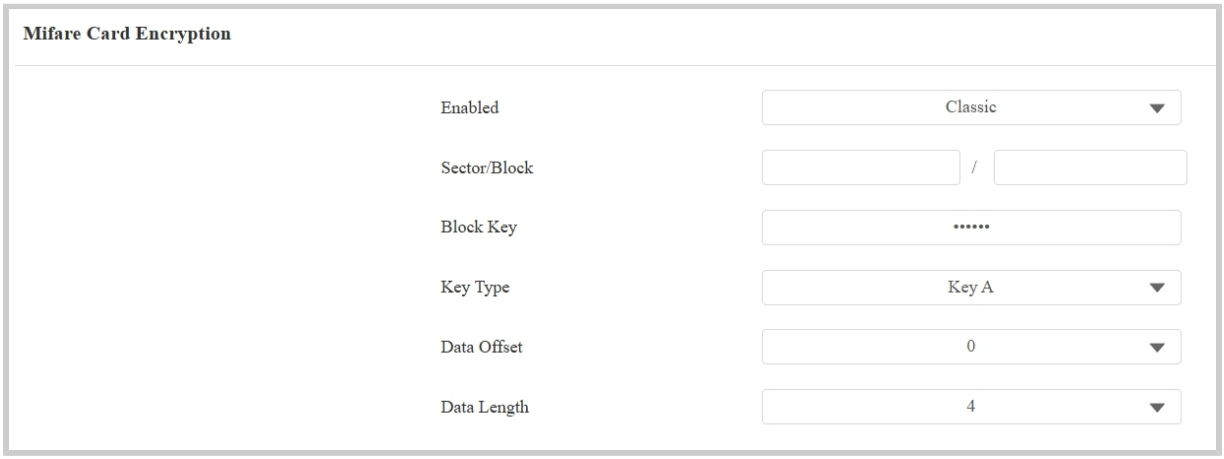
- **Enabled**: Select NFC or Felica from the list.
- **Felica Reading Format**: When Felica is selected, set the card reading format between 8 Bytes and 16 Bytes. The default is 16 Bytes.

> **Note**
>
> The NFC feature is not available on iPhones.

Mifare Card

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

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



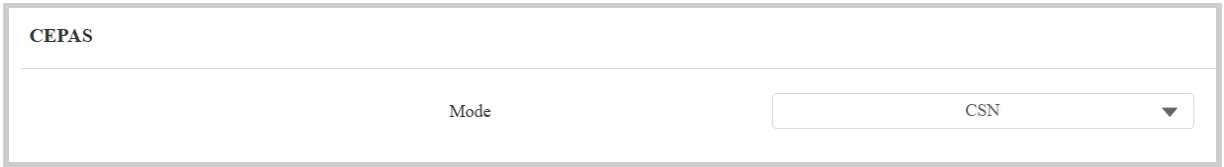
- **Classic**:
  - **Sector/Block**: Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (0 to 15), and each sector has 4 blocks (0 to 3).
  - **Block Key**: Set a password to access the data stored in the predefined sector/block.
  - **Key Type**: The authentication key type used to read the Mifare Classic card
  - **Data Offset**: The starting byte position from which card data is read. The default is 0.
  - **Data Length**: The number of valid data bytes to read from the card. The default is 4.
- **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.

  - **Read Key**: The file key.
  - **Key Index**: The index number for the key, which can be a number from 0 to 11.
  - **Byte Order**: The byte reading order. The default is MSB. The device starts reading bytes after performing **Data Offset** and **Data Length**.
    - **MSB**: Most Significant Bit means the reading order is normal(from left to right).
    - **LSB**: Least Significant Bit means the reading order is reversed(from right to left).
  - **Data Offset**: Define from which byte position to start reading data, with a range of 0 to 43. The default is 0.
  - **Data Length**: Define the length of valid byte data, with a range of 1 to 8. The default is 4.
- **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.

CEPAS Card Reading

The device supports reading CEPAS cards. Under the **CEPAS** functionality module, there are two toggle options available: **CSN** (Card Serial Number) and **CAN** (Card Number).

Select the card reading mode on the **Access Control > Card Setting > CEPAS** interface.



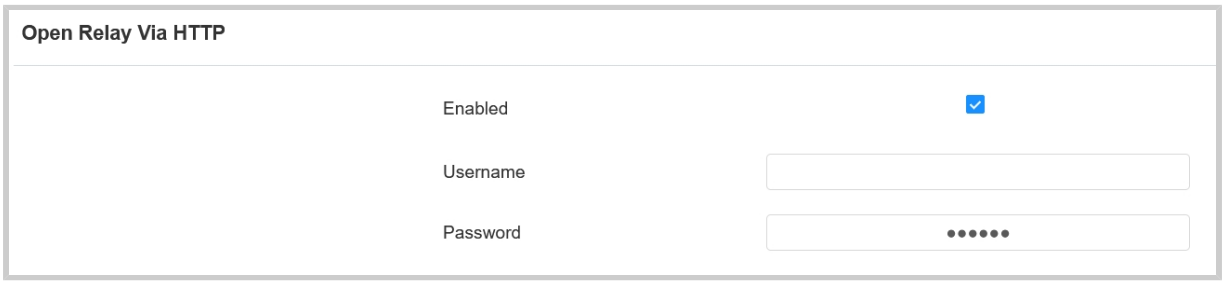
- **CSN**: The default option. This option allows the device to read the **UID** (Unique Identifier) of the CEPAS card, which is a unique value assigned to each card.

- **CAN**: This option allows the device to read the **card number** stored on the CEPAS card, which can be used for identification or access control.

Unlock by HTTP Command

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

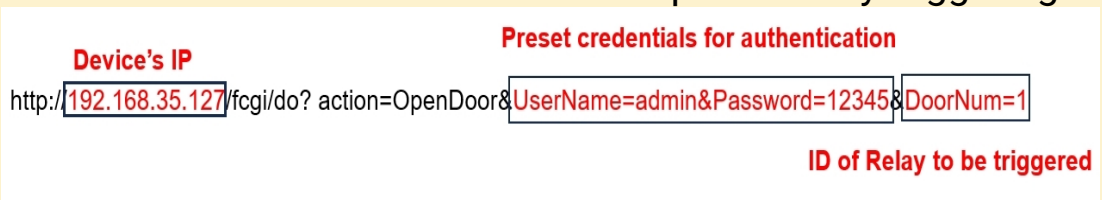
To set it up, go to **Access Control > Relay > Open Relay Via HTTP** interface.



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

Tip:

Here is an HTTP command URL example for relay triggering.

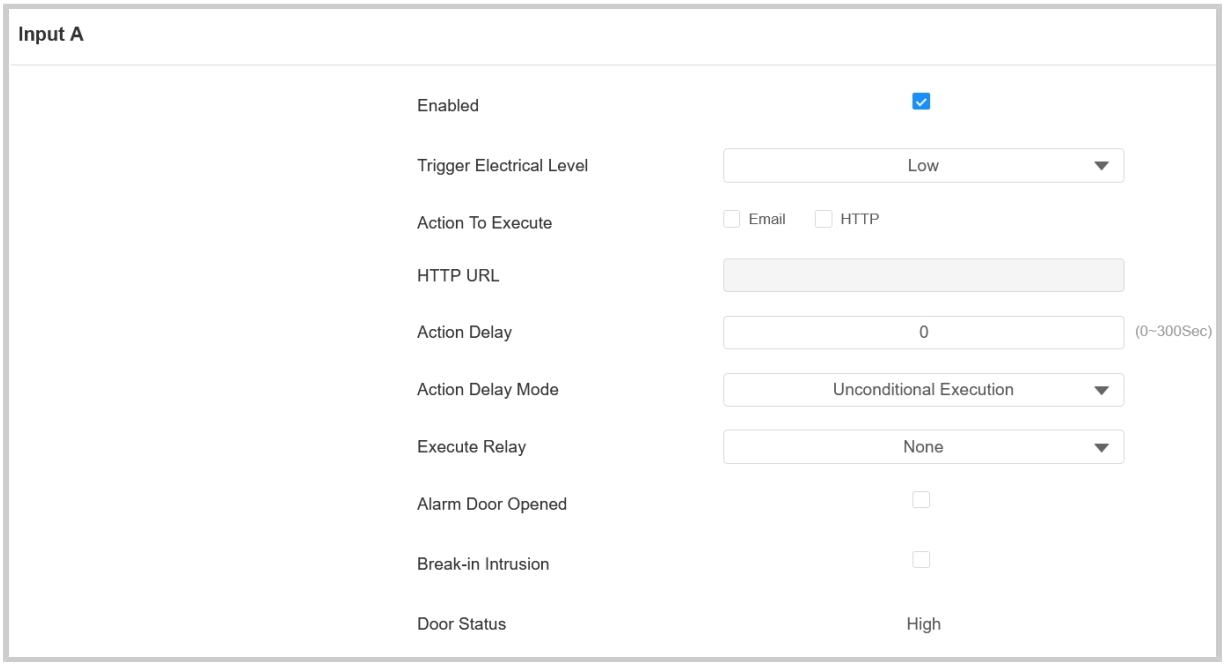


Unlock by Exit Button

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

Click here to watch the instruction video.

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



- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at 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.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions.

- **Action Delay Mode**:
  - **Unconditional Execution**: The action will be carried out when the input is triggered.
  - **Execute If Input Still Triggered**: The action will be carried out when the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay**: Specify the relay to be triggered by the actions.
- **Alarm Door Opened**: If enabled, when the door-opening time exceeds a limit, an alarm will be triggered.
  - **Door Opened Timeout**: The door-opening time limit.
- **Break-in Intrusion**: Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered. Click here to learn more information about this feature.
- **Door Status**: Display the status of the input signal.

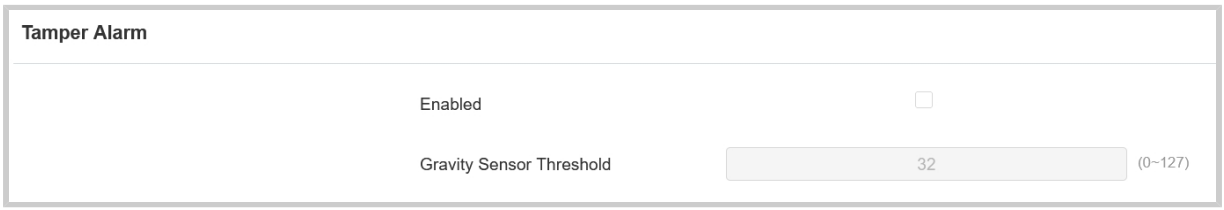
Security

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.



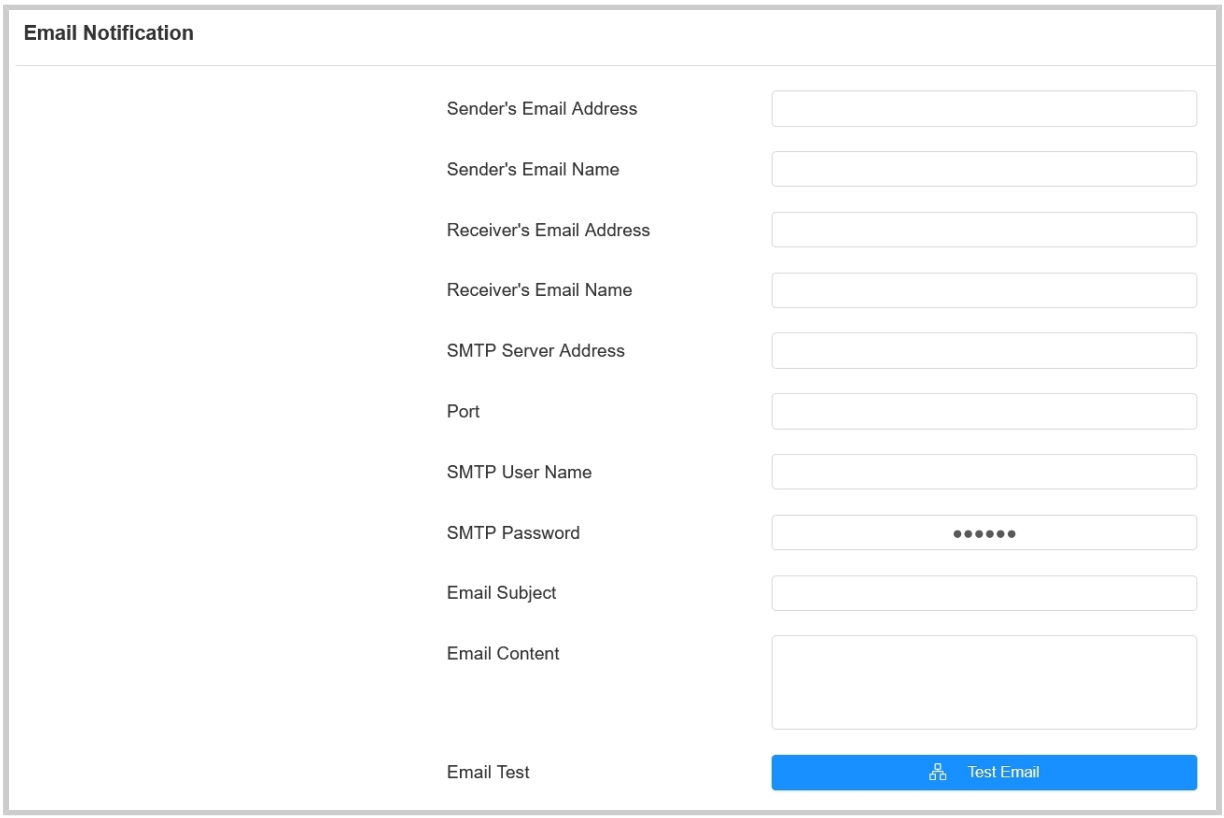
- **Gravity Sensor Threshold**: The threshold for gravity sensory sensitivity. The lower the value is, the more sensitive the sensor will be. It is 32 by default.

Security Notification

Email Notification

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

Go to **Setting > Action > Email Notification** interface.



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:

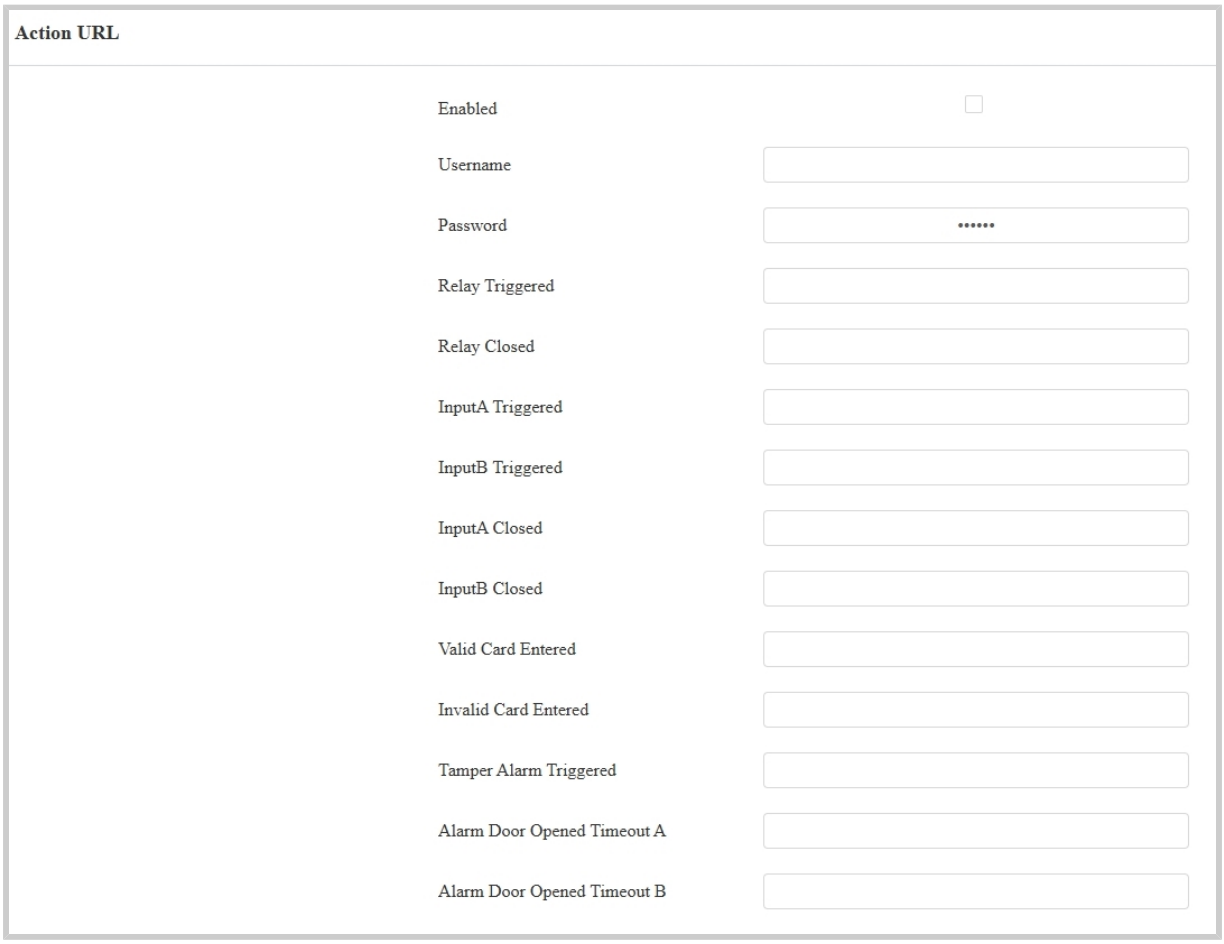
No	Event	Parameter format
1	Relay Triggered	$relay1status
2	Relay Closed	$relay1status
3	Input Triggered	$input1status
4	Input Closed	$input1status

5	Valid Card Entered	$card_sn
6	Invalid Card Entered	$card_sn
7	Tamper Alarm Triggered	$alarm status
8	Alarm Door Opened Timeout	$relay_id $location

Example
Http://server ip/relaytrigger=$relay1status
Http://server ip/relayclose=$relay1status
Http://server ip/inputtrigger=$input1status
Http://server ip/inputclose=$input1status
Http://server ip/validcard=$card_sn
Http://server ip/invalidcard=$card_sn
Http://server ip/tampertrigger=$alarm status
http://server ip/RelayID=$relay_id&Location=$location

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

To set it up, go to the **Setting > Action URL** interface. You can set the username and password for authentication.



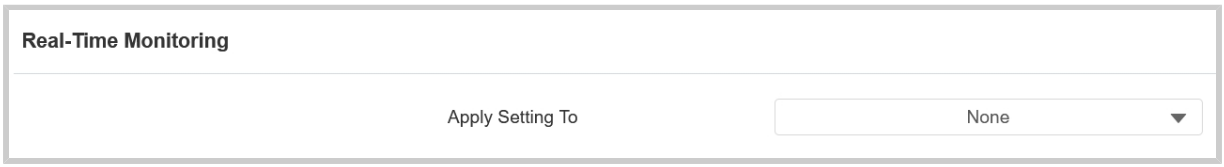
- **Alarm Door Opened Timeout A/B**: The HTTP URL will be sent when the door sensor connected to input A/B detects that the door-opening time exceeds a limit.
  - $relay_id in the URL refers to the relay triggered. RelayID=1 indicates RelayA; RelayID=2 indicates RelayB.
  - $location in the URL refers to the device's location that is configured on the SmartPlus Cloud.

> **Note**
>
> To enable Alarm Door Opened feature and set the time limit, go to the **Access Control > Input** interface.

Real-Time Monitoring

When the device is connected to SmartPlus Cloud or ACMS, the door status can be displayed on the SmartPlus platform or ACMS.

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



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

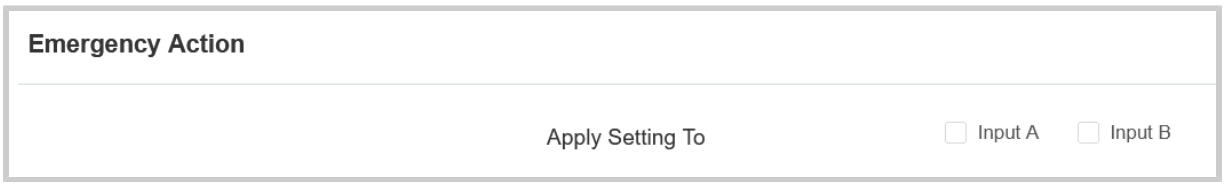
> **Note**
>
> Click here to see the detailed configuration steps.

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.

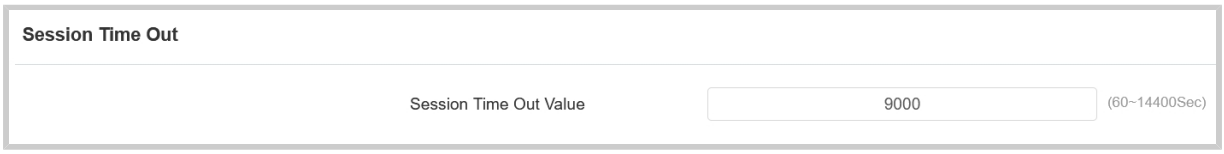
To set it up, go to **System > Security > Emergency Action** interface.



Web Interface Automatic Log-out

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

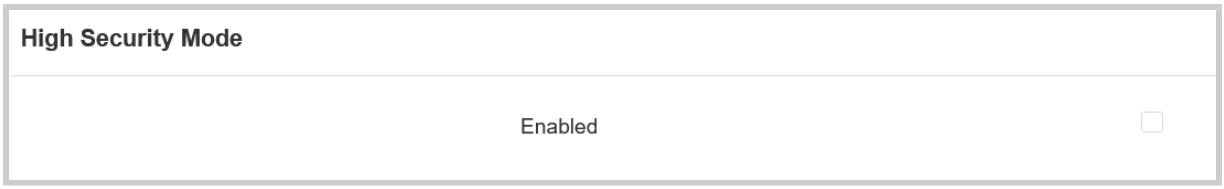
To set it up, go to **System > Security > Session Time Out** interface.



High Security Mode

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

To enable the mode, go to **System > Security > High Security Mode** interface.



Important Notes

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

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

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

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

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

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

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

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

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

Anti-passback Mode

This anti-passback mode restricts users from entering the door by following others.

Set it up on the **Directory > User** interface.

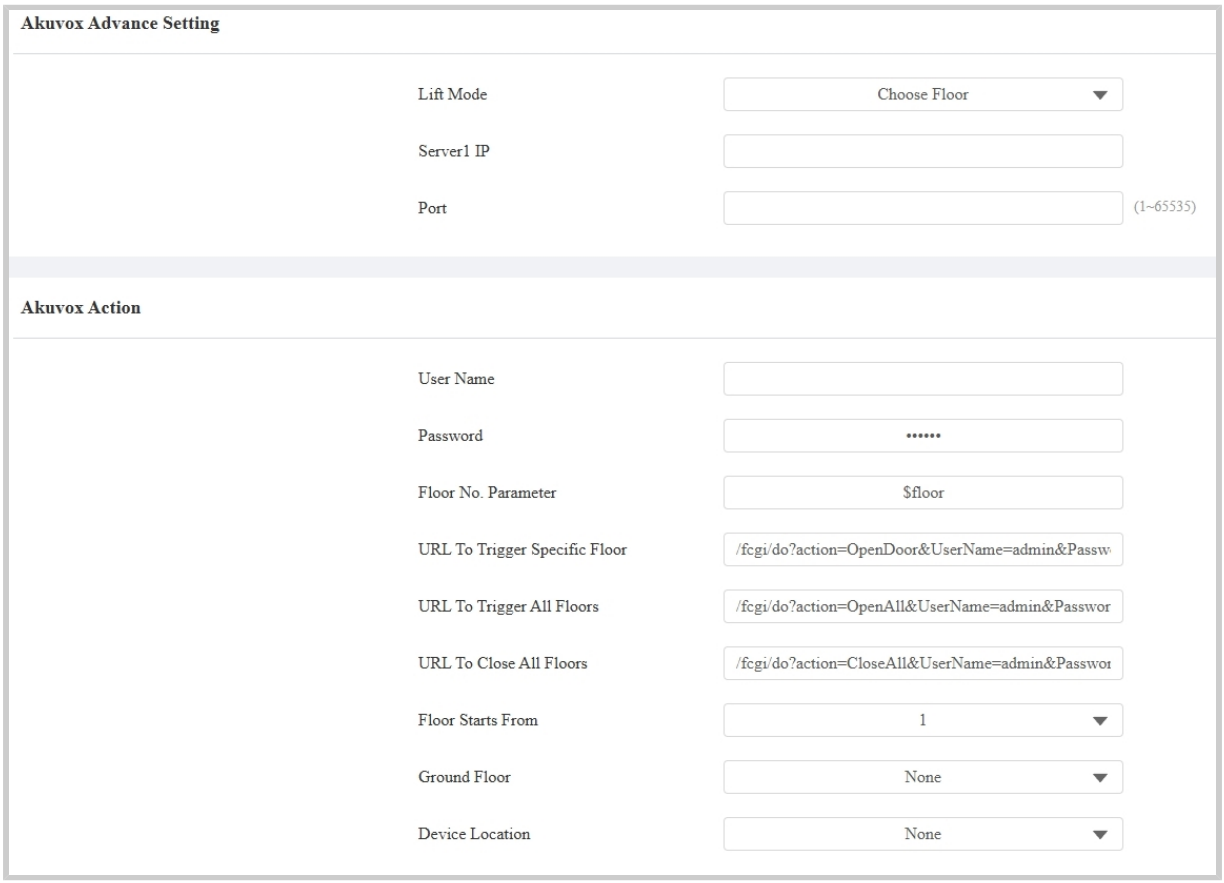


- **Mode**: Select Entry or Exit to enable the feature. For example, if the user follows someone else through the door, the next time he/she cannot swipe his/her card to pass the Entry/Exit door.

Lift Control

The device can be connected to the Akuvox lift controller for the lift control. You can summon the lift to go down to the ground floor when you are granted access through access methods.

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



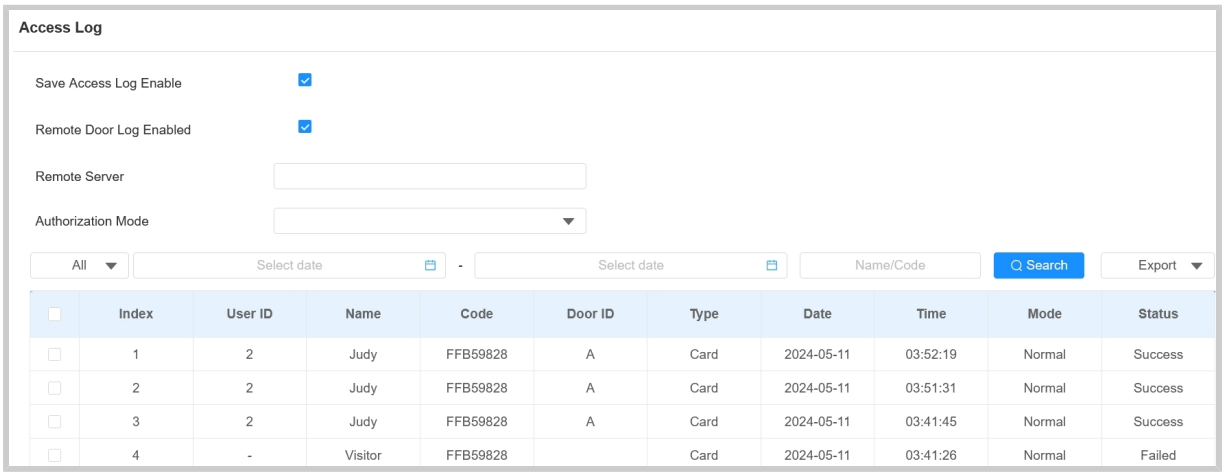
- **Lift Control List**: Select Akuvox for integration with the Akuvox lift controller.
- **Lift Mode:**
  - **Choose Floor**: Users can choose the floor they want to access when they use their credentials on the device.
  - **Direct Access:** Users will be directly sent to the target floor when they 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**: Enter the user name of the lift controller for authentication.
- **Password**: Enter the password of the lift controller for authentication.
- **Floor NO. Parameter**: Enter the Floor number parameter provided by Akuvox.
- **URL To Trigger Specific Floor**: Enter the URL for triggering a specific floor.
- **URL To Trigger All Floors**: Enter the URL for triggering all floors.
- **URL To Close All Floors**: Enter the URL used for closing all floors.
- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **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.

Logs

Access Log

You can search and check door logs on the device web **Status > Access Log** interface.

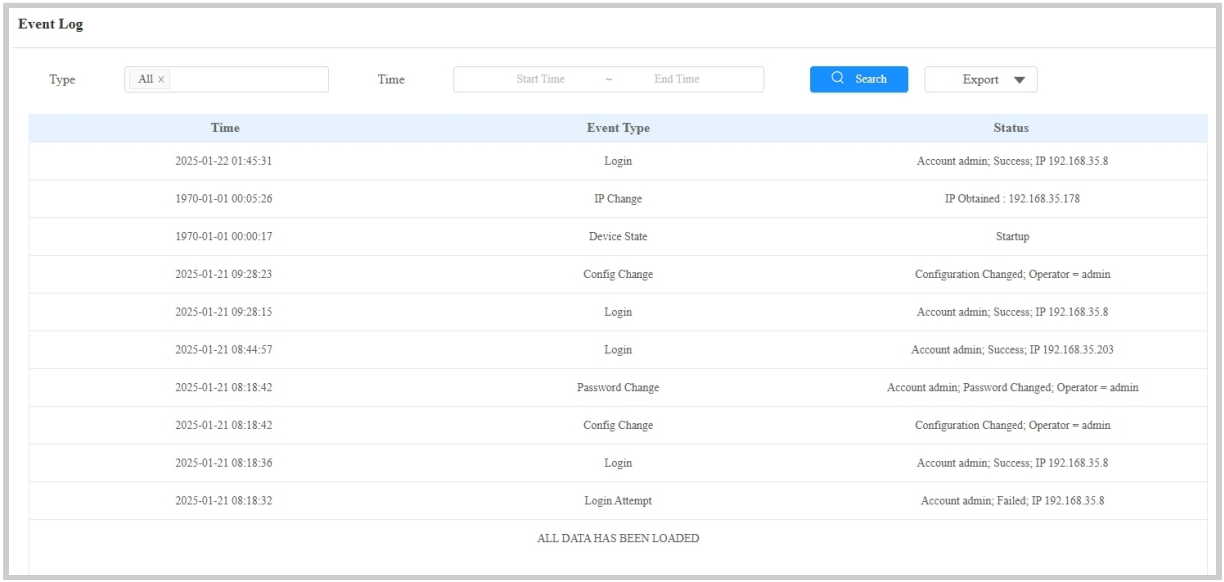


- **Save Access Log Enable**: Decide whether to save the door-opening records.
- **Remote Door Log Enabled**: Decide whether to send the door log to a third-party server.
- **Remote Server**: Enter the remote server address.
- **Authorization Mode**: Select from the **None, Basic, Digest**, and **Token**.
  - **Basic**: You are required to enter the username and password for authentication.
  - **Token**: You are required to enter the token URL, username, and password for authentication.
- **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 Card.

Event Log

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.

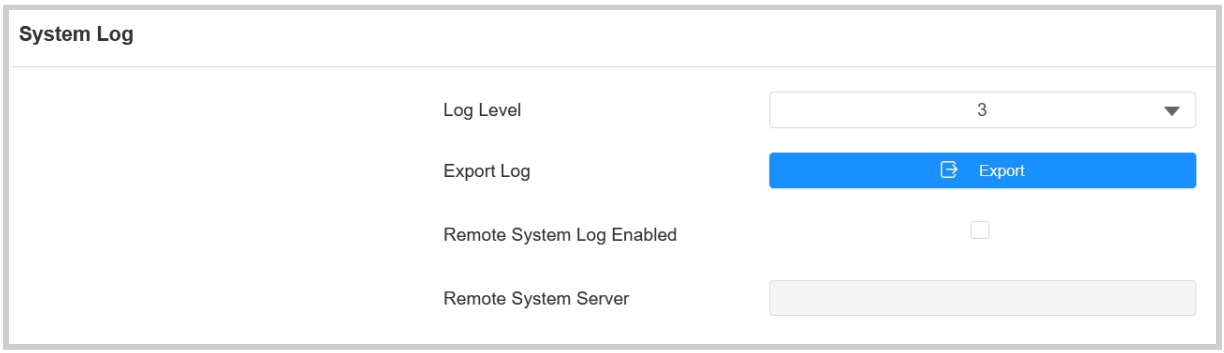


Debug

System Log for Debugging

System logs can be used for debugging purposes.

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

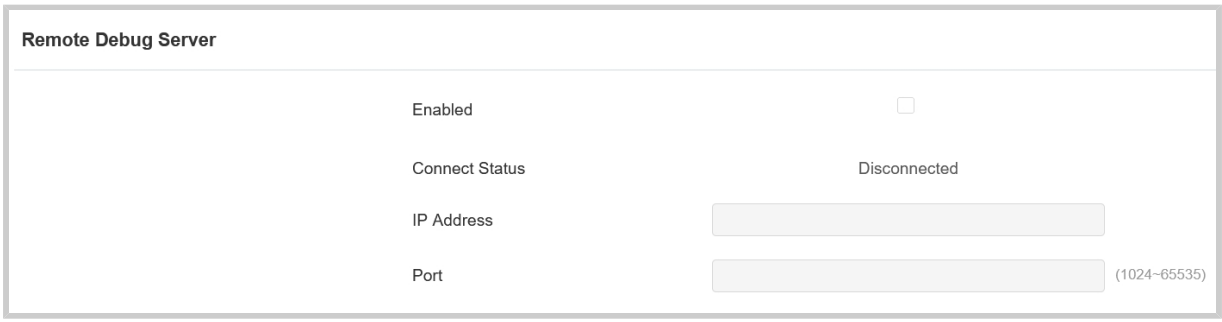


- **Log Level**: Log levels range from 1 to 7. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export the 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.

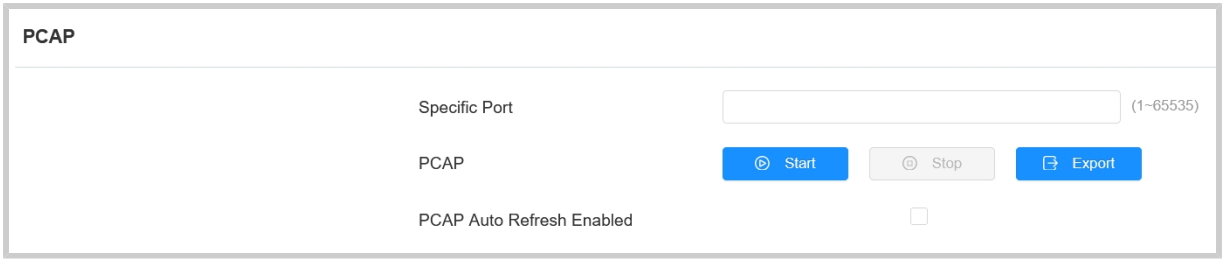


- **Connect Status**: Display the remote debug server connection status.
- **IP Address**: Set the remote debug server IP address. Please ask the Akuvox technical team for the server IP address.
- **Port**: Set the remote debug server port.

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.



- **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.

Set it up on the **System > Maintenance > Ping** interface.



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

Backup

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

Go to **System > Maintenance > Others** interface.

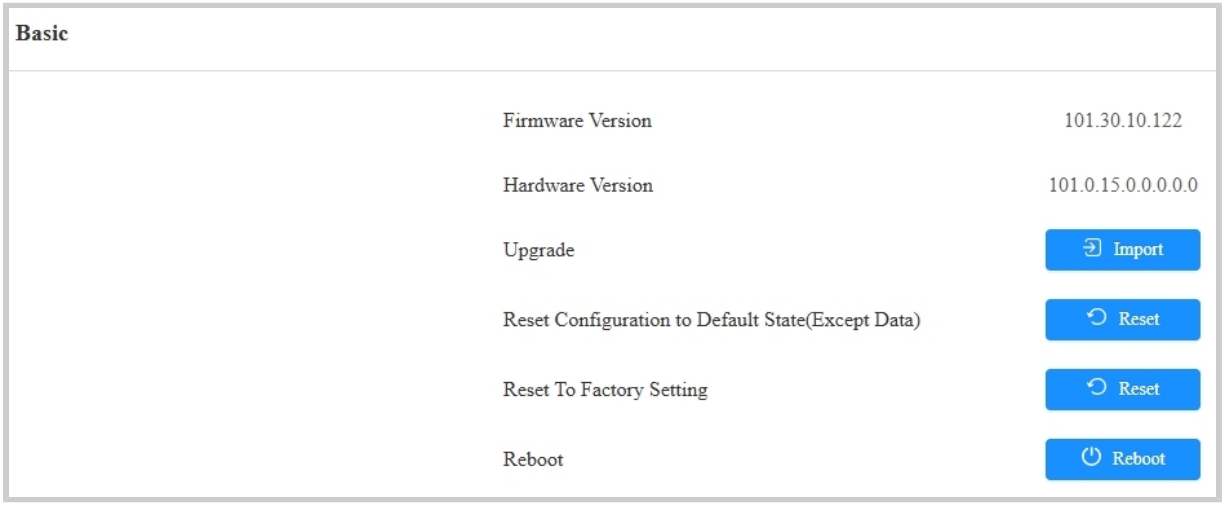


- **Config File**: Click **Export** to export configuration items as an encrypted file; click **Import** to import a configuration file to the device. The Config File is used to back up and restore device **configuration settings** only. It does not include user data and contact data.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



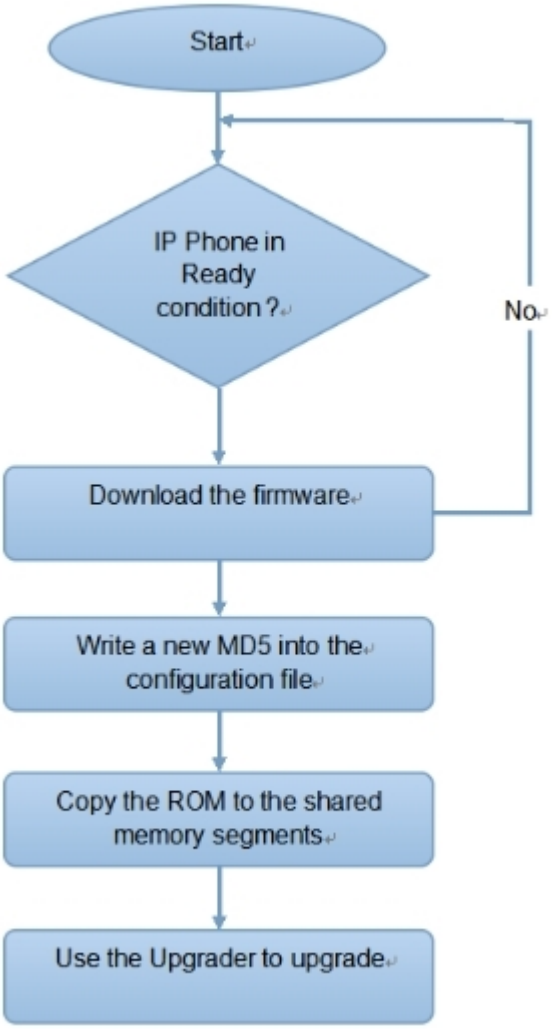
> **Note**
>
> The file should be in .rom format.

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:



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

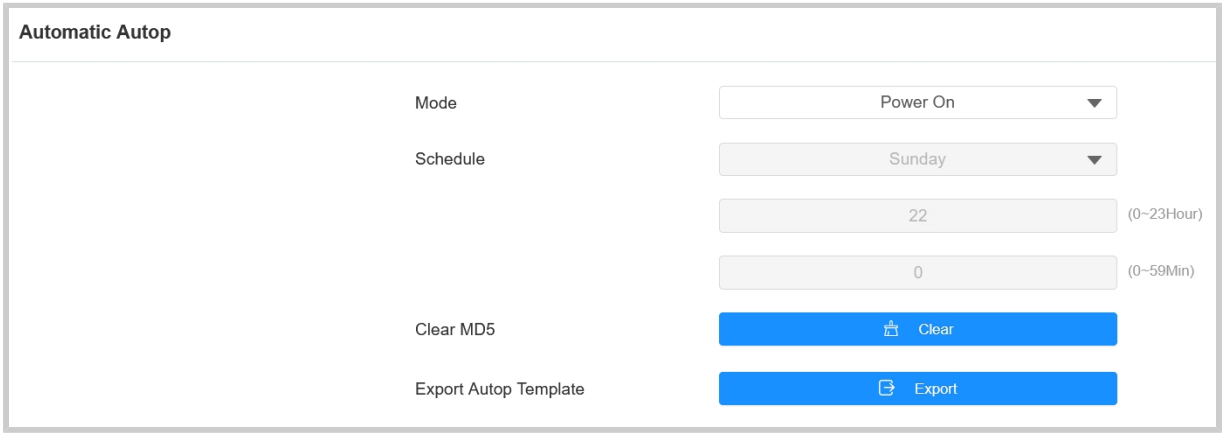
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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.

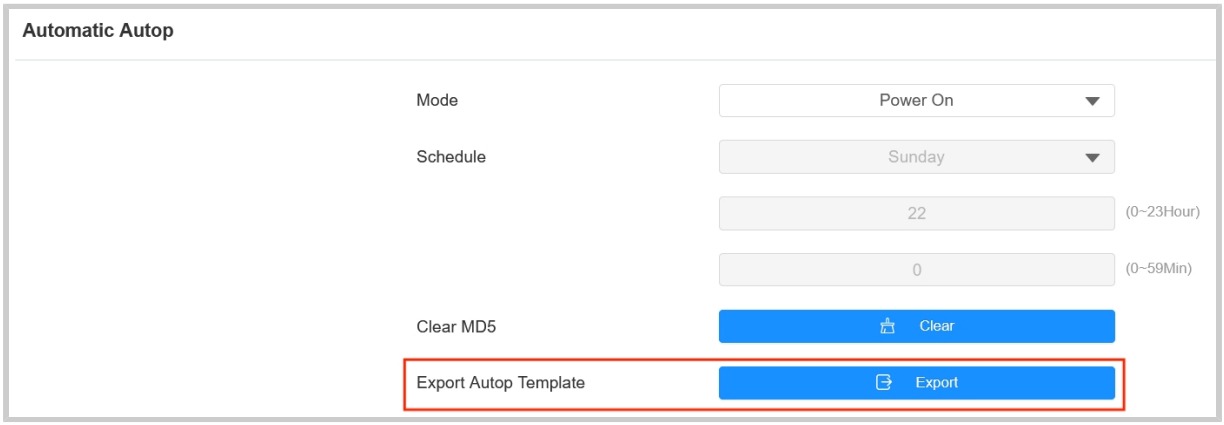


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every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

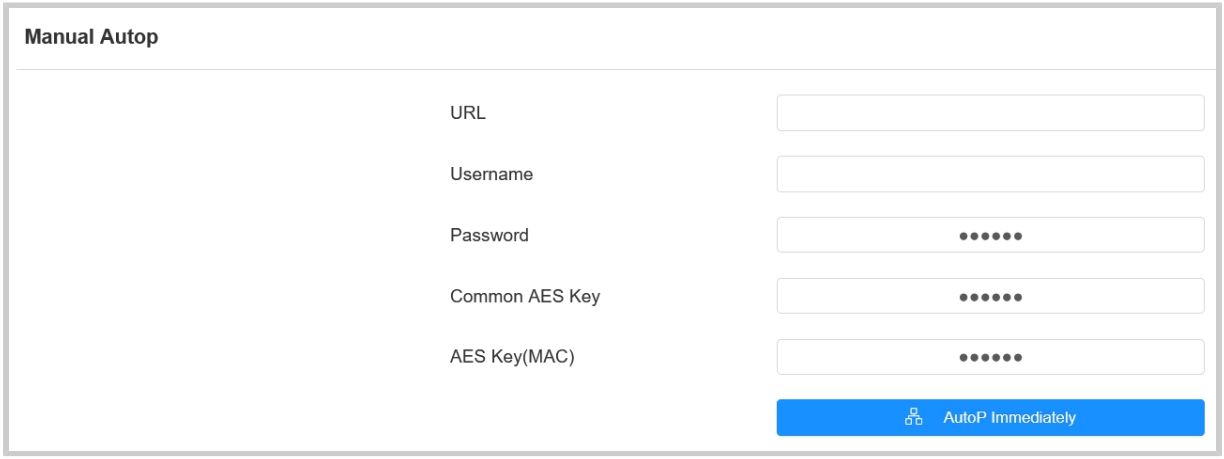
Static Provisioning

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.



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



- **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

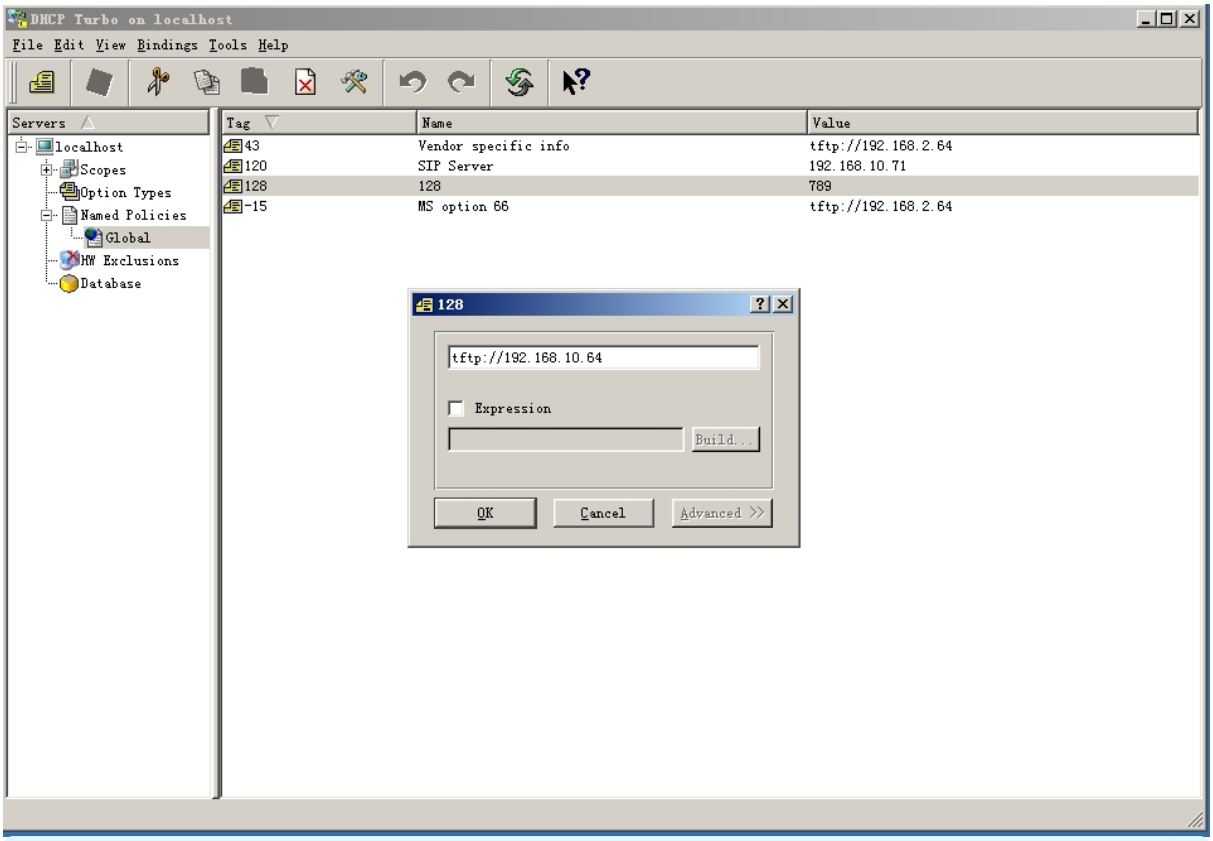
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use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

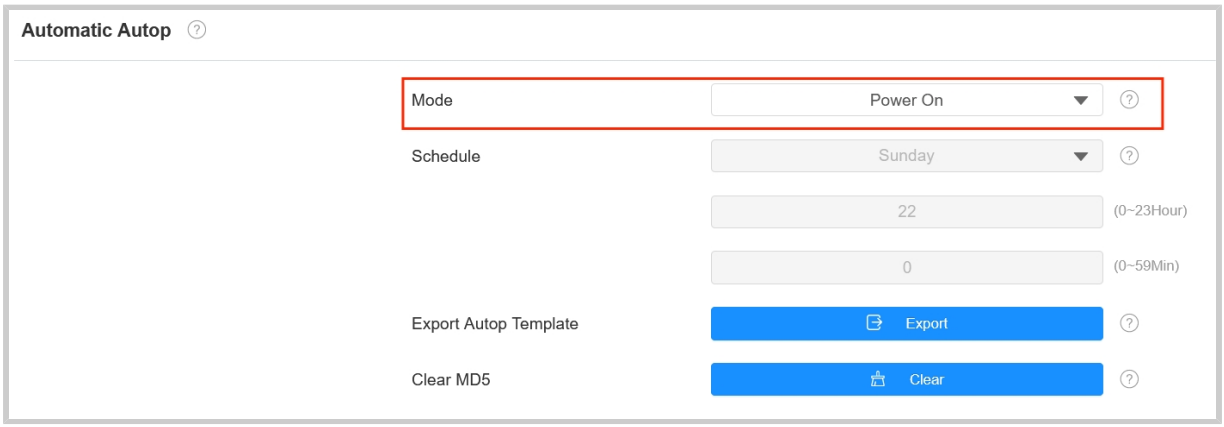
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **CustomOption**as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option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



Note

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

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



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



- **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 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.

Integration with Third-Party Device

Integration via Wiegand

The access control terminal can be integrated with third-party devices via Wiegand.

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



- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options: 8H10D, 6H3D5D, 6H8D, 8HN, 8HR, RAW, 8HR10D, and 6H3D5D-R.
- **Wiegand Card Reader Mode**: The transmission format should be identical between the access control terminal and the third-party device. The device supports **Wiegand 64** output mode. To enable this format, configure the card type as **Wiegand 66** and disable **CRC Verification**.
- **Wiegand Transfer Mode**:
  - **Input**: The device serves as a receiver.
  - **Output**: The device serves as a sender.
- **Wiegand Input Clear Time**: When the interval of entering passwords exceeds the time. All entered passwords will be cleared.

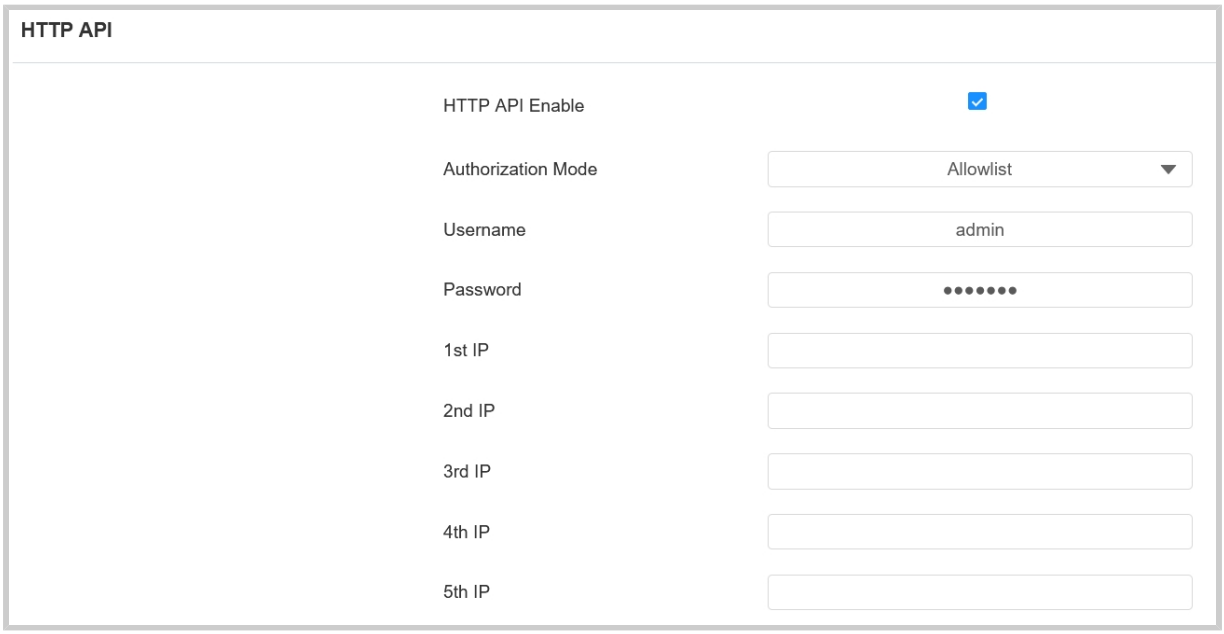
- **Wiegand Input Data Order**: Set the Wiegand input data sequence between Normal and Reversed. If you select Reversed, then the input card number will be reversed.
- **Wiegand Output Data Order:** Determine the sequence of the card number.
  - **Normal**: The card number is displayed as received.
  - **Reversed**: The order of the card number is reversed.
- **ID Card Output Raw Bytes**: This option is available when Wiegand Transfer Mode is **Output**. Select the output bytes of ID cards between 3 and 4 bytes.
- **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 Out Verification**: This feature is for checking the card validity when **Output** mode is selected.
- **Card Entered Action**: HTTP command to be triggered when users swipe a card to open the door.

> **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 intercom device.

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



- **Enabled**: Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode**: Select among 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 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 device when the **Allowlist** authorization is selected for the integration.

Please refer to the following description for the Authentication mode:

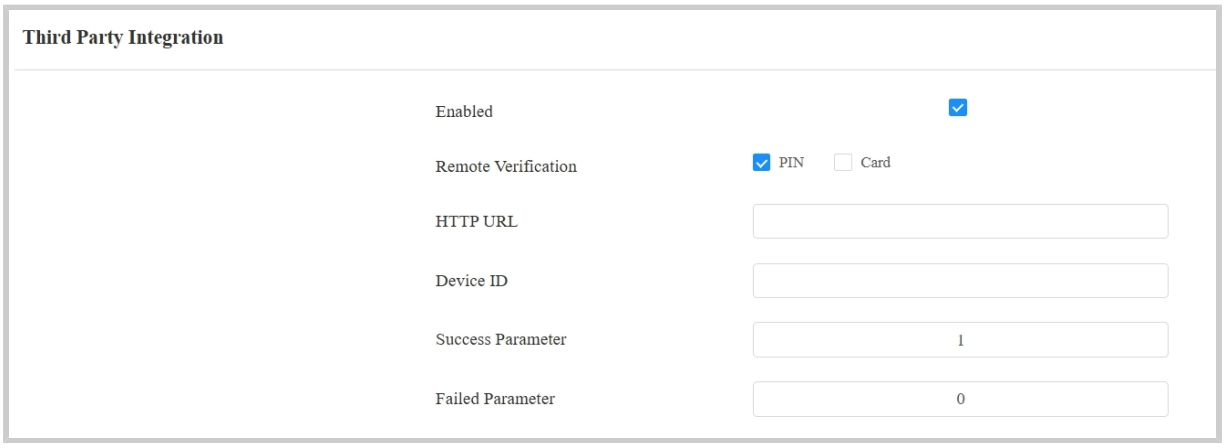
Authorization Mode	Description
None	No authentication is required. This mode is intended for testing only and is not recommended in production environments.

Authorization Mode	Description
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.

Third-Party Integration

The device supports reading PIN codes and card codes and transmitting them to a third-party server. The generation and validation of the codes are handled on the third-party server.

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



- **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 entering the PIN code or swiping the card, the HTTP command will carry the dynamic information automatically before it is sent to the server for verification. See the example: *http://{Server IP}:8090/api/visitor/scan?codeKey={Card}/{PINCode} &deviceId={DeviceID}.* For example, if users open doors with a PIN, the URL will be *http://192.168.35.123:8090/api/visitor/scan?codeKey={Card} /123456&deviceId=1.*
- **Device ID**: As part of the HTTP URL, it is provided by the service provider of the third-party server.
- **Success Parameter**: Receiving this value indicates that opening the door succeeds.
- **Failed Parameter**: Receiving this value indicates that opening the door fails.

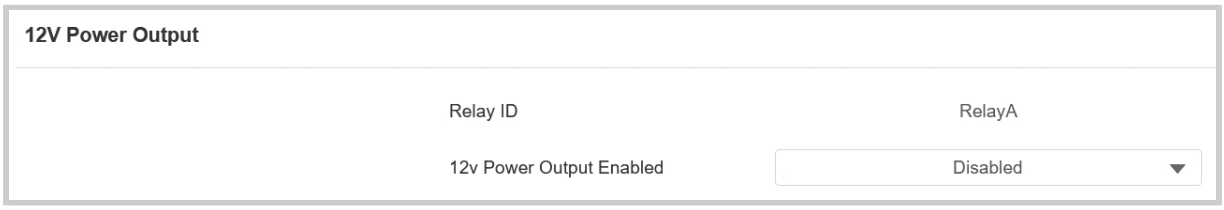
Note

- To transmit PIN values, the device firmware version should be 101.30.10.128 or higher.
- To support Success and Failed Parameters, the device firmware version should be 101.30.11.124 or higher.

Power Output Control

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

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



- **12v Power Output Enabled**:
  - **Always**: The device can provide continuous power to the third-party device.
  - **Security Relay A**: The device can work with the security relay.

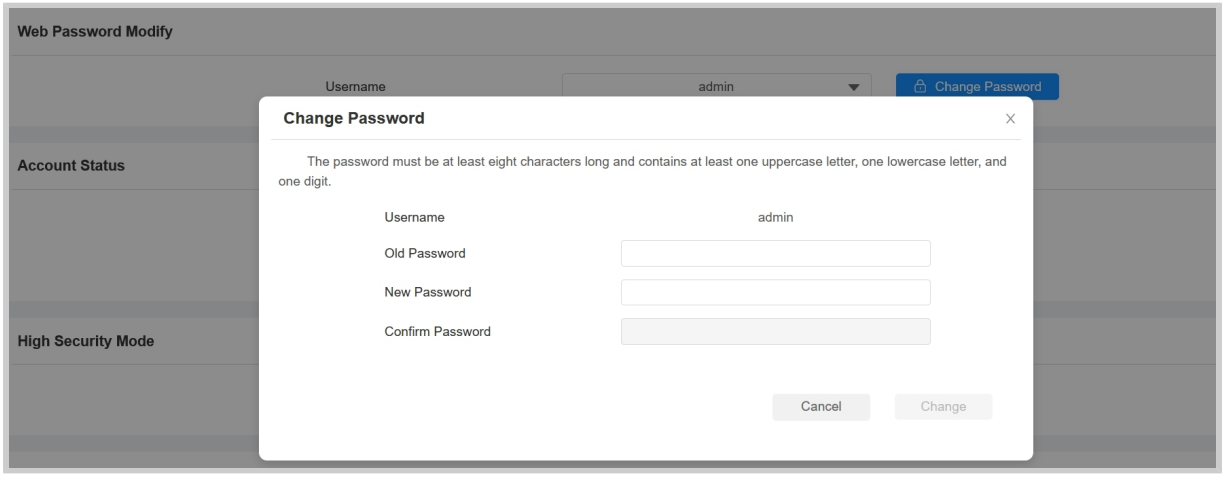
Password Modification

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

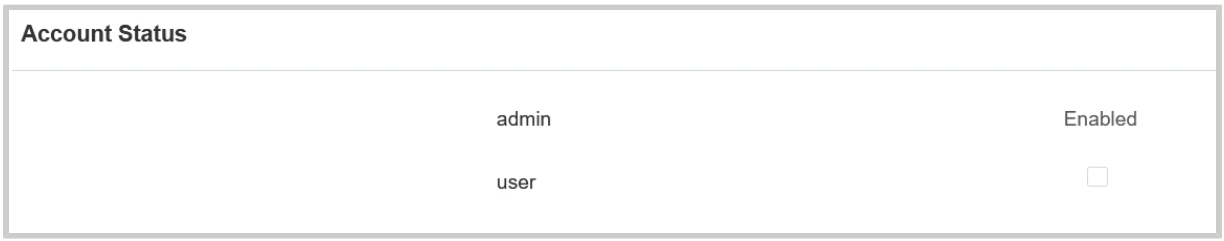
To set it up, go to **System > Security > Web Password Modify** interface.



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



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



Modify Security Questions

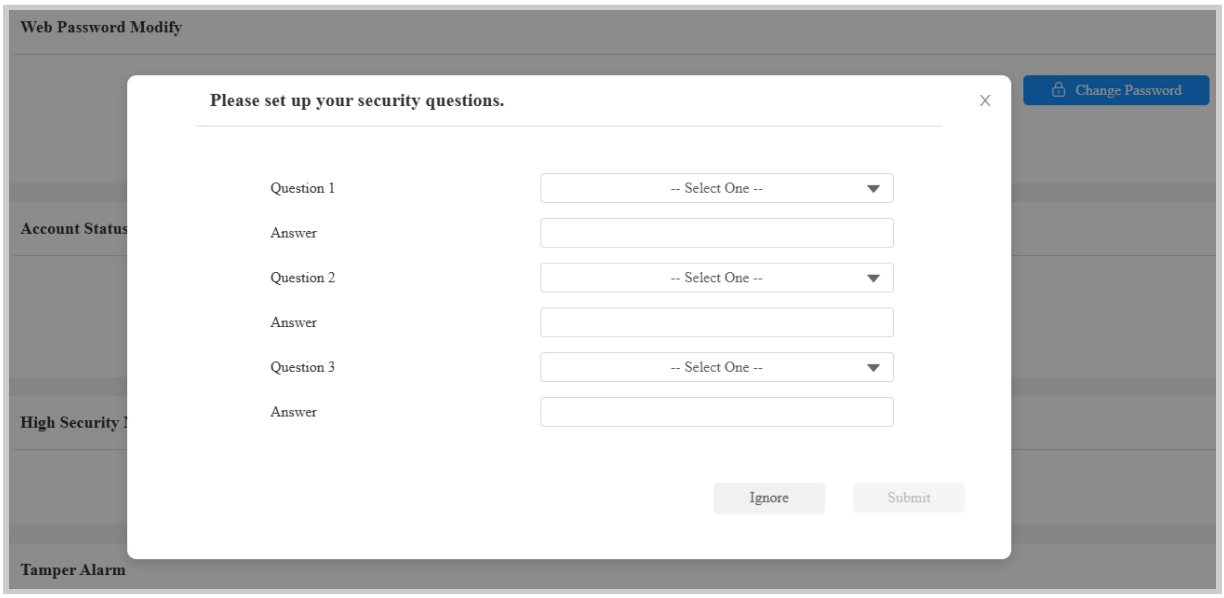
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

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



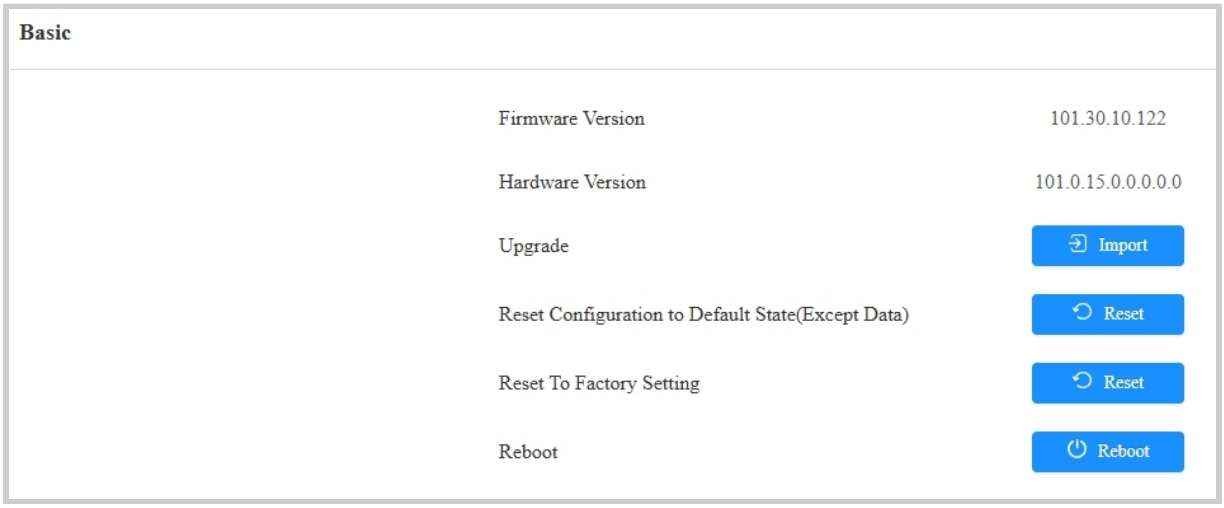
You are required to fill in the correct password before setting the new password.


Web Password Modify
Change Password
Account Status
High Security
Tamper Alarm
Please set up your security questions.
Question 1
-- Select One --
Answer
Question 2
-- Select One --
Answer
Question 3
-- Select One --
Answer
Ignore
Submit

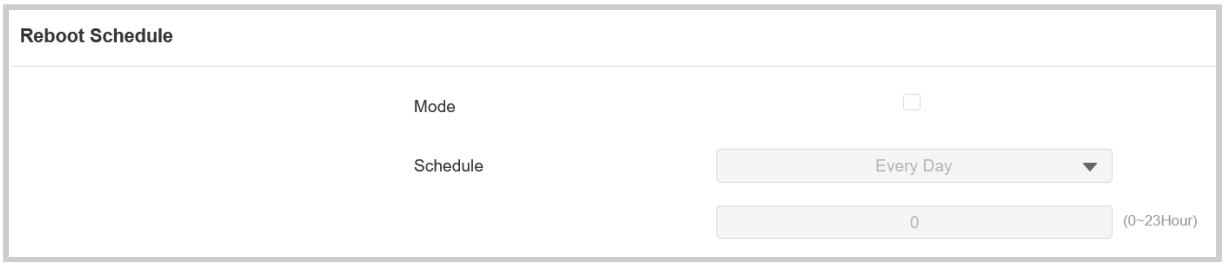
System Reboot and Reset

Reboot

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



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

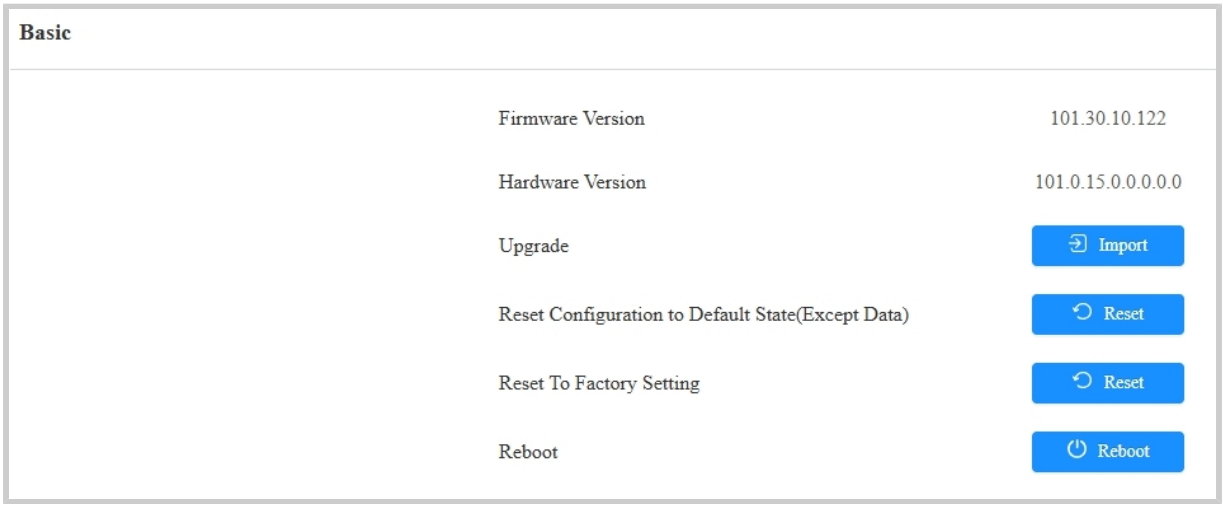


Reset

The device provides two reset options:

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

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



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

