

Table of Contents

Akuvox A01 Access Control Terminal Administrator Guide

About This Manual	3
Product Overview	4
Changelog	5
Model Specification	6
Supported Card Types	6
Introduction to Configuration Menu	7
Access the Device	8
Time and Language	9
Time	9
Language	9
LED Setting	10
LED Setting on Card Reader Area	10
Light Blink Control	10
Volume and Tone Configuration	11
Upload Open Door Tone	11
Network Setting	12
SNMP Setting	12
Device Web HTTP Setting	12
Relay Settings	13
Local Relay	13
Security Relay	13
Web Relay	14
Door Access Schedule Management	16
Door Access Schedule	16
Create Door Access Schedule	16
Import and Export Door Access Schedule	16
Relay Schedule	16
Holiday Schedule	17
Door-opening Configuration	18
User-specific Access Methods	18
Unlock by Private PIN Code	18
Unlock by RF Card	18
Unlock by License Plate	19
Access Setting	19
Import and Export User Data	20
NFC and Felica Card Setting	20
Mifare Card	20
Unlock by HTTP Command	21
Unlock by Exit Button	21
Security	23
Tamper Alarm	23
Security Notification	23
Email Notification	23
Action URL	23
Real-Time Monitoring	24
Emergency Action	25
Web Interface Automatic Log-out	25
High Security Mode	25
Anti-passback Mode	26
Lift Control	27
Logs	28
Access Log	28
Event Log	28
Debug	29
System Log for Debugging	29
Remote Debug Server	29
PCAP for Debugging	29
Ping	29
Backup	31
Firmware Upgrade	32
Auto-provisioning via Configuration File	33
Provisioning Principle	33
Introduction to the Configuration Files for Auto-Provisioning	33
Autop Schedule	33
Static Provisioning	34
DHCP Provisioning	35
Integration with Third-Party Device	37
Integration via Wiegand	37
Integration via HTTP API	37
Power Output Control	38
Password Modification	39
Modify Security Questions	39

System Reboot and Reset 40

Reboot 40

Reset 40

About This Manual



WWW.AKUVOX.COM



AKUVOX A01 ACCESS CONTROL

Administrator Guide

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 101.30.10.221, 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 101.30.10.221:

- Added the 6H3D5D-R option for [Wiegand Display Mode](#), [IC Card Display Mode](#), and [ID Card Display Mode](#).

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

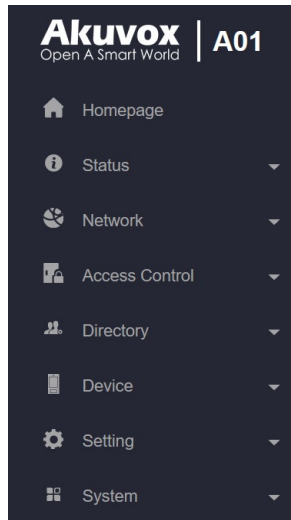
Supported Card Types

The device's firmware should be 101.30.10.127 or higher:

- ID Card:
 - EM4100
 - EM4200
- 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)

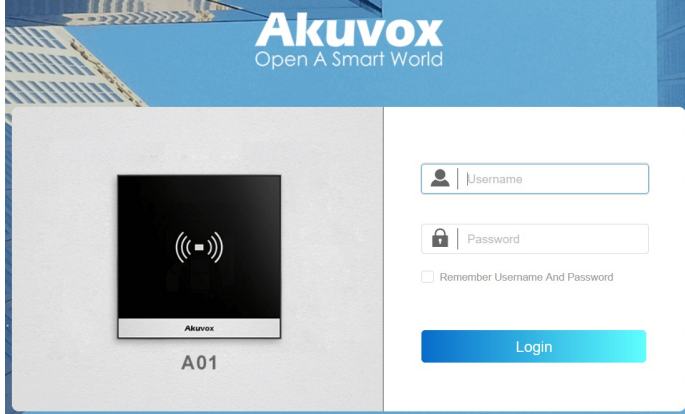
Introduction to Configuration Menu

- **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.



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**.

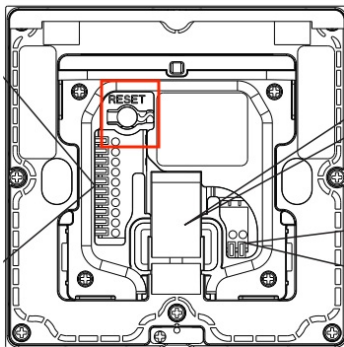


Note

- 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.



IP Announcement	
Loop Times	1 ▼

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.

NTP

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

03:48:15

- **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, Spanish, Dutch, French, German, and Korean.

English

↗

LogOut

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.

Light Of Swiping Card Area

Backlight Intensity

1

(1~5)

Backlight Enabled

☒

Start Time - End Time(Hour)

18

-

6

(0~23)

LED Always On When Relay Triggered

☐

- **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.

Light Blink

Disable Blinking

☒

Effective Schedule

1 item Unselected

☐ 1001:Always

0 item Selected

No Data

- **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 Configuration

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.

Volume Control	
Tamper Alarm Volume	<input type="text" value="8"/> (1~15)
Prompt Volume	<input type="text" value="8"/> (0~15)

- **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.

Open Door Tone Setting	
Open Door Tone Enabled	<input checked="" type="checkbox"/>
Open Door Succeed Tone Upload	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Open Door Failed Tone Upload	<input type="button" value="Import"/> <input type="button" value="Reset"/>

Note

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

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	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Preferred DNS Server	<input type="text"/>
Alternate DNS Server	<input type="text"/>

- **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 **Network > Advanced** interface.

SNMP	
Enabled	<input type="checkbox"/>
Port	<input type="text"/> (1024-65535)
Trusted IP	<input type="text"/>

- **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.

Web Server	
HTTP Redirect	<input checked="" type="checkbox"/>

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

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.

Relay	
Mode	Monostable ▼
Trigger Delay(Sec)	0 ▼
Hold Delay(Sec)	5 ▼
Action To Execute	<input type="checkbox"/> Email <input type="checkbox"/> HTTP
HTTP URL	
Type	Default State ▼
Relay Status	Low
Relay Name	Relay

- **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.

Security Relay

Relay ID	Security Relay A
Connect Type	Relay A Power Output
Trigger Delay(Sec)	0
Hold Delay(Sec)	5
Relay Name	Security Relay A
Enabled	<input type="checkbox"/>
 Test	

- **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.

Web Relay

Type	Disabled
IP Address	
Username	
Password	*****

Web Relay Action Setting

Action ID	Web Relay Action
1	
2	
3	
4	
5	

- **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.

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.

Relay Schedule

Relay ID

RelayA

Schedule Enabled

☒

Activation Required

☐

2 itemsUnselected

☐ 1001:Always
☐ 1002:Never

0 itemSelected

No Data

- **Relay ID:** Specify the relay you need to set up.
- **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.
- **Activation Required:** It means only after the relay is triggered successfully for the first time, can it be triggered by device-supported access methods later.
- **Allow List:** When Activation Required is enabled, you can define who can perform the activation.

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.

Holiday

ALL

+ Add

Import

Export

Index	Source	Holiday Name	Repeat By Year	Operation
No Data				

Selected:0/0

Delete

Delete All

Total:0

Prev

1/1

Next

Go To Page 1

Go

Calendar

Holiday Name

Repeat By Year

Year 2024

Working Hours

Clear

January	February	March	April	May	June
Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4	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 1 2 3	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	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	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	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 7
July	August	September	October	November	December

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.

Holiday

ALL

+ Add

Import

Export

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**.

The screenshot shows the 'User' management interface. At the top, there's a search bar with 'User ID/Name/Code' and a dropdown menu set to 'ALL'. There are buttons for 'Search', 'Reset', '+ Add', 'Import', and 'Export'. Below this is a table with columns: Index, Source, User ID, Name, PIN, RF Card, Floor No., Web Relay, Schedule-Relay, and Edit. Two users are listed: 'iris' (User ID 1) and 'Judy' (User ID 2). Below the table, there are buttons for 'Delete', 'Delete All', and 'Total:2'. At the bottom, there are pagination controls showing '1/1' and a 'Go' button.

Below the table is the 'User Info' form. It has three fields: 'User ID' with the value '2', 'Name' (empty), and 'Role' with a dropdown menu set to 'General User'.

- **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.

The screenshot shows the 'PIN' section of the user configuration interface. It has a label 'PIN' and a text input field for '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

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

The screenshot shows the 'RF Card' section of the user configuration interface. It has a label 'RF Card' and a text input field for 'Code'. There are two buttons: '+ Obtain' and 'Add'.

- **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.

Card Type Support	
IC Card Enabled	<input checked="" type="checkbox"/>
ID Card Enabled	<input checked="" type="checkbox"/>

RF Card Code Format

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

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

RFID	
IC Card Display Mode	8HN
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.

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	<input type="text"/>
	<input type="button" value="Duration"/>
<input type="button" value="Add"/>	

- **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.

Access Setting	
Relay	<input checked="" type="checkbox"/> RelayA
Security Relay	<input type="checkbox"/> Security Relay A
Floor No.	<input type="text" value="None"/>
Web Relay	<input type="text" value="0"/>
HTTP URL	<input type="text"/>
	<input type="button" value="Add"/>
Schedule	<div> <div>1 item Unselected</div> <div> <input type="checkbox"/> 1002:Never </div> </div> <div> <input type="button" value="➤"/> <input type="button" value="➤"/> </div> <div> <div>1 item Selected</div> <div> <input type="checkbox"/> 1001:Always </div> </div>

- **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 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:

Door phone's IP **Preset credentials for authentication**
 http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=1234568DoorNum=1
ID of Relay to be triggered

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.

The screenshot shows the 'User' management interface. At the top, there are search and filter options. Below that, there are buttons for '+ Add', 'Import', and 'Export'. The 'Import' button is highlighted with a red box. Below the buttons is a table with columns: Index, Source, User ID, Name, PIN, RF Card, Floor No., Web Relay, Schedule-Relay, and Edit. The table is currently empty, showing 'No Data'. At the bottom, there are pagination controls and a 'Go' button.

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.

The screenshot shows the 'Contactless Smart Card' settings interface. There is a toggle switch labeled 'Enabled' which is currently turned on. To the right of the toggle is a dropdown menu with 'Disabled' selected.

- **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 > Contactless Smart Card** interface.

The screenshot shows the 'Contactless Smart Card' settings interface. There is a toggle switch labeled 'Enabled' which is currently turned on. To the right of the toggle is a dropdown menu with 'Mifare' selected. Below this, there are two input fields for 'Sector/Block' and 'Block Key'. The 'Sector/Block' field has a '/' separator. The 'Block Key' field has a masked input with dots.

- **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.
- **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	<input checked="" type="checkbox"/>
Username	<input type="text"/>
Password	<input type="password"/>

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

Tip:

Here is an HTTP command URL example for relay triggering.

Device's IP **Preset credentials for authentication**
 http://192.168.35.127/cgi/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	<input checked="" type="checkbox"/>
Trigger Electrical Level	Low ▼
Action To Execute	<input type="checkbox"/> Email <input type="checkbox"/> HTTP
HTTP URL	<input type="text"/>
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution ▼
Execute Relay	None ▼
Alarm Door Opened	<input type="checkbox"/>
Break-in Intrusion	<input type="checkbox"/>
Door Status	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.
- **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.

Tamper Alarm

Enabled ☐

Gravity Sensor Threshold (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

Email Notification

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

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

Email Notification

Sender's Email Address

Sender's Email Name

Receiver's Email Address

Receiver's Email Name

SMTP Server Address

Port

SMTP User Name

SMTP Password

Email Subject

Email Content

Email Test

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 Card Entered	\$card_sn	Http://server ip/validcard=\$card_sn
6	Invalid Card Entered	\$card_sn	Http://server ip/invalidcard=\$card_sn
7	Tamper Alarm Triggered	\$alarm status	Http://server ip/tampertrigger=\$alarm status
8	Alarm Door Opened Timeout	\$relay_id \$location	http://server ip/fcgi/do? action=NotifyAlarm&AlarmMsg=xxx&FromName=xxx&AlarmCode=1&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.

Action URL

Enabled ☐

Username

Password

Relay Triggered

Relay Closed

InputA Triggered

InputB Triggered

InputA Closed

InputB Closed

Valid Card Entered

Invalid Card Entered

Tamper Alarm Triggered

Alarm Door Opened Timeout A

Alarm Door Opened Timeout B

- **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.

Real-Time Monitoring
<div>Apply Setting To</div> <div>None ▼</div>

- **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.

Emergency Action
<div>Apply Setting To</div> <div> <input type="checkbox"/> Input A <input type="checkbox"/> Input B </div>

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
<div>Session Time Out Value</div> <div> <input type="text" value="9000"/> (60~14400Sec) </div>

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.

High Security Mode
<div>Enabled</div> <div><input type="checkbox"/></div>

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.

Anti-passback Mode	
Mode	<div>None ▼</div>

- **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.

Akuvox Advance Setting	
Lift Mode	Choose Floor ▼
Server1 IP	<input type="text"/>
Port	<input type="text"/> (1-65535)
Akuvox Action	
User Name	<input type="text"/>
Password	<input type="password"/>
Floor No. Parameter	<input type="text"/> \$floor
URL To Trigger Specific Floor	<input type="text"/> /cgi/do?action=OpenDoor&UserName=admin&Passw
URL To Trigger All Floors	<input type="text"/> /cgi/do?action=OpenAll&UserName=admin&Passwor
URL To Close All Floors	<input type="text"/> /cgi/do?action=CloseAll&UserName=admin&Passwor
Floor Starts From	1 ▼
Ground Floor	None ▼
Device Location	None ▼

- **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 ☒

Remote Door Log Enabled ☒

Remote Server

Authorization Mode

All

Select date

Select date

Name/Code

Search

Export

	Index	User ID	Name	Code	Door ID	Type	Date	Time	Mode	Status
<input type="checkbox"/>	1	2	Judy	FFB59828	A	Card	2024-05-11	03:52:19	Normal	Success
<input type="checkbox"/>	2	2	Judy	FFB59828	A	Card	2024-05-11	03:51:31	Normal	Success
<input type="checkbox"/>	3	2	Judy	FFB59828	A	Card	2024-05-11	03:41:45	Normal	Success
<input type="checkbox"/>	4	-	Visitor	FFB59828		Card	2024-05-11	03:41:26	Normal	Failed

- **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.

Type

All

Time

Start Time

End Time

Search

Export

Time	Event Type	Status
2025-01-22 01:45:31	Login	Account admin; Success; IP 192.168.35.8
1970-01-01 00:05:26	IP Change	IP Obtained : 192.168.35.178
1970-01-01 00:00:17	Device State	Startup
2025-01-21 09:28:23	Config Change	Configuration Changed; Operator = admin
2025-01-21 09:28:15	Login	Account admin; Success; IP 192.168.35.8
2025-01-21 08:44:57	Login	Account admin; Success; IP 192.168.35.203
2025-01-21 08:18:42	Password Change	Account admin; Password Changed; Operator = admin
2025-01-21 08:18:42	Config Change	Configuration Changed; Operator = admin
2025-01-21 08:18:36	Login	Account admin; Success; IP 192.168.35.8
2025-01-21 08:18:32	Login Attempt	Account admin; Failed; IP 192.168.35.8

ALL DATA HAS BEEN LOADED

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.

Ping

Cloud Server

Verify the network address accessibility



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

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

Backup

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





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

Others	
Config File	 Import  Export (Encrypted)

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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

Basic	
Firmware Version	101.30.10.122
Hardware Version	101.0.15.0.0.0.0.0
Upgrade	 Import
Reset Configuration to Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

Note

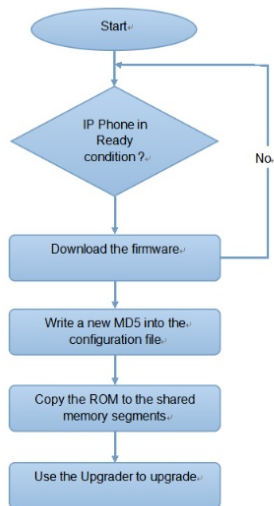
The file should be in .rom format.

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.

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

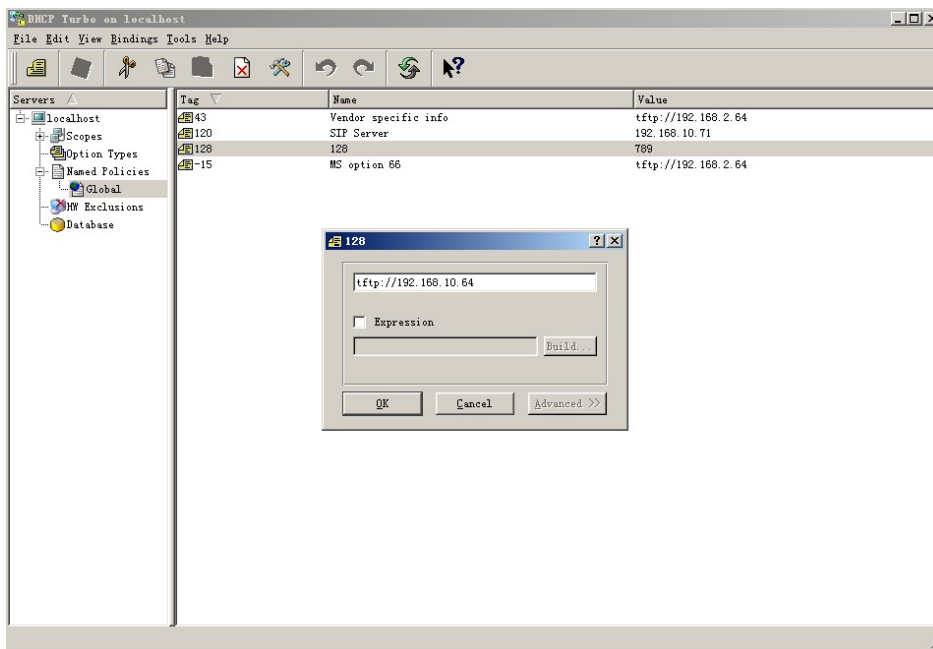
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/(use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

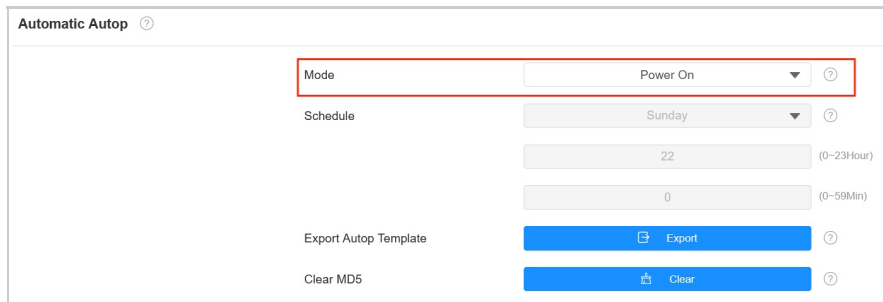
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255, you are required to configure DHCP Custom Option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



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.

DHCP Option	
Custom Option	<input type="text"/> (128~254)
(DHCP option 66/43 is enabled by default.)	

- **Custom Option:** Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 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	
Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	Wiegand-26 ▼
Wiegand Transfer Mode	Input ▼
Wiegand Input Clear Time	5 ▼
Wiegand Input Data Order	Normal ▼
Wiegand Output Data Order	Normal ▼
Wiegand Output CRC Enable	<input checked="" type="checkbox"/>

- **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. It is automatically configured.
- **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.

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, 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	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.
3	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.
4	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".
5	Token	This mode is used by Akuvox developers only.

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

Relay ID

RelayA

12v Power Output Enabled

Disabled

- **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.

Web Password Modify

Username: admin

Change Password

Modify Security Question

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

Web Password Modify

Username: admin

Change Password

Account Status

High Security Mode

Change Password

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

Username: admin

Old Password

New Password

Confirm Password

Cancel Change

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

Account Status

Username	Status
admin	Enabled
user	<input type="checkbox"/>

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

Change Password

Modify Security Question

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

Web Password Modify

Username: admin

Change Password

Account Status

High Security Mode

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.

Basic	
Firmware Version	101.30.10.122
Hardware Version	101.0.15.0.0.0.0.0
Upgrade	<button>Import</button>
Reset Configuration to Default State(Except Data)	<button>Reset</button>
Reset To Factory Setting	<button>Reset</button>
Reboot	<button>Reboot</button>

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

Reboot Schedule	
Mode	<input type="checkbox"/>
Schedule	<div>Every Day</div> <div>0 (0-23Hour)</div>

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	101.30.10.122
Hardware Version	101.0.15.0.0.0.0.0
Upgrade	<button>Import</button>
Reset Configuration to Default State(Except Data)	<button>Reset</button>
Reset To Factory Setting	<button>Reset</button>
Reboot	<button>Reboot</button>

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

