

About This Manual



WWW.AKUVOX.COM



A05 ACCESS CONTROL TERMINAL

Administrator Guide

Thank you for choosing the Akuvox A05 series access control terminal. This manual is intended for administrators who need to properly configure the access control terminal. This manual applies to the 205.30.10.142 version, and it provides all the configurations for the functions and features of A05 series access control terminals. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox A05 series is a Linux-based access control door phone with a display screen. It incorporates access control and video surveillance. Its finely tuned SmartPlus and AI-based communication technology allow featured customization to better suit customers' operation habits. A05 series has multiple ports, such as RS485 and Wiegand ports, which can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, helping to create a holistic control of the building entrance and its surroundings and giving users a great sense of security via a variety of access such as card access, NFC, QR code and newly added door access in an accompaniment with body temperature measurement. A05 series access control terminal applies to residential buildings, office buildings, and their complex.

Changelog

What's new in version 205.30.10.142:

- Support a new web language: Korean.

Click [here](#) to view the changelog of the device's previous versions.

Model Specification

Model	A05
Display	5" IPS
Touch Screen	X
Button	X
Housing Material	Plastic
Relay Out	1
Alarm In	1
RS485	√
PoE	√
Resolution	1280x720
Brightness	500cd/m2
RAM	1GB
ROM	8GB
Card Reader	13.56MHz
Wi-Fi	X
Bluetooth	Optional
IP Rating	IP65
Temperature Detection	Optional
Face Recognition	√
LTE	X
USB	X
External SD Card	X
POE Stand by Power	5.5W
POE Full Load Consumption	9.8W
Power Adapter Standby Power	5.5W
Power Adapter Full Load Consumption	10W

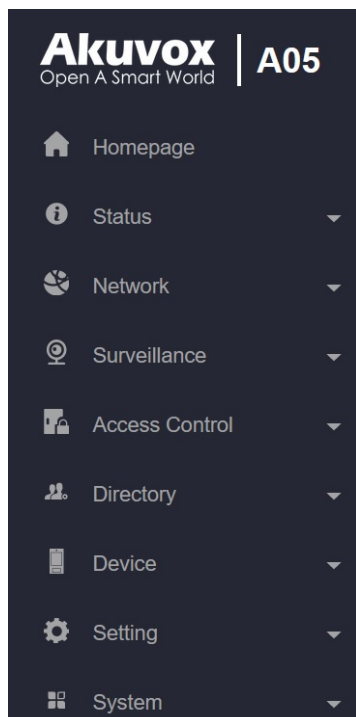
Supported Card Types

The device's firmware should be 205.30.10.138 or higher:

- IC Card:
 - Mifare Ultralight C/EV1
 - Mifare Classic Compatible Card
 - Mifare Plus-S 2K
 - Mifare Desfire EV1 2K D21
 - Mifare Desfire EV2 D42
 - Mifare Desfire EV2 D22
 - Mifare Desfire Compatible Card (CPU Card, 4-byte): Incompatible with SmartPlus NFC service.
 - NFC Type2 216
 - NFC Type2 215
- Felica Card
- SmartPlus APP NFC
- Mifare Classic S50 4-byte Encryption-Compatible Card
- Mifare Plus-S SL3 Encrypted Card
- Mifare Plus-SE SL3 Encrypted Card
- Mifare Desfire EV1 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV2 Encrypted Card(AES file encryption mode)
- Mifare Desfire EV3 Encrypted Card(AES file encryption mode)
- Akuvox Cards:
 - Mifare Classic 1K
 - Mifare S50-1K Card
 - Mifare Desfire EV3 Encrypted Card(AES file encryption mode)

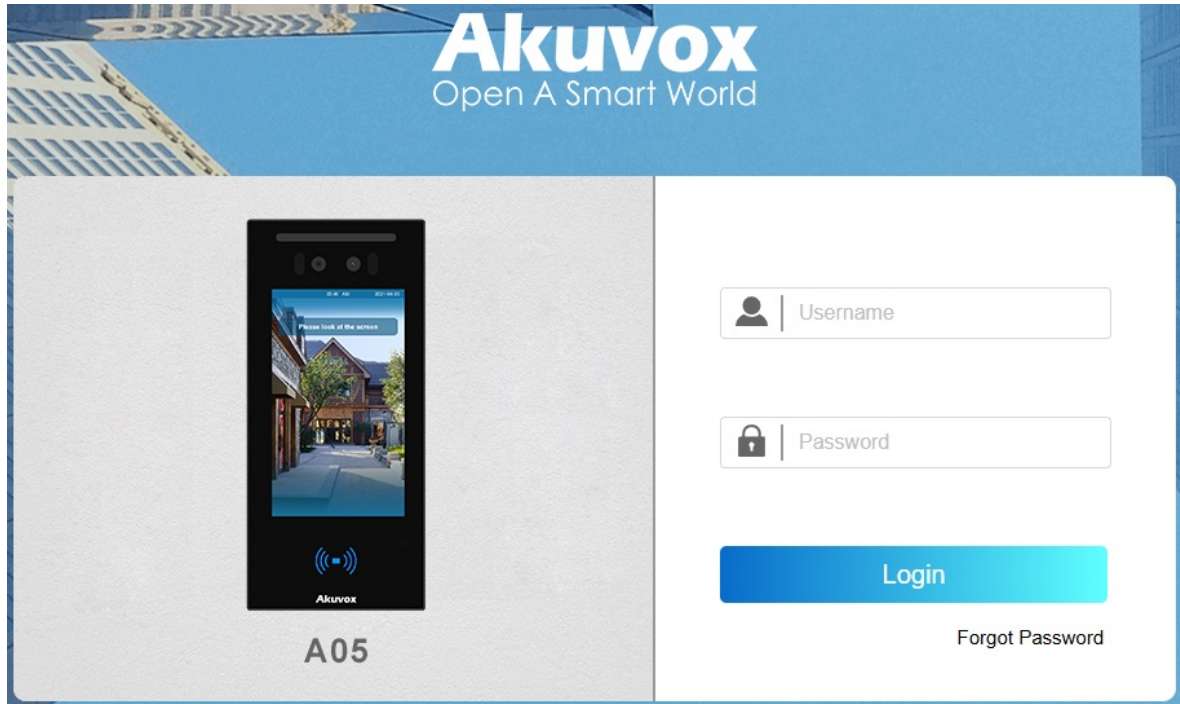
Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, and log-related configurations such as access logs.
- **Network:** This section mainly deals with DHCP and static IP settings, device network deployment, etc.
- **Surveillance:** This section includes audio and video-related settings such as Live stream, RTSP, ONVIF, and MJPEG.
- **Access Control:** This section includes input settings, relay settings, and door access control in terms of facial recognition, RF card, Bluetooth settings, and body temperature settings.
- **Directory:** This section includes access schedule management and user management.
- **Device:** This section includes light, Wiegand, lift control, LCD, audio, and so on.
- **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, remote debug server, PCAP, password modification as well as device backup.



Access the Device

Before configuring Akuvox A05, please make sure the device is installed correctly and connected to a normal network. Using the Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to log 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 username and password entered.

Language and Time

Language

You can select the device LCD language on the **Setting> Time/Lang > LCD Language** interface.

The following languages are supported:

- English, Simplified Chinese, Russian, Korean, Dutch, French, German, Hebrew, Norwegian, Ukrainian, Turkish, Arabic, Spanish, Japanese, and Traditional Chinese.

LCD Language	
Mode	English ▼

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

The following languages are supported: English, Simplified Chinese, Spanish, Japanese, and Korean.

English ▼	LogOut
-----------	--------

Time

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

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

NTP	
Automatic Date&Time Enabled	<input checked="" type="checkbox"/>
Time Zone	GMT+8:00 Casey ▼
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600Sec)
Current Time	16:00:40

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

LED Setting

Card Reader Area LED Control

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 Enabled	<input checked="" type="checkbox"/>	
Start Time - End Time(Hour)	<input type="text" value="18"/>	- <input type="text" value="23"/> (0~23)

- **Backlight Enabled:** Turn on/off the LED on the card reader area.
- **Start Time - End Time(Hour):** Enter 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 during one day (24 hours).

LED White Light Setting

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

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

White Light	
Mode	<input type="text" value="Auto"/>
Max White Light Value	<input type="text" value="3"/>

- **Mode:**
 - **Auto:** The white light will be turned on automatically for facial recognition and QR code scanning for door opening.
 - **Off:** The white light is disabled.
- **Max White Light Value:** Set the white light value from 1-5, and the default white light value is 3. The greater value it is, the brighter the light will be.

Screen Display Configuration

Configure Screensaver

You can conduct the await screen configuration on the web interface where you can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction.

To set it up, go to **Device > LCD > Standby Interface Display** interface.

Standby Interface Display

Screensaver Mode	<input checked="" type="checkbox"/>
Screensaver Time	5seconds ▼
Sleep	10seconds ▼
Wake Up Detection Accuracy	<input type="text"/> (1~6)

- **Screensaver Mode:** Turn on or off the screensaver.
- **Screensaver Time (Sec):** Set the screen saver duration time from 5 seconds up to 2 hours. The device will enter the screensaver mode when no one approaches or operates for the Sleep time.
- **Sleep:** Set the time for the device screen to turn off or go into the screensaver mode when no one approaches or operates on the device.
- **Wake Up Detection Accuracy:** Set the accuracy to wake up the screen. The higher value is, the greater sensitivity.

Upload Screensaver

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

To set it up, go to **Device > LCD > Upload Screensaver** interface. Click **Import** to upload the file and click **Delete** to remove the existing one.

Screensaver ID	File Status	Interval(Sec)	Delete
1	File Exists	5	Delete
2	File Exists	5	Delete
3	File Exists	5	Delete
4	File Exists	5	Delete
5	File Exists	5	Delete

Note

- The pictures uploaded should be in **JPG** or **PNG** format with 2M pixels maximum.
- Recommended resolution: 600×1024.
- If the uploaded image duplicates an existing image ID, the existing image will be overwritten.

Screen Display Mode

You can select the Default or QR Code display mode for facial recognition and QR code scanning respectively.

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

Theme	
Mode	Default ▼
QR Code Recognition Interval(Sec)	4 ▼

- **QR Code Recognition Interval(Sec):** Set the recognition interval between QR code scanning when the QR Code mode is selected.

Screen Display Style

You can enable or disable the gradient mask on the device screen for desired screen display style.

Set it up on the **Device > LCD > UI** interface.

UI

Gradient Mask

☐

Door Access Prompt Text

You can enable the open door text prompt for both door-opening success and failure.

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

Door Setting General

Open Door Succeeded Text Prompt

☒

Open Door Failed Text Prompt

☒

Display User Info

☒

- **Open Door Succeeded Text Prompt:** Display a text prompt after the door is opened.
- **Open Door Failed Text Prompt:** Display a text prompt after opening the door fails.
- **Display User Info:** Display the user information after facial recognition. If facial recognition succeeds, the text prompt "Access Granted" with the user ID and name will pop up on the device screen. If it fails, the text prompt "Access Denied" with "Stranger, Name: Unknown" will be displayed.

Volume & Tone Configuration

Volume and tone configuration includes tamper alarm and prompt volume settings. Moreover, you can upload the door-opening ringtones.

Volume Configuration

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 Volume:** 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 set it up, go to **Device > Audio** interface. Click **Import** to upload the file and click **Reset** to remove 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, sample rate: 16000, Bits: 16.

Ringback Tone Setting

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

Set it up on the **Device > Audio > Ringback Tone Setting** interface.

Ringback Tone Setting

Ringback Source	<input type="text" value="Remote,Local As Backup"/>
-----------------	---

- **Ringback Source:**
 - **Remote, Local As Backup:** The local ringtone will be played.

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

Network Setting

Device Network Connection

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 > LAN Port** interface.

LAN Port

Type

☐ DHCP
 ☒ Static IP

IP Address

Subnet Mask

Default Gateway

Preferred DNS Server

Alternate DNS Server

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

Device Deployment in Network

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

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

Connect Setting

Server Mode

None

Discovery Mode

☒

Device Address

Device Extension

Device Location

- **Server Mode:** It is automatically set up according to the actual device connection with a specific server in the network such as SDMC, Cloud, or None. None is the default factory setting indicating the device is not in any server type.

- **Discovery Mode:** When enabled, the device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address:** Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension:** The device extension number.
- **Device Location:** The location in which the device is installed and used.

Relay Setting

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

Local Relay

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

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

Relay

Type	Default State ▼
Mode	Monostable ▼
Trigger Delay(Sec)	0 ▼
Hold Delay(Sec)	5 ▼
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> TFTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP
HTTP URL	
Relay Status	Low
Relay Name	Relay
Access Method	<input checked="" type="checkbox"/> Face <input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC

- **Type:** Determine the interpretation of the Relay Status regarding the state of the door:
 - **Default State:** A "Low" status in the Relay Status field indicates that the door is closed, while "High" indicates that it is opened.
 - **Invert State:** A "Low" status in the Relay Status field indicates an opened door, while "High" indicates a closed one.
- **Mode:** Specify the conditions for automatically resetting the relay status.
 - **Monostable:** The relay status resets automatically within the relay delay time after activation.
 - **Bistable:** The relay status resets upon triggering the relay again.
- **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.
 - **FTP:** Send a screenshot to the preconfigured [FTP server](#).
 - **TFTP:** Send a screenshot to the preconfigured [TFTP server](#).
 - **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](#).
- **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.
- **Access Method:** Check the method(s) to trigger the relay.

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

Connect Type	RS485
Trigger Delay(Sec)	0
Hold Delay(Sec)	5
Access Method	<input checked="" type="checkbox"/> Face <input checked="" type="checkbox"/> RF Card <input checked="" type="checkbox"/> BLE <input checked="" type="checkbox"/> NFC
Relay Name	Security Relay A
Enabled	<input type="checkbox"/>
<button>Test</button>	

- **Connect Type:** The security relay connects to the device using RS485 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.
- **Access Method:** Check the method(s) to trigger the relay.
- **Relay Name:** Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.
- **Enabled:** When using the SR01 via RS485, you need to set the RS485 mode to **Others** on the **Device > RS485** interface.

Web Relay

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



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

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

Web Relay

Type

Disabled ▼

IP Address

Username

Password

.....

Web Relay Action Setting

Action ID	Web Relay Action
1	
2	
3	
4	
5	
6	

- **Type:** Determine the type of relay activated when employing door access methods for entry.
 - **Disabled:** Only activate the local relay.
 - **Web Relay:** Only activate the web relay.
 - **Local Relay+Web Relay:** Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **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.

Schedule									
ALL									
	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
<input type="checkbox"/>	1	1001	Local	Daily	Always			00:00-23:59	
<input type="checkbox"/>	2	1002	Local	Daily	Never			00:00-00:00	

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

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

Add Schedule

Name:

Mode:

Date Range: -

Day Of Week: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☐ Sunday ☐ Check All

Date Time: -

Cancel Submit

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

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.

Schedule

ALL

+ Add

Import

Export

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

☒

2 items Unselected

☐ 1001:Always
☐ 1002:Never

0 item Selected

No Data

- **Relay ID:** Specify the relay you need to set up.
- **Schedule Enabled:** Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

For instructions on creating schedules, kindly consult the [Create Door Access Schedule](#) section.

Holiday Schedule

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

Set it up on the **Setting > Holiday** interface. Click +Add.

Holiday

All

+ Add

Import

Export

	Index	Source	Holiday Name	Repeat By Year	Operation
<div>No Data</div>					

Selected: 0/0

Delete

Delete All

Total: 0

Prev

1/1

Next

Go To Page

1

Go

Calendar

Holiday Name

Repeat By Year

☐

Year

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
Mo Tu We Th Fr Sa Su 1 2 3 4 5 6 7	Mo Tu We Th Fr Sa Su 1 2 3 4	Mo Tu We Th Fr Sa Su 1	Mo Tu We Th Fr Sa Su 1 2 3 4 5 6	Mo Tu We Th Fr Sa Su 1 2 3	Mo Tu We Th Fr Sa Su 1

Cancel

Submit

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

Door-opening Configuration

User-specific Access Methods

The private RF card and face setting should be assigned to a particular user for door opening.

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

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

User

ALL

ALL

Search

Reset

+ Add

Import

Export

	Index	Source	User ID	Name	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/>	1	Local	1	iris			None	0	1001-1	

Selected:0/1

Delete

Delete All

Total:1

Prev

1/1

Next

Go To Page 1

Go

User Info

User ID

2

Name

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

Unlock by Private PIN Code

When the device is connected to a Wiegand keypad, it can receive Wiegand data. Users can enter the PIN code on the keypad to open doors.

On the **Directory > User > +Add** interface, scroll to the **PIN(For Wiegand Use)** section.

PIN(For Wiegand Use)

Code

Unlock by RF Card/Bkey

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

RF Card & Bkey

Code

+ Obtain

Add

If you want to add Bkey, please make sure the BLE function is set to Enable.

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

Note:

- Click [here](#) to view the detailed steps of configuring Bkey.
- Each user can have a maximum of 5 cards added.
- The device allows to add 20,000 users.
- RF cards operating at 13.56 MHz frequencies are compatible with the device for access.
- A05 only supports IC cards.

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

- **IC Card Display Mode:** Set the card number format from the provided options. The default format in the device is 8HN.

Bkey Trigger Signal

The Bkey trigger signal determines the distance within which users can press the Bkey to open the door.

Set it up on the **Access Control > BLE** interface.

BLE	
Enabled	<input checked="" type="checkbox"/>
RSSI Threshold	72 (-85---50db)
Open Door Interval(Sec)	5
BKey Trigger Signal	

- **Bkey Trigger Signal:** Three ranges are available, setting door opening distance to about 5 meters, 3 meters, and 1 meter.

Unlock by Facial Recognition

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

Face	
Status	UnRegistered
Photo	<input type="button" value="Import"/> <input type="button" value="Reset"/>

Note

Support Format: jpg, png, bmp, and jpeg.

Face Settings

You can adjust facial recognition accuracy, recognition intervals, and more to enhance user experience.

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

Face Basic

Facial Recognition Enabled	<input checked="" type="checkbox"/>
Offline Learning Enabled	<input type="checkbox"/>
Facial Recognition Matching Level	Normal ▼
Face Living Recognition Matching Level	Normal ▼
Facial Recognition Interval (sec)	5 ▼
No Face Detected Interval (sec)	1 ▼
Face Detection Distance (M)	3 ▼

- **Facial Recognition Enabled:** Enable/disable the facial recognition function.
- **Offline Learning Enabled:** Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level:** Determine how strict the facial recognition system is in comparing a person's face with uploaded face data. Each level allows a different degree of difference or face covering (**excluding the mouth area**) to pass the recognition.

- Low: Allow slight differences from the uploaded face data, with little face coverage.

- Highest: Require the face to be identical to the uploaded one, with minimal or no covering.

- The other two levels are in between.

- **Face Living Recognition Matching Level:** Set how strict the system is in preventing fake faces.

- Close: Disable the facial anti-spoofing function. Facial verification can be passed using non-living substitutes for an authorized person's face, such as a photo.

- Highest: The system cannot be fooled by any non-living substitutes for an authorized person's face.

- The other three levels are in between.

- **Facial Recognition Interval(sec):** Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.
- **No Face Detected Interval(sec):** Adjust the time interval between each facial recognition attempt after temperature measurement.
- **Face Detection Distance(M):** Decide the effective facial recognition distance.

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"/> Relay A
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 <input type="checkbox"/> 1002:Never </div> <div> 1 Item Selected <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:** Check Security Relay A if you've configured it on the [Security Relay](#) interface.
- **Floor No.:** Specify the accessible floor(s) to the user via [the elevator](#).
- **Web Relay:** Specify the ID of web relay action commands that you've configured on the [Web Relay](#) interface. A default value of 0 indicates that the web relay will not be triggered.
- **HTTP URL:** Specify the HTTP URL sent to another Akuvox device for door opening.
- **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
http://192.168.35.127/cgi/do?action=OpenDoor&
Preset credentials for authentication
UserName=admin&Password=123456&
ID of Relay to be triggered
DoorNum=1

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.

Access Authentication Mode

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

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

Access Authentication Mode

Authentication Mode	<input type="text" value="Any Method"/>
Entry Restriction	<input type="checkbox"/>

- **Authentication Mode:** Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.
 - **Any Method:** Allow all access methods.
 - **Face + RF Card:** Go through facial recognition first, then swipe the RF card.
- **Entry Restriction:** Set the time interval between each door opening for the same user. For example, if it is set to 30 minutes, the user needs to wait for 30 minutes to open the door again.

Import/Export User Data

The door phone supports User Data of access control to be shared among Akuvox door phones through import and export while you can also export the facial data out of the door phone and then import it to a third-party device.

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

To set it up, go to the **Directory > User** interface.

The import file should be in TGZ or CSV format. The export file is in XML or CSV format.

User

Contactless Smart Card

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

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

Contactless Smart Card

Enabled

Disabled ▼

- **Felica Reading Format:** When Felica is selected, set the card reading format between 8 Bytes and 16 Bytes. The default is 16 Bytes.

Mifare Card

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

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

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

Mifare Card Encryption

Enabled

None ▼

- **Mifare:**
 - **Sector/Block:** Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
 - **Block Key:** Set a password to access the data stored in the predefined sector/block.
- **Mifare DESFire:**
 - **App ID:** A 6-digit hexadecimal number
 - **File ID:** The ID of the encrypted file of the app, which can be a number from 0 to 31.
 - **Crypto:** The encryption method, either AES or DES.

- **Key:** The file key.
- **Key Index:** The index number for the key, which can be a number from 0 to 11.
- **Plus:** You can set up three choices. This means you can use three types of Mifare Plus cards. When swiping a card, as long as one of the choices matches its SL key, the card code in the block you specified will be output.
 - **Block:** Specify the block(s) to be read.
 - **SL3:** The key number within 32 bits.

Unlock By Bluetooth

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

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

BLE	
Enabled	<input type="checkbox"/>
RSSI Threshold	<input type="text" value="72"/> (-85~-50db)
Open Door Interval(Sec)	<input type="text" value="5"/> ▼

- **RSSI Threshold:** Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Open Door Interval (Sec):** Set the time interval between consecutive Bluetooth door access attempts.

Note

Click [here](#) to view how to open doors with Bluetooth-featured SmartPlus App.

Unlock by QR Code

You can use a QR code to open the door. This method requires the Akuvox SmartPlus cloud service. You have to activate this feature before using it.

Enable the feature on the **Access Control > Relay > Open Relay via QR Code** interface.

Open Relay Via QR Code	
Enabled	<input checked="" type="checkbox"/>

Note

The function should work with the Akuvox SmartPlus cloud. Please click [here](#) to view the configuration details.

Unlock by HTTP Command

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

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

Open Relay Via HTTP

Enabled

☐

Username

Password

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

Tip:

Here is an HTTP command URL example for relay triggering.

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

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

Enabled

☒

Trigger Electrical Level

Low

Action To Execute

☐ FTP
 ☐ TFTP
 ☐ Email
 ☐ HTTP

HTTP URL

Action Delay

0

(0~300Sec)

Action Delay Mode

Unconditional Execution

Execute Relay

None

Door Status

High

- **Trigger Electrical Level:** Set the input interface to trigger at low or high electrical level.
- **Action To Execute:** Set the desired actions that occur when the specific Input interface is triggered.
 - **FTP:** Send a screenshot to the preconfigured [FTP server](#).
 - **TFTP:** Send a screenshot to the preconfigured [TFTP server](#).
 - **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.
- **Door Status:** Display the status of the input signal.

Body Temperature Measurement for Door Access (Optional)

A05 series provides you with an optional body temperature measurement function designed to be applied in the situation where the measurement becomes necessary for the safety of the residents and visitors, etc. Residents and visitors are required to go through temperature measurements along with an optional mask detection check before they are allowed door access.

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

Measuring Body Temperature

Mode

Disabled

Mask Detection

Disabled

Temperature Unit

Centigrade

Normal Body Temperature

37.3

(Below 37.3°C)

Low Temperature

34

(Below 34°C)

(If the detected temperature is lower than 34 °C, the device will prompt low temperature, please try again later)

Action For Abnormal Body Temperature

Access Denied

Action For Low Body Temperature

Try Again Later

- **Mode:** The device can be installed with a digital forehead temperature detector.
 - **Disabled:** Turn off the function.
 - **Forehead:** Test the body temperature from the forehead.
 - **Wrist:** Test the body temperature from the wrist.
- **Mask Detection:**
 - **Disabled:** The device will not detect whether the user is wearing a mask.
 - **Set mask-wearing as mandatory:** Users are required to wear a mask for temperature measurement. The device will first detect whether the user is wearing a mask. If not, it will not proceed to the next step.
 - **Display mask-wearing prompt:** Wearing a mask is not mandatory. The device will first detect whether the user is wearing a mask. If not, the prompt "Please wear a mask" will pop up and the device will proceed to the next step.
- **Temperature Unit:** Select the temperature unit.
- **Normal Body Temperature:** Set the body temperature as the measuring basis in either Fahrenheit or Celsius. For example, if you set the temperature 37.3 degrees Celsius as the normal temperature, then any body temperature measured higher than 37.3 degrees Celsius will be deemed as an abnormal temperature.
- **Low Temperature:** Set the body temperature as the measuring basis in either Fahrenheit or Celsius. For example, if you set the temperature 34 degrees Celsius as the threshold, then any body temperature measured lower than 34 degrees Celsius will be deemed as low body temperature.
- **Action for Abnormal Body Temperature:**
 - **Access Denied:** When users are detected abnormal temperatures, the door will not be opened.

- **Just For Reminder:** A prompt reminding abnormal temperature will pop up. The door will be opened.
- **Action for Low Body Temperature:**
 - **Try Again Later:** Users will be prompted to measure their temperatures again when they detect low temperatures. The door will not be opened.
 - **Just For Reminder:** A prompt reminding low temperature will pop up. The door will be opened.

Monitor and Image

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

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

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

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

RTSP Stream Monitoring

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

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

RTSP Basic Settings

To set it up, go to **Surveillance > RTSP** interface.

RTSP Basic

Enabled

☒

Authorization Enabled

☐

Authorization Mode

Digest

Username

admin

Password

•••••

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

RTSP Stream Setting

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

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

H.264 Video Parameters

Video Resolution	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">720P ▼</div>	
Video Framerate	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">25 fps ▼</div>	
Video Bitrate	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">2048 kbps ▼</div>	
2nd Video Resolution	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">VGA ▼</div>	
2nd Video Framerate	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">25 fps ▼</div>	
2nd Video Bitrate	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">512 kbps ▼</div>	
Video Crop	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">Default ▼</div>	<div style="border: 1px solid #007bff; color: white; padding: 2px 5px; display: inline-block;">✎ Edit</div>

- Video Resolution:** Specify the image resolution, varying from the lowest QCIF(176x144 pixels) to the highest 1080P(1920x1080 pixels).
- Video Framerate:** Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 25fps.
- Video Bitrate:** The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth.
- 2nd Video Resolution:** Specify the image resolution for the second video stream channel.
- 2nd Video Framerate:** Set the frame rate for the second video stream channel.
- 2nd Video Bitrate:** Set the bit rate for the second video stream channel. The default is 512 kbps.
- Video Crop:**
 - Original:** Display the full-screen video.
 - Default:** Select the specific area of the video to be displayed. Click Edit to crop the video.

Tip

To view the audio and video stream using RTSP:

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

MJPEG Image Capturing

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

To set it up, go to **Surveillance > MJPEG** interface.

MJPEG Server

Enabled	<input checked="" type="checkbox"/>	
Image Quality	<div style="border: 1px solid #ccc; padding: 2px; text-align: center;">VGA ▼</div>	

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

Tip

- To view a dynamic stream, use the URL `http://device_IP:8080/video.cgi`.
- For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
 - `http://device_IP:8080/picture.cgi`
 - `http://device_IP:8080/picture.jpg`
 - `http://device_IP:8080/jpeg.cgi`

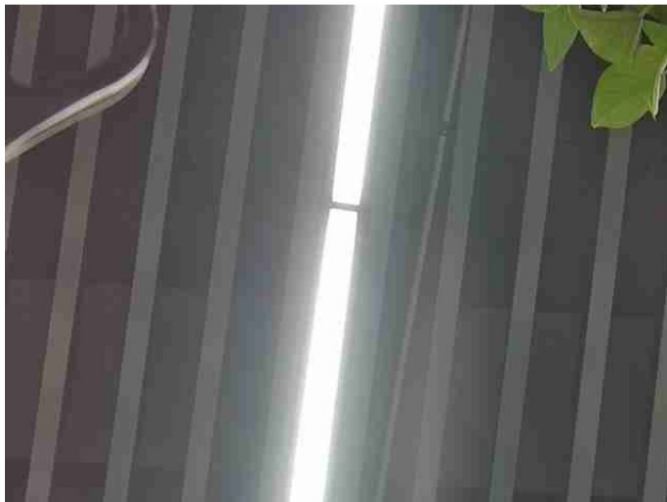
- **Image Quality:** Specify the image resolution, varying from the lowest QCIF(176x144 pixels) to the highest 1080P(1920x1080 pixels).

Live Stream

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

See the live stream on web **Surveillance > Live Stream** interface.

Live Stream



Alternatively, as described in the MJPEG Image Capturing section, enter the correct URL into a web browser.

192.168.36.110:8080/video.cgi



ONVIF

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

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

To set it up, go to **Surveillance > ONVIF > Basic Setting** interface.

Basic Setting	
Discoverable	<input checked="" type="checkbox"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>

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

Tip

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

Camera Mode

You can select the camera mode based on where the device is installed.

To select it, go to **Surveillance > ONVIF > Camera** interface.

Camera

Mode

Indoor ▼

- **Mode:** Select Outdoor or Indoor mode based on the installation environment for better image quality.

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	<input type="checkbox"/>	<button>Disarm</button>
Key Status	High	


- **Enabled:** Check to enable the tamper alarm function. You can click **Disarm** to clear the alarm.
- **Key Status:** The tamper alarm will not be triggered unless the key status is shifted from **Low** to **High** status.

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	<input type="text"/>
Sender's Email Name	<input type="text"/>
Receiver's Email Address	<input type="text"/>
Receiver's Email Name	<input type="text"/>
SMTP Server Address	<input type="text"/>
Port	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
Email Test	<button> Test Email</button>

- **SMTP User Name:** The SMTP username is usually the same as the sender's email address.

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

FTP Notification Setting

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

To set it up, navigate to the web **Setting > Action > FTP Notification** interface.

FTP Notification	
FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password"/>
FTP Path	<input type="text"/>

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

TFTP Notification

To receive security notifications via the TFTP server, you need to enter the TFTP server address.

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

To set it up, go to **Setting > Action > TFTP Notification** interface.

TFTP Notification	
TFTP Server	<input type="text"/>

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	Valid Face Recognition	\$unlocktype	Http://server ip/unlocktype=\$unlocktype

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

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

Action URL

Enabled	<input type="checkbox"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Relay Triggered	<input type="text"/>
Relay Closed	<input type="text"/>
Input Triggered	<input type="text"/>
Input Closed	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<input type="text"/>
Tamper Alarm Triggered	<input type="text"/>
Valid Face Recognition	<input type="text"/>
Invalid Face Recognition	<input type="text"/>

Web Interface Automatic Log-out

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

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

Session Time Out	
Session Time Out Value	<input type="text" value="8000"/> (60~14400Sec)

High Security Mode

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

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

High Security Mode

Enabled	<input checked="" type="checkbox"/>
---------	-------------------------------------

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.

Real-time Monitoring

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

To set it up, go to the **System > Security > Real-time Monitor** interface.

Real-Time Monitor

Apply Setting To

None

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

Emergency Action

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

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

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

Emergency Action

Apply Setting To

☐ Input A

Logs

Access Logs

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

Access Log


Save Access Log Enabled ☒

Save Picture Enabled ☒

Export Picture Enabled ☐

Remote Door Log Enabled ☐

All -

<input type="checkbox"/>	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status	Action
 No Data										

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

- **Save Picture Enabled:** When enabled, the device will capture pictures of the door opening and you can click **Picture** in the Action column to view the screenshot.
- **Export Picture Enabled:** Set whether to export the captured images when exporting the door logs.
- **Remote Door Log Enabled:** Set the remote server to store the door logs.
- **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.

Temperature Logs

You can search the check temperature logs on the **Status > Temperature Log** interface. You can also export temperature logs in CSV or XML files.


Temperature Log

Save Temperature Enabled ☒

Save Picture Enabled ☒

Export Picture Enabled ☐

All -

<input type="checkbox"/>	Index	Temperature	Status	Date	Time	Action
 No Data						

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

- **Save Picture Enabled:** When enabled, the device will capture pictures of the temperature detection and you can click **Picture** in the Action column to view the screenshot.

- **Export Picture Enabled:** Set whether to export the captured images when exporting the temperature logs.
- **Status:** Display the normal, abnormal, or low-temperature status.
- **Temperature:** Display the temperature data.

Event Logs

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

You can check the event logs on the **Status > Event Log** interface. You can export the log in CSV format.

Event Log

Type	Time		Event Type		Status
All x	Start Time	~	End Time	Search	Export
	2024-12-23 09:25:47		Login		Account admin; Success; IP 192.168.35.94
	2024-12-23 09:24:36		IP Change		IP Obtained : 192.168.35.145
	2024-12-23 09:24:31		Device State		Startup
	2024-12-23 09:07:08		Login		Account admin; Success; IP 192.168.35.94
	2024-12-23 08:58:01		IP Change		IP Obtained : 192.168.35.145
	2024-12-23 08:57:54		Device State		Startup
ALL DATA HAS BEEN LOADED					

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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

Basic

Firmware Version	205.30.10.112
Hardware Version	205.0.13.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

Note

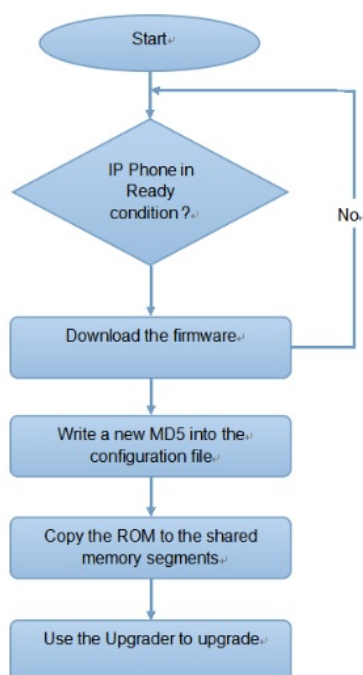
Firmware files should be in **.rom** format for upgrade.

Auto-provisioning via Configuration File

Provisioning Principle

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

Please see the flow chart below:



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

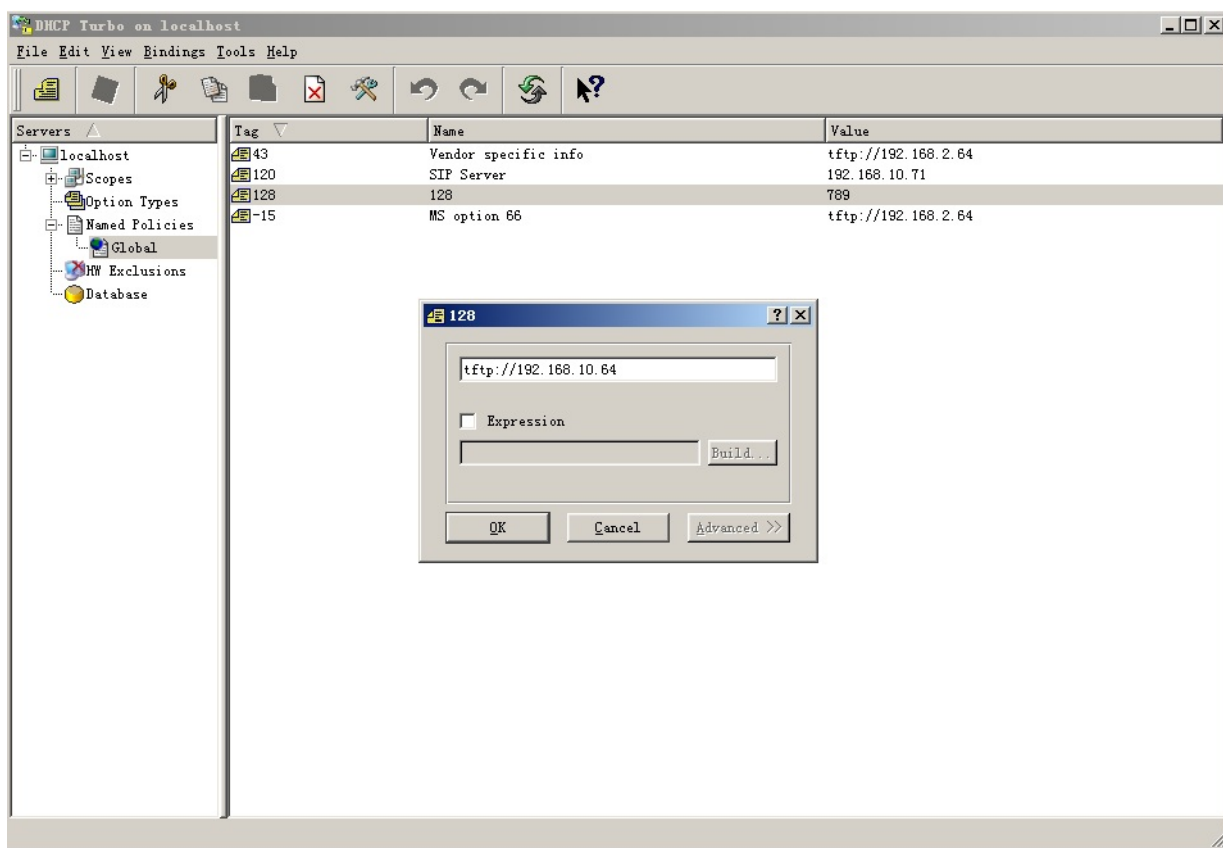
- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/(use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

Automatic Autop

Mode
Power On

Schedule
Sunday
22
0

Export Autop Template
Export

Clear MD5
Clear

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

DHCP Option

Custom Option

(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.

Password Modification

Modify Device Web Interface Password

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

HighSecurityMode

Tamper Alarm

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	
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. Click **Modify Security Question**.

Web Password Modify

Username

admin


 [Change Password](#)

 [Modify Security Question](#)

Web Password Modify

Username

admin

 [Change Password](#)

Please set up your security questions.

Question 1

-- Select One --

Answer

Question 2

-- Select One --

Answer

Question 3

-- Select One --

Answer

Cancel

Submit

Integration with Third Party Device

Integration via Wiegand

A05 access control terminal can be integrated with the 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	4 ▼
Wiegand Input Data Order	Default ▼
Wiegand Output Data Order	Default ▼
Wiegand Output CRC Enable	<input checked="" type="checkbox"/>
RF Card Verification	<input checked="" type="checkbox"/>

- **Wiegand Display Mode:** Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode:** The transmission format should be identical between the access control terminal and the third-party device. It is automatically configured.
- **Wiegand Transfer Mode:**
 - **Input:** The device serves as a receiver.
 - **Output:** The device serves as a sender and users can only open the door by entering a PIN code or swiping an RF card.
 - **Convert To Card No. Output:** The device serves as a sender and users are assigned by multiple door-opening methods such as facial recognition and Bluetooth.
- **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.
- **Wiegand Output CRC Enable:** It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.
- **RF Card Verification:** When enabled, the device will verify whether the card is assigned to a user. If the card is not assigned, a prompt "Opening Door Failed" will pop up on the door phone screen.

Note

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

Integration via HTTP API

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

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

HTTP API

HTTP API Enable

☒

Authorization Mode

Allowlist

Username

admin

Password

1st IP

2nd IP

3rd IP

4th IP

5th IP

- **HTTP API Enable:** 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.

Third-Party Integration

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

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

Third Party Integration	
List	General ▼
HTTP URL	http://192.168.33.40:3000/profile?codeKey={QRCode}&deviceId={DeviceID}
Device ID	1212

- **List:**
 - **None:** Disable the function.
 - **General:** Support scanning third-party QR codes. When enabled, the request URL and device ID are required to be filled in.
- **HTTP URL:** The URL is sent to the third-party server. The URL formats are as follows:
 - http://server_address/api/vistor/scan?codeKey={QRCode}&deviceId={DeviceID}
 - https://server_address/api/vistor/scan?codeKey={QRCode}&deviceId={DeviceID}
- **Device ID:** As part of the HTTP URL, it is provided by the service provider of the third-party server.

Lift Control

The device can be connected to the Akuvox or third-party lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through access methods.

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

Lift Control List	
Lift Control List	Akuvox EC32 ▼
Akuvox EC32 Advance Setting	
Server IP	
Port	
Akuvox EC32 Action	
User Name	
Password	*****
Floor No. Parameter	\$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=\$floor
URL To Trigger All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9

- **Lift Control List:** Select **Akuvox** for integration with the Akuvox lift controller.
- **Server IP:** Enter the IP address of the Akuvox lift controller server.
- **Port:** Enter the port of the Akuvox lift controller server.
- **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.

OSDP Settings

The device can be integrated with the third-party lift controller via OSDP protocol. You are required to check for the device integration protocol and make sure that they are the same.

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

Lift Control List	
Lift Control List	OSDP ▼

OSDP Advanced Setting	
Connect Status	Disconnected
Output With	OSDP ▼

- **Lift Control List:** Select OSDP from the list.
- **Connect Status:** Indicate the connection status.
- **Output With:** Select in what way to send out the card number.
 - **OSDP:** The card number will be sent out to the third-party device via RS485.
 - **None:** The card number will not be sent out but retained in the system.

RS485 Setting

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

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

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

RS485

Apply RS485 Setting To	
	OSDP ▼

OSDP Setting	
Encryption	<input type="checkbox"/>
Transfer Mode	Input ▼
SCBK Value	

- **Disabled:** The RS485 function is disabled.
 - **OSDP:** The device is connected to an OSDP-based external device such as a card reader.
 - **Encryption:** Check this option when the protocol is encrypted.
 - **Transfer Mode:**
 - **Input:** Select this option when the device serves as the relay controller.
 - **Output:** Select this option when the device verifies the user credentials.


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

Debug

System Log for Debugging

System logs can be used for debugging purposes.

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

System Log	
Log Level	3 ▼
Export Log	 Export
Remote System Log Enabled	<input type="checkbox"/>
Remote System Server	

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

Remote Debug Server

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

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

Remote Debug Server	
Enabled	<input type="checkbox"/>
Connect Status	Disconnected
IP Address	
Port	(1024~65535)

- **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.

PCAP

Specific Port

(1~65535)

PCAP

Start

Stop

Export

PCAP Auto Refresh Enabled

☐

- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh Enabled:** When enabled, the PCAP will continue to capture data packets even after the data packets reach their 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets captured reach the maximum capturing capacity of 1MB.

Ping

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

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

Ping

Cloud Server

U Cloud

Verify the network address accessibility

All

Ping

Stop



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

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

Backup

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

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


Others	
Config File	<div><div> Import</div><div> Export (Encrypted)</div></div>
Facial Debug Enabled	<input type="checkbox"/>

System Reboot and Reset

Reboot

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

Basic

Firmware Version	205.30.10.112
Hardware Version	205.0.13.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

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

Reboot Schedule

Mode

☐

Schedule

Every Day

▼

0

(0~23Hour)


Reset

The device provides two reset options:

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

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

Basic

Firmware Version	205.30.10.112
Hardware Version	205.0.13.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot