

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



E16 SERIES DOOR PHONE

Administrator Guide

Thank you for choosing Akuvox E16 series door phones. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to the 216.30.0.67 version, and it provides all the configurations for the functions of E16 series door phones. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

Akuvox E16 series is a Linux system IP video door phone with a touch screen. It integrates audio and video communications, access control, and video surveillance. The E16 series offers customizable features through its advanced system, SmartPlus, and AI-based communication technology, adapting to your operational preferences. With multiple ports like RS485 and Wiegand, it allows easy integration with external digital systems such as elevator controllers and fire alarm detectors. This comprehensive solution ensures holistic control over building entrances and surroundings, providing enhanced security through various access methods such as card access, NFC, Bluetooth, QR code, and door access with body temperature measurement, ideal for residential buildings, office buildings, and complexes.

Change Log

- Support for enabling or disabling Private PIN
- Improved Sequence Call
- Add Security Relay
- Support for displaying **Tenants** on device home screen

Model Specification

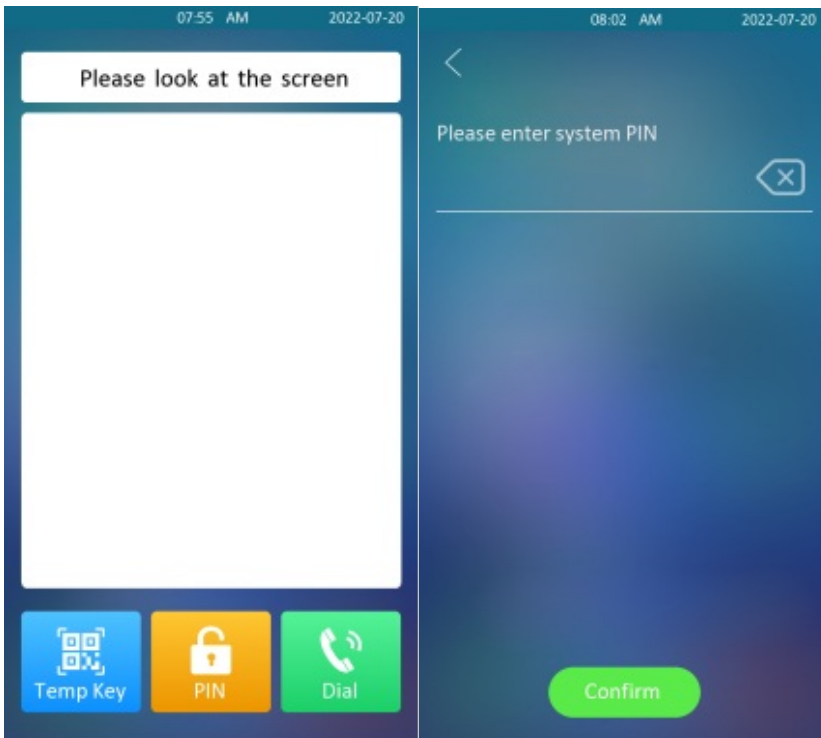
Touch Screen	√
Relay Out	1
Alarm In	1
RS485	√
Card Reader	13.56MHZ
Wi-Fi	X
Bluetooth	√
Temperature Detection	Optional
Face recognition	√
LTE	X
USB	X
External SD Card	X

Access the Device

Door phones' system settings can be either accessed on the device directly or on the device web interface.

Access the Device Setting on the device

To access the device setting, you can long press on the initial screen for approximately five seconds, then enter the default PIN code **admin** and press **Confirm**.



Access the Device Setting on the Web Interface

You can also enter the device IP address on the web browser in order to log in to the device web interface where you can configure and adjust parameters, etc.



Akuvox

User Name

Password

Remember Username/Password

Login

Note

You can obtain IP address by IP scanner.

- 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.
- The initial username and password are **admin** and please be case-sensitive to the user names and passwords entered.

Time and Language Setting

Language Setting

You can select device language and device language icons, and customize interface text including configuration names and prompt text.

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

Setting >> Time/Lang

LCD Language

Mode English ▼

To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device. Navigate to **Setting > Time/Lang > Words Of Language Upload**.

Words Of Language Upload

Web	NULL	📄 Import	📄 Export	↺ Reset
LCD	NULL	📄 Import	📄 Export	↺ Reset

Time Setting

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

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

Time

Automatic Date&Time Enabled

Date 2023-07-11 📅

Time 06:52 🕒

Time Zone GMT+0:00 London ▼

Preferred Server 0.pool.ntp.org

Parameter Set-up:

- **Automatic Date&Time Enabled:** enable it if you want the device's date and time to be automatically set up and synchronized with the default time zone and the NTP server (Network Time Protocol).
- **Primary Server:** enter the primary NTP server you obtained in the **NTP Server**.

Note

- When the check box is not ticked, parameters related to the NTP server cannot be edited.

LED Setting

Configure Card Reader LED Setting

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce electrical power consumption.

To configure the configuration on the web **Device > Light > LED Of Swiping Card Area** interface.

Parameter Set-up:

- **Start Time- End Time (H):** 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).

Configure 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 configure the function, go to **Device > Light > White Light** interface.

Parameter Set-up:

- **Mode:** if you select **Auto**, then the white light will be turned on automatically for face recognition and QR code scan for door opening. If you select **Off**, then the white light will be

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.

Note

- IR LED light should be triggered first before the white light can be valid in the facial recognition, however, IR LED light does not need to be triggered for the white light function in the QR code scan.

Screen Display Configuration

You can set up the device's screen display features such as screensaver to give users a better visual and operational experience.

Configure Screensaver

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

To configure the configuration on web **Device > LCD > Standby Interface Display** interface.

Standby Interface Display

Screensaver Mode	<input checked="" type="checkbox"/>
Screensaver Time	30minutes ▼
Sleep	15seconds ▼
Wakeup Mode	Auto ▼

Parameter Set-up:

- **Screensaver Time (Sec):** set the screen saver start time from 5 seconds up to 2. For example, if you set the start time as 5 minutes, then the screen saver will start if there is no operation on the device or no one is approaching during the five minutes interval.
- **Sleep:** set how long you expect the screen saver to last before turning off the device's screen. You select the screen saver duration from 2 seconds to 30.
- **Wakeup Mode:** select the screen wake-up mode. If you select **Auto mode** then the screen will be awakened when someone approaches without it being touched upon, and if **Manual mode** is selected, then you have to touch and wake up the screen.

Upload Screensaver

You can upload screen-saver pictures separately or in batches to the device and to the device web interface for publicity purposes or for a greater visual experience.

To configure the configuration on web **Device > LCD > Upload Screensaver** interface.

Upload Screensaver

Screensaver1 ▼ Import

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 format** with **2M pixels maximum**.
- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurred.

Configure Screen Display Mode

You can select two types of access screen display mode on the home screen, namely, Default mode for facial recognition and QR code. To configure the configuration on web **Device > LCD > Theme** interface.

Theme

Mode	Default ▼
QR Code Recognition Interval(Sec)	2 ▼
Function Of Call Button	Both, Call Default ▼
Title Of Call Page	Call
Title Of Tenants Page	Tenants

Parameter Set-up:

- **Mode:** If you choose **QR code**, the main screen shows "Please scan your QR code" as default to remind you unlock by QR code. If you choose **Default**, the main screen shows "Please look at the screen" as default to remind you unlock by face recognition.
- **QR Code Recognition Interval(Sec):** this interval is only available when you choose QR Code mode. It is recognition of the interval between two QR codes

Home Screen Configuration

You can change the home screen display through the configuration of tab name and tab arrangement on the device web interface if needed. Path: **Device > LCD > Key In Homepage Of The Default Theme.**

Key In Homepage Of The Default Theme

Display Type Homepage ▼

ID	Name	Type	Value
1	<input type="text"/>	Temp Key ▼	<input type="text"/>
2	<input type="text"/>	PIN ▼	<input type="text"/>
3	<input type="text"/>	Call ▼	<input type="text"/>

Parameter Set-up:

- **Display Type:** Select from five display type: **Homepage**, **Call**, **Tenants**, **PIN**, and **Temp Key**. If you select **Call**, the screen will wake up in the **Call** page by default.
- **Name:** enter a new name to replace the original type of name, but it does not change the attribute of the type.
- **Type:** select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make the **Speed Dial** tab be displayed in position one, you can change the type in index number 1 to **Speed Dial**. And you can change another tab position accordingly.
- **Value:** enter the IP or SIP number to be attached to the reception icon for the speed dial. The number entered will be dialed out as you press the **Reception** icon on the home screen. This field is only valid for speed dial. You can type in five-speed dial numbers maximum and every two of the number must be separated by “;”. You can also select a contact group to be called by pressing the **Reception** icon.

Volume & Tone Configuration

Volume and tone configuration include microphone volume, the AD volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

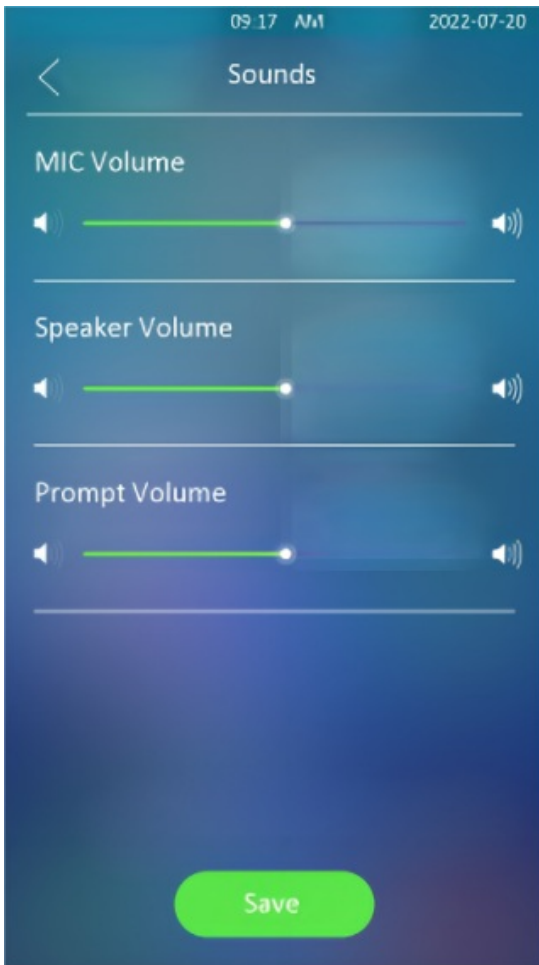
Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

Configure Volume on the Device

You can adjust the microphone volume, speaker volume, keypad volume, and AD volume on the device.

Path: **Display&Sounds > Sounds.**



Parameter Set-up:

- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound, etc.

Configure Volume on the Web Interface

On the web interface, you can set the tamper alarm volume, mic volume, etc.

Path: **Device > Audio > Volume Control**

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

Parameter Set-up:

- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound, etc.

Upload Open Door Tone

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

To configure the configuration on web **Device > Audio > Open Door Tone Setting**.

Open Door Tone Setting

Open Door Tone Enabled

Open Door Succeed Tone Upload

Note

- The open door tone file should be in .wav format and the file size should be smaller than 200KB.

Configure Door Access Prompt Text

You can enable the open door text prompt for both door-opening success and failure. And you can also make the door phone display the user information when users use credentials such as RF cards for access.

To configure the configuration on web **Access Control > Relay > Door Setting General** interface.

Door Setting General

Open Door Succeeded Text Prompt

Open Door Failed Text Prompt

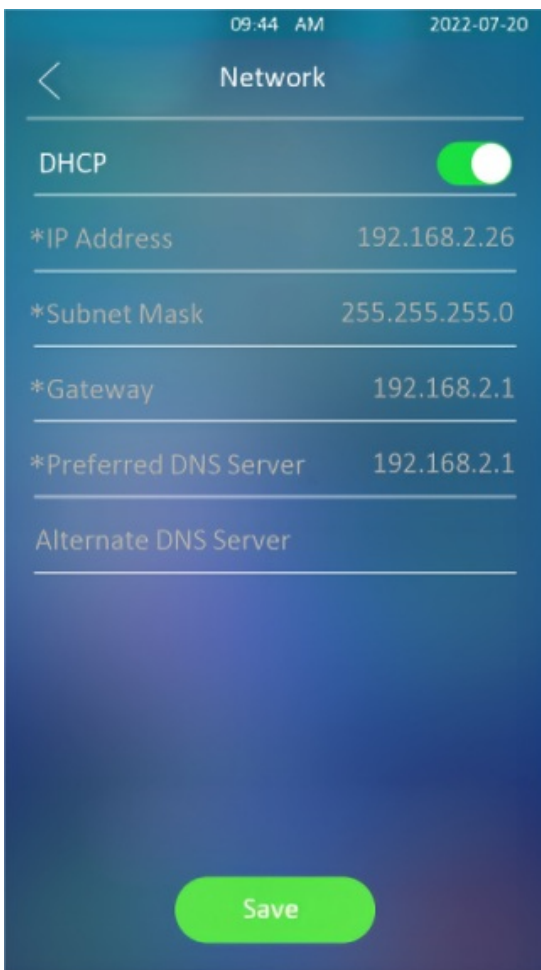
Parameter Set-up:

- **Open Door Succeeded Text Prompt:** tick the check box if you want to see the text prompt after the door opening success.
- **Open Door Failed Text Prompt:** tick the check box if you want to see the prompt words after the door open failure.

Network Setting

Device Network Connection Setting

You can configure the default DHCP mode (Dynamic Host Configuration Protocol) and static IP connection. Moreover, you can set up an IP address, Subnet Mask, Default Gateway, and DNS servers.



Parameter Set-up:

- **DHCP**: select the **DHCP mode** by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: select the **static IP mode** by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server

address have to be manually configured according to your actual network environment.

- **IP Address** : set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.
- **Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **Preferred&Alternate DNS Server**: set up a preferred or alternate DNS Server (Domain Name Server) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address, and the door phone will connect to the alternate server when the primary DNS server is unavailable.

To configure the device network on the web interface, go to **Network > Basic > LAN Port**.

LAN Port

Type

 DHCP Static IP

IP Address

Subnet Mask

Default Gateway

Preferred DNS Server

Alternate DNS Server

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 configure the configuration on web **Network > Advanced > Connect Setting** interface.

Connect Setting

Server Mode
None

Discovery Mode

Device Address

Device Extension

Device Location

Parameter Set-up:

- **Server Mode:** it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC, ACMS Cloud**, and **None**. **None** is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **Discovery Mode:** go to **Enabled** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and go to **Disabled** if you want to conceal the device so as not to be discovered by other devices.
- **Device Address:** specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
- **Device Extension:** enter the device extension number for the device you installed.
- **Device Location:** enter the location in which the device is installed and used.

NAT Setting

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

You can go to **Account > Advanced > NAT**.

NAT	
UDP Keep Alive Messages	<input checked="" type="checkbox"/>
UDP Alive Messages Interval	<input type="text" value="30"/> (5-60Sec)
RPort Enabled	<input type="checkbox"/>

Parameter Set-up:



- **UDP Keep Alive Messages:** if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Messages Interval:** set the message sending time interval from 5-60 seconds, the default is 30 seconds.
- **RPort:** enable the RPort when the SIP server is in WAN (**Wide Area Network**).

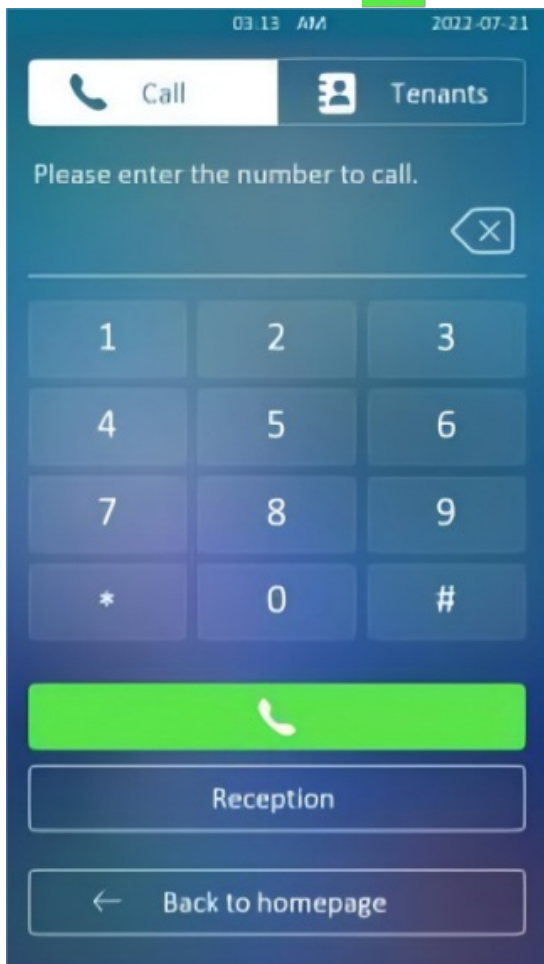
Intercom Call Configuration

IP Call & IP Call Configuration

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

Make IP calls

To make a direct IP call on the device, you can press the Dial  icon, then enter the IP or SIP number and press the Call  icon to call out.



IP Call Configuration

To configure the IP call on the device web **Intercom > Basic > Direct IP** interface.

Direct IP	
Enabled	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1-65535)

Parameter Set-up:

- **Direct IP Port:** the direct IP Port is **5060** by default with the port range from **1-65535**. If you enter any values within the range other than 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

SIP Call & SIP Call Configuration

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

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

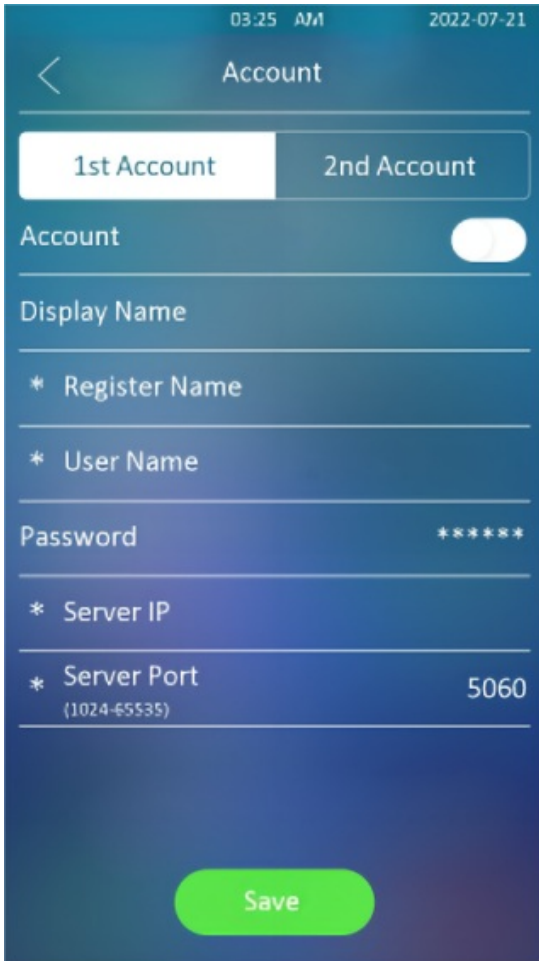
SIP Account Registration

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

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

Configure SIP Account on the Device

On the device **Setting** screen, select **Account**. **Register Name**, **User Name**, and **Password** are obtained from the SIP account administrator.



Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.
- **Display Label:** configure the device label to be shown on the device screen.

SIP Server Configuration

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

To set up a SIP server, you can go to **Account > Basic Preferred SIP Server.**

Preferred SIP Server		
Server Address	<input type="text"/>	
Sip Server Port	<input type="text" value="5060"/>	(1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535 Sec)

Alternate SIP Server		
Server Address	<input type="text"/>	
Sip Server Port	<input type="text" value="5060"/>	(1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535 Sec)

Parameter Set-up:

- **Preferred SIP Server:** enter the primary server IP address number or its IP address or domain.
- **Alternate SIP Server:** enter the backup SIP server IP address or domain.
- **SIP Port:** set up a SIP server port for data transmission.
- **Registration Period:** set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is **1800**, ranging from **30-65535s**.

Configure Outbound Proxy Server

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

To configure the proxy server, you can go to **Account > Basic > Outbound Proxy Server.**

Outbound Proxy Server		
Outbound Enabled	<input type="checkbox"/>	
Preferred Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)
Alternate Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)

Parameter Set-up:

- **Preferred Server IP**: enter the SIP address of the outbound proxy server.
- **Port**: enter the Port number for establishing a call session via the outbound proxy server.
- **Alternate Server IP**: set up Backup Server IP for the backup outbound proxy server.
- **Port**: enter the Port number for establishing a call session via the backup outbound proxy server.

Configure Data Transmission Type

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

To do the configuration, you can go to **Account > Basic > Transport Type**.

Transport Type	
Type	<input type="text" value="UDP"/>

Parameter Set-up:

- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for a reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for Secured and Reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain a DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, **SRV** can also be used to configure the priority and the weight of the server address.

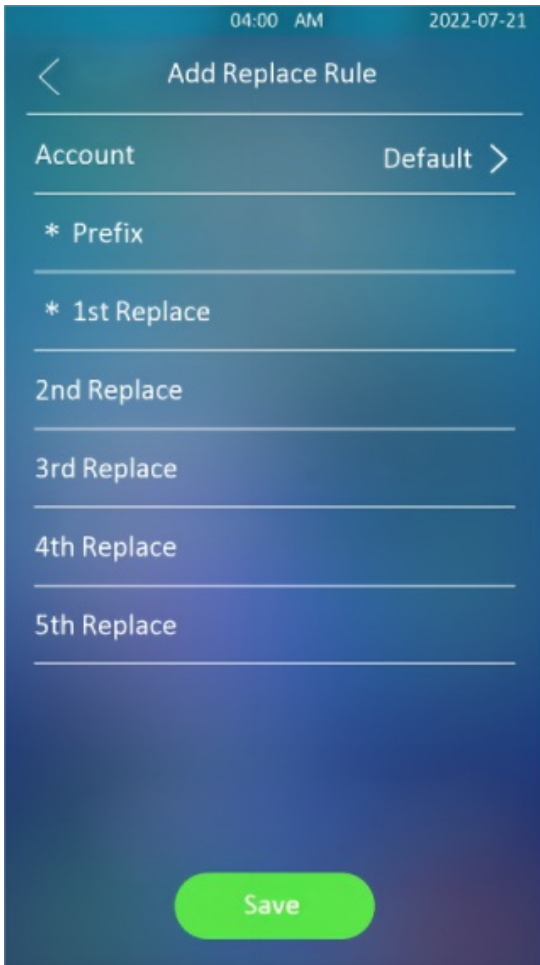
Dial Options Configuration

Quick Dial By Number Replacement on the Device

The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

On the device **Setting** screen, select **Replace Rule**, then select **Add**.





Parameter Set-up:


- **Account:** select the account to which you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the dialed number has been registered). You can select either account 1 or account 2 from which the number can be dialed out. If you have registered the dialed number in both Account 1 and Account 2, then the number will be called out from Account 1 by default.
- **Prefix:** enter the short number to replace the dialed number you wish to replace.
- **Replace 1/2/3/4/5:**enter the dialed number(s) you wish to replace. It supports up to 5 numbers maximum for the replacement of the device configuration. For example, if you replace five original dial numbers with a common short number such as **101** then the five intercom devices with the dialed number will be called at the same time when you dial **101**.

Quick Dial by Number Replacement on the Web Interface

You can not only add a quick dial number separately but also import the quick dial number to the device in batch. Besides, you can edit and delete the numbers if needed.

To configure it, you can go to **Intercom > Dial Plan**.

Dial Plan

<input type="checkbox"/>	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
 No Data									

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

Auto-answer Configuration

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

To configure Auto-answer function:

Go to **Intercom > Call Feature > Auto Answer**.

Auto Answer

Auto Answer Delay (0-5Sec)

Mode

To enable Auto-answer mode:

Go to **Account > Advanced > Call**.

Call

Max Local SIP Port (1024-65535)

Min Local SIP Port (1024-65535)

Auto Answer

Prevent SIP Hacking

Parameter Set-up:

- **Auto Answer Delay:** set up the delay time (from 0-5 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Mode:** set up the Video or Audio mode you preferred for the automatic call answering.

Sequence Call Configuration

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application.

To do the configuration on web **Intercom > Basic > Sequence Call** interface.

Sequence Call	
When Refused	Do Not Call Next
Call Timeout (Sec)	60

Parameter Set-up:

- **When Refused:** Select **Do Not Call Next** when the call is refused, the call will be stopped. Select **Call Next**, the call will be transferred to the next one.
- **Timeout(Sec):** to check the call time interval in between the sequence call number in a targeted sequence Call group. For example, if you set the time interval as 10 seconds, then the call (if not answered in 10 Sec.) will be terminated automatically and be transferred sequentially to the next sequence call number in the targeted sequence call group.

To decide the sequence of calling, navigate to **Directory > User > Add/Edit User > Contact Details**.

Contact Details	
Phone	12345
Group	101
Priority Of Call	Firstly
Dial Account	Auto

Enabling Prevent SIP Hacking

Internet phone eavesdropping is a network attack that allows unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls from being compromised on the Internet.

Call

Max Local SIP Port	<input type="text" value="5062"/>	(1024-65535)
Min Local SIP Port	<input type="text" value="5062"/>	(1024-65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input type="checkbox"/>	

Note

The direct IP calls will be blocked if the direct IP is disabled.

Call Settings

Maximum Call Duration Setting

The door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the call automatically.

To do the configuration, you can go to **Intercom > Call Feature > Max Call Time**.

Max Call Time

Max Call Time	<input type="text" value="5"/>	(2-30Min)
---------------	--------------------------------	-----------

Parameter Set-up:

- **Max Call Time:** enter the call time duration according to your need (ranging from 2-30 min.). The default call time duration is 5 min.

Note

- The max call time of the device is also related to the max call time of SIP. If you use a SIP account to make a call, please pay attention to the max call time of the SIP server. If the max call time of the SIP server is shorter than the max call time of the device, then the SIP server max call time will be applied.

Maximum Dial Duration Setting

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

To do the configuration, you can go to **Intercom > Call Feature> Max Dial Time**.

Max Dial Time

Dial In Time	<input type="text" value="60"/>	(5-120Sec)
Dial Out Time	<input type="text" value="60"/>	(5-120Sec)

Parameter Set-up:

- **Dial In Time:** enter the dial-in time duration for your door phone (ranging from 5-120 sec). For example, if you set the dial-in time duration as 60 seconds in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial-in time duration by default.
- **Dial Out Time:** enter the dial-in time duration for your door phone (ranging from 5-120 sec). For example, if you set the dial-out time duration as 60 seconds in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answered by the device being called to.

Audio& Video Codec Configuration for SIP Calls

Configure Audio Codec

The door phone supports four types of Codec (PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To do the configuration, you can go to **Account > Advanced > Audio Codecs**.

Audio Codecs

Please refer to the bandwidth consumption and sample rate for the four types of codecs below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz

Configure Video Codec

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

To do the configuration, you can go to **Account > Advanced > Video Codec**.

Parameter Set-up:

- **Name:** check to select the H264 video codec format for the door phone video. H264 is the video codec by default.
- **Resolution:** select the code resolution for the video quality among four options: **QCIF**, **CIF**, **VGA**, **4CIF**, and **720P** according to your actual network environment. The default code resolution is 4CIF.

- **Bitrate:** select the video stream bitrate (ranging from 320-2048). The greater the bitrate, the data transmitted every second is greater in amount therefore the video will be clearer. While the default code bitrate is 2048.
- **Payload:** select the payload type (ranging from 90-118) to configure the audio codec payload. The payload between the door phone and the corresponding intercom device should be identical. The default payload is 104.

Configure DTMF Data Transmission

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

To configure the DTMF data transmission, you can go to **Account > Advanced > DTMF**.

DTMF	
Mode	<input type="text" value="RFC2833"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
Payload	<input type="text" value="101"/> (96-127)

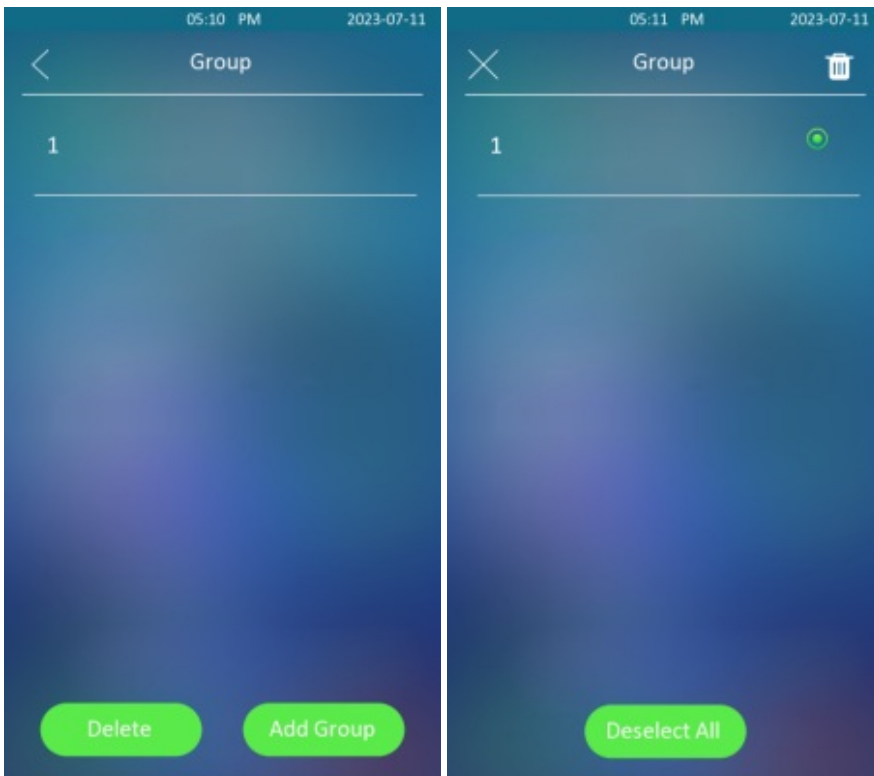
Parameter Set-up:

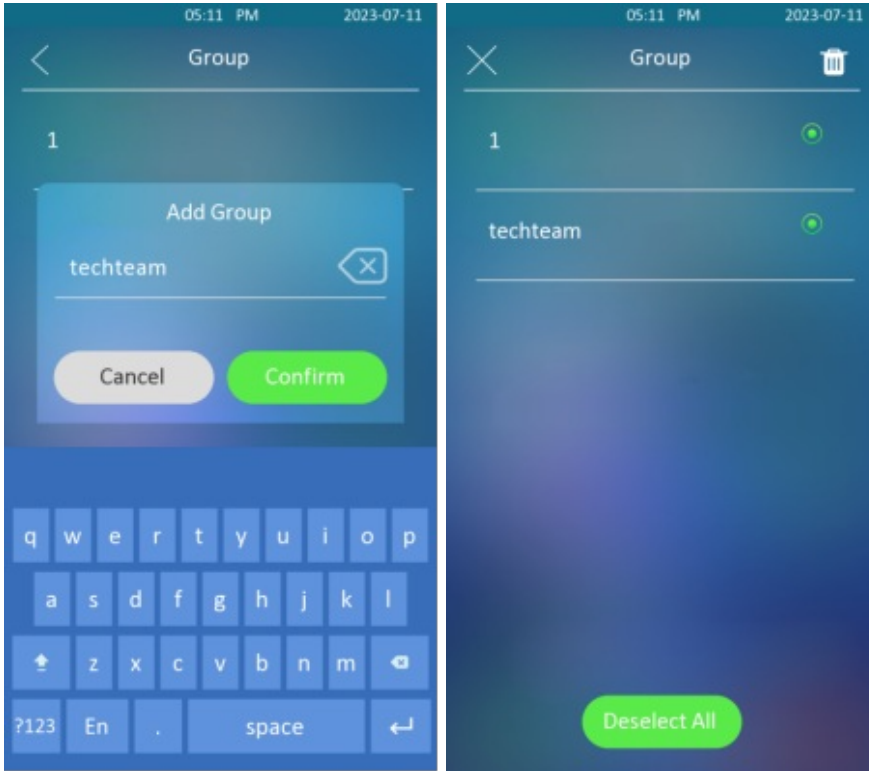
- **Mode:** select DTMF mode among six options: **Info**, **Inband**, **RFC2833**, **Info+Inband**, **Info+RFC2833**, and **Info+Inband+RFC2833** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF:** select among four types: **Disable**, **DTMF**, **DTMF-Relay**, and **Telephone-Event** according to the specific type adopted by the third party device. You are required to set it up only when the third-party device to be matched with adopts **Info** mode.
- **Payload:** set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

Contact List Configuration

Contact List Configuration on the Device

You can configure the contact list in terms of adding and modifying contact groups or contacts on the device directly. To configure the phone book on the device **User > Group**.





Contact List Configuration on the Web Interface

Managing Contact Groups on the Web Interface

You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

Path: [Directory](#) > [User](#) > [Group](#)

Group

[+ Add](#)

<input type="checkbox"/>	Index	Name	Edit
<input type="checkbox"/>	1	1	✎

Selected: 0/1 [Delete](#) [Delete All](#) Total: 1 [Prev](#) 1/1 [Next](#) Go To Page [Go](#)

Managing Contact List Display Setting

If you want to customize your contact list display to your desired visual preference. You can go to the web interface to do the configuration.

Path: Directory > Directory Setting> Tenants List Setting.

Tenants List Setting

Show Local Tenants Enabled	<input type="checkbox"/>
Show Cloud Tenants Enabled	<input type="checkbox"/>
Tenants Sort By	Room No. ▼
Click Tenants To Dial Out	<input checked="" type="checkbox"/>
Contacts Display Mode	Groups Only ▼

Parameter Set-up:

- **Show Tenants of Local Group Enabled:** tick or untick the check box to control the display of the group label. If you untick the check box, then only the group tab will be displayed while the contact tab will be concealed and vice versa.
- **Show Cloud Tenants Enabled:** tick the check box to show the cloud tenants in the tenant's list. And when you untick the check box, the cloud tenants will be hidden.
- **Tenants Sort By:** select **ASCII Code** or **Room No.** or **Import**. When you select ASCII Code, the tenants will be listed by their names in the sequence of the ASCII code. When you select Room No., the tenants will be sorted according to their room numbers. This is applicable to the local contacts and contacts synchronized from the SmartPlus cloud.
- **Click Tenants to Dial Out:** tick the check box to enable the dial-out by pressing the contact tab. When this function is enabled, you can press anywhere on the contact tab to dial out. This function will be disabled when you untick the check box, and when it is disabled, you need to press the Call icon in the middle of the tab to dial out.
- **Contacts Display Mode :** Select from **Groups Only**, **All Contacts**, and **Group On Entry Page And Their Contacts On Subpage**. If you select **Groups Only**, you can tap the group to call all contacts. The group name is displayed when calling.

Relay Setting

Relay Switch Setting

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

Relay	
Trigger Delay(Sec)	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text"/>
DTMF Mode	<input type="text" value="5"/>
1 Digit DTMF	<input type="text" value="Relay"/>
2~4 Digits DTMF	<input type="text" value="0"/>
Relay Status	Low
Relay Name	<input type="text" value="0"/>

Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (ranging from 1-10 Sec). For example, if you set the delay time as 5 sec, then the relay will not be triggered until 5 seconds after you press the **Unlock** tab.
- **Hold Delay (Sec):** set the relay hold delay timing (ranging from 1-10 Sec). For example, if you set the hold delay time as 5 sec, then the relay will stay triggered for 5 seconds after the door is It means the door will stay open for 5 seconds.
- **DTMF Mode:** select the number of DTMF digits for the door access control (**Ranging from 1-4 digits**) For example, you can select a 1-digit DTMF code or 2-digit DTMF code, etc., according to your need.
- **1 Digit DTMF:** set the 1 digit DTMF code within range from (0-9 and *, #).
- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option**. For example, you are required to set the 3-digits DTMF code if **DTMP Mode** is set as 3-digits.
- **Relay Status:** relay status is low by default which means normally closed (NC). If the relay status is high, then it is in normally open status (NO).
- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note

- Only the external devices connected to the relay switch need to be powered by powered adapters as the relay switch does not supply power.
- If DTMF mode is set as **1 Digit DTMF**, you cannot edit DTMF code in **2~4 Digits DTMF** and if you set DTMF mode from 2-4 in **2~4 Digits DTMF** field, you cannot edit DTMF code in **1 Digit DTMF** field.

Web Relay Setting

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.



Configure Web Relay on the Web Interface

Web relay needs to be set up on the web interface where you are required to fill in such information as relay IP address, password, web relay action, etc. Before you can achieve door access via web relay.

Path: **Access Control > Web Relay**. IP Address, User Name, and Password are provided by the web relay manufacturer.

Web Relay

Type	<input type="text" value="Disabled"/>
IP Address	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>

Parameter Set-up:

- **Type:** among three options **Disabled**, **Web Relay** and **Both**. Select **Web Relay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay. If you select **Web Relay**, then the local relay will not be valid.
- **Password:** The passwords are authenticated via HTTP and you can define the passwords using **http get action**.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **Web Relay Key:** enter the configured DTMF code, when the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.

After the web relay is set up, you can select the specific web relay action to be carried out.

You can go to **Directory > User**, then click + Add, then scroll down to **Access Setting**.

User

Local ▾
ALL ▾
Q Search
↺ Reset
+ Add
📄 Import
📄 Export

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
<p>No Data</p>												

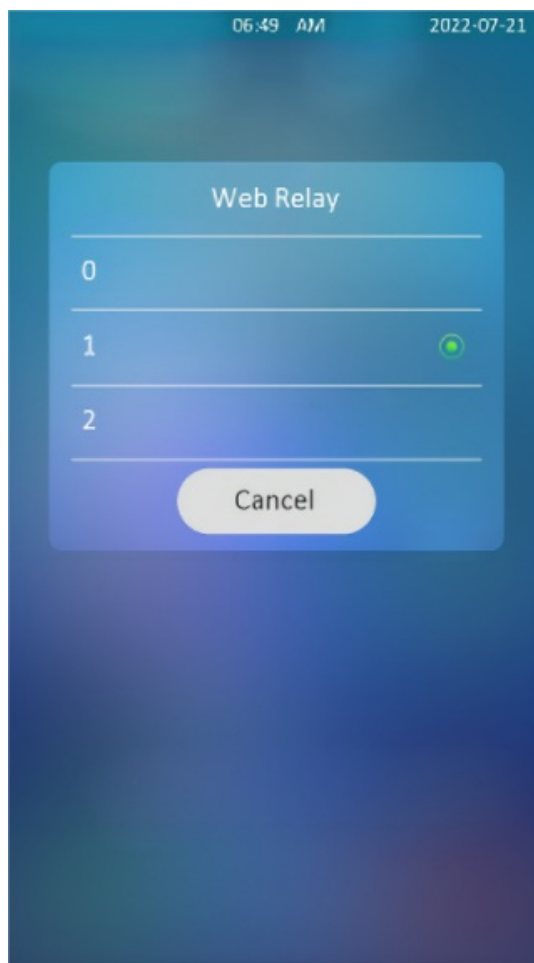
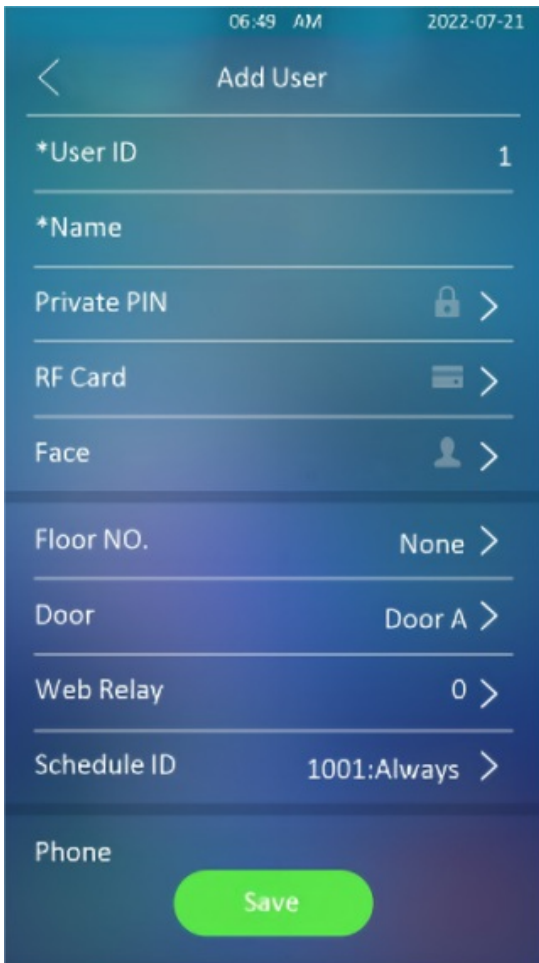
Selected:0/0
🗑 Delete 🗑 Delete All
Total:0
⏪ Prev 1/1 Next ⏩
Go To Page Go

Access Setting

Relay	<input checked="" type="checkbox"/> Relay A															
Security Relay	<input type="checkbox"/> Security Relay A															
Floor No.	<input type="text" value="None x"/>															
Web Relay	<input type="text" value="0"/>															
Schedule	<table border="0"> <tr> <td>1 item</td> <td>Unselected</td> <td></td> <td>1 item</td> <td>Selected</td> </tr> <tr> <td><input type="checkbox"/> 1002:Never</td> <td></td> <td>></td> <td><input type="checkbox"/> 1001:Always</td> <td></td> </tr> <tr> <td></td> <td></td> <td><</td> <td></td> <td></td> </tr> </table>	1 item	Unselected		1 item	Selected	<input type="checkbox"/> 1002:Never		>	<input type="checkbox"/> 1001:Always				<		
1 item	Unselected		1 item	Selected												
<input type="checkbox"/> 1002:Never		>	<input type="checkbox"/> 1001:Always													
		<														

Configure Web Relay on the Device

After the web relay actions are entered on the web interface, you can now select the specific number of the web relay actions to be carried for the specific resident you added for the door unlock. To configure it, go to **User > User List**.



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.



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

Security Relay

Connect Type	RS485
Trigger Delay(Sec)	0
1 Digit DTMF	2
2~4 Digits DTMF	013
Relay Name	Security Relay A
Enabled	<input type="checkbox"/>
	<input type="button" value="Test"/>

Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (ranging from 1-10 Sec.) For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press Unlock tab. The default is 0 meaning triggering relay right after you press the unlock tab.
- **1 Digit DTMF:** set the 1 digit DTMF code within range from (0-9 and *,#).
- **2~4 Digits DTMF:** set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digit DTMF code if DMTP Mode is set as 3- digits.
- **Relay Name:** give a name to the relay if needed. And relay name can be edited on the SmartPlus cloud and SDMC.

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 do the configuration, navigate to **Access Control > Relay > Relay Schedule** interface.

Relay Schedule

Relay ID RelayA ▼

Schedule Enabled

2 items	Unselected	0 item	Selected
<input type="checkbox"/> 1001:Always		No Data	
<input type="checkbox"/> 1002:Never			

>
<

Parameter Set-up:

- **Relay ID:** choose the relay you need to set up.
- **Schedule Enabled:** it is disabled by default. Only choose to enable it, and you can select the schedule.

Note

- You can refer to [Create Door Access Schedule](#) for the relay schedule setting.

Door Access Schedule Management

Configure 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.

To configure the schedule, go to **Setting > Schedule**, then click [+ Add](#).

Schedule

Local + Add Import Export

<input type="checkbox"/>	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

To create a daily schedule, select **Daily** mode.

Add Schedule X

Name

Mode

Date Range -

Day Of Week

Monday Tuesday Wednesday

Thursday Friday Saturday

Sunday Check All

Date Time -

Cancel Submit



Parameter Set-up:

- **Mode:** select daily schedule.

- **Name:** enter the daily schedule name.
- **Date Time:** set up the time schedule for the validity of the door access during the day.

To create a daily schedule, select **Weekly** mode.

Add Schedule





Name	<input type="text"/>
Mode	<input type="text" value="Weekly"/>
Day Of Week	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Check All
Date Time	<input type="text" value="00:00"/>  - <input type="text" value="23:59"/> 

Parameter Set-up:

- **Day of Week:** select the day (s) on which door access can be valid on a weekly.

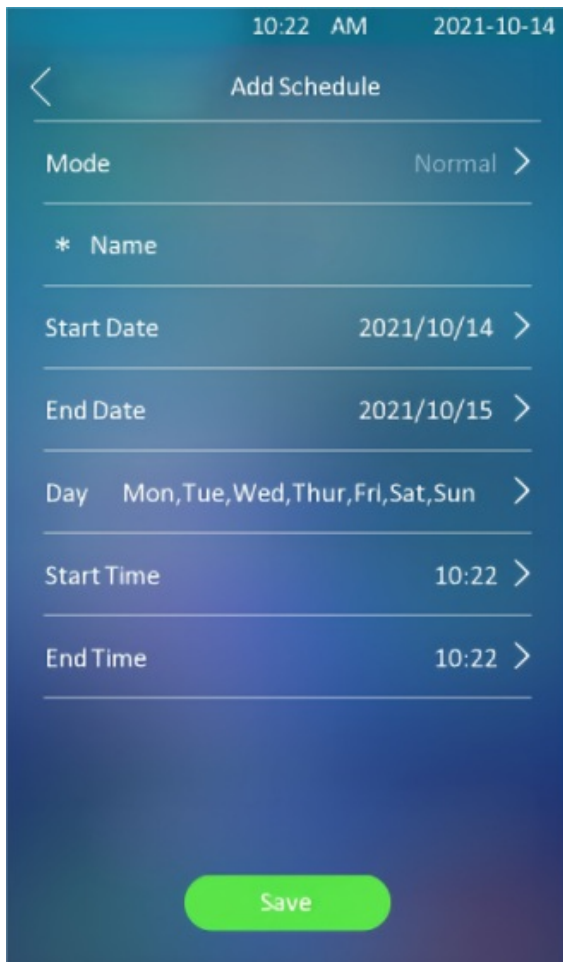
To create a longer period schedule:

Add Schedule

Name	<input type="text"/>
Mode	<input type="text" value="Normal"/>
Date Range	<input type="text" value="2023-07-11"/>  - <input type="text" value="2023-07-12"/> 
Day Of Week	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Check All
Date Time	<input type="text" value="00:00"/>  - <input type="text" value="23:59"/> 

Create Door Access Schedule on the Device

You can also create a door access schedule on the device. You can go to **Schedule > Add Schedule**.

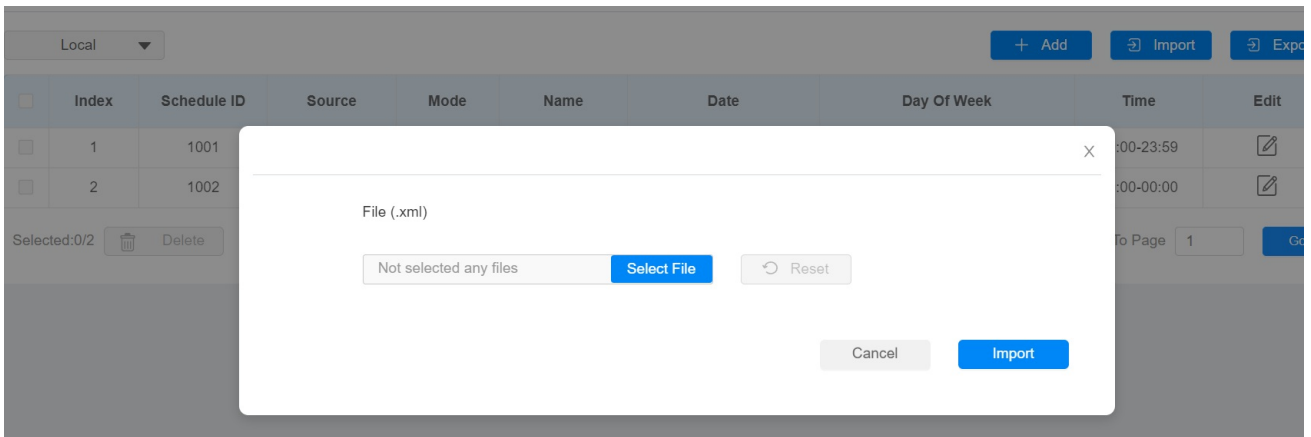


The screenshot shows a mobile application interface for creating a door access schedule. At the top, the status bar displays '10:22 AM' and '2021-10-14'. Below the status bar is a header with a back arrow and the text 'Add Schedule'. The main content area contains several form fields, each with a label on the left and a value on the right, followed by a right-pointing chevron icon. The fields are: 'Mode' with the value 'Normal'; '* Name' which is currently empty; 'Start Date' with the value '2021/10/14'; 'End Date' with the value '2021/10/15'; 'Day' with the value 'Mon, Tue, Wed, Thur, Fri, Sat, Sun'; 'Start Time' with the value '10:22'; and 'End Time' with the value '10:22'. At the bottom of the screen is a prominent green rounded rectangular button with the text 'Save' in white.

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.

You can go to **Setting > Schedule**, then click **Import**.



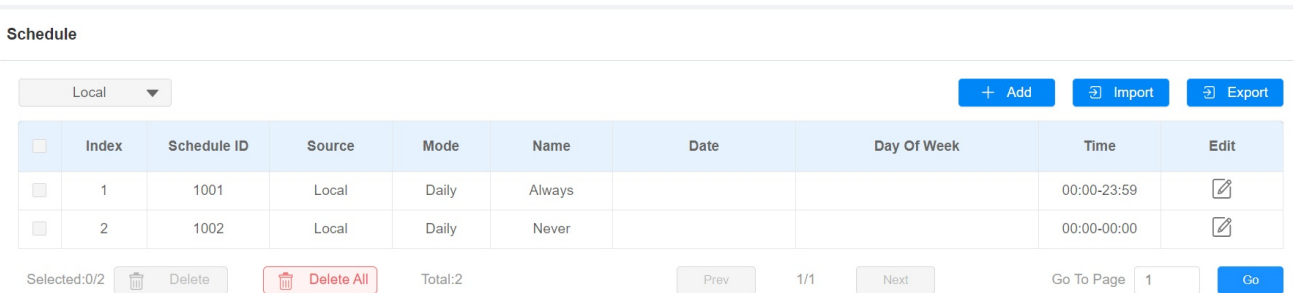
Note

- It only supports .xml format files for importing and exporting the schedule.

Edit the Door Access Schedule

If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch.

To edit the schedule on the web interface, go to **Setting > Schedule**.



To edit the schedule on the device, click **Schedule**, then choose the schedule you want to edit.



Note

- It only supports .xml format files for importing and exporting the schedule.

Door Unlock Configuration

Access Authentication

You can set up multiple access authentication modes, and set up authentication security as needed.

On the web, navigate to **Access Control > Relay > Access Authentication Mode**.

The screenshot shows a configuration page titled "Access Authentication Mode". It features two main settings: "Authentication Mode" with a dropdown menu, and "Entry Restriction" with an unchecked checkbox.

Parameter Set-up:

- **Authentication Mode:** select **Any method** if you allow all the access methods to unlock the door. Select **Face + PIN** if you want to apply dual access methods (Face + PIN) for the door unlock. Select **Face + RF Card** if you want to apply dual access methods (Face+ RF Card) for the door unlock. Select **RF Card+PIN** if you want to apply dual access methods (RF Card+PIN) for the door unlock.
- **Entry Restriction:** enable it to set the time interval of unlocking the door.

Configure PIN Code for Door Unlock

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

Configure Public PIN code

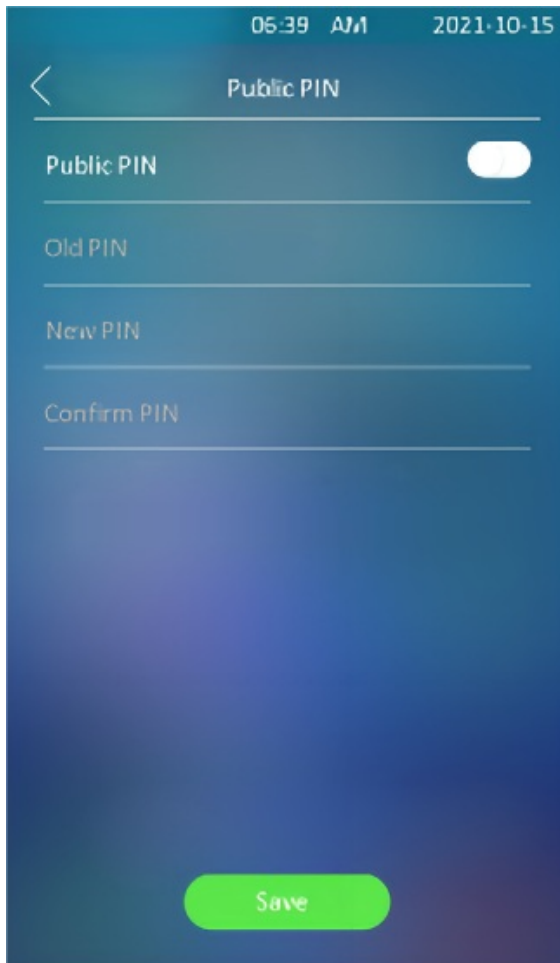
You can configure and change public PIN codes.

On the web interface, go to **Access Control > PIN Setting > Public PIN**.

The screenshot shows a configuration page titled "Public PIN". It features two main settings: "Enabled" with an unchecked checkbox, and "PIN Code" with a text input field containing a single asterisk.

Parameter Set-up:

- **PIN Code:** set the PIN code with a digit limit ranging from 4-8.



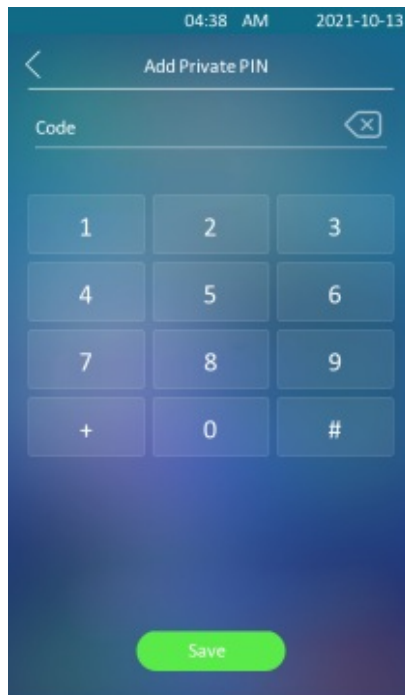
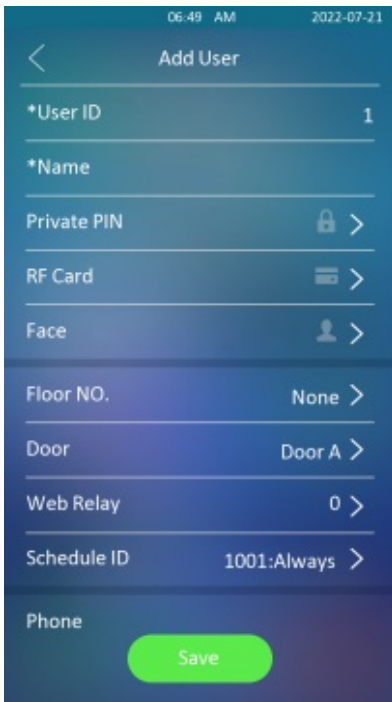
Note

- The public PIN code will not be valid until the function is turned on.
- APT+PIN is applicable only when the device is added to the Akuvox SmartPlus.

Configure Private PIN Code on the Device

You can set up a private PIN code on the device for the specific user.

Path: **User > User List.**



Configure Private PIN Code on the Web Interface

On the web interface, you can create the PIN code and customize additional settings, such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

To configure the PIN code, go to **Directory > User** interface.

User

Local ▾
ALL ▾
🔍 Search
↺ Reset
+ Add
📄 Import
📄 Export

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
<div style="text-align: center;"> <p>No Data</p> </div>												

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

User Info

User ID	<input type="text" value="1"/>
Name	<input type="text"/>

PIN

Code	<input type="text"/>
------	----------------------

After user information and PIN code are entered, you can scroll down to **Access Setting** on the same page to set door access schedule for Private PIN Code door access:

Access Setting

Relay	<input checked="" type="checkbox"/> Relay A
Security Relay	<input type="checkbox"/> Security Relay A
Floor No.	<input type="text" value="None x"/>
Web Relay	<input type="text" value="0"/>
Schedule	<div style="display: flex; align-items: center;"><div style="border: 1px solid #ccc; padding: 5px; width: 45%;"><p>1 item Unselected</p><p><input type="checkbox"/> 1002:Never</p></div><div style="margin: 0 10px; text-align: center;"><p>></p><p><</p></div><div style="border: 1px solid #ccc; padding: 5px; width: 45%;"><p>1 item Selected</p><p><input type="checkbox"/> 1001:Always</p></div></div>

Parameter Set-up:

- **Relay:** select the relay for the door unlock for the user.
- **Floor NO:** enter the resident's floor number.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Schedule:** select from the created door access schedule on the right box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

Note

- This step is applicable to door access by RF card and facial recognition as they are identical in configuration.

Configure Private PIN Access Mode

The device provides two authentication methods for private PIN code access: PIN and APT# + PIN. The latter requires users to input their apartment number followed by their private PIN to unlock the door.

Path: **Access Control > PIN Setting > Private PIN**. And you can disable Private PIN on the same page.

Access Control >> PIN Setting

Private PIN

Enabled

Authorization Mode

Parameter Set-up:

- **Authorization Mode:** select access mode between **PIN** and **APT#+PIN**. If you select the **PIN**, then you are only required to enter the PIN code directly for the door access, while if you select **APT#+PIN**, then you are required to enter the Apartment Number first before entering your PIN code for the door access.

Configure RF Card for Door Unlock

Add RF Card on the Web Interface

To add RF cards, go to **Directory > User**, then click  .

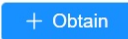
User

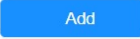
User ID/Name/Code Local ALL Search Reset Add Import Export

Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											

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

RF Card

Code 



Note

- Please refer to PIN code access schedule selection for the RF card user(s)- specific door access.

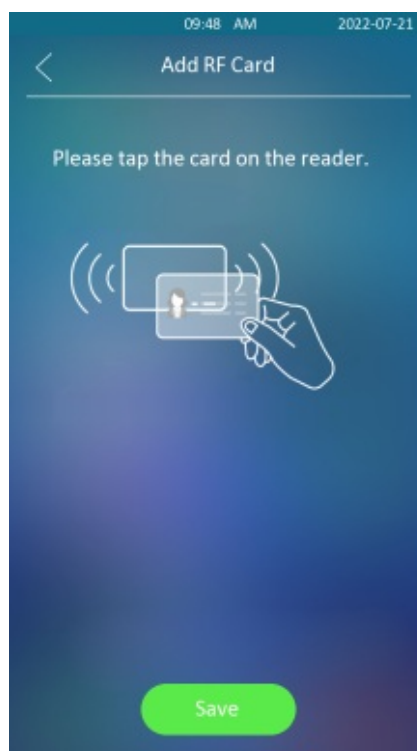
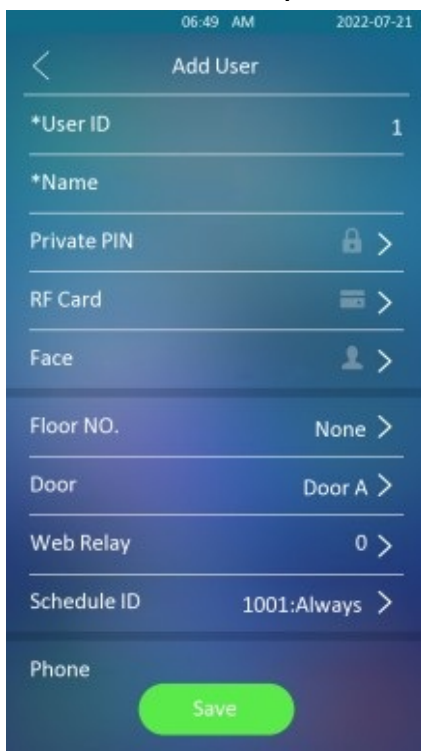
Note

- RF card with 13.56 MHz and 125 KHz can be applicable to the door phone for door access.

Add RF Card to the Device

You can configure the RF card directly on the device for the door access while setting up the time schedule for the validity of the RF card access along with the web relay that can be triggered with the RF card etc.

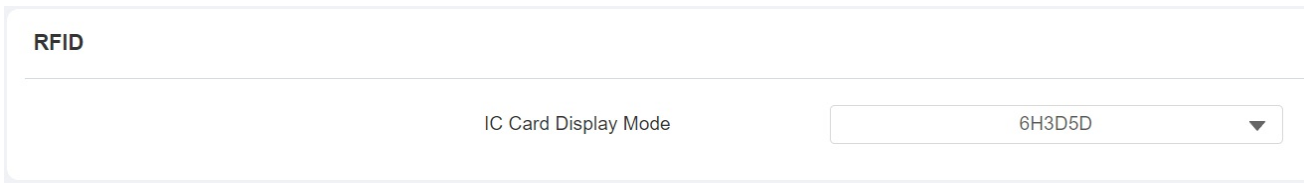
To add an RF card, tap **User**, then **User List**, then **Add**.



Configure 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 configure the configuration on the web **Access Control > Card Setting** interface.



The screenshot shows a configuration interface for RFID. At the top, the word "RFID" is displayed. Below it, there is a label "IC Card Display Mode" and a dropdown menu currently showing "6H3D5D".

Parameter Set-up:

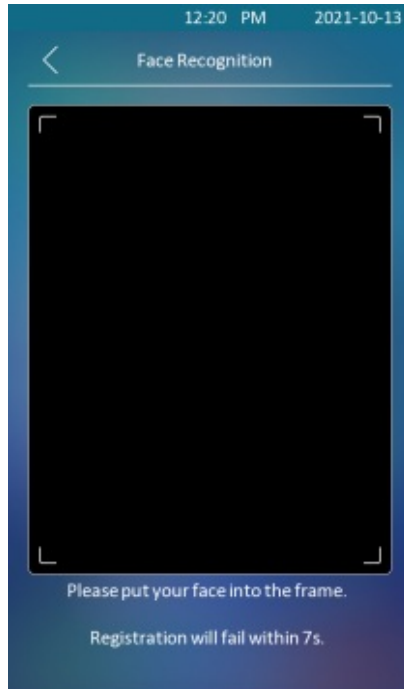
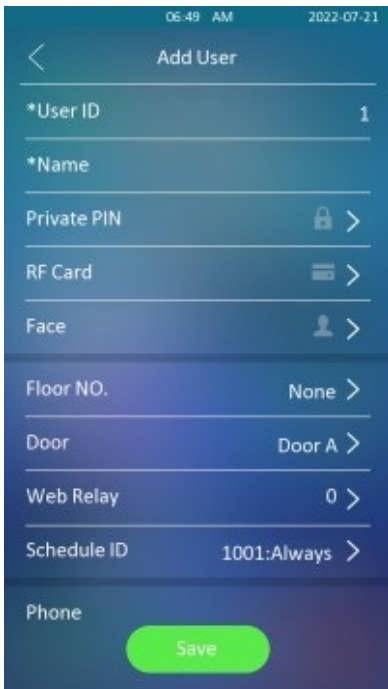
- **IC Card Display Mode:** select the card format for the IC Card for the door access among six format options: 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 8HR10D. The card code format is 8HN by default in the door phone.

Configure Facial Recognition for Door Unlock

Enroll Face Data on the Device

You can enroll face data on the device by entering the user’s name and registering your facial ID on the device for door access.

Tap **User > User List**, then tap **Add**, and **Face**.




Upload Face Data on the Web Interface

You can upload the face data to the device on the web interface.

To do so, go to **Directory > User**, then click **+Add**. After that, upload the face photo.

User

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
 No Data												

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

Face

Status UnRegistered

Photo

Parameter Set-up:

- **Status:** it will show **Registered** when the picture uploaded conforms to the format and standard otherwise it would show **Unregistered** as the default. However, the status will be changed back to **Unregistered** if the picture uploaded is cleared when you press the **Reset**.
- **Photo(jpg/png):** select the picture with jpg or png format to be uploaded to the device.

Note

- Pictures to be uploaded should be in jpg or png format

Configure Facial Recognition

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

To configure the configuration on the web **Access Control > Face Setting** interface.

Face Basic

Facial Recognition Enabled	<input checked="" type="checkbox"/>
Offline Learning Enabled	<input checked="" type="checkbox"/>
Facial Recognition Matching Level	<input type="text" value="Normal"/>
Face Living Recognition Matching Level	<input type="text" value="Close"/>
Facial Recognition Interval (sec)	<input type="text" value="18"/>
No Face Detected Interval (sec)	<input type="text" value="23"/>
Face Detection Distance (M)	<input type="text" value="0"/>

Parameter Set-up:


- **Offline Learning Enabled:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level:** click to select the facial recognition accuracy level among four options: **Low, Normal, High, and Highest**. For example, if you select **Highest**, there will be the least possibility that someone else will be mistaken for you by mistake or in another way round in the facial recognition.
- **Face Living Recognition Matching Level:** select Anti-spoofing level among five options: **Close, Low, Normal, High, Highest**. For example, if you select **Highest** then there will be the least possibility that the device will be fooled by digital images or pictures of any kind.
- **Facial Recognition Interval(Sec):** select the time interval between every two facial recognitions from 1-8 minutes. For example, if you select **5** then you have to wait for 5 min. before you are allowed to perform the facial recognition again.

Configure Door Access Using Configured Files

E16 series door phones allow you to speedily configure user(s)-specific door access in batch by importing the configured all-in-one door access control files incorporating user information, door access type, door access schedule, etc., thus all the door access settings can be done at one stop, saving your time and effort from configuring the door access for users separately when users are large in number. You can go to **Directory > User** interface.

User

User ID/Name/Code Local ALL Search Reset Add Import Export

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
 No Data												

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

Note


- Configured files for facial recognition and the other types of configured door access files are separated with different file forms.

Editing the User(s)-specific Door Access Data

You can search user(s)-specific door access and edit the door access data on the web **Directory > User** interface.

User

User ID/Name/Code Local ALL Search Reset Add Import Export

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
 No Data												

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

Unlock by QR Code

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

You can go to **Access Control > Relay > Open Relay via QR Code**.

Open Relay Via QR Code

Enabled

Note

- The function should work with Akuvox SmartPlus. For more information, please contact Akuvox technical support.

Unlock by Bluetooth

You can also gain the door access by mobile phone with Bluetooth which is used with Akuvox SmartPlus. You can shake the mobile phone close to the access control terminal for the door access. To configure it on web **Access Control > BLE > BLE** interface.

BLE

Enabled	<input type="checkbox"/>
RSSI Threshold	<input type="text" value="0"/> (-85~-50db)
Open Door Interval(Sec)	<input type="text" value="0"/> ▼

Parameter Set-up:

- **RSSI Threshold:** select the signal receiving strength from -85~-50db in absolute terms. The higher value is, the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval:** select the time interval between every two Bluetooth door accesses.

Unlock by NFC

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

Path: **Access Control > Card Setting > NFC**.

NFC

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

Unlock by HTTP Command on Web Browser

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

To configure the configuration on web **Access Control > Relay > Open Relay via HTTP** interface

Open Relay Via HTTP

Enabled	<input type="checkbox"/>
Username	<input type="text" value="0"/>
Password	<input type="password" value="*****"/>

Parameter Set-up:

- **Username:** enter the user name of the device web interface, for example, **admin**.
- **Password:** enter the password for the HTTP command. For example, **12345**.

Please refer to the following example:

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

Note

- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

Unlock by Exit Button by the Door

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.

To configure the configuration on web **Access Control > Input > Input** interface.

Input

Enabled	<input type="checkbox"/>
Trigger Electrical Level	<input type="text" value=""/>
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> TFTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call
HTTP URL	<input type="text" value=""/>
Action Delay	<input type="text" value="0"/> (0~300Sec)
Action Delay Mode	<input type="text" value="Unconditional Execution"/>
Execute Relay	<input type="text" value=""/>
Door Status	High

Parameter Set-up:

- **Trigger Electrical Level:** select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action to Execute:** select the method to carry out the action among five options: **FTP, Email, SIP Call, HTTP, and TFTP.**
- **HTTP URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after you press the button(input is triggered).
- **Action Delay Mode:** if you select **Unconditional Execution**, then action will be carried out when the input is triggered. If you select **Execute If Input Still Triggered**, then the action will be carried out if 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:** set up relays to be triggered by the input.

Unlock by Reception Tab

The Reception button is a tab on the home screen that allows residents and visitors to contact the receptionist or the security guard of the building. They can tap this button to ask for help or access to the door.

To do the configuration, you can go to **Intercom > Basic > Key Setting**.

Key Setting

Reception Enabled	<input type="checkbox"/>
Name	<input type="text" value="0"/>
Number	<input type="text" value="3"/>

Parameter Set-up:

- **Name:** enter the name for the **Reception** icon on the home screen.
- **Number:** enter the SIP/IP number to be called after pressing the **Reception** icon for the door access.

Unlock by DTMF Code

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

To do the extra DTMF configuration on the web interface, you can go to **Account > Advanced >DTMF** interface.

DTMF

Mode	<input type="text" value="RFC2833"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
Payload	<input type="text" value="101"/> (96-127)

Parameter Set-up:

- **Type:** select DTMF type among six options: **Inband, RFC2833,Info, Info+Inband,Info+RFC2833, and Info+Inband+RFC2833** according to your need.
- **How to Notify DTMF:** select among four options: **Disable, DTMF, DTMF-Relay, and Telephone-Event** according to your need.
- **DTMF Payload:** select the payload 96-127 for data transmission identification.

Note

- Please refer to the chapter **Configure DTMF Data Transmission** for the specific DTMF code setting.
- Intercom devices involved must be consistent in the DTMF type otherwise DTMF code cannot be applied.

Configure DTMF White List

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

Open Relay Via DTMF

Assigned The Authority For

Only Tenants List

Body Temperature Measurement for Door Access (Optional)

The body temperature measurement function allows the door phone measures body temperature and checks masks for safety. When enabled, the door phones only opens the door for residents or visitors who pass the test.

Body Temperature Measurement Configuration

You can configure the body temperature measurement function in terms of defining the normal temperature as well as making the schedule for the validity of the function etc. To configure the configuration on web **Access Control > Body Temperature > Measuring Body Temperature** interface.

Mode	<input type="text" value="Disabled"/>	
Mask Detection	<input type="text" value="Disabled"/>	
Temperature Unit	<input type="text" value="Fahrenheit"/>	
Normal Body Temperature	<input type="text" value="99.14"/>	(Below 99.14°F)
Low Temperature	<input type="text" value="93.20"/>	(Below 93.20°F)
	(If the detected temperature is lower than 93.20 °F, the device will prompt low temperature, please try again later)	
Action For Abnormal Body Temperature	<input type="text" value="Access Denied"/>	
Action For Low Body Temperature	<input type="text" value="Try Again Later"/>	
Action To Execute	<input type="checkbox"/> SIP/ IP Call	
SIP/ IP Call Number	<input type="text"/>	

Parameter Set-up:

- **Mode:** select either **Disabled Mode**, **Forehead Mode** or **Wrist Mode** for temperature measurement according to your need. The device can be installed with a digital forehead temperature detector therefore you can are required to set the mode properly according to your application.
- **Mask Detection:** select **Disable** if you want to turn off the mask detection. Select **Set mask-wearing as mandatory** and the device will check if the visitor is wearing a mask or not while reminding the visitor with the announcement **Please wear a mask**. Select **Display mask-wearing prompt** and the device will display the mask-wearing prompt only without making the mask-wearing mandatory. A warning alarm will be triggered when the body temperature measured is detected higher than the defined normal body temperature.
- **Normal Body Temperature:** set the body temperature to the predefined body temperature as the measuring basis in either Fahrenheit or Celsius. For example, if you set

the temperature at 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, while the temperature is lower than 34 degrees celsius will be deemed as low body temperature.

- **Low Temperature:** set the low temperature.
- **Action For Abnormal Body Temperature:** if you select **Access Denied** then anyone who is detected with abnormal body temperature will be denied the door access. If you select **Just For Reminder** then anyone with abnormal body temperature will still be granted the door access.
- **Action for Low Body Temperature:** if **Try again later** is selected, you will be denied the door access with the prompt **Try again later** for the low body temperature. If you select **Just For Reminder** then anyone with low body temperature will still be granted the door access.
- **Action to Execute:** check the box to enable or disable the SIP/IP Call. If you want to be notified via SIP/IP call when abnormal temperature and low temperature are detected.
- **SIP/IP Call Number:** enter the SIP or IP call for the notification. The field will appear for you to fill in SIP/IP numbers when you check the box in the **Action to Execute**.

Security

Tamper Alarm Setting

The tamper alarm function prevents anyone from removing the devices without permission. It does this by setting off the tamper alarm and making calls to a designated location when the device detects a change in its gravity value from the original one.

To configure the configuration on web **System > Security > Tamper Alarm** interface.

Tamper Alarm	
Enabled	<input checked="" type="checkbox"/> Disarm
Key Status	High

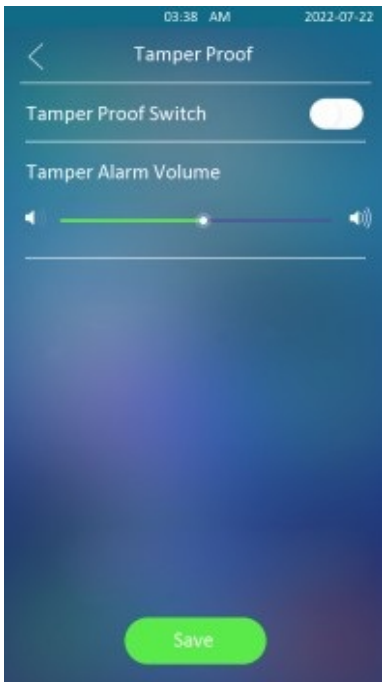
Parameter Set-up:

- **Enable:** tick the check box to enable the tamper alarm function. When the tamper alarm goes off, you can press the **Disarm** tab beside the check box to clear the alarm.
- **Key Status:** when the tamper alarm button pops up, then the status will be changed from low to high. The normal state is high.

Note

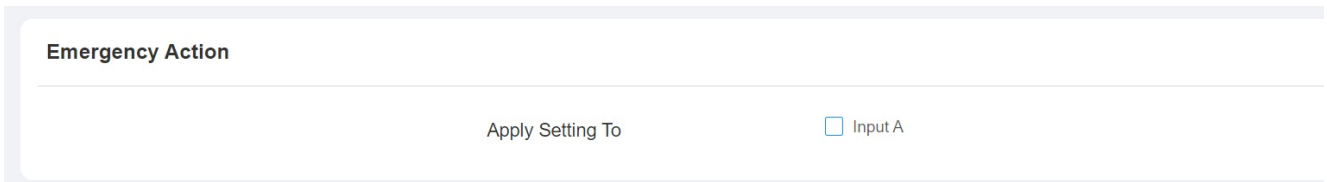
- **Disarm** tab will turn gray when the tamper alarm is cleared.
- The round rubber button at the back of the device must be in press-down status otherwise the alarm will not be fired.

To turn on the tamper-proof function on the device, tap **Security > Tamper Proof**.



Emergency Action

You can keep the door open when emergency happens. Go to **System > Security > Emergency Action**.



Note

- This function needs to work with Akuvox Cloud.

Security Notification Setting

Email Notification Setting

Set up email notification to receive screenshots of unusual motion from the door phone.

To configure the configuration on web **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" value="....."/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
Email Test	<input type="button" value="Test Email"/>

Parameter Set-up:

- **Sender's Email Name:** enter the name of the email sender.
- **Sender's Email Address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's Email Address:** enter the receiver's email address.
- **Receiver's Email Name:** enter the name of the email receiver.
- **SMTP Server Address:** enter the SMTP server address of the sender.
- **Port:** enter the port number from which the email is sent out.
- **SMTP User Name:** enter the SMTP user name, which is usually the same as the sender's email address.
- **SMTP Password:** configure the password of the SMTP service, which is the same as the sender's email address.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the email contents according to your need.

FTP Notification setting

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

To configure the configuration on web **Setting > Action > FTP Notification** interface.

FTP Notification

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

Parameter Set-up:

- **FTP Server:** enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name:** enter the FTP server user name.
- **FTP Password:** enter the FTP server password.
- **FTP Path:** enter the folder name you created in the FTP server.

TFTP Notification Setting

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

To configure the configuration on web **Setting > Action > TFTP Notification** interface.

TFTP Notification

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

Parameter set-up:

- **TFTP Server:** enter the address (URL) of the TFTP server for the FTP notification.

SIP Call Notification

If you want to receive the security notification via SIP call, you can configure the FTP notification on the web interface properly. Path: **Setting > Action > SIP Call Notification**.

SIP Call Notification

SIP Call Number	<input type="text"/>
SIP Caller Name	<input type="text"/>

Parameter set-up:

- **SIP Call Number:** enter the SIP call number IP number.
- **SIP Caller Name:** enter the name of the called party.

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 configure the configuration on web **System > Security > Session Time Out** interface.

Session Time Out

Session Time Out Value	<input type="text" value="300"/>	(60~14400Sec)
------------------------	----------------------------------	---------------

Parameter Set-up:

- **Session Time Out Value:** set the automatic web interface logout timing ranging from 60 seconds to 14400 seconds. The default value is 300.
- **TFTP Server:** enter the address (URL) of the TFTP server for the FTP notification.

Action URL

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

Akuvox Action URL:

No	Event	Parameter format	Example
1	Make Call	\$remote	Http://server ip/ Callnumber=\$remote
2	Hang Up	\$remote	Http://server ip/ Callnumber=\$remote
3	Relay Triggered	\$relay1 status	Http://server ip/ relaytrigger=\$relay1 status
4	Relay Closed	\$relay1 status	Http://server ip/ relayclose=\$relay1 status
5	Input Triggered	\$input1 status	Http://server ip/ inputtrigger=\$input1 status
6	Input Closed	\$input1 status	Http://server ip/ inputclose=\$input1 status
7	Valid Code Entered	\$code	Http://server ip/ validcode=\$code
8	Invalid Code Entered	\$code	Http://server ip/ invalidcode=\$code
9	Valid Card Entered	\$card_sn	Http://server ip/ validcard=\$card_sn
10	Invalid Card Entered	\$card_sn	Http://server ip/ invalidcard=\$card_sn
11	Tamper Alarm Triggered	\$alarm status	Http://server ip/tampertrigger=\$alarm status

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

[mac=\\$mac:ip=\\$ip:model=\\$model:firmware=\\$firmware:card_sn=\\$card_sn](http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

You can navigate to **Setting > Actions URL**

Note

- Action URL and format are provided by a third-party manufacturer, Akuvox door phone only sends the URL to the third-party devices.

Action URL

Enabled

Make Call

Hang Up

Relay Triggered

Relay Closed

Input Triggered

Input Closed

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

Tamper Alarm Triggered

Valid Face Recognition

Invalid Face Recognition

Monitor and Image

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

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

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

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

MJPEG Image Capturing

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 configure the configuration on web **Surveillance > MJPEG > MJPEG Server** interface.

MJPEG Server

Enabled	<input checked="" type="checkbox"/>
Image Quality	<input type="text" value="VGA"/>

Parameter Set-up:

- **Image Quality:** select the quality for the image capturing among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P.**

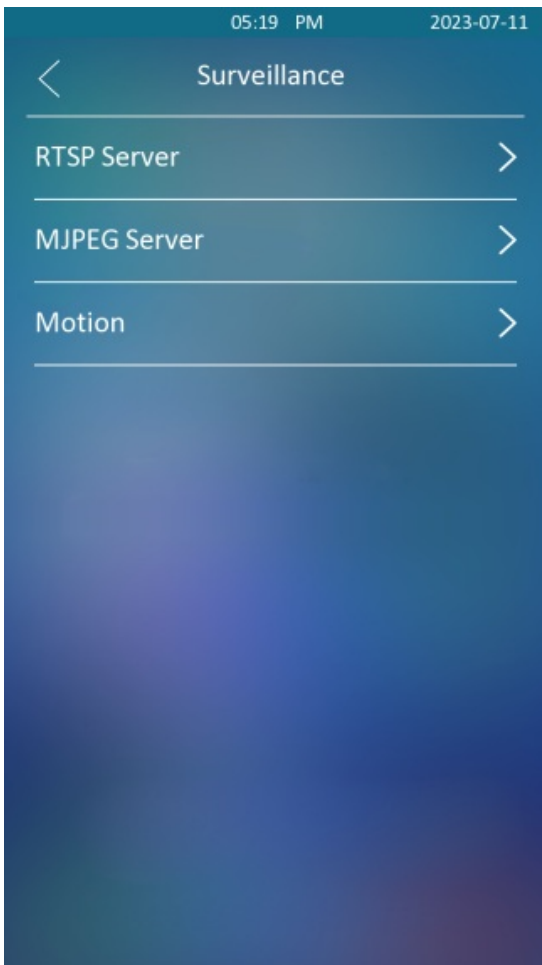
After the MJPEG service is enabled, you can capture the image from the door phone using the following three types of URL format:

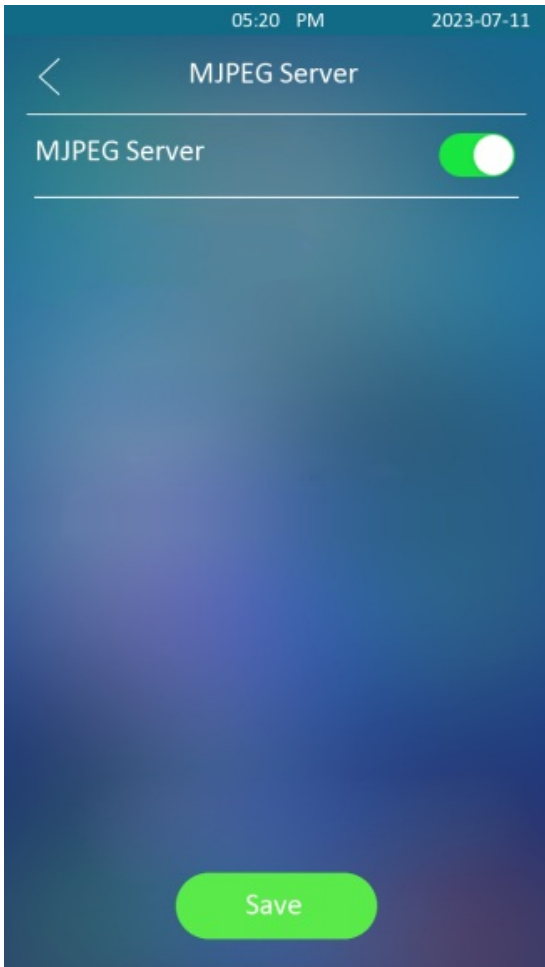
- `http:// device ip:8080/picture.cgi`

- <http://deviceip:8080/picture.jpg>
- <http://deviceip:8080/jpeg.cgi>

For example, if you want to capture the jpg format image of a door phone with the IP address: 192.168.1.104, you can Enter “<http://192.168.1.104:8080/picture.jpg>” on the web browser.

You can also enable the MJPEG server on the device directly. Tap **Advanced > Surveillance > MJPEG server**.



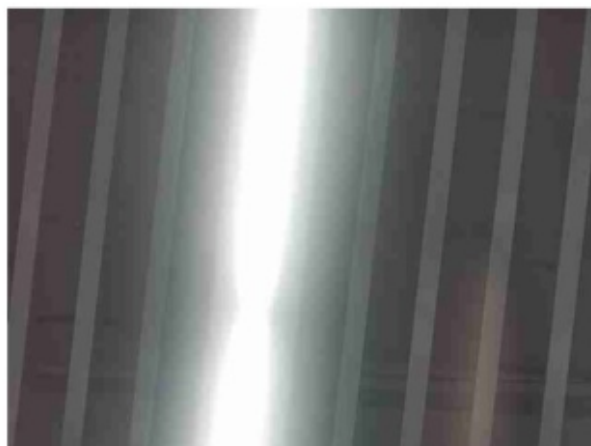


Live Stream

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.

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

Live Stream



To check the real-time video using a URL, you can Enter the correct URL (**http://IP_address:8080/video.cgi**).

For example **http://192.168.2.5:8080/video.cgi**



RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

You are required to set up the RTSP function in terms of RTSP Authorization, authentication, password, etc. before you are able to use the function. To configure the configuration on web **Surveillance > RTSP > RTSP Basic** interface.

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
Authorization Enabled	<input type="checkbox"/>
Authorization Mode	<input type="text" value="Digest"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>

Parameter Set-up:

- **Authorization Enabled:** tick the check box to enable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, and RTSP Password on the intercom device such as an indoor monitor for authorization.
- **Authentication Mode:** select RTSP authentication type between **Basic** and **Digest**. **Basic** is the default authentication type.
- **Username:** enter the name used for RTSP authorization.
- **Password:** enter the password for RTSP authorization.

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 configuration on web **Surveillance > RTSP > H.264 Video Parameters** interface.

H.264 Video Parameters

Video Resolution	4CIF	▼
Video Framerate	25 fps	▼
Video Bitrate	2048 kbps	▼
2nd Video Resolution	VGA	▼
2nd Video Framerate	25 fps	▼
2nd Video Bitrate	512 kbps	▼
Video Crop	Default	▼

[Edit](#)

Parameter Set-up:

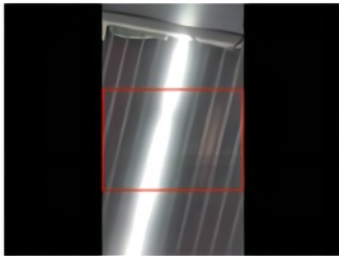
- **Video Resolution:** select video resolutions among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, and 1080P**. The default video resolution is **720P**, and the video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than **720P**.
- **Video Framerate:** **25fps** is the video frame rate by default.
- **Video Bitrate:** select video bit-rate among six options: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps** according to your network environment.

The default video bit rate is **2048 kbps**.

- **2nd Video Resolution2**: select video resolution for the second video stream channel. While the default video solution is **VGA**.
- **2nd Video Framerate**: select the video framerate for the second video stream channel. **25fps** is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate**: select video bit rate among the six options for the second video stream channel. While the second video stream channel is **512 kbps** by default.
- **Video Crop**: select **Original** for the full-screen video display. And select **Default** if you only want to select the specific area on the video to be displayed. You can click **Edit** to start video cropping.

Video Crop Default ▼ Edit

Detection Area



The Start Of Detected Area (%) 34 Apply Cancel

Note

- E16 series supports two video stream channels for H.264 codec video stream.

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.

To configure the configuration on web **Surveillance > ONVIF** interface.

Basic Setting

Discoverable	<input type="checkbox"/>
Username	<input type="text" value="1"/>
Password	<input type="password" value="•"/>

Parameter Set-up:

- **Discoverable:** tick the check box to turn on the ONVIF mode. If you select a video from the door phone camera can be searched by other devices. ONVIF mode is **Discoverable** by default.
- **UserName:** enter the user name. The user name is **admin** by default.
- **Password:** enter the password. The password is **admin** by default.

After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream.

For example: **http://IP address:80/onvif/device_service**

Note

- Fill in the specific IP address of the door phone in the URL

Camera Mode

You can select the camera mode for better video quality depending on where the door phone is located. You can select Indoor mode for better video image(RTSP, ONVIF, and Mjpeg) if the door phone is placed indoors. On the contrary, you can select **Outdoor** mode if the door phone is placed outdoors.

Camera

Mode	<input type="text" value="Outdoor"/>
------	--------------------------------------

Logs

Call Logs

If you want to check on the calls inclusive of the dial-out calls, received calls, and missed calls in a certain period of time, you can check and search the call log on the device web interface and export the call log from the device if needed.

To check the call log, you can go to **Status > Call Log**.

Call Log

Save Call Log Enabled

<input type="checkbox"/>	Index	Type	Date	Time	Local Identity	Name	Number
<input type="checkbox"/>	1	Dialed	2023-07-10	10:05:07	192.168.35.122@192.168.35.122	192.168.33.51	192.168.33.51@192.168.33.51
<input type="checkbox"/>	2	Dialed	2023-07-10	09:52:02	192.168.35.122@192.168.35.122	192.168.33.51	192.168.33.51@192.168.33.51
<input type="checkbox"/>	3	Dialed	2023-07-10	09:08:12	192.168.35.122@192.168.35.122	192.168.33.51	192.168.33.51@192.168.33.51

Parameter Set-up:

- **Call History:** select call history among four options: **All, Dialed, Received, and Missed** for the specific type of call log to be displayed.
- **Start Time ~ End Time:** select the specific time span of the call logs you want to search, check, or export.
- **Local Identity:** displays the door phone's SIP account or IP number that receives incoming calls.
- **Name/Number:** select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

Door Logs

If you want to search and check on the various types of door access history, you can search and check the door logs on the device's web.

To check door logs, go to **Status > Access Log**.

Door Log

Save Door 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
<input type="checkbox"/>	1	-	Visitor	-		Face	2023-07-10	10:04:57	Failed	Picture
<input type="checkbox"/>	2	-	Visitor	-		Face	2023-07-10	08:24:48	Failed	Picture
<input type="checkbox"/>	3	-	Visitor	-		Face	2023-07-10	08:24:46	Failed	Picture
<input type="checkbox"/>	4	-	Visitor	-		Face	2023-07-10	08:24:45	Failed	Picture
<input type="checkbox"/>	5	-	Visitor	-		Face	2023-07-10	08:24:42	Failed	Picture

Parameter Set-up:

- **Status:** select between **Success** and **Failed** options to search for successful door accesses or Failed door accesses.
- **Time:** select the specific time span of the door logs you want to search, check, or export.
- **Name/Code:** select the **Name** and **Code** options to search door log by the name or by the PIN code.
- **Action:** click to display the picture captured.

Temperature Log

To check the temperature log, go to **Status > Temperature Log**.


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

Parameter Set-up:

- **Save Picture Enabled:** enable it if you want to save the temperature measuring

snapshot.

- **Export Picture Enabled:** enable it if you want to export the temperature log with a snapshot picture captured.
- **Time:** select the specific time span of the temperature log you want to search, check, or export.
- **Action:** click to display the picture captured.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

You can set up the function on the web **System > Maintenance > System Log** interface.

System Log

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

Parameter Set-up:

- **Log Level:** select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3, the higher the level is 5, the more complete the log is 7.
- **Export Log:** go to the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Log Enabled:** select **Enable** or **Disable** if you want to enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the device log.

PCAP for Debugging

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

You can set up the PCAP on the device web **System > Maintenance > PCAP** properly before using it.

PCAP

Specific Port	<input type="text"/>	(1-65535)
PCAP	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Export"/>	
PCAP Auto Refresh Enabled	<input type="checkbox"/>	

Parameter Set-up:

- **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:** go to the start tab and Stop tab to capture a certain range of data packets before going to the Export tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** select Enable or Disable to turn on or turn off the PCAP auto refresh function. If you set it as Enable then the PCAP will continue to capture data packets even after the data packets reached their 1M maximum in capacity. If you set it as Disable the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

Remote Debug Server

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

To configure the server, go to **System > Maintenance > Remote Debug Server**.

Remote Debug Server

Enabled	<input type="checkbox"/>	
Connect Status	Disconnected	
IP Address	<input type="text" value="/cdor.cgi?open=0&door=\$floor"/>	
Port	<input type="text" value="/cdor.cgi?open=8"/>	(1024-65535)

Parameter Set-up:

- **Connect Status:** display the remote debug server connection status.
- **IP Address:** enter the remote debug server IP address. Please ask Akuvox technical team

for the server IP address.

- **Port:** type in the remote debug server port.

Face Recognition Debug

You might be required to enable face recognition to debug when you have a face recognition problem. To enable it, go to **System > Maintenance > Others**.

Others

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

User Agent

SIP user agent (UA) is an endpoint device that supports SIP, which is used to establish connections and enable sessions between two endpoint devices. And a UA is comprised of UAC (User Agent Client) and UAS (User Agent server) with the UAC used to issue requests and UAS used to issue responses. UA acts as a SIP service provider for the specific user (device). You can customize the user agent field in the SIP message. If the user agent is set to a specific value, users can see the information from PCAP. If a user agent is blank, by default, users can see the company name “Akuvox”, model number, and firmware version from PCAP. Path: **Account > Advanced > User Agent** interface.

User Agent

User Agent	<input type="text"/>
------------	----------------------

Parameter Set-up:





- **User Agent:** support to enter another specific value, Akuvox is by default.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

You can go to **System > Upgrade**.

Basic

Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

Note

- Firmware files should be in **.zip format** for an upgrade.

Backup

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

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

Others

Config File

 Import

 Export

(Encrypted)

Facial Debug Enabled

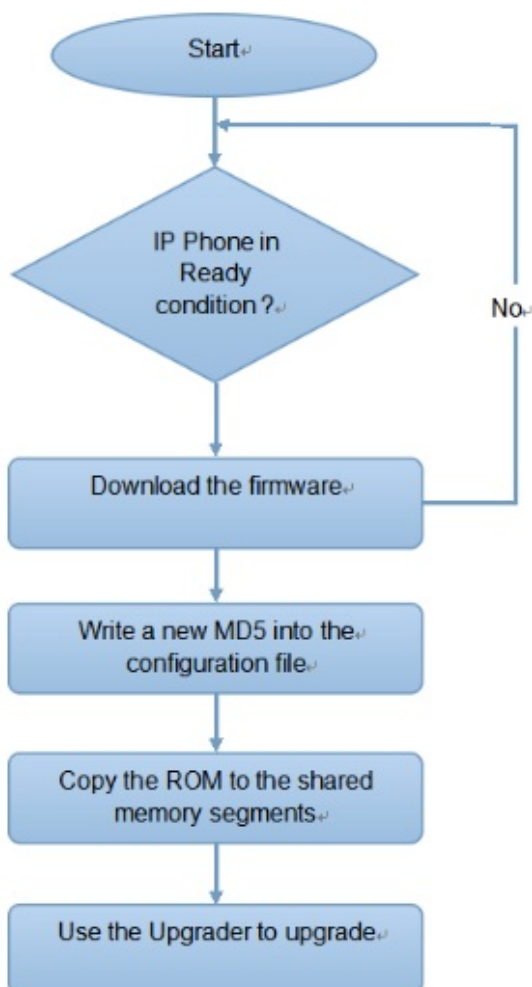
Auto-provisioning via Configuration File

You can configure and upgrade the door phone on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

Configuration files have two formats for auto-provisioning. One is the general configuration files used for the general provisioning and the other one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown below:

- **General configuration provisioning:** a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files are used for auto-provisioning on a specific device, as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

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.

You can go to **System > Auto Provisioning > Automatic Autop**.

Automatic Autop

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0~23Hour)
	<input type="text" value="0"/> (0~59Min)
Clear MD5	<input type="button" value="Clear"/>
Export Autop Template	<input type="button" value="Export"/>

Parameter Set-up:

- **Power On:** select **Power on** if you want the device to perform Autop every time it boots up.
- **Repeatedly:** select **Repeatedly**, if you want the device to perform Autop according to the schedule you set up.
- **Power On + Repeatedly:** select **Power On + Repeatedly** if you want to 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:** select **Hourly Repeat** if you want the device to perform Autop every hour.

PNP Configuration

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

To configure the configuration on the web **System > Auto Provisioning > PNP Option** interface.

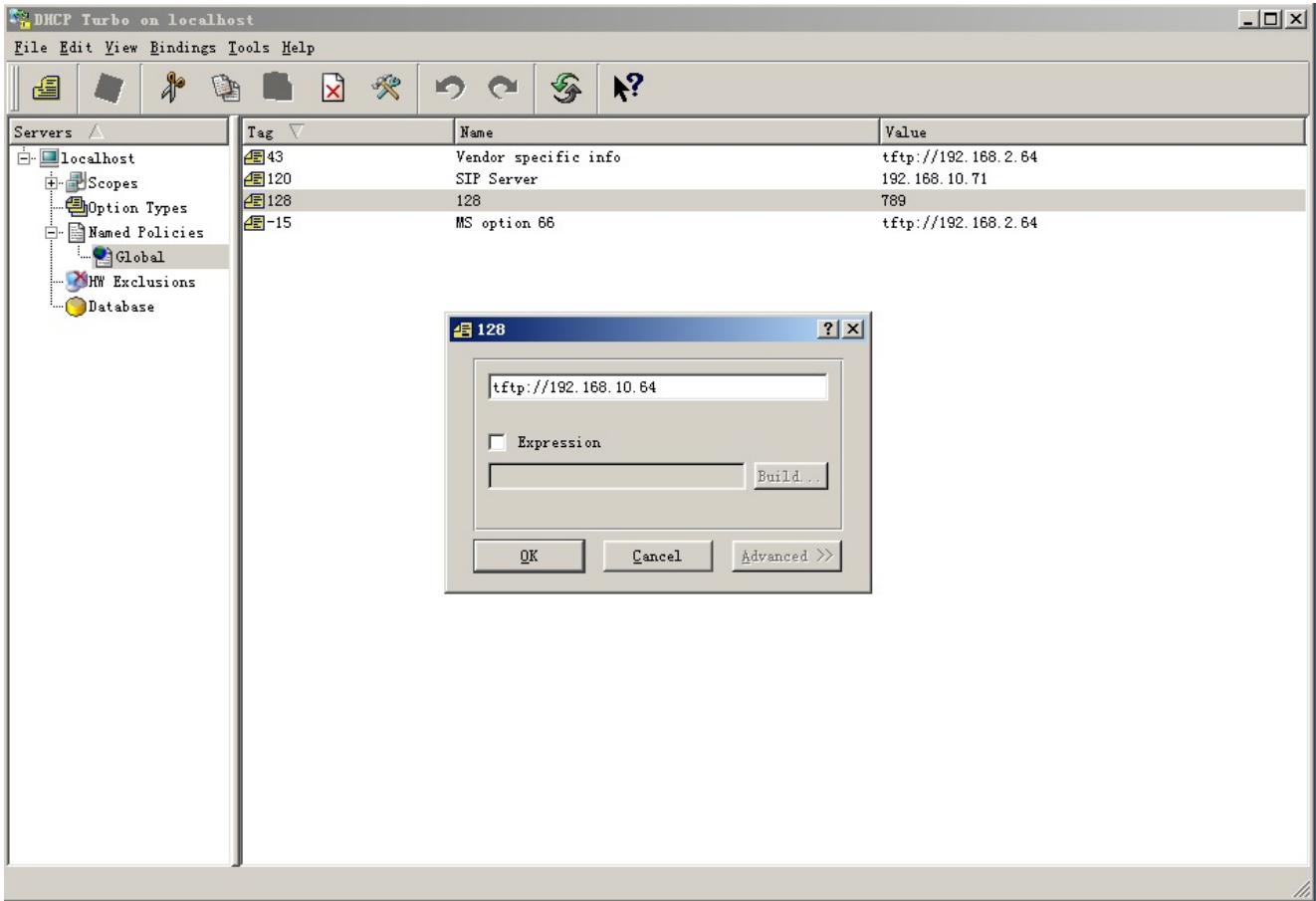
PNP Option

PNP Config Enabled



DHCP Provisioning Configuration

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 TFTP server.

To set up DHCP AutoP with “Custom Option” and “Power on” mode, on web **System > Auto Provisioning > Automatic Autop** interface. Click **Export** tab in **Export Autop Template** to export Autop template. Then set up DHCP Option on DHCP server.

Automatic Autop

Mode	<input type="text" value="Power On"/>	
Schedule	<input type="text" value="Sunday"/>	
	<input type="text" value="22"/>	(0-23Hour)
	<input type="text" value="0"/>	(0-59Min)
Clear MD5	<input type="button" value="Clear"/>	
Export Autop Template	<input type="button" value="Export"/>	

DHCP Option

Custom Option	<input type="text"/>	(128-254)
---------------	----------------------	-----------

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

Parameter Set-up:

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

Note

- The general configuration file for the in-batch provisioning is with the format `rcfg` taking E16 as an example `r000000000116.cfg` (9 zero in total while the MAC-based configuration file for the specific device provisioning is with the format `MAC_Address of the device.cfg`), for example, `0C110504AE5B.cfg`.

Static Provisioning Configuration

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 download the Autop template on **System > Auto Provisioning > Automatic Autop**, and setup Autop server on **System > Auto Provisioning > Manual Autop** interface.

Automatic Autop

Mode	<input type="text" value="Power On"/>	▼
Schedule	<input type="text" value="Sunday"/>	▼
	<input type="text" value="22"/>	(0-23Hour)
	<input type="text" value="0"/>	(0-59Min)
Clear MD5	<input type="button" value="Clear"/>	
Export Autop Template	<input type="button" value="Export"/>	

Manual Autop

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Common AES Key	<input type="password" value="*****"/>
AES Key(MAC)	<input type="password" value="*****"/>
	<input type="button" value="AutoP Immediately"/>

Parameter Set-up:

- **URL:** set up TFTP, HTTP, HTTPS, and FTP server addresses for the provisioning.
- **User Name:** set up a user name if the server needs a user name to be accessed otherwise leave it.
- **Password:** set up a password if the server needs the password to be accessed otherwise leave it.
- **Common AES Key:** set up AES code for the intercom to decipher the general Auto

Provisioning configuration files.

- **AES Key (MAC):** set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Tip

- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.

Note

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

Integration with Third Party Device

Integration via Wiegand

The Wiegand feature enables Akuvox door phone to act as a controller or a card reader.

To configure it, you can go to the web **Device > Wiegand** interface.

Wiegand

Wiegand Display Mode	8H10D ▼
Wiegand Card Reader Mode	Wiegand-26 ▼
Wiegand Transfer Mode	Output ▼
Wiegand Input Data Order	Compatible ▼
Wiegand Output Data Order	Compatible ▼
Wiegand Output CRC Enable	<input checked="" type="checkbox"/>

Parameter Set-up:

- **Wiegand Display Mode:** select Wiegand Card code format among **8H10D; 6H3D5D; 6H8D; 8HN; 8HR,RAW,8HR10D**.
- **Wiegand Card Reader Mode:** set the Wiegand data transmission format among three options: **Wiegand 26, Wiegand 34, Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode:** set the Transfer mode between **Input, Output** or **Convert To Card NO.Output** if the door phone is used as a receiver, then set it as **Input** for the door phone and vice versa.
- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Default** and **Compatible** if you select **Compatible** then the input card number will be reversed and vice versa.
- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Default** and **Compatible**. If you select **Compatible**, then the input card number will be reversed and vice versa.
- **Wiegand Output CRC:** this function is used for Wiegand data inspection. It is turned on by default. If it is not turned on, you might not be able to integrate the device with third-party

devices.

Integration via HTTP API

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

You can configure the HTTP API function on the web **Setting > HTTP API** interface for the integration.

HTTP API

HTTP API Enable	<input checked="" type="checkbox"/>
Authorization Mode	Allowlist ▼
Username	admin
Password
1st IP	<input type="text"/>
2nd IP	<input type="text"/>
3rd IP	<input type="text"/>
4th IP	<input type="text"/>
5th IP	<input type="text"/>

Parameter Set-up:

- **HTTP API Enable:** HTTP API Enables or disables the HTTP API function for third-party integration. For example, if the function is disabled, any request to initiate the integration will be denied and HTTP 403 forbidden status will be returned.
- **Authorization Mode:** select among five 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** and **Digest** authorization mode is selected. The default user name is Admin.
- **Password:** enter the password when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **1stIP- 5th IP:** enter the IP address of the third-party devices when the **WhiteList** authorization is selected for the integration.

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Allow List	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
3	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
4	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In 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 <u>Akuvox</u> developer only.

Lift Control

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

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

Lift Control List

Lift Control List

None ▼

Parameter Set-up:

- **Lift Control List:** select integration mode among seven Options: **None, OSDP, Akuvox EC32, KEYKING**. The detail for the options will be provided in the following chart.

NO.	Integration Mode	Description
1	None	If you select None then the RS485 integration will be disabled.
2	OSDP	If you select OSDP Mode, then the integration communication between the E16 series door phone and the third-party device is via OSDP protocol. You are required to check for Select KEYKING if you want to integrate with the KEYKING lift controller. the device integration protocol and make sure that they use the same integration protocol.
3	Akuvox EC32	Select Akuvox EC32 if you want to connect the device with the Akuvox EC32 lift controller.
4	KEYKING	Select KEYKING if you want to integrate with the KEYKING lift controller.

Integrate with Third-party Access Control Server

You can access the door phone using the QR code or access card generated by a third-party server. For example, when you use the QR code on the door phone, the QR code will be sent to the third-party server for verification. And you will be granted access if the QR code passes the verification. To configure it, you can go to **Access Control > Relay > Third Party Integration**.

Third Party Integration

List	<input type="text" value="General"/>
HTTP URL	<input type="text" value="3"/>
Device ID	<input type="text"/>

Parameter Set-up:

- **List:** select the integration modes.
 - If you want to disable the function, select **None**.
 - If you want to use QR code only, select **General**.
 - If you want to select between a QR code and an access card with customized features, select **Customize**.
- **HTTP URL:**
 - For **General** mode: enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before its being sent to the QR code server for verification. See the example below: `http://wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode} &deviceId={DeviceID}`

- For Customize mode: select the QR code or Card verification.
- For QR code verification: enter the QR code HTTP command provided by the third-party service provider. See the example below:
`/hs/ACS/checking/QR">http://www.server.com//hs/ACS/checking/QRCode/{DeviceID}/{Card}`
- For Card verification: enter the access card HTTP command, provided by the third-party service provider. See the example below:
`http://www.server.com//hs/ACS/checking/{QRCode}/{DeviceID}/Card`
- **Prompt On LCD:** select **Default**, if you want to adopt the Akuvox door phone prompt for the door access. Select **Return** value, if you want to use the return value from the third-party server as the prompt.
- **Remote Verification:** select **QR code** or **Card** verification.
- **Device ID:** enter your device ID, which will be added to the HTTP command automatically when you use a QR code or card for access.

Password Modification

You can set and change both the System PIN Code for accessing the device setting and the login password for accessing the web interface. In addition, you can also select the user role when setting passwords.

To set the password, go to **System > Security > Web Password Modify**

System » [Security](#)

Web Password Modify

Username [Change Password](#)

Account Status

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

Change Password X

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	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

To set up the system PIN code, you can go to the **system PIN** section.

System PIN

PIN Code

System Reboot&Reset

Reboot

If you want to restart the device system, you can operate it on the device web interface as well. Moreover, you can set up a schedule for the device to be restarted.





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

Reboot Schedule

Mode	<input type="checkbox"/>
Schedule	Every Day ▼
	0 (0~23Hour)

To reboot the device manually, go to **System > Upgrade > Basic**.

Basic

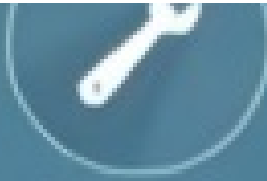
Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

To reboot the device, tap **Advanced > Reboot**.





Surveillance



Reset







Reboot

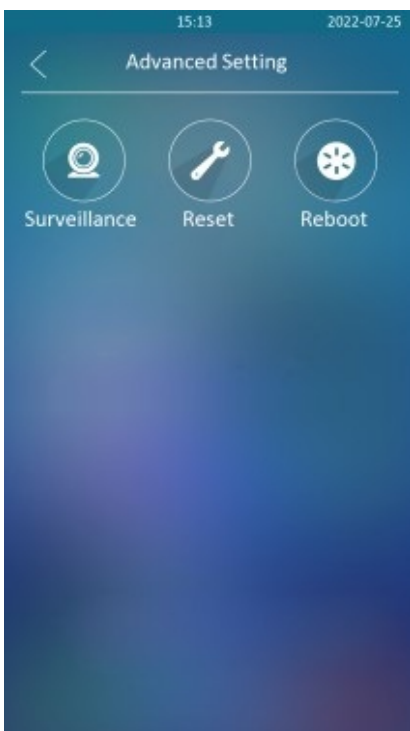
Reset

You can select **Reset To Factory Setting** if you want to reset the device (deleting both configuration data and user data such as RF cards, face data, and so on). Or, select **Reset Configuration to Default State (Except Data) Reset**, if you want to reset the device (retaining the user data).

To reset the device, go to **System > Upgrade**.

Basic	
Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

To reset the device to the factory setting on the device, go to **Advanced > Reset**.

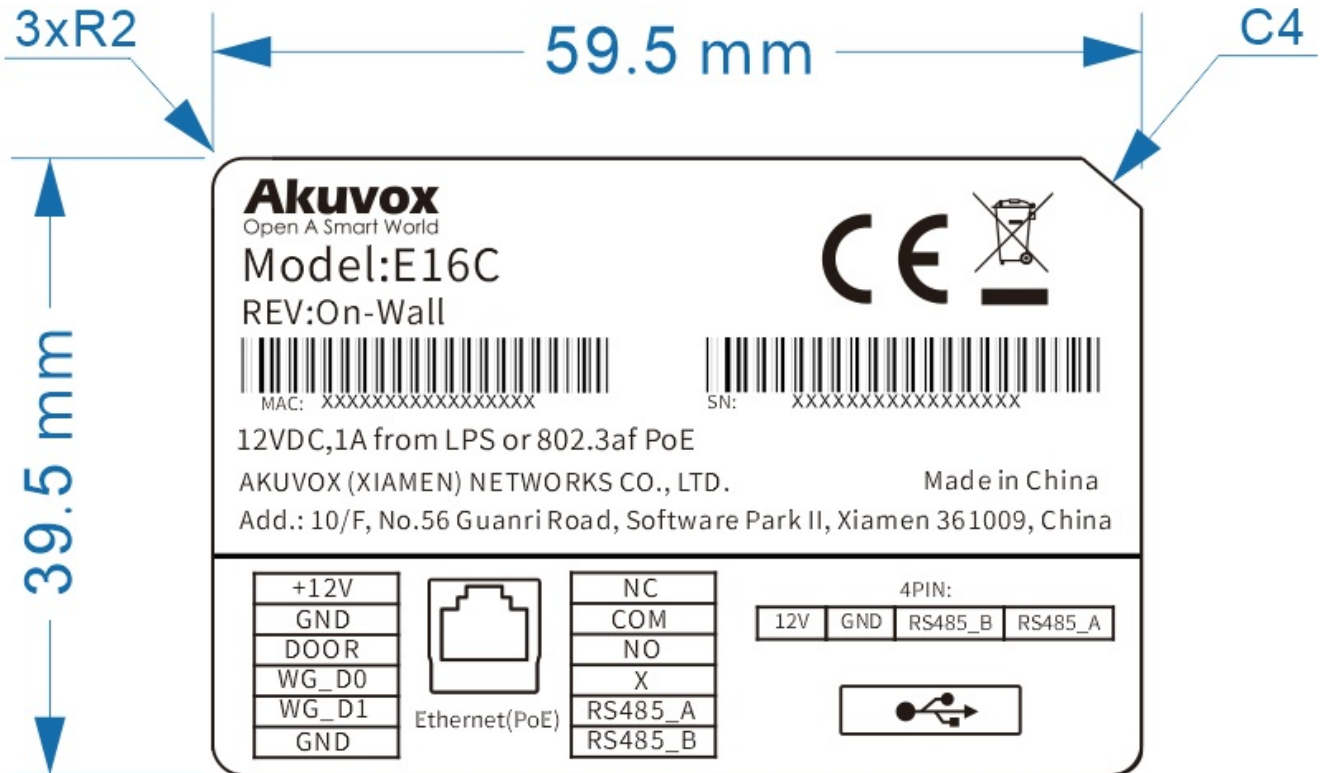


FAQ

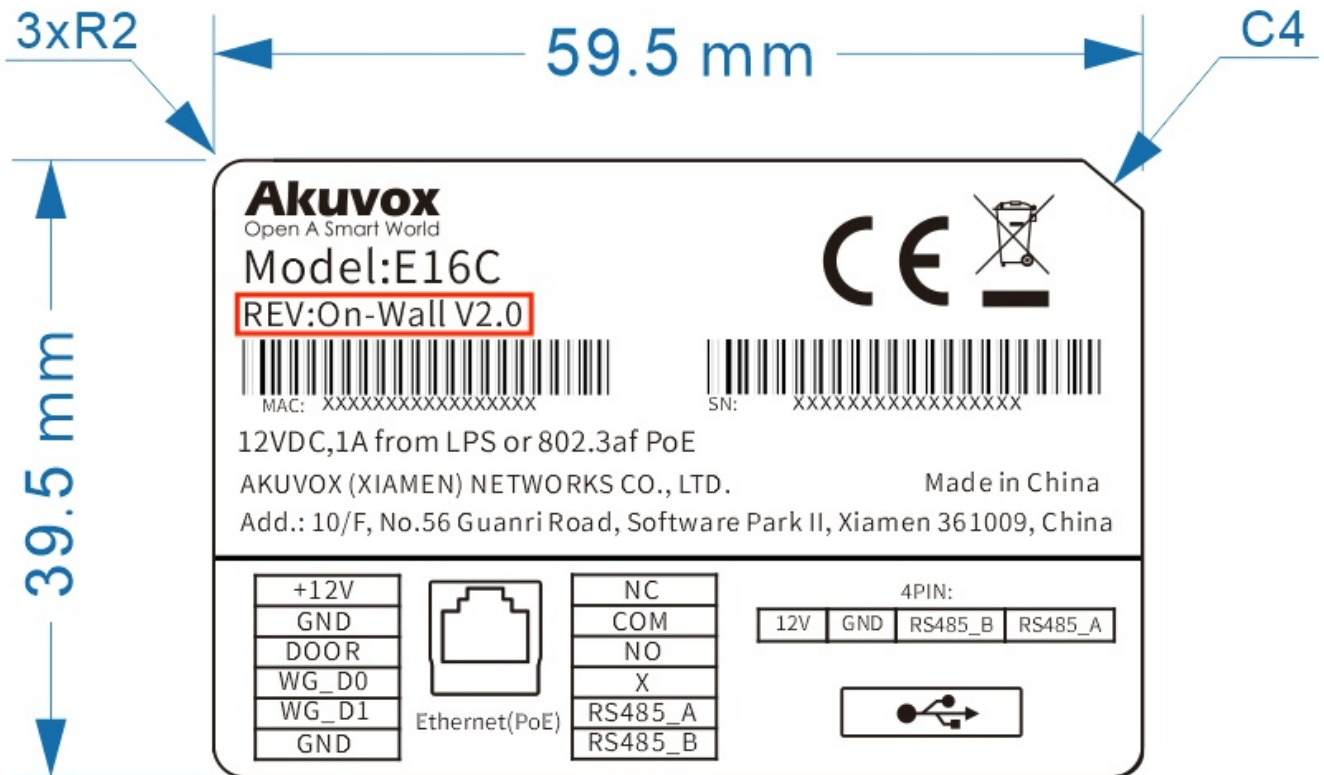
Q: How to confirm whether my device is hardware version 1 or hardware version 2?

A: 1. Label

- Hardware version 1



- Hardware version 2



- Firmware Version

The firmware is different between hardware version1 and hardware version2.

Go to **Web > Status > Firmware Version**

116.X.X.X is hardware version1.

216.X.X.X is hardware version2.

- Hardware version

The firmware is different between hardware version 1 and hardware version 2.

Go to **Web > Status > Firmware Version**

If the hardware version is 216.X, then the device is the hardware version 2.

Firmware Version

216.30.0.67

Hardware Version

216.0.9.0.0.0.0.0