

## About This Manual



[WWW.AKUVOX.COM](http://WWW.AKUVOX.COM)



# AKUVOX X912S DOOR PHONE Administrator Guide

Thank you for choosing Akuvox X912 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual is written based on 912.30.1.118 version, and it provides all the configurations for the functions and features of X912 series door phone. Please visit [Akuvox forum](#) or consult technical support for any new information or latest firmware.

# Product Overview












Akuvox X912 is a Linux IP video door phone with a 4 inch touch screen and physical keypad. It incorporates audio and video communications, access control and video surveillance. Its finely tuned Linux OS, Cloud and AI based communication technology allow featured customization to better suit your operation habit. X912 has multiple ports, such as RS485 and Wiegand ports, which can be used to easily integrate external digital systems, such as lift controller and fire alarm detector, helping to create a holistic control of the building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, Facial recognition NFC, Bluetooth, QR code. X912 series door phone is applicable to mid-end and upscale residential buildings, and upscale single-tenant residential buildings.

# Introduction to Configuration Menu

- **Status:** this section gives you basic information such as product information, Network Information, call log, and door log, etc.
- **Account:** this section concerns SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, etc.
- **Network:** this section mainly deals with DHCP&Static IP setting, RTP port setting, and device deployment, etc.
- **Intercom:** this section covers Intercom settings, call feature, and dial plan.
- **Surveillance:** this section covers Motion Detection, RTSP, MJPEG, ONVIF, Live stream, etc.
- **Access Control:** this section covers Input control, Relay, Card settings, Face Recognition settings, Private PIN Code, etc.
- **Directory:** this section involves user management, RF card, PIN, Face recognition management, and contact management.
- **Device:** this section includes Light settings, LCD settings and Audio settings, lift control, Wiegand connection.
- **Setting:** this section includes time&language, action settings, schedule for access control, screen display, HTTP API.
- **System:** this section covers firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault diagnosis, security, PCAP, system log, web call, temper alarm, and password modification.

# Akuvox | X912

Open A Smart World

-  Home Screen
-  Status ▾
-  Account ▾
-  Network ▾
-  Intercom ▾
-  Surveillance ▾
-  Access Control ▾
-  Directory ▾
-  Device ▾
-  Setting ▾
-  System ▾

Status» Info

## Product Information

Model

MAC Address

Firmware Version

Hardware Version

Server Mode

Location

Uptime

## Network Information

Port Type

Link Status

## Model Specification




Model	X912
Touch Screen	✓
Relay In	3
Relay Out	2
Alarm In	X
RS485	✓
Card Reader	13.56MHz&125kHz,NFC
Wi-Fi	X
Bluetooth	✓
Temperature Detection	X
Facial Recognition	✓
LTE	X
USB	X
External SD Card	X

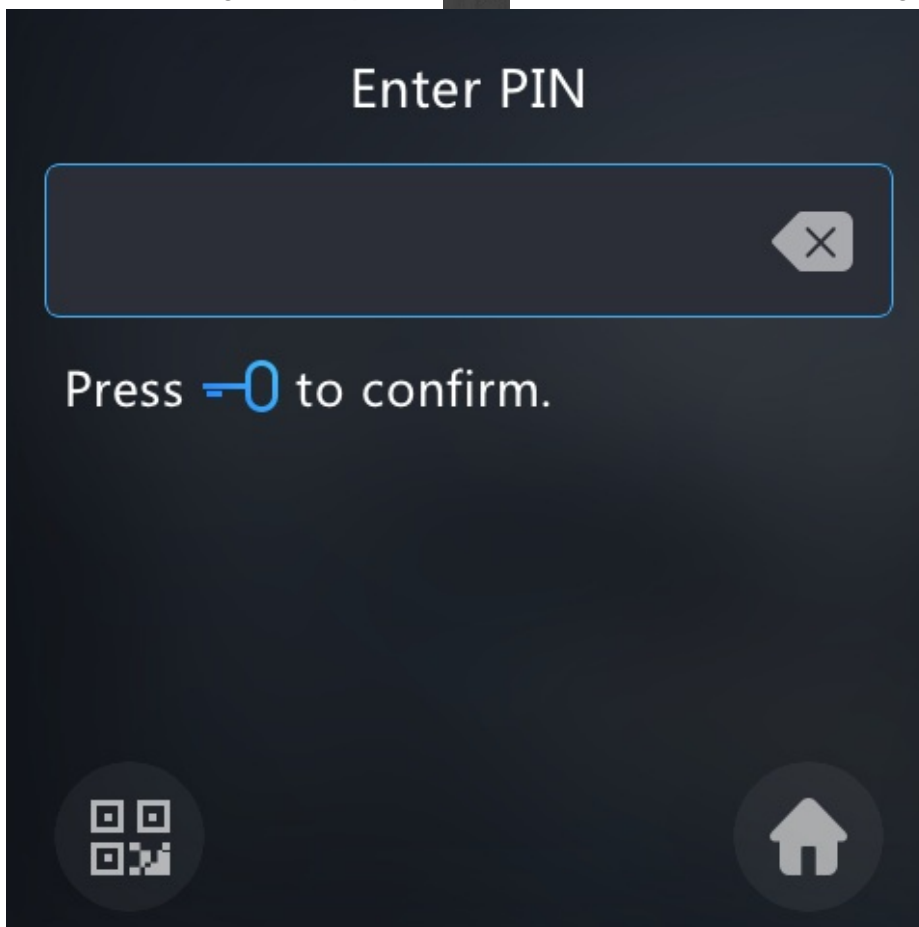
## Access the Device

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

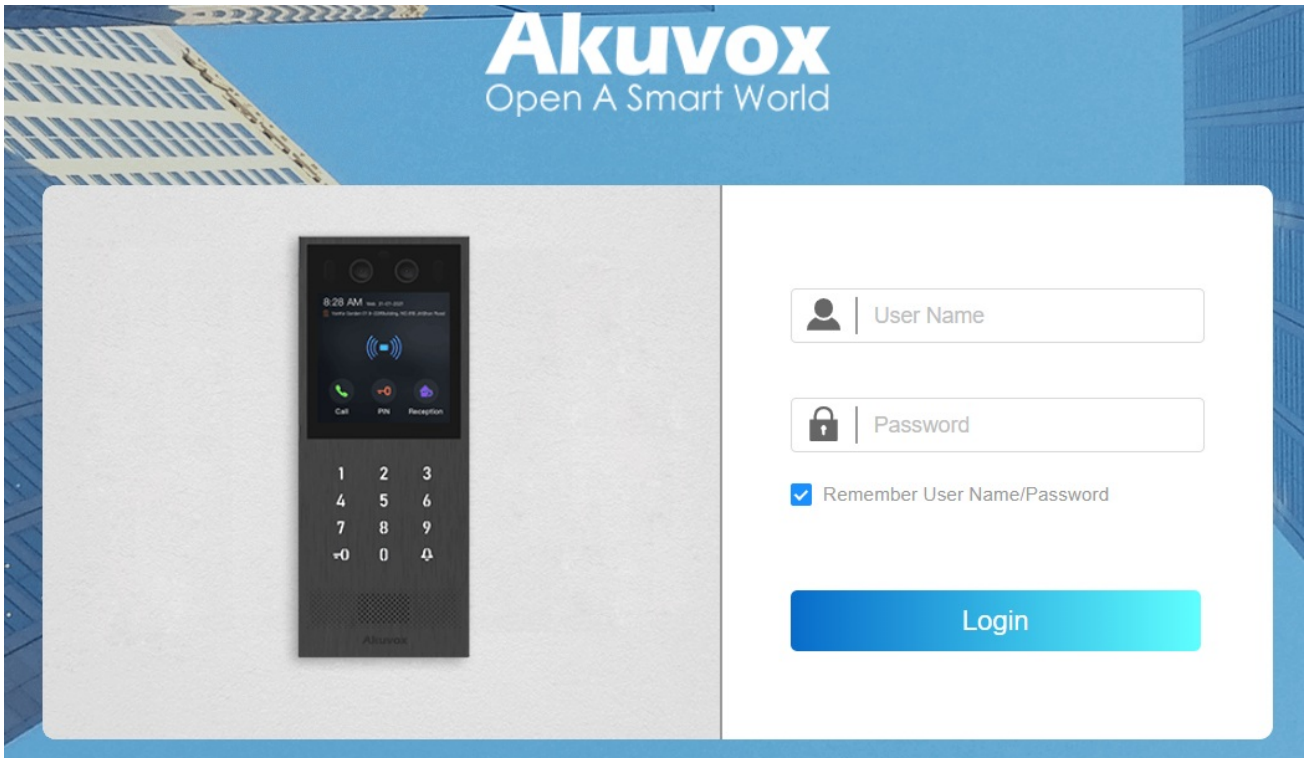
Before configuring door phone, please make sure the device is installed correctly and connected to a normal network. Using the Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to login into the web browser by user name and password **admin** and **admin**.

To access the device system setting on the device, you can press icon  on the screen or on the keypad, enter the default system PIN code **2396**, then press  for the confirmation. To access the setting screen, press , then enter the default Setting PIN code **3888**.



### 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.



### Note

You can also obtain the device IP address using the Akuvox IP scanner to log in to the device web interface.

- 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.

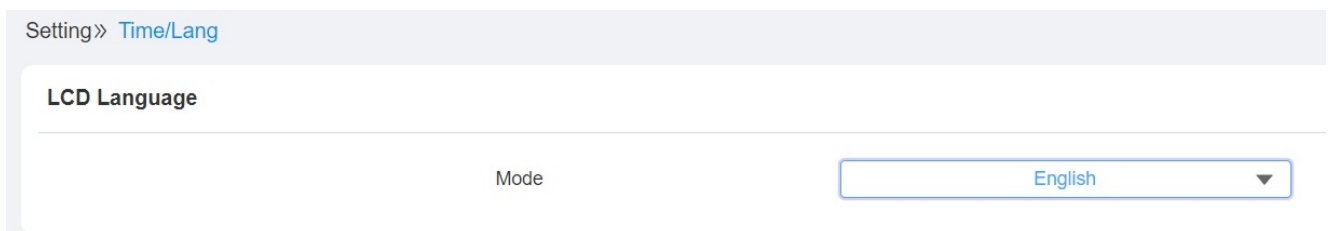


# Language and Time Setting

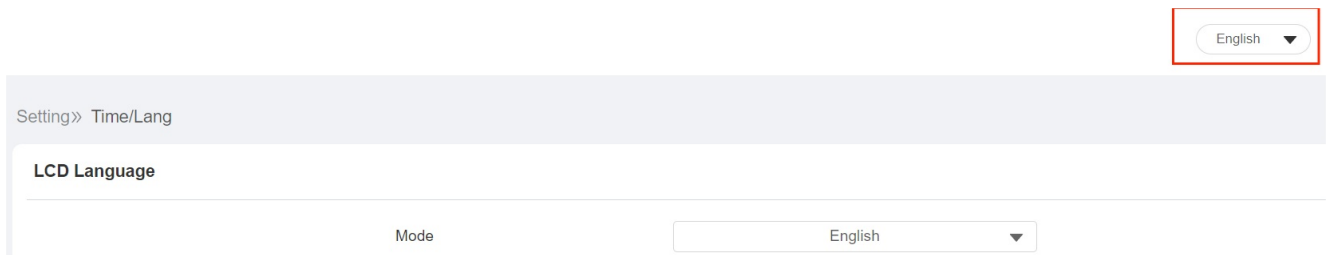
## Language Setting

Set up the language during initial device setup or later through the device or web interface according to your preference.

To select the language for device screen display, navigate to **Setting > Time/Lang > LCD Language** interface.



You can also select the web language on the upper right corner of the same web interface.



## 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 configure it on the web **Setting > Time/Lang** interface.

Format Setting	
Date Format	YYYY-MM-DD ▼
Time Format	24-hour format ▼

---

Time	
Time Zone	GMT-5:00 New_York ▼
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>=3600s)
System Time	01:18:27

### Parameter Set-up:

- **Primary/Secondary Server:** the time zone server, normally will automatically obtain the time when connecting to the network. The alternate server will take effect when the primary server is invalid.
- **Update Interval:** configure the interval between two consecutive NTP requests.

# LCD Setting

## LCD Screen Brightness Setting on the Web Interface

On the web interface, you can set and adjust the backlight brightness for the screen and screen saver.

To configure the configuration on the web **Device > LCD > Screen Backlight Brightness**.

**Screen Backlight Brightness**

---

Mode	<input type="text" value="Auto"/>	
Backlight Brightness(Day)	<input type="text" value="200"/>	(1-255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="15"/>	(1-255)
Backlight Brightness(Night)	<input type="text" value="15"/>	(1-255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="3"/>	(1-255)

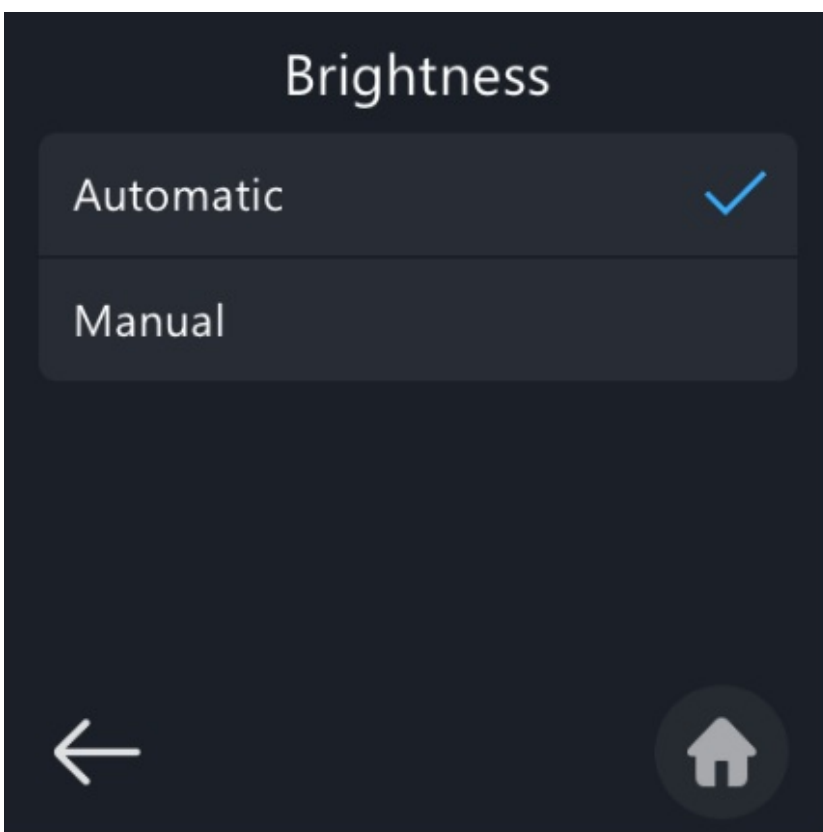
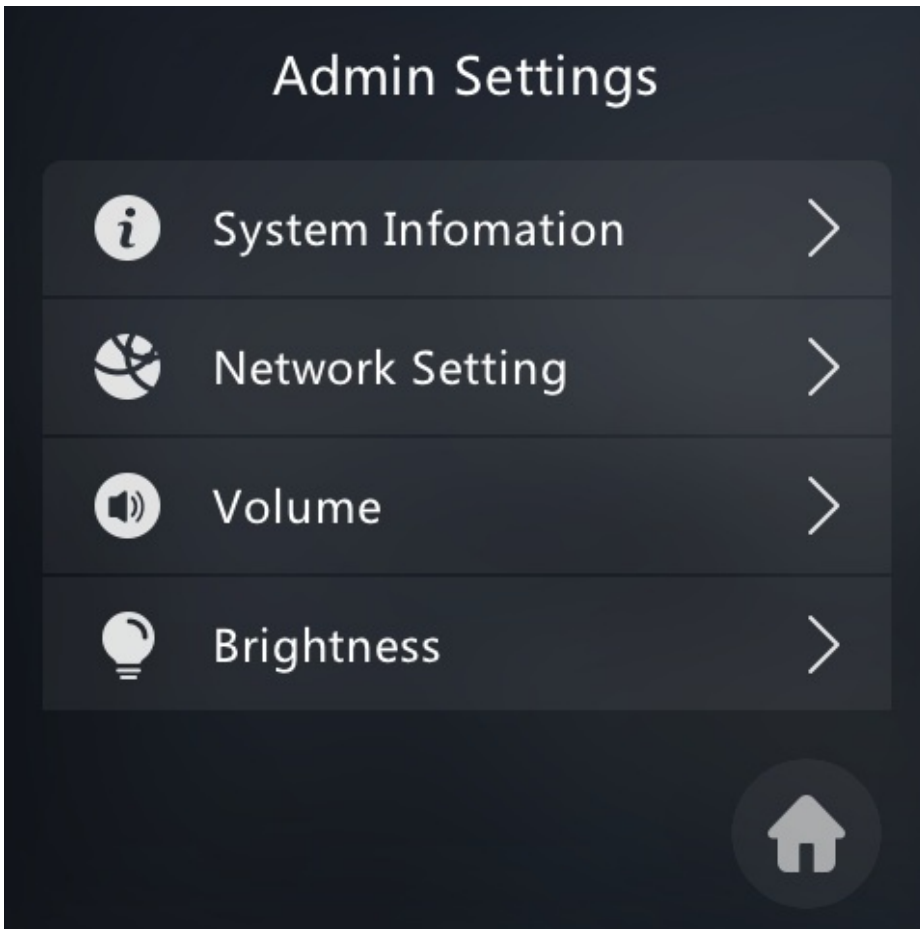
### Parameter Set-up:

- **Mode:** click to select **Manual** or **Auto** mode for the backlight. Backlight will be adjusted automatically for the screen backlight brightness when **Auto** is selected and vice versa.
- **Backlight Brightness (Day):** select the brightness value from 1-255. The default value is 200. The larger value, the brighter screen.
- **Backlight Brightness Of Screensaver (Day):** adjust the backlight for the screensaver in the daytime with the value ranging from (1-255).
- **Backlight Brightness (Night):** adjust the backlight for the screen saver at the night with the value ranging from (1-255).
- **Backlight Brightness Of Screensaver (Night):** adjust the backlight for the screensaver in the nighttime with the value ranging from (0-255).

## LCD Screen Brightness Setting on the Device

On the device, you can set and adjust the screen backlight brightness.

Select **Brightness**, and select **Automatic** for automatic brightness adjustment or select **Manual** to adjust the brightness manually.



## Keypad Light Setting

You can control the keypad light to turn it on/off or to make it turned or off according to your time schedule. To do so, navigate to **Device > Light > Keypad Light**.

Device» Light

Keypad Light

Mode: Specific Time

Start Time - End Time: 18:00 - 06:00

### Parameter Set-up:

- **Mode:** select **Always OFF** to make the keypad stay off. Select **Auto** to make the keypad light turn on automatically when the screen is turned off. Select **Specific Time** to make the keypad light turn on/off according to your time schedule ( Start Time-End Time). However, the keypad light will change to **Auto** mode for the time not covered in the time schedule.

# Screen Display Configuration

The door phone allows you to enjoy a variety of screen displays to enrich your visual and operational experience through customized settings to your preference.

## Screensaver Configuration

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

On web interface, navigate to **Device > LCD > Sleep**.

### Sleep

Auto-Sleep Time	15 seconds
Screensaver Mode	Image
Screensaver Time	15 seconds
Wake Up Mode	Auto

### Parameter Set-up:

- **Auto-Sleep Time:** if you set sleep time, for example as 15 seconds, then the device will go into screen saver mode (displaying screen saver in your defined duration) when the device detects no operation or no approaching object for the consecutive 15 seconds. However, if the screen saver mode is disabled, then device screen will be turned off directly in 15 seconds. Auto-sleep time ranges from 5 seconds to 30 min.
- **Screensaver Mode:** select **Image** to display the personalized pictures uploaded to the device; select **Disable** to disable the screen saver function.
- **Screensaver Time(Sec):** select the screen saver duration. Time range: 5 seconds to 30 min.
- **Wake up mode:** If you select **Auto** mode, then the screen will be automatically woken up when the device detects an approaching object or operation. Select **Manual** if you wake up the screen through touch.

## 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 the web **Device > LCD > Upload ScreenSaver** interface.

Upload Screensaver

Transition Time  Sec

Screensaver ID	File Status	Import	Delete
1	NULL	<input type="button" value="Import"/>	<input type="button" value="Delete"/>
2	NULL	<input type="button" value="Import"/>	<input type="button" value="Delete"/>
3	NULL	<input type="button" value="Import"/>	<input type="button" value="Delete"/>
4	NULL	<input type="button" value="Import"/>	<input type="button" value="Delete"/>
5	NULL	<input type="button" value="Import"/>	<input type="button" value="Delete"/>

Parameter Set-up:

- **Transition Time:** set the display time of each individual picture you uploaded in **Interval (Sec)**, the display time range is from 1-120 seconds. The default setting is 5 seconds.

### Note

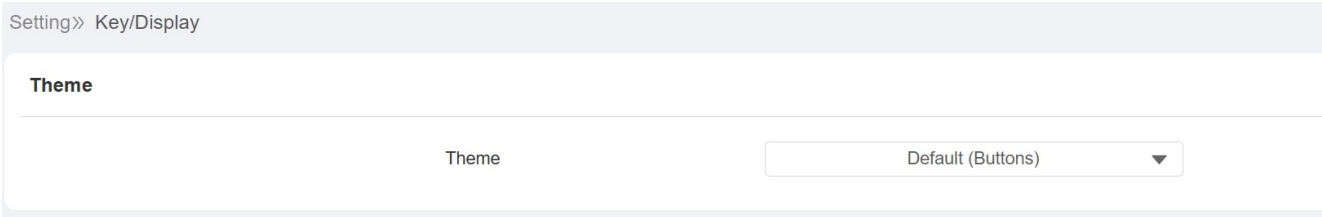
- The pictures uploaded should be in **JPG** format with 2M pixels maximum.

### Note

- The previous pictures with a specific ID order will be overwritten when repetitive designation of pictures to the same ID order occurred.

## Configuration for Scenario-based Screen Display Mode

X912 door phones offer you four types of screen display modes for different applications: **Default (buttons) mode**, **Directly mode**, **Speed Dial mode**, and **Customized Text mode**. On the web interface, navigate to **Setting > Key/Display > Theme**.

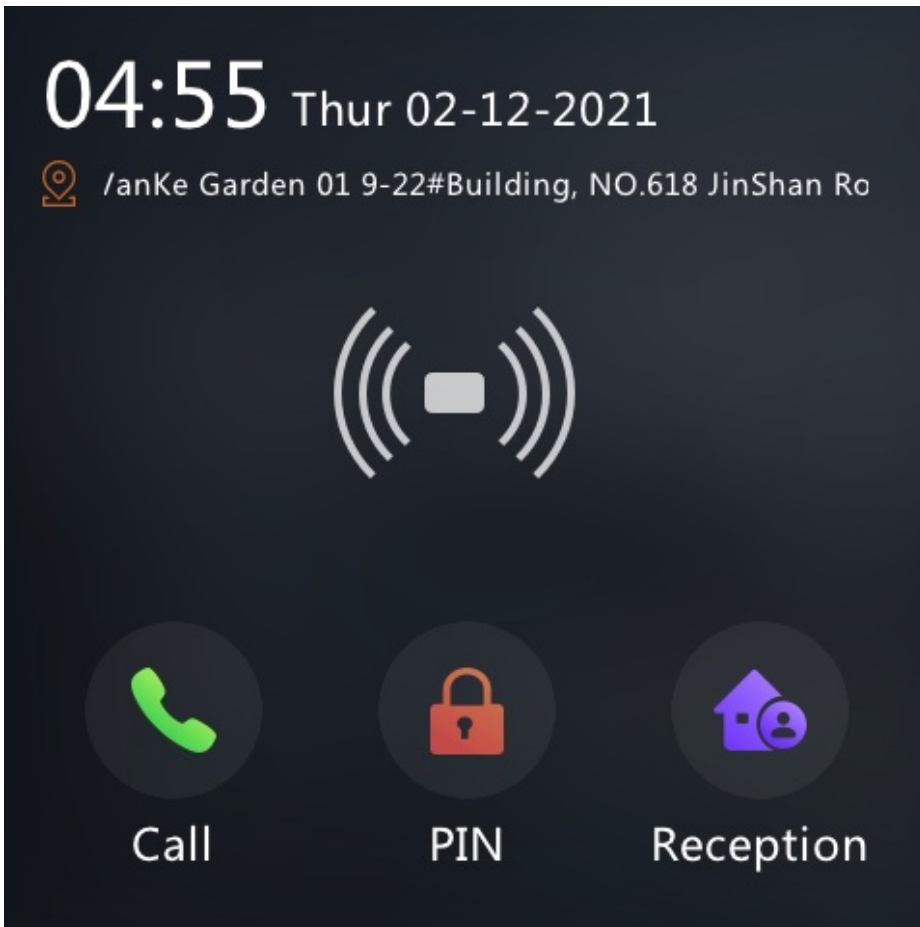


### Directory Mode





## Default(buttons) Mode



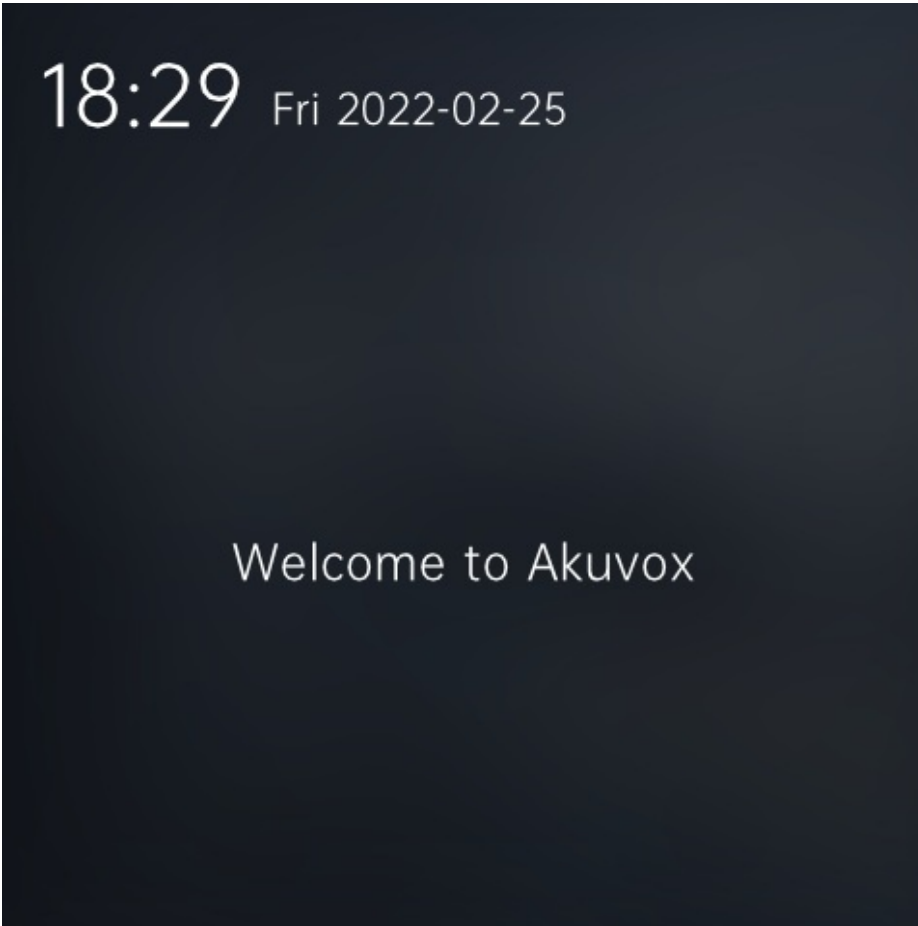
## Speed Dial Mode

18:33 Fri 2022-02-25

Management Center



## Customized Text Mode



## Default (Buttons) Mode Home Screen Display

You can change the home screen display through the configuration of tab arrangement, and the language icon display as needed on the device web **Setting > Key/Display > Keys on Homepage of the Building Theme**.

Device» [Key/Display](#)

Theme

Theme Default (Buttons) ▼

### Key on Homepage of the Building Theme

Index	Type	Name	Number
1	Call ▼		
2	PIN ▼		
3	Speed Dial ▼		

## Parameter Set-up:

- **Type:** select the tab type (Call, PIN, Speed Dial, Directory, and Temp Key-QR code) corresponding to the ID order which indicates the tab position. For example, if you want to make **Temp Key** tab be displayed in position one of tab row one, you can click to select the type of the ID order 1. And you can change other tab positions accordingly.
- **Name:** enter a new name to replace the original type name, but it does not change the attribute of the type.
- **Number:** it is available for those features which need to be set up numbers, like **Speed Dial** feature.

## Directory Mode Home Screen Display

You can set the Contact directory as the home screen so that you can easily dial out the contact number. To set it up, go to **Setting > Key/Display > Theme**.

Theme

---

Theme Directory ▼

Please go and set up the tenants list in [User](#).

## Speed Dial Mode Home Screen Display

When you set speed dial mode for the home screen display, the speed dial numbers will be displayed on the home screen, so that you can easily make speed dial to a specific contact you set up. You can navigate to **Setting > Key/Display > Speed Dial Setting**.

Theme

---

Theme Speed Dial ▼

**Speed Dial Setting**

Index	Show	Account	Name	Number	Delete
1	Show ▼	Auto ▼	Management Center	192.168.35.111	Delete
2	Show ▼	Auto ▼	VV	192.168.35.112	Delete
3	Show ▼	Auto ▼			Delete

[Add](#)

### Note

- X912 supports up to five speed dials on the screen.

## Customized Text Mode Home Screen Display

X912 allows you to display people's names or company names etc. on the home screen for identification purpose. To do so, navigate to **Setting > Key/Display > Customized Text**.

Theme

---

Theme

---

Customized Text

---

Text

---

### Note

- X912 supports 63-digit character maximum in length for customized text.

## Dial Screen Prompt Display

You can customize your prompt to be displayed on the dial screen if needed. To do so, navigate to **Setting > Key/Display > Prompt Of The Call Page**.

Prompt Of The Call Page

---

Text Prompt

---

### Note

- X912 supports a 128-digit character maximum in length for the text prompt.

## Open Door Text Prompt Display

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 do so, navigate to **Access Control > Relay > Door Setting General**.

Door Setting General	
Open Door Succeeded Text Prompt	<input checked="" type="checkbox"/>
Open Door Failed Text Prompt	<input checked="" type="checkbox"/>

# Volume and 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.

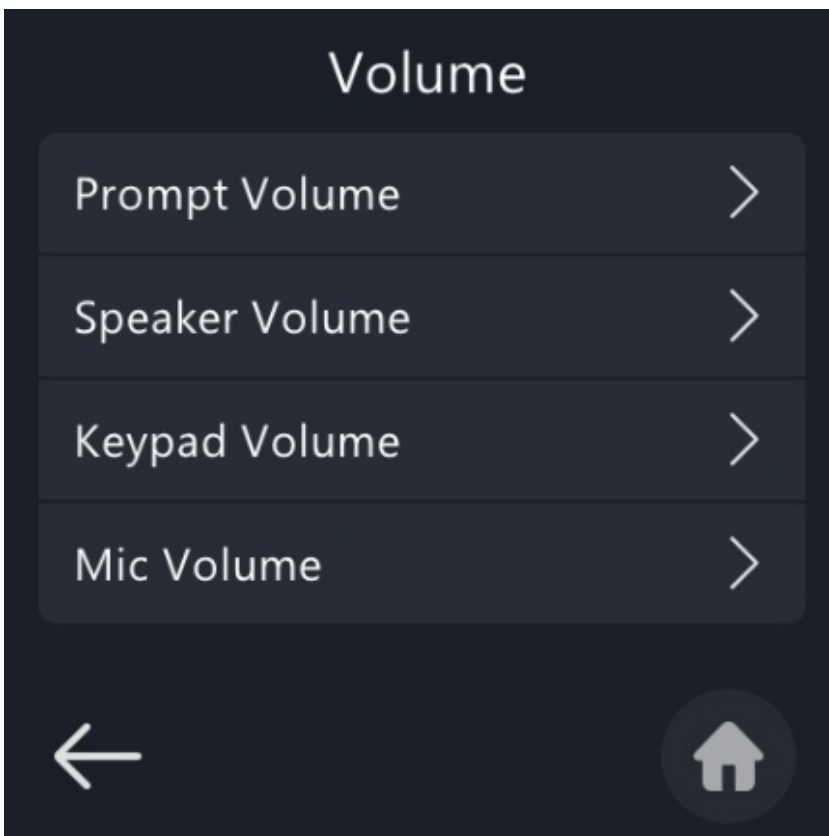
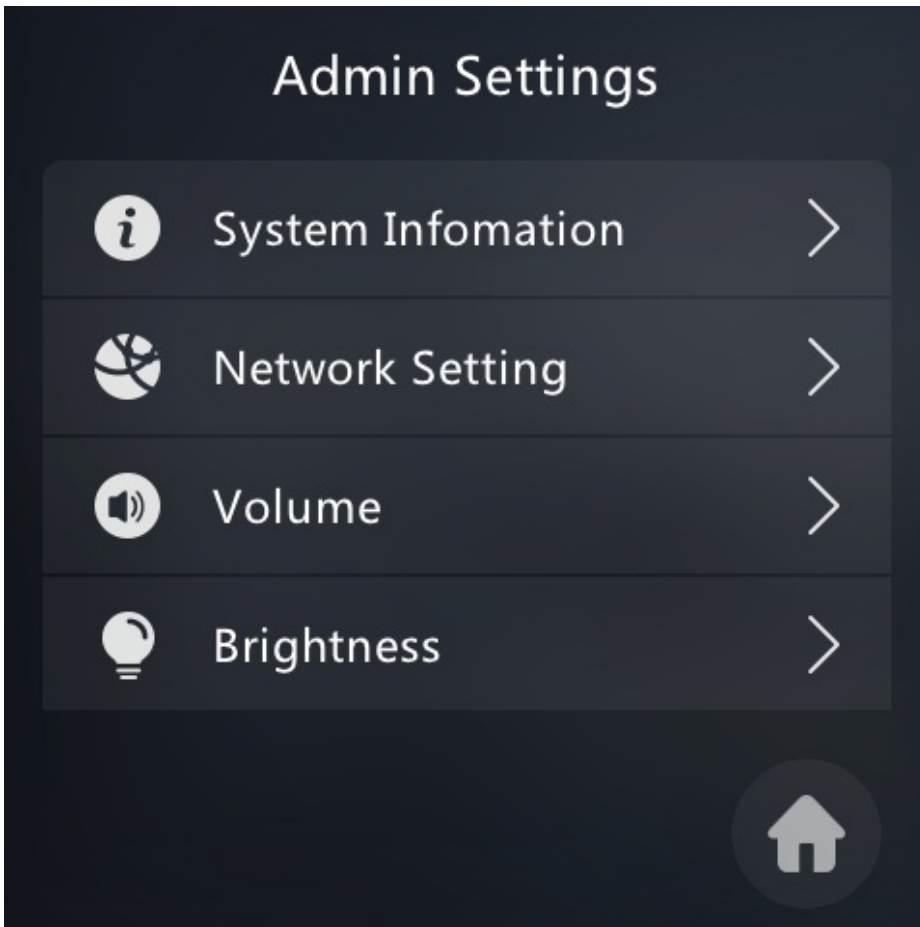
## Volume Configuration

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.

To configure on the device **Admin Setting > Volume** interface.



**Parameter Set-up:**



- **Prompt Volume:** includes prompt tone, ringback tone, open door success tone and so on. The default prompt volume is 50.

## Configure Volume on the Web Interface

To configure the configuration on the web Device > Audio interface.

Device >> Audio

### Volume Control

Prompt Volume	<input type="text" value="50"/>	(0~100)
Mic Volume	<input type="text" value="50"/>	(1~100)
Speaker Volume	<input type="text" value="50"/>	(1~100)
Keypad Volume	<input type="text" value="50"/>	(1~100)
Tamper Alarm Volume	<input type="text" value="50"/>	(1~100)

### Volume Control On Talking Interface

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

### Mic Mode

Select On	<input type="text" value="Left Mic"/>
-----------	---------------------------------------

### Parameter Set-up:

- **Prompt Volume:** includes prompt tone, ringback tone, open door success time and so on. The default prompt volume is 50.
- **Enabled:** tick the check box if you allow the adjustment to be made on the call volume on the talking screen during a call.

## Upload Open-door Tone

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

Go to Device > Audio > Tone Setting interface.

**Tone Setting**

Enable Prompt of Open Door	<input checked="" type="checkbox"/>
Enable Voice Prompts of Guiding	<input checked="" type="checkbox"/>
Door Open Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Directory Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Call Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
PIN Entry Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Scan QR Code Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Temp Key Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Apartment Number Entry Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Tap Card Guiding Tone	<input type="button" value="Import"/> <input type="button" value="Reset"/>

**Parameter Set-up:**

- **Enable Voice Prompt of Guiding:** when enabled, the voice promotion will be played, for example, "Please enter the number, then press the call button" as you tap the **Call** icon on the screen.
- **Door Open Tone:** upload the open door tone. Click **Reset** to reset the tone to the default one.
- **Directory Guiding Tone:** upload the voice prompt tone for door opening success.
- **Call Guiding Tone:** upload your voice prompt for the call, which will be played when you tap call icon.
- **PIN Entry Guiding Tone:** upload the customized voice prompt tone on PIN code entry screen.
- **Scan QR Code Guiding Tone:** upload the voice prompt tone for the QR code screen.
- **Temp Key Guiding Tone:** upload the customized prompt tone on temporary PIN code entry screen.
- **Apartment Number Entry Guiding Tone:** upload the prompt tone for entering the apartment number.
- **Tap Card Guiding Tone:** upload the card taping voice prompt tone for the dual authentication door entry. It will be played after your finished first authentication. For example, Face+Card dual authentication.

## Note

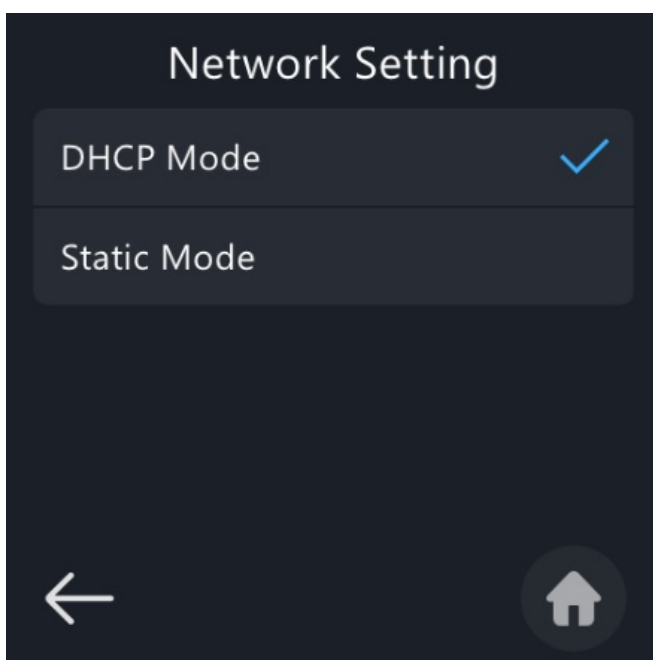
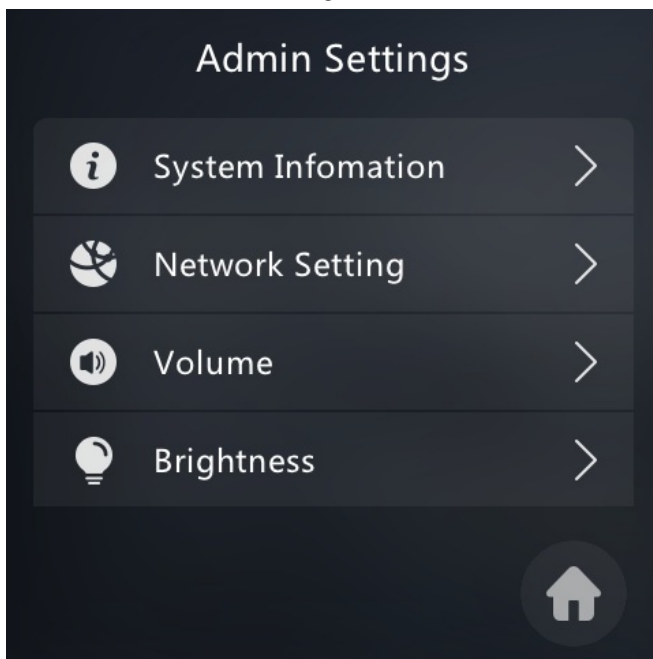
- All the tone files uploaded should be in .wav format, size 200KB, Sample Rate:16000, Bits:16

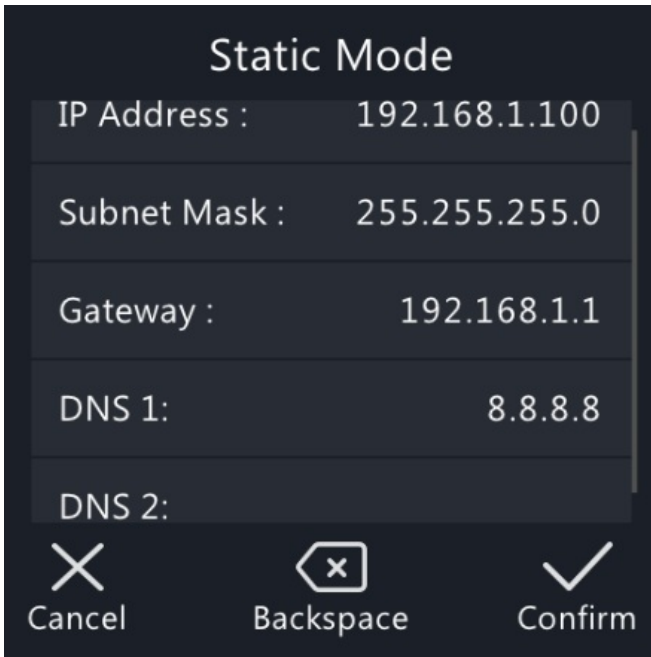
# Network Setting

## Device Network Configuration

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

Select **Network Setting** on the device screen.

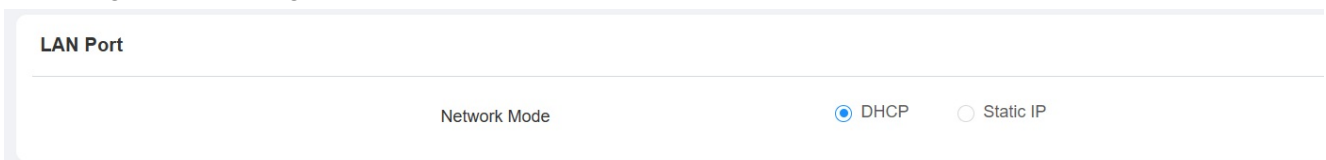




**Parameter Set-up:**

- **DHCP:** 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:** When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers 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.
- **Default Gateway:** set up the correct gateway default gateway according to the IP address of the default gateway.
- **DNS1/2:** set up a preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. DNS1 server is the primary DNS server address while DNS2 is the secondary server address, and the door phone will connect to the DNS2 server when the primary DNS 1 server is unavailable.

To configure the configuration on the web **Network > Basic > LAN Port** interface.



## Device Local RTP configuration

Real-time Transport Protocol(RTP) lets devices stream audio and video data over a network in real time.

To use RTP, devices need a range of ports. A port is like a channel for data on a network. By setting up RTP ports on your device and router, you can avoid network interference and improve audio and video quality.

To configure the configuration on the web **Network > Advanced > Local RTP** interface.

Network» [Advanced](#)

Local RTP

Starting RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

### Parameter Set-up:

- **Starting RTP Port:** enter the Port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port:** enter the Port value to establish the endpoint for the exclusive data transmission range.

## 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 the web **Network > Advanced > Connect Setting** interface.

Connect Setting

Server Mode	None
Discovery Mode	<input checked="" type="checkbox"/>
Device Address	<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="Stair Phone"/>

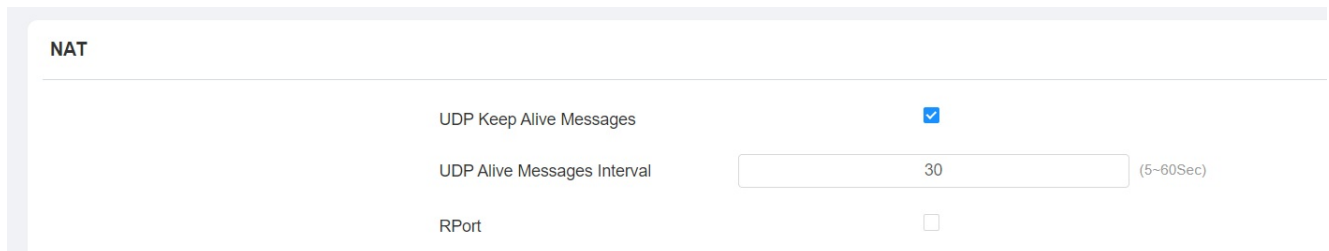
### Parameter Set-up:

- **Server Mode:** it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC** or **Cloud** and **None**. **None** is the default factory setting.
- **Discovery Mode:** click **Enable** to turn on the discovery mode of the device so that it can be discovered by other devices in the network and click **Disable** 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.

Path: **Account > Advanced > NAT.**



The screenshot shows the NAT configuration page with the following settings:

Parameter	Value	Unit/Constraint
UDP Keep Alive Messages	<input checked="" type="checkbox"/>	
UDP Alive Messages Interval	30	(5-60Sec)
RPort	<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 that 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**).

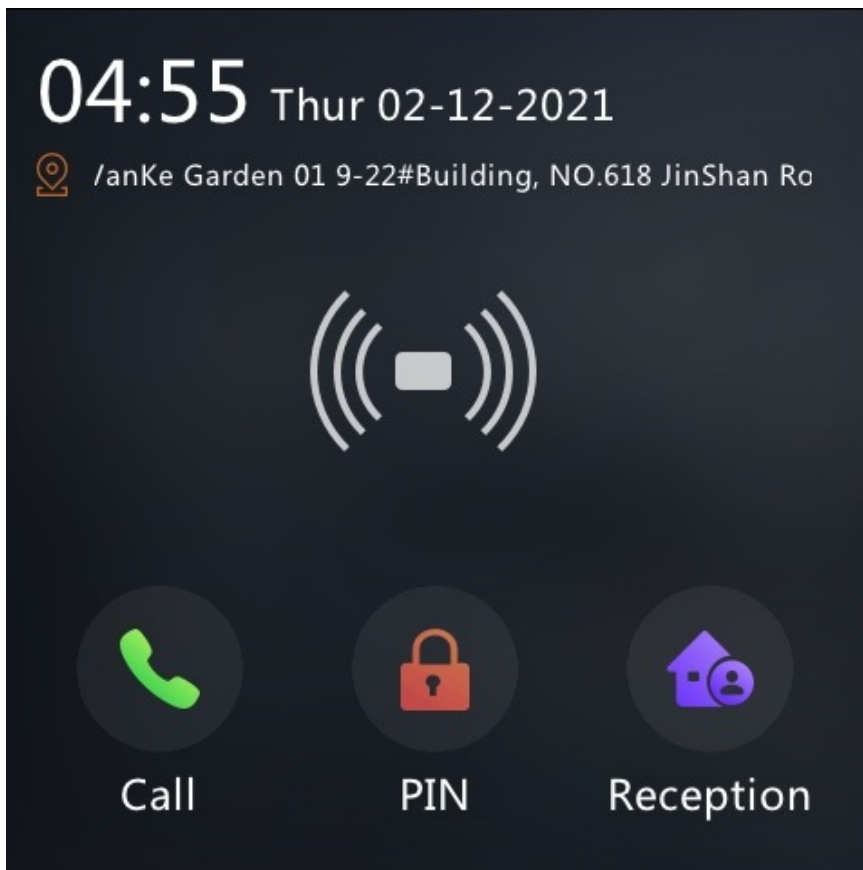
# Intercom Call Configuration

## 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 SIP calls or IP calls on the device by clicking on dial or home screen.



## IP Call Configuration

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



Intercom» Basic

Direct IP

Enabled	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1024-65535)

### Parameter Set-up:

- **Port:** the direct IP Port is 5060 by default with the port range from 1024-65535. And you enter any values within the range other than the 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

To configure the SIP account, navigate to **Account > Basic > SIP Account** interface. **Register Name, User Name, and Password** are obtained from SIP account administrator.

Account» Basic

**SIP Account**

Status	Disabled
Account	Account1 ▼
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	*****

**Parameter Set-up:**

- **Account:** select account 1 or account 2 to be configured for making or receiving SIP calls.
- **Display Label:** configure the device label to be shown on the device screen.
- **Display Name:** configure the device's name to be shown on the called party.

## 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 configure it on the web **Account > Basic > Preferred/Alternate SIP Server** interface.

**Preferred SIP Server**

Server IP	<input type="text"/>	
Port	5060	(1024-65535)
Registration Period	1800	(30-65535Sec)

---

**Alternate SIP Server**

Server IP	<input type="text"/>	
Port	5060	(1024-65535)
Registration Period	1800	(30-65535Sec)

**Parameter Set-up:**

- **Preferred SIP Server:** enter the primary server IP address number or its URL.
- **Alternate SIP Server:** enter the backup SIP server IP address or its URL.
- **Port:** set up SIP server port for data transmission.
- **Registration Period:** set up SIP account registration time span. 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.

## DND Configuration

The Do Not Disturb(DND) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

To configure the configuration on the web **Intercom > Call Feature > DND** interface.

The screenshot shows the 'DND' configuration page within the 'Intercom > Call Feature' section. The page contains the following fields:

Account	Account1
Enabled	<input type="checkbox"/>
Return Code When DND	486(Busy Here)
DND On Code	
DND Off Code	

### Parameter Set-up:

- **Account:** select the Account you want to apply DND function.
- **Return Code When DND:** select what code should be sent to the calling device via SIP server. 404 for "not found"; 480 for "temporary unavailable" 486 for "busy here"; 603 for "decline".
- **DND On Code:** enter the DND on Code to turn on DND function on the SIP server. The DND on code is 78.
- **DND Off Code:** enter the DND off code to turn off DND function on the SIP server. The DND off code is 79.

## 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 configuration on the web **Account > Basic > Outbound Proxy Server** interface.

The screenshot shows the 'Outbound Proxy Server' configuration page. It features a title bar 'Outbound Proxy Server' and a main content area with the following fields:

- Outbound Enabled:** A checkbox that is currently unchecked.
- Preferred Server IP:** An empty text input field.
- Port:** A text input field containing '5060', with a range '(1024~65535)' indicated to the right.
- Alternate Server IP:** An empty text input field.
- Port:** A text input field containing '5060', with a range '(1024~65535)' indicated to the right.

**Parameter Set-up:**

- **Preferred Server IP:** enter the SIP address of the primary outbound proxy server.
- **Alternate Server IP:** set up backup Server IP for the backup outbound proxy server.

## Configure Data Transmission Type

SIP messages can be transmitted in three data transmission protocols: **UDP (User Datagram Protocol)**, **TCP (Transmission Control Protocol)**, **TLS (Transport Layer Security)**, and **DNS-SRV**. In the meantime, you can also identify the server from which the data come.

To configure the configuration on the web **Account > Basic > Transport Type** interface.

The screenshot shows the 'Transport Type' configuration page. It features a title bar 'Transport Type' and a main content area with the following field:

- Type:** A dropdown menu currently set to 'UDP'.

At the bottom of the form, there are two buttons: 'Cancel' and 'Submit'.

**Parameter Set-up:**

- **UDP:** select UDP for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP:** select TCP for Reliable but less-efficient transport layer protocol.
- **TLS:** select TLS for Secured and Reliable transport layer protocol.

## Dial Options Configuration

### Quick Dial by Number Replacement

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.

To configure the configuration on the web **Intercom > Dial Plan > Replace Rule** interface.

<input type="checkbox"/>	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
<input checked="" type="checkbox"/>	1	Account1	101	192.168.35.37	192.168.35.38	192.168.35.39	192.168.35.40	192.168.35.41	
<input type="checkbox"/>	2	Account1	102	192.168.35.118	192.168.35.119	192.168.35.200	192.168.35.201	192.168.35.202	

#### Parameter Set-up:

- **Account:** select the account you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the dial number has been registered). You can select either account 1 or account 2 from which the number can be dial out. if you have registered the dial 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 dial number you wish to replace.
- **Replace 1/2/3/4/5:** enter the dial number(s) you wish to replace. It supports up to 5 number maximum for the replacement on 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 dial number will be called to at the same time when you dial **101**.

#### Note

- The check box for each line of **Prefix** should be checked before you can see the **Edit** tab, which you click to carry out the modification.

## Call Auto-answer Configuration

Auto-answer feature allows door phones 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 the configuration on the web **Intercom > Call Feature > Auto Answer** interface.

Auto Answer

Auto Answer Delay  (0~5Sec)

Mode

Cancel Submit

### 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.

## Manager Dial Call

Manager Dial Call includes two types of calls: Sequence call and group call. It allows quick initiation of pre-configured numbers by pressing the Management key on the door phone.

You can create up 10 numbers. To do the configuration on the web **Intercom > Basic > Manager Dial** interface.

**Manager Dial**

Enabled

Call Type Sequence Call ▼

Time Out (Sec) 60 ▼

**Sequence Call Number**

RobinCallNum1

RobinCallNum2

RobinCallNum3

RobinCallNum4

RobinCallNum5

RobinCallNum6

RobinCallNum7

RobinCallNum8

RobinCallNum9

RobinCallNum10

**Manager Dial**

Enabled

Call Type Group Call ▼

**Group Call Number**

<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>
<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>	<input style="width: 95%;" type="text"/>

**Parameter Set-up:**

- **Timeout (Sec):** click to select 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.
- **Call Type:** select the group call or sequence call for the manager dial call.
- **Sequence Call:** sequence call is used to initiate multiple numbers when your press the

manager dial button. If the previous callee does not answer within the sequence call timeout, the call will be transferred to the next one. If the call is answered by one of the callees, the call will not be transferred anymore. You can enter five sequence call number maximum in each line.

- **Group Call:** group call is used to initiate calls to multiple numbers at the same when you press the manager dial button. Local group call numbers are the numbers you added locally from your web interface. And the Cloud group call are the numbers you created on the SmartPlus Cloud.

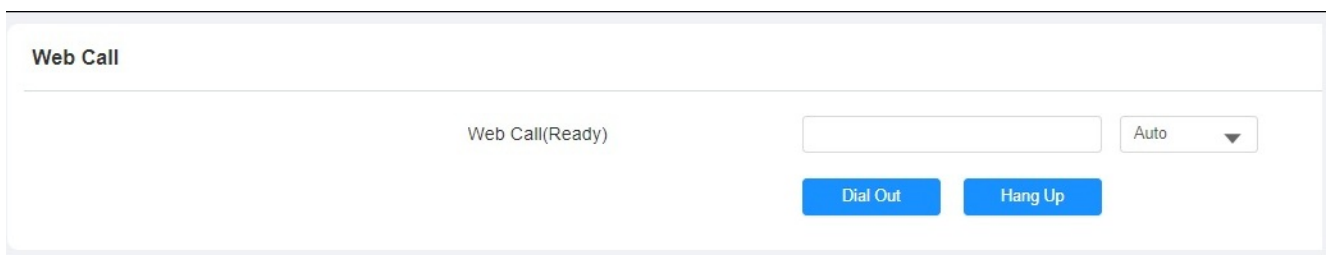
### Note

- The sequence call function should be supported by SmartPlus, please contact Akuvox technical support for more information.

## Web Call

The web call feature allows for making calls via the device's web interface, commonly used for remote call testing purposes.

To make a web call, navigate to **System > Maintenance > Web Call**.



The screenshot shows a web interface titled "Web Call". It features a text input field containing "Web Call(Ready)", a dropdown menu set to "Auto", and two blue buttons labeled "Dial Out" and "Hang Up".

### Parameter Set-up:

- **Web Call (Ready):** enter the IP/SIP number to dial out.

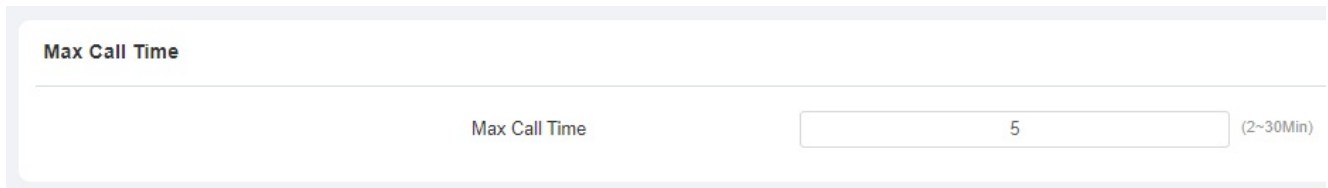


# Call Settings

## 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 configure the configuration on the web **Intercom > Call Feature > Max Call Time** interface.



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

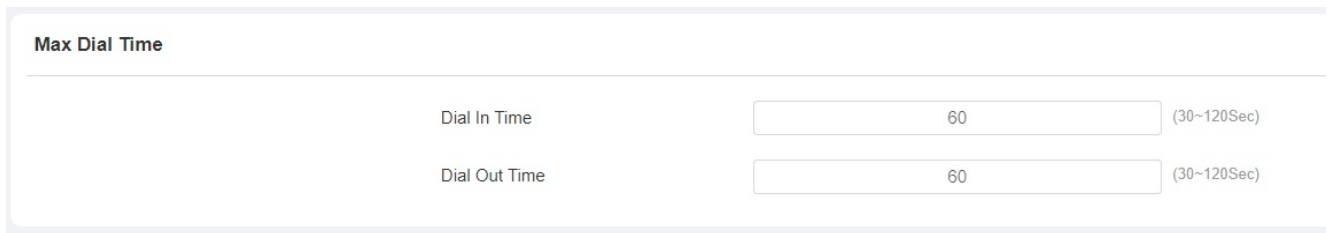
### Parameter Set-up:

- **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.

## 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 configure the configuration on the web **Intercom > Call Feature > Max Dial Time** interface.



Max Dial Time	
Dial In Time	<input type="text" value="60"/> (30~120Sec)
Dial Out Time	<input type="text" value="60"/> (30~120Sec)

### Parameter Set-up:

- **Dial In Time:** enter the dial in time duration for your door phone (ranging from 30-120 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 30-120 Sec.) for example, if you set the dial out time duration is 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 called party.

## Hang Up After Open Door

This feature automatically ends the call once the door is released, allowing for the seamless reception of subsequent calls.

To do this configuration on the web Intercom > Call Feature > Hang Up After Opening Door interface.

### Hang Up After Opening Door

Type	<input type="text" value="Only DTMF"/>
Time Out (Sec)	<input type="text" value="5"/> (0~15Sec)

### Parameter Set-up :

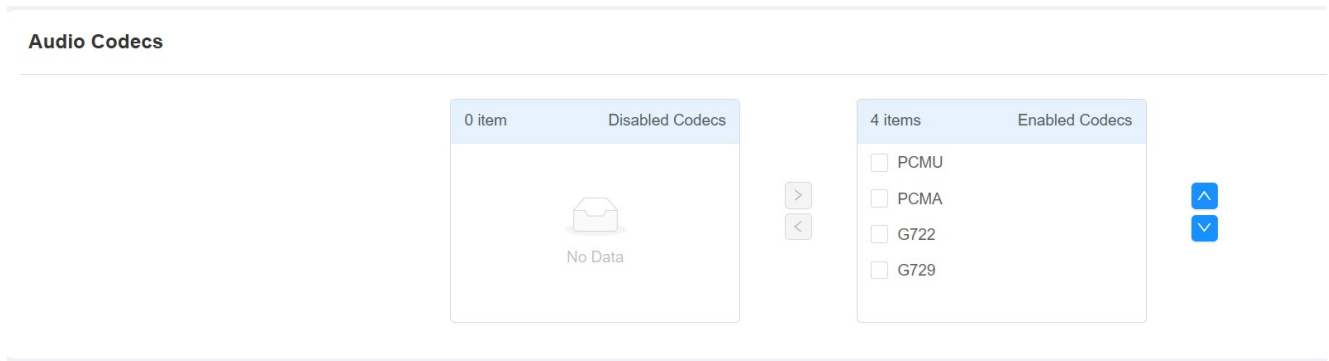
- **Type:** select the open door type. Door can be unlocked via **Only DTMF, Only HTTP, DTMF and HTTP, and Input, DTMF and HTTP.**
- **Timeout:** the timeout value can be set up from 0 second to 15 seconds. 5 seconds is the default. Set it 0 if you want to disable the function. The call will automatically hang up within this value after the door is opened.

## Audio& Video Codec Configuration for SIP Calls

### Audio Codec Configuration

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 configure it on the web **Account > Advanced > SIP Account** interface.



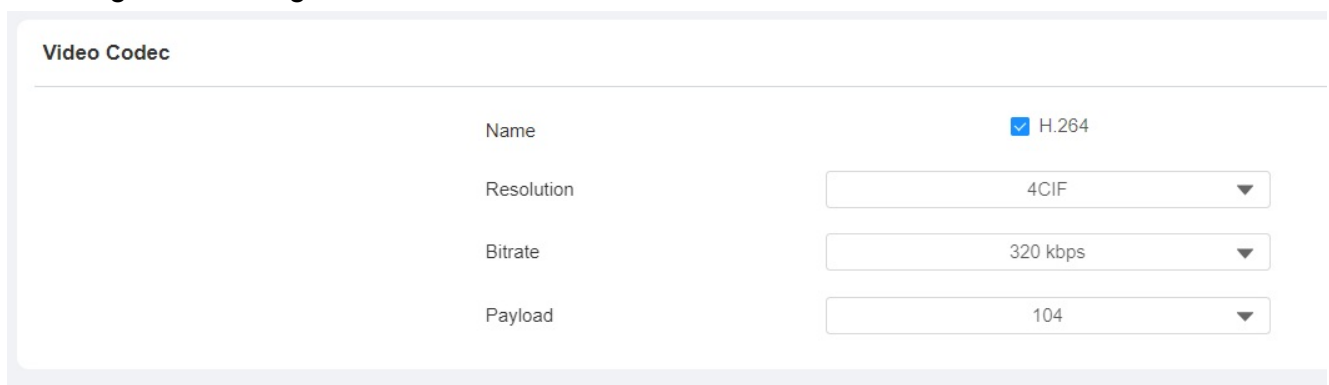
Please refers to the bandwidth consumption and sample rate for the four codecs types below:

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

## Video Codec Configuration

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 configure the configuration on the web **Account > Advanced > Video Codec** interface.



### Parameter Set-up:

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

- **Bitrate**: select the video stream bit rate (ranging from **128-2048**). 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 **90-119**) to configure audio/video configuration file. 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 configuration on the web **Account > Advanced > DTMF** interface.

**DTMF**

---

Type	<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 five options: **Inband**, **RFC2833**, **Info+Inband**, **Info+RFC2833**, and **Info** based on the specific DTMF transmission type of the third-party device to be matched with the party for receiving signal data. The default is **RFC2833**.
- **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 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. The default payload 101. The payload range is from 96 to 127.

# Phone Book Configuration

## Manage Contact Groups

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

To do so, navigate to **Directory > User > Group**.

Group

+ Add

<input checked="" type="checkbox"/>	Index	Name	Edit
<input checked="" type="checkbox"/>	1	Technical Department	

Delete
Delete All

Prev
1/1
Next

Go

## Contact Configuration

After the contact group is created, you start setting up user's contact which will be displayed on the home screen of the Directory mode. Before setting up the user's contact, you need to add users by entering their User ID and user name. To set it up, navigate to **Directory > User**, click **+Add**, then go to **User Basic > Contact Details**.

Access Control» [User](#)

User

All
User ID/Name/Code
Search
+ Add

<input type="checkbox"/>	Index	Source	User ID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/>	1	Local	1	CBD432DB			None	0	1001-1;	

Delete
Delete All

Prev
1/1
Next

Go

User» [Add User](#)

User Basic

User ID

Name

**Contact Details**

---

Phone	<input type="text"/>
Group	<input type="text" value="Default"/>
Priority Of Call	<input type="text" value="Primary"/>
Dial Account	<input type="text" value="Auto"/>

**Parameter Set-up:**

- **Group:** select the contact group. Select specific contact group for the user. Select the default for the user in the default group.
- **Priority of Call:** set the priority of call among three options: **Primary**, **Secondary**, and **Tertiary**. For example, if you set the priority of call for one of the contacts in a specific contact group as **Primary** then the contact will be the first to be called among all the contacts in the same contact group when someone press on the contact group for making a group call.
- **Dial Account:** select the account that you want to call to be dialed out from.

**Note**

- All the contacts without a specific group will go into the default group.

**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.

Navigate to **Directory > Directory Setting** interface.

**Directory Setting**

---

Show Cloud Contacts	<input checked="" type="checkbox"/>
Show Local Contacts	<input checked="" type="checkbox"/>
Contacts Display Settings	<input type="text" value="Groups On Entry Page And Their Contacts ..."/>
Sort By	<input type="text" value="ASCII Code"/>
Search Function Enabled	<input checked="" type="checkbox"/>

## Parameter Set-up:

- **Show Cloud Contacts:** tick the checkbox so that the contacts synchronized from the SmartPlus cloud can be displayed.
- **Show Local Contacts:** tick the check box to show the local list
- **Contact Display Setting:** select **All Contacts** if you want to see all the contacts. Select **Groups Only** if you only want to display contact group and press it for making group call. Select **Groups On Entry Page And Their Contacts On Subpage** you want to display the contact by group, then you can press it to see the contact list.
- **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.
- **Search Function Enabled:** enable the contact search function. You will see a search icon on the screen.

# Relay Setting

## Relay Switch Setting

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

Access Control >> [Relay](#)

**Relay**

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

### Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (ranging from 0-10 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.
- **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 resume the initial state after maintaining the triggered state for 5s.
- **DTMF Mode:** select the number of DTMF digit for the door access control (ranging from 1-4 digits ) For example, you can select 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 \*,#) if the DTMF Option is set as 1-digit.
- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DMTP Option** 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** field. 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 door phone can use a web relay to either control a local relay, or a remote relay somewhere else on the network.



## Configure Web Relay

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.

To configure the configuration on the web **Access Control > Web Relay** interface. **IP address** and **User Name** are provided by the web relay manufacturer.

Access Control >> [Web Relay](#)

---

**Web Relay**

Type	<input type="text" value="Disabled"/>
IP Address	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>

---

**Web Relay Action Setting**

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 02	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 03	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 04	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 05	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 06	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Parameter Set-up:**

- **Type:** select among three options **Disabled**, **WebRelay**, 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.
- **Password:** enter the password provided by the web relay manufacturer. The password is authenticated via HTTP and you can define the passwords using **HTTP Get in 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 DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension:** enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional.

And please refer to the example below:

<http://admin:admin@192.168.1.2/state.xml?relayState=2>.

After the web relay is set up, you can configure the specific web relay to be triggered based on the relay location for the door access. To do so, navigate to **Directory > User**, click **+ Add**, then scroll down to **Access Setting**. And select the specific web relay action you need.

Access Control» [User](#)

User

All  Search [+ Add](#)

---

**Access Setting**

Allow To Open	<input checked="" type="checkbox"/> RelayA <input type="checkbox"/> RelayB
Floor No.	<input type="text" value="None x"/>
Web Relay	<input type="text" value="0"/>

## Configure 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 door phone.



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

Security Relay

Relay ID	Security Relay A ▼	Security Relay B ▼
Server Mode	Relay A Power Output ▼	RS485 ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼
1 Digit DTMF	2 ▼	3 ▼
2~4 Digits DTMF		
Relay Name	Security Relay A	Security Relay B
Enabled	<input type="checkbox"/>	<input type="checkbox"/>
	<b>Test</b>	<b>Test</b>

**Parameter Set-up:**

- **Server Mode:** select the connection type between the security relay and the door phone. You can select connection via the door phone **Relay A Power Output** or **RS485**.
- **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.
- **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 be delayed for 5 after the door is unlocked.
- **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-digits DTMF code if **DTMP 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.

**Note**

- For the specific wiring, please refer to [SR01 Quick Guide](#).

# 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.

## Create Door Access Schedule

You can create door access schedules for daily, weekly, or custom time periods.

To do so , navigate to **Setting > Schedule**, then click **+ Add**.

Setting» [Schedule](#)

Schedule

All

<input type="checkbox"/>	Index	ScheduleID	Source	Mode	Name	Date	Day of Week	Time	Edit
<input type="checkbox"/>	1	1002	Local	Daily	Never	--	--	-	<input type="button" value="Edit"/>
<input type="checkbox"/>	2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59	<input type="button" value="Edit"/>

1/1

To create a daily schedule, you can do as follows:

**Add Schedule** X

Mode

Name

Start Time - End Time  -

### To create a weekly schedule:

#### Add Schedule ✕

---

Mode Weekly ▼

Name

Day  Mon  Tue  Wed  
 Thur  Fri  Sat  
 Sun  Check All

Start Time - End Time  🕒 -  🕒

### To create a longer period schedule:

#### Add Schedule ✕

---

Mode Normal ▼

Name

Start Date - End Date  ~

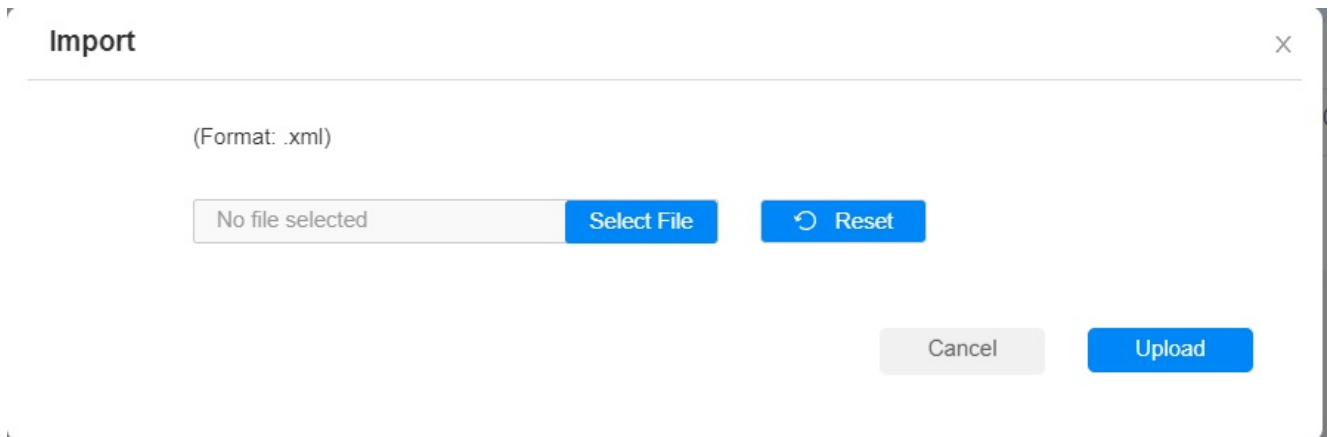
Day  Mon  Tue  Wed  
 Thur  Fri  Sat  
 Sun  Check All

Start Time - End Time  🕒 -  🕒

## Import and Export Door Access Schedule

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

To do so, navigate to **Setting > Schedule**, then click **Import**.

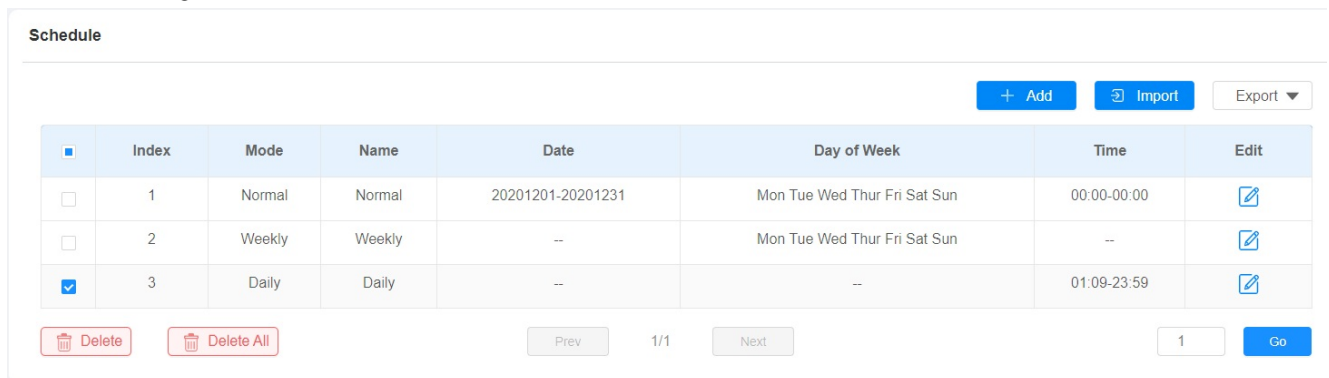


**Note:**

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

## Edit the Door Access Schedule

Go to **Setting > Schedule** interface.



**Note**

- It only supports .xml format file for importing and exporting the schedule.
- The access control schedule synchronized from the SmartPlus cannot be edited or deleted.

# Door Unlock Configuration

## 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.

Go to **Access Control > PIN Setting > Public PIN** interface.

Public PIN	
Enabled	<input checked="" type="checkbox"/>
PIN Code	<input type="text" value="33333333"/>

### Parameter Set-up:

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

#### Note:

- Public PIN code will not be valid until the function is turned on.

## Add User

You need to create a user before you can set up a private PIN, RF card, and face data for the user. Also, you can set up access control settings and related call settings for the user.

User Basic	
User ID	<input type="text" value="3"/>
Name	<input type="text"/>

## Configure Private PIN Code



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 configuration on the web **Directory > User**, then click **+Add**.

Access Control >> User

User

All User ID/Name/Code Search + Add

User >> Add User

User Basic

User ID

Name

Private PIN

Code

After that, scroll down to **Access Setting**, and select relays and the door access schedule for the PIN code.

#### Access Setting

Allow To Open  RelayA  RelayB

Floor No. None x

Web Relay 0

Authentication Mode Any Method

1 item Unselected Schedules

1002:Never

1 item Selected Schedules

1001:Always

#### Parameter Set-up:

- **Allow to Open:** select the relays to be triggered by the PIN code.

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

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

Private PIN

PIN Mode	PIN
Display Temp PIN Icon	<input checked="" type="checkbox"/>

### Parameter Set-up:

- **PIN Mode:** select access mode between **PIN** and **APT#+PIN**. If you select PIN, then you are only required to enter 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.
- **Display Temp PIN Icon:** enable it if you want to display the QR code Icon, which you can press for the QR code access on the screen.

### Note:

- **QR Code** can only be applicable when the device is added to the Akuvox SmartPlus.

## Mifare Card

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

To do so, go to **Access Control > Card setting > Mifare Card Encryption**.

#### Mifare Card Encryption

Enabled	<input type="checkbox"/>
Sector/Block	<input type="text" value="0"/> / <input type="text" value="0"/>
Block Key	<input type="text" value="*****"/>

#### Parameter Set-up:

- **Sector/Block:** enter the sector and block in which the card number is located in the Mifare Card. For example, the card number can be in sector 3 and block 3 in the card.
- **Block Key:** enter the block password to access the block to get the code.

#### Note

- Mifare card must be encrypted first otherwise the card reader will not read the card for the door opening.

## Configure RF Card for Door Unlock

### Configure RF Card on the Web Interface

To configure RF card, navigate to **Directory > User**, then click **+Add**. After that, enter the user information, and obtain the QR code.

User

All	<input type="text" value="User ID/Name/Code"/>	Search	+ Add
-----	--	--------	-------

RF Card

Code

<input type="text"/>	Obtain	Delete
Add		

#### Note

- Please refer to PIN code access schedule selection for the RF card user(s)-specific door access.
- RF card with 13.56 MHz and 125 KHz can be applicable to the door phone for door access.

## 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.

Access Control >> Card Setting

RFID

IC Card Display Mode	8HN ▼
ID Card Order	Normal ▼
ID Card Display Mode	8HN ▼

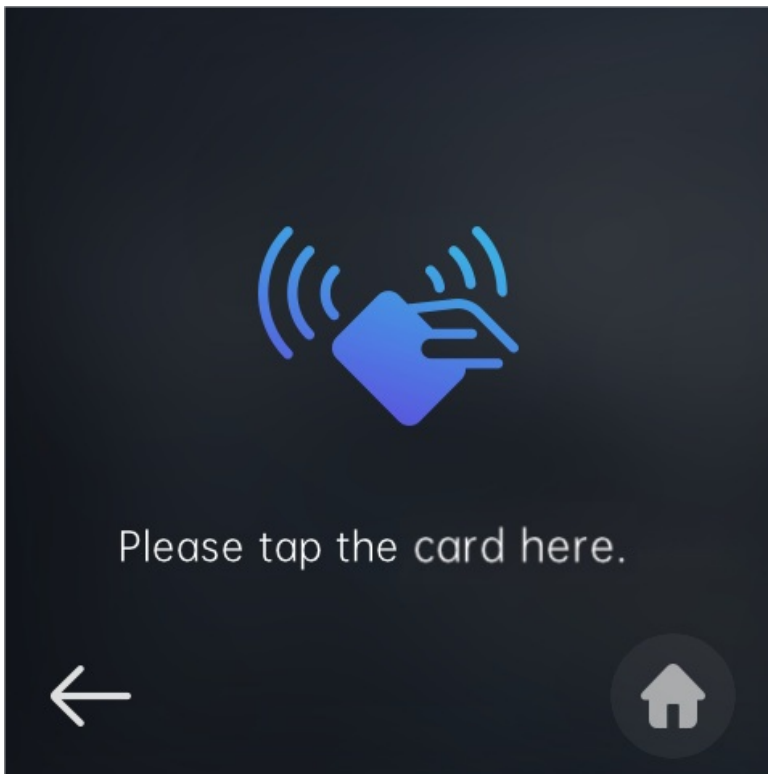
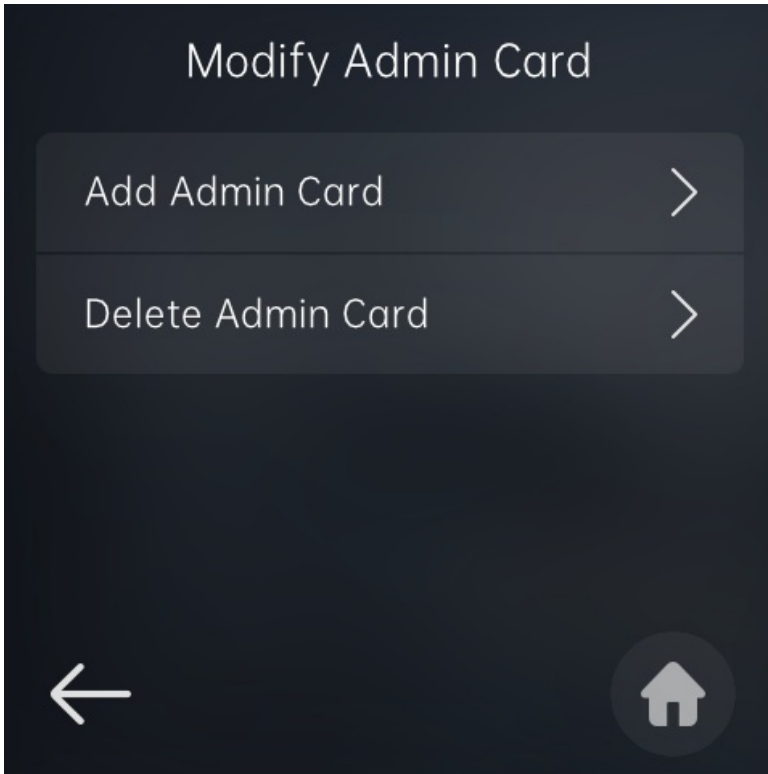
### Parameter Set-up:



- **IC Card Display Mode:** select the card code format for the **IC card** for the door access among seven format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D**. The card code format is **8HN** by default in the door phone.
- **ID Card Order:** select normal or reversed display of ID card.
- **ID Card Display Mode:** select the card format for the **ID Card** for the door access among seven format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D**. The card code format is **8HN** by default in the door phone.

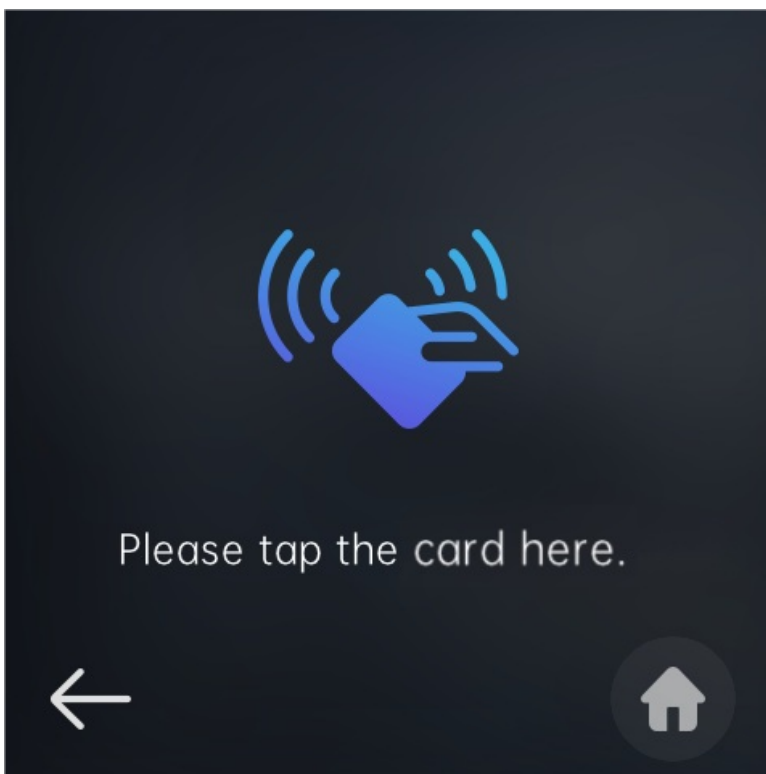
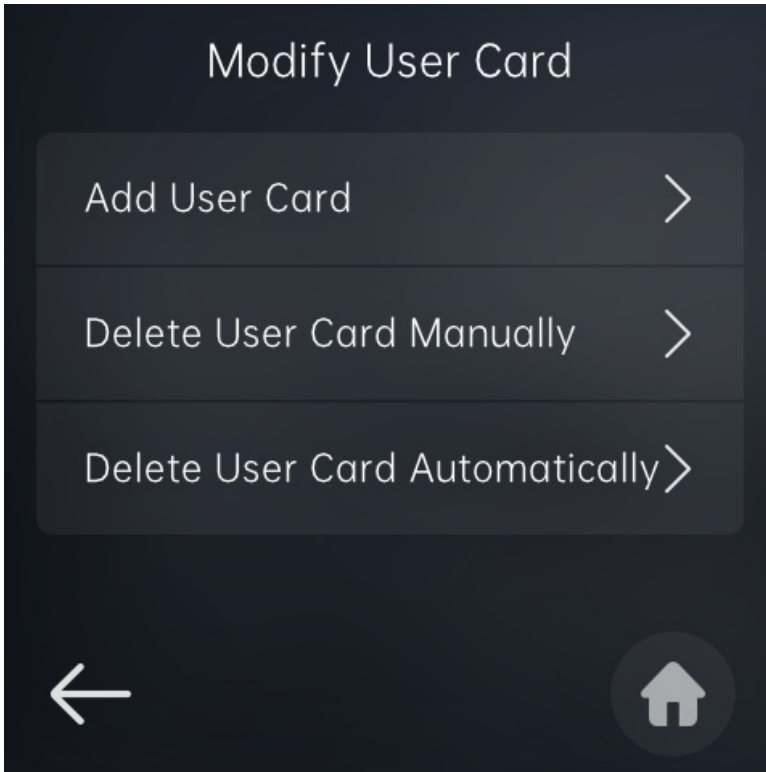
## Configure RF Card on the Device

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 configure admin card, go to **Advanced Settings > Admin Access > Modify Admin Card > Add Admin card.**



To configure user card, press  icon on the home screen, then enter your setting default setting password 3888, then press  icon on the keypad. After that select **Modify User Card**, then enter the system PIN code, which is **2396** by default. Then press **Add User Card**.



## Configure Facial Recognition for Door Unlock

You can import the face data to the device on the web interface. To do so, navigate to **Directory > User**, then click **+Add**. After that, enter the user information, and upload the face recognition photos.

The screenshot shows a web interface for user management. At the top, it says "Access Control» User". Below this, there is a "User" section with a search bar containing "User ID/Name/Code", a "Search" button, and a "+ Add" button. Below the "User" section is a "Face" section. It displays "Status: Unregistered" and "Photo" with two buttons: "Import" (with a camera icon) and "Reset" (with a refresh icon).

### 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** tab.
- **Photo:** select the picture with jpg or png format to be uploaded to the device and press if you want to clear the picture uploaded.

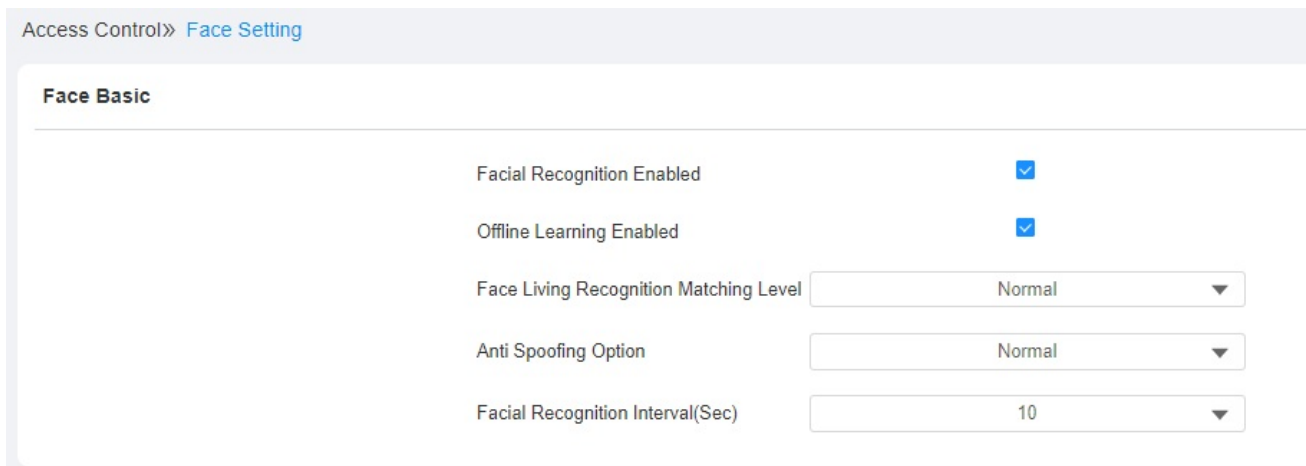
### Note

- Pictures to be uploaded should be in jpg or png format.
- Please refer to PIN code access schedule selection for face recognition user(s)-specific door access.

## Basic Facial Recognition Configuration on the Web Interface

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

Navigate to **Access Control > Face Setting > Face Basic** interface.



Parameter	Value
Facial Recognition Enabled	<input checked="" type="checkbox"/>
Offline Learning Enabled	<input checked="" type="checkbox"/>
Face Living Recognition Matching Level	Normal
Anti Spoofing Option	Normal
Facial Recognition Interval(Sec)	10

### Parameter Set-up:

- **Offline Learning Enabled:** enable it 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.
- **Face Living Recognition Matching Level:** click to select the facial recognition accuracy level among four options: **Low, Normal, High, Highest**. For example, if you select **Highest** then 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.
- **Anti-Spoofing Option:** select **Anti-spoofing** level among four options: **Low, Normal, High, Highest, Close**. 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 time interval between every two facial recognition from 2-60Sec. For example, if you select **5** then you have to wait for 5 seconds. Before you are allowed to perform the facial recognition again.

#### Note

- Please refer to PIN code access schedule selection for Face recognition user(s)-specific door access.

## Edit the User-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

All

<input type="checkbox"/>	Index	Source	User ID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/>	1	Local	1213	Jim			None	0	1001-1;	<input type="button" value="Edit"/>
<input type="checkbox"/>	2	Local	12345	Ryan			None	0	1001-1;	<input type="button" value="Edit"/>

1/1

**Note**

- Users synchronized from the SmartPlus cannot be edited or deleted.

## Import and Export User Data of Access Control

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

To configure the configuration on the web **Directory** > **User** > **Import/Export User** interface.

Import/Export User

User Data

## Configure Bluetooth for Door Unlock

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

To set up the function, navigate to **Access Control > BLE > BLE Basic**.

Access Control >> BLE

**BLE Basic**

Enable BLE Function	<input checked="" type="checkbox"/>
Enable Hands Free Mode	<input checked="" type="checkbox"/>
Trigger Distance	<input type="text" value="About 1 meter"/>
Open Door Interval(Sec)	<input type="text" value="10"/>

**Parameter Set-up:**

- **Enable Hands Free Mode:** if enabled, you can gain door access hands-free. If disabled, you have to wave your hand in front of the door phone for door access.
- **Trigger Distance:** set the triggering distance of the Bluetooth for the door access. You select **About 1 meter**, **Within 1 meter**, and **More than 2 meters**. The trigger distance is **3 meters maximum**.
- **Open Door Interval (Sec):** select the time interval between every two Bluetooth door accesses.

## Configure Open Relay via HTTP for Door Unlock

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

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

Open Relay via HTTP

Enabled	<input checked="" type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="password" value="*****"/>

**Parameter Set-up:**

- **User Name:** 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:

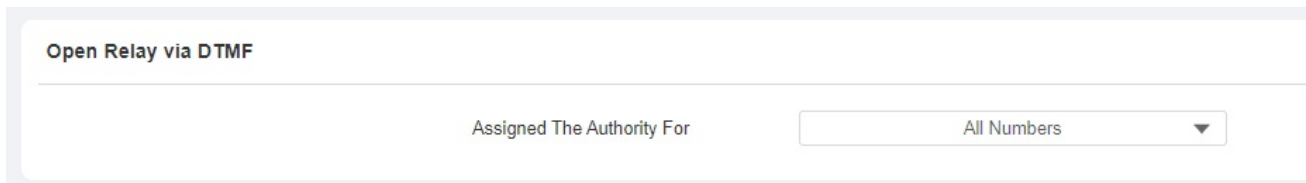
```
http://192.168.35.127/fcgi/do?  
action=OpenDoor&UserName=admin&Password=12345&DoorNum=1
```

#### Note

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

## Configure Open Relay via DTMF for Door Unlock

You can authorize the contacts to be able to unlock the door via DTMF or deny all the contacts for the DTMF unlock if needed. To do so, navigate to **Access Control > Relay > Open Relay via DTMF**.



Open Relay via DTMF

Assigned The Authority For

#### Parameter Set-up:

Select **All Numbers**, **None** or **Only Contact List** to be allowed to unlock the door DTMF.

## 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.

Press the QR code icon on the left lower corner.

Enter PIN

Press  to confirm.



You can also enter the code.



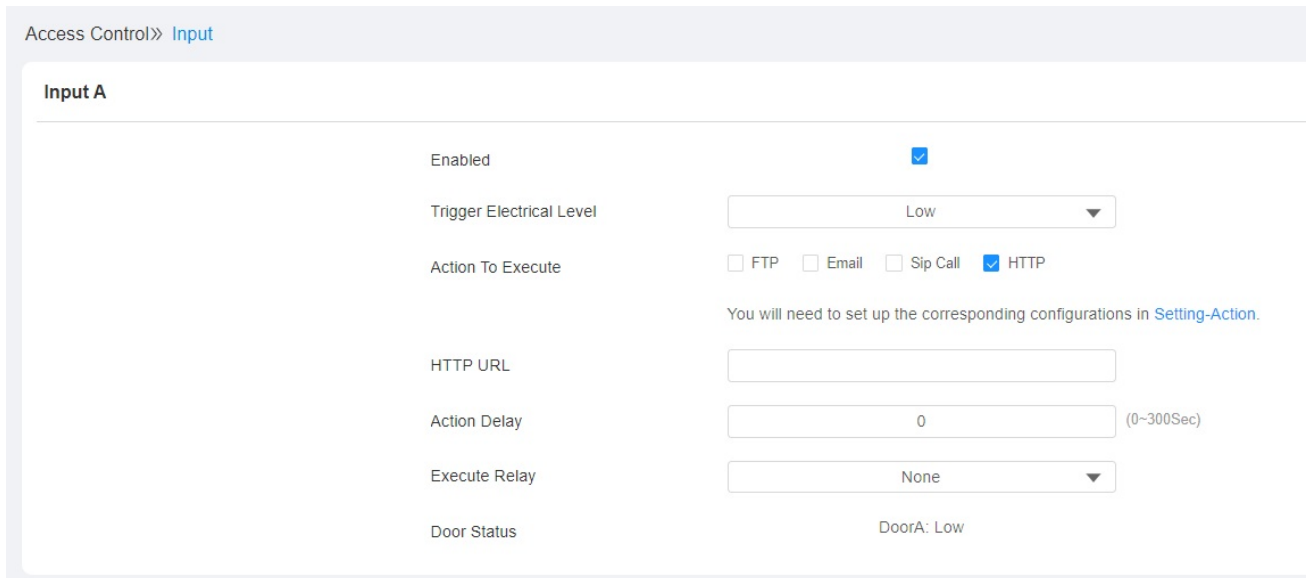
#### Note

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

## Configure Exit Button for Door Unlock

When you need to open the door from inside using the Exit button installed by the door, you can configure the door phone Input to trigger the relay for the door access.

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



Access Control >> Input

Input A

Enabled	<input checked="" type="checkbox"/>
Trigger Electrical Level	Low
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> Email <input type="checkbox"/> Sip Call <input checked="" type="checkbox"/> HTTP
You will need to set up the corresponding configurations in <a href="#">Setting-Action</a> .	
HTTP URL	
Action Delay	0 (0~300Sec)
Execute Relay	None
Door Status	DoorA: Low

### 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 four options: **FTP**, **Email**, **HTTP**, and **SIP Call**.
- **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 your press the button.
- **Execute Relay:** set up relays to be triggered by the input.

## Configure Reception Tab for Door Unlock

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 configure the configuration on the web **Setting > Key/Display > Speed Dial Setting**.

Speed Dial Setting

Account	<input type="text" value="Auto"/>
Open Relay	<input type="text" value="None"/>
Action To Execute	<input type="checkbox"/> HTTP

**Parameter Set-up:**

- **Account:** select the account you want to dial out a call from.
- **Open Relay:** select the relay(s) to be triggered by pressing the **Reception** icon.
- **Action To Execute:** tick the check box to enable the HTTP option.
- **HTTP URL:** enter the URL command to be sent for door access. For example:  
`http://192.168.35.127/fcgi/do?
 action=OpenDoor&UserName=admin&Password=12345&DoorNum=1`

## Door Entry Authentication

You can gain door entry through single authentication or double authentication. You can set up dual authentication for greater security. To set it up, go to **Directory > User**, then click **+Add**, then scroll down to **Access Setting**.

Access Setting

Allow To Open	<input checked="" type="checkbox"/> RelayA <input type="checkbox"/> RelayB
Floor No.	<input type="text" value="None x"/>
Web Relay	<input type="text" value="0"/>
Authentication Mode	<input type="text" value="Face + PIN"/>

1 item    Unselected Schedules

1002:Never

1 item    Selected Schedules

1001:Always

**Parameter Set-up:**

- **Authentication Mode:** select your door entry authentication mode (**Any Method, Face+PIN, Face+RF Card, and RF Card+PIN**). If you select **Any Method**, then you can gain door entry using any one of the access methods you have set up (single

authentication). If you select any of the double authentication modes such as **Face+PIN**, you are required to pass both face and PIN authentication for the door entry.

# Security

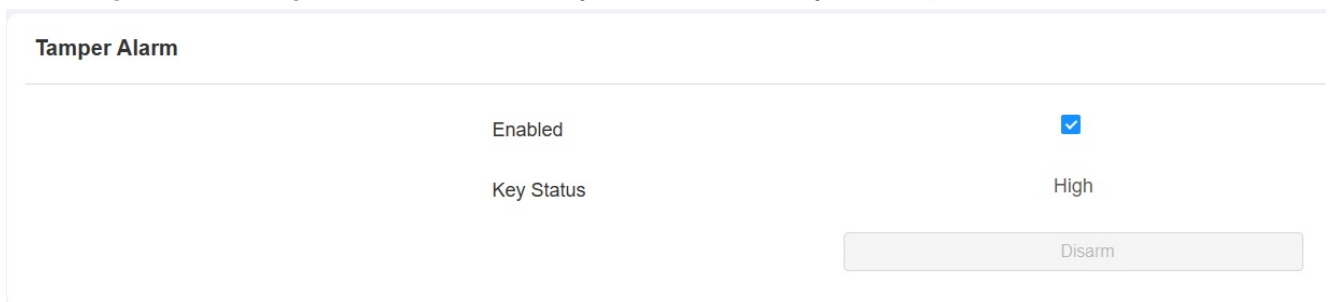
## Tamper Alarm Setting

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 door phone detects a change in its gravity value from the original one.

## Configure Tamper Alarm on the Device Web

You can customize the tamper alarm and adjust sensor settings on the web interface.

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



The screenshot shows the 'Tamper Alarm' configuration page. It features a table with two rows of settings. The first row is for 'Enabled', which is checked with a blue checkbox. The second row is for 'Key Status', which is set to 'High'. Below the table is a 'Disarm' button.

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

### Parameter Set-up:

- **Key Status:** tamper alarm will not be triggered unless the key status is shifted from **Low** to **High** status.

## 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?>

mac=\$mac:ip=\$ip:model=\$model:firmware=\$firmware:card\_sn=\$card\_sn

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

**Action URL**

Enabled	<input type="checkbox"/>
Type	GET ▼
Make Call	<input type="text"/>
Hang Up	<input type="text"/>
RelayA Triggered	<input type="text"/>
RelayB Triggered	<input type="text"/>
RelayA Closed	<input type="text"/>
RelayB Closed	<input type="text"/>
InputA Triggered	<input type="text"/>
InputB Triggered	<input type="text"/>
InputC Triggered	<input type="text"/>
InputA Closed	<input type="text"/>
InputB Closed	<input type="text"/>
InputC Closed	<input type="text"/>
Valid Code Entered	<input type="text"/>
Invalid Code Entered	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<input type="text"/>

## Virtual PIN

The virtual PIN allows you to protect your PIN code from being leaked to someone.

To enable the virtual PIN feature, navigate to **Access Control > PIN Setting > Virtual PIN**.

Access Control» [PIN Setting](#)

**Virtual PIN**

Enabled

**Parameter Set-up:**

- **Enabled:** if enabled, you are allowed to put fake numbers on both sides of the PIN code for PIN code protection. For example, if your password is 1234567 you can put 99 and 88 on both sides (99123456788). And the virtual password is matched to the users by the number of digits that are matched. For example, if user A has greater number of digits that are matched with the virtual password entered than user B, then it will be regarded as user A's password. However, when the double authentication is applied, then the virtual password will be matched with the users who passes the first level of authentication, for example, Face + PIN.

**Note**

- This feature is not used for Public PIN and Apartment+PIN.

## Client Certificate Setting

Certificates ensure communication integrity and privacy. To use the SSL protocol, you need to upload the right certificates for verification.


## Web Server Certificate

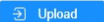
It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. The Akuvox door phone only accepts certificates in the \*.PEM file format.

To upload a Web Server certificate on the device web **System > Certificate > Web Server Certificate**.

System >> Certificate

Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	 Delete


Web Server Certificate Upload  Upload

## Client Certificate

This certificate verifies the server to the Akuvox door phone when they want to connect using SSL. The door phone verifies the server's certificate against its client certificate list.

To upload and configure client certificates on the same page.

**Client Certificate**

	Index	Issue To	Issuer	Expire Time
 No Data				

Delete
Delete All

Index Auto ▼

Client Certificate Upload Upload

Only Accept Trusted Certificates

### Parameter Set-up:

- **Index:** select the desired value from the drop-down list of Index. If you select **Auto** value, the uploaded certificate will be displayed in numeric order. If you select the value from **1 to 10**, the uploaded certificate will be displayed according to the value that the user selected.
- **Client Certificate Upload:** locate and upload the desired certificate (\*.pem only).
- **Only Accept Trusted certificates:** if you select **Enabled**, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If you select **Disabled**, the phone will not verify the server certificate no matter whether the certificate is valid or not.

## Motion Detection

Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved, and activates the system to perform the appropriate action.

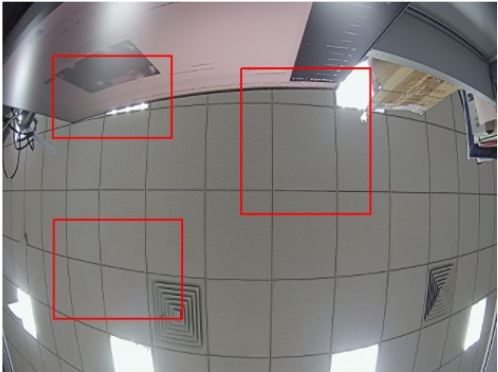
To set up motion detection, navigate to **Surveillance > Motion > Motion Detection Options**.

Surveillance» [Motion](#)

**Motion Detection Options**

Suspicious Object Moving Detection

Detection Area



Clear

Detection Accuracy  (0-6)

Time Interval  (3-65535Sec)

Action To Execute  FTP  Email  Sip Call  HTTP

Move the arrow to the start point where you left click and hold down the mouse button, then drag the arrow to select an area. You can draw up to three detection area.

### Parameter Set-up:

- **Suspicious Moving Object Detection:** select from **Video Detection**, **IR Detection**, and **Disabled**. IR detection is based on sensing infrared radiation emitted or reflected by objects, while video detection focuses on analyzing visual information captured through cameras.
- **Detection Area :** select the detection area in the video. You can select up to three detection areas.
- **Time Interval:** set the time interval in the same way as you do on the device.
- **Detection Accuracy:** set the detection accuracy for the detection sensitivity. The higher value, the greater sensitivity. The default detection accuracy value is **3**.
- **Action to Execute :** select the notification type: **FTP**, **Email**, **HTTP**, **SIP Call**. If you select **FTP** , then the FTP notification will be sent to a designated server. If you select **Email** then the notification will be sent in the form of emails when motion detection is triggered.

Scroll down the page, you can also set the motion detection time schedule.

**Motion Detect Time Setting**

---

Day	<input checked="" type="checkbox"/> Mon	<input checked="" type="checkbox"/> Tue	<input checked="" type="checkbox"/> Wed
	<input checked="" type="checkbox"/> Thur	<input checked="" type="checkbox"/> Fri	<input checked="" type="checkbox"/> Sat
	<input checked="" type="checkbox"/> Sun	<input type="checkbox"/> CheckAll	

Start Time - End Time

00:00	-	23:59
-------	---	-------

## Security Notification Setting

### Email Notification Setting

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

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

**Email Notification**

---

Sender Email Address	<input type="text"/>
Receiver Email Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP Username	<input type="text"/>
SMTP Password	<input type="password" value="....."/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>

### 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.

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

FTP Notification

FTP Server	<input type="text"/>
FTP Username	<input type="text"/>
FTP Password	<input type="password" value="....."/>

**Parameter set-up:**

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

## 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 the web **System > Security > Session Time Out** interface.

Session Time Out

Session Time Out Value	<input type="text" value="900"/>	(60~14400Sec)
------------------------	----------------------------------	---------------

**Parameter Set-up:**

- **Session Time Out Value:** set the automatic web interface log-out timing ranging from 60 seconds to 14400 seconds. The default value is 900.

# 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 door phones 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 door phone. You can add a camera's stream by adding its URL.

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

## RTSP Stream Monitoring

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

## RTSP Basic Setting

To configure the configuration on the web **Surveillance > RTSP > RTSP Basic** interface.

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
Mjpeg Authorization Enabled	<input checked="" type="checkbox"/>
Authentication Mode	<input type="text" value="Digest"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

### Parameter Set-up:

- **RTSP Authorization Enabled:** 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.

## 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 parameters for H.264 codec on the web **Surveillance > RTSP > H.264 Video Parameters** interface.

### H.264 Video Parameters

Video Resolution	720P
Video Framerate	30fps
Video Bitrate	2048kbps
2nd Video Resolution	VGA
2nd Video Framerate	30fps
2nd Video Bitrate	512kbps

### 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 in 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 bitrate among six options: **“128 kbps”**, **“256kbps”**, **“512 kbps”**, **“1024 kbps”**, **“2048 kbps”**, **“4096 kpbs”** according to your network environment. The default video bitrate is **“2048 kpbs”**.
- **2 nd Video Resolution:** select video resolution for the second video stream channel. While the default video solution is **“VGA”**.
- **2 nd Video Framerate:** select the video framerate for the second video stream channel. **“30fps”** is the video frame rate by default for the second video stream channel.
- **2 nd Video Bitrate:** select video bitrate among the six options for the second video stream channel. While the second video stream channel is **“512 kpbs”** by default.

## Note

- X912 has two channels of RTSP video streaming with two formats.

For example:

Channel 1: `rtsp://192.168.1.40/live/ch00_0.`

Channel 2: `rtsp://192.168.1.40/live/ch00_1.`

## MJPEG Image Capturing

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

Go to **Surveillance > MJPEG** interface.

MJPEG Server

Enabled



Image Quality

VGA



### Parameter Set-up:

- **Image Quality:** select the quality for the image capturing among six options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P**,  
After the MJPEG service is enabled, you can capture the image from the door phone using following three types of URL format:
- `http:// device ip:8080/picture.cgi`
- `http://device ip:8080/picture.jpg`
- `http://device ip:8080/jpeg.cgi`

For example, if you want to capture the JPG format image of 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.

## ONVIF

You can access the real-time video from the door phone 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 door phone will allow its video to be visible on other devices.

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

Basic Setting

Discoverable	<input checked="" type="checkbox"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

**Parameter Set-up:**

- **Discoverable:** tick the check box to enable the Discoverable ONVIF mode. If you select “Discoverable” then the video from the door phone camera can be searched by other devices.
- **User Name:** enter the user’s name. The user’s 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.

## Live Stream

There are two ways to check the real-time video from the door phone. 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 view the real time video on the web **Surveillance > Live Stream** interface.

Surveillance» [Live Stream](#)



# 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 on the web **Status > Call Log** interface.

### Call Log

Save Call Log Enabled

Save Picture Enabled

All ▾

Start Time ~ End Time

Name/Number

Search

Export ▾

<input type="checkbox"/>	Index	Type	Date	Time	Local Identity	Name	Number	Action
<input type="checkbox"/>	1	Dialed	2022-09-06	15:27:53	6339100009@test84.akuvox.com	Ryan	6336000002@test84.akuvox.com	<a href="#">Picture</a>
<input type="checkbox"/>	2	Dialed	2022-09-06	13:51:11	6339100009@test84.akuvox.com	Ryan	6336000002@test84.akuvox.com	<a href="#">Picture</a>
<input type="checkbox"/>	3	Dialed	2022-09-06	13:50:16	6339100009@test84.akuvox.com	Ryan	6339100007@test84.akuvox.com	<a href="#">Picture</a>
<input type="checkbox"/>	4	Dialed	2022-09-06	11:53:10	6339100009@test84.akuvox.com	11	11@test84.akuvox.com	<a href="#">Picture</a>

### 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.
- **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.

## Go to Status > Access Log interface.

### Access Log

Save Access Log Enabled

Save Picture Enabled

Export Picture Enabled

All  ~

<input type="checkbox"/>	Index	User ID	Name	Code	Type	Door ID	Date	Time	Status	Action
<input type="checkbox"/>	1	--	Unknown	12348	Private PIN	--	2022-09-06	15:30:26	Failed	<a href="#">Picture</a>
<input type="checkbox"/>	2	--	Unknown	111	Private PIN	--	2022-09-06	15:30:13	Failed	<a href="#">Picture</a>
<input type="checkbox"/>	3	1	Jim	CBD432DB	Card	A	2022-09-06	14:55:11	Success	<a href="#">Picture</a>

### Parameter Set-up:

- **Status:** select between **Success** and **Failed** options to search for successful door accesses or Failed door accesses.
- **Name/Code:** select the **Name** and **Code** options to search door log by the name or by the PIN code.

# 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"/>
Remote System Port	<input type="text" value="(1-65535)"/>

### 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 purpose. The default log level is “3”. the higher the level is, the more complete the log is.
- **Export Log:** click the **Export** tab to export temporary debug log file to a local PC.
- **Export Debug Log:** click the **Export** tab to export debug log file to a local PC.
- **Remote System Server:** enter the remote server address to receive the device log. And the remote server address will be provided by Akuvox technical support.

## 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:** click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **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 packet even after the data packets reached its 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.






# Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Go to **System > Upgrade > Basic** interface.

---

Firmware Version	912.30.1.118
Hardware Version	912.1
Upgrade	
Reset To Factory Setting	
Reboot	

---

## Upgrade ×

---

(Format: .rom)

No file selected  

Reset After Upgrade

Cancel

Install

### Note:

- Firmware files should be .rom format for 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)

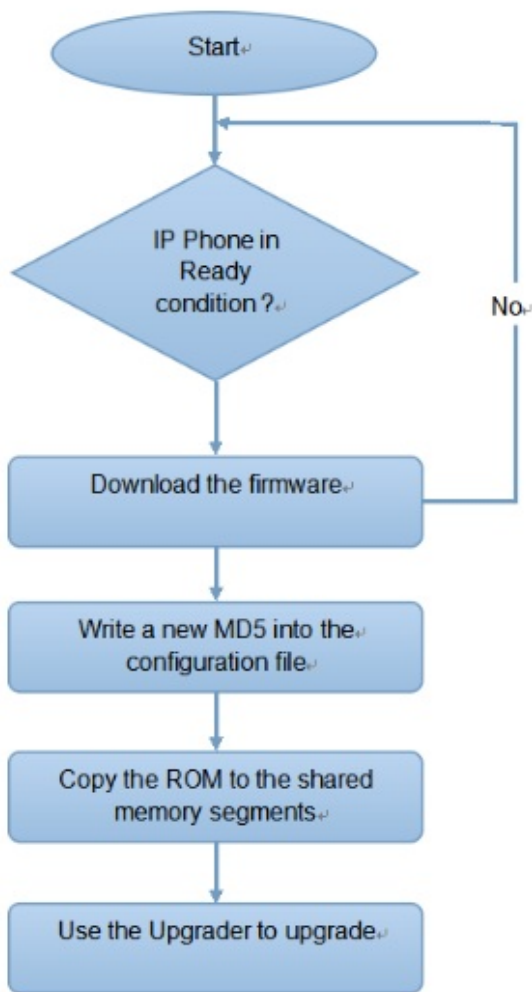
# Auto-provisioning via Configuration File

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 intercom 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.

To configure the configuration on the web **System > Auto Provisioning > Automatic 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"/>

### Parameter Set-up:

- **Mode:**
  - **Power On:** allows the device to perform Autop every time it boots up.
  - **Repeatedly:** allows the device to perform Autop according to the schedule.
  - **Power On + Repeatedly:** combines **Power On** and **Repeatedly** modes, allowing the device to perform Autop every time it boots up or according to the schedule.
  - **Hourly Repeat:** allows the device to perform Autop every hour.
- **Schedule:** when **Power On + Repeatedly** mode is selected, you can select the specific day and time for the Autop.

- **Clear MD5:** used to compare the existing autop file with the autop file in the server, if the files are the same, then the provisioning will be stopped, thus avoiding unnecessary auto provisioning.

## 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 the **System > Auto Provisioning > Automatic Autop**, and set up Autop server on the **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:** the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username:** set up a user name if the server needs a user name to be accessed.

- **Password:** set up a password if the server needs a password to be accessed.
- **Common AES Key:** set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key(MAC):** set up AES code for the intercom to decipher the MAC-based auto-provisioning configuration file.

### Note

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

### Tip

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

## 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



# 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 the configuration on the web **Device > Wiegand > Wiegand** interface.

### Wiegand

Wiegand Display Mode	<input type="text" value="8HN"/>
Wiegand Card Reader Mode	<input type="text" value="Wiegand-26"/>
Wiegand Transfer Mode	<input type="text" value="Input"/>
Wiegand Input Data Order	<input type="text" value="Normal"/>
Wiegand Output Data Order	<input type="text" value="Normal"/>
Wiegand Output CRC Enabled	<input checked="" type="checkbox"/>

### Parameter Set-up:

- **Wiegand Display Mode:** select Wiegand Card code format among **8H10D; 6H3D5D; 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.**
- **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:** select **Input, Output, Convert to Card No.Output Wiegand.** If the door phone is used as a receiver, then set it as **Input** for the door phone. Select **Output** if you want to make the door phone the sender. Select **Convert to Card No.Output Wiegand** if you want wiegand output to be converted to card number before sending it from the door phone to a receiver.
- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Normal** and **Reversed.** If you select **Reversed**, then the input card number will be reversed and vice versa.
- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Normal** and **Reversed** if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output CRC Enabled:** This function is used for Wiegand data inspection. It is

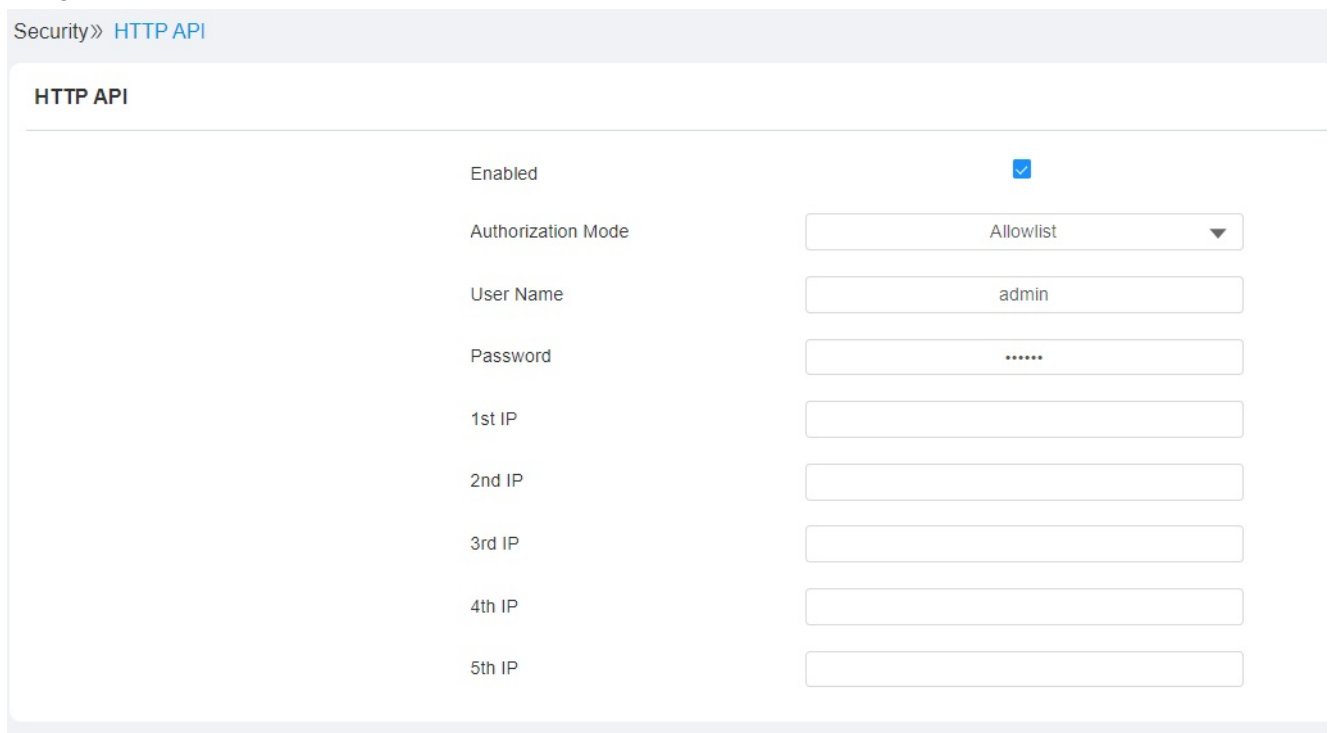


turned on by default. If it is not turned on, you might not be able to integrate the device with third-party devices.

## Integration via HTTP API

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

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



Security >> HTTP API

### HTTP API

Enabled	<input checked="" type="checkbox"/>
Authorization Mode	Allowlist ▼
User Name	admin
Password	*****
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

### Parameter set-up:

- **Enabled:** enable or disable the HPTT API function for the third-party integration. For example, if the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode:** select among the following options: **None**, **Normal**, **Allowlist**, **Basic**, **Digest**, and **Token** for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when **Basic** or **Digest** authorization mode is selected. The default user name is Admin.
- **Password:** enter the password when **Basic** or **Digest** authorization mode is selected. The default user name is Admin.
- **1st IP-5th IP:** enter the IP address of the third-party devices when the **Allowlist**

**authorization** is selected for the integration.

Please refer to the following description for the Authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developer only
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The allowlist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the username and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	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".
6	Token	This mode is used by Akuvox developer only.

## Power Output Control

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

You can go to **Access Control > Relay >12V Power Output**.

12V Power Output

---

Relay ID	RelayA
Power Output Type	<input style="width: 100%;" type="text" value="Disabled"/>

---

### Parameter Set-up:

- Power Output Type:** select **Disabled** to disable the power output function. Select **Always** to enable the access controller to provide continuous power to the third-party device. Select **Triggered By Open Relay** if you want the X912 to provide power to the third party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high. Select **Security Relay A** if you need to configure security relay.

# 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, navigate to **Device > Lift Control**.

**Lift Control List**

---

Lift Control List Akuvox EC32 ▼

---

**Akuvox EC32 Advanced Setting**

---

Server IP

Server Port  (1~65535)

---

**Akuvox EC32 Action**

---

Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Floor No. Parameter	<input type="text" value="\$floor"/>
URL To Trigger Specific Floor	<input type="text" value="/cdor.cgi?open=0&amp;door=\$floor"/>
URL To Trigger All Floors	<input type="text" value="/cdor.cgi?open=8"/>
URL To Close All Floors	<input type="text" value="/cdor.cgi?open=9"/>

## Parameter Set-up:

- **Lift Control List:** select **None** to disable the function, and select the **Akuvox E32** to integrate the door phone with the Akuvox EC32 controller.
- **Server IP:** the IP address of the Akuvox controller server.
- **Server Port:** the server port of the Akuvox controller server.
- **Username:** the username of the lift controller for the authentication.
- **Password:** the password of the lift controller for the authentication.
- **Floor NO. Parameter:** enter the floor number parameter provided by Akuvox. The default parameter string is "\$floor". You can define your own parameter string if needed.
- **URL To Trigger Specific Floor:** enter the Akuvox lift control URL for triggering a specific

floor. The URL is /cdor.cgi?open=0&door= \$ floor, but the string “\$floor” at the end must be identical to the parameter string you defined.

- **URL To Trigger All Floors:** enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors:** enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.

## Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature.

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

Advanced Setting

---

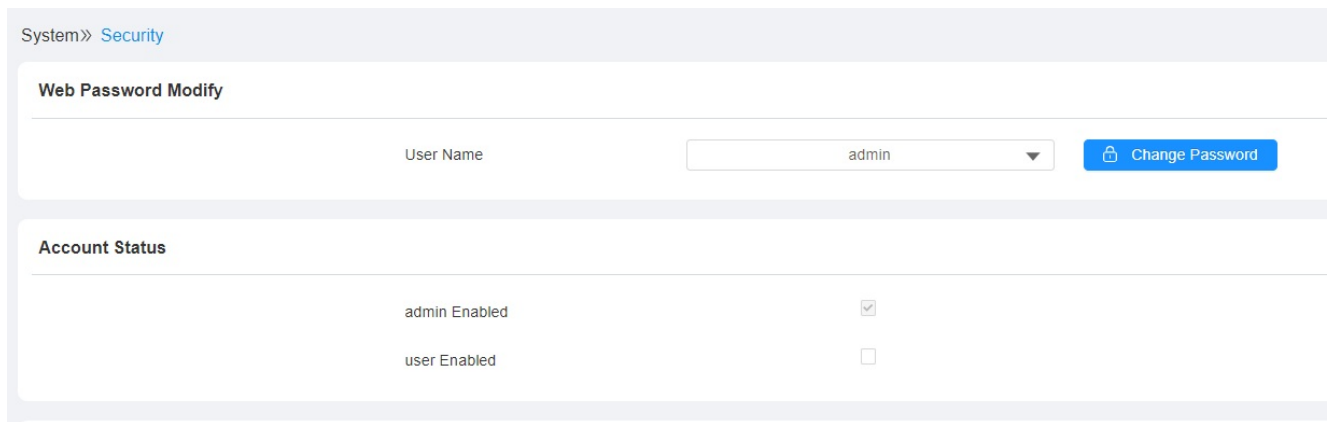
Milestone Enable

# Password Modification

## Modifying Device Web Interface Password

To change the default web password on web **System > Security > Web Password Modify** interface.

Select **admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.



System >> Security

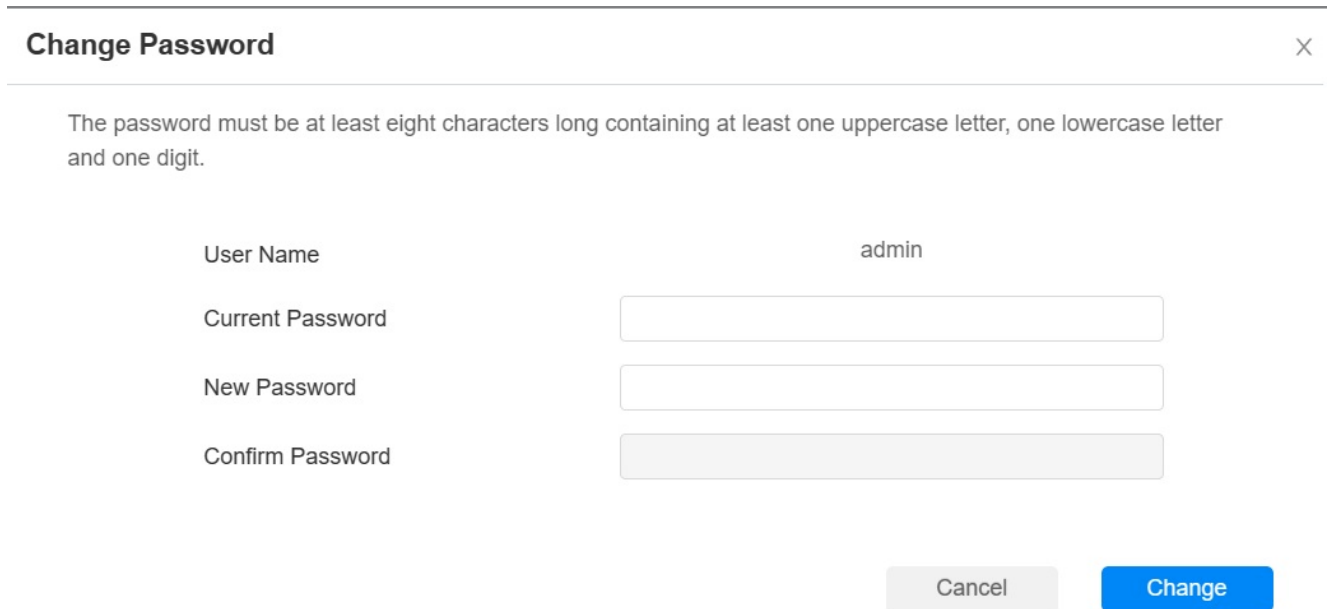
Web Password Modify

User Name: admin

Change Password

Account Status

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



Change Password

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

User Name: admin

Current Password: [input field]

New Password: [input field]

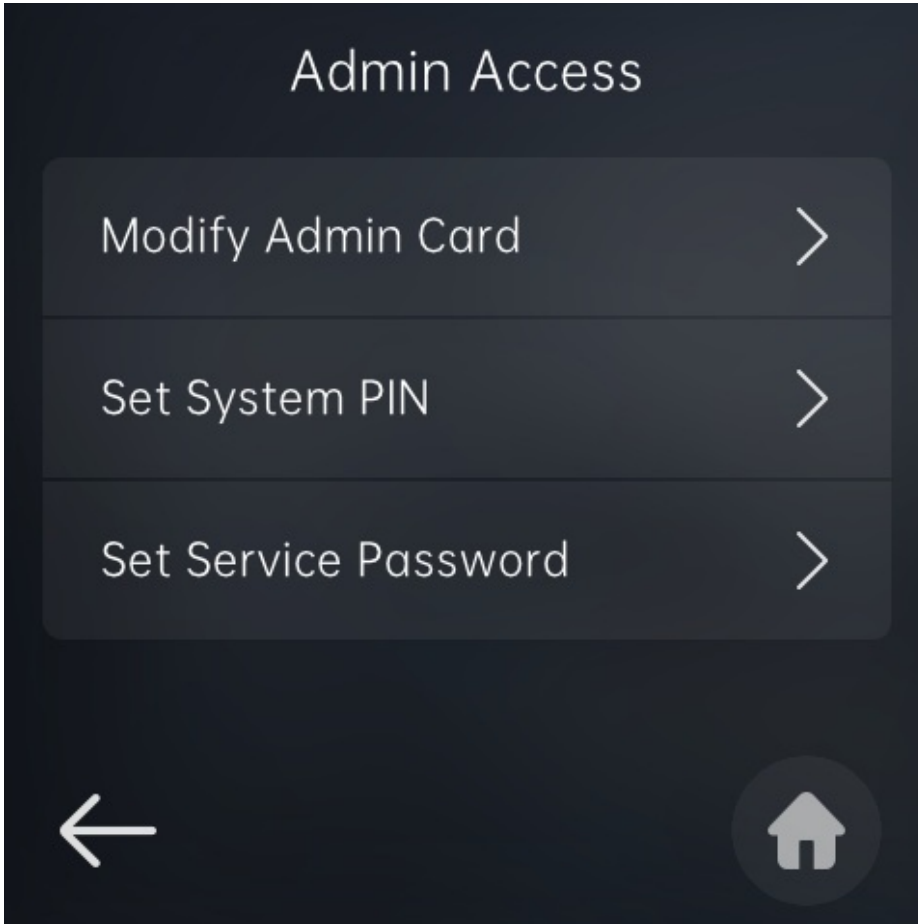
Confirm Password: [input field]

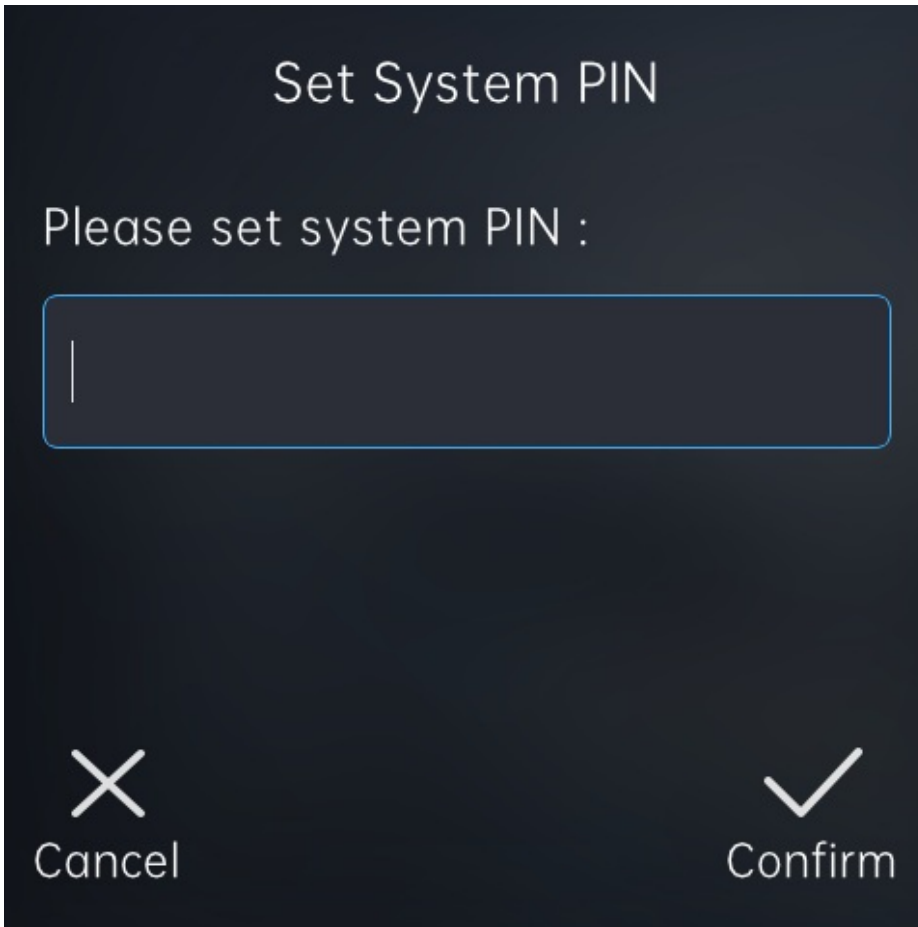
Cancel Change

## Modifying System Password

The system PIN code is used to access the device system. You can modify the system PIN code on the device and web interface.

Go to **Advance Settings > Admin Access > Set System PIN**.

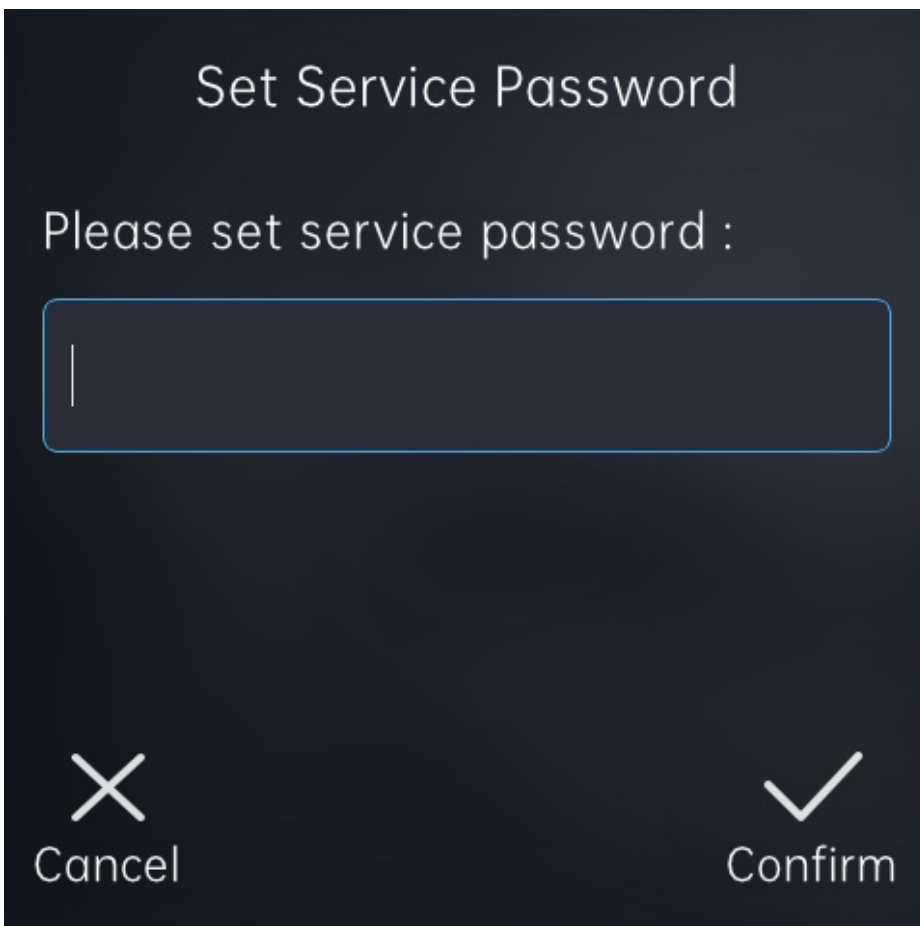
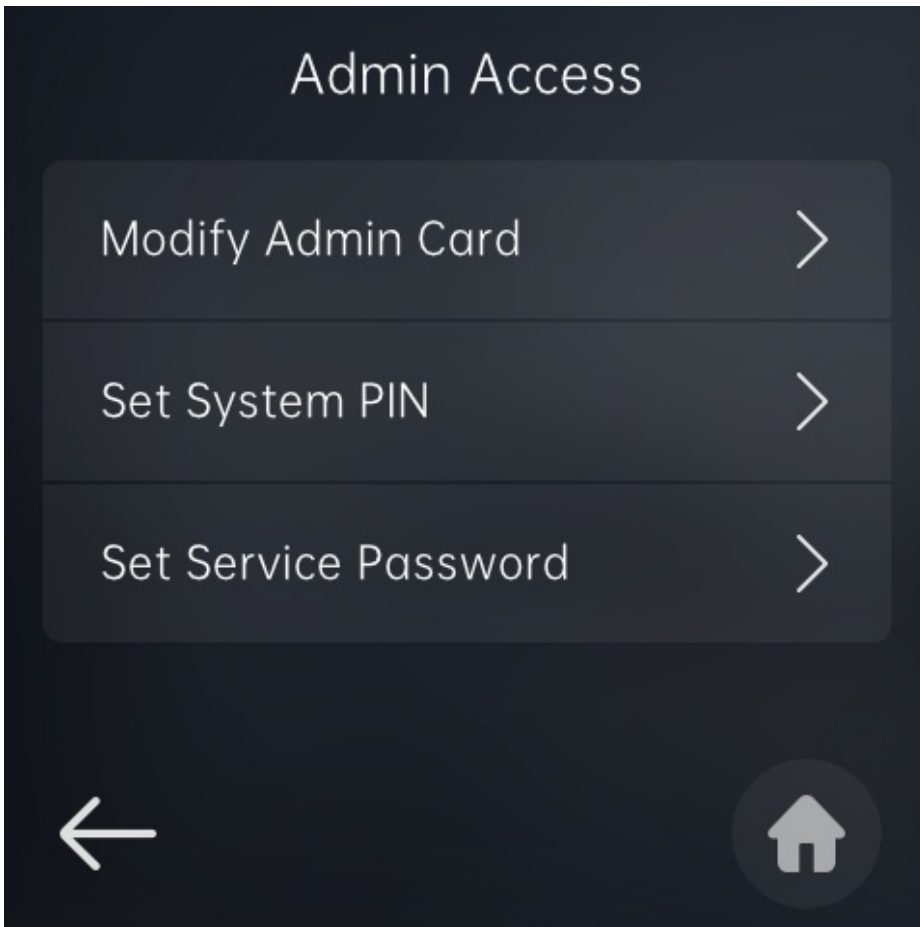




## Modifying Setting Password

Setting PIN code is used to access the device setting. You can modify the system PIN code on the device and web interface.

Go to **Advanced Settings > Admin Access > Set Service Password.**







# 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 restart the system setting on the web **System > Upgrade > Basic** interface. To set the schedule on **System > Auto Provisioning > Reboot Schedule**.

### Basic

Firmware Version 912.30.1.118

Hardware Version 912.1

Upgrade 

Reset To Factory Setting 

Reboot 

### Reboot Schedule

Mode

Schedule

(0~23Hour)

To reboot the device, go to **Advanced Setting > Reboot**.

## Advanced Setting

Admin Access



Reboot



Restore



## Reboot

Confirm to reboot?



Cancel



Confirm

## Reset

If you want to reset the device system to the factory setting, you can it on the web **System > Upgrade > Basic** interface.

### Basic

Firmware Version 912.30.1.57

Hardware Version 912.0

Upgrade

 Upgrade

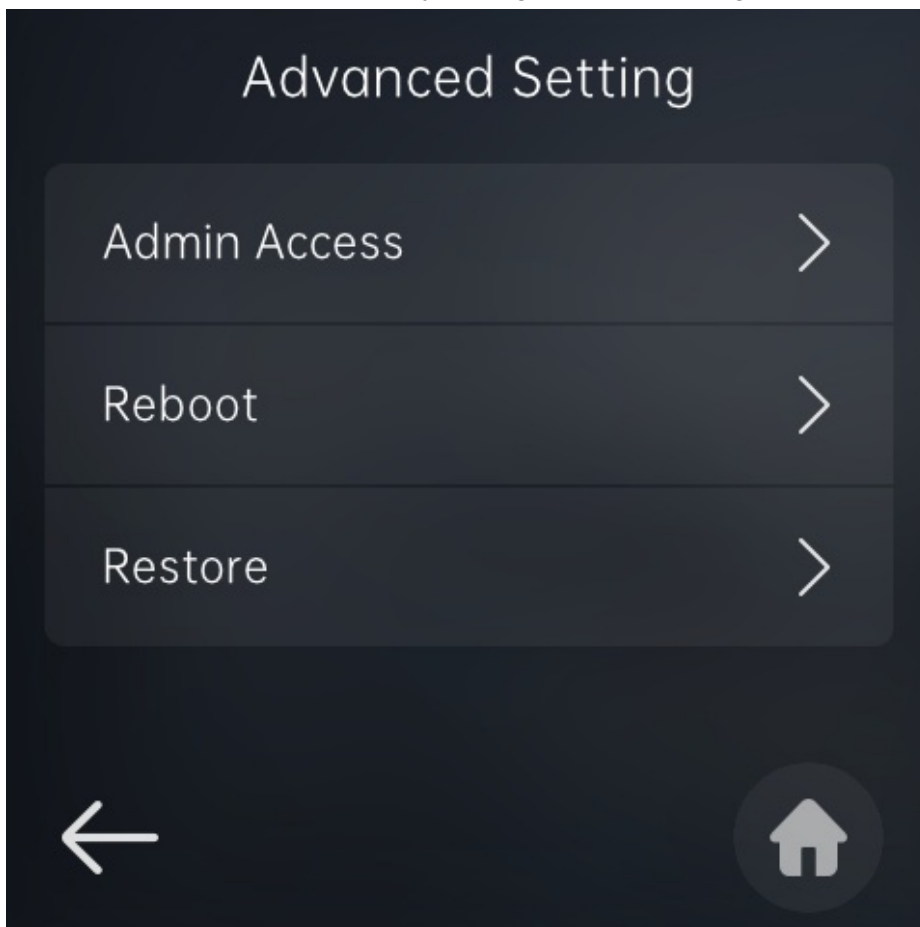
Reset To Factory Setting

 Reset

Reboot

 Reboot

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



## Restore

Please confirm if you want to restore to the factory settings.



Cancel



Confirm