



AKUVOX X912S DOOR PHONE

Administrator Guide

About This Manual

Thank you for choosing Akuvox X912S series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 912.30.1.46 version, and it provides all the configurations for the functions and features of X912S series door phone. Please visit [Akuvox forum](#) or consult technical support for any new information or latest firmware.

Introduction of Icons and Symbols



Warning:

- Always abide by this information in order to prevent the person from injury.



Caution:

- Always abide by this information in order to prevent damages to the device.



Note:

- Informative information and advice from the efficient use of the device.

Related Documentation

You are advised to refer to the related documents for more technical information via the link below:

<https://knowledge.akuvox.com>



FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.

Table of Contents

1. Product Overview	1
2. Change Log	2
3. Model Specification	3
4. Introduction to Configuration Menu	5
5. Access the Device	7
5.1. Access the Device Setting on the device	7
5.2. Access the Device Setting on the Web Interface	8
6. Language and Time Setting	9
6.1. Language Setting	9
6.2. Time Setting	9
7. LCD Setting	11
7.1. LCD Screen Brightness Setting on the Web Interface	11
7.1.1.1. LCD Screen Brightness Setting on the Device	12
8. Keypad Light Setting	13
9. Screen Display Configuration	14
9.1.1. Screensaver Configuration	14
9.1.2. Upload Screensaver	15
9.1.3. Configuration for Scenario-based Screen Display Mode	16
9.1.3.1. Default (Buttons) Mode Home Screen Display	17
9.1.3.2. Directory Mode Home Screen Display	18
9.1.3.3. Speed Dial Mode Home Screen Display	18
9.1.3.4. Customized Text Mode Home Screen Display	19
9.1.3.5. Dial Screen Prompt Display	19
9.1.3.6. Open Door Text Prompt Display	20
10. Volume and Tone Configuration	21
10.1. Volume Configuration	21
10.1.1. Configure Volume on the Device	21
10.1.1.1. Configure Volume on the Web Interface	22
10.1.2. Upload Open-door Tone	23
11. Network Setting	25
11.1. Device Network Configuration	25
11.2. Device Local RTP configuration	26
11.3. Device Deployment in Network	27
11.4. NAT Setting	28
12. Intercom Call Configuration	29
12.1. IP call & IP Call Configuration	29
12.1.1. Make IP Calls	29
12.1.2. IP Call Configuration	30
12.2. SIP Call & SIP Call Configuration	30
12.2.1. SIP Account Registration	30

12.2.1.1. Configure SIP Account	31
12.2.2. SIP Server Configuration	32
12.2.3. SIP Call DND&Return Code Configuration	33
12.2.4. Configure Outbound Proxy Server	33
12.2.5. Configure Data Transmission Type	34
12.3. Dial Options Configuration	35
12.3.1. Quick Dial by Number Replacement	35
12.4. Call Auto-answer Configuration	36
12.5. Manager Dial Call	37
12.6. Web Call	39
13. Call Settings	40
13.1.1. Maximum Call Duration Setting	40
13.1.2. Maximum Dial Duration Setting	41
13.1.3. Hang Up After Open Door	41
13.1.4. Audio& Video Codec Configuration for SIP Calls	42
13.1.4.1. Audio Codec Configuration	42
13.1.4.2. Video Codec Configuration	43
13.2. Configure DTMF Data Transmission	44
14. Phone Book Configuration	45
14.1. Manage Contact Groups	46
14.1.1. Contact Configuration	46
14.1.1.1. Contact List Display Setting	47
15. Relay Setting	49
15.1. Relay Switch Setting	49
15.2. Web Relay Setting	50
15.2.1. Configure Web Relay	51
15.2.2. Configure Security Relay	52
16. Door Access Schedule Management	54
16.1. Configure Door Access Schedule	54
16.1.1. Create Door Access Schedule	54
16.1.2. Import and Export Door Access Schedule	56
16.1.3. Edit the Door Access Schedule	57
17. Door Unlock Configuration	58
17.1. Configure PIN Code for Door Unlock	58
17.1.1. Configure Public PIN code	58
17.1.2. Configure Private PIN Code	59
17.1.3. Configure Private PIN Access Mode	60
17.2. Configure RF Card for Door Unlock	61
17.2.1. Configure RF Card on the Web Interface	61
17.2.2. Configure RF Card Code Format	62
17.2.3. Configure RF Card on the Device	63
17.3. Configure Facial Recognition for Door Unlock	64
17.4. Basic Facial Recognition Configuration on the Web Interface	66
17.5. Edit the User-specific door access data	67

17.6. Import and Export User Data of Access Control	68
17.7. Configure Bluetooth for Door Unlock	68
17.8. Configure Open Relay via HTTP for Door Unlock	69
17.9. Configure Open Relay via DTMF for Door Unlock	70
17.10. Unlock by QR Code	71
17.11. Configure Exit Button for Door Unlock	71
17.12. Configure Reception Tab for Door Unlock	72
18. Security	74
18.1. Tamper Alarm Setting	74
18.1.1. Configure Tamper Alarm on the Device	74
18.2. Action URL	75
18.3. Virtual PIN	76
18.4. Client Certificate Setting	77
18.4.1. Web Server Certificate	77
18.4.2. Client Certificate	77
18.5. Motion Detection	78
18.6. Security Notification Setting	80
18.6.1. Email Notification Setting	80
18.6.2. FTP Notification Setting	82
18.7. Web Interface Automatic Logout	82
19. Monitor and Image	84
19.1. RTSP Stream Monitoring	84
19.1.1. RTSP Basic Setting	84
19.1.2. RTSP Stream Setting	85
19.2. MJPEG Image Capturing	86
19.3. ONVIF	87
19.4. Live Stream	88
20. Logs	89
20.1. Call Logs	89
20.2. Door Logs	90
21. Debug	91
21.1. System Log for Debugging	91
21.2. PCAP for Debugging	92
22. Firmware Upgrade	93
23. Backup	94
24. Auto-provisioning via Configuration File	95
24.1. Provisioning Principle	95
24.2. Configuration Files for Auto-provisioning	96
24.3. AutoP Schedule	96
24.4. PNP Configuration	97
24.5. DHCP Provisioning Configuration	98
24.6. Static Provisioning Configuration	99
25. Integration with Third Party Device	102
25.1. Integration via Wiegand	102

25.2. Integration via HTTP API	103
25.3. Power Output Control	104
26. Lift Control	105
27. Password Modification	107
27.1. Modifying Device Web Interface Password	107
27.2. Modifying System Password	109
27.3. Modifying Setting Password	109
28. System Reboot&Reset	110
28.1. Reboot	110
28.2. Reset	111
29. Abbreviations	113
30. Contact us	115


1. Product Overview

Akuvox X912S is 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 allows featured customization to better suit your operation habit. X912S has multiple ports, such as RS485 and Wiegand ports, 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. X912S series door phone is applicable to mid-end and upscale residential buildings, upscale single tenant residential buildings.

2. Change Log

The change log will be updated here along with the changes in the new software version.

3. Model Specification

	X912S
Model & Feature	
Display	8 Inch color TFT LCD
Touch Screen	√
Button	√
Housing Material	Stainless Steel and Aluminum
Relay In	3
Relay Out	2
Alarm In	X
RS485	√
PoE	POE+
Resolution	480x480p
Brightness	680nits
RAM	1GB
ROM	8GB
Card Reader	13.56MHz & 125kHz, NFC
Wi-Fi	X
Bluetooth	√
IP Rating	IP65
IK Rating	IK10
Temperature detection	X
Face recognition	√
LTE	X
USB	X
External SD card	X

Wall Mounting	√
Flush Mounting	X
Desk Mounting	X
Wall Mounting Dimension	234x94.5x34mm
POE+ Standby Power Consumption	9.5W
POE+ Full Load Power Consumption	11.5W
Power Adapter Standby Power Consumption	8.5
Power Adapter Full Load Power Consumption	22.5W
Color Option	Tarnish Grey

4. 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 setting, 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.
- **Settings:** 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.

- **Mode selection:**

1. **Discovery mode:** it is a plug and play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to network. It is super time-saving mode, and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations previously by the administrator.
2. **Cloud mode:** Akuvox SmartPlus is an all-in-one management system. Akuvox Cloud is a mobile service that allows audio, video, remote access control between smart phones and Akuvox intercoms. All configurations in the device will be issued automatically from cloud. If users decide to use Akuvox SmartPlus, please contact Akuvox technical support, and they will help you configure the related settings before using.
3. **SDMC mode:** SDMC (**SIP Device Management Controller**) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for the door access, intercom, monitoring, alarm and so on. It is a convenient tool for the property manager to manage, operate and maintain the community.

- **Tool selection**

Akuvox has many configuration tools for you to set up devices more conveniently. Here we list some common tools, please contact your administrator to get the tool if you need them.

1. **SDMC:** SDMC is suitable for the management of Akuvox devices in large communities, including access control, resident information, remote device control, etc.
2. **Akuvox Upgrade tool:** upgrade Akuvox devices in batch on a LAN (**Local Area Network**)
3. **Akuvox PC Manager:** distribute all configuration items in batch on a LAN.

4. **IP scanner:** it is used to search Akuvox device IP addresses on a LAN.

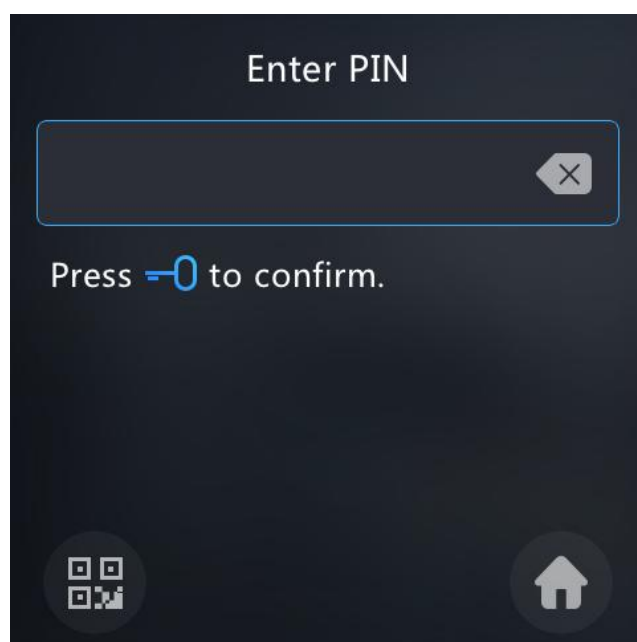
5. Access the Device

X912S series door phone system setting can be either accessed on the device directly or on the device web interface.

5.1. Access the Device Setting on the device

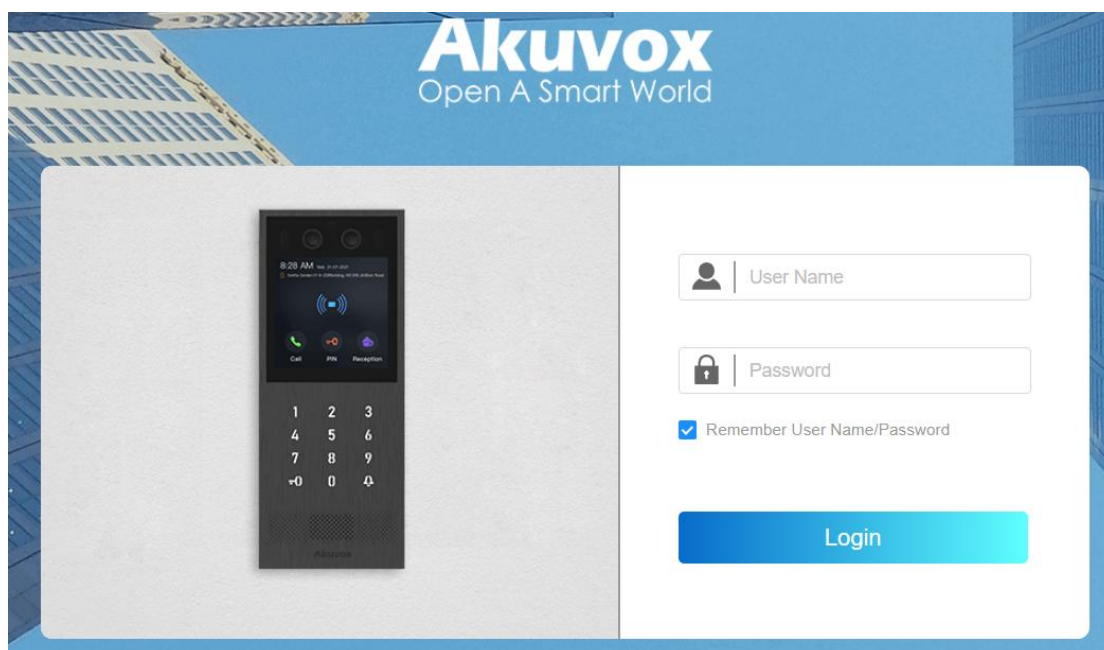
Before configuring Akuvox X912S, please make sure the device is installed correctly and connect to a normal network. Using Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to login in to the web browser by user name and password **admin** and **admin**.

To access the device system setting on the device, you can press **=0** 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 **=0** , then enter the default Setting PIN code "3888".



5.2. 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. Please refer to the URL below for the IP scanner application:
<https://knowledge.akuvox.com/docs/how-to-obtain-ip-address-via-ip-scanner-1?highlight=IP%20SCANNER>
- Google Chrome browser is strongly recommended.
- The Initial user name and password are **admin** and please be case-sensitive to the user names and passwords entered.

6. Language and Time Setting

6.1. Language Setting

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

Setting >> Time/Lang

LCD Language

Mode English

6.2. Time Setting

Time setting on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. And when your time zone is selected, the device will automatically notify the NTP server of its time zone so that the NTP server can synchronize the time zone setting in your device. To configure the configuration on the web **Setting > Time/Lang > Time** 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

- **Date Format:** select the date format as you like among three format options: "M-D-Y"; "D-M-Y"; "Y-M-D" and then press the **Confirm** tab for the confirmation.
- **Time Format:** you can either select 12 hour or 24-hour time format as you like, and then press the Confirm tab for the confirmation.
- **Time Zone:** select the specific time zone depending on where the device is used and then press **Confirm** tab for the confirmation. The default time zone is **GMT GMT+0.00**.
- **Primary/Secondary Server:** the time zone server, normally it will automatically obtain the time when connecting to the network. The alternate server will take effect when the primary server is invalid.
- **Update Interval:** to configure interval between two consecutive NTP requests.
- **System Time:** indicate the current device time.

7. LCD Setting

If you want to brighten up the screen in order to see the screen at greater ease in an environment with higher light intensity, you need to set up the related parameters.

7.1. LCD Screen Brightness Setting on the Web Interface

On the web interface, you can set and adjust 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)

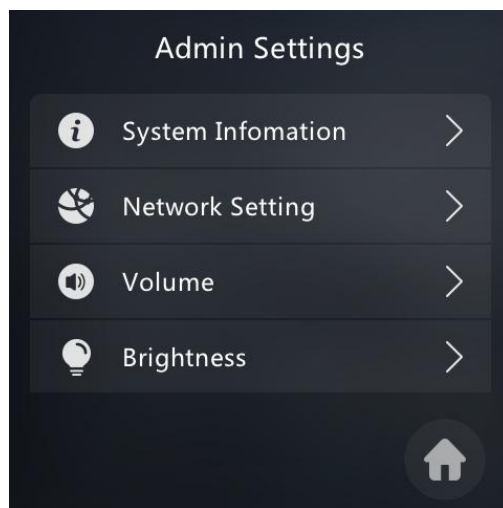
Parameter Set-up:

- **Mode:** click to select "**Manual**" or "**Auto**" mode for the backlight. Backlight will be adjusted automatically for the screen back light 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 day time with the value ranging from (1-255).
- **Backlight Brightness Night:** adjust the back light for the screen saver in the night with the value ranging from (1-255).

- **Backlight Brightness Of Screensaver (night)**: adjust the backlight for the screensaver in the night time with the value ranging from (0-255).

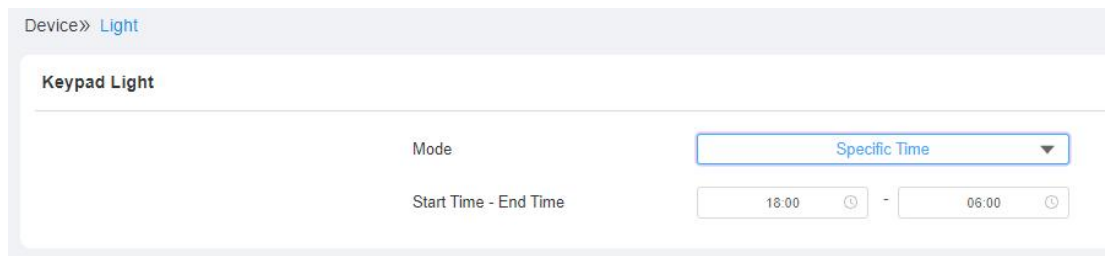
7.1.1.1. LCD Screen Brightness Setting on the Device

To set screen brightness on the device, select **Brightness**, and select **Automatic** for automatic brightness adjustment or select **Manual** to adjust the brightness manually.



8. 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.

9. Screen Display Configuration

X912S door phone allows you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

9.1.1. Screensaver Configuration

Sleep mode and screen saver mode are designed for screen protection. You can set the two modes to prevent the device screen from getting overheated and to reduce energy consumption. You can define when the device should go into sleep mode, screen saver mode, and turn off the screen. On web interface, navigate to **Device > LCD > Sleep** interface.

The screenshot shows the 'Sleep' configuration page with the following settings:

Parameter	Value
Auto-Sleep Time	30 minutes
Screensaver Mode	Default (Animation of Tap Card)
Screensaver Time(Sec)	5 seconds
Wake Up Mode	Manual

Parameter Set-up:

- **Auto-Sleep Time:** if you set sleep time, for example as "15" seconds, then the device will go in to 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 "Default (Animation of Tap Card)" to display Akuvox Logo pictures as screen saver; select "Image" 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 waked up when the device detects approaching object or operation. Select “ Manual” if you wake up the screen through touching.

9.1.2.Upload Screensaver

You can upload screen saver pictures one by one on the device web interface for publicity purpose or 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.

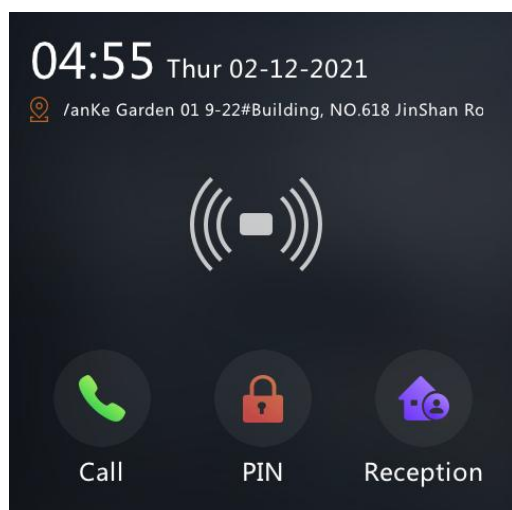
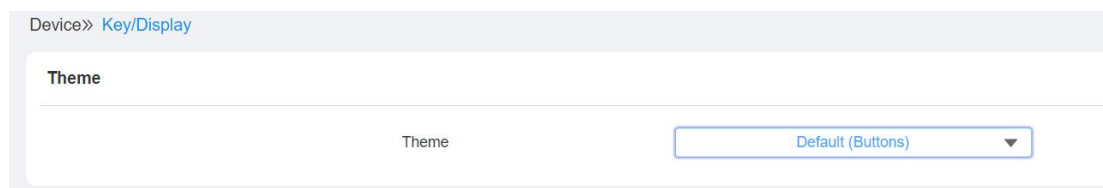


Note:

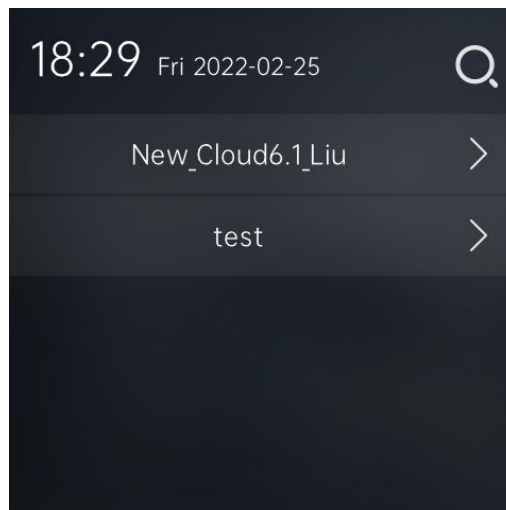
- The previous pictures with a specific ID order will be overwritten when repetitive designation of pictures to the same ID order occurred.

9.1.3. Configuration for Scenario-based Screen Display Mode

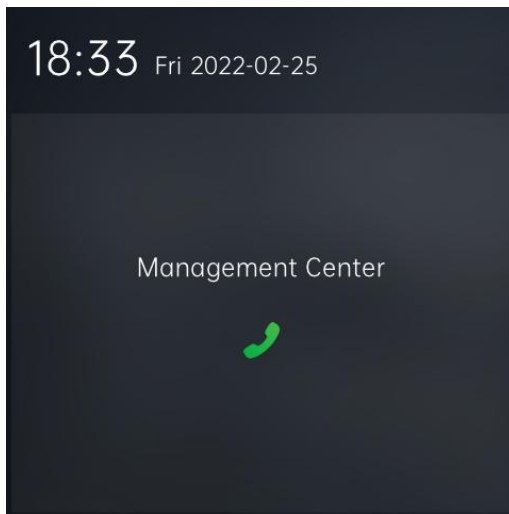
X912S door phones offer you four types of screen display modes for the different applications: **Default(buttons)**mode, **Directly Mode**, **Speed Dial Mode**, and **Customized Text Mode**. On the web interface, navigate to **Setting > Key/Display > Theme**.



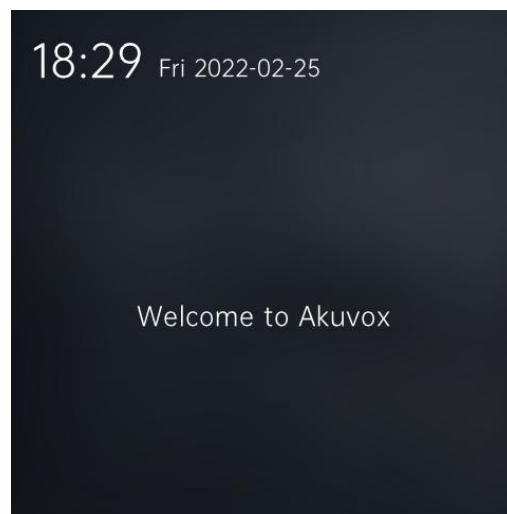
Default(buttons) Mode



Directory Mode



Speed Dial Mode



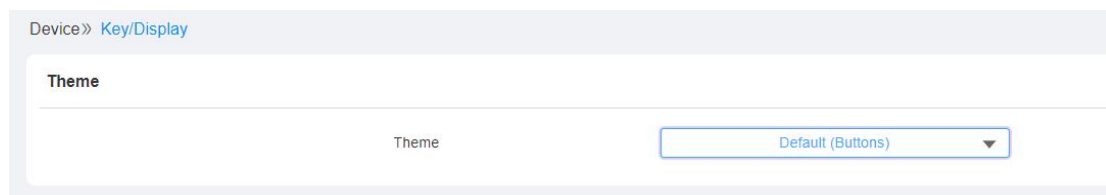
Customized Text Mode

Parameter Set-up:

- **Theme:** select the home screen display mode you need.

9.1.3.1. 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 in Homepage**.



Keys in Homepage

Index	Type	Name	Number
1	Call		
2	PIN		
3	Speed Dial		

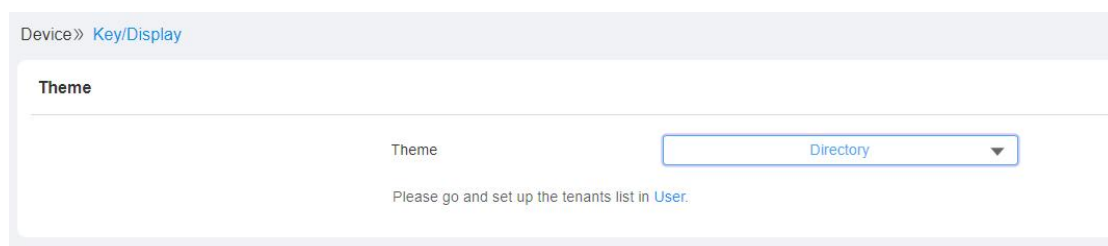
- **Theme:** select the default(Buttons) mode.
- **Type:** select the tab type (Call, PIN, Speed Dial, Directory, Temp Key-QR code) corresponding to the ID order which indicates the tab position. For

example, if you want to make **Temp Key** tab to 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 setup numbers, like Speed Dial feature.

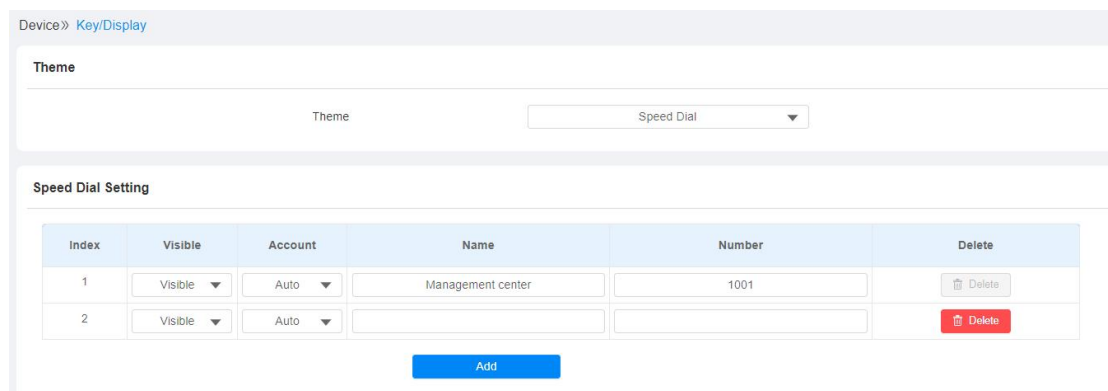
9.1.3.2. Directory Mode Home Screen Display

You can set the Contact directory as the home screen so that you can easily dial out the contact number.



9.1.3.3. 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**.





Note:

- X912S supports up to five speed dial display on the screen.

9.1.3.4. Customized Text Mode Home Screen Display

X912S allows you to display (people's name or company name etc.) on the home screen for identification purpose. To do so, navigate to **Setting > Key/Display > Customized Text**.

Device >> Key/Display

Theme

Theme Customized Text

Customized Text

Text Akuvox



Note:

- X912S supports 10-digit character maximum in length for the customized text.

9.1.3.5. Dial Screen Prompt Display

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

Prompt Of The Call Page

Text Prompt



Note:

- X912S supports 128-digit character maximum in length for the text prompt.

9.1.3.6. Open Door Text Prompt Display

You can enable or disable the open door prompt if needed. 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"/>

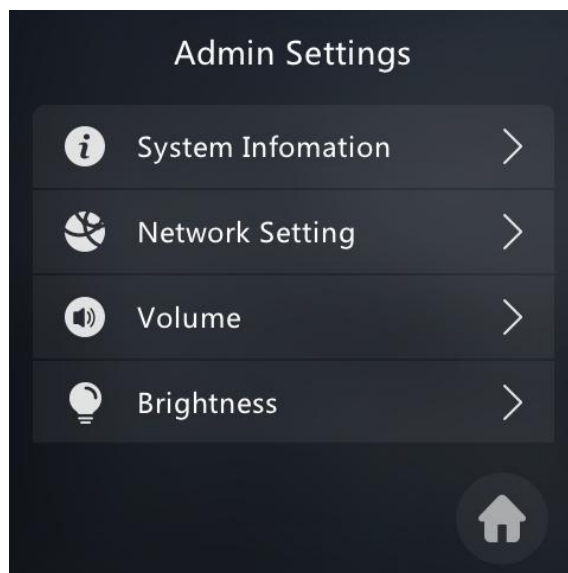
10. Volume and Tone Configuration

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

10.1. Volume Configuration

10.1.1. Configure Volume on the Device

You can adjust the microphone volume, speaker volume, keypad volume, and AD volume on the device. To configure the language display on the device **Basic 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.
- **Speaker volume:** adjust the loudspeaker volume according to your need. The default Mic volume is 50.
- **Keypad Volume:** adjust the keypad volume for the keypad touching sound. The default Mic volume is 50.
- **Mic Volume:** adjust the microphone volume according to your need. The default Mic volume is 50.

10.1.1.1. Configure Volume on the Web Interface

On the web interface, you can set the temper alarm volume, Mic volume, etc.

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

Mic Mode

Select On

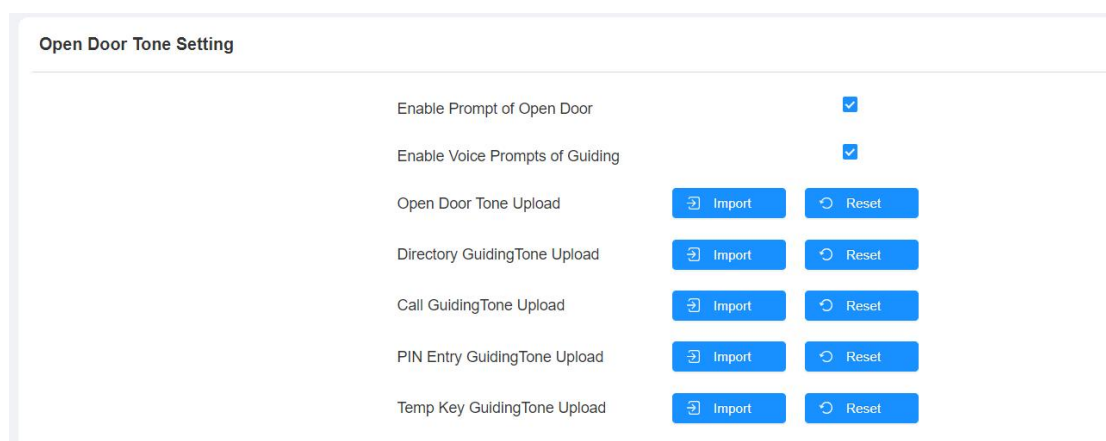
Parameter Set-up:

- **Tamper Alarm Volume:** set the tamper alarm volume from 1-100 according to your need. The default volume is "50".

- **Prompt Volume:** includes prompt tone, ringback tone, open door success time and so on. The default prompt volume is 50.
- **Speaker volume:** adjust the loudspeaker volume according to your need. The default Mic volume is 50.
- **Keypad Volume:** adjust the keypad volume for the keypad touching sound. The default Mic 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.
- **Mic Mode:** select which mic to be applied between left and right microphones.

10.1.2. Upload Open-door Tone

You can not only enable or disable the Open-Door Tone but also upload the open-door tones in batch that you favored on the web **Device > Audio > Open Door Tone Setting** interface.



Parameter Set-up:

Guide

- **Enable Prompt of Open Door:** enable the open door tone so that you can hear it when you open the door.
- **Enable Voice Prompts of Guiding:** enable the prompt tone for the different operations
- **Open Door Tone UploadImportReset:** upload the open door tone. Click the Reset to reset the tone to the previous one.
- **Directory GuidingTone UploadImportReset:** upload the prompt tone on the directory screen.
- **Call GuidingTone UploadImportReset:** upload your customized prompt tone on the call screen.
- **PIN Entry GuidingTone UploadImportReset:** upload the customized prompt tone on PIN code entry screen
- **Temp Key GuidingTone Upload:** upload the customized prompt tone on temporary PIN code entry screen.



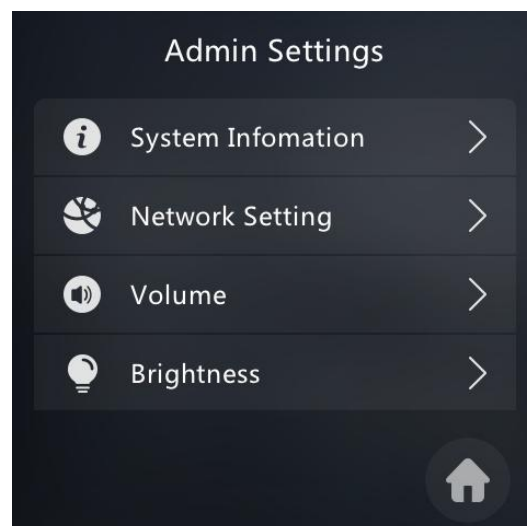
Note:

- All the tone files uploaded should be in .wav format, size200KB,Sample Rate:16000,Bits:16

11. Network Setting

11.1. Device Network Configuration

You can check for the door phone's network connection info and configure the default DHCP mode (**Dynamic Host Configuration Protocol**) and static IP connection for the device either on the device or on the device web interface. To configure the Network setting on the device, select **Network Setting**.



Parameter Set-up:

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

Network > Basic

LAN Port

DHCP Static IP

11.2. Device Local RTP configuration

For the device network data transmission purpose, device needs to be set up with a range of RTP ports (**Real-time Transport Protocol**) for establishing an exclusive range of data transmission in the network. To configure the configuration on the web **Network > Advanced > Local RTP** interface.

Network > Advanced

Local RTP

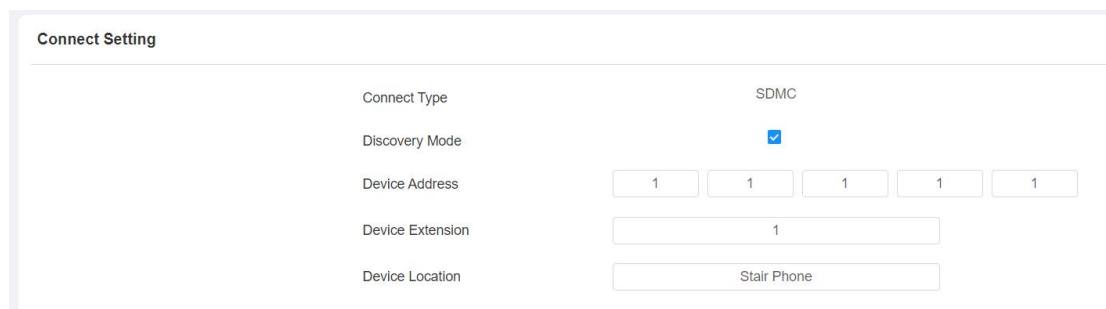
Starting RTP Port	<input type="text" value="11800"/>	(1024-65535)
Max RTP Port	<input type="text" value="12000"/>	(1024-65535)

Parameter set-up:

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

11.3. Device Deployment in Network

Door phones should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address and extension numbers as opposed to other devices for the device control and the convenience of the management. To configure the configuration on the web **Network > Advanced > Connect Setting** interface.



The screenshot shows the 'Connect Setting' configuration page. It includes the following fields and values:

Connect Type	SDMC
Discovery Mode	<input checked="" type="checkbox"/>
Device Address	1 1 1 1 1
Device Extension	1
Device Location	Stair Phone

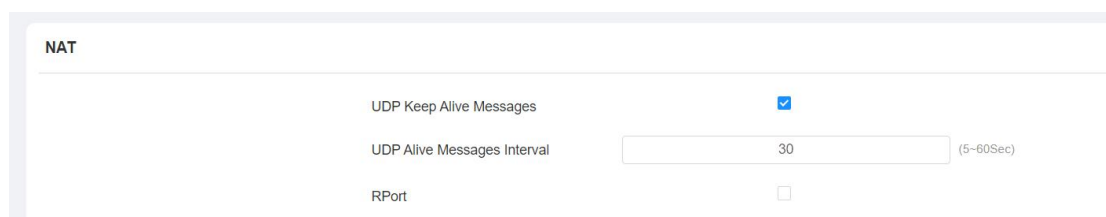
Parameter Set-up:

- **Connect Type:** 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 indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **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.

11.4.NAT Setting

NAT (**Network Address Translation**) allows hosts in an organization's private intranet to transparently connect to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. The NAT in the device web is limited to maintaining a connection with the remote SIP server. The principle is to send a heartbeat message to the remote SIP server at a set interval after the function is turned on. Otherwise, the server may judge that the device is offline and allocate the SIP assigned to other devices, resulting in failure to connect to it in the future. Path: **Account > Advanced > NAT**.



NAT	
UDP Keep Alive Messages	<input checked="" type="checkbox"/>
UDP Alive Messages Interval	<input type="text" value="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 SIP server will recognize that the device is in on-line status.
- **UDP Alive Msg 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).

12. Intercom Call Configuration

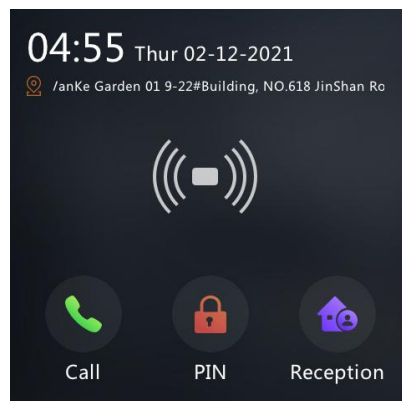
Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

12.1. IP call & IP Call Configuration

IP calls and SIP calls can be made directly on the intercom device by entering the IP number on the device. And you can also disable the direct IP call if you allow no IP call to be made on the device.

12.1.1. Make IP Calls

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



12.1.2. 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:

- **Enabled:** tick the check box if you want to enable the IP call.
- **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.

12.2. SIP Call & SIP Call Configuration

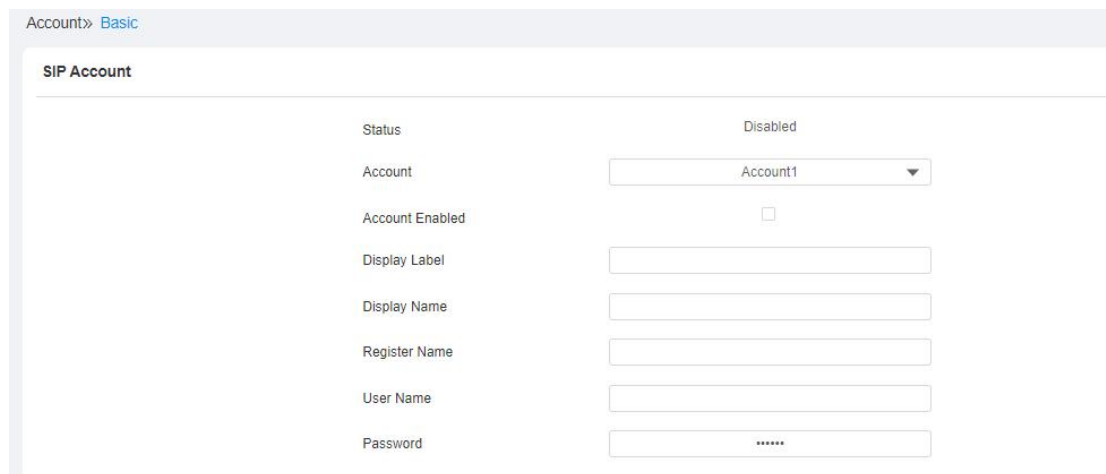
You can make SIP call (**Session Initiation Protocol**) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to configure first before you can make calls on the device.

12.2.1. SIP Account Registration

X912S door phones support two SIP accounts that can all be registered according to your applications. You can, for example, switch between them if any one of the accounts failed and become invalid.

12.2.1.1. Configure SIP Account

To configure the SIP account, navigate to **Account > Basic > SIP Account** interface.



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:

- **Status:** check to see if the SIP account is registered or not.
- **Account:** select account 1 or account 2 to be configured for making or receiving SIP calls.
- **Account Enabled:** enable the registered SIP account.
- **Display Label:** configure the device label to be shown on the device screen.
- **Display Name:** configure the name, for example, the device's name to be shown on the called party.
- **Register Name:** enter the SIP account register Name obtained from your

SIP account administrator.

- **User Name:** enter the user name obtained from SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

12.2.2. SIP Server Configuration

SIP servers can be set up for device in order to achieve call session through SIP server between intercom devices. To configure the configuration on the web **Account > Basic > Preferred SIP Server** interface.

Preferred SIP Server

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

Alternate SIP Server

Server IP	<input type="text"/>
Port	<input type="text" value="5060"/> (1024-65535)
Registration Period	<input type="text" value="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.

12.2.3. SIP Call DND&Return Code Configuration

DND (**Do not disturb**) setting allows you not to be disturbed by any unwanted incoming SIP calls. You can set up DND related parameters properly on the device web interface to block SIP calls you do not intend to answer. In the meantime, you can also define the code to be sent to the SIP server when you want to reject the call. To configure the configuration on the web **Intercom > Call Feature > DND** interface.

The screenshot shows the 'DND' configuration page within the 'Call Feature' section of the web interface. The page contains the following fields:

Parameter	Value
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.
- **Enabled:** enable the DND function if needed.
- **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".
- **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.

12.2.4. Configure Outbound Proxy Server

Guide

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish call session via port-based data transmission. To configure the configuration on the web **Account > Basic > Outbound Proxy Server** interface.

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

Parameter Set-up:

- **Enable Outbound:** enable the outbound proxy server function if needed.
- **Preferred Server IP:** enter the SIP address of the primary outbound proxy server.
- **Port:** enter the port number for establishing call session via the primary outbound proxy server
- **Alternate Server IP:** set up Backup Server IP for the backup outbound proxy server.
- **Port:** enter the port number for establishing call session via the backup outbound proxy server.

12.2.5. Configure Data Transmission Type

SIP message 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 where the data come from. To configure the configuration on the web **Account > Basic > Transport Type** interface.

Transport Type

Type

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.
- **DNS-SRV:** select **DNS-SRV** to obtain DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

12.3.Dial Options Configuration

X912S offers a variety of Dial options that allows you to have fast dial experience while relieving you off memory burden due to long and complex dial numbers.

12.3.1. Quick Dial by Number Replacement

If you want to replace the long and complex dial number with a shorter number that can be memorized at greater ease and convenience for making calls. You can not only add quick dial number separately but also import the quick dial number to the device in batch. Besides, you can edit and delete the numbers if need. To figure the configuration on the web **Intercom > Dial Plan > Replace Rule** interface.

Replace Rule

+ Add Import Export ▾

<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	

Delete Delete All Prev 1/1 Next 1 Go

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:

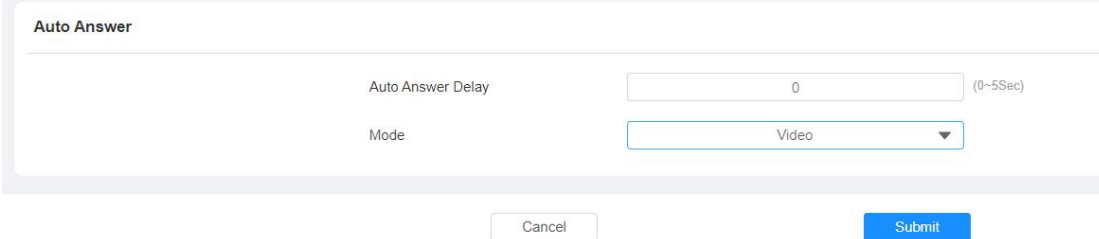
- The check box for each line of **“Prefix”** should be checked before you can see the **Edit** tab, which you click to carry out the modification.

12.4.Call Auto-answer Configuration

You can define how quickly the door phone should respond in answering the incoming SIP/IP call automatically by setting up the time related parameters.

Guide

In addition, you can also define the answering mode (video mode or audio mode). 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.

12.5. Manager Dial Call

Manager dial call consist of Sequence call and Group call. Manager Dial is used to quickly initiate the preconfigured numbers by pressing Management key on door phone. You can create up 10 numbers. To do the configuration on the web **Intercom > Basic > Manager Dial** interface.

Manager Dial

Call Type	<input style="width: 95%;" type="text" value="Sequence Call"/>
Time Out (Sec)	<input style="width: 95%;" type="text" value="60"/>
Sequence Call Number	
1st Call	<input style="width: 95%;" type="text"/>
2nd Call	<input style="width: 95%;" type="text"/>
3rd Call	<input style="width: 95%;" type="text"/>
4th Call	<input style="width: 95%;" type="text"/>
5th Call	<input style="width: 95%;" type="text"/>
6th Call	<input style="width: 95%;" type="text"/>
7th Call	<input style="width: 95%;" type="text"/>
8th Call	<input style="width: 95%;" type="text"/>
9th Call	<input style="width: 95%;" type="text"/>
10th Call	<input style="width: 95%;" type="text"/>

Manager Dial

Call Type	<input style="width: 95%;" type="text" value="Group Call"/>
Group Call Number	
	<input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/>
	<input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/>
	<input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/>
	<input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/> <input style="width: 20%;" type="text"/>

Parameter Set-up:

- **Enable:** tick the check box if you want to enable the Robin call function.
- **Timeout (Sec):** click to select the call time interval in between the Robin call number in a targeted Robin 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 robin call number in the targeted robin call group.
- **Call Type:** select the group call or sequence call (Robin 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 robin call timeout, the call will be transferred to 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.



Note:

- Sequence Call function should be supported by **SmartPlus**, please contact Akuvox technical support for more information.

12.6. Web Call

In addition to making IP/SIP call directly on the device, you can also make the call on the device web interface without approaching to device physically for testing purpose, etc. To make web call, navigate to System > Maintenance > Web Call.

Web Call

Web Call(Ready)

Auto

Dial Out Hang Up

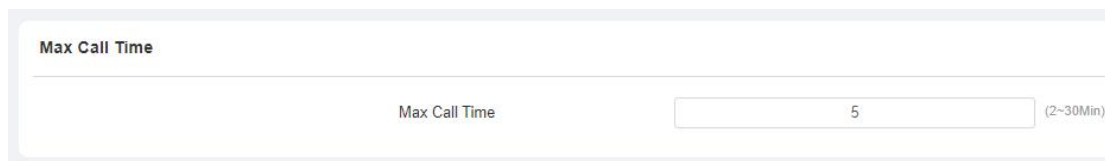
Parameter Set-up:

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

13. Call Settings

13.1.1. Maximum Call Duration Setting

X912S 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 calling automatically. To configure the configuration on the web **Intercom > Call Feature > Max Call Time** interface.



The screenshot shows a configuration interface for 'Max Call Time'. At the top, the text 'Max Call Time' is displayed. Below this, there is a horizontal line. Underneath the line, the label 'Max Call Time' is positioned to the left of a text input field. The input field contains the number '5'. To the right of the input field, the text '(2~30Min)' is displayed.

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.

13.1.2. Maximum Dial Duration Setting

Maximum Dial duration consist of Maximum dial-in time duration and the maximum dial-out time. Maximum dial in time refers to the maximum time duration before the door phone hang up the call if the call is not answered by the door phone. On contrary, Maximum dial-out time refers to the maximum time duration before the door phone hang up itself automatically when the call from the door phone is not answered by the intercom device being called to. 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 is 60 seconds in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial in time duration by default.
- **Dial Out Time:** enter the dial in time duration for your door phone (ranging from 5-120 Sec.) for example, if you set the dial out time duration 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.

13.1.3. Hang Up After Open Door

Guide

This feature is used to hang up the call automatically after the door is released during a call. So the caller or callee does not need to click hang up key again. To do this configuration on the web **Intercom > Call Feature > Hang Up After Open Door** interface.

Hang Up After Open Door

Type	Only DTMF
Time Out (Sec)	5 (0-15Sec)

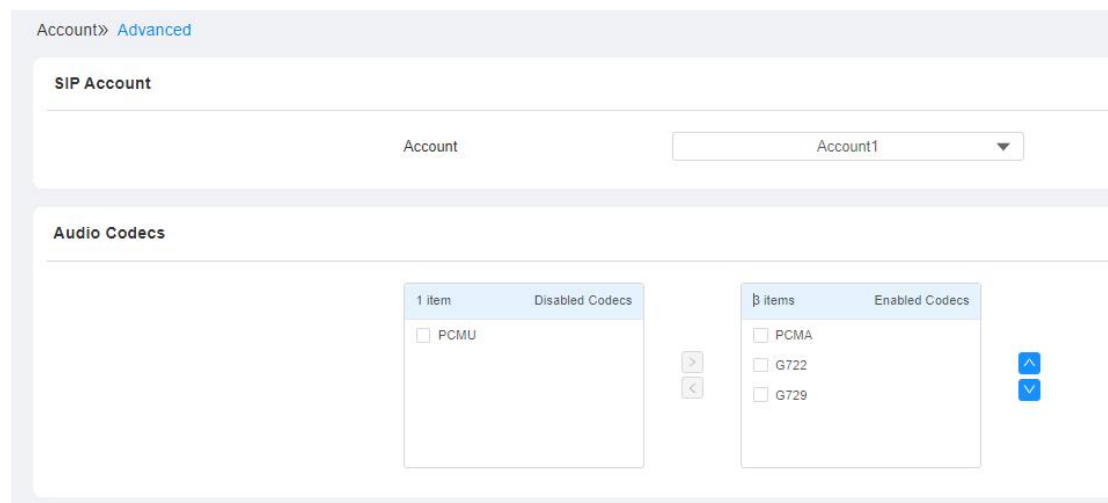
Parameter Set-up :

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

13.1.4. Audio& Video Codec Configuration for SIP Calls

13.1.4.1. Audio Codec Configuration

X912S supports four types of Codec (PCMU, PCMA, G729, 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 bandwidth and sample rate flexibly according to the actual network environment. To configure it on the web **Account > Advanced > SIP Account** interface.



Please refer 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

13.1.4.2. Video Codec Configuration

X912S support H264 codec that provides a 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.

Video Codec

Name	<input checked="" type="checkbox"/> H.264
Resolution	4CIF
Bitrate	320 kbps
Payload	104

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 four options: "QCIF", "CIF", "VGA", "4CIF" and "720P" according to your actual network environment. The default code resolution is 4CIF.
- **Bitrate:** select the video stream bit rate (Ranging from 128-2048). The greater the bitrate, the data transmitted in 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.

13.2. Configure DTMF Data Transmission

In order to achieve the 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)

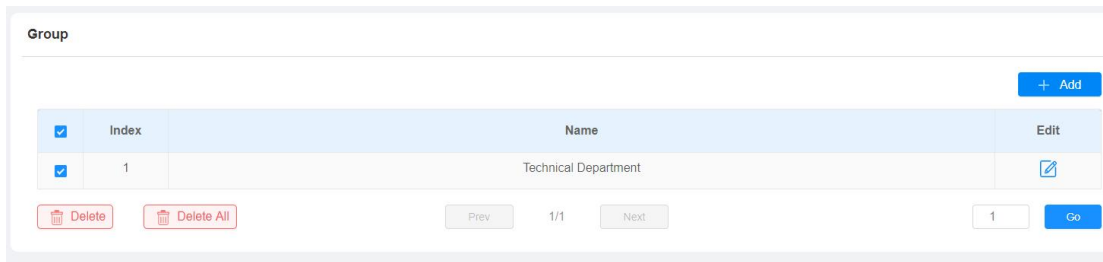
Parameter Set-up:

- **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 as the party for receiving signal data. The default is RFC2833.
- **How to Notify DTMF:** select among four types: **"Disable"** "DTMF" **"DTMF-Relay"** **"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.

14. Phone Book Configuration

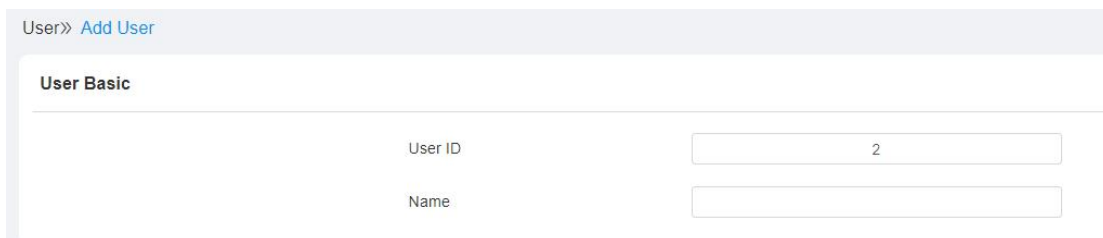
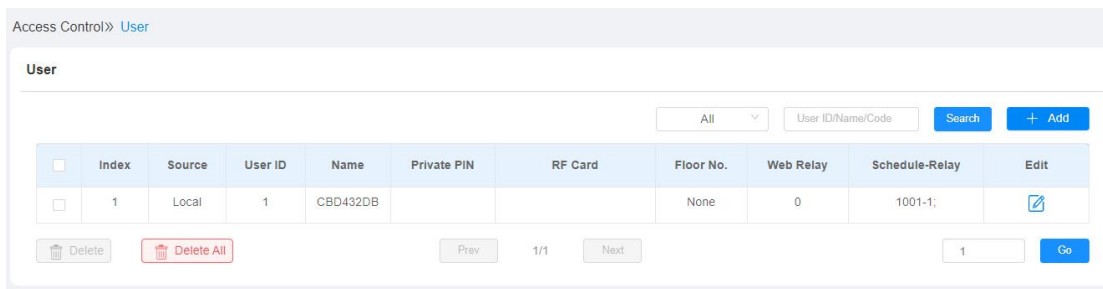
14.1. Manage Contact Groups

Contact group must be created first before you can put the specific user into the contact group you want. To do so, **navigate to Directory > User > Group**.



14.1.1. Contact Configuration

After the contact group is created, you start setting up user's contact that 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 > Contact Details**.



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:

- **Phone:** enter the user's contact number.
- **Group:** select the contact group. If you select "Default", then the **Priority of Call feature** will not be seen. Select specific contact group for the user.
- **Priority of Call:** set the priority of call among three options: "**Primary**", "**Secondary**", "**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 to 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.

14.1.1.1. Contact List Display Setting

You can customize your contact list display to your liking. To do so, navigate to **Directory > User > Directory Setting** interface.

Directory» [Directory](#)

Directory Setting

Show Cloud Contacts	<input checked="" type="checkbox"/>
Show Local Contacts	<input checked="" type="checkbox"/>
Contacts Display Settings	<input type="text" value="All 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" select it 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.

15. Relay Setting

15.1. Relay Switch Setting

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

The screenshot shows the 'Relay' configuration page. It has a breadcrumb 'Access Control >> Relay'. The page title is 'Relay'. The settings are as follows:

Parameter	Relay A	Relay B
Relay ID	RelayA	RelayB
Trigger Delay(Sec)	0	0
Hold Delay(Sec)	5	5
DTMF Mode	1 Digit DTMF	
1 Digit DTMF	0	0
2~4 Digits DTMF		
Relay Status	RelayA: Low	RelayB: Low
Relay Name		

Parameter Set-up:

- **Relay ID:** indicates Relay A and Relay B.
- **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-digt 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.



Note:

- 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 can not edit DTMF code in **1 Digit DTMF** field.

15.2.Web Relay Setting

In addition to the relay that is connected to the door phone, you can also control the door access using the network-based web relay on the device and on the device web interface.

15.2.1. Configure Web Relay

Web relay needs be to 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.

Access Control > Web Relay

Web Relay

Type

IP Address

User Name

Password

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 **Webrelay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.
- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.
- **User Name:** enter the User name provided by the web relay manufacturer.
- **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.

Guide

- **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.

The screenshot shows the 'User' management interface. At the top, there is a breadcrumb 'Access Control >> User'. Below it, the 'User' section has a search bar with a dropdown set to 'All', a text input for 'User ID/Name/Code', and buttons for 'Search' and '+ Add'. The 'Access Setting' section below contains:

- 'Allow To Open' with four checkboxes: 'RelayA' (checked), 'RelayB', 'Security Relay A', and 'Security Relay B'.
- 'Floor No.' with a dropdown menu currently showing 'None'.
- 'Web Relay' with a dropdown menu currently showing '0'.

15.2.2. Configure Security Relay

Akuvox security relay is connected to the door lock via Akuvox door phone. It is installed in side of the door and serves as extra protection against the forced door unlock through tampering of the door phone. The security relay is applied in applications requiring a higher level of security. To set up the security relay, navigate to **Access Control > Relay > Security Relay**.

Security Relay

Relay ID	Security Relay A ▼	Security Relay B ▼
Connect Type	Relay A Power Output ▼	RS485 ▼
Enabled	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="button" value="Test"/>	<input type="button" value="Test"/>

Parameter Set-up:

- **Relay ID:** displays relay ID.
- **Connect Type:** 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**".
- **Enabled:** enable the security relay you want.

16. Door Access Schedule Management

You are required to configure and make schedule for the user-based door access via RF card, Private PIN and Facial recognition.

16.1. Configure Door Access Schedule

You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. Moreover, you can edit your door access schedule if needed.

16.1.1. Create Door Access Schedule

You can create the door access schedule on a daily or monthly basis, and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis. To do so, navigate to **Setting > Schedule**, then click "**+ Add**".

Setting > Schedule

Schedule

All Search + Add Import Export

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

Delete Delete All Prev 1/1 Next 1 Go

To create a daily schedule:

Add Schedule ×

Mode: Daily

Name:

Start Time - End Time: 00:00 - 23:59

Cancel Submit

To create a weekly schedule:

Add Schedule ×

Mode: Weekly

Name:

Day: Mon Tue Wed
 Thur Fri Sat
 Sun Check All

Start Time - End Time: 00:00 - 23:59

Cancel Submit

To create a longer period schedule:

Add Schedule ✕

Mode: Normal

Name:

Start Date - End Date: 20220221 ~ 20220221

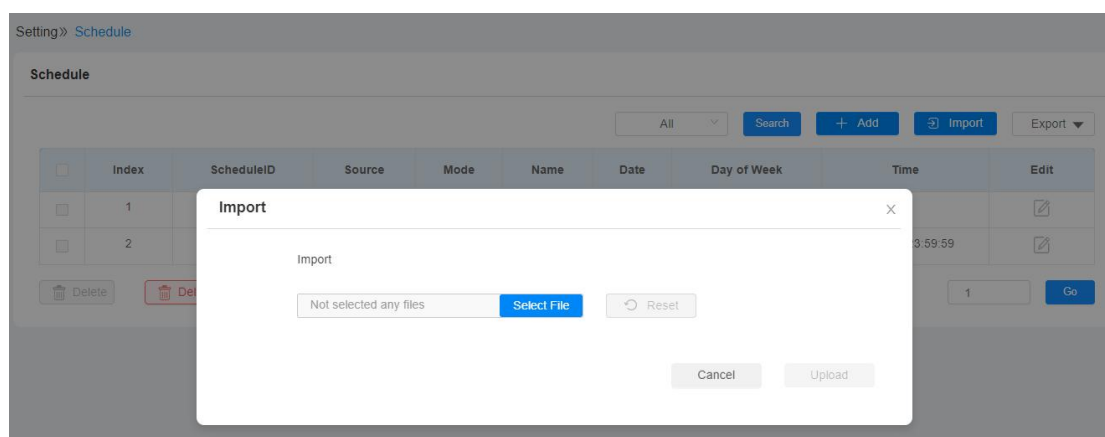
Day: Mon Tue Wed
 Thur Fri Sat
 Sun Check All

Start Time - End Time: 00:00 - 23:59

Cancel Submit

16.1.2. Import and Export Door Access Schedule

In addition to creating door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency. To do so, navigate to **Setting > Schedule**, then click **Import**.





Note:

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

16.1.3. Edit the Door Access Schedule

If you want to edit or delete your door access schedule you created, you can edit or delete the configured schedule separately or in batch. To do so, navigate to **Setting > Schedule**.

Schedule

+ Add
📄 Import
Export ▼

☐	Index	Mode	Name	Date	Day of Week	Time	Edit
☐	1	Normal	Normal	20201201-20201231	Mon Tue Wed Thur Fri Sat Sun	00:00-00:00	✎
☐	2	Weekly	Weekly	--	Mon Tue Wed Thur Fri Sat Sun	--	✎
☑	3	Daily	Daily	--	--	01:09-23:59	✎

🗑 Delete
🗑 Delete All
Prev
1/1
Next
1
Go



Note:

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



Note:

- The access control schedule synchronized from the SmartPlus can not be edited or deleted.

17. Door Unlock Configuration

X912S series door phone offers you three types of door access via PIN code, RF card and Facial recognition. You can configure them on the device and web interface. Moreover, you can import or export the configured files to maximize your RF card configuration efficiency.

17.1. Configure PIN Code for Door Unlock

You can create and modify both Public PIN code and private PIN code for door access on X912S series door phones.

17.1.1. Configure Public PIN code

You can configure and modify Public PIN codes on the device web **Access Control > PIN Setting > Public PIN** interface.

Public PIN

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



Note:

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

17.1.2. Configure Private PIN Code

You can not only set up PIN code, but also set and select the door access schedule that you created for the validity of the PIN Code access during a certain time span you scheduled. To configure the configuration on the web **Directory > User**, then click " +Add". After that enter the user information, and enter the private PIN code.

Access Control» User

User

All Search + Add

User» Add User

User Basic

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

Private PIN

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

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

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.

17.1.3. Configure Private PIN Access Mode

X912S door phone offers you two types of access modes for private PIN code access, namely "PIN" and "APT#+PIN". To configure the configuration on the web **Access Control > PIN Setting > Private PIN** interface.

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.

17.2. Configure RF Card for Door Unlock

17.2.1. 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.



Note:

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



Note:

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

17.2.2. Configure RF Card Code Format

If you want to integrate with the third-party intercom system in terms of RF card door access, you can change the RF card code format to be identical with that applied in 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	<input type="text" value="8HN"/>
ID Card Order	<input type="text" value="Normal"/>
ID Card Display Mode	<input type="text" value="8HN"/>

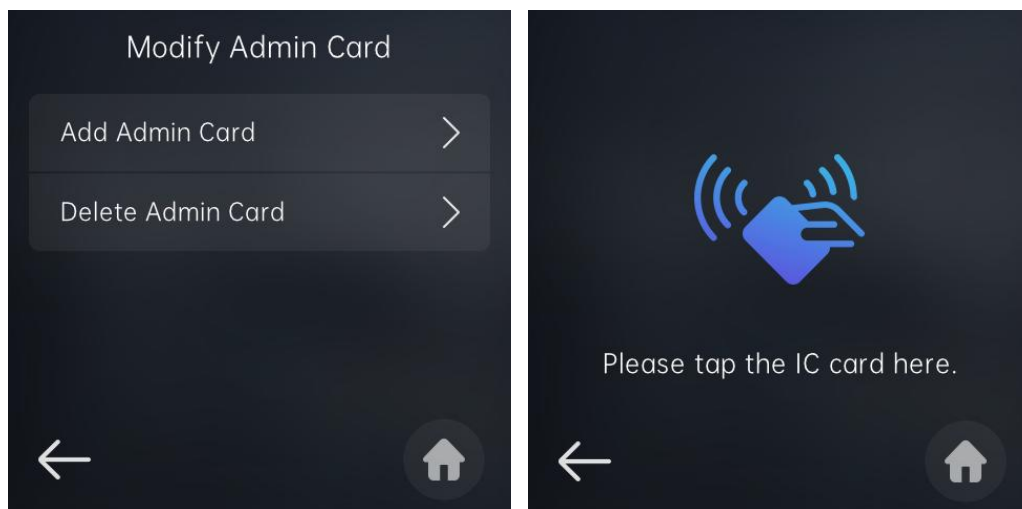
Parameter Set-up:



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

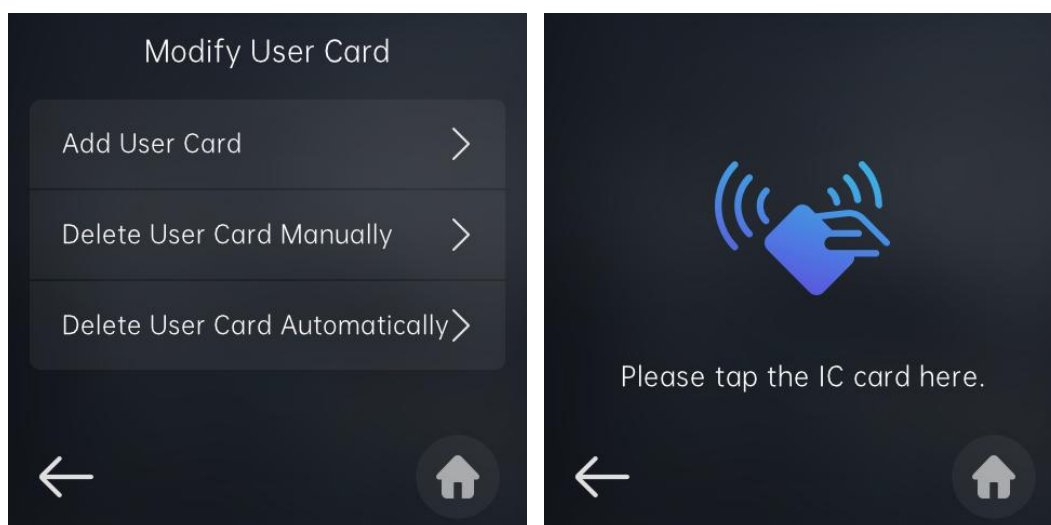
17.2.3. Configure RF Card on the Device

You can configure RF cards for administrators and users. And Administrator is allowed to create RF cards for the users after the administrator RF card is created. And the administrators need to tap their cards on the card reader before creating RF cards for the users. Go to Modify **Admin Card > Add Admin card**.

To configure administrator card, go to **Modify Admin Card > Add Admin card**.

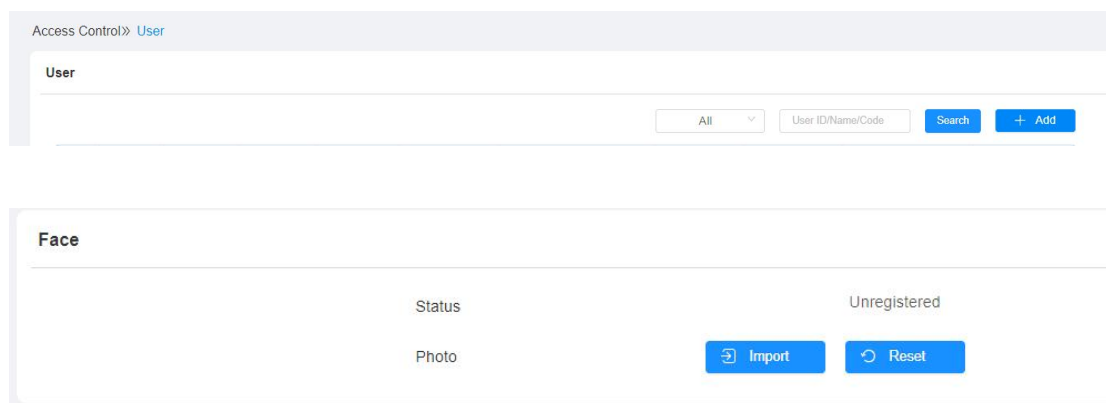


To configure user card, press  icon on the home screen, then enter your setting default setting password "3888", then press  icon on the keypad. After that select "Modify User Card", then enter the system PIN code, which is "2369" by default. Then press "Add User Card".



17.3. 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.



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:

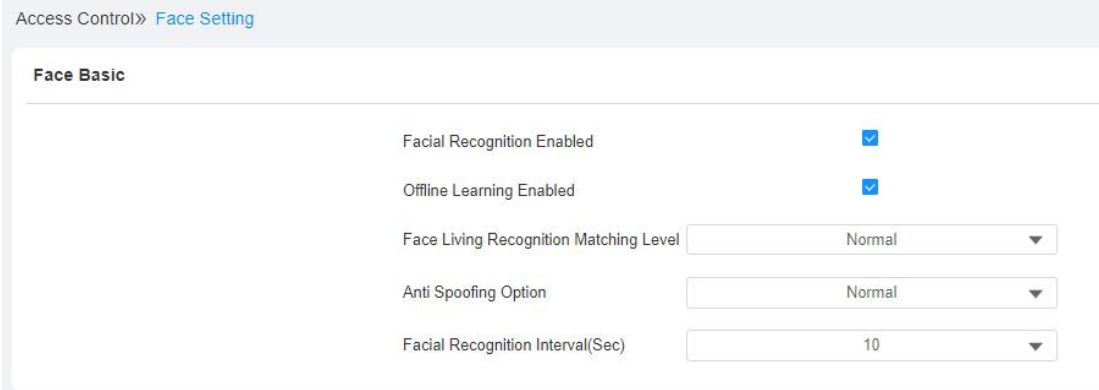
- Pictures to be uploaded should be in jpg or png format.

Note:

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

17.4. Basic Facial Recognition Configuration on the Web Interface

X912S door phone allow you to adjust facial recognition accuracy, recognition intervals according to your actual need. And you can also improve the recognition quality and user experience through the basic facial recognition setting on device web **Access Control > Face Setting > Face Basic** interface.



Access Control > Face Setting

Face Basic

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:

- **Face Recognition Enabled:** click on **Enable** to turn on the facial recognition function. Facial recognition is enabled by default.
- **Offline Learning:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level:** click to select the facial recognition accuracy level among four options: **Low, Normal, High, 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**. 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:** 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.

17.5. 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.

Access Control >> User

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

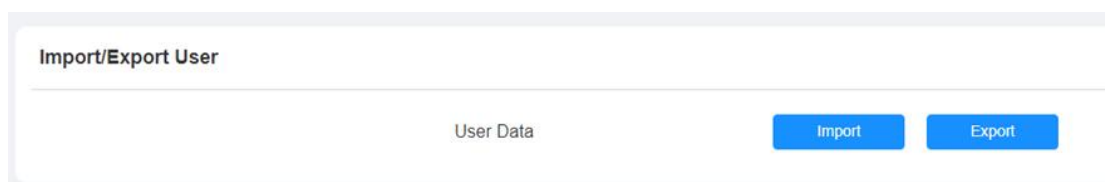


Note:

- Users synchronized from the SmartPlus can not be edited or deleted.

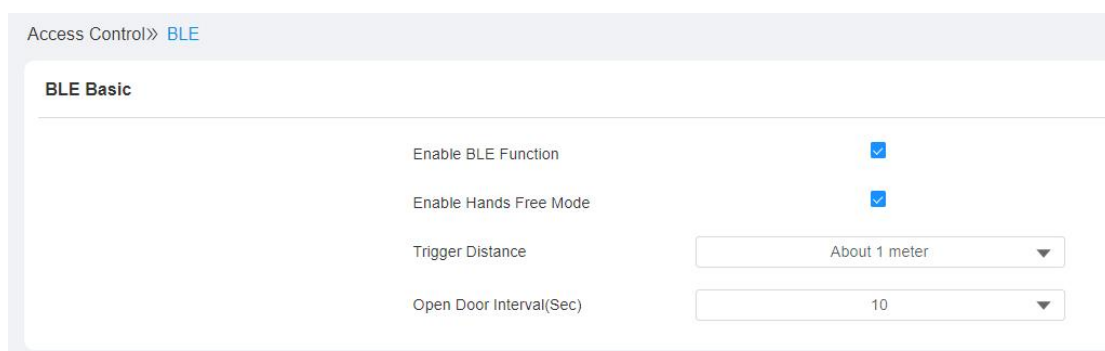
17.6.Import and Export User Data of Access Control

X912S series support User Data of access control to be shared among Akuvox X912S series door phones through import and export while you can also export the facial data out of the door phone and then import to a third-party device. To configure the configuration on the web Directory > User > Import/Export User interface.



17.7.Configure Bluetooth for Door Unlock

You can also gain door access by mobile phone with Bluetooth which is used together with Akuvox SmartPlus. You can gain door access through the Bluetooth-enabled hands-free door access or by waving your hands in front of the door phone for access. To set up the function, navigate to **Access Control > BLE > BLE Basic**.



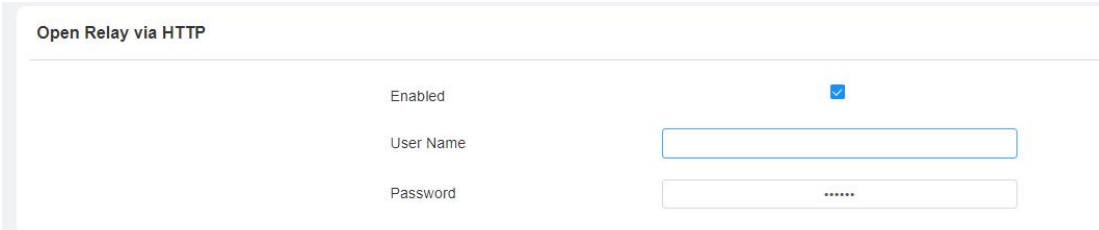
Parameter Set-up:

- **Enable BLE Function:** enable the Bluetooth function.

- **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 the 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".
- **Open Door Interval (Sec):** select the time interval between every two Bluetooth door accesses.

17.8. Configure Open Relay via HTTP for Door Unlock

You can unlock the door remotely without approaching the device physically for the door access 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 the door access. 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"/>

Parameter Set-up:

- **Enable:** enable the HTTP command unlock function by clicking on **Enable** field.
- **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.

17.9. Configure Open Relay via DTMF for Door Unlock

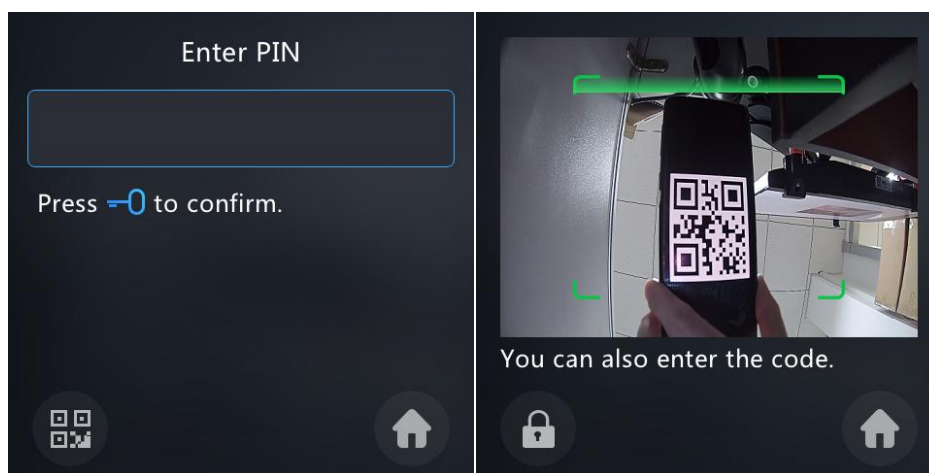
You can authorize the contacts to be able to unlock the door via DTMF or deny all the contacts for the DTMF unlock if needed. To do so, navigate to **Access Control > Relay > Open Relay via DTMF**.

Parameter Set-up:

- **All Numbers:** all numbers are allowed to unlock the door via DTMF.
- **None:** none of the contacts is allowed to unlock the door via DTMF.
- **Only Contact List:** only the contacts in the contact list are allowed to unlock the door DTMF.

17.10. Unlock by QR Code

If your door phone is connected to the SmartPlus Cloud, you can gain door access via QR code. QR code will be sent to your SmartPlus app upon requesting QR door access.



Note:

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

17.11. 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 Setting-Action .	
HTTP URL	<input type="text"/>
Action Delay	0 (0~300Sec)
Execute Relay	None
Door Status	DoorA: Low

Parameter Set-up:

- **Enabled:** enable the function as needed.
- **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, TFTP.
- **HTTP URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds., then the corresponding actions will be carried out 5 minutes after your press the button.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

17.12. Configure Reception Tab for Door Unlock

In the device home screen, X912S door phone provide residents and visitors quick door access by pressing the **Reception icon** on the lower right corner of the home screen. 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 the door access. For example:
<http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1>

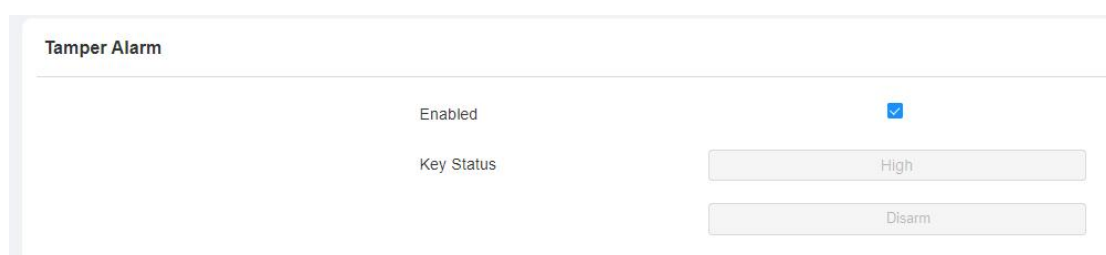
18. Security

18.1. Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm while sending out calls to the designated location. Tamper alarm will be triggered off when the door phone changes its gravity value as opposed to its original gravity value set up when the device is installed.

18.1.1. Configure Tamper Alarm on the Device

You can set up the temper alarm function in terms of switching on the function and setting up the gravity sensor sensitivity to suit your need. To configure the configuration on the web System > **Security** > **Tamper Alarm** interface.



Tamper Alarm

Enabled

Key Status

High

Disarm

Parameter Set-up:

- **Enable:** tick the check box to enable the temper alarm function. When the temper alarm goes off, you can press the **Disarm** tab beside the check box to clear the alarm.
- **Key Status:** temper alarm will not be triggered unless the key status is shifted from "Low" to "High" status.

18.2.Action URL

X912S allows you to set up specific HTTP URL command that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occurs any changes in the relay status, input status, PIN code, and RF card access for security purpose. You can navigate to **Setting > Actions URL**.

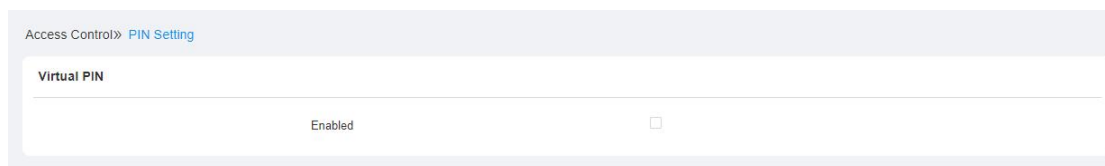
Setting» [Action](#)

Action URL

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

18.3.Virtual PIN

Virtual PIN allows you to protect your PIN code from being leaked to someone. To enable the virtual PIN feature, **navigate to Access > PIN Setting > Virtual PIN.**



Parameter Set-up:

- **Enabled:** enable it if you want to prevent your password from being leaked to someone. For example, if your real password is 123456, you can enter the password as **"99123456788"** which is considered as a valid password as your real password numbers are included in the virtual password. And if user A's real password is "123456", while user B's password is "1234", then if the virtual password "99123456788" is entered, the virtual password entered will be taken as the password for user A, because user A's password "123456" has the most of numbers overlapping with the virtual PIN code. However, it will be different when you apply dual-authentications (Face+ PIN, RF card+PIN, or Bluetooth+PIN), then user B's password "1234" will be given the priority, namely, the virtual PIN "99123456788" entered will be taken as "1234" the user B's password.

Note:

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

18.4. Client Certificate Setting

Certificates can ensure communication integrity and privacy when deploying Akuvox door phone. So, when users need to establish an SSL protocol, it is necessary to upload corresponding certificates for verification.

Web Server Certificate: it is the certificate that sends to client for authentication when the client requires an SSL connection with Akuvox door phone. Currently, the format of certificate that can be accepted by Akuvox door phone is *.PEM file.

Client Certificate: when Akuvox door phone required an SSL connection with server, the phone must verify the server to make sure it can be trusted. And the server will send its certificate to the Akuvox door phone. Then the door phone will verify this certificate according to client certificate list.

18.4.1. Web Server Certificate

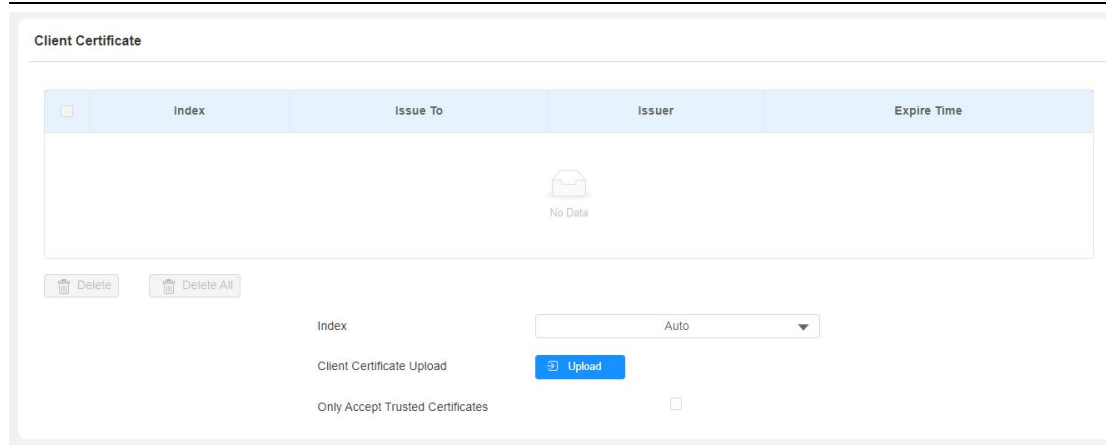
To upload Web Server certificate on the device web **System > Certificate > Web Server Certificate**.

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

Web Server Certificate Upload

18.4.2. Client Certificate

To upload and configure client certificate on the same page.

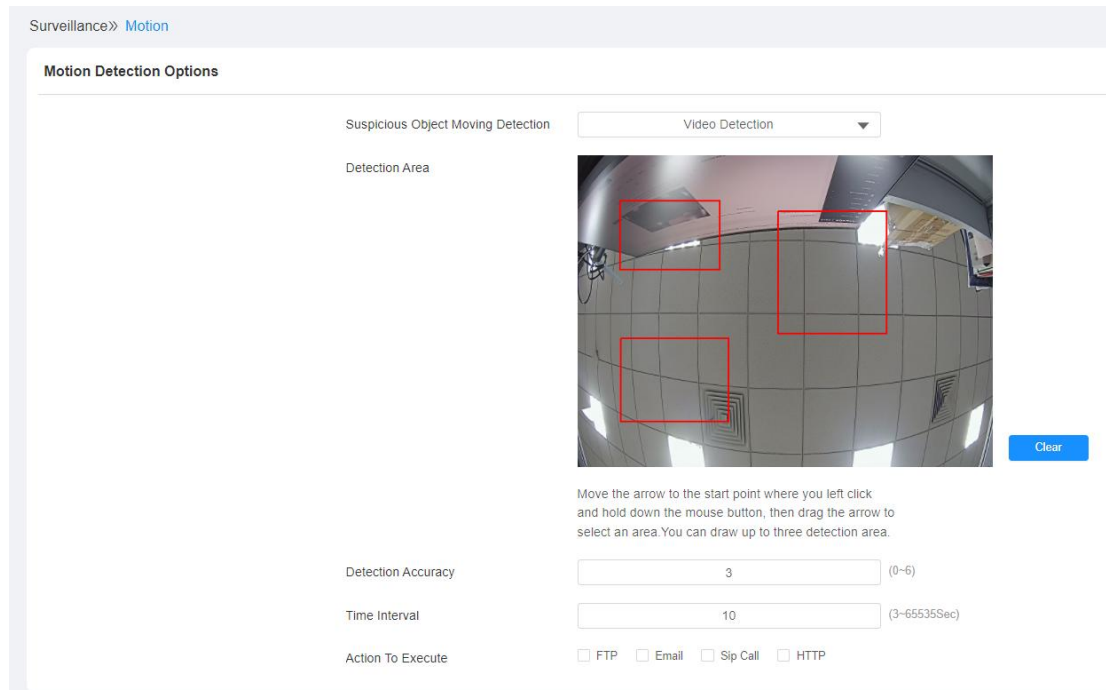


Parameter Set-up:

- **Index:** select the desired value from drop-down list of Index. If you select **Auto** value, the uploaded certificate will be displayed in numeric order. If you select value is 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 select **Enabled**, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If select **Disabled**, the phone will not verify the server certificate no matter whether the certificate is valid or not.

18.5. Motion Detection

Motion Detection is often used for unattended surveillance video and automatic alarms. The images collected by the camera at different frame rates will be calculated and compared by the CPU according to a certain algorithm. When the picture changes, if someone walks by, the lens is moved, the number obtained by the calculation and comparison result will exceed the threshold and indicate that the system can the corresponding processing is made automatically. To set up motion detection, navigate to **Surveillance > Motion > Motion Detection Options**.



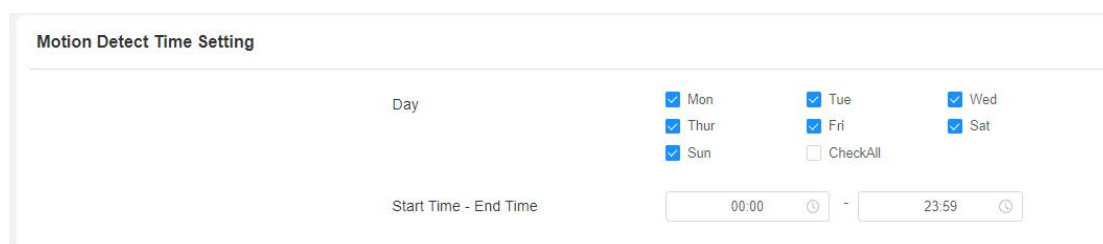
Parameter Set-up:

- **Suspicious Moving Object Detection:** select "Video Detection" to enable motion detection during the monitoring for the suspicious moving object. Select " Disabled" to turn off the function.
- **Detection Area:** select the detection area in the video. You can select up to three detection areas.
- **Time Interval:** set the time interval for the motion detection. If you set the default time interval as "10" Sec, then the motion detection time span will be 10 seconds. Assuming that we set the time interval as "10" then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) anywhere between 7-10 seconds once movement is detected."10" Sec interval is a complete cycle of the motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the "Time interval

minus three”.

- **Detection Accuracy:** set the detection accuracy for the detection sensitivity. The smaller value, the greater sensitivity. the default detection accuracy value is “3”.
- **Action to Execute:** select the notification type: FTP,TFTP, 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.



The screenshot shows the 'Motion Detect Time Setting' interface. It features a 'Day' section with checkboxes for each day of the week: Mon, Tue, Wed, Thur, Fri, Sat, and Sun. All days are currently checked. There is also a 'CheckAll' checkbox which is unchecked. Below the day selection, there is a 'Start Time - End Time' field with two time pickers. The first picker is set to '00:00' and the second is set to '23:59'.

18.6. Security Notification Setting

18.6.1. Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web **Setting > Action > Email Notification** interface properly.

Setting» Action

Email Notification

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

Parameter Set-up:

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

18.6.2. FTP Notification Setting

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

FTP Notification

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

Parameter Set-up:

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

18.7. Web Interface Automatic Logout

You can set up the web interface automatic logout timing, requiring re-login by entering the user name and the passwords for security purpose or for the convenience of operation. To configure the configuration on the **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 logout timing ranging from 60 seconds to 14400 seconds. The default value is 300.

19. Monitor and Image

19.1. RTSP Stream Monitoring

X912S door phone supports RTSP stream that allows intercom devices such as the indoor monitor or the monitoring unit from the third party to monitor or obtain the real time audio/ video (RTSP stream) from the door phone using the correct URL.

19.1.1. RTSP Basic Setting

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

Surveillance >> RTSP

RTSP Basic

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

Parameter Set-up:

- **Enabled:** tick the check box to turn on or turn off the RTSP function.
- **RTSP Authorization Enabled:** enable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, RTSP Password on the intercom device such as indoor monitor for authorization.

- **Authentication Mode:** select RTSP authentication type between " **Basic**" and " **Digest**". "Basic " is the default authentication type.
- **User Name:** enter the user name for the RTSP authentication.
- **Password:** enter the user name for the RTSP authentication.

19.1.2. RTSP Stream Setting

You can select the video codec for the RTSP stream. You can also configure video resolution and bitrate etc. for H.264 codec based on your actual network environment on the web **Surveillance > RTSP > H.264 Video Parameters**.

H.264 Video Parameters	
Video Resolution	720P
Video Framerate	25fps
Video Bitrate	1024kbps
2nd Video Resolution	VGA
2nd Video Framerate	25fps
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 kbps"

according to your network environment. The default video bitrate is "2048 kpbs".

- **2nd Video Resolution2:** select video resolution for the second video stream channel. While the default video solution is "VGA".
- **2nd Video Framerate:** select the video framerate for the second video stream channel. "25fps" is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate:** select video bitrate among the six options for the second video stream channel. While the second video stream channel is "512 kpbs" by default.

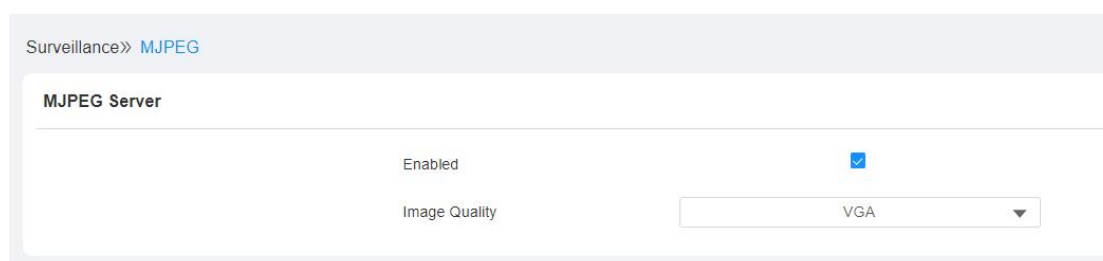


Note:

- X912S has two channels of RSTP 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.

19.2.MJPEG Image Capturing

X912S series allow you to capture the Mjpeg format monitoring image if needed. You can enable the MJPEG function and set the image quality on the web **Surveillance > MJPEG** interface.



Parameter Set-up:

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

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

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

And you can enter "http://192.168.1.104:8080/picture.jpg" on the web browser

19.3.ONVIF

Real-time video from the X912S door phone camera can be searched and obtained by the Akuvox indoor monitor or by third-party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function in the door phone so that other devices will be able to see the video from the door phone. To configure the configuration on the web **Surveillance > ONVIF** interface.

Surveillance» ONVIF

Basic Setting

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

Parameter Set-up:

- **Discoverable:** if enabled, the video from the door phone camera can be searched by other devices.

- **User Name:** enter the user name. The user name is "admin" by default.
- **Password:** enter the password. The password is "admin" by default.

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

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



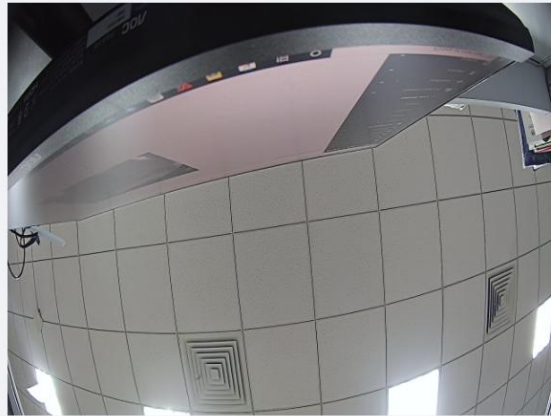
Note:

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

19.4.Live Stream

If you want to check the real-time video from the X912S door phone, you can go to the device web interface to obtain the real-time video or you can also enter the correct URL on the web browser to obtain it directly. To view the real time video on the web **Surveillance > Live Stream** interface. You can also enter the correct URL (**http://IP_address:8080/video.cgi**) on the web browser if you want to obtain the real-time video directly by going to the web interface.

Surveillance» Live Stream



20. Logs

20.1. 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

Call History All Start Time ~ End Time Name/Number Search Export

Index	Type	Date	Time	Local Identity	Name	Number
<p>No Data</p>						

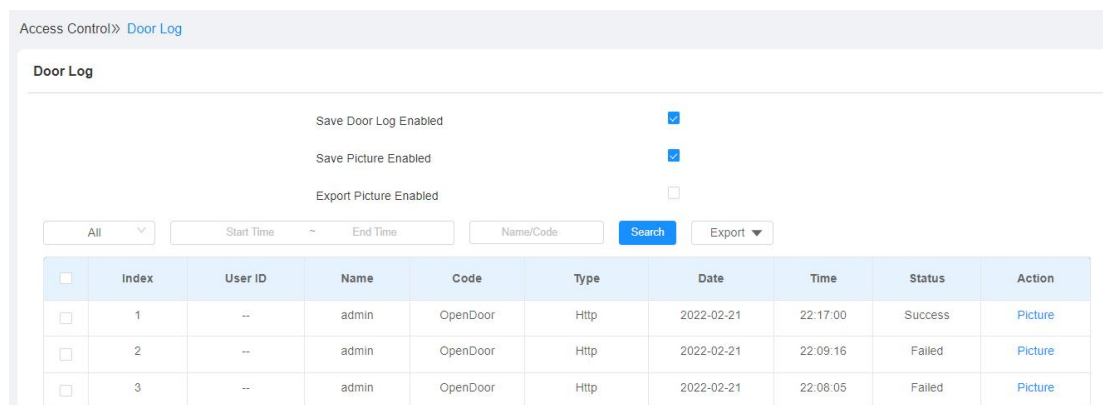
Delete
Delete All
Prev
1/1
Next
1
Go

Parameter Set-up:

- **Save Call Log Enabled:** enable the call log function.
- **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.

20.2. 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 web Status > **Access log** interface.



Parameter Set-up:

- **Save Door Log Enabled:** tick the check box to turn on or turn off the door log function.
- **Save Picture Enabled:** enable it if you want to save the door open snapshot captured.
- **Export Picture Enabled:** enable it if you want to export the door log with

snapshot picture captured.

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

21. Debug

21.1. System Log for Debugging

System log in the door phone can be used for debugging purpose. If you want to export the system out to a local PC or to a remote server for debugging, you can set up the function on the web **System > Maintenance**.

System» Maintenance

System Log

Log Level	<input type="text" value="3"/>
Export Log	<input type="button" value="Export"/>
Remote System Log Enabled	<input checked="" type="checkbox"/>
Remote System Server	<input type="text"/>
Remote System Port	<input type="text" value="(1-65535)"/>

Parameter Set-up:

- **LogLevel:** 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 "5", the more complete the log is "7".
- **Export Log:** click the **Export** tab to export the temporary debug log file to a local PC.
- **Remote System Log Enabled:** tick the checkbox to enable the function.
- **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.
- **Remote System Port:** enter the remote system server port provided by Akuvox technical team.

21.2.PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **System > Maintenance > PCAP** interface properly before using it.

The screenshot shows the PCAP configuration page. At the top, it says 'PCAP'. Below that is a 'Specific Port' label followed by an empty text input field and '(1-65535)' in small text. Underneath is the 'PCAP' label, followed by three buttons: 'Start' (blue), 'Stop' (grey), and 'Export' (blue). At the bottom, there is a 'PCAP Auto Refresh Enabled' label followed by an unchecked checkbox.

Parameter Set-up:

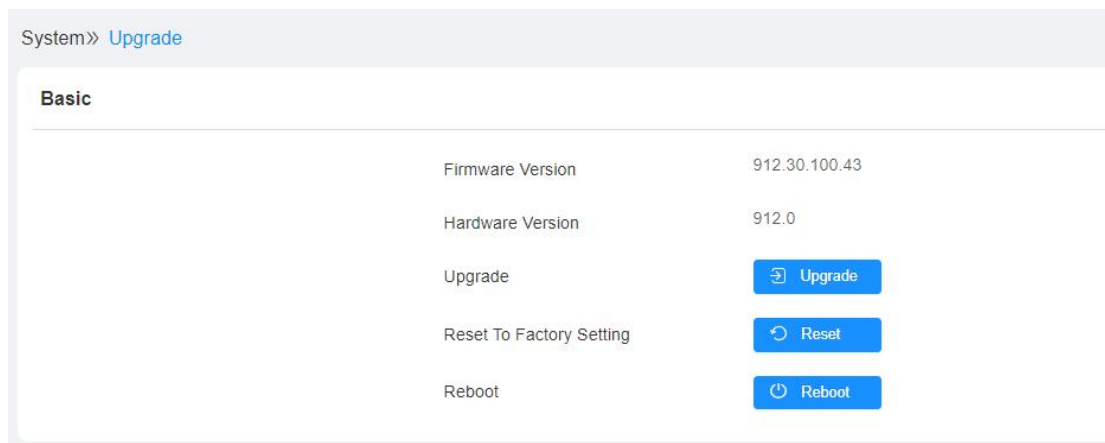
- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** click **Start** tab and **Stop** tab to capture a certain range of data

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 fresh 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.

22. Firmware Upgrade

Firmware of different versions for X912S series door phone can be upgraded on the device web **Upgrade > Basic** interface.




Upgrade ×

(Format: .rom)

Not selected any files Select File Reset

Reset After Upgrade

Cancel Install



 **Note:**

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

23. Backup

Configuration files can be imported to or exported out of the device to your local PC on the device web System > **Maintenance** > **Others** interface if needed.

Others

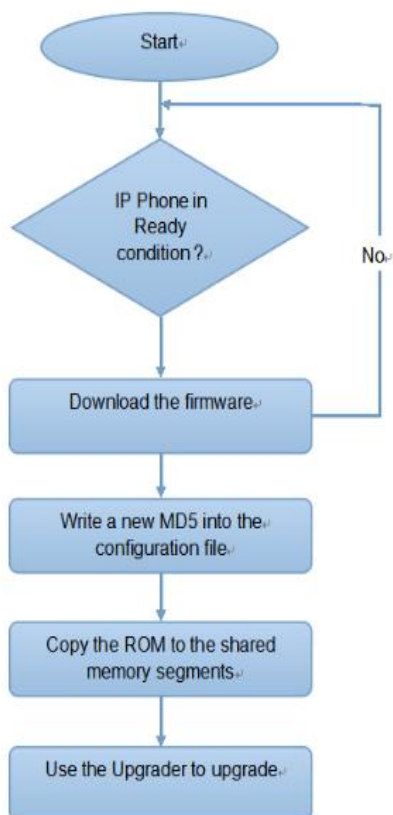
Config File  Import  Export (Encrypted)

24. Auto-provisioning via Configuration File

Configurations and upgrading on X912S door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the door phone.

24.1. Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade the devices in batch via third party servers. **DHCP, PNP, TFTP, FTP, 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 door phone.



24.2. Configuration Files for Auto-provisioning

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

The difference between the two types of configuration files is shown as 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. For example: r000000000912.cfg.

MAC-based configuration provisioning: MAC-based configuration files are used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.



Note:

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

24.3. AutoP Schedule

Akuvox provides you with different Autop methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule.

To configure the configuration on the web **System > Auto Provisioning > Automatic Autop.**

Automatic Autop

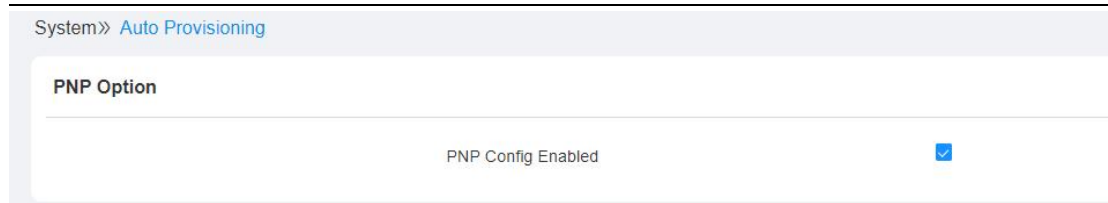
Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0-23Hour)
	<input type="text" value="0"/> (0-59Min)
Clear MD5	<input type="button" value="Clear"/>
Export Autop Template	<input type="button" value="Export"/>

Parameter Set-up:

- **Mode:** select **“Power on”**, **“Repeatedly”**, **“Power On + Repeatedly”**, and **“Hourly Repeat”** as your Autop schedule.
 Select **“Power on”** if you want the device to perform Autop every time it boots up.
 Select **“Repeatedly”**, if you want the device to perform Autop according to the schedule you set up.
 Select **“Power On + Repeatedly”** if you want to combine **Power On Mode** and **Repeatedly mode**, it would enable the device to perform Autop every time it boots up or according to the schedule you set up.
 Select **“Hourly Repeat”** if you want 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 automatic provisioning.
- **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.
- **Export Autop Template:** export Autop Template if needed.

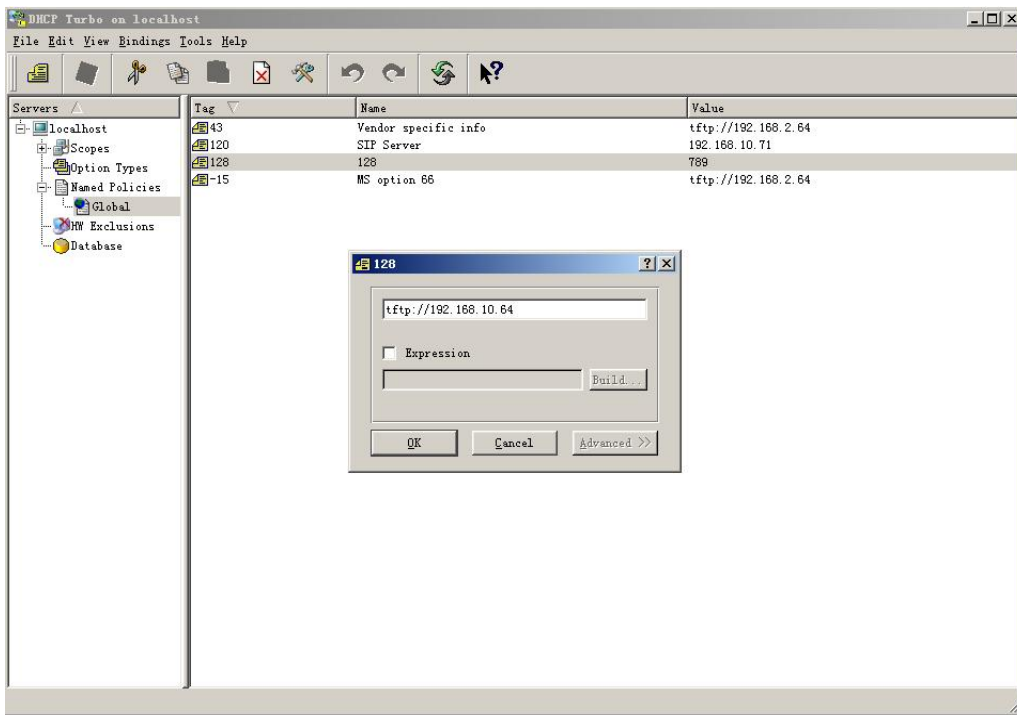
24.4.PNP Configuration

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.



24.5.DHCP Provisioning Configuration

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



Note:

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

DHCP Option

Custom Option (128~254)

(DHCP option 66/43 is enabled by default)

Parameter set-up:

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



Note:

- The general configuration file for the in-batch provisioning is with the format "r0000000000xx.cfg" taking X912S as an example "r0000000000912.cfg (10 "zeros" in total while the MAC-based configuration file for the specific device provisioning is with the format" MAC Address of the device.cfg, for example, "0C110504AE5B.cfg."

24.6.Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the door phone will

Guide

perform the auto provisioning at a specific timing according to the autop 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, navigate to **System > Auto Provisioning > Automatic Autop**.

Automatic Autop

Mode: Power On + Repeatedly

Schedule: Sunday

22 (0-23Hour)

0 (0-59Min)

Clear MD5: Clear

Export Autop Template: Export

To set up Autop server, navigate to **System > Auto Provisioning > Manual Autop**.

Manual Autop

URL: [input field]

User Name: [input field]

Password: [input field with asterisks]

Common AES Key: [input field with asterisks]

AES Key(MAC): [input field with asterisks]

Autop Immediately

Parameter set-up:

- **URL:** set up tftp, http, https, ftp server address for the provisioning
- **User Name:** set up a user name if the server needs a user name to be accessed otherwise leave it blank.
- **Password:** set up a password if the server needs a password to be

accessed otherwise leave it blank.

- **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 is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

 **Note:**

Server Address format:

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/ (use the default port 80)
http://192.168.0.19:8080/ (use other ports, such as 8080)
- HTTPS: https://192.168.0.19/ (use the default port 443)

 **Note:**

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

25. Integration with Third Party Device

25.1. Integration via Wiegand

If you want to integrate the X912S series door phone with third-party devices via Wiegand. To configure the configuration on the web **Access Control > Card Setting > Wiegand** interface.

Wiegand	
Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	Wiegand-26 ▼
Wiegand Transfer Mode	Input ▼
Wiegand Input Data Order	Normal ▼
Wiegand Output Data Order	Normal ▼

Parameter Set-up:

- **Wiegand Display Mode:** select Wiegand Card code format among **8H10D**; **6H3D5D**; **6H8D**; **8HN**; **8HR**.
- **Wiegand Card Reader Mode:** set the Wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode:** set the Transfer mode between **Input** or **Output** if the door phone is used as a receiver, then set it as **Input** for the door phone and vice versa.
- **Wiegand Input Data Order:** set the Wiegand input data sequence between **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.

25.2. 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.

The screenshot shows the 'HTTP API' configuration page. At the top, there is a breadcrumb 'Security >> HTTP API'. The page title is 'HTTP API'. The configuration options are as follows:

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 be returned HTTP 403 forbidden status.
- **Authorization Mode:** select among four options: **"None"** **"WhiteList"** **"Basic"**, **"Digest"** for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when **"Basic"** and **"Digest"** authorization mode is selected. The default user name is "Admin".

- **Password:** enter the password when “**Basic**” and “**Digest**” authorization mode is selected. The default user name is “Admin”.
- **1st IP-5th IP:** enter the IP address of the third party devices when the “WhiteList” authorization is selected for the integration.

25.3. Power Output Control

X912S can serve as a power supply for the external relays. Path: **Intercom > Access Control >> 12V Power Output.**

Relay ID	RelayB
12v Power Output Enabled	Disabled
Timeout(Sec)	3

Parameter Set-up:

- **Relay ID:** select the relay to be powered by X912S
- **12V Power Output:** 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 E18 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.
- **Time Out (Sec):** select the power supply time duration after the relay is triggered. Three options: 3, 5, 10. It is 3 seconds by default. The power output is 12V, and the maximum output amperage is 0.8A.

26. Lift Control

X912S door phone can be connected to Akuvox EC32 lift controller for the lift control. You can summon the lift to go down to the ground floor when you are granted through various types of access methods on the door phone. To set up the lift control, navigate to **Device > Lift > Control**.

Device » Lift Control

Lift Control List

Lift Control List	<input type="text" value="Akuvox EC32"/> <ul style="list-style-type: none"> None <li style="background-color: #e0f0ff;">Akuvox EC32
-------------------	---

Akuvox EC32 Advanced Setting

Server IP	<input type="text"/>
Server Port	<input type="text" value="80"/> (0-65535)

Akuvox EC32 Action

User Name	<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&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, select Auvox E32 to integrate the door phone with the Akuvox EC32 controller.
- **Server IP:** enter the IP address of the Akuvox EC32 controller server.
- **Server Port:** enter the Sever port of Akuvox EC32 controller server.

Guide

- **User Name:** enter the user name of the lift controller for the authentication.
- **Password:** enter 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 is needed.
- **URL To Trigger Specific Floor:** enter the Akuvox life 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 with 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.

27. Password Modification

27.1. 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.

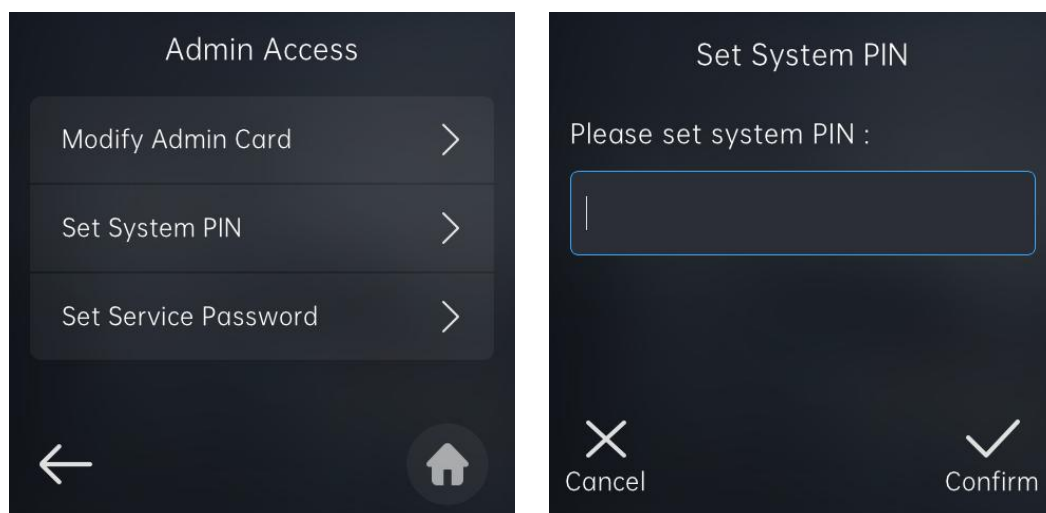
The screenshot shows the 'Web Password Modify' interface. At the top, there is a breadcrumb 'System >> Security'. Below it, the 'Web Password Modify' section has a 'User Name' dropdown menu set to 'admin' and a 'Change Password' button. The 'Account Status' section shows 'admin Enabled' with a checked checkbox and 'user Enabled' with an unchecked checkbox. A 'Change Password' modal is open, displaying a warning: 'The password must be at least eight characters long containing one uppercase letter, one lowercase letter and one digit at least.' The modal contains a 'User Name' field with 'admin' selected, and three password input fields: 'Current Password', 'New Password', and 'Confirm Password'. At the bottom of the modal are 'Cancel' and 'Change' buttons.

Parameter Set-up:

- **User Name:** modify the Admin or user password if needed.
- **User:** enable the user account if needed.

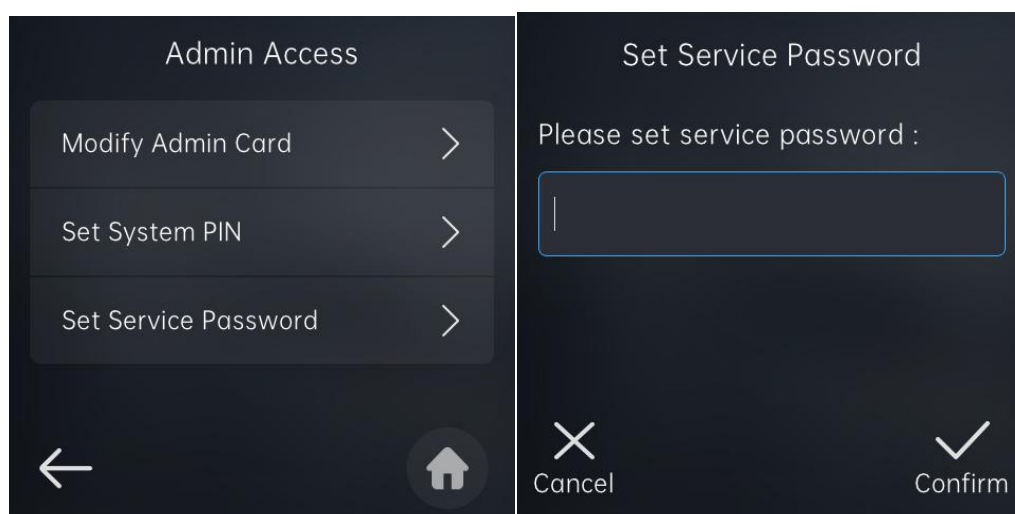
27.2.Modifying System Password

System PIN code is used to access the device system. You can modify the system PIN code on the device. Go to **Advanced Settings> Admin Access > Set System PIN.**



27.3.Modifying Setting Password

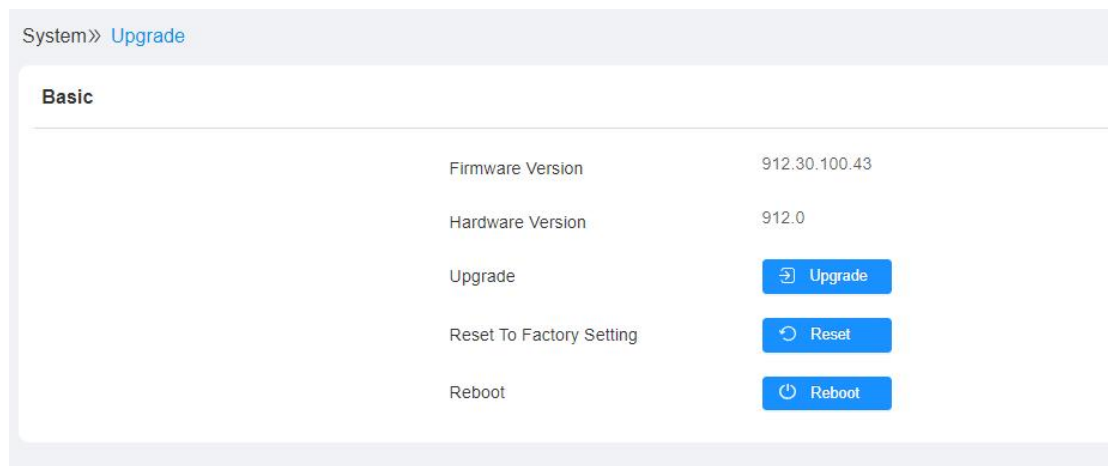
Setting PIN code is used to access the device setting. You can modify the system PIN code on the device. Go to **Advanced Settings> Admin Access > Set Service password.**



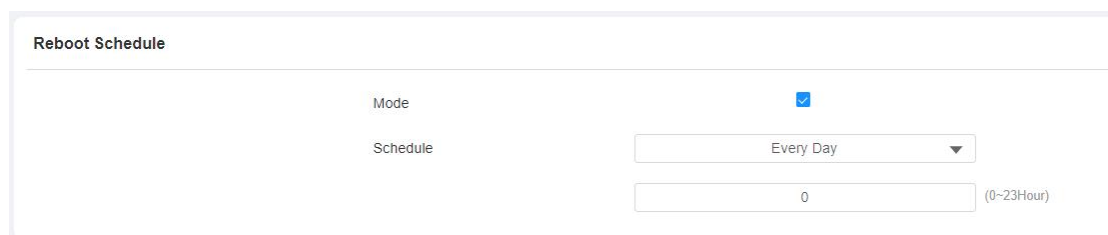
28. System Reboot&Reset

28.1.Reboot

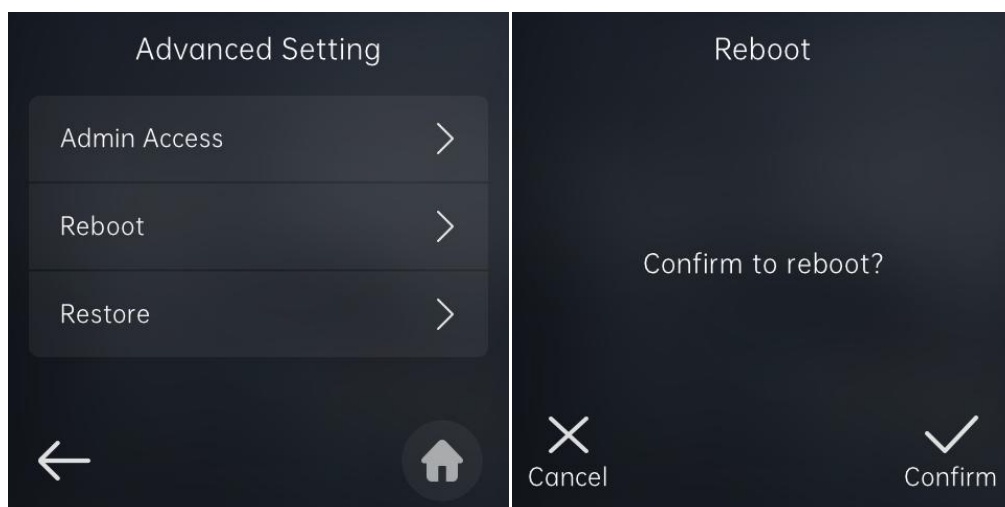
If you want to restart the device system, you can operate it on the device web interface as well. Moreover, you can set up schedule for the device to be restarted. To restart the system setting on the web **Upgrade > Basic** interface.



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

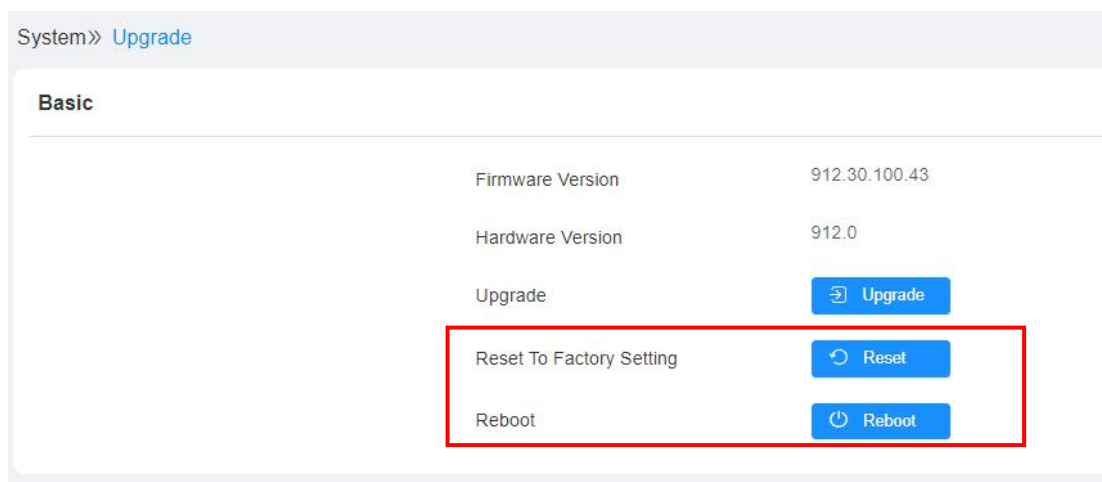


You can also reboot the device directly on the device. On the screen, go to **Advanced Setting > Reboot**.

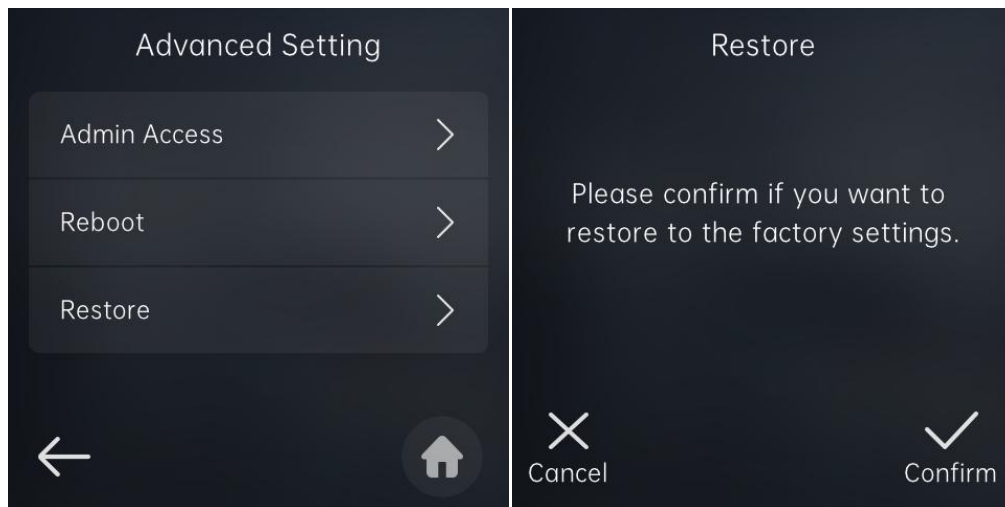


28.2.Reset

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



You can also reboot the device directly on the device. On the screen, go to **Advanced Setting > Reset**.



29. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatic Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation μ -Law

PCAP: Packet Capture

PNP: Plug and Play

RFID: Radio Frequency Identification

RTP: Real-time Transport Protocol

RTSP: Real Time Streaming Protocol

MPEG: Moving Picture Experts Group

MWI: Message Waiting Indicator

NO: Normal Opened

NC: Normal Connected

NTP: Network Time Protocol

NAT: Network Address Translation

NVR: Network Video Recorder

ONVIF: Open Network Video Interface Forum

SIP: Session Initiation Protocol

SNMP: Simple Network Management Protocol

STUN: Session Traversal Utilities for NAT

SMTP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

30. Contact us

For more information about the product, please visit us at www.akuvox.com or feel free to contact us by

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

Telephone: +86-592-2133061 ext.7694/8162

We highly appreciate your feedback about our products.

