



X915 SERIES DOOR PHONE

Administrator Guide

About This Manual

Thank you for choosing Akuvox X915 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 915.30.1.305 version, and it provides all the configurations for the functions and features of X915 series door phone. Please visit Akuvox forum or consult technical support for any new information or the latest firmware.

Introduction of Icons and Symbols



Warning:

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



Caution:

- **Always abide by this information in order to prevent the 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>

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	10
6.1. Language Setting.....	10
6.1.1. Language Setting on the Device.....	10
6.1.2. Language Setting on the Device Web Interface.....	11
6.2. Time Setting.....	11
6.2.1. Time Setting on the Device.....	12
6.2.2. Time Setting on the Device Web Interface.....	13
7. LED&LCD Setting	14
7.1. Infrared LED Setting.....	14
7.1.1. Infrared LED Setting on the Device.....	14
7.1.2. Infrared LED Setting on the Web Interface.....	15
7.2. LED Setting on Card Reader Area.....	16
7.3. LCD Screen Brightness Setting.....	17
7.3.1. LCD Screen Brightness Setting on the Web Interface.....	17
7.3.2. LCD Screen Brightness Setting on the Device.....	18
7.4. LED White Light Setting.....	18
8. Screen Display Configuration	20
8.1. Screensaver Configuration.....	20
8.1.1. Configure Screensaver on the Device.....	20
8.1.2. Configure Screensaver on the Web Interface.....	21
8.2. Upload Screensaver.....	22
8.2.1. Upload Device Booting Image.....	23
8.3. Upload Device Contact List Background Image.....	24
8.4. Configuration for Scenario-based Screen Display Mode.....	24
8.5. Villa Mode Home Screen Display.....	25
8.6. Building Mode Home Screen Display.....	26
8.7. Dial Key Order.....	27
8.7.1. Dial Screen Prompt Display.....	27
8.7.2. Open Door Text Prompt Display.....	28
9. Volume and Tone Configuration	29
9.1. Volume Configuration.....	29
9.1.1. Configure Volume on the Device.....	29
9.1.2. Configure Volume on the Web Interface.....	30

9.2. Upload Open-door Tone.....	31
10. Network Setting.....	32
10.1. Device Network Configuration.....	32
10.2. Device Local RTP configuration.....	33
10.3. Device Deployment in Network.....	34
10.4. NAT Setting.....	35
11. Intercom Call Configuration.....	36
11.1. IP call & IP Call Configuration.....	36
11.1.1. Make IP Calls.....	36
11.1.2. IP Call Configuration.....	37
11.2. SIP Call &SIP Call Configuration.....	37
11.2.1. SIP Account Registration.....	37
11.2.1.1. Configure SIP Account on the Device.....	38
11.2.1.2. Configure SIP Account on the Web Interface.....	39
11.2.2. SIP Server Configuration.....	40
11.2.3. SIP Call DND&Return Code Configuration.....	40
11.2.4. Configure Outbound Proxy Server.....	41
11.2.5. Configure Data Transmission Type.....	42
11.3. Dial Options Configuration.....	43
11.3.1. Quick Dial by Number Replacement.....	43
11.3.1.1. Quick Dial by Number Replacement on the Device....	43
11.3.1.2. Quick Dial by Number Replacement on the Web Interface.....	44
11.3.2. Speed Dial.....	45
11.3.2.1. Speed Dial in Villa Mode.....	45
11.3.2.2. Speed Dial in Building Mode.....	47
11.4. Call Auto-answer Configuration.....	47
11.5. Robin Call Configuration.....	48
11.5.1. Web Call.....	49
12. Call Settings.....	50
12.1. Maximum Call Duration Setting.....	50
12.2. Maximum Dial Duration Setting.....	50
12.3. Audio& Video Codec Configuration for SIP Calls.....	51
12.3.1. Audio Codec Configuration.....	51
12.3.2. Video Codec Configuration.....	52
12.4. Configure DTMF Data Transmission.....	53
13. Phone Book Configuration.....	55
13.1. Phone Book Configuration on the Device.....	55
13.2. Phone Book Configuration on the Web Interface.....	57
13.2.1. Manage Contact Groups on the Web Interface.....	57
13.2.2. Contact List Configuration on the Web Interface.....	57
13.2.2.1. Contact List Display Setting.....	58
14. Relay Setting.....	61
14.1. Relay Switch Setting.....	61

14.2. Web Relay Setting.....	62
14.2.1. Configure Web Relay on the Web Interface.....	62
14.2.2. Configure Web Relay on the Device.....	64
14.3. Relay Schedule.....	65
15. Door Access Schedule Management.....	66
15.1. Configure Door Access Schedule.....	66
15.1.1. Create Door Access Schedule on the Web Interface.....	66
15.1.2. Create Door Access Schedule on the Device.....	68
15.1.3. Import and Export Door Access Schedule.....	69
15.1.4. Edit the Door Access Schedule.....	70
15.1.4.1. Edit the Door Access Schedule on the Web Interface	70
15.1.4.2. Edit the Door Access Schedule on the Device.....	70
16. Door Unlock Configuration.....	72
16.1. Access Authentication.....	72
16.2. Configure PIN Code for Door Unlock.....	73
16.2.1. Configure Public PIN code.....	73
16.2.2. Configure Private PIN Code on the Device.....	75
16.2.3. Configure Private PIN Code on the Web Interface.....	75
16.2.4. Configure Private PIN Access Mode.....	77
16.3. Configure RF Card for Door Unlock.....	79
16.3.1. Configure RF Card on the Web Interface.....	79
16.3.2. Configure RF Card on the device.....	80
16.3.3. Configure RF Card Code Format.....	80
16.4. Mifare card Encryption.....	81
16.5. Configure Facial Recognition for Door Unlock.....	81
16.5.1. Configure Facial Recognition on the Device.....	81
16.5.2. Configure Facial Recognition on Web Interface.....	82
16.6. Edit the User-specific door access data.....	83
16.7. Import and Export User Data of Access Control.....	84
16.8. Configure Bluetooth for Door Unlock.....	84
16.9. Configure Open Relay via HTTP for Door Unlock.....	85
16.10. Unlock by QR Code.....	86
16.11. Configure Exit Button for Door Unlock.....	86
16.12. Configure Reception Tab for Door Unlock.....	87
16.13. Unlock by DTMF code.....	88
17. Security.....	90
17.1. Tamper Alarm Setting.....	90
17.1.1. Configure Tamper Alarm on the Device.....	90
17.1.2. Configure Tamper Alarm on the Web Interface.....	91
17.2. Lock Security.....	91
17.3. Motion Detection.....	92
17.3.1. Configure Motion Detection on the Device.....	92
17.3.2. Configure Motion Detection on the Web Interface.....	94
17.4. Security Notification Setting.....	95

17.4.1. Email Notification Setting.....	95
17.4.2. FTP Notification Setting.....	96
17.4.3. TFTP Notification Setting.....	97
17.5. Web Interface Automatic Log-out.....	97
17.6. Action URL.....	97
17.7. Client Certificate Setting.....	99
17.7.1. Web Server Certificate.....	100
17.7.2. Client Certificate.....	100
18. Monitor and Image.....	102
18.1. RTSP Stream Monitoring.....	102
18.1.1. RTSP Basic Setting.....	102
18.1.2. RTSP Stream Setting.....	102
18.2. MJPEG Image Capturing.....	104
18.3. ONVIF.....	104
18.4. Live Stream.....	105
19. Logs.....	107
19.1. Call Logs.....	107
19.2. Door Logs.....	107
20. Debug.....	109
20.1. System Log for Debugging.....	109
20.2. PCAP for Debugging.....	110
20.3. Remote Debug Server.....	110
21. Firmware Upgrade.....	112
22. Backup.....	113
23. Auto-provisioning via Configuration File.....	114
23.1. Provisioning Principle.....	114
23.2. Configuration Files for Auto-provisioning.....	115
23.3. AutoP Schedule.....	115
23.4. PNP Configuration.....	116
23.5. DHCP Provisioning Configuration.....	117
23.6. Static Provisioning Configuration.....	118
24. Integration with Third Party Device.....	121
24.1. Integration via Wiegand.....	121
24.2. Integration via HTTP API.....	122
24.3. Power Output Control.....	123
24.4. Mobile Community.....	123
25. Lift Control.....	125
26. Password Modification.....	127
26.1. Modifying Device Web Interface Password.....	127
26.2. Modifying System Password.....	127
26.3. Modifying Setting Password.....	129
27. System Reboot&Reset.....	131
27.1. Reboot.....	131
27.2. Reset.....	132

28. Abbreviations.....	134
29. FAQ.....	136
30. Contact us.....	139


1. Product Overview

Akuvox X915 series is an Android-based IP video door phone with a touch screen. It incorporates audio and video communications, access control and video surveillance. Its finely tuned Android OS, Cloud and AI based communication technology allows featured customization to better suit your operation habit. X915 series multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controllers and fire alarm detectors, helping to create a holistic control of building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, NFC, Bluetooth, QR code and newly added voice control door access in an accompaniment with body temperature measurement. X915 series door phone is applicable to residential buildings, office buildings and their complex.

2. Change Log

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

3. Model Specification

	X915S
Model & Feature	
Display	8 Inch IPS LCD
Touch Screen	√
Button	X
Housing Material	316 grade stainless steel and Aluminum
Relay In	3
Relay Out	3
Alarm In	X
RS485	√
PoE	POE+
Resolution	1280x800
Brightness	650nits
RAM	2G
ROM	16G
Card Reader	13.56MHZ & 125KHZ
Wi-Fi	X
Bluetooth	√
IP Rating	IP65
IK Rating	IK10
Temperature detection	Optional
Face recognition	√
LTE	X
USB	X
External SD card	X

	X915S
Wall Mounting	√
Flush Mounting	√
Desk Mounting	X
Wall Mounting Dimension	350x130x41.6mm
Wall Mounting Dimension	350x130x53.9mm
POE+ Standby Power Consumption	5.263W
POE+ Full Load Power Consumption	18.796W
Power Adapter Standby Power Consumption	5.107W
Power Adapter Full Load Power Consumption	19.376W
Color Option	Tarnish Grey

4. Introduction to Configuration Menu

- **Status:** this section gives you basic information such as product information, Network Information, and account information, 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 Log, etc.
- **Surveillance:** this section covers Motion Detection, RTSP, MJPEG, ONVIF, Live stream.
- **Access Control:** this section covers Input control, Relay, Card settings, Face Recognition setting, Private PIN Code, Wiegand connection, etc.
- **Tenants:** this section involves Tenants management and Dial Plan.
- **Device:** this section includes Light settings, tab&button display, LCD settings and Voice settings.
- **Settings:** this section includes Time&language, Action settings, Door settings, Schedule for access control.
- **Upgrade:** this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault Diagnosis.
- **Security:** this section is for 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 a 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 it.
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 property managers 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.

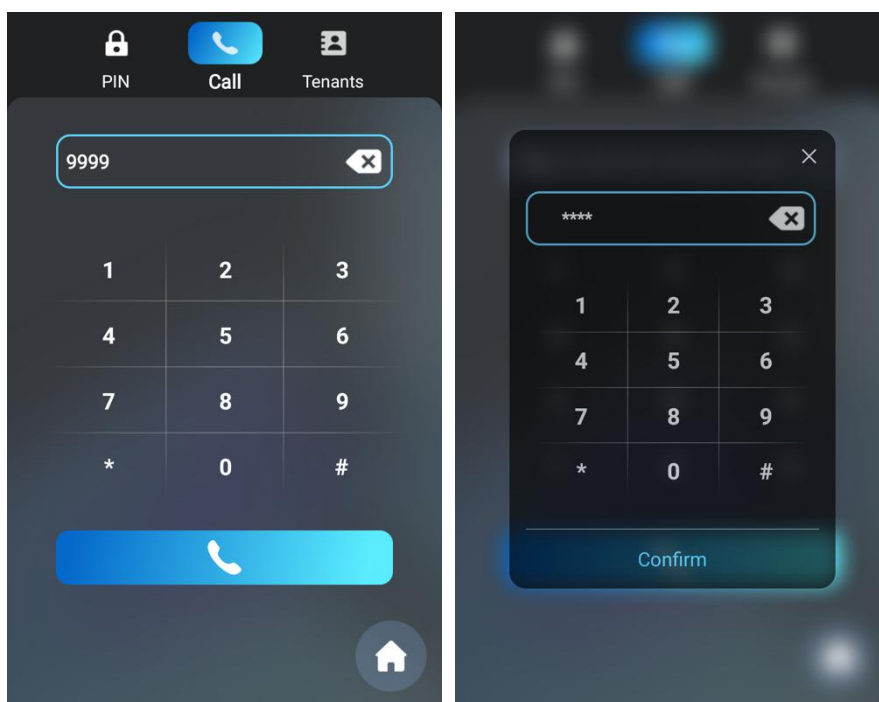
1. **SDMC:** SDMC is suitable for the management of Akuvox devices in large communities, including access control, resident information, remote device control, etc.
2. **Akuvox Upgrade tool:** upgrade Akuvox devices in batch on a LAN (**Local Area Network**)
3. **Akuvox PC Manager:** distribute all configuration items in batch on a LAN.
4. **IP scanner:** it is used to search Akuvox device IP addresses on a LAN.
5. **FacePro:** manage face data in batch for the door phone on a LAN.

5. Access the Device

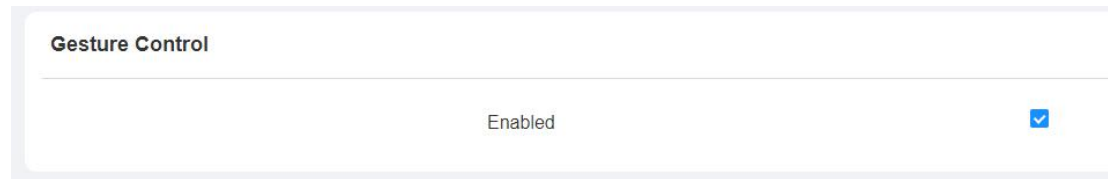
X915 series door phone system settings can be either accessed on the device directly or on the device web interface.

5.1. Access the Device Setting on the device

Before configuring Akuvox X915, please make sure the device is installed correctly and connects 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**. Or set up some basic settings on the device screen by pressing **9999** + **Dial** key + **3888**(password) on **Dial** screen.

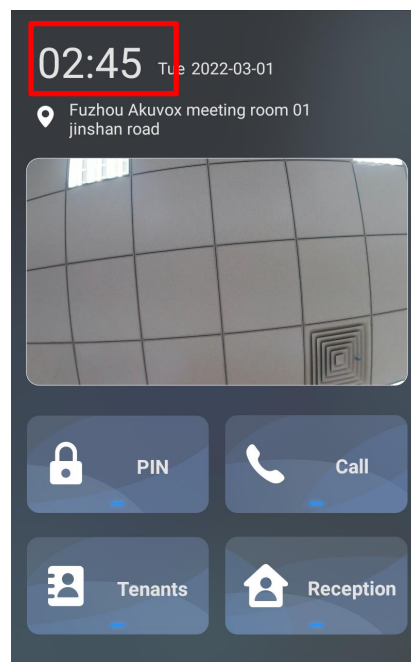


In certain application scenarios where the dial icon is missing on the screen, you can still access the device setting using gesture control feature. You can navigate to **Security > Basic > Gesture Control**.



Parameter Set-up:

- **Enabled:** if enabled, you can keep tapping the upper left corner of the screen for 10 times to access the setting screen.



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.

 Remember User Name/Password**Note:**

- You can also obtain the device IP address using the Akuvox IP scanner to log in 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>

**Note:**

- 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.

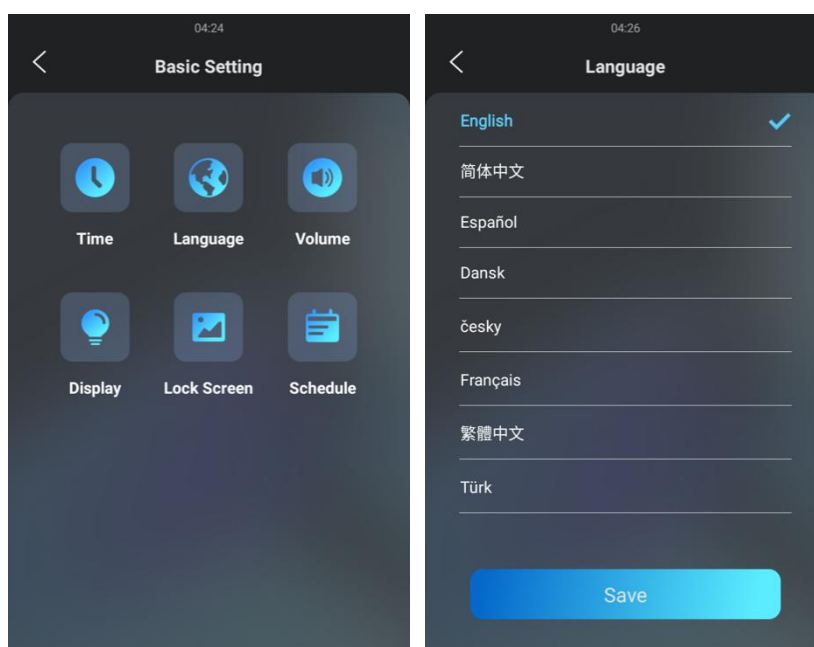
6. Language and Time Setting

6.1. Language Setting

When you first set up the device, you might need to set the language to your needs, or you can do it later if needed. And the language can either be set up directly on the device or on the device web interface according to your preference.

6.1.1. Language Setting on the Device

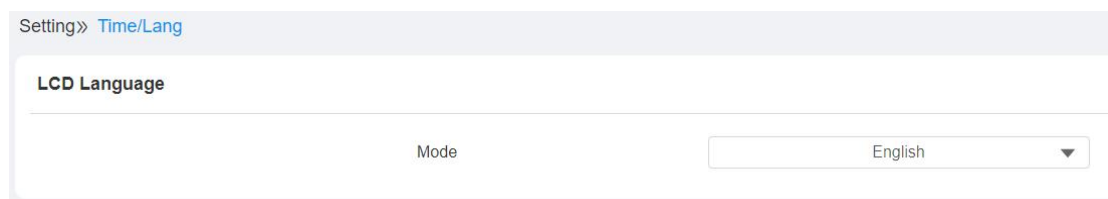
Language settings can be configured on the device and on the device web interface that allows you to select or change the language for screen display to your preference. To configure the language display on the device **Basic Setting > Language** interface.



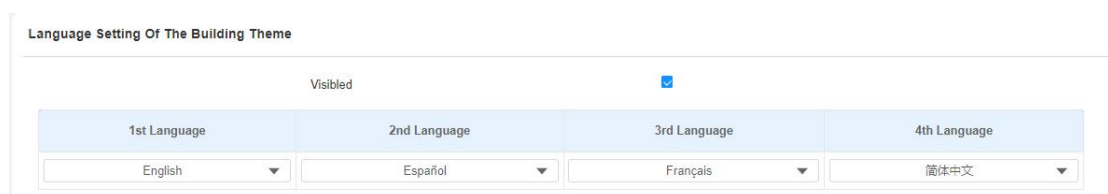
6.1.2. Language Setting on the Device Web Interface.

In the building mode, you can not only select the language for the device, but also create language icons on the home screen so that you can easily select the language you need.

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



To create the language icons, navigate to **Device > Key/Display > Language Setting Of The Building Theme**.



Parameter Set-up:

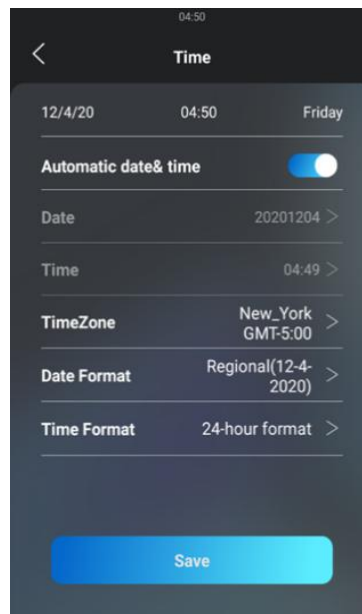
- **Visible:** enabled it if you want the four language icons to be displayed on the home screen for the language selection.
- **Language 1/2/3/4:** select the order the language display. For example, if you set the 1st language as English, then English language will be displayed first from left to right on the screen.

6.2. Time Setting

Time settings can be set up on the device and on the device web interface in terms of time zone, date, and time format, etc.

6.2.1. Time Setting on the Device

To configure the time, go to **Basic Setting > Time** interface.



Parameter Set-up:

- **Automatic Date&Time:** Automatic Date is toggled on by default, which allows the date& time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**). You can also set it up manually by toggling off the switch first then entering the time and date you want before pressing the **Save** tab for the validation.
- **Date:** click on **Date** to set the date.
- **Time:** click on **Time** to set the time.
- **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**.
- **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.

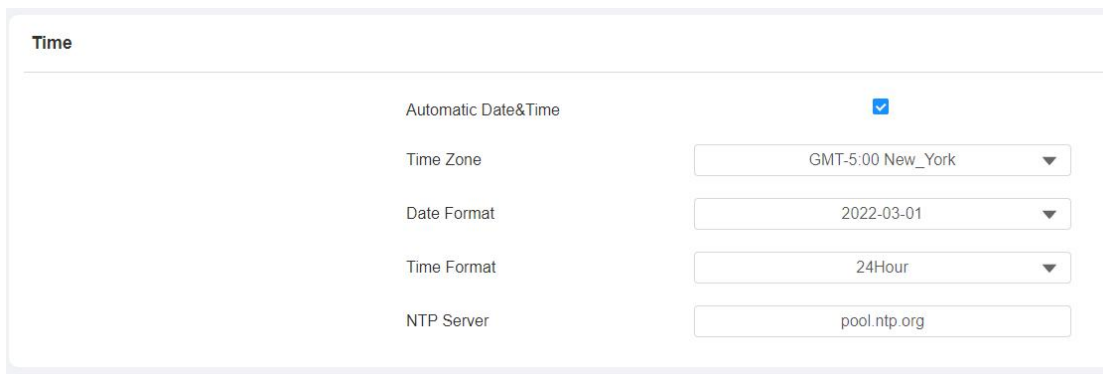
- **Time Format:** you can either select 12 hour or 24-hour time format as you like, and then press the Confirm tab for the confirmation.

 **Note:**

- When the **Automatic Date&Time** toggle switch is toggled off then parameters related to NTP server will become not editable. And when the switch is toggled on, then time and date will be denied editing.

6.2.2. Time Setting on the Device Web Interface

Time setting on the web interface also 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.



Time	
Automatic Date&Time	<input checked="" type="checkbox"/>
Time Zone	GMT-5:00 New_York
Date Format	2022-03-01
Time Format	24Hour
NTP Server	pool.ntp.org

Parameter Set-up:

- **NTP Server:** enter the NTP server you obtained in the **NTP server** field.

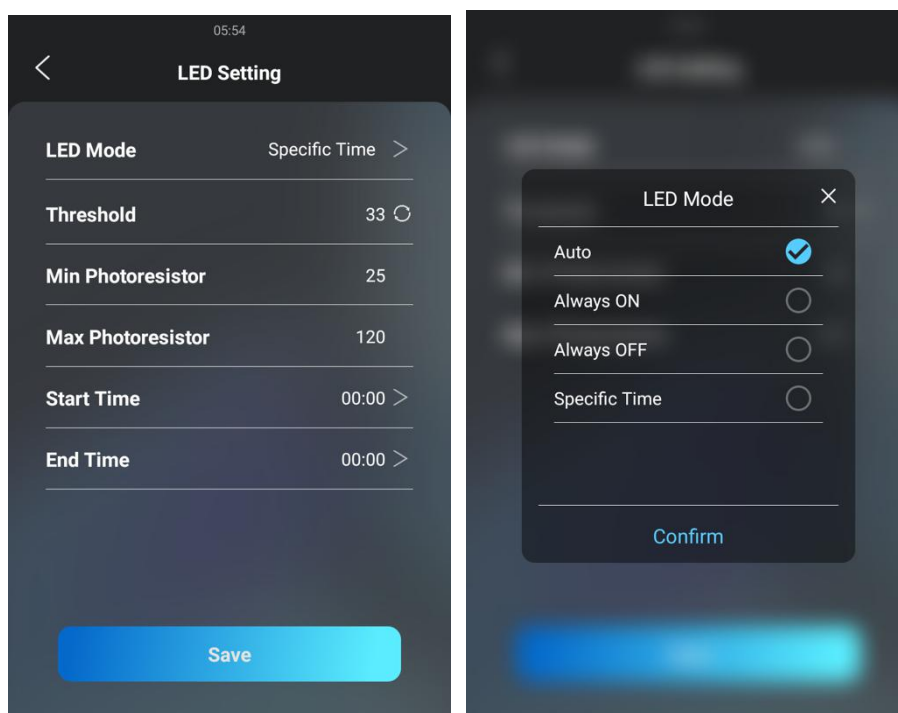
7. LED&LCD Setting

7.1. Infrared LED Setting

Infrared LED is used to help you see the surroundings or visitors in front of the door phone through the door phone camera in the dark environment.


7.1.1. Infrared LED Setting on the Device

To configure the language display on the device **Basic Setting > Display > LED Setting** interface.



Parameter Set-up:

- **Auto:** select "Auto" if you want the Infrared LED light to be turned on automatically according to the setting.

- **Always ON:** select "**Always ON**" to enable the Infrared LED light to stay on permanently.
- **Always OFF:** select "**Always OFF**" to turn off the Infrared LED light. LED mode is set "**Always OFF**" by default.
- **Specific Time:** select "**Specific Time**" to turn on the infrared LED according to the time schedule.
- **LED Type:** you can see the LED type "**Auto**" "**Always ON**" "**Always OFF**" "**Specific Time**" you selected.
- **Threshold:** refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is "**33**", however, you can tap the  icon several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on to configure the minimum and maximum photo-resistor values.
- **Min/Max Photoresistor:** set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the **ON-OFF** of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default Minimum and maximum photoresistor value are from "**0**" minimum to "**1000**" maximum respectively.
- **Start Time:** set the start time for the infrared LED to be turned on.
- **End Time:** set the end time for the infrared LED to be turned off.

 **Note:**

- **Start Time** and **End Time** will not be displayed unless you select **Specific Time** for your LED mode.

7.1.2. Infrared LED Setting on the Web Interface

You can also select the LED type on the device web interface if needed. To configure the configuration on the web **Device > Light > LED** interface.

Device» Light

LED

Mode

Photoresistor Setting - (0-1200)

Note:

- Please refer to the infrared LED parameter setting on the device.

7.2. LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, If you do not want to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce the electrical power consumption. To configure the configuration on the web **Device > Light > LED Of Swiping Card Area** interface.

LED Of Swiping Card Area

Enabled

Start Time (0-23Hour)

End Time (0-23Hour)

Parameter Set-up:

- **Enabled:** tick the check box if want to enable the card reader LED lighting and vice versa.
- **Start Time- End Time (H):** enter the time span for the LED lighting to be valid, e.g, if the time span is set from **8-0 (Start time- End time)** it means the LED light will stay on during the time span from **8:00 am to 12:00 pm**

during one day (24 hours).

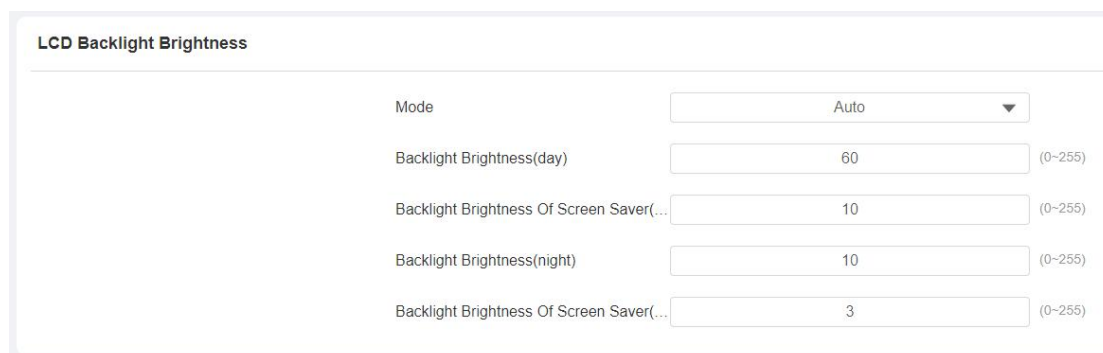
7.3. LCD Screen Brightness Setting

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.

7.3.1. 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 > Light > LCD Backlight Brightness** interface.



LCD Backlight Brightness		
Mode	<input type="text" value="Auto"/>	
Backlight Brightness(day)	<input type="text" value="60"/>	(0-255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="10"/>	(0-255)
Backlight Brightness(night)	<input type="text" value="10"/>	(0-255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="3"/>	(0-255)

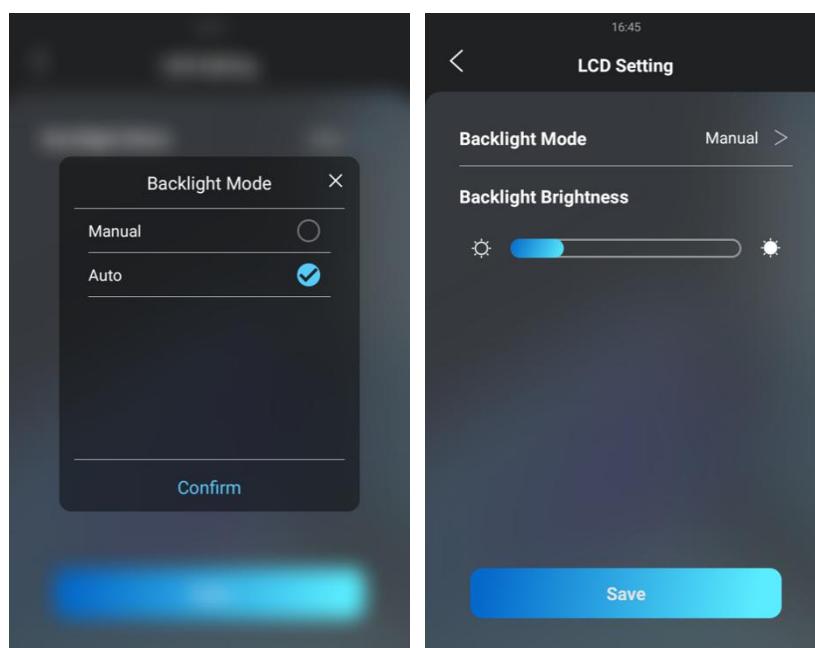
Parameter Set-up:

- **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):** set the screen backlight brightness during the daytime with the value ranging from (0-255).
- **Backlight Brightness Of Screen Saver (day):** set the screen backlight brightness for the screen saver during the day time with the value ranging from (0-255).

- **Backlight Brightness (night)**: set the screen backlight brightness in night with the value ranging from (0-255).
- **Backlight Brightness Of Screen Saver (night)**: set the screen backlight brightness for the screen saver during the day time with the value ranging from (0-255).

7.3.2.LCD Screen Brightness Setting on the Device

On the device, you can set and adjust the screen backlight brightness. To configure the language display on the device **Basic Setting > Display > LCD Setting** interface.



7.4. LED White Light Setting

White light LED is mainly used to reinforce the lighting for the QR code access and for the greater visibility of the visitors when see their images from indoors in a dark environment. You can set the white light function properly on the device web interface. To configure the configuration on the **Device > Light > White Light** interface.

White Light

Mode

OFF

OFF

Auto

Cancel

Submit

Parameter Set-up:

- **Mode:** select **"Auto"** or **"OFF"**. If you select **"Auto"** then the white light will turn on for 5 minutes for facial recognition and QR code scan.

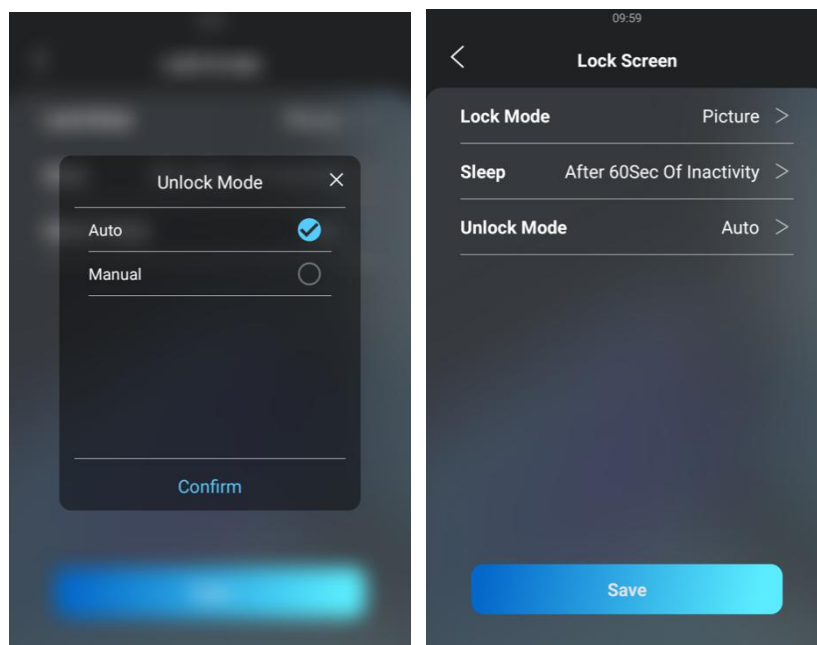
8. Screen Display Configuration

X915 series 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.

8.1. Screensaver Configuration

8.1.1. Configure Screensaver on the Device

Sleep mode and screen saver 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 the device screen, go to **Basic Setting > Lock Screen**.



Parameter Set-up:

- **Lock Mode:** select among three options "NONE", "Blank Screen", and

“Picture”. “NONE” is selected when you want the screen to stay on without going in to screen saver mode; if “Blank Screen” is selected, the screen will go black. If “Picture” is selected, then the picture you uploaded will be shown as the screen saver.

- **Sleep:** set the screen saver start time from 5 seconds up to 180 seconds. Screen saver starts when the device detects no operation, or no one is approaching.
- **Unlock Mode:** select the screen wake-up mode. If you select “Auto” mode then the screen will be awakened when someone approaches without its being touched upon, and if “Manual” mode is selected, then you have to touch and wake up the screen.



Note:

- **Unlock Mode** cannot be changed from “Auto” to “Manual” when the **Lock mode** is set as “Blank Screen”.

8.1.2. Configure Screensaver on the Web Interface

You can also conduct the await screen configuration on the web interface where you can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction. To configure the configuration on the web **Device > LCD > Standby Interface Display** interface.

Device» LCD

Standby Interface Display

Screensaver Mode	<input type="text" value="Image"/>
Screensaver Time(Sec)	<input type="text" value="60"/>
Wake Up Screensaver Mode	<input type="text" value="Auto"/>
Deep Sleep Enabled	<input type="checkbox"/>
Deep Sleep Interval(Min)	<input type="text" value="30"/>

Parameter Set-up:

- **Screensaver Mode:** select among three options “**NONE**”, “**Blank**”, and “**Image**”. “**NONE**” is selected when you want the screen to stay on without going in to screen saver mode; if “**Blank**” is selected, the screen will go black. If “**Image**” is selected, then the picture you uploaded will be shown as the screen saver.
- **Screensaver Time (Sec):** set the screen saver start time from 5 seconds up to 180 seconds. Screen saver starts when the device detects no operation, or no one is approaching.
- **Wake Up Screensaver Mode:** select the screen wake-up mode. If you select “Auto” mode then the screen will be awakened when someone approaches without its being touched upon, and if “Manual” mode is selected, then you have to touch and wake up the screen.
- **Deep Sleep Enabled:** tick the check box if you want the screen to be turned off after the screensaver reaches the end of duration as predefined.
- **Deep Sleep Interval (Min):** set the screensaver time duration before the screen can be turned off.

**Note:**

- **Wake Up Screensaver Mode** cannot be changed from **Auto** to **Manual** when the **Screensaver Mode** is set as **Blank Screen**.

8.2. Upload Screensaver

You can upload screen saver pictures separately or in batch to the device and to the device web interface for publicity purpose or for a greater visual experience. To configure the configuration on the web **Device > LCD > Upload ScreenSaver** interface.

Upload Screensaver

ScreenSaver1 ▾ Import

Screensaver ID	File Status	Interval(Sec)	Submit	Delete
1	File Exists	<input type="text" value="5"/>	Submit	Delete
2	File Exists	<input type="text" value="5"/>	Submit	Delete
3	File Exists	<input type="text" value="5"/>	Submit	Delete
4	File Exists	<input type="text" value="5"/>	Submit	Delete
5	File Exists	<input type="text" value="5"/>	Submit	Delete

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 the repetitive designation of pictures to the same ID order occurred.

8.2.1.Upload Device Booting Image

You can upload the booting image to be displayed during the device's booting process if needed. To configure it on the web, navigate to **Device > Key/Display > Picture/File Import** interface.

Picture/File Import

Boot Animation (.png / .zip)

Import

Reset

Background of Tenants List(.png)

Import

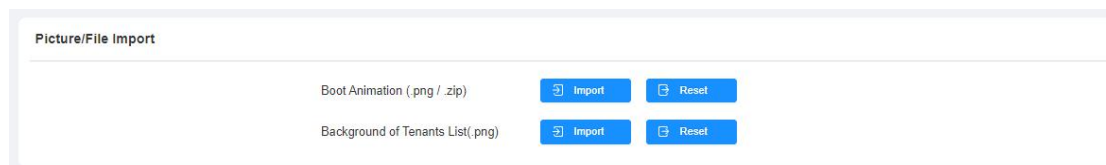
Reset

 **Note:**

- The pictures uploaded should be in **.png or .zip format**.

8.3. Upload Device Contact List Background Image

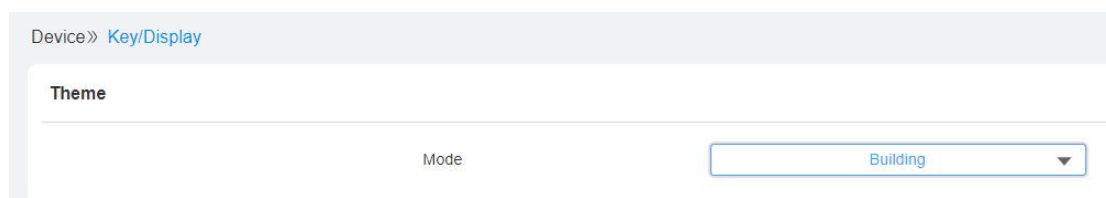
X915 allows you to customize the background display for the contact list. You can select the picture you like before uploading. On the web , navigate to **Device > Key/Display > Picture/File Import** interface.

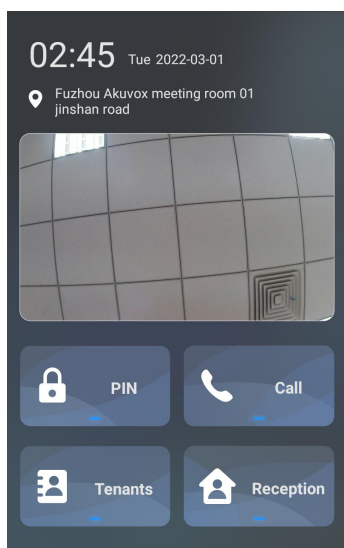
 **Note:**

- The pictures uploaded should be in **.png or .zip format**

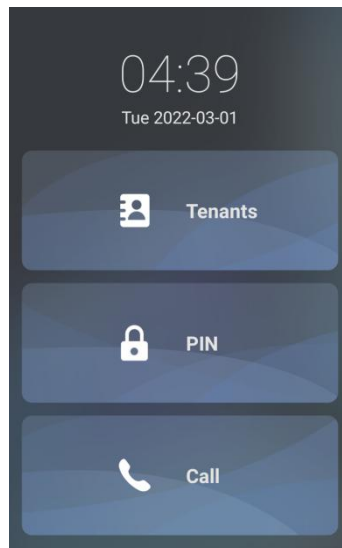
8.4. Configuration for Scenario-based Screen Display Mode

X915 door phones offer you two types of screen display modes for different applications: Building mode, and Villa Mode. On the web interface, navigate to **Device > Key/Display > Theme**.





Building Mode



Villa Mode

8.5. Villa Mode Home Screen Display

You can configure the screen display for the layout of Tenant icon, PIN icon and Call icon on the home screen in villa mode. You can navigate to Device > Key/Display > Key In Homepage Of The Office Theme And Villa Theme interface.

View Control of The Villa Theme

Default Page:

Index	Key	Label	Value
1	Tenants		VISIBLE
2	PIN		VISIBLE
3	Call		VISIBLE

Parameter Set-up:

- **Default Page:** select **"Home Page"** if you display the tenants, PIN and Call icon vertically on the home screen. Select **"Tenant"** if you want to display the contact on the home screen. Select **"PIN"** if you want to display PIN icon with keypad on the home screen. Select **"Call"** if you want to display Call icon with dial pad on the home screen.
- **Key:** set the type of icon you want to display on the villa mode home

screen.

- **Label:** name the icons on the villa mode home screen.
- **Visible:** if you set the icon as invisible, the icon will not be seen on the screen.

8.6. Building Mode Home Screen Display

You can change the home screen display through the configuration of tab name and tab arrangement on the device web **Device > Key/Display > Key In Homepage Of The Building Theme** interface.

Key In Homepage Of The Building Theme

Voice Prompts Enabled

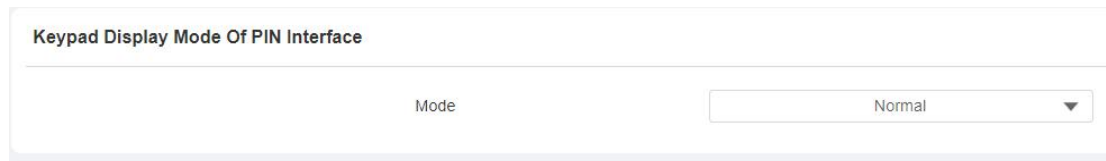
Index	Label	Type	Value
1	<input type="text"/>	PIN	<input type="text"/>
2	<input type="text"/>	Call	<input type="text"/>
3	<input type="text"/>	Tenants	<input type="text"/>
4	<input type="text"/>	Speed Dial	<input type="text"/>

Parameter Set-up:

- **Type:** select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make **Speed Dial** tab be displayed in position one, you can change the type in index number 1 to **Speed Dial**. And you can change another tab position accordingly.
- **Label:** enter a new name to replace the original tab name, but it does not change the attribute of the type.
- **Value:** enter the speed dial number.
- **Voice Prompts Enabled:** if enabled, you will hear the voice prompt.

8.7. Dial Key Order

You can select normal or disordered key display on the door phone. You can select the disordered key display for the security concern. You can navigate to **Device > Key/Display > Keypad Display Mode of PIN Interface**.



Keypad Display Mode Of PIN Interface

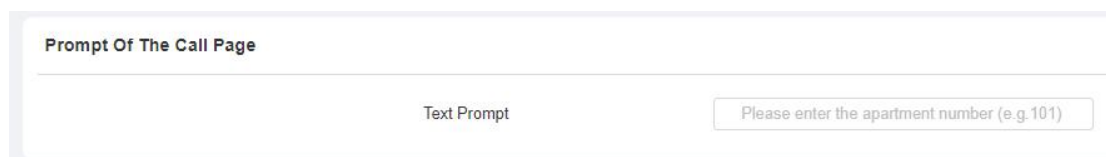
Mode

Parameter Set-up:

- **Display Mode:** select the key order display. Select the disorder key display to better protect your PIN code from being seen by others as you enter the PIN code.

8.7.1. Dial Screen Prompt Display

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



Prompt Of The Call Page

Text Prompt



Note:

- X915 supports 128-digit character maximum in length for the text prompt.

8.7.2. Open Door Text Prompt Display

You can enable or disable the open door prompt if needed. To do so, navigate to **Setting > Door > Door Setting General**.

Door Setting General

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

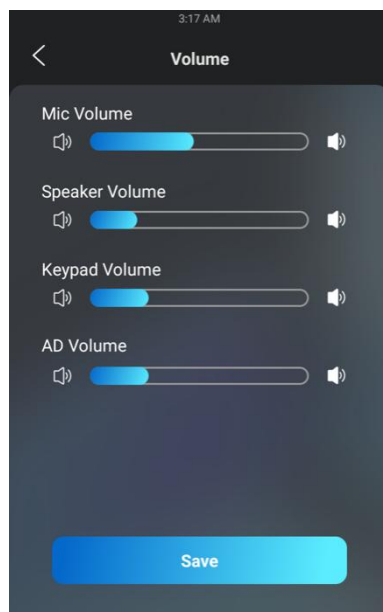
9. Volume and Tone Configuration

Volume and tone configuration in X915 refers to the microphone volume, the AD 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.

9.1. Volume Configuration

9.1.1. 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:

- **Mic Volume:** adjust the microphone volume according to your need.
- **Speaker volume:** adjust the loudspeaker volume according to your need.
- **Keypad Volume:** adjust the keypad volume for the button touch sound.

- **AD Volume:** adjust the announcement volume. Announcement can be, for example, the open-door success announcement, ring-back sound, and other prompt sounds.
- **Key Volume:** adjust the volume for the button touch sound.

9.1.2. 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 > Voice** interface.

Device» Voice

Volume Control

Tamper Alarm Volume (0~15)

Mic Volume (0~127)

Volume Control On Talking Interface

Enabled

Mic Mode

Select On

Parameter Set-up:

- **Tamper Alarm Volume:** set the tamper alarm volume from 0-15 according to your need. The default volume is "8".
- **Mic Volume:** set the mic volume from 0-15 according to your need. The default volume is "8".
- **Enabled:** tick off the check box if you allow the adjustment to be made on the call volume on the talking screen during a call.
- **Select On:** select which mic to be applied between the left and right

microphones.

**Note:**

- When the Call volume on the above web interface is enabled, you are allowed to adjust the call volume during the call session.

9.2. 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 > Voice > Open Door Tone Setting** interface.

Open Door Tone Setting

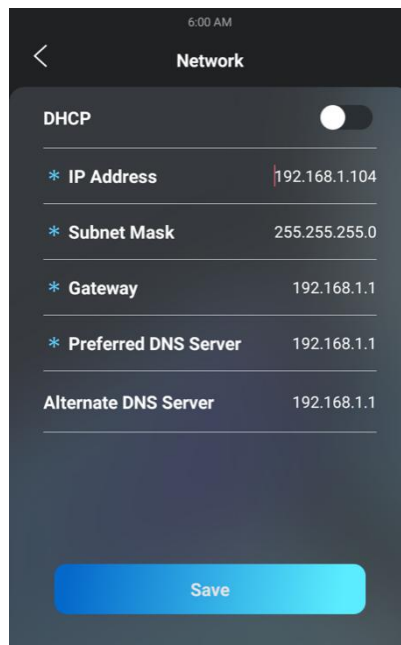
Open Door Tone Enabled

Open Door Tone Upload

10. Network Setting

10.1. 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 language display on the device **Setting > Network** interface.



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.
- **Preferred&Alternate DNS Server:** set up preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address, and the door phone will connect to the alternate server when the primary DNS server is unavailable.

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

10.2. Device Local RTP configuration

For the device network data transmission purpose, the device needs to be set up with a range of RTP port (**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.

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.

10.3. 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 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 features several settings:

- Server Mode:** Set to SDMC.
- Discovery Mode:** Enabled (checked).
- Device Address:** Five input boxes, each containing the number '1'.
- Device Extension:** One input box containing the number '1'.
- Device Location:** One input box containing the text 'Door Phone'.

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

Parameter Set-up:

- **Server 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.

10.4.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. To configure the configuration on the web **Account > Advanced > NAT** interface.

The screenshot shows the NAT configuration page. It has a title 'NAT' and three settings:

- UDP Keep Alive Messages:** A checkbox that is checked.
- UDP Alive Messages Interval:** A text input field containing the value '30', with '(5-60Sec)' written to its right.
- RPort:** A checkbox that is unchecked.

Parameter Set-up:

- **UDP Keep Alive Messages:** if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive 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**).

11. Intercom Call Configuration

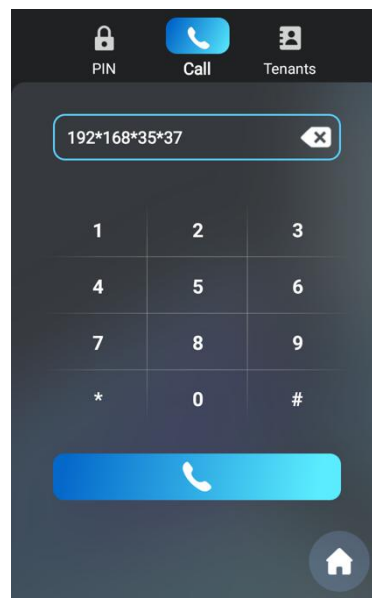
Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

11.1. 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.

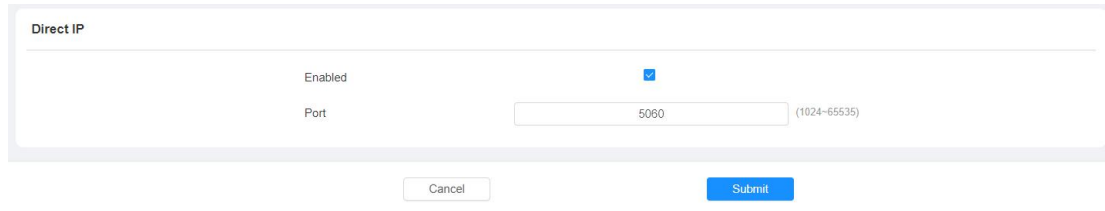
11.1.1. Make IP Calls

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



11.1.2. IP Call Configuration

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



Direct IP

Enabled

Port (1024-65535)

Cancel Submit

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 1-65535. And you enter any values within the range other than 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

11.2.SIP Call &SIP Call Configuration

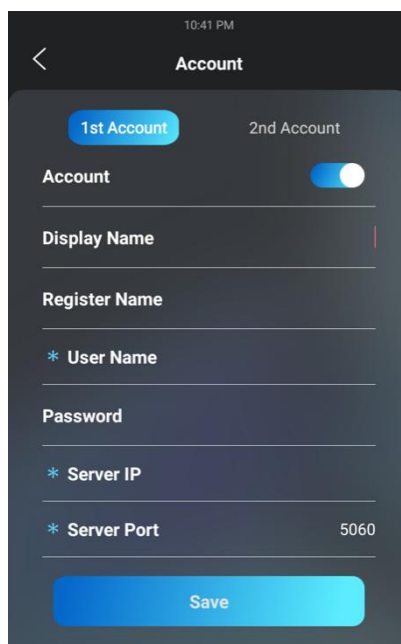
You can make SIP call (**Session Initiation Protocol**) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

11.2.1. SIP Account Registration

X915 series 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. The SIP account can be configured on the device and on the device interface.

11.2.1.1. Configure SIP Account on the Device

To configure the SIP account on the device **Setting > Account** interface.



Parameter Set-up:

- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **User Name:** enter the user name obtained from SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.
- **Server IP:** enter the SIP server address for the SIP account selected.
- **Server port:** enter the SIP server port for communication. The SIP port is "5060" by default.

11.2.1.2. Configure SIP Account on the Web Interface

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

The screenshot shows the 'SIP Account' configuration page. It features a table with the following fields and values:

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

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account Active:** click **Enable** or **Disable** to activate or deactivate the registered SIP account.
- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.
- **User Name:** enter the user name obtained from the SIP account administrator.
- **Account:** select the exact account (Account 1&2) to be configured.
- **Display Label:** configure the device label to be shown on the device screen.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

administrator.

11.2.2. SIP Server Configuration

SIP servers can be set up for devices in order to achieve call sessions 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 pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is "1800", ranging from 30-65535s.

11.2.3. 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.

Parameter Set-up:

- **DND:** enable or disable the DND function. DND function is disabled by default.
- **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”.

11.2.4. Configure Outbound Proxy Server

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

Parameter Set-up:

- **Enable Outbound:** click **Enable** and **Disable** to turn on or turn off the outbound proxy server.
- **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.

11.2.5. Configure Data Transmission Type

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

Transport Type

Type

Cancel Submit

Parameter Set-up:

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

- **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.

11.3.Dial Options Configuration

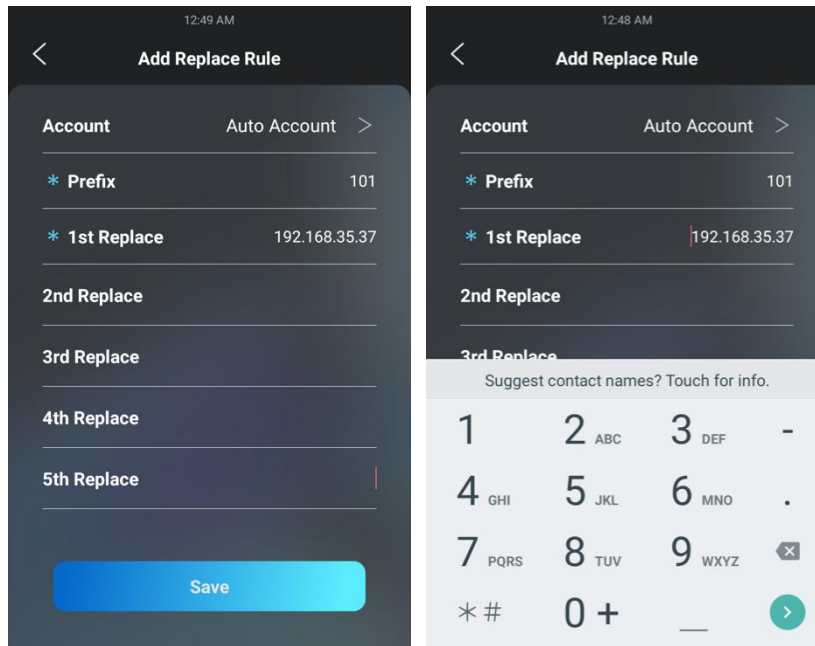
X915 series offers a variety of Dial options that allows you to have fast dial experience while relieving you off memory burden due to long and complex dial numbers.

11.3.1. 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 configure the dial number replacement on the device and on the device web interface. You can replace a multiple device dial numbers such as IP addresses or SIP numbers with only one short number.

11.3.1.1. Quick Dial by Number Replacement on the Device

To configure the language display on the device **Setting > Replace Rule > Add Replace Rule** interface.



Parameter Set-up:

- **Account:** select the account to which you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the 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 of the device configuration. For example, if you replace five original dial numbers with a common short number such as **101** then the five intercom devices with the dial number will be called at the same time when you dial **101**.

11.3.1.2. Quick Dial by Number Replacement on the Web Interface

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

Replace Rule

+ Add
Ⓜ Import
Export ▼

Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
<input checked="" type="checkbox"/>	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"/>	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

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.

11.3.2. Speed Dial

11.3.2.1. Speed Dial in Villa Mode

Speed dial is a function that allows you to create tab or a combination of organized tabs to be displayed on the device's dial screen. You can make call by pressing the specific tabs to make speedy calls without entering any dial numbers. To configure the speed dial on the web **Device > Key Display > Display Mode of Call Interface (Speed Dial)**.

Display Mode of Call Interface (Speed Dial)

Mode

Keys

<input type="checkbox"/>	Index	Name	Number
<input checked="" type="checkbox"/>	1	Management Center	1001
<input type="checkbox"/>	2		
<input type="checkbox"/>	3		
<input type="checkbox"/>	4		
<input type="checkbox"/>	5		
<input type="checkbox"/>	6		
<input type="checkbox"/>	7		
<input type="checkbox"/>	8		

Parameter Set-up:

- **Mode:** select speed dial tab layout among 9 options to your preference. Each option offers you the different layout of dial tabs along with changes to the soft keypad arrangement on the dial screen. The 9 options are explained as follows:
- **Name:** enter the speed dial tab name.
- **Number:** enter the speed dial number.

Options	Descriptions
Standard	Select " Standard " if you want to display the time and key pad only with no dial tabs.
Auto	Select " Auto " if you want to select the dial tab layout that does match with any one of the other 8 options. For example, if you want to create 3dial tabs, 5 dial tabs or 7 tabs, etc., that does not match with other options.
1 Key	Select " 1 Key " if you display only one dial tab with no keypad.
1 Key + Keypad	Select " 1 Key+Keypad " if you want to display one dial tab with keypad.
2 Keys+ Keypad	Select " 2 Key+Keypad " if you want to display two dial tabs with keypad.
8 Keys	Select " 8 Keys " if you want to display 8 dial tabs with no keypad.
16 Keys	Select " 16 keys " if you want to display 16 dial tabs with

	no keypad.
--	------------



Note:

- This function cannot be applied in **Building Mode**.
- Keypad will not be displayed if the number of the dial tabs is over 4 tabs.

11.3.2.2. Speed Dial in Building Mode

X915 allows you to call a group of people at the same by pressing the “Reception” button. On the web, navigate to **Device > Key/Display > Speed Dial Setting**.

Speed Dial Setting

Group Disabled ▼

Parameter Set-up:

Group: select the contact group to be called by pressing the “Reception” button.

11.4.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. In addition, you can also define the mode in which the calls are to be answered (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

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.

11.5. Robin Call Configuration

Robin Call is a function supported by Akuvox SmartPlus which releases a group of robin call numbers for the application. You can call the targeted group of robin calls (e.g., your extension numbers in your kitchen, bedroom, etc.) in sequential orders until the call is answered. Robin call sequence will complete as soon as the call is answered by any of the targeted extension devices. To configure the configuration on the web **Intercom > Basic > Sequence Call** interface.

Sequence Call

Enabled

Time Out (Sec)

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.

**Note:**

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

11.5.1. Web Call

In addition to making IP/SIP calls directly on the device, you can also make the call on the device web interface without approaching to device physically for testing purpose, etc. You can navigate to **Intercom > Basic > 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.

12. Call Settings

12.1. Maximum Call Duration Setting

X915 series 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.

Max Call Time

Max Call Time (2~30Min)

Parameter Set-up:

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

12.2. Maximum Dial Duration Setting

Maximum Dial duration consists of the 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 hangs 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 hangs 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 (30~120Sec)

Dial Out Time (30~120Sec)

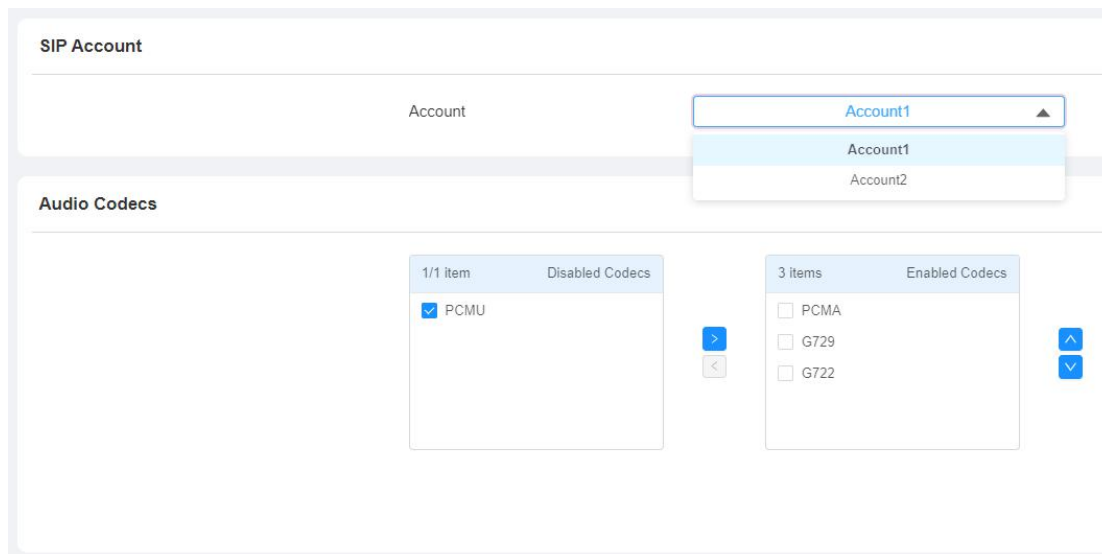
Parameter Set-up:

- **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 device being called.

12.3.Audio& Video Codec Configuration for SIP Calls

12.3.1. Audio Codec Configuration

X915 series 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 bandwidths and sample rates flexibly according to the actual network environment. To configure the configuration 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

12.3.2. Video Codec Configuration

X915 series 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	<input type="text" value="4CIF"/>	▼
Bitrate	<input type="text" value="320 kbps"/>	▼
Payload	<input type="text" value="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 320-2048). The greater the bitrate, the data transmitted every second is greater in amount therefore the video will be clearer. While the default code bitrate is 2048.
- **Payload:** select the payload type (ranging from 90-118) to configure audio/video configuration file. The default payload is 104.

12.4. Configure DTMF Data Transmission

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

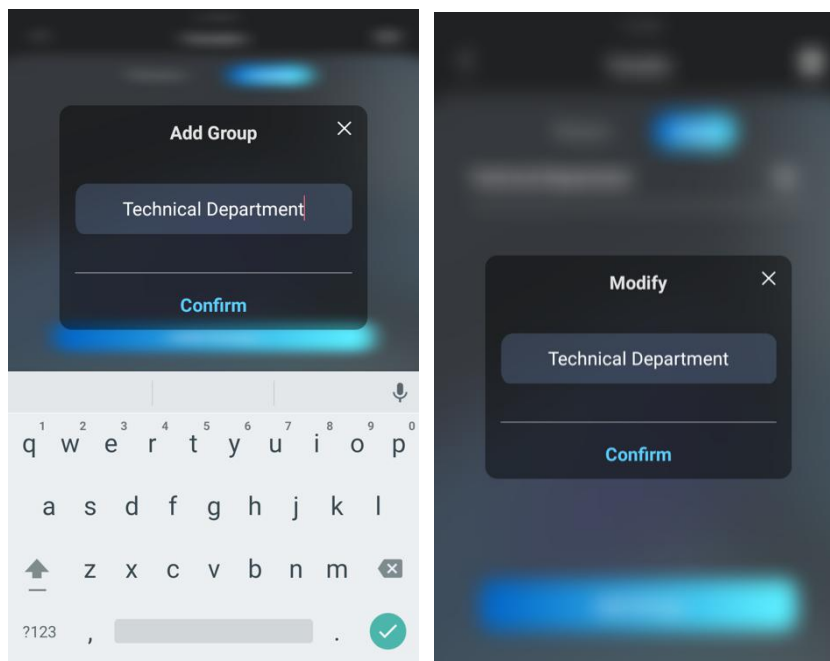
Parameter Set-up:

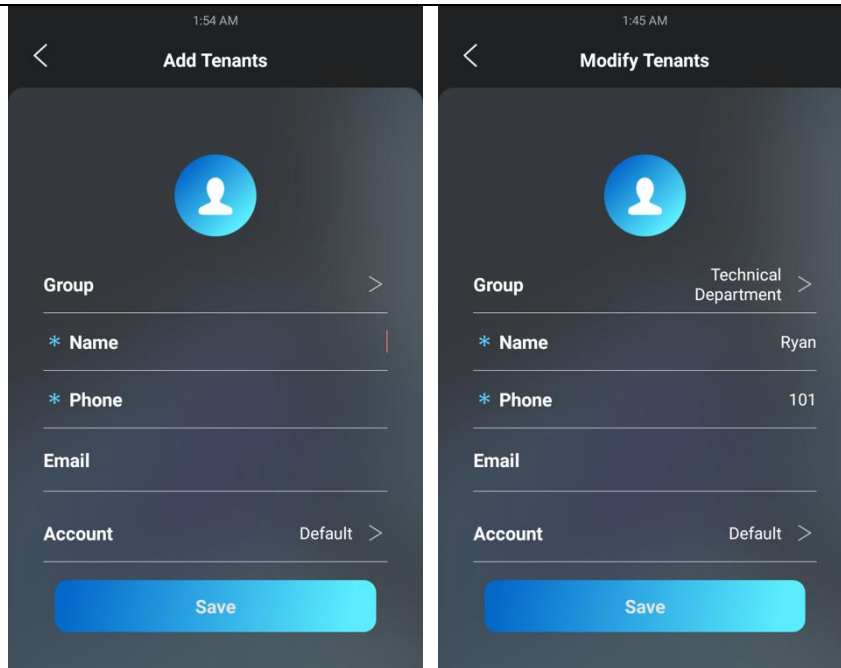
- **Mode:** select DTMF mode among five options: **"Inband"**, **"RFC2833"**, **"Info+Inband"** and **"Info+RFC2833"** based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF:** select among four types: **"Disable"**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

13. Phone Book Configuration

13.1. Phone Book Configuration on the Device

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





Parameter Set-up:

- **Group:** click the green tab to select the group name you have created. You cannot select the group name if no group name has been created.
- **Name:** enter the contact name, which is required.
- **Phone:** enter the phone number of the contact, which is required.
- **Email:** enter the contact's Email, which is optional.
- **Account:** select and assign the group name to an account. If you select the default option, then the contact number will be called out from SIP account 1 if the contact number are set up in both SIP Account 1 and 2.



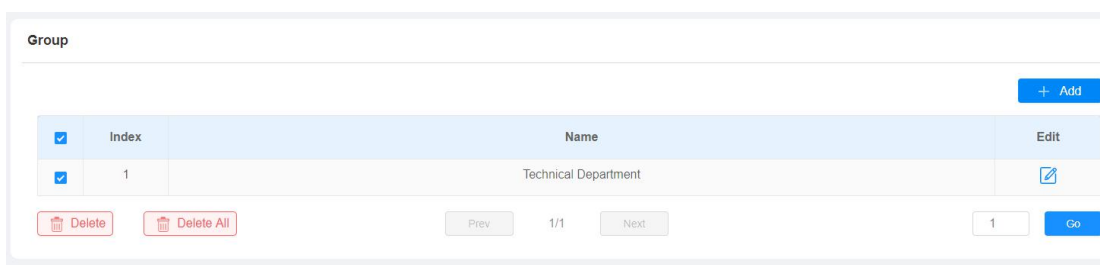
Note:

- Only the SIP numbers of the contacts can be called out through SIP account. IP numbers are not valid for this application.
- Group must be created first before you can select or change the Group.

13.2. Phone Book Configuration on the Web Interface

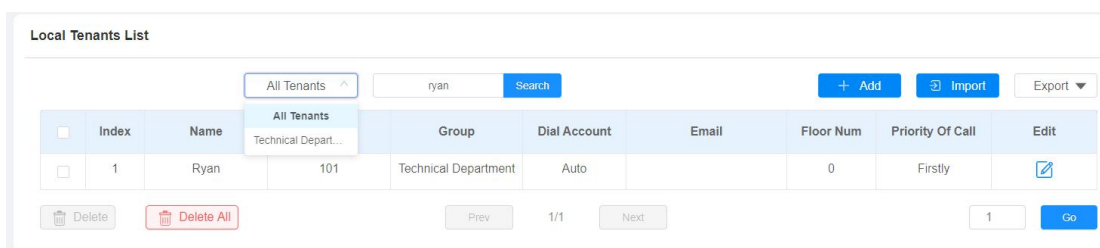
13.2.1. Manage Contact Groups on the Web Interface

You can configure contact and contact groups by adding and editing them on the web **Tenants > Tenants List > Group** interface.



13.2.2. Contact List Configuration on the Web Interface

Contact can also be configured on the web interface where you can also upload the contact pictures if needed. To configure the configuration on the web **Tenants > Tenants List** interface.



Parameter Set-up:

- **Priority of Call:** set the priority of call among four options: **“Null”**, **“Firstly”**, **“Secondary”**, **“Lastly”**. This feature is mainly applicable to the contacts in a specific contact group. For example, if you set the priority of call for one of the contacts in a specific contact group as **“Firstly”** 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.

Note:

- Priority of Call of a contact cannot be set when the contact does belong to any contact group.

Note:

- The contact file format for import should be in .vcf, .csv or .xml format while the contact file format for export should be .vcf format only. And the maximum contact import size is 3000.

13.2.2.1. Contact List Display Setting

If you want to customize your contact list display to your liking, you can go to the web interface to do the configuration. To configure the configuration on the web **Tenants > Tenants List > Tenants List Setting** interface.

Tenants List Setting

Show Tenants Of Local Group Enabled	<input checked="" type="checkbox"/>
Show Cloud Tenants Enabled	<input checked="" type="checkbox"/>
Tenants Sort By	ASCII Code ▼
Click Tenants To Dial Out	<input checked="" type="checkbox"/>
Local Tenants Profile Display Mode	Enabled ▼
Expand Tenants List View Mode	<input type="checkbox"/>
Hide Group Label For Local Tenants List	<input type="checkbox"/>
Tenant List Search Box Visibled	<input checked="" type="checkbox"/>

Parameter Set-up:

- **Show Tenants of Local Group Enabled:** tick or untick the check box to control the display of the group label. If you untick the check box, then only the group tab will be displayed while the contact tab will be concealed and vice versa.
- **Show Cloud Tenants Enabled:** tick the check box to show the cloud tenants in the tenants' list. And when you untick the check box, the cloud tenants will be concealed.
- **Tenants Sort By:** select ASCII Code or Room No. or Import. When you select ASCII Code, the tenants will be listed by their names in the sequence of the ASCII code. When you select Room No., the tenants will be sorted according to their room numbers.
- **Click Tenants to Dial Out:** tick the check box to enable the dial-out by pressing the contact tab. When this function is enabled, you can press anywhere on the contact tab to dial out. This function will be disabled when you untick the check box, and when it is disabled, you need to press the Call icon in the middle of the tab to dial out.
- **Local Tenants Profile Display Mode:** select Enable or Disabled or Auto. When the function is enabled, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, the default contact icon will be displayed next to the name. When disabled, the picture or the icon will not be displayed. When the function is set as Auto, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, there won't be an icon next to the name.
- **Expand Contact List View Mode:** tick the check box to control contact tab size. For example, if you tick the check box then the contact tab will be widened. And the tab will turn to normal size when you untick the check box.
- **Hide Group Label for Contact List:** tick or untick the check box to control the display of the group label. If you untick the check box, then only the contact tab will be displayed while the group tab will be concealed and vice versa.
- **Contact List Search Box Visible:** tick or untick the check box to control the display of the "Tap here to search field" on the top of the screen. If

you untick the check box, then the “Tap here to search field” will be concealed.

14. Relay Setting

14.1. Relay Switch Setting

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

Relay

Relay ID	<input type="text" value="RelayA"/>	<input type="text" value="RelayB"/>	<input type="text" value="RelayC"/>
Trigger Delay(Sec)	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>	<input type="text" value="5"/>	<input type="text" value="5"/>
DTMF Mode	<input type="text" value="1 Digit DTMF"/>		
1 Digit DTMF	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="2"/>
2~4 Digits DTMF	<input type="text" value="010"/>	<input type="text" value="012"/>	<input type="text" value="013"/>
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	<input type="text" value="RelayA"/>	<input type="text" value="RelayB"/>	<input type="text" value="RelayC"/>

Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (Ranging from 1-10 Sec.) For example, if you set the delay time as "5" Sec. Then the relay will not be triggered until 5 seconds after you press "unlock" tab.
- **Hold Delay (Sec):** set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as "5" Sec. Then the relay will be delayed for 5 seconds after the door is unlocked.
- **DTMF Mode:** select the number of DTMF digits for the door access control (**Ranging from 1-4 digits**) For example, you can select 1 digit DTMF code or 2-digit DTMF code, etc., according to your need.
- **1-digit DTMF:** set the 1-digit DTMF code within range from (0-9, *, and #).
- **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

DTMF Mode is set as 3-digits.

- **Relay Status:** relay status is low by default which means normally closed (NC) If the relay status is high, then it is in Normally Open status (NO).
- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

**Note:**

- Only the external devices connected to the relay switch needs to be powered by powered adapters as 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.

14.2. 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.

14.2.1. Configure Web Relay on the Web Interface

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

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

Web Relay

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

Web Relay Action Setting

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

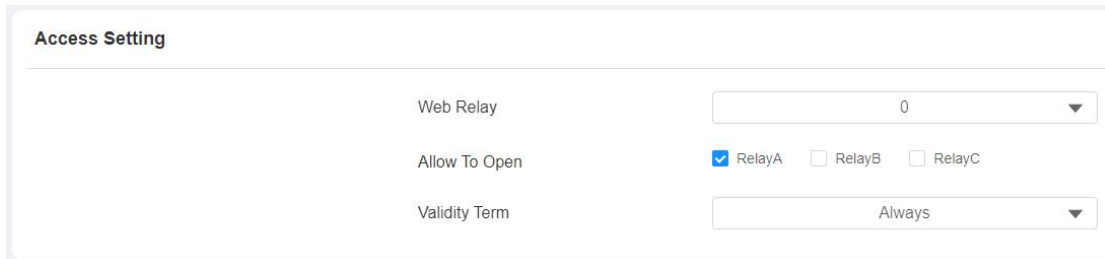
Parameter Set-up:

- **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.
- **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.](http://admin:admin@192.168.1.2/state.xml?relayState=2)

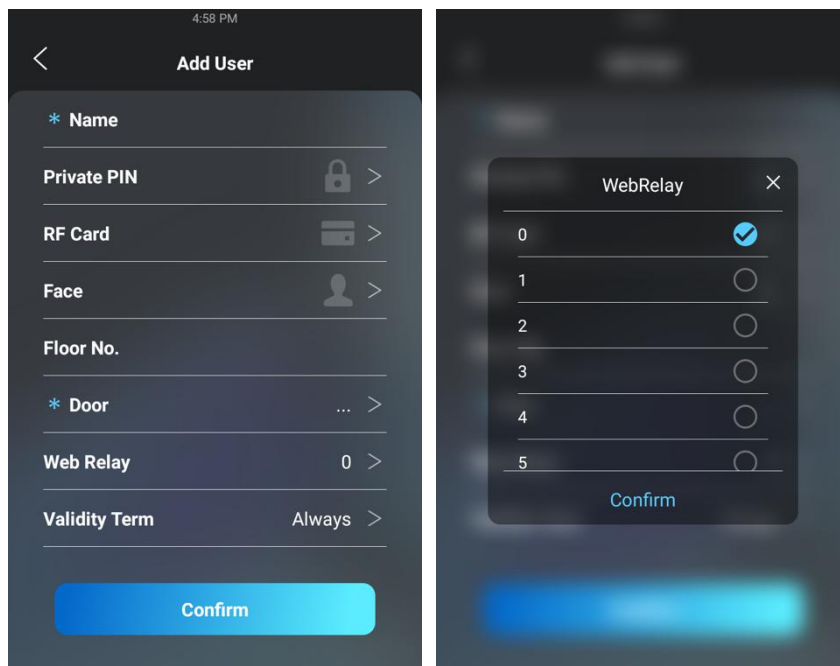
After the web relay is set up, you can configure the specific web relay to be triggered based on the relay location for the door access.

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



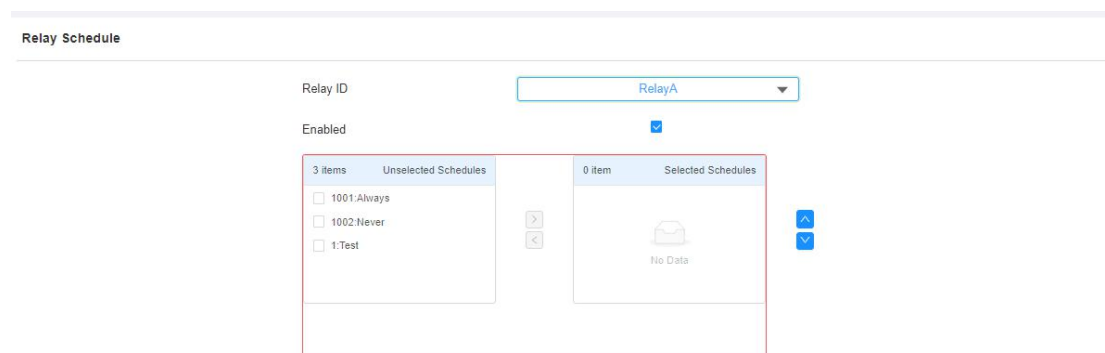
14.2.2. Configure Web Relay on the Device

You can also assign a specific web relay to a resident for the door access based on the order of the web relay set up on the web **Setting > User > Add** interface.



14.3. Relay Schedule

Set the corresponding relay always open at a specific time. This feature is designed for some specific scenarios, for example, the time after school, or for morning work time. To do the configuration, navigate to **Access Control > Relay > Relay Schedule** interface.



Parameter Set-up:

- **Relay ID:** choose on relay you need to set up.
- **Schedule Enabled:** it is disable by default. Only choose to enable it, that you can select the schedule. For creating the schedule, please refer to door access schedule configuration.



Note:

- You can refer to chapter 15.1.1 **Create Door Access Schedule** for the relay schedule setting as the configuration of the relay schedule is identical to the door access schedule.

15. Door Access Schedule Management

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

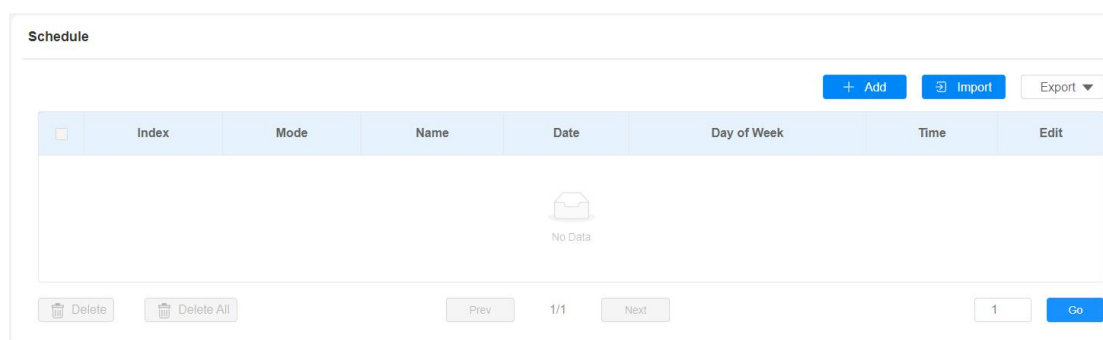
15.1. Configure Door Access Schedule

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.

15.1.1. Create Door Access Schedule on the Web

Interface

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 configure the configuration on the web **Setting > Schedule** interface.



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

The screenshot shows a modal window titled "Add Schedule" with a close button (X) in the top right corner. It contains three input fields: "Mode" is a dropdown menu set to "Daily"; "Name" is an empty text box; and "Start Time - End Time" consists of two time pickers, both set to "00:00". At the bottom right, there are two buttons: "Cancel" (disabled) and "Submit" (active).

Parameter Set-up:

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

To create a weekly schedule:

The screenshot shows a modal window titled "Add Schedule" with a close button (X) in the top right corner. It contains four input fields: "Mode" is a dropdown menu set to "Weekly"; "Name" is an empty text box; "Day" is a section with checkboxes for "Mon", "Tue", "Wed", "Thur", "Fri", "Sat", and "Sun", all of which are checked, and an unchecked "Check All" checkbox; and "Start Time - End Time" consists of two time pickers, both set to "00:00". At the bottom right, there are two buttons: "Cancel" (disabled) and "Submit" (active).

Parameter Set-up:

- **Mode:** select daily schedule.
- **Name:** enter the daily schedule name.
- **Day:** select the day (s) on which door access can be valid on a weekly

basis.

- **Start Time-End Time:** set up the time schedule for the validity of the door access during the day.

To create a longer period schedule:

Add Schedule [X]

Mode: Normal

Name: []

Start Date - End Date: [Start Date] ~ [End Date]

Day: Mon Tue Wed
 Thur Fri Sat
 Sun CheckAll

Start Time - End Time: [00:00] - [00:00]

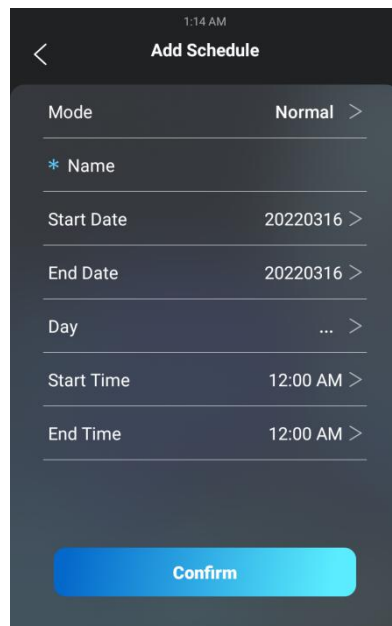
[Cancel] [Submit]

Parameter Set-up:

- **Mode:** select daily schedule.
- **Name:** enter the daily schedule name.
- **Start Date- End Date:** set the date range of the validity of the door access.
- **Day:** select the day (s) on which door access can be valid on a weekly basis.
- **Start Time-End Time:** set up the time schedule for the validity of the door access during the day.

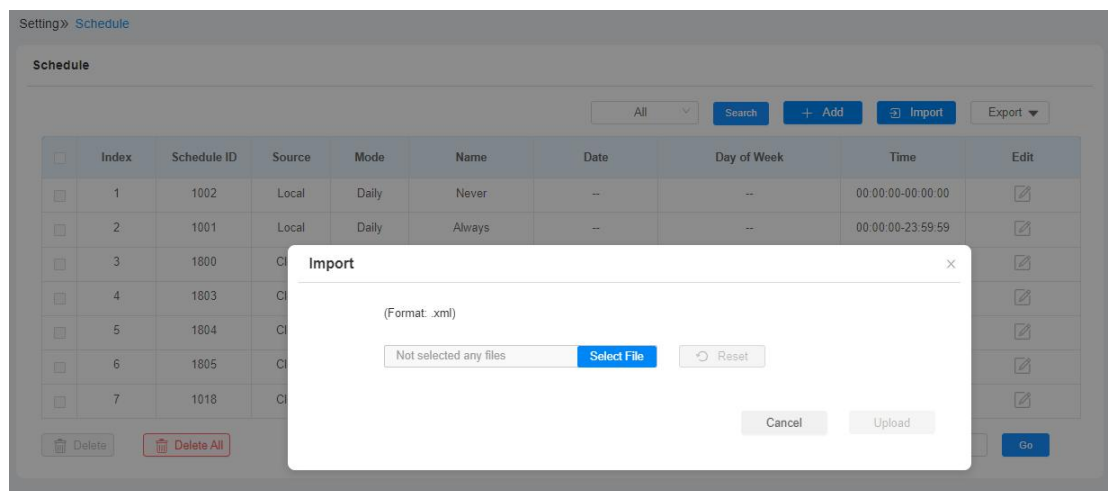
15.1.2. Create Door Access Schedule on the Device.

You can also create door access schedule on the device. Path: **Schedule > Add Schedule**.



15.1.3. Import and Export Door Access Schedule

In addition to creating door access a schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency. To configure the configuration on the web **Setting > Schedule**.





Note:

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

15.1.4. Edit the Door Access Schedule

15.1.4.1. Edit the Door Access Schedule on the Web Interface

If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch on the web **Setting > Schedule** interface.

Schedule

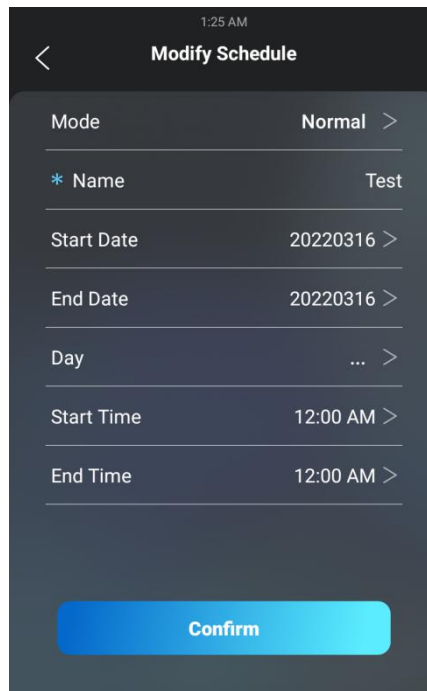
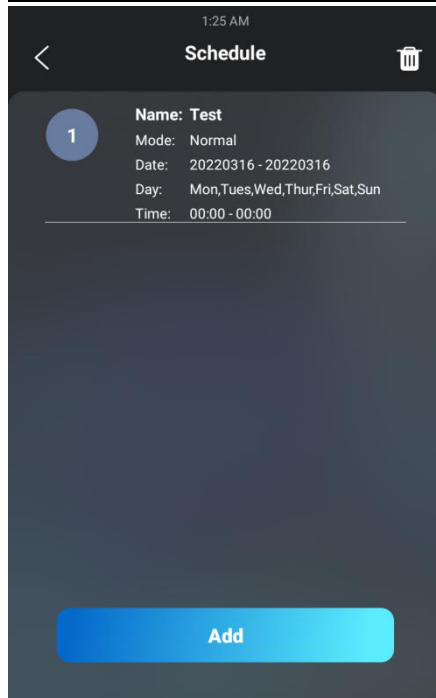
+ Add Import Export ▾

<input type="checkbox"/>	Index	Mode	Name	Date	Day of Week	Time	Edit
<input type="checkbox"/>	1	Normal	Normal	20201201-20201231	Mon Tue Wed Thur Fri Sat Sun	00:00-00:00	
<input type="checkbox"/>	2	Weekly	Weekly	--	Mon Tue Wed Thur Fri Sat Sun	--	
<input checked="" type="checkbox"/>	3	Daily	Daily	--	--	01:09-23:59	

Delete Delete All
Prev 1/1 Next
1 Go

15.1.4.2. Edit the Door Access Schedule on the Device

You can also edit or delete the door access schedule on the device. Path: **Schedule > Schedule**.



16. Door Unlock Configuration

X915 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.

16.1. Access Authentication

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

On the web, navigate to **Access Control > Basic > Access Authentication Mode of The Building Theme**.

The screenshot shows a web configuration page titled "Access Authentication Mode of The Building Theme". It contains four rows of configuration options, each with a label and a dropdown menu:

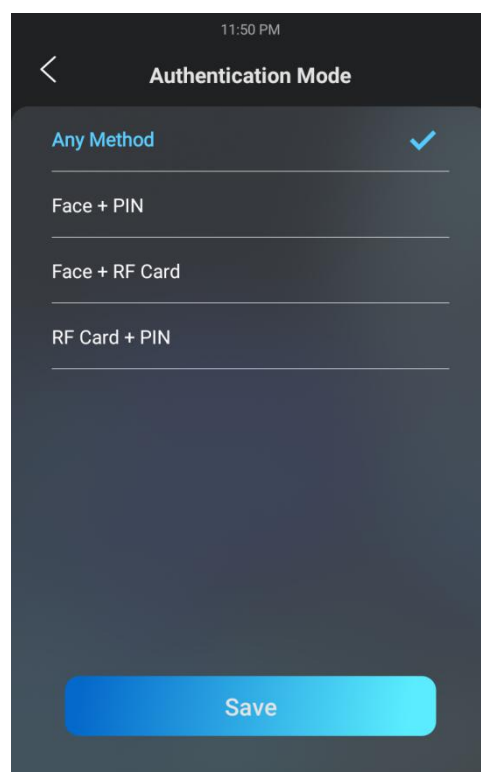
Authentication Mode	Any Method
Inactivity (Sec)	10
Blocked Duration (Sec)	30
Number of Attempts	3

Parameter Set-up:

- **Authentication Mode:** select "Any method" if you allow all the access methods to unlock the door. Select "Face + PIN" if you want to apply dual access methods (Face + PIN) for the door unlock. Select "Face + RF Card" if you want to apply dual access methods (Face+ RF Card) for the door unlock.
- **Inactivity (Sec):** set the authentication timeout for the second authentication. For example, in "Face+PIN" authentication, if you set the authentication timeout as "10" seconds, then you have to enter the PIN code in ten seconds after you passed the face recognition, otherwise, the screen will return to the home screen.

- **Blocked Duration (Sec):** set the block time for the first authentication. For example, if you set the number of attempts as "3", and you failed to pass the second authentication three times, then you will be temporarily blocked from the first authentication according to the block time you defined.
- **Number of Attempts:** set the number of attempts you are allowed for the second authentication.

To set up authentication mode on the device, go to **Security > Authentication Mode**.



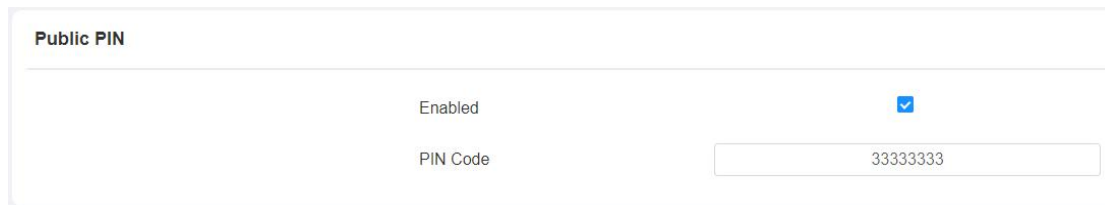
16.2. Configure PIN Code for Door Unlock

You can create and modify both Public PIN code and private PIN code for door access on X915 series door phones.

16.2.1. Configure Public PIN code

You can configure and modify public PIN codes on the device and on the device's web interface.

To configure it on the web interface, navigate to **Access Control > PIN Setting > Public PIN** interface.



The screenshot shows a web interface for configuring the Public PIN. It features a title "Public PIN" at the top left. Below the title, there are two rows of configuration options. The first row is labeled "Enabled" and has a checked checkbox. The second row is labeled "PIN Code" and has a text input field containing the value "33333333".

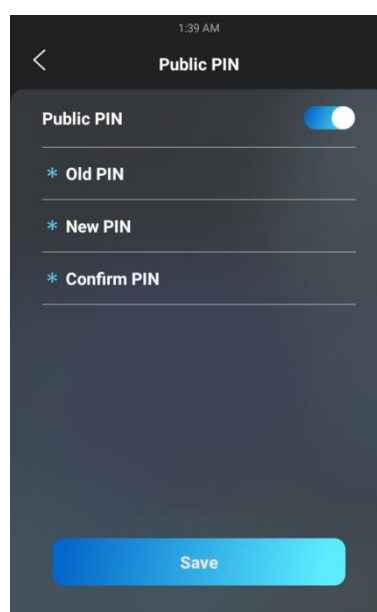
Note:

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

Parameter Set-up:

- **Enabled:** tick the checkbox to enable the Public PIN code application.
- **PIN Code:** set the PIN code with digit limit ranging from "4-8".

To configure it on the web device, go to **Security > Public PIN**.



The screenshot shows a mobile application interface for configuring the Public PIN. It features a title "Public PIN" at the top. Below the title, there is a toggle switch for "Public PIN" which is turned on. Below the toggle, there are three input fields labeled "* Old PIN", "* New PIN", and "* Confirm PIN". At the bottom of the screen, there is a blue "Save" button.

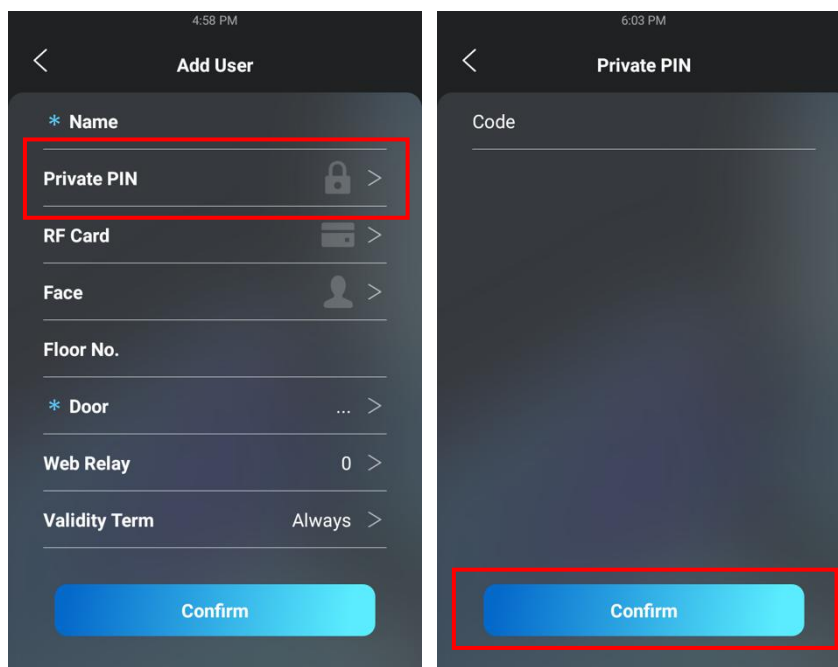


Note:

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

16.2.2. Configure Private PIN Code on the Device

You can configure door access by Private PIN code on the device by entering the user's name and the PIN code for the door access. To configure the language display on the device **Setting > User > Add** interface.



16.2.3. Configure Private PIN Code on the Web Interface

On the web interface, 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. In addition, you can set the limit for the total number of valid PIN code door access. To configure the configuration on the web **Access Control > User** interface.

Access Control > User

User

All User ID/Name Search + Add

<input type="checkbox"/>	Index	Source	UserID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/>	1	Cloud	D000000395	Building SuperVisor	1029	2191341329	All	0	1800-1	
<input type="checkbox"/>	2	Cloud	304126992	Thad A		2462330641	1	0	1803-1	
<input type="checkbox"/>	3	Cloud	D000000394	UPS	1028	0002995331	All	0	1805-1	
<input type="checkbox"/>	4	Cloud	304132699	Apartment 1 Owner			1	0	1018-1	
<input type="checkbox"/>	5	Cloud	304136224	Office Manager			9	0	1018-1	
<input type="checkbox"/>	6	Cloud	304132709	Apartment 2 Owner			1	0	1018-1	

Delete Delete All Prev 1/1 Next 1 Go

Private PIN

Code

Select door access Schedule for Private PIN Code door access:

Access Setting

Allow To Open RelayA RelayB RelayC

Web Relay

Building

Floor No.

Room

2 items Unselected Schedules

1002:Never

1:Test

1 item Selected Schedules

1001:Always

Parameter Set-up:

- **Allow To Open Relay:** select the relay for the door unlock for the user.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Building:** enter the build name.

- **Floor NO:** enter the resident's floor number.
- **Schedule:** select from the created door access schedule on the right box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

**Note:**

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

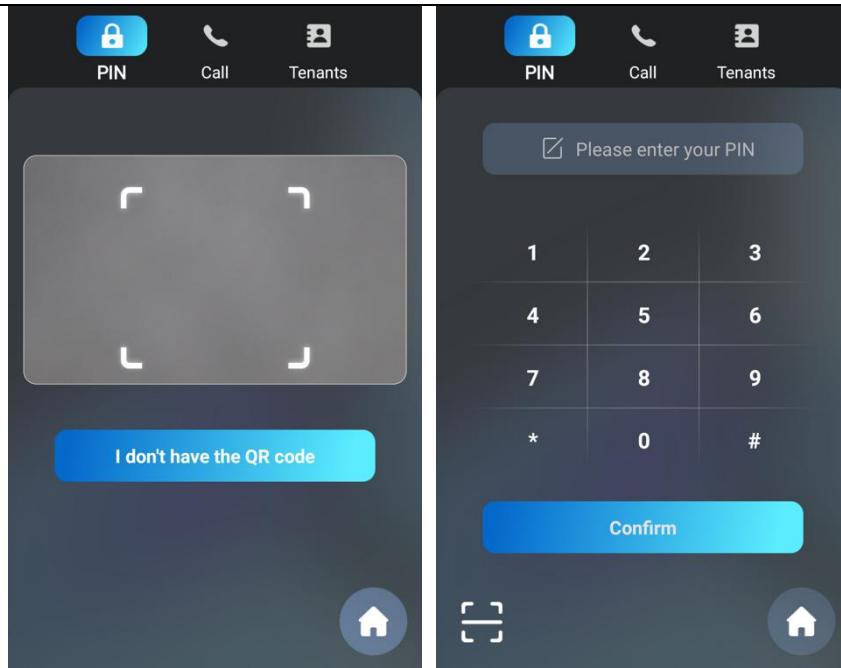
16.2.4. Configure Private PIN Access Mode

X915 series 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.

Private PIN	
Display Mode	Keyboard ▼
PIN Mode	PIN ▼

Parameter Set-up:

- **Display Mode:** select access mode between "QR Code" and "Keyboard".



Note:

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

To configure the Display Mode and PIN Mode:

Private PIN	
Display Mode	Keyboard
PIN Mode	PIN

Parameter Set-up:

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

**Note:**

- **APT+PIN** can only be applicable when the device is added to the Akuvox SmartPlus.

16.3. Configure RF Card for Door Unlock

16.3.1. Configure RF Card on the Web Interface

To configure the configuration on the web **Access Control > User > RF Card** interface.

RF Card

Reader Status	<input type="text" value="Normal"/>	
Code	<input type="text"/>	<input type="button" value="Obtain"/>
<input type="button" value="Add"/>		

**Note:**

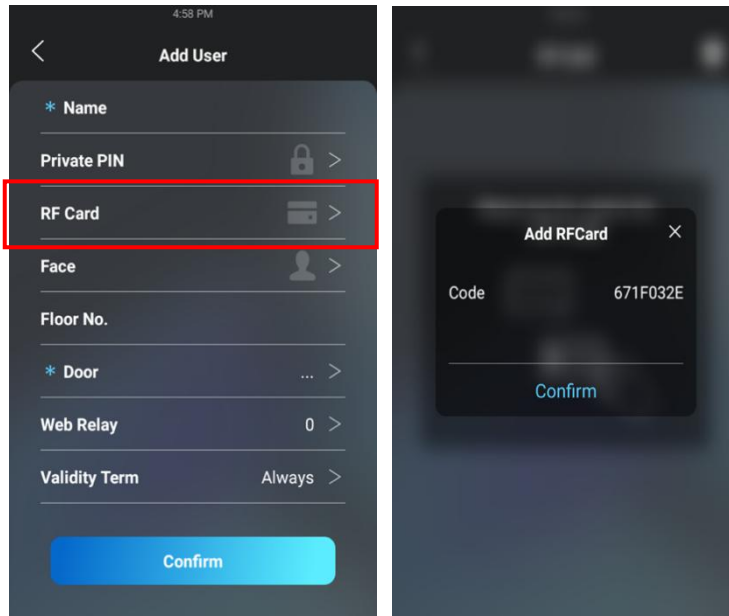
- Please refer to PIN code access schedule selection for the RF card user(s)-specific door access.

**Note:**

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

16.3.2. Configure RF Card on the device

You can configure the RF card directly on the device for the door access while setting up the time schedule for the validity of the RF card access along with the web relay that can be triggered with RF card etc. To configure the language display on the device **Setting > User > Add** interface.



16.3.3. 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.

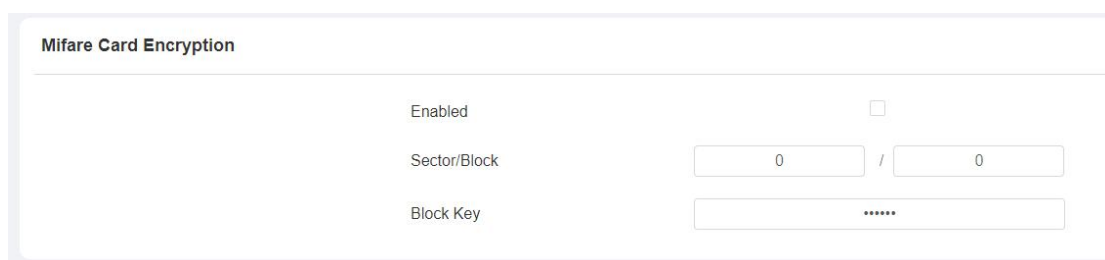
RFID	
IC Card Display Mode	8HN
ID Card Display Mode	8HN

Parameter Set-up:

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

16.4. Mifare card Encryption

X915 can read the encrypted Mifare card for greater security. To do so you can navigate to **Access Control > Card setting > Mifare Card Encryption**.



Mifare Card Encryption

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

Parameter Set-up:

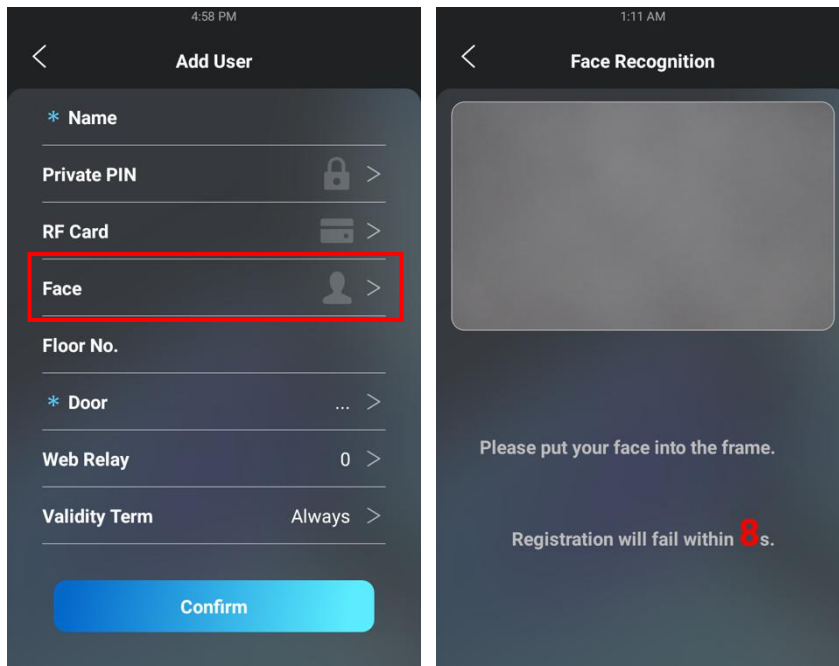
- **Enabled:** enable the Mifare/Defire Card Encryption.
- **Sector/Block:** enter the sector and block in which the card number is located in the Mifare/Defire Card. For example, the card number can be in sector 3 and block 3 in the card.
- **Block Key:** enter the block password for access.

16.5. Configure Facial Recognition for Door Unlock

16.5.1. Configure Facial Recognition on the Device

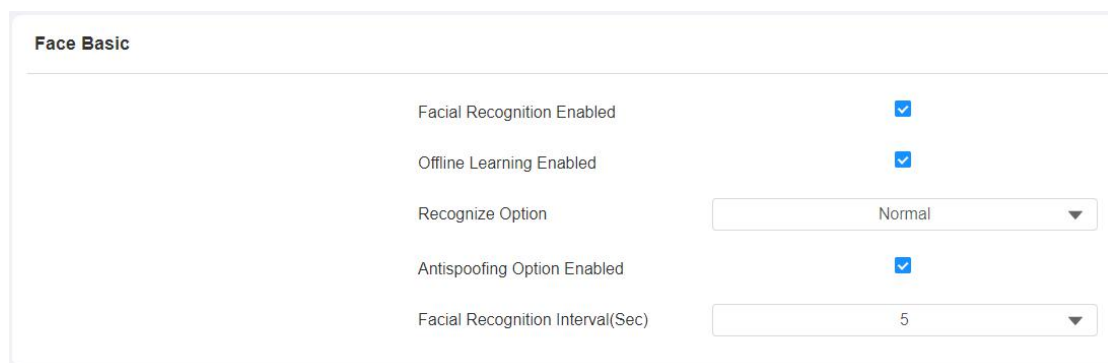
You can configure door access by facial recognition on the device by entering the user's name and registering your facial ID on the device for the door access. To configure the language display on the device **Setting >**

User > face interface.



16.5.2. Configure Facial Recognition on Web Interface

X915 series door phone allows 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. To configure the configuration on the web **Access Control > Face Setting** interface.



Parameter Set-up:

- **Face Recognition Enabled:** click on **Enable** to turn on the facial

recognition function. Facial recognition is enabled by default.

- **Offline Learning Enabled:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **Recognize Option:** 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.
- **Antispoofing Option Enabled:** 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(Sec):** select the time interval between every two facial-recognitions from 1-8 minutes. For example, if you select **"5"** then you have to wait for 5 min. before you are allowed to perform the facial recognition again.

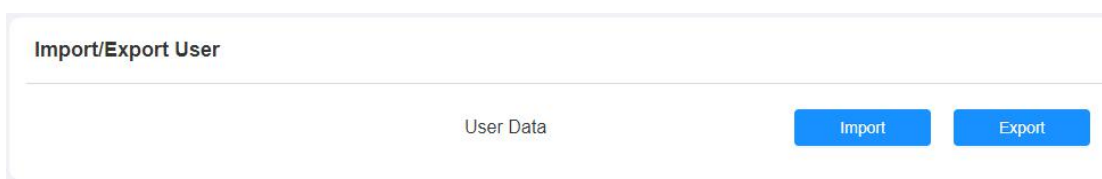
16.6.Edit the User-specific door access data

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

Index	Name	Private PIN	RF Card	Schedule ID	Times	Floor No.	Relay	Web Relay	Edit
1	Ryan			1,2	0	100	1	0	

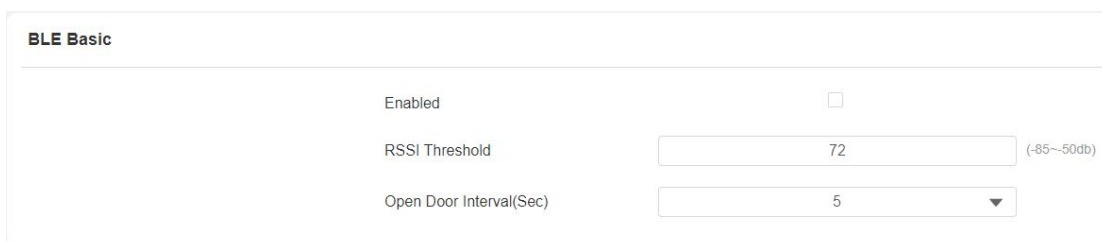
16.7.Import and Export User Data of Access Control

X915 series support User Data of access control to be shared among Akuvox X915 series door phones through import and export while you can also export the facial data out of the door phone and then import it to a third-party device. To configure the configuration on the web **Access Control > User > Import/Export User** interface.



16.8.Configure Bluetooth for Door Unlock

You can also gain the door access by mobile phone with Bluetooth which is used together with Akuvox SmartPlus. You can shake the mobile phone closer to the door phone for door access. To configure the configuration on the web **Access Control > BLE Basic** interface.



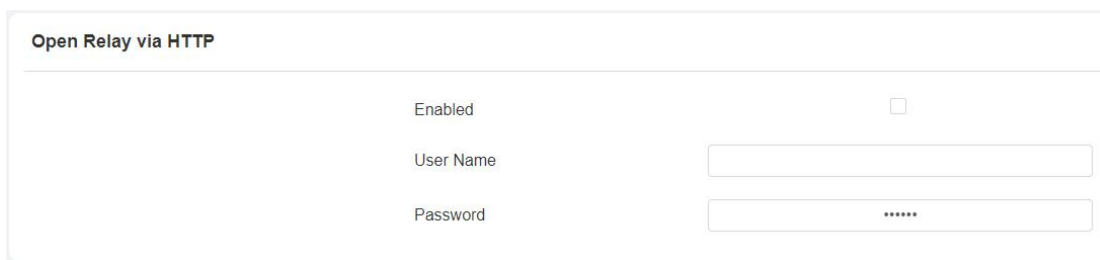
Parameter Set-up:

- **BLE Enable:** enable or disable the Bluetooth function. Bluetooth is turned off by default.
- **RSSI Threshold:** select the signal receiving strength from -85~-50db in absolute terms, The higher value it is, the greater strength it has. The default value is 72db in absolute terms.

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

16.9. 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 type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="password" value="*****"/>

Parameter Set-up:

- **Enable:** enable the HTTP command to 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.

16.10. Unlock by QR Code

QR code is another option for door access. If you want to apply for QR code access, you need to enable the QR code function. To configure the configuration on the web **Access Control > Relay > Open Relay via QR Code** interface.

Open Relay Via QR Code

Enabled

**Note:**

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

16.11. 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.

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"/> HTTP <input type="checkbox"/> TFTP
HTTP URL	<input type="text"/>
Action Delay	<input type="text" value="0"/> (0~300Sec)
Execute Relay	RelayA ▼
Door Status	DoorA: High

Parameter Set-up:

- **Trigger Electrical Level:** select the trigger electrical level options between “High” and “Low” according to the actual operation on the exit button.
- **Action to Execute:** select the method to carry out the action among 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 the input signal.

16.12. Configure Reception Tab for Door Unlock

On the device home screen, X915 series door phone provides residents and visitors quick door access by pressing the **Reception** tab at the bottom of the home screen. To configure the configuration on the web **Device > Key/Display > Speed Dial Action In Building Theme** interface.

Speed Dial Action In Building Theme

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

Parameter Set-up:

- **Open Relay:** select the relay(s) to be triggered by pressing the Reception Icon.
- **Action To Execute:** tick the check box to enable 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>

16.13. Unlock by DTMF code

DTMF codes can be configured on the door phone web interface and set up identical DTMF code on the corresponding intercom devices such as indoor monitor, which allows residents to enter the DTMF code on the soft keypad or press DTMF code attached unlock tab on the screen to unlock the door for visitors etc., during a call. To configure the configuration on the web **Account > Advanced > DTMF** interface.

DTMF

Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96-127)

Parameter Set-up:

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

**Note:**

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

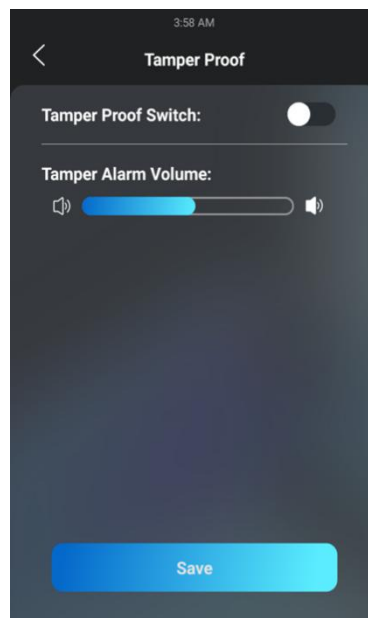
17. Security

17.1. Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the tamper 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.

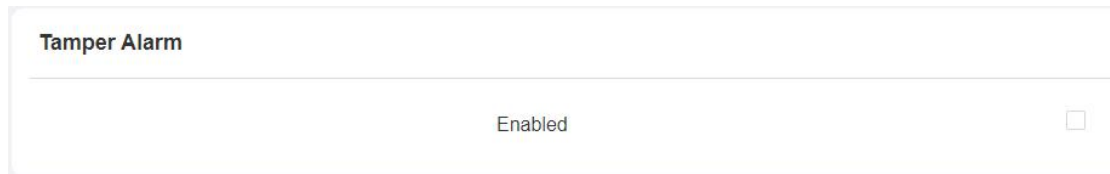
17.1.1. Configure Tamper Alarm on the Device

Tamper alarm can be conveniently set up and adjusted directly on the door phone. You can set up the gravity value as well as the adjusting the gravity sensor sensitivity according to your actual need. To configure the tamper alarm go to **Setting > Security > Tamper Proof**.



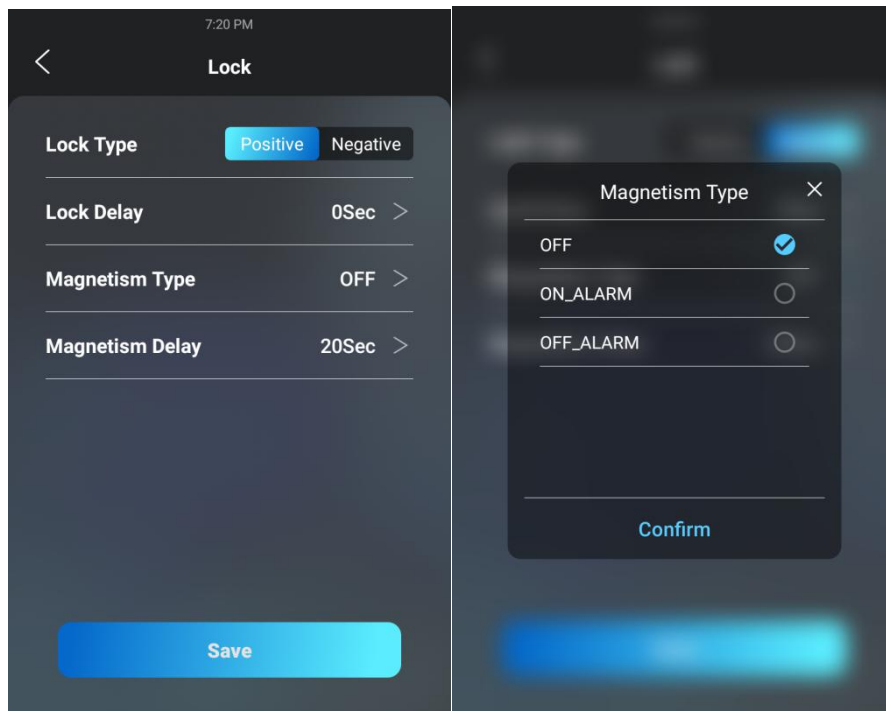
17.1.2. Configure Tamper Alarm on the Web Interface

You can also 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 **Security > Basic > Tamper Alarm** interface.



17.2. Lock Security

X915 can be connected with third-party door locks and door sensors to ensure lock security. When the door sensor detects the door is not closed or is left ajar, it will immediately trigger the alarm for notification. On the device, go to **Security > Lock** for the setting.



Parameter Set-up:

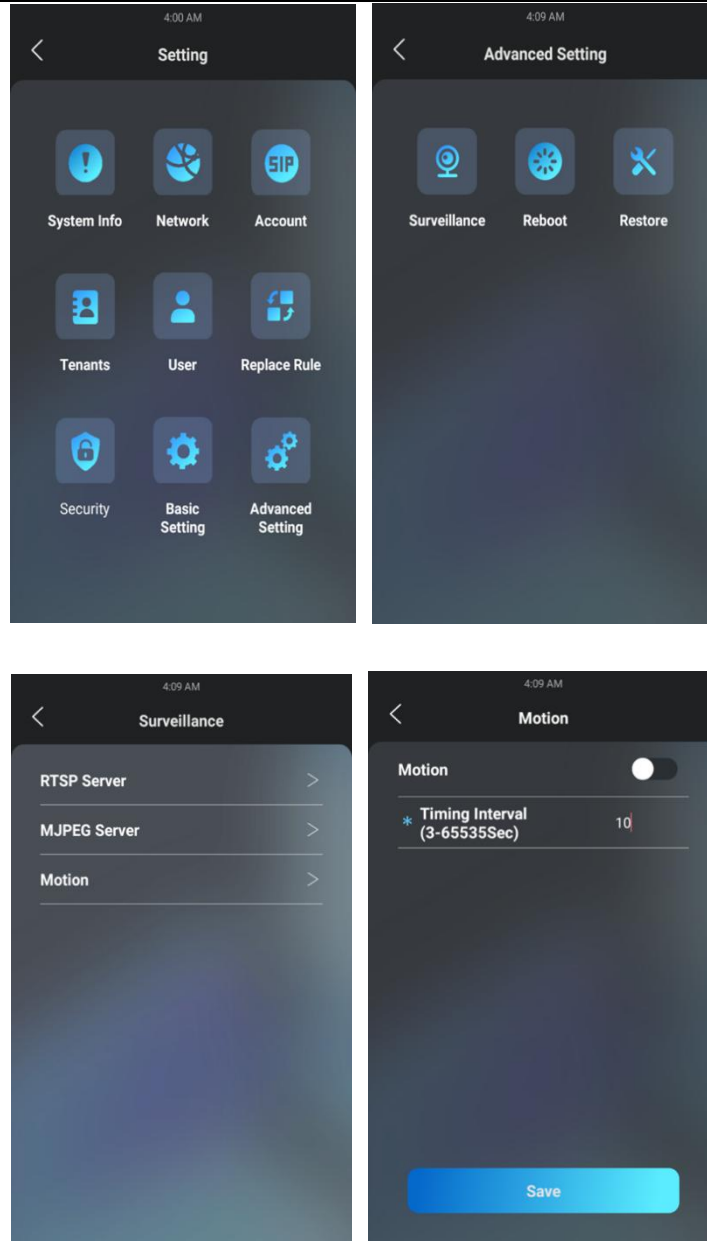
- **Lock Type:** select "**Positive**" for the lock that unlocks when the power is on and select "**Negative**" for the lock that unlocks when the power is off.
- **Lock Delay:** select door unlock delay time after you are granted the door access. The delay time range is from "0-10" seconds.
- **Magnetism Type:** select "**OFF**" if you want to disable the door sensor and alarm. To set the alarm trigger type, you must select "**ON-ALARM**" and "**OFF_ALARM**" according to the type of lock you applied. Select "**ON_ALARM**" for a positive lock, while select "**OFF_ALARM**" alarm for a negative lock.
- **Magnetism Type:** select the alarm delay time after its being triggered. The delay range is from "10-120" seconds.

17.3. 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.

17.3.1. Configure Motion Detection on the Device

You can turn on the motion detection and set up the motion detection interval on the device **Advanced Setting > Surveillance > Motion** screen.



Parameter Set-up:

- **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 the 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”.

17.3.2. Configure Motion Detection on the Web Interface

On the device web interface, you can not only configure the time interval but also the motion detection sensitivity and notification type when the motion detection action is triggered. To configure the configuration on the web **Surveillance > Motion > Motion Detection Options** interface.

Motion Detection Options

Suspicious Moving Object Detection	<input type="checkbox"/>	
Notification	FTP	
Time Interval	10	(3-65535Sec)
Detection Accuracy	20	(0-100)

Parameter Set-up:

- **Suspicious Moving Object Detection:** tick the check box to enable the motion detection function.
- **Notification:** select the notification type between FTP and Email. If you select “FTP”, then the notification will be sent in FTP to a designated serve while if you select “Email” then the notification will be sent in the form of emails when motion detection action is triggered.
- **Time Interval:** set the time interval in the same way as you do on the device.
- **Detection Accuracy:** set the detection accuracy for the detection sensitivity. The small value is, the greater sensitivity. the default detection accuracy value is “20”.

17.4. Security Notification Setting

17.4.1. 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.

Email Notification

Sender's Email Address	<input type="text"/>
Email Send 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 address:** enter the sender's email address from which the email notification will be sent out.
- **Email Send Name:** enter the name of the email sender.
- **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 with sender's email address.
- **SMTP Password:** configure the password of SMTP service, which is same with sender's email address.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the contents of emails according to your need.

17.4.2. 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

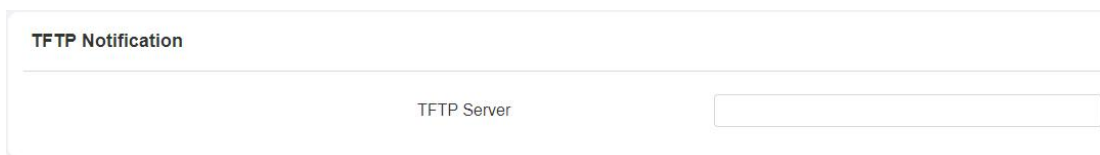
FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password" value="*****"/>
FTP Path	<input type="text"/>

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.

17.4.3. TFTP Notification Setting

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



TFTP Notification

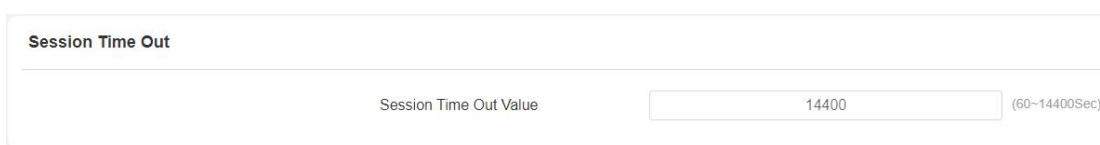
TFTP Server

Parameter set-up:

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

17.5. Web Interface Automatic Log-out

You can set up the web interface automatic log-out 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 web **Security > Basic > Session Time Out** interface.



Session Time Out

Session Time Out Value (60-14400Sec)

17.6. Action URL

X915 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**.



Note

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

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"/>
RelayC Triggered	<input type="text"/>
RelayA Closed	<input type="text"/>
RelayB Closed	<input type="text"/>
RelayC 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"/>

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"/>

17.7. Client Certificate Setting

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

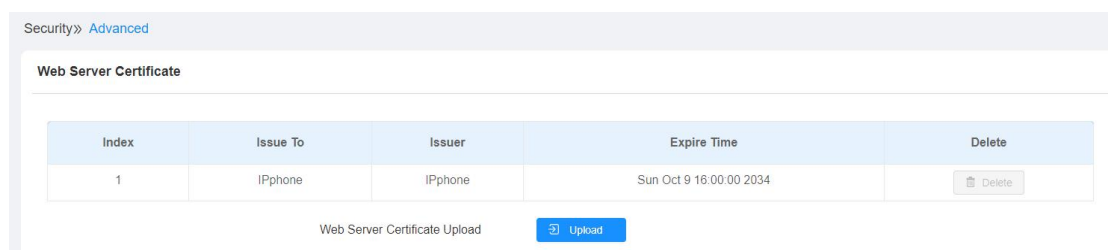
Web Server Certificate: it is the certificate that sends to the client for authentication when the client requires an SSL connection with Akuvox door phone. Currently, the format of certificate that can be accepted by Akuvox

door phone is *.PEM file.

Client Certificate: when Akuvox door phone 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 the client certificate list.

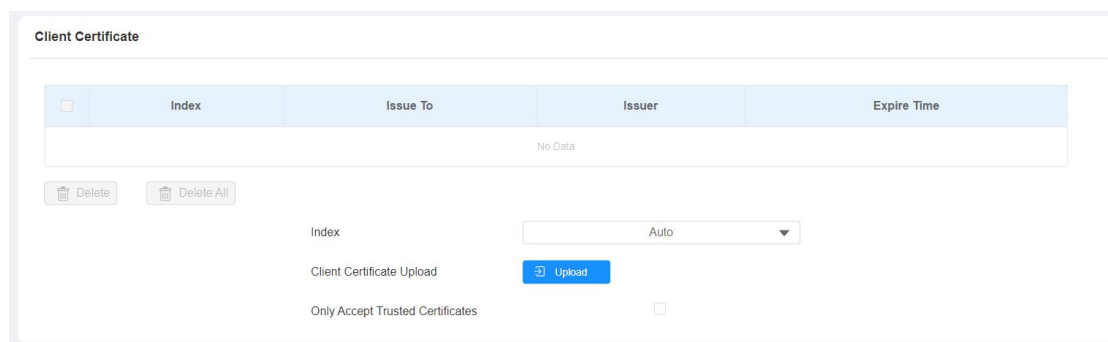
17.7.1. Web Server Certificate

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



17.7.2. Client Certificate

To upload and configure client certificate on the same page.



Parameter Set-up:

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

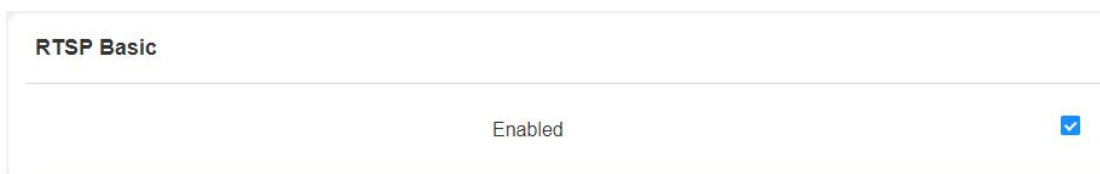
18. Monitor and Image

18.1. RTSP Stream Monitoring

X915 series door phone support RTSP stream that allows intercom devices such as 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.

18.1.1. RTSP Basic Setting

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

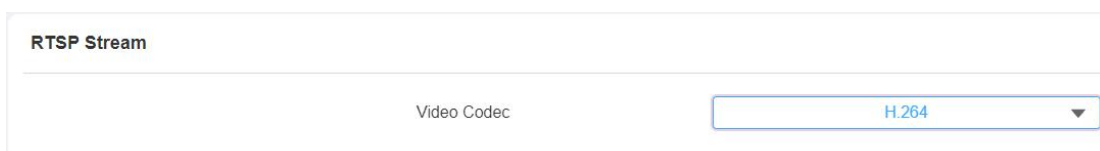


RTSP Basic

Enabled

18.1.2. 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 > RTSP Stream** interface.



RTSP Stream

Video Codec

To configure the parameters for H.264 codec on the web **Surveillance >**

RTSP > H.264 Video Parameters interface.

H.264 Video Parameters

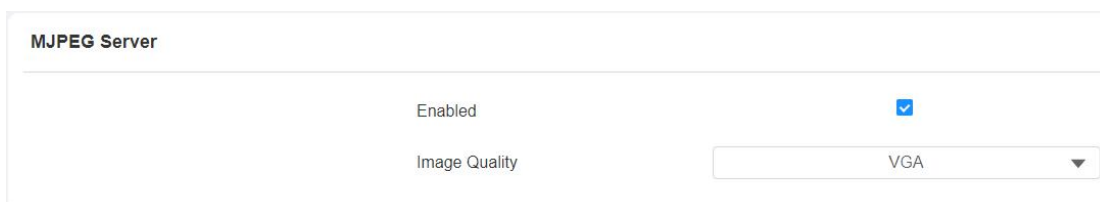
Video Resolution	<input type="text" value="720P"/>
Video Framerate	<input type="text" value="25fps"/>
Video Bitrate	<input type="text" value="1024kbps"/>
2nd Video Resolution	<input type="text" value="VGA"/>
2nd Video Framerate	<input type="text" value="25fps"/>
2nd Video Bitrate	<input type="text" value="512kbps"/>

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 on the indoor monitor if the resolution is set higher than "720P".
- **Video Framerate:** "25fps" is the video frame rate by default.
- **Video Bitrate:** select video bitrate among six options: "128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs" according to your network environment. The default video bitrate is "2048 kpbs".
- **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.

18.2.MJPEG Image Capturing

X915 series allows 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.



MJPEG Server

Enabled

Image Quality VGA

Parameter Set-up:

- **Enabled:** tick the check box to 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, you can enter "http://192.168.1.104:8080/picture.jpg" on the web browser.

18.3.ONVIF

Real-time video from the X915 series 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.

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

Parameter Set-up:

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

18.4.Live Stream

If you want to check the real-time video from the X915 series 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.

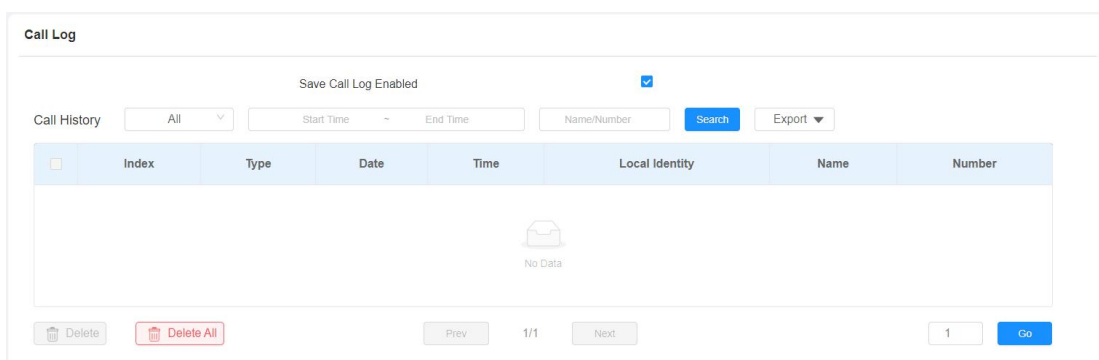
Surveillance» [Live Stream](#)



19. Logs

19.1. 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 **Intercom > Call Log** interface.



Parameter Set-up:

- **Save Call Log Enabled:** tick the check box to 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.

19.2. 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 **Access Control >**

Door log interface.

Door Log

Save Door Log Enabled

All Start Time ~ End Time Name/Code Search Export

Index	Name	Private PIN	RF Card	Type	Date	Time	Status
No Data							

Delete Delete All Prev 1/1 Next 1 Go

Parameter Set-up:

- **Save Door Log Enabled:** tick the check box to enable the door log function.
- **Status:** select between **"Success"** and **"Failed"** options to search for successful door accesses or Failed door accesses.
- **Start Time ~ End 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.

20. Debug

20.1. 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 **Upgrade > Diagnose > System Log** interface.

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

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, the more complete the log is.
- **Export Log:** click the **Export** tab to export the temporary debug log file to a local PC.
- **Export Debug Log:** click the **Export** tab to export debug log file to a local PC.
- **Remote System Log:** select "Enable" or "Disable" if you want to enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the device log. And the remote server address will be provided by Akuvox technical support.

20.2.PCAP for Debugging

PCAP in X915 series door phone 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 **Upgrade > Diagnose > PCAP** interface properly before using it.

The screenshot shows the PCAP configuration interface. At the top, it says 'PCAP'. Below that, there is a 'Specific Port' label followed by an empty text input field and a '(1-65535)' hint. Underneath, there is a 'PCAP' label and 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.

20.3.Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purpose. On the web, Navigate to **Upgrade > Diagnosis > Remote Debug Server**.

Remote Debug Server

Server	Enabled
Connect Status	Connected
IP	47.241.17.214

Parameter Set-up:

- **Server:** disable or enable the remote debug server.
- **Connect Status:** displays the remote debug server connection status.
- **IP:** enter the remote debug server IP address. Please ask Akuvox technical team for the server IP address.




**Note:**

You are required to send the door phone's MAC address to the Akuvox technical team.

21. Firmware Upgrade

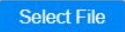

Firmware of different versions for X915 series door phone can be upgraded on the device web **Upgrade > Basic** interface.



Basic

Firmware Version	915.30.101.71
Hardware Version	915.1.0.0
Upgrade	 Upgrade
Reset To Factory Setting	 Reset
Reboot	 Reboot

Upgrade ×

(Format: .zip)

Not selected any files  

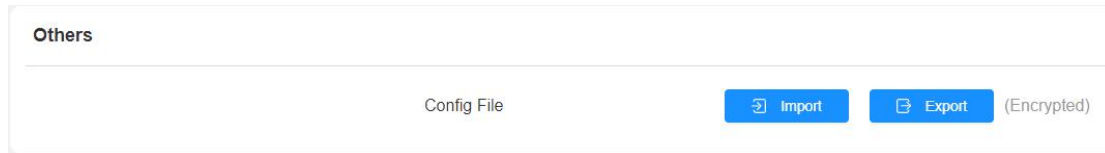


Note:

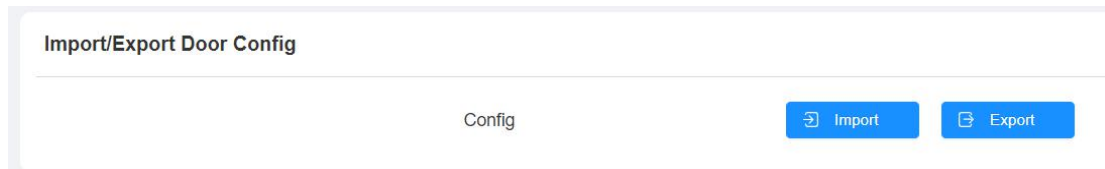
- Firmware files should be .zip format for upgrading.

22. Backup

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



If you want import or export non-encrypted configuration files, navigate to **Setting > Door > Import/Export Door Config**.

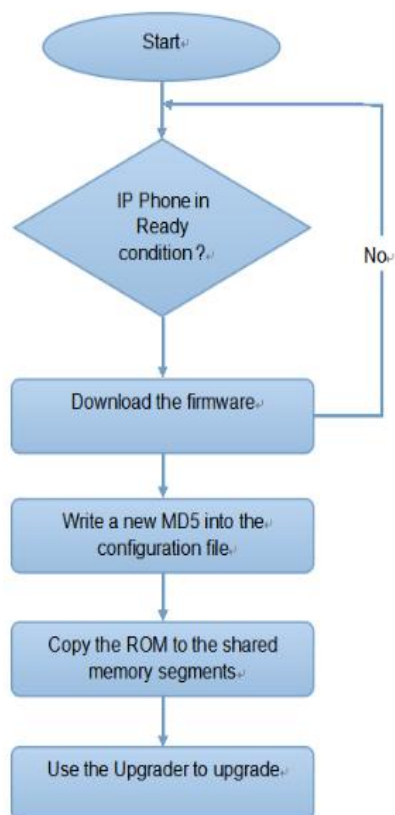


23. Auto-provisioning via Configuration File

Configurations and upgrading on X915 series 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.

23.1. 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.



23.2. 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 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: r000000000915.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 the 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.

23.3. AutoP Schedule

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

To configure the configuration on the web **Upgrade > Advanced > Automatic Autop** interface.

Automatic Autop

Mode	<input style="width: 95%;" type="text" value="Power On"/>
Schedule	<input style="width: 95%;" type="text" value="Sunday"/>
	<input style="width: 95%;" type="text" value="22"/> (0-23Hour)
	<input style="width: 95%;" type="text" value="0"/> (0-59Min)
Clear MD5	<input style="width: 95%; background-color: #007bff; color: white;" type="button" value="Clear"/>
Export Autop Template	<input style="width: 95%; background-color: #007bff; color: white;" 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.

23.4.PNP Configuration

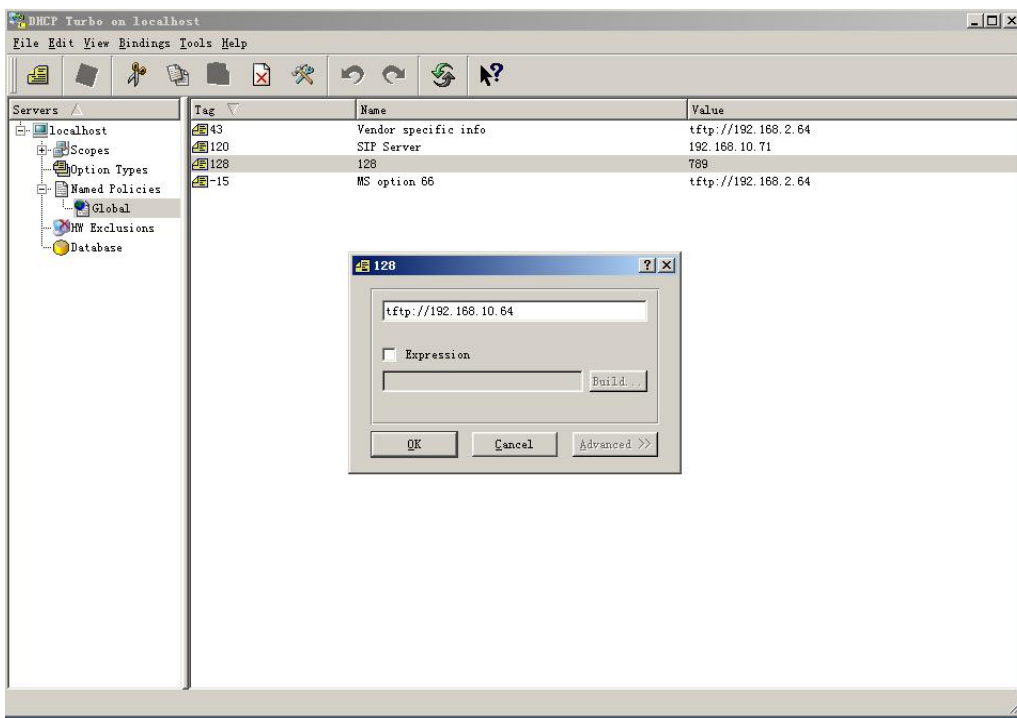
Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. To configure the configuration on the web **Upgrade > Advanced > PNP Option** interface.

PNP Option

PNP Config Enabled

23.5.DHCP Provisioning Configuration

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



Note:

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

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 the corresponding URL so that 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 update 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 update server URL in it.

**Note:**

- The general configuration file for the in-batch provisioning is with the format "r000000000xx.cfg" taking X915 as an example "r000000000915.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."

23.6. 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 perform the auto provisioning on a specific timing according to 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 on **Upgrade > Advanced > Automatic Autop** , and setup Autop server on **Upgrade > Advanced > Manual Autop** interface.

Automatic Autop

Mode Power On ▾

Schedule Sunday ▾

Hour(0~23)
 Min(0~59)

Clear MD5 [Submit](#)

Export Autop Template
[Export](#)

Manual Autop

URL

User Name

Password


Common AES Key

AES Key(MAC)

[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 the 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.

24. Integration with Third Party Device

24.1. Integration via Wiegand

If you want to integrate the X915 series door phone with the 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.

24.2. 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 **Security > HTTP API** interface for the integration.

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.

24.3. Power Output Control

X915 can serve as a power supply for the external relays. Path: Setting > Door > 12V Power Output.

12V Power Output	
12V Power Output	Disabled
Time Out (Sec)	3

Parameter Set-up:

- **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.

24.4. Mobile Community

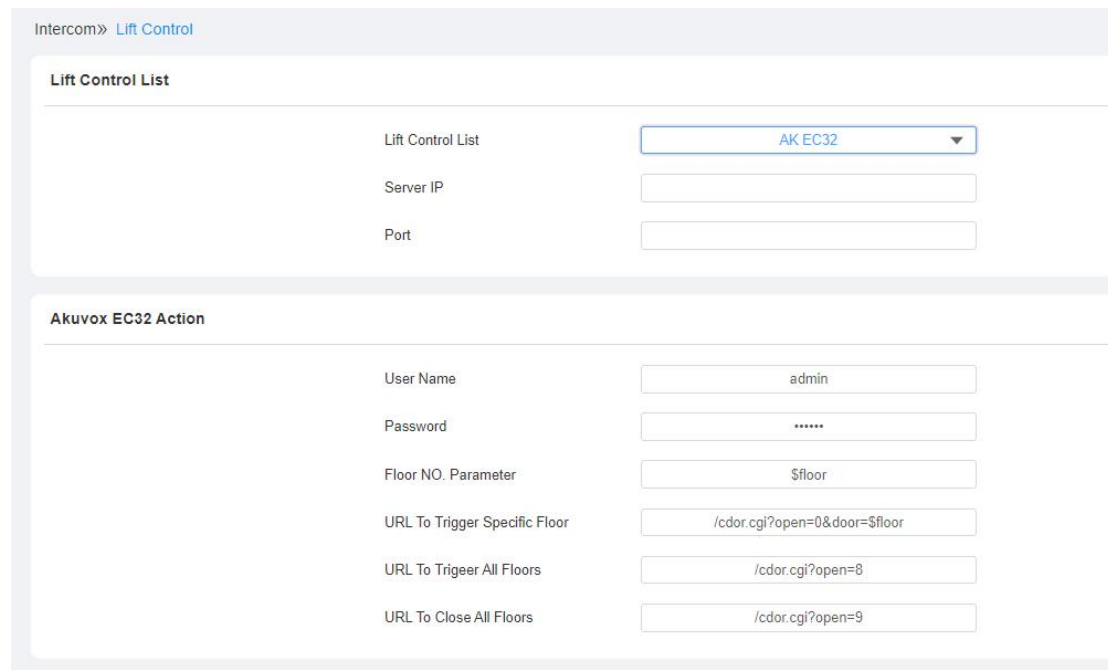
You can connect the door phone to the third party QR code server for QR code verification. When you access the door using a QR code, the QR code will be sent to the QR code server for verification before granting you access permission. This feature is applied to the devices not deployed in the SmartPlus platform for the QR code door access. You can navigate to **Access Control > Relay > Mobile Community**.

Mobile Community

Enabled	<input checked="" type="checkbox"/>
HTTP URL	<input type="text"/>
Device ID	<input type="text"/>

25. Lift Control

X915 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 **Intercom > Lift Control**.



Intercom > Lift Control

Lift Control List

Lift Control List	AK EC32
Server IP	
Port	

Akuvox EC32 Action

User Name	admin
Password	*****
Floor NO. Parameter	\$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=\$floor
URL To Trigeer All Floors	/cdor.cgi?open=8
URL To Close All Floors	/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.
- **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

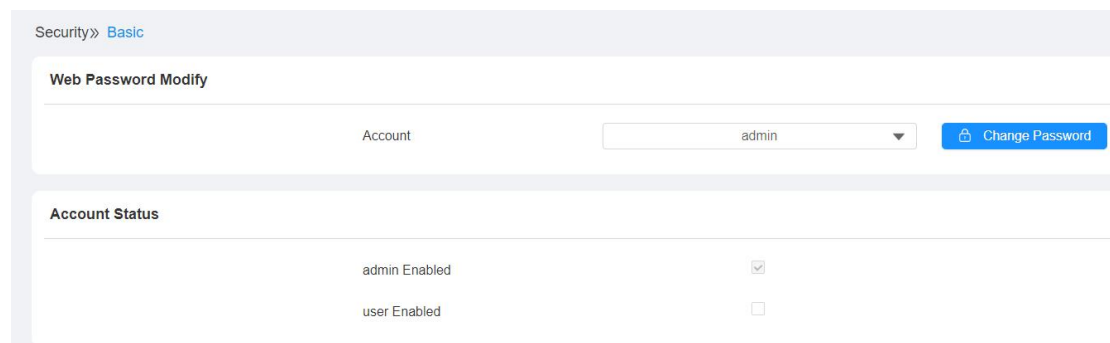
parameter string if needed.

- **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, meaning all the buttons that are triggered for the corresponding floors will become invalid.

26. Password Modification

26.1. 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.



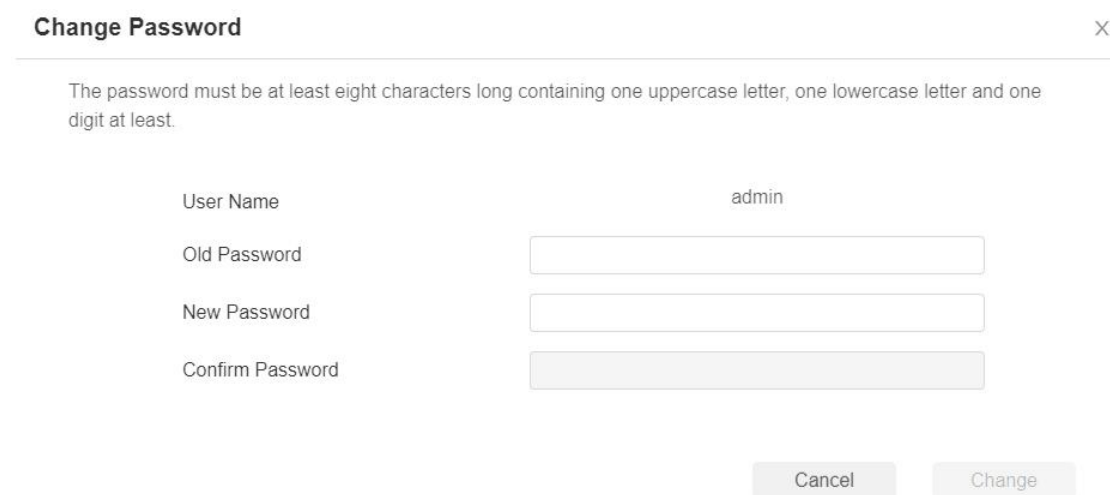
Security» Basic

Web Password Modify

Account [Change Password](#)

Account Status

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



Change Password X

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

User Name

Old Password

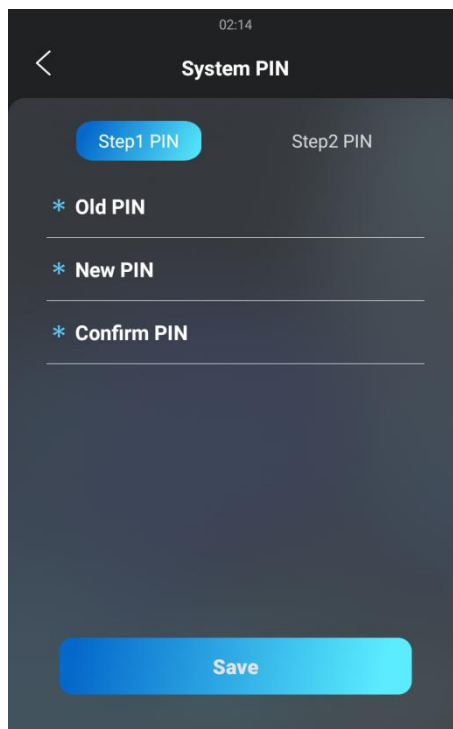
New Password

Confirm Password

26.2. Modifying System Password

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

To set the system pin code on the device, go to **Security > System PIN**, then select **Step1 PIN**.



Parameter Set-up:

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

To set up system PIN on the web interface, navigate to **Security > Basic > System PIN**.

System PIN	
Step1 PIN	<input type="text" value="9999"/>
Step2 PIN	<input type="text" value="3888"/>

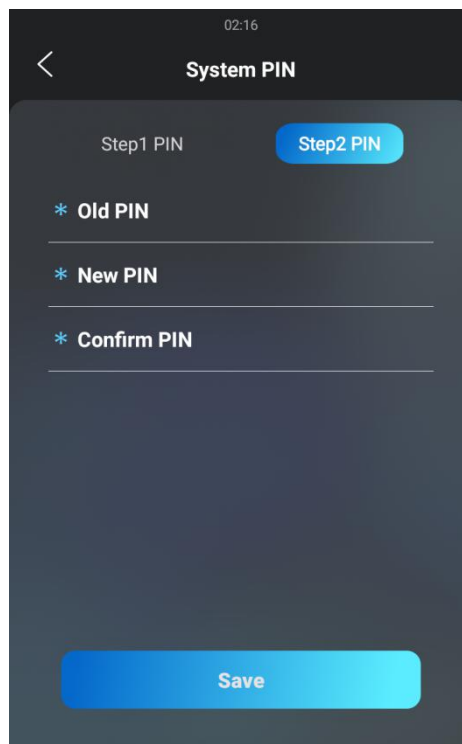
**Note:**

- The default system password is "9999".

26.3. Modifying Setting Password

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

To set the system pin code on the device, go to **Security > System PIN**, then select **Step2 PIN**.



To set up Setting password on the web interface, navigate to **Security > Basic > System PIN**.

System PIN

Step1 PIN	<input type="text" value="9999"/>
Step2 PIN	<input type="text" value="3888"/>



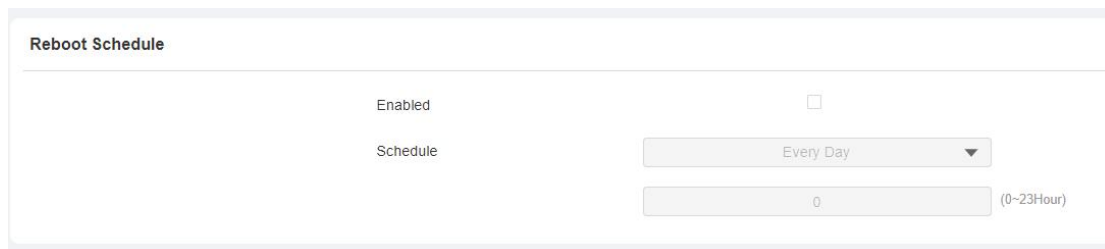
Note:

- The default system password is "3888".

27. System Reboot&Reset

27.1.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.

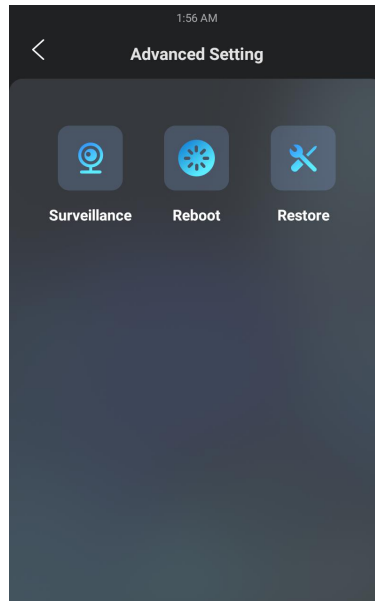


The screenshot shows a web interface titled "Reboot Schedule". It contains two main settings: "Enabled" with a checkbox that is currently unchecked, and "Schedule" with a dropdown menu set to "Every Day" and a time input field set to "0". The time input field has a range of "(0~23Hour)" indicated to its right.

Parameter Set-up:

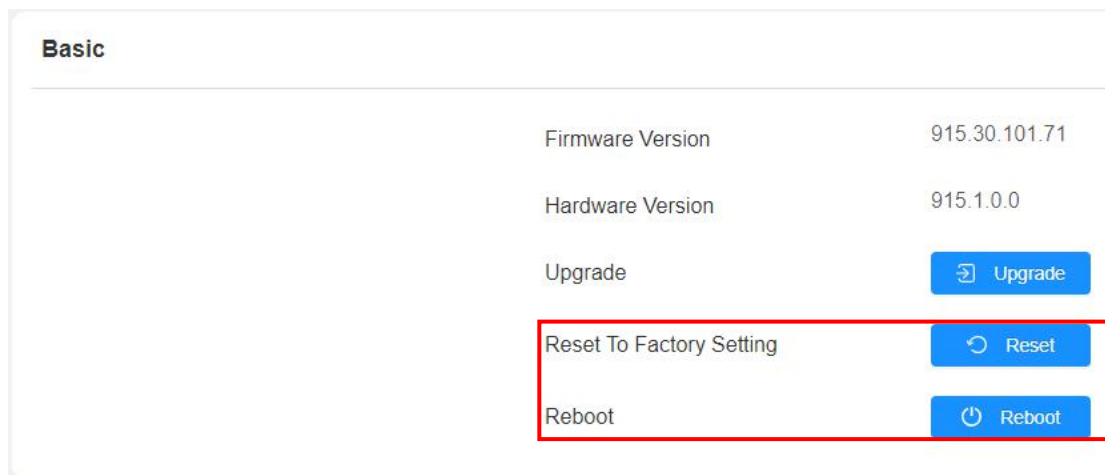
- **Enabled:** enable the reboot mode, or choose **Schedule** mode for setting the reboot time regularly.
- **Schedule:** if you choose schedule mode, also need to set up the reboot schedule. From Monday to Sunday and 00: 00 to 24: 00.

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

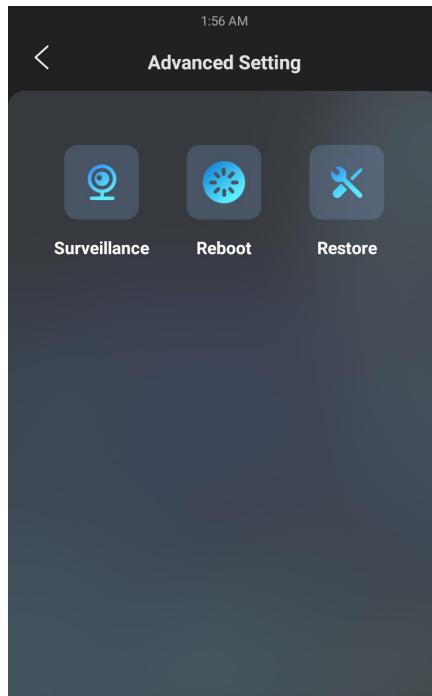


27.2.Reset

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



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



28. 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

WG: Wiegand

29. FAQ

Q1: How to obtain IP address of R2X

A1: ✓ For devices with a single button - E21/ R20/ R23/ R26:

While E21/ R20/ R23/ R26 power up normally, hold the call button for 5 seconds after the statue LED turns blue and it will enter IP announcement mode. In announcement mode, the IP address will be announced repeatedly. Press call button again to quit the announcement mode.

✓ For devices with multiple numeric keyboard - R27:

While R27 power up normally, press "*2396#" to enter the home screen and press "1" to go to system Information screen to check the IP address.

✓ For devices with touch screen - X915:

While X915 power up normally, in the dial interface, press "9999", "Dial key", "3888" and "OK" to enter the system setting screen. Go to info screen to check the IP address.

✓ Common method:

Using Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: Do Akuvox devices support opus codec?

A2: For now, only Akuvox Android video IP phone R48G can support Opus audio codec.

Q3: What is the supported temperature range for akuvox doorphone?

A3: R20/E21/R26/R23/Standard R27/Standard X915 -- 14° to 112°F (-10° to 45°C)

R27/X915 with heating supporting --- 40 degrees

R28 -- (-40°C~55°C)

Indoorphone -- 14° to 112°F (-10° to 45°C)

IPPhone -- 32°~104°F(0~40°C)

Q4: Do Akuvox devices support Modbus protocol?

A4: No.

Q5: Failure in importing the X915 face data to another X915 using the exported face data.

A5: Please confirm the following steps:

The import format is zip.

1. After you export, you need to unzip the .tgz folder, then make the unzipped folder into .zip again.

Q6: Which version of ONVIF do R20 and X915 support?

A6: Onvif 18.04 profiles

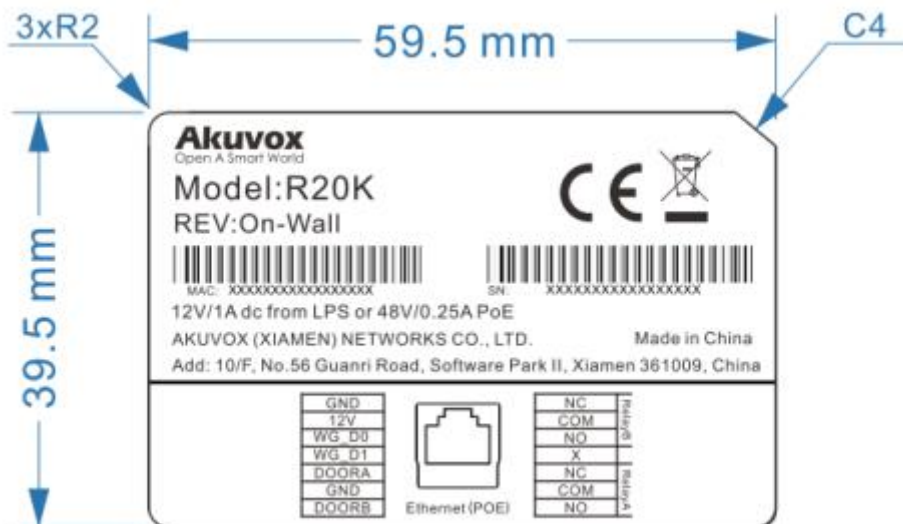
Q7: Do door phones support these card types? Prox, Legacy iClass, iClassSE, HID Mifare, HID DESFire, and HID SEOS

A7: Sorry, they are not supported. They need to be implemented via hardware modifications.

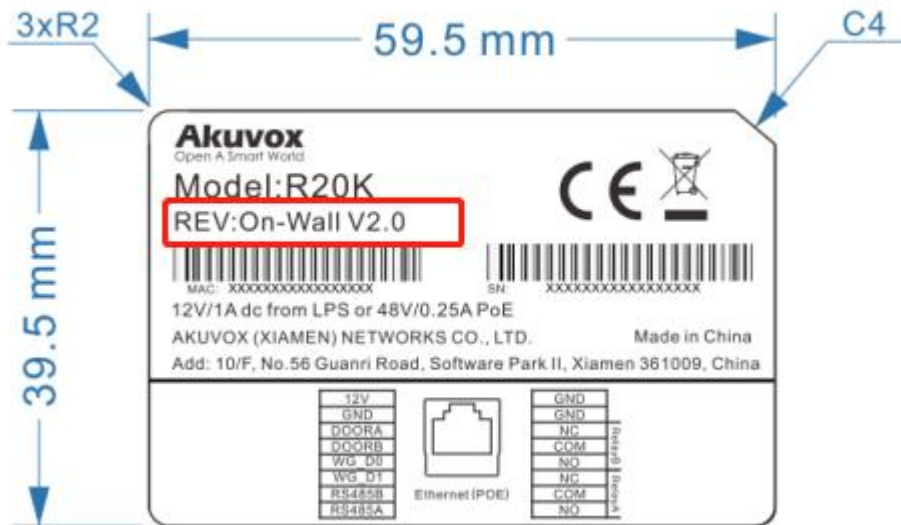
Q8: How to confirm whether my device is hardware version 1 or hardware version 2?

A8: 1. Label

- **Hardware version 1**



- **Hardware version 2**



- **Firmware Version**

The firmware is different between hardware version1 and hardware version 2.

Go to Web-Status -Firmware Version.

20.X.X.X is hardware version 1.

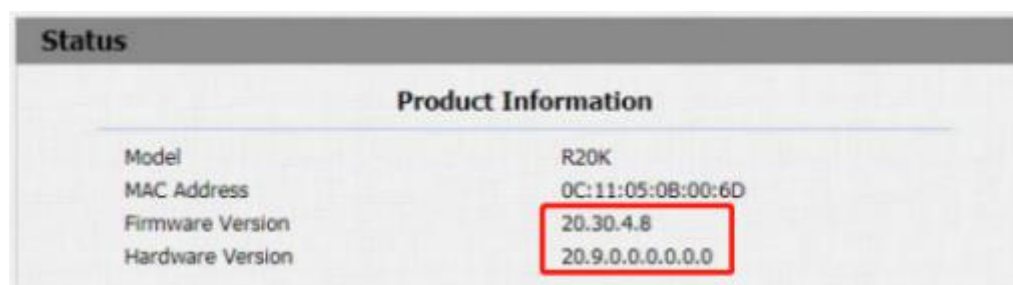
220.X.X.X is hardware version 2.

- **Hardware version**

The firmware is different between hardware version1 and hardware version 2.

Go to Web-Status -Firmware Version.

If the hardware version is 220.x, then the device is hardware version 2.



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.

