Akuvox
Open A Smart World

WWW.AKUVOX.COM

X915 SERIES
DOOR PHONE
Administrator Guide

Version: 1.0 | Date: Jan.2021

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 915.30.101.71 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 latest firmwares.

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.**

Tip:

- **Useful information for the quick and efficient use of the device.**

Related Documentation

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

http://wiki.akuvox.com

Table of Contents

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 controller and fire alarm detector, 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.

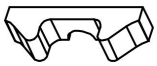
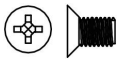
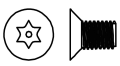
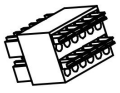
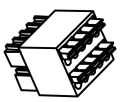
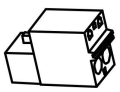
3. Model Specification

	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

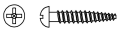
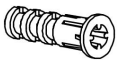
	X915S
Wall Mounting	√
Flush Mounting	√
Desk Mounting	X
Wall Mounting Dimension	350x130x41.6mm
Wall Mounting Dimension	350x130x53.9mm
POE+ Standy Power Consumption	5.263W
POE+ Full Load Power Consumption	18.796W
Power Adapter Standby Power Consumption	5.107W
Power Adapter Full Load Power Consumption	19.376W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

4. Installation

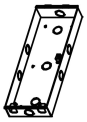
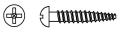
- **Mainframe Accessories**

No.	Accessories	Description	Quantity
1		X915	1
2		Rubber Plug(Small)	2
3		Rubber Plug(Medium)	2
4		Rubber Plug(Large)	2
5		Back Cover	1
6		Silicon Rubber Sealing Ring	1
7		M3x4 Screw	6
8		Torx Screw	2
9		Torx Wrench	1
10		Card Reader Touch Plate	1
11		Plate Removal Key	1
12		Rope	1
13		2 x 6 PIN Terminal Block	1
14		2 x 5 PIN Terminal Block	1
15		2 PIN Terminal Block	1
16		Pry barx	1

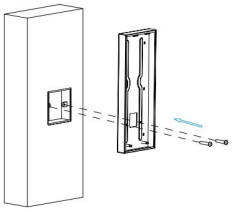
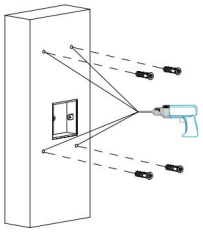
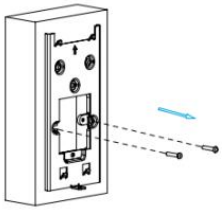
- **Wall-mounting Accessories (Please find in On-wall installation Kit box)：**

No.	Accessories	Description	Quantity
1		Wall-mounting box	1
2		M4 x 30 Screw	2
3		ST4 x 20 screw	4
4		Plastic Wall Anchor	4

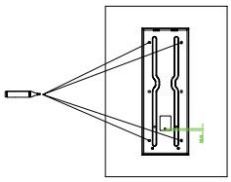
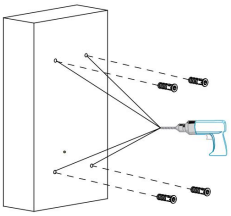
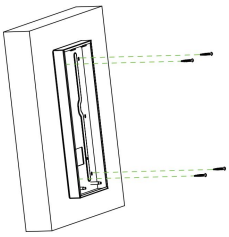
- **Flush Mounting Accessories (Please find in In-wall Installation Kit box)：**

No.	Accessories	Description	Quantity
1		Flush-mounting box	1
2		ST4 x 20 screw	4
3		Embedded box	4

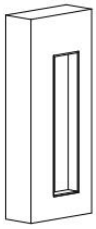
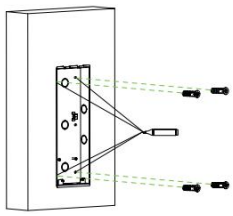
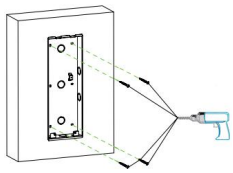
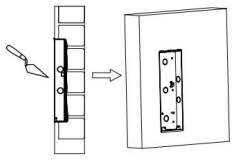
- **Wall-Mounting Bracket Installation with 86x86 mm Embedded Junction Box in the Wall.**

Steps	Installation Picture	Installation Description
1		Fix the wall-mounting box on to the embedded box (86) with two M4x30 Screws, mark the positions of the four holes of the wall mounting box at the hole center.
2		Take off the box and drill the four marked holes using a 5mm drill bit hand drill before inserting the plastic wall anchors into the drilled holes.
3		Place the wall mounting box closely against the wall while lining up its four holes with their corresponding drilled holes and then fix the wall mounting box on the wall by tightening the four ST4 x 20 screws to the plastic wall anchors.

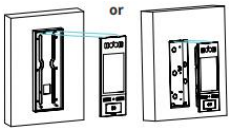
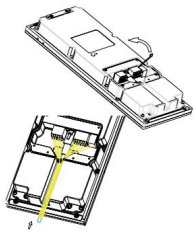
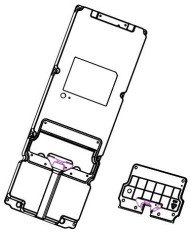
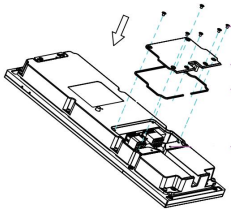
- **Wall-Mounting Bracket Installation without Embedded Junction Box in the Wall**

Steps	Installation Picture	Installation Description
1		According to the position of the wire on the wall, put the wall-mounting box closely on to the wall and mark the four positioning holes, while making sure that relative positions between the wall-mounting box and wiring hole are correct. Note: The wiring hole is recommended to be located at the green round hole in the drawing.
2		Drill the marked holes using a 5mm drill bit hand drill before inserting plastic wall anchors into the drilled holes.
3		Place the wall-mounting box closely against the wall while lining up its four holes with their corresponding drilled holes and then fix the wall-mounting box on the wall by tightening four ST x 20 screws to the plastic wall anchors.

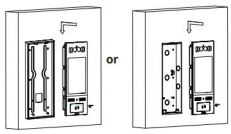
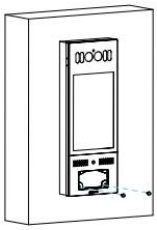
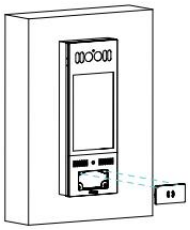
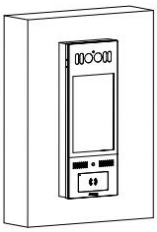
- **Flush-Mounting Installation**

Steps	Installation Picture	Installation Description
1		Cut out a square hole with the dimension (height*width*depth = 314*123*52mm).
2		Insert the flush-mounting box in to the hole and mark the the positions of the four holes of the flush-mounting box on the wall, then take off the box and drill the holes on the marked positions using 5mm drill bit hand drill before inserting the plastic anchors in to the drilled holes.
3		Break off the round knock-out wiring holes and lead the wires through the corresponding hole in to the flush-mounting box, then press the the flush-mounting box in to the square hole. The upper and lower folded edges of the flush-mounting box must fit snugly against the wall. Then fix the box using the four plastic wall anchors and the four ST4x20 screws.
4		Make sure that the flush-mounting box are well tightened and its upper and lower folded edges are fit snugly against the wall, fill in the gap between the wall and the flush-mounting box using cement or non-corrosive structural adhesive and wait until the cement is hardened.

- **Back Cover Installation**

Steps	Installation Picture	Installation Description
1		Hang the one end of the rope on to the square hanger on the wall-mounting/flush-mounting box then hang the other end of the rope on to the square hook on the device for the convenience of the later wire installation, etc.
2		Connect the wires to the terminal blocks as needed (for details, refer to "Device Wiring"), then insert the terminal blocks into the corresponding interface of the main board as indicated in the drawing according to the number of PIN. Note: The pry bar attached can be used to unplug the terminal blocks if needed.
3		Choose a suitable size rubber plug (small, large and medium) to hold down the wires, while tearing off the adhesive sticker on the selected rubber plug and stick it on to the X915 back cover and then tear off the adhesive sticker on the other rubber plug of the same size and stick it on to the back cover in the position as indicated in the drawing.
4		Press the X915 back cover silicone rubber sealing ring in to the corresponding groove as indicated by the arrow and then tighten the back cover using the six M3x4 screws to its corresponding holes.

- **Device Mounting**

Steps	Installation Picture	Installation Description
1		Take off the rope and hang the device on to the two square hangers on the wall-mounting/ flflush-mounting box. Stick the plate removal key in to the small hole on the upper left corner of the card reader touch plate to pull out the plate.
2		Drive the two M3x6 screw in to their corresponding holes.
3		Press the card reader touch plate in to the card reader opening.
4		Installation completed.

5. Introduction to Configuration Menu

- **Status:** this sections 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 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 Cloud is an all-in-one management system. Akuvox Cloud is the 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 cloud, please contact Akuvox technical support, and they will help you configure the related settings before using.

3. **SDMC mode**: SDMC (**SIP Device Management Controller**) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for the door access, intercom, monitoring, alarm etc.,. It is a convenient tool for property manager to manage , operate and maintain the community.

- **Tool selection**

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

1. **SDMC**: SDMC is suitable for the management of Akuvox devices 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.

6. Access the Device

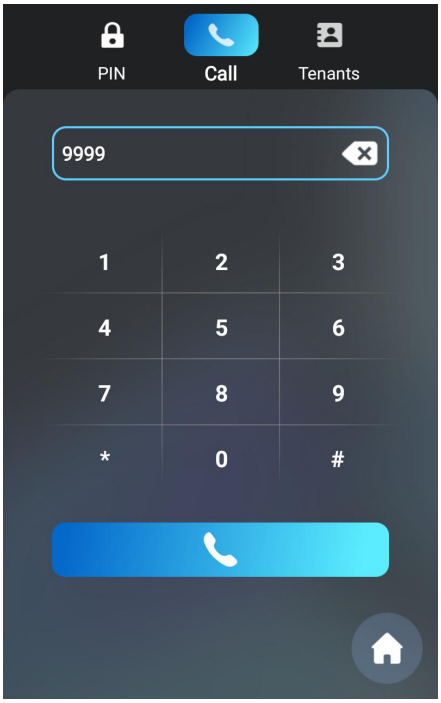
X915 series door phone system setting can be either accessed on the device directly or on the device web interface.

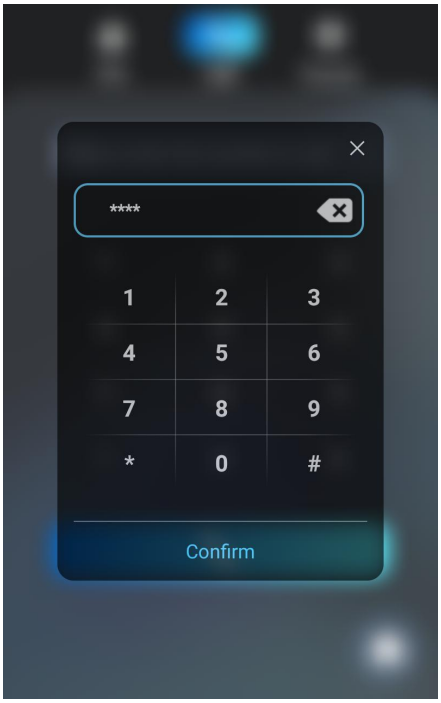
6.1. Access the Device Setting on the device

If you want to access the device setting in order to configure and adjust the parameters, you can do it directly on the device.

To access the device setting, you can do as follows:

1. Press **Dial** icon on the home screen.
2. Enter the first system code "**9999**" on the dial screen on the device and press dial icon
3. Enter the second system code "**3888**", and press on **Confirm** for the confirmation.
4. Press **System Info** icon on the **Setting** screen and press on **Network** on the **System Info** screen if you want to check for device IP address with which you can access the device setting on the web interface.



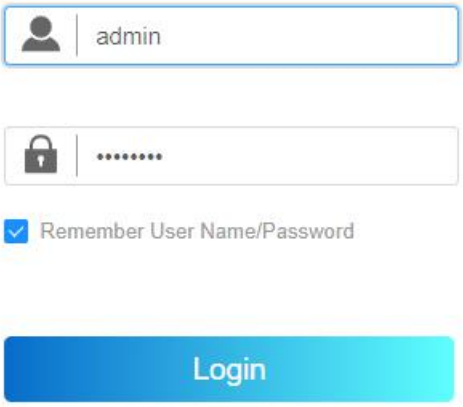


6.2. Access the Device Setting on the Web Interface

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

To log in device web interface, you can do as follows:

1. Check the device IP address on the device.
2. Enter the IP address on the web browser.
3. Enter the **User name** and **Password** of the device web interface.
4. Click **Login** tab to log in the web interface.



Tip:

- 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: http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s[]=ip&s[]=scanner

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.

7. Language and Time Setting

7.1. Language Setting

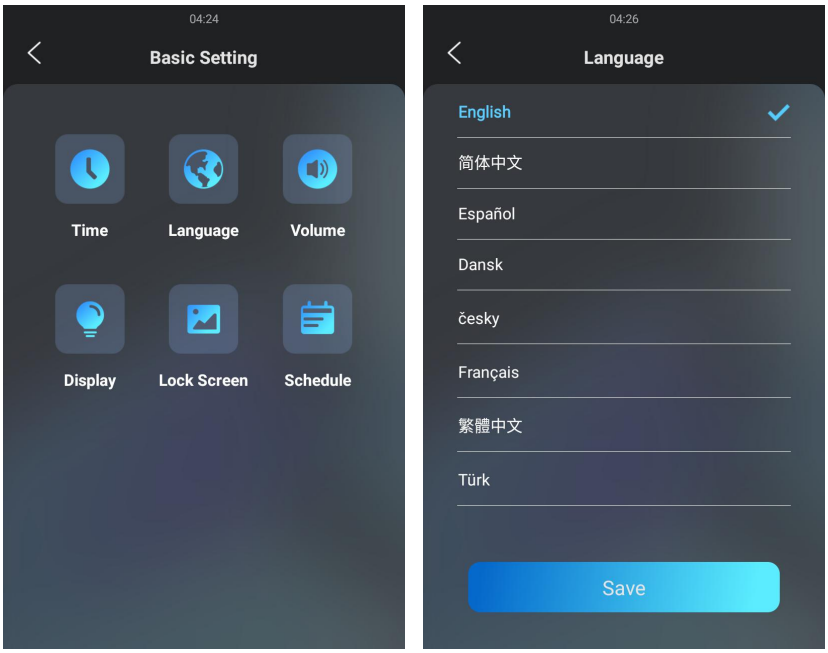
When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can either be set up directly on the device or on the device web interface according to your preference.

7.1.1. Language Setting on the Device

Language setting 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 , you can do as follows:

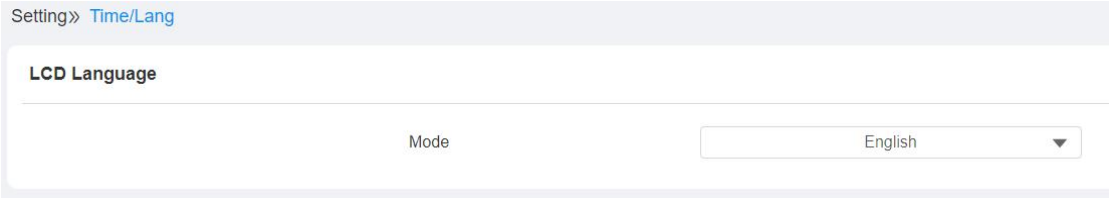
1. Press the **Basic Setting** icon on the **Setting** screen
2. Press the **Language** icon on the **Basic Setting** screen
3. Click to select the language you like, then press the **Save** tab.



7.1.2. Language Setting on the Device Web Interface.

To configure the language display on the device web interface, you can do as follows:

1. Click **Setting >Time/Lang > LCD Language**
2. Select the language you need and click **Submit** tab for validation.



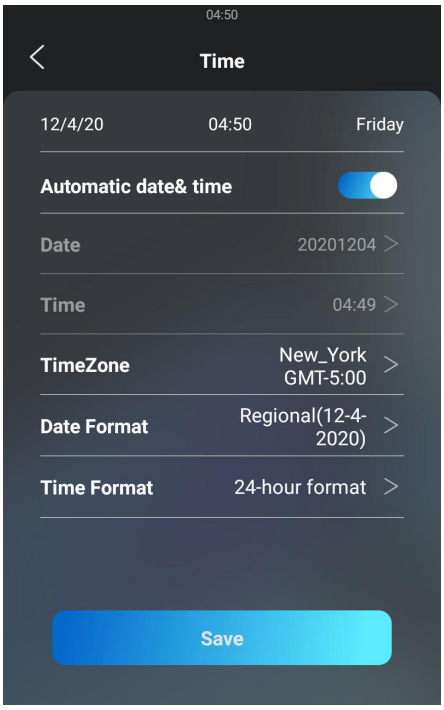
7.2. Time Setting

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

7.2.1.Time Setting on the Device

To set up time setting on the device, you can do as follows:

1. Press the **Basic Setting** icon on the home screen.
2. Press the **Time** icon on the **Basic Setting** screen
3. Configure the time setting properly.
4. Press **Save** tab for the validation.



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 enter 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:

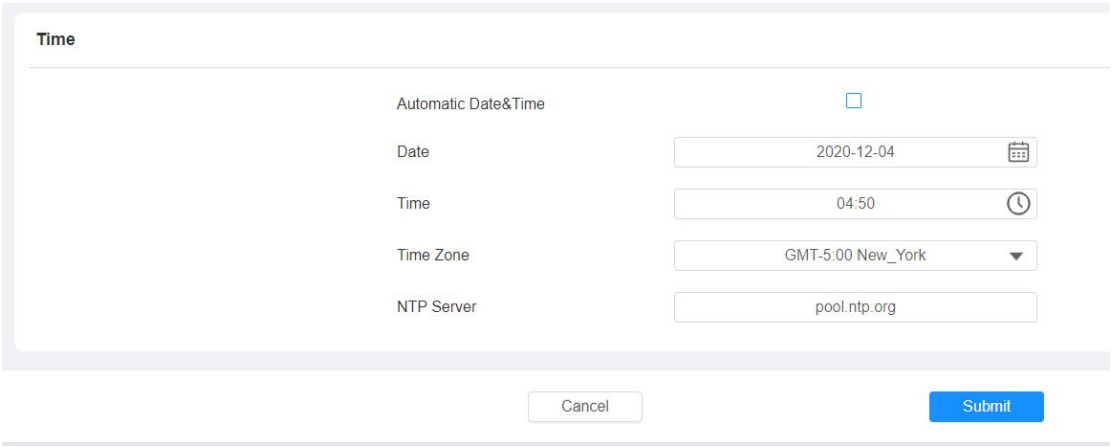
- When the **Automatic Date&Time** toggle switch is toggled off then parameters related to NTP server will become ineditable. And when the switch is toggled on, then time and date will be denied editing.

7.2.2.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 time setting on the web interface, you can do as follows:

1. Click **Setting >Time/Lang > Time**
2. Untick the check box to allow you to set the time and date manually.
3. Tick the check box to enable the NPT sever function that allows you to synchronize your time setting via NTP server.
4. Enter the NPT server you obtained in the field of the primary and secondary NTP **server**.
5. Set up the update timing via NTP server.
6. Click the **Submit** tab for the validation and the **Cancel** tab for the cancellation.



Parameter Set-up:

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

8. LED&LCD Setting

8.1.1. Infrared LED Setting

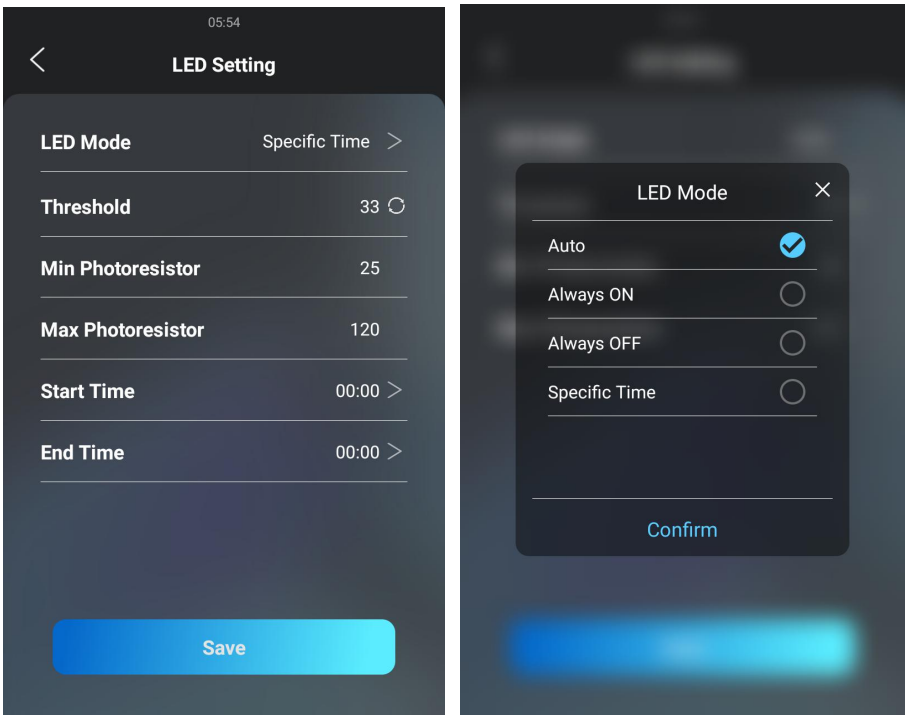
Infrared LED is mainly designed to reinforce the light for the facial recognition in the night or in the dark environment, you can configure the infrared LED in device and on the web interface.

.

8.1.1.1. Infrared LED Setting on the Device

To configure the infrared LED setting on the device, you can do as follows:

1. Press **Basic Setting** icon on the **Setting** screen
2. Press **Display** icon on the **Basic Setting** screen.
3. Press on **LED Setting** on the **Display** screen
4. Set the parameters and then press **Confirm** tab for the confirmation.
5. Press the **Save** tab for the validation.



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 "**Aways ON**" to enable the Infrared LED light to stay on permanently.
- **Always OFF**: select "**Aways OFF**" to turn off the Infrared LED light. LED mode is set "**Always OFF**" by default.
- **Specfic Time**: select "**Specfic Time**" to turn on the infrared LED according to the time schedule.
- **LED Type**: you can see the LED type "**Auto**" "**Aways ON**" "**Aways OFF**" "**Specfic 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 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 is from "**0**" minimum to "**1000**" maximume 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:

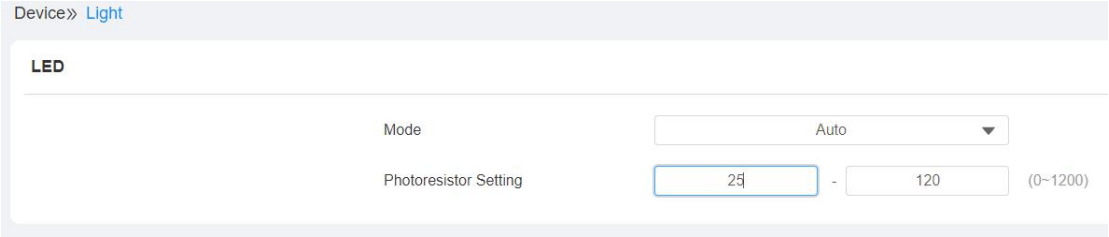
- **Start Time** and **End Time** will not be displayed unless you select **Specfic Time** for your LED mode.

8.1.1.2. Infrared LED Setting on the Web Interface

You can also select the LED type on the device web interface if needed.

To do so, you can do as follows:

1. Click **Device > Light > LED**
2. Click **Mode** field to select LED mode mode.
3. Click **Photoresistor Setting** field to select the minimum and maximum photoresistor value.
4. and click the **Submit** tab for the validation.



Note:

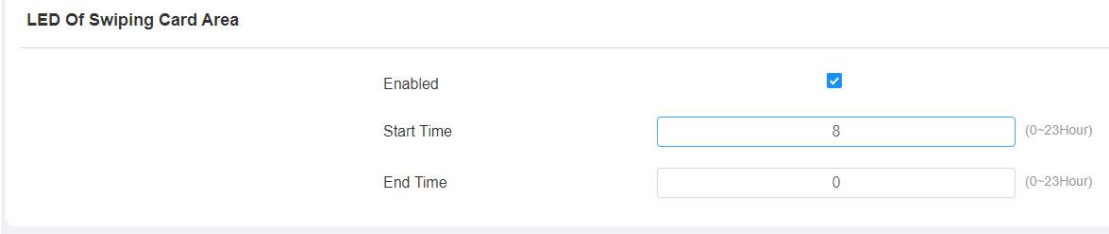
- Please refer to the infrared LED parameter setting on the device.

8.1.2.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 to 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 do the configuration, you can do as follows:

1. Click **Intercom > LED Setting > LED Control**
2. Set the parameter and press **Submit** tab for the validation.



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 (Sart time- End time)** it means LED light will stay on during the time span from **8:00** am to **12:00** pm during one day (24 hours).

8.1.3.LCD Screen Brightness Setting

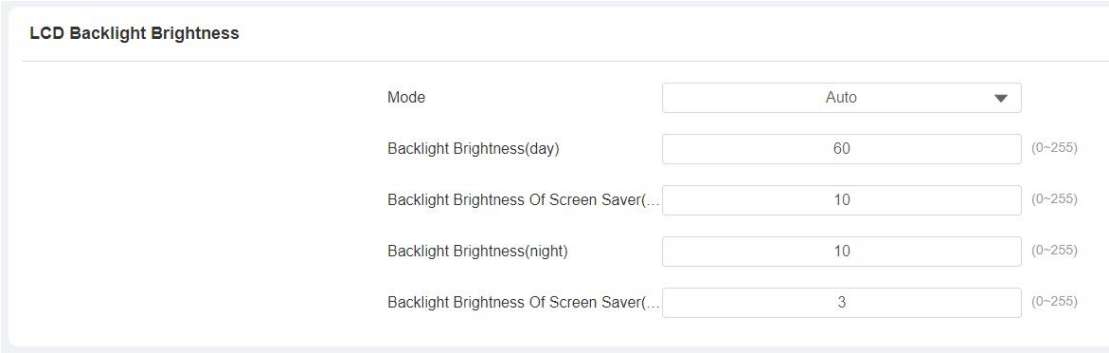
If you want to brighten up the screen in order to see the screen at greater ease in an environment with higher light intensity, you need to set up the related parameters.

8.1.3.1. LCD Screen Brightness Setting on the Web Interface

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

To do so, you can do as follows:

1. Click **Device > Light > LCD Backlight Brightness**
2. Set the screen backlight brightness parameters.
3. Press the **Submit** tab for the validation or the **Cancel** tab for the cancellation.



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 day time 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 the night with the value ranging from (**0-255**).

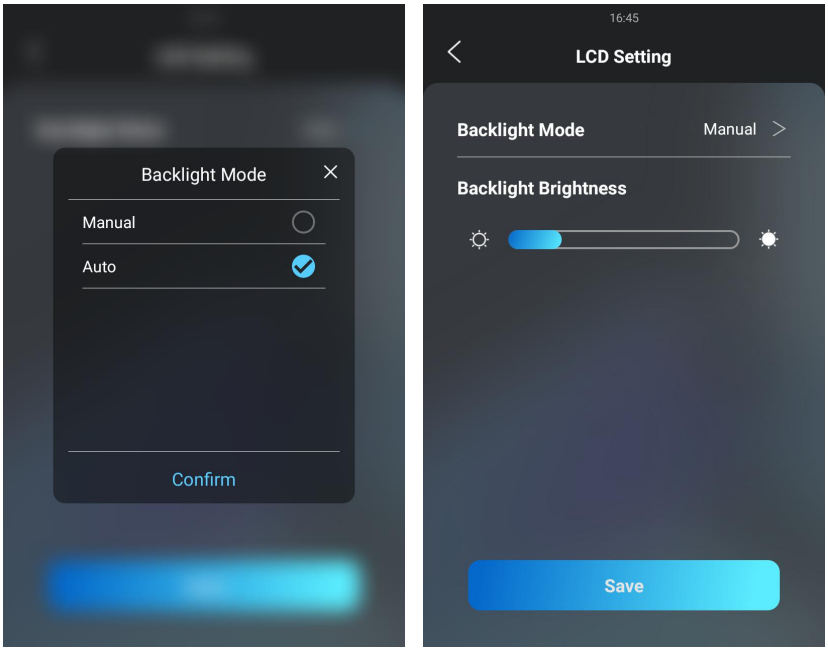
- **Backlight Brightness Of Screen Saver (night)**: set the screen backlight brightness for the screen saver during the day time with the value ranging from (**0-255**)

8.1.3.2. LCD Screen Brightness Setting on the Device

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

To set the screen backlight brightness, you can do as follows:

1. Press **Basic Setting** icon on the **Setting** screen
2. Press **Display** icon on the **Basic Setting** screen.
3. Press on **LCD Setting** on the **Display** screen.
4. Press the arrow on the **LCD Setting** screen.
5. Select brightness mode and press on **Confirm** for the confirmation.
6. Slide the adjustment bar for the backlight brightness according to your need.



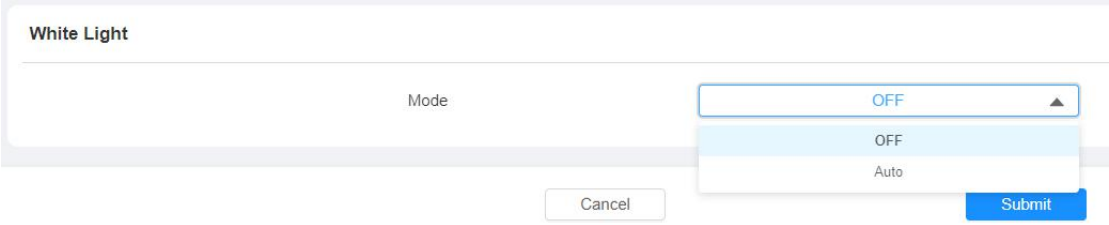
8.1.4. LED White Light Setting

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 the dark environment. You can set the white light function properly on the device web interface.

To set up the white light function, you can do as follows:

1. Click **Device > Light > White Light**
2. Set up parameter properly.

Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



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

9. Screen Display Configuration

X915 series door phone allow you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

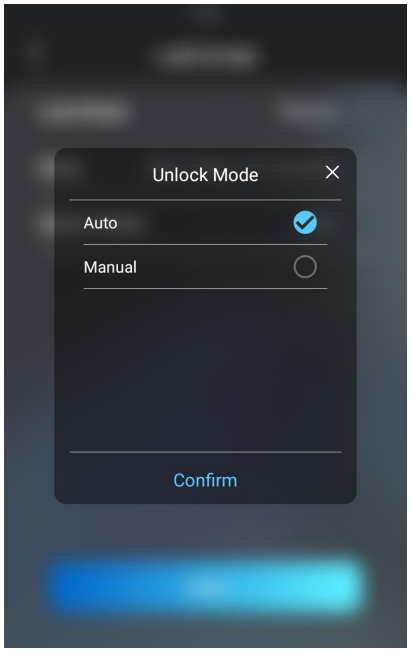
9.1.1. Screensaver Configuration

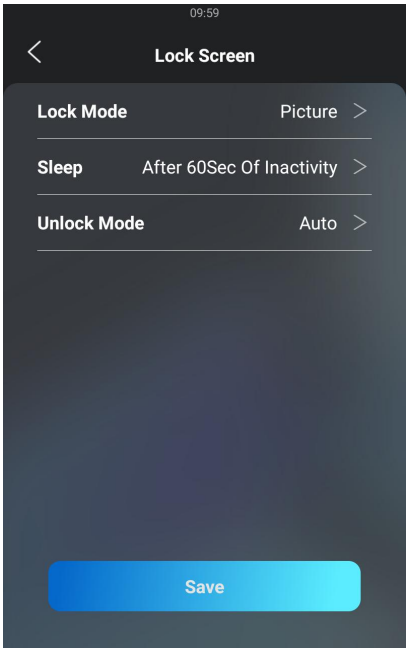
9.1.1.1. Configure Screensaver on the Device

Await screen is mainly a function for the screen protection. You can make the device to go into idle status for a predefined time span when there is no operation on the device or no one is detected approaching.

To set up await screen setting on the device, you can do as follows:

1. Press **Basic Setting** icon on the **Setting** screen.
2. Press **the Lock** Screen icon on the **Basic Setting** Screen.
3. Select the screen saver mode in **Lock Mode on the Lock Screen.**
4. Configure the screen saver start-time in **Sleep** on the Lock screen**.**
5. Select screen awakening mode in **Unlock Mode** on the **Lock** screen**.**
6. Press the **Save** tab for the validation.
7.





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** can not be changed from **"Auto**" to "**Manual**" when the **Lock mode** is set as " **Blank Screen**".

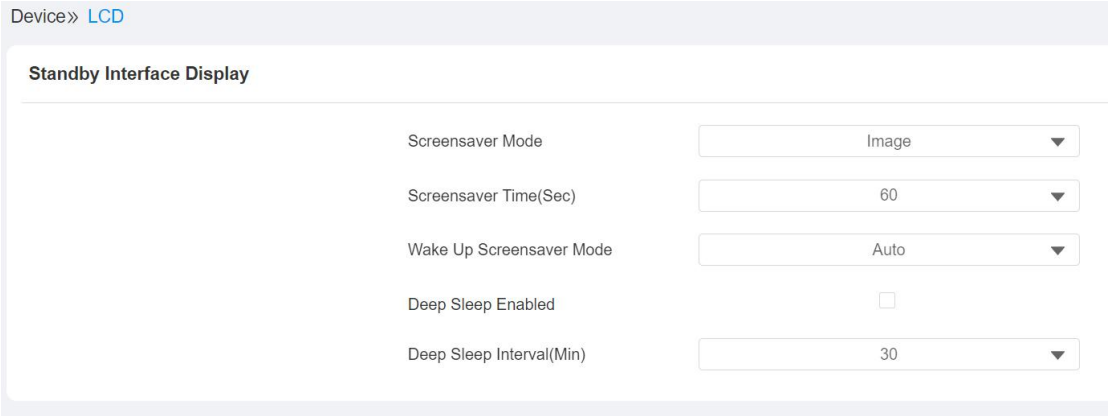
9.1.1.2. Configure Screensaver on the Web Interface

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 turn off for both screen protection and power reduction.

To set up the await screen setting on the web interface, you can do as follows:

1. Click **Device > LCD > Standby Interface Display**
2. Set up parameters properly according to your need.

3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



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 Enbabled**: tick the check box if you want the screen to be turned of 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:

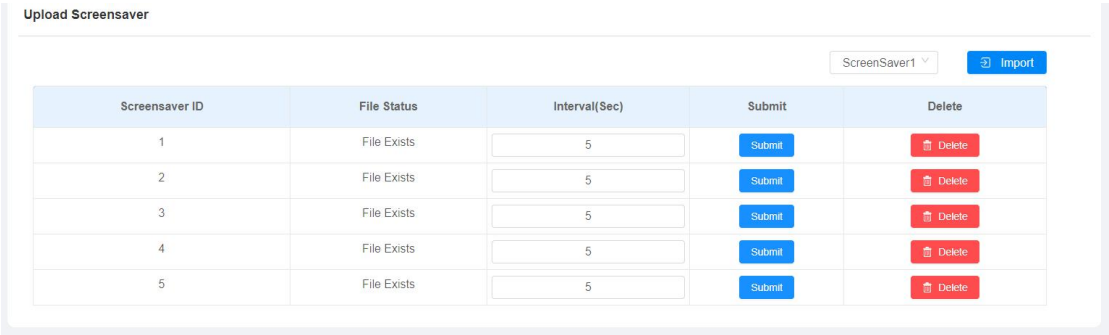
- **Wake Up Screensaver Mode** can not be changed from **"Auto"** to "**Manual**" when the **Screensavor Mode** is set as " **Blank Screen**".

9.1.2.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 do so, you can do as follows:

1. Click **Device > LCD > Upload ScreenSaver**
2. Select and designate the specific ID order number to the picture to be uploaded from image 1 to image 5.
3. Click **Import** tab to select the the picture from your Local PC
4. Click **Select File** tab to upload the picture selected.
5. Click **Upload** tab to start uploading the picture or click **Reset** tab to clear the picture.
6. Set the screensaver picture display interval in the **Interval** (**Sec**) field.
7. Click **Submit** tab for the validation



Note:

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

Note:

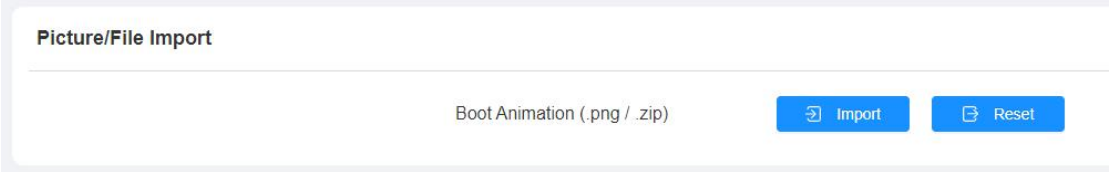
- The previous pictures with a specific ID order will be overwritten when repetitive designation of pictures to the same ID order occurred.

9.1.3.Upload Device Booting Image

You can upload the booting image to be displayed during the device's booting process if needed.

To upload the booting image, you can do as follows:

1. Click **Device > Key/Display > Picture/File Import**
2. Click **Import** tab to upload the picture to the device.
3. Click **Reset** tab if you want to change back to the default background picture.
4. Click the **Submit** tab for the validation or the **Cancel** tab for the cancellation.



Note:

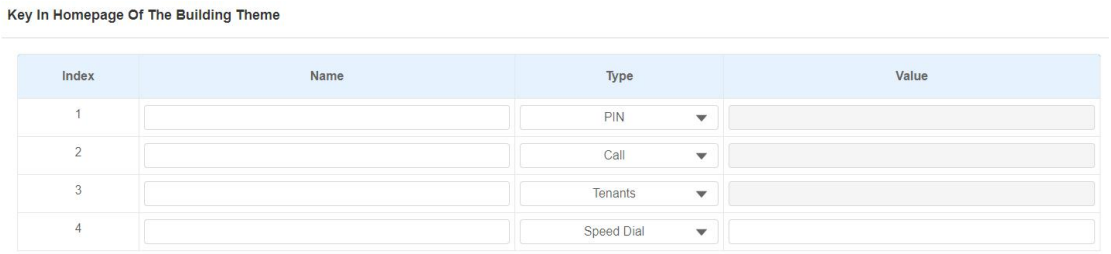
- The pictures uploaded should be in **.png or .zip format**

9.1.4.Home Screen Configuration

You can change the home screen display through the configuration of tab name and tab arrangement on the device web interface.

To configure the tab arrangement , you can do as follows:

1. Click **Device > Key/Display > Key In Homepage Of The Building Theme**
2. Click and select the tab type in the chosen **Index** number that indicates the tab position.
3. Enter tab name you like in the **Name** field if needed.
4. Click the **Submit** tab for the validation or the **Cancel** tab for the Cancellation.



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 to be displayed in position one, you can change the type in index number 1 to **Speed Dial**. And you can change other tab position accordingly.

- **Name**: enter a new name to replace the original type name, but it does not change the attribute of the type.

Note:

- Currently, tab icon selection can only be applicable to the **Speed Dial Type**.

10. 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.

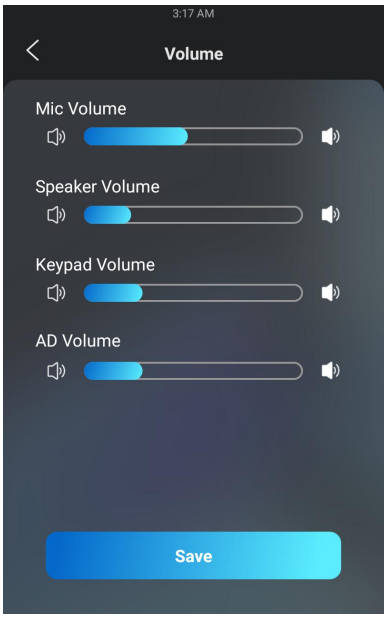
10.1.1. Volume Configuration

10.1.1.1. Configure Volume on the Device

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

To set up the volumes on the device , you can do as follows:

1. Press Basic setting  icon on the Setting screen
2. Press the **Volume** icon  on the **Basic Setting** screen on the device.
3. Move the volume adjustment bar to the left or right for the various types of volume adjustment.
4. Press **Save** tab for the validation.



Parameter set-up:

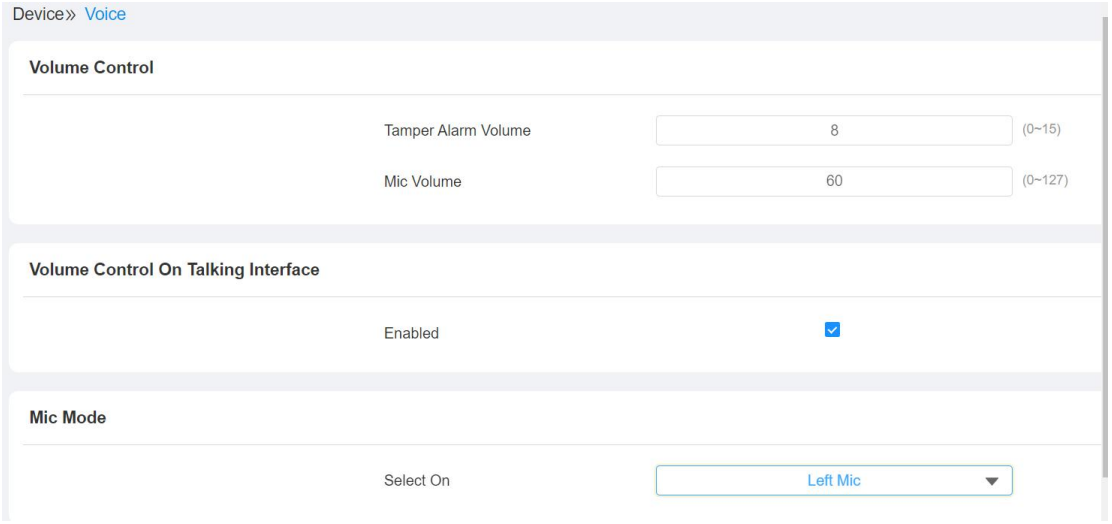
- **Mic Volume**: adjust the microphone volume according to your need.
- **Speaker volume**: adjust the loudspeaker volume according to your need.
- **Keypad Volume**: adjust the keypad volume for the button touch sound.
- **AD Volume**: adjust the announcement volume. Announcement can be,for example the open door success announcement, ringback sound and other prompt sounds.
- **Key Volume:** adjust the volume for the button touch sound.

10.1.1.2. Configure Volume on the Web Interface

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

To do so , you can do as follows:

1. Click **Device > Voice**
2. Set volume parameters according to your need
3. **Press Submit** tab for the validation or **Cancel** tab for the cancellation



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 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 the which mic to be applied between left and right microphones.

Tip:

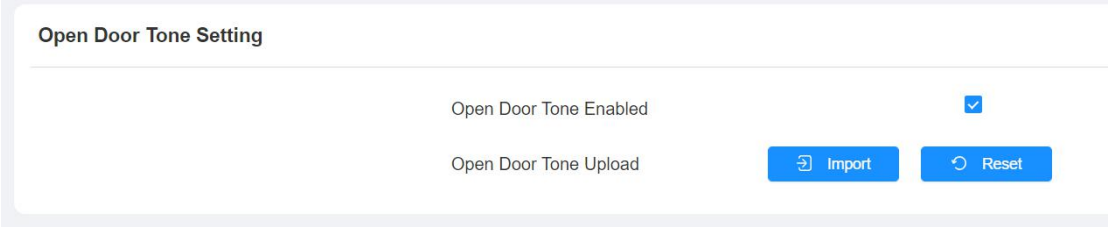
- When the Call volume on the above web interface is enabled, you are allowed to adjust the call volume during the call session.

10.1.2. Upload Open-door Tone

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

To configure the open door tone, you can do as follows:

1. Click **Device > Voice > Open Door Tone Setting**
2. Tick the check box if you want to enable the open door tone function.
3. Click on **Import** tab to import the open door tone files.
4. Click **Reset** tab to clear the file selected.
5. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



11. Network Setting

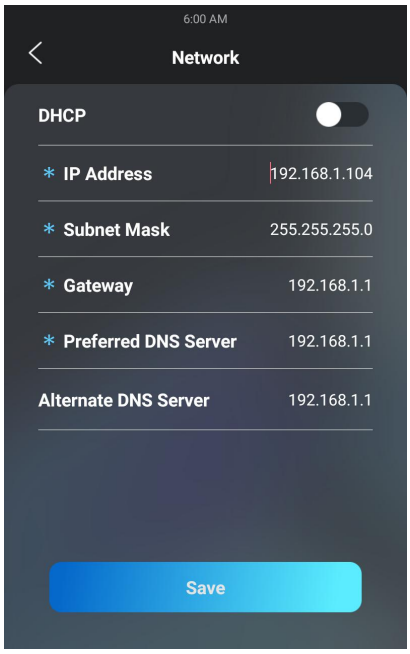
11.1.Device Network Configuration

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

To check and configure the network connection on the device , you can do as follows:

1. Click Network icon on the **Setting** Screen to go to **Address** Screen
2. Check to see if device connection is with DHCP mode or static IP mode.
3. Move the toggle switch to the right to apply the DHCP mode.
4. Move the toggle switch to left to go to static mode

5. Set up the IP Address according to your actual network environment if **Static IP mode** is selected.



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.

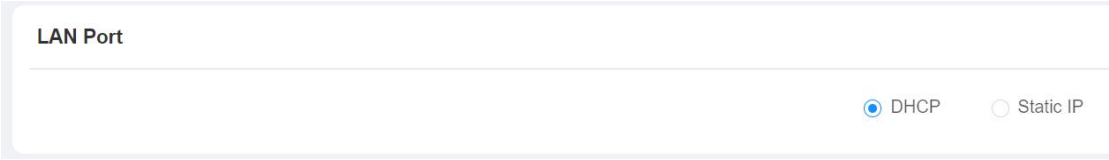
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.

- **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 Serve**r)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 connects to the alternate server when the primary DNS server is unavailable .

To check the network on the web interface, you can do as follows:

1. Click **Network > Basic > LAN Port**
2. Select **DHCP** mode or **static IP** mode by ticking their respective check box.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



To check and configure network connection on the device web interface, you can do as follows:

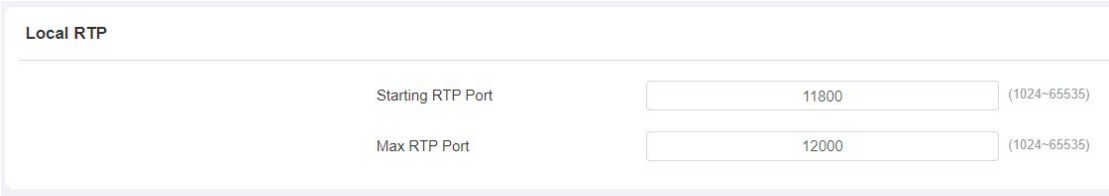
1. Click **Network > Basic > LAN Port**
2. Select **DHCP** mode or **static IP** mode by clicking their respective check box.
3. Set up the parameters in the exact the same way as you do for the set-up on the device .
4. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.

11.2.Device Local RTP configuration

For the device network data transmission purpose, 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 set up device local RTP, you can do as follows:

1. Click **Network > Advanced > Local RTP**
2. Set the **Starting RTP port** to establish the (**start point**) for the data transmission within the range from 1024 -65535.
3. Set the **Max RTP Port** to establish the (**end point**) for the data transmission within the range from 1024 -65535.



Parameter set-up:

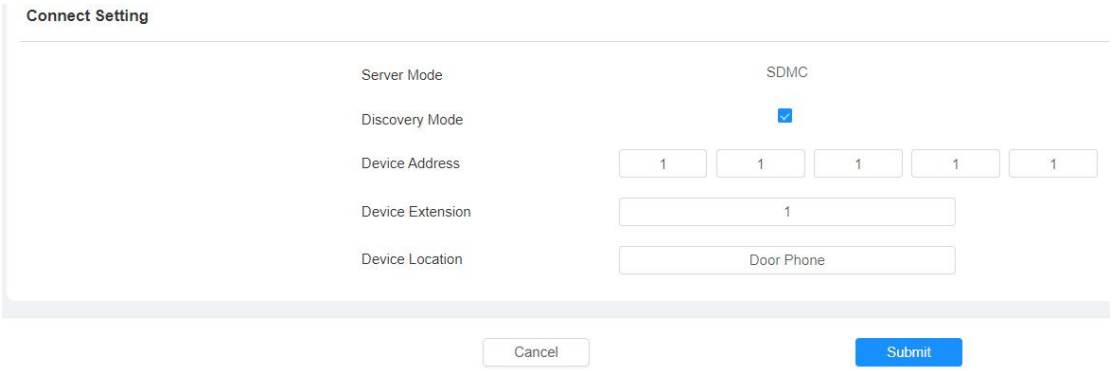
- **Starting RTP Port**: enter the Port value in order to establish the start point for the exclusive data transmission range.
- **Max RTP port**: enter the Port value in order to establish the end point for the exclusive data transmission range.

11.3.Device Deployment in Network

Door phones should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address and extension numbers as opposed to other devices for the device control and the convenience of the management.

To deploy the device in the network, you can do as follows:

1. Click **Network > Advanced > Connect Setting**.
2. Set up correct parameters according to your actual application and deployment.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



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.

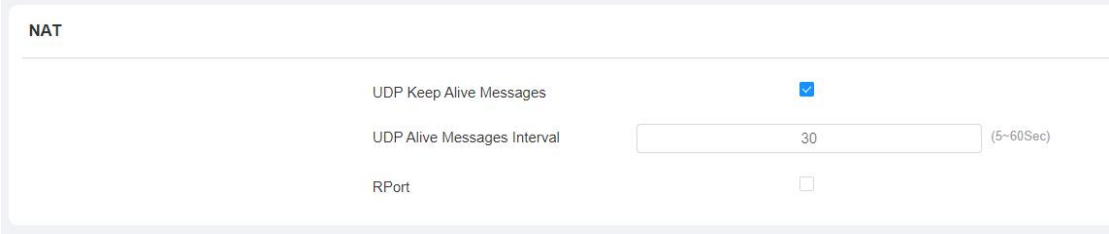
- **Device Location**: enter the location in which the device is installed and used.

11.4.NAT Setting

In order to speed up the communication between the door phone and the SIP server, you can configure the NAT setting (**Network Address Translation**) on the web interface.

To set up NAT, you can do as follows:

1. Click **Account > Advanced > NAT**
2. Set parameters properly.
3. Click **Submit tab** for the validation and **Cancel** tab for the Cancellation.



Parameter Set-up:

- **UDP Keep Alive Messages**: If enabled, the device will send out the massage to the SIP server so that SIP server will recognize that 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**).

12. Intercom Call Configuration

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

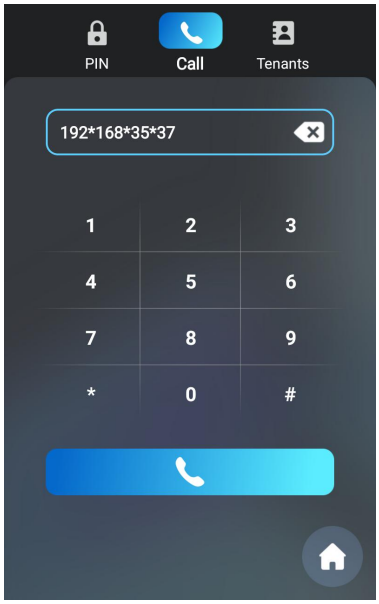
12.1.IP call & IP Call Configuration

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

12.1.1. Make IP Calls

To make SIP calls or IP calls on the device, you can do as follows:

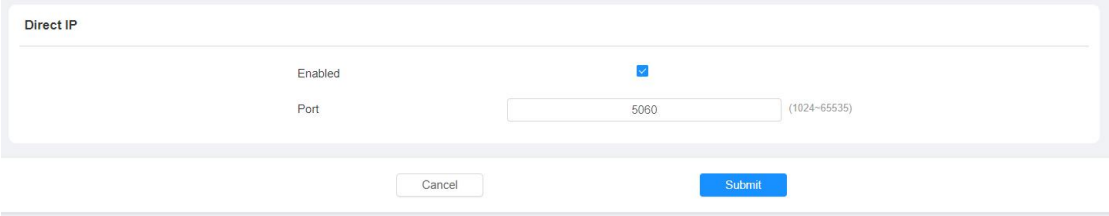
1. Click **Dial** icon on the home screen
2. Enter the IP or SIP number you wish to call on the soft key board.
3. Press the **Call** icon to dial out.



12.1.2. IP Call Configuration

To configure the IP call on the device web interface, you can do as follows:

1. Click **Intercom > Basic > Direct IP**
2. Set up related parameters as needed.
3. Press **Submit** tab for the validation or **Cancel** tab for the cancellation.



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 the 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

12.2.SIP Call &SIP Call Configuration

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

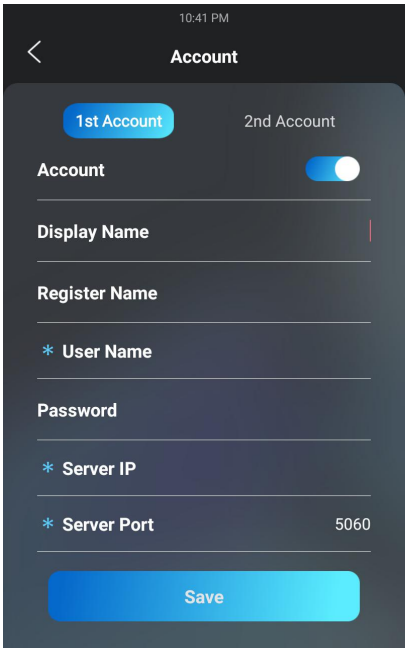
12.2.1. SIP Account Registration

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 account failed and become invalid. The SIP account can be configured on the device and on the device interface.

12.2.1.1. Configure SIP Account on the Device

To configure the SIP account on the device, you can do as follows:

1. Press **Account** icon on the **Setting** Screen.
2. Select Account by pressing **1st Account** or **2nd Account** tab on **Account** screen.
3. Move the toggle switch to the right to enable the account selected.
4. Enter the port number in the **Reg Server Port** field for the data transmission.
5. Press **Save** tab for the validation.



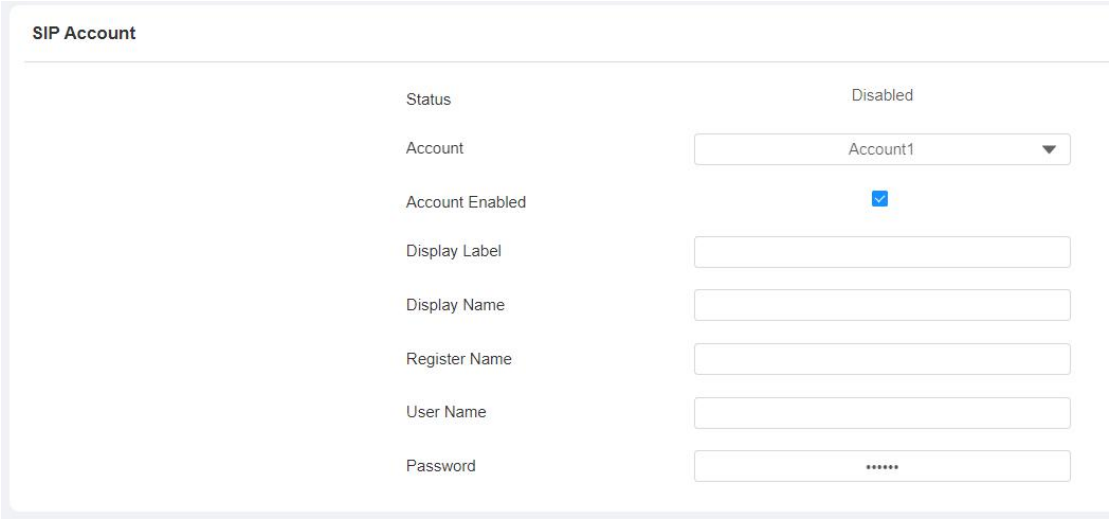
Parameter set-up:

- **Display Name:** configure the name, for example the device's name to be 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.

12.2.1.2. Configure SIP Account on the Web Interface

To perform the SIP account setting on the Web Interface, you can do as follows:

1. Click **Account > Basic > SIP Account**
2. Set up parameters for the SIP Account.
3. Click the **Submit** tab for the validation or the **Cancel** tab for the cancellation.



Parameter setup:

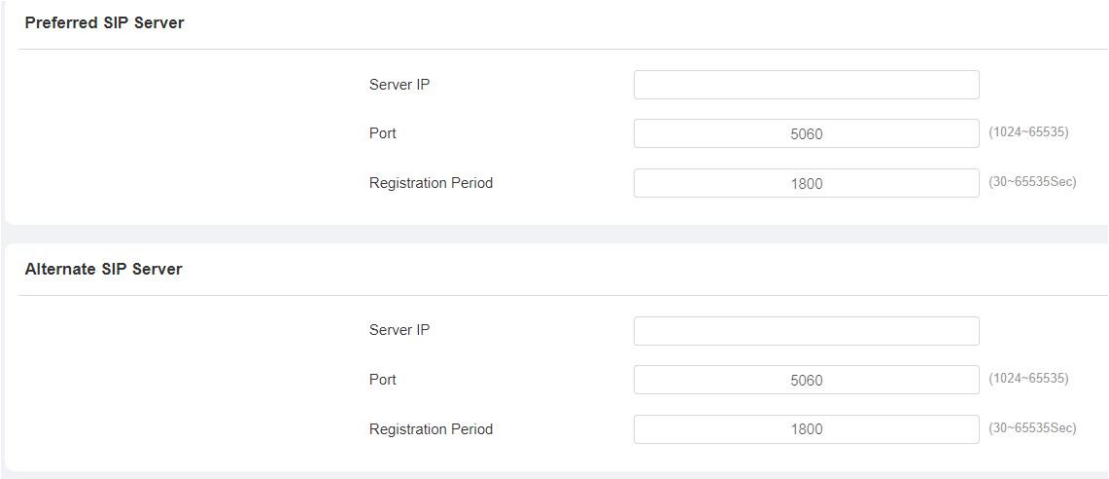
- **Status:** check to see if the SIP account is registered or not.
- **Account Active:** click "**enable**" or "**Disable**" to activate or deactivate the registered SIP account.
- **Display Name:** configure the name, for example the device's name to be be shown on the device being called to.
- **User Name:** enter the user name obtained from 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.

12.2.2. SIP Server Configuration

SIP servers can be set up for device in order to achieve call session through SIP server between intercom devices.

To set up SIP server , you can do as follows :

1. Click **Account - Basic - Preferred SIP Server**
2. Enter parameters required.
3. Press **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter Set-up:

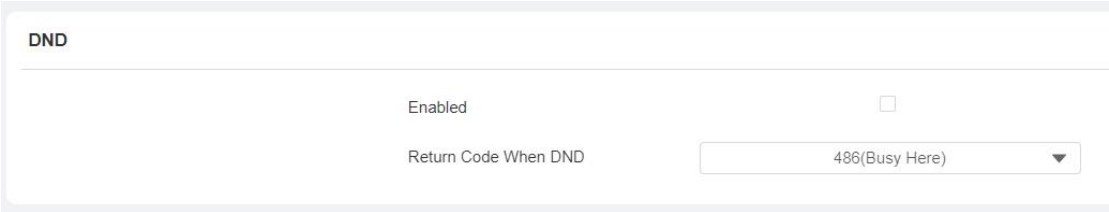
- **Preferred SIP Server:** enter the primary server IP address number or its URL.
- **Alternate SIP Server:** enter the backup SIP server IP address or its URL.
- **Port:** set up SIP server port for data transmission
- **Registration Period:** set up SIP account registration time pan. SIP re-registration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

12.2.3. SIP Call DND&Return Code Configuration

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

To configure the DND setting on the interface, you can do as follows:

1. Click **Intercom > Call Feature > DND**
2. Tick the check box to enable the DND function
3. Set up parameter in DND **Return code**
4. Press the Submit tab for the validation or Cancel tab for the cancellation.



Parameter Set-up:

- **Account:** select **"Account1"**, **"Account2"** or **"All account"** for the DND application.
- **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**".
- **DND On Code:** turn on the DND on server using the Code obtained. The DND on Code is **78** by default.
- **DND Off Code:** turn off the DND on server using the code obtained. The

DND off Code is **79** by default.

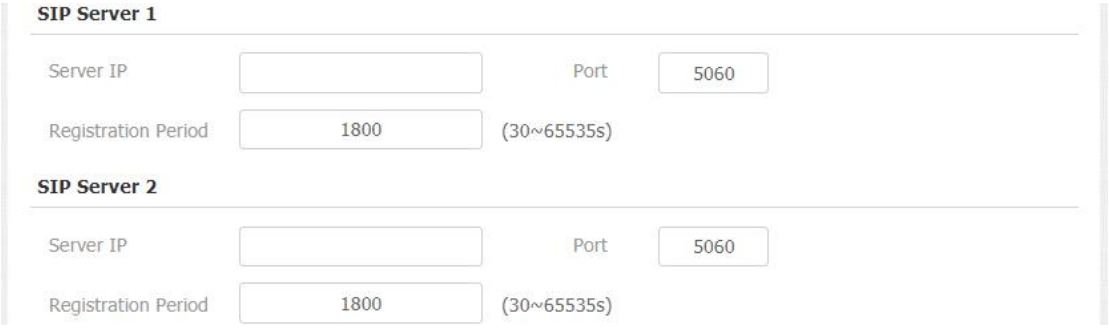
- **Return Code When Refuse**: select code to be sent the caller side via SIP server when you rejected the incoming call.

12.2.4. SIP Server Configuration

Two SIP servers can be set up for device in order to achieve call session through SIP server between intercom devices. SIP server 2 serves as a backup to the SIP server 1.

To do the setup, please do as follows :

4. Click **Account - Basic - SIP server1 /SIP serer 2**
5. Enter parameters required.
6. Press **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter Set-up:

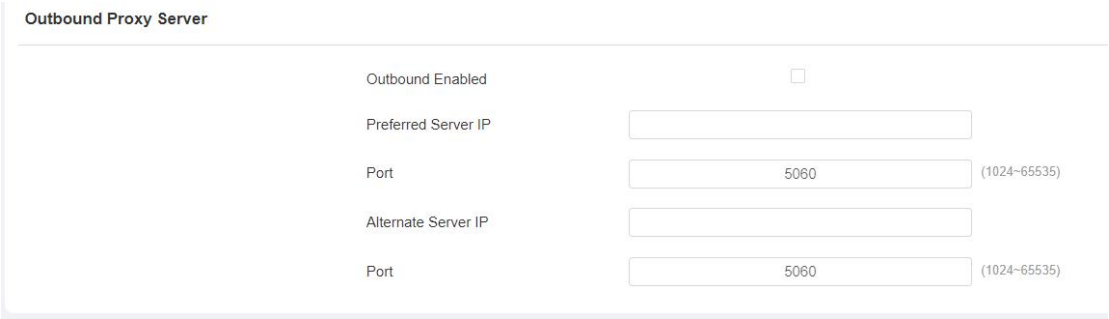
- **Server IP**: enter the Server's IP address number or its URL.
- **Port:** set up SIP server port for data transmission
- **Registration Period:** set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span.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

12.2.5. 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 session via port-based data transmission.

To configure outbound Proxy server, you can do as follows:

1. Click **Account > Basic > Outbound Proxy Server**
2. Set up parameters properly.
3. Press **Submit** for the validation.



Parameter Set-up:

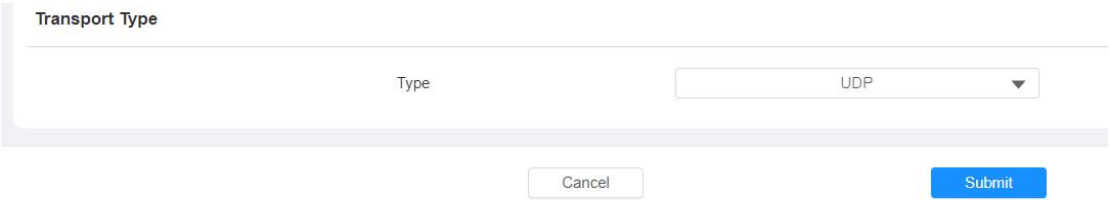
- **Enable Outbound:** click "**Enable**" and "**Disable**" to turn on or turn off the outbound proxy server.
- **Preferred Server IP:** enter the SIP address of the primary outbound proxy server.
- **Port:** enter the Port number for establish call session via the primary outbound proxy server
- **Alternate Server IP:** set up Backup Server IP for the backup outbound proxy server.
- **Port:** enter the Port number for establish call session via the backup outbound proxy server.

12.2.6. Configure Data Transmission Type

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

To do the configuration , you can do as follows:

1. Click **Account > Basic > Transport Type**
2. Select the Transport type according to your need.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



Parameter Setup:

- **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 services. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

12.3.Dial Options Configuration

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.

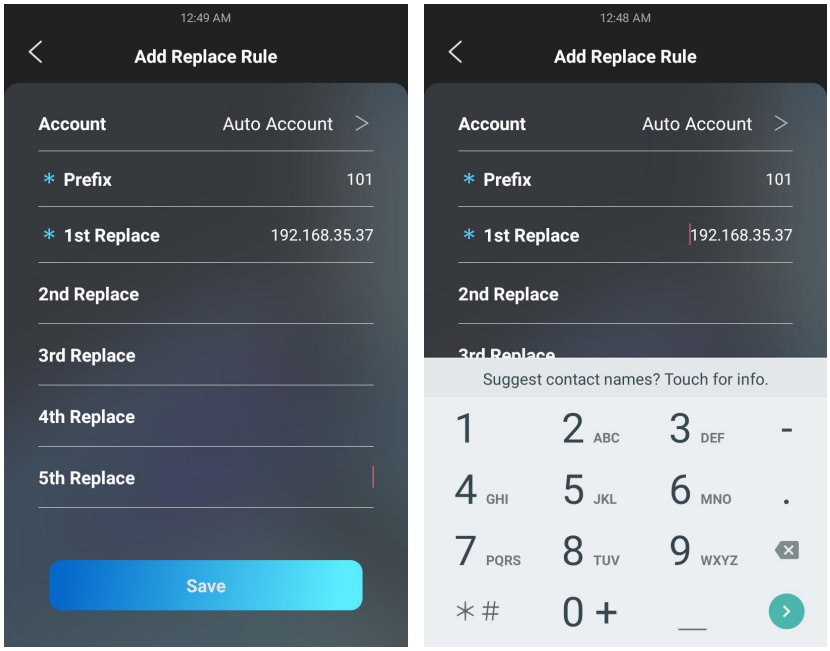
12.3.1. Quick Dial By Number Replacement

If you want to replace the long and complex dial number with a shorter number that can be memorized at greater ease and convenience for making calls, you can 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 address or SIP numbers with only one short number.

12.3.1.1. Quick Dial By Number Replacement on the Device

To configure the number replacement on the device , if you can do as follows:

1. Press **Replace Rule**  icon on the Setting screen.
2. Press **Add Replace Rule** tab on the **Replace Rule** screen
3. Press on **Account** to select the account to which you want to apply the setting.
4. Enter the short number in the **Prefix** field for the dial number replacement.
5. Enter the dial number to be replaced in the **Replace** field.
6. Press  to proceed to the next dial number and press  for the confirmation.
7. Press **Save** tab for the validation.



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.

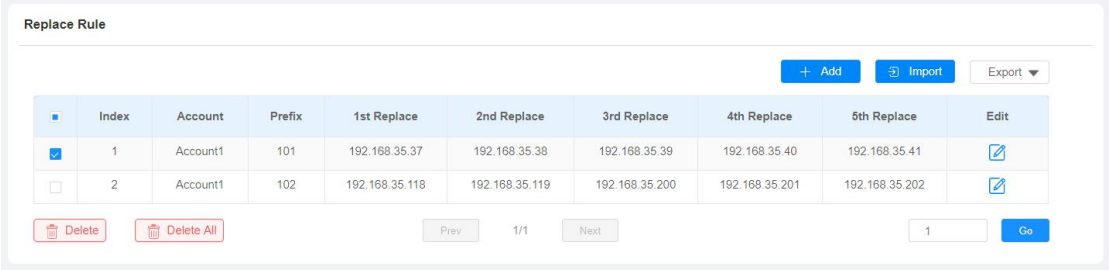
- **Replace 1/2/3/4/5:** enter the dial number(s) you wish to replace. It supports up to 5 number maximum for the replacement on the device configuration. For example if you replace five original dial numbers with a common short number such as " **101**" then the five intercom devices with the dial number will be called to at the same time when you dial **101**.

12.3.1.2. 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. Beside, you can edit and delete the numbers if need.

To configure the setting on the web interface, you can do as follows:

1. Click **Tenants > Dial Plan > Replace Rule**
2. Click **Add** tab to add new short dial numbers (Prefix).
3. Click the **Import** tab to select the file (xml.format)if you want to import the dial number in batch.
4. Press **Export** tab to export the existing file in tgz. Format.
5. Click **Edit** **icon if you want to edit the dial numbers**
6. Press **Save** tab to validate the setting.
7. Tick the check box of the specific line of the short number to be modified.
8. Click **Submit** tab for the validation.



Note:

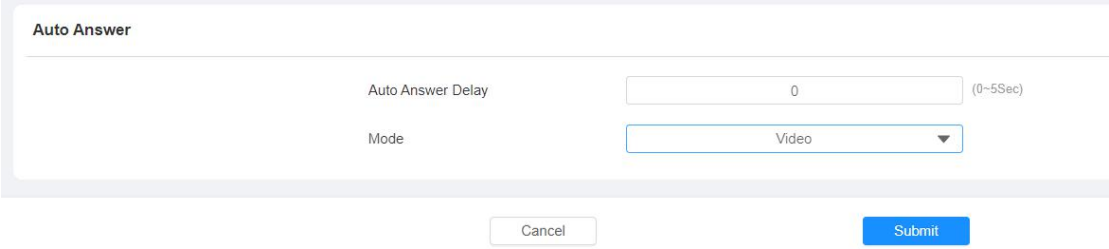
- The check box for each line of "**Prefix**" should be checked before you can see the **Edit** tab, which you click to carry out the modification.

12.4.Call Auto-answer Configuration

You can define how quick the door phone should response 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 do the configuration, you can do as follows:

1. Click **Intercom > Call Feature > Auto Answer**
2. **Set auto answer parameters**
3. Click the **Submit** tab for the validation or the **Cancel** tab for the validation



Parameter Set-up:

- **Auto Answer Delay:** set up the delay time (from 0-5 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.

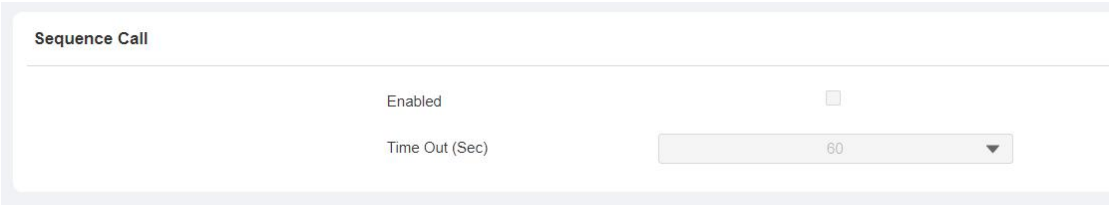
- **Mode:** set up the video or audio mode you preferred for the automatic call answering.

12.5.Robin Call Configuration

Robin Call is a function supported by Akuvox cloud 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 device.

To do the configuration, you can do as follows:

1. Click **Intercom > Basic > Sequence Call**
2. Set the Robin Call parameters.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



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.

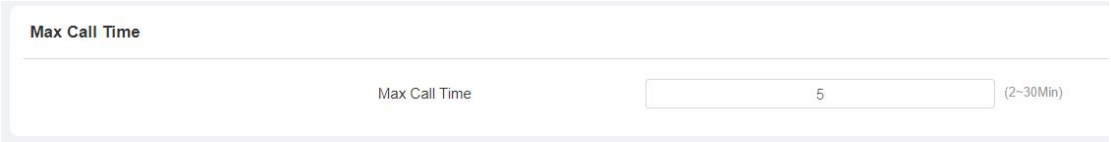
13. Call Settings

13.1.1. 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 do the configuration, you can do as follow:

1. Click **Intercom > Call Feature > Max Call Time**
2. Enter the time duration in in the **Max Call Time** field.



Parameter Set-up:

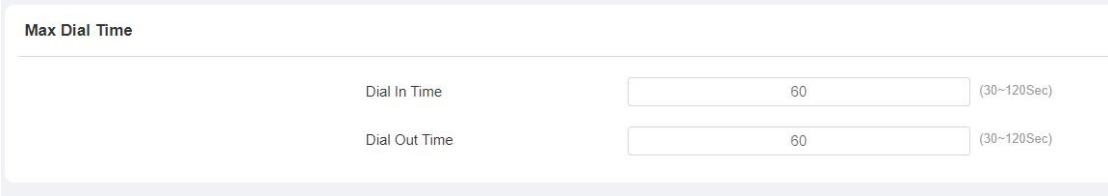
- **Max Call Time**: enter the call time duration according to your need (Ranging from 2-30 min.). The default call time duration is 5 min.

13.1.2. Maximum Dial Duration Setting

Maximum Dial duration is consisted of Maximum dial-in time duration and the maximum dial-out time. Maximum dial in time refers to the maximum time duration before the door phone hang up the call if the call is not answered by the door phone. In contrary, Maximum dial-out time refers to the maximum time duration before the door phone hang up itself automatically when the call from the door phone is not answered by the intercom device being called to.

To do the configuration, you can do as follows:

1. Click **Intercom > Call Feature > Max Dial Time**
2. Click and enter the timing parameters you need.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



Parameter set-up:

- **Dial In Time:** enter the dial in time duration for you door phone (ranging from 30-120 sec.) for example, if you set the dial in time duration is 60 second 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.

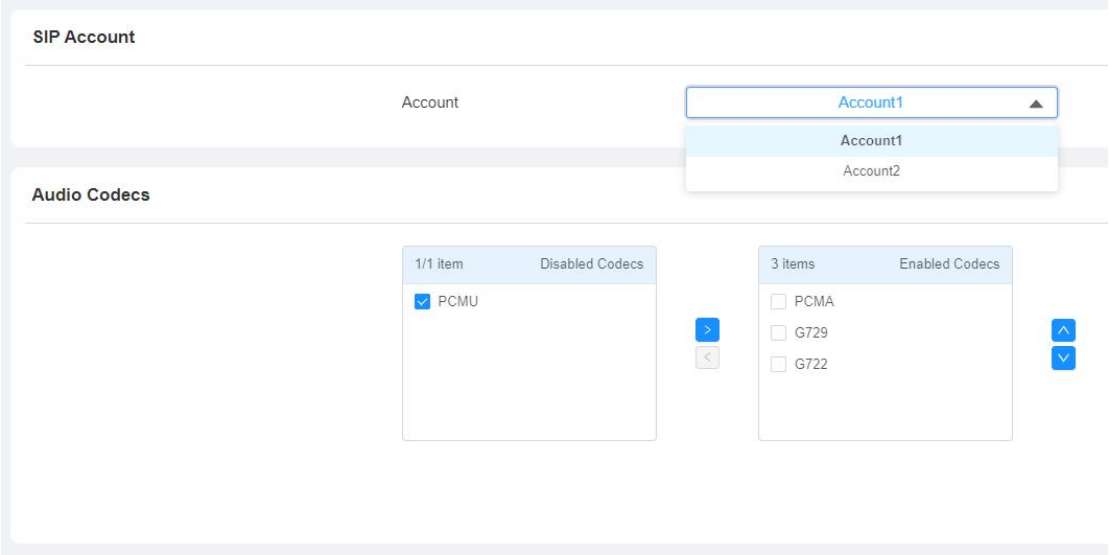
13.1.3. Audio& Video Codec Configuration for SIP Calls

13.1.3.1. Audio Codec Configuration

X916 series supports four types of Codec (PCMU, PCMA, G729, G722) for encoding and decoding the the audio data during the call session. Each type of Codec vary in terms of the sound quality. You can select the specific codec with different bandwidth and sample rate flexibly according to the actual network environment.

To do the configuration, you can do as follows:

1. Click **Account** > **Advanced > SIP Account**
2. Select the Account for which you want to apply the codec.
3. Go to **Audio Codecs** section below.
4. Click on arrows and move the codec type left and right in order to enable or disable the codec function.
5. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



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

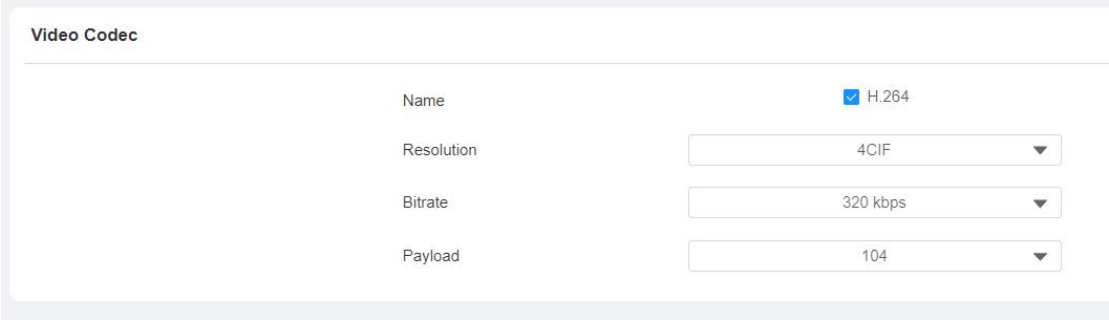
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ

13.1.3.2. Video Codec Configuration

X915 series support H264 codec that provides a better video quality at much lower bit rate with different video quality and payload.

To do the configuration, you can do as follows:

1. Account > Advanced > **Video Codec**
2. Check the H264 Codec name check box.
3. Set up parameters according to your need.
4. Click **Submit** tab for the validation.



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 in every second is greater in amount therefore the video will be clearer.. While the default code bitrate is 2048.

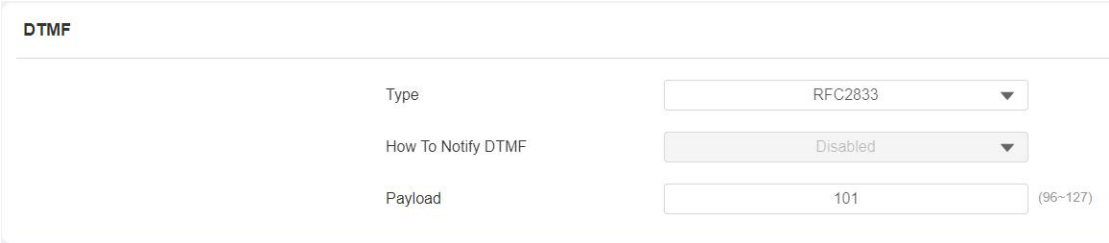
- **Payload:** select the payload type (ranging from 90-118) to configure audio/video configuration file. The default payload is 104.

13.2.Configure DTMF Data Transmission

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

To set up the DTMF data transmission, you can do as follows:

1. Click **Account > Advanced > DTMF**
2. Set up parameters properly according to your need.
3. Press **Submit** tab fore the validation or **Cancel** tab for the Cancellation.



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 the the specific data transmission payload agreed on between the sender and receiver during the data transmission.

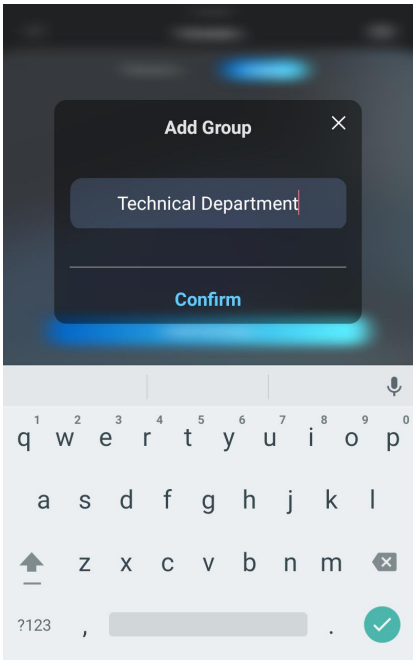
14. Phone Book Configuration

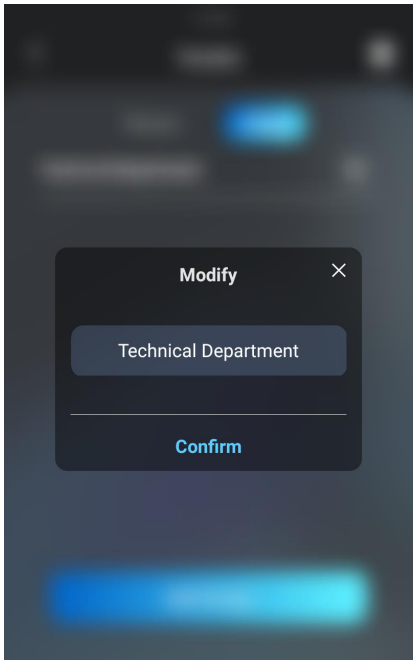
14.1.Phone Book Configuration on the Device

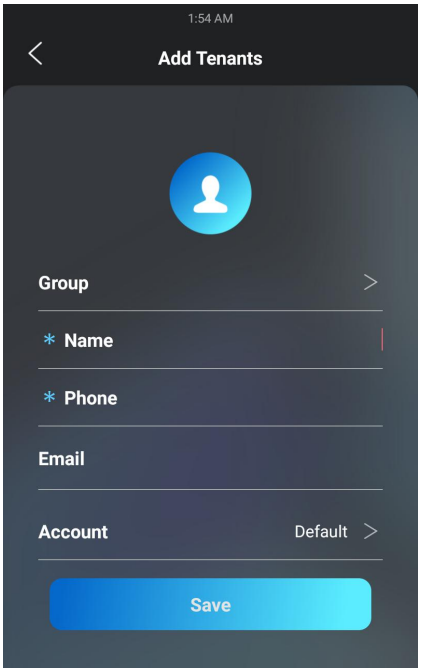
You can configure the contacts list in terms of adding and modifying contact groups or contacts on the device directly.

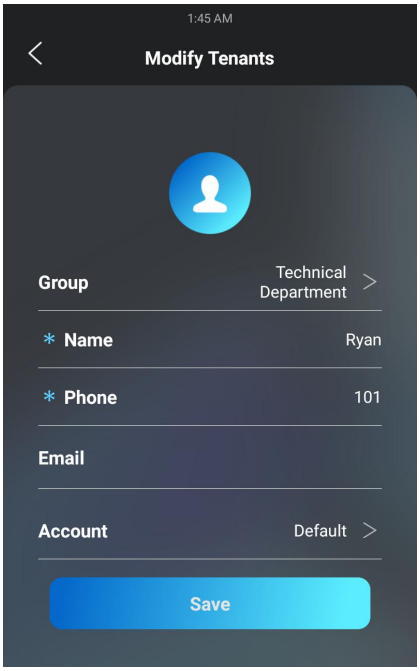
To configure the phone book on the device , you can do as follows:

1. Press **Tenants** icon on the Setting screen.
2. Press on **Group** and then press **Add Tenants** tab to enter the group name before pressing on **Confirm** for the confirmation.
3. Press icon to edit the group name and press on **Confirm** for the confirmation.
4. Press on **Tenants** and click **Add Tenants** tab to enter the contact information and press the **Save** tab to add contact.
5. Press on the specific contact to edit or delete.









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 default option, then the contact number will be call 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.

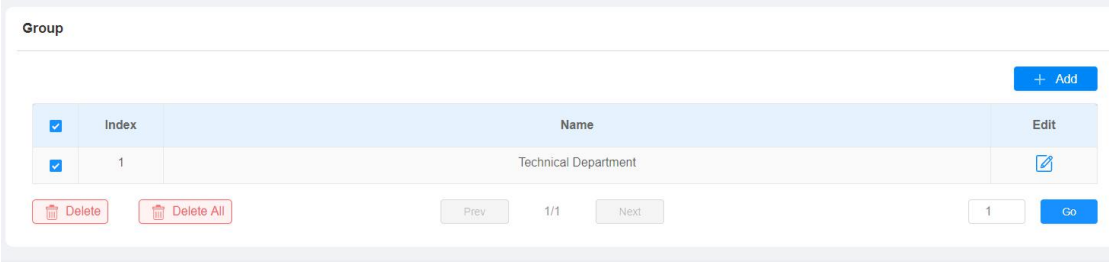
14.2.Phone Book Configuration on the Web Interface

14.2.1. Manage Contact Groups on the Web Interface

You can configure contact and contact groups by adding and editing them on the web interface.

To configure contact group, you can do as follows:

1. Click **Tenants > Tenants List > Group**
2. Click **Add** tab to enter the group name
3. Click the **Submit** tab for confirmation and click **Cancel** tab for the cancellation.
4. Tick the specific check box for the group name to be deleted or edited.
5. Edit the name in the **Name** field and click the **Submit** tab to finish the editing.



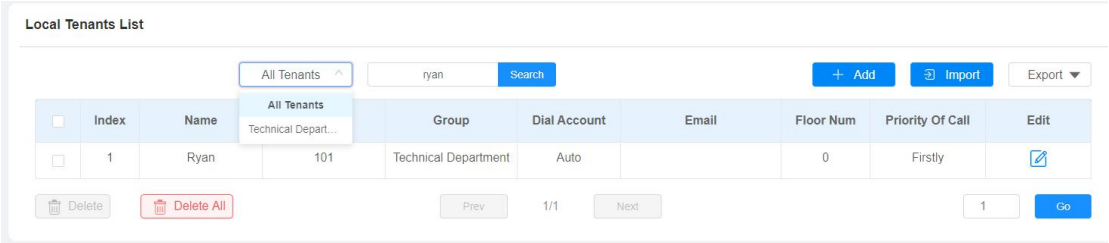
14.2.2. Contact List Configuration on the Web Interface

Contact can also be configured on the web interface where you can also upload the contact pictures if needed.

To conduct contact configuration, you can do as follows:

Parameter set-up:

1. Click **Add** tab and fill in the contact information to create contact.
2. Click **Import** tab to import the contacts in batch or click the the export contact to export the contacts.
3. Click the **Edit** icon on the specific contact if you want to edit the contact.
4. Enter the the specific contact name and select the contact group, then click the **Search** tab if you want to find the contact you need.



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 contact 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 some one 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.

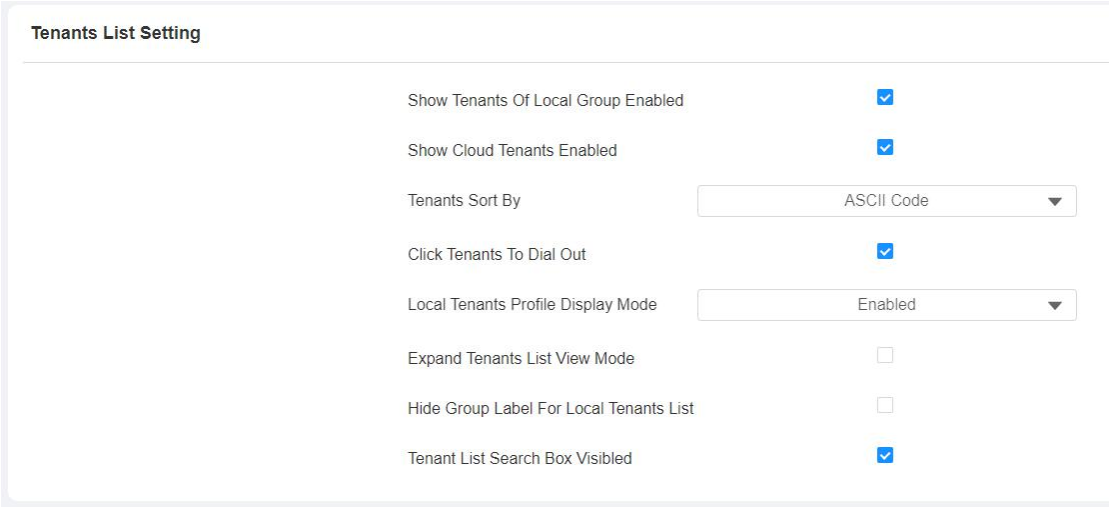
14.2.2.1. Contact List Display Setting

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

To do it , you can do as follows:

1. Click **Tenants > Tenants List > Tenants List Setting**
2. Set up the parameter according to you need.
3. Press **Submit** tab for the validation or **Cancel** tab for the cancellation.

Please refer to the setting below:



Parameter set-up:

- **Show Tenants Of Local Group Enabled:** tick or untick the check box to control the display the 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 vise 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 sort 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 any where 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

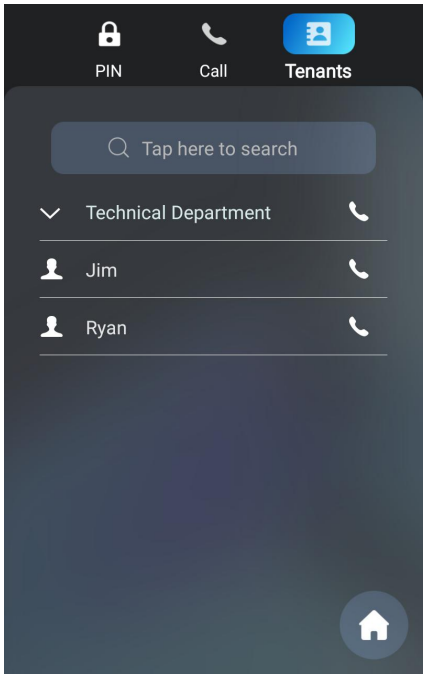
be displayed next to the name; if not, there won't be a icon next to the name.

- **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 to control the display the 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 vise versa.

- **Contact List Search Box Visibled:** 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.

Please refer to the contact list display on the screen below:



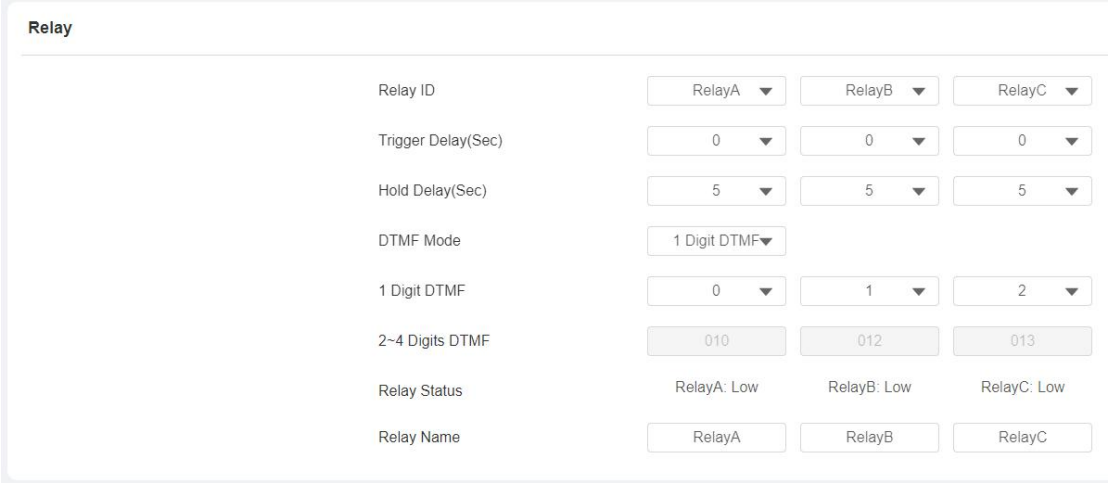
15. Relay Setting

15.1.Relay Switch Setting

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

To do the configuration, please do as follows:

1. Click **Access Control > Relay**
2. Set up relay related parameters properly according to your need.
3. Click **Submit** tab for the validation and Cancel tab for the validation.



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 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 after the door is unlocked.

- **DTMF Mode:** select the number of DTMF digit for the door access control (**Ranging from 1-4 digits**) For example, you can select 1 digit DTMF code or 2-digit DTMF code etc., according to your need.

- **1-digt DTMF :** set the 1-digt DTMF code within range from (**0-9 and *,#**).

- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMP Mode** is set as 3-digits.

- **Relay 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 the 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.

15.2.Web Relay Setting

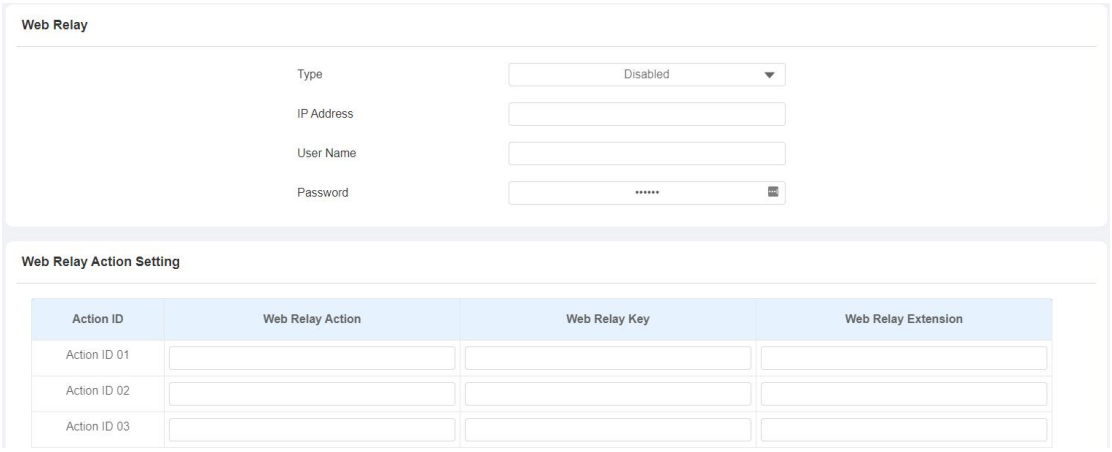
In additional to the relay that is connected to the door phone, you can also control the door access using the network-based web relay on the device and on the device web interface.

15.2.1. Configure Web Relay on the Web Interface

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

To do the configuration , you can do as follows:

1. Click **Access Control > Web Relay**
2. Enter the parameters properly.
3. Go to the "**Web Relay Action Setting**" below in the same interface.
4. Configure the parameter properly.
5. Press the **Submit** tab for the validation and **Cancel** tab for the cancellation.



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 we 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 passwords 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 unlock via DTMF code, the action command will be sent to the web relay automatically.

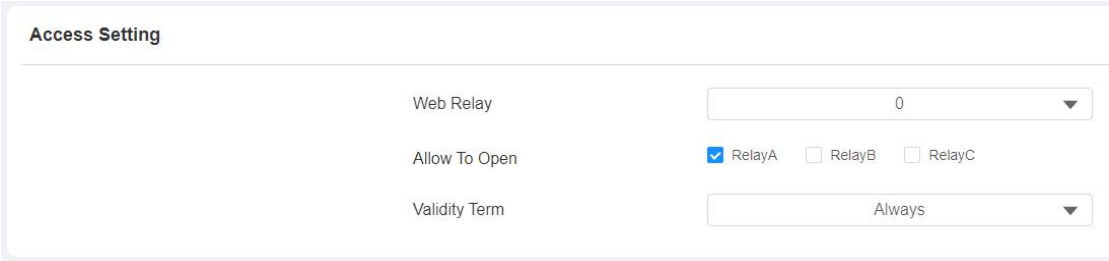
- **Web Relay Extension:** enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below:

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

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

To configure the the web relay for the door access, you can do as follows:

1. Click **Access Control > User**
2. Click **Add** tab on the **User** Interface page.
3. Go to the **Access Setting** on the Bottom.
4. Click to select the specific web relay to be triggered at the corresponding location in the **Web Relay** field.
5. Tick the check box to select the corresponding relay you want to open.
6. Click **Submit** tab for the validation.



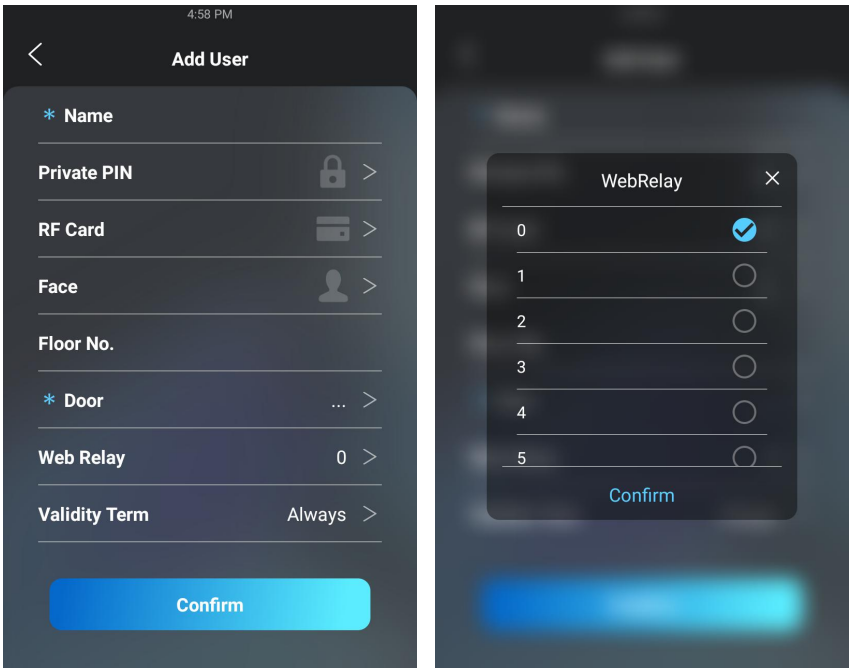
15.2.2. Configure Web Relay Configuration on the Device

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

To do so , you can do as follows:

1. Press **User** Icon on the **Setting** screen.
2. Press **Add** tab.
3. Press Web Relay arrow .
4. Tick the circle icon to assign the specific web relay to a resident for the door access.
5. Press the **Save** tab on the **Add User** screen for the validation

Please see the picture below:


4:58 PM
Add User
* Name
Private PIN
RF Card
Face
Floor No.
* Door
...
Web Relay
0
Validity Term
Always
Confirm
WebRelay
0
1
2
3
4
5
Confirm

16. Door Access Schedule Management

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

16.1. Configure Door Access Schedule

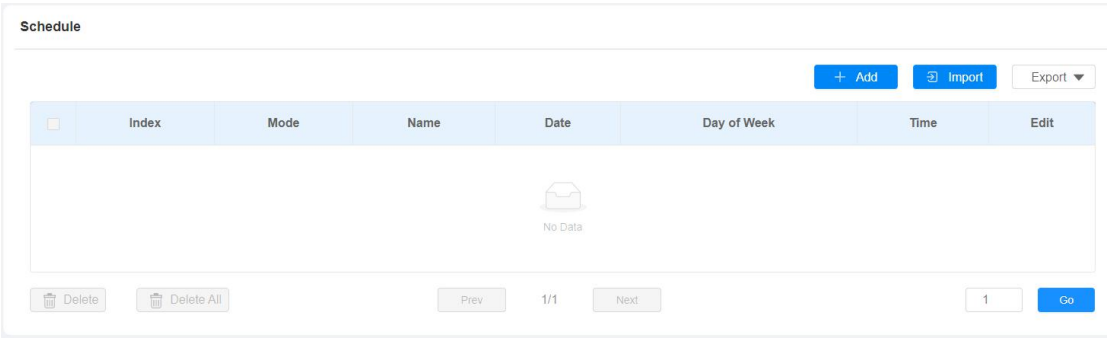
You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. More over, you can edit your door access schedule if needed.

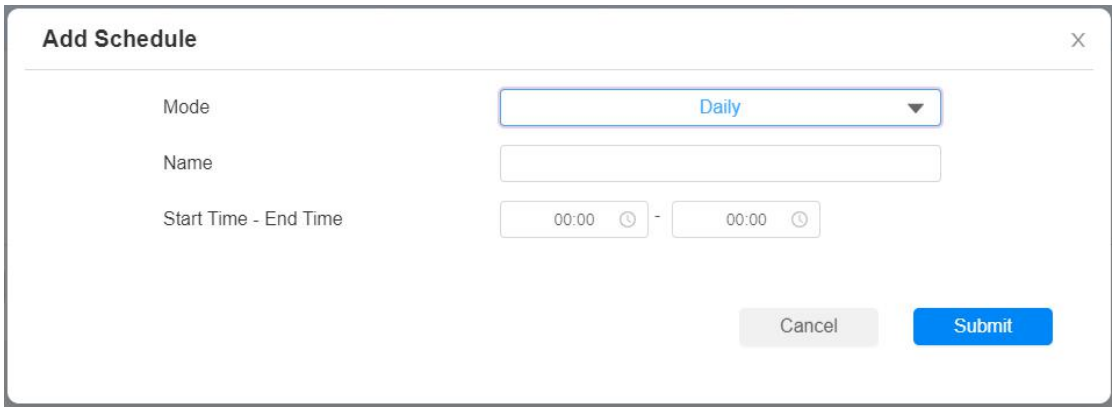
16.1.1. Create Door Access Schedule

You can create the door access schedule on a daily or monthly basis and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis.

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

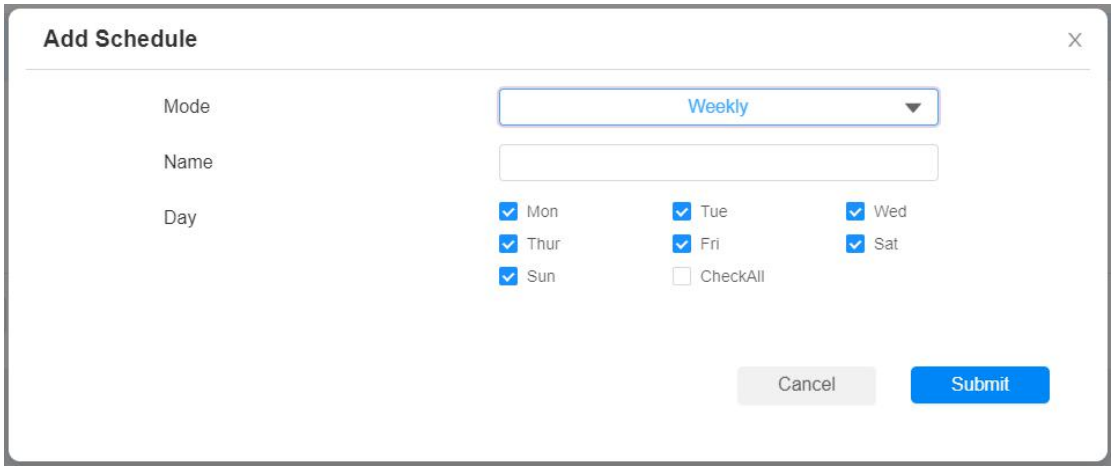
1. Click **Setting > Schedule**
2. Click **Add**
3. Click **Mode** field to select "**Daily**" Type
4. Enter the schedule name .
5. Set up the daily time schedule for the validity of the door access
6. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.





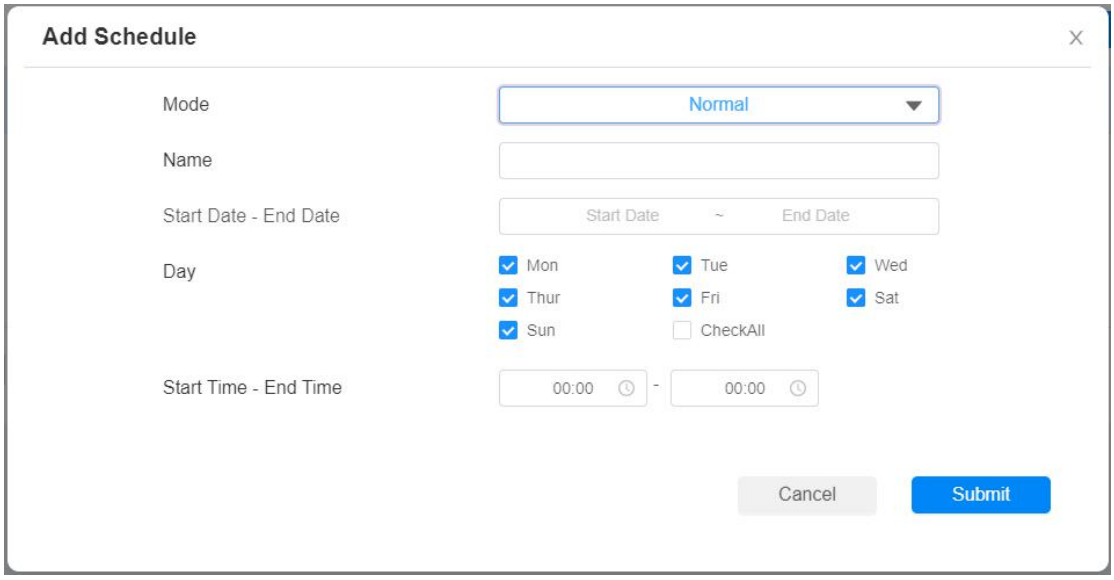
To create a weekly schedule, you can do as follows:

1. Click **Mode** field to select "**Weekly**" Type.
2. Enter the Schedule name according to your need.
3. Select the day (s) on which door access can be valid on monthly basis
4. Set up the time schedule for the validity of the door access during a day.
5. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



To create a longer period schedule, you can do as follows:

1. Click **Mode** field to select "**Normal**" Type.
2. Repeat the setting in the identical way as you do for the " Weekly" schedule.
3. Set the time period specifying year, month and date.
4. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

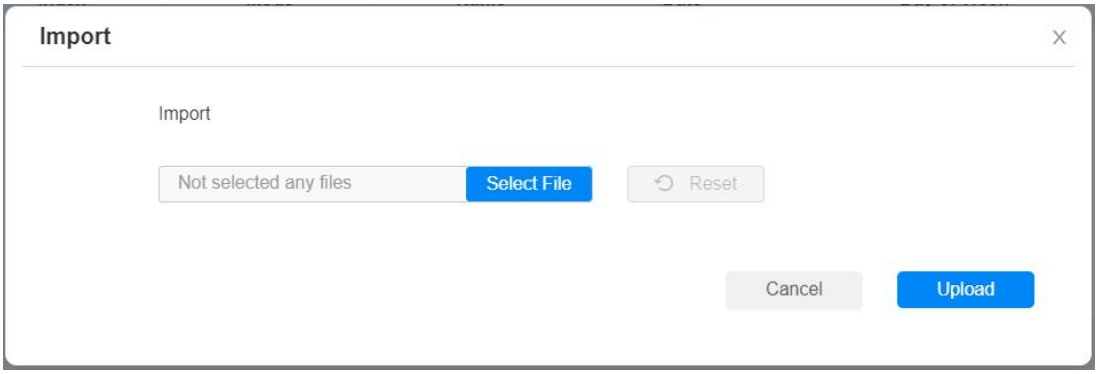


16.1.2. Import and Export Door Access Schedule

In addition to creating door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency.

To import and export the schedule, you can do as follows:

1. Click **Setting > Schedule > Schedule > Import**
2. Click **Select file** tab to upload your schedule data file.
3. Click **Reset** tab to clear the file you have selected.
4. Click **Upload** tab to start uploading the file and **Cancel** tab for the cancellation.



Note:

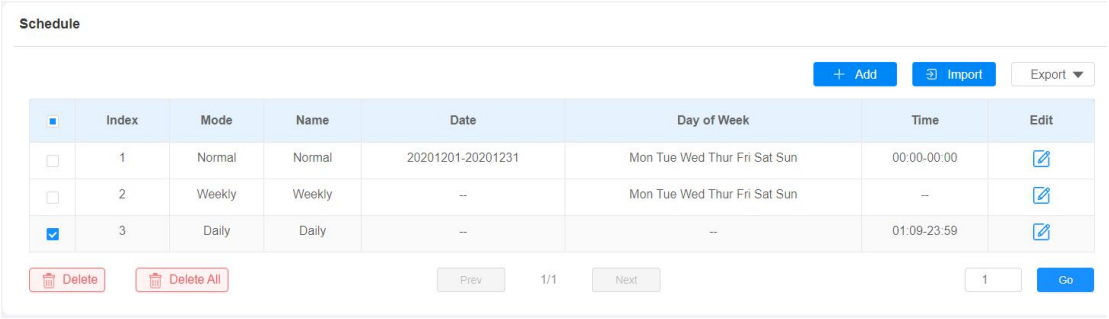
- It only supports .xml format file for importing and exporting the schedule.

16.1.3. Edit the Door Access Schedule

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

To edit or delete the schedule , you can do as follows:

1. Click **Setting > Schedule**
2. Click **Edit** icon to edit the schedule according to your need.



17. Door Unlock Configuration

X915 series door phone offer you three types of door access via PIN code, RF card and Facial recognition. You can configure them on the device and web interface. More over, you can import or exporting the configured files to maximize your RF card configuration efficiency.

17.1.Configure PIN Code for Door Unlock

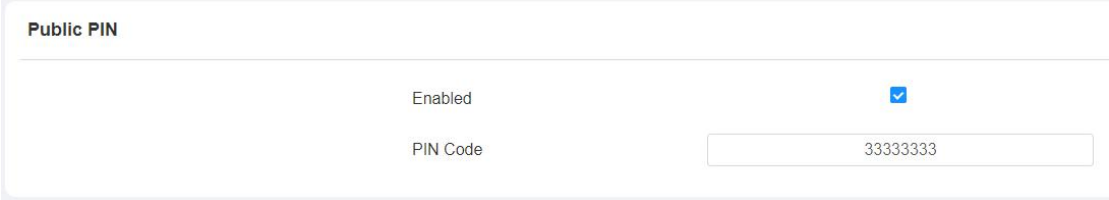
You can create and modify both Public PIN code and private PIN code for the door access on X915 series door phones

17.1.1. Configure Public PIN code

You can configure and modify a total of 3 sets of separate PIN codes on the device web interface.

To configure Public PIN code, you can do as follows:

1. Click **Access Control > PIN Setting > Public PIN**
2. Tick the ☑ check box to enable the Public PIN code application
3. Set the PIN code digit limit ranging from "4-8" in Public PIN Bits Limit field
4. Enter the Public PIN codes.



Note:

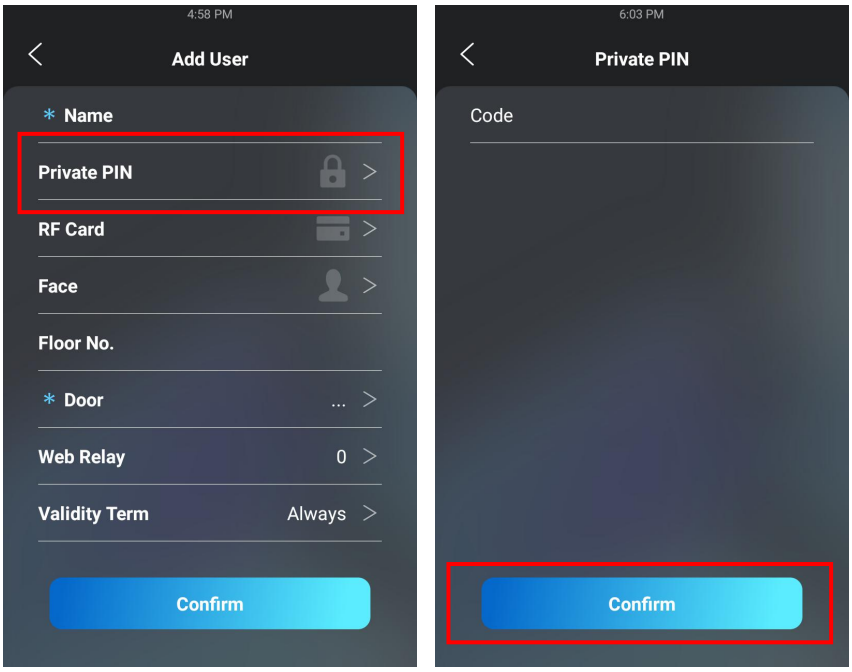
- Public PIN code will not valid until the function is turned on.

17.1.2. 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 private PIN code , you can do as follows:

1. Press **User** Icon on the **Setting** screen.
2. Press **Add** tab.
3. Press **Private Key** arrow .
4. Enter the **Private PIN** in the Code field.
5. Press **Confirm** tab for the validation.

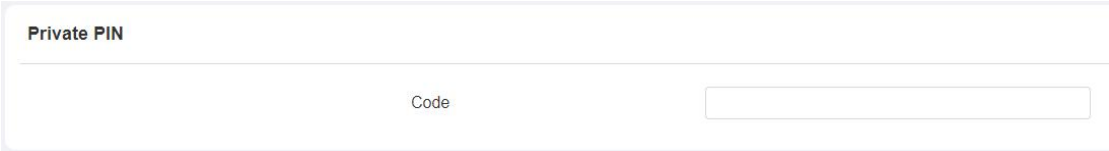


17.1.3. Configure Private PIN Code on the Web Interface

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.

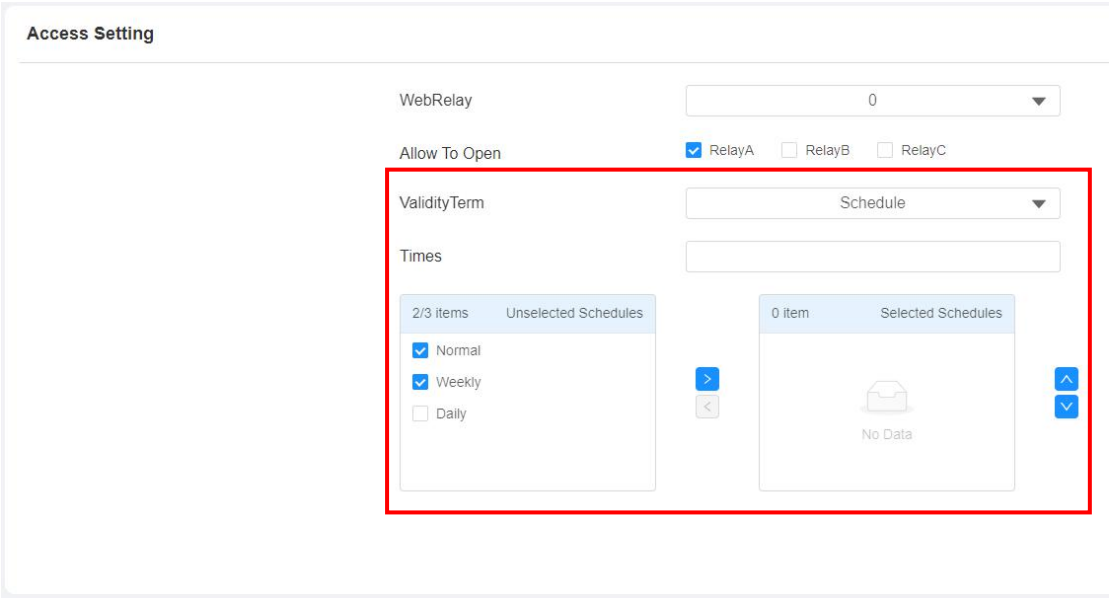
To configure PIN code , you can do as follows:

1. Click **Access Control > User**
2. Click the **Add** tab.
3. Go to **Private PIN** section.
4. Enter the private PIN code in **Code** field.
5. Click **Submit** tab for the validation.



To select door access Schedule for Private PIN Code door access, you can do as follows:

1. Go to **Access Setting** section in the same interface page
2. Set up PIN code validity time in the **Validity Term** field.
3. Select door access schedule for the targeted user(s).
4. Set the limit for the total times of PIN code door access.
5. Click the **Submit** tab for the validation.



Parameter Set-up:

- **Validity Term:** select validity term among three options: "**Always**", " **Schedule**" and " **Never**". if you select "**Always**", then the door access via PIN code will always be valid with no restriction. If you select **" Schedule"**, then you are required to select among the created schedule for user-based PIN code access. If you select **"Never"** than the PIN code access will never be valid.

- **Times:** set the total number of valid PIN code access allowed.

Note:

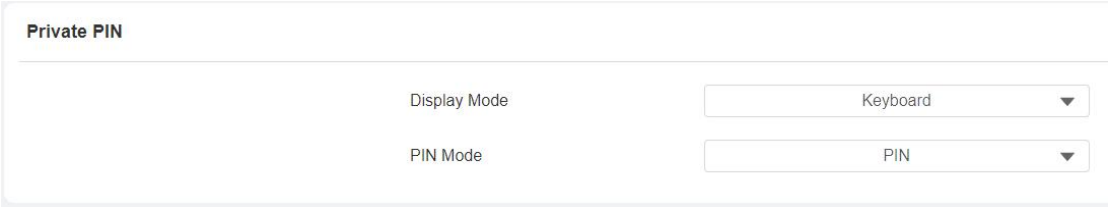
- This step is applicable to door access by RF card and Facial recognition as they are identical in configuration.

17.1.4. Configure Private PIN Access Mode

X915 series door phone offer you two types of access modes for private PIN code access, namely " **PIN**" and " **APT#+PIN**".

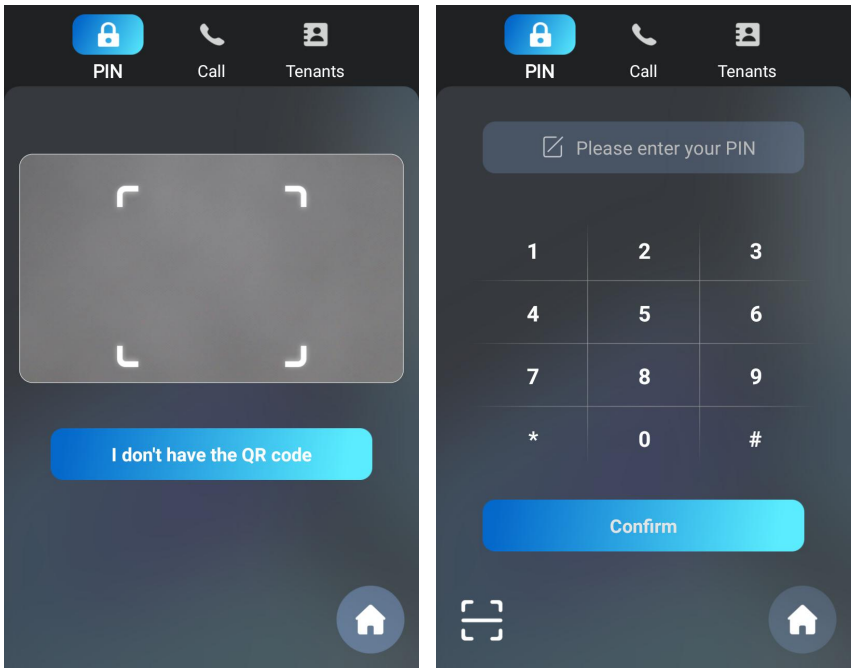
To configure the Display Mode, you can do as follows:

1. Click **Access Control > PIN Setting > Private PIN**
2. Click **Display Mode** field to select the display mode you need.
3. Click **Submit** tab for the validation and **Cancel** tab for the Cancellation.



Parameter Set-up:

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

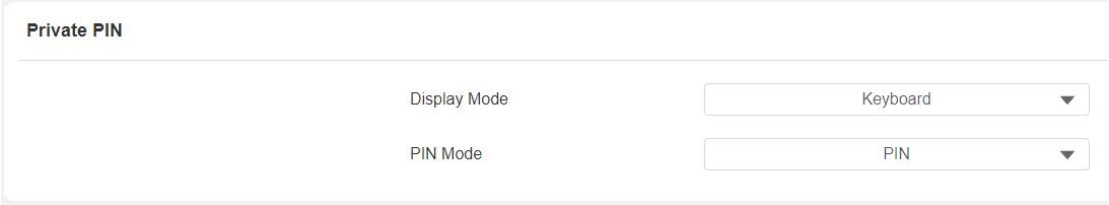


Note:

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

To configure the Display Mode and PIN Mode, you can do as follows:

1. Click **Access Control > PIN Setting > Private PIN**
2. Click **PIN Mode** field to select the display mode you need.
3. Click **Submit** tab for the validation and **Cancel** tab for the Cancellation.



Parameter Set-up:

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

Note:

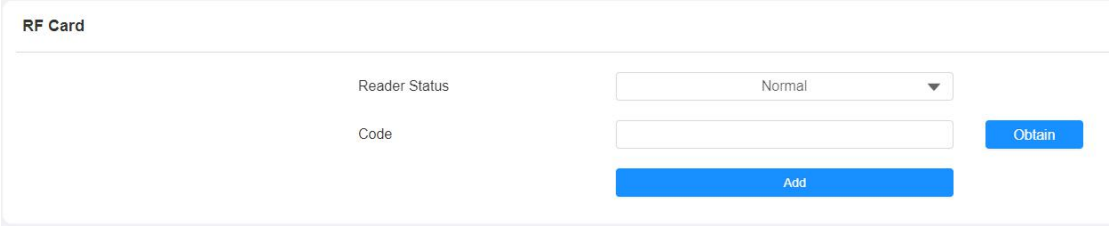
- **APT+PIN** can only be applicable when the device is added to the Akuvox SmartPlus.

17.2.Configure RF Card for Door Unlock

17.2.1. Configure RF Card on the Web Interface

To configure RF code , you can do as follows:

1. Click **Access Control > User > User**
2. Click the **Add** tab.
3. Go to **RF Card** section.
4. Click the **Obtain** tab and place the card on the card reader area.
5. Click the **Add** tab to add this card.



Note:

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

Note:

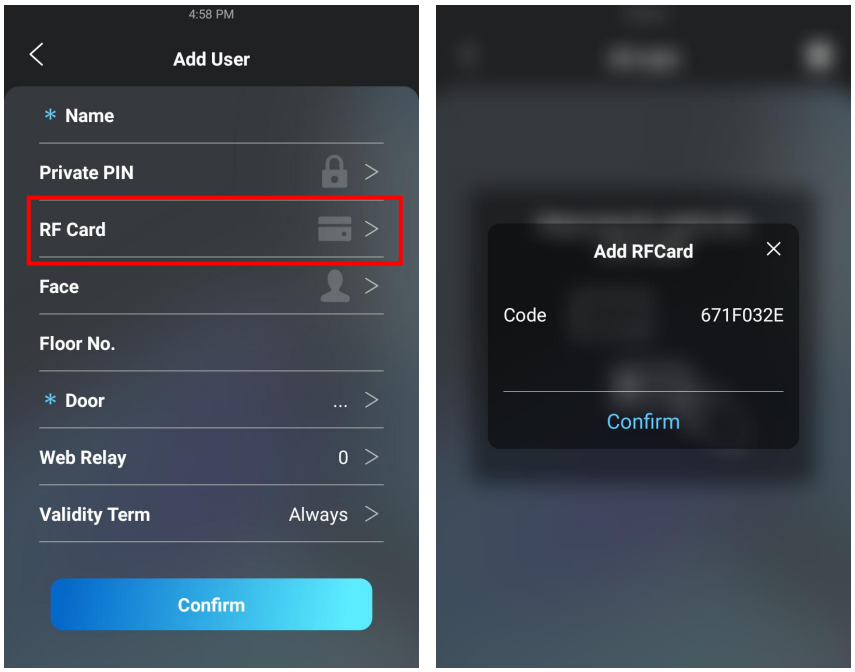
- RF card with 13.56 MHz and 125 KHz can be applicable to the door phone for the door access.

17.2.2. 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 trigger with RF card etc.

To configure facial recognition , you can do as follows:

1. Press **User** Icon on the **Setting** screen.
2. Press **Add** tab.
3. Press **RF Card** arrow .
4. Place your card on the card reader.
5. Press **Confirm** to add your card.

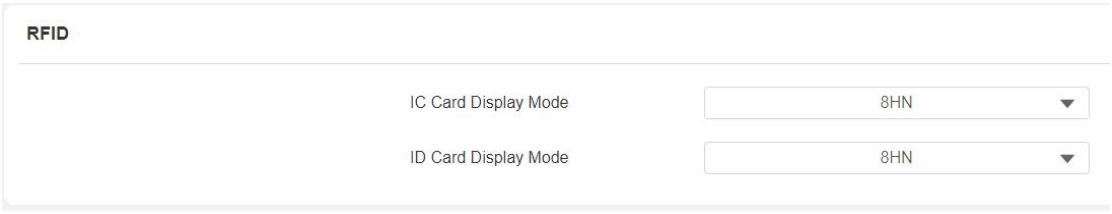


17.2.3. Configure RF Card Code Format

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 select the RF card format, you can do as follows：

1. Click **Access Control > Card Setting**
2. Click **IC Card Display Mode** field to select the IC Card Display Mode you need.
3. Click **ID Card Display Mode** field to select the ID Card Display Mode you need.



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; 8HR.** The card code format is 8HN by default in the door phone

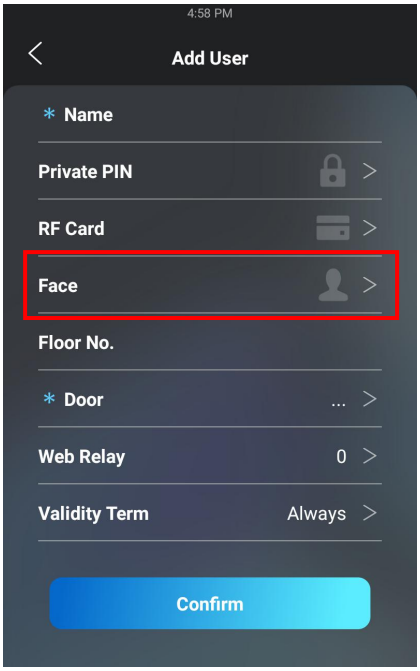
17.3.Configure Facial Recognition for Door Unlock

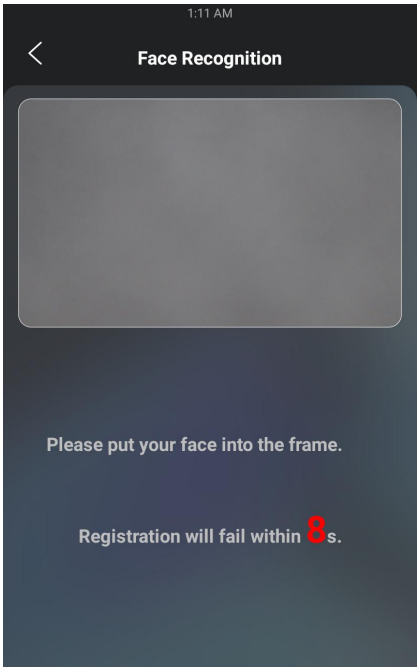
17.3.1. Configure Facial Recognition on the Device

You can configure door access by facial recognition on the device by entering the user's name and register your facial ID on the device for the door access.

To configure facial recognition , you can do as follows:

1. Press **User** Icon on the **Setting** screen.
2. Press **Add** tab.
3. Press **Face** arrow .
4. Stand in front of door phone camera in distance between 0.5 to 1 meter and keep your face in the center of square frame for ten seconds until your facial ID is successfully collected.
5. Press **Save** tab on the bottom to save the facial registration.



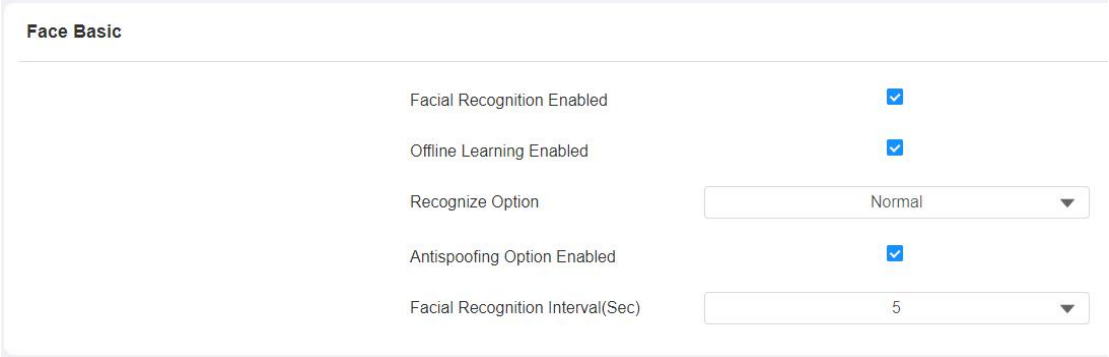


17.3.2. Configure Facial Recognition on Web Interface

X915 series door phone allow you to adjust facial recognition accuracy, recognition intervals according to your actual need. And you can also improve the recognition quality and user experience through the basic facial recognition setting.

To adjust the facial recognition, you do as follows:

1. Click **Access Control > Face Setting**
2. Set up the parameters for facial recognition accuracy and intervals etc.,.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



Parameter set-up:

- **Face Recognition:** click on "**Enable**" to turn on the facial recognition function. Facial recognition is enabled by default.
- **Offline Learning:** select "**Enable**" if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **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:** 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 the pictures of any kinds.

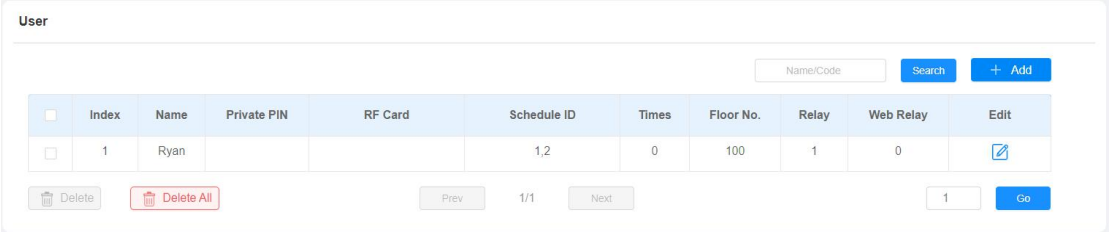
- **Facial Recognition Interval:** select time interval between every two facial recognition from 1-8 minutes. For example, if you select "**5**" then you have to wait for 5 min. before you are allowed to perform the facial recognition again.

17.4.Edit the User-specific door access data

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

To search and edit the user data, you can do as follows:

1. Click **Access Control > User**
2. Enter the search information in the **Search** field.
3. Click **Edit** tab to add the user data.
4. Tick the check box of the specific user if you want to delete the user or ticket the check box by the the **Index** to delete all the user data.

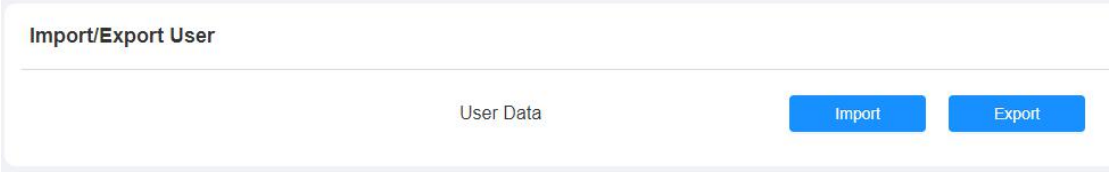


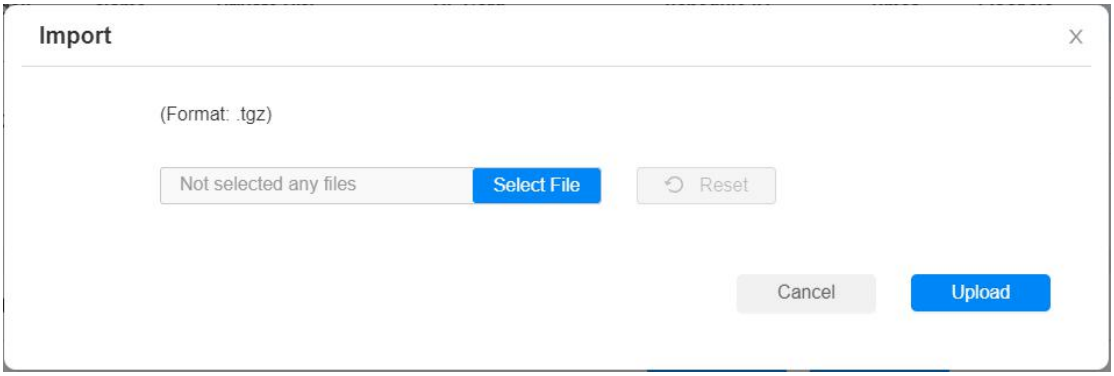
17.5.Import and Export User Data of Access Control

X915 series support User Data of access control to 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 to a third party device.

To import user data, you do as follows:

1. Click **Access Control > User > Import/Export User > Import**
2. Click **Select file** tab to upload your schedule data file.
3. Click **Reset** tab to clear the file you have selected.
4. Click **Upload** tab to start uploading the file and **Cancel** tab for the cancellation.





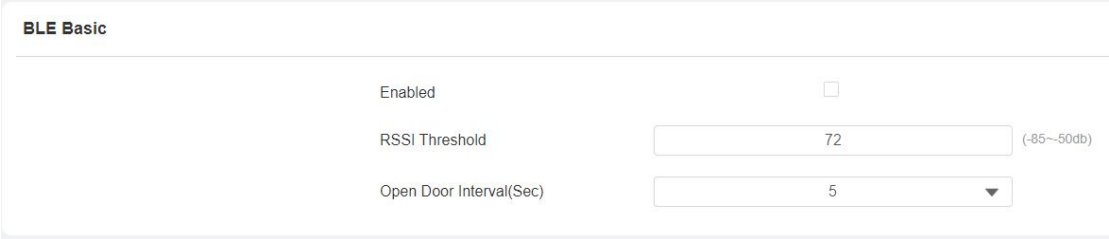
To import user data, you do as follows:

1. Click **Access Control > User > Import/Export User > Export**

17.6.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 the door access.

1. Click **Access Control > BLE**
2. Set up parameter according to your need.
3. Click on **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter Set-up:

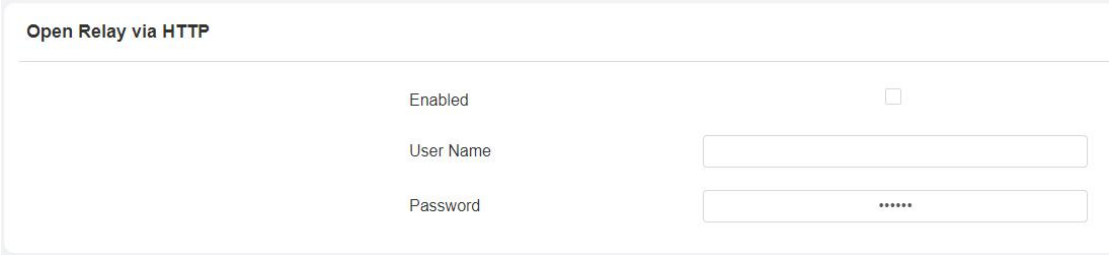
- **BLE Enable:** enable or disable the Bluetooth function. Bluetooth is turned off by default.
- **Rssi Threshold:** select the signal receiving strength from -85~-50db in absolute terms, The higher value it is , the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval(Sec):** select the time interval between the every two Bluetooth door accesses.

17.7.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 the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access.

To do the configuration, you can do as follows:

1. Click **Access Control > Relay > Open Relay via HTTP**
2. Set up parameters properly.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter Set-up:

- **Enable:** enable the HTTP command unlock function by clicking on **Enable** field.
- **User Name:** enter the user name of the device web interface, for example "**Admin**".
- **Password**: enter the password for the HTTP command. For example : "**12345**".

Please refer to the following example:

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

Note:

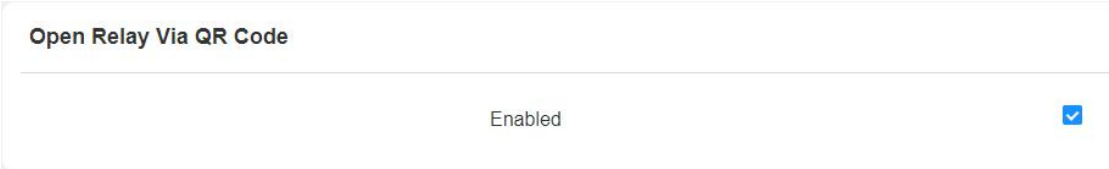
- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

17.8.Unlock by QR Code

QR code is another option for door access. If you want to apply QR code access, you need to enable the QR code function.

To enable the QR code function , you can do as follows:

1. Click **Access Control > Relay > Open Relay via QR Code**
2. Tick the check box to enable the QR code function
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



Note:

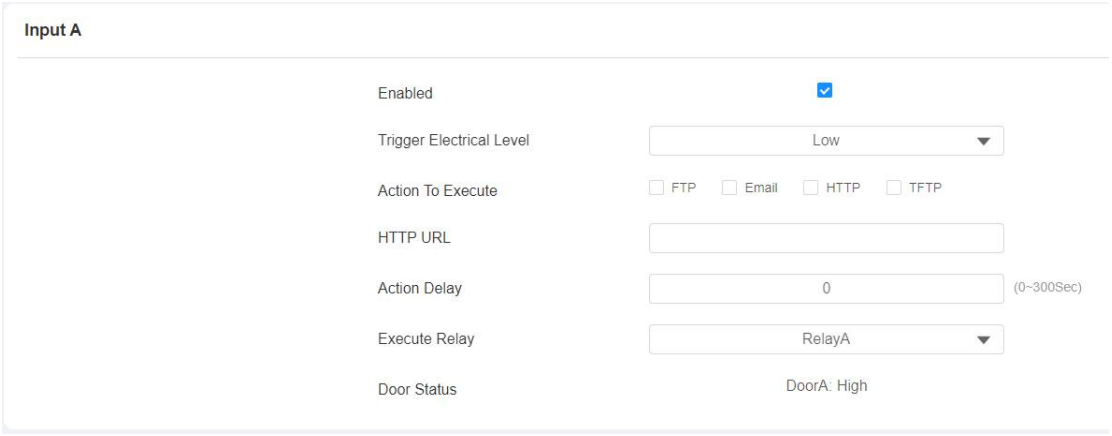
- The function should work with Akuvox cloud. For more information, please contact Akuvox technical support.

17.9.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 do the configuration, you can do as follows:

1. **Click Access Control > Input > Input**
2. Tick **Enabled** to enable the Input function.
3. Set up the parameters according to your need.
4. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter set-up:

- **Trigger Electrical Level:** select the trigger electrical level options between "H**igh**" and "L**ow**" according 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 sec., then the corresponding actions will be carried out 5 minutes after your press the button.

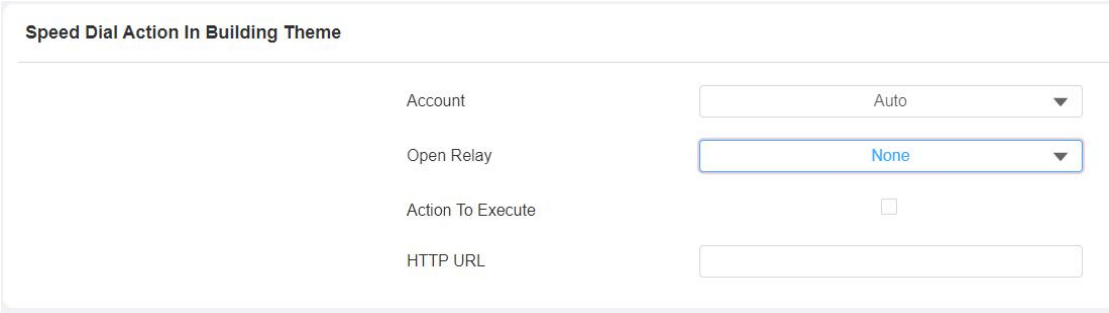
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

17.10. Configure Reception Tab for Door Unlock

In the device home screen, X915 series door phone provide residents and visitors a quick door access by pressing the **Reception** tab on the bottom of the home screen.

To do the configuration, you can do as follows:

1. Click **Intercom > Key/Display > Reception Action In Building**
2. Set the parameters properly.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



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:

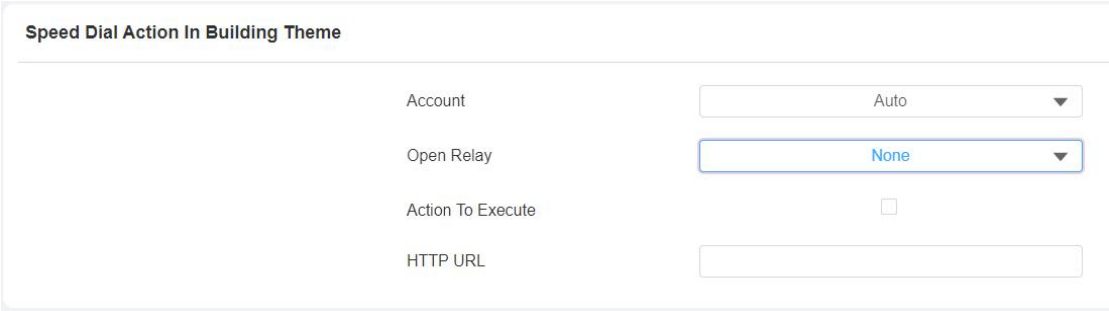
http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

17.11. Configure Reception Tab for Door Unlock

In the device home screen, X915 series door phone provide residents and visitors a quick door access by pressing the **Reception** tab on the bottom of the home screen.

To do the configuration, you can do as follows:

4. Click **Intercom > Key/Display > Reception Action In Building**
5. Set the parameters properly.
6. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



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

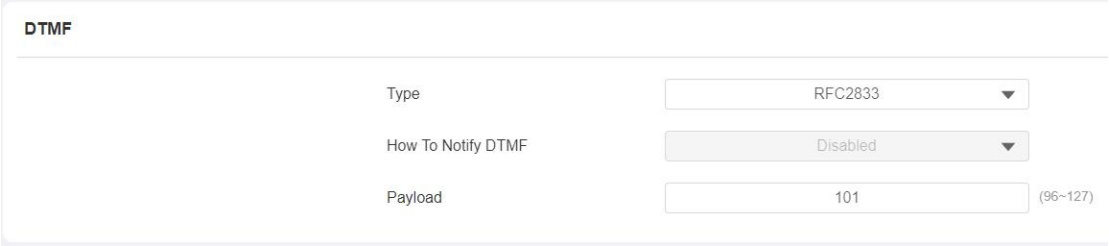
17.12. Unlock by DTMF code

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 do the extra DTMF configuration on the web interface, you can do as follows:

1. Click **Account > Advanced > DTMF**
2. Set up parameters properly.
3. Click **Submit** tab for the **validation** and Cancel tab for the cancellation.

Parameter Set-up:



- **Type:** select DTMF type among five options: **" Inband", " RFC2833", " Info+Inband" and "Info+RFC2833"** according to you 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 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.

18. Security

18.1.Tamper Alarm Setting

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

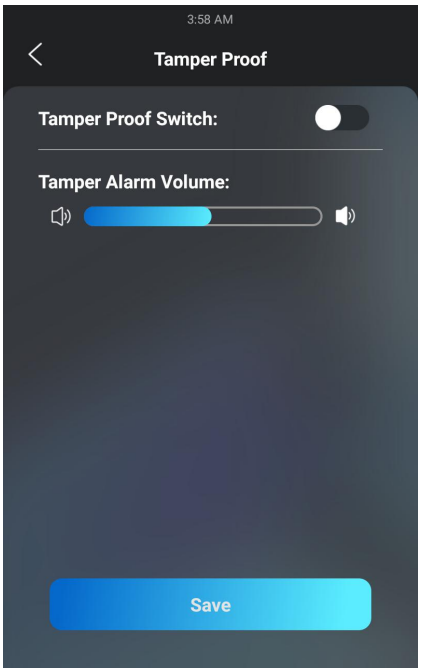
18.1.1. Configure Tamper Alarm on the Device

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 set up the temper alarm on the device , you can do as follows:

1. Press **Security** icon on the setting screen.
2. Press **Temper Proof** icon on the security screen.
3. Move the toggle switch on in **Tamper Proof Switch** to enable the temper alarm function.
4. Set the temper alarm volume according to your need.
5. Press **Save** tab for the validation and **Cancel** for the cancellation.

Please see the picture in the next page：

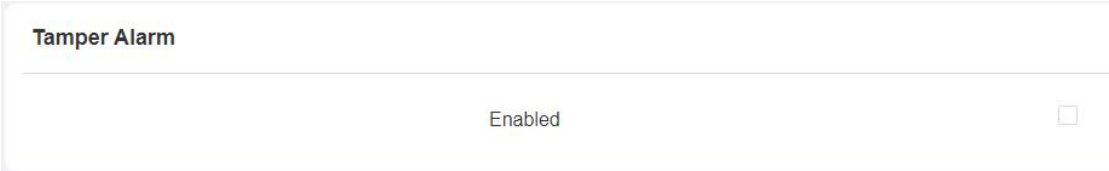


18.1.2. Configure Tamper Alarm on the Web Interface

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 do the configuration on the web interface, please do as follows:

1. Click **Security > Tamper Alarm**
2. Tick the check box to enable the anti-theft alarm function.
3. Click **Submit** tab for validation and **Cancel** tab for the cancellation.



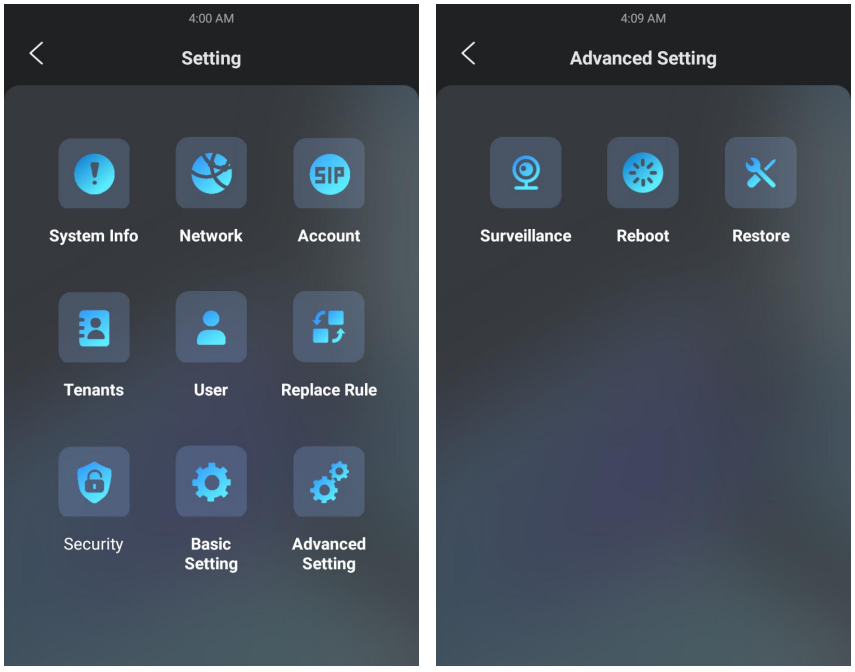
18.2. Motion Detection

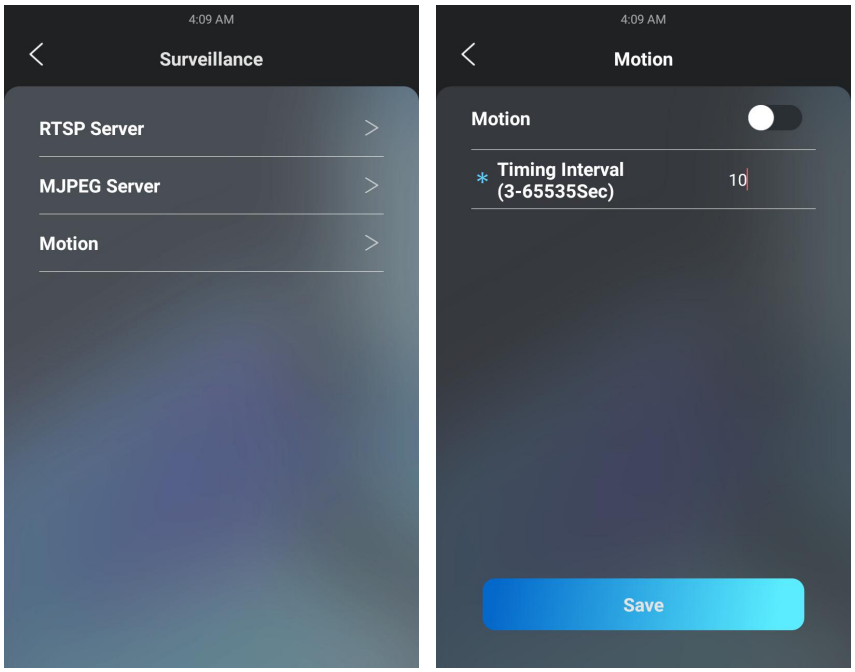
18.2.1. Configure Motion Detection on the Device

You can turn on the motion detection and set up the motion detection interval on the device.

To do so, you can do as follows:

1. Press **Advanced Setting** icon on the Setting Screen.
2. Press **Surveillance** icon on the Advanced Setting Screen.
3. Press **Motion** on the Surveillance Screen.
4. Move the toggle switch to switch on the motion detection function.
5. Set the Timing Interval to trigger the alarm.
6. Press **Save** tab to validate the setting.





Parameter set-up

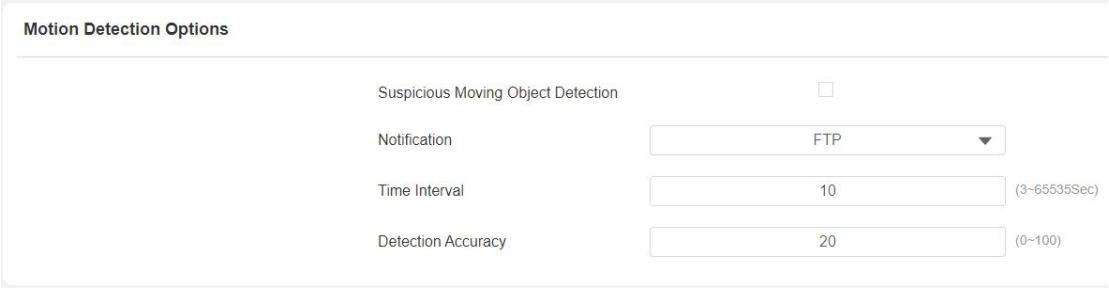
Interval: set the time interval for the motion detection. If you set the default time interval as "**10** "second, then the motion detection time span will be 10 seconds.Assuming that we set the time interval as "**10**" then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 second (the first trigger point) and motion detection action can be triggered (sending out notification) any where between **7-10** seconds once movement is detected."10"second 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"**

18.2.2. 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 do the configuration, you can do as follows:

1. Click **Surveillance > Motion > Motion Detection Options**
2. Set up parameters according to your need.
3. Click **Submit** for the validation and **Cancel** for Cancellation.



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**" than 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 away as you do on the device.

- **Detection Accuracy**: set the detection accuracy for the detection sensitivity. The small value it is , the greater sensitivity. the default detection accuracy value is "**20**".

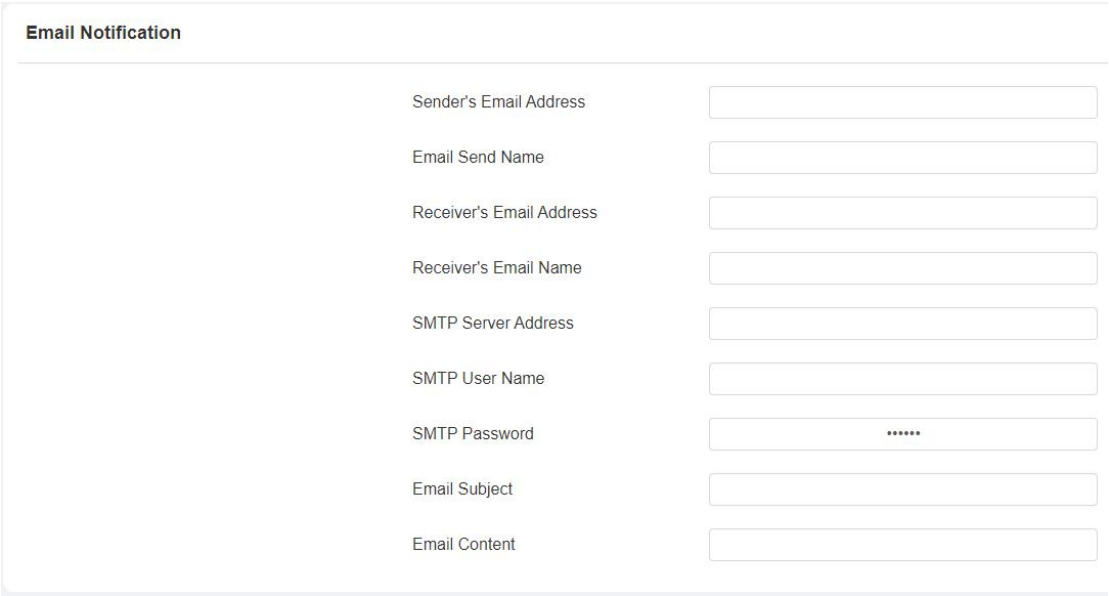
18.3.Security Notification Setting

18.3.1. Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web interface properly.

To do the configuration, you can do as follows:

1. Click **Setting > Action > Email Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for Validation and **Cancel** tab for cancellation.



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.

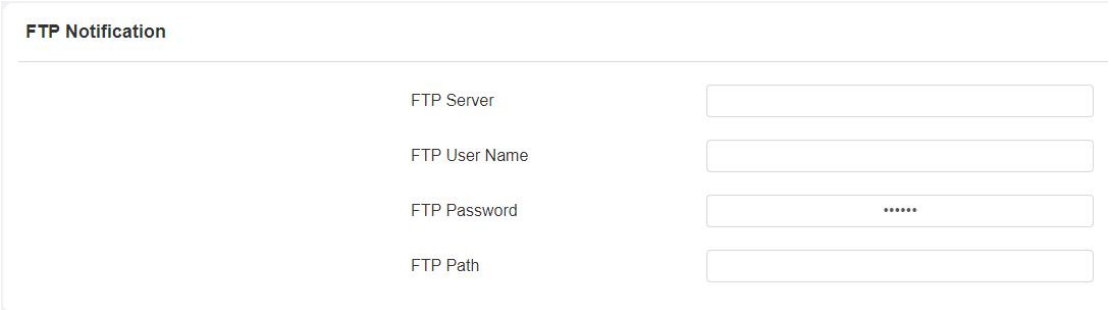
- **Receiver's Email Address:** enter the receiver's email address.
- **Receiver's Email Name:** enter the the name of the email receiver.
- **SMTP Server Address:**enter the SMTP server address of the sender.
- **SMTP User Name:** enter the SMTP user name, which is usually the same with sender's email 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 emails contents according to your need

18.3.2. FTP Notification Setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the web interface properly.

To do the configuration, you can do as follows:

1. Click **Setting > Action > FTP Notification**
2. Set up parameters properly according to your need
3. Click **Submit** tab for Validation and **Cancel** tab for cancellation



Parameter set-up:

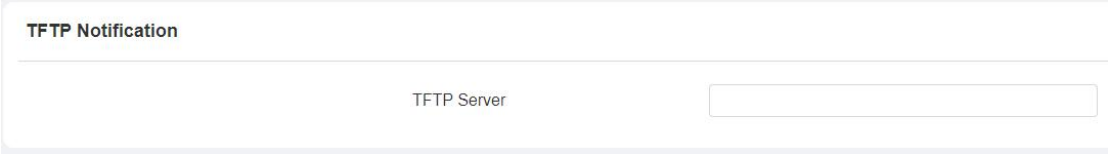
- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name**: enter the FTP server user name.
- **FTP Password**: enter the FTP server password.
- **FTP Path**: enter the folder name you created in FTP server.

18.3.3. TFTP Notification Setting

If you want to receive the security notification via TFTP, you can configure the FTP notification on the web interface properly.

To do the configuration, you can do as follows:

1. Click **Setting > Action > TFTP Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for Validation and **Cancel** tab for cancellation.



Parameter set-up:

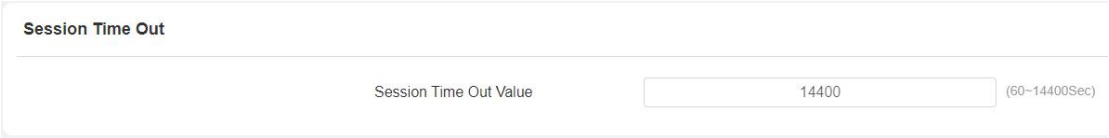
- **TFTP server**: enter the address (URL) of the TFTP server for the FTP notification

18.4.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 the security purpose or for the convenience of operation.

To configure the web interface time-out, you can do as follows:

1. Click **Security > Basic > Session Time Out**
2. Enter the time-out value in the **Session Time Out Value** field.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



19. Monitor and Image

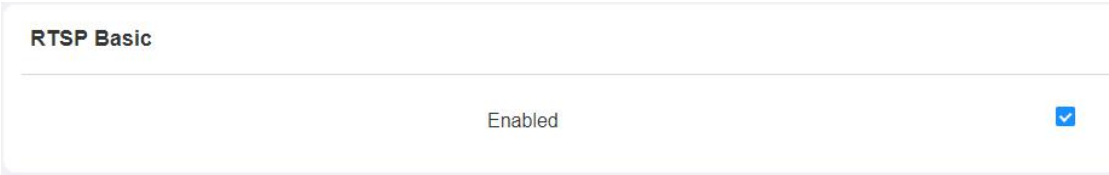
19.1.RTSP Stream Monitoring

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 the real time audio/ video (RTSP stream) from the door phone using the correct URL.

19.1.1. RTSP Basic Setting

To enable RTSP function, you can do as follows:

1. Click **Surveillance > RTSP > RTSP Basic**
2. Tick the check box to to turn on the RTSP function.
3. Click **Submit** tab for validation and **Cancel** tab for Cancellation.

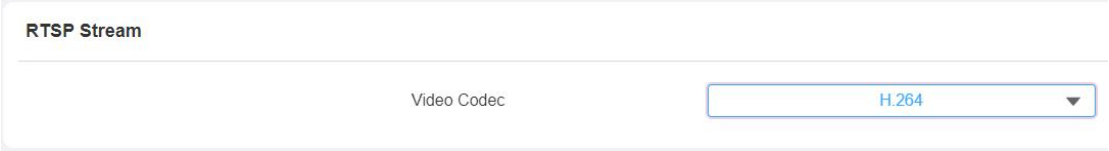


19.1.2. RTSP Stream Setting

You can select the video codec for the RTSP stream. You can also configure video resolution and bit-rate etc. for H.264 codec based on your actual network environment on the web interface.

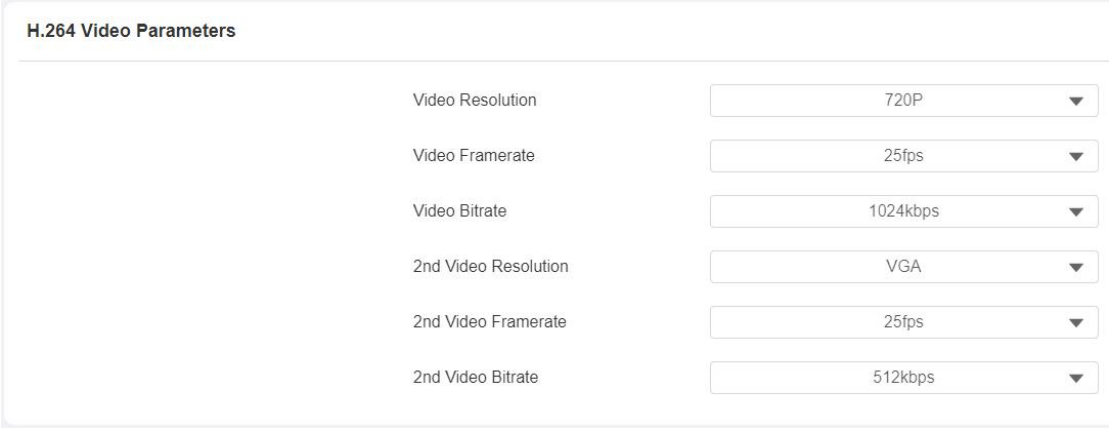
To select the video codec, please do as follows:

1. Click **Surveillance > RTSP > RTSP Stream**
2. Select the video codec according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



To configure the parameters for H.264 codec, please do as follows:

1. Click **Surveillance > RTSP > H.264 Video Parameters**
2. Set up video parameters according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: "**QCIF**", "**QVGA**","**CIF**","**VGA**","**4CIF**","**720P**,""**1080P**". The default video resolution is "**720P.** and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than "**720P**".

- **Video Framerate: "25fps"** is the video frame rate by default.

- **Video Bitrate**: select video bit-rate among six options: "**128 kbps**", "**256kbps**", "**512 kbps**", "**1024 kbps**", "**2048 kbps**", "**4096 kpbs**" according to your network environment. The default video bit-rate is " **2048 kpbs**".

- **2nd Video Resolution2**: select video resolution for the second video stream channel. While the default video solution is "**VGA**".

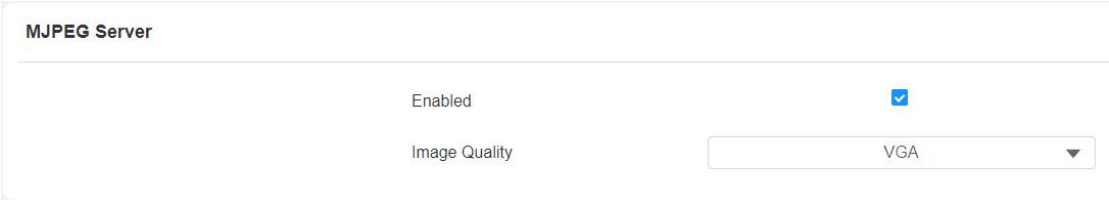
- **2nd Video Framerate**: select the video framerate for the second video stream channel. **"25fps"** is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate**: select video bit-rate among the six options for the second video stream channel. While the second video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

19.2.Mjpeg Image Capturing

X915 series allow you to capture the Mjpeg format monitoring image if needed. You can enable the Mjpeg function and set the image quality on the web interface.

To do the configuration, you can do as follows:

1. Click **Surveillance > Mjpeg**
2. Set the parameters properly according to your need.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



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 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 do as follows:

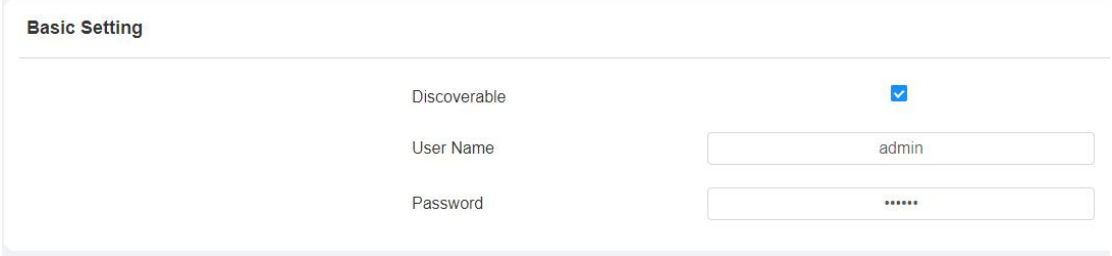
1. Enter "http://192.168.1.104:8080/picture.jpg" on the web browser
2. press Enter key in your keyboard to capture the image.

19.3.ONVIF

Real-time video from the X915 series door phone camera can be searched and obtained by the Akuvox indoor monitor or by the third party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function in the door phone so that other device will be able to see the video from the door phone.

To do the configuration, you can do as follows:

1. Click **Surveillance > ONVIF**
2. Set up parameters properly.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



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:

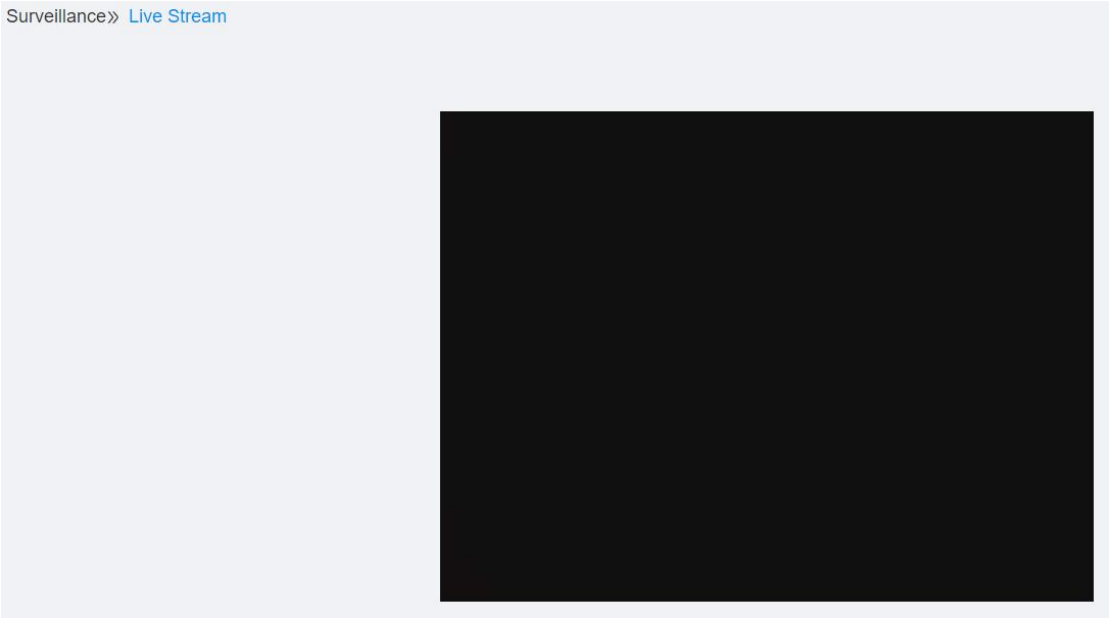
- Fill in the specific IP address of the door phone in the URL.

19.4.Live Stream

If you want to check the real-time video from the X915 series door phone, you can go to the the device web interface to obtain the real-time video or you can also enter the correct URL on the we browser to obtain it directly.

To check the real time video on the web interface, you can do as follows:

1. Click **Surveillance > Live Stream**
2. Check the real time video on the web interface.



To check the real time video using URL, you can do as follows:

1. Enter the correct URL (**http://IP_address:8080/video.cgi**) on the web browser if you want to obtain the real-time video directly with going to the web interface.
2. Check he real time video.

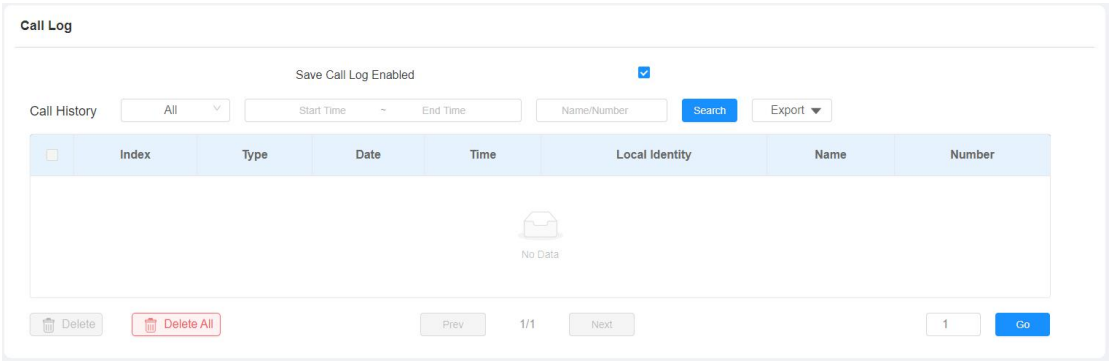
20. Logs

20.1. Call Logs

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

To check the call log, you can do as follows:

1. Click **Intercom > Call Log**
2. Set up parameters properly according to your need.
3. Click **Search** if you want to search call log of a specific contact SIP/ IP number.
4. Click **Export** tab if you want to export the call log.



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**" " **Missed**" for the specific type of call log to be displayed.
- **Start Time ~ End Time**:select the specific time span of the call logs you want to search, check or export.

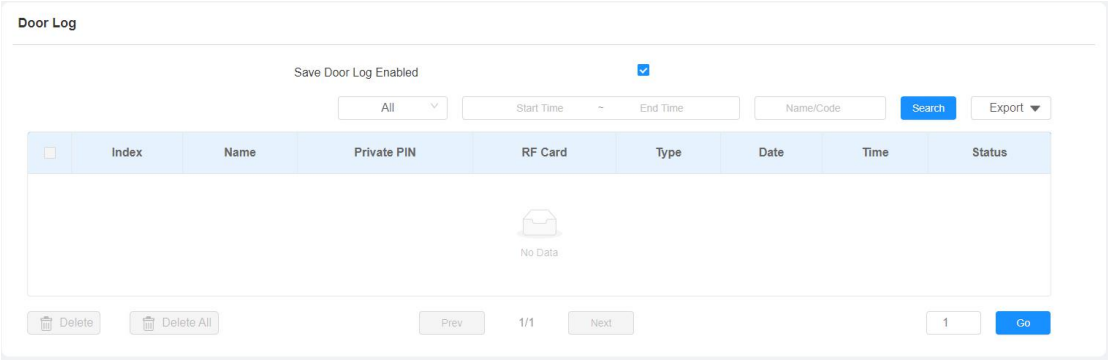
- **Name/Number**: select the "**Name**" and " **Number**" options to search call log by the name or by the SIP or IP number.

20.2.Door Logs

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

To access the door logs , you can do as follows:

1. Click **Access Control > Door log**
2. Set up parameters properly according to your need.
3. Click **Search** tab if you want to search door access by the name and PIN code.
4. Click **Export** tab if you want to export the door log.



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.

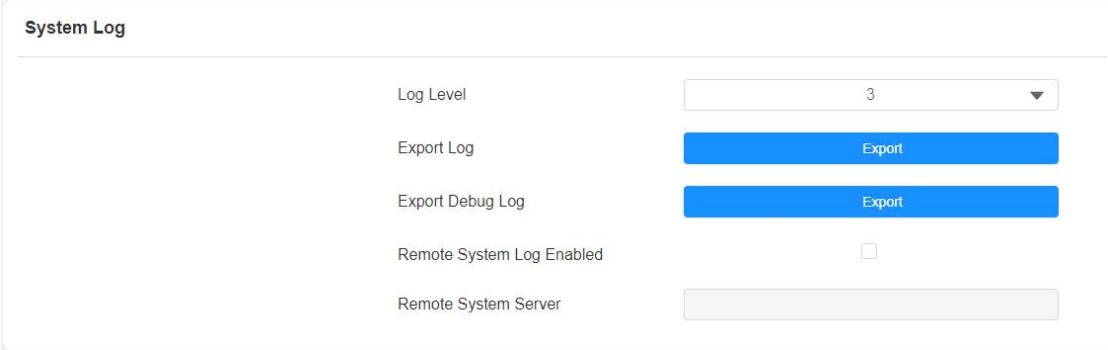
21. Debug

21.1.System Log for Debugging

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

To do the configuration, you can do as follows:

1. Click **Upgrade > Diagnose > System Log**
2. Set up parameters properly.
3. Reproduce the problem occurred.
4. Click **Export** tab to export logs.
5. Click **Submit** tab for validation and **Cancel** for cancellation.



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 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 wan to enable or disable the remote system log.

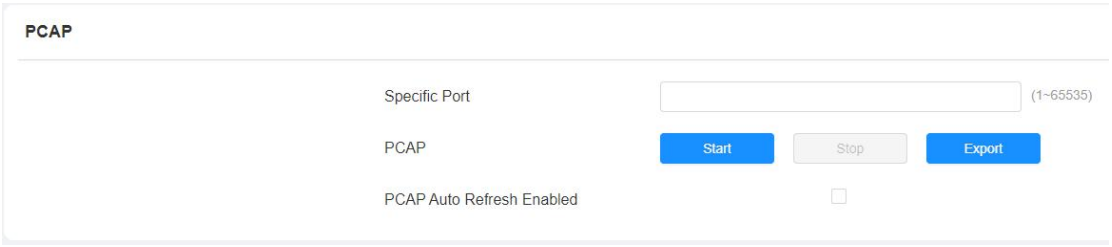
- **Remote System Server**: enter the remote server address to receive the the device **log.** And the remote server address will be provide by Akuvox technical support.

21.2.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 interface properly before using it.

To do the configuration, you can do as follows:

1. Click **Upgrade > Diagnose > PCAP**
2. Set up parameters properly.
3. Start PCAP data packets capturing by clicking on **Start** tab.
4. Stop PCAP data packets capturing by clicking on the **Stop** tab.
5. Export the data packets captured by PCAP by clicking on **Export** tab.



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 the a certain range of data packets before clicking **Export** tab to export the data packets to you Local PC.

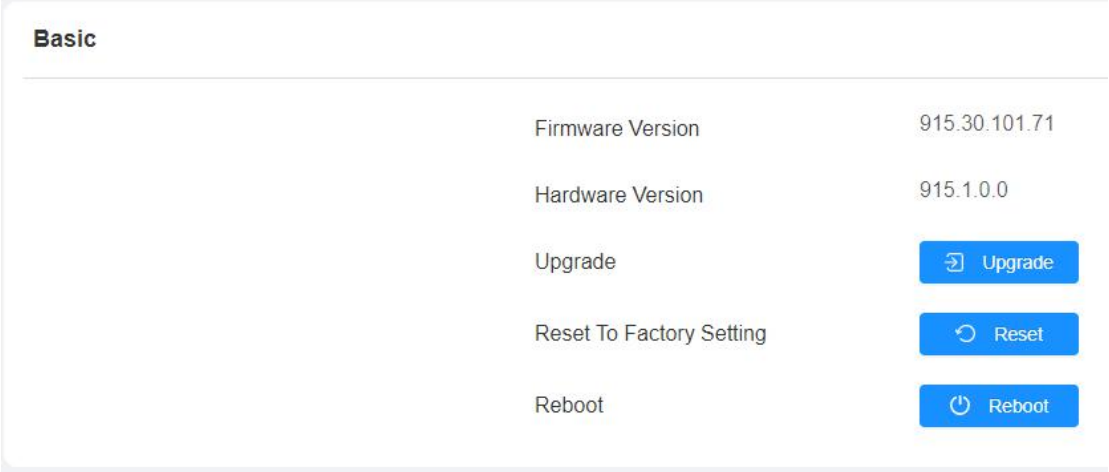
- **PCAP Auto Refresh**: select "**Enable**" or " **Disable**" to turn on or turn off the PCAP auto fresh function. If you set it as " Enable" then the PCAP will continue to capture data packet even after the data packets reached its 50M maximum in capacity. If you set it as " **Disable**" the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

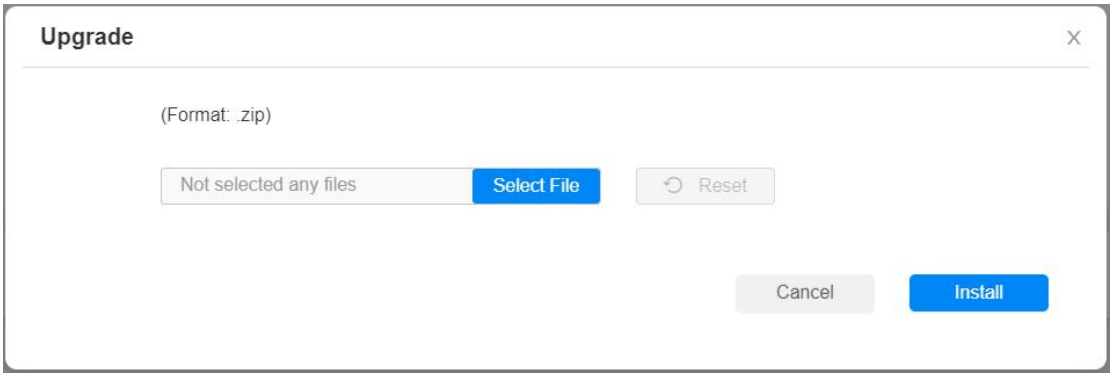
22. Firmware Upgrade

Firmwares of different versions for X915 series door phone can be upgraded on the device web interface.

To upgrade the firmware, you can do as follows:

1. Click **Upgrade > Basic**
2. Click **Upgrade** tab to select firmware files from your local PC.
3. Press **Install** tab for the validation and **Cancel** tab for the cancellation.





Note:

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

23. Backup

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

To do so , you can do as follows:

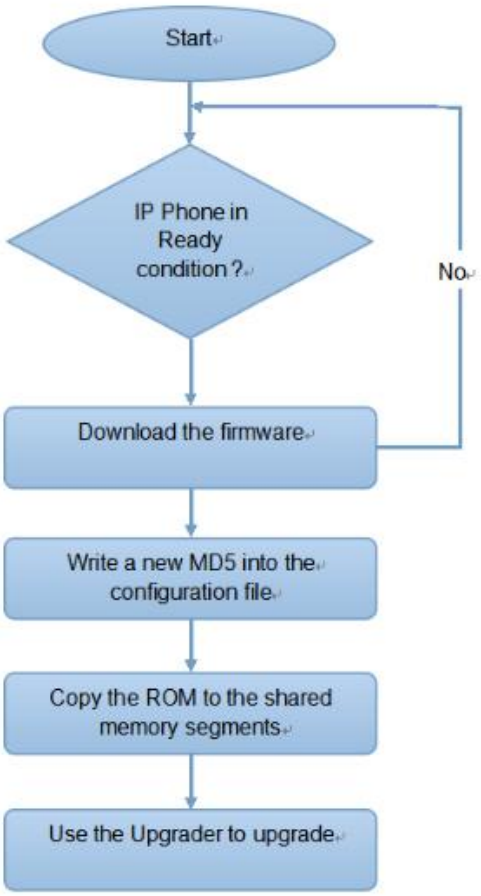
1. Click **Upgrade > Diagnose > Others**
2. Click **Import** tab if you want to import the selected config file.
3. Click **Export** tab if you want to export the existing config files to you local PC.

24. 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.

24.1.Provisioning Principle

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



24.2. Configuration Files for Auto-provisioning

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

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

- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example：r000000000915.cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files is used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.

Note:

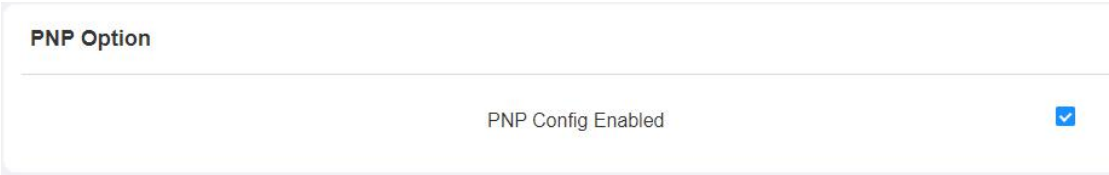
- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

24.3.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 configuratio n changes with little or no intervention by a user.

To enable PNP function , you can do as follows:

1. Click **Upgrade > Advanced > PNP Option**
2. Tick the check box to enable PNP function

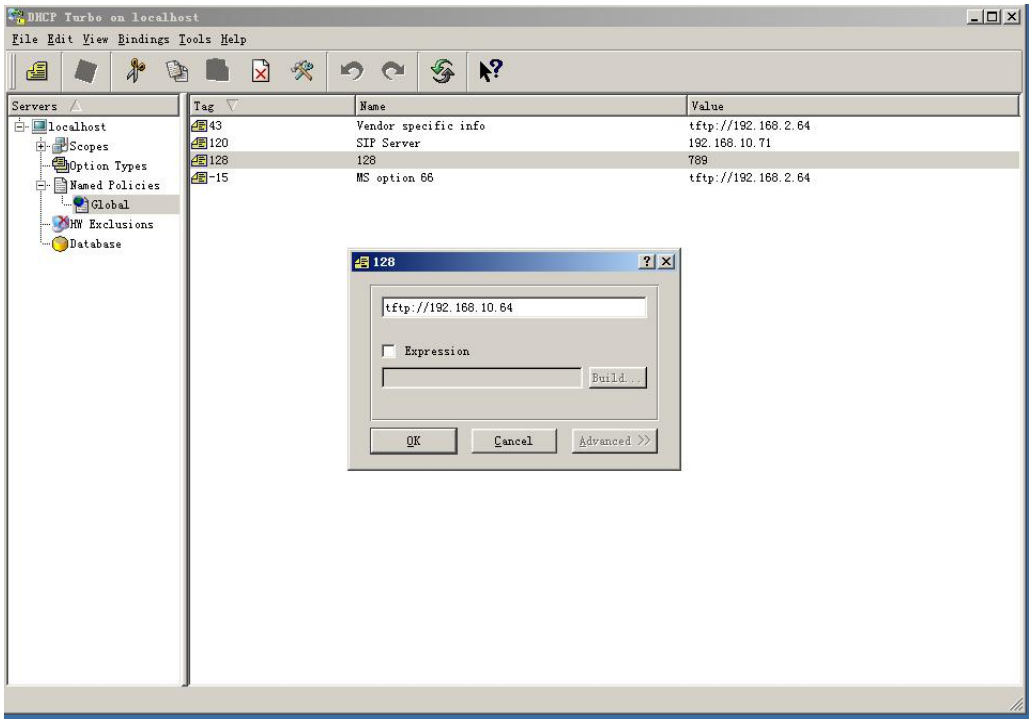


24.4.DHCP Provisioning Configuration

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

To set up DHCP AutoP with "Custom Option" and "Power on" mode, you can do as follows:

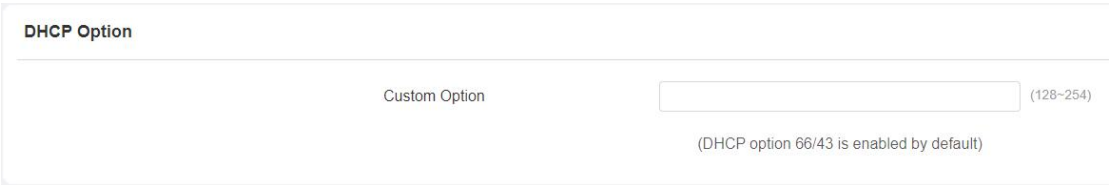
1. Set up DHCP Option on DHCP server



Note:

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

2. Rename the AutoP config template.
3. Select general provisioning configuration file for the device in-batch provisioning or the MAC-based configuration file for the specific device provisioning.
4. Go to **Upgrade > Advanced > DHCP Option** on the device web interface.
5. Enter the DHCP code in the **Custom Option field** for the URL to the config file server
6. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter set-up:

- **Custom Option**: enter the DHCP code that matched with 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 the 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 the option 43 with the update server URL in it.

Note:

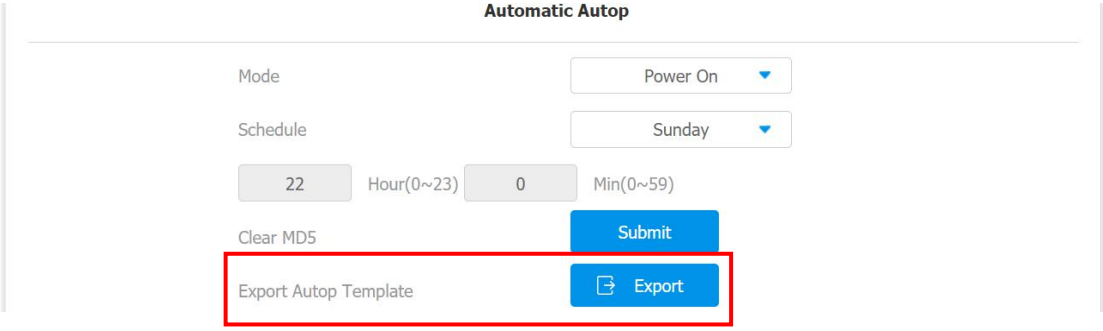
- The general configuration file for the in-batch provisioning is with the format "r**0000000000xx.cfg**" taking E16 as an example "r000000000016.cfg (10 "zeros" in total while the MAC-based configuration file for the specific device provisioning is with the format "MAC_Address of the device.cfg, for example "**0C110504AE5B.cfg.**"

24.5.Static Provisioning Configuration

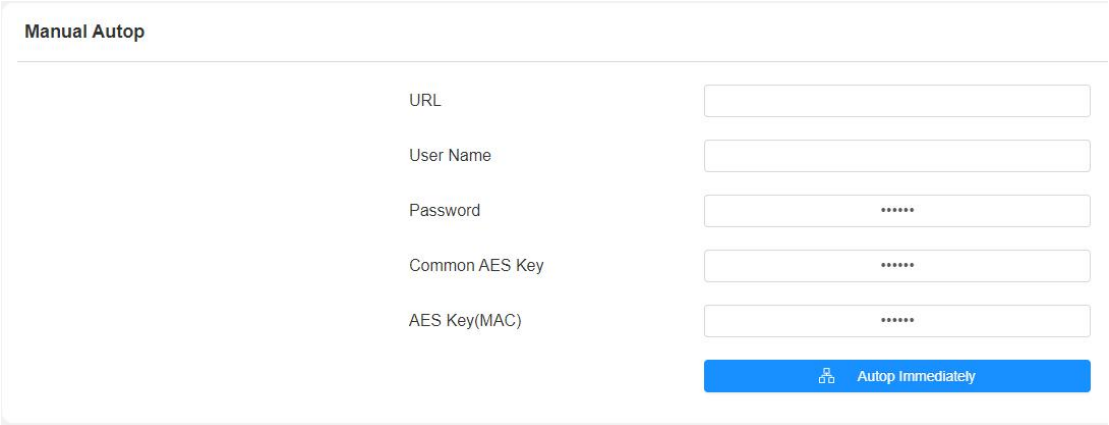
You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the door phone will perform the auto provisioning on a specific timing according to autop schedule you set up. In addition,TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.

To set up static provisioning autop, you can do as follows

1. Click **Upgrade > Advanced > Automatic Autop**
2. Click **Export** tab in **Export Autop Template** to export Autop template



3. Rename the AutoP config template
4. Select general provisioning configuration file for the device in-batch provisioning or the MAC-based configuration file for the specific device provisioning. (for example: r000000000**915** for X915)
5. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server;
6. Edit AutoP config template.
7. Upload the AutoP config template to DHCP/TFTP/FTP/HTTP/HTTPS server.
8. Go to **Upgrade > Advanced > Manual Autop** on the web interface.
9. Enter TFTP URL into the box(under the path "Upgrade-Advanced") and click 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 an user name to be accessed to otherwise leave it blank.
- **Password**: set up a password if the server needs a password to be accessed to otherwise leave it blank.
- **Common AES Key**: set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note:

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

Note:

Server Address format:

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

Tip:

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

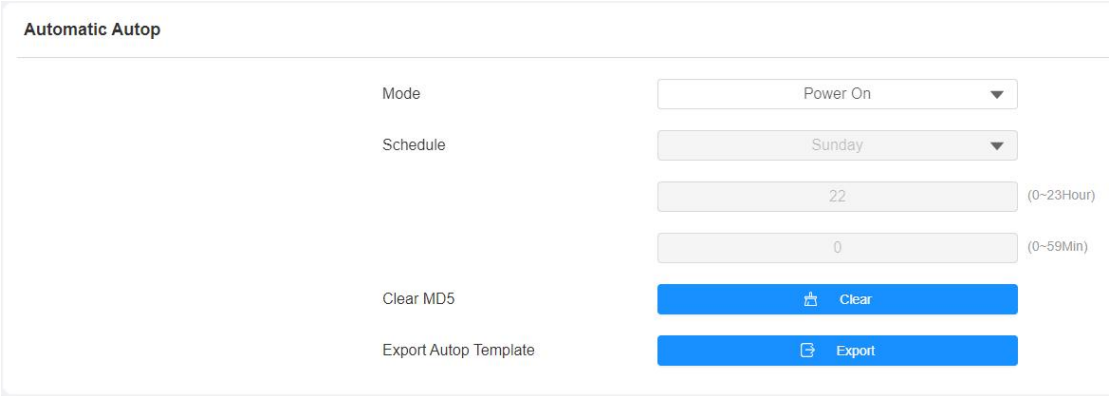
24.6.AutoP Schedule

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 set up the schedule, you can do as follows:

1. Click **Upgrade > Advanced > Automatic Autop**
2. Set up mode and schedule according to your need.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

Please see the picture below:



Parameter Set-up:

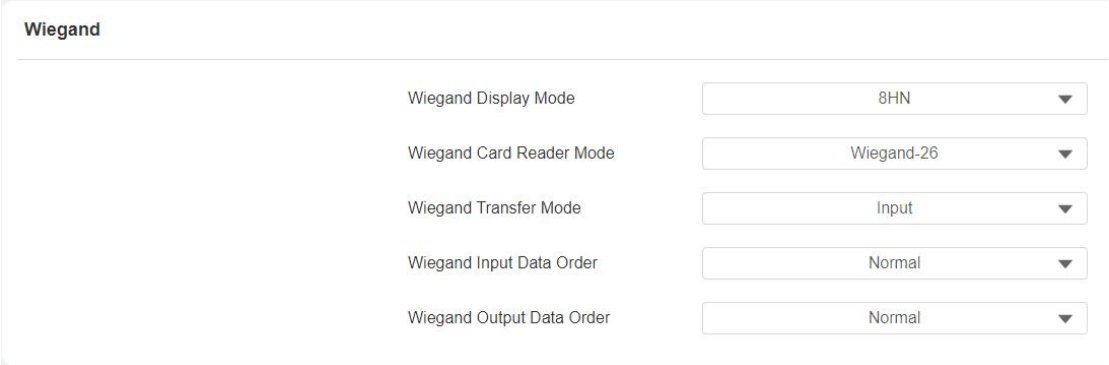
- **Mode:** select "**Power on**", " **Repeatedly**", "**Power On + Repeatedly**", "**Hourly Repeat**" as your Autop schedule.
  Select "**Power on**", if you want the device to perform Autop every time it boots up.
  Select " **Repeatedly**", if you want the device to perform Autop according to the schedule you set up.
  Select "**Power On + Repeatedly**", if you want to combine **Power On** Mode and **Repeatedly** mode that will 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.

25. Integration with Third Party Device

25.1.Integration via Wiegand

If you want to integrate the E16 series door phone with the third party devices via Wiegand, you can configure the Wiegand on the web interface.

1. Click **Access Control > Card Setting > Wiegand**
2. Set up parameters according to your need.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.



Parameter set-up:

- **Wiegand Display Mode：select Wigand 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 an 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 an vice versa.

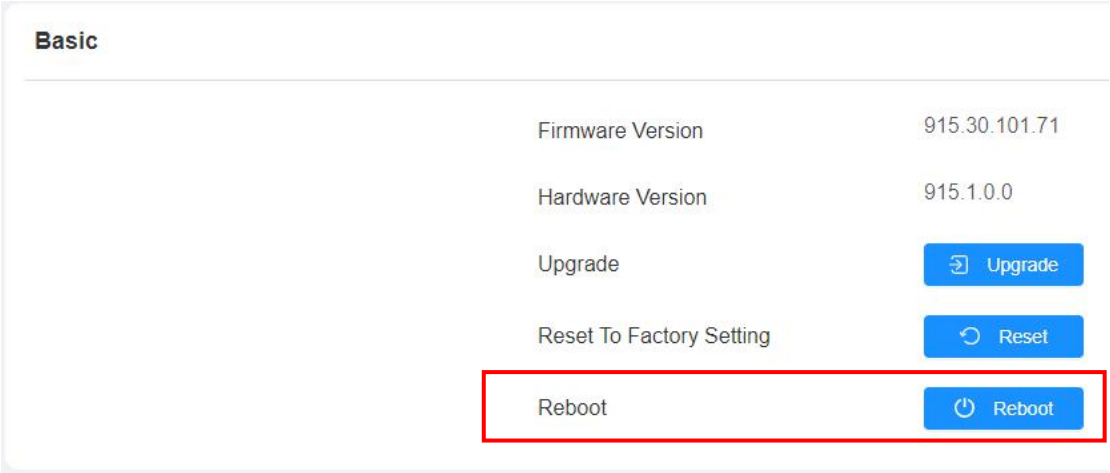
26. System Reboot&Reset

26.1.Reboot

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

To restart the system setting on the web interface, you can do as follows:

1. Click **Upgrade > Basic**
2. Click on **Reboot** tab for restarting the device.

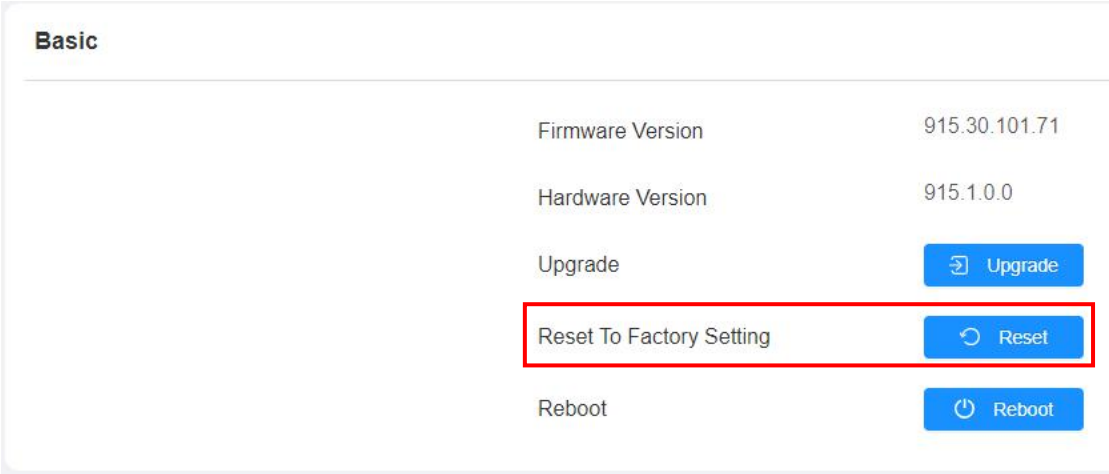


26.2.Reset

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

To reset to the factory setting, you can do as follows:

1. Click **Upgrade > Basic**
2. Click on **Reset** tab for Reset to Factory Setting.



27. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical 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

SNMP: 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

28. FAQ

Q1: How to obtain IP address of R2X
A1: ✔ For devices with 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 into 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 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 -- 32º~104ºF(0~40ºC)

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;
3. After you export , you need to unzip the .tgz folder , then make the unziped folrder into .zip again.

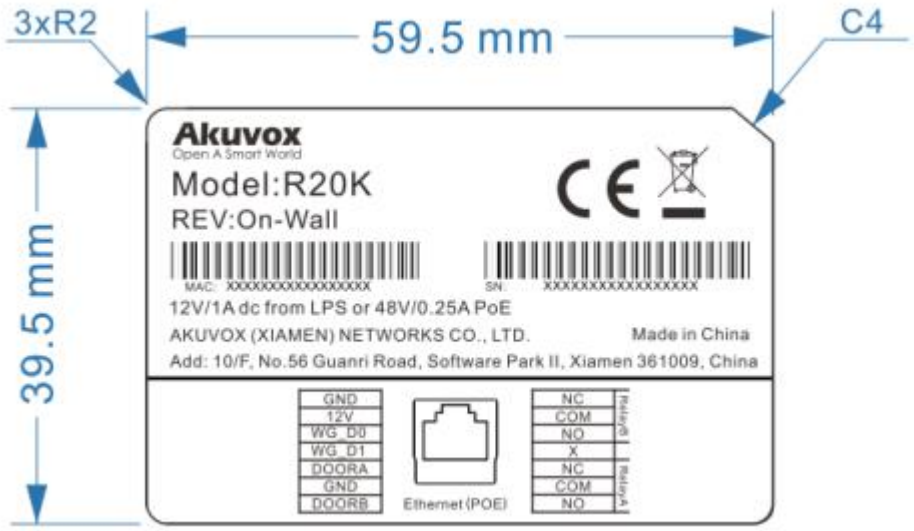
Q55: Which version of ONVIF does R20 and X915 support?
A55: Onvif 18.04 profiles

Q6: Do door phones support these card types? Prox, Legacy iClass,iClassSE,HID Mifare, HID DESFire,HID SEOS
A6: Sorry, they are not supported. They need to be implemented via hardware modifications.

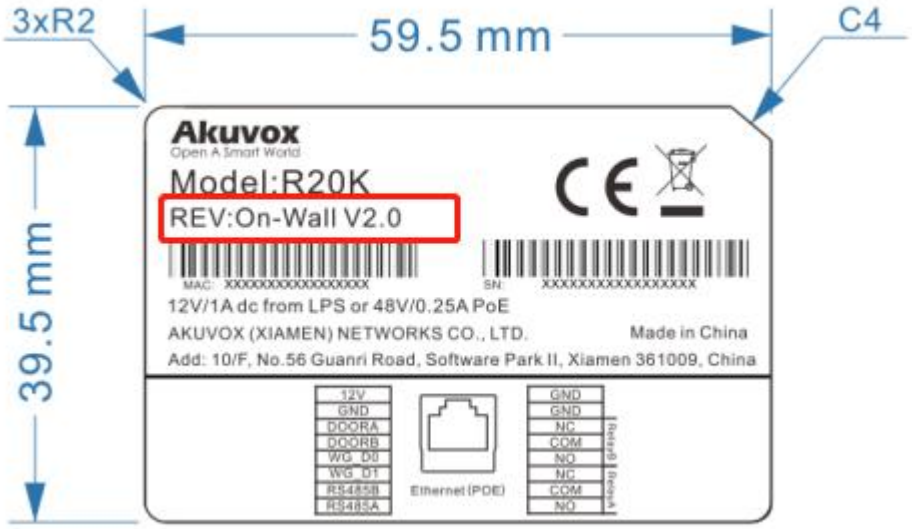
Q7: How to confirm whether my device is hardware version 1 or hardware version 2?

A7: 1.Label

- **Hardware version 1**



- **Hardware version 2**

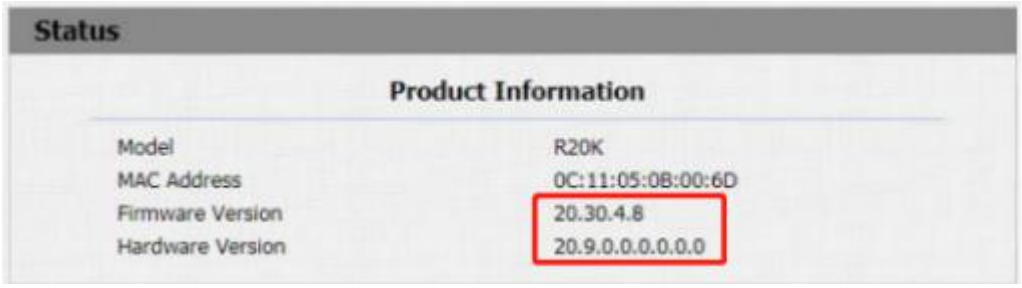


- **Firmware Version**

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.



29. Contact us

For more information about the product, please visit us atwww.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.