About This Manual

Thank you for choosing the Akuvox S539 series door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to version 539.30.1.7, and it provides all the configurations for the functions and features of the S539 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Introduction of Icons and Symbols

Note:

- Informative information and advice from the efficient use of the

Related Documentation

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

https://knowledge.akuvox.com

Content

1. Product Overview

Akuvox S539 series products are Android-based IP video door phones with touch screens. It incorporates audio and video communications, access control, and video surveillance.

Its finely tuned Android OS, Cloud, and AI-based communication technology allow featured customization to better suit your operation habit. S539 series multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controllers and fire alarm detectors, helping to create a holistic control of the 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. S539 series door phones are 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

	S539
Model & Feature	
Display	10 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	IP66
IK Rating	IK08
Temperature detection	Optional
Face recognition	√
LTE	X
USB	X
External SD card	X
Wall Mounting	√

Flush Mounting	√
Desk Mounting	X
Wall Mounting Dimension	367.5x183x35.5mm
Wall Mounting Dimension	363.5x179.8x64mm
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. Introduction to Configuration Menu

- **Status:** this section gives you basic information such as product information, Network Information, call log, and door log,
- **Account**: this section concerns the SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, et
- **Network**: this section mainly deals with DHCP&Static IP setting, RTP port setting, device deployment, etc.
- **Intercom**: this section covers Intercom settings, call features, dial plans, etc.
- **Surveillance**: this section covers Motion Detection, RTSP, MJPEG, ONVIF, Live stream, etc.
- **Access Control**: this section covers input control, relay, card settings, face recognition settings, Private PIN codes, etc.
- **Directory:** this section involves user management, RF card, PIN, Face recognition management, and contact management.
- **Device**: this section includes light settings, LCD settings, audio settings, lift control, Wiegand
- **Settings**: this section includes time, language, action settings, schedule for access control, Screen display, and HTTP API.
- **System:** this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault Diagnosis, security, PCAP, system log, web call, temper alarm, and password modification.

- **Mode selection:**

1. **Discovery mode**: It is a plug-and-play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to the network. It is a super time-saving mode, and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations by the administrator.

2. **Cloud mode:** Akuvox SmartPlus is an all-in-one management system. Akuvox Cloud is a mobile service that allows audio, video, and remote access control between smartphones and Akuvox intercoms. All configurations in the device will be issued automatically from the cloud. If users decide to use Akuvox SmartPlus, please contact Akuvox technical support, and they will help you configure the related settings before using it.
3. **SDMC mode**: SDMC (**SIP Device Management Controller**) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for door access, intercom, monitoring, alarm, and so on. It is a convenient tool for property managers to manage, operate and maintain the community.

- **Tool selection**

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

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

3. **Akuvox PC Manager**: Distribute all configuration items in batch on a LAN.

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

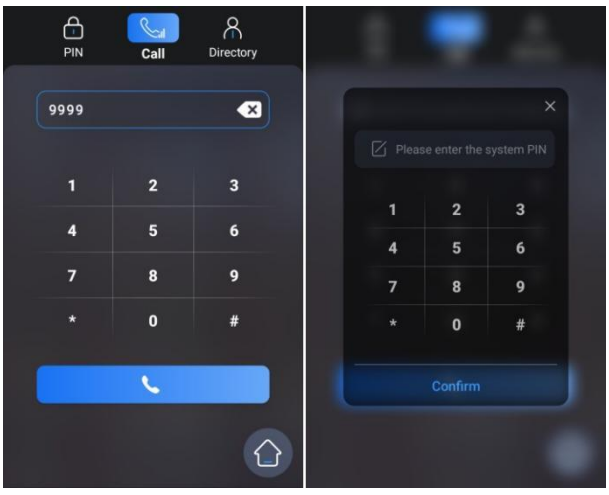
5. **FacePro**: Manage face data in batch for the door phone on a LAN.

5. Access the Device

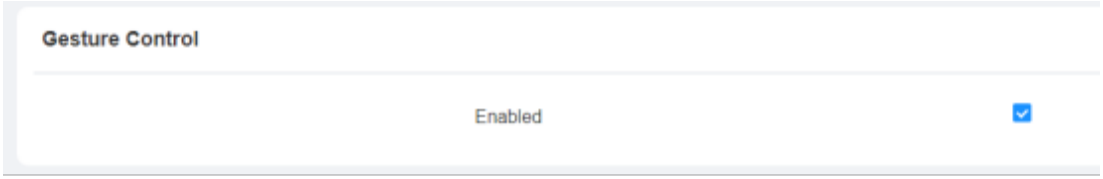
S539 series door phones' system settings can be either accessed on the device directly or on the device web interface.

5.1. Access the Device Setting on the device

Before configuring Akuvox S539, please make sure the device is installed correctly and connected to a normal network. Using the Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to login into the web browser by user name and password **admin** and **admin**. Or set up some basic settings on the device screen by pressing **9999** + **Dial** key + **3888** (password) on the **Dial** screen.

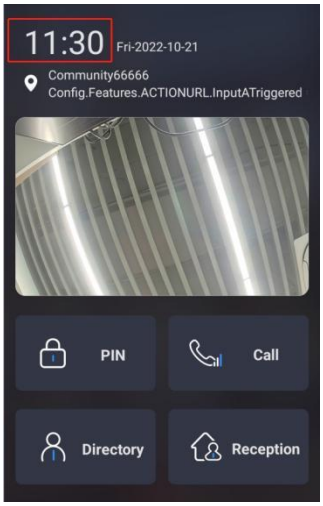


In certain application scenarios where the dial icon is missing on the screen, you can still access the device setting using the gesture control feature. You can navigate to **System > Security > Gesture Control**.


Gesture Control
Enabled

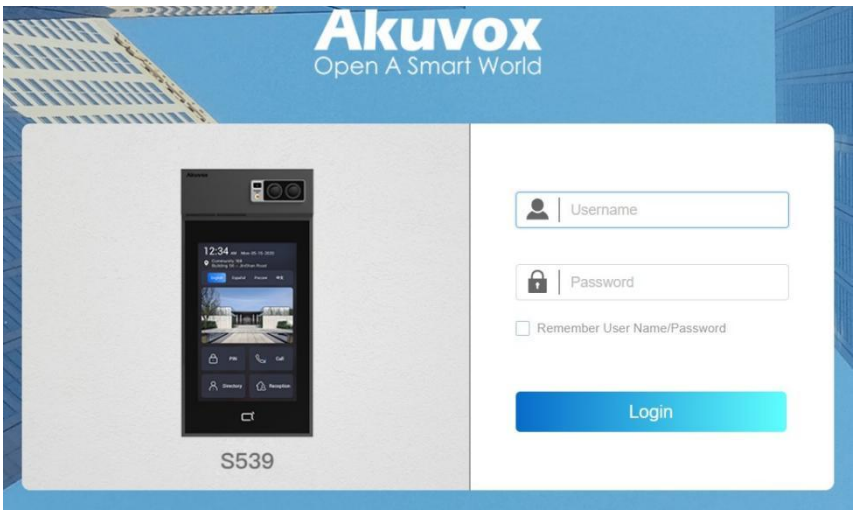
Parameter Set-up:

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



5.2. Access the Device Setting on the Web Interface

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



Note

- You can also obtain the device IP address using the Akuvox IP scanner to log in to the device web interface. Please refer to the URL below for the IP scanner application:

Note

- Google Chrome browser is strongly recommended.
- The initial user name and password are **admin** and please be case-sensitive

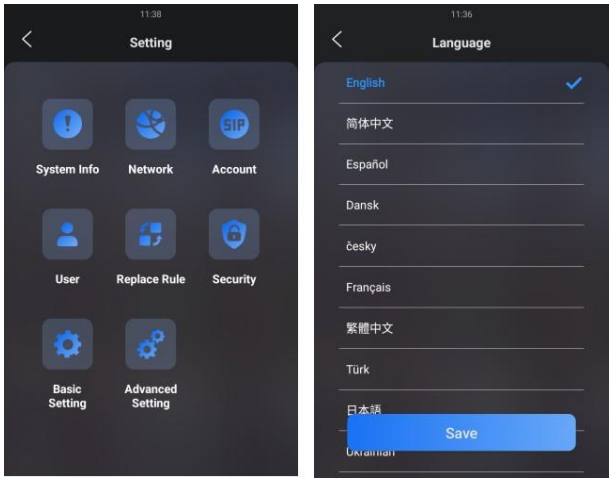
6. Language and Time Setting

6.1. Language Setting

When you first set up the device, you might need to set the language that you 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.

6.1.1. Language Setting on the Device

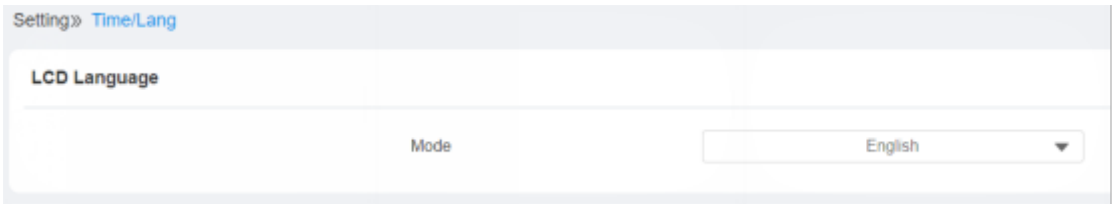
The language setting can be configured on the device or on the device web interface so that you can select or change the language for screen display to your preference. To configure the language display on the device **Basic Setting > Language** interface.



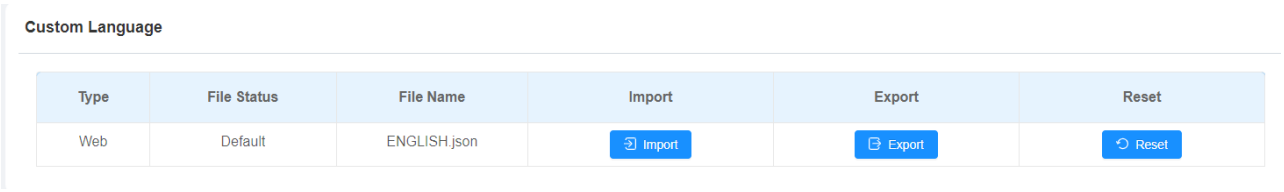
6.1.2. Language Setting on the Device Web Interface

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

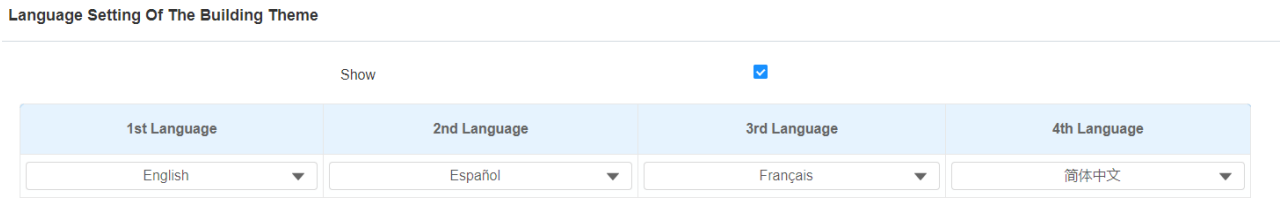
To select the device language, go to **Setting > Time/Lang > LCD Language** interface.



To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device. Path: **Setting > Time/Lang**.



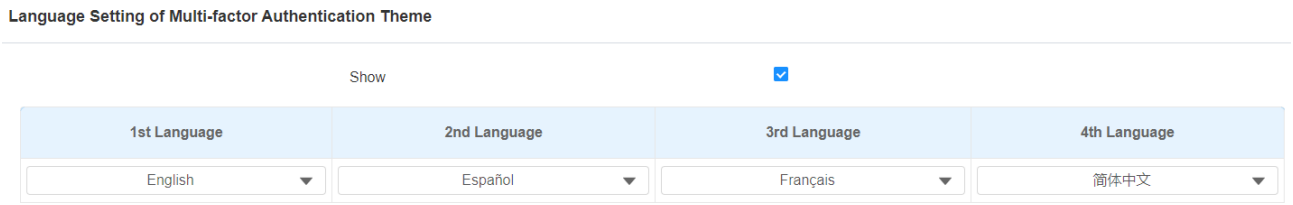
To create the language icons for the building mode, go to **Setting > Key/Display > Language Setting Of The Building Theme.**



Note

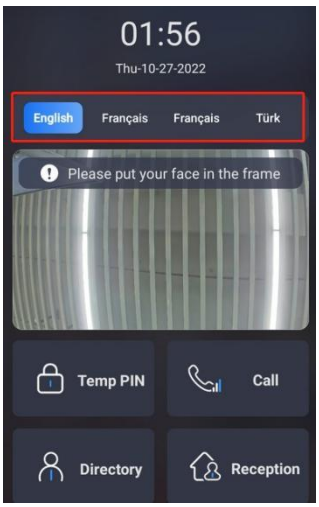
You need to select the building mode or multi-factor authentication mode first before you can set the language icon on the home screen for them.

To create the language icons for the multi-factor authentication mode, go to **Setting > Key/ Display > Language Setting of Multi-factor Authentication Theme**.



Parameter Set-up:

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

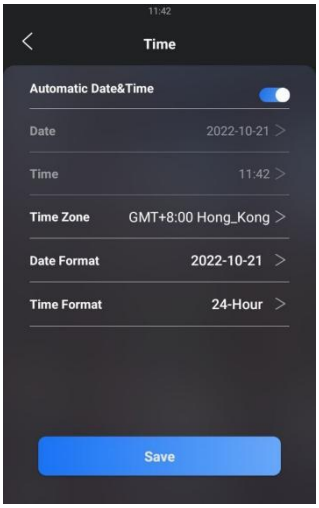


6.2. Time Setting

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

6.2.1. Time Setting on the Device

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



Parameter Set-up:

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

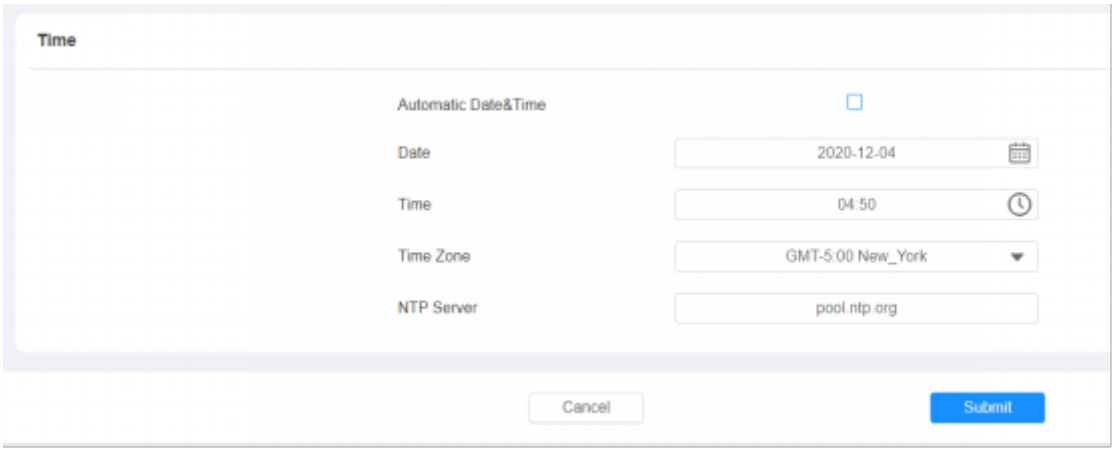
- **Time Format**: you can either select the 12-hour or 24-hour time format as you like and then press the **Confirm** tab for confirmation.

Note

- When the **Automatic Date&Time** toggle switch is toggled off, parameters related to the NTP server will become not editable. And when the switch is

6.2.2. Time Setting on the Device Web Interface

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



Parameter Set-up:

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

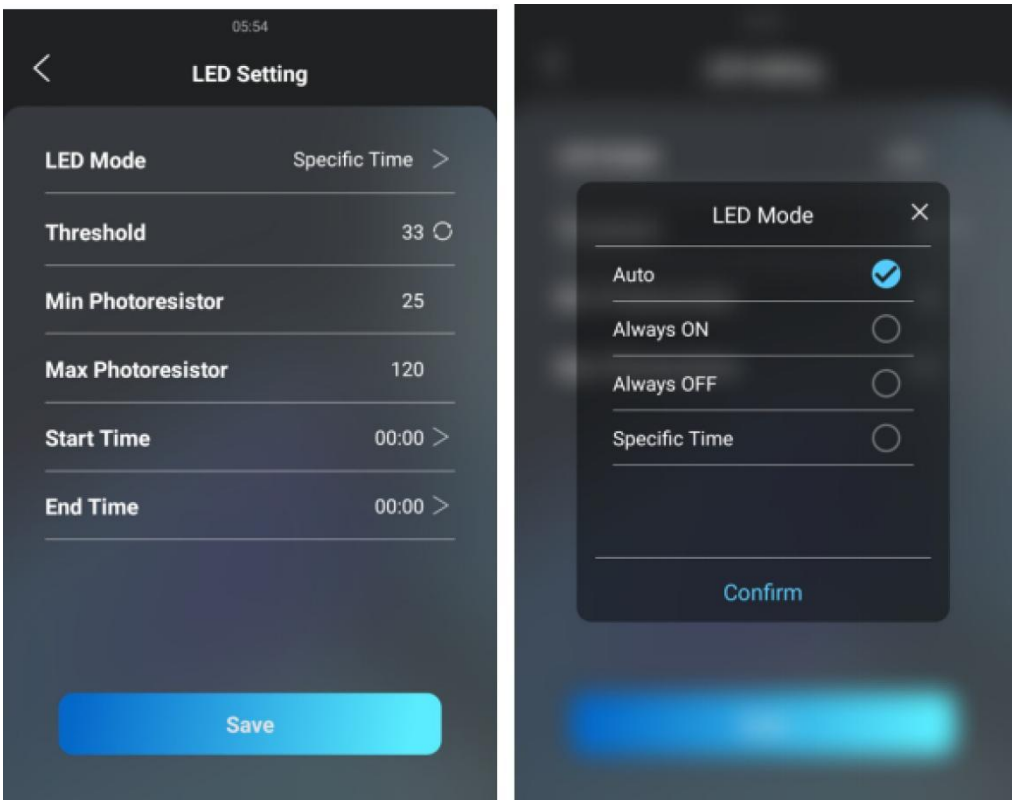
7. LED&LCD Setting

7.1. Infrared LED Setting

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

7.1.1. Infrared LED Setting on the Device

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



Parameter Set-up:

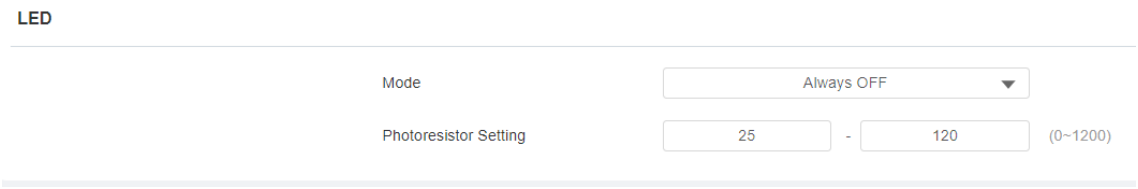
- **Auto**: select **Auto** if you want the Infrared LED light to be turned on automatically according to the setting.
- **Always ON**: select **Always ON** to enable the Infrared LED light to stay on permanently.
- **Always OFF**: select **Always OFF** to turn off the Infrared LED light. LED mode is set **Always OFF** by default.
- **Specific Time**: select a **Specific Time** to turn on the infrared LED according to the time schedule.
- **LED Type: you** can see the LED type **Auto Always ON Always OFF Specific Time** you selected.
- **Threshold**: refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value **(Threshold)** is **33**, however, you can tap the icon  several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on 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 values are from **0** minimum to **1000** maximum.

Note

- **Start Time** and **End Time** will not be displayed unless you select **Specific Time** for your LED mode.
  End Time: set the end time for the infrared LED to be turned off.

7.1.2. Infrared LED Setting on the Web Interface

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

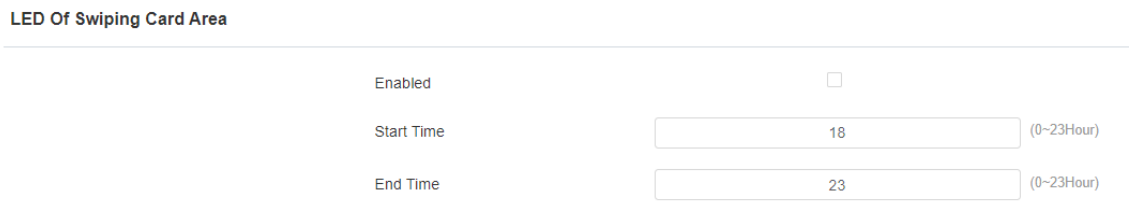


Note

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

7.2. LED Setting on Card Reader Area

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



Parameter Set-up:

- **Enabled**: tick the check box if you want to enable the card reader LED lighting and

vice versa.

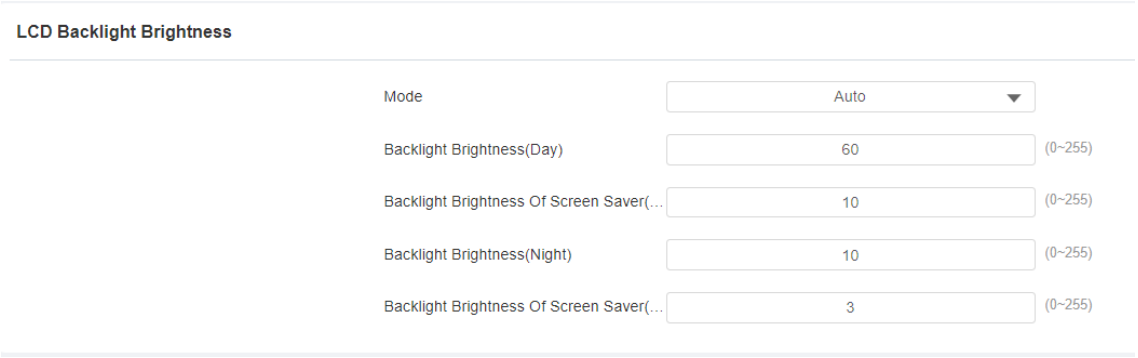
- **Start Time- End Time(H)**: enter the time span for the LED lighting to be valid, eg., if the time span is set from **8-0 (Start time- End time)**, it means the LED light will stay on during the time span from **8:00** am to **12:00** pm during one day (24 hours).

7.3. LCD Screen Brightness Setting

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

7.3.1. LCD Screen Brightness Setting on the Web Interface

On the web interface, you can set and adjust the backlight brightness for the screen and screen saver. To configure the configuration on the web **Device > Light > LCD Backlight Brightness** interface.



Parameter Set-up:

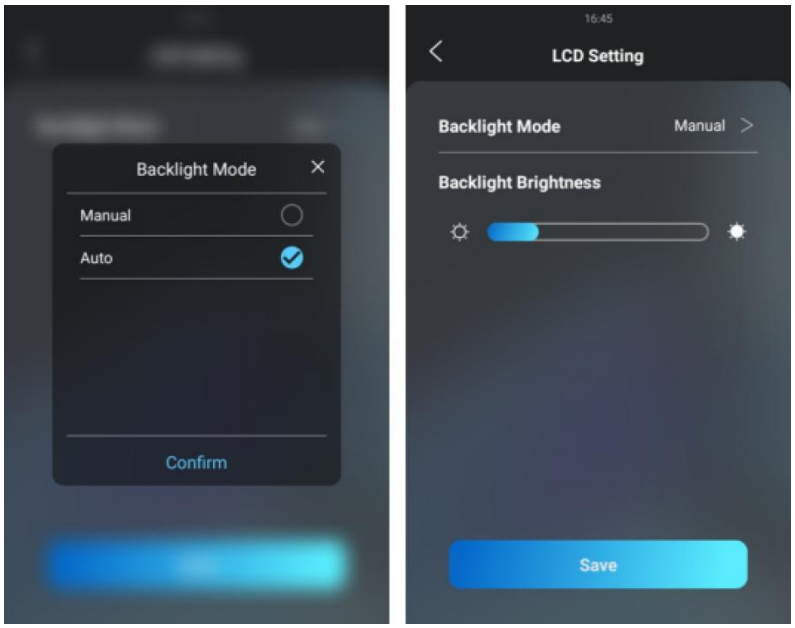
- **Mode**: click to select **Manual** or **Auto** mode for the backlight. The backlight will be adjusted automatically for the screen backlight brightness when **Auto** is selected and vice versa.
- **Backlight Brightness (day)**: set the screen backlight brightness during the daytime

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

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

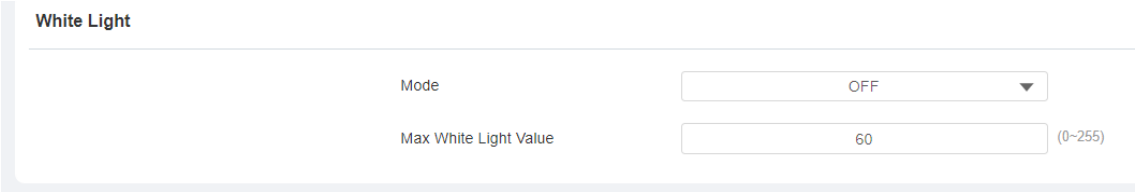
7.3.2. LCD Screen Brightness Setting on the Device

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



7.4. LED White Light Setting

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



Parameter Set-up:

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

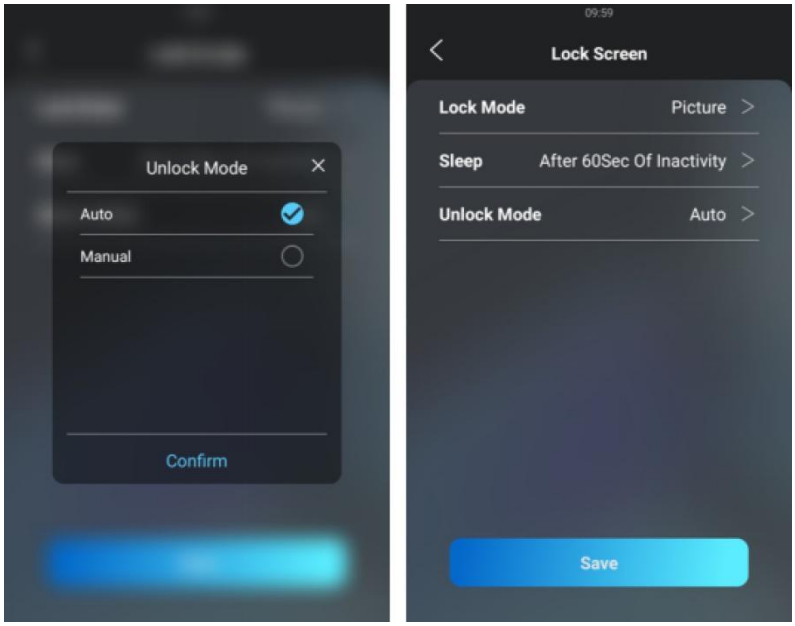
8. Screen Display Configuration

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

8.1. Screensaver Configuration

8.1.1. Configure Screensaver on the Device

Sleep mode and screen saver are designed for screen protection. You can set these two modes to prevent the device screen from getting overheated and to reduce energy consumption. You can define when the device should go into sleep mode, screen saver mode, and turn off the screen. On the device screen, go to **Basic Setting > Lock Screen**.



Parameter Set-up:

- **Lock Mode**: select among three options **NONE**, **Blank Screen**, **and Picture**. **NONE** is selected when you want the screen to stay on without going into 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.

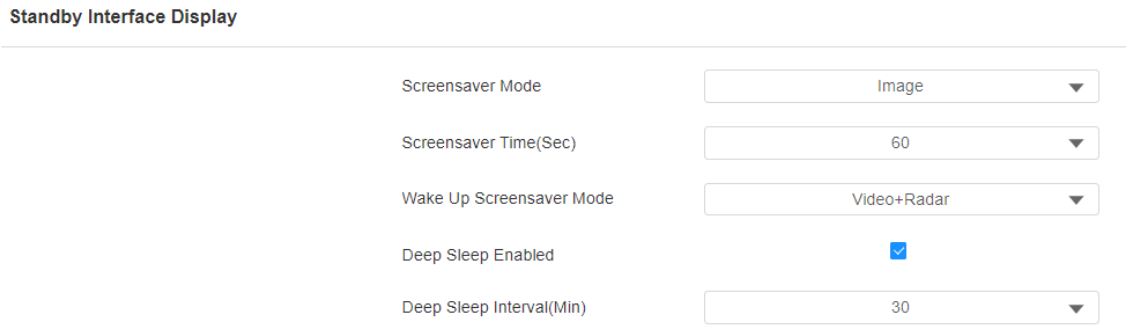
- **Sleep**: set the screen saver start time from 5 seconds up to 180 seconds. The screen saver starts when the device detects no operation, or no one is approaching.
- **Unlock Mode**: select the screen wake-up mode. If you select **Auto mode** then the screen will be awakened when someone approaches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

Note

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

8.1.2. Configure Screensaver on the Web Interface

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



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 into screen saver mode; if **Blank** is selected, the screen will go black. If the **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. The screen saver starts when the device detects no operation, or no one is approaching.
- **Wake Up Screensaver Mode:** select the screen wake-up mode.

  i. Select Manual, if you want to wake up the screen manually by tapping the touch screen.
  ii. Select Video, the device screen will be wakened up when an object is detected in the video image.
  iii. Select Radar, then the device screen will be wakened up when an object is detected by the Radar.
  iv. Select Radar+Video, then the device will be wakened up when an object is detected by Radar or video image.

- **Deep Sleep Enabled**: tick the check box if you want the screen to be turned off after the screensaver reaches the end of duration as predefined.
- **Deep Sleep Interval (Min)**: set the screensaver time duration before the screen can be turned off.

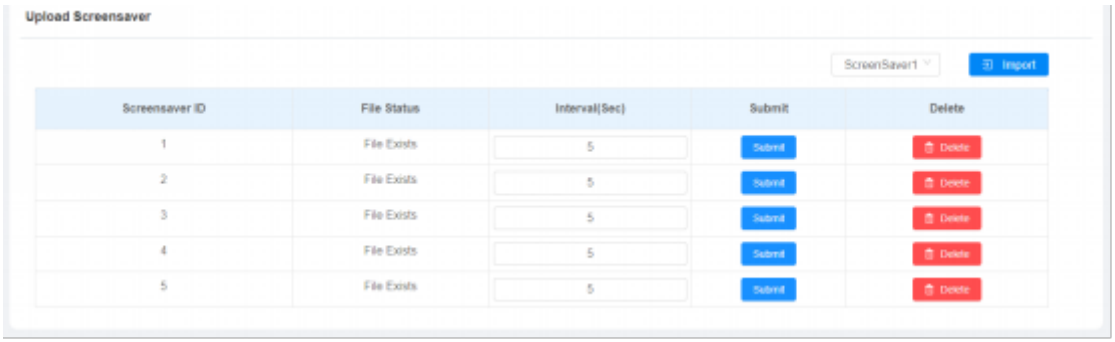
Note

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

8.2. Upload Screensaver

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

the configuration on the web **Device > LCD > Upload ScreenSaver** interface.

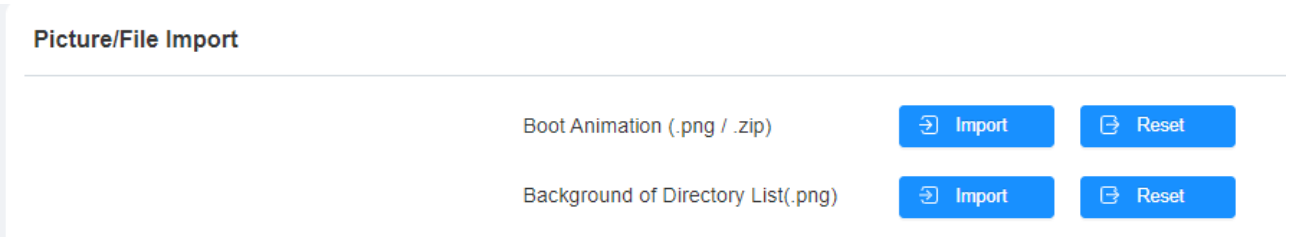


Note

- The pictures uploaded should be in **JPG format with** 2M pixels maximum.
- The previous pictures with a specific ID order will be overwritten when the

8.3. Upload Device Booting Image

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

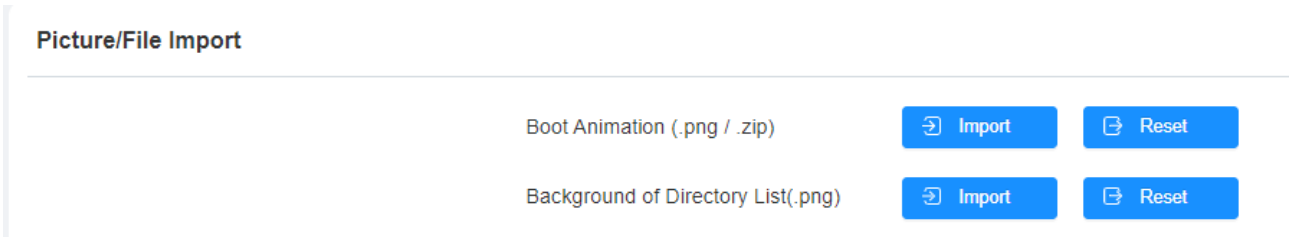


Note

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

8.4. Upload Device Contact List Background Image

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

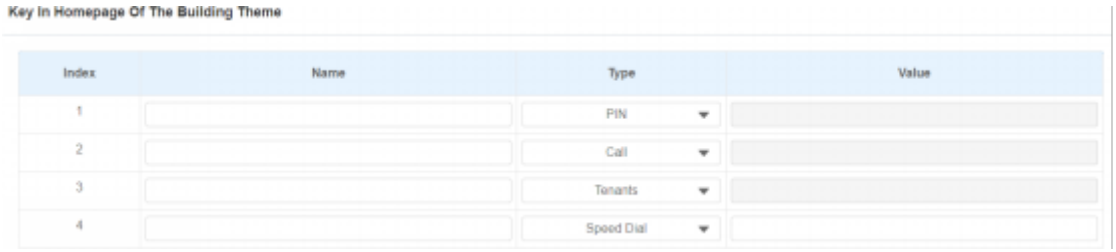


Note

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

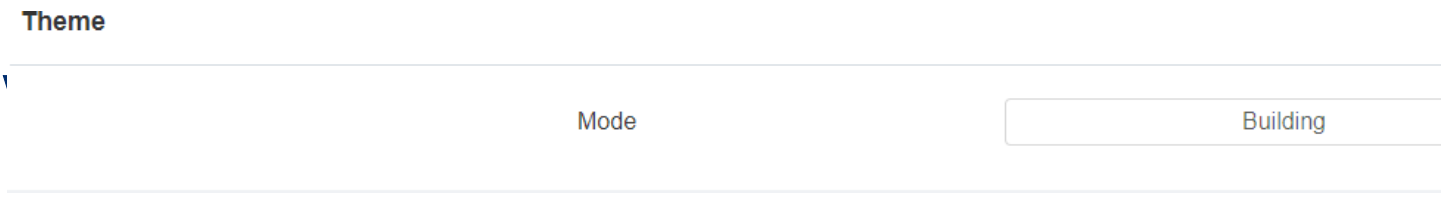
8.5. Home Screen Configuration

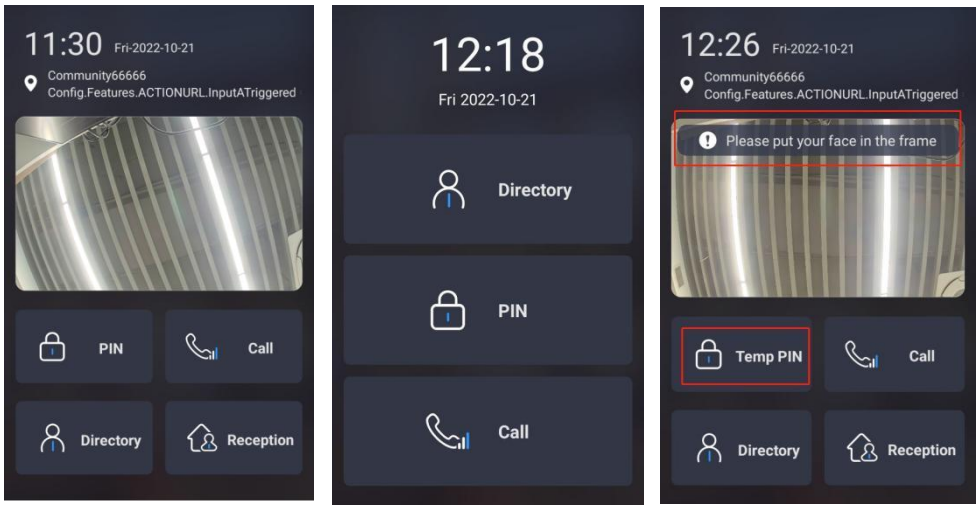
You can change the home screen display through the configuration of tab name and tab arrangement on the device web **Device > Key/Display > Key In Homepage Of The Building Theme** interface.



8.6. Configuration for Scenario-based Screen Display Mode

The door phones offer you two types of screen display modes for different applications: Building mode, Villa Mode, and Multi-factor authentication mode. To set it up, go to **Device > Key/Display > Theme**.





8.7. Villa Mode Home Screen Display

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

View Control of The Villa Theme

Default Page | PIN

Index	Key	Label
1	Directory	
2	PIN	
3	Call	

Parameter Set-up:

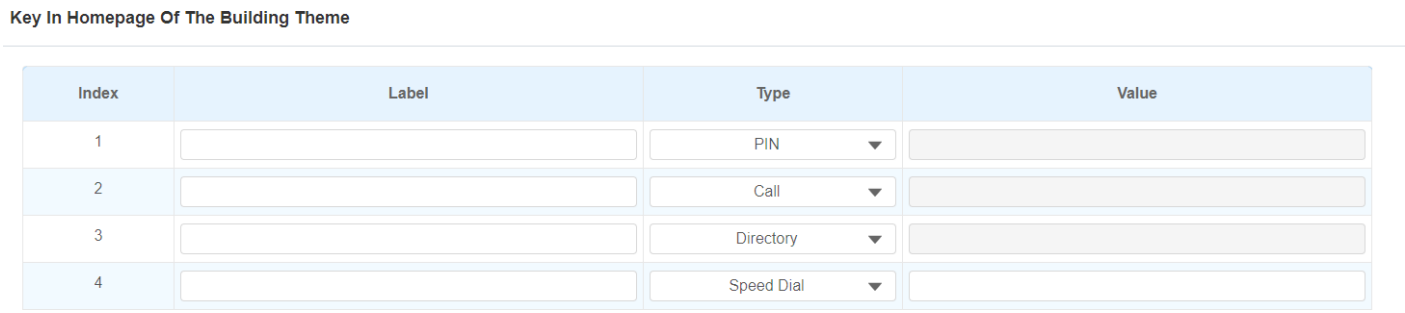
- **Default Page**: select **Home Page** if you display the tenants, PIN, and Call icon vertically on the home screen. Select Directory if you want to display the contact on the home screen. Select PIN if you want to display the PIN icon with the keypad on

the home screen. Select **Call** if you want to display the Call icon with a dial pad on the home screen.

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

8.8. Building Mode Home Screen Display

You can customize your building mode home screen icon display if needed. To do so, go to **Setting > Key/Display > Key In Homepage Of The Building Theme**



Parameter Set-up:

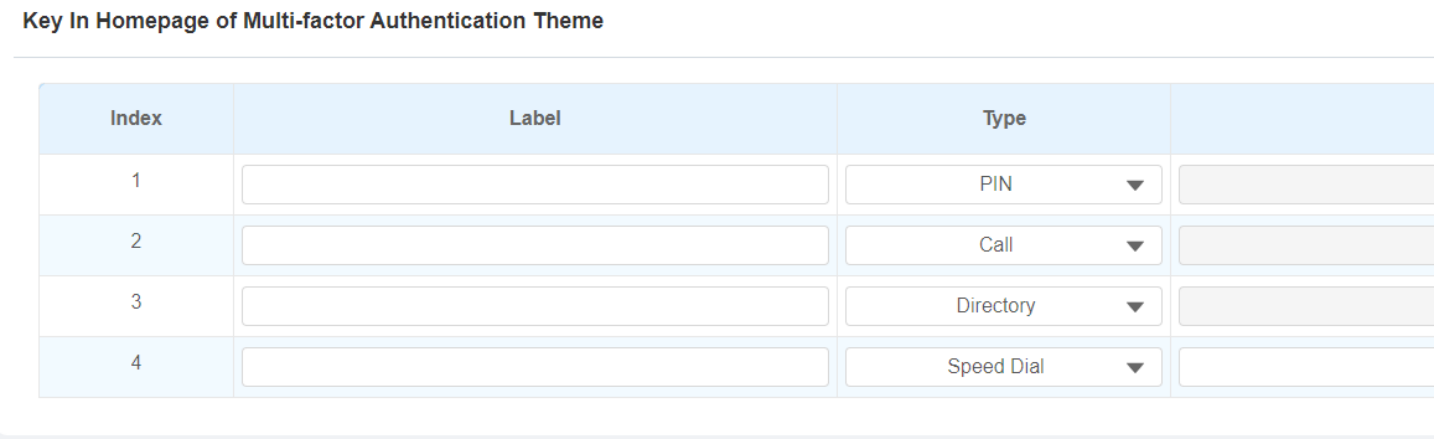
- **Type**: select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make the **Speed Dial** tab displayed in position one, you can change the type in index number 1 to **Speed Dial**. And you can change another tab position accordingly.
- **Label**: enter a new name to replace the original tab name, but it does not change the attribute of the type.

- **Value:** enter the speed dial number.

- **Voice Prompts Enabled**: if enabled, you will hear the voice prompt.

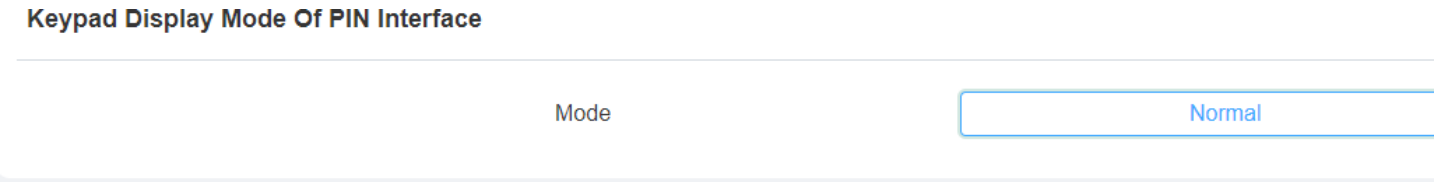
8.9. Two-factor Authentication Mode Screen Display

You can also customize your home screen icon display for the multi-factor authentication mode if needed. To do so, go to **Setting > Key/Display > Key In Homepage Of The Building Theme**.



8.10. Dial Key Order

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

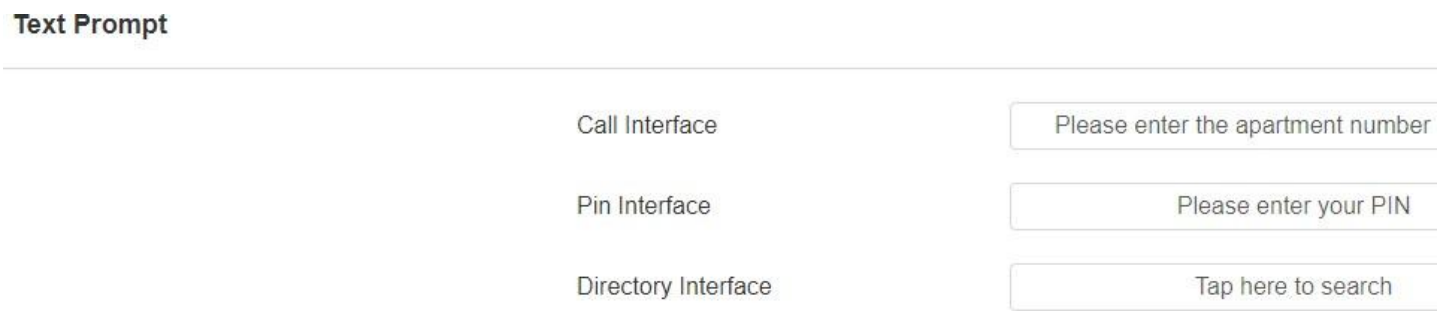


Parameter Set-up:

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

8.10.1. Prompt Display

You can customize your prompts to be displayed on the screen. To do so, navigate to **Setting > Key/Display > Text Prompt**.



Parameter Setup:

- **Call interface:** type in the prompt for the call screen.
- **PIN Interface**: type in the prompt for the PIN screen.
- **Directory Interface**: type in the prompt for the directory screen.

Note

- The door phone supports a 128-digit character maximum in length for the text prompt.

8.10.2. Open Door Text Prompt Display

You can enable the open door text prompt for both door-opening success and failure. And

you can also make the door phone display the user information when users use credentials such as RF cards for access.

To do so, navigate to **Access Control > Relay > Text Prompt**.

Text Prompt

Access Granted	☑
Access Denied	☑
Display User Info	☑

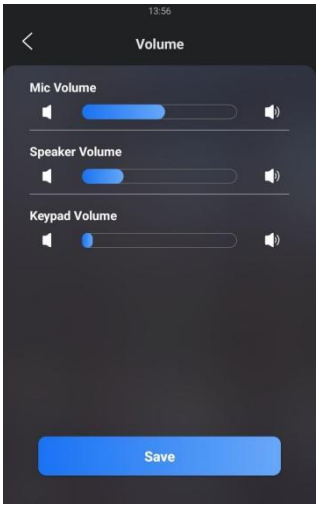
9. Volume and Tone Configuration

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

9.1. Volume Configuration

9.1.1. Configure Volume on the Device

You can adjust the microphone volume, speaker volume, keypad volume, and AD volume on the device. To configure the language display on the device **Basic Setting > Volume** interface.



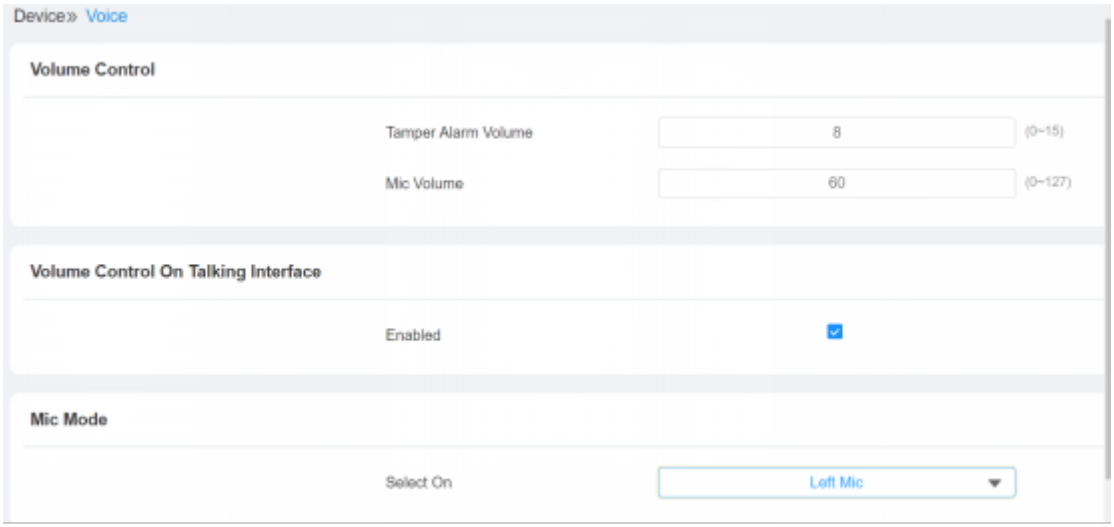
Parameter Set-up:

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

- **Key Volume:** adjust the volume for the button touch sound.

9.1.2. Configure Volume on the Web Interface

On the web interface, you can set the temper alarm volume, mic volume, etc. To configure the configuration on the web **Device > audio**.



Parameter Set-up:

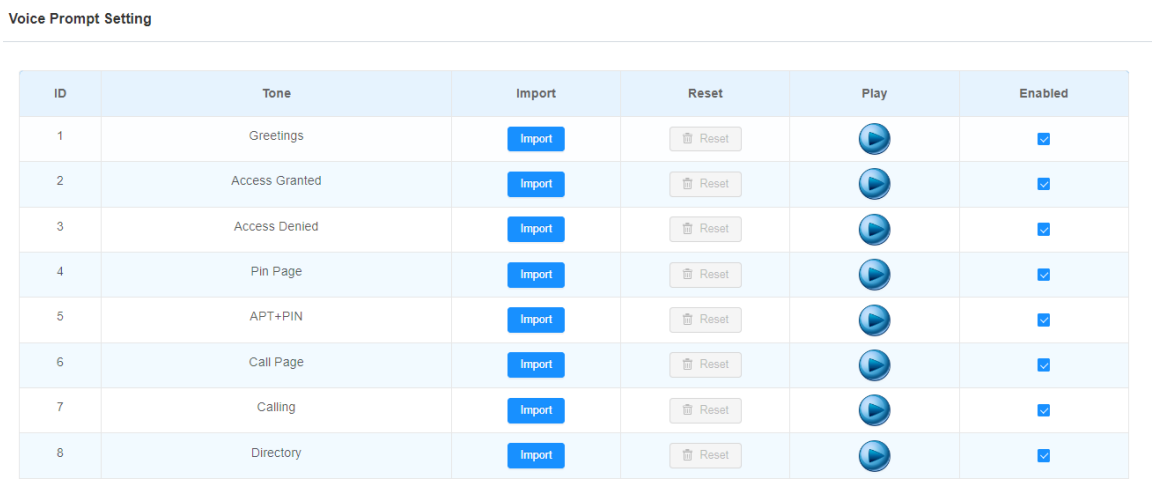
- **Tamper Alarm Volume**: set the tamper alarm volume from 0-15 according to your need. The default volume is **8**.
- **Mic Volume**: set the mic volume from 0-15 according to your need. The default volume is **8**.
- **Enabled**: tick off the check box if you allow the adjustment to be made on the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

Note

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

9.2. Upload Prompt Tone

You can upload various types of voice prompt. Go to **Device > Audio > Voice Prompt Setting.**



Parameter Set-up:

- **Greetings**: import the greeting tone when the device is booted.
- **Access Granted**: import the prompt tone for door-opening success.
- **Access Denied**: import the prompt tone for door opening failure.
- **Pin Page**: import the prompt tone for the PIN screen.
- **Apart+PIN**: import the prompt tone for the Apartment+ PIN screen.
- **Call page**: import the prompt tone for the call screen.

Note

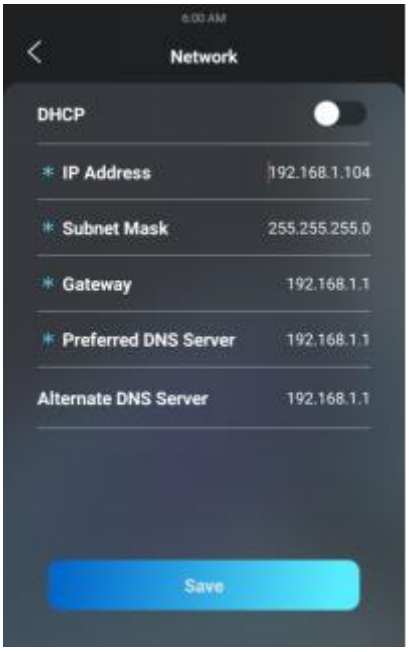
- The open door tone file should be in .wav format and the file size should be smaller than 200KB.

10. Network Setting

10.1. Device Network Configuration

You can check 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's web interface.

To configure the language displayed on the device **Setting > Network** interface.



Parameter Set-up:

- **DHCP**: Select the **DHCP** mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the door

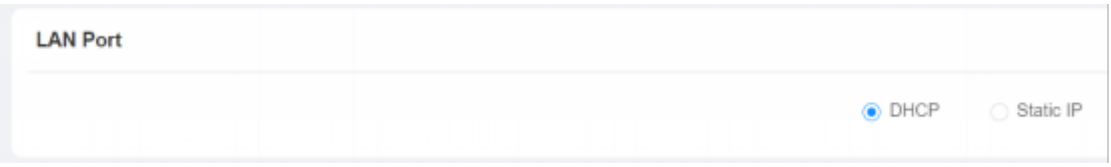
phone will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.

- **Static IP**: select the static IP mode by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS

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

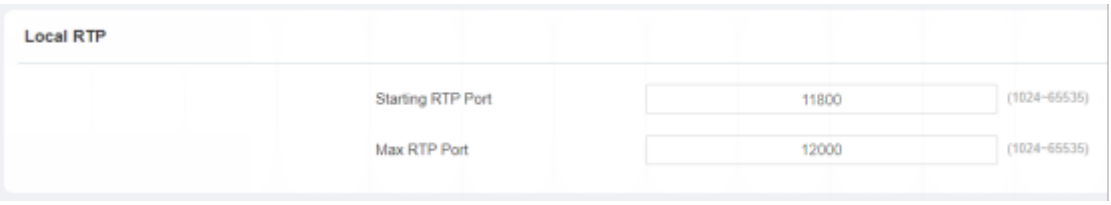
- **IP Address**: set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **Preferred & Alternate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

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



10.2. Device Local RTP Configuration

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



Parameter Set-up:

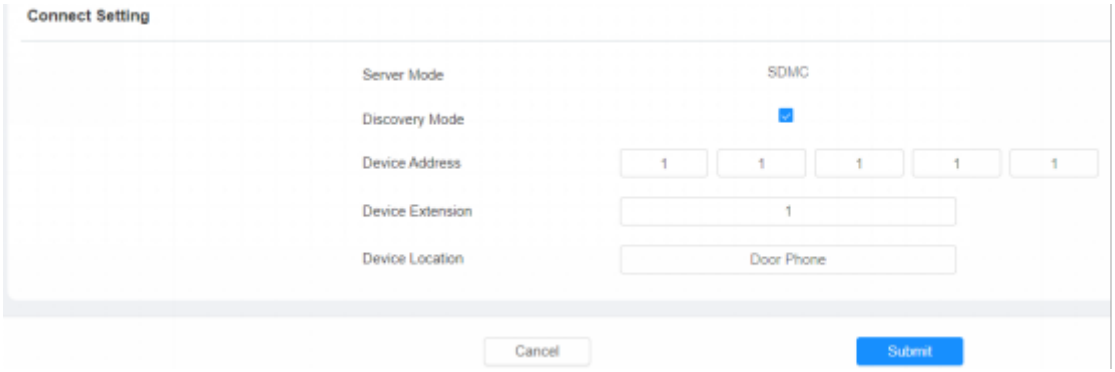
- **Starting RTP Port**: enter the Port value in order to establish the start point for the exclusive data transmission range.

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

10.3. Device Deployment in Network

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

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



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 or 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

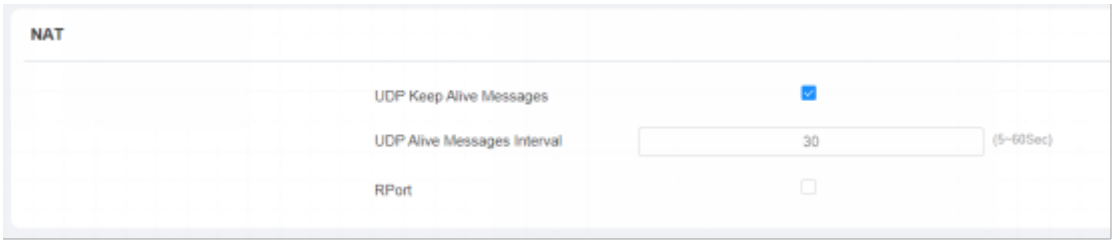
conceal the device so as not to be discovered by other devices.

- **Device Address:** specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, and Room** in sequence.
- **Device extension**: enter the device extension number for the device you installed.
- **Device Location**: enter the location in which the device is installed and used.

10.4. NAT Setting

NAT (**Network Address Translation**) allows hosts in an organization's private intranet to transparently connect to hosts in the public domain.

There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. To configure it, go t **Account > Advanced > NAT** interface.



Parameter Set-up:

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

11. Intercom Call Configuration

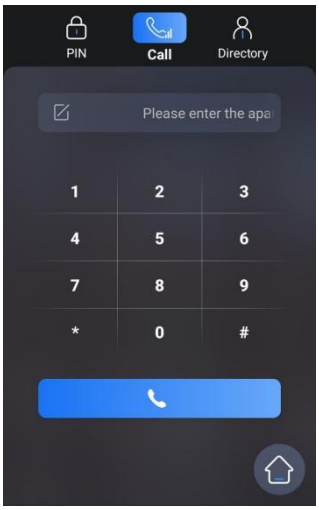
The intercom calls in the device can be configured to allow you to perform a variety of customized intercom calls such as IP calls and SIP calls for different application scenarios.

11.1. IP call & IP Call Configuration

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

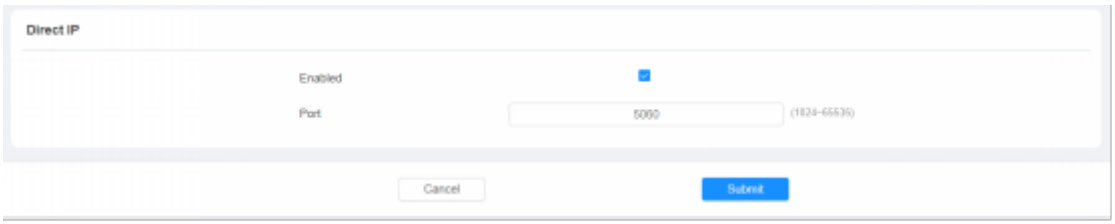
11.1.1. Make IP Calls

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



11.1.2. IP Call Configuration

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



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

11.2. SIP Call &SIP Call Configuration

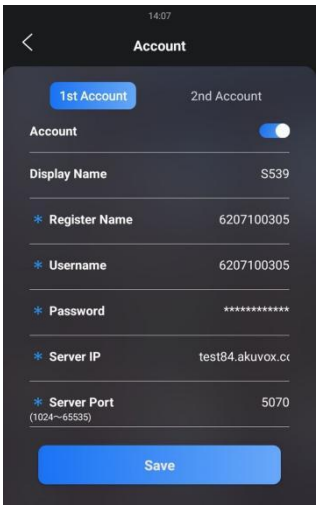
You can make a SIP call (**Session Initiation Protocol**) in the same way as you do to make the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

11.2.1. SIP Account Registration

The door phone supports two SIP accounts that can all be registered according to your applications. You can, for example, switch between them if any one of the accounts fails and becomes invalid. The SIP account can be configured on the device and on the device interface.

11.2.1.1. Configure SIP Account on the Device

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

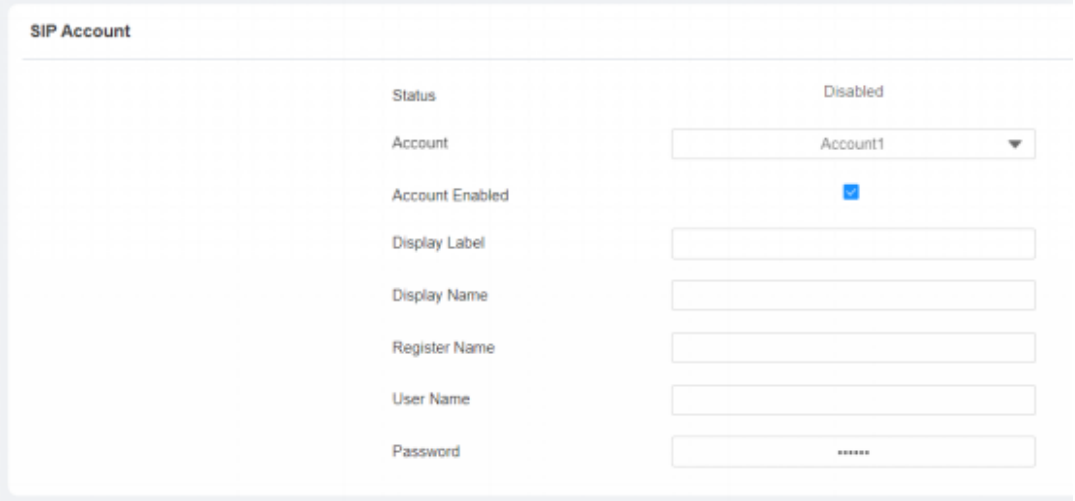


Parameter Set-up:

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

11.2.1.2. Configure SIP Account on the Web Interface

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



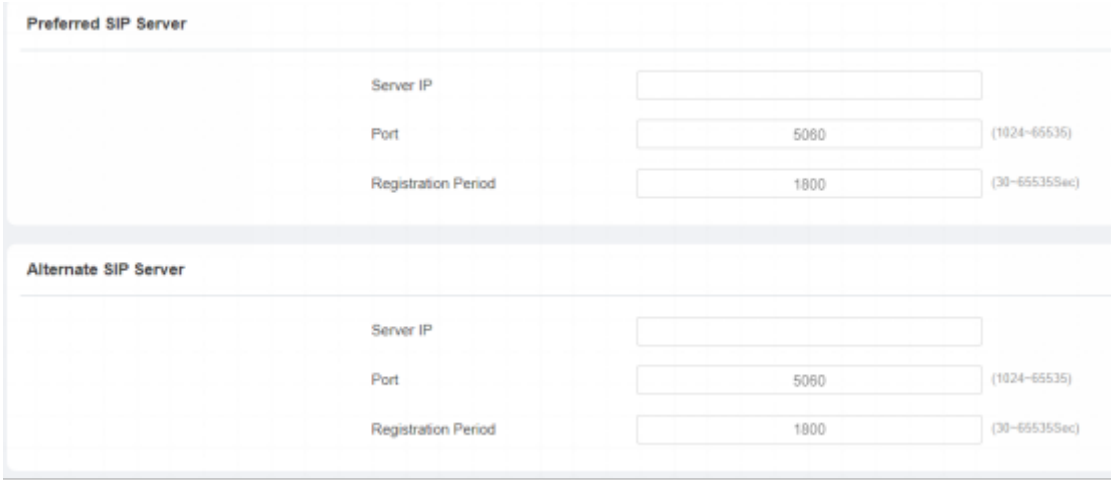
Parameter Set-up:

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

11.2.2. SIP Server Configuration

SIP servers can be set up for devices in order to achieve call sessions through SIP servers

between intercom devices. To configure the configuration on the web **Account > Basic > Preferred SIP Server** interface.

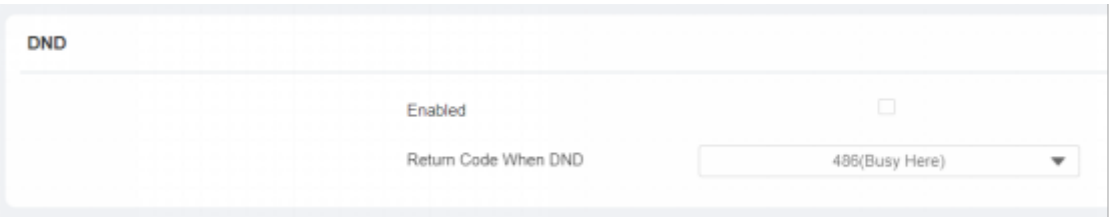


Parameter Set-up:

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

11.2.3. SIP Call DND&Return Code Configuration

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

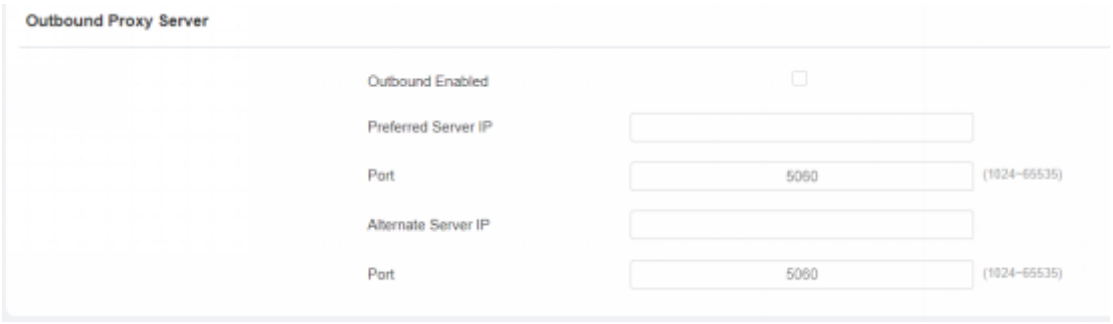


Parameter Set-up:

- **DND**: enable or disable the DND function. DND function is disabled by default.
- **Return Code When DND**: select what code should be sent to the calling device via the SIP server. **404 for Not found**; **480 for Temporary unavailable**; **486 for Busy Here**.

11.2.4. Configure Outbound Proxy Server

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



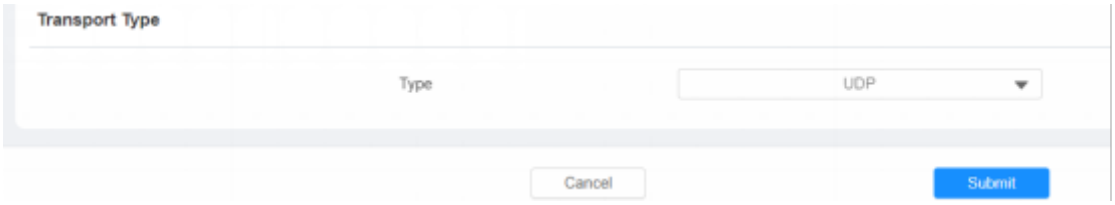
Parameter Set-up:

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

- **Port:** enter the Port number for establishing a call session via the backup outbound proxy server.

11.2.5. Configure Data Transmission Type

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



Parameter Set-up:

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

11.3. Dial Options Configuration

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

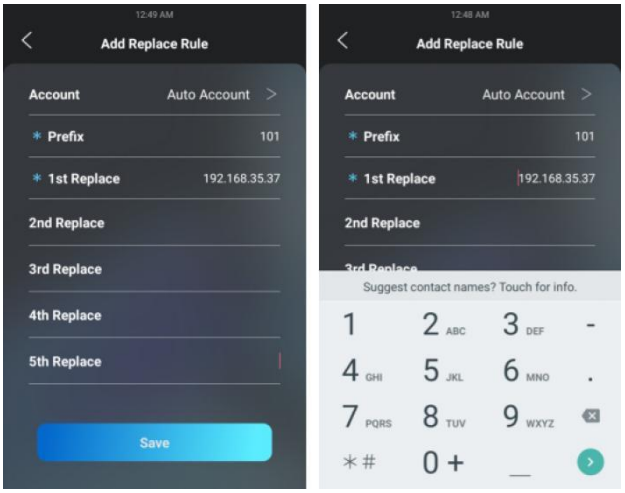
11.3.1. Quick Dial by Number Replacement

If you want to replace the long and complex dial number with a shorter number that can be memorized at greater ease and convenience for making calls, you can configure the dial

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

11.3.2. Quick Dial by Number Replacement on the Device

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



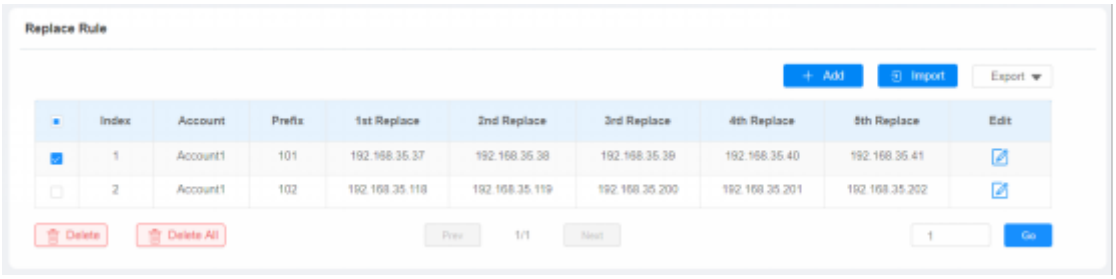
Parameter Set-up:

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

11.3.3. Quick Dial by Number Replacement on the Web Interface

You can not only add a quick dial number separately but also import the quick dial number to the device in batch. Besides, you can edit and delete the numbers if needed. To configure the configuration on the web **Intercom > Dial Plan > Replace Rule** interface.



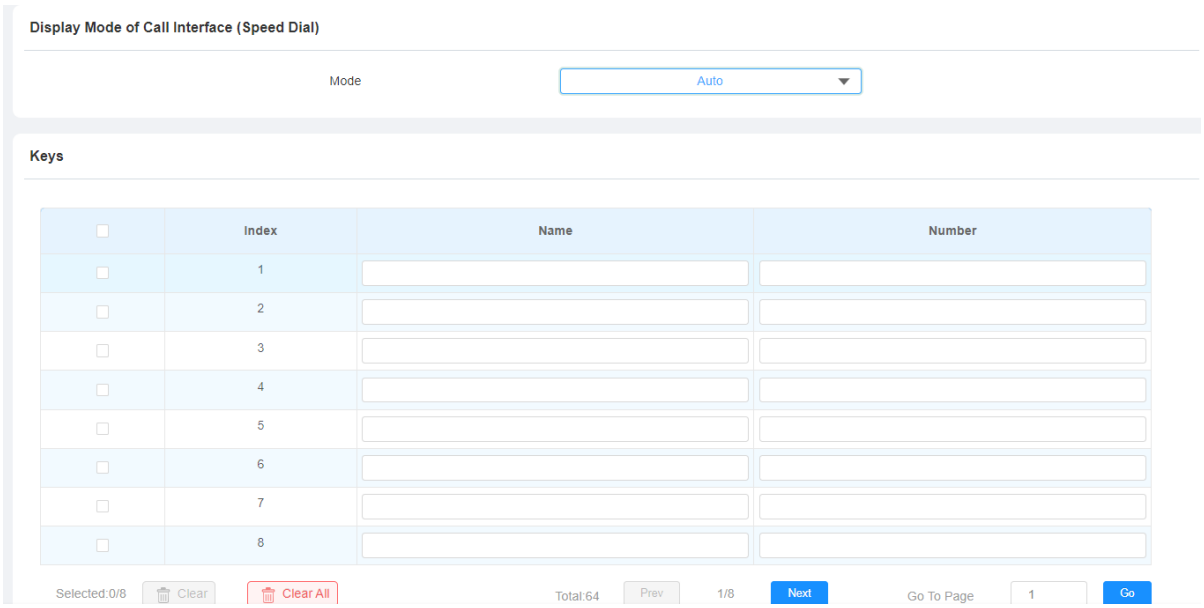
Note

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

11.4. Speed Dial

11.4.1. Speed Dial in Villa Mode

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



Parameter Set-up:

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

Options	Descriptions
Standard	Select **Standard** if you want to display the time and keypad only with no dial tabs.
Auto	Select **Auto** if you want to select the dial tab layout that does match any one of the other 8 options. For example, if you want to create 3 dial tabs, 5 dial tabs, or 7 tabs, etc.,

	that does not match with other options.

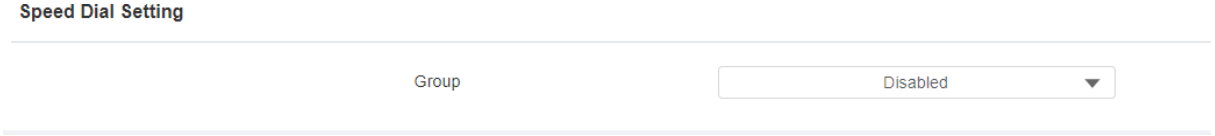
1 Key	Select **1 Key** if you display only one dial tab with no keypad.
1 Key + Keypad	Select **1 Key+Keypad** if you want to display one dial tab with the keypad.
2 Keys+ Keypad	Select **2 Key+Keypad** if you want to display two dial tabs with the keypad.
8 Keys	Select **8 Keys** if you want to display 8 dial tabs with no keypad.
16 Keys	Select **16 keys** if you want to display 16 dial tabs with no keypad.

Note

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

11.4.2. Speed Dial in Building Mode

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



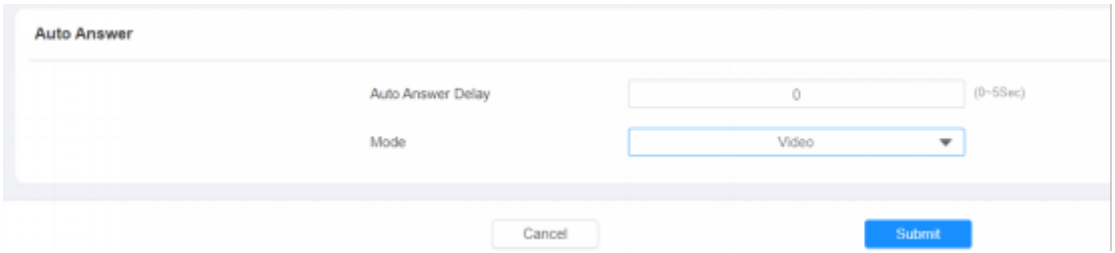
Parameter Set-up:

- **Group:** select the contact group to be called by pressing the Reception button.

11.5. Call Auto-answer Configuration

You can define how quickly the door phone should respond by answering the incoming SIP/IP call automatically by setting up the time-related parameters. In addition, you can also define the mode in which the calls are to be answered (video mode or audio mode).

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



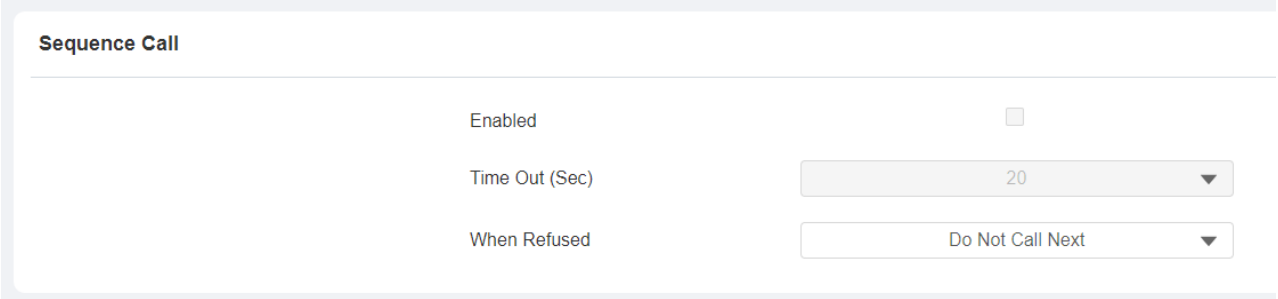
Parameter Set-up:

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

11.6. Sequence Call Configuration

Sequence Call is a function supported by Akuvox SmartPlus which releases a group of sequence call numbers for the application. You can call the targeted group of sequence calls (e.g., your extension numbers in your kitchen, bedroom, etc.) in sequential orders until

the call is answered. Sequence calls will be completed as soon as the call is answered by any of the targeted extension devices. To configure it, go to **Intercom > Basic > Sequence Call** interface.



Parameter Set-up:

- **Enable** tick the check box if you want to enable the sequence call.
- **Timeout (Sec)**: click to select the call time interval in between the sequence call number in a targeted sequence call group. For example, if you set the time interval as 10 seconds, then the call (if not answered in 10 Sec.) will be terminated automatically and be transferred sequentially to the next sequence call number in the targeted sequence call group.
- **When Refused**: if you select **Don Not Call Next** then the sequence call will be terminated if the call is rejected by the called party. If you select **Call Next** then the sequence call will be continued to the next called party if it is rejected by the first called party.

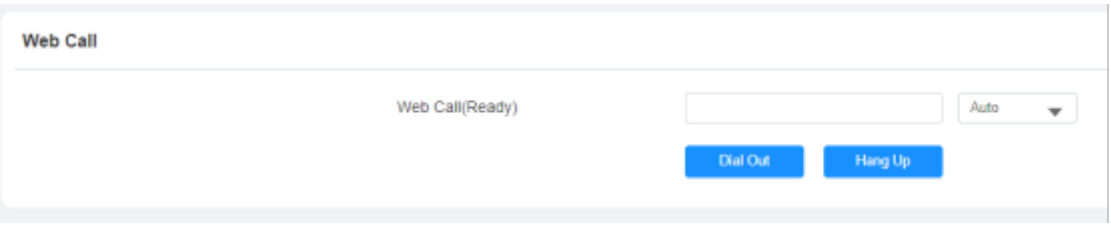
Note

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

11.7. Web Call

In addition to making IP/SIP calls directly on the device, you can also make the call on the device web interface without approaching to device physically for testing purposes, etc.

You can navigate to **Intercom > Basic > Web Call**.



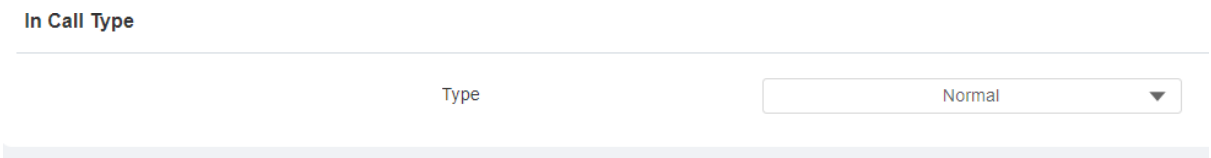
Parameter Set-up:

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

12. Call Settings

12.1. Customize Calling

You can customize your calling on the door phone for a greater call experience. For example, you can choose an audio call, a two-way video call, and so on. Also, you can put a human simulator on the screen that will follow and mimic the real person's talk with added body gestures. To set it up, go to **Intercom > Basic > In Call Type**.

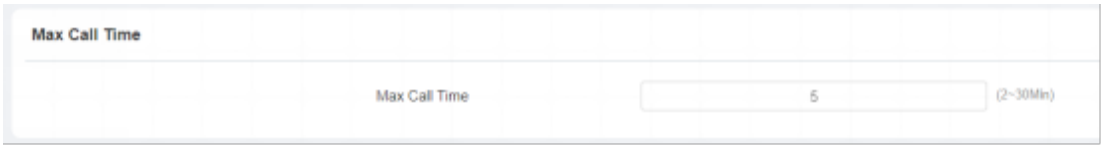


Parameter Set-up:

- Type: select your call type:
  - Normal: select the normal for the audio call.
  - Two-way call: select the two-way call so that both the called party and the calling party can see each other during the video call.
  - Meta-com: select it if you want to create a human simulator simulating the speaker on the other side during the video call.

12.2. Maximum Call Duration Setting

The door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the call automatically. To configure it, go to **Intercom > Call Feature > Max Call Time** interface.

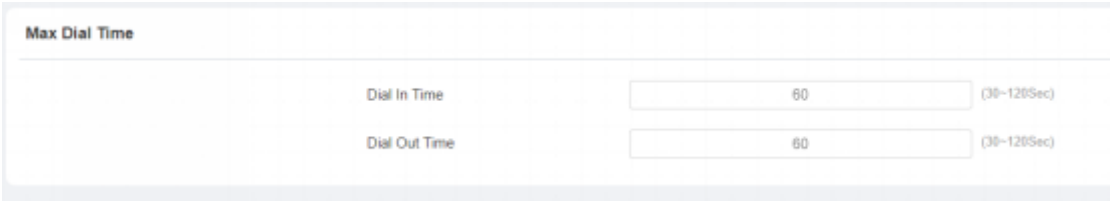


Parameter Set-up:

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

12.3. Maximum Dial Duration Setting

Maximum Dial duration consists of the maximum dial-in time duration and the maximum dial-out time. Maximum dial-in time refers to the maximum time duration before the door phone hangs up the call if the call is not answered by the door phone. In contrast, maximum dial-out time refers to the maximum time duration before the door phone hangs up automatically when the call from the door phone is not answered by the intercom device being called to. To configure the configuration on the web **Intercom > Call Feature > Max Dial Time** interface.



Parameter Set-up:

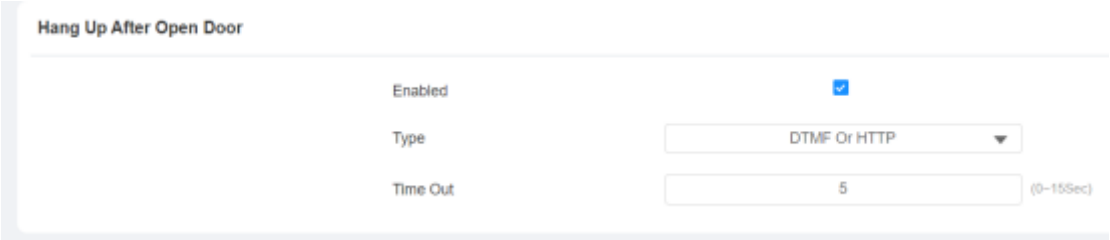
- **Dial In Time:** enter the dial-in time duration for your door phone (ranging from 30-120S) for example, if you set the dial-in time duration is 60 seconds in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial-in time duration by default.

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

12.4. Hang Up After Open Door

This feature is used to hang up the call automatically after the door is released during a call. So, a caller or a called party does not need to click the hang-up button to hang up the call.

To set the feature, go to **Intercom > Call Feature > Hang Up After Open Door** interface.



Parameter Set-up:

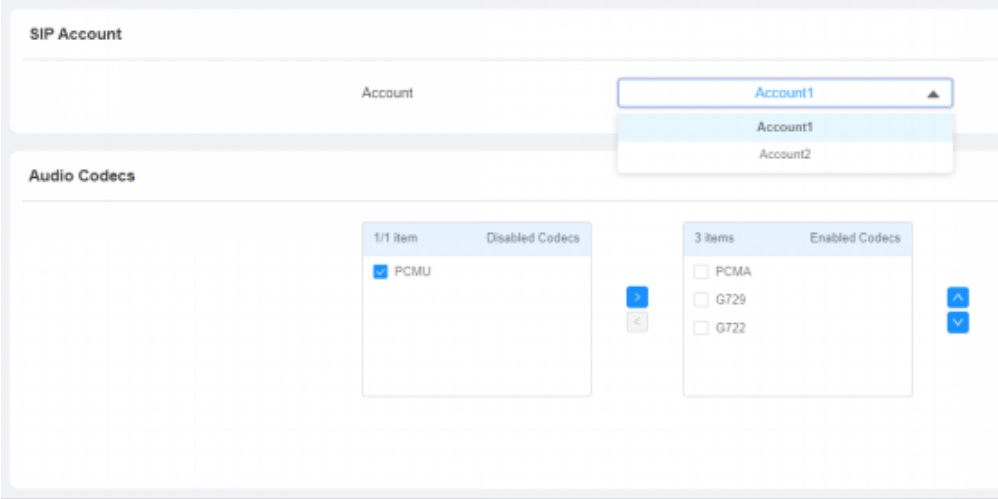
- **Enabled:** the feature is enabled by default.
- **Type**: select the open door type. The door can be unlocked via the **DTMF**, **HTTP** command, **DTMF Or HTTP**, and **DTMF, HTTP or Input**.
- **Timeout:** set up from 1 second to 15 seconds. 5 seconds is the default. If you set it to 5 seconds, then the call will be hung up 5 seconds after the door is opened. If you want to disable the feature, set the timeout as 0.

12.5. Audio& Video Codec Configuration for SIP Calls

12.5.1. Audio Codec Configuration

The door phone supports four types of Codec (PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in

terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment. To configure it, go to **Account > Advanced > SIP Account**.

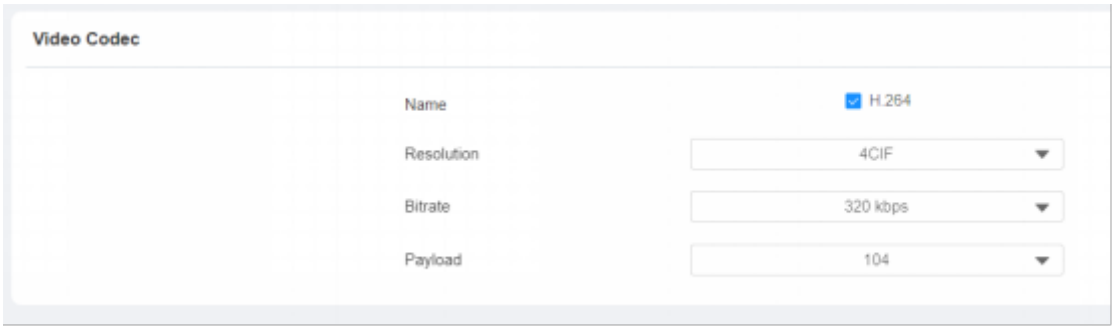


Please refers to the bandwidth consumption and sample rate for the four codecs types below:

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

12.5.2. Video Codec Configuration

The door phone supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload. To configure it , go to **Account > Advanced > Video Codec** interface.

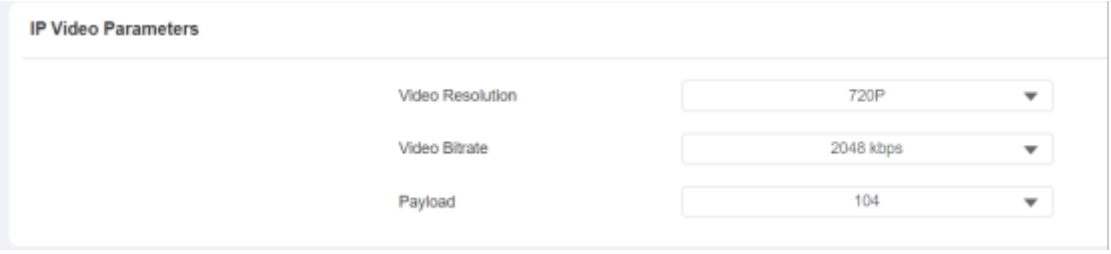


Parameter Set-up:

- **Name**: check to select the H264 video codec format for the door phone video H264 is the video codec by default.
- **Resolution:** select the code resolution for the video quality among four options: **QCIF, CIF, VGA, 4CIF, and 720P** according to your actual network environment. The default code resolution is 4CIF.
- **Bitrate:** select the video stream bit rate (Ranging from 320-2048). The greater the bitrate, the data transmitted every second is the greater in amount therefore the video will be clearer. While the default code bitrate is 2048.
- **Payload:** select the payload type (ranging from 90-118) to configure the audio/video configuration file. The default payload is 104.

12.5.3. Video Codec Configuration for IP Direct Calls

You can select the IP call video quality by selecting the proper codec resolution according to your actual network condition. To do so, you can go to **Intercom >Call Feature > IP Video Parameters.**

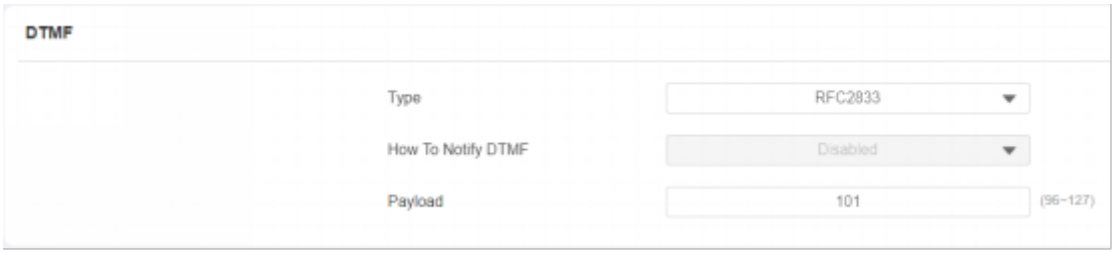


Parameter Set-up：

- **Video Resolution**: select the code resolution for the video quality among four options: **CIF, VGA, 4CIF, and 720P**. The default code resolution is 4CIF.
- **Video Bitrate**: **Video Bitrate**: select video bit-rate among six options: **64 kbps, 256 kbps, 512 kbps, 1024 kbps, and 2048 kbps** according to your network environment. The default video bit rate is **2048 kbps**.
- **Video Payload**: select the payload type (ranging from 90-118) to configure the audio/ video configuration file. The default payload is 104.

12.6. Configure DTMF Data Transmission

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



Parameter Set-up:

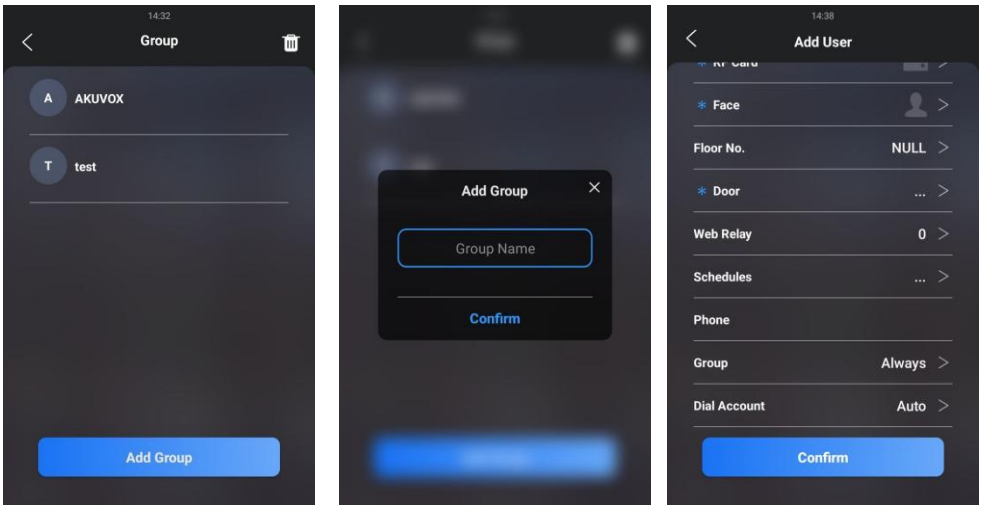
- **Mode:** select DTMF mode among five options: **Inband**, **RFC2833**, **Info+Inband,** and **Info+RFC2833** based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.

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

13. Phone Book Configuration

13.1. Phone Book Configuration on the Device

You can create contact groups for users. Go to **Setting> User > Group** to create a contact group, then go to the Users List to configure the contact setting for the users.



Parameter Set-up:

- **Phone:** type in the user's contact number.
- **Group:** select a contact group for the user.
  - Select the **Default group** if you have not created a contact group for the users.
  - Select Hidden Contacts if you want to hide the contact on the directory screen.
  - Select a contact group you have created for the users.

- **Dial Account**: select the dial account from which you want to call the contact on the door phone.

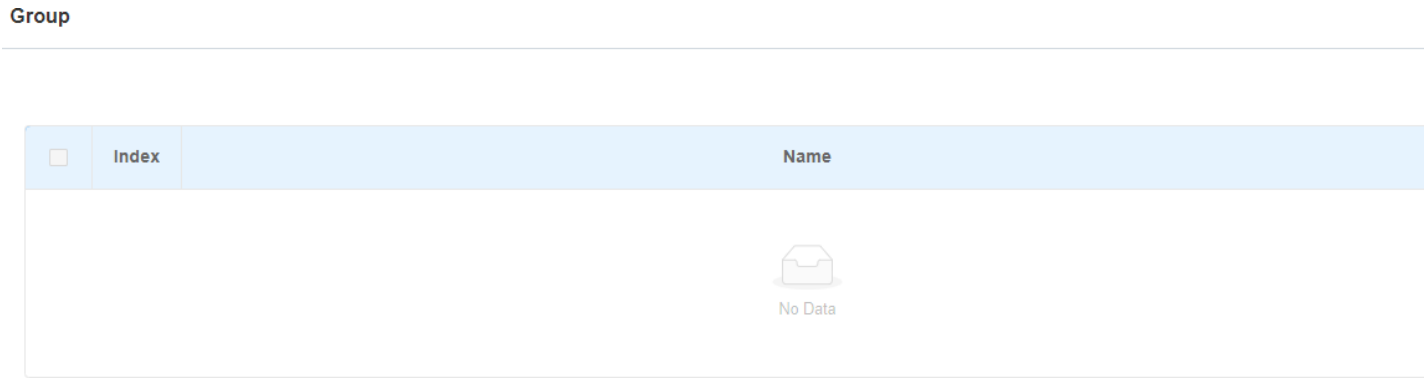
Note

- Only the SIP numbers of the contacts can be called out through the SIP account. IP numbers are not valid for this application.

13.2. Phone Book Configuration on the Web Interface

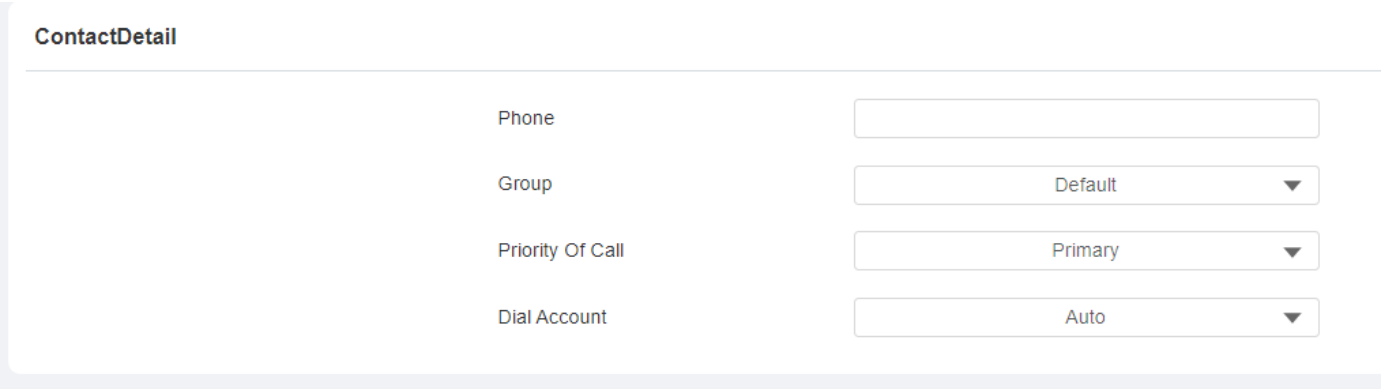
13.2.1. Manage Contact Groups on the Web Interface

You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user. To create and edit a contact group, go to **Directory > User> Group** interface.



13.2.2. Contact Configuration for User

You can configure the users' contact settings when adding a user. Go to **Directory > User**, click **+Add**, then scroll down to **Contact Detail Setting**.



Parameter Set-up:

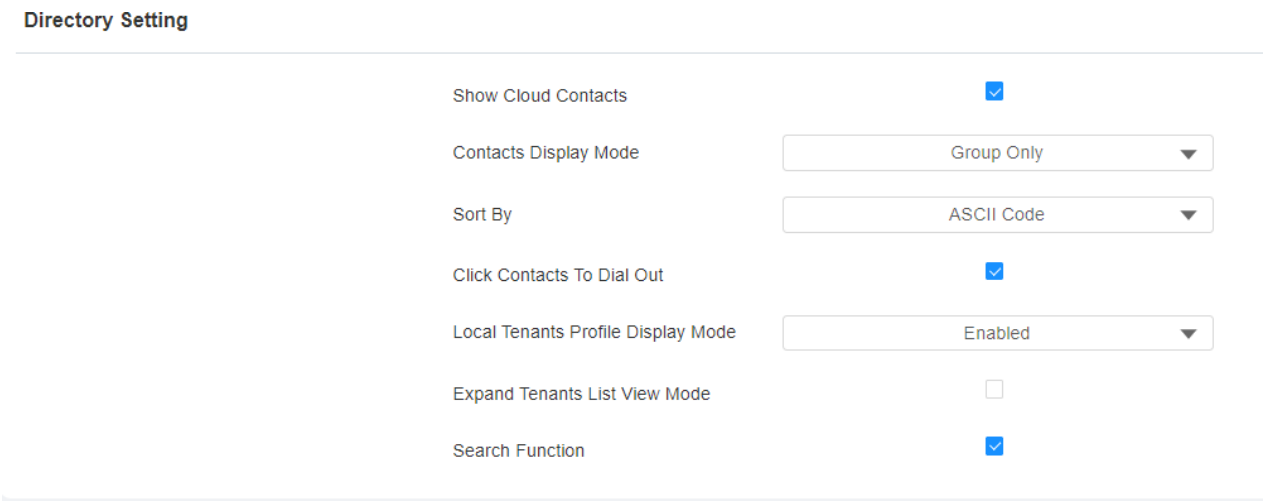
- **Phone:** type in the user's contact number.
- **Group:** select a contact group for the user.
  - select the **Default** group if you have not created a contact group for the users.
  - select **Hidden Contacts** if you want to hide the contact on the directory screen.
  - select a contact group you have created for the users.
- **Priority of Call:** set the call priority for the user in a contact group (Primary, Secondary, and Tertiary) for group calls. for example, if you set it as primary for a user in a selected contact group, then the user will be called first among all the users in the contact group when someone is making a group call.
- **Dial Account**: select the dial account from which you want to call the contact on the door phone.

Note

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

13.2.2.1. Contact List Display Setting

If you want to customize your contact list display it to your desired visual preference. You can go to the web interface to do the configuration. To set it up, go to **Directory > Directory Setting**.



Parameter Set-up:

- **Show Cloud Contacts:** tick the check box to show the cloud contacts in the contact list. And when you untick the check box, the cloud contact will be hidden.
- **Contacts Display Mode:** select the contact display mode.
  - If **Group Only** is selected, then all the contact groups will be displayed in order by room number.
  - If **All Contacts** is selected, then all the contacts will be displayed in order by room number.
  - If **Contact Display by Group** is selected, then all the contacts will be displayed

in order by ASCII when you unfold the contact group.

- **Sort By:** select **ASCII Code** or **Room No. or Import**. When you select ASCII Code, the tenants will be listed by their names in the sequence of the ASCII code. When you select Room No., the tenants will be sorted according to their room numbers.
- **Click Contacts to Dial Out:** tick the check box to enable the dial-out by pressing the contact tab. When this function is enabled, you can press anywhere on the contact

tab to dial out. This function will be disabled when you untick the check box, and when it is disabled, you need to press the **Call icon** in the middle of the tab to dial out.

- **Local Tenants Profile Display Mode:** select **Enable** or **Disabled** or **Auto**. When the function is enabled, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, the default contact icon will be displayed next to the name. When disabled, the picture or the icon will not be displayed. When the function is set as Auto, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, there won't be an icon next to the name.

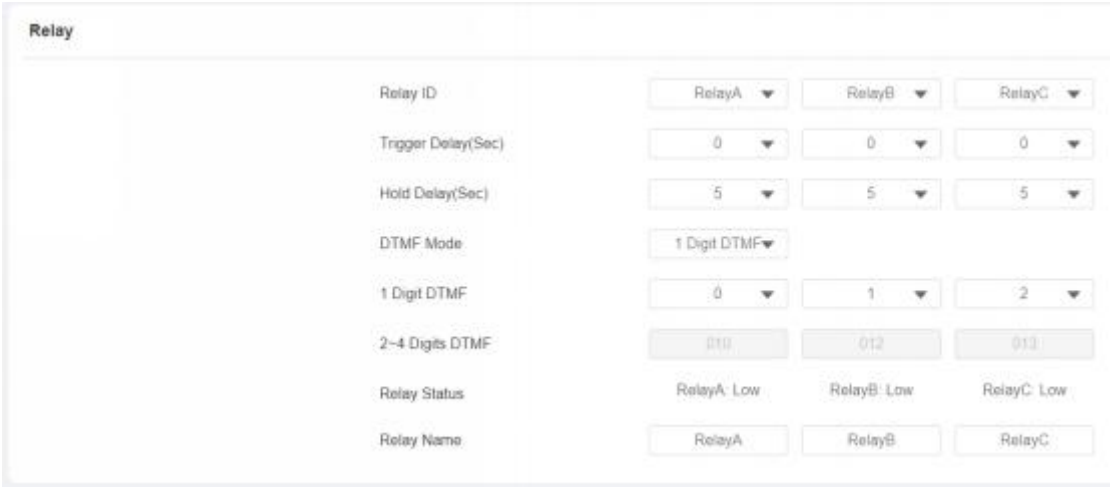
- **Expand Contact List View Mode:** tick the check box to control contact tab size. For example, if you tick the check box then the contact tab will be widened. And the tab will turn to normal size when you untick the check box.

- **Search Function:** tick or untick the check box to control the display of the **Tap here to search field** on the top of the screen. If you untick the check box, then the **Tap here to search field** will be concealed.

14. Relay Setting

14.1. Relay Switch Setting

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



Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (Ranging from 1-10 Sec). For example, if you set the delay time as **5** Sec. Then the relay will not be triggered until 5 seconds after you press **unlock** tab.
- **Hold Delay (Sec):** set the relay hold delay timing (Ranging from 1-10 Sec). For example, if you set the hold delay time as **5** Sec. Then the relay will be delayed for 5 seconds after the door is unlocked.
- **DTMF Mode:** select the number of DTMF digits for the door access control (**Ranging**

from 1-4 digits) For example, you can select a 1-digit DTMF code or a 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.** For example, you are required to set the 3-digit DTMF code if **DTMF Mode** is set as 3 digits.

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

Note

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

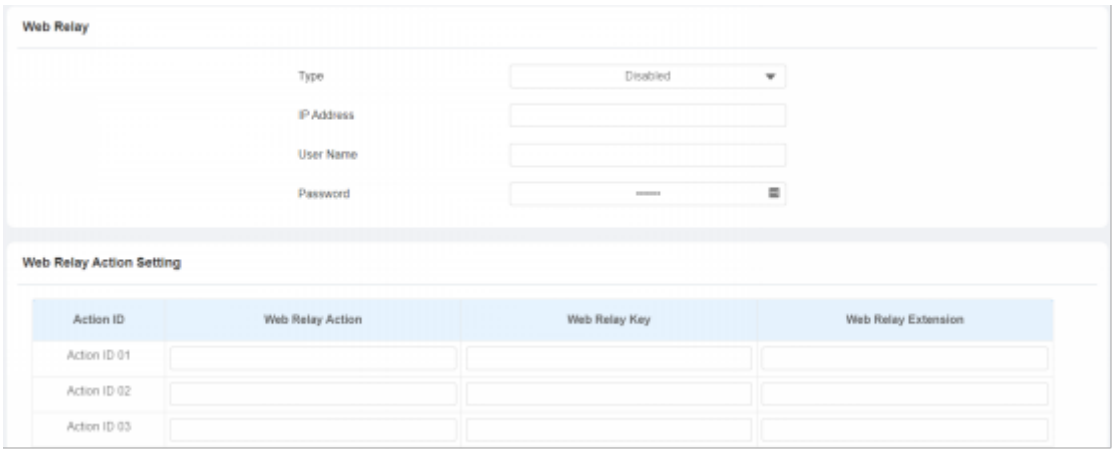
14.2. Web Relay Setting

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

14.2.1. Configure Web Relay on the Web Interface

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

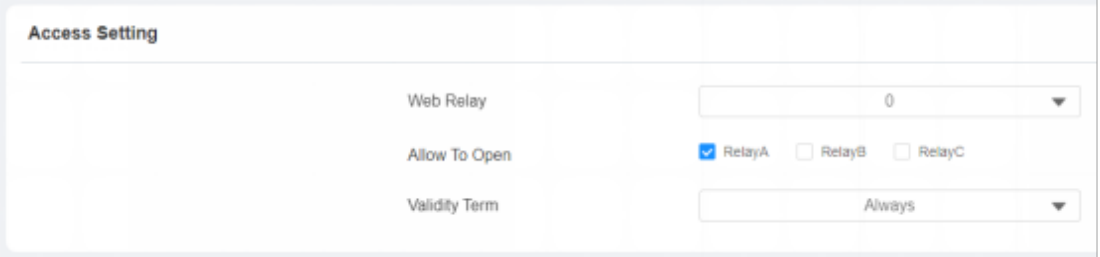
To configure it, go to **Access Control > Web Relay** interface.



Parameter Set-up:

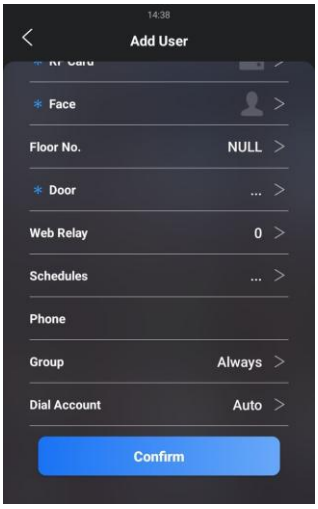
- **Type:** select among three options **Disabled**, **WebRelay**, and **Both**. Select **WebRelay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.
- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.
- **User Name**: enter the User name provided by the web relay manufacturer.
- **Password:** enter the password provided by the web relay manufacturer. The password is authenticated via HTTP and you can define the passwords using **http get** in Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **Web Relay Key:** enter the configured DTMF code, when the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.

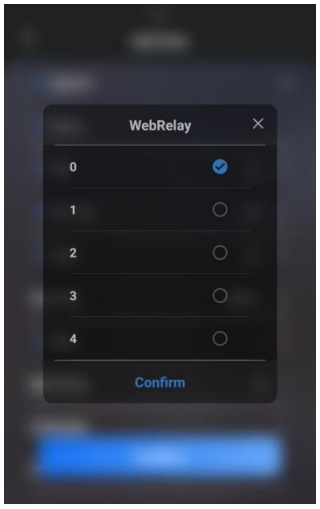
To configure the configuration on the web **Access Control > User** interface.


Access Setting
Web Relay
0
Allow To Open
RelayA
RelayB
RelayC
Validity Term
Always

14.2.2. Configure Web Relay Configuration on the Device

You can select the web relay action ID to trigger certain web relay actions, for example for the door opening. Go to **Setting> User**, then press **Add**.

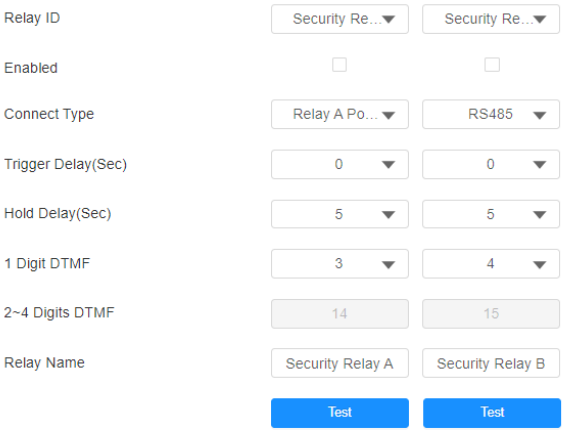




14.3. Security Relay

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

Security Relay



Parameter Set-up:

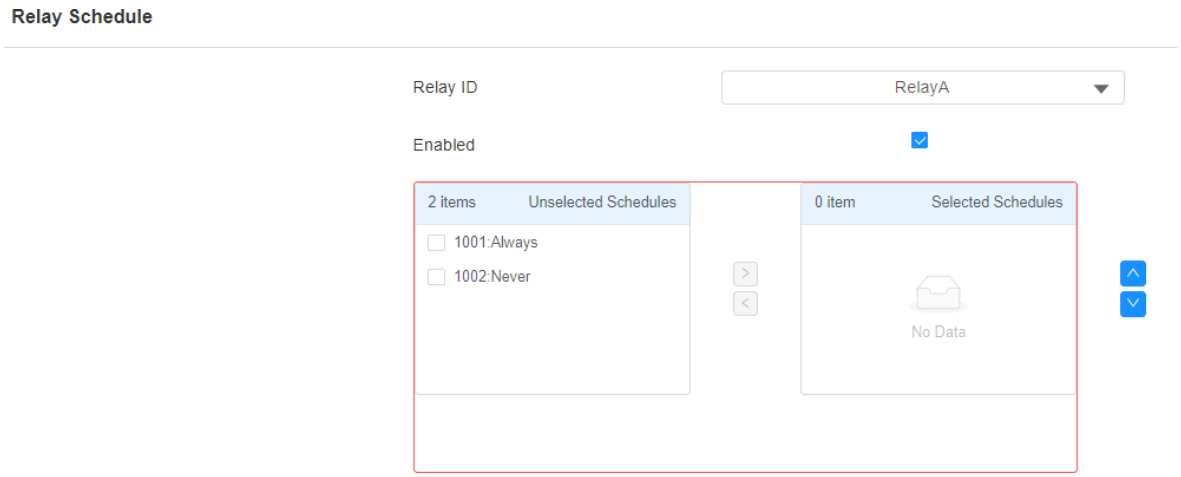
- **Relay ID**: displays relay ID.
- **Connect Type**: select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Connect Delay (Sec)**: set the relay trigger delay timing (ranging from 1-10 Sec.) For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press Unlock tab. The default is 0 meaning triggering relay right after you press the unlock tab.
- **Hold Delay (Sec)**: set the relay hold delay timing (ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. then the relay will be delayed for 5 after the door is unlocked.
- **1-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-digit DTMF code if DTMP Mode is set as 3-digits.
- **Relay Name**: give a name to the relay if needed. And relay name can be edited on the SmartPlus cloud and SDMC.
- **Enabled**: enable the security relay you want.

You can also test the security relay on the device, go to **Security > Security Relay**.


12:23
Security Relay
Test Security Relay A
Test Security Relay B

14.4. Relay Schedule

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



Parameter Set-up:

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

Note

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

15. Door Access Schedule Management

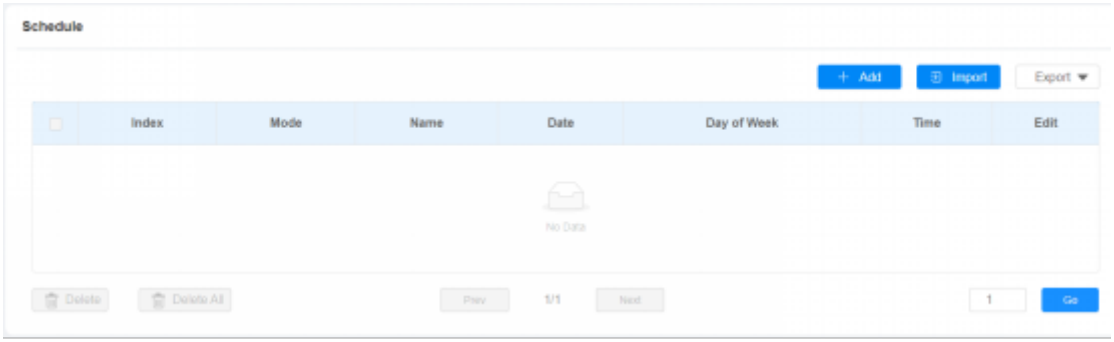
You are required to configure and make a schedule for the user-based door access via RF card, Private PIN, and Facial recognition.

15.1. Access Schedule

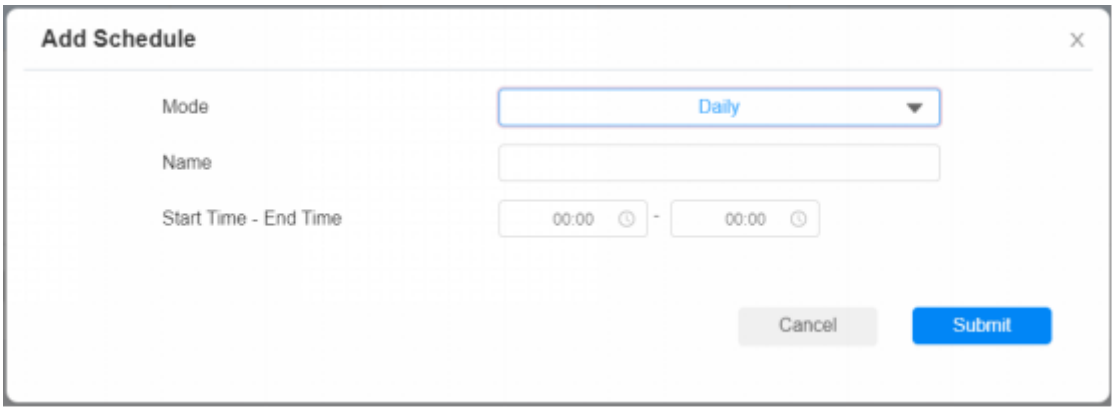
You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual users or a group of users created. Moreover, you can edit your door access schedule if needed.

15.1.1. Create 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 configure it, go to the **Setting > Schedule** interface.



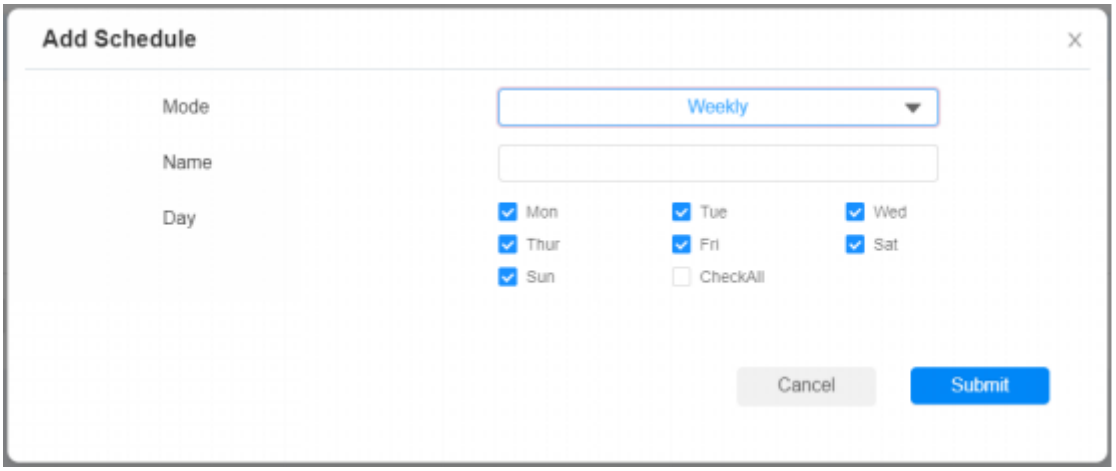
To create a daily schedule, you can do as follows:



Parameter Set-up:

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

To create a weekly schedule:

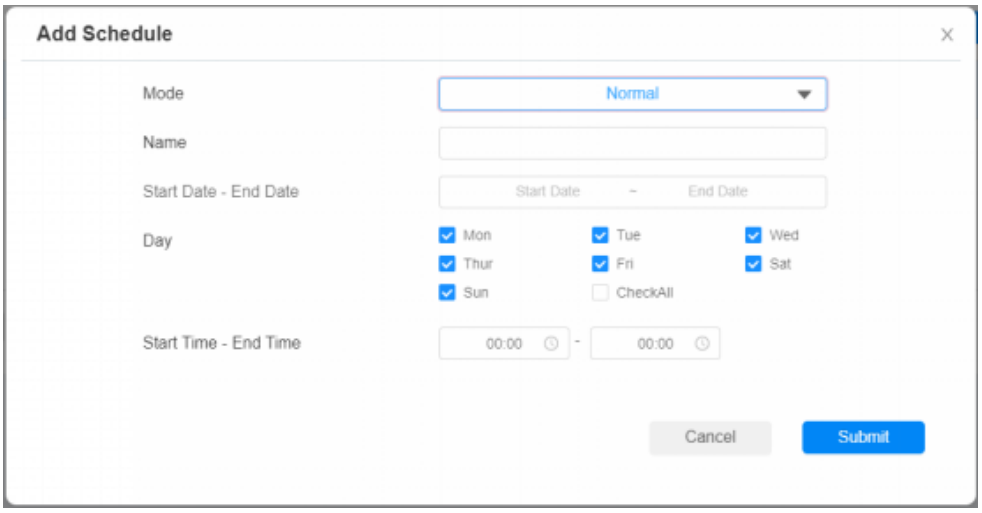


Parameter Set-up:

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

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

To create a longer period schedule:



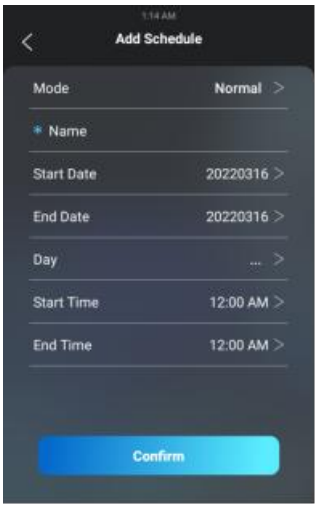
Parameter Set-up:

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

15.1.2. Create Access Schedule on the Device

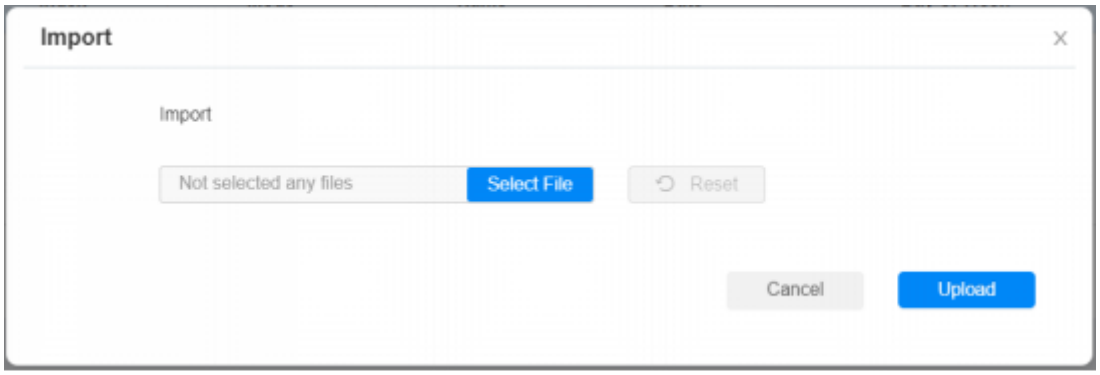
You can also create a door access schedule on the device. Path: Basic **Setting > Schedule**

> Add.



15.1.3. Import and Export Access Schedule

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



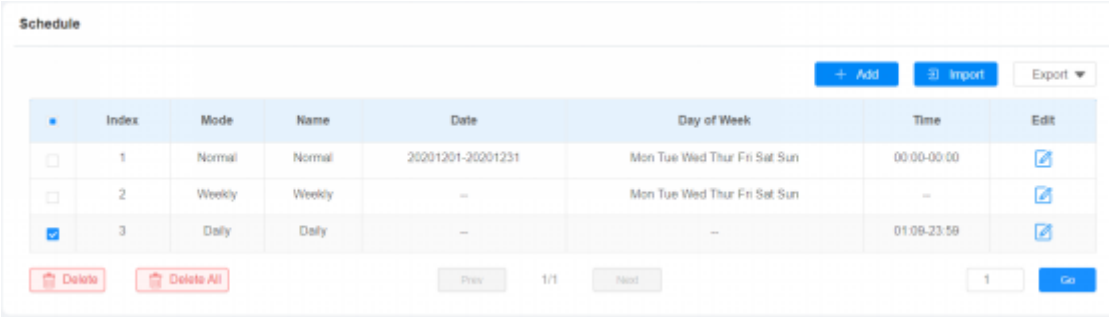
Note

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

15.1.4. Edit the Door Access Schedule

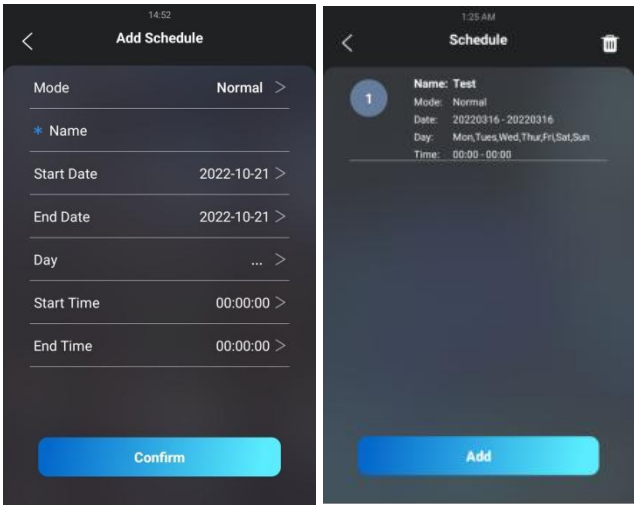
15.1.4.1. Edit the Door Access Schedule on the Web Interface

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



15.1.4.2. Edit the Door Access Schedule on the Device

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



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

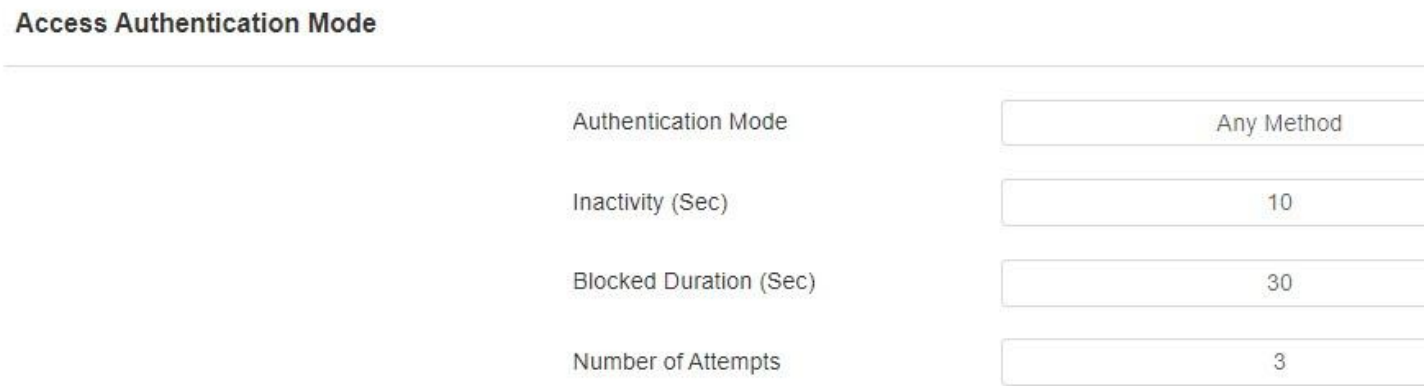
16. Door Unlock Configuration

S539 series door phone offers you three types of door access via PIN code, RF card, and Facial recognition. You can configure them on the device and web interface. Moreover, you can import or export the configured files to maximize your RF card configuration efficiency.

16.1. Access Authentication

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

On the web, navigate to **Settings> Key Display > Access Authentication Mode.**

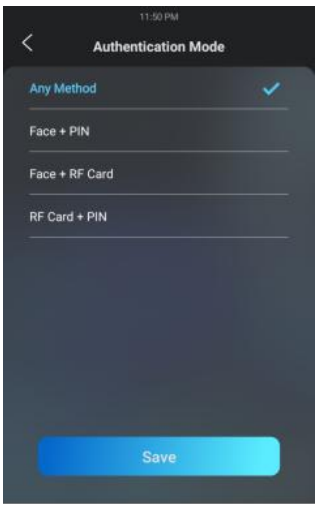


Parameter Set-up:

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

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

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



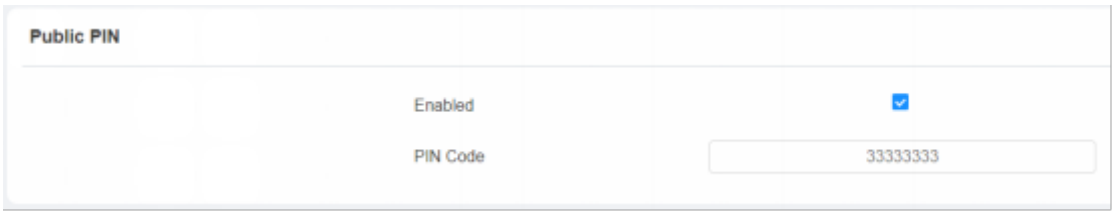
16.2. Configure PIN Code for Door Unlock

You can create and modify both the Public PIN code and the private PIN code for door access on the door phone.

16.2.1. Configure Public PIN code

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

Access > Control > PIN Setting > Public PIN interface.



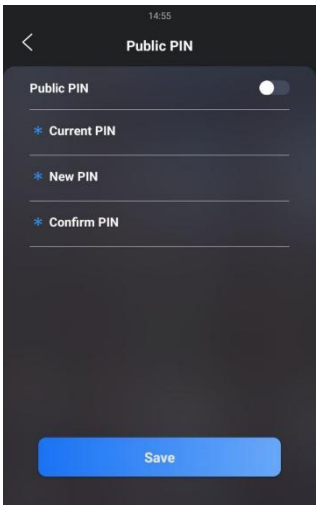
Note

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

Parameter Set-up:

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

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



Note

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

16.2.2. Add User

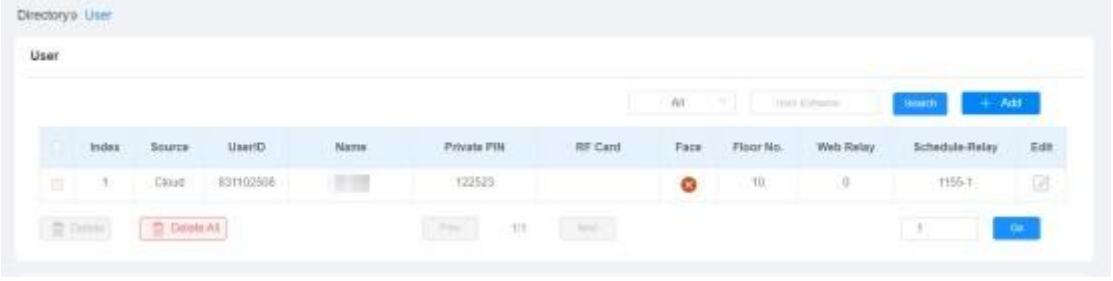
You need to create a user before you can set up a private PIN, RF card, and face data for the user. Also, you can set up access control settings and related call settings for the user. Go to **Directory > User >User Basic**.

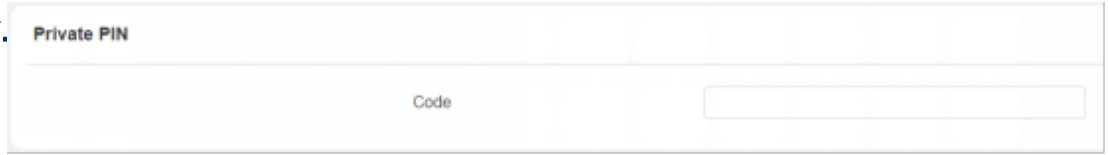
Parameter Set-up:

- **User ID:** User ID can be generated by the system automatically.
- **Name**: enter the username.

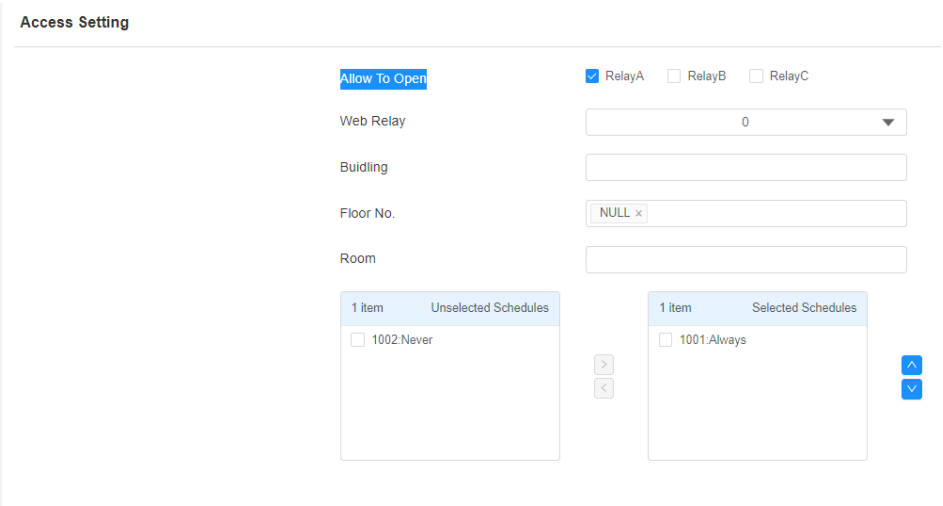
16.2.3. Configure Private PIN Code on the Web Interface

On the web interface, you can not only set up the PIN code but also set and select the door access schedule that you created for the validity of the PIN Code access during a certain time span you scheduled. In addition, you can set the limit for the total number of valid PIN code door access. To configure the configuration on the web **Directory > User** interface.





Select door access schedule for Private PIN Code door access:



Parameter Set-up:

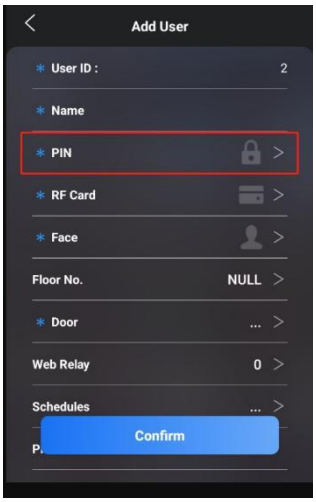
- **Allow To Open Relay:** select the relay for the door unlock for the user.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Building**: enter the build name.
- **Floor NO:** enter the resident's floor number.
- **Schedule:** select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

Note

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

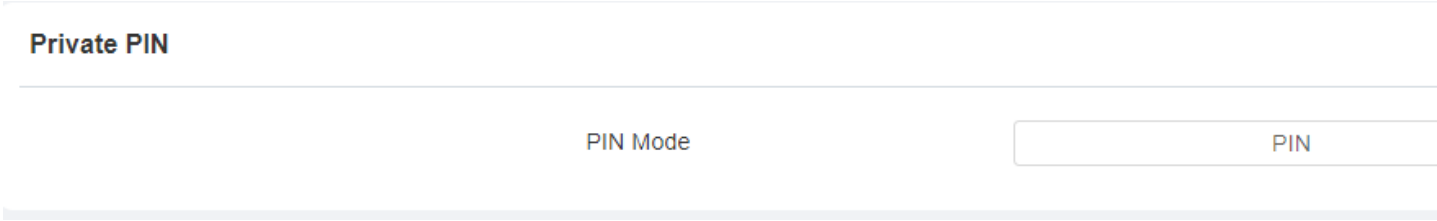
16.2.4. Configure Private PIN Code on the Device

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



16.2.5. Configure Private PIN Access Mode

The door phone offers you two types of access modes for private PIN code access, namely **PIN** and **APT#+PIN**. To configure it, go to **Access Control > PIN Setting > Private PIN**.



Parameter Set-up:

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

Note

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

Note

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

16.3. Configure RF Card for Door Unlock

16.3.1. Configure RF Card on the Web Interface

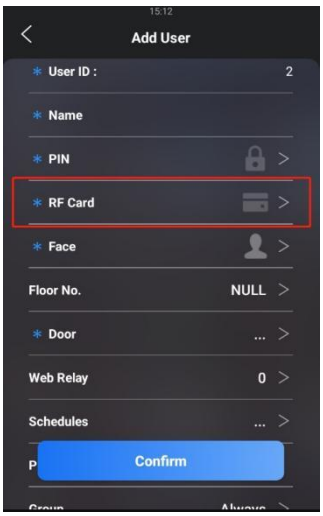
To configure the configuration on the web **Directory > User > RF Card**.

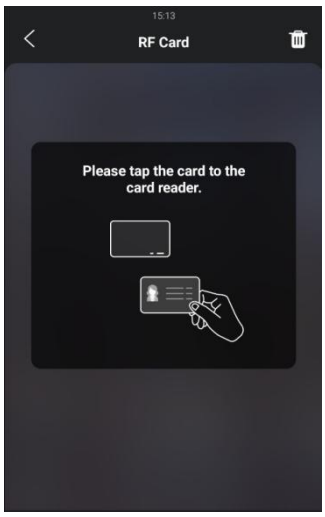
Note

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

16.3.2. Configure RF Card on the device

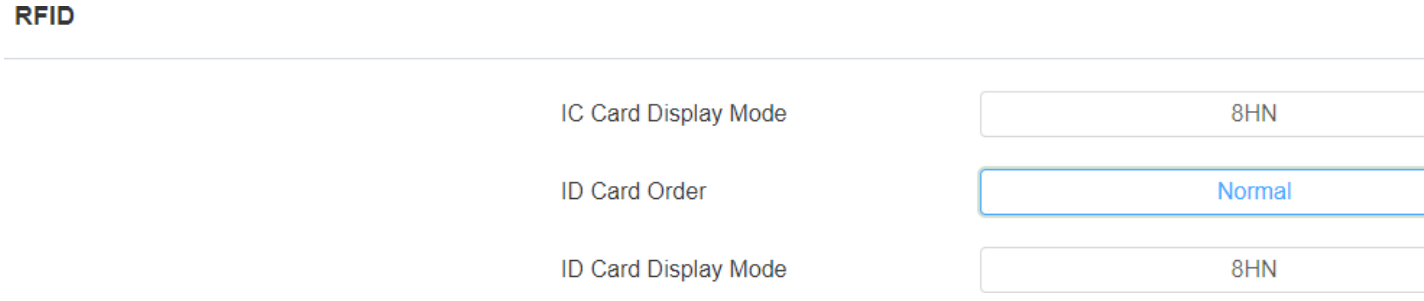
You can configure the RF card directly on the device for the door access while setting up the time schedule for the validity of the RF card access along with the web relay that can be triggered with the RF card etc. To configure the language display on the device **Setting > User > Add** interface.





16.3.3. Configure RF Card Code Format

If you want to integrate with the third-party intercom system in terms of RF card door access, you can change the RF card code format to be identical to that applied in the third-party system. To configure it, go to **Access Control > Card Setting** interface.

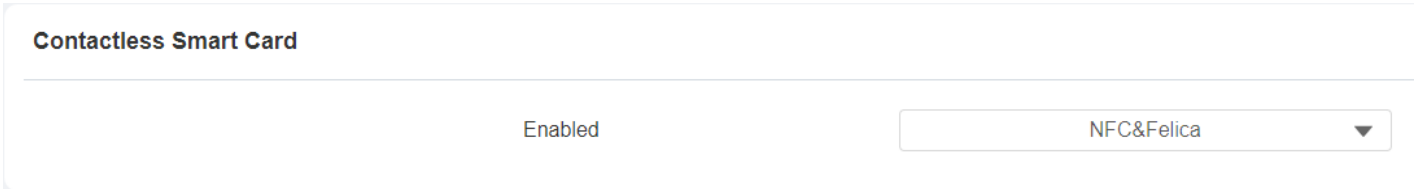


Parameter Set-up:

- **IC-Card Display Mode**: select the card format for the **ID Card** for the door access (**8H10D, 6H3D5D(W26), 6H8D, 8HN, and 8HR)**. The card code format is 8HN by default.
- **ID Card order**: select ID card reading in normal order or reversed order. You might need to select card orders for third-party integration (eg. third-party access control). and you can also reverse the card number for card protection.
- **IDCard Display Mode:** Select the card format for the **ID Card** for the door access: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR, 6H3D5D-R(W26), And 8HR10D.** The card code format is 8HN by default in the door phone.

16.4. Contactless Smart Card

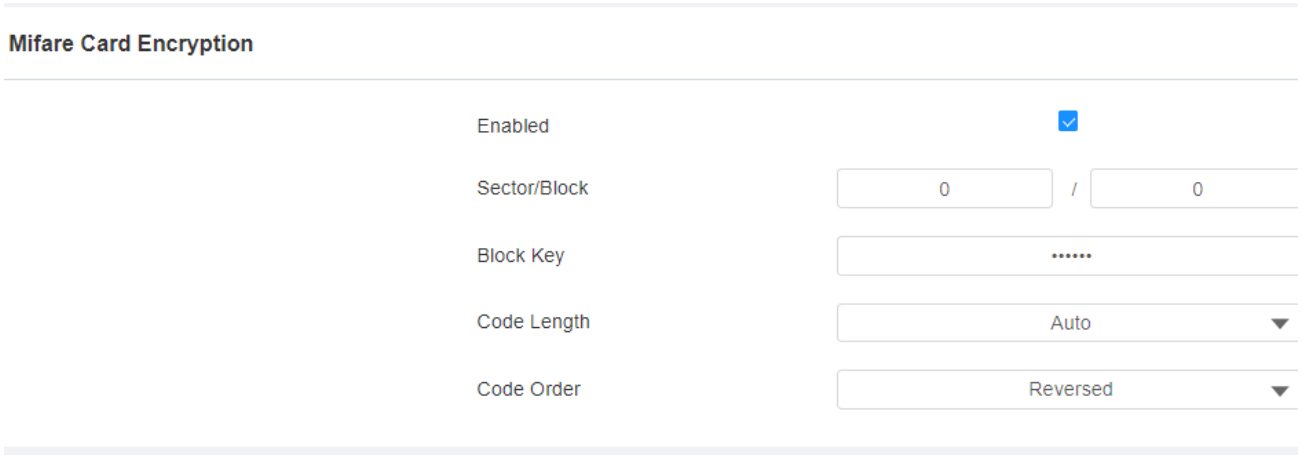
You can select an NFC card or Felica card for contactless access. For example, if you enable both NFC and Felica cards, you can gain contactless entry with the two types of cards. Path: **Access Control > Card Setting.**



16.5. Mifare card Encryption

The door phone can read the encrypted Mifare card for greater security. To do so you can

navigate to **Access Control > Card setting > Mifare Card Encryption.**



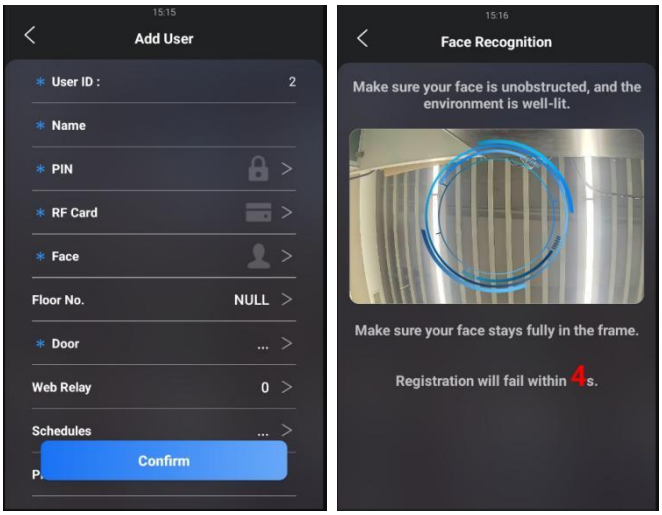
Parameter Set-up:

- **Enabled**: enable the Mifare/ Defire Card Encryption.
- **Sector/Block**: enter the sector and block in which the card number is located in the Mifare/ Defire Card. For example, the card number can be in sector 3 and block 3 in the card.
- **Block Key**: enter the block password for access.
- **Code length**: select the code length:
  - if Auto is selected, the door phone will send the exact number of bytes of the card code it reads to the access control system for the door opening.
  - if 7 Byte to 4 Byte is selected, then the door phone will convert the 7-byte card to 4 bytes by taking the four bytes in the middle while ignoring the first byte and the last two bytes.

16.6. Configure Facial Recognition for Door Unlock

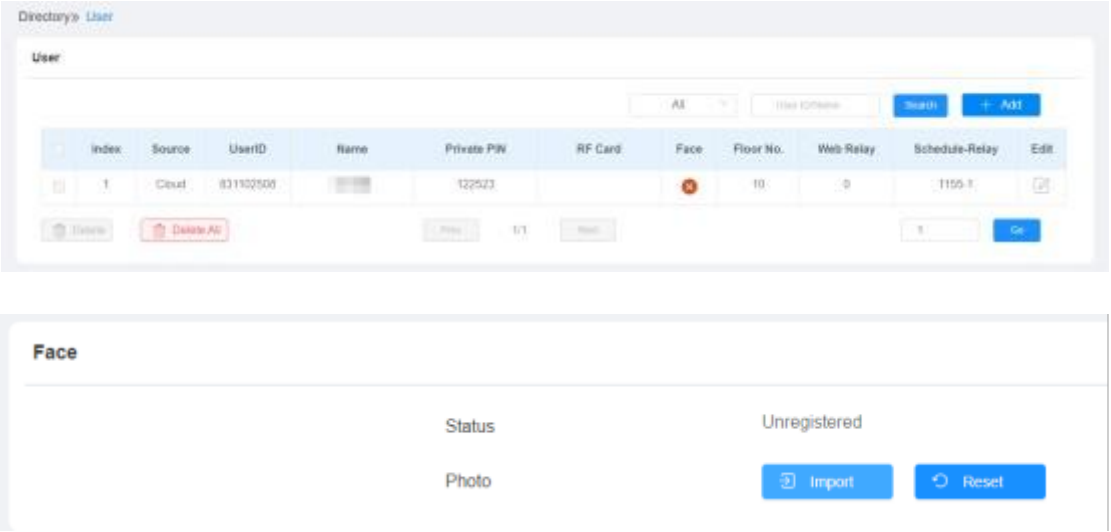
16.6.1. Enroll Face Data on the Device

You can enroll face data on the device by entering the user's name and registering your facial ID on the device for door access. To do it on the device, go to **Setting > User > face** interface.



16.6.2. Upload Face Data on the Web Interface

You can upload the face data to the device on the web interface. To do so, go to **Directory > User,** then click **+Add**. After that, you can upload the face photo.

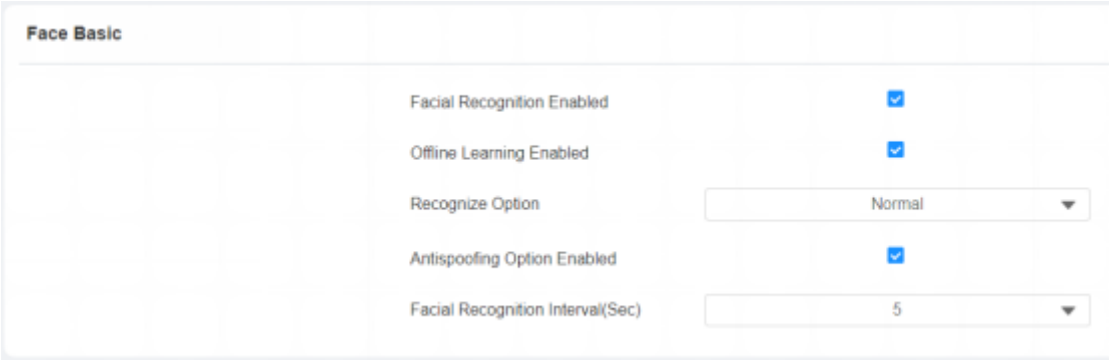


Note

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

16.6.3. Configure Facial Recognition on Web Interface

The door phone allows you to adjust facial recognition accuracy, and recognition intervals according to your actual need. And you can also improve the recognition quality and user experience through the basic facial recognition setting. To configure it, go to **Access Control > Face Setting** interface.



Parameter Set-up:

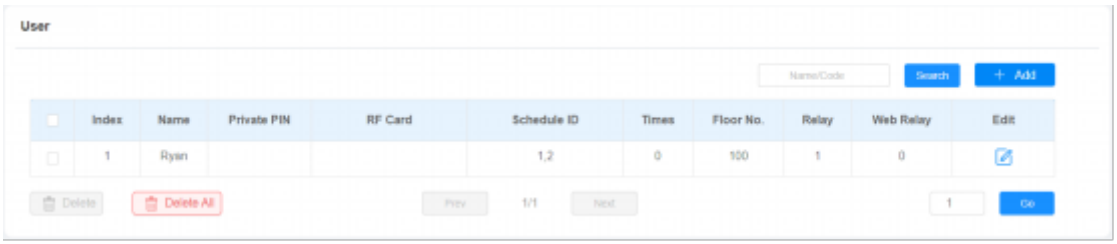
- **Face Recognition:** click on **Enable** to turn on the facial recognition function. Facial recognition is enabled by default.
- **Offline Learning:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor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

- **Antispoofing Option:** select the Anti-spoofing level among four options: **Low, Normal, High, and Highest.** For example, if you select **Highest** then there will be the least possibility that the device will be fooled by digital images or pictures of any kind.

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

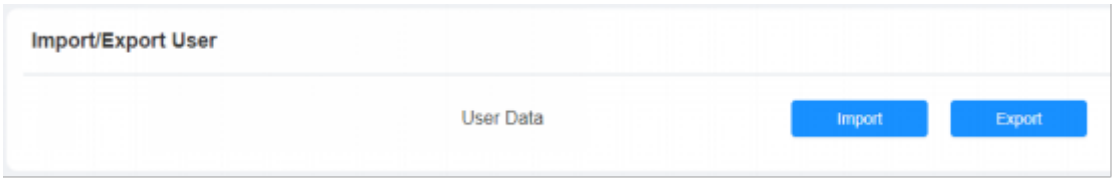
16.7. Edit the User-specific door Access Data

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



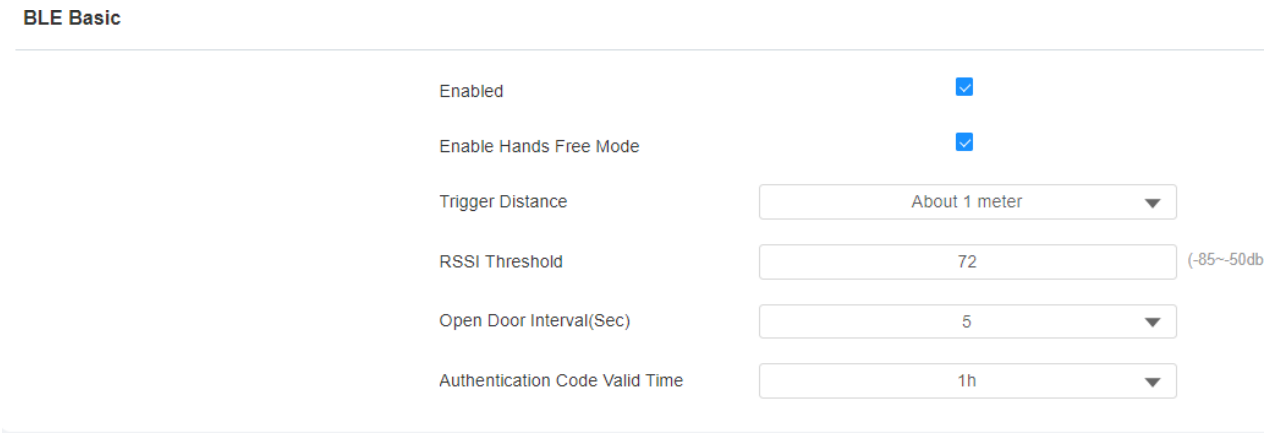
16.7.1. Import and Export User Data of Access Control

The door phone supports User Data of access control to be shared among Akuvox S539 series door phones through import and export while you can also export the facial data out of the door phone and then import it to a third-party device. To configure it, go to **Access Control > User > Import/Export User** interface.



16.8. Configure Bluetooth for Door Unlock

You can gain hands-free door entry via the Bluetooth-enabled SmartPlus app. You can open the door hands-free or wave your hands to the door phone as you walk closer to the door. To set up the function, navigate to **Access Control > BLE > BLE Basic**.



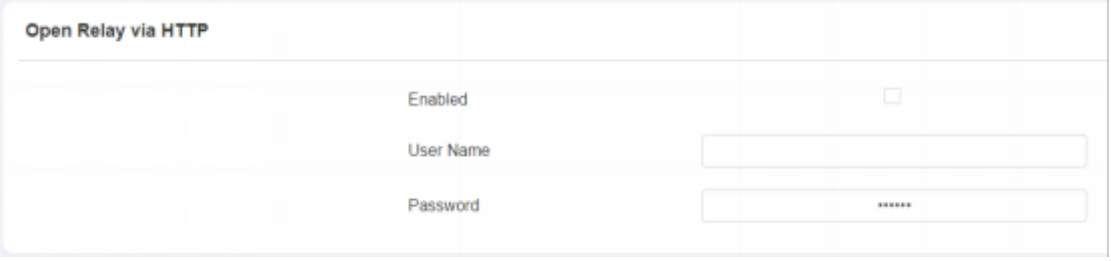
Parameter Set-up:

- **Enabled:** enable the Bluetooth function.
- **Enable Hands Free Mode:** if enabled, you can gain door access hands-free. If disabled, you have to wave your hand in front of the door phone for door entry.
- **Trigger Distance**: set the triggering distance of the Bluetooth for the door access. You select **About 1 meter**, **Within 1 meter**, and **More than 2 meters**. The trigger distance is **3 meters maximum**.
- **RSSI Threshold:** select the signal receiving strength from -85~-50db in absolute terms, The higher value it is, the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval (Sec):** select the time interval between every two Bluetooth door accesses.

- **Authentication Code Valid Time**: set the valid time for the authentication code that you use for matching your SmartPlus App or My Mobilekey App with the door phone for the Bluetooth-enabled hands-free door entry. for example, if you set it as 1 hour, then you have to use the authentication for the matching within one hour after the code is generated.

16.9. Configure Open Relay via HTTP for Door Unlock

You can unlock the door remotely without approaching the device physically for door entry by typing in the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for door entry. To set it up, go to **Access Control > Relay > Open Relay via HTTP** interface.



Parameter Set-up:

- **Enable:** Enable the HTTP unlock.
- **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:

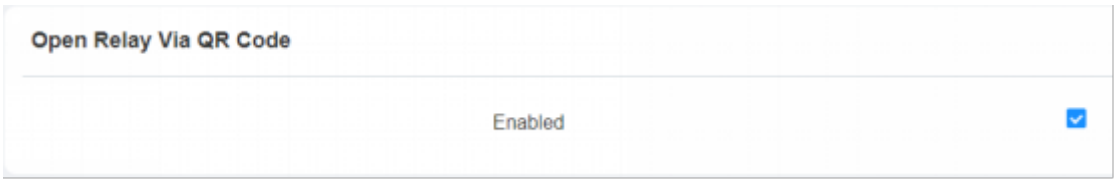
http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note

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

16.10. Unlock by QR Code

QR code is another option for door access. If you want to apply for QR code access, you need to enable the QR code function. To set it up, go to **Access Control > Relay > Open Relay via QR Code** interface.

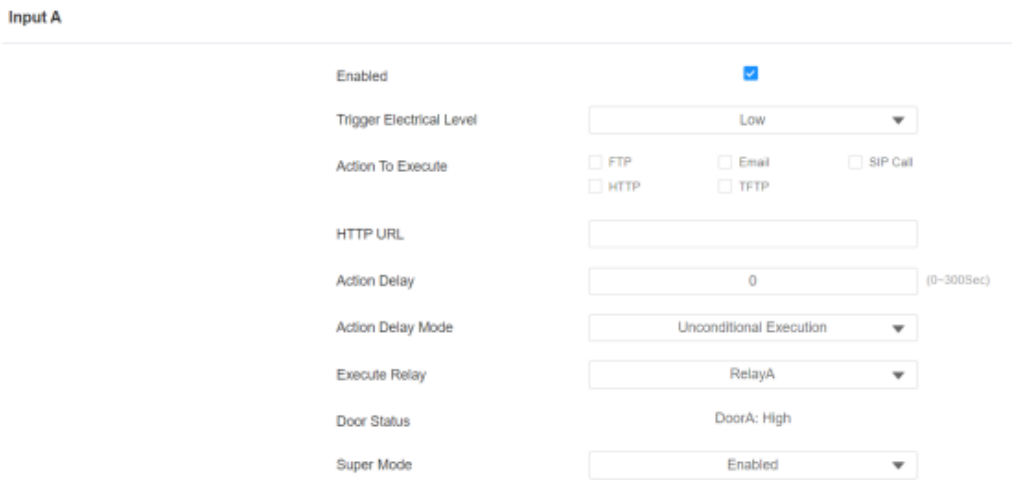


Note

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

16.11. Configure Exit Button for Door Unlock

When you need to open the door from inside using the Exit button installed by the door, you can configure the door phone Input to trigger the relay for the door access. To configure it, go to **Access Control > Input > Input** interface.



Parameter Set-up:

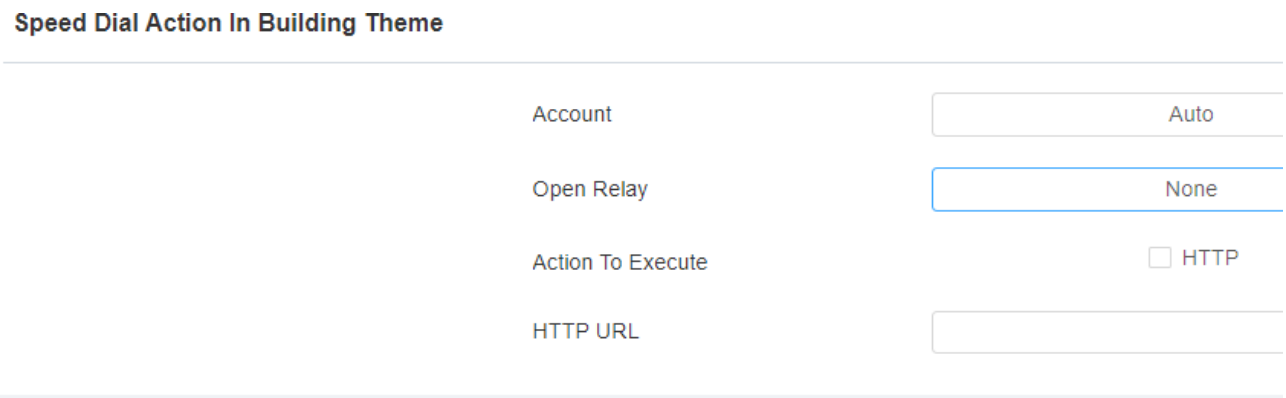
- **Enabled**: it is enabled by default.

- **Trigger Electrical Level:** select the trigger electrical level options between **High** and **Low** according to the actual operation of the exit button.
- **Action to Execute:** select the method to carry out the action among four options: **FTP**, **Email**, **HTTP**, and **TFTP**.

- **HTTP URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after you press the button(input is triggered).
- **Action Delay Mode**: if you select **Unconditional Execution**, then action will be carried out when the input is triggered. If you select **Execute If Input Still Triggered**, then the action will be carried out if the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of the input signal.
- **Super Mode**: if you enable the super mode, the administrator will be able to open the door using an RF card even when the door phone breaks down or malfunctions.

16.12. Configure Reception Tab for Door Unlock

On the device's home screen, the door phone provides residents and visitors quick door access by pressing the **Reception** tab at the bottom of the home screen. To configure it, go to **Setting > Key/Display > Speed Dial Action In Building Theme** interface.



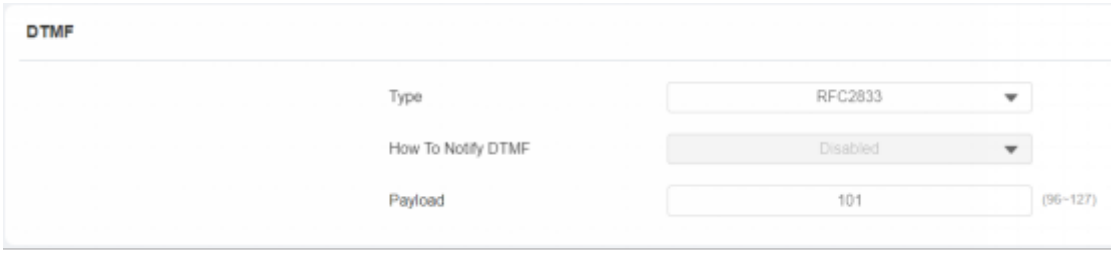
Parameter Set-up:

- **Open Relay:** select the relay(s) to be triggered by pressing the Reception Icon.

- **Action To Execute:** tick the check box to enable the HTTP option.
- **HTTP URL:** enter the URL command to be sent for door access. For example, http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

16.13. Unlock by DTMF Code

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



Parameter Set-up:

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

Note

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

17. Security

17.1. Tamper Alarm Setting

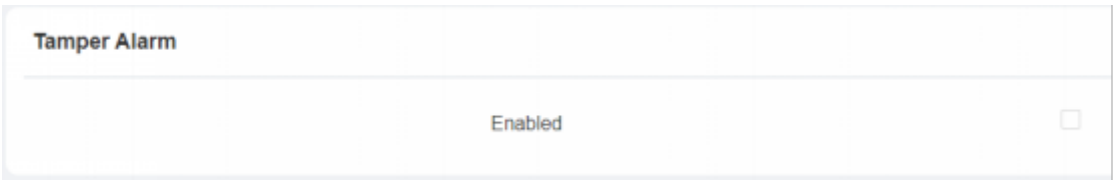
The tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm while sending out calls to the designated location. The tamper alarm will be triggered off when the door phone changes its gravity value as opposed to its original gravity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

17.1.1. Configure Tamper Alarm on the Device

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

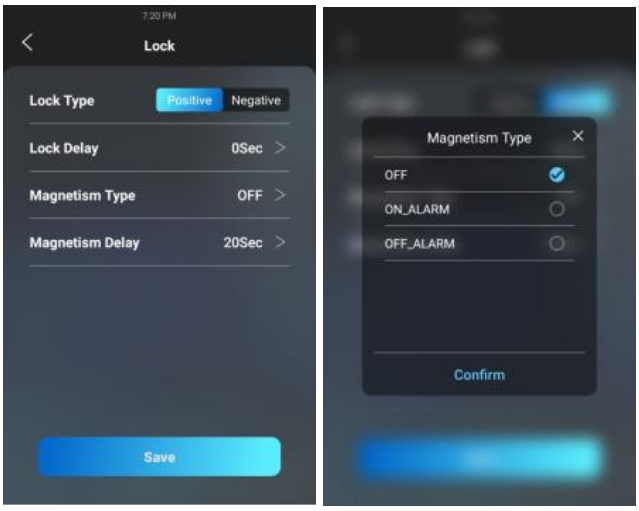
17.1.2. Configure Tamper Alarm on the Web Interface

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



17.2. Lock Security

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



Parameter Set-up:

- **Lock Type**: select **Positive** for the lock that unlocks when the power is on and select **Negative** for the lock that unlocks when the power is off.
- **Lock Delay**: select door unlocks delay time after you are granted door access. The delay time range is from 0-10 seconds.

- **Magnetism Type**: select **OFF** if you want to disable the door sensor and alarm. To set the alarm trigger type, you must select **ON-ALARM** and **OFF_ALARM** according to the type of lock you applied. Select **ON_ALARM** for a positive lock, while select **OFF_ALARM** alarm for a negative lock.

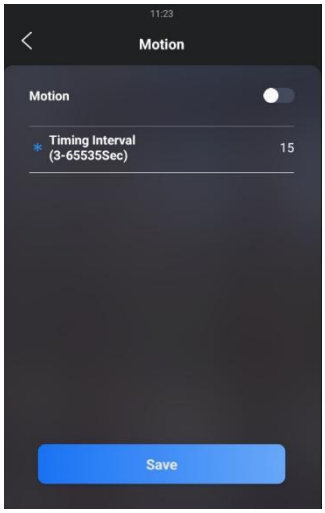
- **Magnetism Type:** select the alarm delay time after its being triggered. The delay range is from 10-120 seconds.

17.3. Motion Detection

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

17.3.1. Configure Motion Detection on the Device

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



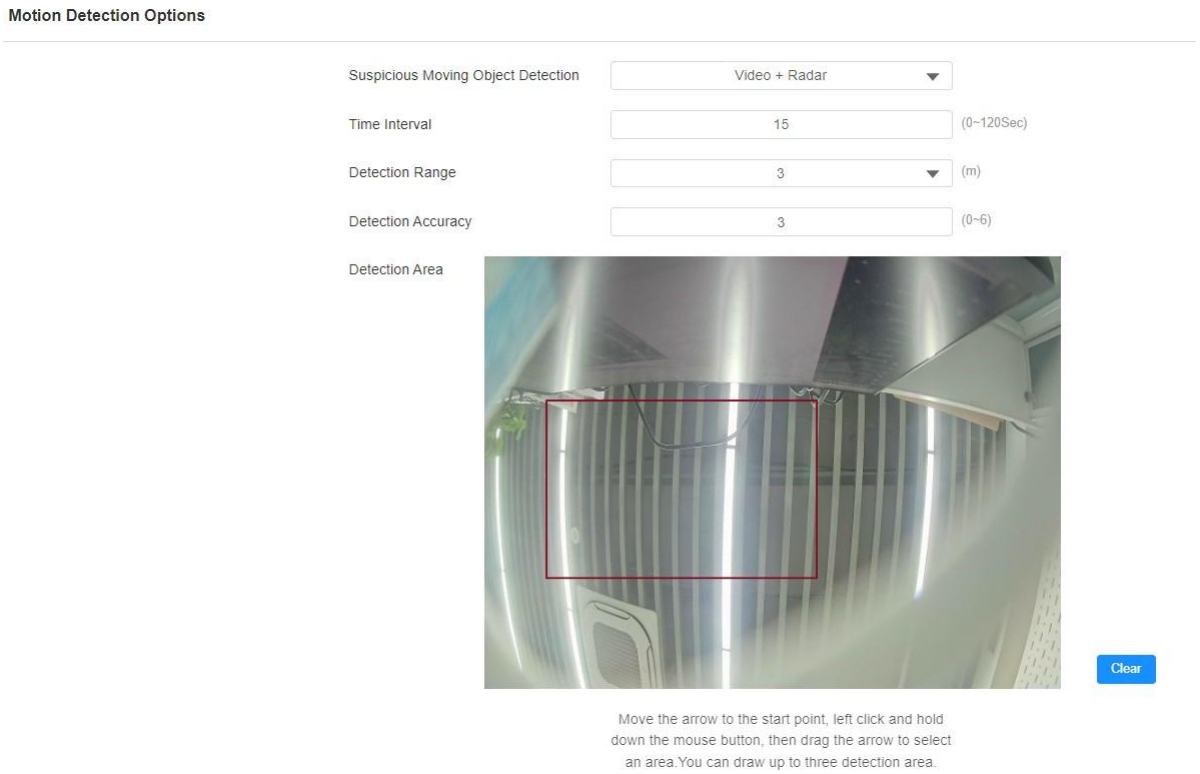
Parameter Set-up:

- **Interval**: the absolute triggering interval is 3 seconds. If you select a number greater than 3 seconds, then it requires a second triggering interval to trigger the alarm. For example, if you select 3 seconds, then the alarm will be triggered when a moving object is detected one time from 0 to 3 seconds (triggered any time from 0 to 3

seconds). However, for example, if you select 5 seconds (greater than 3), then the alarm will not be triggered until a moving object is detected for the second time from 3 to 5 seconds (triggered any time from 3 to 5 seconds). The default interval is 10 seconds.

17.3.2. Configure Motion Detection on the Web Interface

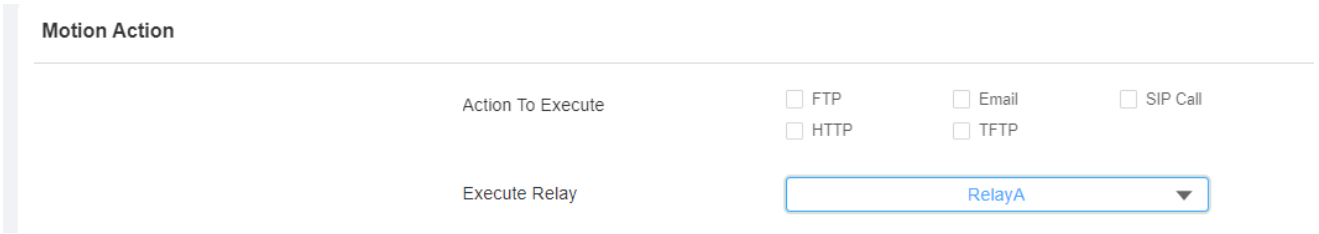
On the device web interface, you can not only configure the time interval but also the motion detection sensitivity and notification type when the motion detection action is triggered. To configure the configuration on the web **Surveillance > Motion > Motion Detection Options** interface.



- **Suspicious Moving Object Detection**: tick the check box to enable the motion detection function.
- **Time Interval**: set the time interval in the same way as you do on the device.

- **Detection Range:** set the radar detection range (1-3 meters). The default detection range is 3 meters.
- **Detection Accuracy**: set the detection accuracy for the detection sensitivity (0-6). The higher value, the greater sensitivity. The default detection accuracy value is 3.

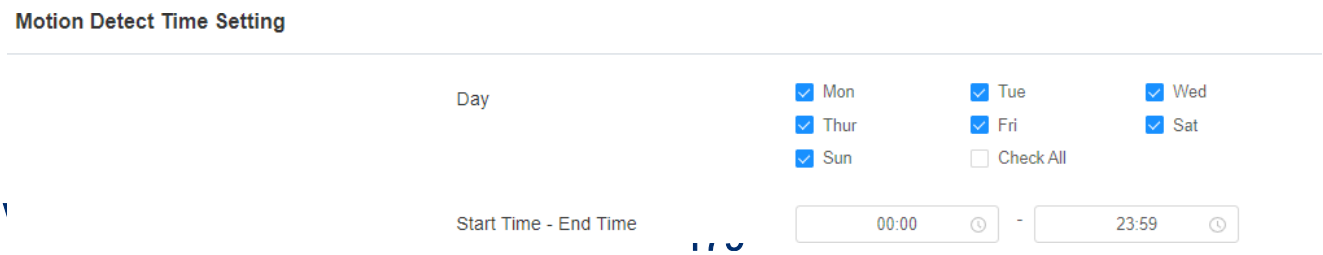
After you set up the interval, you can set up the action you need.



Parameter Set-up:

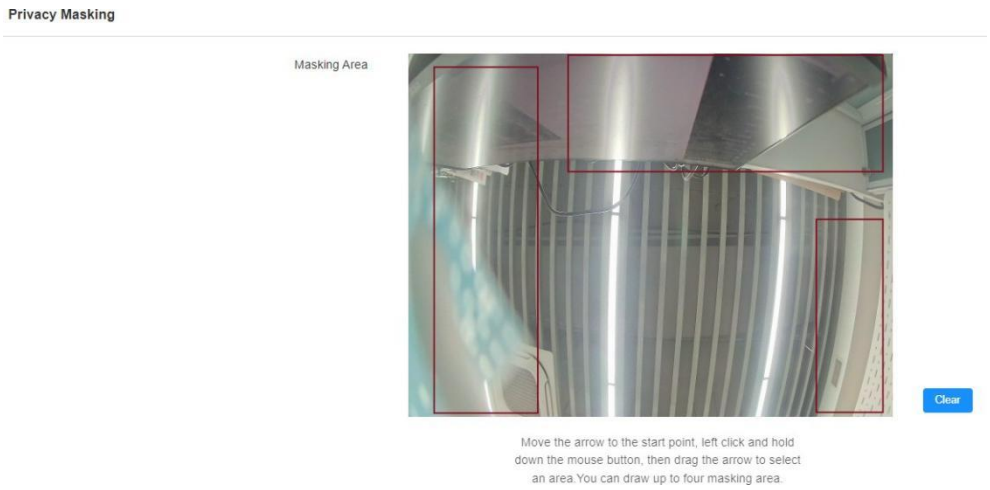
- **Action To execute**: select the method to carry out the action: FTP, Email, HTTP, TFTP, SIP Call. For example, if you select **Email**, then an Email will be sent to you after the motion detection alarm is triggered.
- **Action HTTP URL**: enter the HTTP command that will be sent to a third-party server to carry out the predefined action.
- **Action Relay**: select one of the door phone relays to carry the predefined action.

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



17.4. Privacy Masking

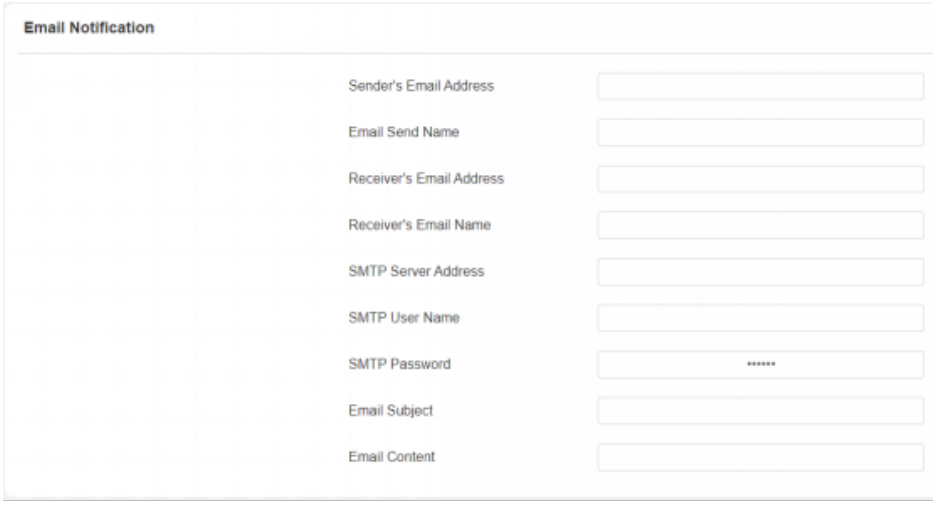
This feature is used to avoid the infringement of personal privacy. You can select any of the three spots in the video image, and those three spots will be blackened up in the video image for privacy protection. To set it up, go to **Surveillance > Motion > Privacy Masking**.



17.5. Security Notification Setting

17.5.1. Email Notification Setting

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

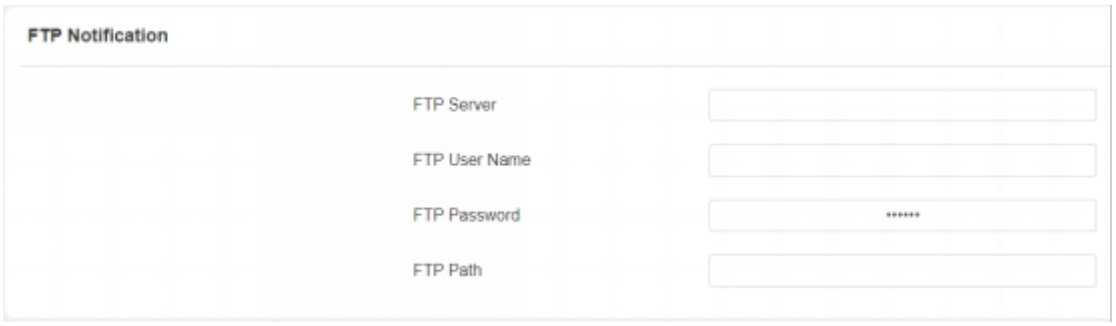

Email Notification
Sender's Email Address
Email Send Name
Receiver's Email Address
Receiver's Email Name
SMTP Server Address
SMTP User Name
SMTP Password
Email Subject
Email Content

Parameter Set-up:

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

17.5.2. FTP Notification Setting

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



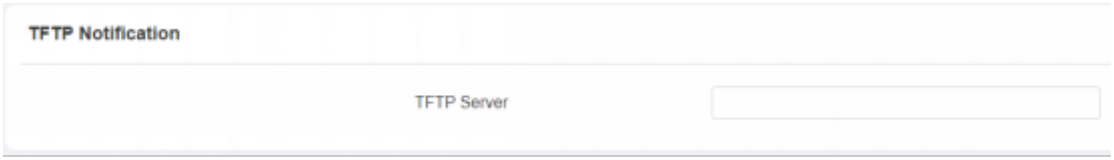
Parameter Set-up:

- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name**: enter the FTP server user name.

- **FTP Password**: enter the FTP server password.
- **FTP Path**: enter the folder name you created in the FTP server.

17.5.3. TFTP Notification Setting

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

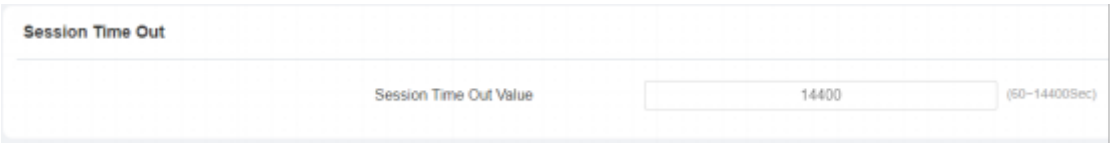


Parameter set-up:

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

17.6. Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation. To configure the configuration on the web **System > Security > Session Time Out** interface.



Parameter Set-up:

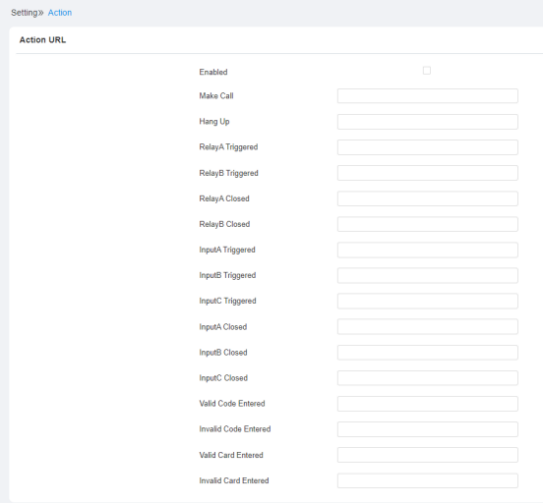
- **Session Time Out Value:** set the automatic web interface log-out timing ranging from 60 seconds to 14400 seconds. The default value is 300.

17.7. Action URL

The door phone allows you to set up specific HTTP URL commands that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occur any changes in the relay status, input status, PIN code, and RF card access for security purposes. You can navigate to **Settings > Actions URL**.

Note

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



Akuvox Action URL:

No	Event	Parameter format	Example

1	Make Call	$remote	Http://server ip/ Callnumber=$remote

2	Hang Up	$remote	Http://server ip/ Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Relay Closed	$relay1status	Http://server ip/ relayclose=$relay1status
5	Input Triggered	$input1status	Http://server ip/ inputtrigger=$input1status
6	Input Closed	$input1status	Http://server ip/ inputclose=$input1status
7	Valid Code Entered	$code	Http://server ip/ validcode=$code
8	Invalid Code Entered	$code	Http://server ip/ invalidcode=$code
9	Valid Card Entered	$card_sn	Http://server ip/ validcard=$card_sn
10	Invalid Car Entered	$card_sn	Http://server ip/ invalidcard=$card_sn
11	Tamper Alarm Triggered	$alarm status	Http://server ip/ tampertrigger=$alarm status

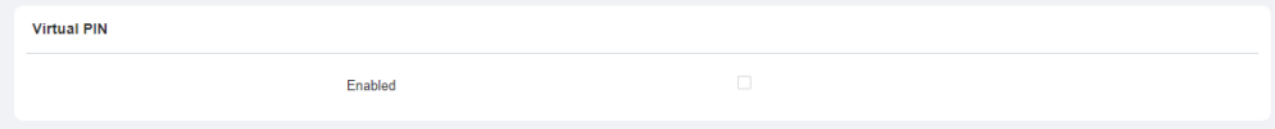
For example:

http://192.168.16.118/help.xml?

mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

17.8. Virtual PIN

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



Parameter Set-up:

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

Note

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

Parameter Set-up:

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

is applied, then the virtual password will be matched with the users who pass the first level of authentication, for example, Face + PIN.

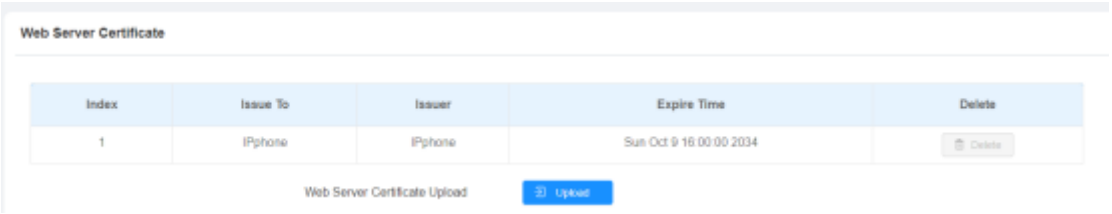
17.9. Client Certificate Setting

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

- **Web Server Certificate:** it is the certificate that sends to the client for authentication when the client requires an SSL connection with the Akuvox door phone. Currently, the format of the certificate that can be accepted by Akuvox door phone is *.PEM file.
- **Client Certificate:** when Akuvox door phone required an SSL connection with the server, the phone must verify the server to make sure it can be trusted. And the server will send its certificate to the Akuvox door phone. Then the door phone will verify this certificate according to the client certificate list.

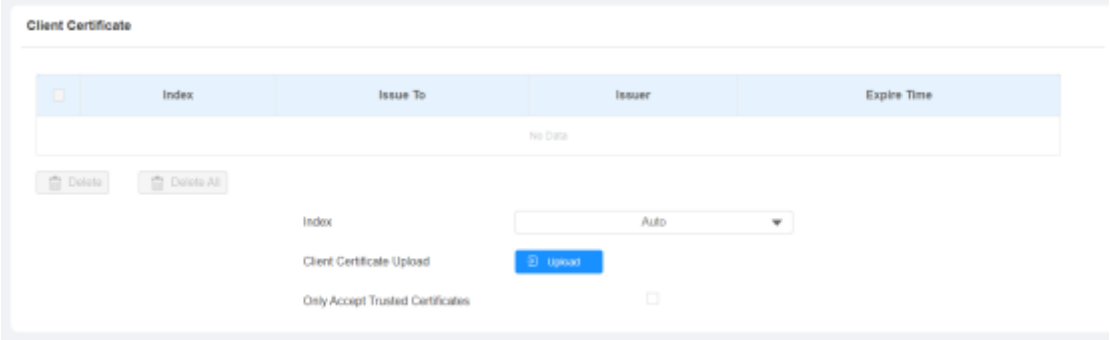
17.9.1. Web Server Certificate

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



17.9.2. Client Certificate

To upload and configure client certificates on the same page.



Parameter Set-up:

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

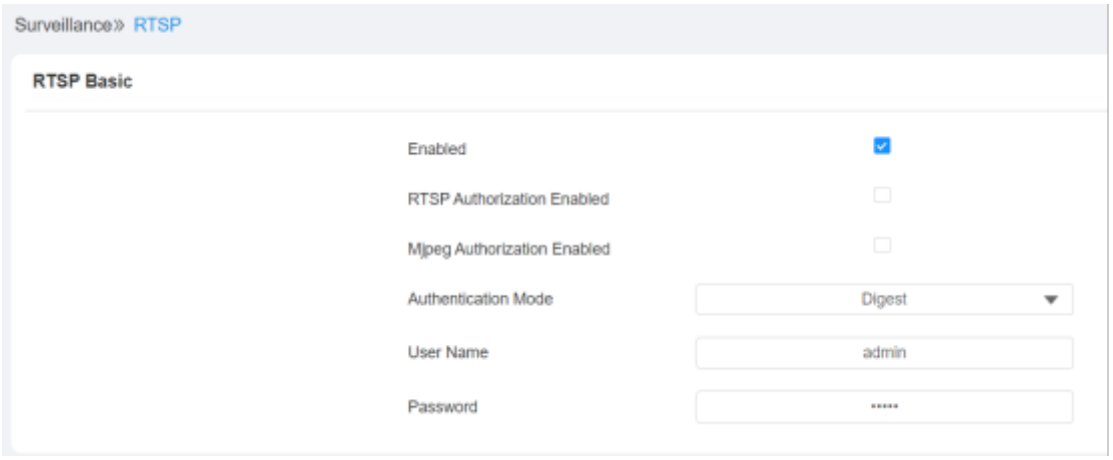
18. Monitor and Image

18.1. RTSP Stream Monitoring

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

18.1.1. RTSP Basic Setting

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



Parameter Set-up:

- **Enabled:** tick the check box to turn on or turn off the RTSP function.
- **RTSP Authorization Enabled**: enable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP

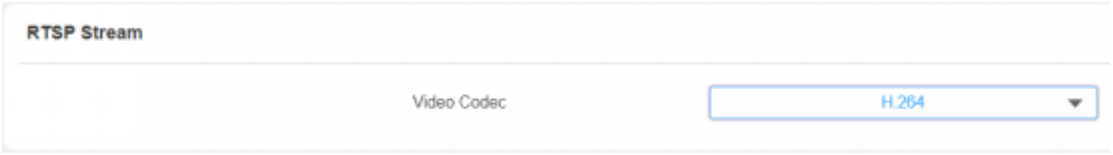
Username, and RTSP Password on the intercom device such as an indoor monitor for authorization.

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

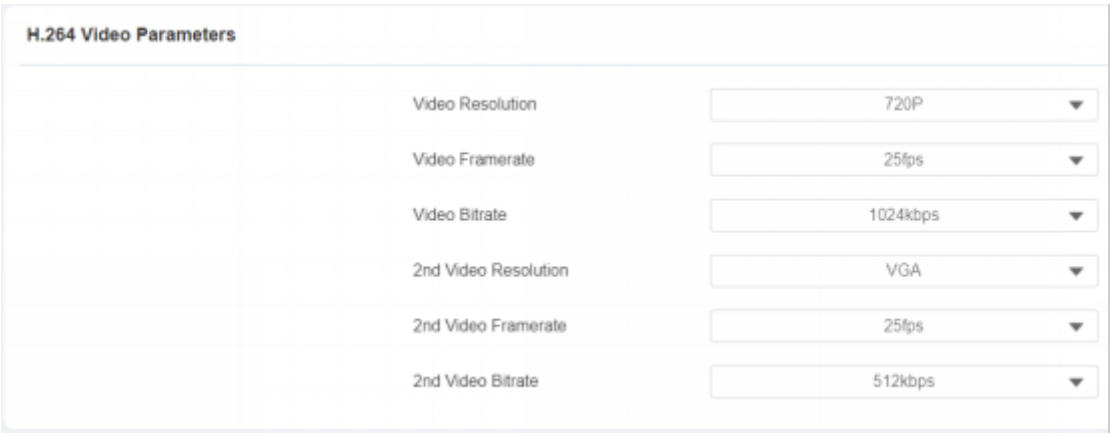
- **Password**: enter the username for the RTSP authentication.

18.1.2. RTSP Stream Setting

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



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



Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: **QCIF**, **QVGA**, **CIF**, **VGA**, **4CIF**, **720P**, and **1080P**. The default video resolution is that the video

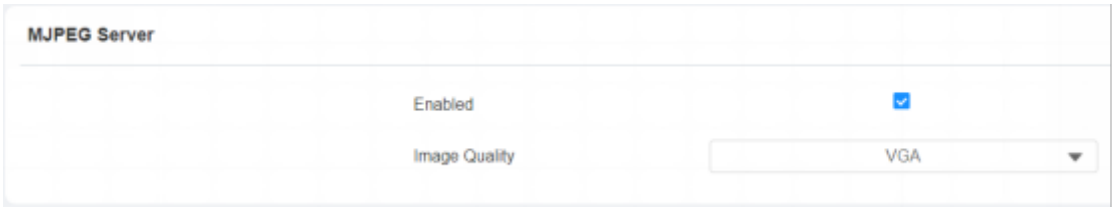
from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than **720P**.

- **Video Framerate: 25fps** is the video frame rate by default.
- **Video Bitrate**: select video bitrate among six options: **128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps** according to your network environment. The default video bitrate is **2048 kbps**.

- **2nd Video Resolution2**: select the 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 default video frame rate for the second video stream channel.
- **2nd Video Bitrate**: select video bitrate among the six options for the second video stream channel. While the second video stream channel is **512 kbps** by default.

18.2. MJPEG Image Capturing

The door phone allows you to capture the Mjpeg format monitoring image if needed. You can enable the MJPEG function and set the image quality on the web **Surveillance > MJPEG** interface.



Parameter Set-up:

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

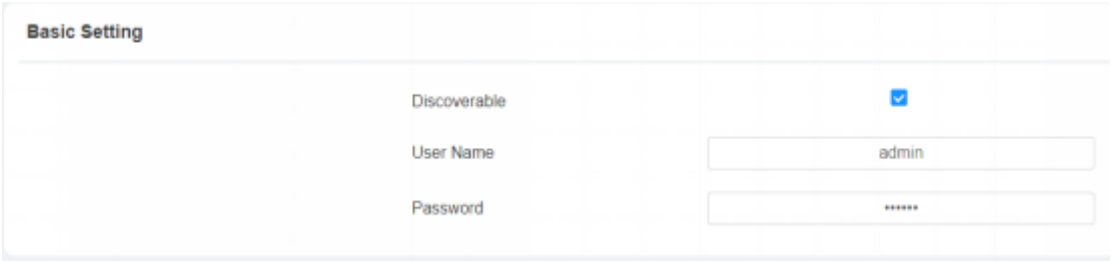
After the MJPEG service is enabled, you can capture the image from the door phone using the following three types of URL format:

- http:// device ip:8080/picture.cgi
- http://deviceip:8080/picture.jpg
- http://deviceip:8080/jpeg.cgi

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

18.3. ONVIF

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



Parameter Set-up:

- **Discoverable:** tick the check box to enable the DiscoverableONVIF mode. If you select **Discoverable** then the video from the door phone camera can be searched by other devices.
- **User Name:** enter the user name. The user name is **admin** by default.
- **Password**: enter the password. The password is **admin** by default.

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

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

Note

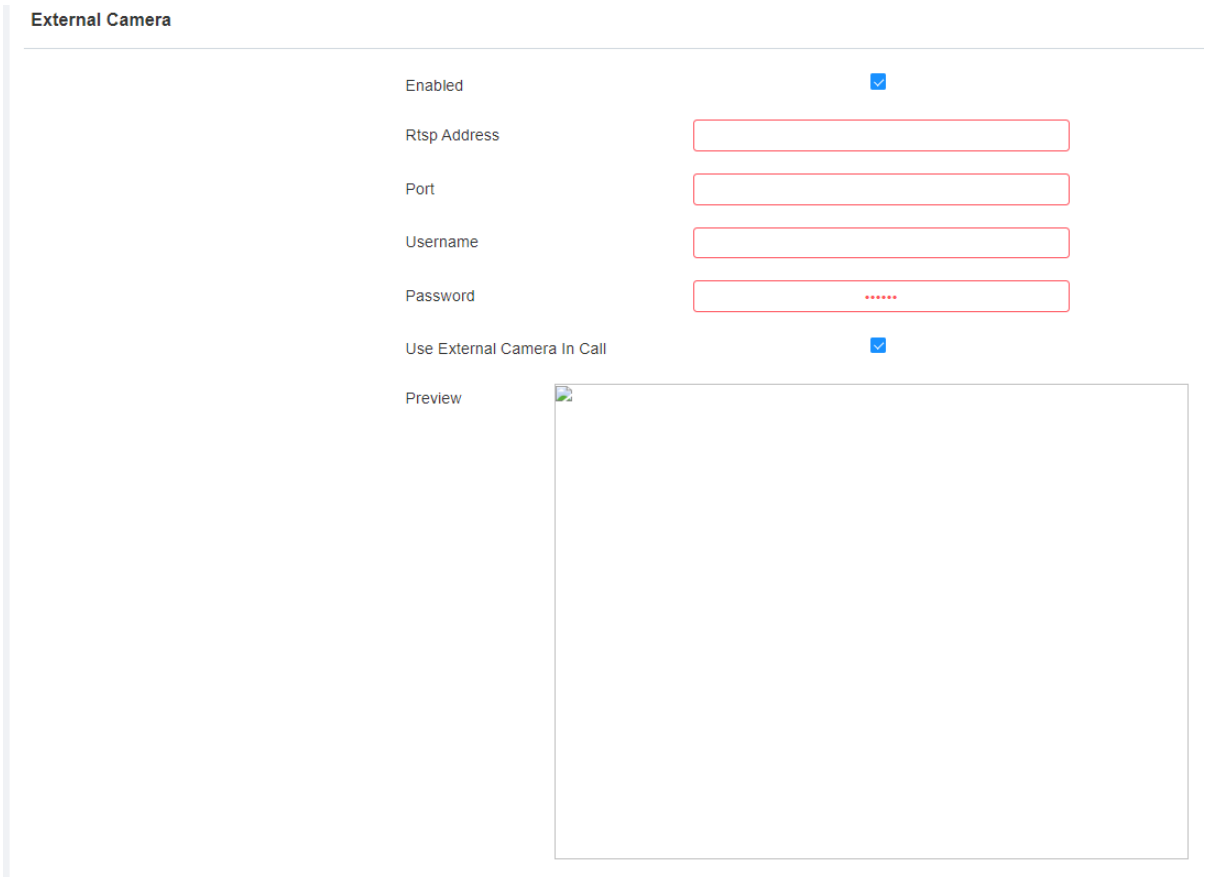
- Fill in the specific IP address of the door phone in the URL.

18.4. Live Stream

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

18.5. External Camera

The door phone can be integrated with a third-party camera.



Parameter Set-up:

- **Enabled:** enable the external features. when it is enabled, the setting will be displayed.
- **RTSP Address**: type in the RTSP address (URL) of the third-party camera.
- **Port**: type in the communication port of the third-party camera.
- **Username**: type in the username used by the third-party camera for RTSP authentication.
- **Password**: type in the password used by the third-party camera for RTSP authentication.
- **User External Camera In Call**: if disabled, the RTSP video from the door phone

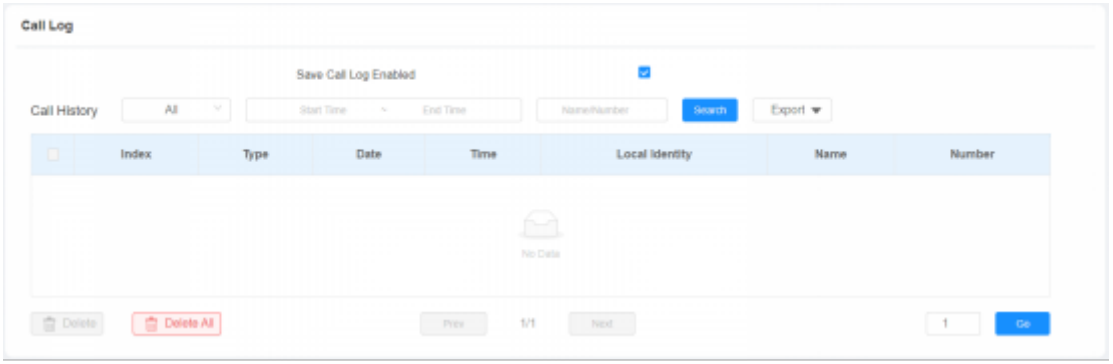
camera will be used during a call. If enabled, the external cameral RTSP video will be used during a call.

- **Preview**: if the external camera is connected properly, the RTSP video from the camera will be displayed. if it is not, then the cause of the failure will be displayed.

19. Logs

19.1. Call Logs

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

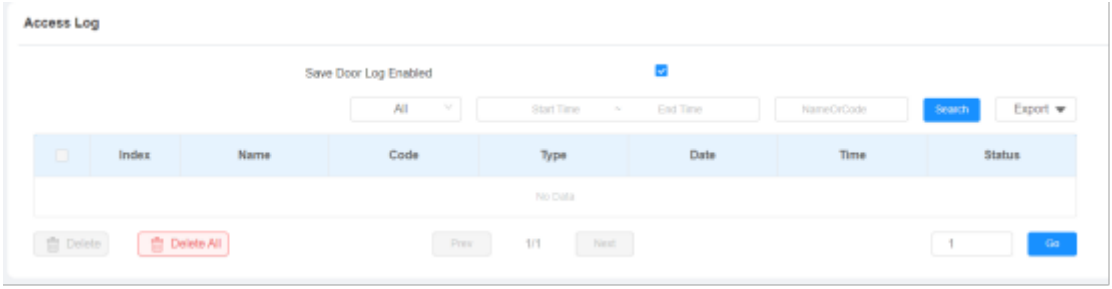


Parameter Set-up:

- **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**, and **Missed** for the specific type of call log to be displayed.
- **Start Time- End Time**: select the specific time span of the call logs you want to search, check, or export.
- **Name/Number**: select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

19.2. Door Logs

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



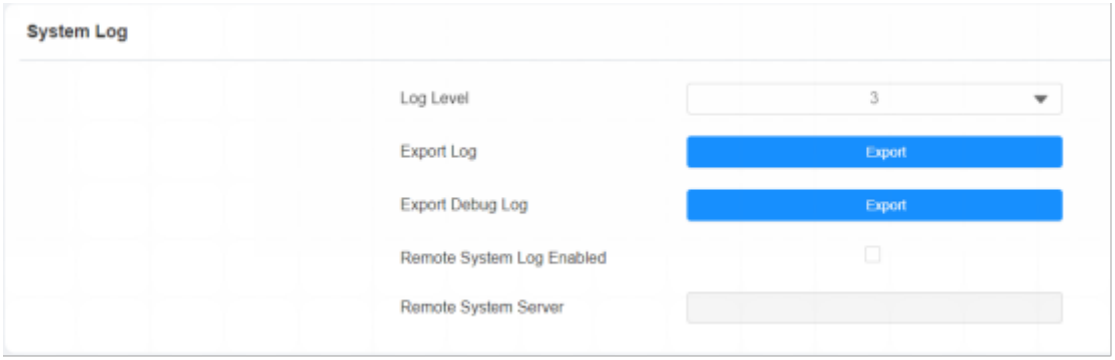
Parameter Set-up:

- **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 the door log by the name or by the PIN code.

20. Debug

20.1. System Log for Debugging

System logs can be used for debugging purposes. If you want to export the system out to a local PC or to a remote server for debugging, you can set up the function on the web **System > Maintenance > System Log interface.**



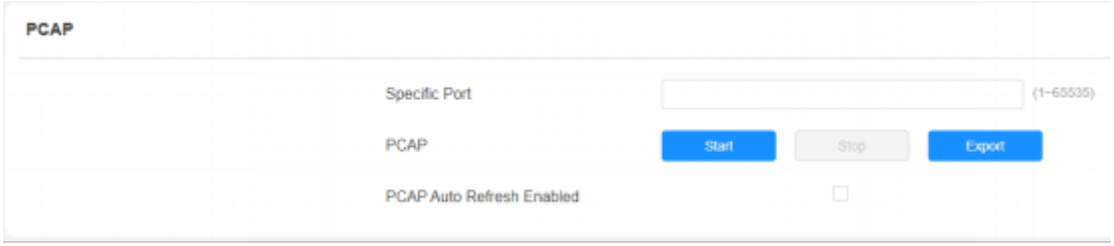
Parameter Set-up:

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

And the remote server address will be provided by Akuvox technical support.

20.2. PCAP for Debugging

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



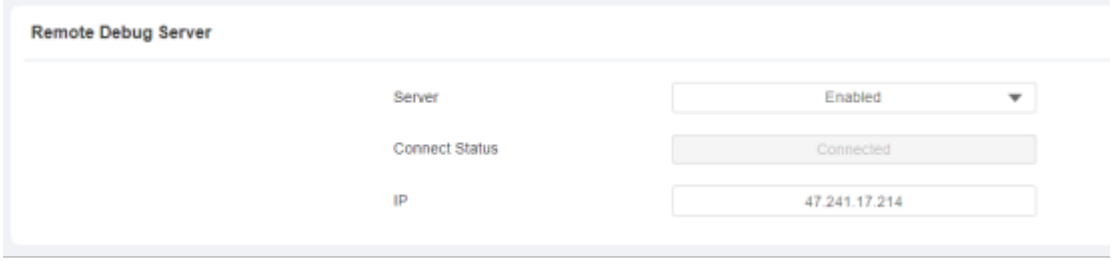
Parameter Set-up:

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

20.3. Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the

device log remotely for debugging purposes. On the web, navigate to **System > Maintenance.**



Parameter Set-up:

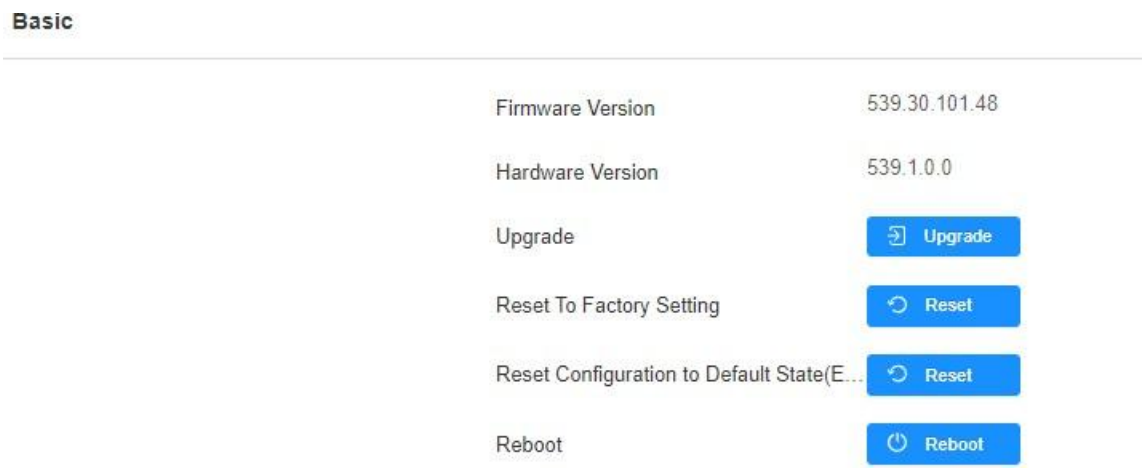
- **Server**: disable or enable the remote debug server.
- **Connect Status**: displays the remote debug server connection status.
- **IP**: enter the remote debug server IP address. Please ask Akuvox technical team for the server IP address.

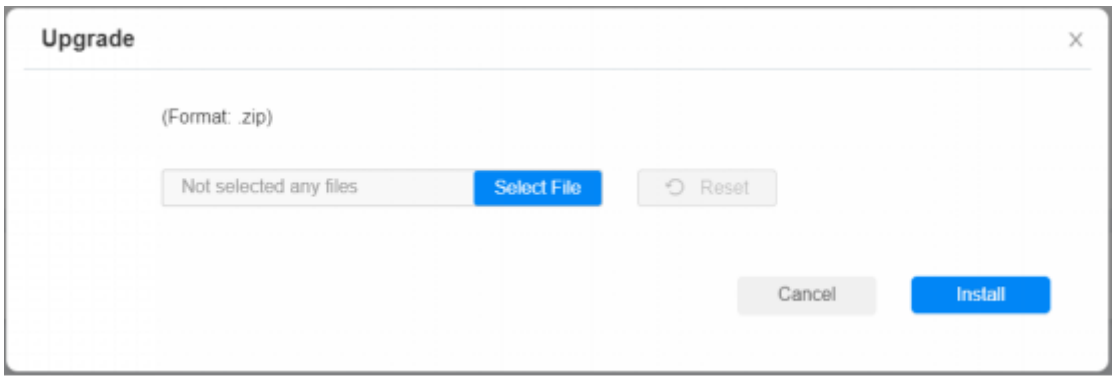
Note

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

21. Firmware Upgrade

S539 series door phones can be upgraded on the device web interface. You can go to **System> Upgrade**.



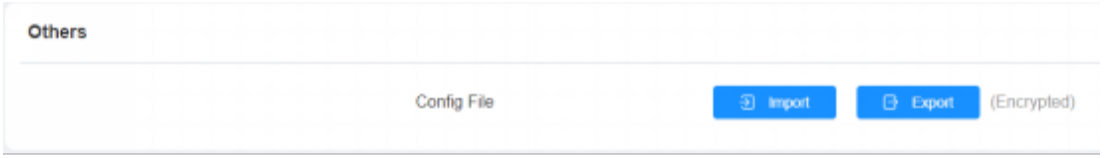


Note

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

22. Backup

If you want to import or export encrypted configuration files to your Local PC, go to **System > Maintenance > Others**.

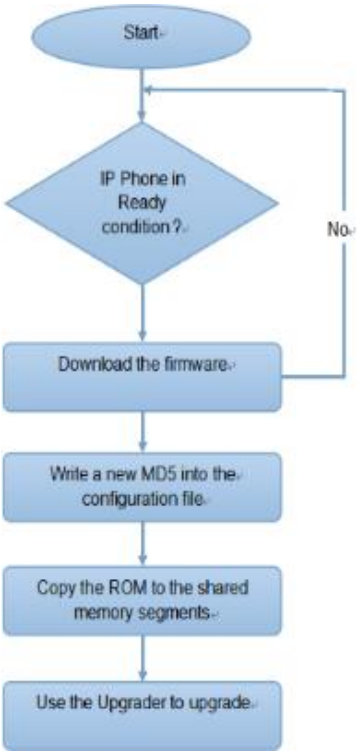


23. Auto-provisioning via Configuration File

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

23.1. Provisioning Principle

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


Start
IP Phone in Ready condition?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments
Use the Upgrader to upgrade

23.2. Configuration Files for Auto-provisioning

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

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

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

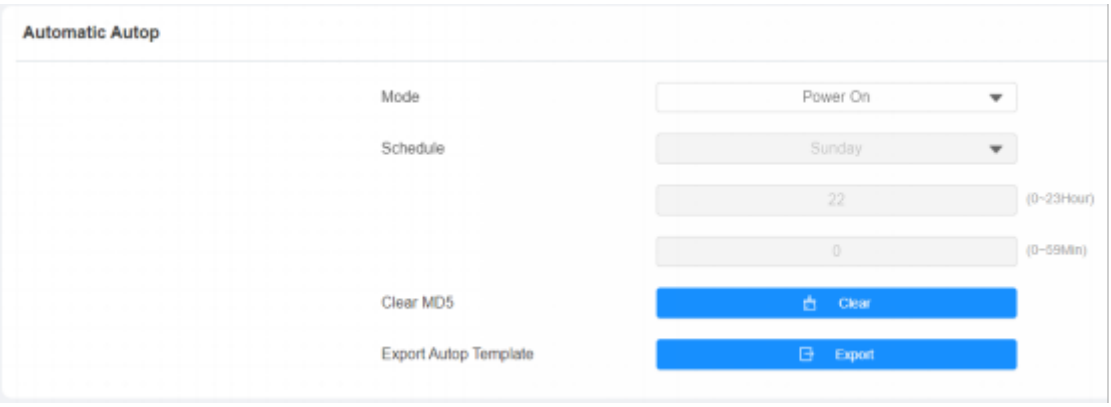
Note

- 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

23.3. Auto Provision Schedule

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

To configure it, go to **System > Auto Provisioning** interface.

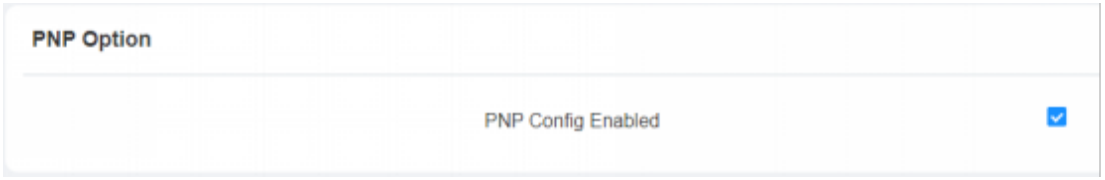


Parameter Set-up:

- **Mode:** Select **Power on**, **Repeatedly**, **Power On + Repeatedly**, and **Hourly Repeat** as your AutoP schedule.
  - Select **Power on** if you want the device to perform AutoP every time it boots up.
  - Select **Repeatedly**, if you want the device to perform AutoP according to the schedule you set up.
  - Select **Power On + Repeatedly** if you want to combine **Power On Mode** and **Repeatedly mode,** it would enable the device to perform AutoP every time it boots up or according to the schedule you set up.
  - Select **Hourly Repeat** if you want the device to perform AutoP every hour.

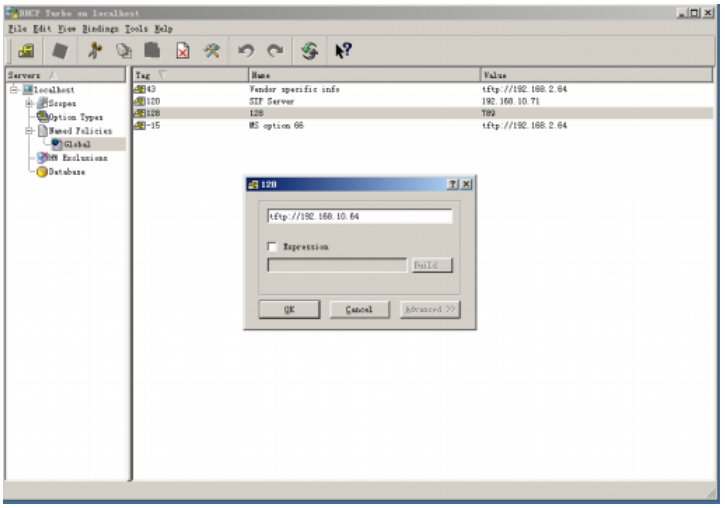
23.4. PNP Configuration

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


PNP Option
PNP Config Enabled

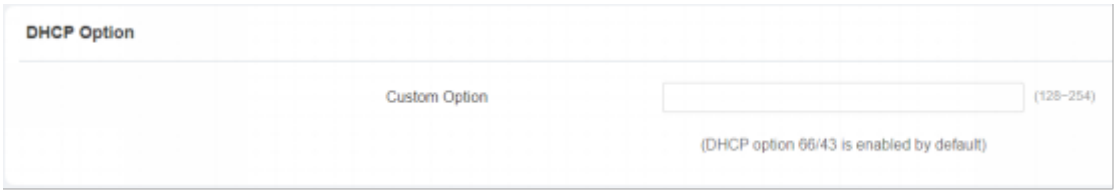
23.5. DHCP Provisioning Configuration

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



Note

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



Parameter Set-up:

- **Custom Option**: enter the DHCP code that matched the corresponding URL so that

the device will find the configuration file server for the configuration or upgrading.

- **DHCP Option 66:** If none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and

the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.

- **DHCP Option 43:**If the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

Note

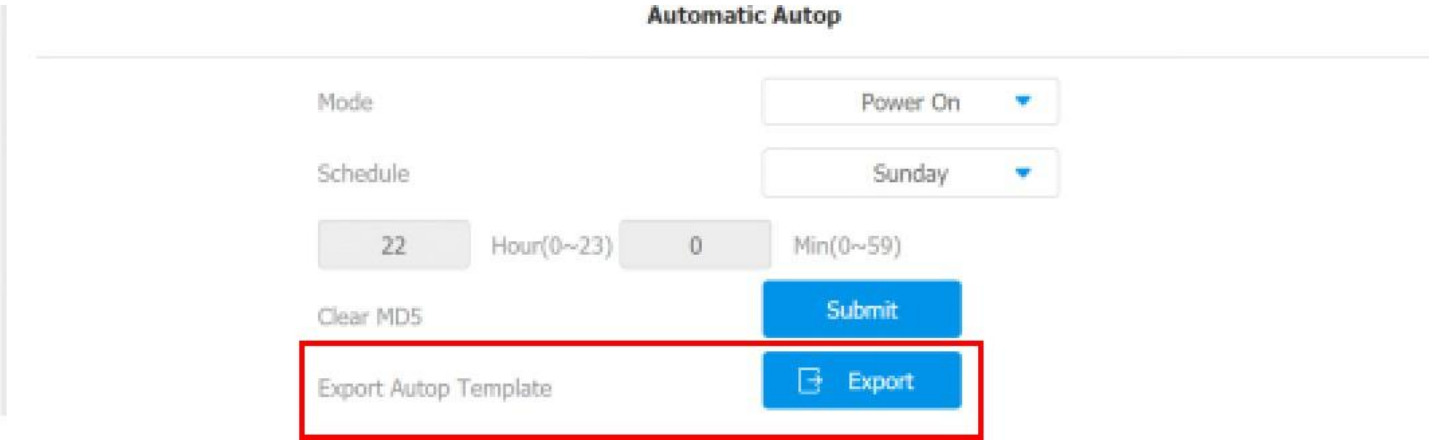
- The general configuration file for the in-batch provisioning is in the format **r0000000000xx.cfg**. Taking X915 as an example r000000000915.cfg (**10 zeros** in total while the MAC-based configuration file for the specific device provisioning is with the format MAC Address of the device.cfg, for example

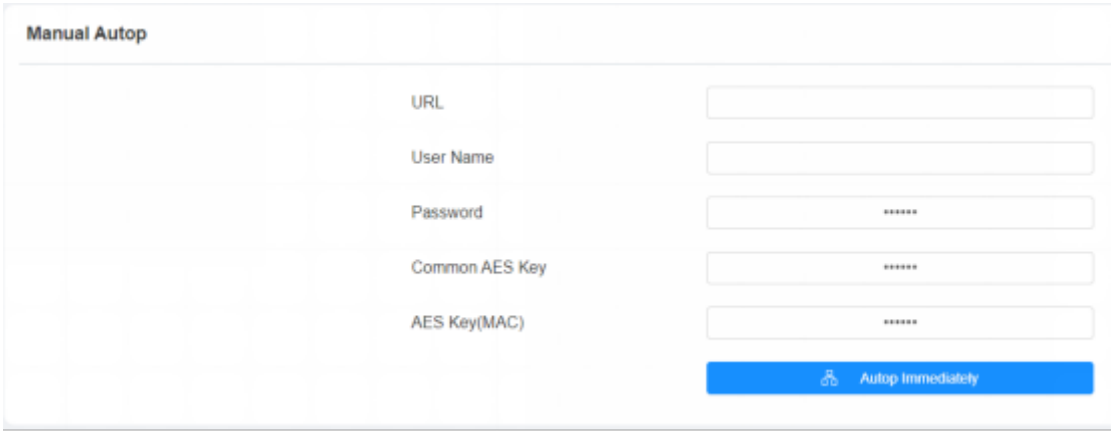
Note

- You can upload the screen saver by Auto-provisioning.

23.6. Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the door phone will perform the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration. To download the AutoP template on **System > Auto Provisioning > Automatic Autop ,** and set up the Auto provisioning server on **System > Auto Provisioning > Manual Autop** interface.





Parameter Set-up:

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

Auto Provisioning configuration files.

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

Note

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

Note

Server Address format:

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

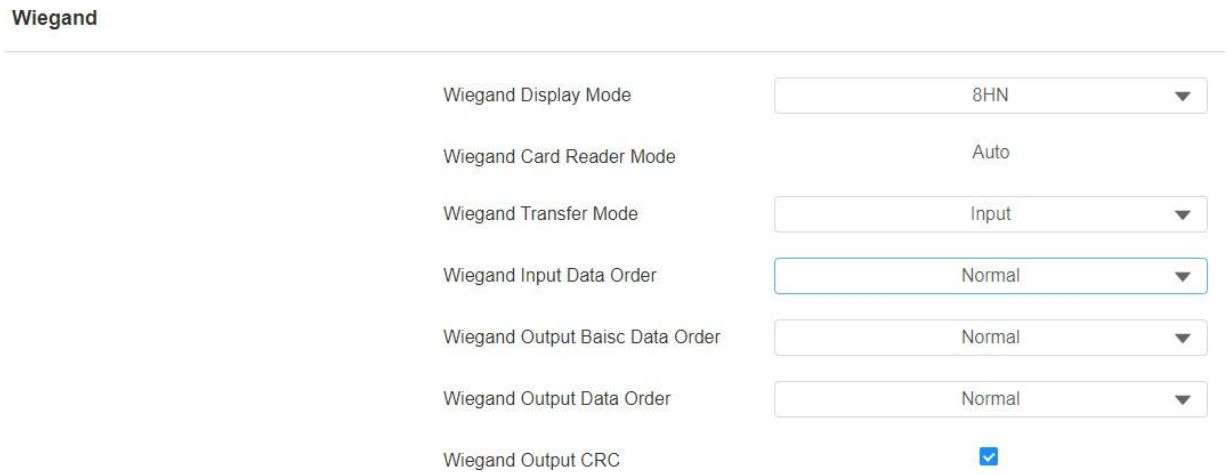
Note

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

24. Integration with Third Party Device

24.1. Integration via Wiegand

If you want to integrate the door phone with third-party devices via Wiegand. To configure the configuration on the web **Device > Wiegand** interface.



Parameter Set-up:

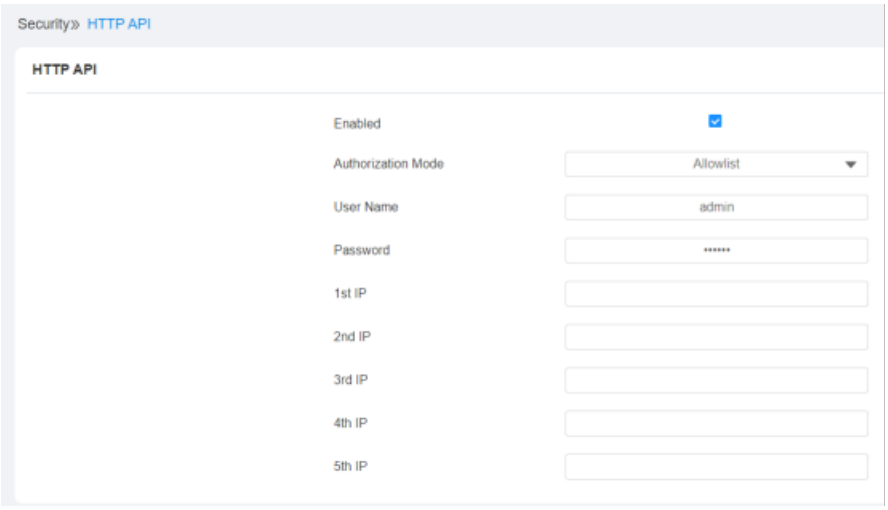
- **Wiegand Display Mode:** select Wiegand Card code format among **8H10D; 6H3D5D; 6H8D; 8HN; 8HR.**
- **Wiegand Card Reader Mode:** this field is dimmed and is not available for changing because the Wiegand card reader can adapt to all types of data input.
- **Wiegand Transfer Mode:** set the Transfer mode between **Input** or **Output** if the door phone is used as a receiver, then set it as **Input** for the door phone and vice versa.

- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Normal** and **Reversed** if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output Basic Data Order:** select **Normal** if you want Wiegand output data to be displayed in a normal state. Select **Reversed** if you want to reverse the output data, for example from 0x110x220x330x44 to 0x440x330x220x11.

- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Normal and Reversed** if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output CRC: This function** is used for Wiegand data inspection. It is turned on by default. If it is not turned on, you might not be able to integrate the device with third-party devices.

24.2. Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device with the Akuvox intercom device. You can configure the HTTP API function on the web **Security > HTTP API** interface for the integration.



Parameter Set-up:

- **Enabled:** enable or disable the HPTT API function for third-party integration. For example, if the function is disabled any request to initiate the integration will be

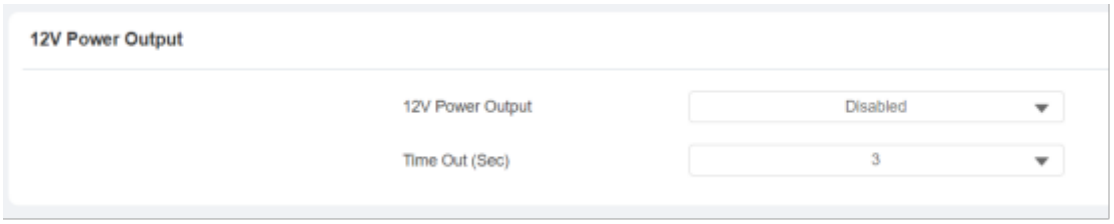
denied and be returned HTTP 403 forbidden status.

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

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

24.3. Power Output Control

The door phone can serve as a power supply for the external relays. You can go to **Access Control > Relay >12V Power Output.**

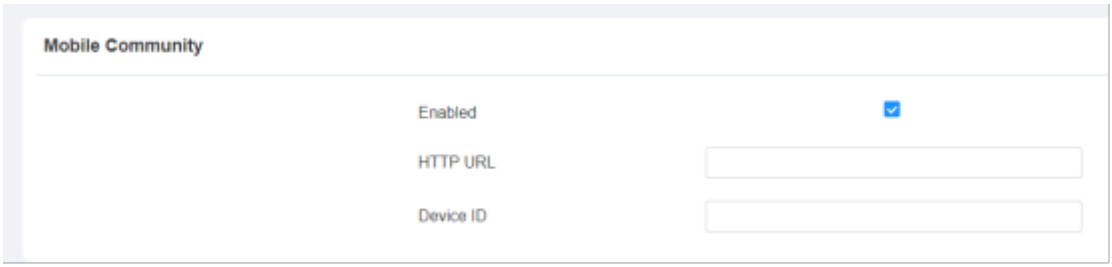


Parameter Set-up:

- **12V Power Output:** select **Disabled** to disable the power output function; select **Always** to enable the access controller to provide continuous power to the third-party device. Select **Triggered By Open Relay** if you want the door phone to provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.
- **Time Out (Sec)**: select the power supply time duration after the relay is triggered. Three options: 3, 5, 10. It is 3 seconds by default. The power output is 12V, and the maximum output amperage is 0.8A.

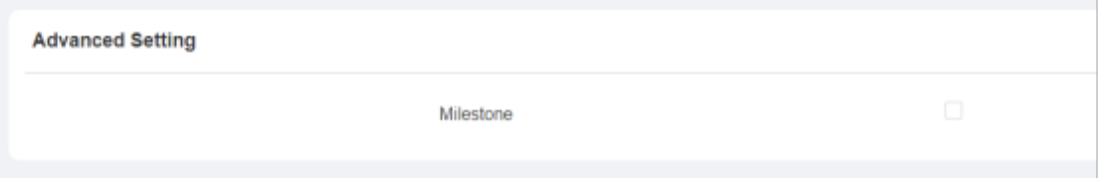
24.4. Mobile Community

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



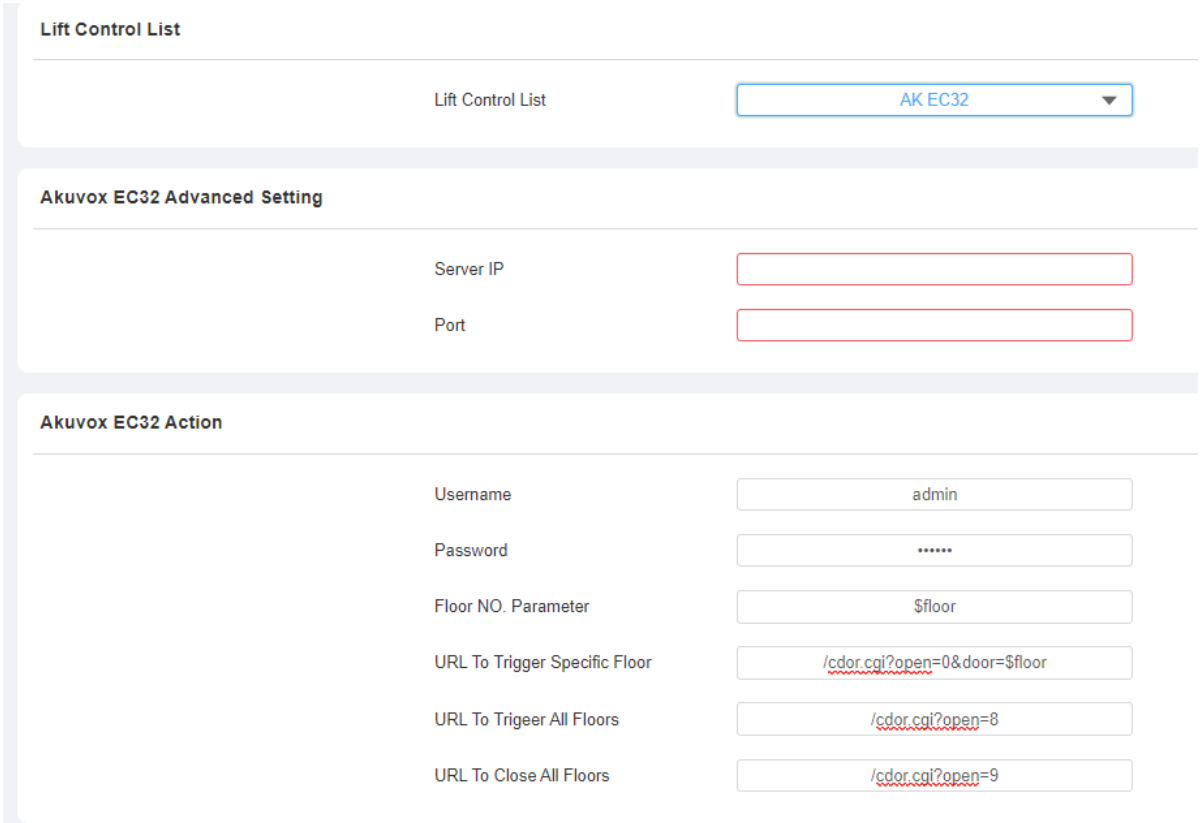
24.5. Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature. To do so, go to **Surveillance > ONVIF > Advanced Setting**.



25. Lift Control

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



Parameter Set-up:

- **Lift Control List:** select **None** to disable the function, and select the Akuvox E32 to integrate the door phone with the Akuvox EC32 controller.
- **Server IP**: enter the IP address of the Akuvox EC32 controller server.

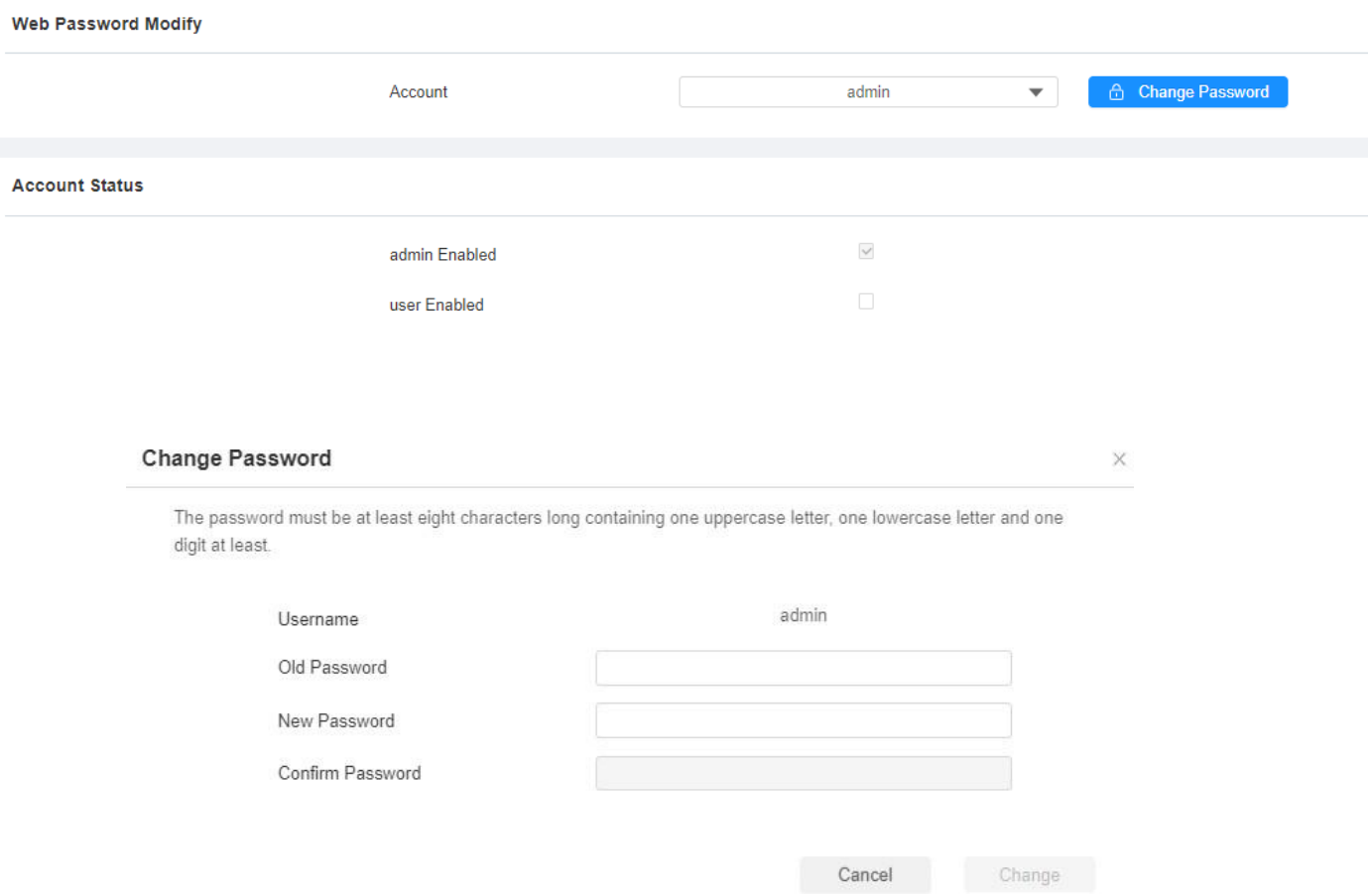
- **Server Port:** enter the Sever port of the Akuvox EC32 controller server.
- **Username:** enter the user's name of the lift controller for authentication.
- **Password:** enter the password of the lift controller for authentication.

- **Floor NO. Parameter:** enter the Floor number parameter provided by Akuvox. The default parameter string is "**$floor**". You can define your own parameter string if needed.
- **URL To Trigger Specific Floor:** enter the Akuvox life control URL for triggering a specific floor. The URL is "**/cdor.cgi?open=0&door=$floor**", but the string "$floor" at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors:** enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors:** enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.

26. Password Modification

26.1. Modifying Device Web Interface Password

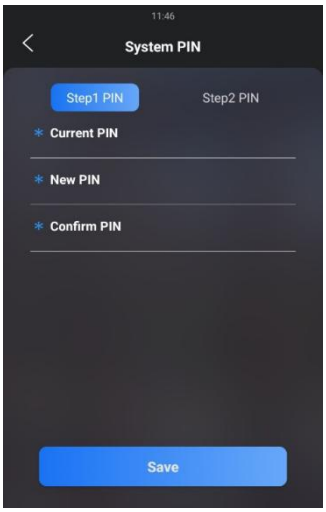
To change the default web password on web **System > Security > Web Password Modify** interface. Select **admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.



26.2. Modifying System Password

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

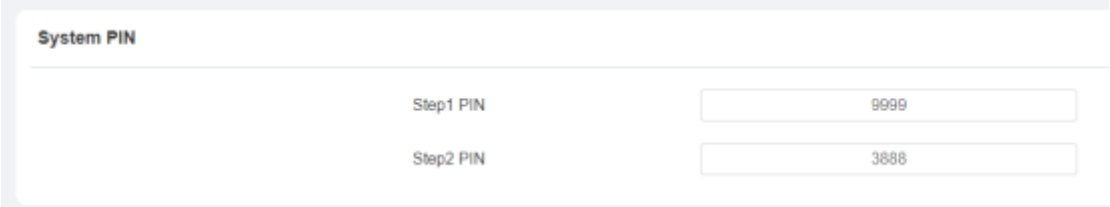
To set the system PIN code on the device, go to **Security > System PIN**, then select **Step1 PIN**.



Parameter Set-up:

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

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



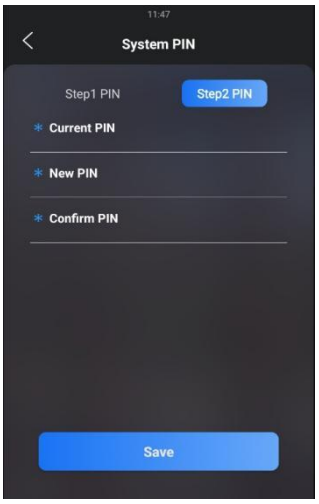
Note

- The default system entry password is 9999 and the system setting password is 2888.

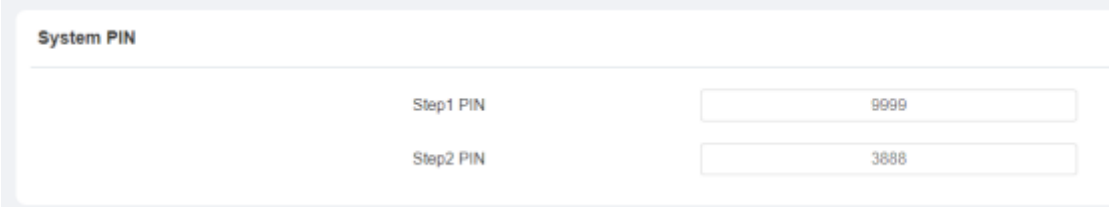
26.3. Modifying Setting Password

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

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



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



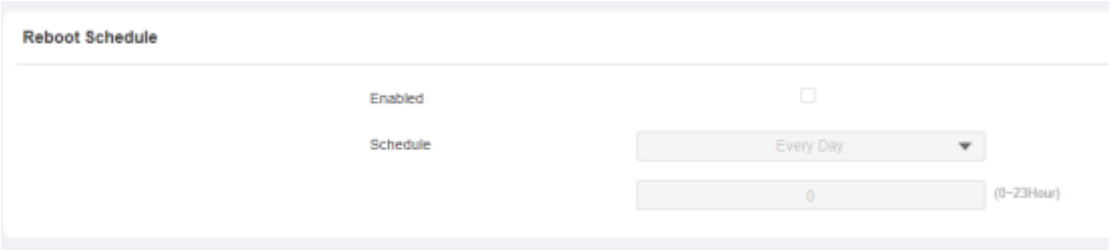
Note

- The default system entry password is 9999 and the system setting password is 3888.

27. System Reboot&Reset

27.1. Reboot

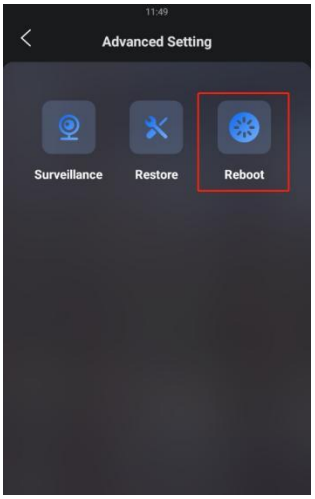
If you want to restart the device system, you can operate it on the device web interface as well. Moreover, you can set up a schedule for the device to be restarted. To restart the system setting on the web **System > Upgrade** interface.



Parameter Set-up:

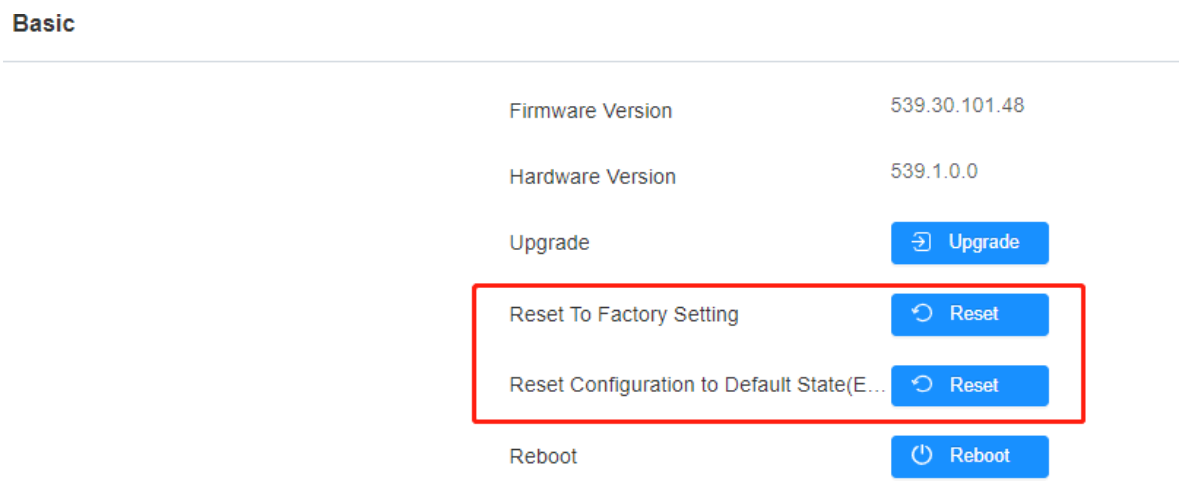
- **Enabled:** enable the reboot mode, or choose **Schedule** mode for setting the reboot time regularly.
- **Schedule:** if you choose schedule mode, you also need to set up the reboot schedule. From Monday to Sunday and 00：00 to 24:00.

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

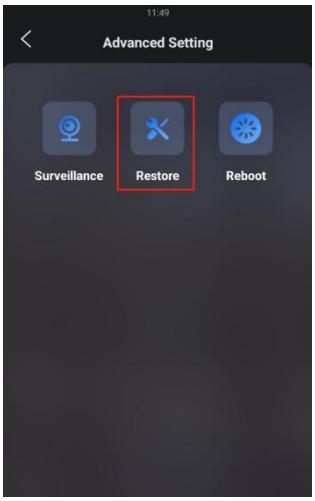

11:49
Advanced Setting
Surveillance
Restore
Reboot

27.2. Reset

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



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



28. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatic Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol **DTMF:** Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code

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

29. FAQ

Q1: How to obtain the IP address of R2X

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

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

✔ For devices with multiple numeric keyboards - R27:

While R27 power up normally, press ***2396#** to enter the home screen and press **1** to go to the **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 the **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 the Akuvox door phone?

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)

Indoor Monitor -- 14° to 112°F (-10° to 45°C)

IP Phone -- 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.

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

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

A6: Onvif 18.04 profiles.

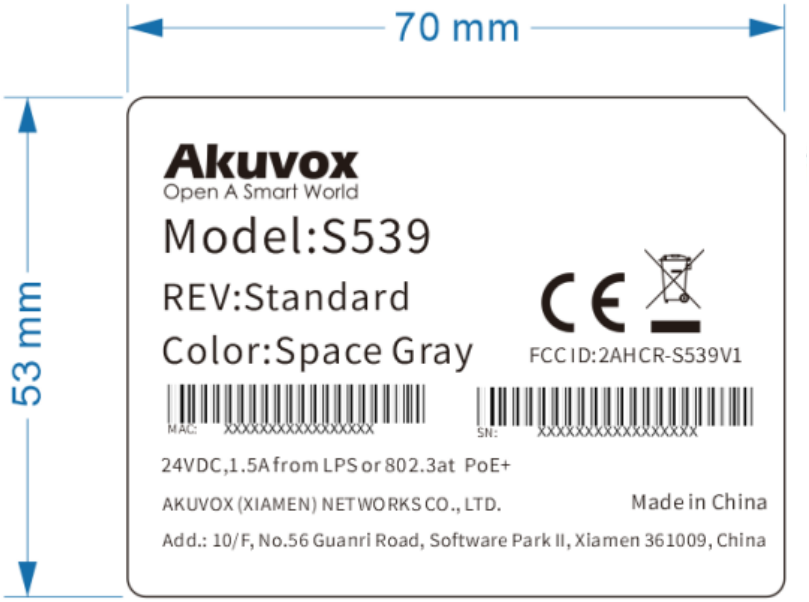
Q7: Do door phones support these card types? Prox, Legacy iClass, iClassSE, HID Mifare, HID DESFire, and HID SEOS

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

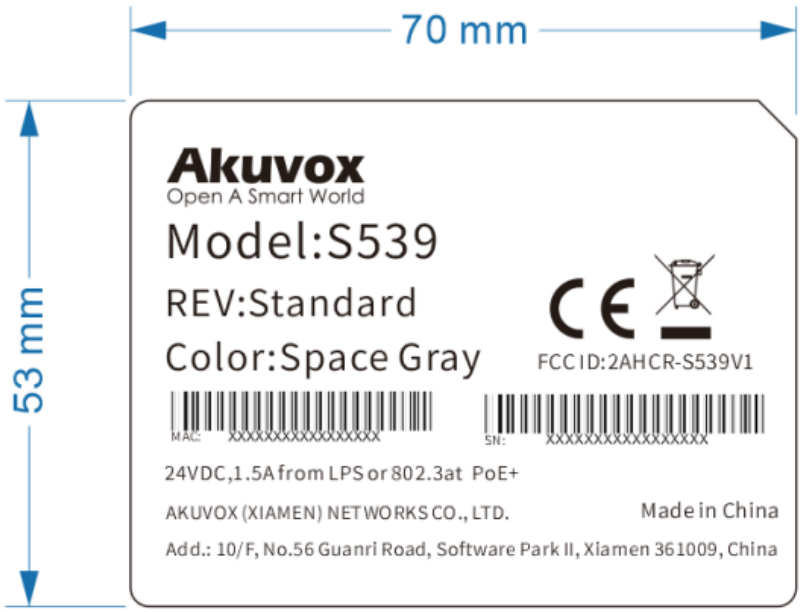
Q8: How to confirm whether my device is hardware version 1 or hardware version 2?

A8: 1. Label

- Hardware version 1



- Hardware version 2



- Firmware Version

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

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

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

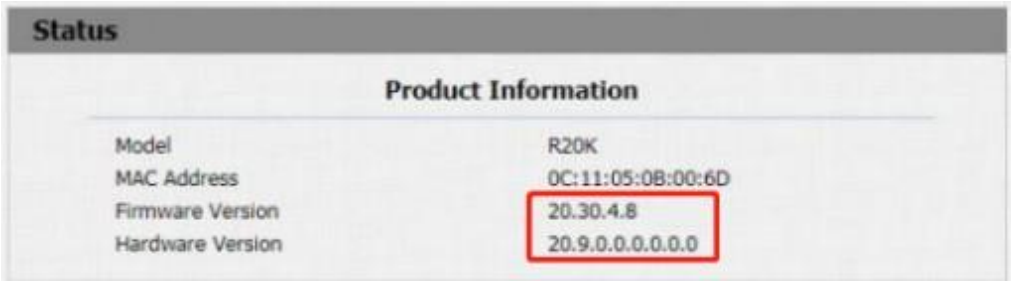
220.X.X.X is hardware version 2.

- **Hardware version**

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

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

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



30. Contact us

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

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

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

We highly appreciate your feedback about our products.

FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .
This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.