About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

X915 SERIES
DOOR PHONE
Administrator Guide

Thank you for choosing the Akuvox X915 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to version 915.30.10.14, and it provides all the configurations for the functions and features of the X915 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

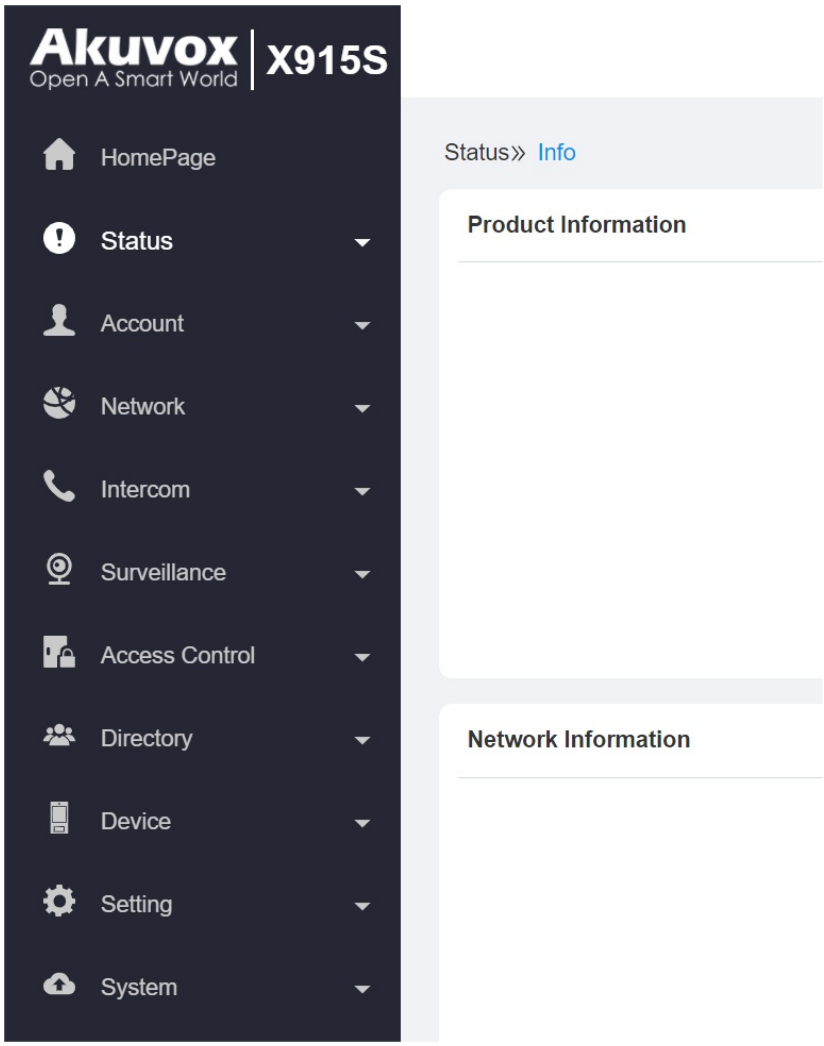
The Akuvox X915 series is an Android-based IP video door phone with a touch screen. It combines audio and video communication, access control, and video surveillance functionalities. With its advanced Android OS, Cloud, and AI-based communication technology, it offers customizable features to meet your operational preferences. The X915 series supports multiple ports such as RS485 and Wiegand, allowing easy integration with external systems like elevator controllers and fire alarm detectors. This comprehensive solution provides complete control over building entrances and surroundings, ensuring enhanced security through various access methods such as card access, NFC, Bluetooth, QR code, voice-controlled door access, and body temperature measurement, ideal for residential and office buildings as well as complexes.

Model Specification

Model	X915S
Touch Screen	✔
Relay In	3
Relay Out	3
Alarm In	X
RS485	✔
Card Reader	13.56MHZ&125KHZ
Wi-Fi	X
Bluetooth	✔
Temperature detection	Optional
Facial Recognition	✔
LTE	X
USB	X
External SD Card	X

Introduction to Configuration Menu

- **Status:** this section gives you basic information such as product information, network information, account information, etc.
- **Account:** this section concerns the SIP account, SIP server, proxy server, transport protocol type, audio and video codec, DTMF, session timer, etc.
- **Network:** this section mainly deals with DHCP & Static IP settings, RTP port settings, and device deployment, etc.
- **Intercom:** this section covers intercom settings, call logs, etc.
- **Surveillance:** this section covers motion detection, RTSP, MJPEG, ONVIF, live stream, etc.
- **Access Control:** this section covers input control, relay, card settings, facial recognition setting, private PIN codes, Wiegand connection, etc.
- **Directory:** this section involves tenant management.
- **Device:** this section includes light settings, tab&button display, LCD settings, and voice settings.
- **Setting:** this section includes time & language, action settings, door settings, and schedule management for access control.
- **System:** this section is for password modification.


Akuvox
Open A Smart World
X915S
HomePage
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System
Status» Info
Product Information
Network Information

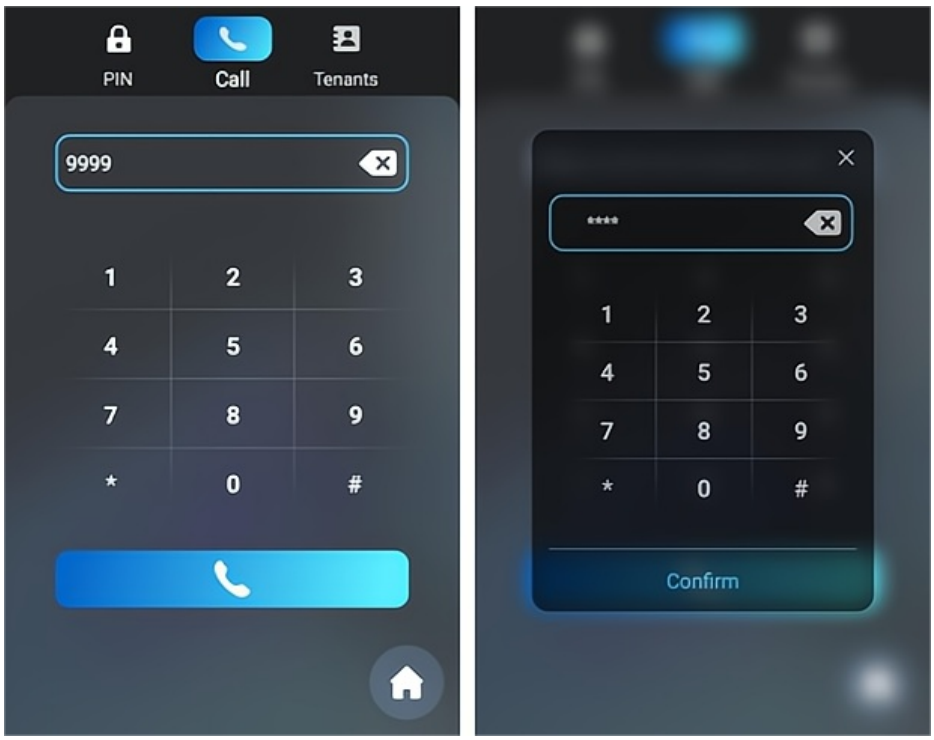
Access the Device

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

Access the Device Setting on the device

Before configuring the device, please ensure the device is installed correctly and connected to a normal network. Use the Akuvox IP scanner tool to search the device's IP address in the same LAN. Then use the IP address to log into the web browser by user name and password **admin** and **admin**.

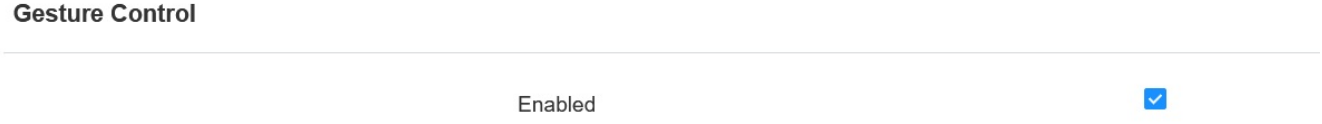
Or set up some basic settings on the device screen by pressing **9999** + **Dial** key + **3888**(password) on the **Dial** screen.



Gesture Control Setting

When the device is in the Building or Villa theme, tap on the time area ten times on the device's home screen to access the settings screen. The default password is 3888.

To enable the feature, navigate to the web **System > Security > Gesture Control** interface.

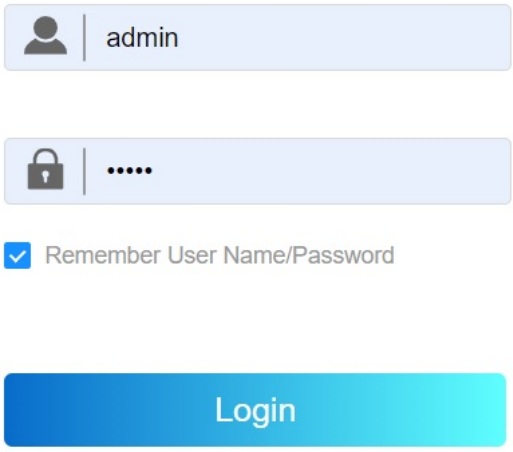


> **Note**
>
> See theme configuration in Screen Display Configuration chapter.

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.

The initial user's name and password are **admin**.



Note

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

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See the detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- Please be case-sensitive to the user names and passwords entered.

Language and Time Setting

Language Setting

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

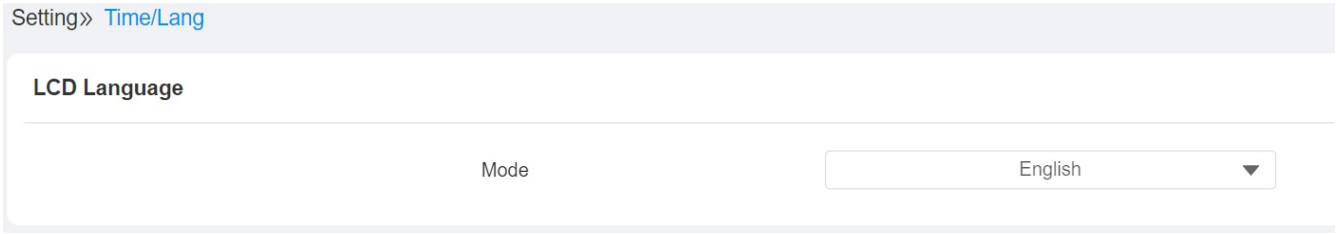
Language Setting on the Device Web Interface

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.

The device LCD supports the following languages:

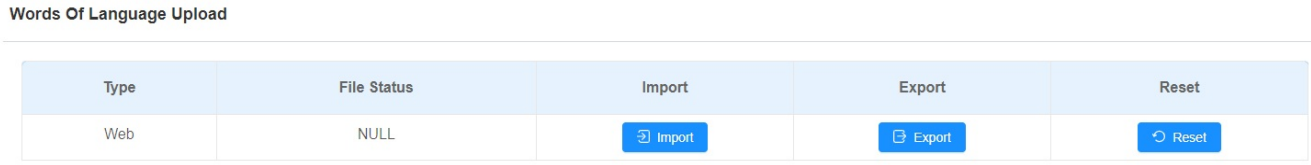
English, Simplified Chinese, Spanish, Danish, French, Czech, Traditional Chinese, Turkish, Japanese, Norwegian, Korean, Russian, Dutch, Polish, Swedish, German, and Ukrainian.



To switch the device web language in the upper right corner.

To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device.

Navigate to the web **Setting > Time/Lang > Words Of Language Upload** interface.



Language Setting on the Device

To configure the language on the device **Basic Setting > Language** screen.

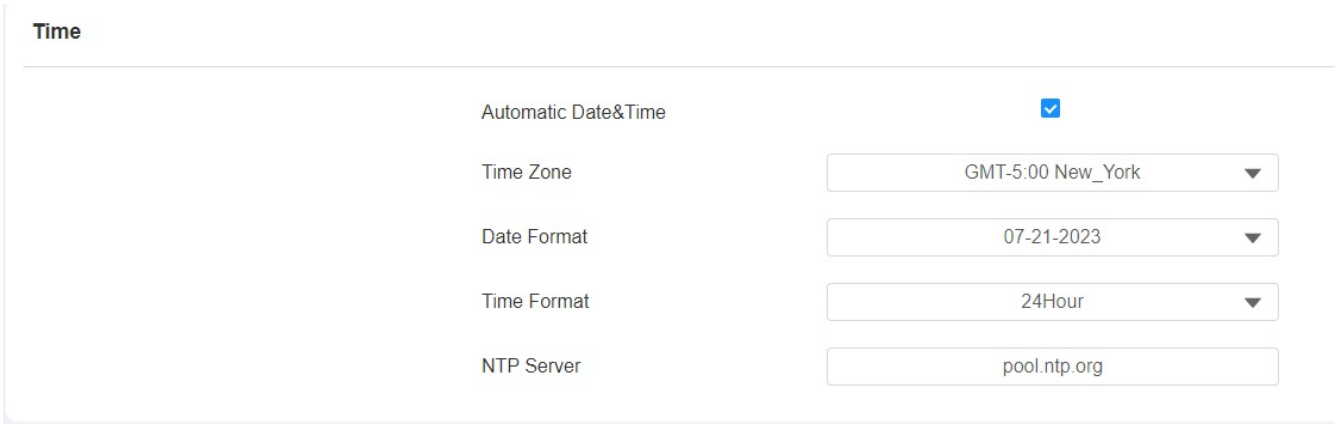
Time Setting

Time settings, including time zone, date and time format, and more, can be configured either on the device or the web interface.

Time Setting on the Device Web Interface

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

To configure time on the web **Setting > Time/Lang > Time** interface.



- **Automatic Date&Time**: allow the date and time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by entering the time and date.
- **NTP Server**: the NTP server address.

Time Setting on the Device

To configure time on the device **Basic Setting > Time** screen.

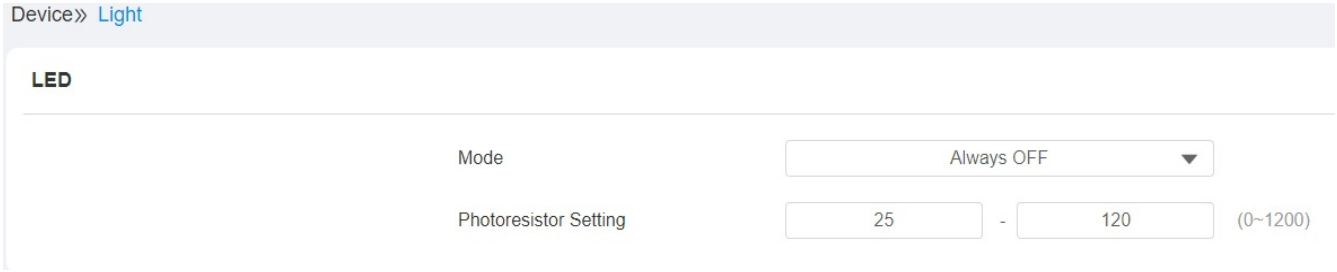
LED&LCD Setting

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.

Infrared LED Setting on the Web Interface

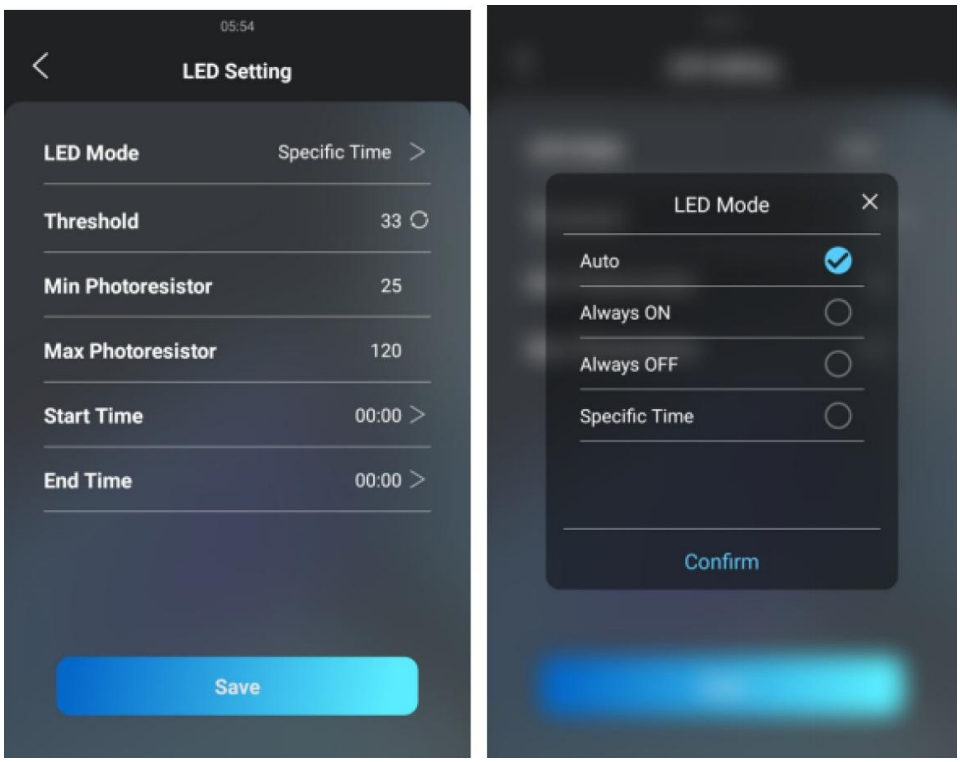
Navigate to the web **Device > Light > LED** interface.



- **Mode:**
  - Auto: the device will set up an LED automatically.
  - Always On: enable the function all the time.
  - Always Off: disable the function all the time.
  - Specific Time: specify the LED start time and end time.
- **Photoresistor Setting**: 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. The default minimum and maximum photoresistor values are 25 and 120 respectively.

Infrared LED Setting on the Device

To configure it on the device **Basic Setting > Display > LED Setting** screen.

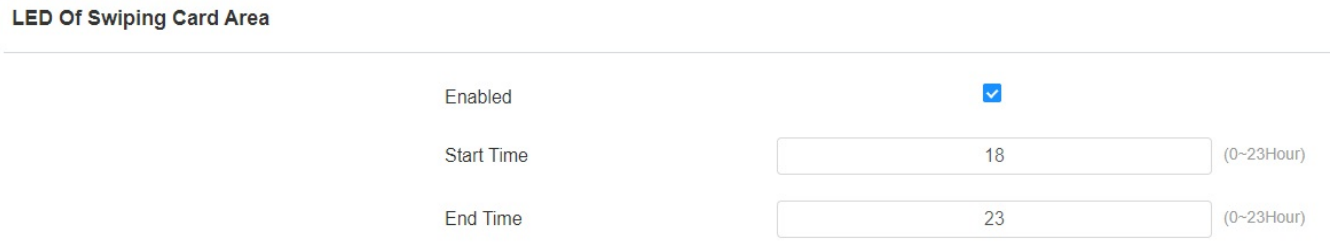


Threshold: the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is **33**. However, you can tap the icon several times to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you base on to configure the minimum and maximum photo-resistor values.

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.

Navigate to the web **Device > Light > LED Of Swiping Card Area** interface.



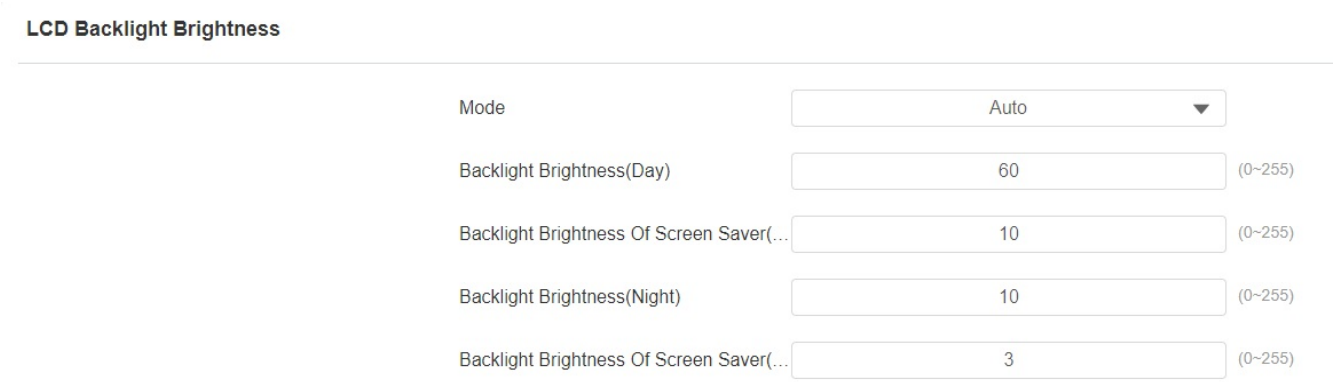
Start Time- End Time (H): enter the period for the LED lighting to be valid, e.g., if the period is set from 8-0 (Start time- End time), it means LED light will stay on during the period from **8:00** am to **12:00** pm during one day (24 hours).

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.

LCD Screen Brightness Setting on the Web Interface

Navigate to the web **Device > Light > LCD Backlight Brightness** interface.



- **Mode**: when **Auto** is selected, the screen backlight brightness will be adjusted automatically.

The backlight brightness has two modes, Day and Night. They are determined by the photoresistor.
-If the current value is between the minimum and maximum photoresistor, the device is in **Day** mode.
-If the current value is higher than the maximum photoresistor, the device is in **Night** mode.

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

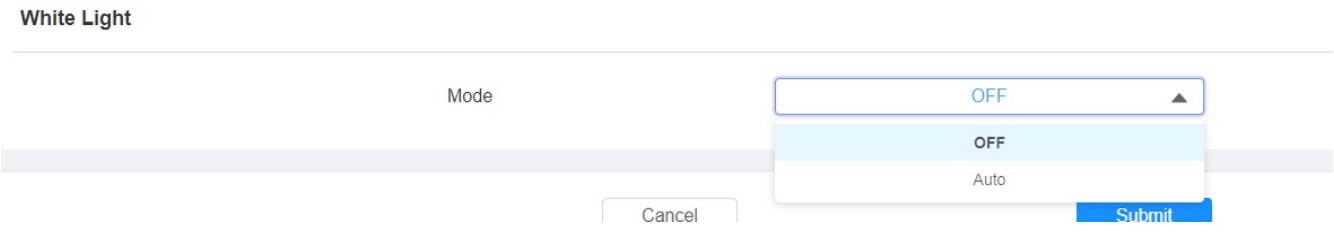
LCD Screen Brightness Setting on the Device

To configure the brightness on the device **Basic Setting > Display > LCD Setting** screen.

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.

Navigate to the web **Device > Light > White Light** interface.



- **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.

Screen Display Configuration

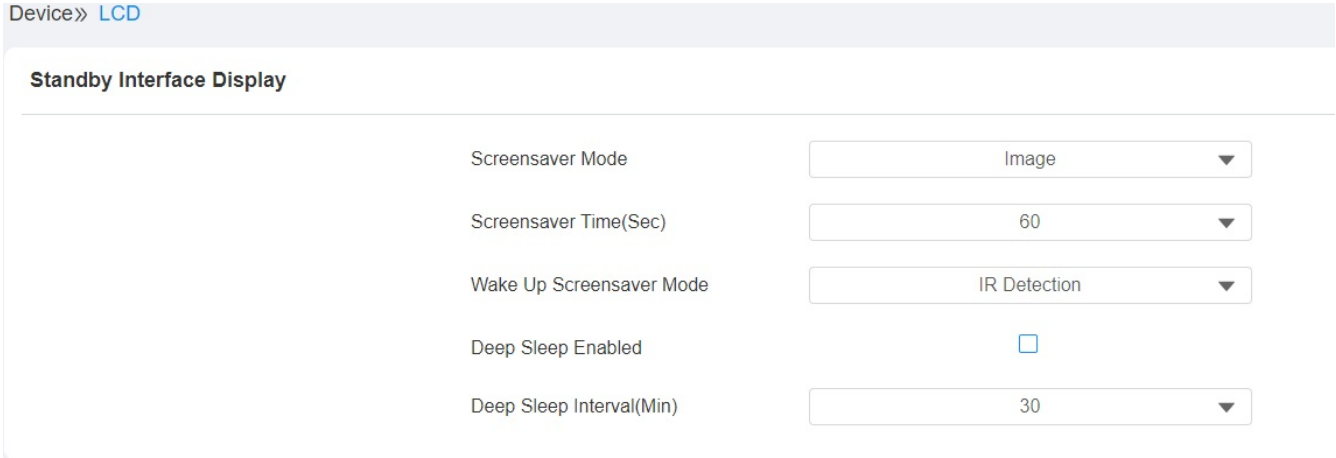
You can set up the device's screen display features such as screensaver to give users a better visual and operational experience.

Screensaver Configuration

Configure Screensaver on the Web Interface

You can 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.

Navigate to the web **Device > LCD > Standby Interface Display** interface.



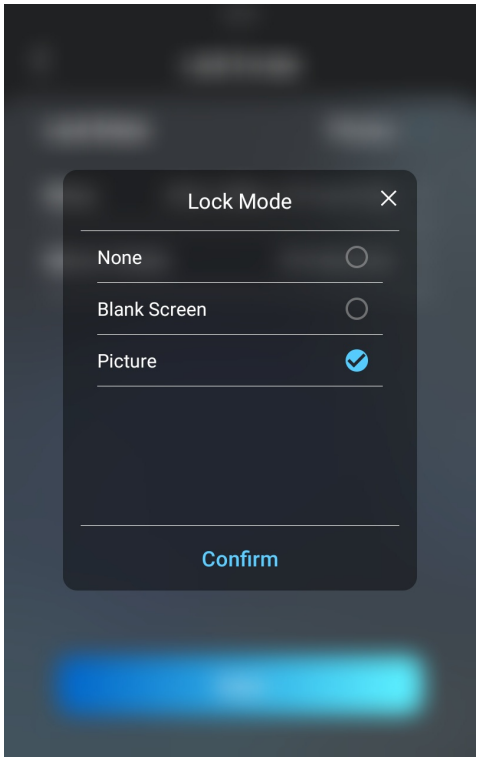
- **Screensaver Mode**:
  - **None:** the screen will stay on without going into screen-saver mode.
  - **Blank**: the screen will go black.
  - **Image**: the picture you uploaded will be shown as the screen saver.
- **Screensaver Time (Sec)**: set the screen saver start time from 5 seconds up to 180 seconds. The screen saver starts when the device detects no operation, or no one is approaching.
- **Wake Up Screensaver Mode**:
  - **Auto**: the screen will be awakened when someone approaches without it being touched upon.
  - **Manual**: touch and wake up the screen.
- **Deep Sleep Enabled**: the screen will turn off after the screensaver reaches the end of the 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.

Configure Screensaver on the Device

You can also configure the screensaver on the device.

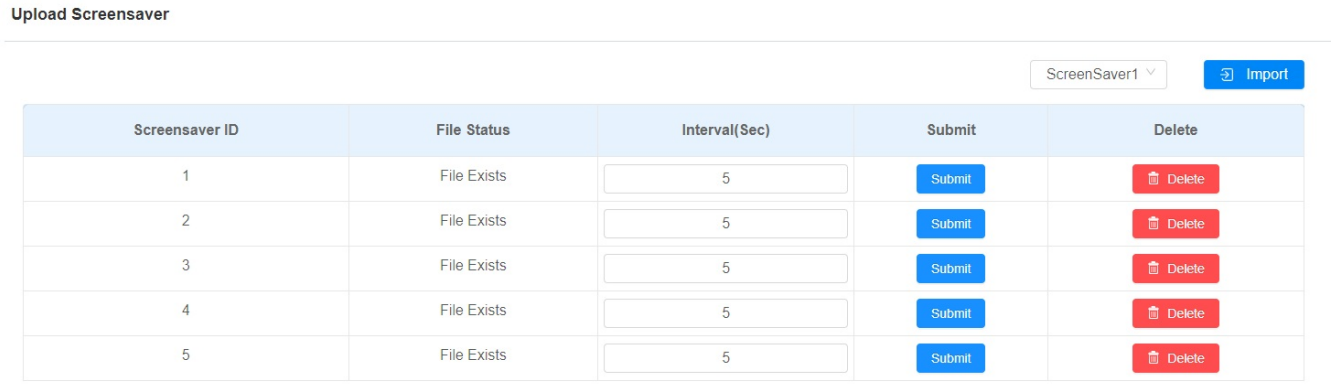
Go to the **Basic Settings> Lock** screen.



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.

Navigate to the web **Device > LCD > Upload Screensaver** interface.



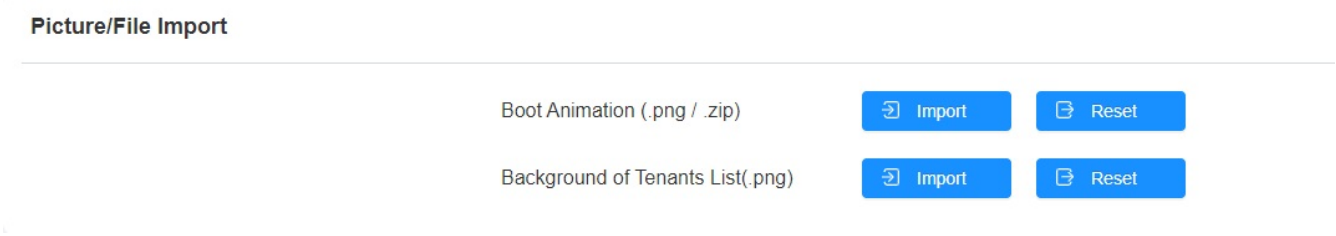
Note

- 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 repetitive designation of pictures to the same ID order occurs.

Upload Device Booting Image

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

Navigate to the web **Setting > Key/Display > Picture/File Import** interface.

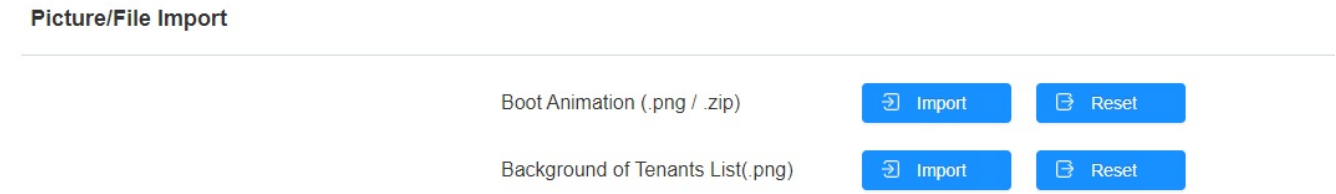


> **Note**
>
> - The pictures uploaded should be in **.png or .zip** format.
> - Max .zip file size: 20MB; Max picture size: 1MB; Max resolution: 800*1280.

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.

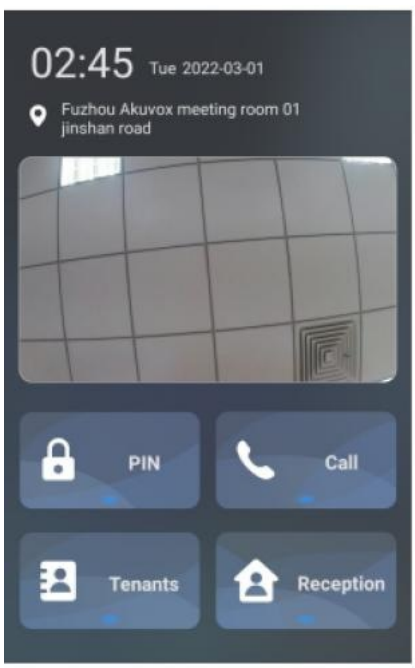
Navigate to the web **Setting > Key/Display > Picture/File Import** interface.

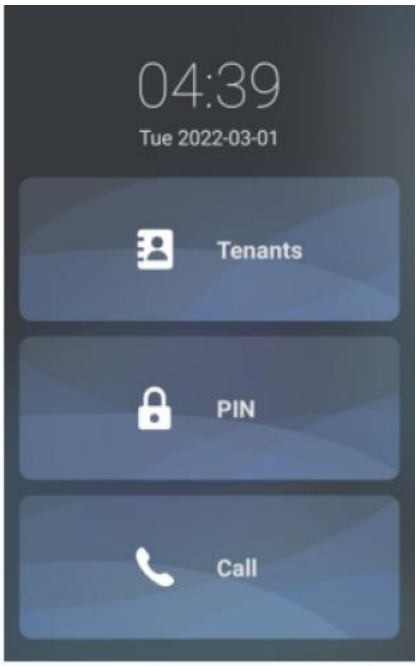


> **Note**
>
> - The pictures uploaded should be in **.png** format.
> - Max picture size: 1MB; Max resolution: 800*1280.

Home Screen Configuration

You can change the home screen display through the configuration of the tab name and tab arrangement on the device web. You can switch between Building and Villa themes on the web Setting > Key/Display > Theme interface.



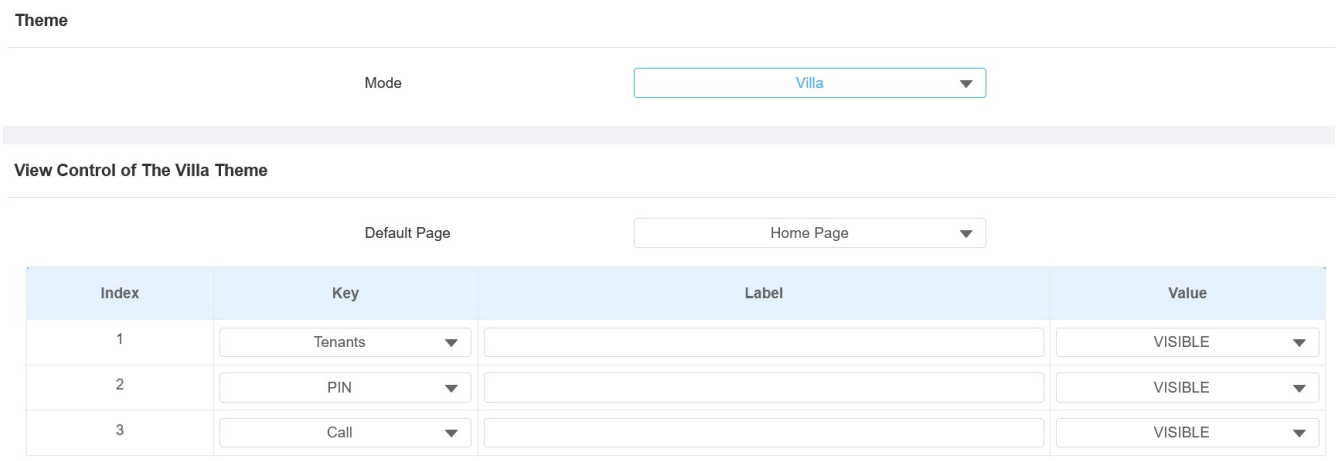


Building Mode Villa Mode

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.

Navigate to the web **Setting > Key/Display** interface. Select **Villa** as the theme.

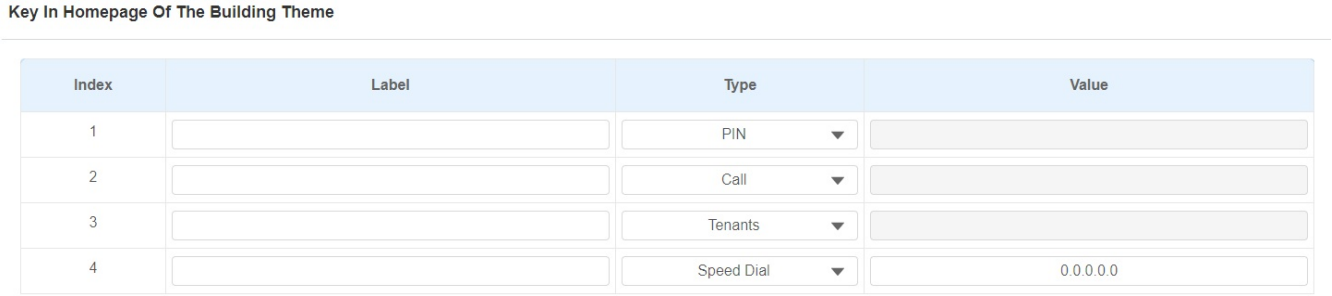


- **Default Page**:
  - **Home Page**: display the tenants, PIN, and Call icons vertically on the home screen.
  - **Tenant**: display the contact on the home screen.
  - **PIN**: display the PIN icon with the keypad on the home screen.
  - **Call**: the Call icon with a dial pad on the home screen.
- **Key**: set the type of icon to be displayed 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.

Building Mode Home Screen Display

You can customize your building mode home screen icon display if needed.

Navigate to the web **Setting > Key/Display > Key In Homepage Of The Building Theme** interface.

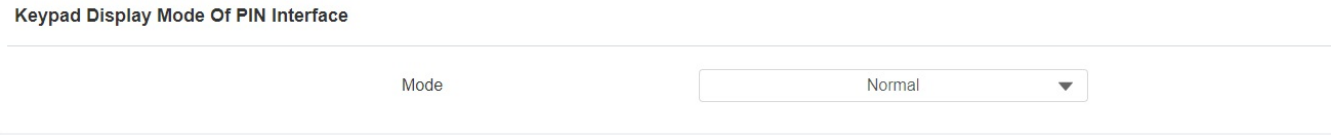


- **Type**: select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make the **Speed Dial** tab displayed in position one, you can change the type in index number 1 to **Speed Dial**. And you can change another tab position accordingly.
- **Label**: 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.

Dial Key Order

The door phone provides two keypad key display options: Normal and disordered. Opting for the Disordered setting means that the arrangement of keys is randomized each time, enhancing security by preventing password spying.

Navigate to the web **Setting > Key/Display > Keypad Display Mode of PIN** Interface.



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.

Dial Screen Prompt Display

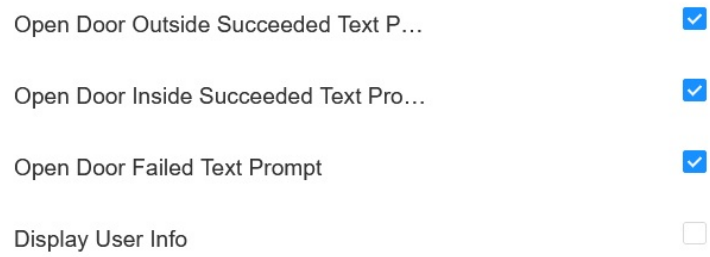
Navigate to the web **Setting > Key/Display > Prompt Of The Call Page** interface.

> **Note**
>
> X915 supports a 128-digit character maximum in length for the text prompt.

Open Door Text Prompt Display

Navigate to the web **Access Control > Relay > Open Door Text Prompt** interface.

Open Door Text Prompt



- **Open Door Outside Succeeded Text Prompt:** when the door is opened, the text prompt will pop up on the device screen. The default is “Access Granted”.
- **Open Door Inside Succeeded Text Prompt:** when input is triggered, the text prompt will pop up.
- **Open Door Failed Text Prompt:** when the door opening fails, the text prompt will pop up.
- **Display User Info**: display the user information after facial recognition. If facial recognition succeeds, the text prompt “Access Granted” with the user ID and name will pop up on the device screen. If it fails, the text prompt “Access Denied” with “Stranger, Name: Unknown” will be displayed.

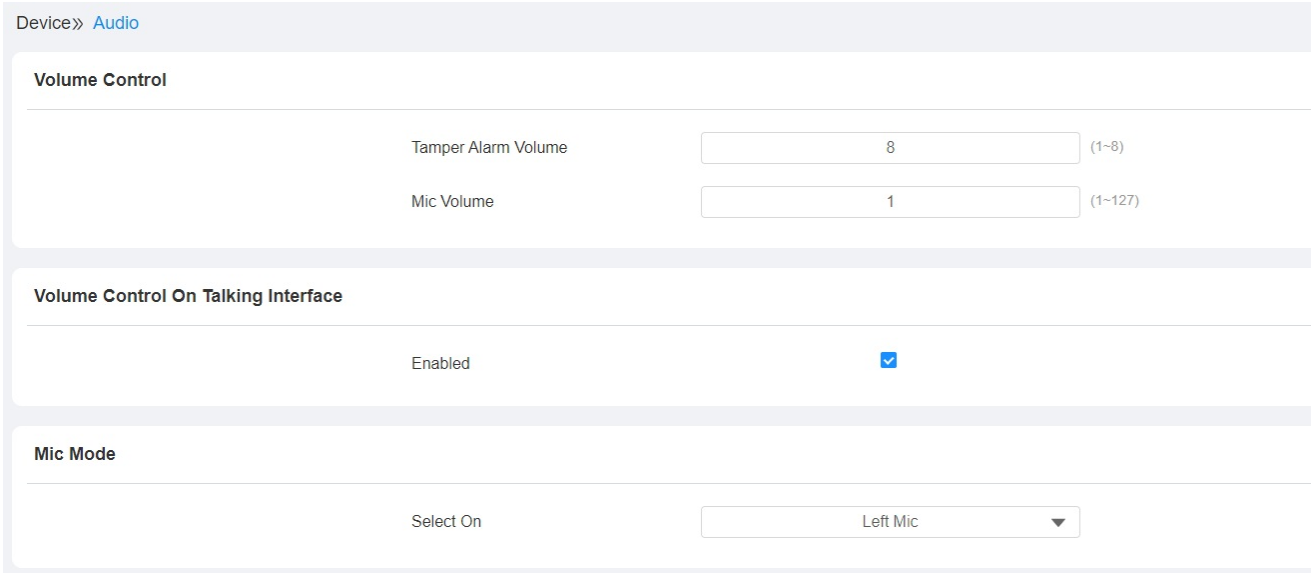
Volume and Tone Configuration

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

Volume Configuration

Configure Volume on the Web Interface

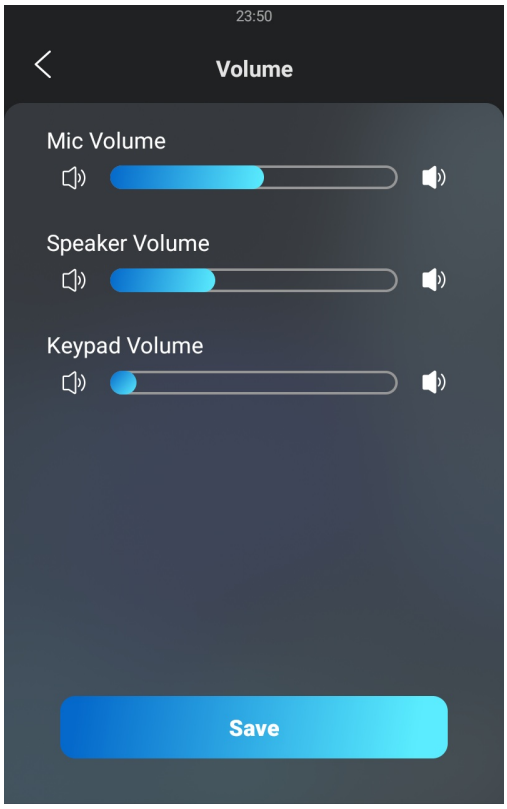
Navigate to the web **Device > Audio** interface.



- **Volume Control on Talking Interface**: when enabled, users can adjust the call volume during the call session.
- **Select On**: select which mic to be applied between the left and right microphones.

Configure Volume on the Device

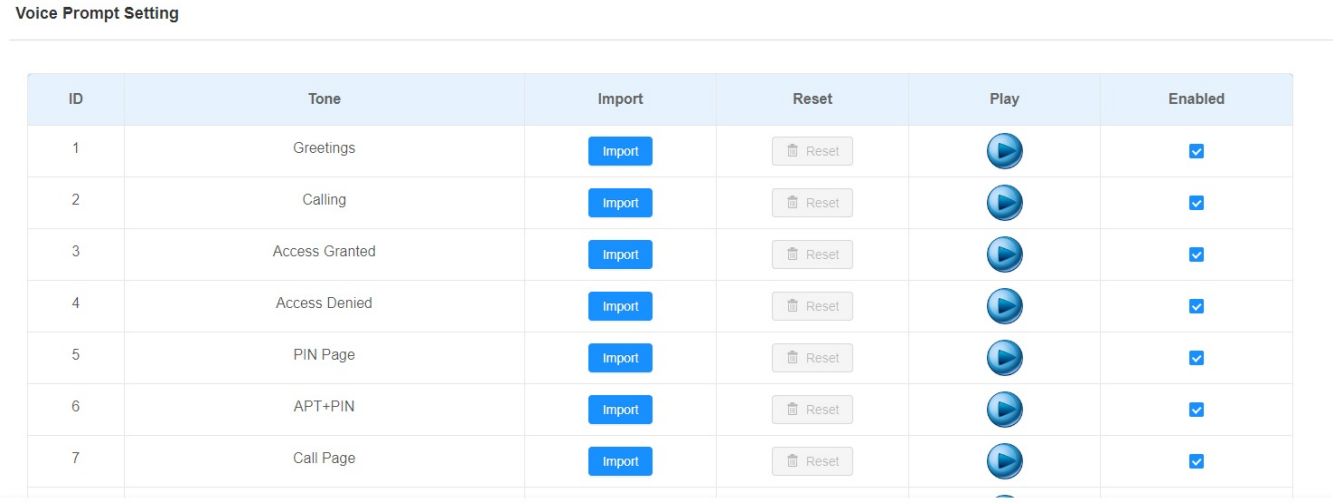
To configure the volume on the device **Basic Setting > Volume** screen.



Voice Prompt Setting

You can upload the tone for different scenarios on the device's web interface.

Navigate to the web **Device > Audio > Voice Prompt Setting** interface.



Note

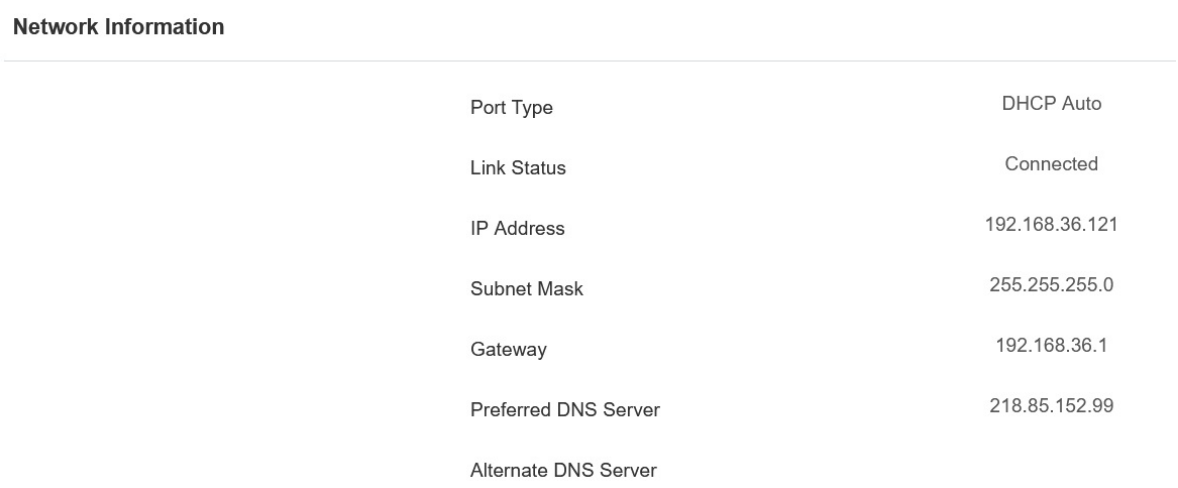
File Format: wav mp3, size: < 200KB, Sample Rate: 16000, Bits: 16.

Network Setting

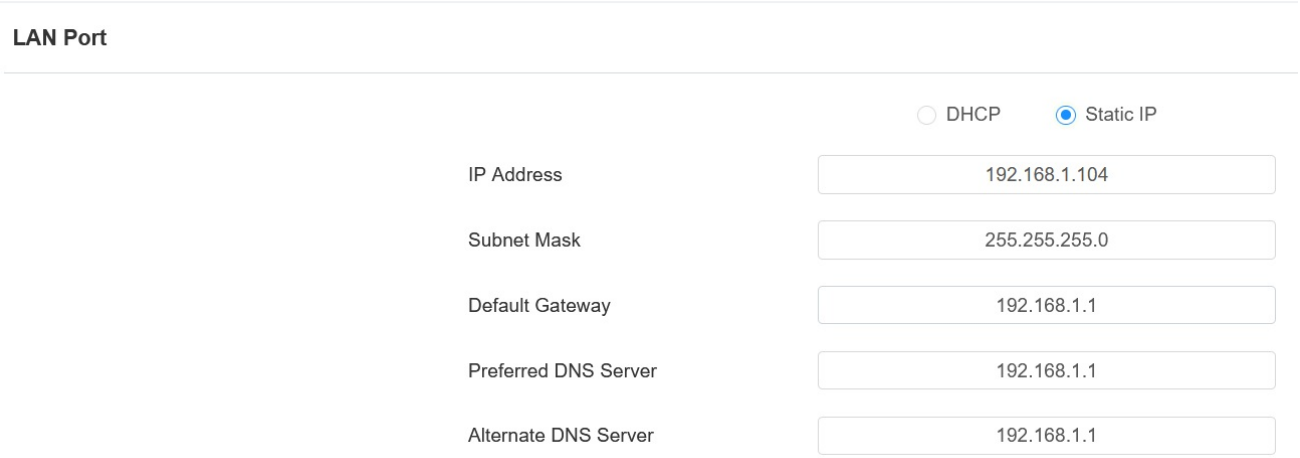
Device Network Connection Setting

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

To check the network status on the web **Status > Info > Network Information** interface.



To change the network connection on the web **Network > Basic** interface.



- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: when static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **IP Address**: set up the IP address when the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to the actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.

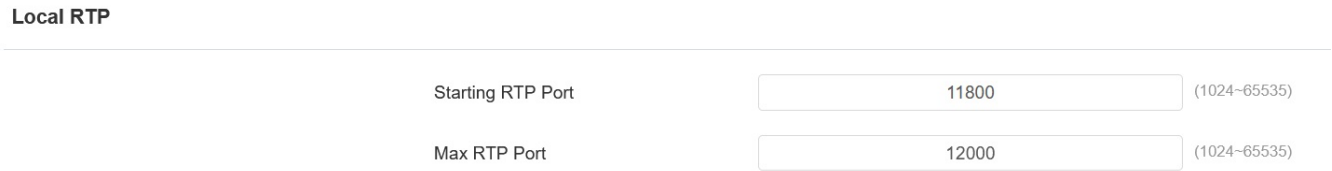
- **Preferred/Alternate DNS Server**: set up the Domain Name Server(DNS) according to the actual network environment. The Preferred DNS Server is the primary DNS server address while the Alternate DNS Server is the secondary. The door phone connects to the alternate DNS server when the primary one is unavailable.

Device Local RTP Configuration

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

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

Navigate to the web **Network > Advanced > Local RTP** interface.

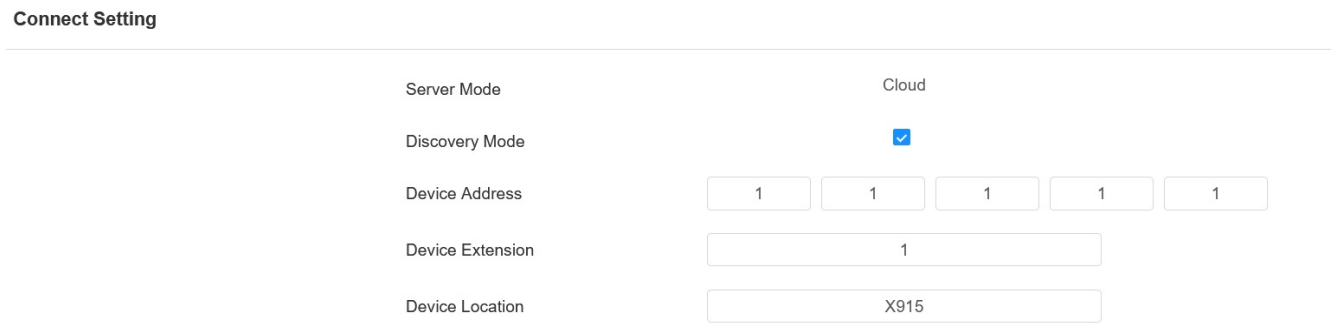


- **Starting RTP Port**: enter the port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: enter the port value to establish the endpoint for the exclusive data transmission range.

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

Navigate to the web **Network > Advanced > Connect Setting** interface.

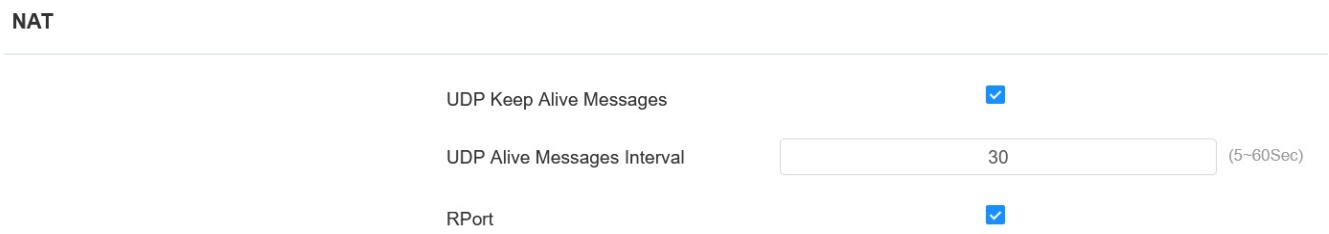


- **Server Mode**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud,** or **None**. **None** is the default factory setting indicating the device is not in any server type.
- **Discovery Mode**: the discovery mode makes the device be discovered by other devices in the network. Disable it if you want to conceal the device so as not to be discovered by other devices. After turning off the discovery mode, you need to restart the device to take effect.
- **Device Address**: specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
- **Device Extension**: enter the device extension number for the device you installed.
- **Device Location**: enter the location in which the device is installed and used.

NAT Setting

Network Address Translation(**NAT**) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

Navigate to the web **Account > Advanced > NAT** interface.



- **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 a Wide Area Network(WAN).

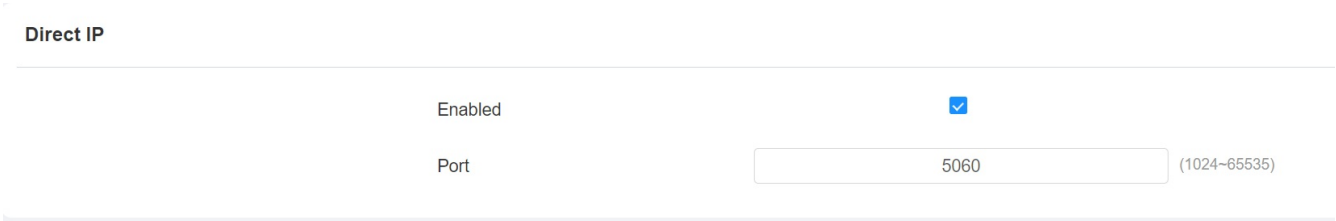
Intercom Call Configuration

IP Call & IP Call Configuration

An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

IP Call Configuration

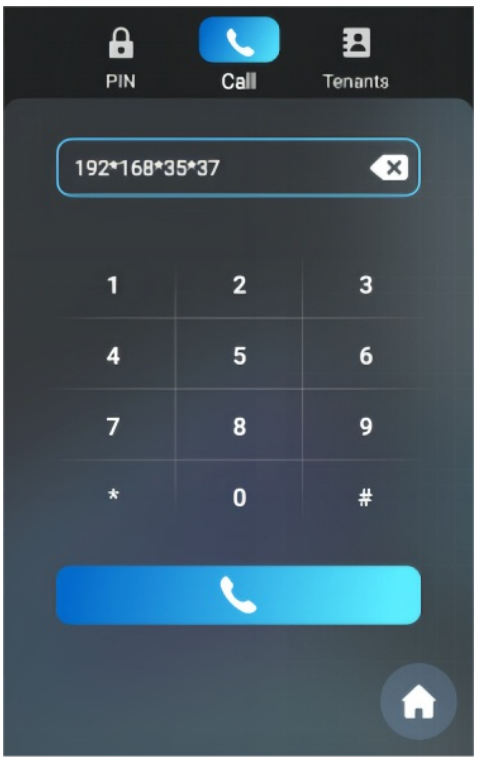
To configure the IP direct call on the device **Intercom > Basic > Direct IP** interface.



Port: set the port for direct IP calls. The default is 5060, with a range from 1-65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

Make IP Calls

To make SIP calls or IP calls on the device, tap the dial button and enter the IP number.



SIP Call & SIP Call Configuration

Session Initiation Protocol(**SIP**) is a signaling transmission protocol used for initiating, maintaining, and terminating calls.

A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

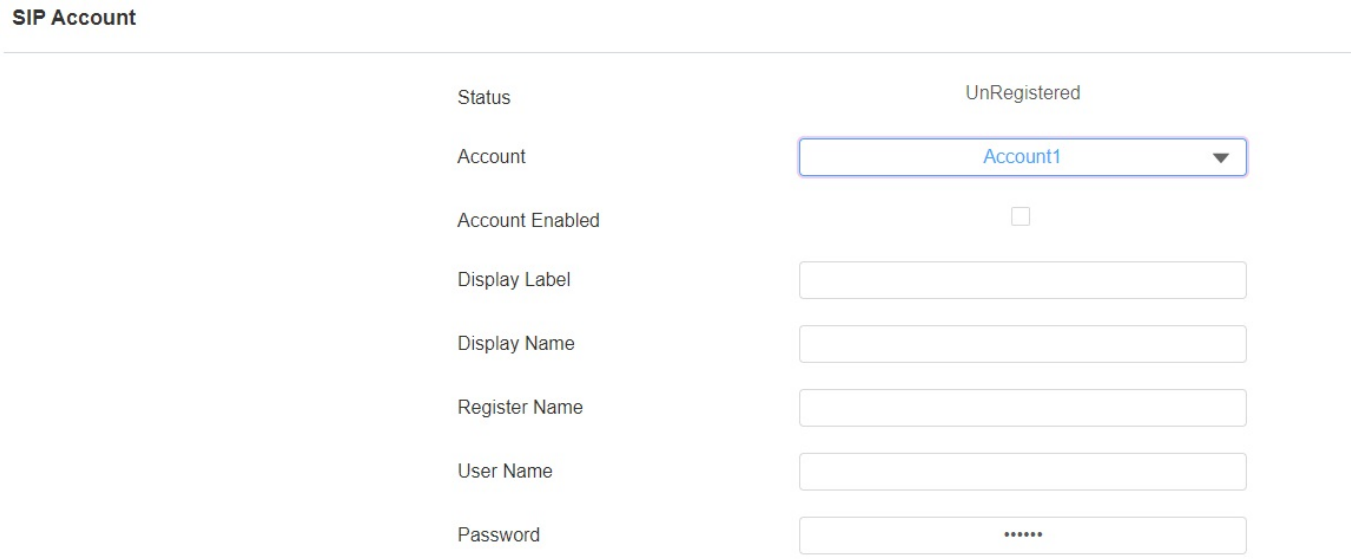
SIP Account Registration

Each device needs a SIP account to make and receive SIP calls.

Akuvox intercom devices support the configuration of two SIP accounts, which can be registered under two independent servers.

Configure SIP Account on the Web Interface

Navigate to the web **Account > Basic > SIP Account** interface.



- **Account 1/Account 2:** the door phone supports 2 SIP accounts.

  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.

  - The system switches to Account 2 if Account 1 is not registered.

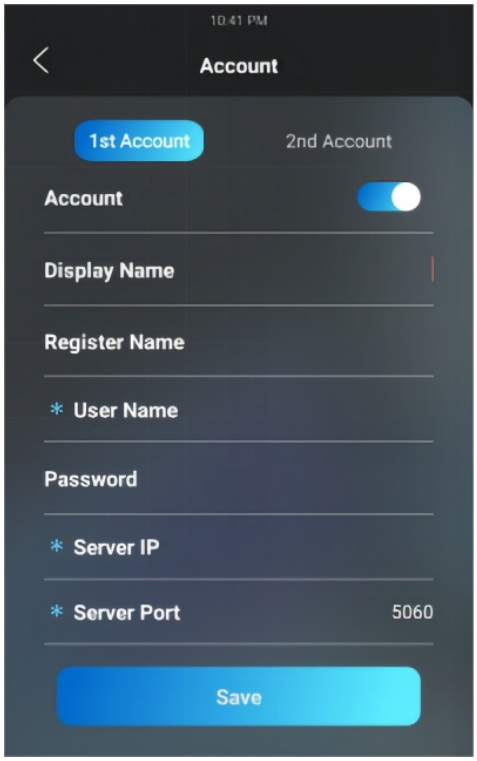
  - To designate the account to be used for outgoing calls, select the account number for contacts or dial plan prefixes in their settings.

> **Tip**
>
> For configuring contact call and dial plan, see here.

- **Display Label:** the label of the device.
- **Display Name:** the designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** same as the username from the PBX server.
- **User Name:** same as the username from the PBX server for authentication.
- **Password:** same as the password from the PBX server for authentication.

Configure SIP Account on the Device

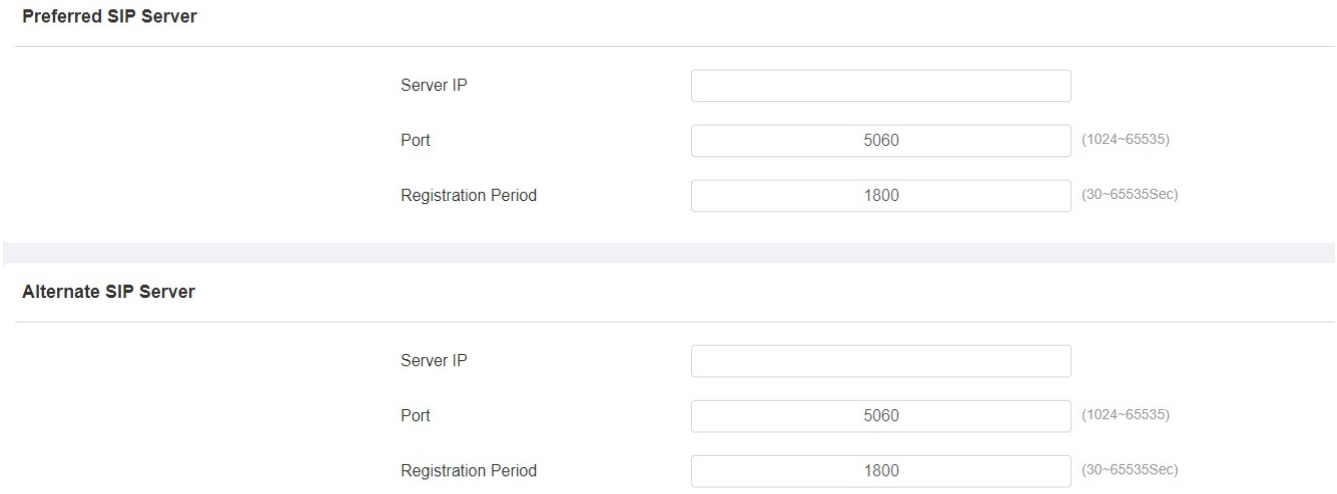
To configure the SIP account on the device **Setting > Account** interface.



SIP Server Configuration

SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

Navigate to the web **Account > Basic > Preferred SIP Server** interface.

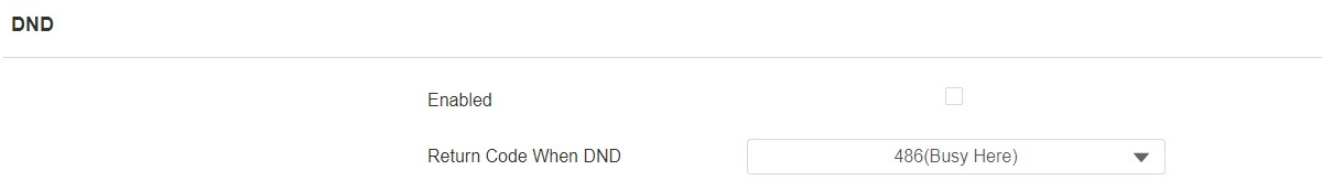


- **Server IP**: enter the Server's IP address number or its URL.
- **Port**: set up SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time. SIP re-registration will start automatically if the account registration fails during the registration time. The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

SIP Call DND & Return Code Configuration

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

Navigate to the web **Intercom > Call Feature > DND** interface.



- **Return Code When DND**: specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

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.

Navigate to the web **Account > Basic > Outbound Proxy Server** interface.

- **Preferred Server IP:** enter the SIP proxy IP address.
- **Port:** set the port for establishing a call session via the outbound proxy server.
- **Alternate Server IP:** enter the SIP proxy IP address to be used when the main proxy malfunctions.
- **Port:** set the proxy port for establishing a call session via the backup outbound proxy server.

Data Transmission Type Configuration

Akuvox intercom devices support four data transmission protocols: **User Datagram Protocol(UDP)**, **Transmission Control Protocol(TCP)**, **Transport Layer Security(TLS)**, and **DNS-SRV**.

Navigate to the web **Account > Basic > Transport Type** interface.

- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.

- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.
- **DNS-SRV:** A DNS service record defines the location of servers. This record includes the hostname and port number of the server, as well as the priority and weight values that determine the order and frequency of using the server.

Dial Options Configuration

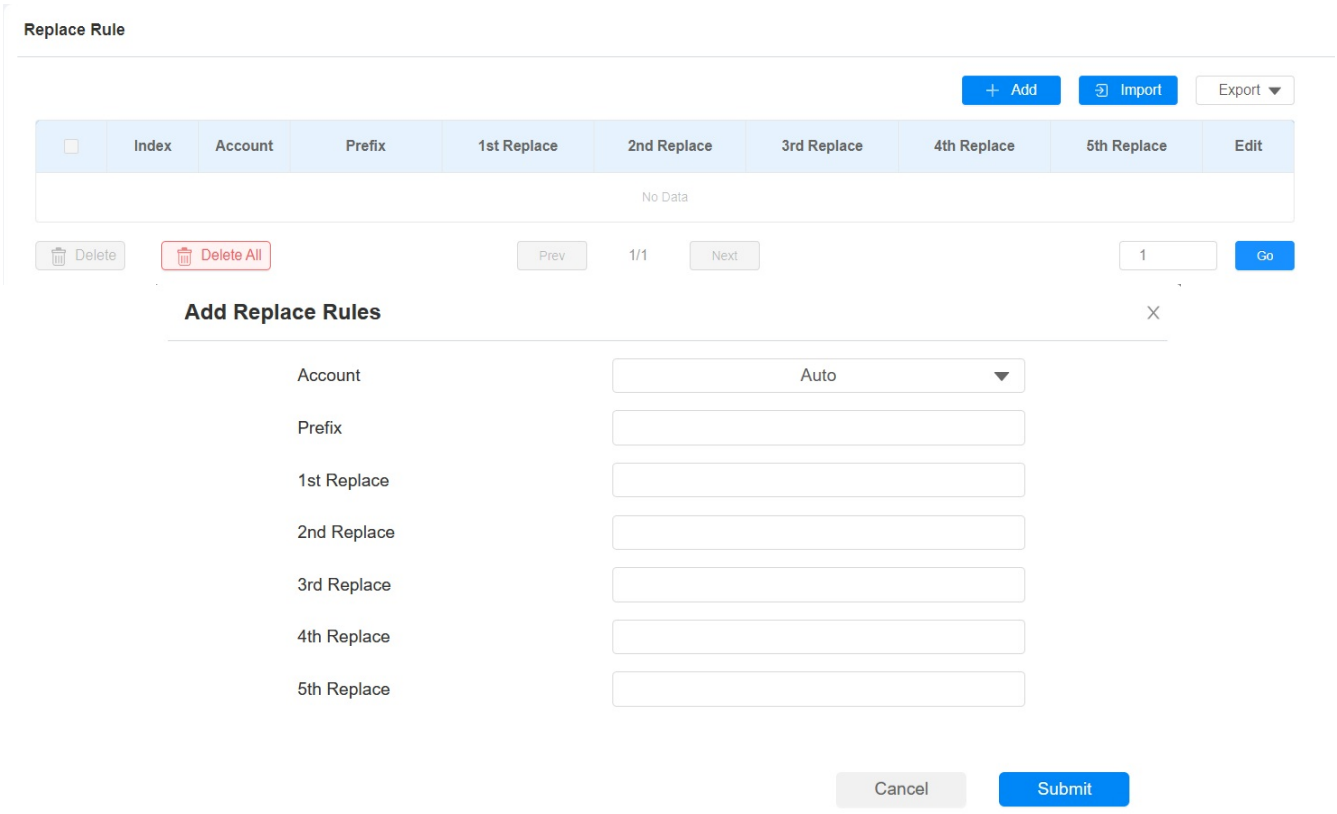
Quick Dial by Number Replacement

The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

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.

Navigate to the web **Intercom > Dial Plan > Replace Rule** interface. Click +Add.



- **Account:** select the dial-out account.

  - **Auto:** dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.

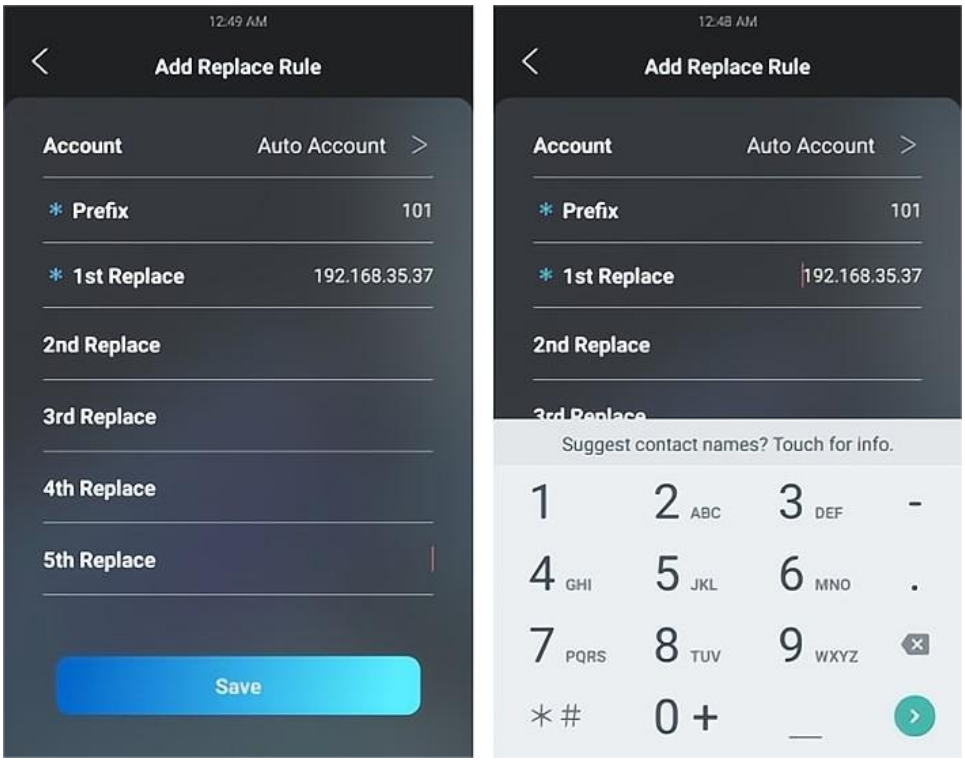
  - **Account 1/2:** dial-out using the chosen account.

- **Prefix:** specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** specify up to 5 numbers, which can be SIP numbers or IP addresses, to be replaced by the prefix. All these numbers will be called simultaneously when the caller dials the prefix.

> **Note**
>
> The check box for each line of **Prefix** should be checked before you can see the **Edit** tab, which you click to modify.

Quick Dial by Number Replacement on the Device

To configure number replacement on the device **Setting > Replace Rule > Add Replace Rule** screen.

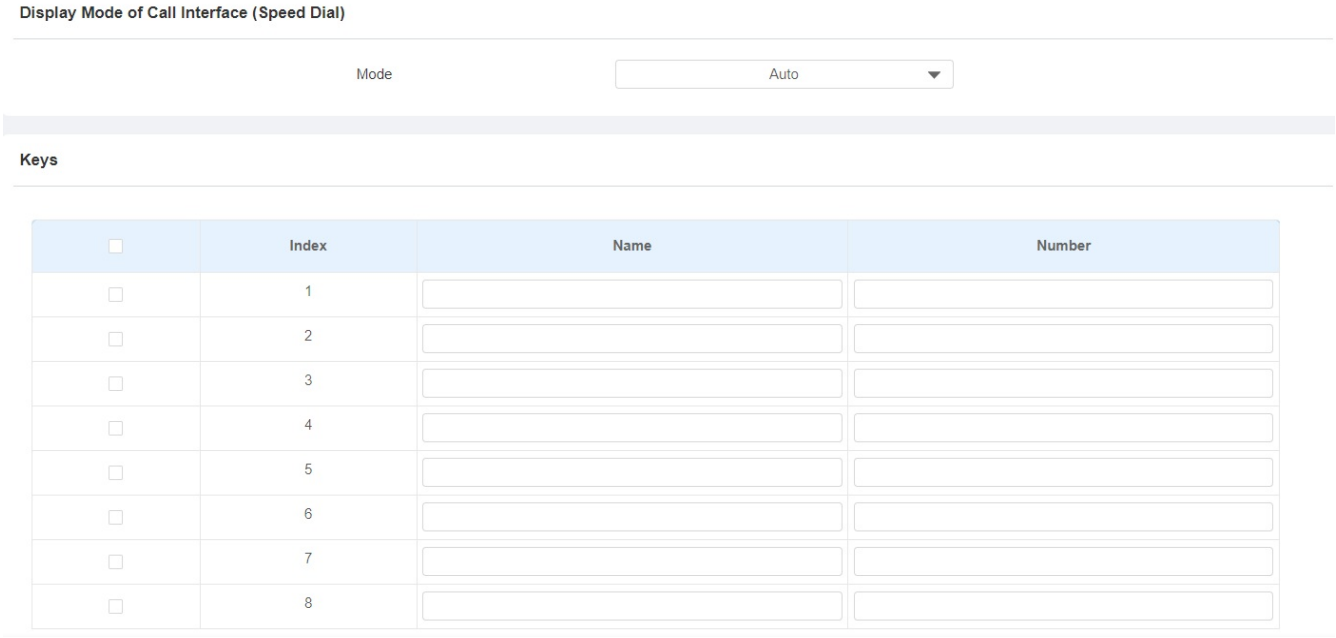


Speed Dial

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 **Setting > Key/Display > Display Mode of Call Interface (Speed Dial)**.



- **Mode:** define layouts for speed dial buttons and the keypad on the dial screen. The 9 options are explained as follows:

Options	Descriptions
Standard	Display time and keypad.
Auto	Display all speed dail buttons set by the users.
1 Key	Display a single contract without the keypad.
1 Key + Keypad	Display a single dial button with the keypad.
2 Keys+ Keypad	Display up to 2 dial buttons with the keypad.
4 Keys+ Keypad	Display up to 4 dial buttons with the keypad.
8 Keys	Display up to 8 dial buttons without the keypad.
16 Keys	Display up to 16 dial buttons without the keypad.
64 Keys	Display up to 64 dial buttons without the keypad.

Note

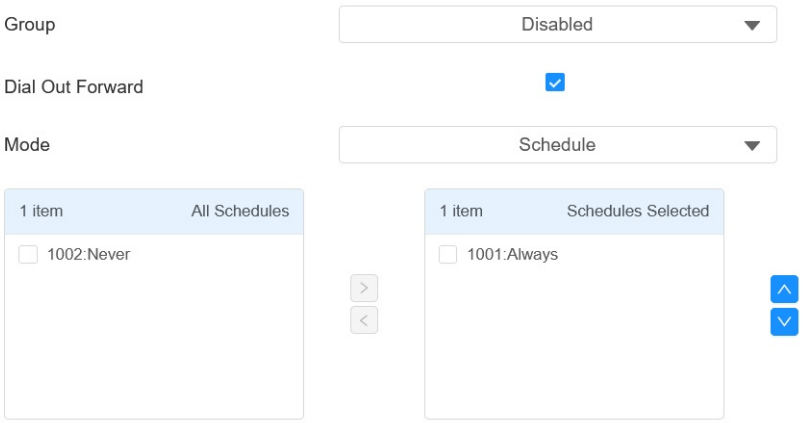
- This function cannot be applied in **Building Mode**.
- The keypad will not be displayed if the number of the dial tabs is over 4 tabs.

Speed Dial in Building Mode

The door phone allows you to call a group of people at the same by pressing the **Reception** button.

Navigate to the web **Setting > Key/Display > Speed Dial Setting** interface.

Speed Dial Setting



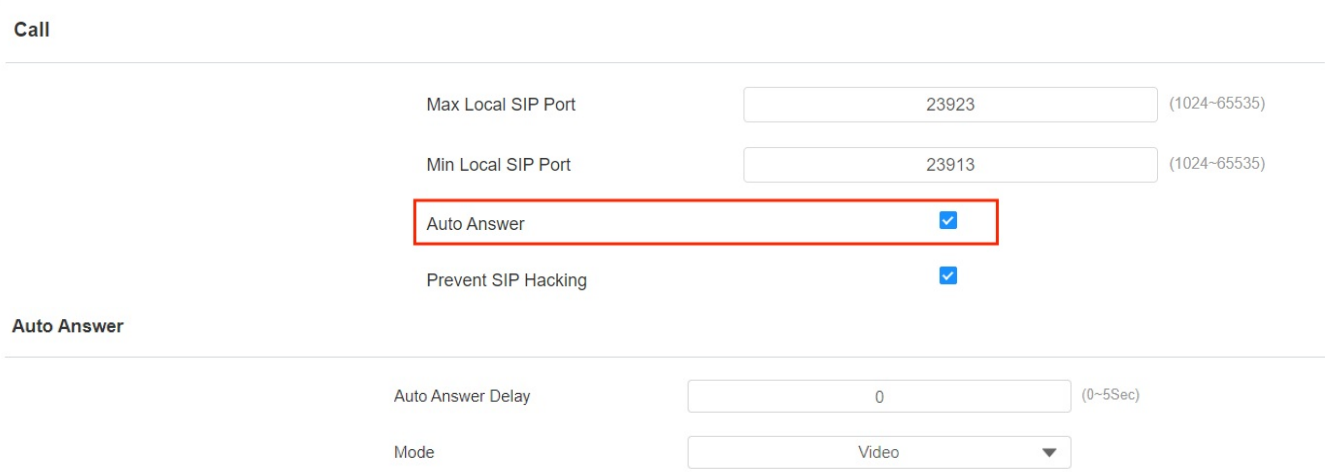
- **Group**: select the contact group to be called by pressing the Reception button.
- **Dial Out Forward**: when enabled, all calls will be made to the same target number when pressing the Reception button.
- **Mode**: when Dial Out Forward is enabled, configure the schedule when the feature is working. You can also select **Auto Disable** and decide after how many hours, the feature will be turned off.

Call Settings

Call Auto-answer Configuration

Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To enable the feature on the web **Account > Advanced > Call** interface and to configure it on the web **Intercom > Call Feature > Auto Answer** interface.

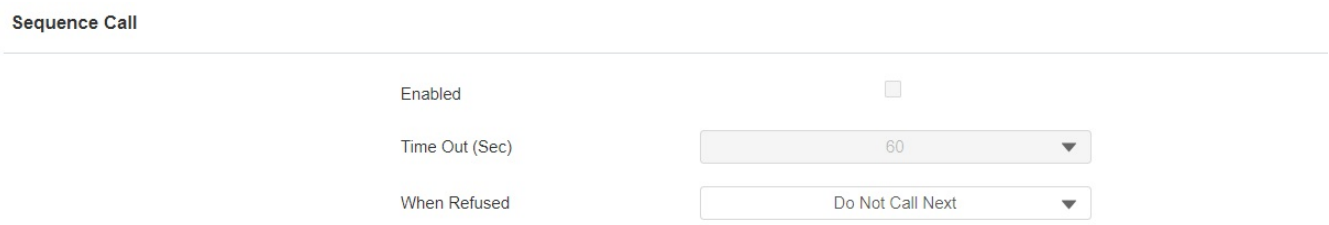


- **Auto Answer Delay:** set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Mode:** determine whether to auto-answer the call as a video or audio call.

Sequence Call Configuration

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application.

Navigate to the web **Intercom > Basic > Sequence Call** interface.



- **Time Out(Sec):** specify the time limit for the call between two sequential call numbers. For example, if the time value is set to 10, the call that is not answered in 10 seconds will be ended automatically and transferred to the next call number in order.
- **When Refused:** determine whether to call the next if a call was rejected by the previously called party.

  - Do Not Call Next: the sequence call will stop when the call is refused.

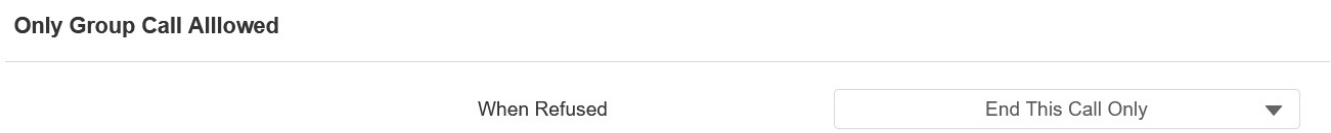
- **Call Next:** the device will call the next number in order when the call is refused.

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

Group Call

You can configure the action when a group call is refused.

Navigate to the web **Intercom > Basic > Only Group Call Allowed** interface.

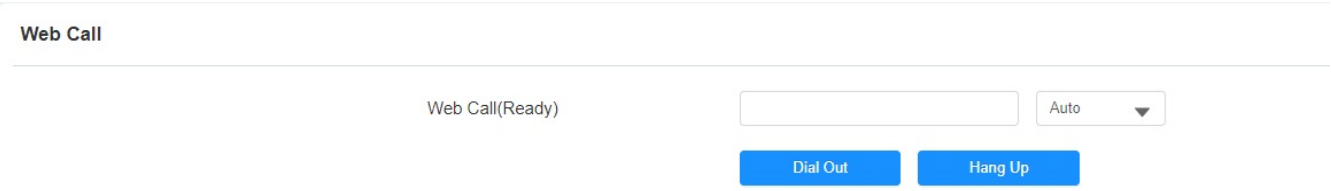


When Refused: if you select **End All Calls**, the group call will be terminated if the call is rejected by the called party. If you select **End This Call Only**, the group call will be continued when it is refused by one of the callees.

Web Call

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

Navigate to the web **System > Maintenance > Web Call** interface. Select the registered SIP account to make the web call.



Make Two-way Video Call

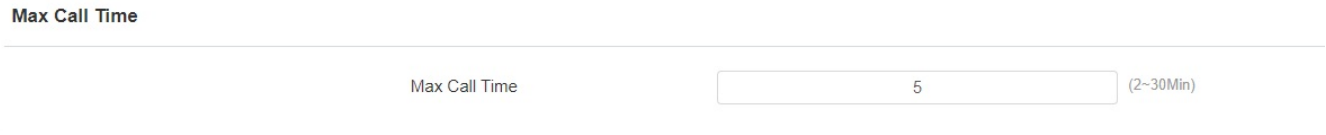
The two-way video feature allows for visual connection with both callers and recipients via the door phone, providing a more interactive and secure conversation.

Navigate to the web **Intercom > Basic > Two-way Video** interface.

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.

Navigate to the web **Intercom > Call Feature > Max Call Time** interface.

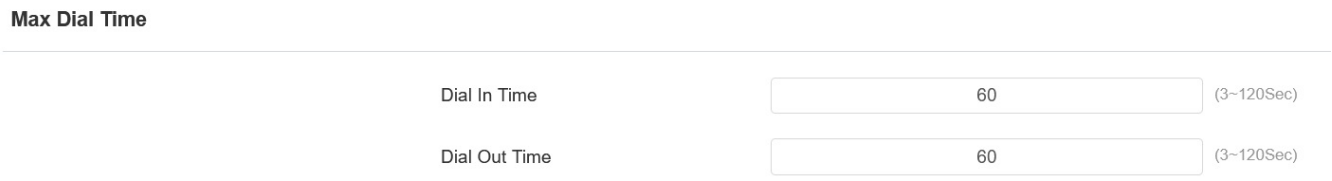


- **Max Call Time:** specify the maximum duration of all calls. The door phone will end the call automatically when the time limit is reached.

Maximum Dial Duration Setting

Maximum Dial Duration is the time limit for incoming- and/or outgoing calls on the door phone. If configured, the door phone will automatically terminate the call if no one answers the call within the preset time, whether it is incoming or outgoing.

Navigate to the web **Intercom > Call Feature > Max Dial Time** interface.

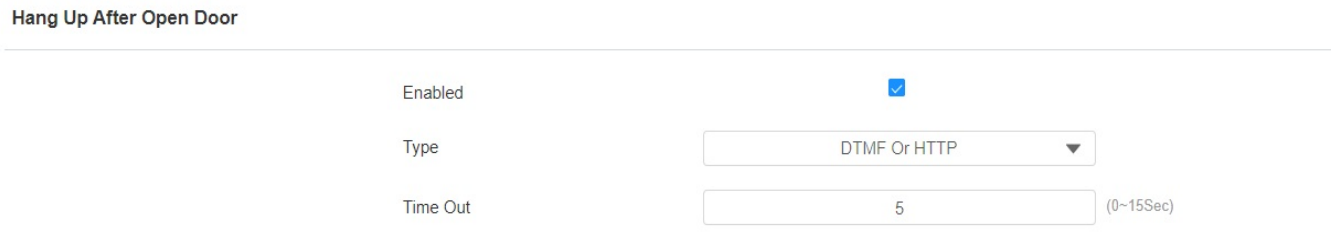


- **Dial In Time:** specify the maximum duration of an incoming call. The door phone will automatically end the incoming call if it is not answered within the preset time.
- **Dial Out Time:** specify the maximum duration of an outgoing call. The door phone will automatically end the call it dialed out if there is no answer from the recipient within the preset time.

Hang Up After Open Door

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

Navigate to the web **Intercom > Call Feature > Hang Up After Open Door** interface.



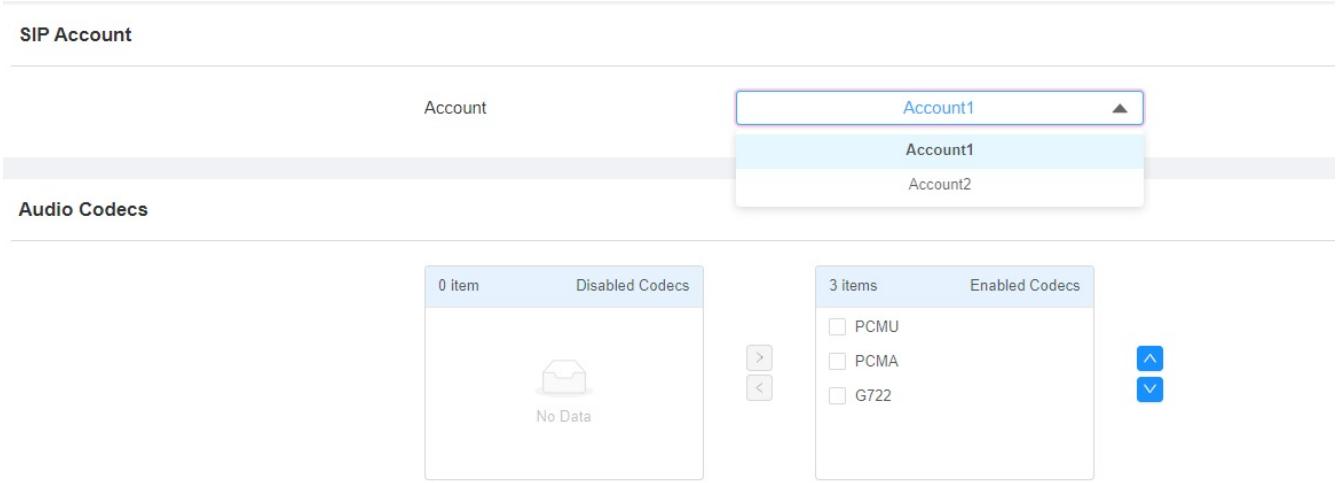
- **Type:** specify the door unlock method. If this specific method is used to release the door during a call, the door phone will end the call when the preset hang-up time is reached.
- **Time Out:** specify the hang-up time limit. The door phone will automatically terminate the call when the specific time reached after the door is opened.

Audio& Video Codec Configuration for SIP Calls

Audio Codec Configuration

The door phone supports three types of codec (PCMU, PCMA, 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.

Navigate to the web **Account > Advanced > SIP Account** interface.



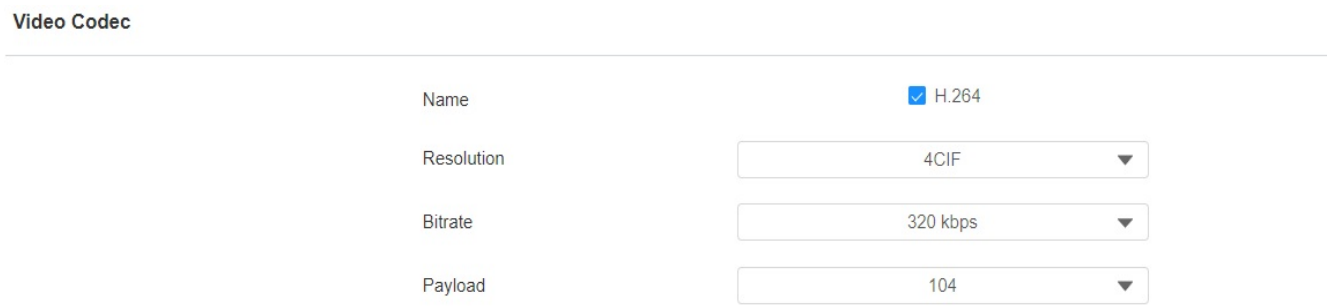
Please refer to the bandwidth consumption and sample rate for the codec types below:

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

Video Codec Configuration

The door phone supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

Navigate to the web **Account > Advanced > Video Codec** interface.



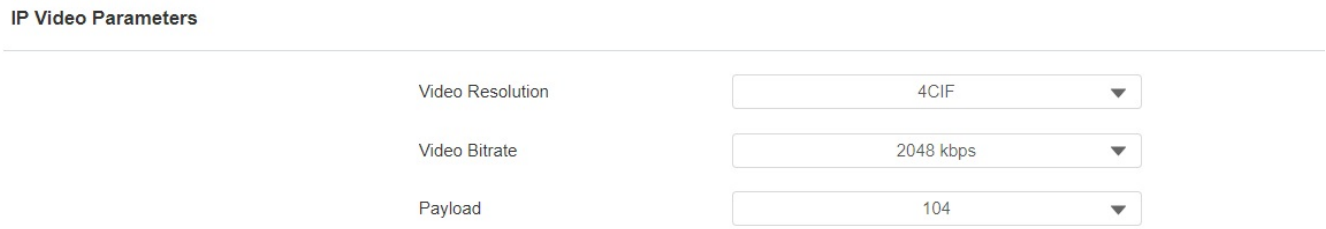
- **Name**: check to select the H264 video codec format for the door phone video H264 is the video codec by default.
- **Resolution**: select the code resolution for the video quality among **QCIF, CIF, VGA, 4CIF,** and **720P** according to the actual network environment. The default code resolution is VGA.
- **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, the clearer the video will be. The default code bitrate is 512 kbps.

- **Payload**: select the payload type (ranging from 90-119) to configure the audio/video configuration file. The default payload is 104.

Video Codec Configuration for IP Direct Calls

You can select the IP call video quality by selecting the proper codec resolution according to the network condition.

Navigate to the web **Intercom > Call Feature > IP Video Parameters** interface.

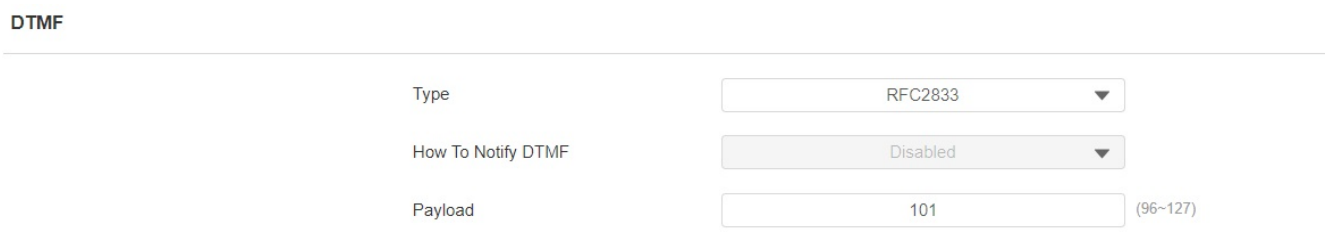


- **Video Resolution**: select the code resolution for the video quality among **CIF, VGA, 4CIF,** and **720P**. The default code resolution is 720P.
- **Video Bitrate**: select video bit-rate among **128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps,** and **4096 kbps** according to the network environment. The default video bit rate is **2048 kbps**.
- **Video Payload**: select the payload type (ranging from 90-119) to configure the audio/ video configuration file. The default payload is 104.

Configure DTMF Data Transmission

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

Navigate to the web **Account > Advanced > DTMF** interface.



- **Mode**: select DTMF mode among **Inband, RFC2833, Info, Info+Inband, Info+RFC2833,** and **Info+Inband+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: **Disabled, 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.

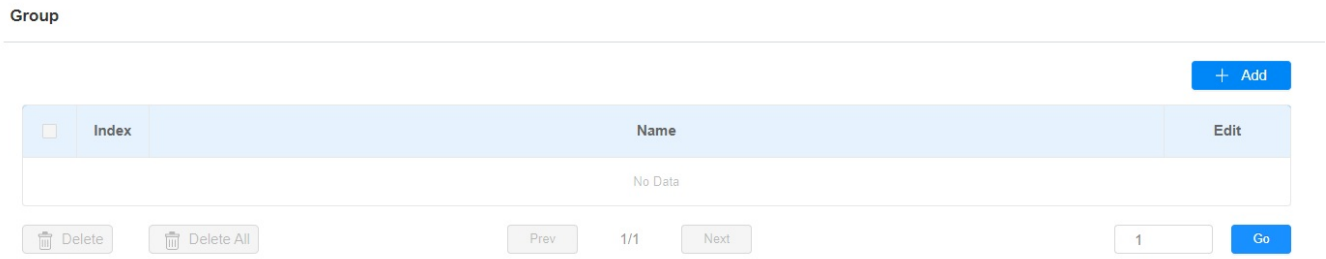
Phone Book Configuration

Phone Book Configuration on the Web Interface

Manage Contact Groups on the Web Interface

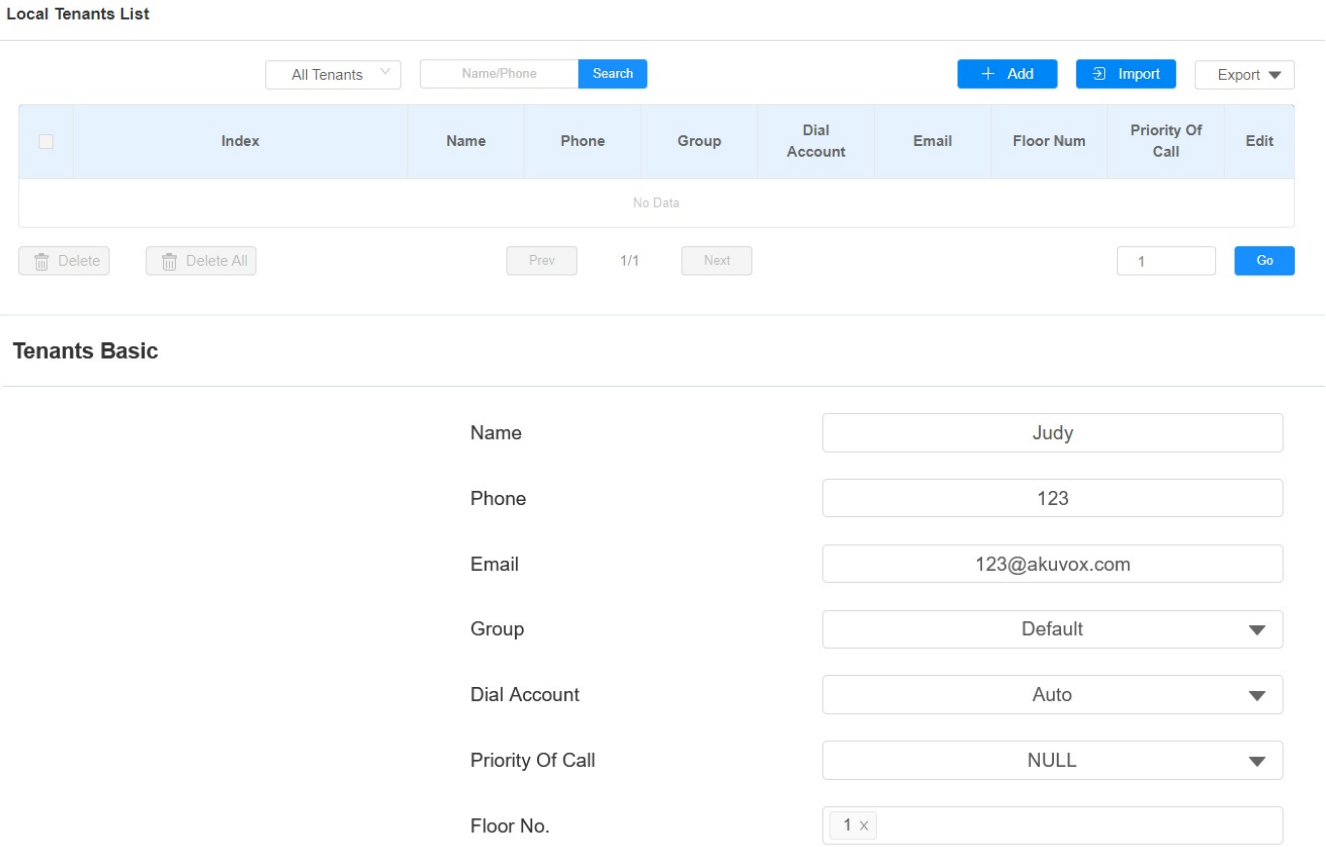
You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

Navigate to the web **Directory > Tenants List > Group** interface.



Contact List Configuration on the Web Interface

Navigate to the web **Directory > Tenants List > Local Tenants List** interface. Click **+Add** to add a contact.



Priority of Call: set the priority of the call among four options: **Null, Firstly, Secondary**, and **Lastly**. This feature is mainly applicable to the contacts in a specific contact group. For example, if you set the priority of call for one of the contacts in a specific contact group as **Firstly,** then the contact will be the first to be called among all the contacts in the same contact group when someone presses on the contact group for making a group call.

Note

- Priority of Call of a contact cannot be set when the contact does belong to any contact group.
- The contact file format for import should be in CSV or XML format while the contact file format for export should be XML, CSV, and VCF format. And the maximum contact import number is 3000.
- Only the SIP numbers of the contacts can be called out through the SIP account. IP numbers are not valid for this application.
- Group must be created first before you can select or change the group.

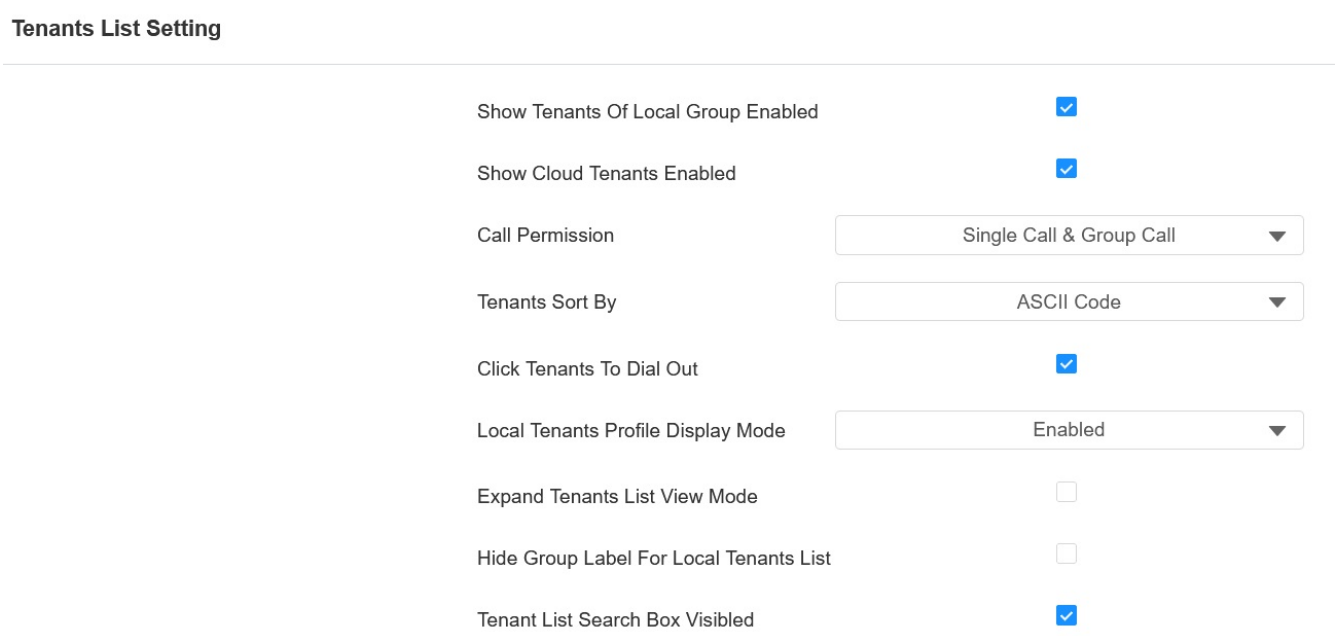
Phone Book Configuration on the Device

You can also configure the phone book on the device **Setting > Tenants** screen.

Contact List Display Setting

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

Navigate to the web **Directory > Tenants List > Tenants List Setting** interface.



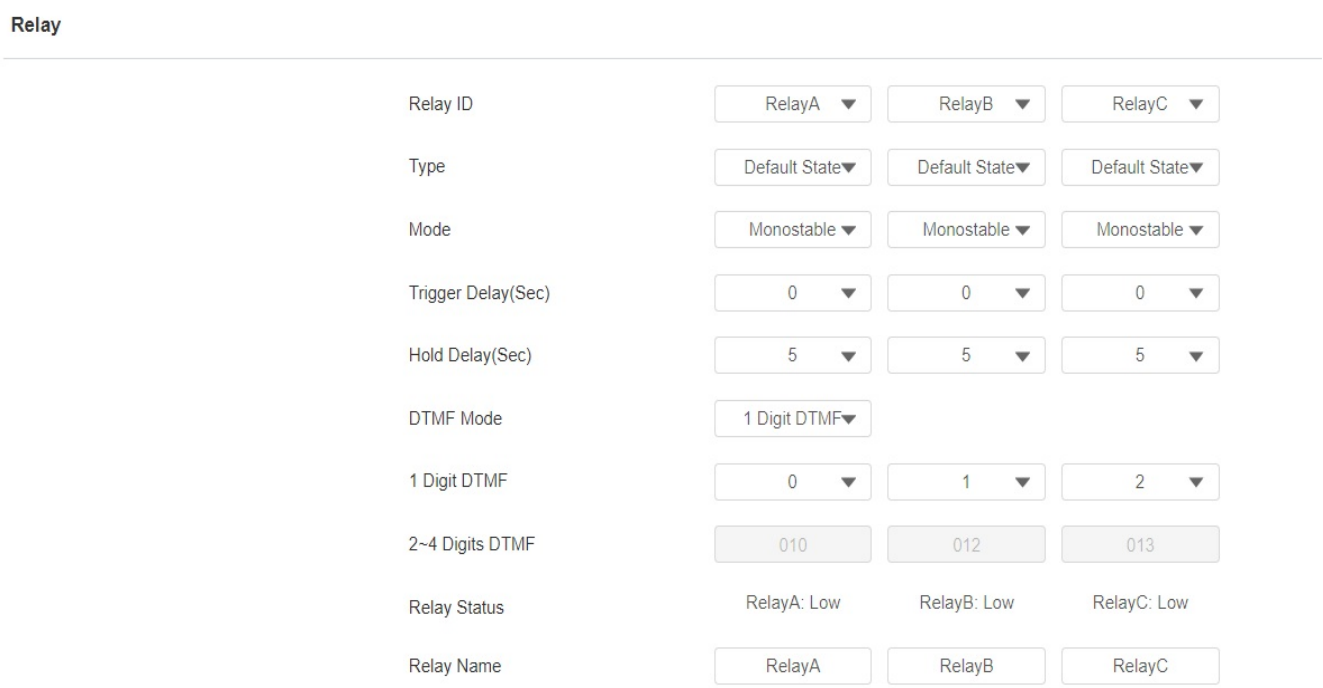
- **Show Tenants of Local Group Enabled**: tick or untick the check box to control the display of the group label. If you untick the check box, then only the group tab will be displayed while the contact tab will be concealed and vice versa.
- **Show Cloud Tenants Enabled**: tick the check box to show the cloud tenants in the tenants' list. And when you untick the check box, the cloud tenants will be concealed.
- **Tenants Sort By**:
    - ASCII Code: the tenants will be listed by their names in the sequence of the ASCII code.
    - Room No.: the tenants will be sorted according to their room numbers.
    - Import: the tenants will be sorted according to their orders in the imported file.

- **Click Tenants to Dial Out**: when enabled, you can press anywhere on the contact tab to dial out. When disabled, users need to press the Call icon to dial out.
- **Local Tenants Profile Display Mode**:
    - Enabled: if the tenant has the 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.
    - Disabled: the picture or the icon will not be displayed.
    - Auto: if the tenant has the 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. When enabled, the contact tab will be widened.
- **Hide Group Label for Local Tenants List**: control the display of the group label. When enabled, only the contact tab will be displayed while the group tab will be concealed.
- **Contact List Search Box Visible**: control the display of the **Tap here to search field** on the top of the screen. When disabled, the **Tap here to search** field will be concealed.

Door Access Control Configuration

Relay Switch Setting

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



- **Relay ID**: you are allowed to set up three relay switches in total for the door access control.
- **Type**: if the Default state is selected, the Relay Status shows Low which means the door is closed, and if the Relay Status shows High, the door is opened. If Invert State is selected, the Relay Status shows High which means the door is closed, and Low means the door is opened.
- **Mode**: there are two modes Monostable and Bistable. If Monostable is selected, the relay status will be automatically reset within the relay delay time after the relay is triggered. If Bistable is selected, the relay status will be reset after the relay is triggered again.
- **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 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 resume the initial state after maintaining the triggered state for 5s.
- **DTMF Option**: select the number of DTMF digits for the door access control (ranging from 1-4 digits) For example, you can select 1-digit DTMF code or 2-digit DTMF code, etc., according to your need.
- **DTMF**: set the 1-digit DTMF code within the range (**0-9 and *,#**) if the DTMF Option is set as **1-Digit**.
- **Multiple DTMF**: set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digit DTMF code if the **DTMP Option** is set as 3 digits.
- **Relay Status**: relay status is low by default which means normally closed(NC). If the relay status is high, then it is in Normally Open status(NO).

- **Relay Name**: name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

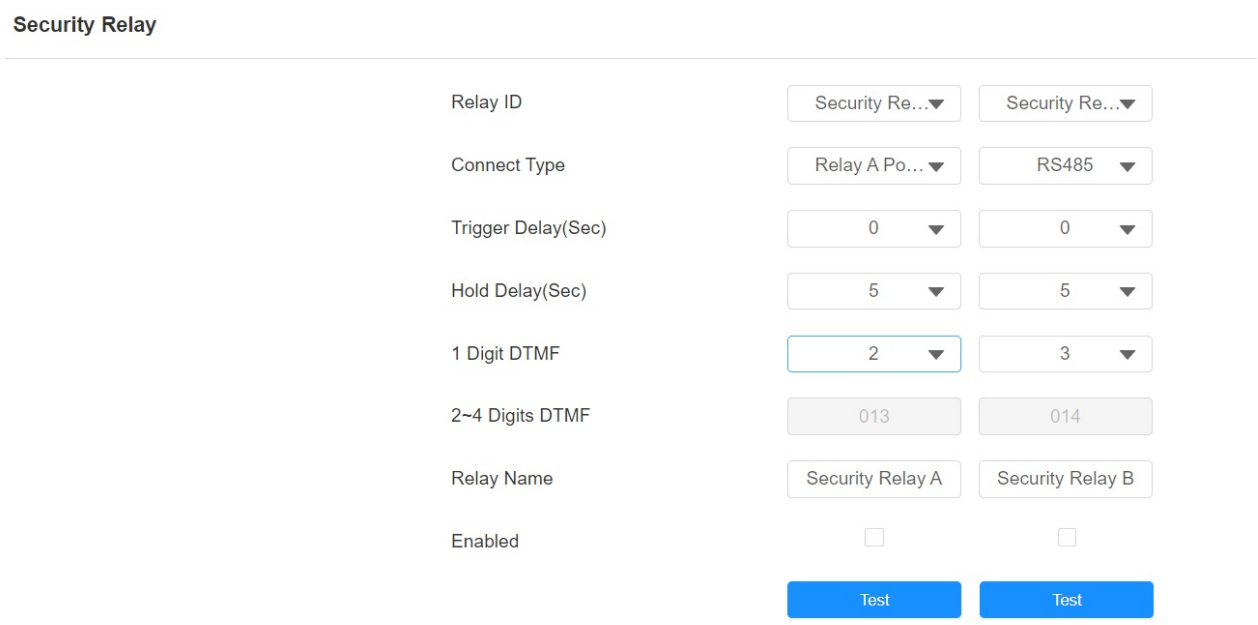
Note

- Only the external devices connected to the relay switch need to be powered by powered adapters as the relay switch does not supply power.

Security Relay Setting

The Security Relay, known as Akuvox SR01, is a product designed to bolster access security by preventing unauthorized forced entry attempts. Installed inside the door, it directly governs the door opening mechanism, ensuring that the door remains secure even in the event of damage to the device.

Navigate to the web **Access Control > Relay > Security Relay** interface.



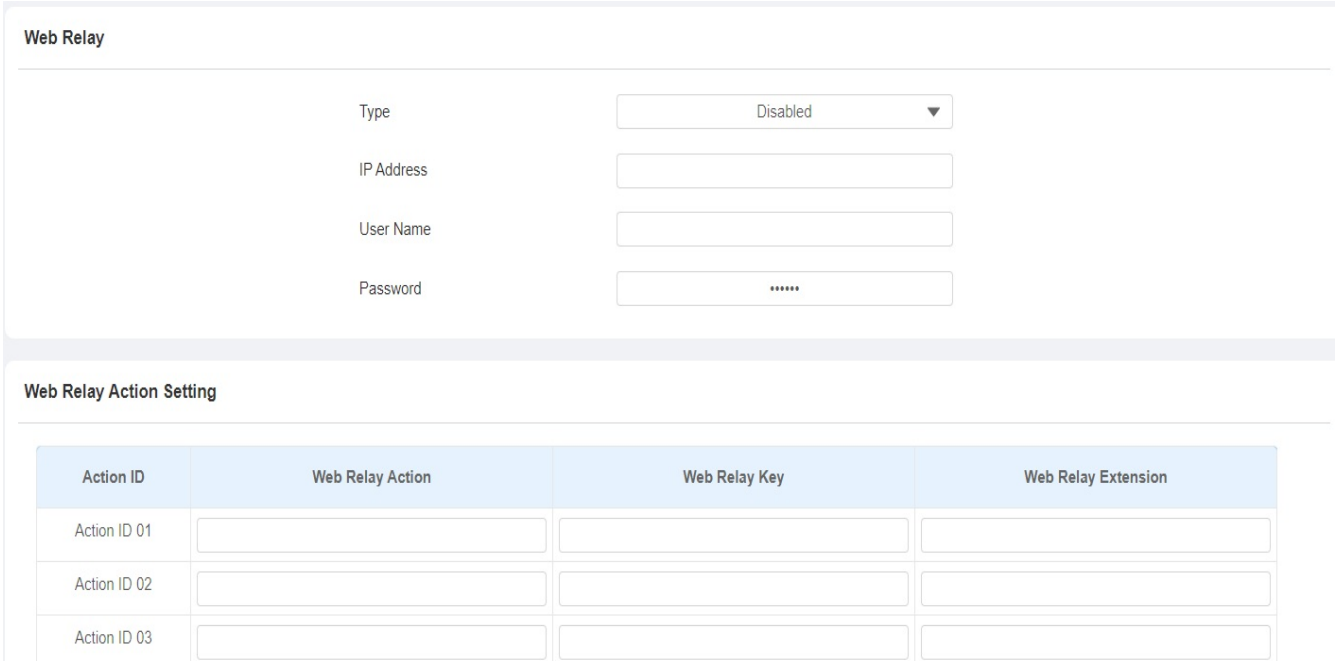
- **Connect Type**: select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Trigger Delay (Sec)**: set the relay trigger delay timing (ranging from 1-10 Sec.). For example, if you set the delay time as 5 seconds, then the relay will not be triggered until 5 seconds after you press the Unlock tab. The default is 0, meaning triggering relay right after you press the unlock tab.

- **Hold Delay (Sec)**: set the relay hold delay time (ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. then the relay will be delayed for 5 after the door is unlocked.
- **1 Digit DTMF**: set the 1 digit DTMF code 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**: name the relay to distinguish it from others.

Web Relay Setting

A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.

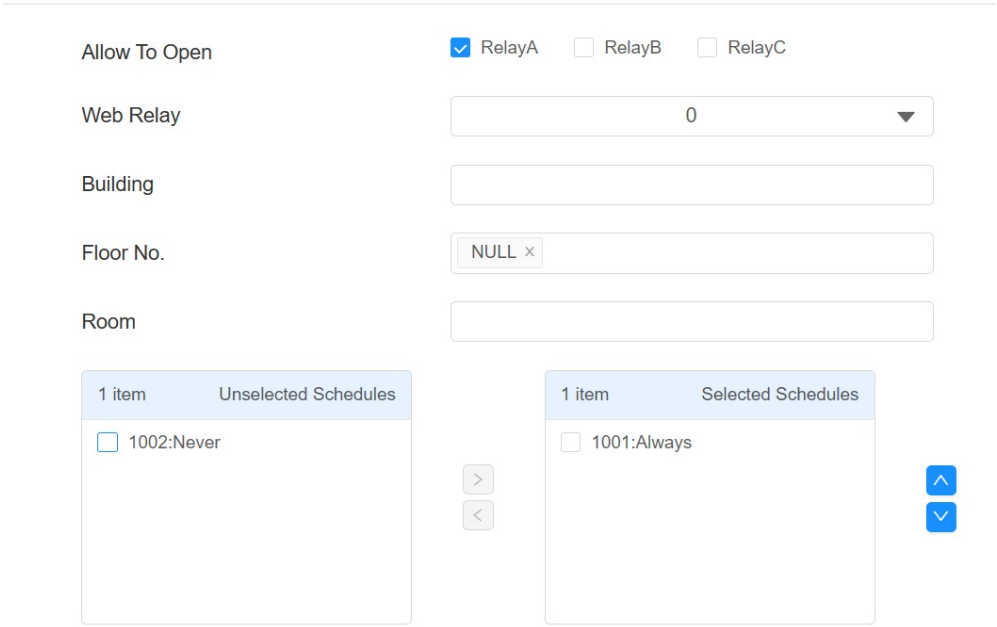
To set up a WebRelay, navigate to the web **Access Control > Web Relay**. **IP address, User Name**, and **Password** are provided by the web manufacturer.



- **Type**: select among three options **Disabled, Web Relay**, and **Both**. Select **Web Relay** to enable the web relay. Select **Disabled** to disable the web relay. Select **Both** to enable both local relay and web relay.

- **Password**: 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.
- **Web Relay Extension**: enter the SIP/IP number of a specific device to trigger WebRelay via DTMF code.

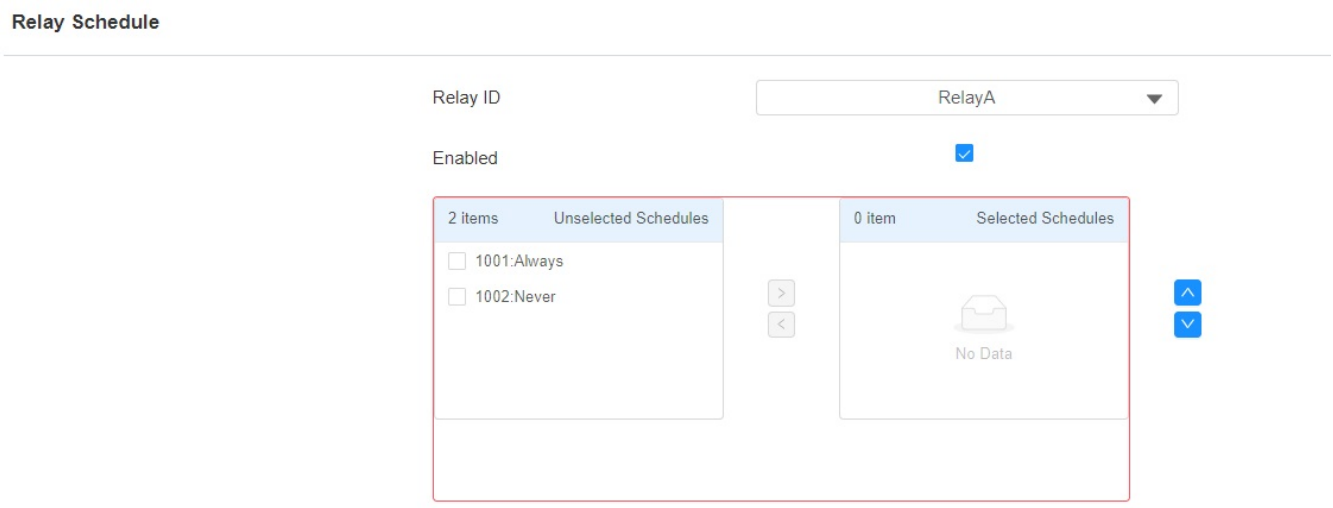
You can select the configured WebRelay on the web **Directory > User > Add/Edit** interface.



Relay Schedule

The relay schedule allows you to set a specific relay to always open at a certain time. This is helpful for situations like keeping the gate open after school or keeping the door open during work hours.

Navigate to the web **Access Control > Relay > Relay Schedule** interface.



- **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 Configure Door Access Schedule.

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

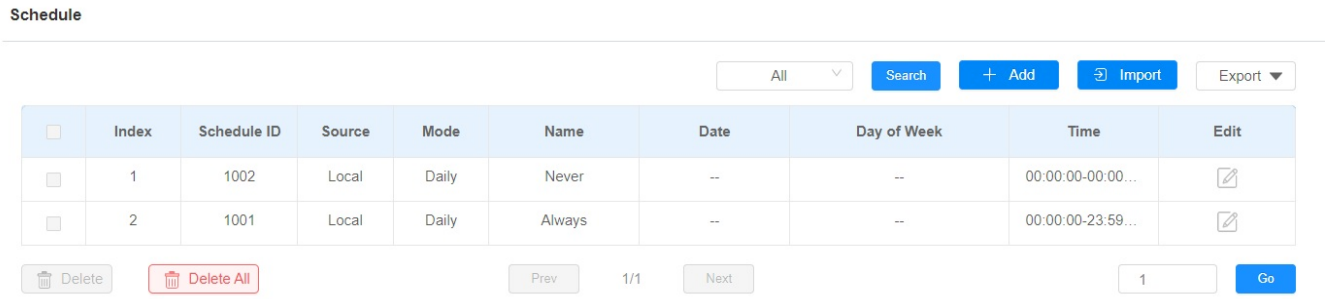
Configure Door Access Schedule

A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

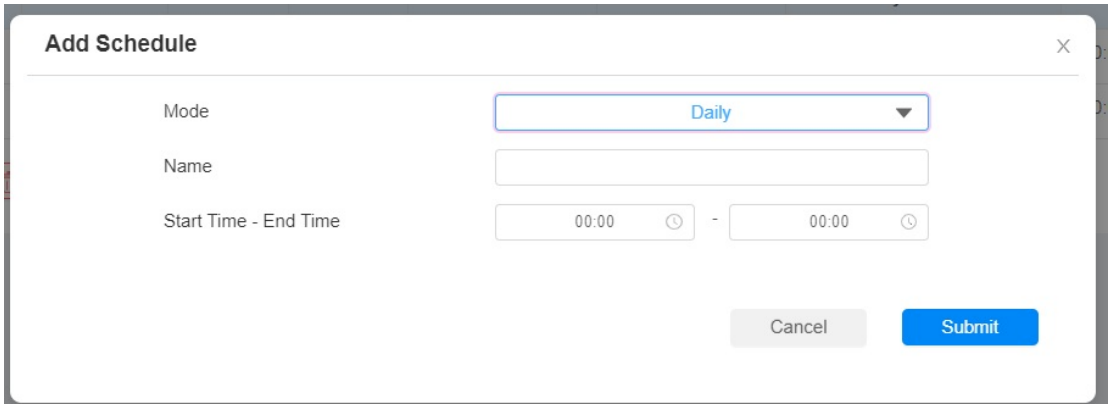
Create Door Access Schedule

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

Navigate to the web **Setting > Schedule** interface.

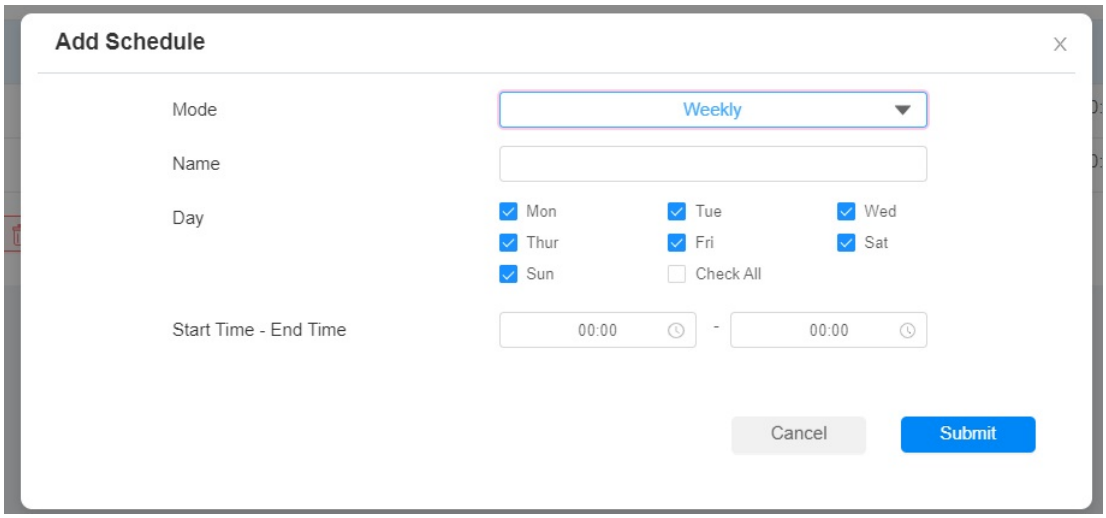


To create a daily schedule:

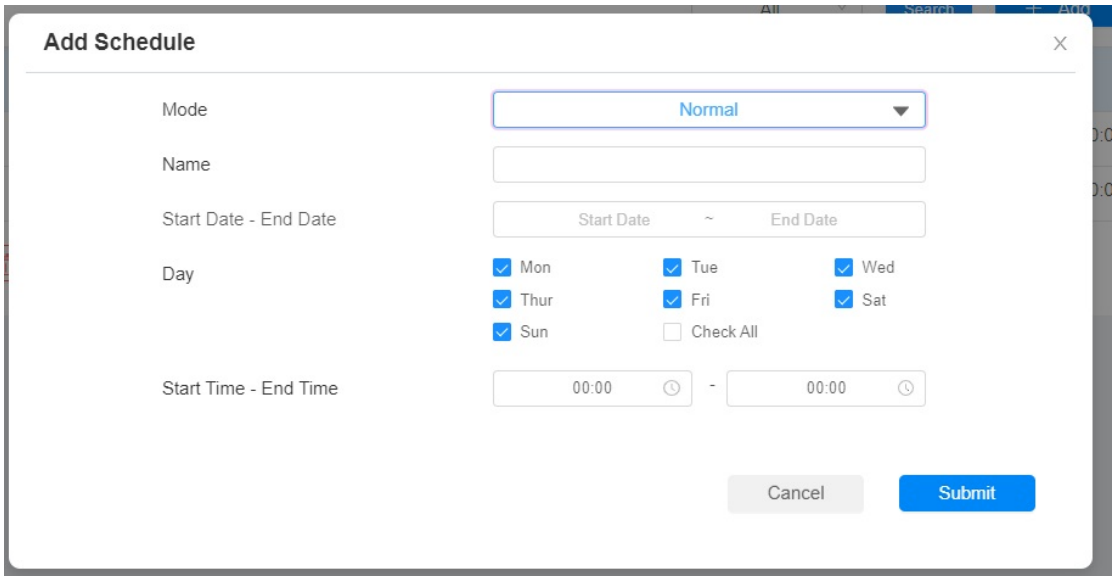


- **Start Time-End Time**: set up the schedule for the validity of the door access during the day.

To create a weekly schedule:



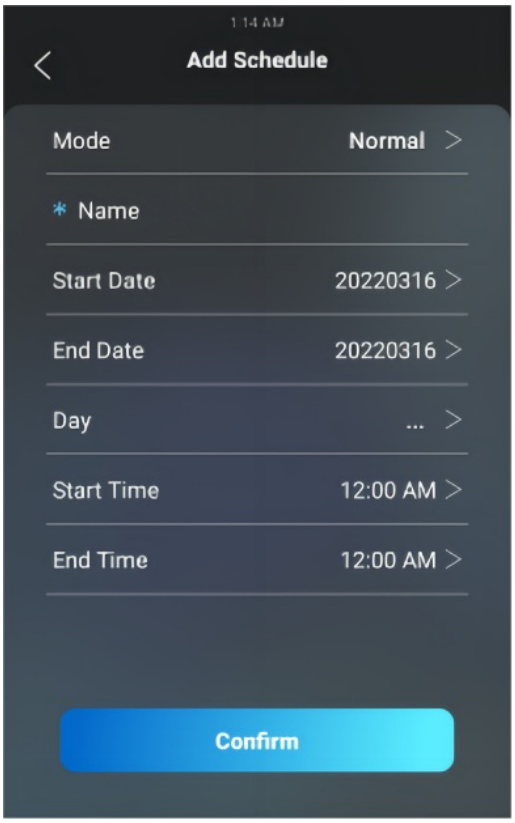
To create a longer period schedule:



Create Door Access Schedule on the Device

You can also create a door access schedule on the device.

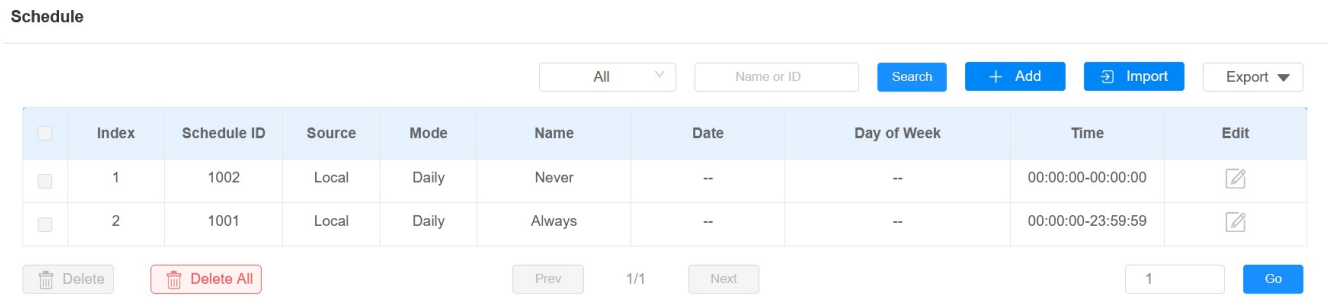
Navigate to the **Schedule > Add Schedule** screen.



Import and Export Door Access Schedule

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

Navigate to the web **Setting > Schedule** interface. Click Import or Export.



Note

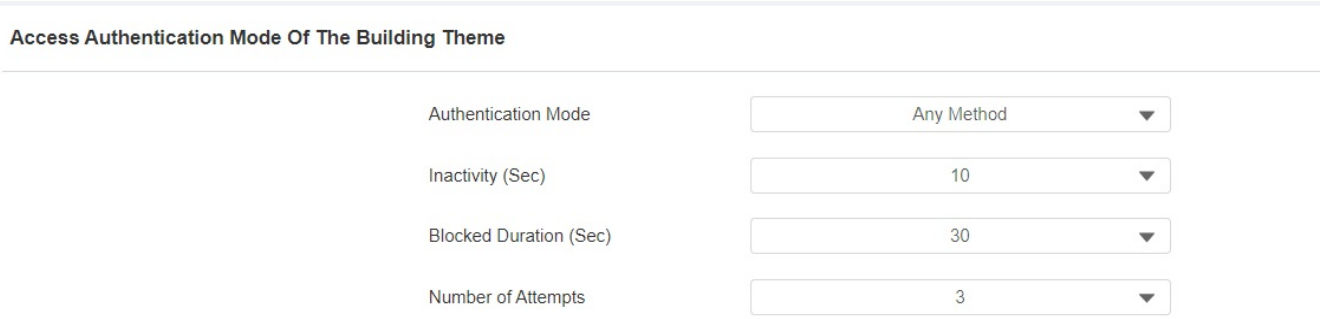
It only supports a .xml format file for importing and exporting the schedule.

Door Unlock Configuration

Access Authentication

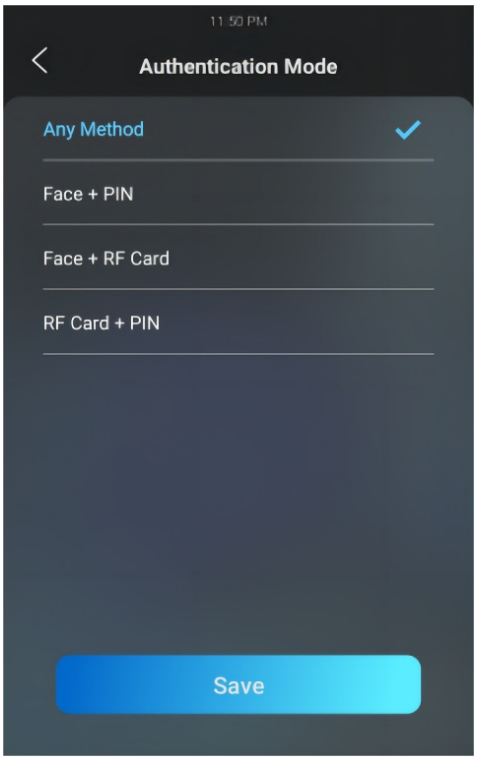
You can set up multiple access authentication modes, and set up authentication security as needed.

Navigate to the web **Access Control > Relay > Access Authentication Mode of The Building Theme** interface.



- **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 users have to enter the PIN code ten seconds after they go through 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 users fail to pass the second authentication three times, then users will be temporarily blocked from the first authentication according to the block time.
- **Number of Attempts**: the number of attempts users are allowed for the second authentication.

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



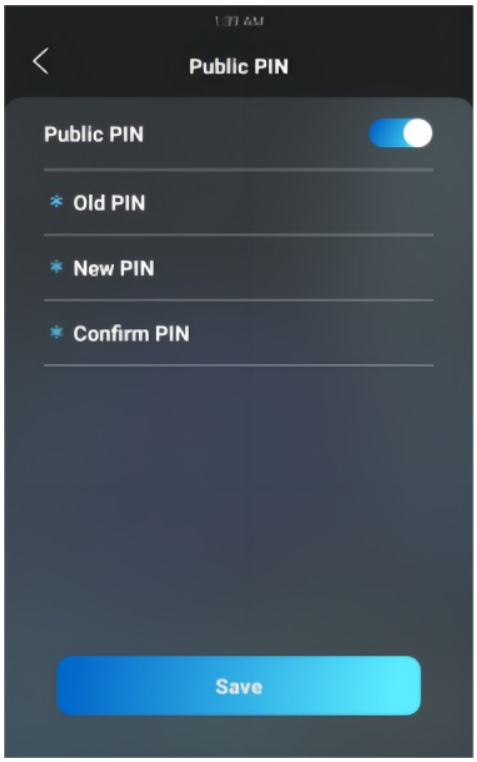
Configure PIN Code for Door Unlock

There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex. You can create and modify both the public and private PIN codes.

Navigate to the web **Access Control > PIN Setting > Public PIN** interface.

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

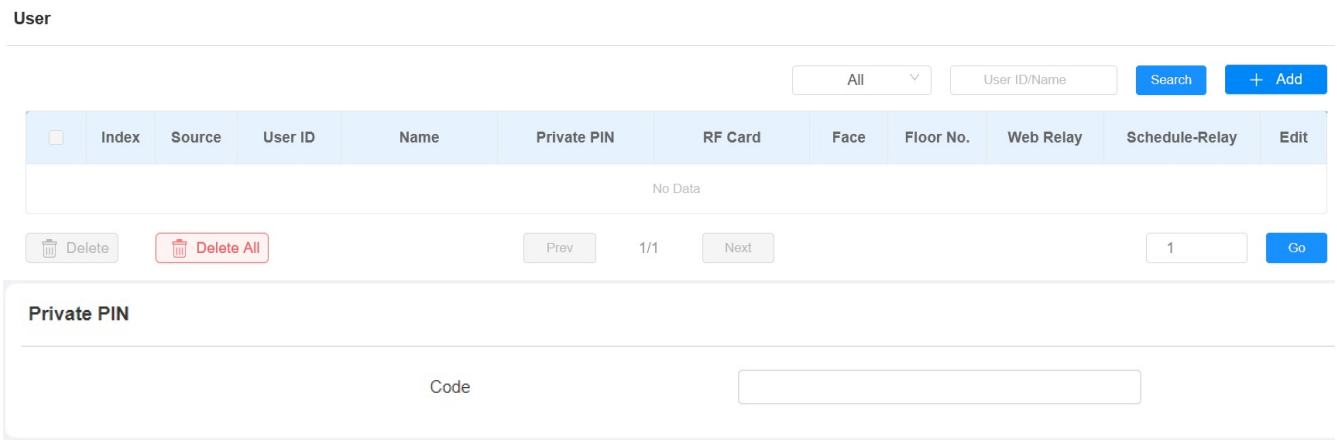
To configure it on the device, go to the **Security > Public PIN** screen.



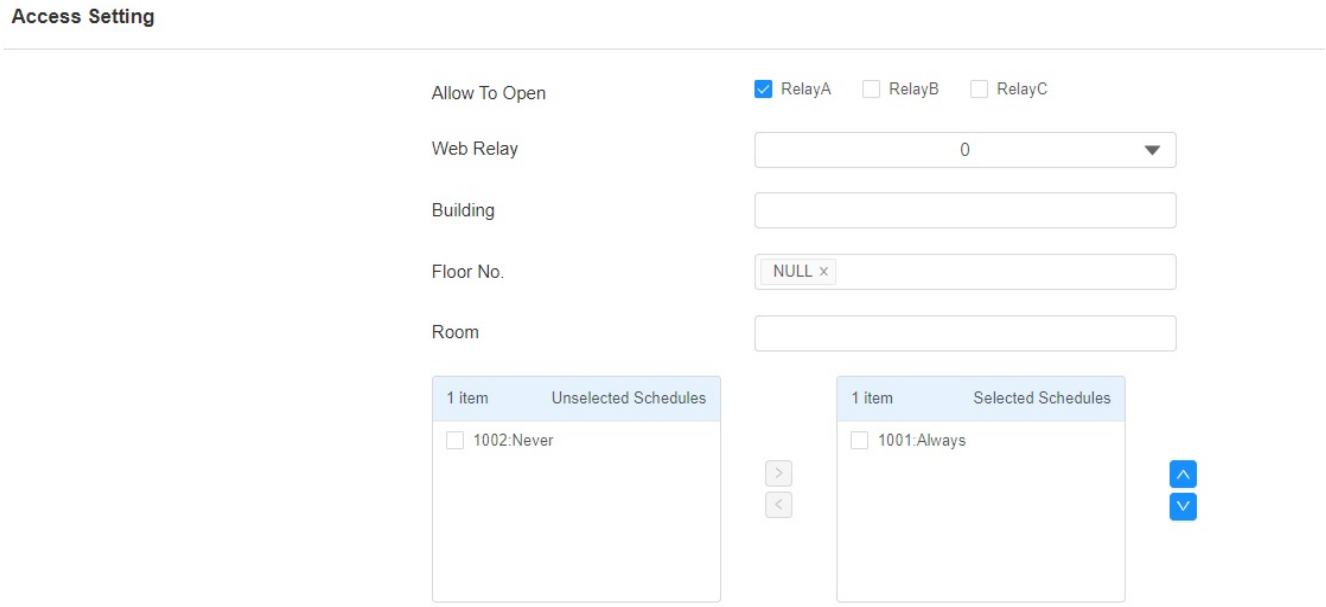
Configure Private PIN Code on the Web Interface

On the web interface, you can create the PIN code and customize additional settings, such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

Navigate to the web **Directory > User** interface. Click +Add.



Scroll down and select door access schedule for private PIN Code door access:



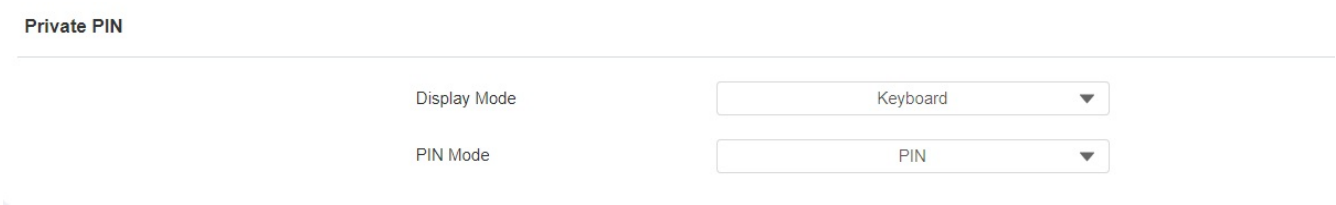
- **Allow To Open Relay**: select the relay to be triggered.
- **Web Relay**: select the specific number of web relay action commands you have set up on the web interface.
- **Schedule**: select from the created door access schedule on the left box and move the one to be applied to the user(s)-specific PIN code door access to the right box.

> **Note**
>
> This step applies to door access by RF card and facial recognition as they are identical in configuration.

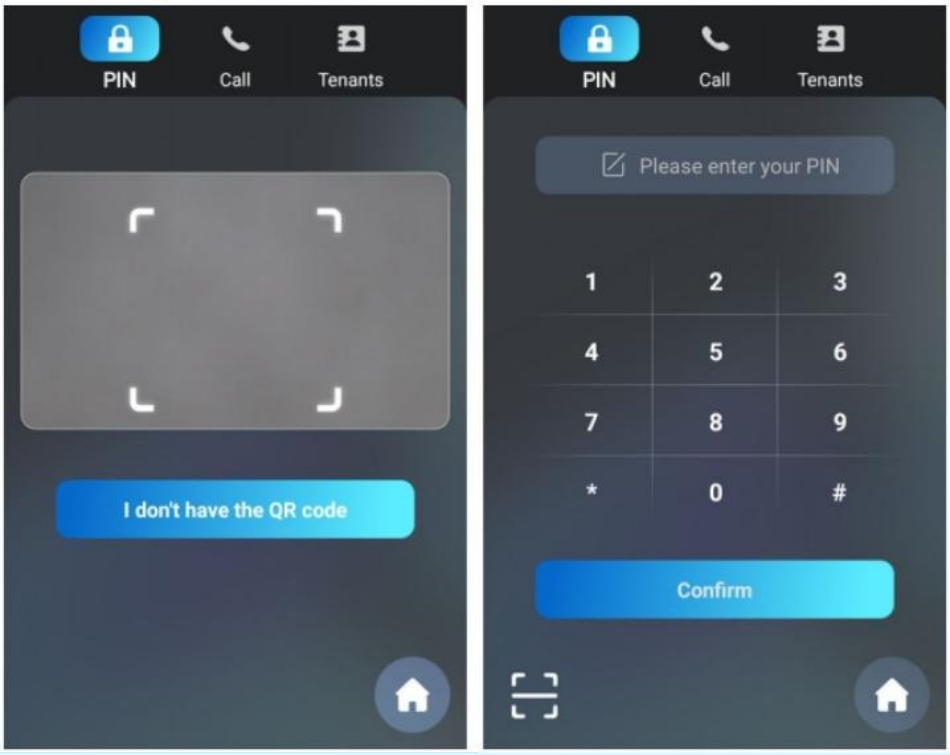
Configure Private PIN Access Mode

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

Navigate to the web **Access Control > PIN Setting > Private PIN** interface.



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



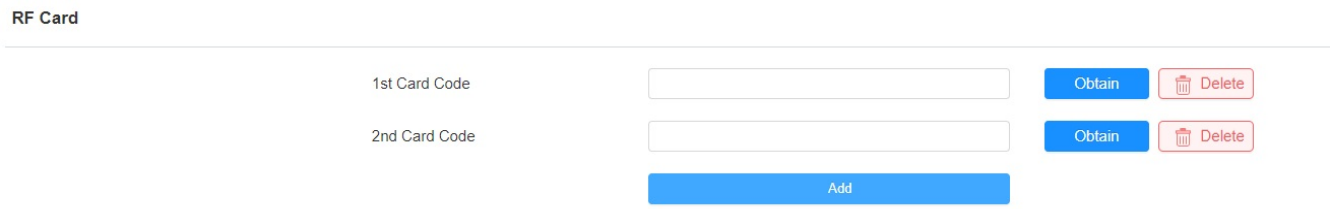
Note

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

Configure RF Card for Door Unlock

Configure RF Card on the Web Interface

Navigate to the web **Directory > User > +Add > RF Card** interface.



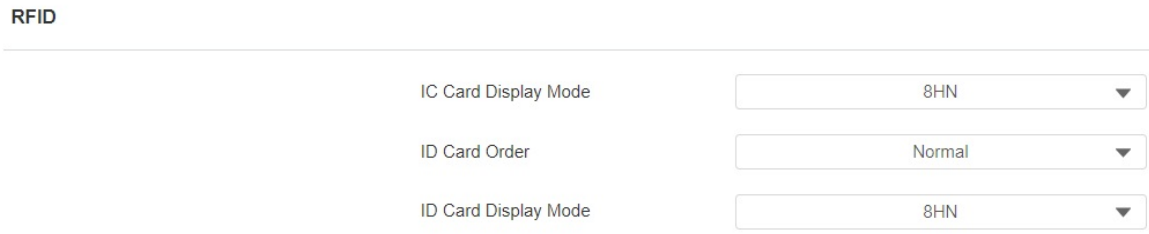
Note

RF cards with 13.56 MHz and 125 KHz can be applied to the door phone for door access.

Configure RF Card Code Format

To integrate the RF card door access with the third-party intercom system, you need to match the RF card code format with the one used by the third-party system.

To configure it on the web **Access Control > Card Setting** interface.

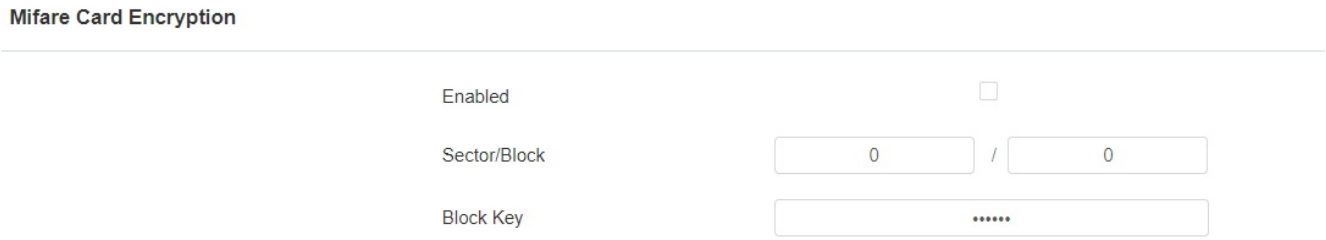


- **IC/ID Card Display Mode**: select the card format for the **IC/ID Card** for the door access among **8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 6H3D5D-R(W26),** and **8HR10D**. The card code format is 8HN by default.

Mifare Card Encryption

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

Navigate to the web **Access Control > Card setting > Mifare Card Encryption** interface.



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

Configure Facial Recognition for Door Unlock

Upload Face Data on the Web Interface

You can upload the face data to the device on the web interface.

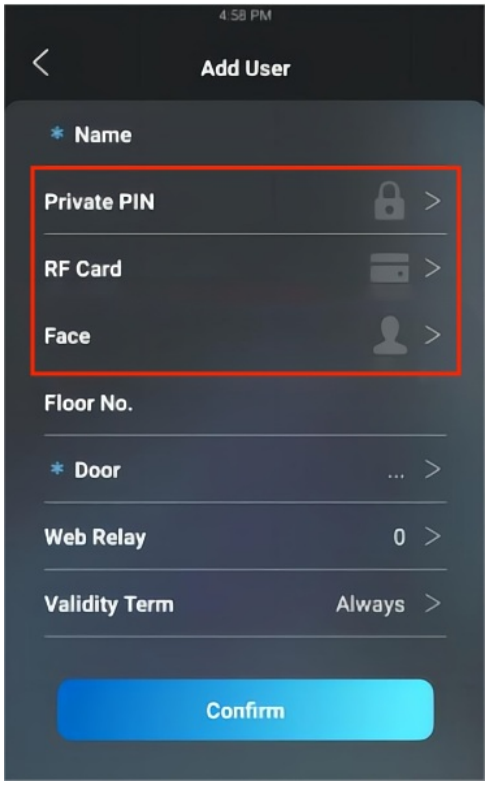
Navigate to the web **Directory > User > +Add > Face** interface.

Note

Max File Size: 2M, Format: .jpg/.png/.bmp

Add Users on the Device

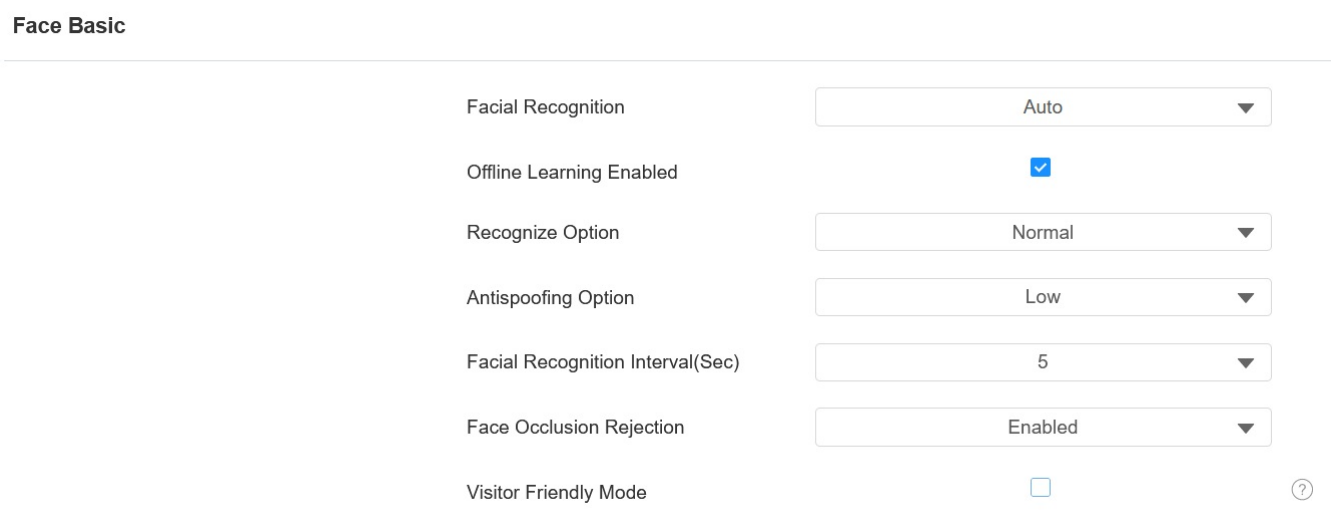
Users can also be added on the device **User** screen.



Configure Facial Recognition on the Web Interface

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

Navigate to the web **Access Control > Face Setting** interface.

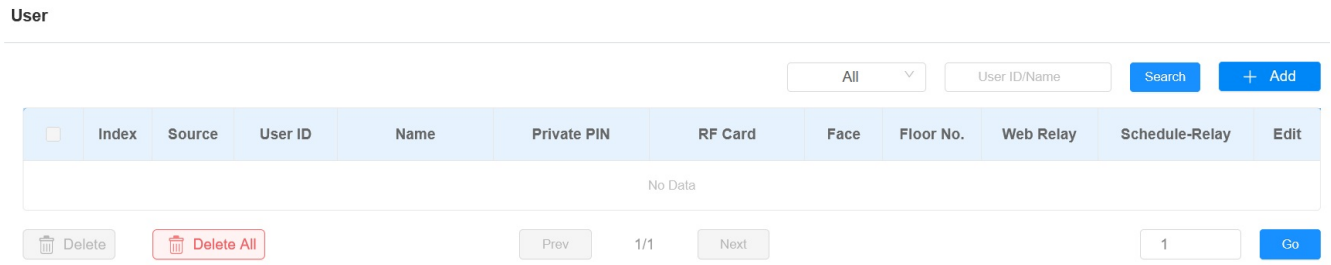


- **Offline Learning Enabled**: when enabled, it improves the device's recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occur to your face. Facial recognition accuracy improves as the number of facial recognition increases.

- **Recognize Option**: select the facial recognition accuracy level among **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 **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(Sec)**: select a time interval between every two facial recognitions from 1-8 seconds. For example, if you select 5, then users have to wait for 5 seconds before they are allowed to perform the facial recognition again.
- **Face Occlusion Rejection**: when enabled, the device will detect whether the user is wearing a mask.
- **Visitor Friendly Mode**: when enabled, no visual or auditory prompt will be given when recognition fails.

Edit the User-specific Door Access Data

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



Import and Export User Data of Access Control

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

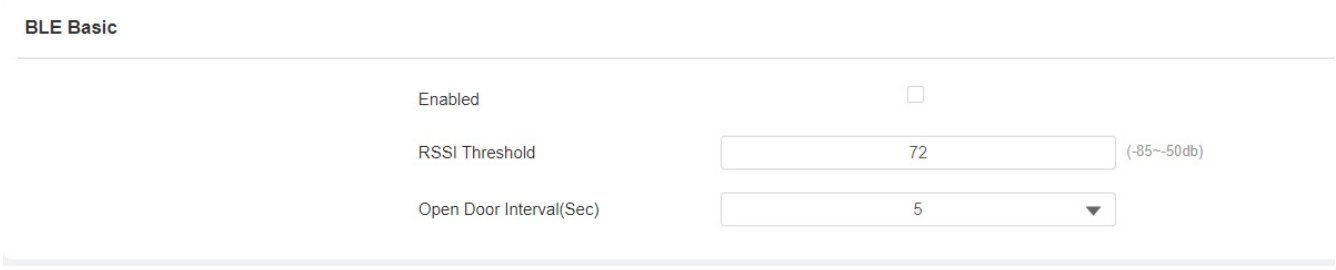
Navigate to the web **Directory > User > Import/Export User** interface.

> **Note**
>
> The imported/exported file is in TGZ format.

Configure Bluetooth for Door Unlock

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

Navigate to the web **Access Control > BLE** interface.

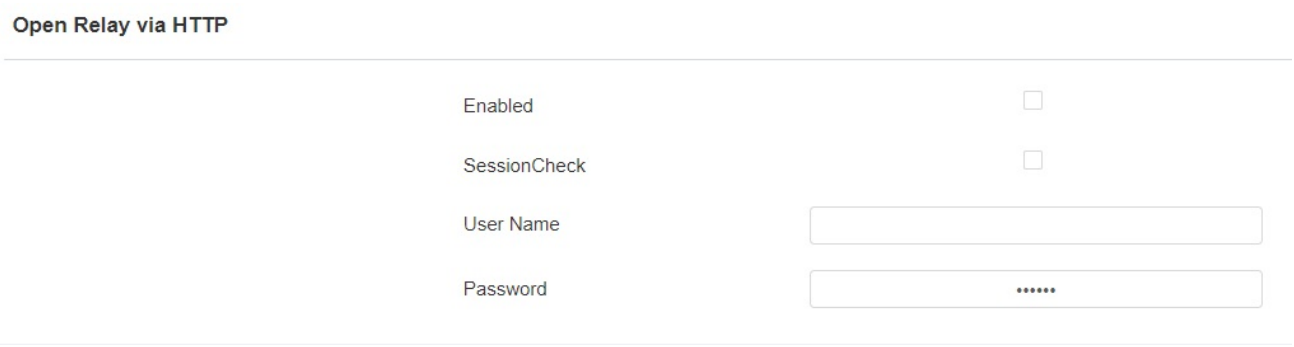


- **RSSI Threshold**: select the signal receiving strength from -85~-50db in absolute terms, The higher the value it is, the greater the strength it has. The default value is 72db in absolute terms.
- **Open Door Interval (Sec)**: select the time interval between every two Bluetooth door accesses.

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.

Navigate to the web **Access Control > Relay > Open Relay via HTTP** interface.



- **Session Check**: this feature is for some network security limitations, if you enable it, the door may not be unlocked in this way.
- **User Name**: enter the user name of the device web interface, for example, **admin**.
- **Password**: enter the password for the HTTP command, for example, **12345**.

Please refer to the following example:

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

Note

DoorNum in the HTTP command above refers to the relay number #1 to be triggered for the door access.
The device with high security mode enabled only supports the new HTTP formats. Please refer to **Security**.

Unlock by QR Code

You can use a QR code to unlock the door with the door phone. This method requires the Akuvox SmartPlus cloud service. You have to activate this feature before using it.

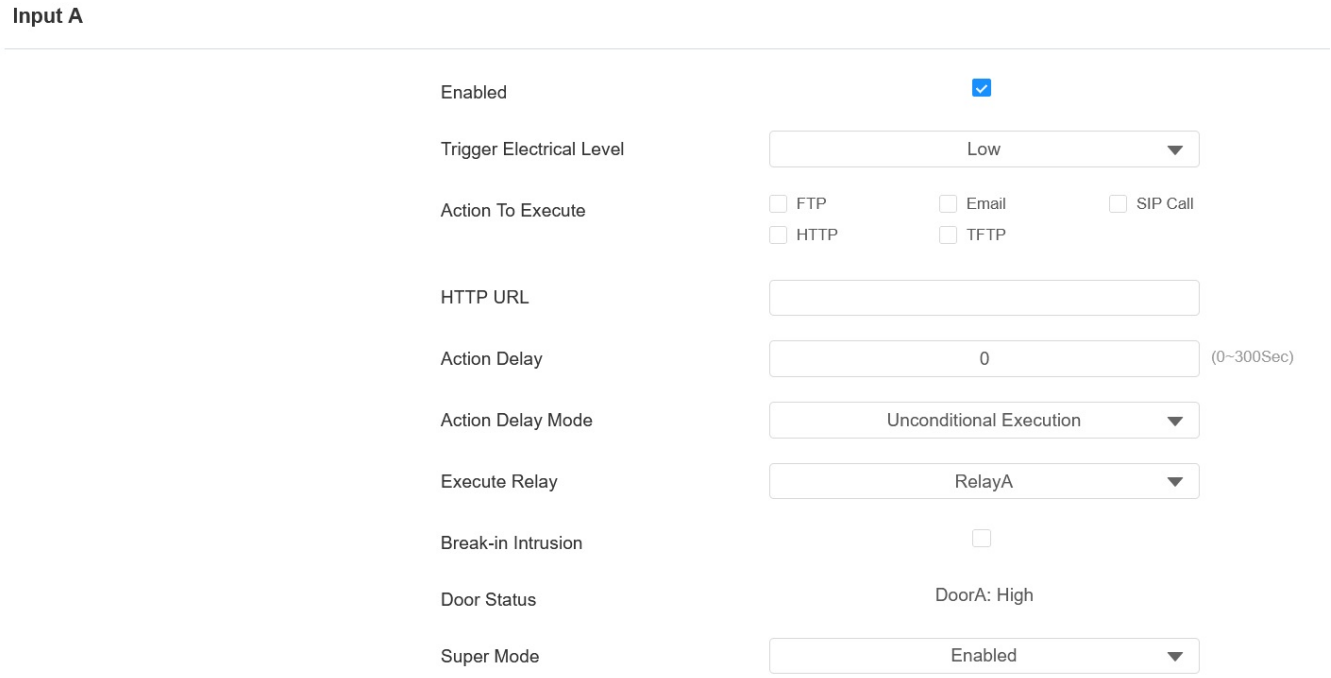
Navigate to the web **Access Control > Relay > Open Relay via QR Code** interface.

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

Configure Exit Button for Door Unlock

When users need to open the door from inside by pressing the Exit button, you need to set up the Input terminal that matches the Exit button to activate the relay for the door access.

Navigate to the web **Access Control > Input > Input** interface.



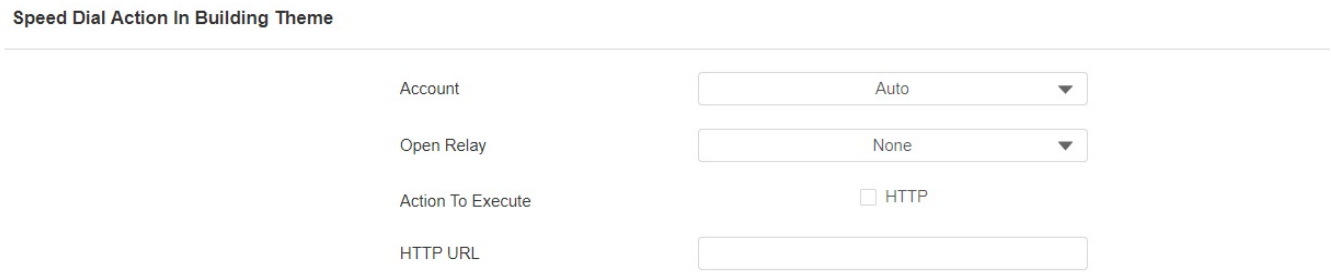
- **Trigger Electrical Level**: select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action to Execute**: select the method to carry out the action among **FTP, Email, SIP Call, HTTP,** and **TFTP.**
- **HTTP URL**: enter the 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 seconds after you press the button(input is triggered).
- **Action Delay Mode**: if you select **Unconditional Execution**, the 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.
- **Break-in Intrusion**: enable it to trigger the alarm when the door is opened abnormally.

- **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.

Configure the Reception Tab for Door Unlock

The Reception button is a tab on the home screen that allows residents and visitors to contact the receptionist or the security guard of the building. They can tap this button to ask for help or access to the door.

Navigate to the web **Setting > Key/Display > Speed Dial Action In Building Theme** interface.

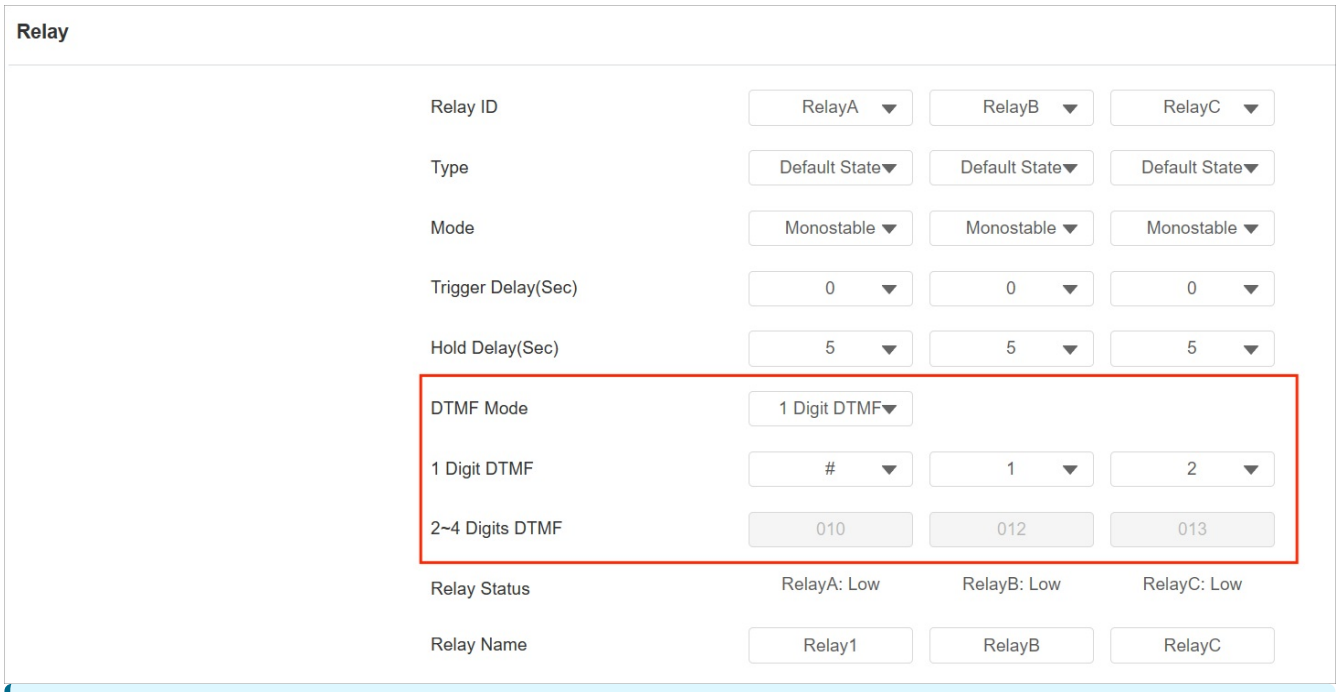


- **Open Relay**: select the relay(s) to be triggered by pressing the Reception Icon.
- **Action To Execute**: tick the check box to enable the HTTP option.
- **HTTP URL**: enter the URL command to be sent for door access. For example, http:// 192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Unlock by DTMF Code

Dual-tone multi-frequency signaling(**DTMF**) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad, or tapping the unlock tab with the DTMF code on the screen.

Navigate to the web **Access Control > Relay** interface.



Note

- Please refer to **Configure DTMF Data Transmission** in Call Setting for the specific DTMF code setting.
- Intercom devices involved must be consistent in the DTMF type. Otherwise, the DTMF code cannot be applied.

Monitor and Image

MJPEG and RTSP are the primary monitoring stream types discussed in this chapter.

MJPEG, or Motion JPEG, is a video compression format that uses JPEG images for each video frame. Akuvox devices display live streams on the web interface and capture monitoring screenshots in MJPEG format. Settings related to MJPEG determine video quality and the on/off status of the live stream function.

RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

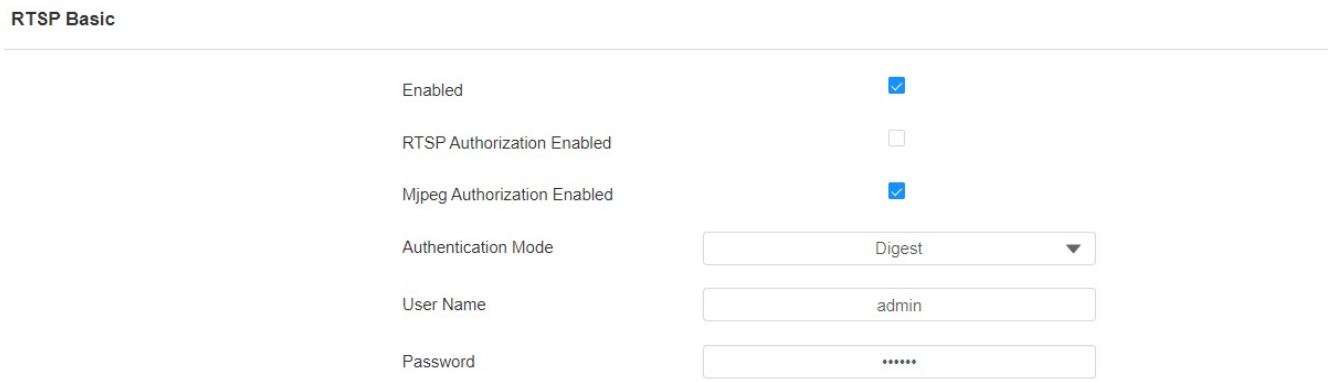
ONVIF is an Open Network Video Interface Forum. It enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

RTSP Stream Monitoring

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

RTSP Basic Setting

Navigate to the web **Surveillance > RTSP > RTSP Basic** interface.

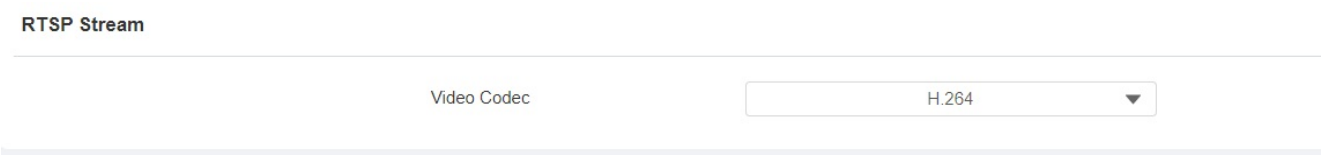


- **RTSP Authorization Enabled**: enable the RTSP authorization. If you enable the RTSP Authorization, you are required to select the RTSP Authentication Mode and enter the RTSP Username, and RTSP Password on the intercom device such as an indoor monitor for authorization.
- **Authentication Mode**: select the RTSP authentication type between Basic and Digest. Basic is the default authentication type.

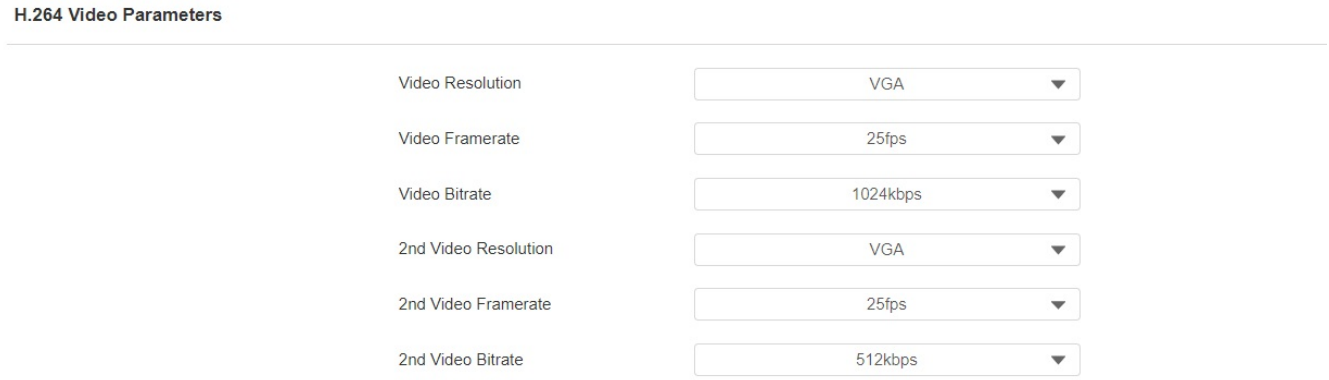
RTSP Stream Setting

The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

Navigate to 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.

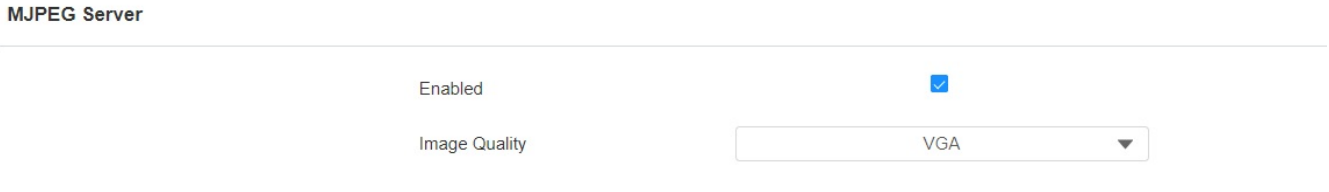


- **Video Resolution**: select video resolutions among **QCIF, QVGA, CIF, VGA, 4CIF, 720P**, and **1080P**. The default video resolution is **VGA** and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than **VGA**.
- **Video Framerate**: **25fps** is the video frame rate by default.
- **Video Bitrate**: select video bitrate among **128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps,** and **4096 kbps** according to the network environment. The default video bitrate is **1024 kbps**.
- **2nd Video Resolution**: select the video resolution for the second video stream channel. The default video solution is **VGA**.
- **2nd Video Framerate**: select the video framerate for the second video stream channel. **25fps** is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate**: select the video bitrate for the second video stream channel. While the second video stream channel is **512 kbps** by default.

MJPEG Image Capturing

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

Navigate to the web **Surveillance > MJPEG** interface.



- **Image Quality**: select the quality for the image capturing among **QCIF, QVGA, CIF, VGA, 4CIF, 720P**, and **1080P**. After the MJPEG service is enabled, you can capture the image from the door phone using the following three types of URL format:
    - http:// device ip:8080/picture.cgi

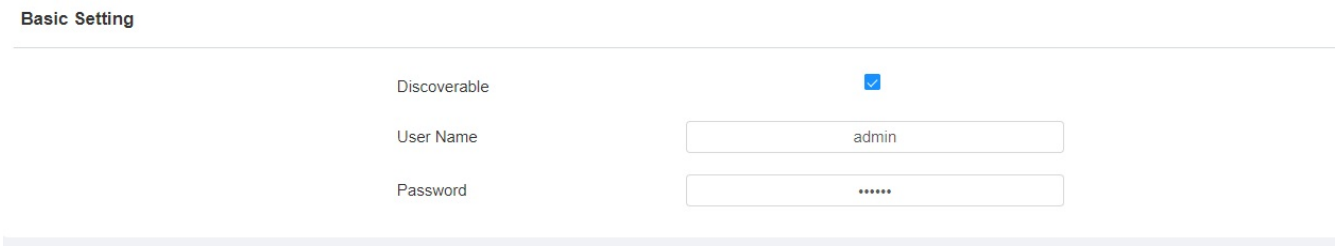
- http://device ip:8080/picture.jpg
- http://device ip:8080/jpeg.cgi

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

ONVIF

You can access the real-time video from the device's camera using the Akuvox indoor monitor or other third-party devices like Network Video Recorder(**NVR**). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

Navigate to the web **Surveillance > ONVIF** interface.



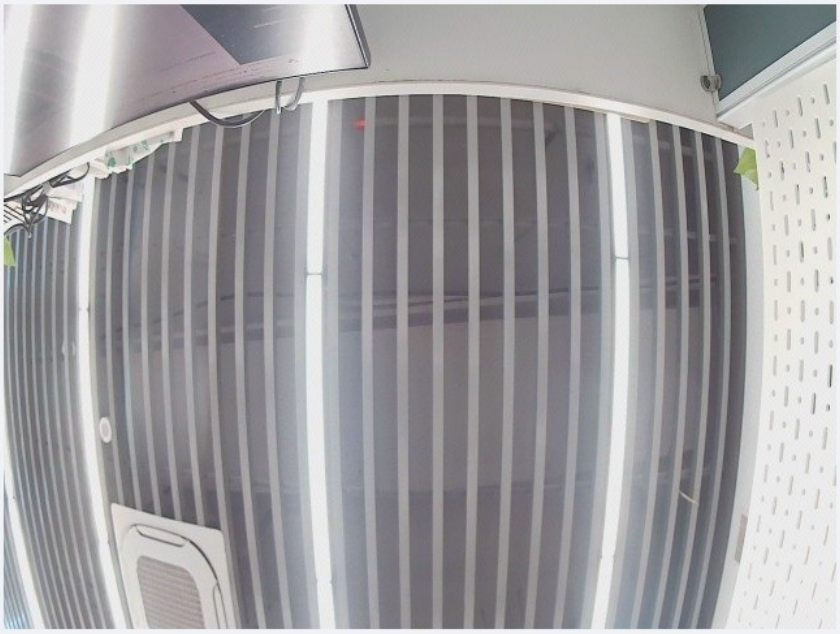
- **Discoverable**: when enabled, the video from the door phone camera can be searched by other devices.
- **User Name**: customize the user's name. The user's name is **admin** by default.
- **Password**: customize the password. The password is **admin** by default.

After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream. For example: http://doorphone IP address:80/onvif/device_service

Live Stream

There are two ways to check the real-time video from the device. One is to go to the device web interface and view the video there. The other is to enter the correct URL on the web browser and access the video directly.

To view the real-time video on the web **Surveillance > Live Stream** interface.



Security

Tamper Alarm Setting

The tamper alarm function prevents anyone from removing the devices without permission. It does this by setting off the tamper alarm and making calls to a designated location when the device detects a change in its gravity value from the original one.

Configure Tamper Alarm on the Web Interface

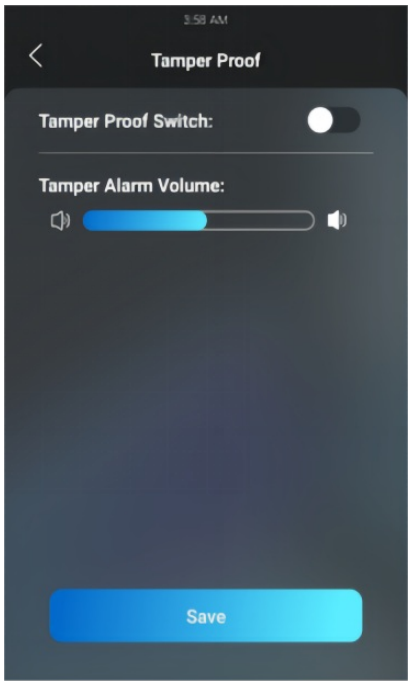
You can customize the tamper alarm and adjust sensor settings on the web interface.

Navigate to the web **System > Security > Tamper Alarm** interface.

Configure Tamper Alarm on the Device

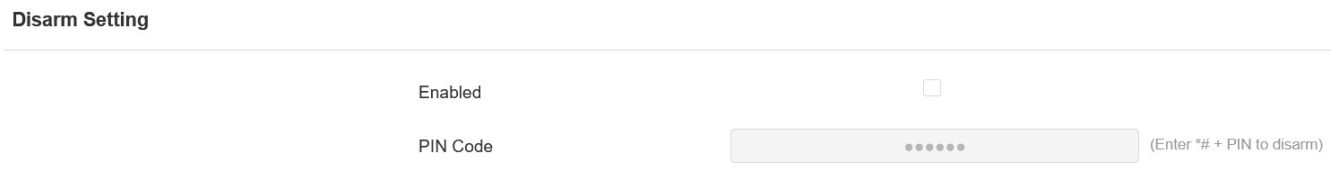
The tamper alarm and gravity sensor can be easily set up on the door phone.

Navigate to the device **Setting > Security > Tamper Alarm** screen.



Disarm Setting

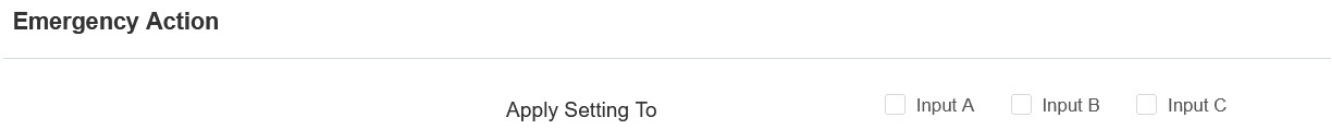
You can set the disarm code on the device **System > Security > Disarm Setting** interface.



Emergency Action

You can keep the door open when an emergency happens.

Navigate to the web **System > Security > Emergency Action** interface.

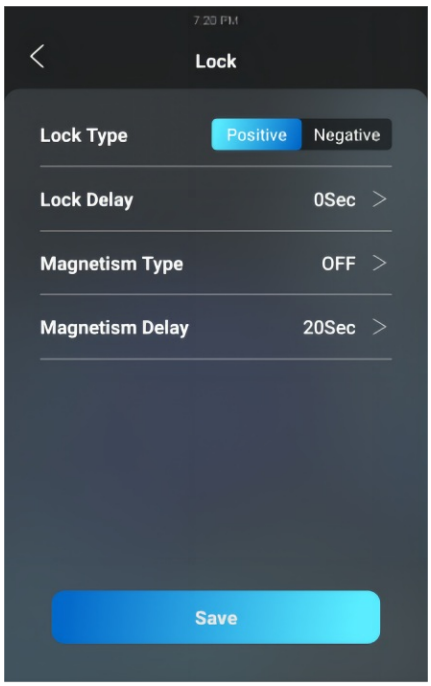


> **Note**
>
> This features works with SmartPlus Cloud.

Lock Security

The door phone can work with other door locks and sensors to keep the lock secure. It will sound the alarm to alert users if the door sensor finds the door open or not fully closed.

On the device, go to **Security > Lock** for the setting.



- **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 users 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.

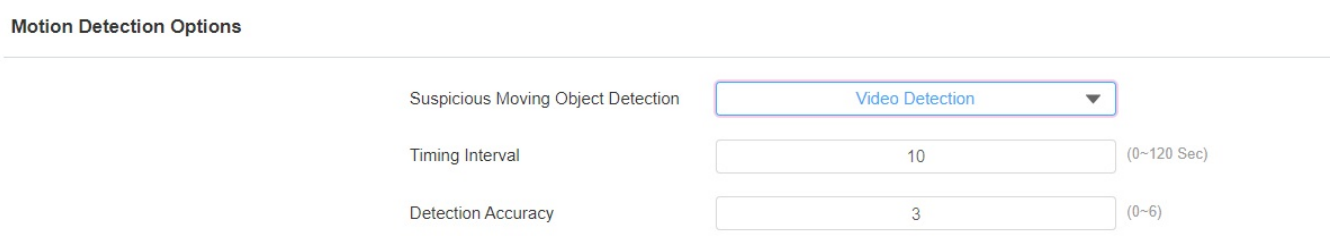
Motion Detection

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

Configure Motion Detection on the Web Interface

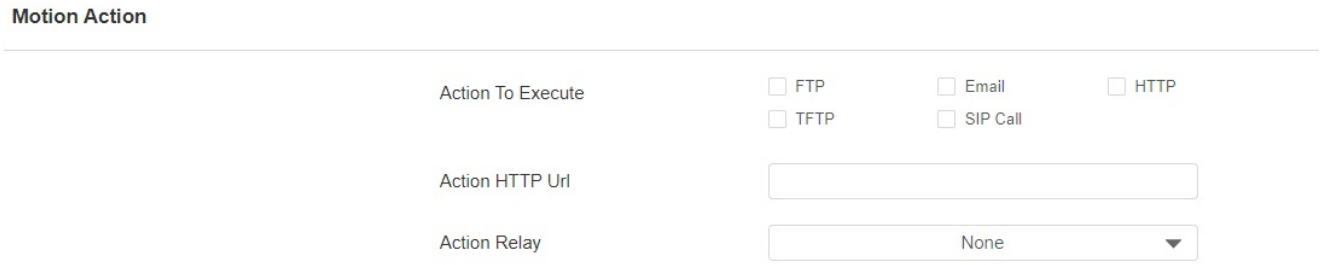
You can adjust various motion detection settings on the device web interface, such as the time interval, the sensitivity level, the notification method when motion is detected, and more.

Navigate to the web **Surveillance > Motion > Motion Detection Options** interface.



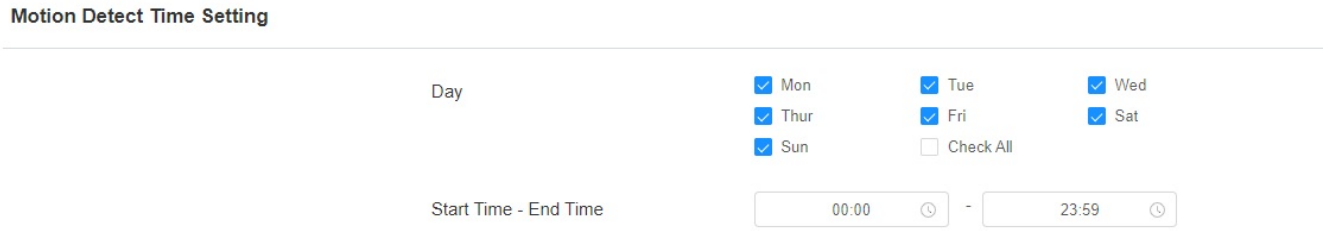
- **Suspicious Moving Object Detection**: select from **Video Detection, IR Detection**, and **Disabled**. IR detection is based on sensing infrared radiation emitted or reflected by objects, while video detection focuses on analyzing visual information captured through cameras.
- **Time Interval**: 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.
- **Detection Accuracy**: set the detection accuracy for the detection sensitivity. The higher the value, the greater the sensitivity. The default detection accuracy value is **2**.

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



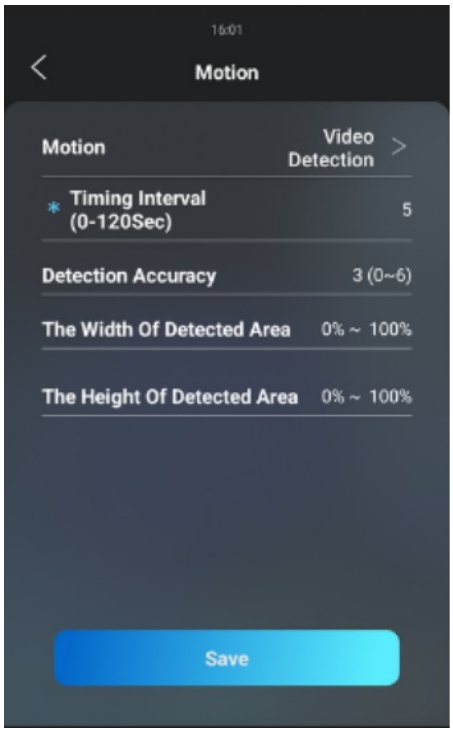
- **Action To execute**: select the method to carry out the action: FTP, Email, HTTP, TFTP, and SIP Call. For example, if you select **Email**, then an Email will be sent to you after the motion detection alarm is triggered.
- **Action HTTP URL**: enter the HTTP command that will be sent to a third-party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

Scroll down and you can also set the motion detection schedule.



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.

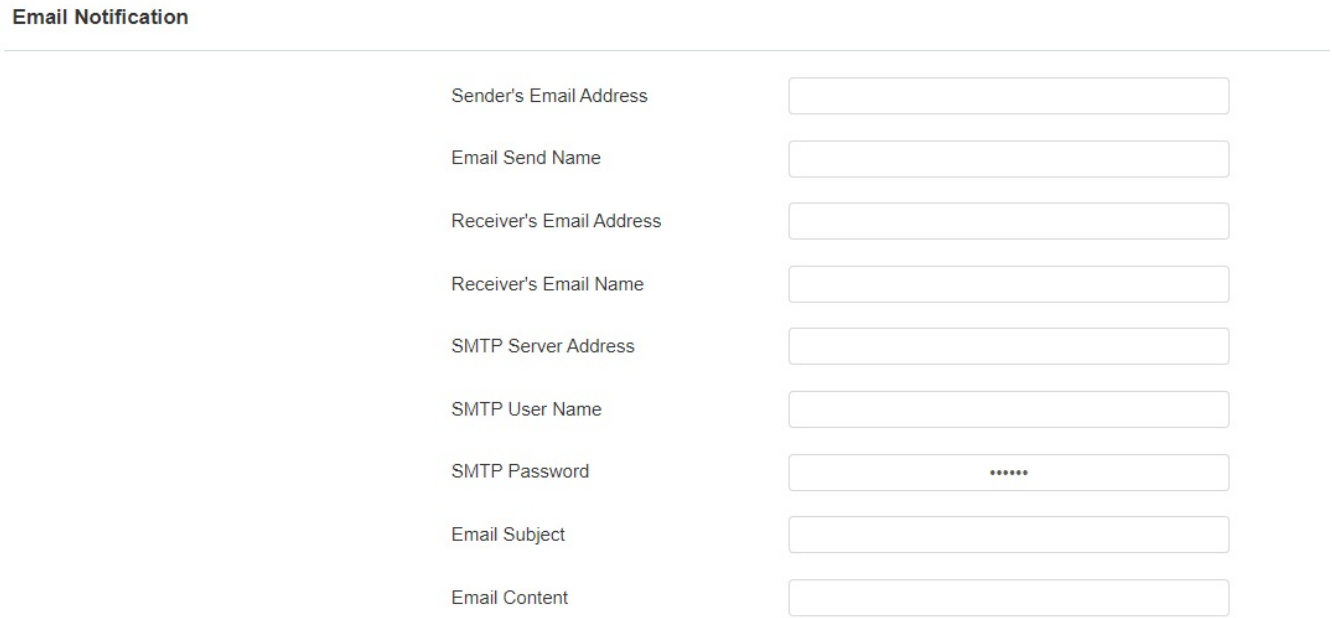


Security Notification Setting

Email Notification Setting

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

Navigate to the web **Setting > Action > Email Notification** interface.



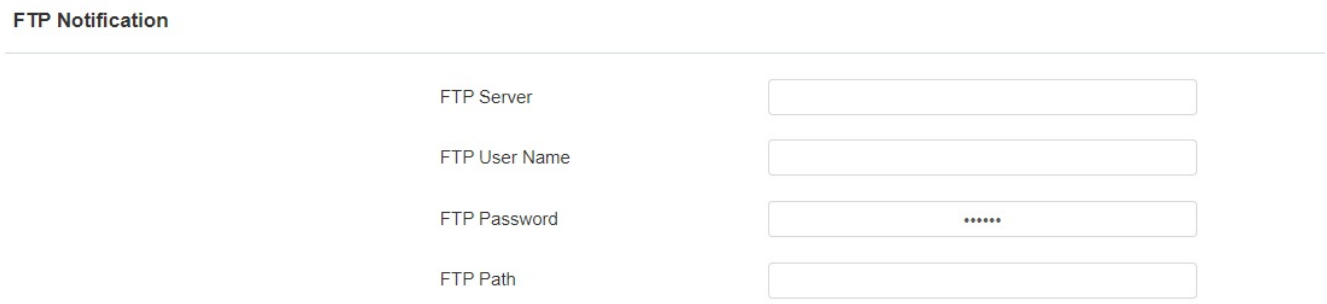
- **SMTP Server Address**: enter the SMTP server address of the sender.
- **Port**: enter the port number from which the email is sent out.
- **SMTP User Name**: enter the SMTP user name, which is usually the same as the sender's email address.

- **SMTP Password**: configure the password of the SMTP service, which is the same as the sender's email address.

FTP Notification Setting

To get notifications through FTP server, you need to set up the FTP settings. The door phone will upload a screenshot to the specified FTP folder if it senses any unusual motion.

Navigate to the web **Setting > Action > FTP Notification** interface.

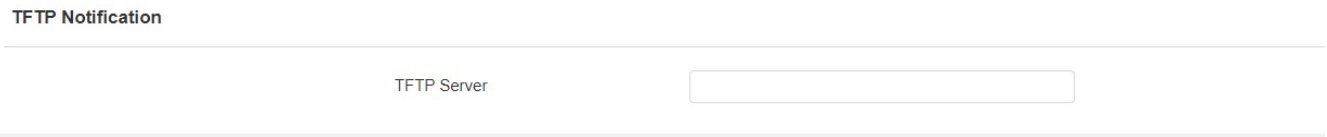


- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP Path**: enter the folder name you created in the FTP server.

TFTP Notification Setting

To receive security notifications via TFTP server, you need to enter the TFTP server address.

Navigate to the web **Setting > Action > TFTP Notification** interface.



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

Action URL

You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

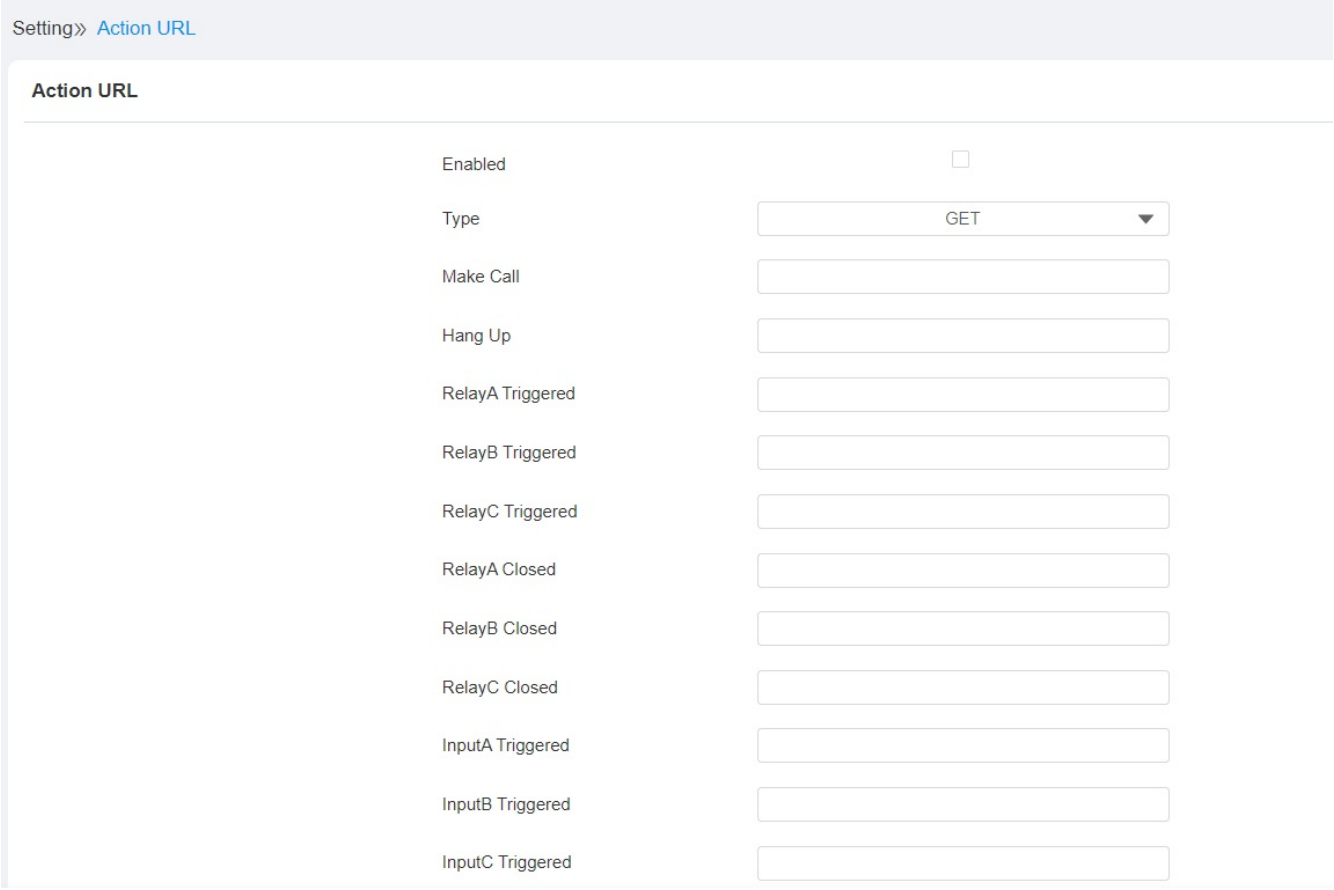
No	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/ Callnumber=$remote
2	Hang Up	$remote	Http://server ip/ Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Relay Closed	$relay1status	Http://server ip/ relayclose=$relay1status
5	Input 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 Card Entered	$card_sn	Http://server ip/ invalidcard=$card_sn
11	Tamper Alarm Triggered	$alarm status	Http://server ip/tampertrigger=$alarm status

For example: http://192.168.16.118/help.xml? mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

Navigate to the web **Setting > Actions URL** interface.

Note:

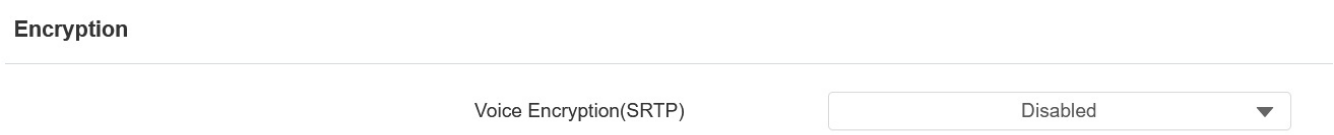
Action URLs and formats are provided by third-party manufacturers. Akuvox door phone only sends the URL to third-party devices.



Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the Real-time Transport Protocol (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance, and replay protection.

Navigate to the web **Account > Advanced > Encryption** interface.



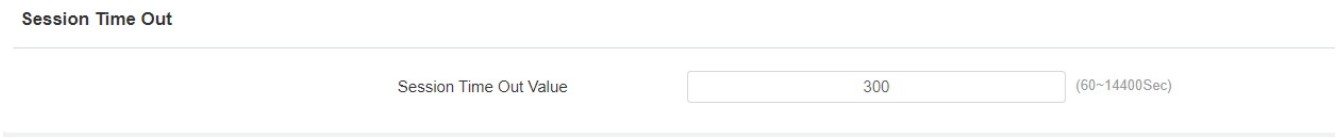
Voice Encryption(SRTP): select the encryption mode. If you select to disable it, the call will not be encrypted.

- **Compulsory:** all audio signals (technically speaking, it is RTP streams) will be encrypted to improve security.
- **Optional**: encrypt voice from the called party, if the called party also enables SRTP, the voice signals will also be encrypted.

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.

Navigate to the web **System > Security > Session Time Out** interface.



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

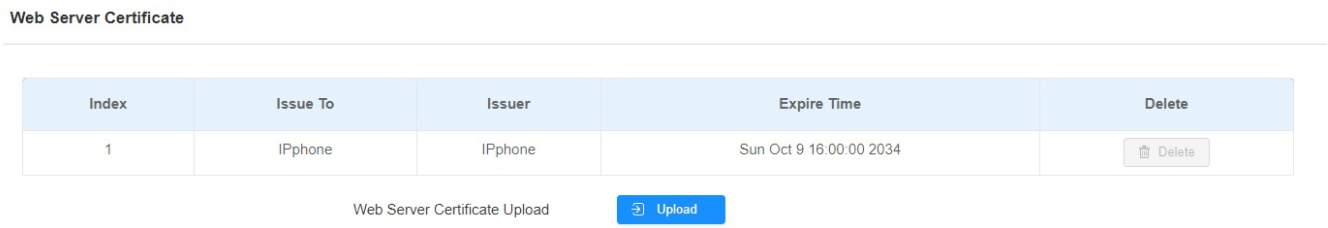
Client Certificate Setting

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

Web Server Certificate

It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

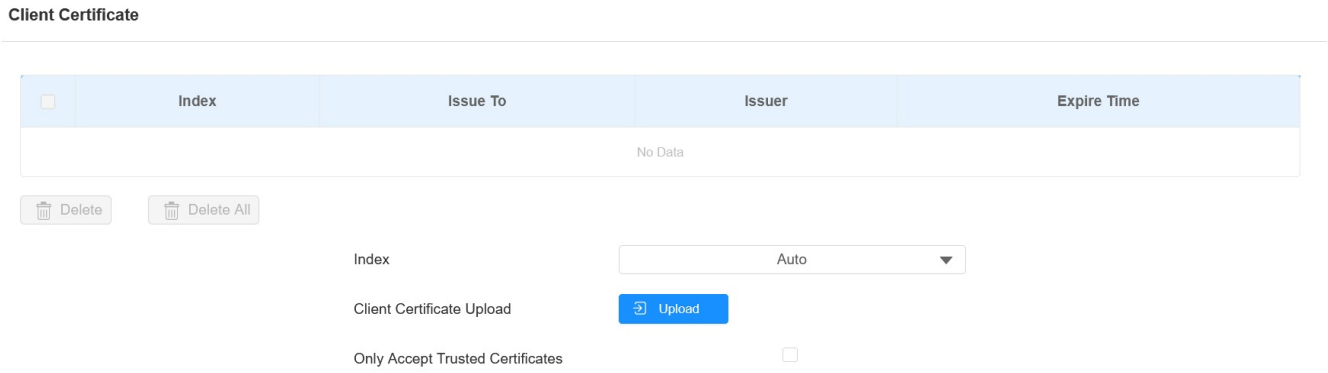
To upload a web server certificate on the web **System > Certificate > Web Server Certificate** interface.



Client Certificate

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

To upload and configure client certificates on the web **System > Certificate > Web Server Certificate** interface.



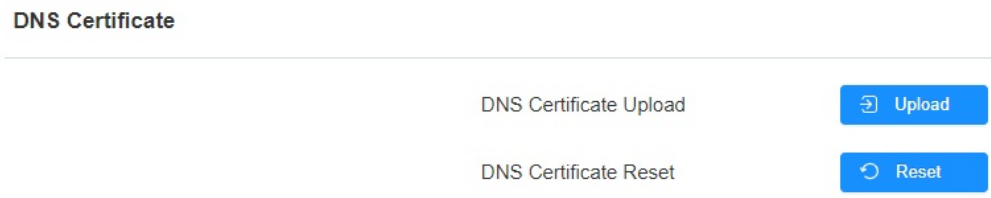
- **Index**: select the desired value from the drop-down list of Index. If you select **Auto** value, the uploaded certificate will be displayed in numeric order. If you select the value from **1 to 10**, the uploaded certificate will be displayed according to the value that the user selected.
- **Client Certificate Upload**: locate and upload the desired certificate (*.pem only).

- **Only Accept Trusted Certificates**: when enabled, as long as the authentication is successful, the phone will verify the server certificate based on the client certificate list. When disabled, the phone will not verify the server certificate no matter whether the certificate is valid or not.

Upload TLS Certificate for SIP Account Registration

Before applying for a SIP account from a SIP or a DNS server using the TLS protocol, you'll need to upload a TLS certificate. This certificate is essential for server authentication.

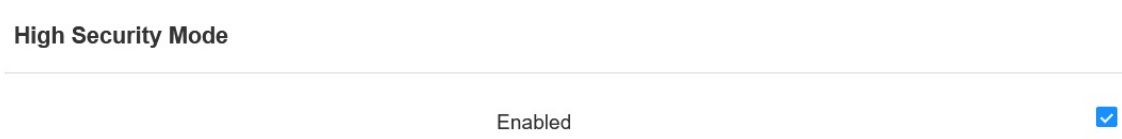
To upload the TLS certificate, go to **System > Certificate > DNS Certificate** interface.



High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods, and more.

Navigate to the web **System > Security > High Security Mode** interface.



Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.

2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

3. The supported HTTP format for relay triggering varies depending on whether high secure mode is enabled or disabled.

If the mode is on, the device only accepts the new HTTP formats below for door opening.

- l http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- l http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is off, the device can use both the new formats above and the old format below:

- l http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

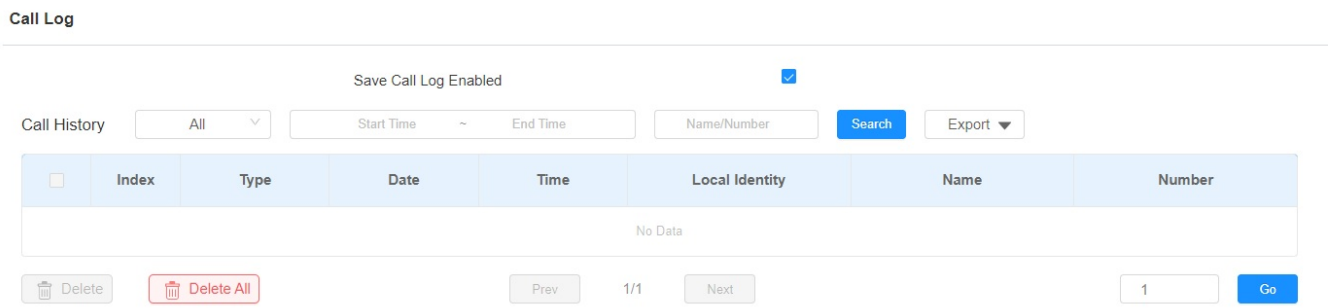
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

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

To check the call log on the web **Status > Call Log** interface. Call logs can be exported in CSV format.

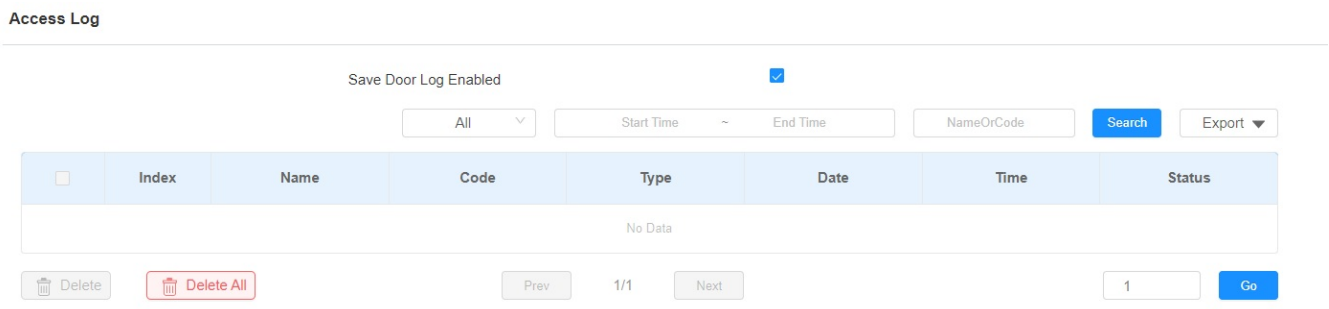


- **Call History**: select call history among **All**, **Dialed**, **Received**, and **Missed** for the specific type of call log to be displayed.
- **Start Time ~ End Time**: select the specific time of the call logs you want to search, check, or export.
- **Name/Number**: search the call log by the name, IP, or SIP number.

Door Logs

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

Navigate to the web **Status > Access Log** interface. Door logs can be exported in XML or CSV format.



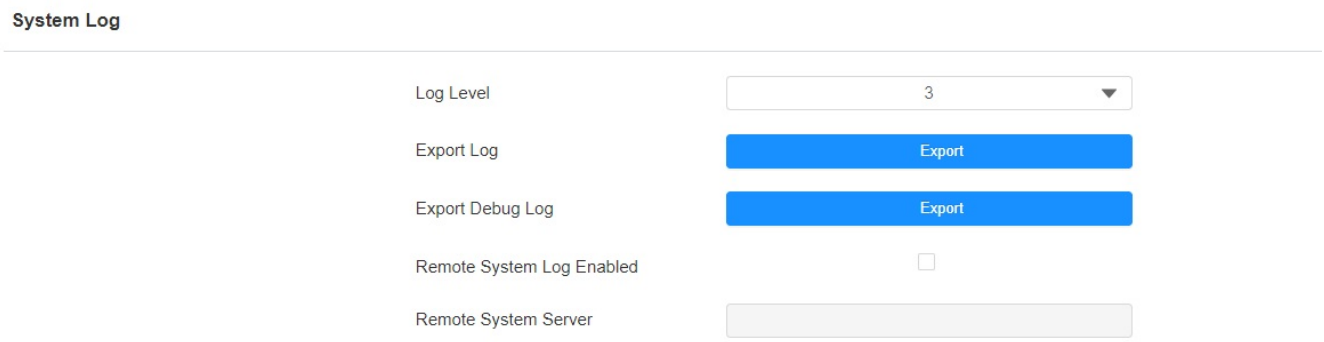
- **Status**: select between **Success** and **Failed** to search for successful or failed door accesses.
- **Name/Code**: search the door log by name or PIN code.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Navigate to the web **System > Maintenance > System Log interface** interface.

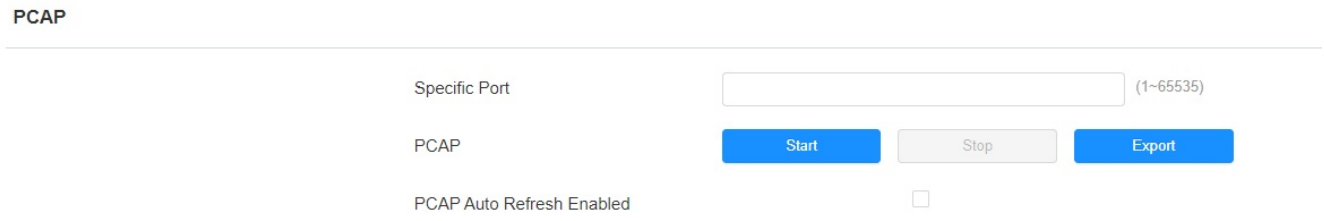


- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is **3**. The higher the level is, the more complete the log is.
- **Export Log**: click the **Export** tab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

PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

Navigate to the web **System > Maintenance > PCAP** interface.

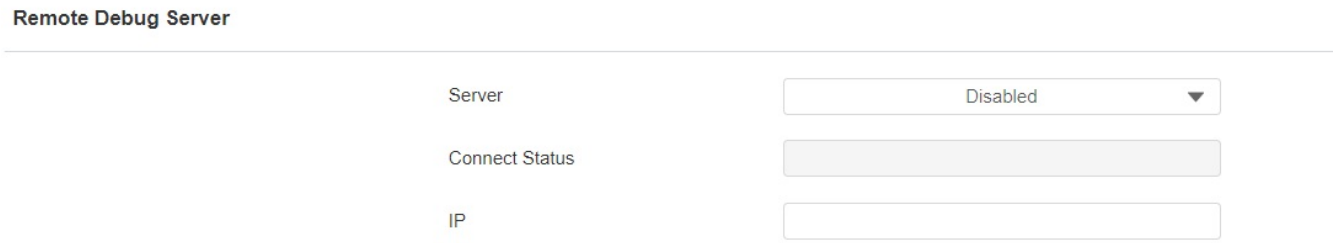


- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: when enabled, the PCAP will continue to capture data packets even after the data packets reach its 1M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1MB.

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.

Navigate to the web **System > Maintenance** interface.



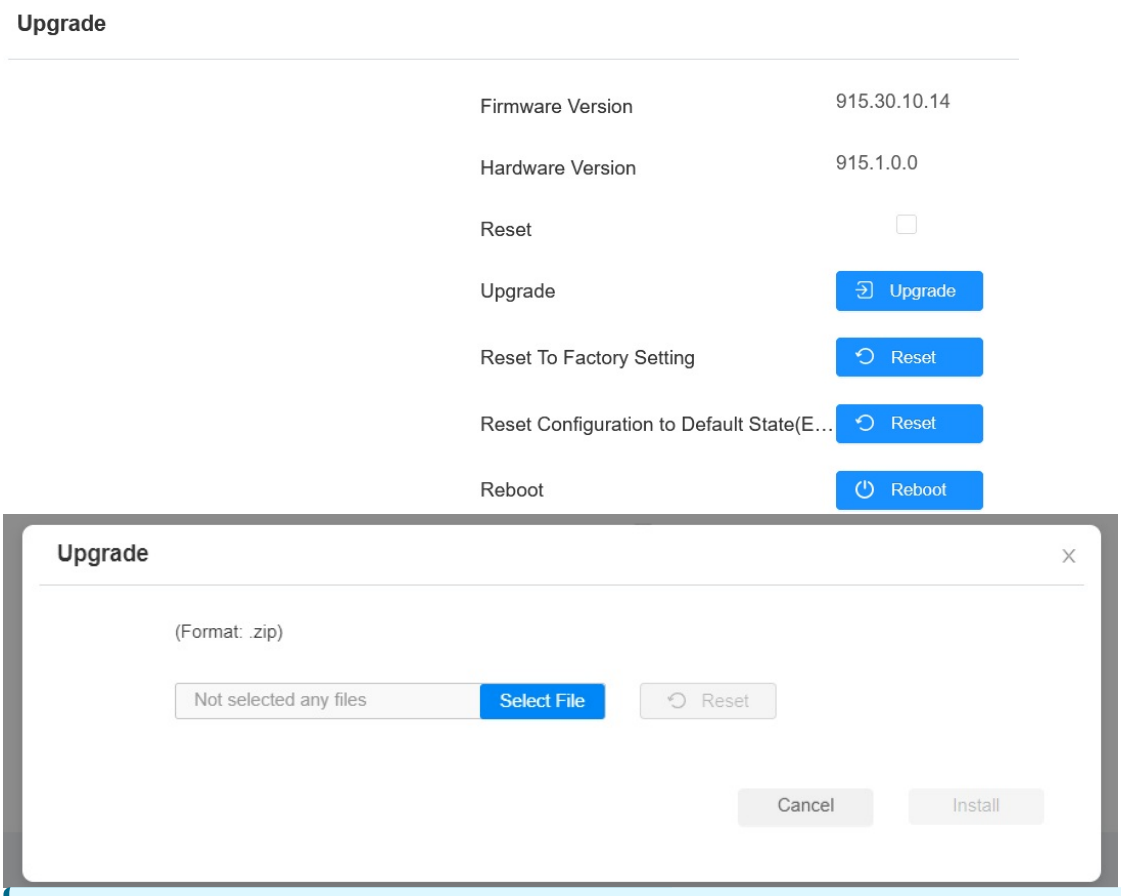
- **Connect Status**: display the remote debug server connection status.
- **IP**: enter the remote debug server IP address. Please ask the Akuvox technical team for the server IP address.

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

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Navigate to the web System > **Upgrade** > **Basic** interface.



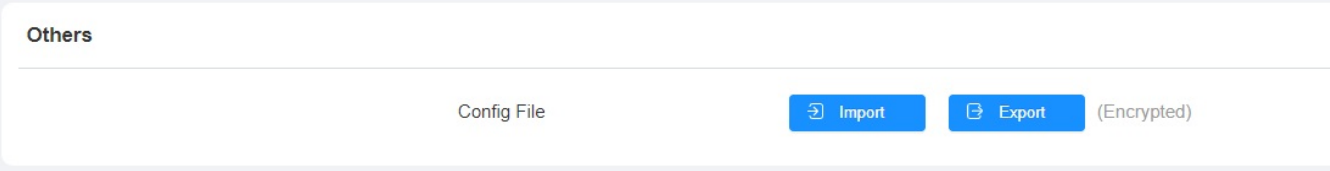
Note

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

Backup

You can import or export encrypted configuration files to your Local PC.

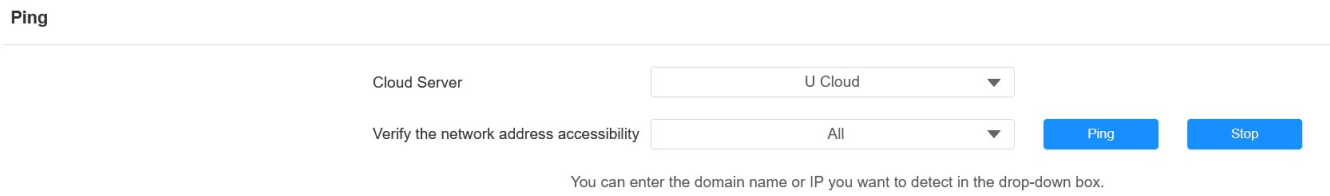
Navigate to the web **System > Maintenance > Others** interface.



Ping

The device allows you to verify the accessibility of the target server.

Navigate to the web **System > Maintenance > Ping** interface.



- **Cloud Server**: the server to be verified.
- **Verify the network address accessibility**: the service type.

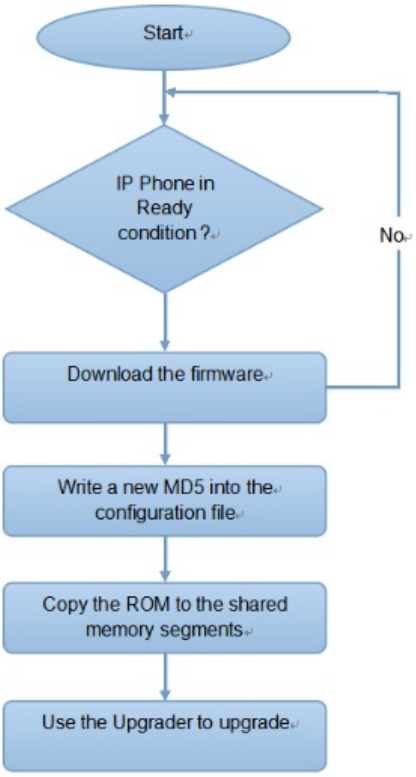
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

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

- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used for auto-provisioning on a specific

device, as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

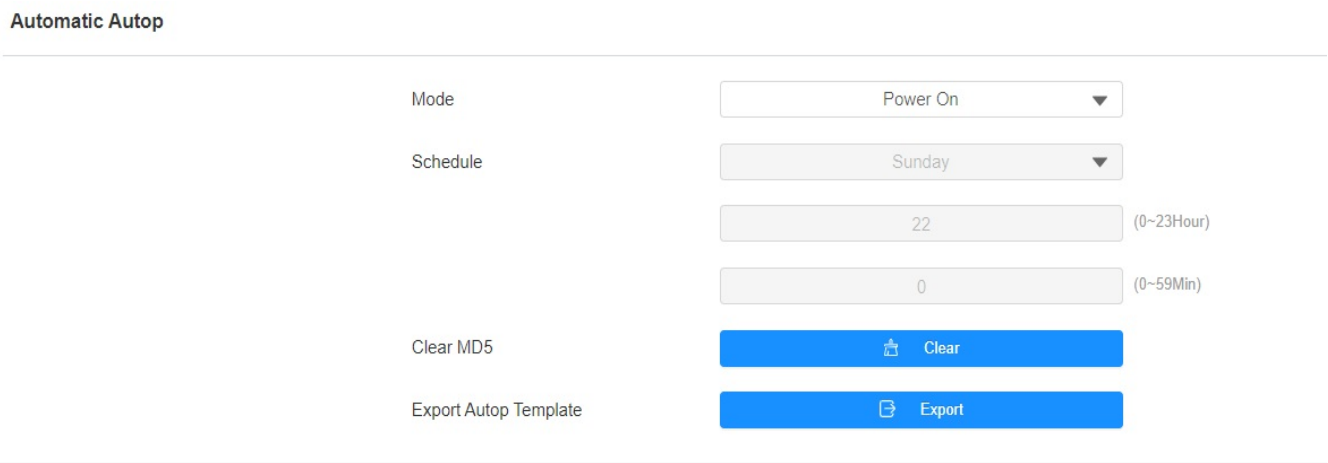
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

You may click here to see the detailed format and steps.

AutoP Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself according to the schedule.

Navigate to the web **System > Auto Provisioning > Automatic Autop** interface.



- **Mode**:

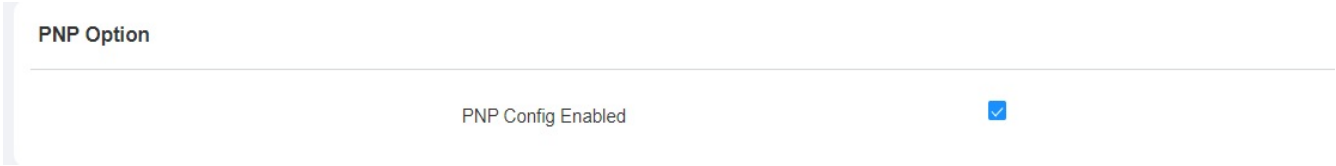
  - **Power on** allows the device to perform Autop every time it boots up.
  - **Repeatedly** allows the device to perform Autop according to the schedule that is set up.
  - **Power On + Repeatedly** combines **Power On** mode and **Repeatedly** mode which will enable the device to perform Autop every time it boots up or according to the schedule.
  - **Hourly Repeat** allows the device to perform Autop every hour.

- **Schedule**: when **Repeatedly** is selected, you can set up the Autop schedule.

PNP Configuration

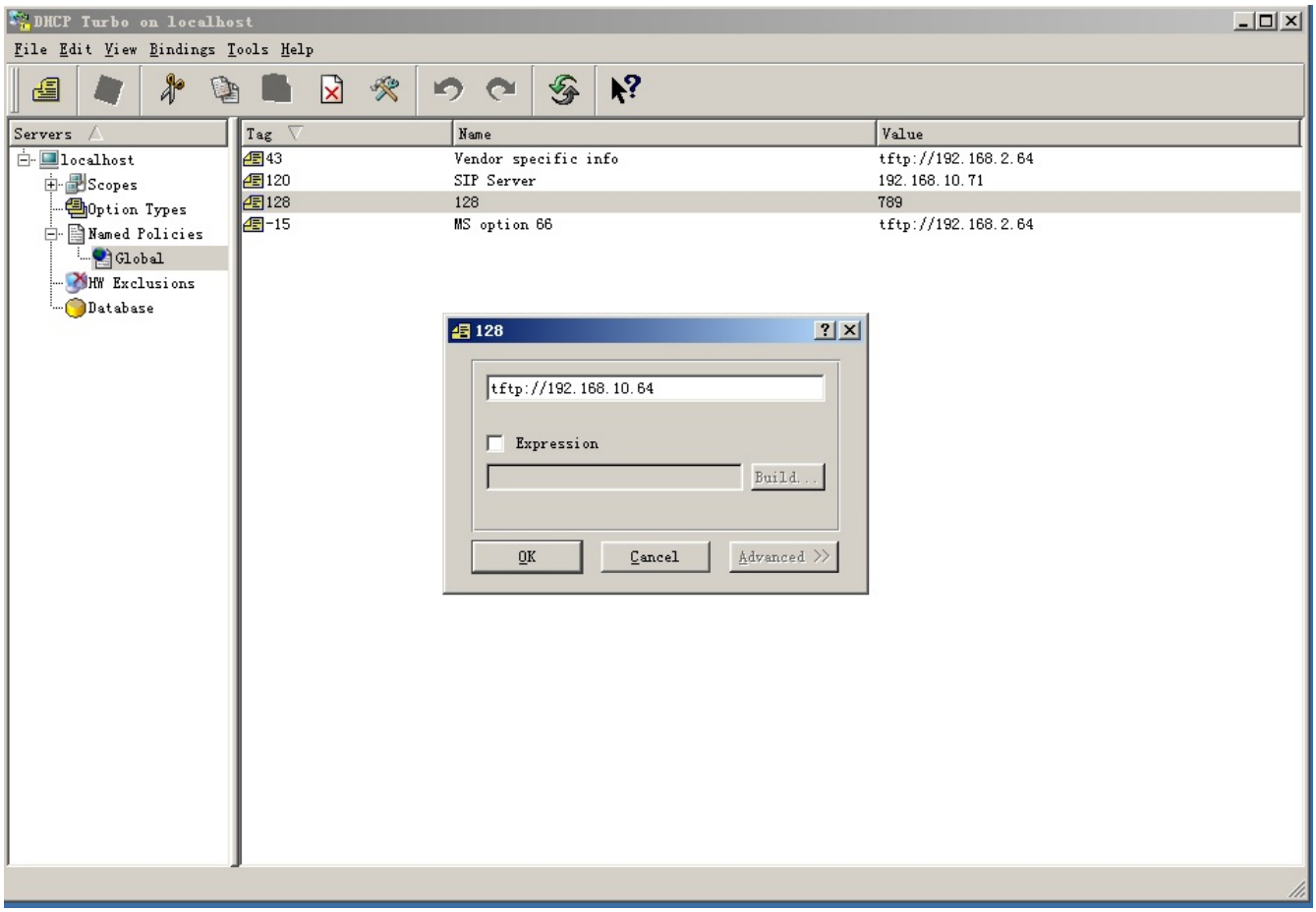
Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user.

Navigate to the web **System > Auto Provisioning > PNP Option** interface.



DHCP Provisioning Configuration

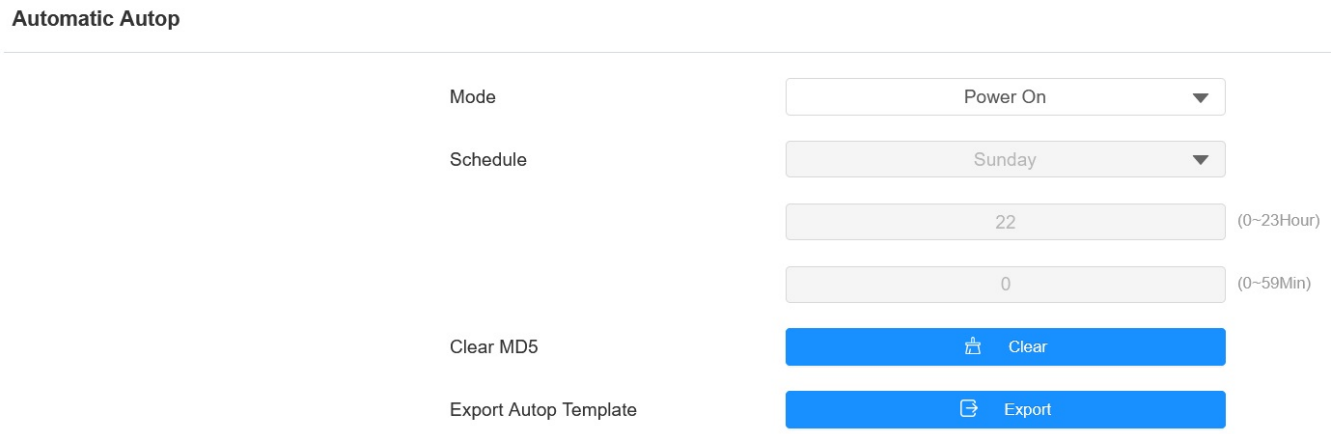
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option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



Note

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

To set up DHCP Autop with Power On mode and export Autop Template to edit the configuration. Navigate to the web **System > Auto Provisioning > Automatic Autop** interface.



Then set up the DHCP Option on **System > Auto Provisioning > DHCP Option** interface.

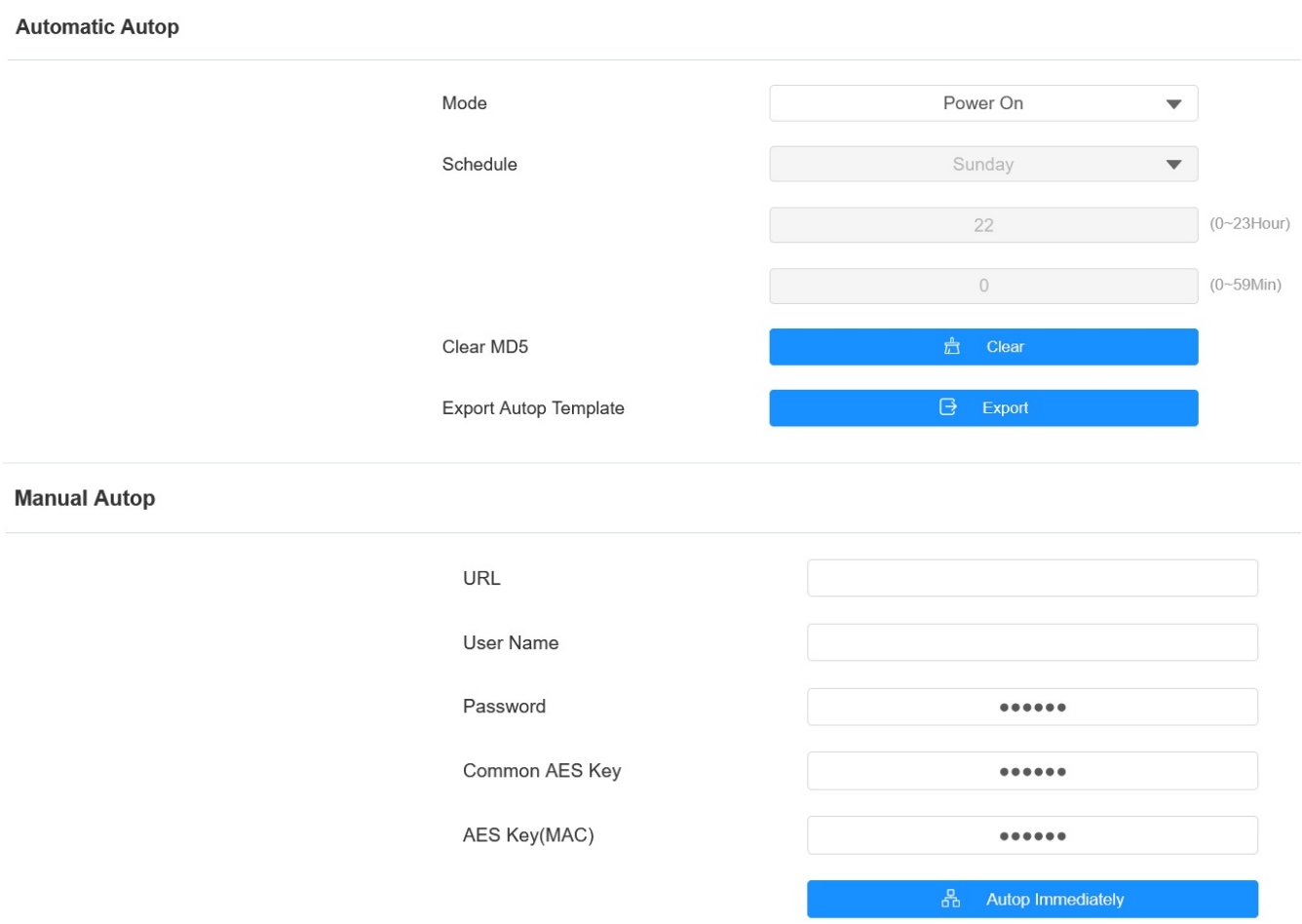
- **Custom Option**: enter the DHCP code that matches with corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL. 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 a 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 while the MAC-based configuration file for the specific device provisioning is with the format MAC Address of the device. cfg, for example, **0C110504AE5B.cfg**.

Static Provisioning Configuration

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

To download the Autop template on **System > Auto Provisioning > Automatic Autop**, and set the Autop server on **System > Auto Provisioning > Manual Autop** interface.



- **URL**: set up TFTP, HTTP, HTTPS, or FTP server addresses for the provisioning
- **User Name**: set up a user name if the server needs a user name to be accessed.
- **Password**: set up a password if the server needs a password to be accessed.
- **Common AES Key**: set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key(MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

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

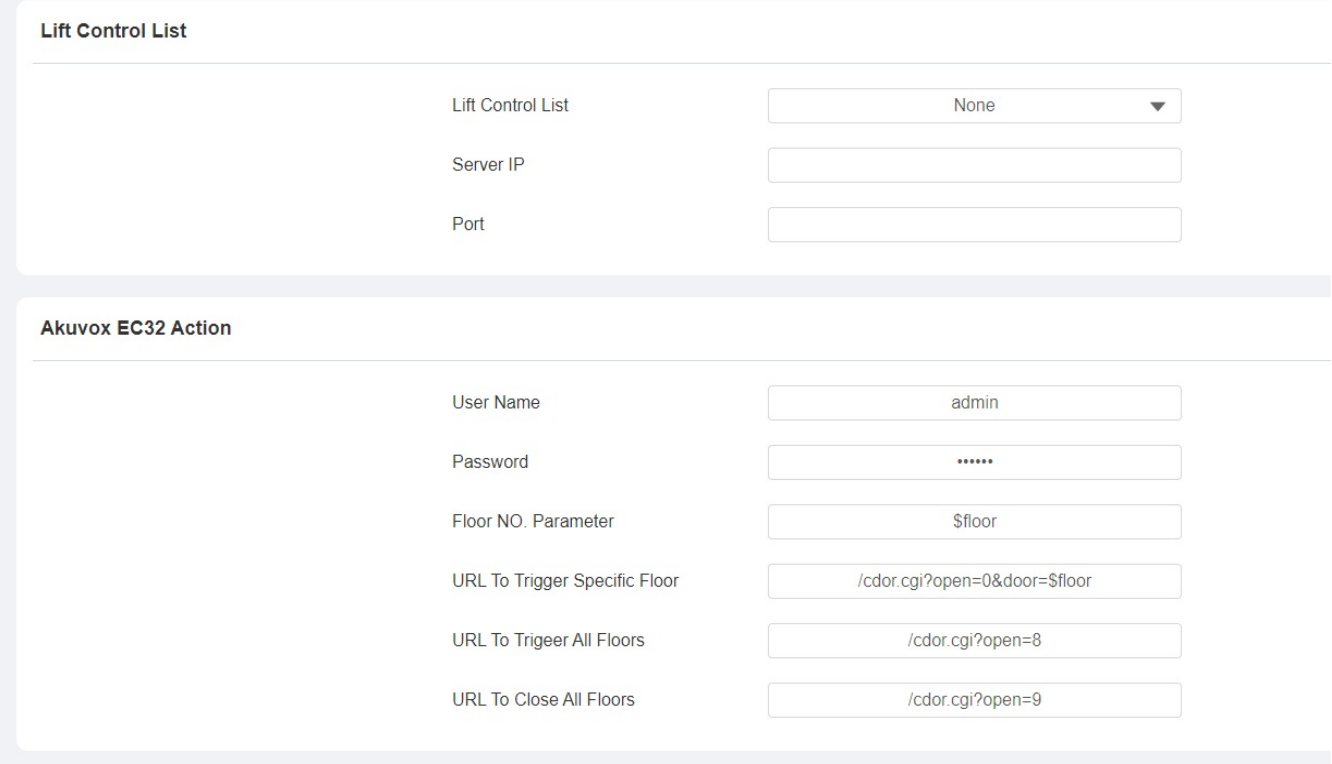
Tip

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

Lift Control

The door phones can be connected to the Akuvox lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through various types of access methods on the door phone.

To set up the lift control, navigate to the web **Device > Lift Control** interface.



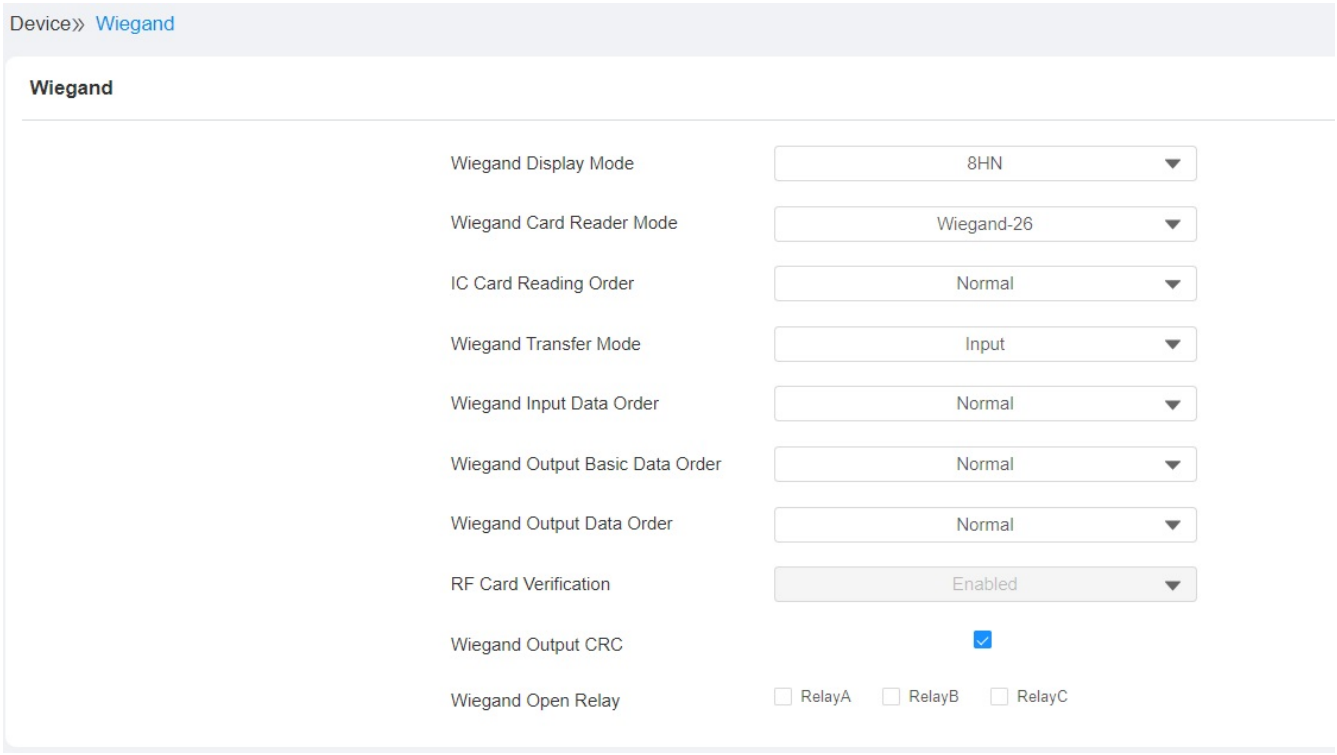
- **Lift Control List**: select None to disable the function, and select the Akuvox E32 to integrate the door phone with the Akuvox EC32 controller.
- **Server IP**: enter the IP address of the Akuvox EC32 controller server.
- **Server Port**: enter the Sever port of the Akuvox EC32 controller server.
- **User Name**: enter the user's name of the lift controller for the authentication.
- **Password**: enter the password of the lift controller for the authentication.
- **Floor NO. Parameter**: enter the Floor number parameter provided by Akuvox. The default parameter string is $floor. You can define your own parameter string if needed.
- **URL To Trigger Specific Floor**: enter the Akuvox life control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string $floor at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.

Integration with Third Party Device

Integration via Wiegand

The Wiegand feature enables Akuvox door phone to act as a controller or a card reader.

Navigate to the web **Device > Wiegand** interface.



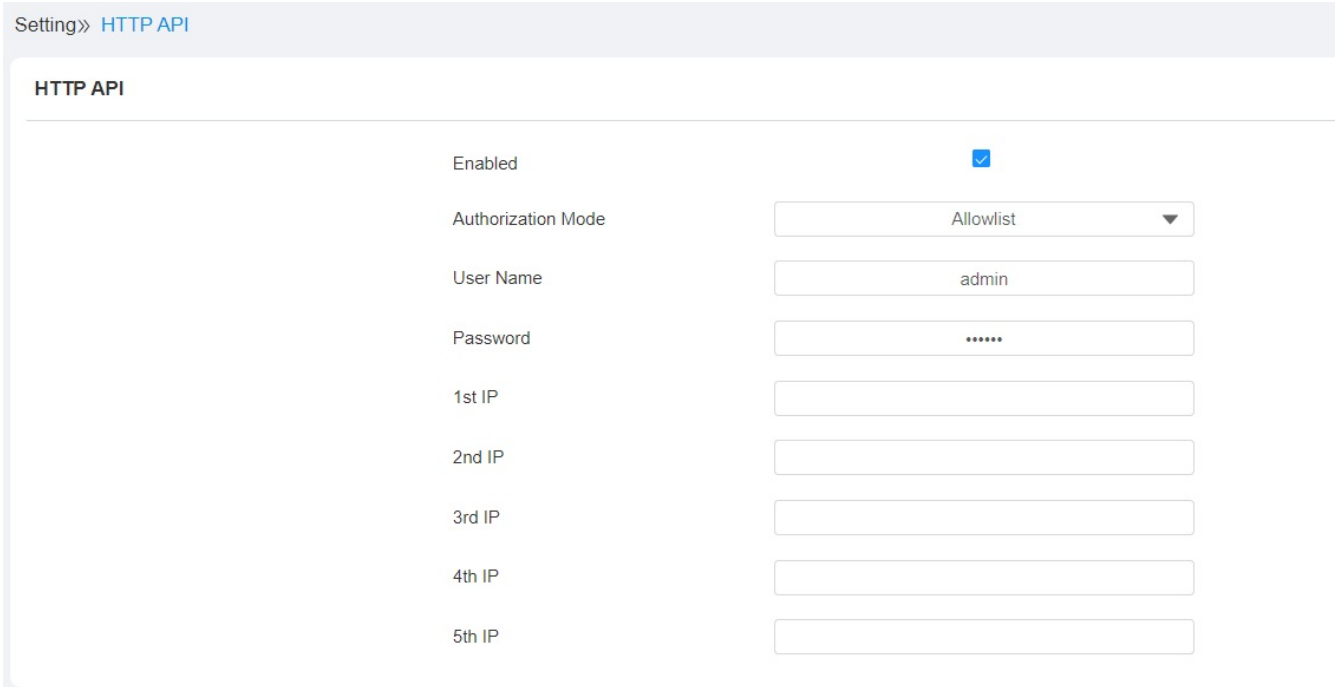
- **Wiegand Display Mode**: select Wiegand Card code format among 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.
- **Wiegand Card Reader Mode**: set the Wiegand data transmission format among three options: **Wiegand 26, Wiegand 34,** and **Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **IC Card Reading Order**: this option only works when Wiegand-26 is selected.
    - Normal: the device will read the last three bytes of the IC card. For example, if the IC card number is 840C9F50, 0C9F50 will be read.
    - Reversed: the device will read the first three bytes of the IC card. For example, if the IC card number is 840C9F50, 840C9F will be read.
- **Wiegand Transfer Mode**:
    - Input: the door phone is used as a receiver.
    - Output: the door phone is used as a sender.
    - Convert to Card No.Output Wiegand: the Wiegand output will be converted to a card number before sending it from the door phone to a receiver.

- **Wiegand Input Data Order**: set the Wiegand input data sequence between **Normal** and **Reversed.** If you select **Reversed**, then the input card number will be reversed and vice versa.
- **Wiegand Output 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.
- **Wiegand Open Relay**: the relay to be triggered.

Integration via HTTP API

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

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



- **Enabled**: enable or disable the HPTT API function for the third-party integration. For example, if the function is disabled, any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Authorization Mode**: select among **None, Normal, Allowlist, Basic, Digest,** and **Token** for authorization type, which are 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.

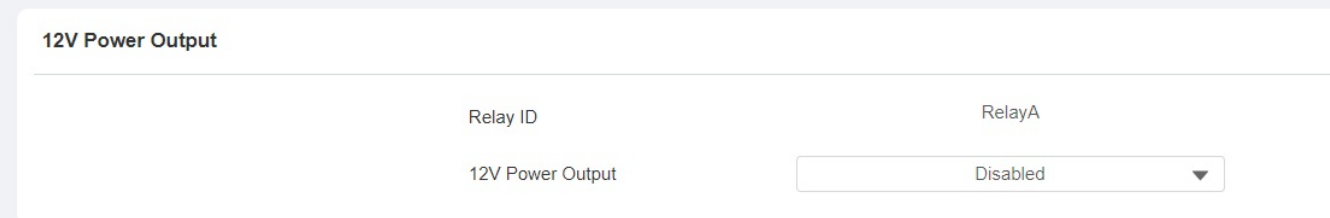
Please refer to the following description for the authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third-party device for the authentication. The allowlist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode of username and password.
5	Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of HTTP request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

Power Output Control

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

Navigate to the web **Access Control > Relay >12V Power Output** interface.

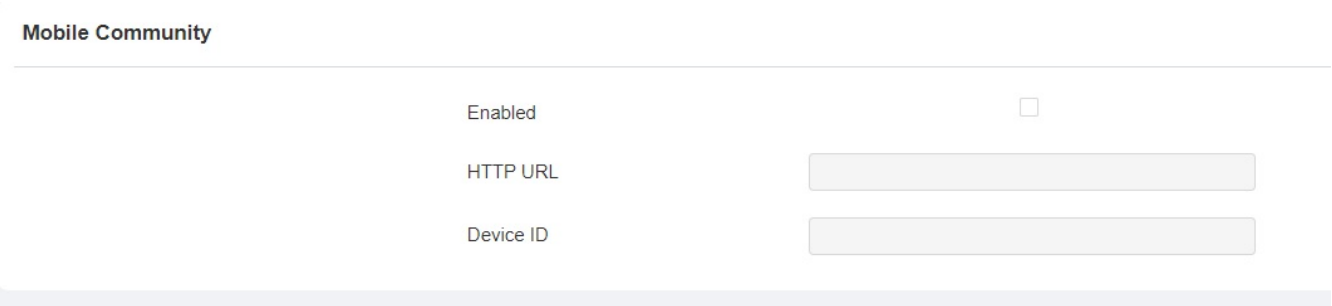


- **12V Power Output**:
  - **Disabled**: disable the power output function;
  - **Always**: enable the access controller to provide continuous power to the third-party device.
  - **Triggered By Open Relay**: provide power to the third-party device via 12 output and GND interface during the timeout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

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.

Navigate to the web **Access Control > Relay > Mobile Community** interface.



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.

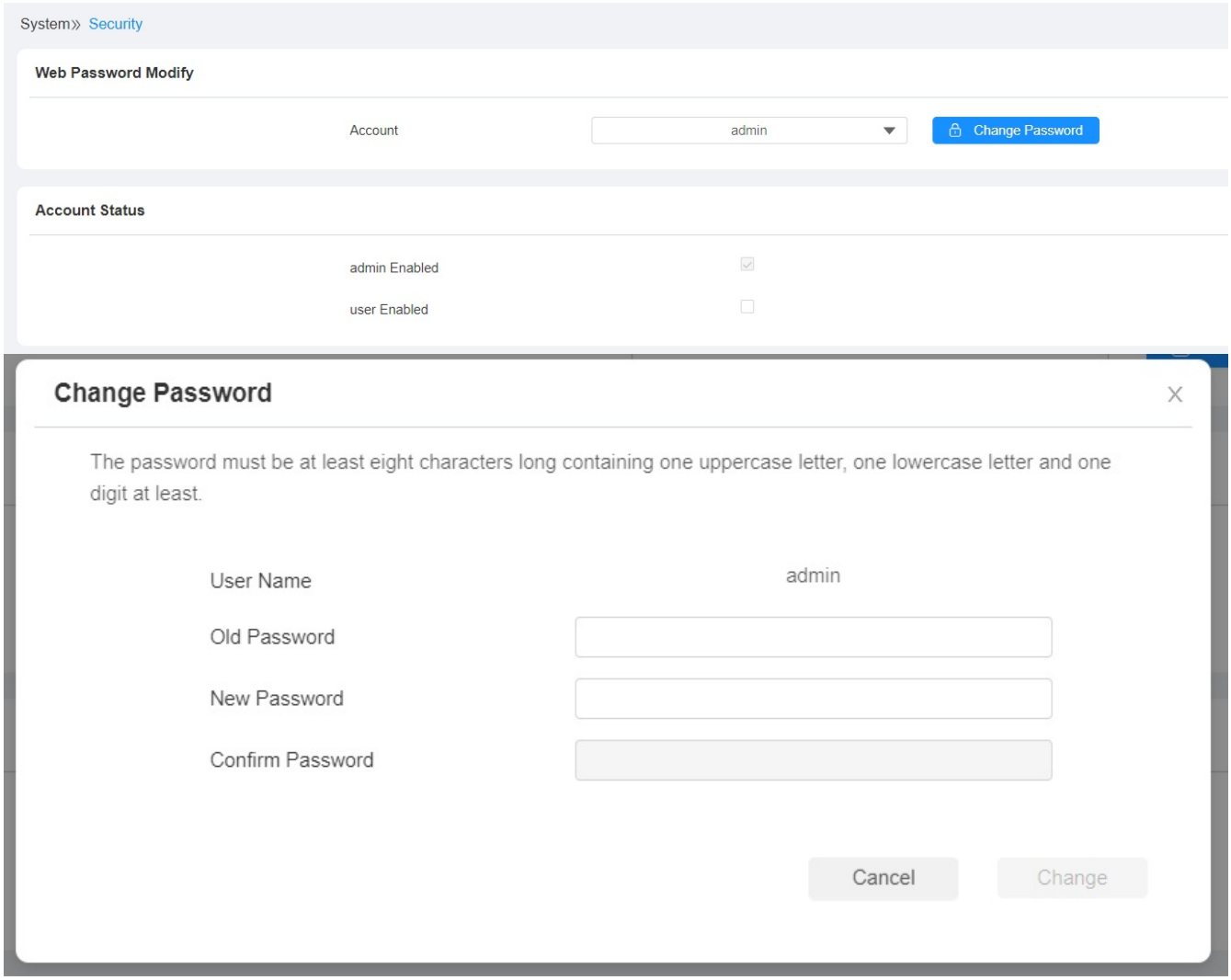
Navigate to the web **Surveillance > ONVIF > Advanced Setting** interface.

Password Modification

Modify Device Web Interface Password

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

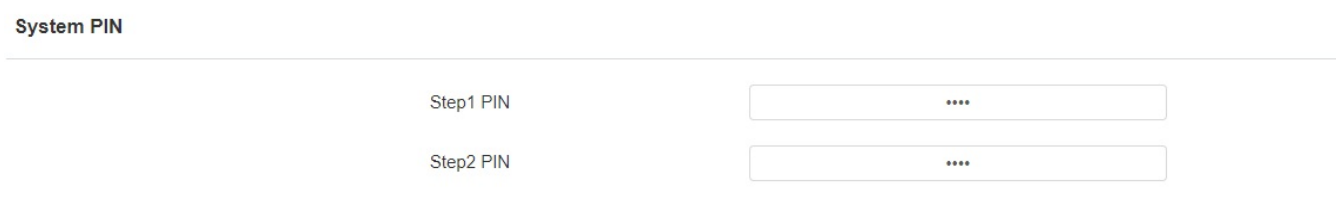
To change the default web password on web **System > Security > Web Password Modify** interface. You can also enable the user account on the interface.



Modify System Password

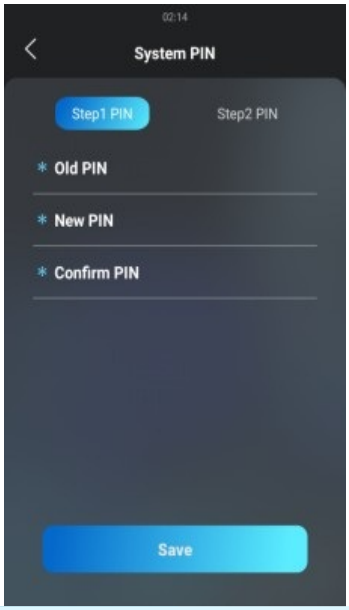
The system PIN code is used to access the device system. You can modify the system PIN code on the device and web interface.

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



- **Step1 PIN**: enter the four-digit project new password to replace the old one. The initial project password is **9999**.
- **Step2 PIN**: enter the four-digit setting password to replace the old one. The initial setting password is **3888**.

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

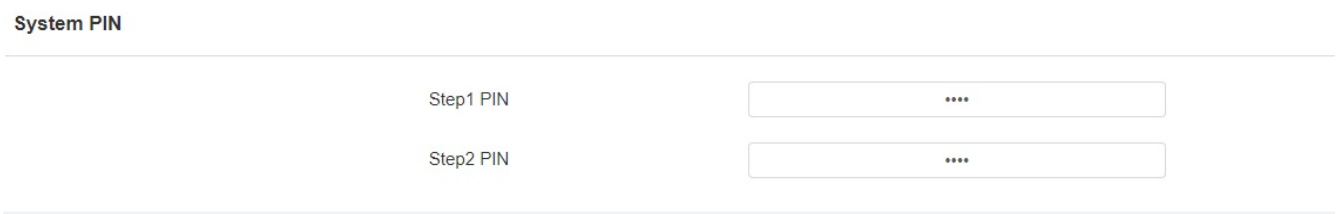


> **Note**
>
> The default system entry password is 9999 and the system setting password is 3888.

Modify Setting Password

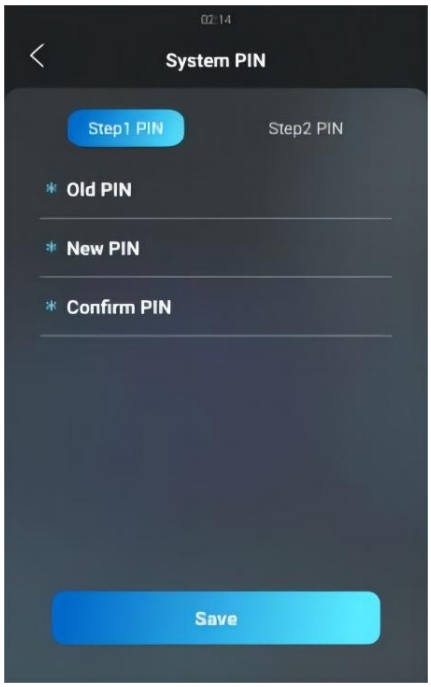
Setting PIN code is used to access the device setting. You can modify the system PIN code on the device and web interface.

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



- **Step1 PIN**: enter the four-digit project new password to replace the old one. The initial project password is **9999**.
- **Step2 PIN**: enter the four-digit setting password to replace the old one. The initial setting password is **3888**.

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


02:14
System PIN
Step1 PIN
Step2 PIN
Old PIN
New PIN
Confirm PIN
Save

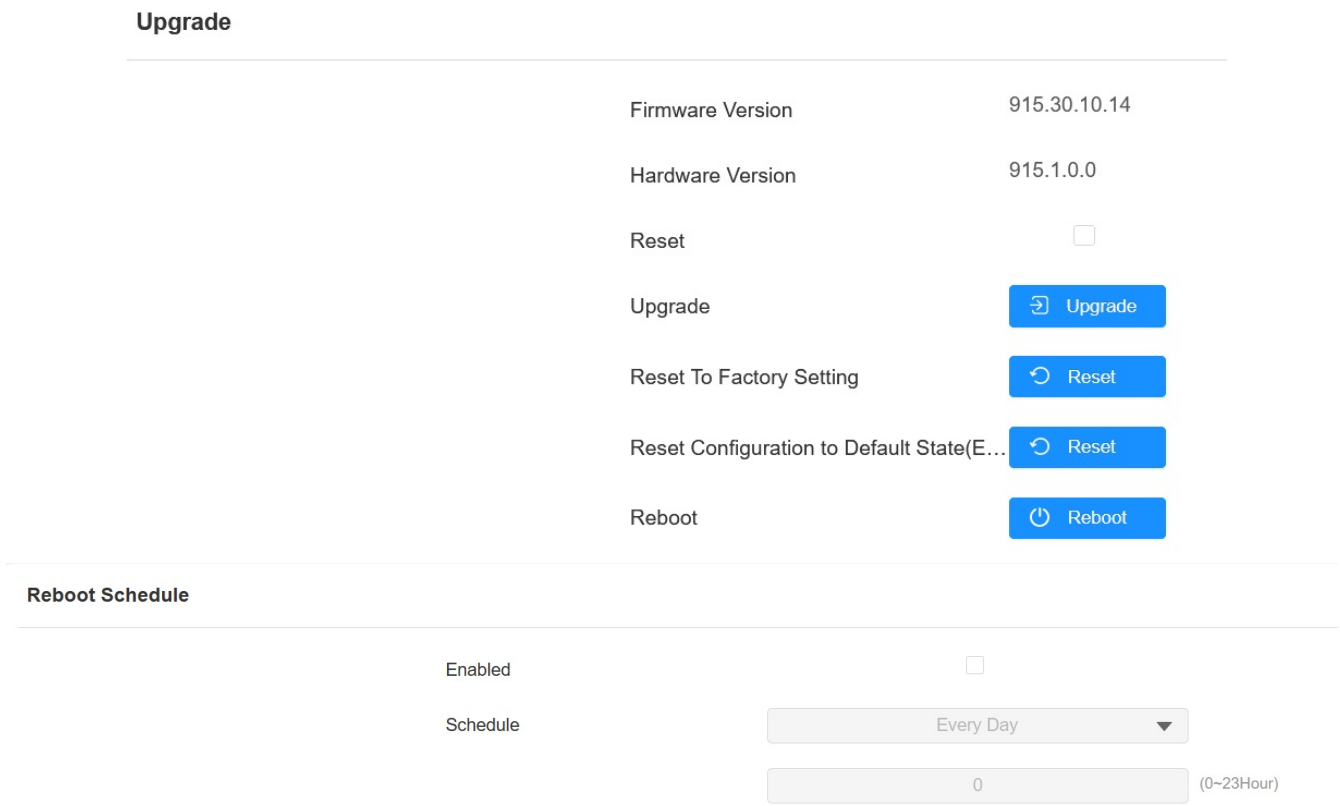
System Reboot&Reset

Reboot

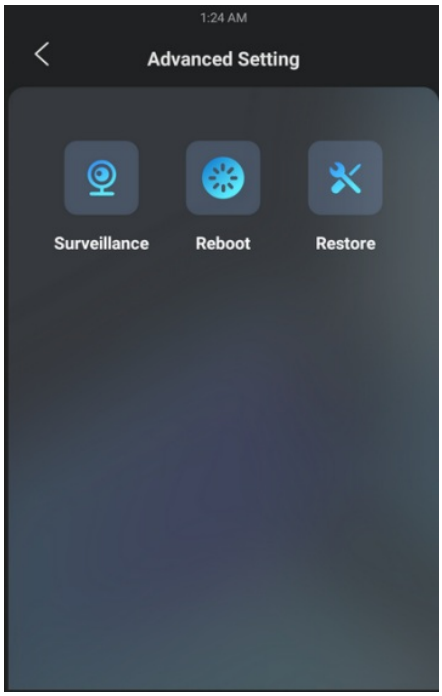
Reboot on the Web

If you want to reboot 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. To set the schedule on **System > Auto Provisioning > Reboot Schedule**.



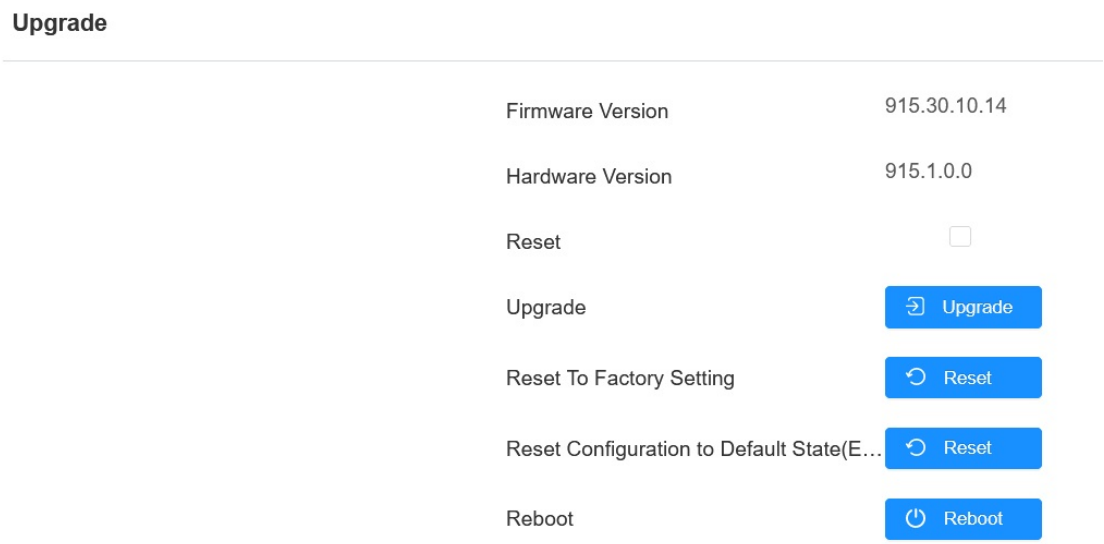
To reboot the device, go to the **Advanced Setting > Reboot** screen.



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**.