About This Manual

Thank you for choosing Akuvox X916 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 916.30.10.2 version and above, and it provides all the configurations for the functions and features of X916 series door phone. Please visit Akuvox forum or consult technical support for any new information or latest firmware.

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX X916 DOOR PHONE

Administrator Guide

Product Overview

X916 series is an Android-based IP video door phone with a large size LCD touch screen. It incorporates audio and video communications, access control and video surveillance.

Its finely-tuned Android OS allows for feature customization to better suit the habit of usage of local people. X916 is with one star light camera and one auxiliary camera. In addition to the multiple ports such as RS485, POE ports, Wiegand ports, the door phone is also designed to include such ports and interfaces as 2 USB(s), HDMI, TF card, SIM, RJ45 ports etc., in order to maximize its connections with external digital systems such as elevator controller, fire alarm detector, LTE wireless connection, as well as data storage. With these integrated features, X916 is built to create a holistic control of building entrance and its surroundings and giving you a greater sense of security and smart living experience.

X916 is applicable to luxurious apartment buildings for intercom cloud application and office buildings and their complexes for visitor management system.

Change Log

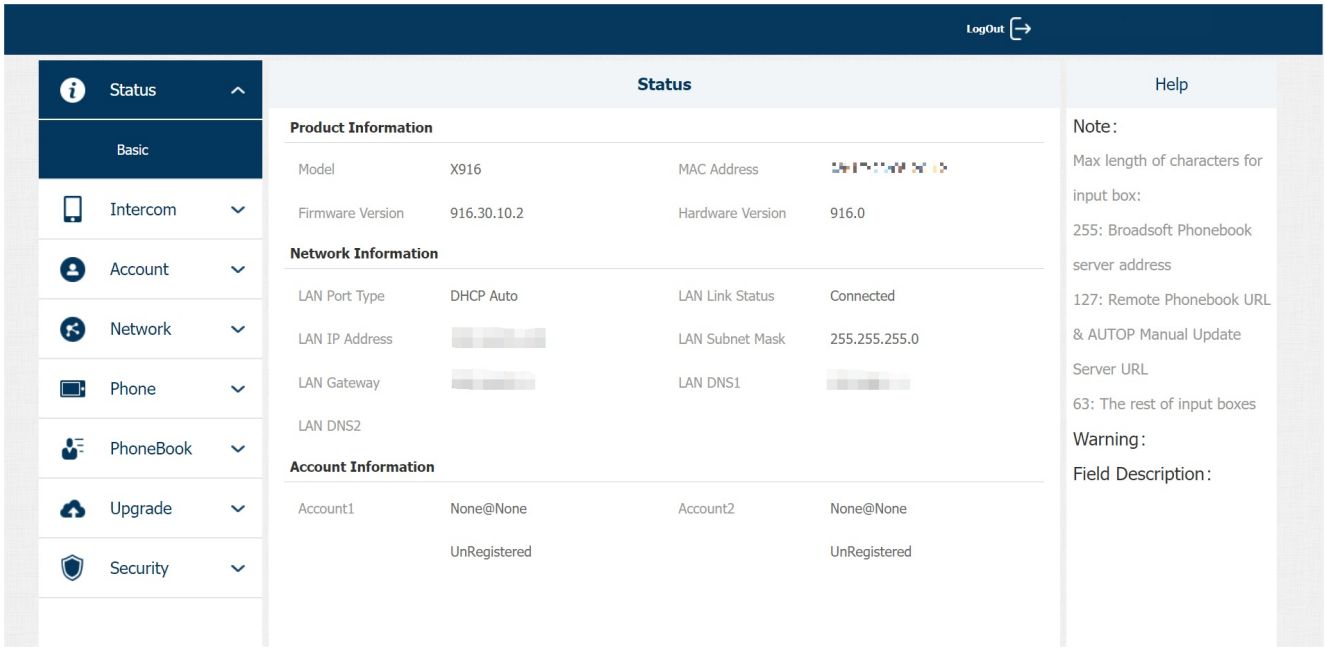
Add High Security Mode.

Model Specification

X916S	
Touch Screen	✔
Relay In	4
Relay Out	4
Alarm In	X
RS485	✔
Card Reader	13.56MHZ&125KHZ
Wi-Fi	X
Bluetooth	✔
Temperature Detection	Optional
Face Recognition	✔
LTE	✔
USB	✔
External SD Card	✔

Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, network Information, and account information etc.
- **Intercom**: this section covers intercom call, LED & LCD setting, relay, input control, live stream, RTSP, ONVIF, motion detection, card setting, face recognition setting, tab & button display, camera, private PIN code, RS485 connection, etc.
- **Account**: this section concerns SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer etc.,
- **Network**: this section mainly deals with DHCP & Static IP setting, RTP port setting, and device deployment etc.,
- **Phone**: this section includes time & language, call feature, dial management, data import & export, door log, web relay.
- **PhoneBook**: this section involves call log and phone book management.
- **Upgrade**: this section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.
- **Security**: this section is for password modification.

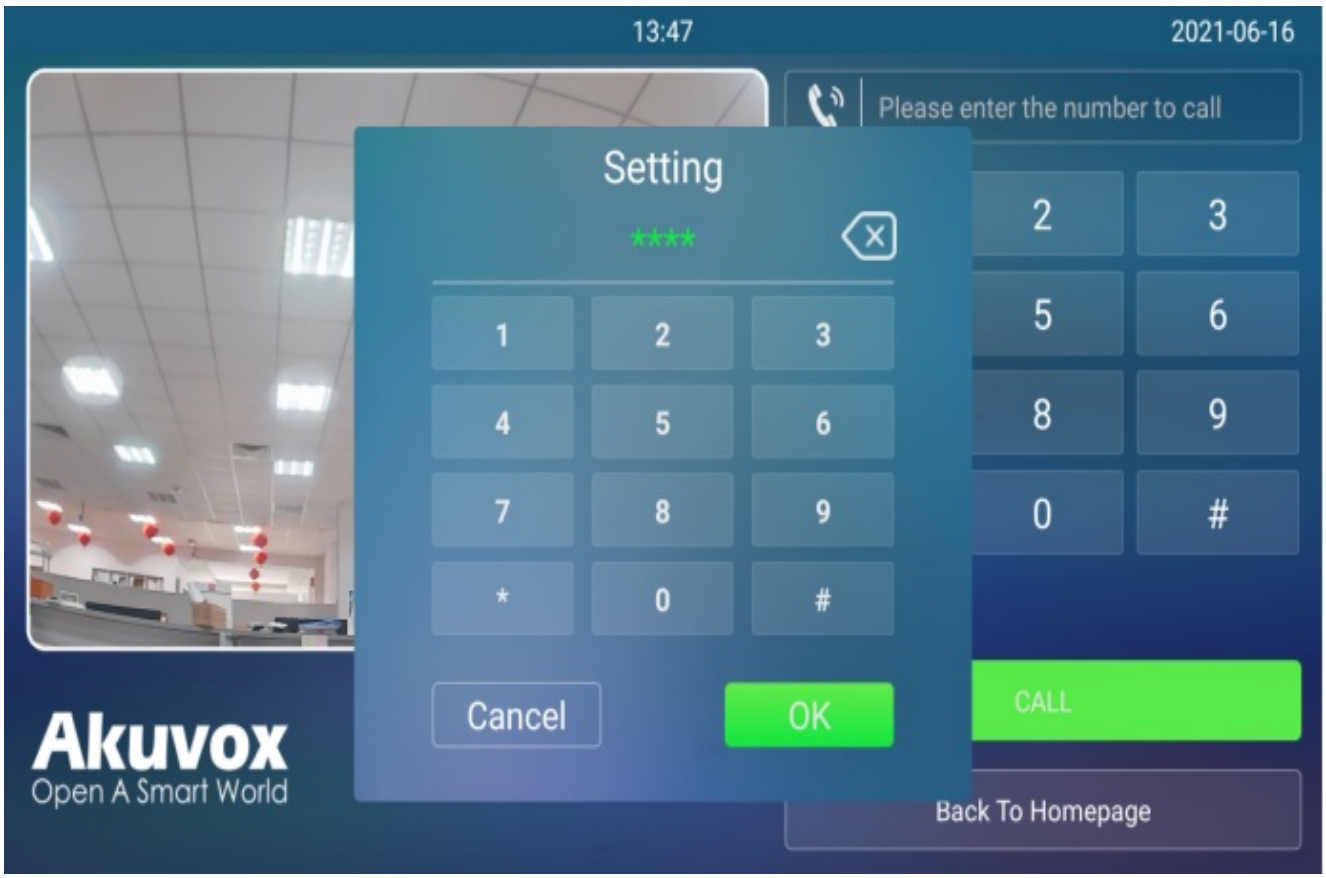


Access the Device

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

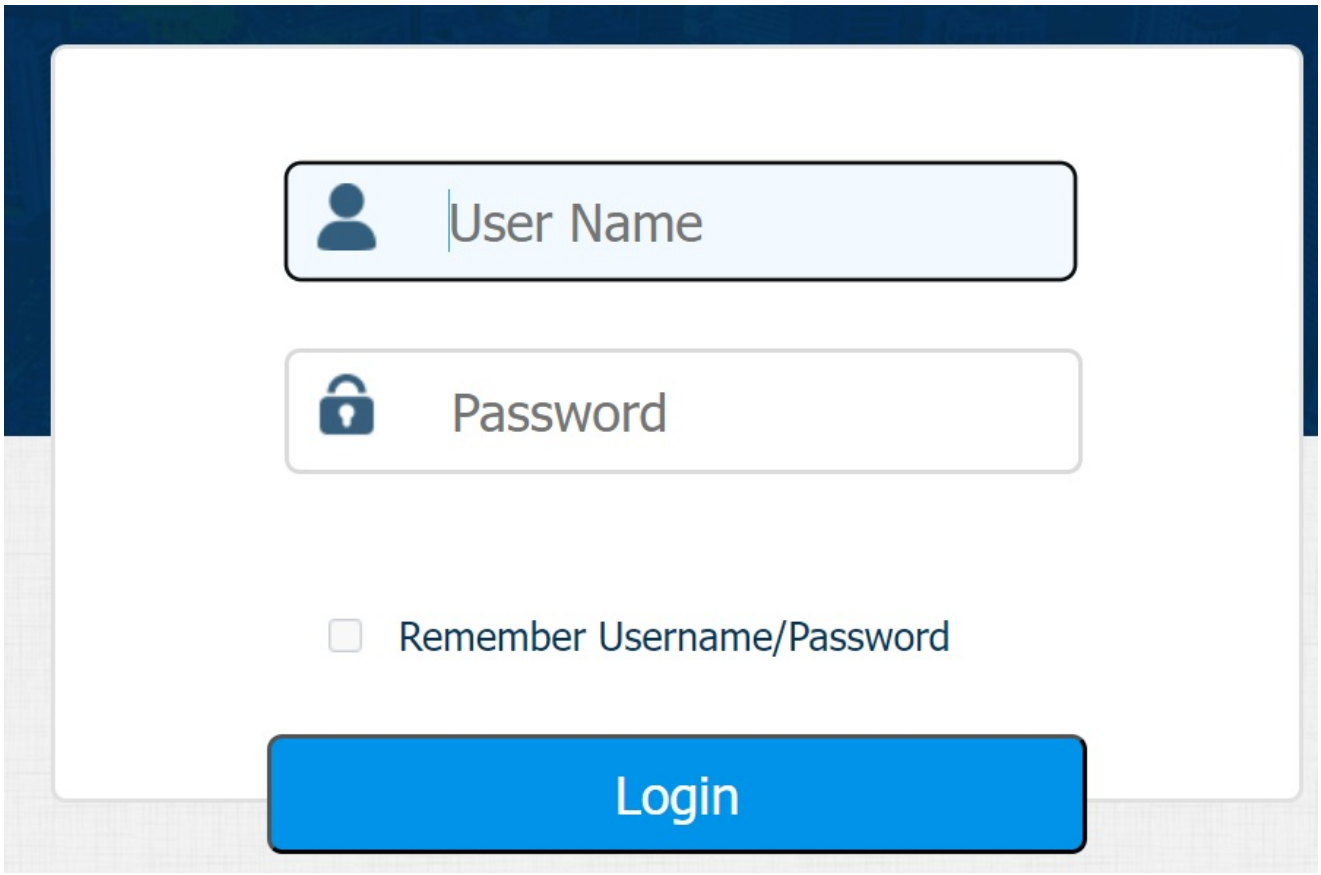
Access the Device Setting on the Device

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



Access the Device Setting on the Web Interface

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



Note

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

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See 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.
- The initial username and password are **admin** and 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

To configure the language display on the device **Settings > Language** screen.

The device supports the following languages:

- Simplified Chinese, English, Spanish, Danish, Czech, French, Traditional Chinese, Turkish, German, Japanese, Ukrainian, Korean, and Dutch.

Language Setting on the Device Web Interface.

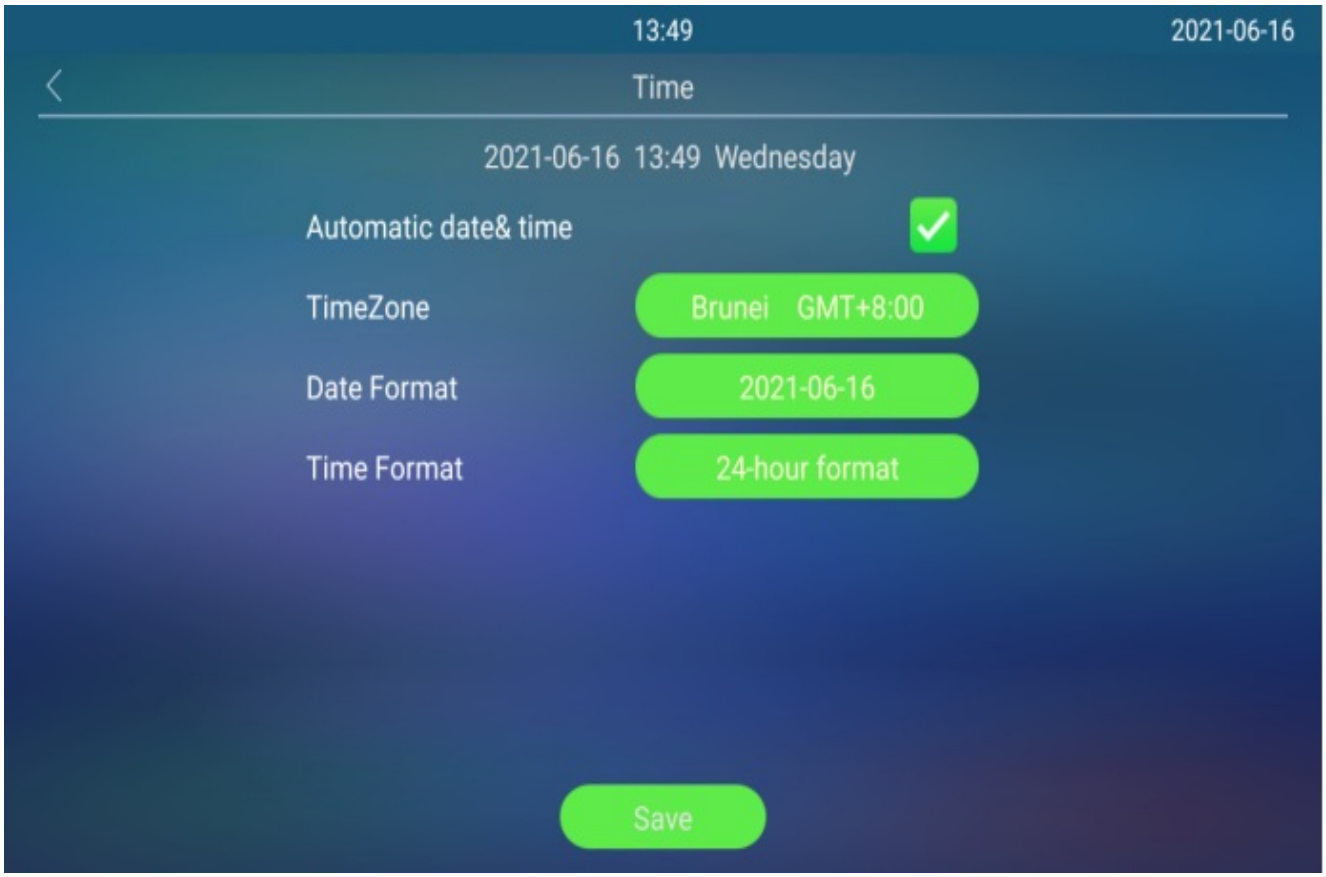
To configure the configuration on the web **Phone >Time/Lang > Web/LCD Language** interface.

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

To configure it on the device **Settings > Time** interface.

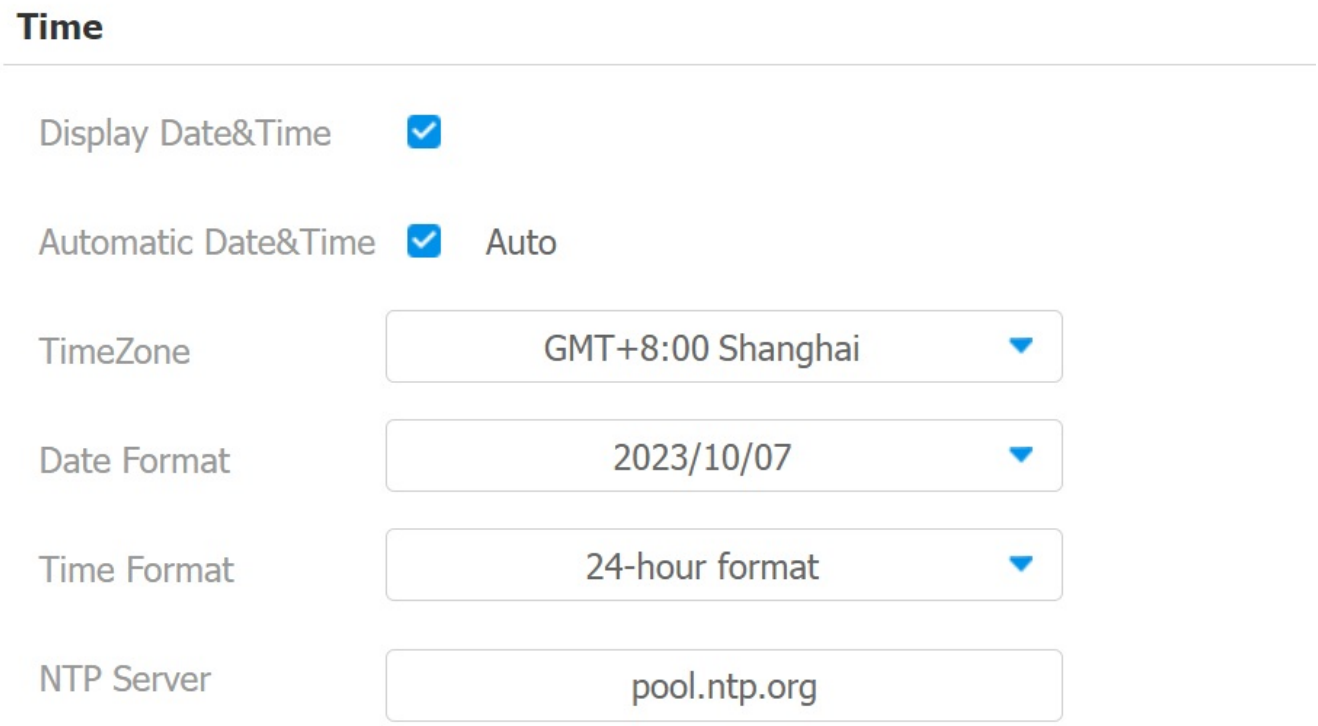


Parameter Set-up:

- **Automatic Date & Time**: automatic date & time is turned on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**). You can also set it up manually by turning off automatic date & time first, then enter the desired time and date before pressing the **Save** for the validation.

Time Setting on the Device Web Interface

To configure it on the web **Phone >Time/Lang > Time** interface.



Parameter Set-up:

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

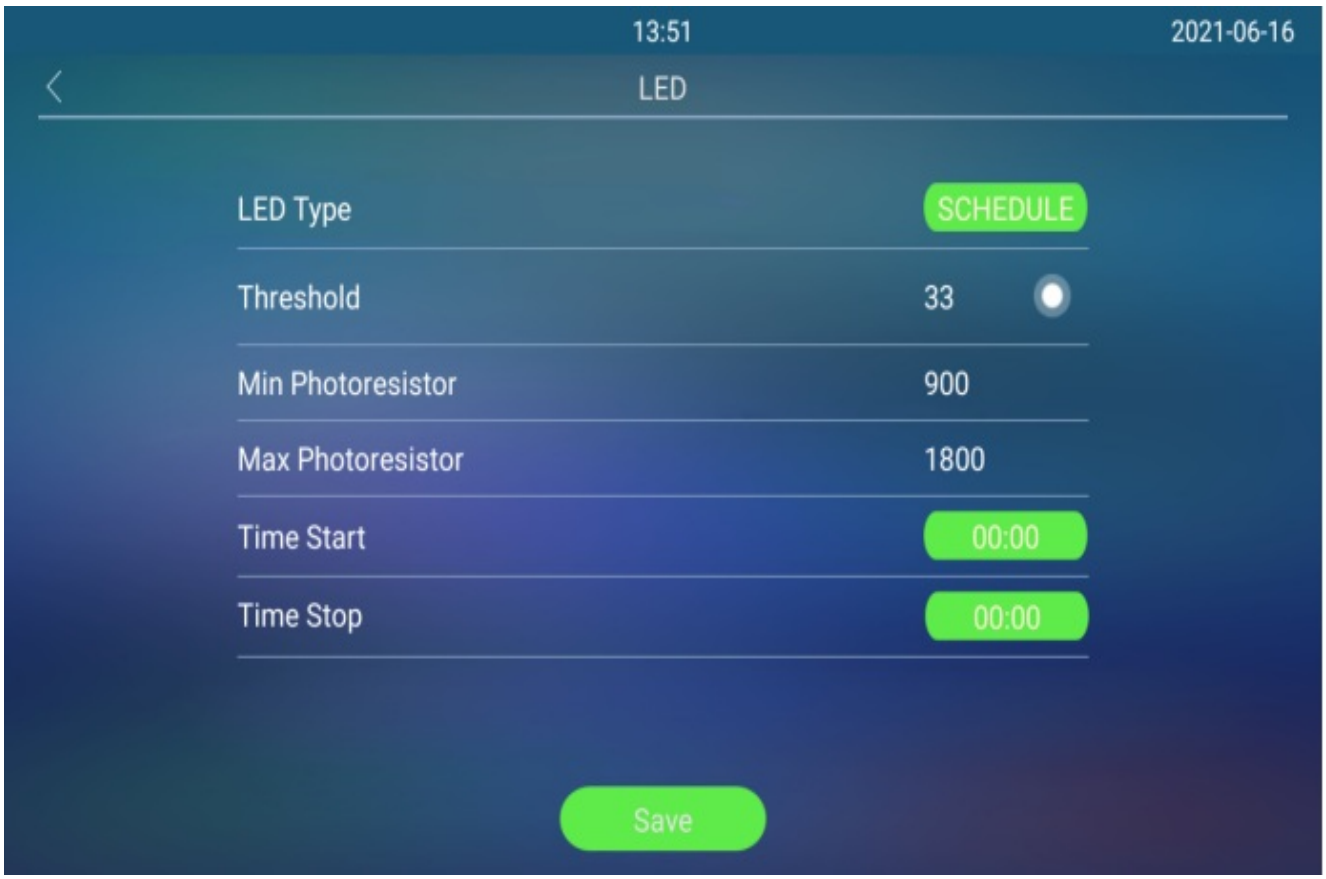
LED & LCD Setting

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 Device

To configure it on the device **Setting > LED** interface.



Parameter Set-up:

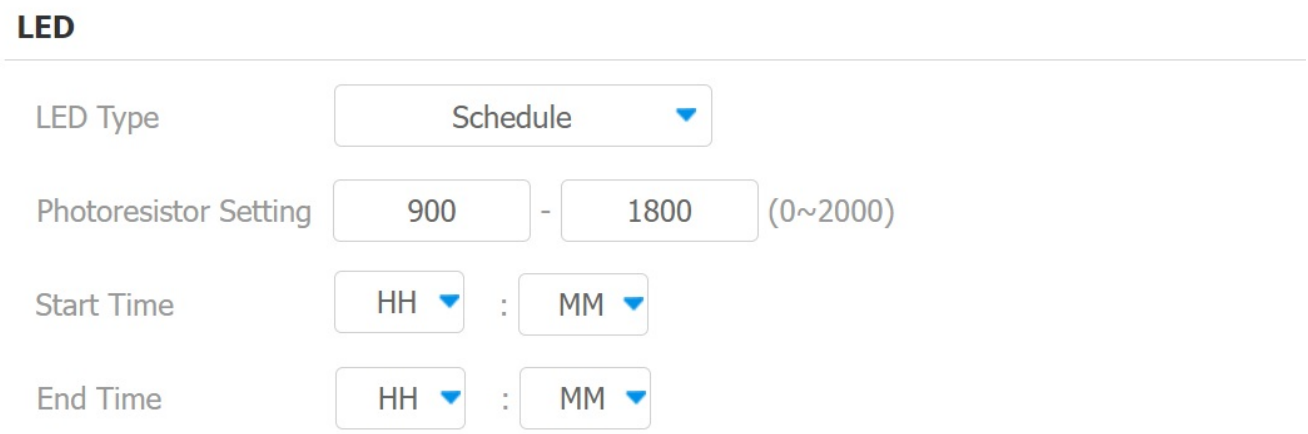
- **LED Type**: you can see the LED type: **Auto, ON, OFF**, and **Schedule**. Select **Schedule** to turn on the infrared LED according to the time schedule.
- **Threshold**: refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is **33**, however, you can tap the icon

several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on to configure the minimum and maximum photo-resistor values.

- **Min/Max Photoresistor**: set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the ON-OFF of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default Minimum and maximum photoresistor value is from **0** minimum to **1000** maximum respectively.

Infrared LED Setting on the Web Interface

To configure the configuration on the web **Intercom > Advanced > LED** interface.



Note:

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

LED Setting on Card Reader Area

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

To configure it on the web **Intercom > LED Setting > LED Control** interface.

Parameter set-up:

- **Start Time- End Time (H)**: enter the time span for the LED lighting to be valid, e.g., if the time span is set from 8-0 (Start time- End time), it means LED light will stay on during the time span 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

To configure it on the web **Intercom > Advanced > LCD** interface.

Parameter Set-up:

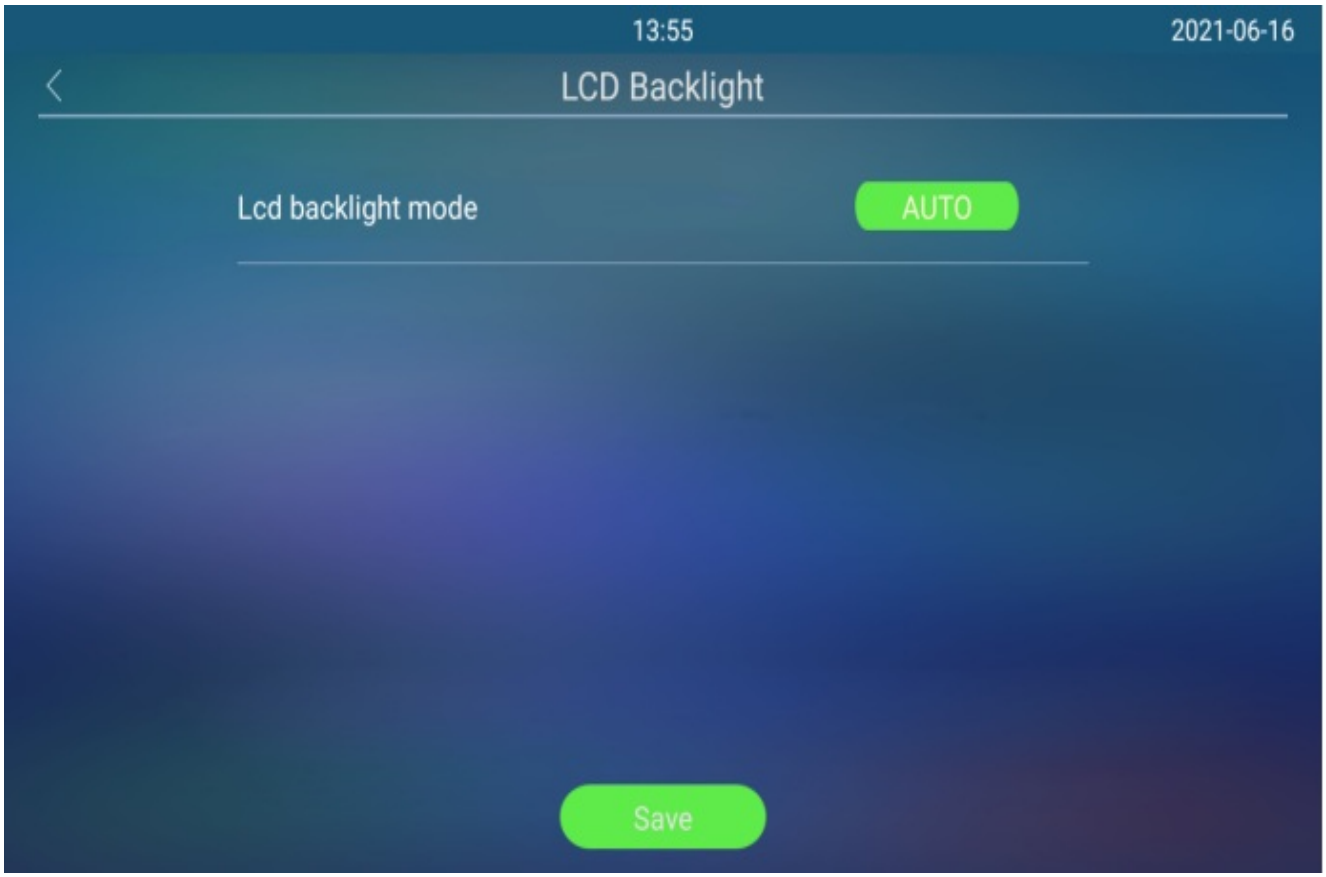
- **Backlight Mode**: click to select **Manual** or **Auto** mode for the backlight. Backlight will be adjusted automatically for the screen back light brightness when **Auto** is selected and vice versa.
- **Backlight (day)**: set the screen backlight brightness during the daytime with the value

ranging from (**0-255**).

- **Backlight (day) Standby**: set the screen backlight brightness for the screen saver during the day time with the value ranging from (**0-255**).
- **Backlight (night)**: set the screen backlight brightness in the night with the value ranging from (**0-255**).
- **Backlight (night) Standby**: set the screen backlight brightness for the screen saver during the day time with the value ranging from (**0-255**).
- **Deep Sleep Enable**: it decides whether the door phone enters deep sleep mode when idle. (Deep sleep means the device screen will be dark)
- **Deep Sleep Interval**: the time from screensaver to enter deep sleep. The interval can be set up as **5 Minutes, 10 Minutes, 15 Minutes, 20 Minutes, 30 Minutes**.

LCD Screen Brightness Setting on the Device

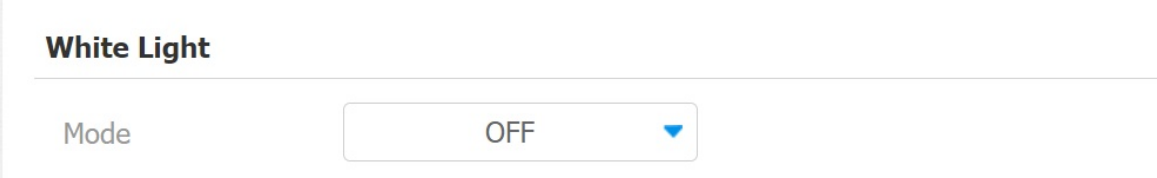
To configure the brightness on the device **Setting > LCD Backlight** interface.



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.

To configure it on the **Intercom > Advanced > White Light** interface.



Parameter Set-up:

- **Mode**: select **Auto** or **OFF**. If you select **Auto**, then the white light will turn on for 10 seconds within three conditions - staying home page; the photosensitive detection and the IR detection are triggered.

QR Code with Light Setting

White light LED is mainly used to reinforce the lighting for the QR code access in the dark environment. You can set the white light function properly on the device **Intercom > Advanced > QR Code White Light** web interface.

Parameter Set-up:

- **Mode**: select **Auto** or **OFF**. If you select **Auto** then the white light will turn on for 10 seconds within two conditions - staying Temp Key page; the photosensitive detection is triggered.
- **Exposure Mode**: select **Auto** or **Manual**. If you select **Auto**, then the white light will be changed along with the exposure grain changes due to ambient environment changes.

Screen Display Configuration

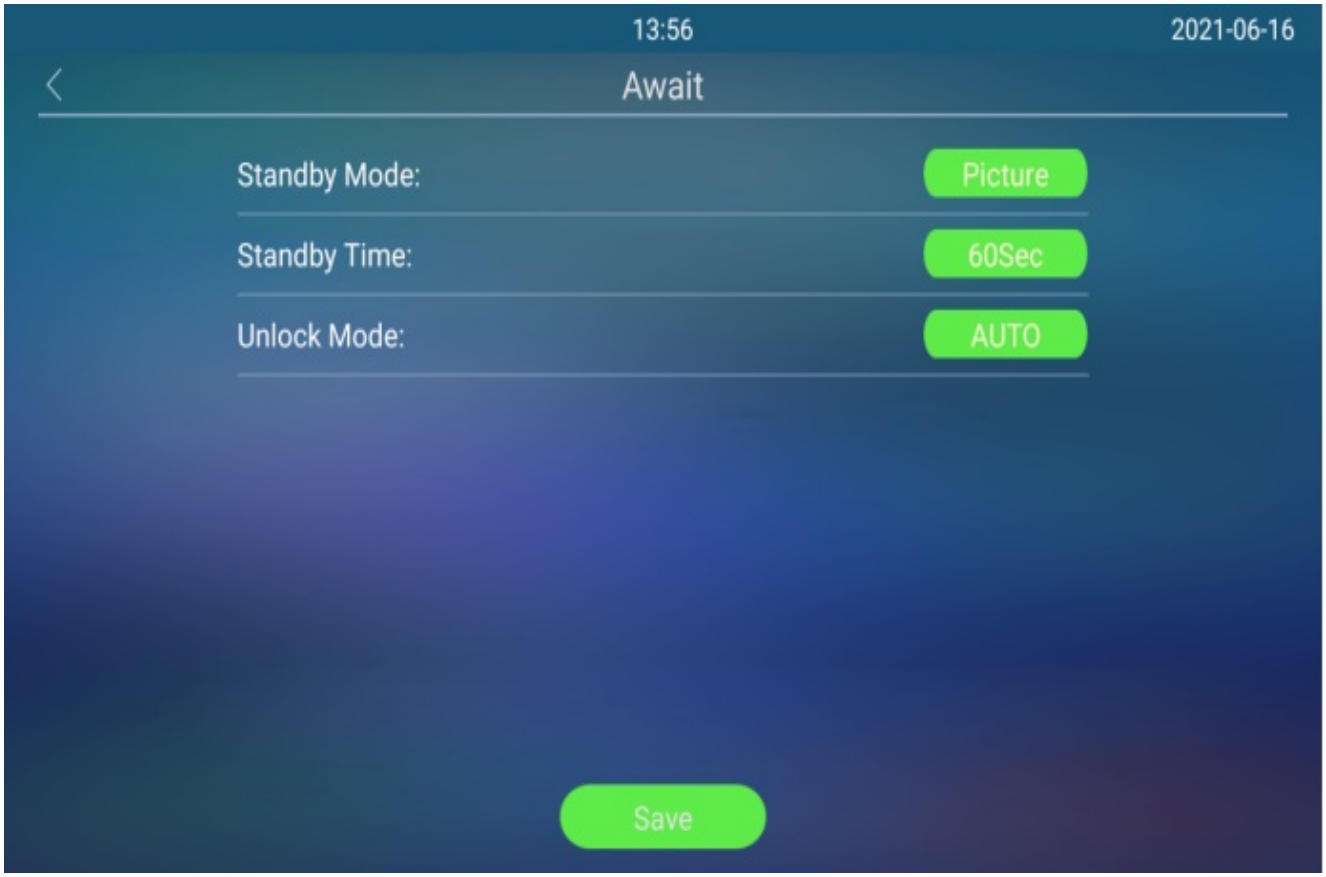
You can set up the device's screen display features such as screensaver to give users a better visual and operational experience.

Screensaver Configuration

Configure Screensaver on the Device

Standby Mode is designed for screen protection. You can set the mode to prevent the device screen from getting overheated and to reduce energy consumption. You can define when the device should go into standby mode.

To configure the feature on the device **Setting > Await** interface.



Parameter Set-up:

- **Standby Mode**: select among three options **NO**, **Blank Screen**, and **Picture**. **NO** is selected when you want the screen to stay on without going into screen saver mode; if

Blank Screen is selected, the screen will go black. If **Picture** is selected, then the picture you uploaded will be shown as the screen saver.

- **Standby Time**: set the screen saver start time from 30 seconds to 180 seconds. Screen saver starts when the device detects no operation, or no one is approaching.
- **Unlock Mode**: select the screen wake-up mode. If you select **Auto** mode, then the screen will be awakened when someone approaches without its being touched upon, and if **Manual** mode is selected, then you have to touch and wake up the screen.

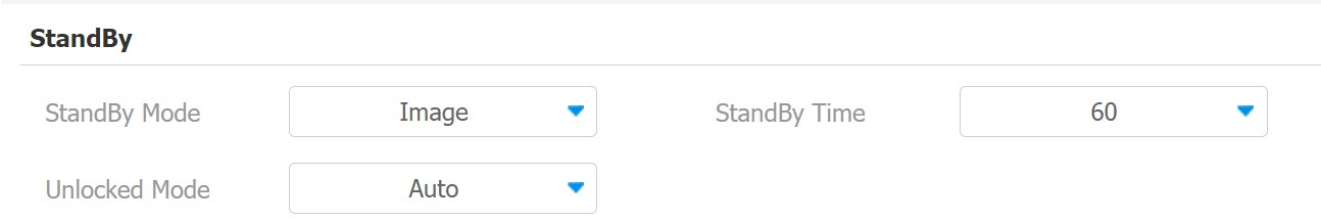
Note:

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

Configure Screensaver on the Web Interface

You can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction.

To configure it on the web **Intercom > Advanced > Standby** interface.



Parameter Set-up:

- **Standby Mode**: select among three options **NONE**, **Blank**, and **Image**. **NONE** is selected when you want the screen to stay on without going into screen saver mode; if **Blank** is selected, the screen will go black. If **Image** is selected, then the picture you uploaded will be shown as the screen saver.
- **Standby Time (Sec)**: set the screen saver start time from 30 seconds to 180 seconds. Screen saver starts when the device detects no operation, or no one is approaching.
- **Unlock Mode**: select the screen wake-up mode. If you select **Auto** mode, then the screen will be awakened when someone approaches without its being touched upon, and if **Manual** mode is selected, then you have to touch and wake up the screen.

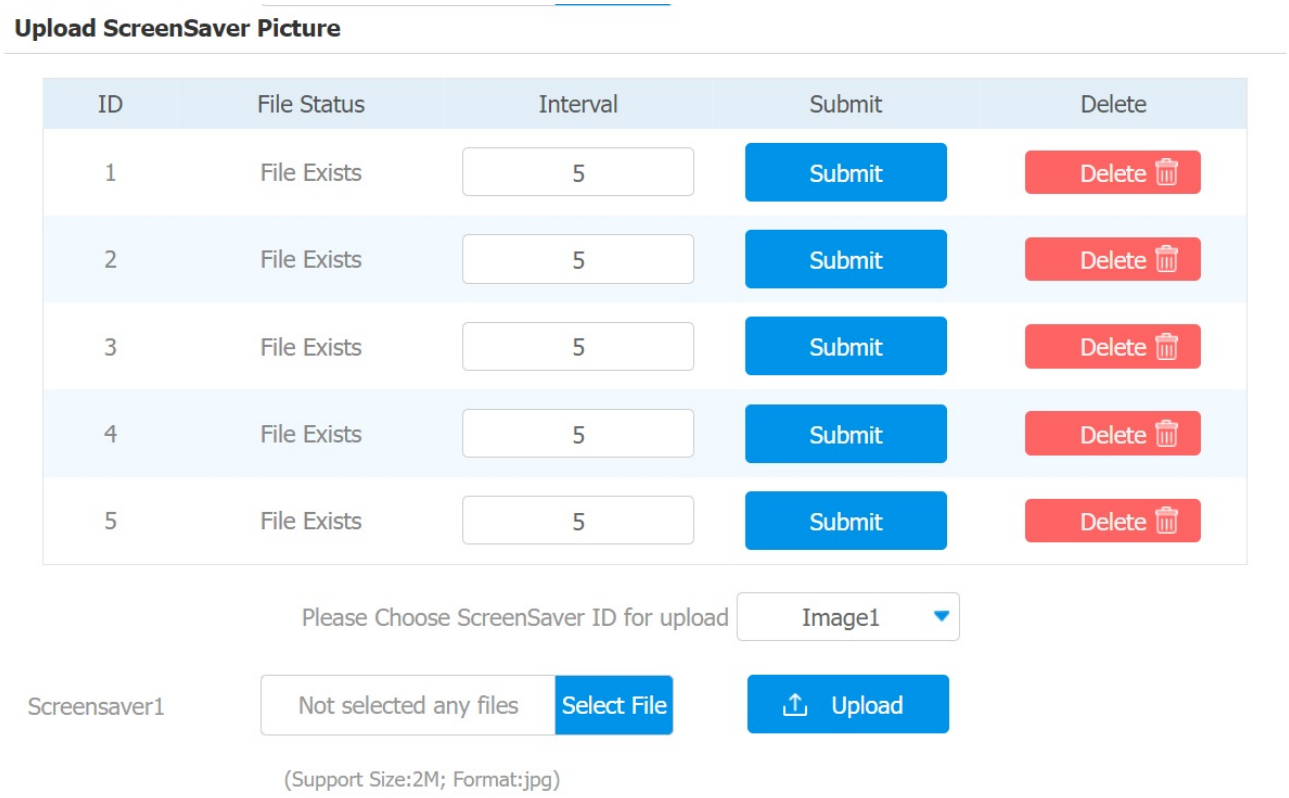
Note

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

To configure the configuration on the web **Phone > Import/Export > Upload ScreenSaver Picture** interface.



Parameters Set-up:

- **Interval**: The time for playing the screensaver picture. The time range is from 0 to 120 seconds. The picture will not be shown if the time is 0.

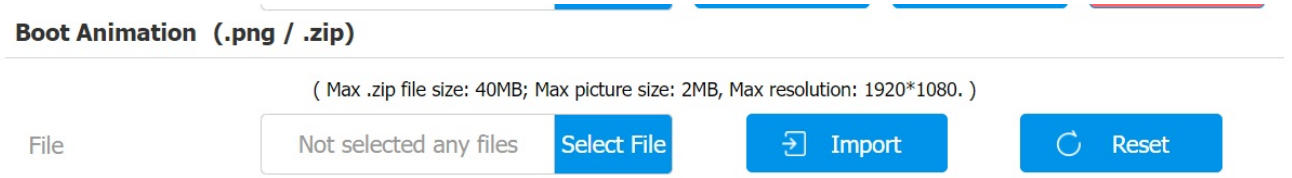
Note:

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

To configure it on the web **Phone > Import/Export > Boot Animation** interface.

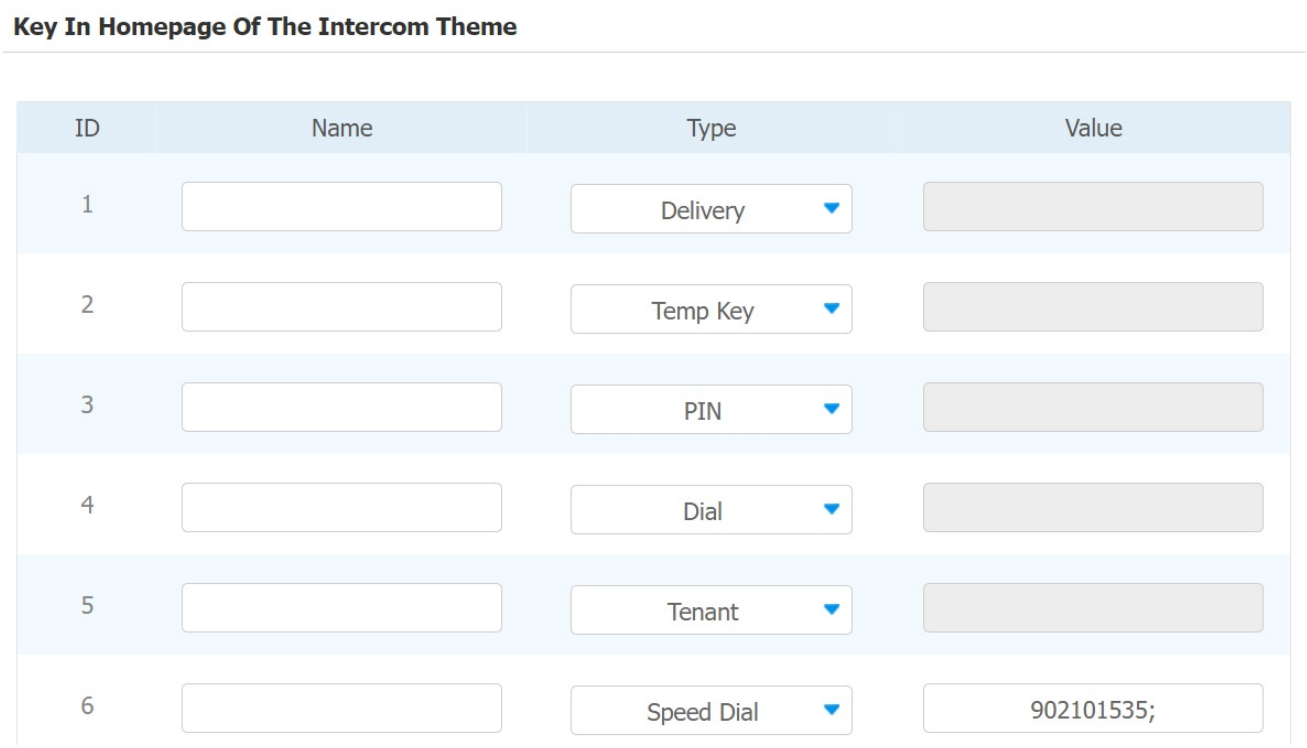


Note:

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

Home Screen Configuration

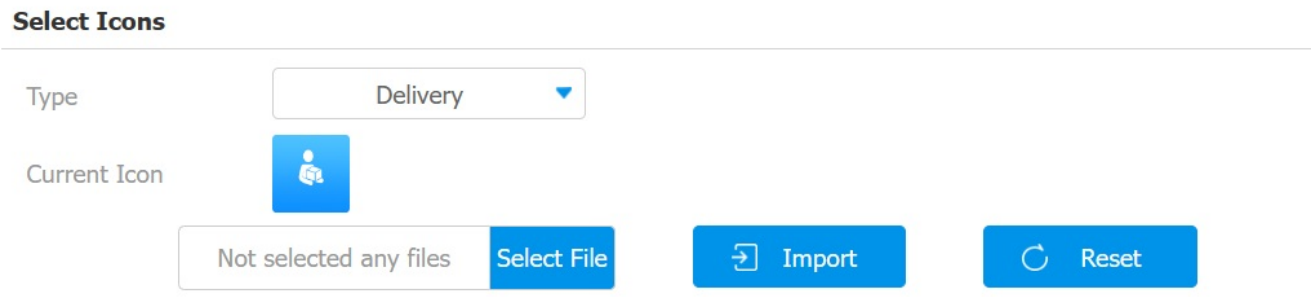
You can change the home screen display through the configuration of tab name and tab arrangement on the device web **Intercom > Key/Display > Key in Homepage of The Intercom Theme** interface.



Parameter Set-up:

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

To configure the tab icons on the web **Intercom > Key/Display >Select Icons** interface.



To configure the language icon display on web **Intercom > Key/Display > Language Setting Of The Intercom Theme** interface.

Parameter Set-up:

- **Language**: select **Visible** and **Invisible** respectively if you want the language icons to be displayed or concealed on the home screen.

Note:

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

Configuration for Scenario-based Screen Display Mode

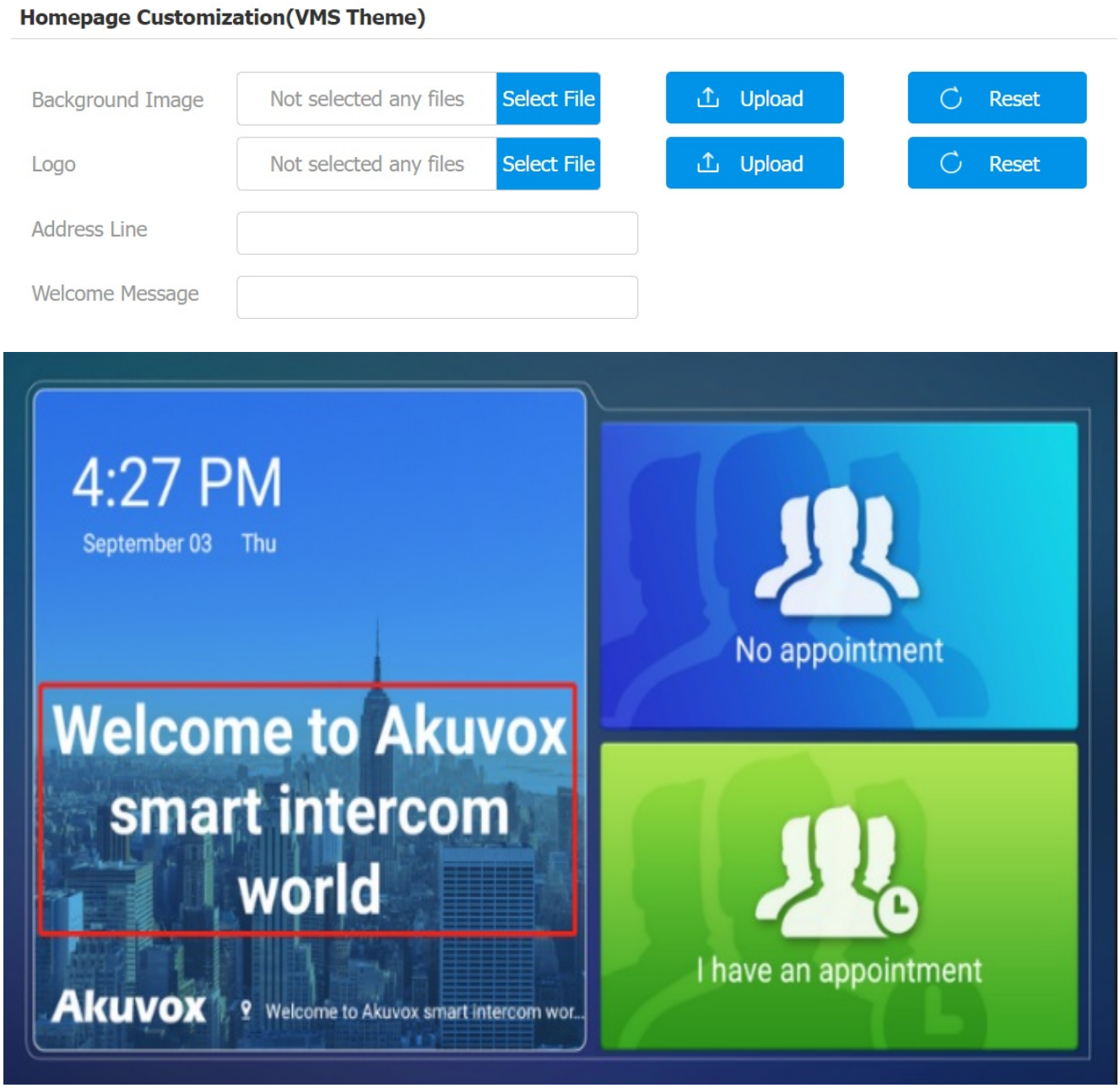
X916 series door phones offer you three types of screen display modes for the application scenarios: Intercom mode, VMS mode and Directory mode. You can make the configuration on the device web **Intercom > Key/Display >Theme** interface to select the specific mode based on actual application scenarios.

Parameters Set-up:

- **Theme**: **Intercom** theme is default theme which including six parts - **Delivery, Temp Key, PIN, Dial, Tenants** and **Reception**. **VMS** theme includes two parts - **I have an appointment, No appointment** which need to be used with Akuvox SmartPlus. **Directory** theme displays contacts on the home page.

Upload VMS Theme Home Screen Background Pictures

X916 door phones allow you to customize the home screen background picture display in the VMS mode on the device web **Intercom > Key/Display > Homepage Customization (VMS Theme)** interface.

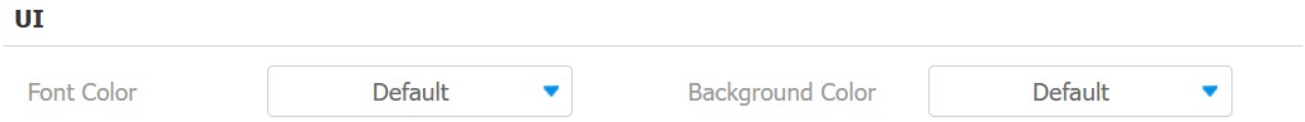


Parameters Set-up:

- **Background Image**: you can customize the picture on the left of home page.
- **Logo**: you can customize the logo on the left side.
- **Address Line**: display the current community address of the device, the default is blank in non-cloud mode, display the address issued by the cloud. It supports customization with no more than 255 characters.
- **Welcome Message**: “Welcome!” is by default. It supports up to 255 characters.

UI Setting

You can change the device's font color and background color on the web **Intercom > Advanced > UI** interface.



Parameters Set-up:

- **Font Color**: select from **Default, Black, White**, and **Custom**.
- **Background Color**: select from **Default, Black, White**, and **Custom**.

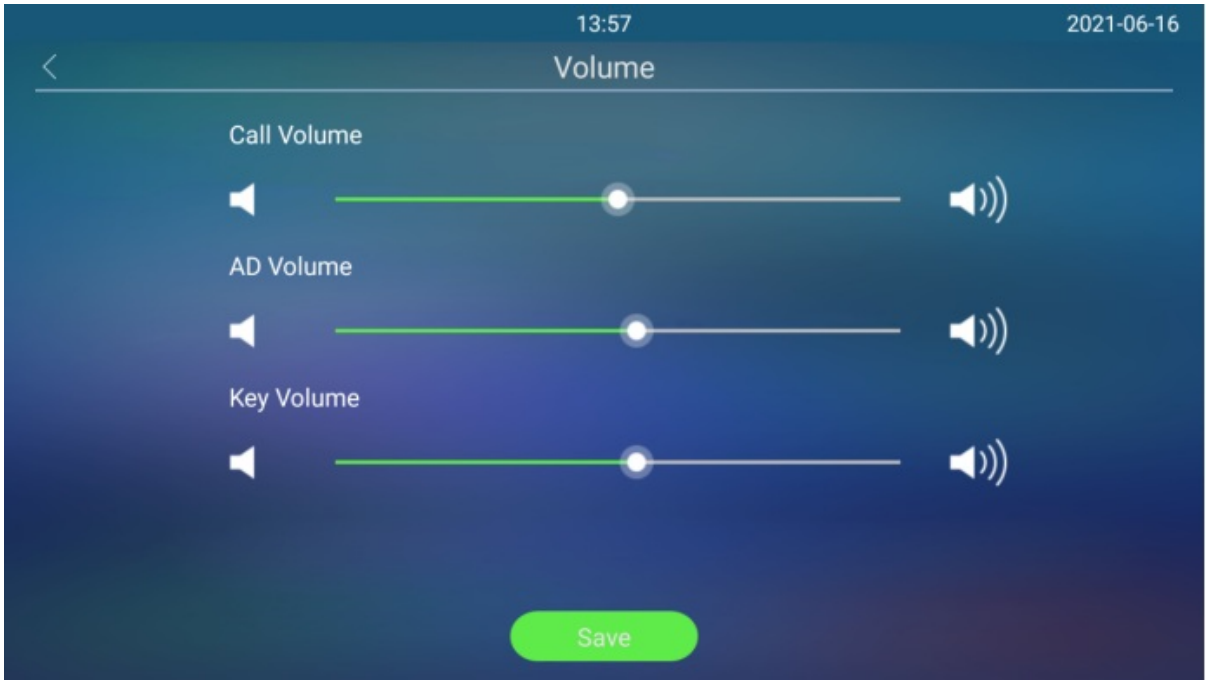
Volume and Tone Configuration

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.

Configure Volume on the Device

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

To configure it on the device **Setting > Volume** screen.

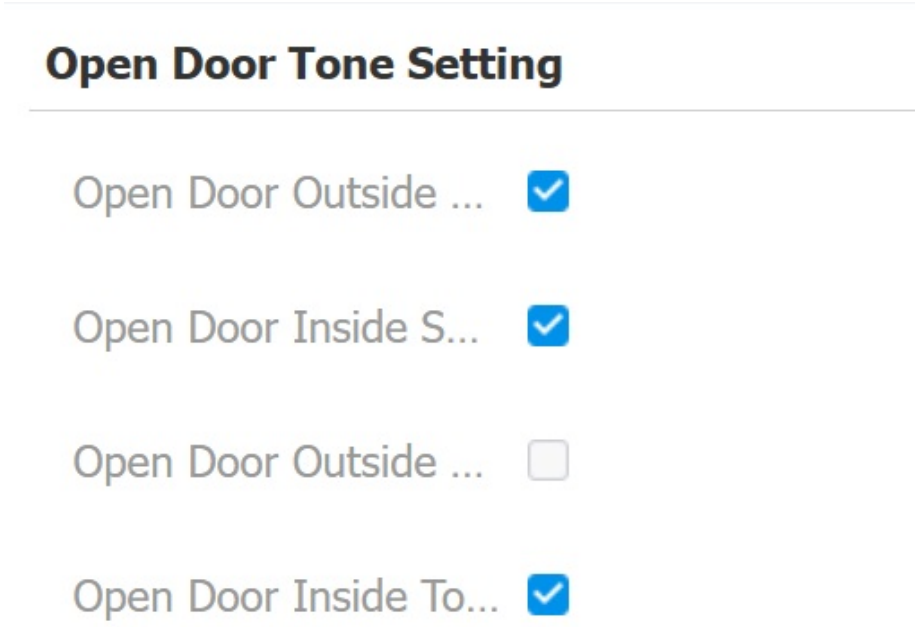


Parameter Set-up:

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

Open Door Tone Configuration

You can enable or disable various types of open door tones on the web **Phone > Audio > Open Door Tone Setting** interface.



Parameter Set-up:

- **Open Door Outside Succeeded Text Prompt**: tick the check box if you want to see the text prompt after the door opening success via access methods.
- **Open Door Inside Succeeded Text Prompt**: tick the check box if you want to see the text prompt after the door opening success via pressing an exit button.
- **Open Door Outside Tone**: enable it so that you can hear the open door tone when you open the door using the access method on the door phone.
- **Open Door Inside Tone**: enable it so that you can hear the open door tone when you open the door by pressing the exit button.

You can also configure the open door warning tone on the web **Intercom > Advanced > Open Door Warning** interface,

Upload Open Door Tone

You can not only enable or disable the open door tones but also upload them in batch on the web **Phone > Import/Export > Upload Tone** interface. Click **Reset** to clear the uploaded files.

Upload Tone (.wav)

ID	Type	Select File	Import	Reset
1	Open Door Outside	Not selected any files Select File	Import	Reset
2	Open Door Inside	Not selected any files Select File	Import	Reset

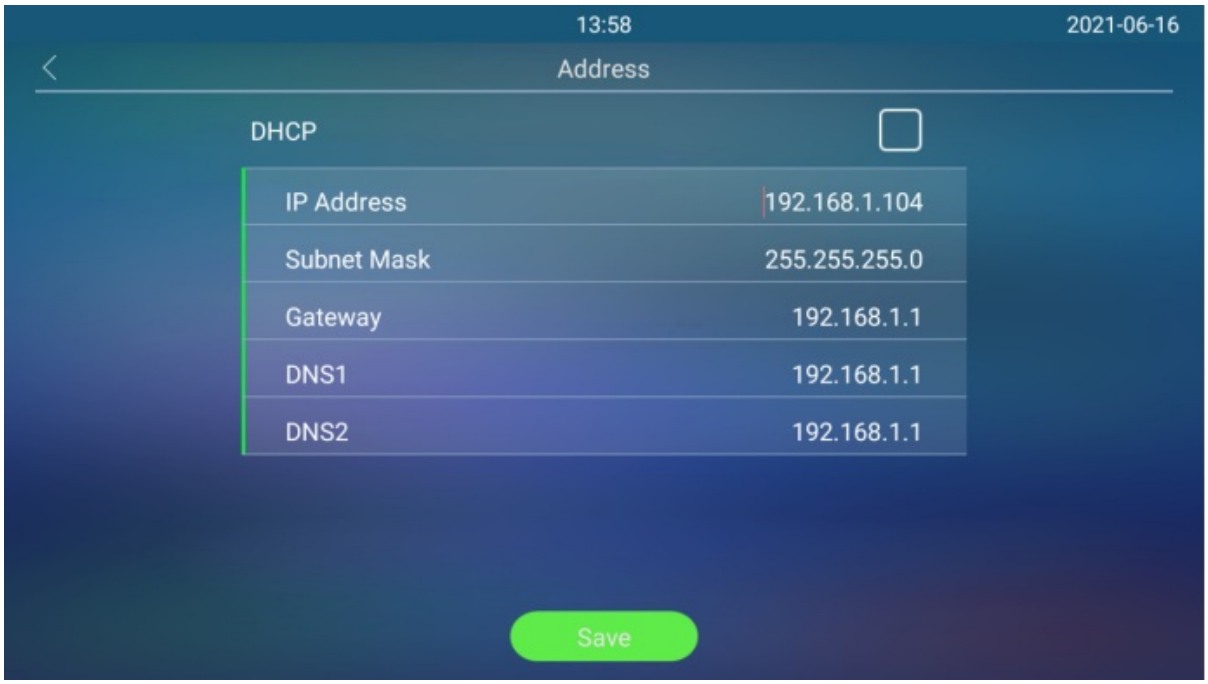
Reset All

Network Setting

Device Network Configuration

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

To configure it on the device **Setting > Address** screen.

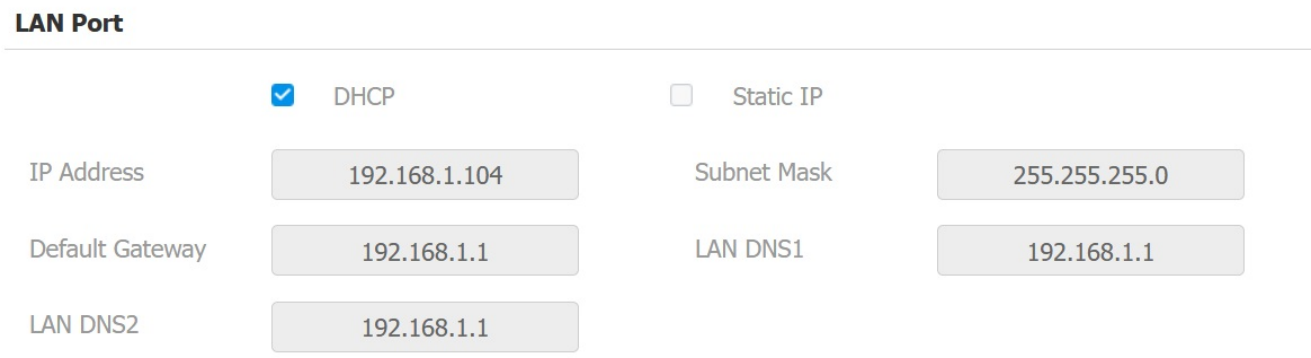


Parameter Set-up:

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

- **Preferred&Alternate DNS Server**: set up preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. DNS 1 is the primary DNS server address while the DNS 2 is the secondary one, and the door phone will connect to the secondary server when the primary DNS server is unavailable.

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



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.

To do the configuration on the web **Network > Advanced > Local RTP** interface.

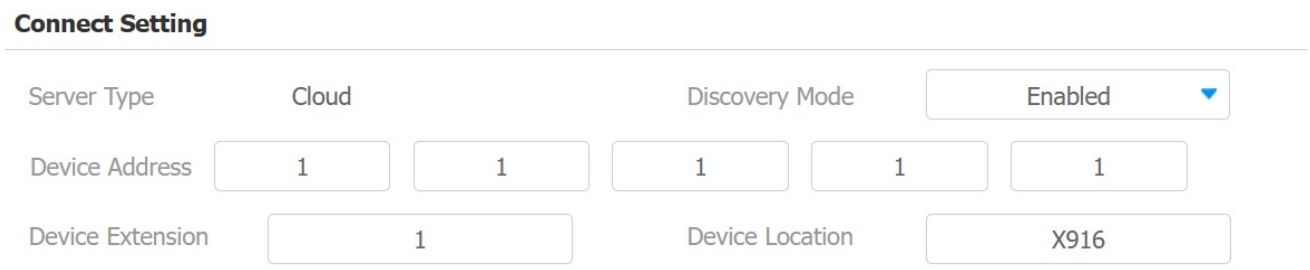
Parameter set-up:

- **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 end point 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.

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



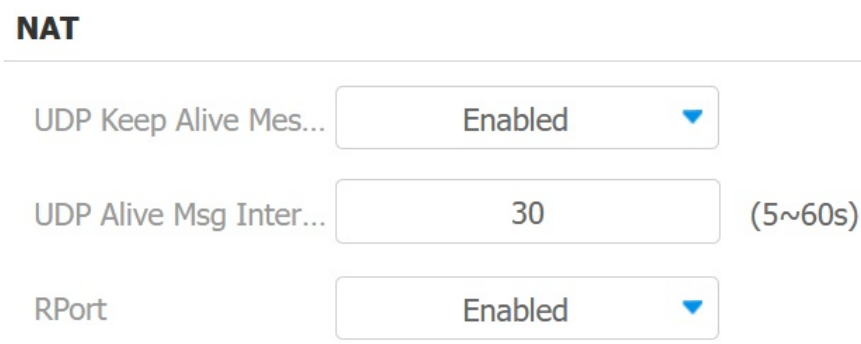
Parameter Set-up:

- **Server Type**: It is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type. Therefore, you are allowed to choose **Cloud** or **SMDC** in discovery mode.
- **Discovery Mode**: select **Enabled** to turn on the discovery mode of the device so that it can be discovered by other devices in the network.
- **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 to distinguish it from others.

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.

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



Parameter Set-up:

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

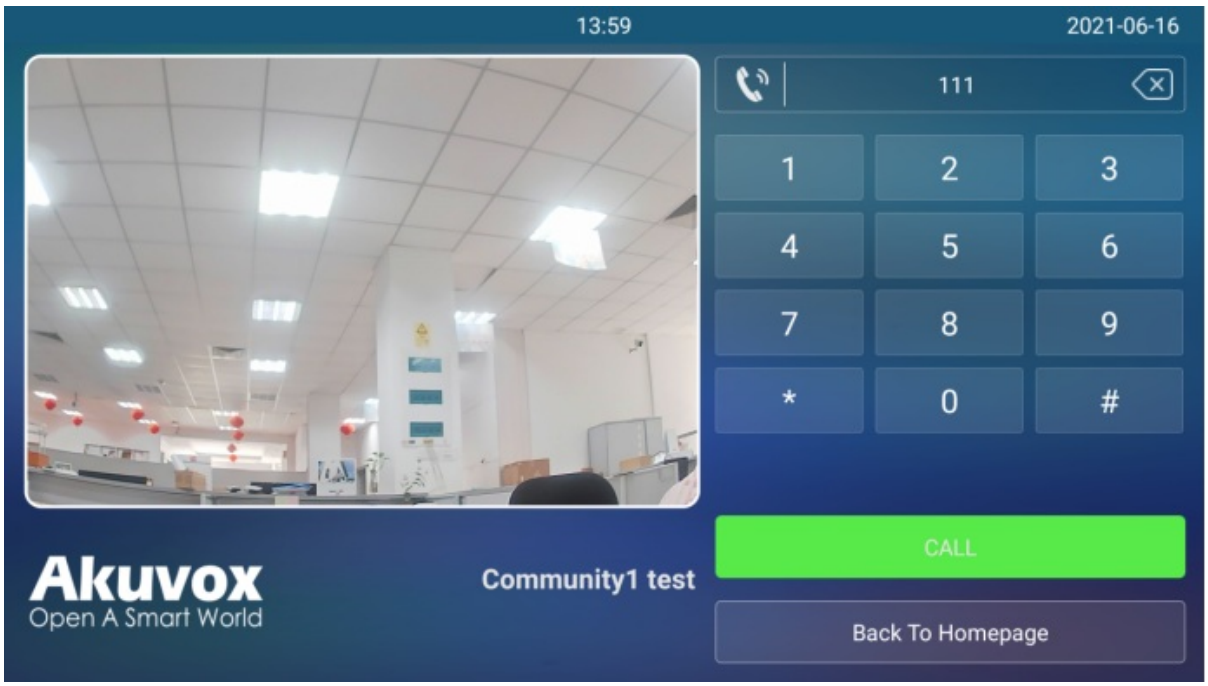
Intercom Call Configuration

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.

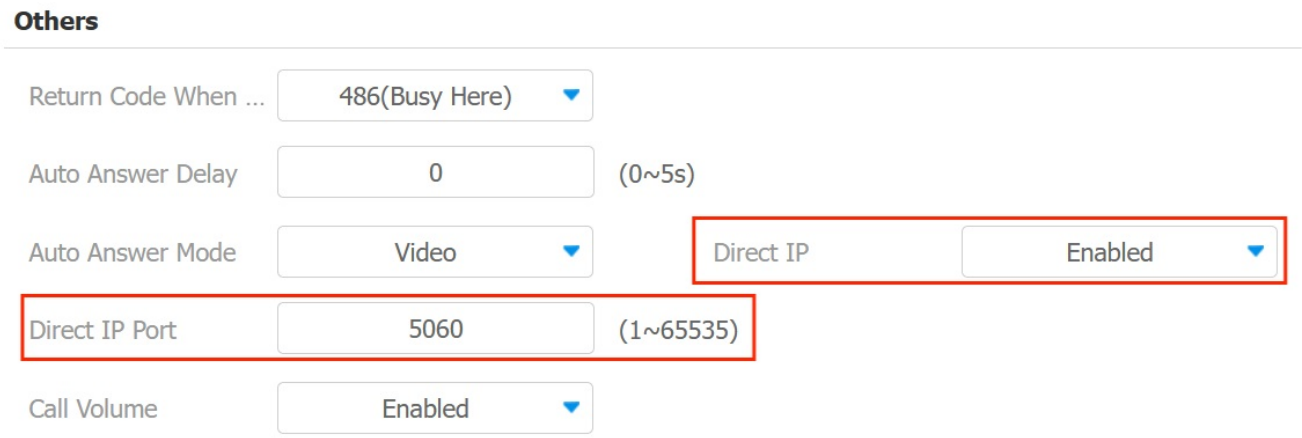
Make IP Calls

To make SIP calls or IP calls on the device by entering number on the dial pad.



IP Call Configuration

To configure the direct IP call on the device **Phone > Call Feature > Others** interface.



Parameter Set-up:

- **Direct IP Port**: the direct IP Port is 5060 by default with the port range from 1-65535. And you enter any values within the range other than 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

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.

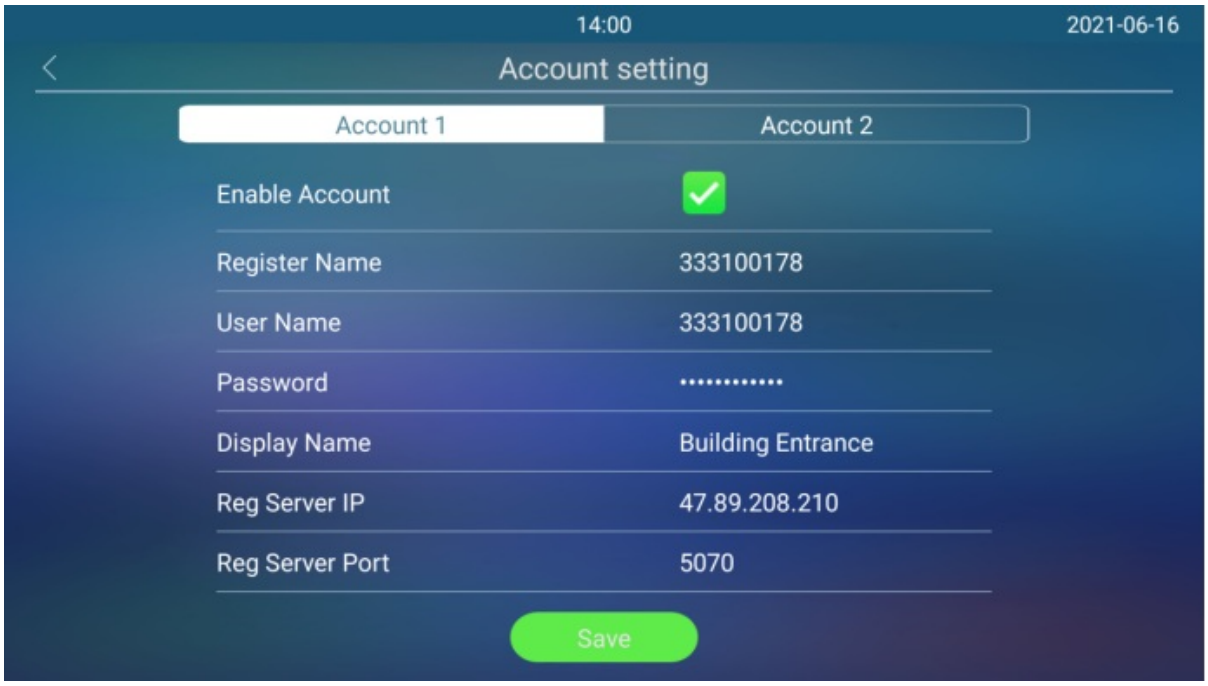
SIP Account Registration

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 Device

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



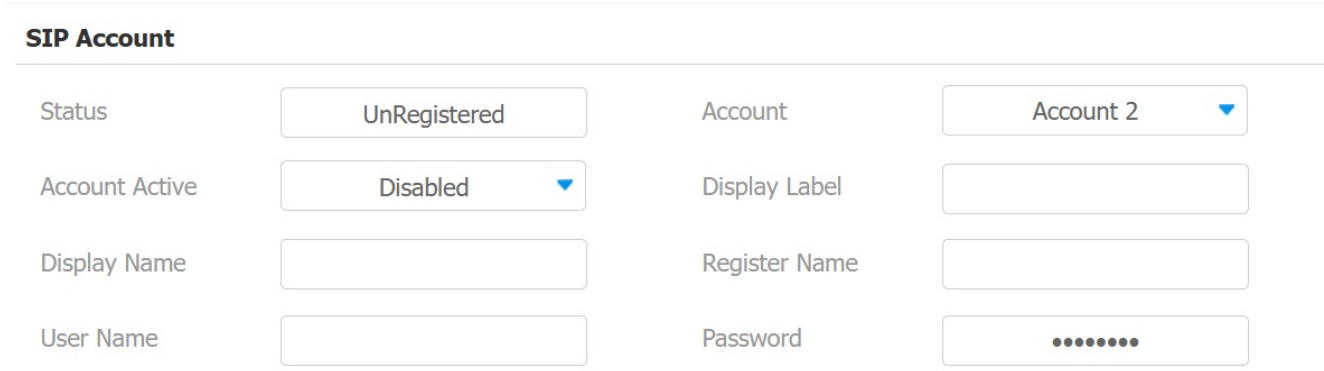
Parameter Set-up:

- **Account1/Account2**: select Account1 or Account2. Account 1 is the default SIP account.
- **Enable Account**: check to activate the registered SIP account.
- **Display Name**: configure the device's name to be shown on the device being called to.

a. To register SIP account for Akuvox indoor monitors, obtain **Register Name, Username, Password, Server IP**, and **Server Port** from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain **Register Name, Username, Password, Server IP**, and **Server Port** from third-party service provider.

Configure SIP Account on the Web Interface

To register the SIP account on the web **Account > Basic > SIP Account** interface.



Parameter Set-up:

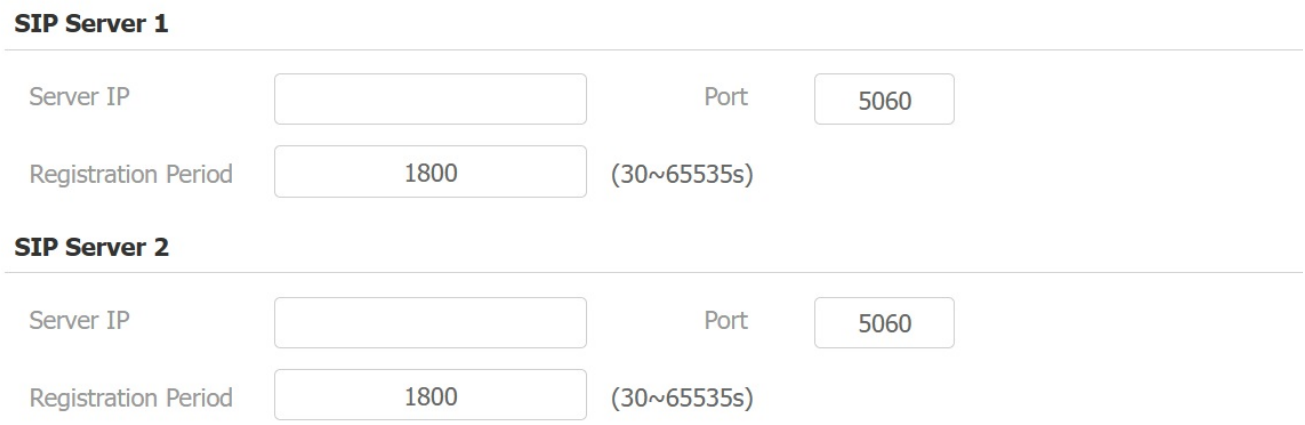
- **Status**: displays the registration status of the account.
- **Account**: select Account 1 or Account 2. Account 1 is the default SIP account.
- **Account Active**: check to activate the registered SIP account.
- **Display Label**: configure the device label to be shown on the device screen.
- **Display Name**: configure the device's name to be shown on the device being called to.

a. To register SIP account for Akuvox indoor monitors, obtain **Register Name, Username,** and **Password** from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain **Register Name, Username**, and **Password** from third-party service provider.

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.

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



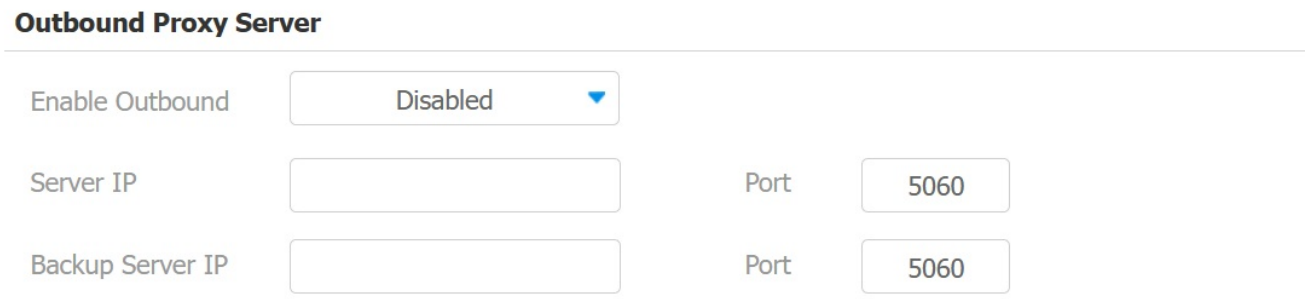
Parameter Set-up:

- **SIP Server 1**: enter the primary server IP address or its URL.
- **SIP Server 2**: enter the backup server IP address or its URL.
- **Port**: set up SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is **1800**, ranging from **30-65535**s.

Configure Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission.

To configure it on the web **Account > Basic > Outbound Proxy Server** interface.



Parameter Set-up:

- **Server IP**: enter the SIP address of the primary outbound proxy server.
- **Backup Server IP**: set up backup server IP for the backup outbound proxy server.
- **Port**: enter the port number for establishing call session via the primary/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**.

To configure it on the web **Account > Basic > Transport Type** interface.

Parameter Setup:

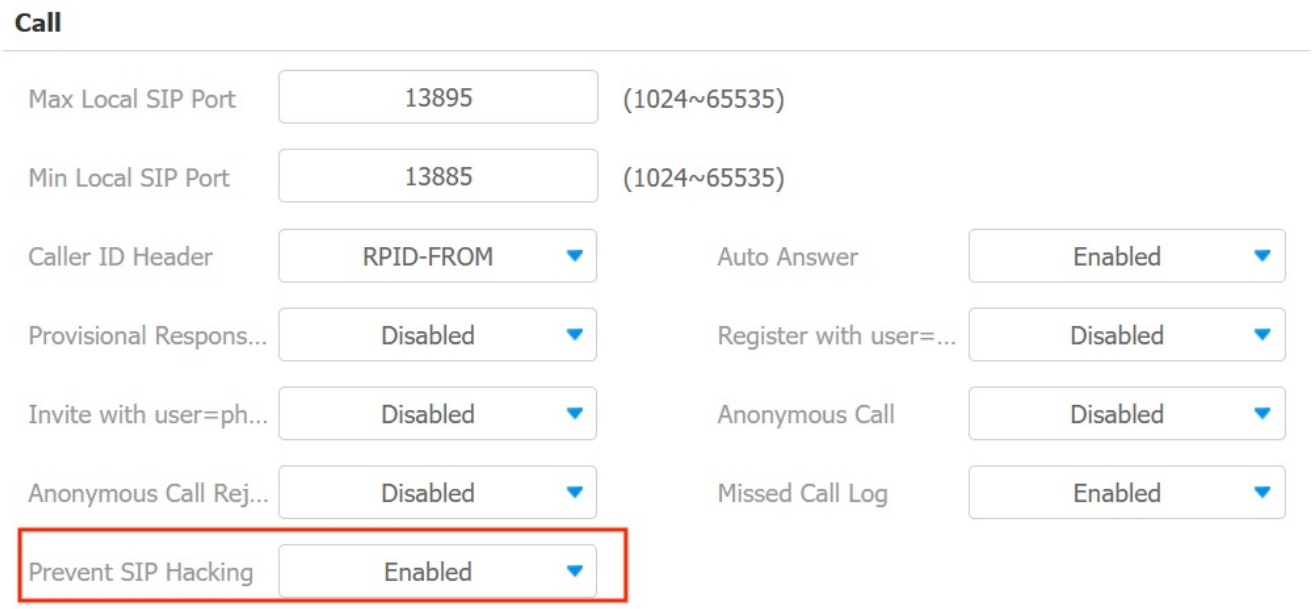
- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for Reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for Secured and Reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain DNS record for specifying the location of servers. And SRV not only records the server address but also the server port. Moreover, SRV can

also be used to configure the priority and the weight of the server address.

SIP Hacking Protection

Internet phone eavesdropping is a network attack that allows unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls from being compromised on the Internet.

Navigate to **Account > Advanced > Call** interface.

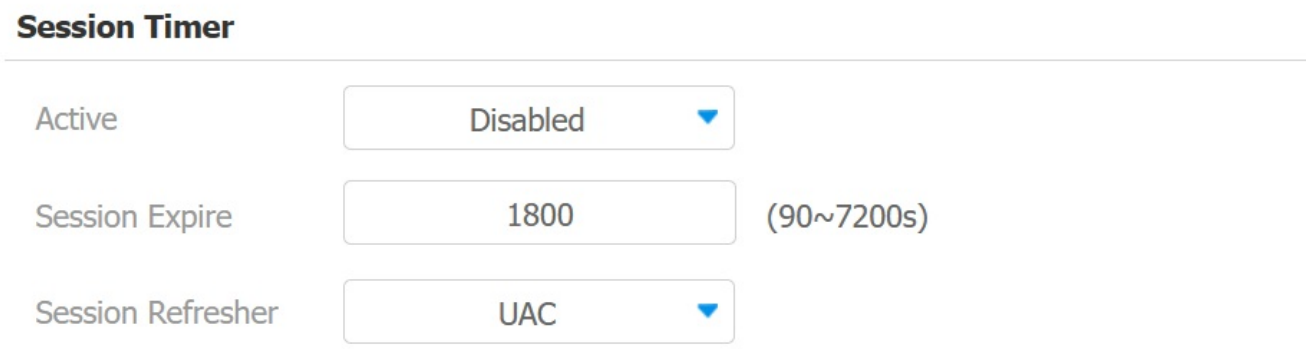


Call Session Timer

SIP does not have a built-in way to keep track of active sessions. While the user agent can figure out if a session has timed out using its own specific method, the proxy server lacks this capability. As a result, the proxy server may not always know if a session is still ongoing. For instance, if a user agent fails to send a BYE message at the end of a session or if the BYE message gets lost due to network issues, the proxy server won't be aware that the session has ended. Consequently, the proxy server will continue to hold the call status without knowing if it's still valid.

To address this problem, RFC4028 introduces a survival mechanism for SIP sessions. Either the user agent or the proxy server periodically sends re-INVITE or UPDATE requests to keep the session active. The interval between these update requests is determined by the negotiation mechanism defined in the session. If no update request is received within the specified interval, the session is considered terminated.

To do the configuration on the web **Account > Advanced > Session Timer** interface.



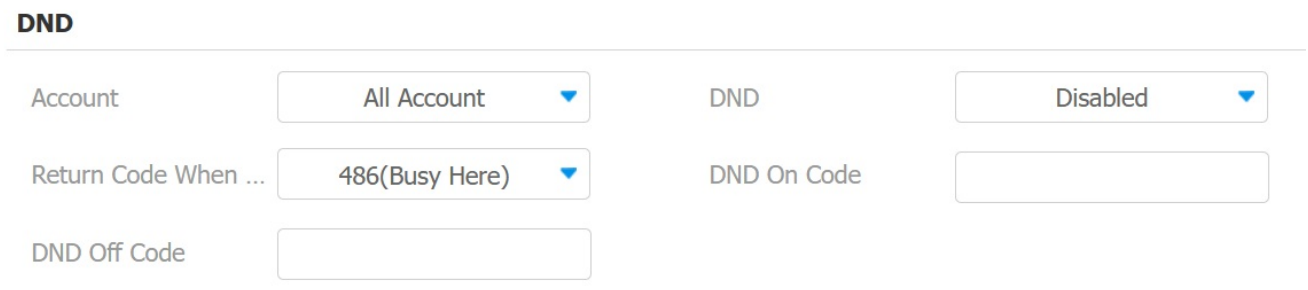
Parameters Set-up:

- **Active**: call session timer is disabled by default.
- **Session Expire**: enter the session call duration before the call expires or ends automatically for refreshment. For example, if you set the session expiration as 1800 seconds (Ranging from 90- 7200 sec) you can have the door phone to terminate the ongoing call with another intercom device in 1800 seconds.
- **Session Refresher**: select UAC (**User Agent Client**) or UAS (**User Agent Server**) for the call session refreshment.

DND 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.

To configure it on the web **Phone > Call Feature > DND** interface.



Parameter Set-up:

- **Account**: select the account that applies DND.
- **Return Code When DND**: select what code should be sent to the calling device via SIP server. **404 for Not Found; 480 for Temporarily Unavailable; 486 for Busy Here**.
- **DND On Code**: turn on the DND on server using the code obtained. The DND On Code

is **78** by default.

- **DND Off Code**: turn off the DND on server using the code obtained. The DND Off Code is **79** by default.

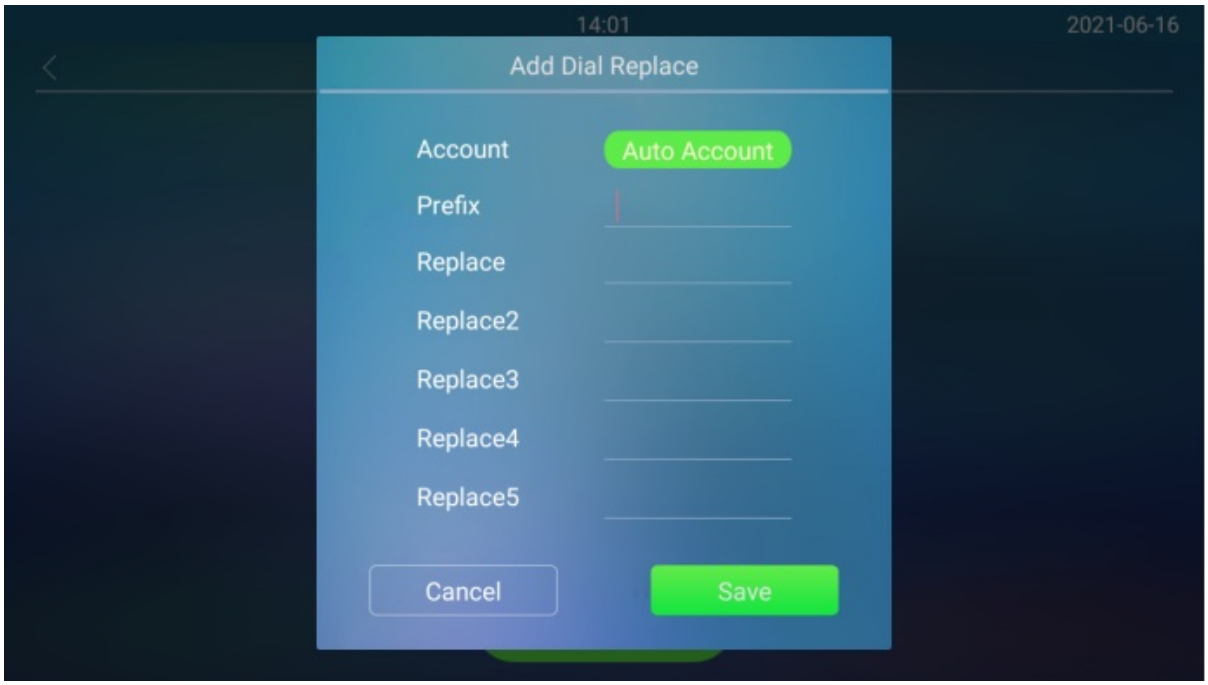
Dial Options Configuration

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 Device

To configure it on the device **Setting > Replace Rule** screen.



Parameter Set-up:

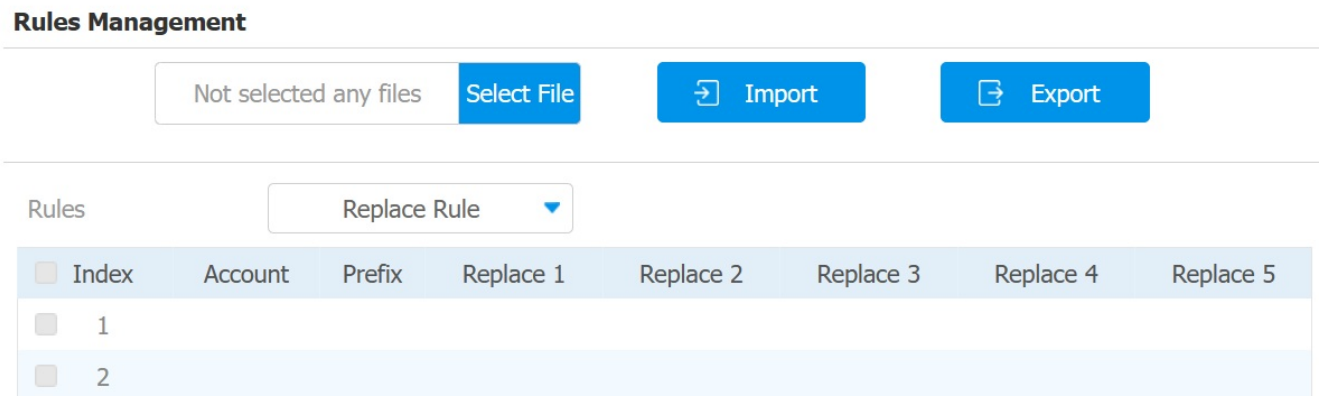
- **Account**: select the account to which you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the dial number has been registered). You can select either account 1 or account 2 from which the number can be dial out. if you have registered the dial number in both Account 1 and Account 2, then the number will be called out from Account 1 by default.
- **Prefix**: enter the short number to replace the dial number you wish to replace.

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

Quick Dial by Number Replacement on the Web Interface

You can not only add a quick dial number separately but also import the quick dial number to the device in batch. Besides, you can edit and delete the numbers if needed.

To configure it on the web **Phone > Dial Plan > Rules Management** interface.

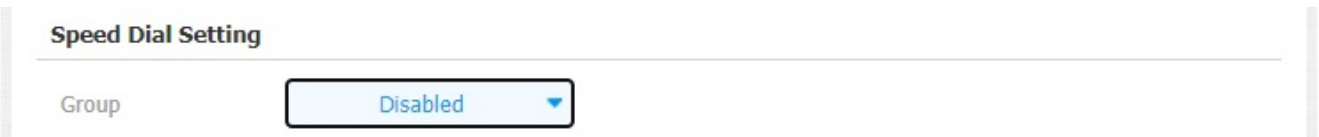


Note:

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

Group Speed Dial

The device allows you to make speed dial to the contacts in one contact group. When you press the **Reception** icon on the door phone, you can dial the all contact numbers in the group at the same. You can navigate to **Intercom > Key/Display > Speed Dial Setting** interface.



Parameter Set-up:

- **Group**: select **Disabled** to disable the speed dial function. And select the specific contact

group if you want to make speed dial to the contacts in the selected contact group.

Hang Up After Open Door

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

To do this configuration on the web **Intercom > Basic> Hang Up After Open Door** interface.

Parameter Set-up:

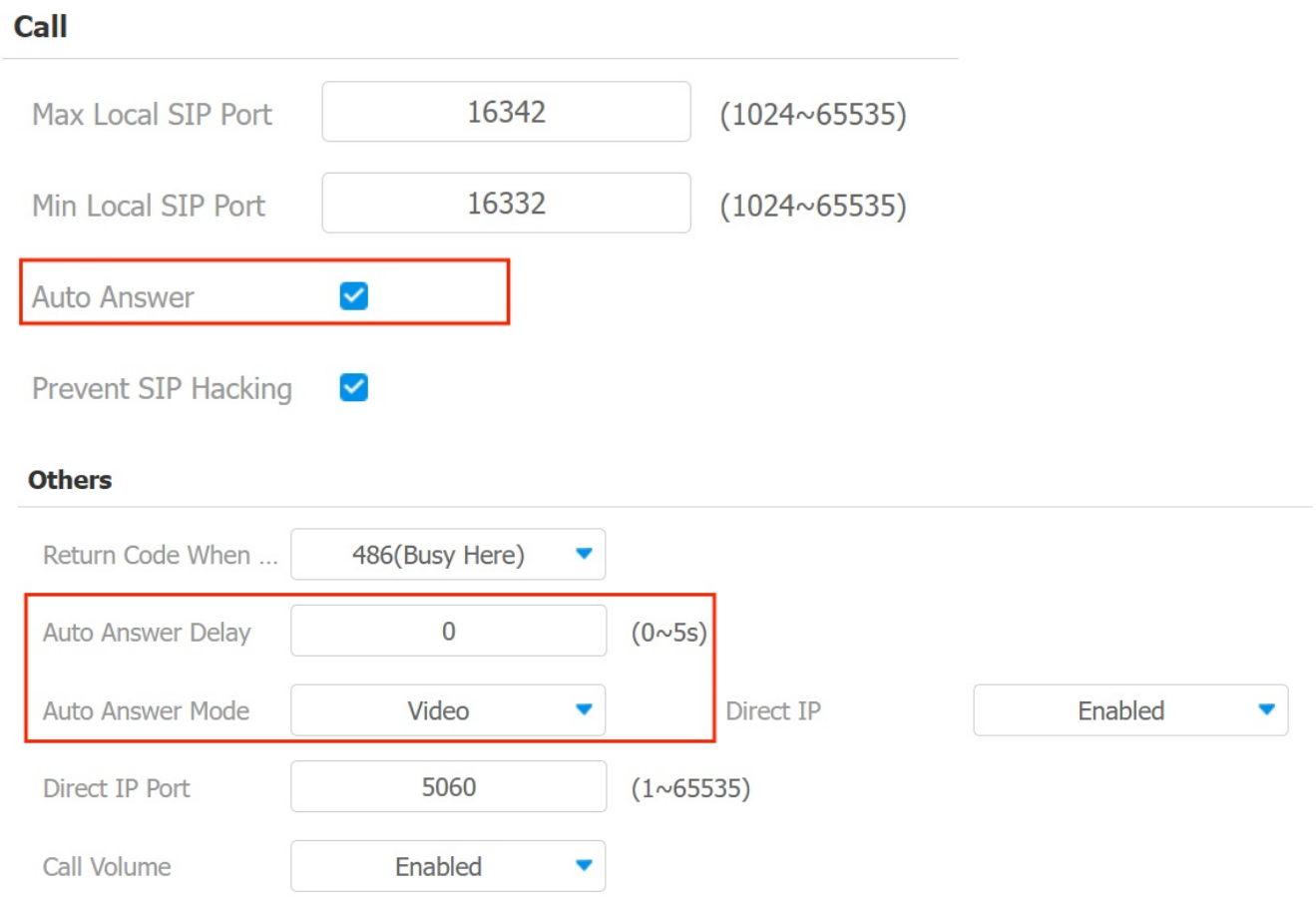
- **Timeout**: set up from 1 second to 15 seconds. 5 seconds is the default. If you set it 5 seconds, then the call will be hung up 5 seconds after the door is opened. If you want to disable the feature, set the timeout as 0.

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 set it up on the web **Phone > Call Feature > Auto Answer** interface.



Parameter Set-up:

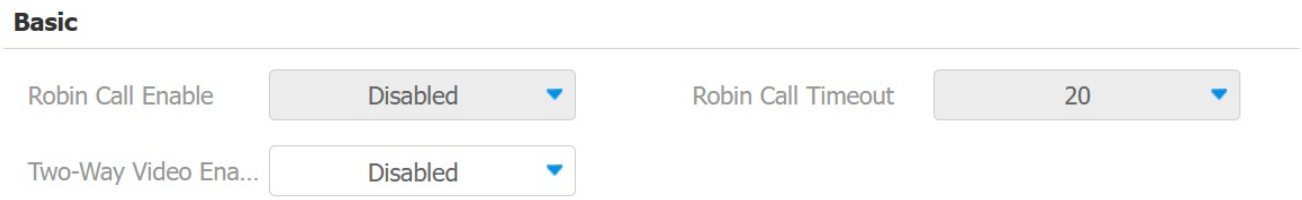
- **Auto Answer Delay**: set up the delay time (from 0-5 Sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Auto Answer Mode**: set up the video or audio mode you preferred for the automatic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

answering.

Robin 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.

To configure it on the web **Intercom > Basic > Basic** interface.



Parameter Set-up:

- **Timeout (Sec)**: click to select the call time interval in between the Robin call number in a targeted Robin Call group. For example, if you set the time interval as 10 seconds, then the call (if not answered in 10 Sec.) will be terminated automatically and be transferred sequentially to the next robin call number in the targeted robin call group.
- **Two-Way Video Enabled**: this feature allows for visual connection with both callers and recipients via the door phone, providing a more interactive and secure conversation.

Note:

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

Maximum Call Duration Setting

The door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the call automatically.

To configure it on the web **Intercom > Basic > Max Call Time** interface.

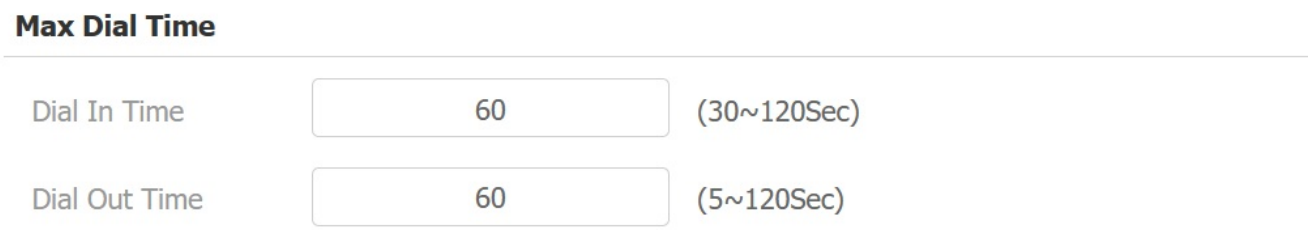
Parameter Set-up:

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

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.

To configure it on the web **Intercom > Basic > Max Dial Time** interface.



Parameter Set-up:

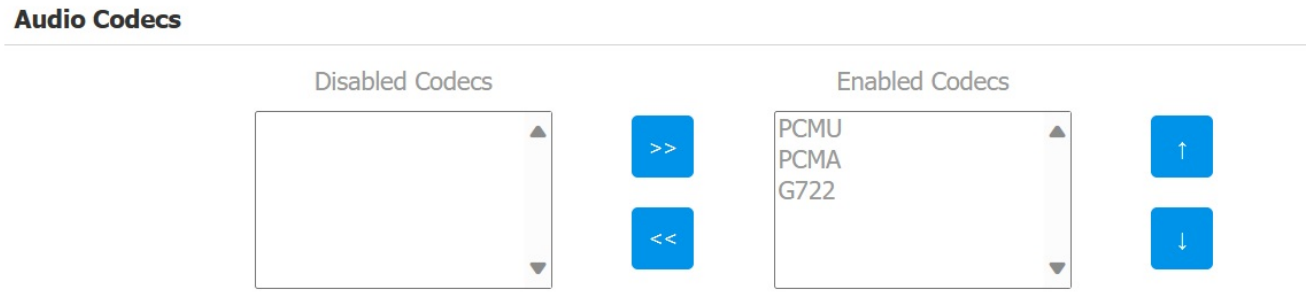
- **Dial In Time**: enter the dial in time duration for you door phone (ranging from 30-120 Sec.) for example, if you set the dial in time duration as 60 seconds in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial in time duration by default.
- **Dial Out Time**: enter the dial in time duration for your door phone (ranging from 5-120 Sec.) for example, if you set the dial out time duration as 60 seconds in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answered by the device being called.

Audio & Video Codec Configuration

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.

To configure it on the web **Account > Advanced > Audio Codecs** interface.



Please refers to the bandwidth consumption and sample rate for the codecs 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.

To configure it on the web **Account > Advanced > Video Codec** interface.

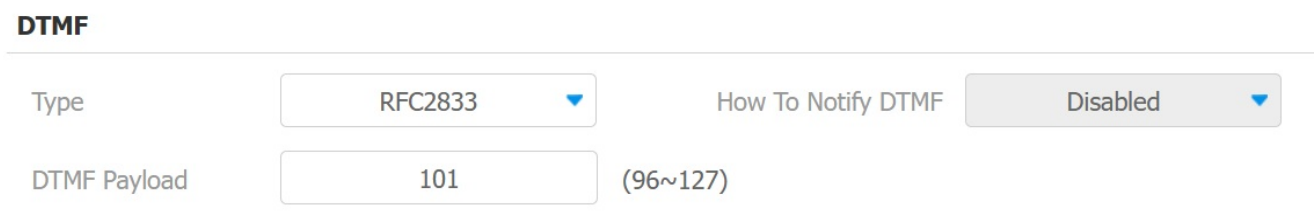
Parameter Set-up:

- **Codec Resolution**: select the code resolution for the video quality among options: **QCIF, CIF, VGA, 4CIF** and **720P** according to your actual network environment. The default code resolution is **4CIF**.
- **Codec Bitrate**: select the video stream bit rate (Ranging from 128-2048). The greater the bitrate, the data transmitted in every second is greater in amount therefore the video will be clearer. The default code bitrate is 2048.
- **Codec Payload**: select the payload type (ranging from 90-119) to configure 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.

To configure it on the web **Account > Advanced > DTMF** interface.



Parameter Set-up:

- **Type**: select DTMF mode among options: **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 **Disabled**, **DTMF**, **DTMF-Relay**, and **Telephone-**

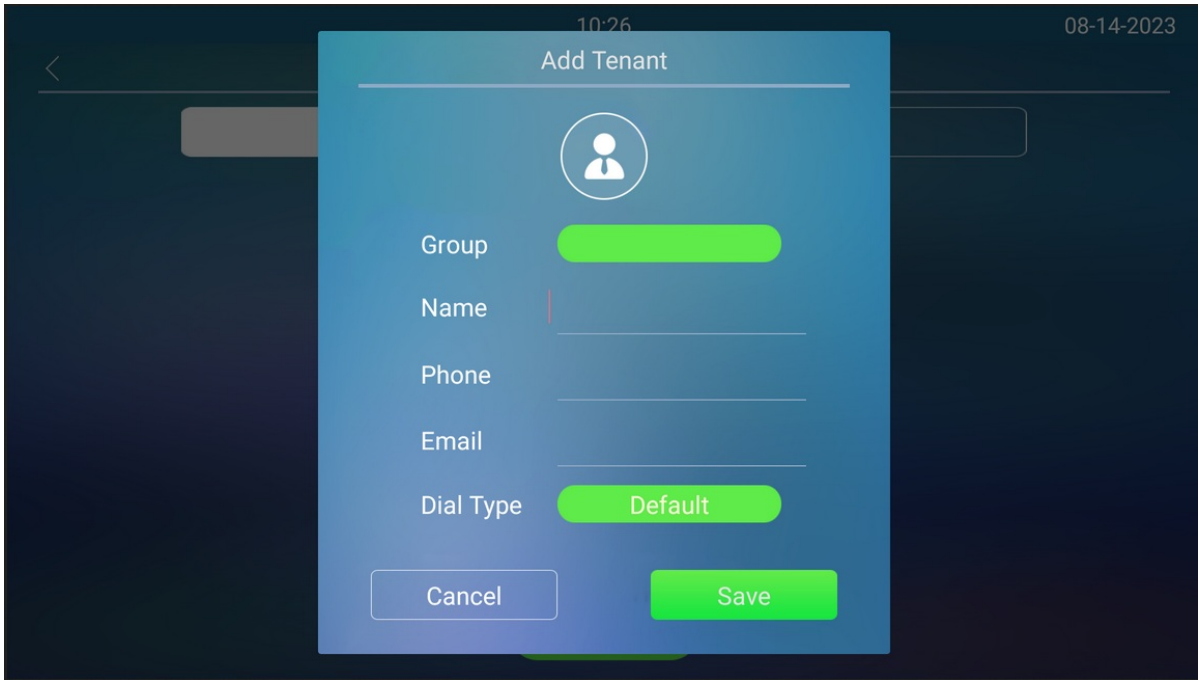
Event according to the specific type adopted by the third-party device. You are required to set it up only when the third-party device to be matched with adopts **Info** mode.

- **DTMF 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 Device

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



Parameter Set-up:

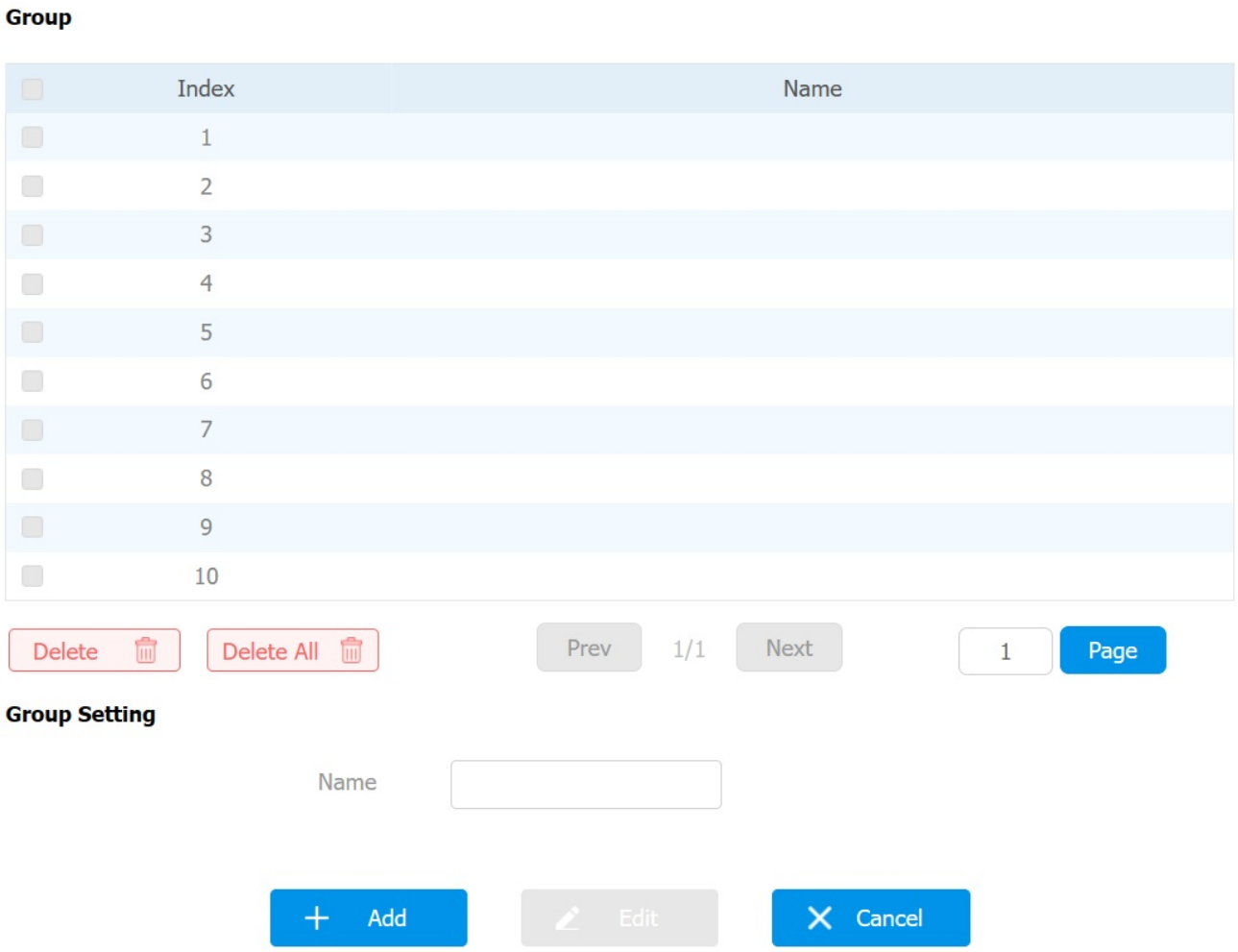
- **Group**: click the green tab to select the group name you have created. You cannot select the group name If no group name has been created.
- **Dial Type**: select and assign the group name to an account. If you select default option, then the contact number will be called out from SIP account 1 if the contact number are set up in both SIP account 1 and 2.

Note:

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

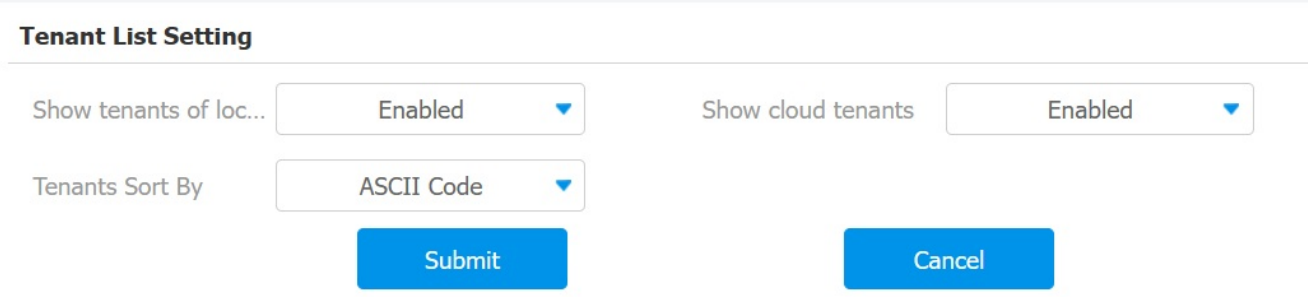
Manage Contact Groups on the Web Interface

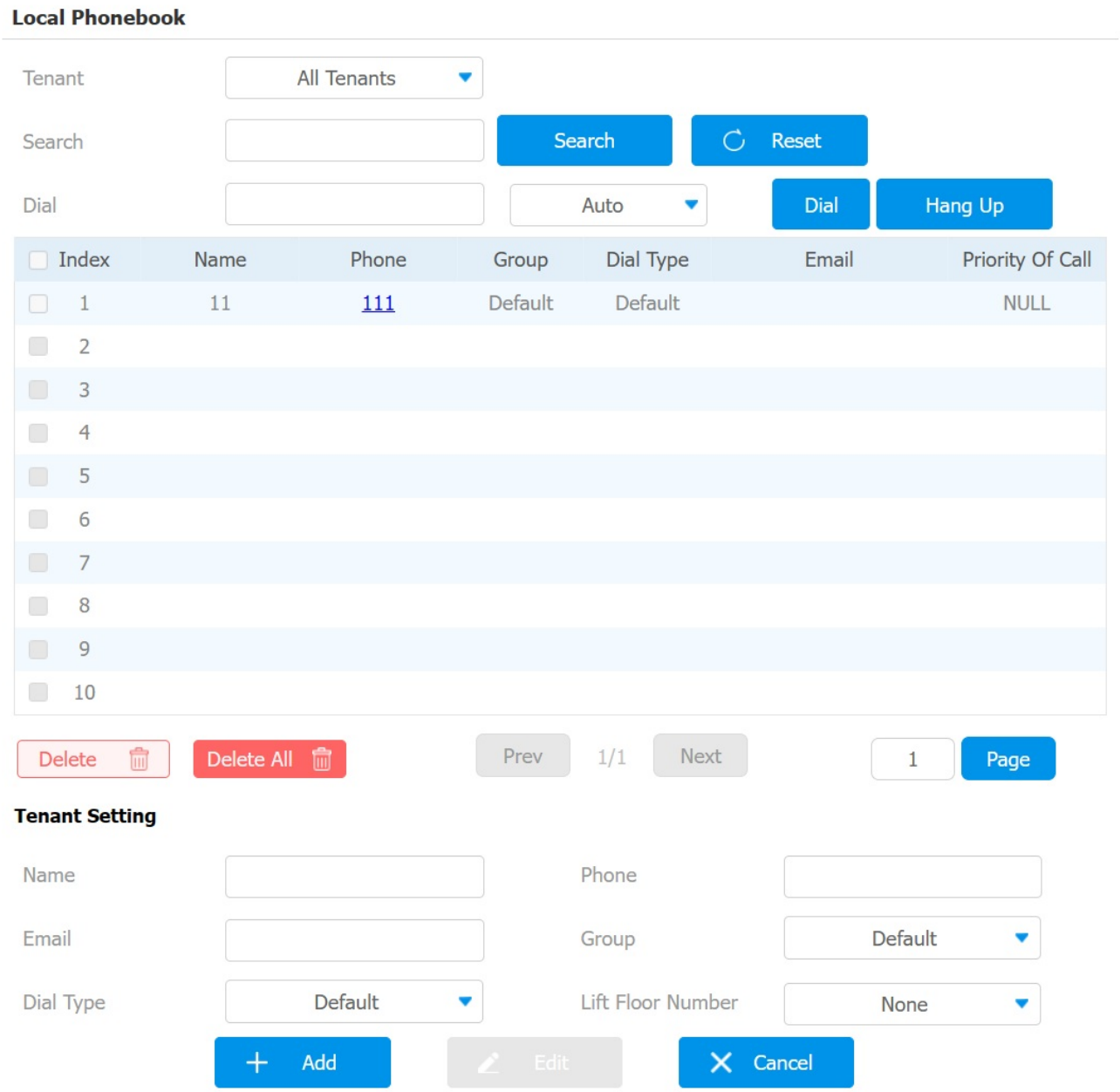
You can configure contact groups by adding and editing them on the web **PhoneBook > Phonebook > Group** interface.



Contact List Configuration on the Web Interface

Contacts can also be configured on the web interface where you can also upload the contact pictures if needed. To configure it on the web **PhoneBook > Phonebook** interface.



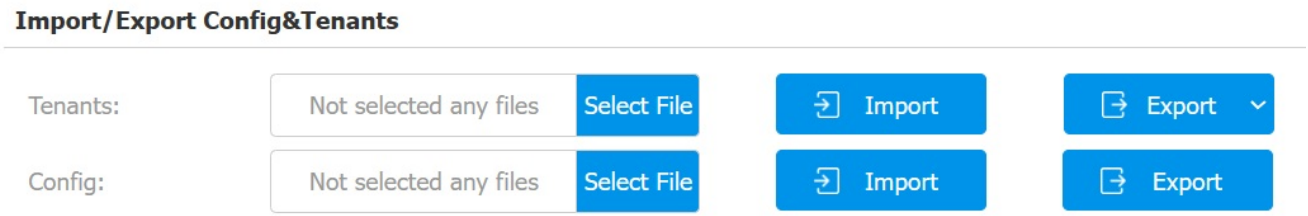


Parameter Set-up:

- **Show cloud tenants**: enable it to show the contacts issued from Akuvox SmartPlus.
- **Tenants Sort By**: there are three options **ASCII Code, Room Number** and **Import**. If **ASCII Code** is selected, sort in ascending ASCII order, for example: 0-9, a-z, numbers take precedence over letters. Not case sensitive, but the same letter, lowercase is sorted before uppercase. If **Room Number** is selected, sort by room name. if there is no room name, the room number is taken as the room name by default. Room number is available after enable Cloud contact. If **Import** is selected, sort by contacts in the imported file.
- **Tenant**: you can choose to show all contacts information or one group contact information.
- **Search**: enter the key number or key letter of the name to quick search the contact.
- **Dial**: enter a phone number, then click **Dial** to initiate the call from the web.

- **Group**: select the desired group name you have created.
- **Dial Type**: select which SIP account will be used to call out. If using IP direct call, it is not available.
- **Priority of Call**: set the priority of call among four options: **Null, Firstly, Secondary, Lastly**. This feature is mainly applicable to the contacts in a specific contact group. For example, if you set the priority of call for one of the contacts in a specific contact group as **Firstly**, then the contact will be the first to be called to among all the contacts in the same contact group when someone presses on the contact group for making a group call.
- **Lift Floor Number**: select the floor number that the tenant is allowed to access when the device is integrated with elevator controller.

You can import and export contacts on the web **Phone > Import/Export** interface.



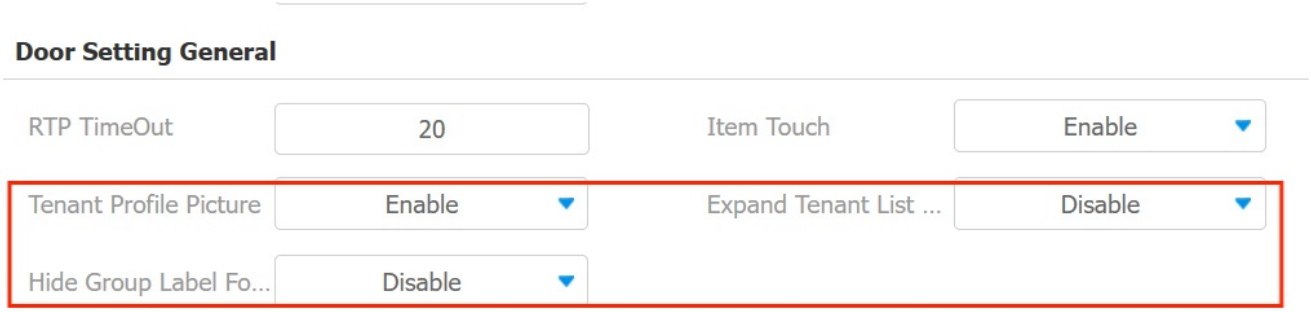
Note:

- **Priority of Call** of a contact cannot be set when the contact does not belong to any contact group.
- The contact file format for import should be in .vcf, .csv or xml format while the contact file format for export should be .vcf format only. And the maximum contact import size is 3000.

Contact List Display Setting

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

To configure it on the web **Intercom > Basic > Door Setting General** interface.



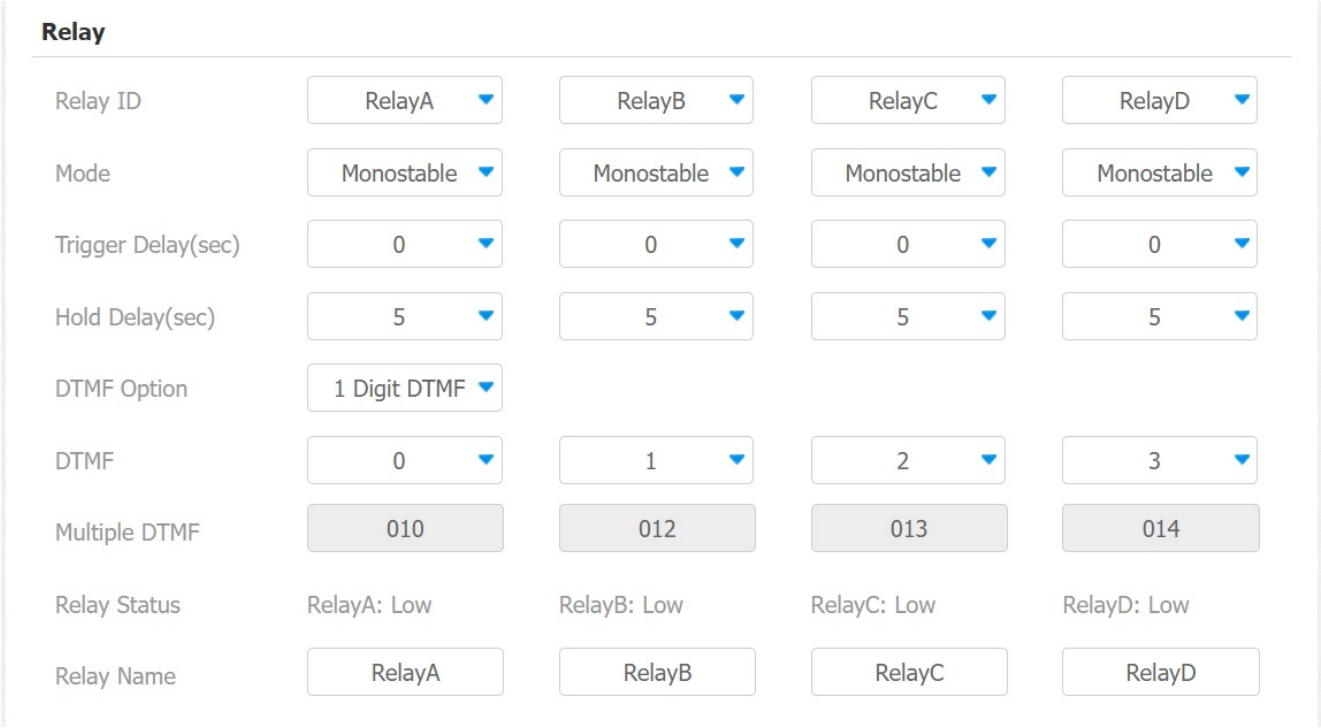
Parameter Set-up:

- **Tenants Profile Picture**: select **Enable, Disable** or **Auto**. When the function is enabled, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, the default contact icon will be displayed next to the name. When disabled, the picture or the icon will not be displayed. When the function is set as **Auto**, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, there won't be an icon next to the name.
- **Expand Contact List View Mode**: if you enable this feature, then the contact tab will be widened. And the tab will turn to normal size when you disable the feature.
- **Hide Group Label For Tenant List**: tick or untick the check box to control the display of the group label. If you untick the check box, then only the contact tab will be displayed while the group tab will be concealed and vice versa.

Door Access Control Configuration

Relay Switch Setting

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



Parameter Set-up:

- **Trigger Delay (Sec)**: set the relay trigger delay timing (Ranging from 1-10 Sec.) For example, if you set the delay time as 5 Sec. Then, the relay will not be triggered until 5 seconds after you press **Unlock** tab.
- **Hold Delay (Sec)**: set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. Then, the relay will be delayed for 5 seconds after the door is unlocked.
- **DTMF Option**: select the number of DTMF digit for the door access control (**Ranging from 1-4 digits**). For example, you can select 1-digit DTMF code or 2-digit DTMF code etc., according to your need.
- **1 Digit DTMF**: set the 1 digit DTMF code within range from (**0-9, *, and #**).
- **2~4 Digits DTMF**: set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMF Mode** is set as 3-digits.

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

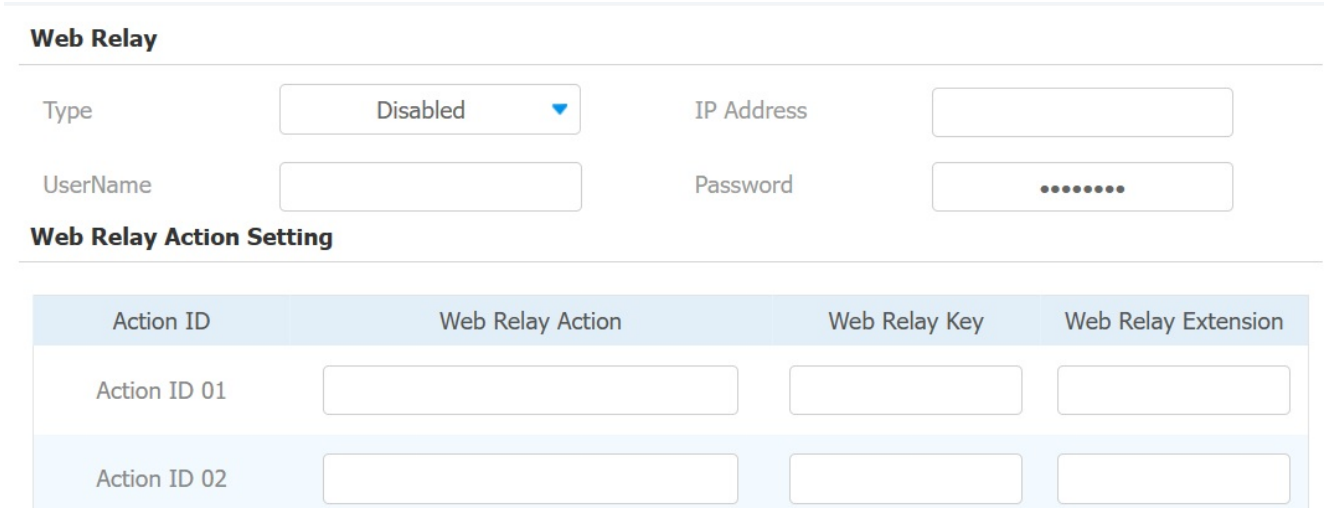
Note:

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

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.

Web relay needs to set up on the web interface where you are required to fill in such information as relay IP address, password, web relay action etc. Before you can achieve the door access via web relay. To configure it on the web **Phone > Web Relay**. Relevant parameters are provided by the web relay manufacturer.



Parameter Set-up:

- **Type**: select among three options **Disabled, WebRelay**, and **Both**. Select **Webrelay** 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 DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension**: enter the relay extension information, which can be a SIP account username of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below: **http://admin:admin@192.168.1.2/state.xml?relayState=2**.

Door Access Schedule Management

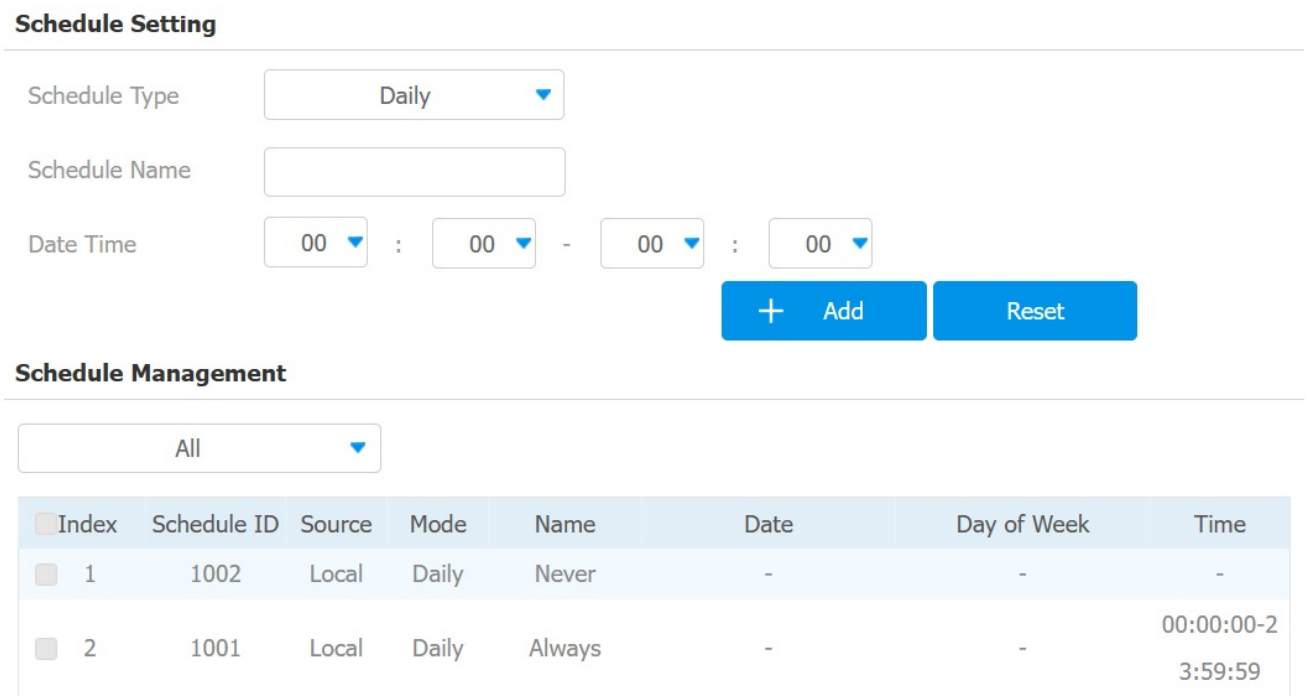
Access Schedule

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

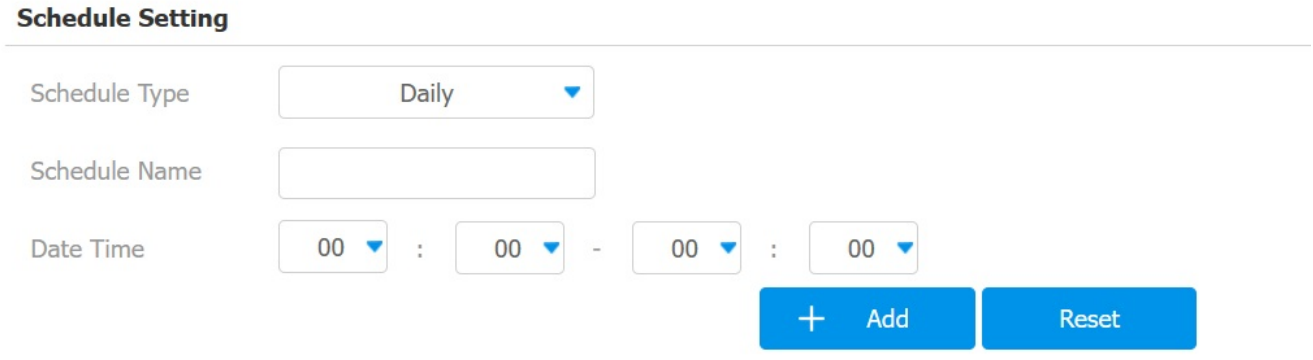
Create Access Schedule on the Web

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

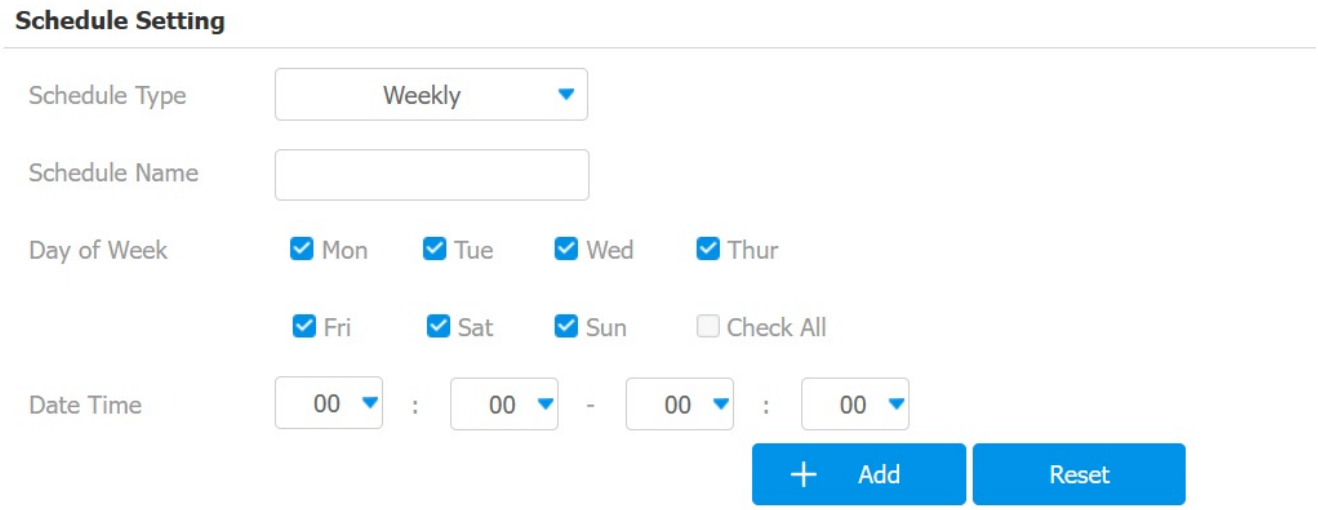
To configure it, go to **Intercom > Schedule** interface.



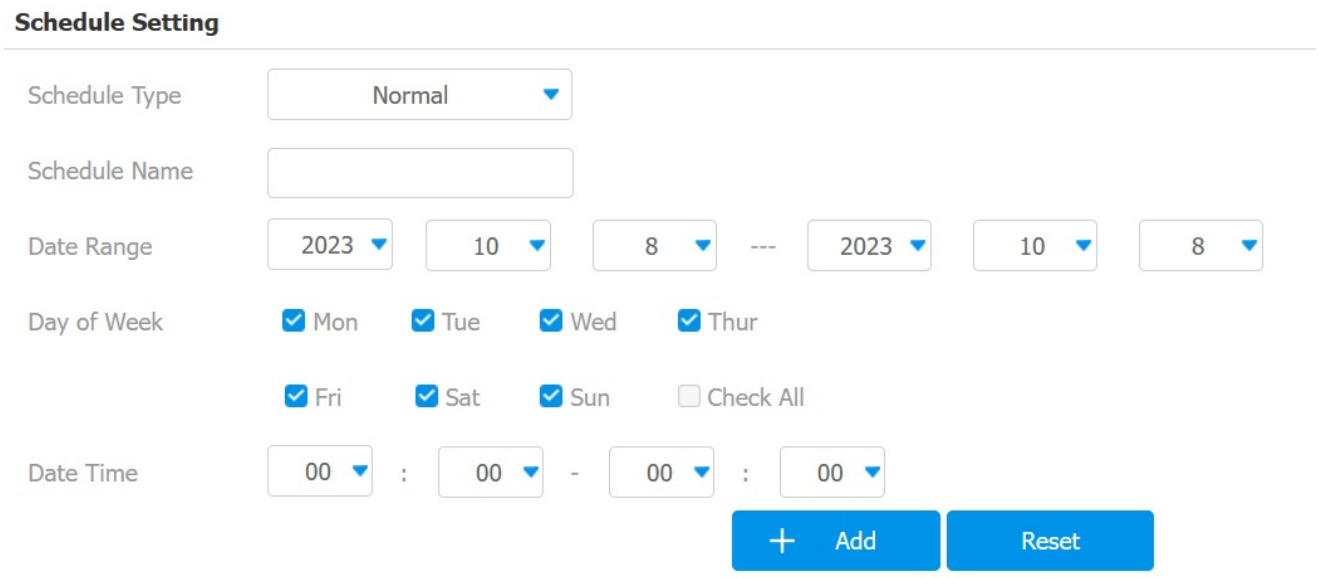
To create a daily schedule, select **Daily** in **Schedule Type**:



To create a weekly schedule, select **Weekly** in **Schedule Type**:



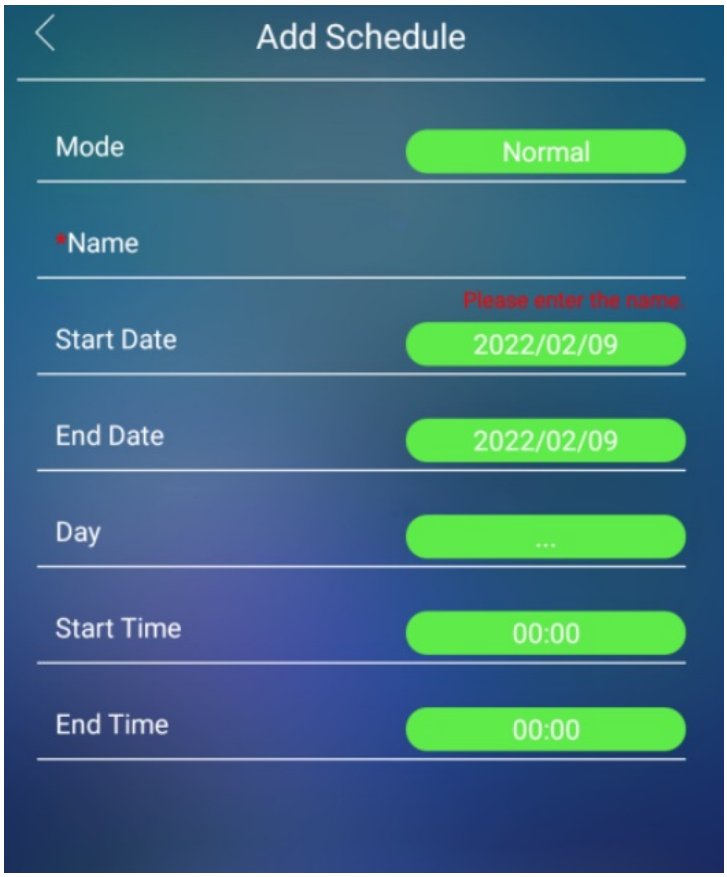
To create a longer period schedule, select **Normal** in **Schedule Type**:



Create Access Schedule on the Device

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

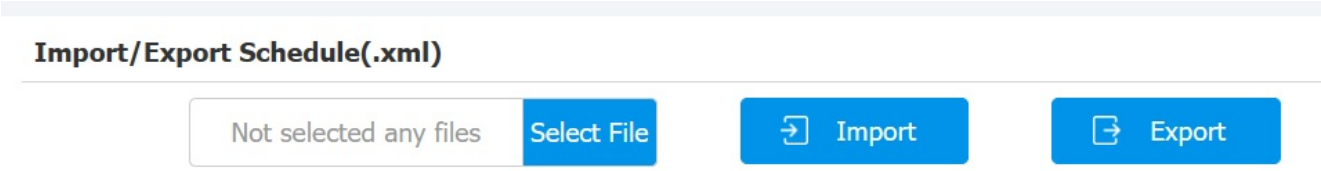
To configure it on the **Setting > Schedule** screen.



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.

To configure it on the **Intercom > Schedule** interface.



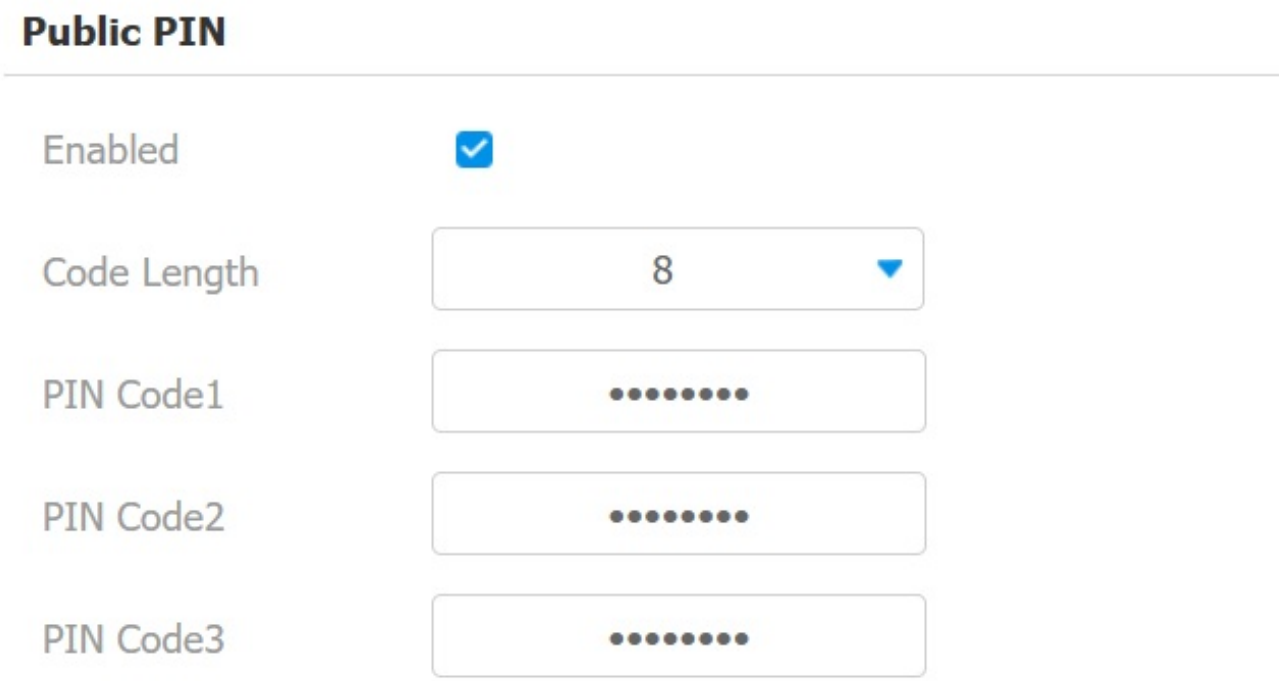
Door Unlock Configuration

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.

Configure Public PIN Code on the Web Interface

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



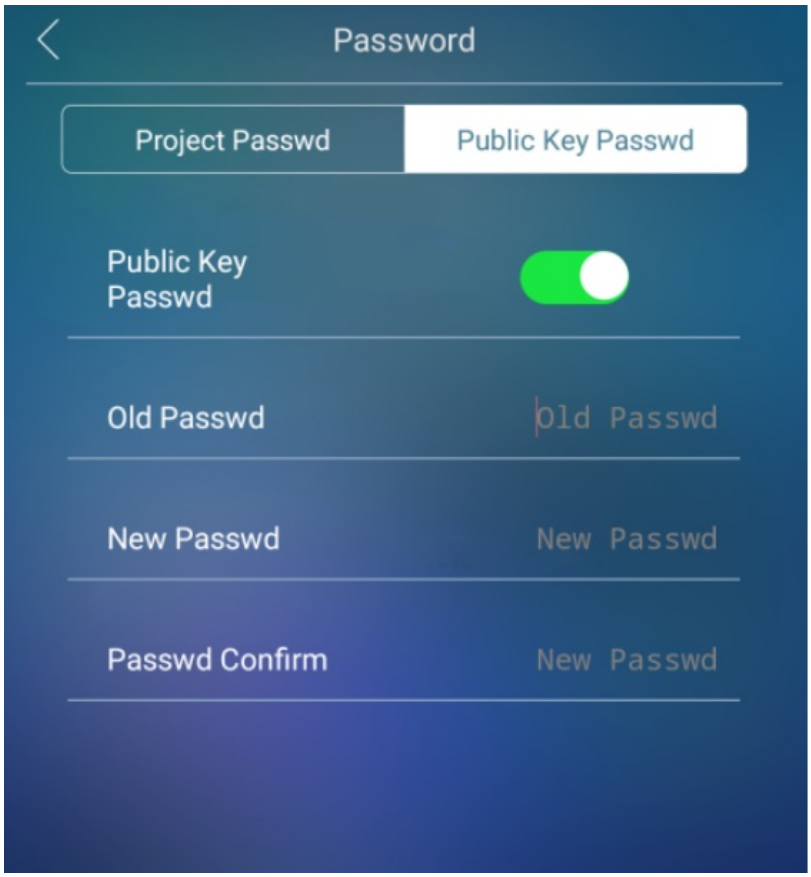
Parameter Set-up:

- **Code Length**: select the code length ranging from 4 to 8.
- **PIN Code 1/2/3**: set the desired PIN code to unlock the door.

Configure Public PIN Code on the Device

You can also set up a Public PIN code on the device.

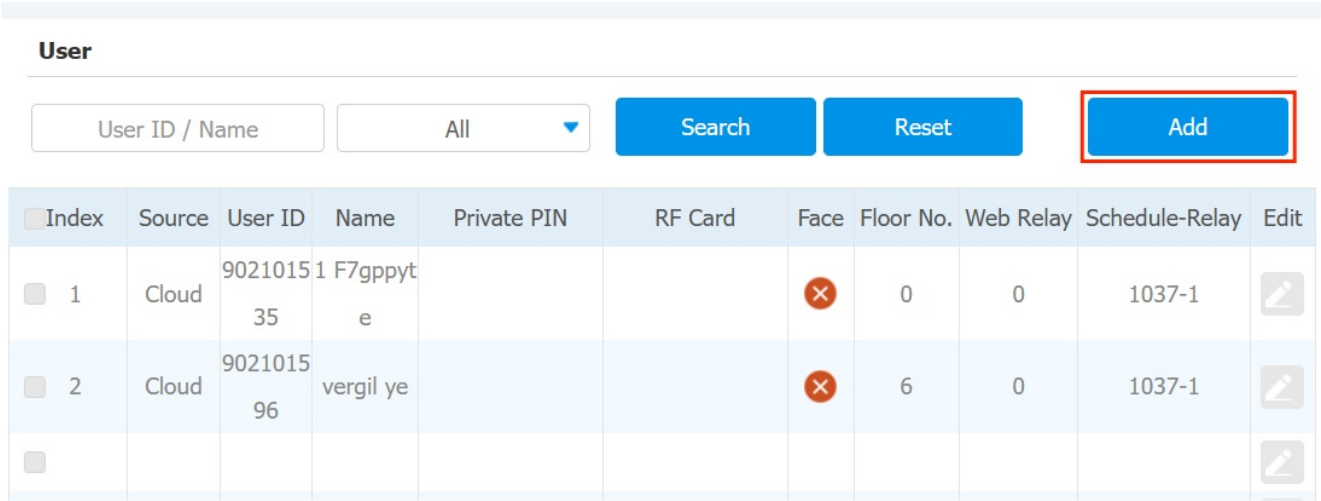
Go to **Setting > Password > Public Key Password** screen.



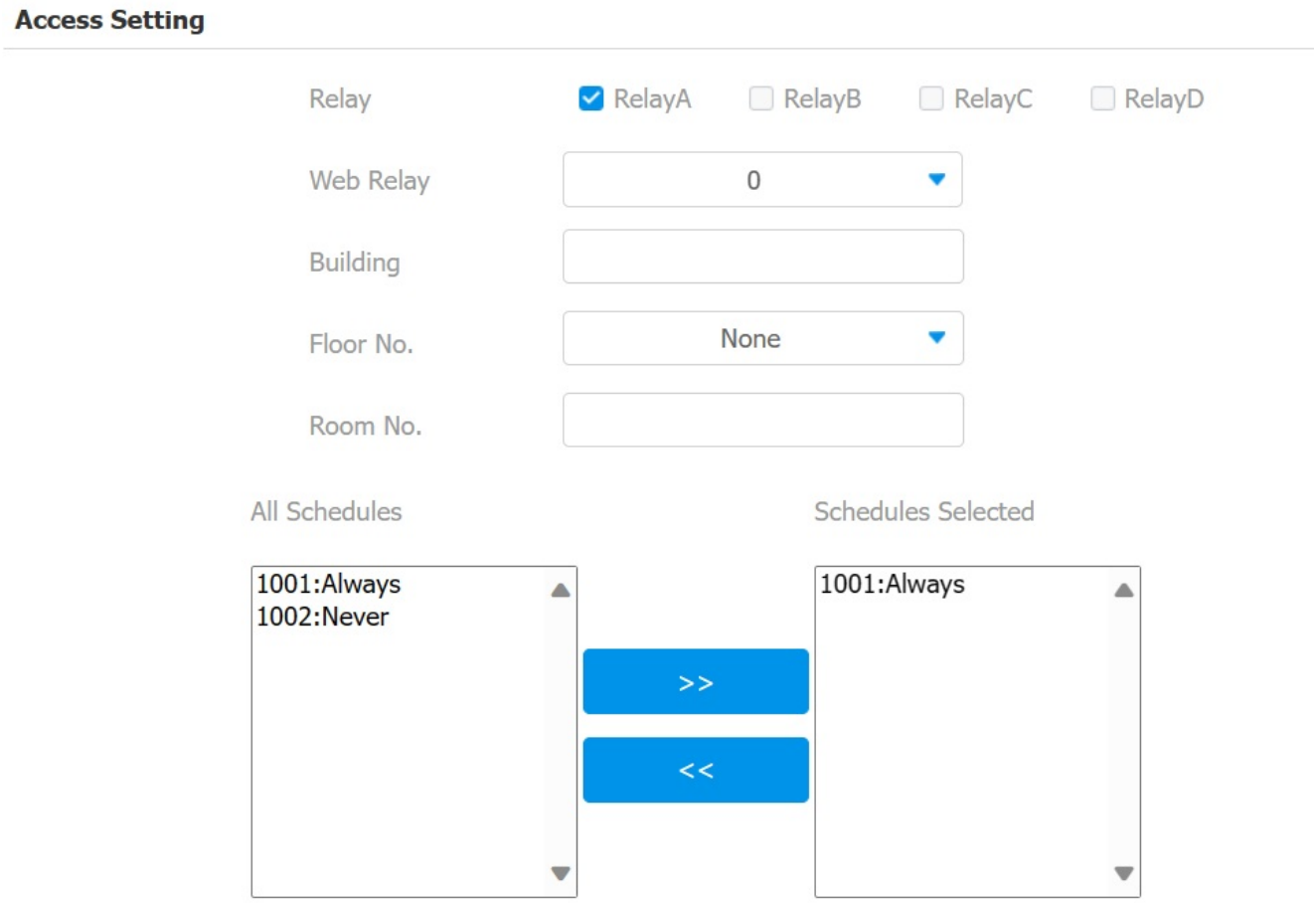
Configure Private PIN Code on the Web Interface

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 **Intercom > User** interface. Click **Add** to configure the private PIN.



Scroll down and select door access schedule for private PIN code door access if needed.



Parameter Set-up:

- **Relay**: select the relay for the door unlock.
- **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.

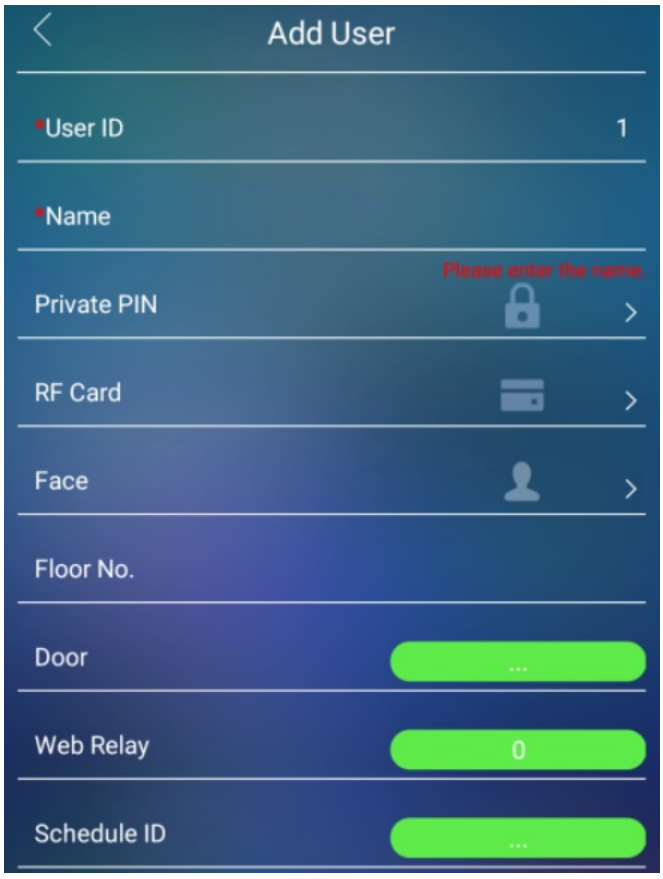
Note:

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

Configure Private PIN Code on the Device

You can set up a private PIN code on the device for the specific user.

To configure it on the device **Setting > User** screen.



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.

To configure it on the web **Intercom > PIN Setting** interface.

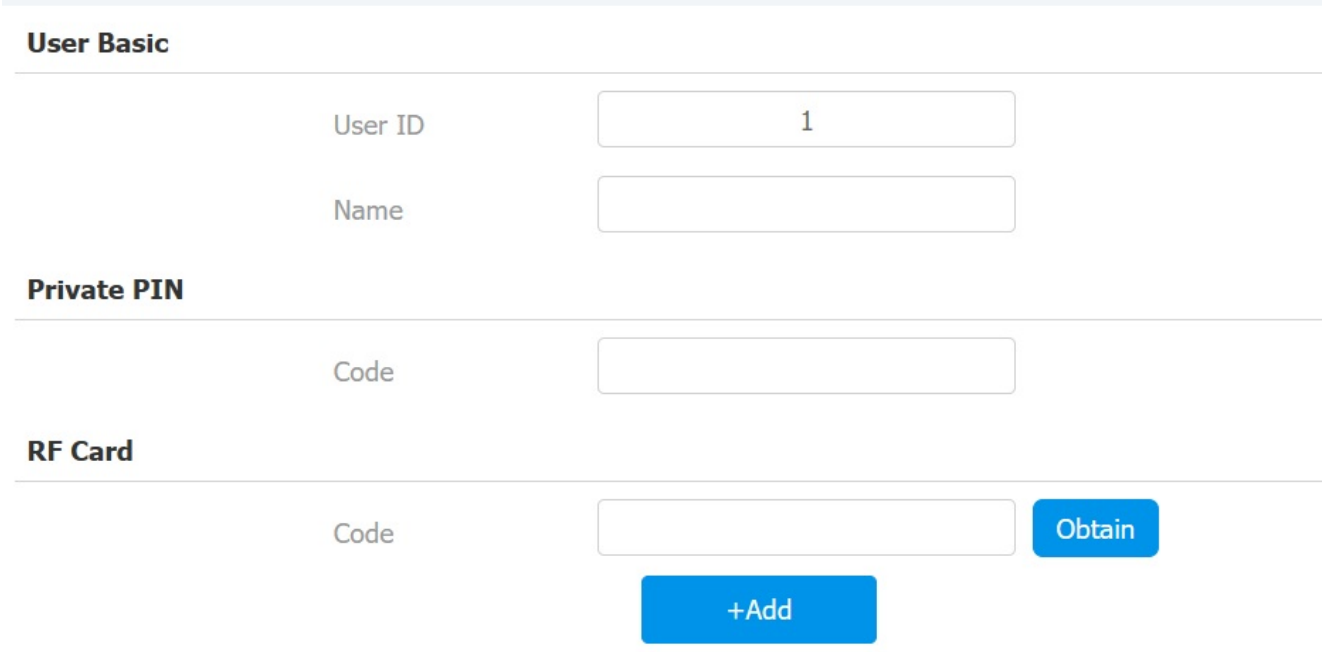
Note:

- **APT+PIN** 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 **Intercom > User** interface. Click **Add** to configure the RF card.



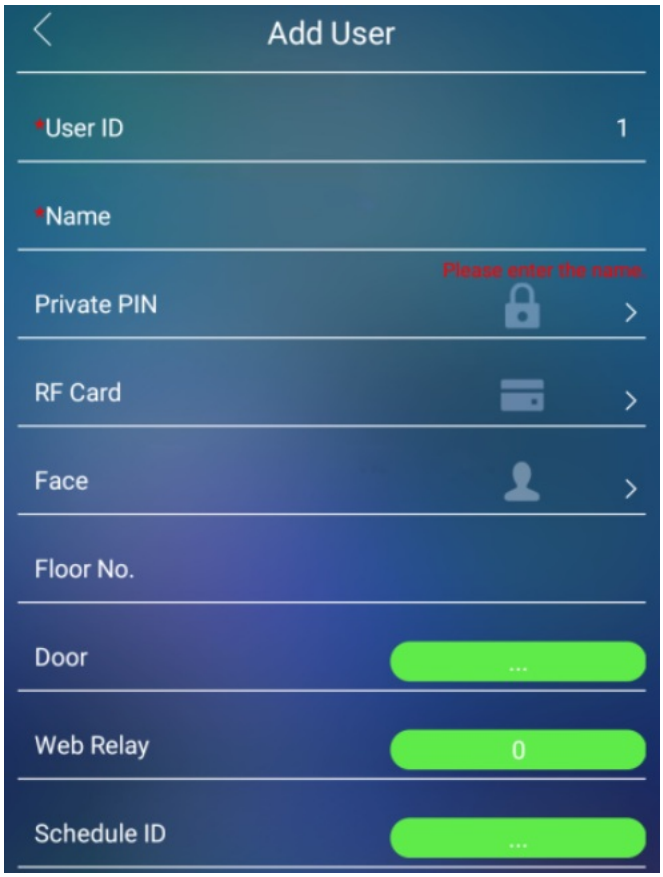
Note:

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

Configure RF Card on the Device

You can configure the RF card directly on the device for the door access while setting up the time schedule for the validity of the RF card access along with the web relay that can be triggered with the RF card etc.

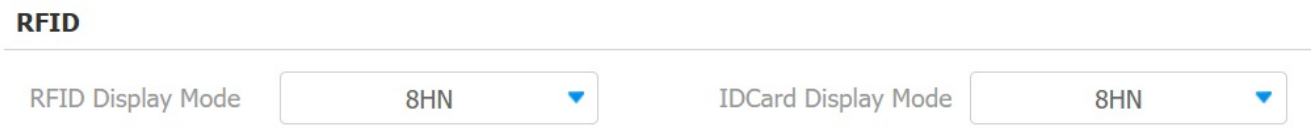
To configure it on the device **Setting > User** screen.



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 **Intercom > Advanced > RFID** interface.



Parameter Set-up:

- **RFID Display Mode**: select the card format for the IC card for the door access among **8H10D**, **6H3D5D(W26)**, **6H8D**, **8HN**, **8HR** and **8HR10D**. The card code

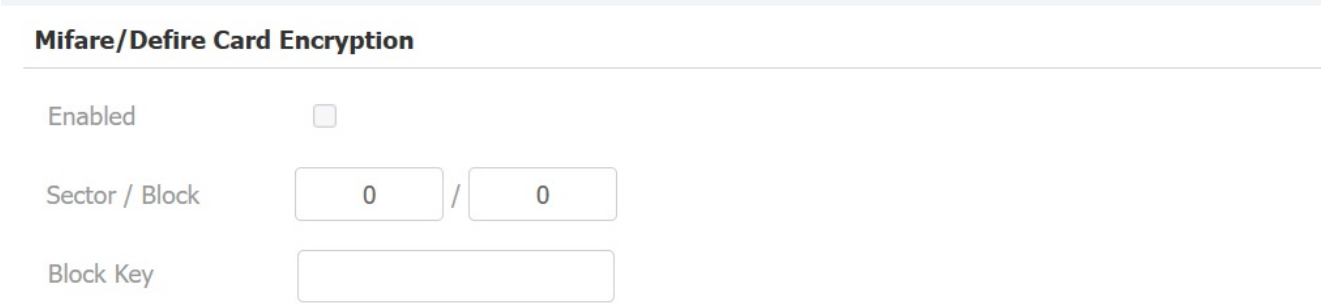
format is **8HN** by default.

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

Mifare/Defire Card Encryption

The door phone can read the encrypted Mifare/Defire card for greater security.

Navigate to **Intercom > Card Setting** interface.



Parameter Set-up:

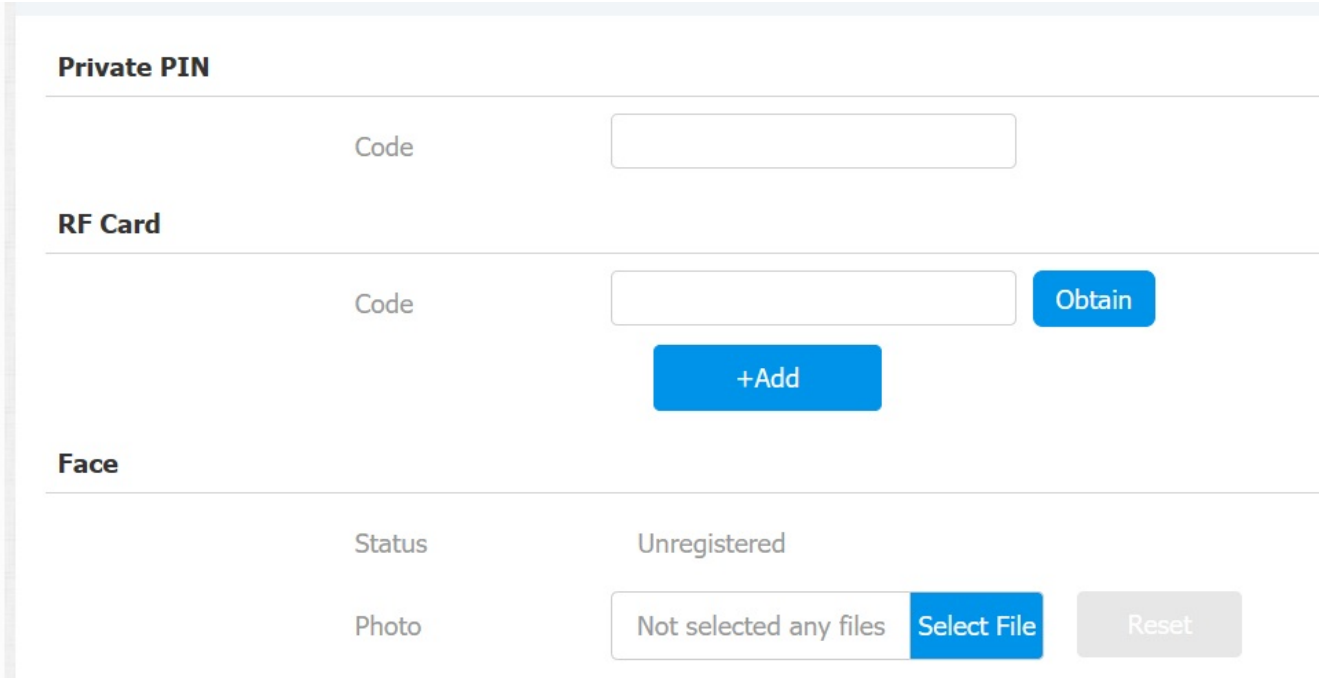
- **Sector/Block**: enter the sector and block in which the card number is located in the Mifare/Defire Card. For example, the card number can be in sector 3 and block 3 in the card.
- **Block Key**: enter the block password for access.

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 **Intercom > User** interface. Click **Select File** to upload the face picture and click **Reset** to clear the uploaded file.



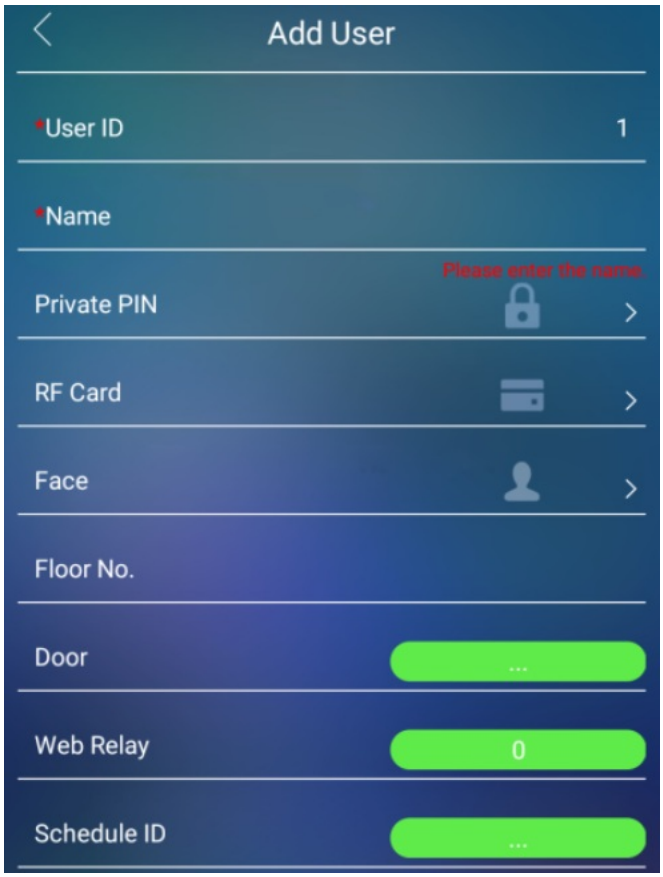
Note:

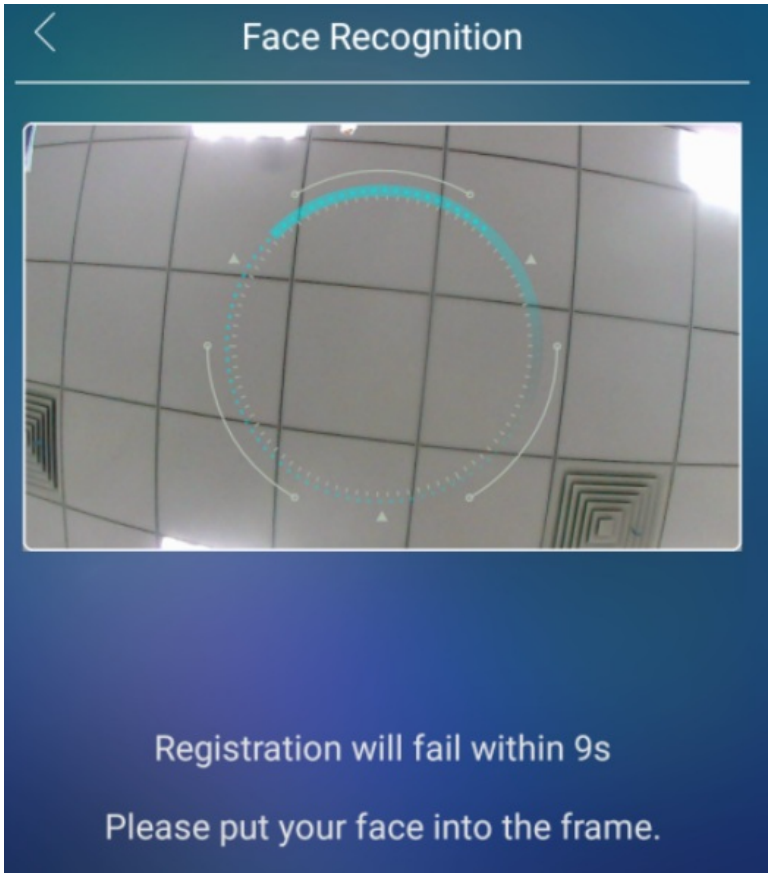
- Pictures to be uploaded should be in .jpg or .png format.

Enroll Face Data on the Device

You can enroll face data on the device by entering the user's name and registering your facial ID on the device for door access.

To configure it on the device **Setting > User** screen.

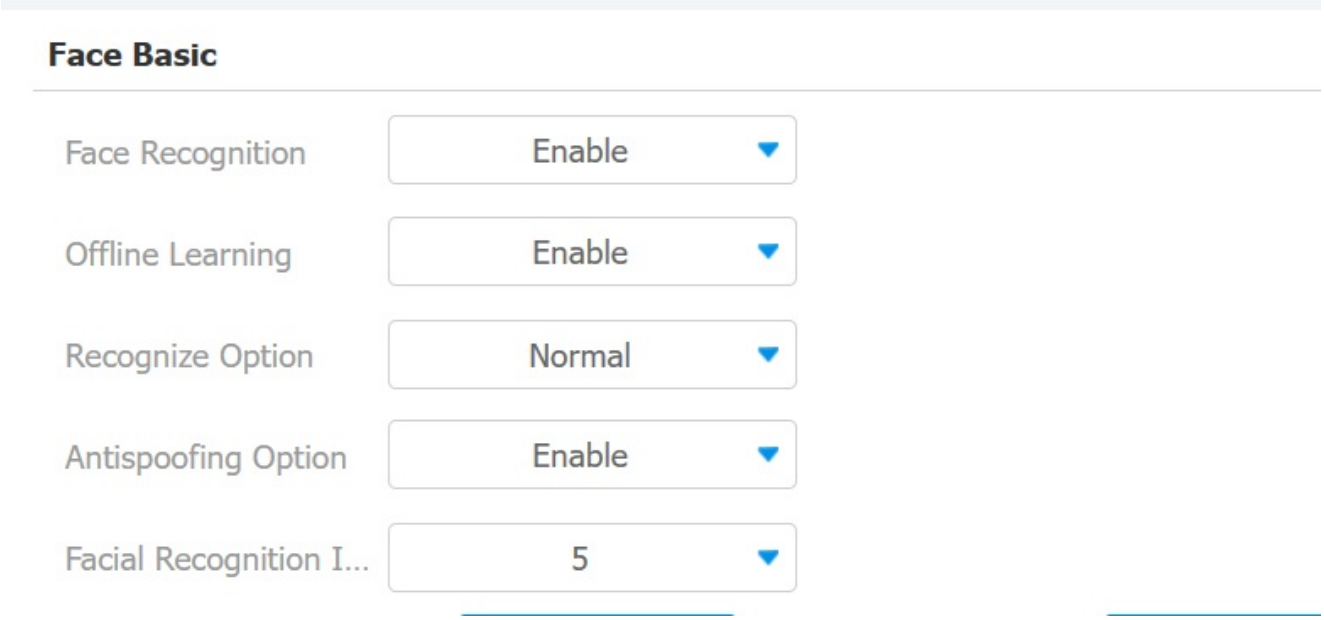




Configure Facial Recognition on Web Interface

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

To configure the configuration on the web **Intercom > Face Setting** interface.

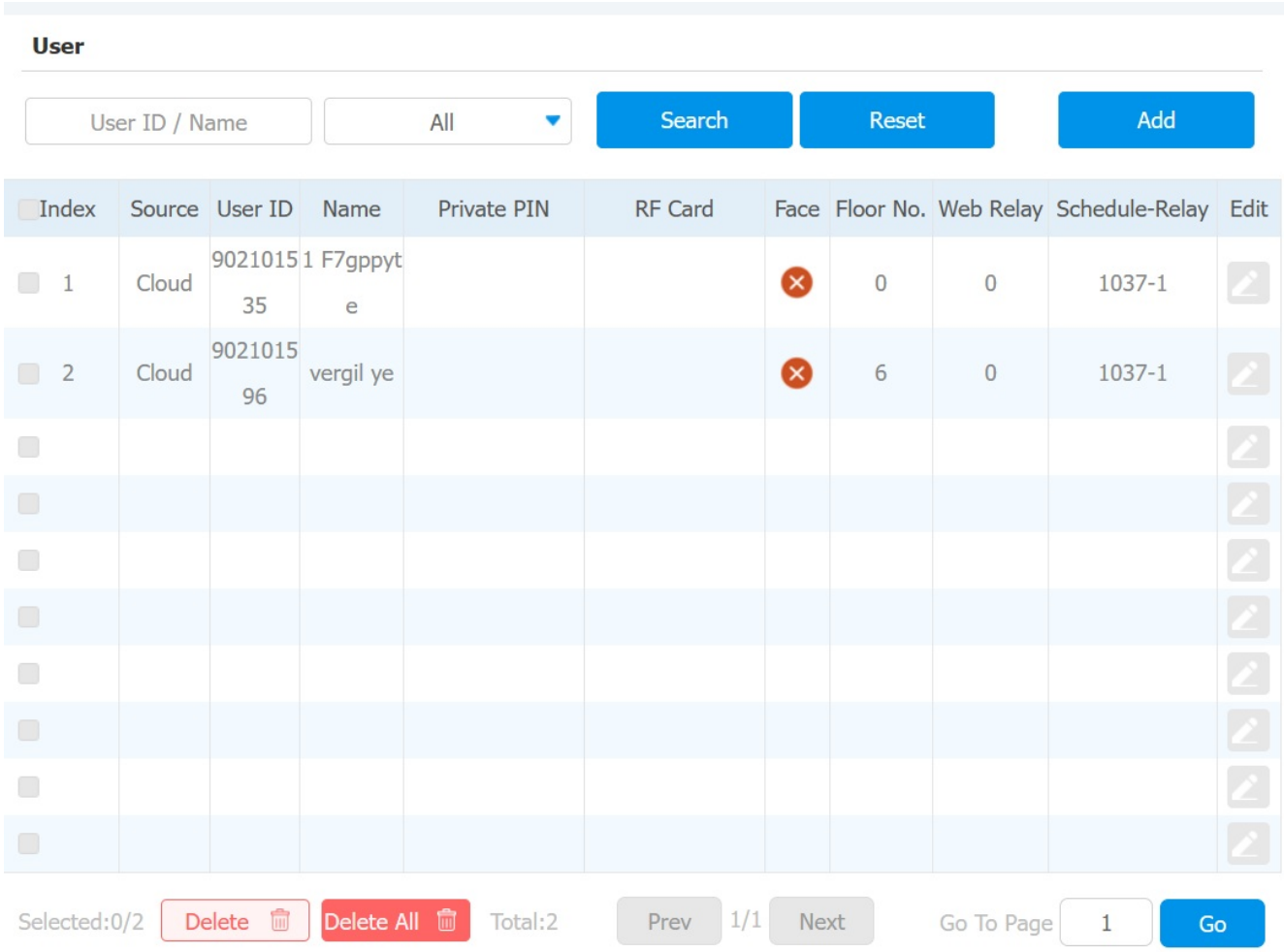


Parameter Set-up:

- **Offline Learning**: select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes occurred to your face. Facial recognition accuracy improves as the number of facial recognitions increases.
- **Recognize Option**: click to select the facial recognition accuracy level among four options: **Low, Normal, High, Highest**. For example, if you select **Highest**, then there will be the least possibility that someone else will be mistaken for you by mistake or in another way round in the facial recognition.
- **Antispoofing Option**: select anti-spoofing level among four options: **Low, Normal, High, Highest**. For example, if you select **Highest**, then there will be the least possibility that the device will be fooled by digital images or the pictures of any kinds.
- **Facial Recognition Interval**: select time interval between every two facial-recognitions from 1-8 minutes. For example, if you select **5**, then you have to wait for 5 mins before you are allowed to perform the facial recognition again.

Edit the User-specific Door Access Data

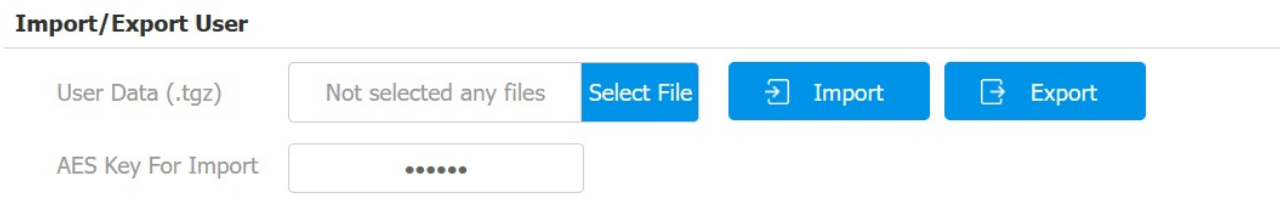
You can search user(s)-specific door access and edit the door access data on the web **Intercom > User** interface.



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.

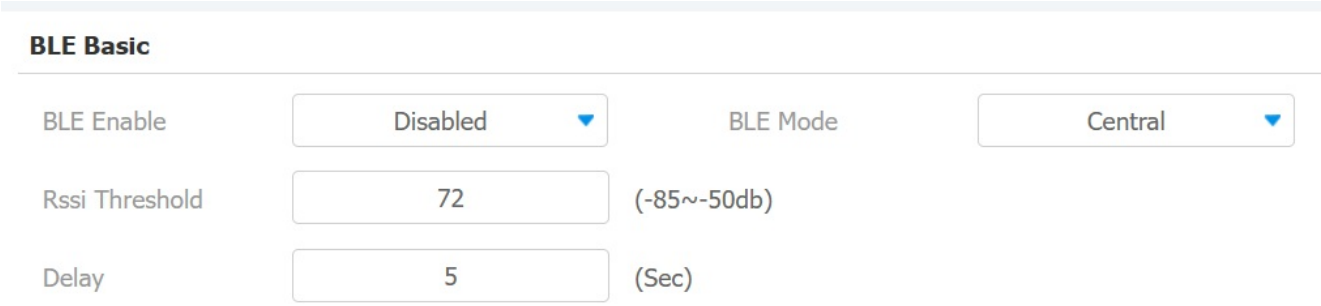
To set it up on the web **Intercom > User** interface.



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.

To configure it on the web **Intercom > BLE** interface.



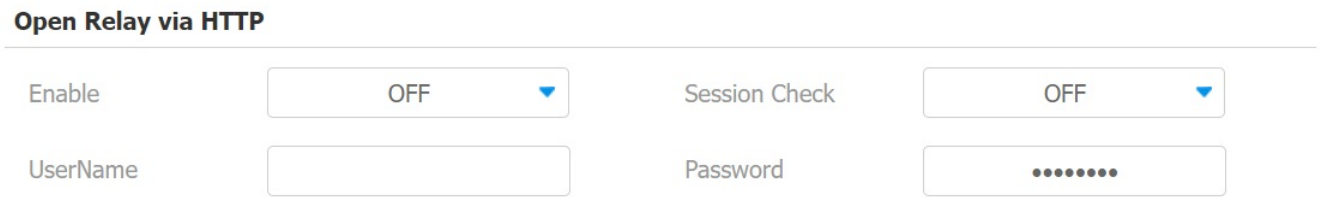
Parameter Set-up:

- **BLE Mode**: select **Central** mode to enable the door phone to receive Bluetooth signals. BLE mode is **Central** by default.
- **RSSI Threshold**: select the signal receiving strength from -85~-50db in absolute terms, The higher value it is, the greater strength it has. The default value is 72db in absolute terms.
- **Delay**: 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.

To configure it on the web **Intercom > Relay > Open Relay via HTTP** interface.



Parameter Set-up:

- **UserName**: enter the user's 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

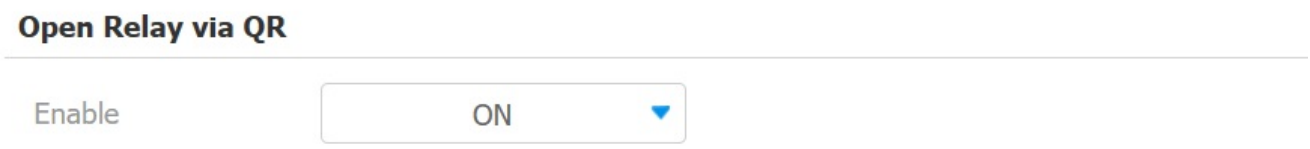
Note:

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

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.

To configure it on the web **Intercom > Relay > Open Relay via QR Code** interface.



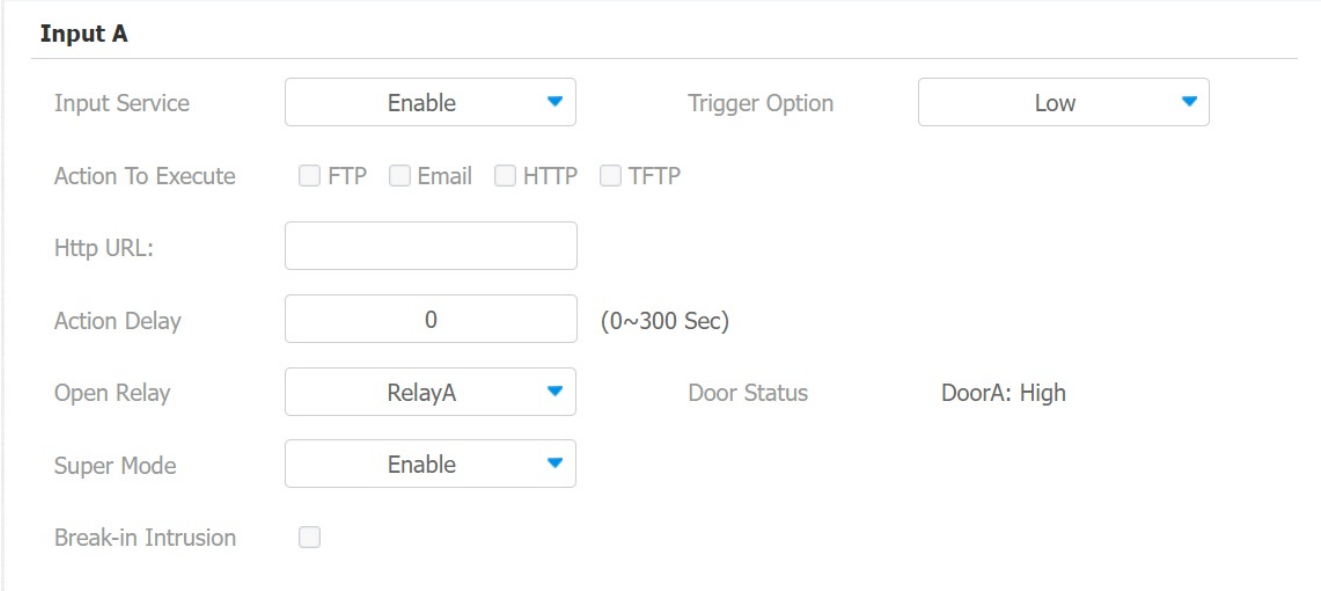
Note:

- 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.

To configure it on the web **Intercom > Input** interface.



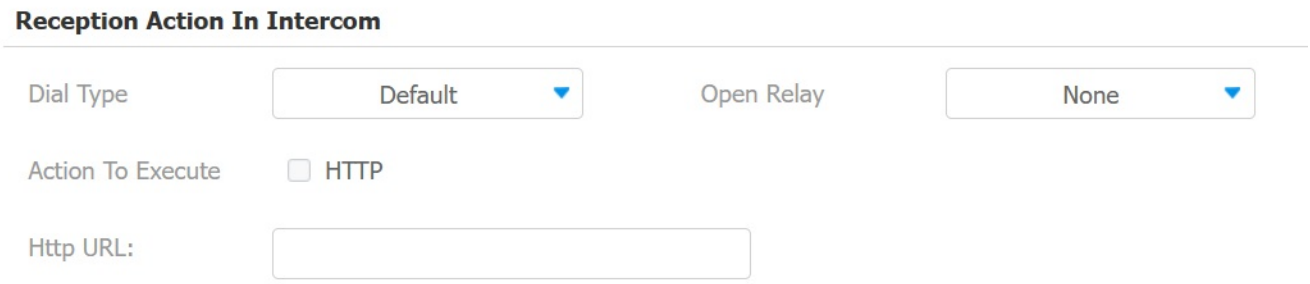
Parameter Set-up:

- **Trigger Option**: select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action to Execute**: select the method to carry out the action among four options: **FTP, Email, HTTP, TFTP**.
- **Http URL**: enter the URL if you select the HTTP to carry out the action.
- **Action Delay**: set up the delay time when the action is carried out. For example, if you set the action delay time as 5 seconds., then the corresponding actions will be carried out 5 minutes after your press the button.
- **Open Relay**: set up relays to be triggered by the input.
- **Door Status**: display the status of the input signal.
- **Super Mode**: if you enable the super mode, the administrator will be able to open the door using an RF card even when the door phone breaks down or become malfunctioned.
- **Break-in Intrusion**: enable it to trigger alarm when the door is opened abnormally.

Configure 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.

To configure it on the web **Intercom > Key/Display > Reception Action In Intercom** interface.



Parameter Set-up:

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

To configure it on the web **Intercom > Relay** interface.

Parameter Set-up:

- **DTMF Option**: select the number of DTMF digit for the door access control (**Ranging from 1-4 digits**). For example, you can select 1-digit DTMF code or 2-digit DTMF code etc., according to your need.
- **1 Digit DTMF**: set the 1 digit DTMF code within range from (**0-9, *, and #**).
- **2~4 Digits DTMF**: set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMF Mode** is set as 3-digits.

Note

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

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

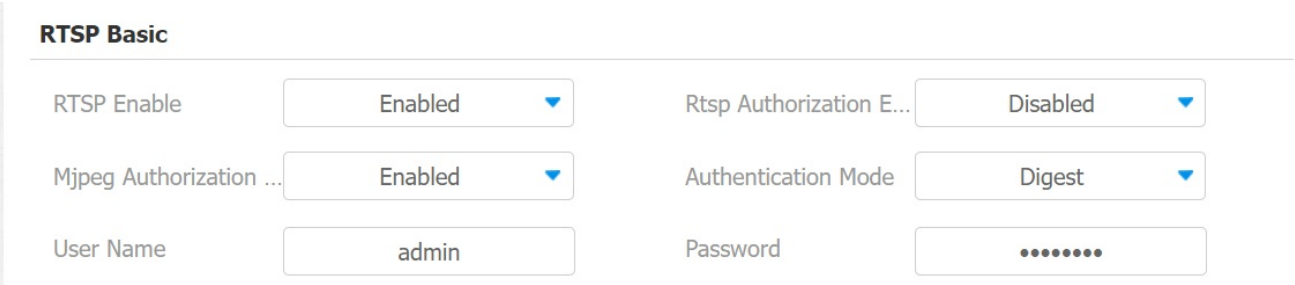
ONVIF is an Open Network Video Interface Forum. It enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

RTSP Stream Monitoring

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

RTSP Basic Setting

To configure it on the web **Intercom > RTSP > RTSP Basic** interface.



Parameter Set-up:

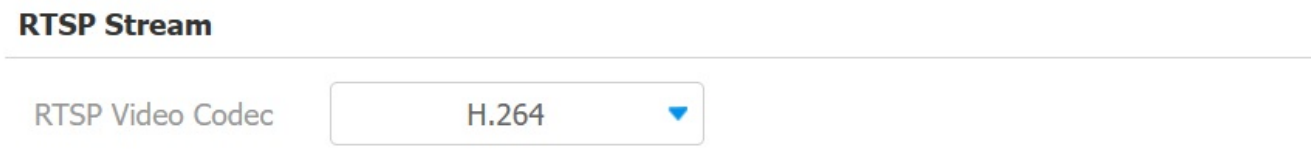
- **RTSP Authorization Enabled**: enable the RTSP authorization. If you enable the RTSP authorization, you are required to enter RTSP Authentication Mode, RTSP User Name, and RTSP Password on the intercom device such as an indoor monitor for authorization.
- **Authentication Mode**: select RTSP authentication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

Basic is the default authentication type.

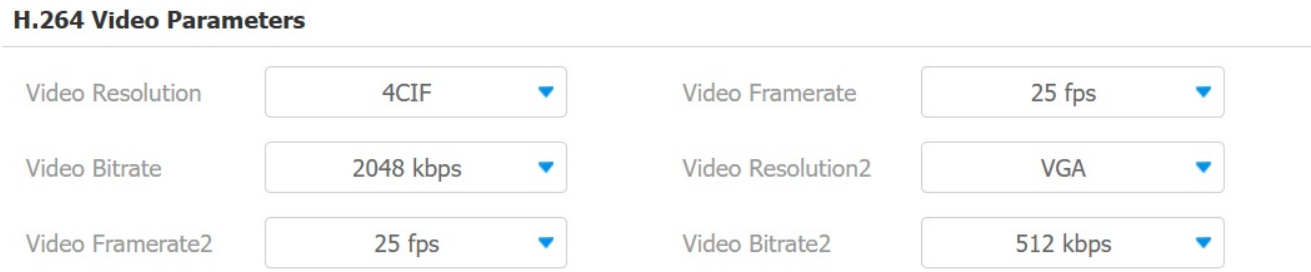
RTSP Stream Setting

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.

Go to **Intercom > RTSP > RTSP Stream** interface.



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



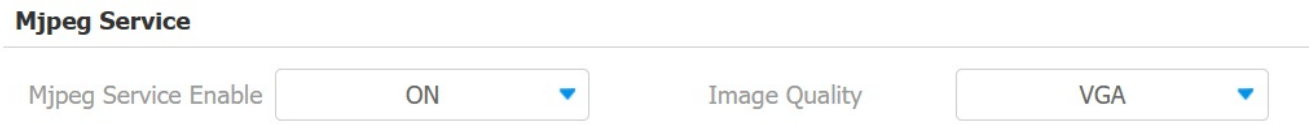
Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P**, and **1080P**. The default video resolution is **4CIF**. 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 **4CIF**.
- **Video Framerate**: **25fps** is the video frame rate by default.
- **Video Bitrate**: select video bitrate among six options: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, 4096 kpbs** according to your network environment. The default video bitrate is **2048 kpbs**.
- **Video Resolution2**: select video resolution for the second video stream channel. While the default video solution is **VGA**.
- **Video Framerate2**: select the video framerate for the second video stream channel. **25fps** is the video frame rate by default for the second video stream channel.
- **Video Bitrate2**: select video bitrate among the six options for the second video stream channel. While the second video stream channel is **512 kpbs** 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.

Go to **Intercom > Advanced > Mjpeg Service** interface.



Parameter Set-up:

- **Image Quality**: select the quality for the image capturing among six options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P**,

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

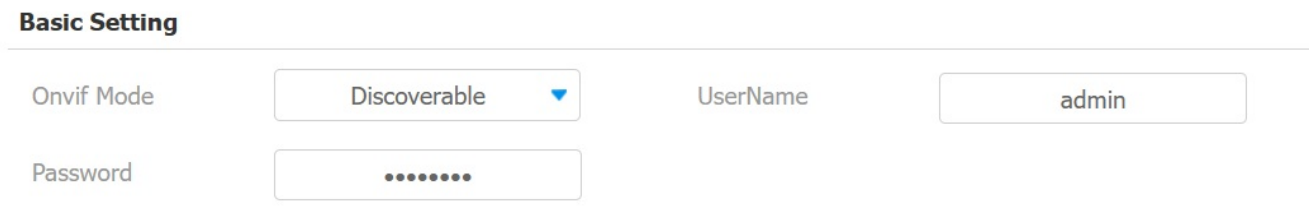
- http:// device ip:8080/picture.cgi
- http://device ip:8080/picture.jpg
- http://device ip:8080/jpeg.cgi

For example, if you want to capture the JPG format image of door phone with the IP address: 192.168.1.104, you can 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.

To configure it on the web **Intercom > ONVIF** interface.



Parameter Set-up:

- **Onvif Mode**: if you select **Discoverable**, then the video from the door phone camera can be searched by other devices.
- **User Name**: enter the username. It is **admin** by default.
- **Password**: enter the password. It is **admin** by default.

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

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

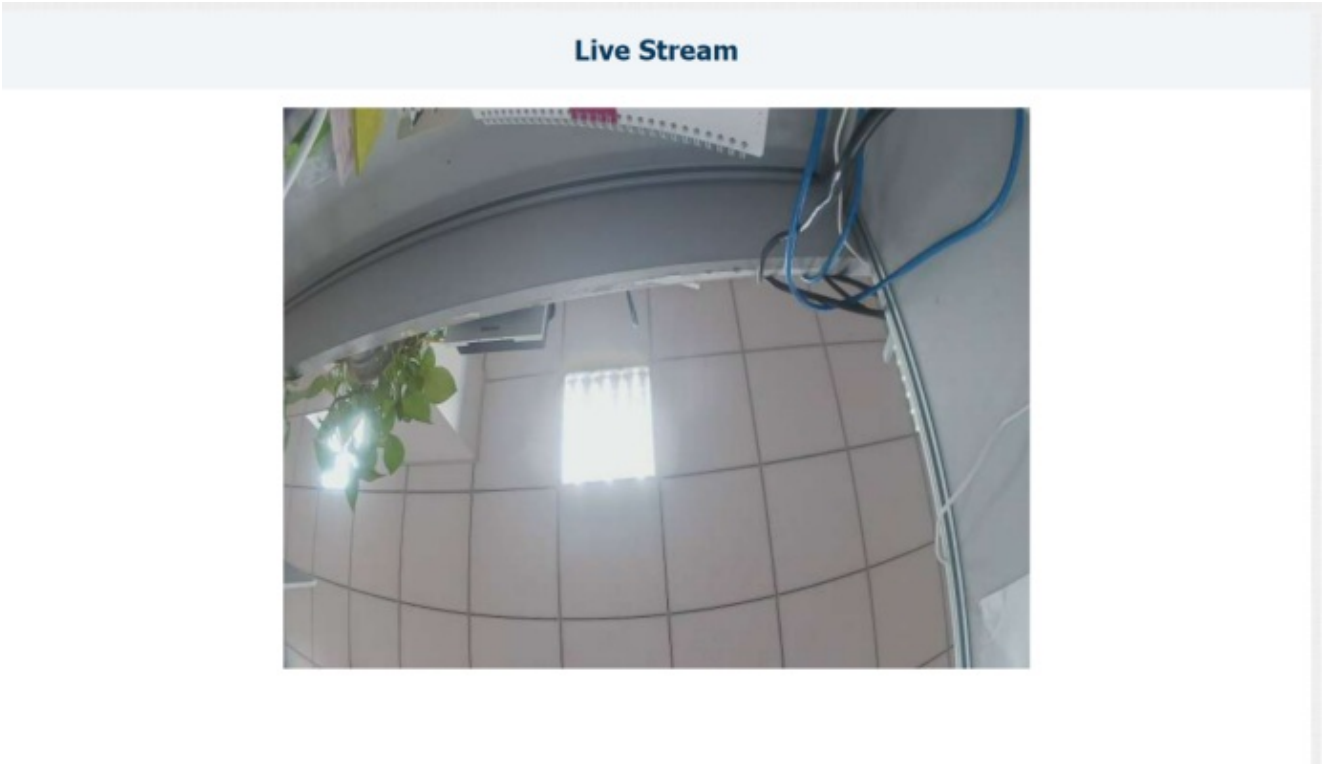
Note

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

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.

Go to **Intercom > 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.

To configure it on the web **Intercom > Advanced > Tamper Alarm** interface.

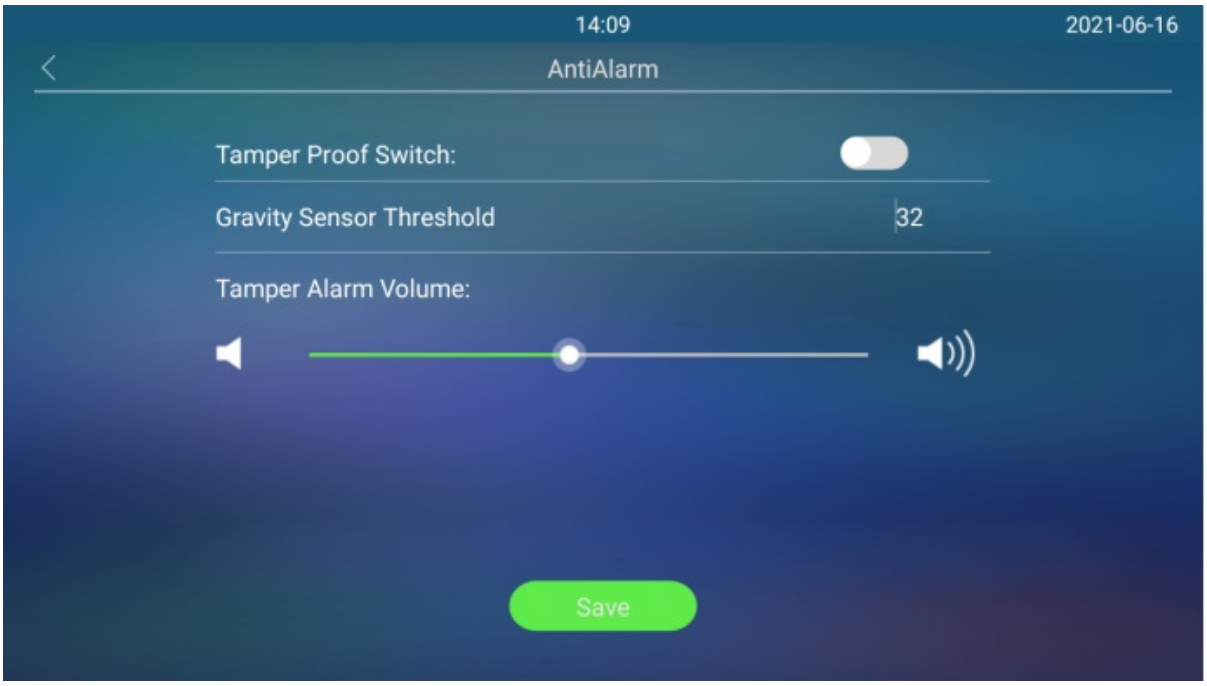
Parameter Set-up:

- **Gravity Sensor Threshold**: set the threshold for gravity sensory sensitivity. The lower the value is, the higher the sensitivity will be. The gravity sensor value is 32 by default.

Configure Tamper Alarm on the Device

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

To configure it on the device **Setting > AntiAlarm** interface.



Disarm Setting

You can set the disarm code directly on the device **Setting > Disarm** screen or on device web interface.

Navigate to **Security > Basic > Disarm Setting** interface.

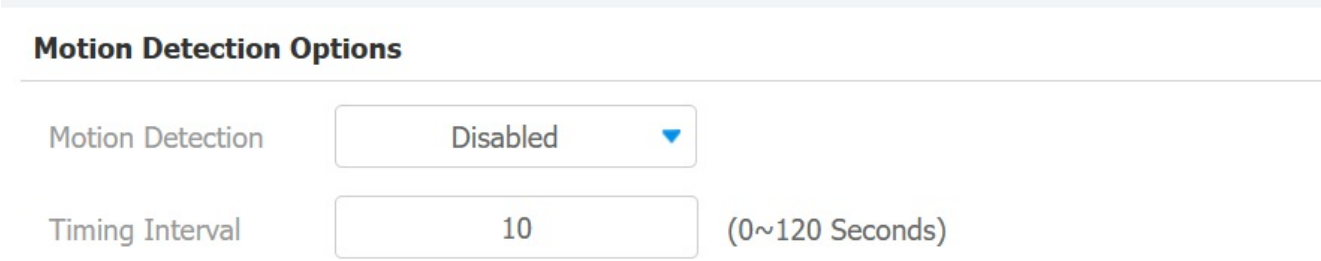
Motion Detection

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.

To configure it on the web **Intercom > Motion > Motion Detection Options** interface.

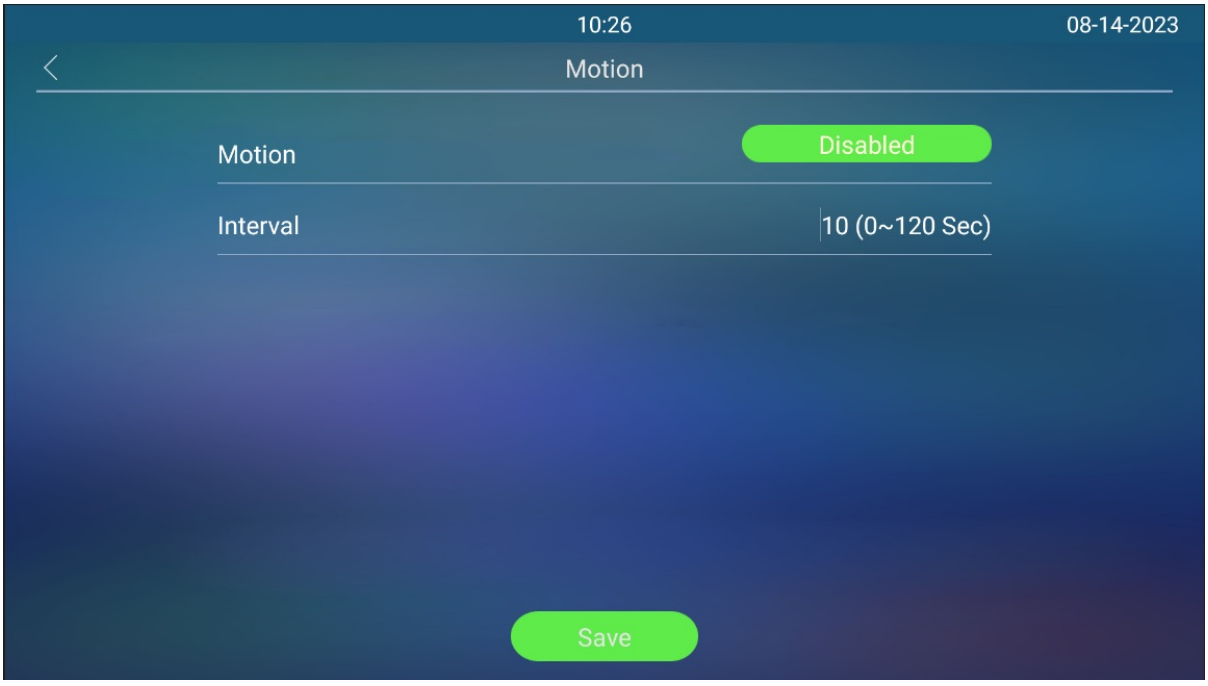


Parameter Set-up:

- **Time Interval**: set the time interval for the motion detection. If you set the default time interval as **10** Sec, then the motion detection period will be 10 seconds. Assuming that we set the time interval as **10** then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) anywhere between **7-10** seconds once movement is detected.“10” Sec interval is a complete cycle of the motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the **Time interval minus three**.

Configure Motion Detection on the Device

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



Parameter Set-up:

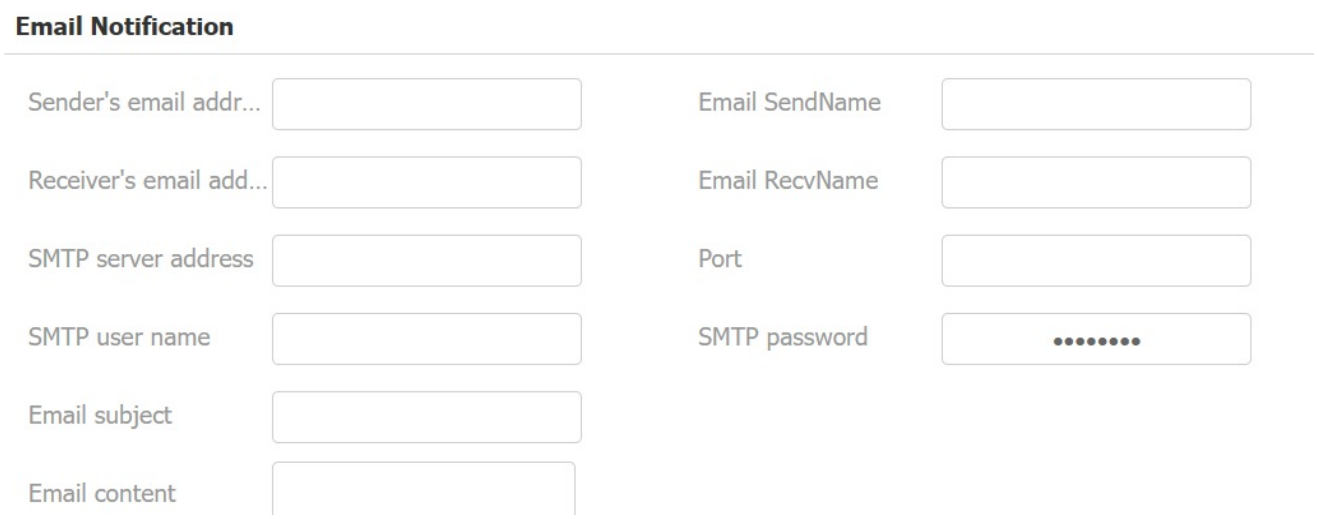
- **Interval**: set the time interval as you do on the device web interface.

Security Notification Setting

Email Notification Setting

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

Go to **Intercom > Action > Email Notification** interface.



Parameter Set-up:

- **SMTP Server Address**: enter the SMTP server address of the sender.
- **SMTP User Name**: enter the SMTP username, which is usually the same with sender's email address.
- **SMTP Password**: configure the password of SMTP service, which is same with sender's email address.

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.

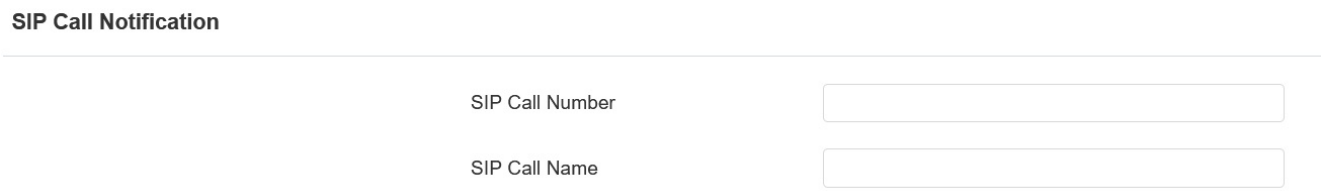
Go to **Intercom > Action > FTP Notification** interface.

TFTP Notification Setting

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

SIP Call Notification Setting

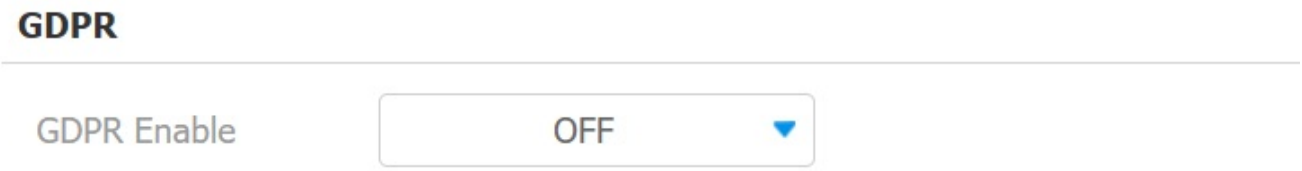
To receive security notifications via SIP calls, you need to enter the SIP call number and name on the web **Setting > Action > SIP Call Notification** interface.



GDPR Setting

General Data Protection Regulation (GDPR) is a regulation in European Union's law on data protection and privacy. The GDPR feature in Akuvox door phone is to encrypts the card data you enter for better security.

To enable this feature on the **Intercom > Advanced > GDPR** interface.



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 **Phone > Actions URL** interface.

Action URL

Active	☐
Type	GET
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayC Triggered	
RelayD Triggered	
RelayA Closed	
RelayB Closed	
RelayC Closed	
RelayD Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	

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.

To enable it on the web **Security > Basic > 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

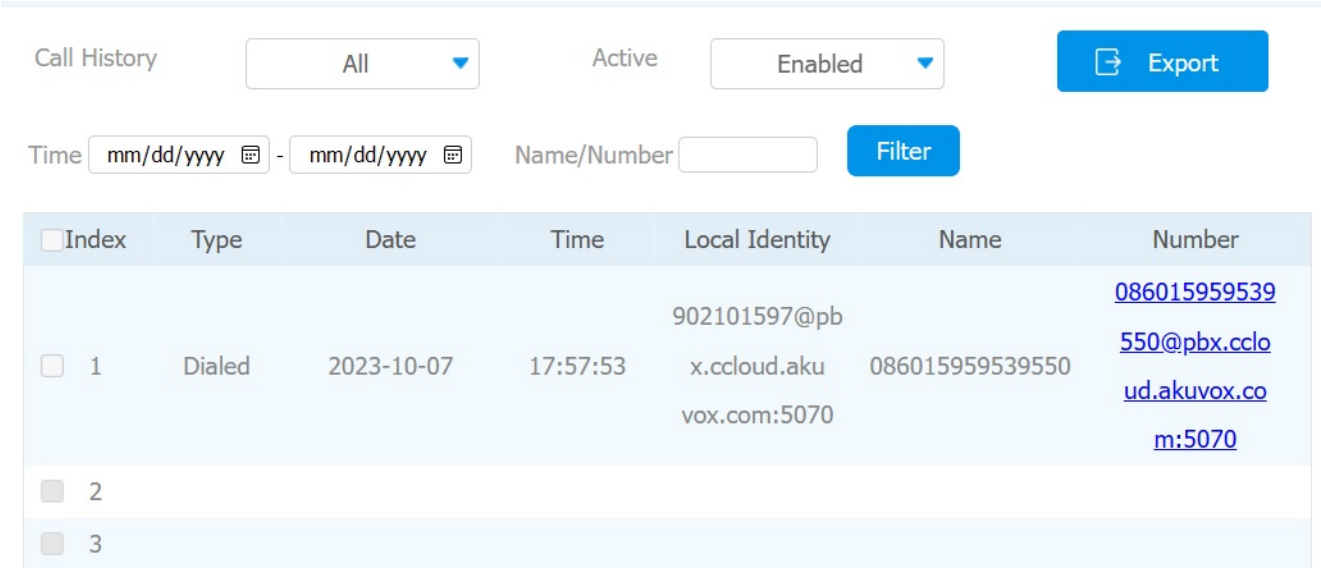
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

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 **PhoneBook > Call Log** interface.



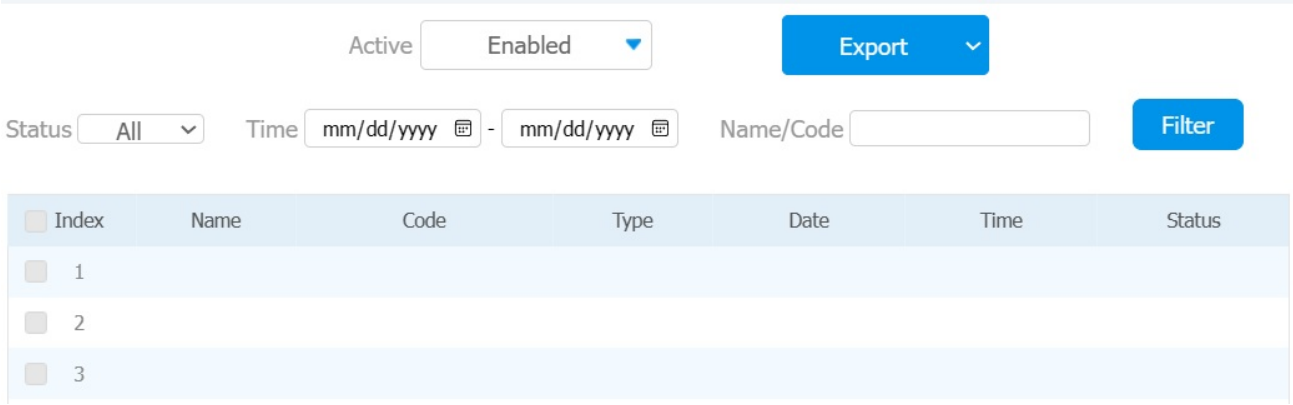
Parameter Set-up:

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

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.

Go to **Phone > Door Log** interface.



Parameter Set-up:

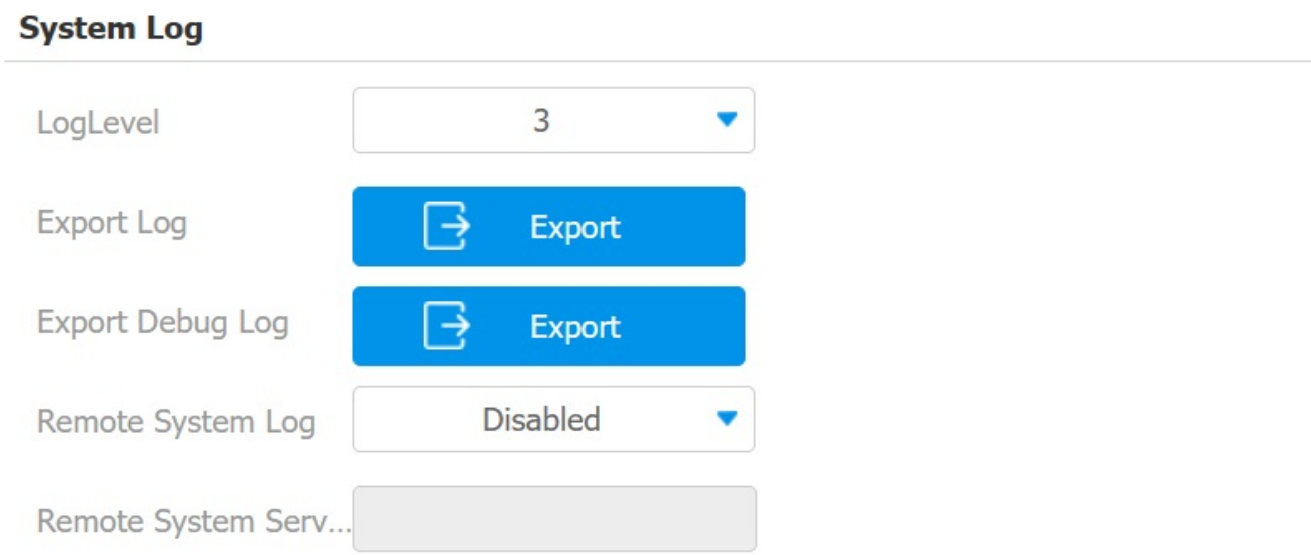
- **Status**: select between **Success** and **Failed** options to search for successful or failed door accesses.
- **Start Time ~ End Time**: select the specific time span of the door logs you want to search, check, or export.
- **Name/Code**: enter the **Name** or **Code** to search door log by the name or by the PIN code.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Go to **Upgrade > Advanced > System Log** interface.



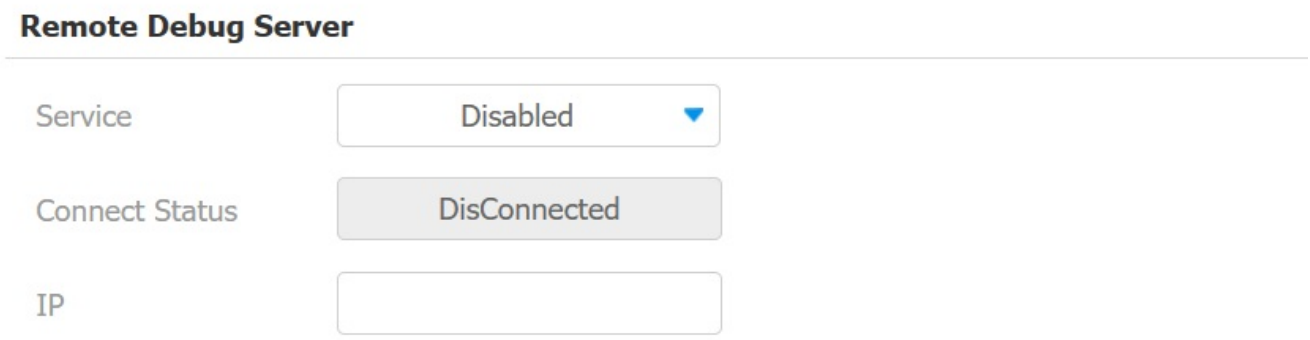
Parameter Set-up:

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

Remote 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.

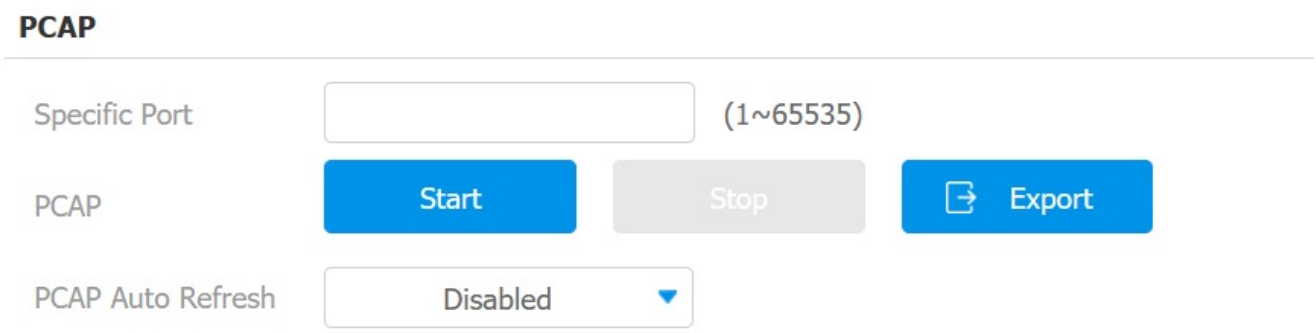
Navigate to **Intercom > Advanced > Remote Debug Server** interface.



PCAP for Debugging

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

You can set up the PCAP on the device web **Upgrade > Advanced > PCAP** interface properly before using it.



Parameter Set-up:

- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: select **Enabled** or **Disabled** to turn on or turn off the PCAP auto fresh function. If you set it as **Enabled**, then the PCAP will continue to capture data packet even after the data packets reach its 1M maximum in capacity. If you set it as **Disabled**, the PCAP will stop data packet capturing when the data packets captured reach the maximum capturing capacity of 1MB.

User Agent

User agent is used for identification purpose when you are analyzing the SIP data packet.

To configure it on the web **Account > Advanced > User Agent** interface.

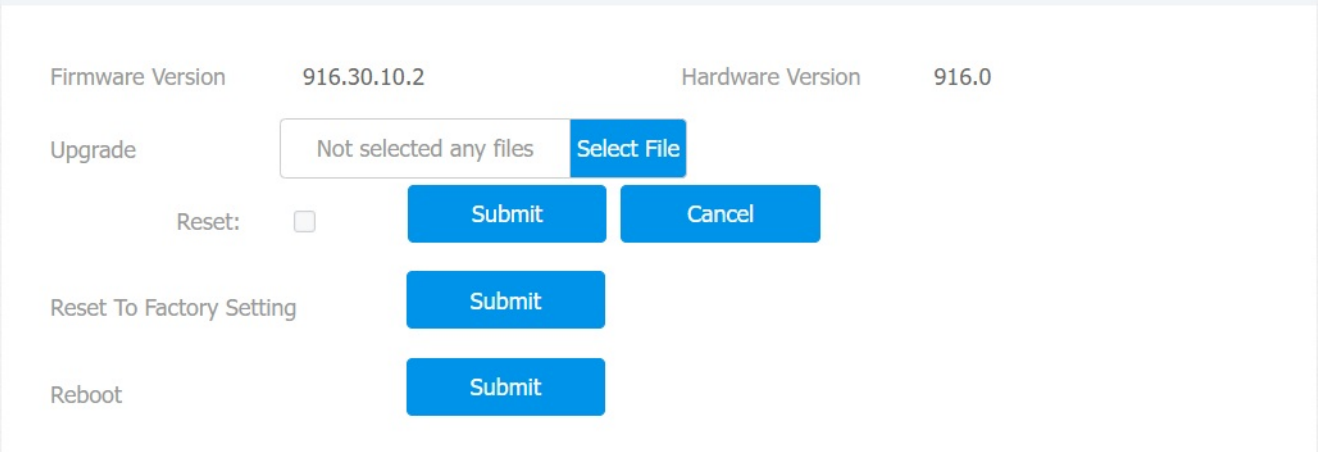
Parameter Set-up:

- **User Agent**: support to enter another specific value, Akuvox is by default.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Go to **Upgrade > Basic** interface.



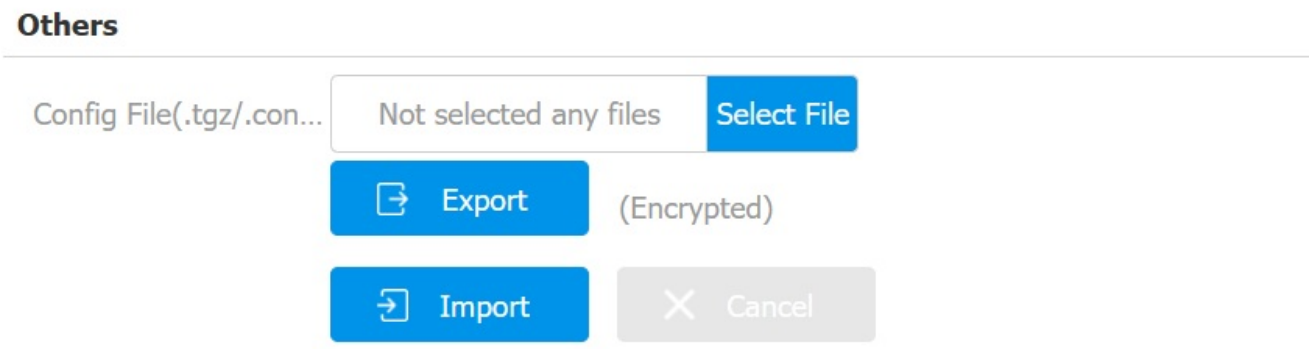
Note:

- Firmware files should be .zip format for upgrade.

Backup

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

Go to **Upgrade > Advanced > Others** interface if needed.



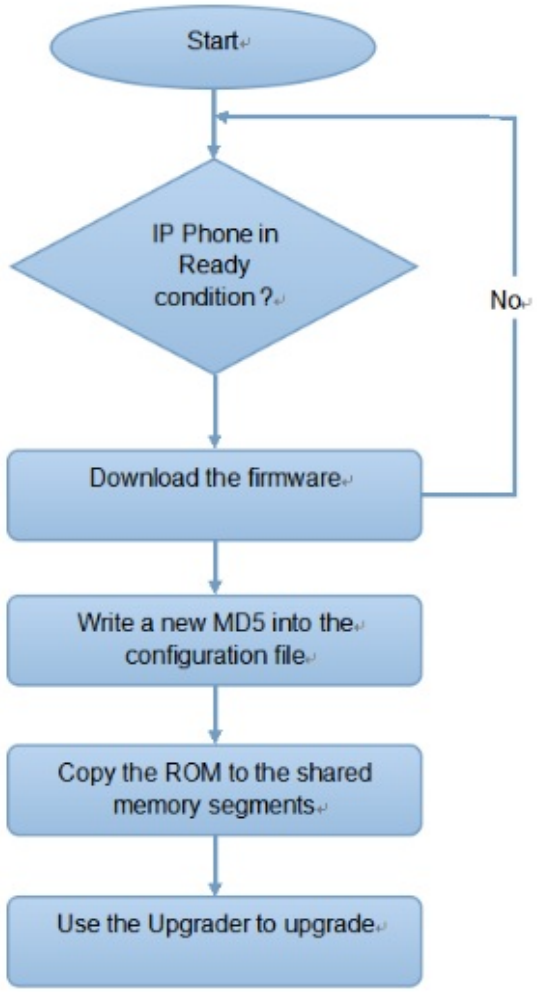
Auto-provisioning

Configurations and upgrading on the device can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the access control terminal.

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

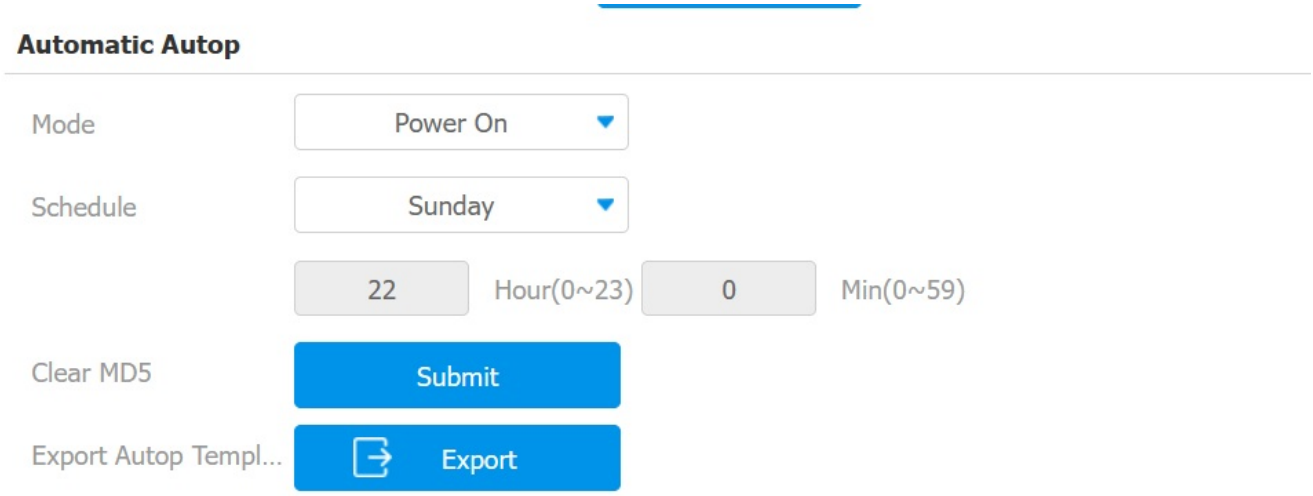
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will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

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

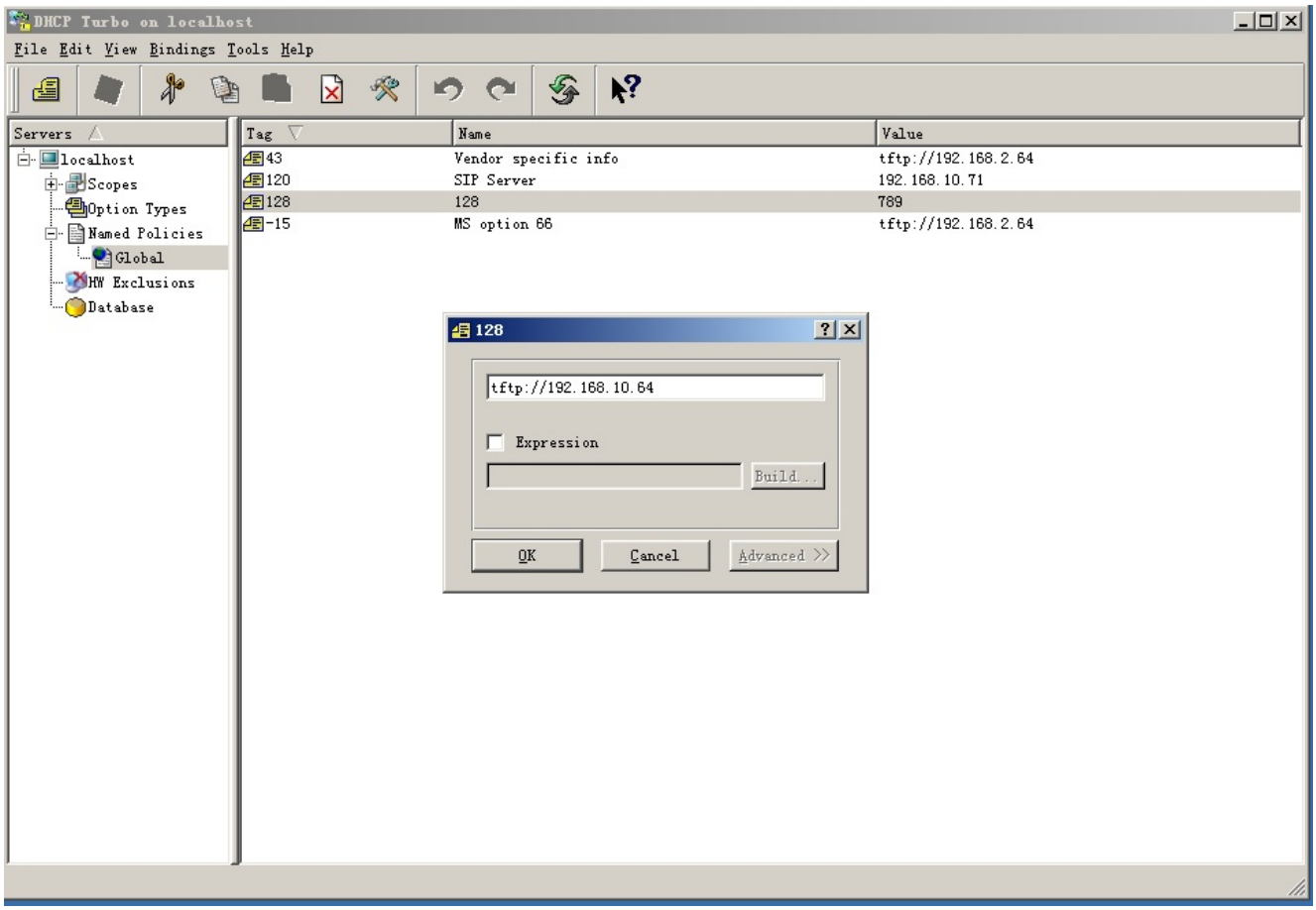


Parameter Set-up:

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

DHCP Provisioning Configuration

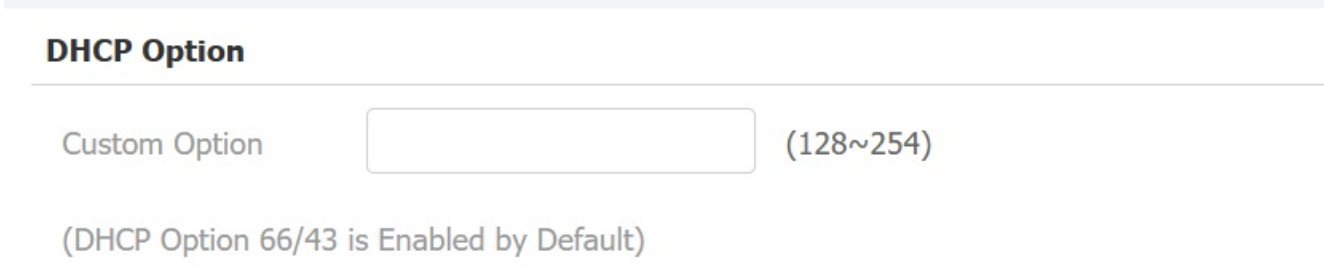
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option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



Note

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

To configure it on the web **Upgrade > Advanced** interface.



Parameter set-up:

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

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

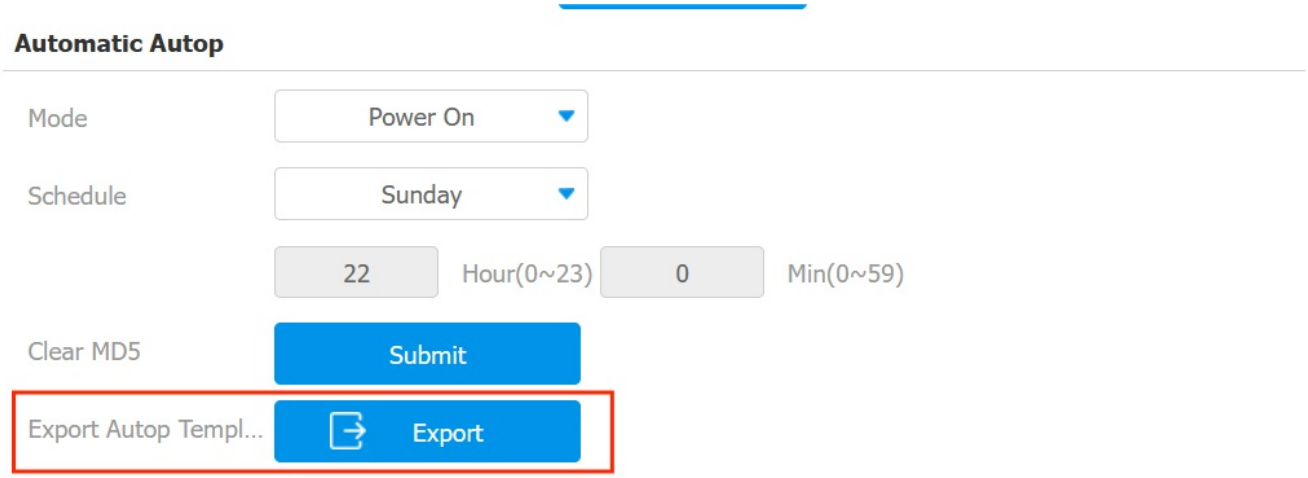
Note

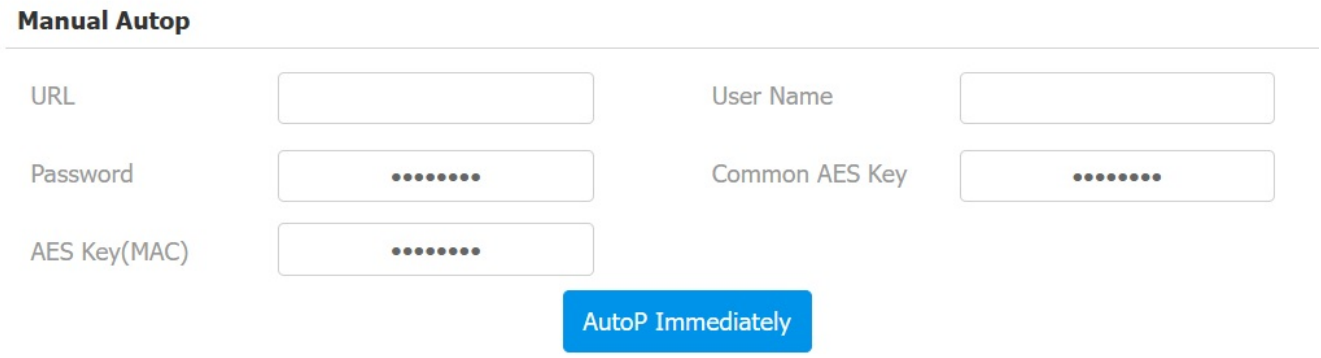
- The general configuration file for the in-batch provisioning is with the format "**r0000000000xx.cfg**" taking X915 as an example "r000000000915.cfg (10 "zeros" in total while the MAC-based configuration file for the specific device provisioning is with the format" MAC Address of the device.cfg, for example, "**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 **Upgrade > Advanced > Automatic Autop** , and setup Autop server on **Upgrade > Advanced > Manual Autop** interface.





Parameter set-up:

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

Note

- AES 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

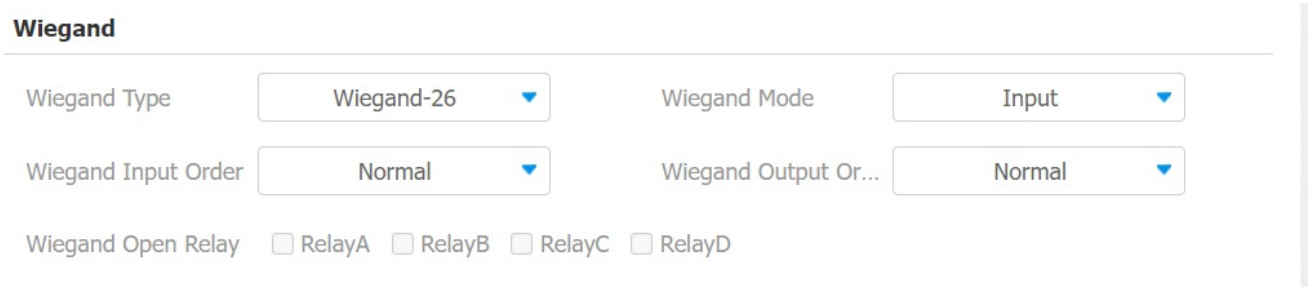
- Akuvox do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Integration with Third Party Device

Integration via Wiegand

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

To configure it on the web **Intercom > Advanced > Wiegand** interface.



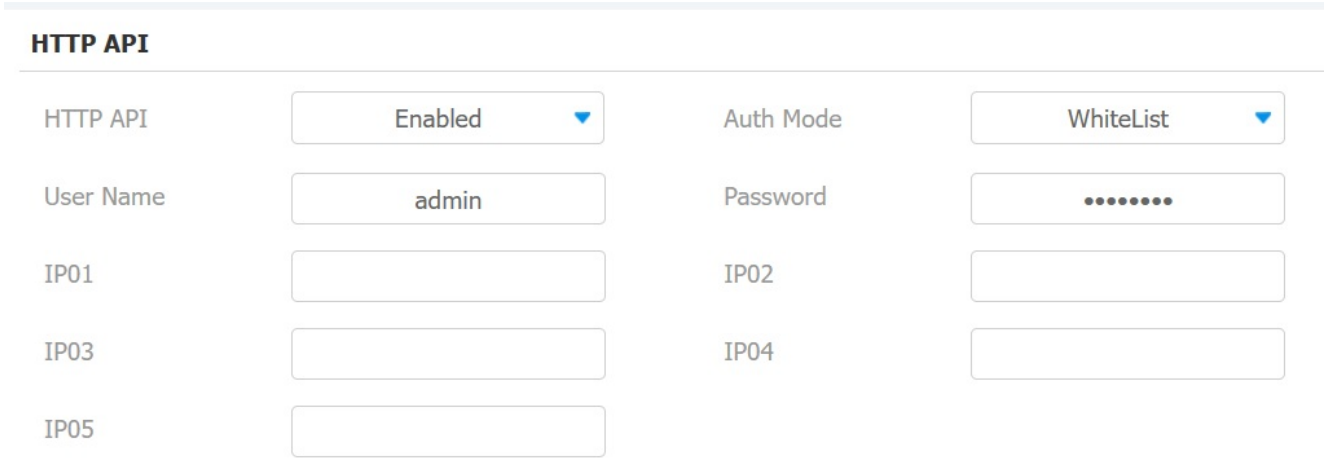
Parameter Set-up:

- **Wiegand Type**: set the Wiegand data transmission format among two options: **Wiegand 26, Wiegand 34**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Mode**: set the transfer mode between **Input** or **Output** if the door phone is used as a receiver, then set it as **Input** for the door phone and vice versa.
- **Wiegand Input 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 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.

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 **Intercom > HTTP API** interface for the integration.



Parameter set-up:

- **HTTP API**: 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.
- **Auth Mode**: select among options: **None, Normal, WhiteList, Basic, Digest** and **Token** for authorization type, which will be explained in detail in the following chart.
- **User Name**: enter the user name when **Basic** and **Digest** authorization mode is selected. The default username is **admin**.
- **Password**: enter the password when **Basic** and **Digest** authorization mode is selected. The default password is **admin**.
- **IP 01-05**: 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 developer only
3	WhiteList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication.In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In 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 developer only.

Lift Control Configuration

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.

Life control should be configured properly on the door phone's web **Intercom > Lift Control > Lift Control List** interface before you can implement the integration between the door phone and the third party devices.

Parameter Set-up:

- **Life Control List**: select integration mode among **None, OSDP, Dahua, Lift control, Akuvox EC32**. The detail for the options will be provided in the following chart.

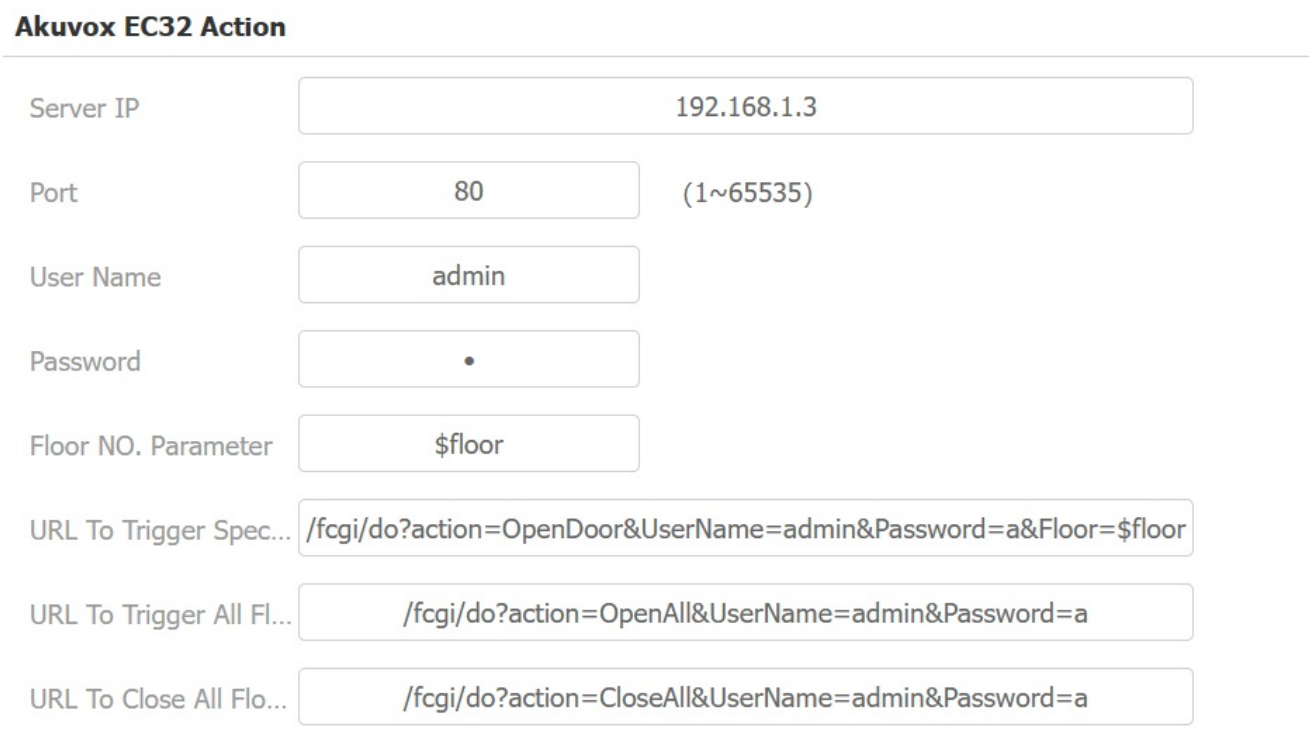
NO.	Integration Mode	Description
1	None	If you select **None** then the RS485 integration will be disabled.
2	OSDP	If you Select **OSDP** Mode, then the integration communication between the R29 series door phone and the third party device is via OSDP protocol. You are required to check for the device integration protocol and make sure if that they use the same integration protocol.
3	Akuvox EC32	Select **Akuvox EC32** if you want to connect the device with Akuvox EC32 lift controller.
4	Dahua	Dahua is originally manufacturer of the Dahua lift controller, which is also seen as an integration mode for the integration with the Dahua lift controller in the OEM project.

Note:

- Please consult with Akuvox technical support if you have any inquiries on the integration mode of any OEM lift controller integration project.

Akuvox EC32 Lift Controller

You are required to configure Akuvox EC32 before you can connect the door phone to the lift controller. You can navigate to **Intercom > Lift Control** interface.



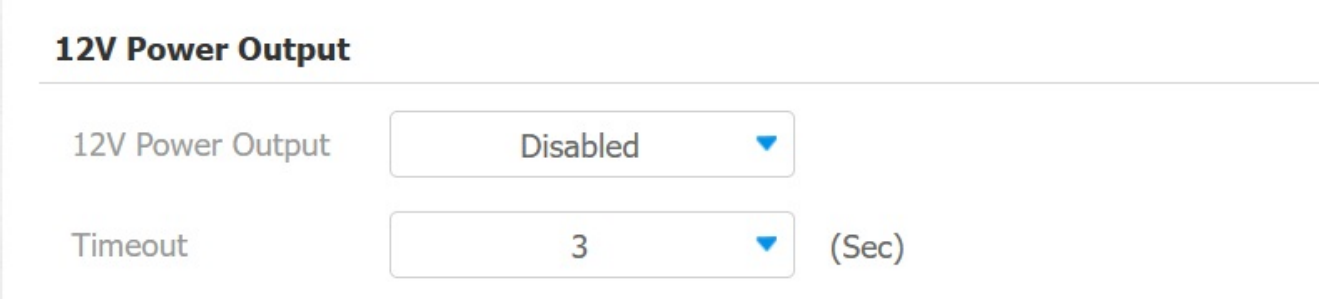
Parameter Set-up:

- **Server IP**: enter the IP address of the Akuvox EC32 controller server.
- **Port**: enter the port of Akuvox EC32 controller server.
- **User Name**: enter the user name of the lift controller for authentication.
- **Password**: enter the password of the lift controller for authentication.
- **Floor NO. Parameter**: enter the floor number parameter provided by Akuvox.
- **URL To Trigger Specific Floor**: enter the URL for triggering a specific floor.
- **URL To Trigger All Floors**: enter the URL for triggering all floors.
- **URL To Close All Floors**: enter the URL used for closing all floors.

Power Output Control

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

Navigate to **Intercom > Advanced** interface.



Parameter Set-up:

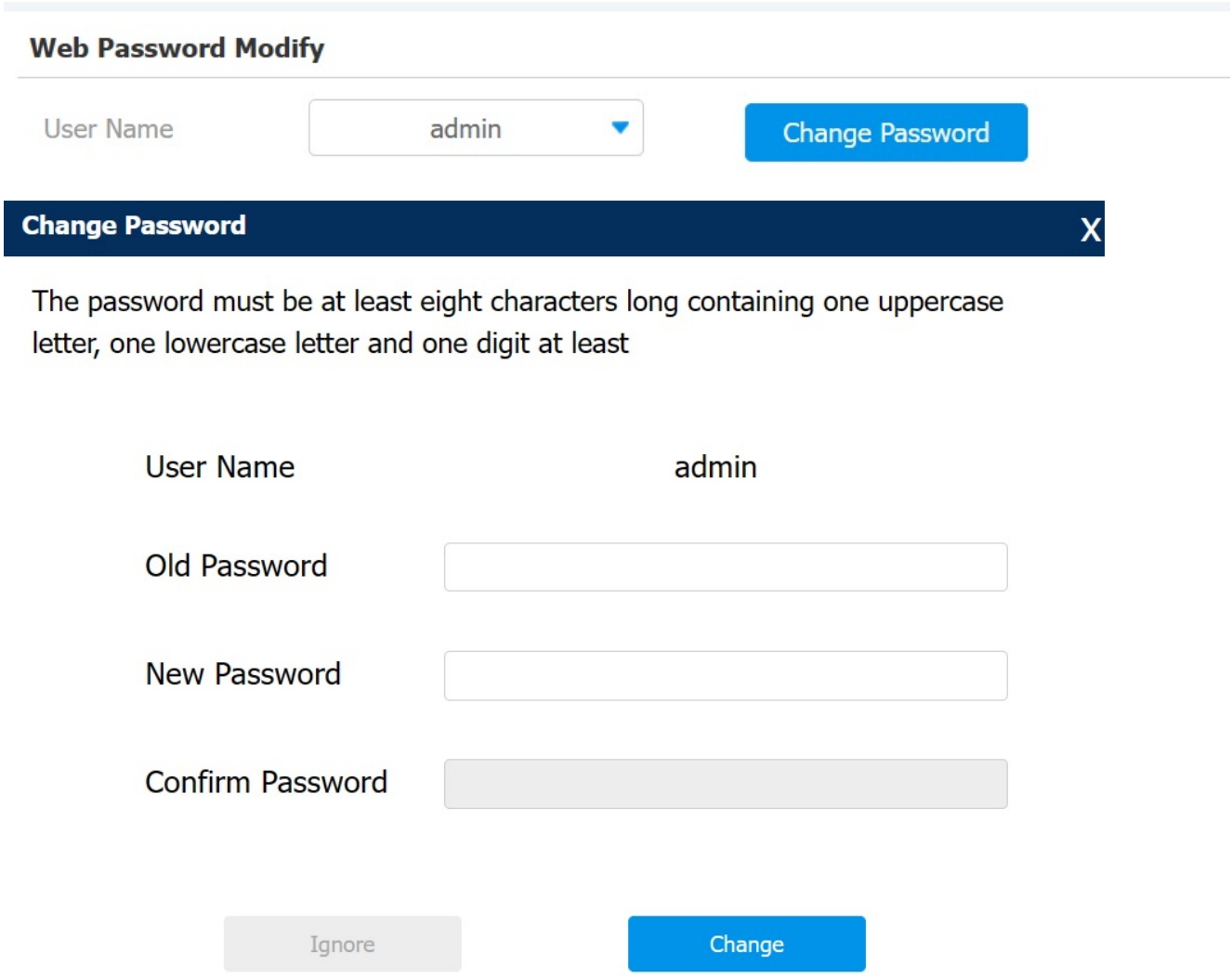
- **12V Power Output**: select **Disabled** to disable the power output function; select **Always** to enable the access controller to provide continuous power to the third-party device. Select **Triggered By Open Relay** if you want the device to provide power to the third party device via 12 output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

Password Modification

Modify Device Web Interface Password

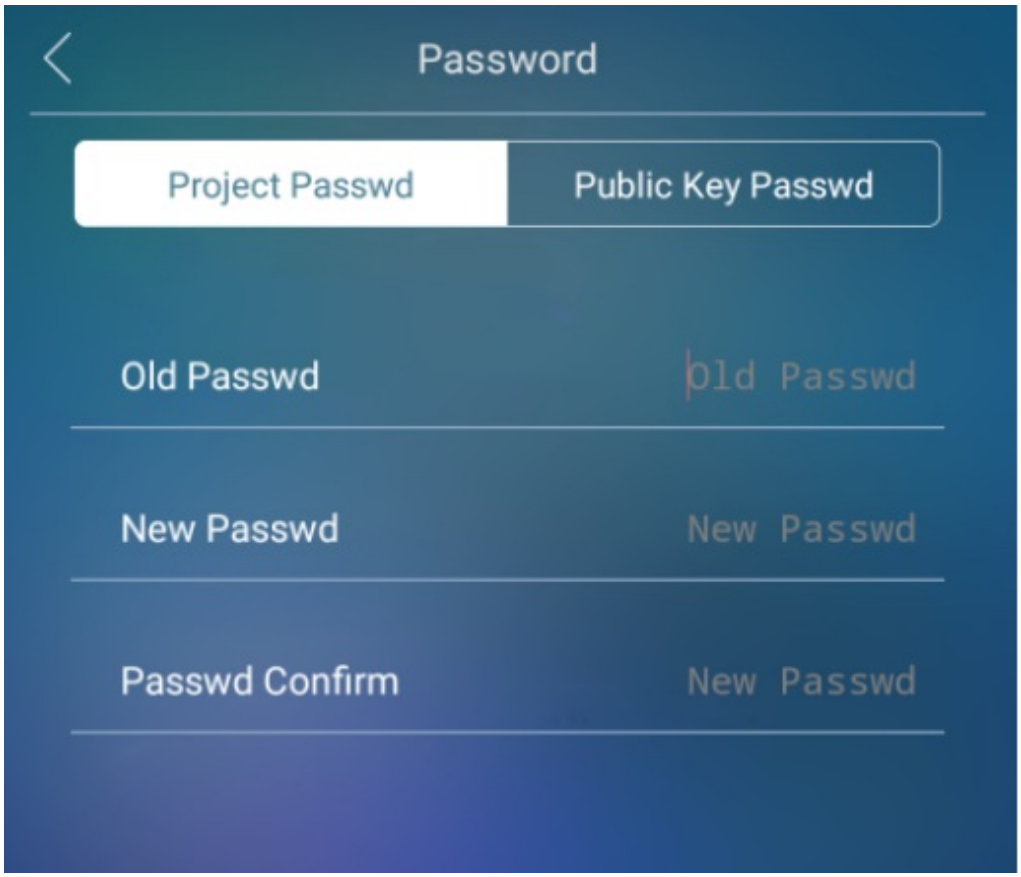
To modify web interface password, you can do it on device web interface. Select **Admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.

To change the default web password on web **Security > Basic > Web Password Modify** interface.



Modify Device Setting Password

Project passwords are what need to be entered before you are allowed to enter the setting screen. You can change the project password on the device directly.



Note:

- The initial project password is 9999, which can be considered as the old password when you modify the project password for the first time.

To modify password on the web interface, navigate to **Intercom > Basic > System PIN** interface, you can access and change both the project passwords and setting passwords if needed.

Parameter Set-up:

- **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**.

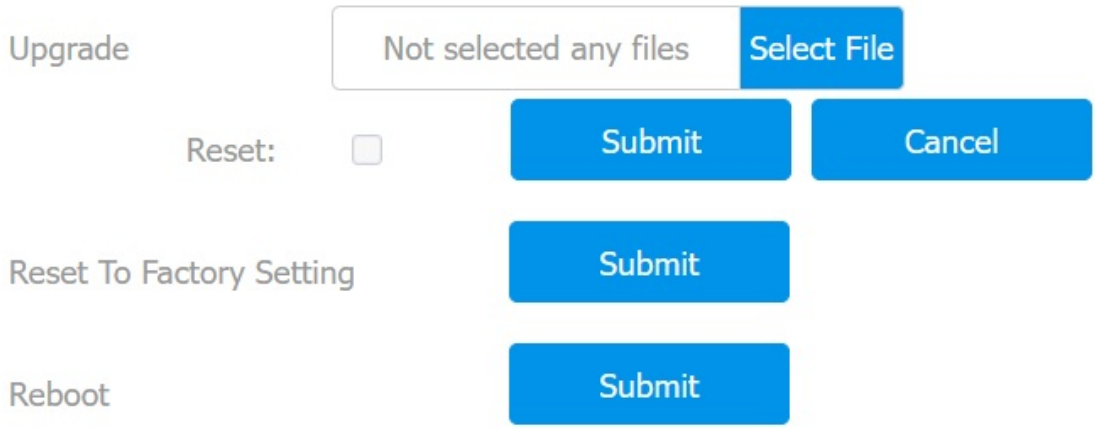
System Reboot & Reset

Reboot

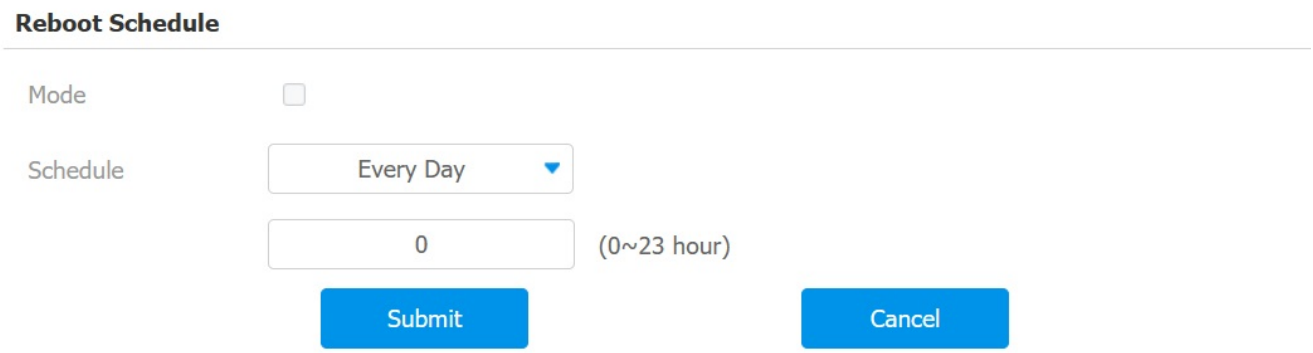
Reboot on the Web Interface

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 **Upgrade > Basic** interface.



To set up the device restart schedule on the device web **Upgrade > Advanced > Reboot Schedule** interface.



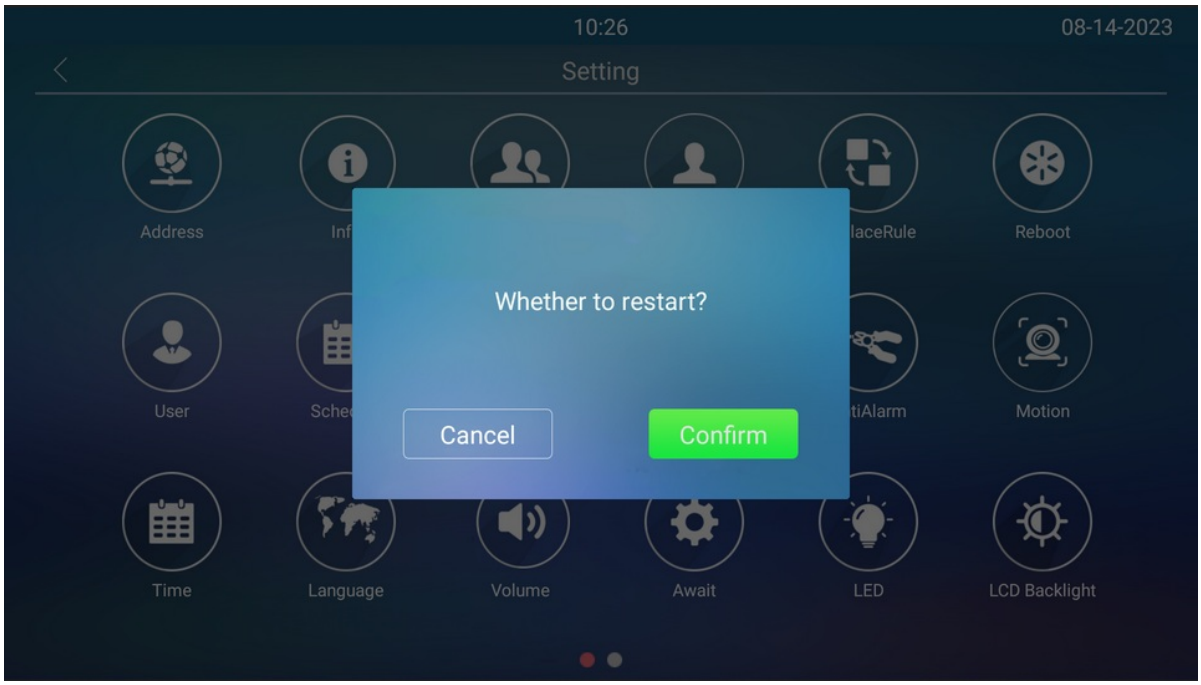
Parameter Set-up:

- **Mode**: **disable** or **enable** the mode to active or inactive reboot. Or choose **Schedule** mode for setting the reboot time regularly.

- **Schedule**: if you choose schedule mode, you need to set up the reboot schedule from Monday to Sunday and 00:00 to 24:00.

Reboot on the Device

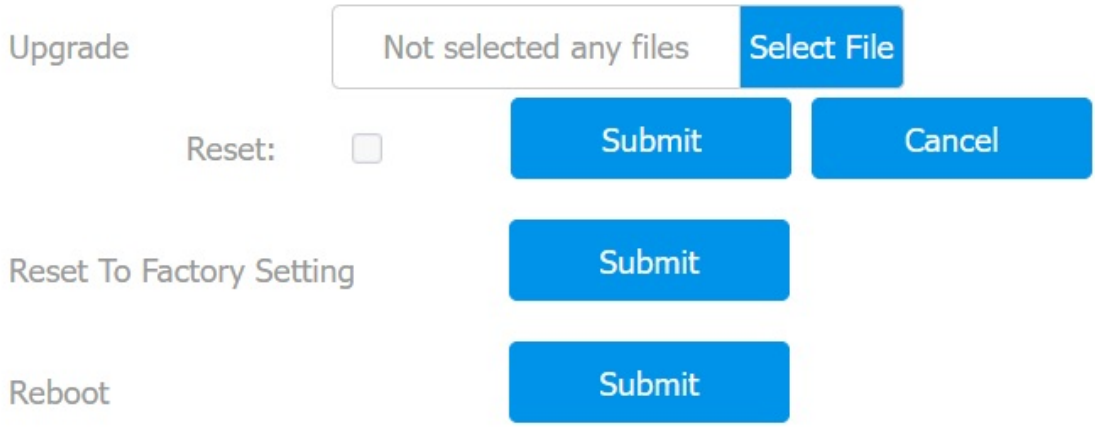
If you want to reboot the system setting of the device, you can operate it directly on the device setting screen or on the device web interface.



Reset

Reset on the Web

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



Reset on the Device

If you want to reset the device system to the factory setting, you can operate it directly on the device **Restore** screen.