

About This Manual



WWW.AKUVOX.COM



R29 SERIES DOOR PHONE

Administrator Guide

Thank you for choosing Akuvox R29 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 29.30.10.15 version, and it provides all the configurations for the functions and features of R29 series door phone. Please visit [Akuvox forum](#) or consult technical support for any new information or the latest firmware.

Product Overview



The Akuvox R29 series is an Android-based IP video door phone that combines audio and video communications, access control, and video surveillance. Its advanced Android OS, Cloud, and AI-based communication technologies allow for customization to meet your specific operational needs. The R29 series includes multiple ports for integrating external digital systems like access control and fire alarm systems, providing comprehensive control over building entrances and surroundings. It offers various secure access methods such as card, NFC, Bluetooth, QR code, voice control door access, and even body temperature measurement, ideal for residential buildings, office buildings, and complexes.

Change Log

















* Add High Security Mode

Model Differences

Model	R29C	R29S	R29C-B	R29C-L
Touch Screen	√	√	√	√
Relay In	3	3	3	3
Relay Out	3	3	3	3
Alarm In	X	X	X	X
RS485	√	√	√	√
Card Reader	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ
Wi-Fi	X	X	X	X
Bluetooth	√	X	√	√
Temperature Detection	X	X	√	X
Face Recognition	√	X	√	√
LTE	X	X	X	√
USB	X	X	X	X
External SD card	X	X	X	X

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 settings, 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 the 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 settings, RTP port setting, and device deployment, etc.
- **Phone:** this section includes time & language, call feature, dial management, data import&export, door log, and web relay.
- **Contacts:** this section involves contacts management.
- **Upgrade:** this section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.
- **Security:** this section is for password modification.

 Status 	
Basic	
 Intercom 	
 Account 	
 Network 	
 Phone 	
 Contacts 	
 Upgrade 	
 Security 	

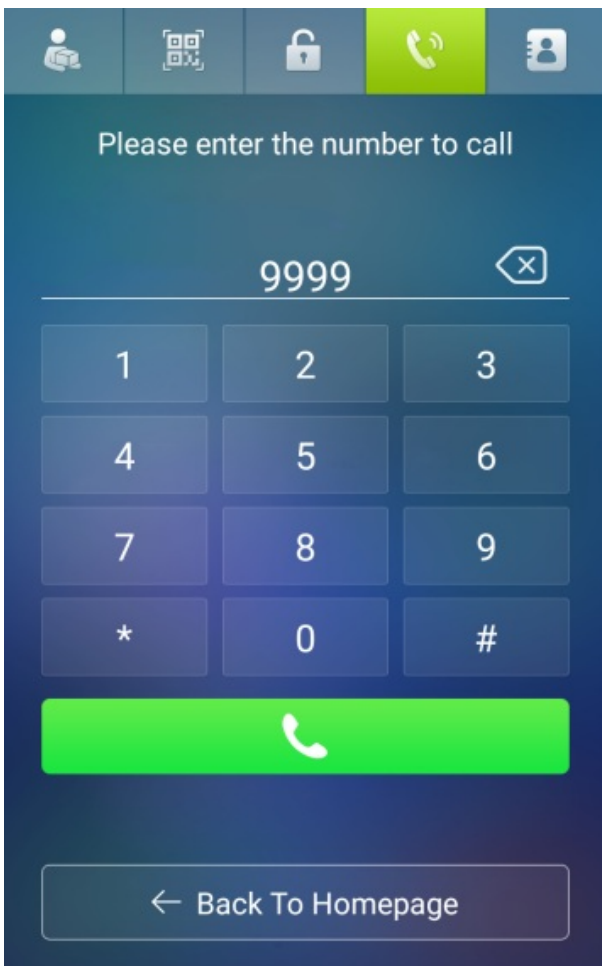
Product Information
Model
Firmware Version
Location
Network Information
IP Channel
Port Type
IP Address
Gateway
Alternate DNS Server
Account Information
Account1

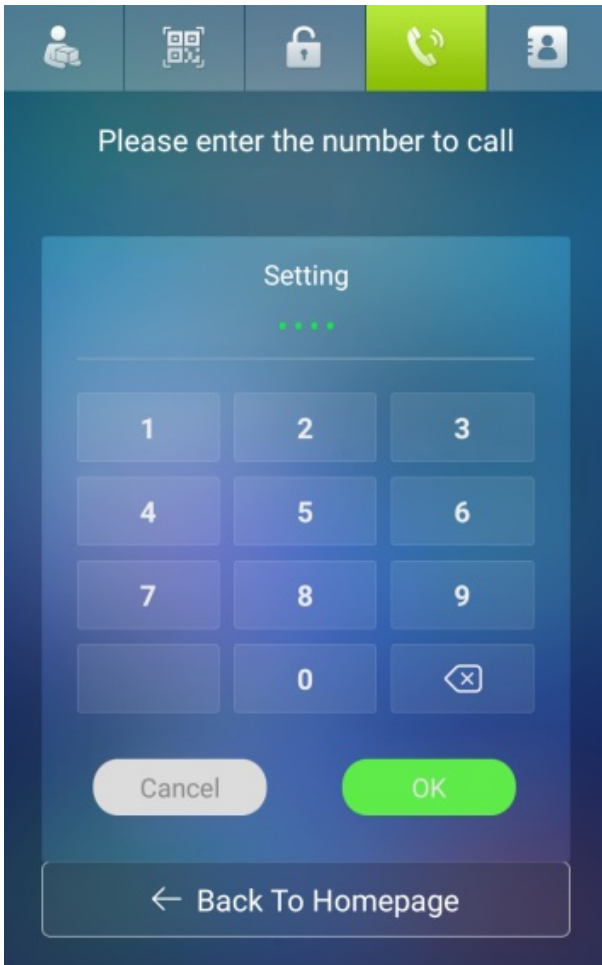
Access the Device

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

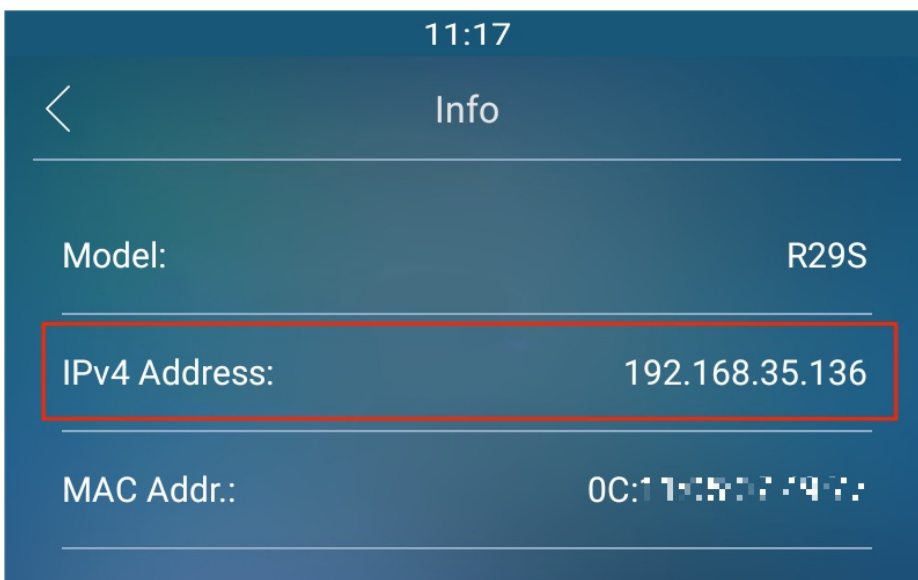
You can set up some basic settings on the device screen by pressing **9999 + Dial key + 3888** (password) on the Dial screen.

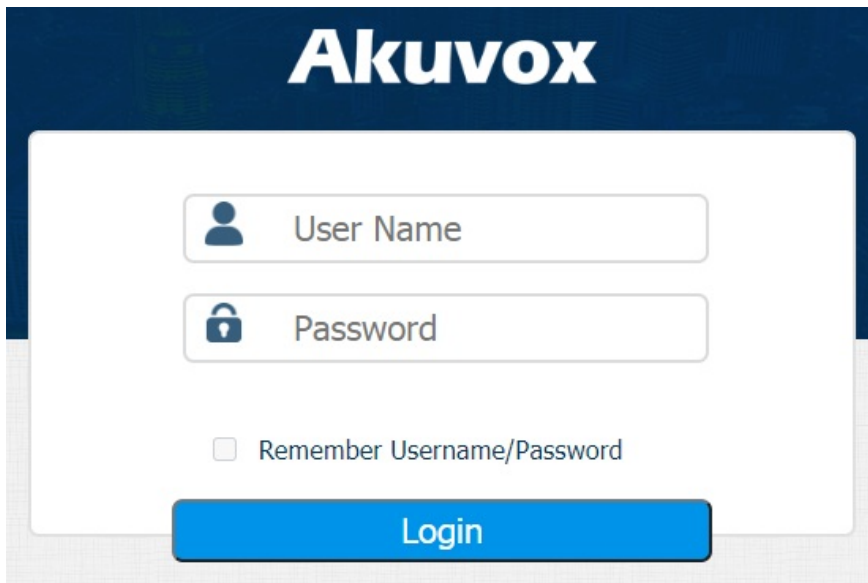




Access the Device Setting on the Web Interface

You can also enter the device IP address on the web browser to log in to the device web interface where you can configure parameters, etc. You can check the IP address on the device **Settings > Info** screen.





Akuvox

User Name

Password

Remember Username/Password

Login

Note

- You can obtain the device IP address using Akuvox IP scanner.
 - 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 user name 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.

Note

- R29Z/R29Z-L's language is Chinese by default, so there is no such option the first time it boots up.

Language Setting on the Device

To configure the language display on the device **Language** setting screen.



Language Setting on the Device Web Interface

To configure the language display on the device web interface **Phone > Time/Lang > LCD Language**.

- The device web supports the following languages:

English, Simplified Chinese, Traditional Chinese, Polish, Korean, Dutch, French, German, Japanese, and Russian.

- The device screen supports the following languages:

English, Simplified Chinese, Spanish, Danish, French, Czech, Traditional Chinese, Turkish, Japanese, German, Polish, Portuguese, Hungarian, Russian, Norsk, Korean, Swedish, Ukrainian, Azerbaijani, Hebrew, and Dutch.

Web Language

Mode

English



LCD Language

Mode

English



To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device. Navigate to **Phone > Time/Lang > Words of Language Upload** interface.

Words Of Language Upload

Type	File Status	Select File	Import	Export	Reset
Web	NULL	Not selected any files Select File	Import	Export	Reset

Note

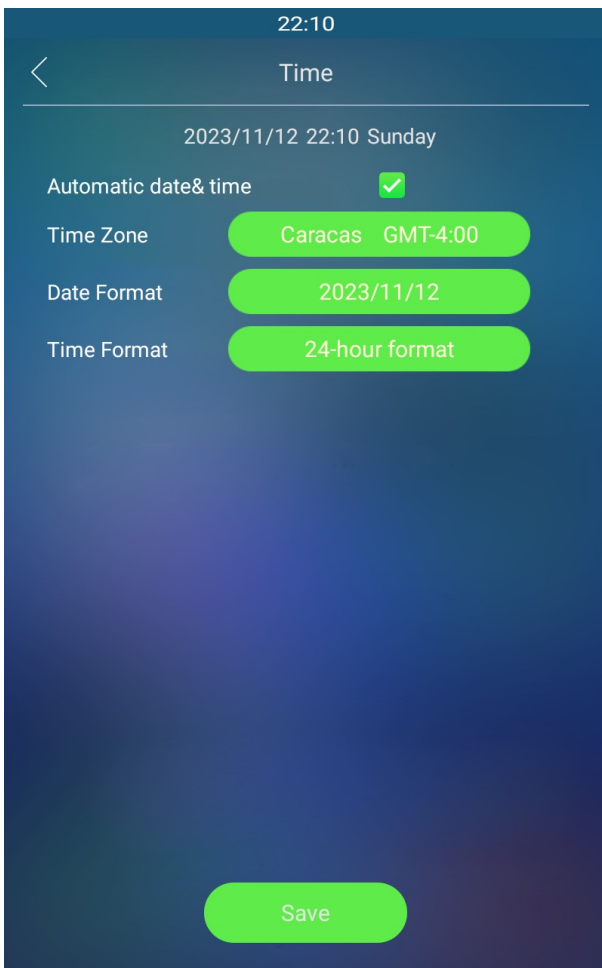
- R29Z/R29Z-L only supports English and Chinese for LCD and web display.

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 set up time settings on the device **Time** interface.



Parameter Set-up:

- **Automatic Date:** Automatic Date is switched 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 checking off the square box and then entering the time and date you want before pressing the **Save** tab for validation.

Time Setting on the Device Web Interface

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

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

The screenshot shows a web interface titled "Time" with a horizontal line below the title. Below the line, there are five settings:

- Automatic Date&Time**: A checkbox that is checked with a blue checkmark.
- TimeZone**: A dropdown menu showing "GMT+12:00" and "McMurdo" with a blue downward arrow.
- Date Format**: A dropdown menu showing "2022/02/10" with a blue downward arrow.
- Time Format**: A dropdown menu showing "24-hour format" with a blue downward arrow.
- NTP Server**: A text input field containing "pool.ntp.org".

Parameter Set-up:

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

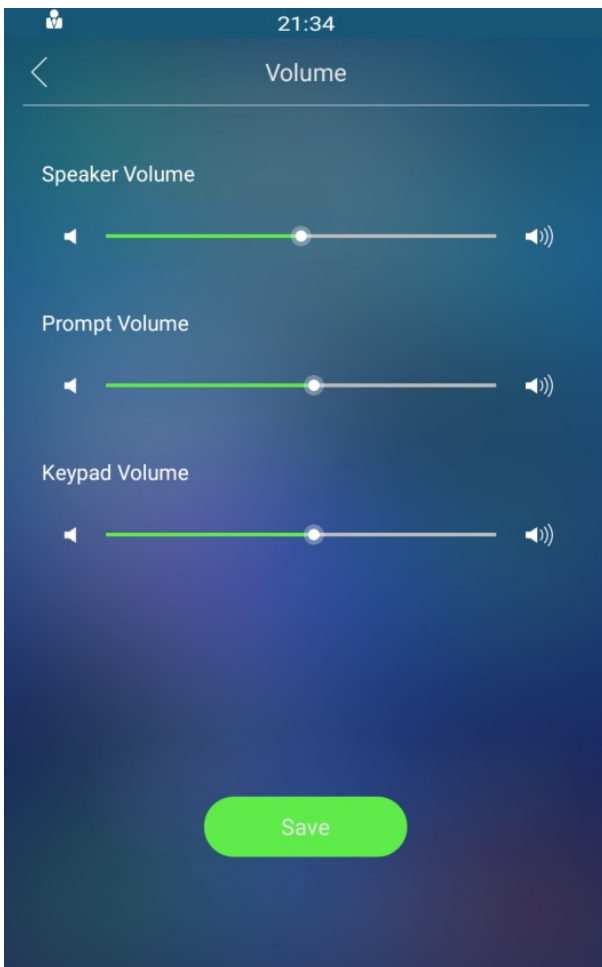
Volume and Tone Configuration

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

Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

To set up the volumes on the device **Volume** screen.



Parameter Set-up:

- **Prompt Volume:** adjust the announcement volume. The announcement can be, for

example, the open door success announcement, ringback sound, and other prompt sounds.

To set up the volume on the web interface, navigate to **Phone > Audio > Volume Control**.

Volume Control		
Mic Volume	<input type="text" value="60"/>	(1~127)
Speaker Volume	<input type="text" value="8"/>	(1~15)
Keypad Volume	<input type="text" value="8"/>	(0~15)
Tamper Alarm Volume	<input type="text" value="7"/>	(1~15)
Prompt Volume	<input type="text" value="8"/>	(0~15)

In addition, call volume can be configured on the web **Phone > Call Feature > Others** interface to allow you to adjust the volume when you are answering the call.

Others	
Return Code When ...	<input type="text" value="486(Busy Here)"/>
Call Volume	<input checked="" type="checkbox"/>

Note:

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

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.

Open Door Tone Setting

Open Door Outside ...

Open Door Inside S...

Open Door Failed Te...

Open Door Outside ...

Open Door Inside To...

Open Door Failed To...

Guiding Tone Of Contact List

Guiding Tone Mode

Apartments 



















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.
- **Open Door Inside Succeeded Text Prompt:** tick the check box if you want to see the text prompt after opening the door by pressing the exit button.
- **Open Door Failed Text Prompt:** tick the check box if you want to see the prompt words after the door open failure.
- **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.
- **Open Door Failed Tone:** enable it so that you can hear the tone when door opening fails.
- **Guiding Tone Mode:** select Apartment or Building guiding tone for the contact list screen.

Upload Tones

You can upload various types of tones for door openings and tones for the various types of icons etc on the **Phone > Import/Export > Upload Tone** interface.

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
3	Hello	Not selected any files	Select File	 Import	 Reset
4	Calling	Not selected any files	Select File	 Import	 Reset
5	Delivery	Not selected any files	Select File	 Import	 Reset
6	Temp Key	Not selected any files	Select File	 Import	 Reset
7	PIN	Not selected any files	Select File	 Import	 Reset
8	Dial	Not selected any files	Select File	 Import	 Reset
9	Contacts	Not selected any files	Select File	 Import	 Reset
10	InputA Triggered	Not selected any files	Select File	 Import	 Reset
11	InputB Triggered	Not selected any files	Select File	 Import	 Reset
12	InputC Triggered	Not selected any files	Select File	 Import	 Reset

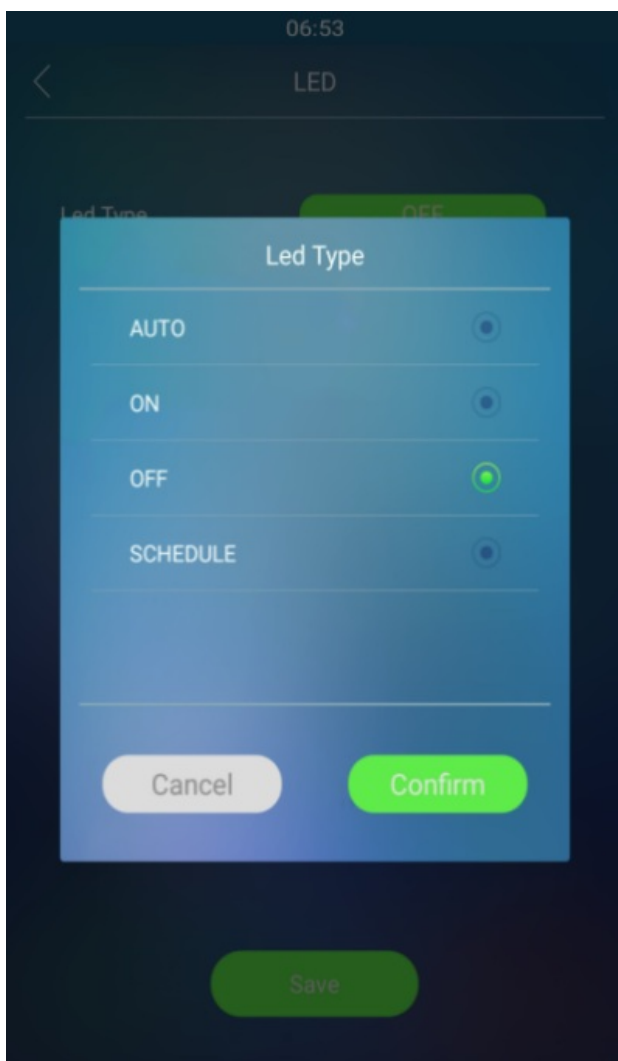
 Reset All

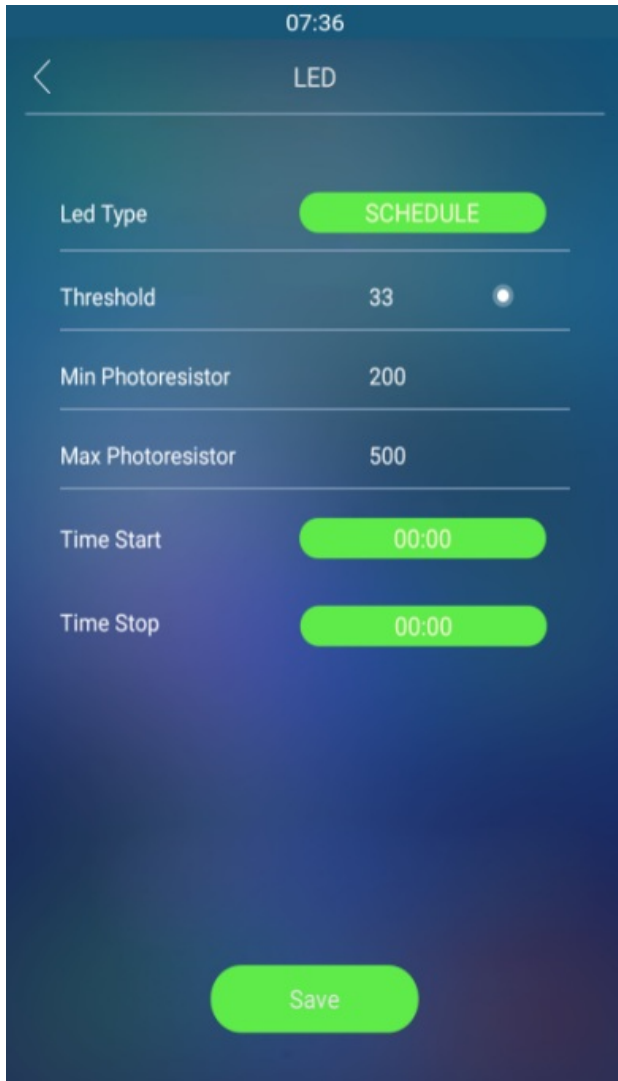
LED & LCD Setting

Infrared LED Setting on the Device


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.

To configure the infrared LED setting on the device LED interface.





Parameter Set-up:

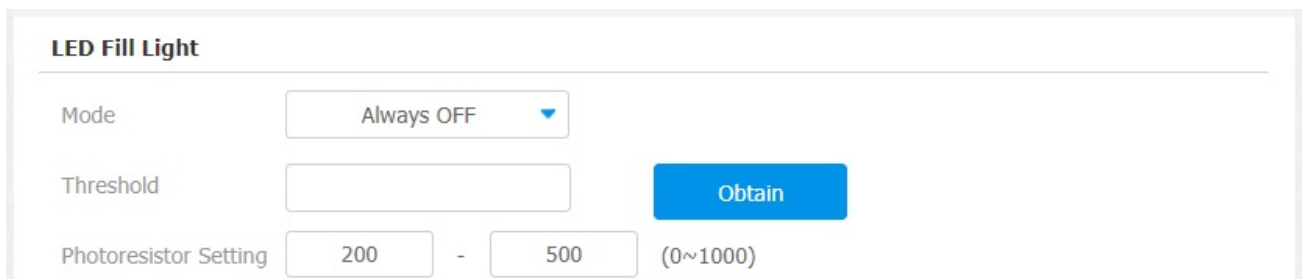
- **LED Type:** you can see the LED type **Auto**, **ON**, **OFF**, **Schedule** you selected.
- **Threshold:** refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is 33, however, you can tap the icon  several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on configuring 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. The default minimum and maximum photoresistor value are **200** and **500** respectively.

Note

- The threshold value will not be shown on the screen unless you change the LED type to either **Auto** or **Schedule**.

Infrared LED Setting on the Web Interface

You can also select the LED type on the device web **Intercom > LED Setting > LED Fill Light** interface if needed.




LED Fill Light

Mode: Always OFF

Threshold: [] Obtain

Photoresistor Setting: 200 - 500 (0~1000)

Parameter Set-up:

- **Mode:** you can see the LED type **Auto**, **Always ON**, **Always OFF**, **Schedule** you selected.
- **Threshold:** refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is **33**, however, you can tap the icon  several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on configuring the minimum and maximum photo-resistor values.
- **Photoresistor Setting:** set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the **ON-OFF** of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. The default minimum and maximum photoresistor values are **200** and **500** respectively.

LED Setting on Card Reader Area

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

Navigate to **Intercom > LED Setting > LED Control** interface.

Parameter Set-up:

- **Time (H):** enter the time span for the LED lighting to be valid, e.g. if the time span is from 18-22 it means LED light will stay on during the time span from 6:00 pm to 10:00pm 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.

Navigate to **Intercom > Advanced > LCD** interface.

Parameter Set-up:

- **Mode:** you can see the LED type **Auto**, **Always ON**, **Always OFF**, **Schedule** you selected.
- **Threshold:** refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is **33**, however, you can tap the icon



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

- **Photoresistor Setting:** set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the **ON-OFF** of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. The default minimum and maximum photoresistor values are 200 and 500 respectively.

LED White Light Setting

White light LED is mainly used to reinforce the lighting for the QR code access and for the greater visibility of the visitors when seeing their images from indoors in a dark environment.

You can set the white light function properly on the device web **Intercom > Advanced > White Light** interface.

The screenshot shows the 'White Light' configuration page. It has a title 'White Light' at the top. Below the title, there are three settings: 'Mode' with a checked checkbox, 'Limit Backlight Value' with a text input field containing '50' and a range '(0~255)', and 'White Light PWM Va...' with a text input field containing '40' and a range '(0~100)'.

Parameter Set-up:

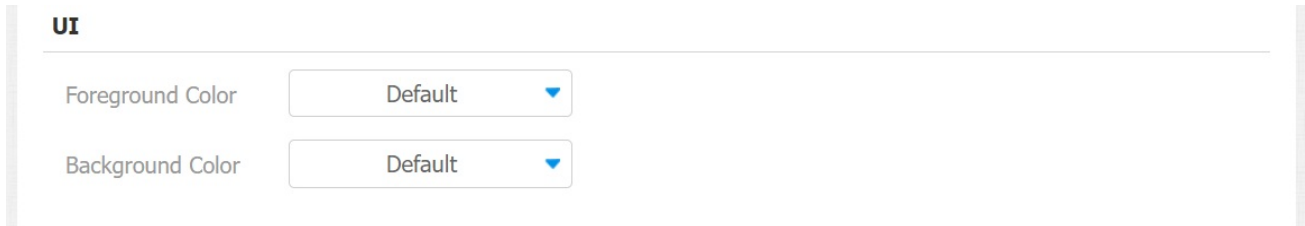
- **Max White Light Value:** set the white light value from 0-255, and the default white light value is “50”.
- **White Light PWM Value:** set the white light PWM value from 0-100. PWM value affects the white light brightness that is set with the same white light value. For example, if the white light value remains the same, and you bring up the PWM value, you will get brighter white light. In short, the higher the PMW value is the brighter the light is.

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.

Home Screen Display Setting

You can configure the home screen background display and the foreground colors for **Villa** mode, **Building** mode, and **Office** mode home screen display according to your preference on the web **Intercom > Advanced > UI** interface.



The screenshot shows a web interface for configuring the UI. At the top, the word "UI" is displayed in a bold, dark font. Below it, there are two rows of settings. The first row is labeled "Foreground Color" and has a dropdown menu currently set to "Default". The second row is labeled "Background Color" and also has a dropdown menu currently set to "Default". The interface is clean and modern, with a light gray background and a white border around the settings area.

Parameter Set-up:

- **Foreground Color:** select among four foreground color options: **Default**, **Black**, **White**, and **Custom**. The default foreground color is **White**.
- **Background Color:** select among four foreground color options: **Default**, **Black**, **White**, and **Custom**. The default foreground color is **Blue**. If you select **Custom**, you can customize your foreground and background color by adjusting the color and hue controller underneath and pressing the **Submit** tab for validation.

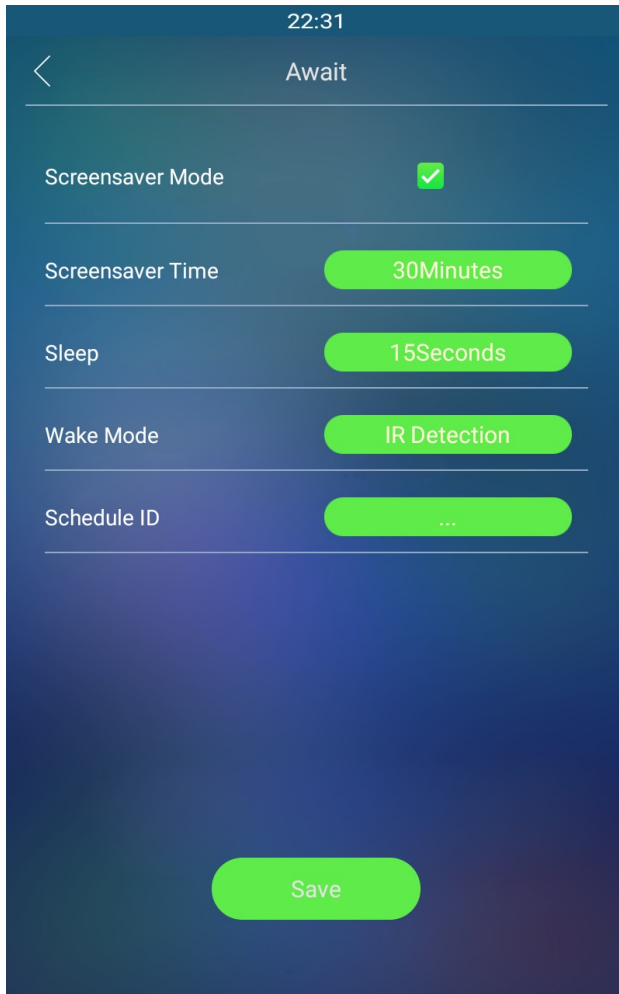
Note

- If you want to select **Custom**, you need to click the **Submit** tab before you can see a color and hue controller with which you can adjust the color to your preference, and you are required to click **Submit** tab again for validation.

Await Screen Setting

Await Screen Setting on the Device

Await screen function is for screen protection. It allows the device to enter an idle status for a preset duration when there is no activity or no one is detected approaching the device. To configure it by tapping **Await** on the device screen.



Parameter Set-up:

- **Screensaver Time:** set up the screen saver display duration from 5 seconds to 2 hours. The screensaver display will start when the device goes into sleep mode.
- **Sleep:** set up the sleep mode timing from 5 seconds to 30 min. For example, if you set it to 10 seconds, then the device will go into sleep mode when detecting no approaching object or no operation on the device. When the screen saver is disabled, the device screen will be turned off.
- **Wake Mode:** select the method for the screen awake mode. Select **IR Detection** if you want to awake the screen via IR detection. Select **Manual** if you want to awake the screen by touching the screen. Select **video detection** if you want to awake the screen by video-based motion detection.
- **Schedule ID:** select the schedule to apply the screensaver settings.

Await Screen Setting on the Web Interface

You can also conduct the await screen configuration on the web **Intercom > Advanced > Standby Interface**.

Standby Interface Display

Screensaver Mode

Screensaver Time

Sleep

Wake Mode

All Schedules

1001:Always
1002:Never

Schedules Selected

1001:Always



Parameter Set-up:

- **Screensaver Mode:** enable the screen saver mode if needed.
- **Screensaver Time:** set up the screen saver display duration from 5 seconds to 2 hours. The screensaver display will start when the device goes into sleep mode.
- **Sleep:** set up the sleep mode timing from 5 seconds to 30 min. For example, if you set it to **10 seconds**, then the device will go into sleep mode when detecting no approaching object or no operation on the device. When the screen saver is disabled, the device screen will be turned off.
- **Wake Mode:** select the method for the screen awake mode. Select **IR Detection** if you want to awake the screen via IR detection. Select **Manual** if you want to awake the screen by touching the screen. Select video detection if you want to awake the screen by video-based motion detection.
- **Schedule:** select the schedule to apply the screensaver settings.

Upload Screen Saver

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

Navigate to **Phone > Import/Export > Upload Screensaver Picture**. You are allowed to upload a maximum of 5 pictures, and each picture will be displayed in rotation according to the ID order with the specific time duration (**Play Time**) you set.

Upload ScreenSaver Picture

ID	File Status	Play Time	Submit	Delete
1	File Exists	<input type="text" value="5"/>	Submit	Delete
2	File Exists	<input type="text" value="5"/>	Submit	Delete
3	File Exists	<input type="text" value="5"/>	Submit	Delete
4	File Exists	<input type="text" value="5"/>	Submit	Delete
5	File Exists	<input type="text" value="5"/>	Submit	Delete

Please Choose ScreenSaver ID for upload Image1 ▾

Screensaver1 Not selected any files [Select File](#) [Upload](#)

(Support Size:2M; format:jpg)

Parameter Set-up:

- **Play Time:** the time for playing the screensaver picture. The time ranges 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 there is repetitive designation of pictures to the same ID order.

Upload Pictures for Alphanumeric Mode Screen Display

Go to **Phone > Import/Export > Import Alphanumeric Theme Background(.png)**.

Import Alphanumeric Theme Background (.png)

(Max picture size: 1MB, Recommend resolution: 800*1280.)

Main Page:	Not selected any files	Select File	Import 	Reset
Other Pages:	Not selected any files	Select File	Import 	Reset

Parameter Set-up:

- **Main Page:** upload the picture for the poster display. Visitors need to tap the poster (screen) first before they can go to the home screen.
- **Other Page:** upload the picture for a background display for the screens other than the poster screen display.

Note:

- The pictures uploaded should be in **png format**.
- This function can be applied to both the home screen background and the contact screen background.
- The recommended picture resolution is 800*1280.

Upload Background Picture in the Time-displaying Area

You can upload pictures on the web **Phone > Import/Export > Import Villa/Office Call Page Time View** interface as the background for the time-displaying area on the dial screen in Villa mode and Office mode.

Import Villa/Office Call Page Time View (.png)

(Max picture size: 1MB, Recommend resolution: 800*314.)

Picture

Not selected any files

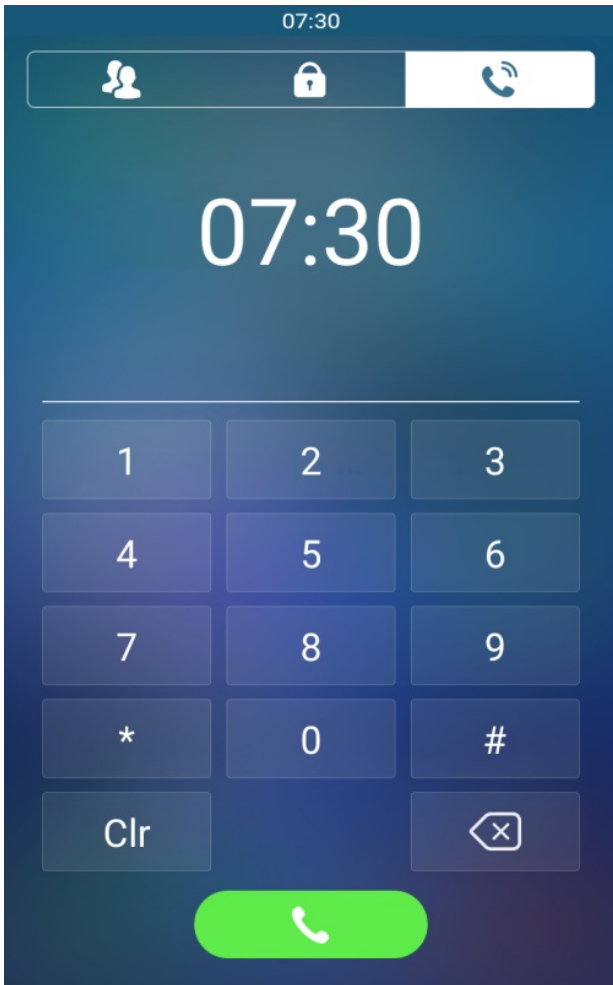
Select File



Import



Reset



Note:

- This function can only be applied in the Villa mode and Office mode.
- Pictures uploaded should be in png format with 1 MB in maximum.
- The ideal picture size is 800*314 in order to achieve the best effect.

Upload Device Booting Image

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

To configure the configuration on the web **Phone > Import/Export > Boot Animation (.png / .zip)** interface.

Boot Animation (.png / .zip)

(Max .zip file size: 20MB; Max picture size: 1MB, Max resolution: 800*1280.)

File

Not selected any files

Select File

Import

Reset

Upload Device Logo

You can navigate to **Phone > Import/Export > Import Alphanumeric Theme Logo (.png)**.

Import Alphanumeric Theme Logo (.png)

(Max picture size: 1MB, Recommend resolution: 500*150.)

Logo Picture:

Not selected any files

Select File



Import



Reset

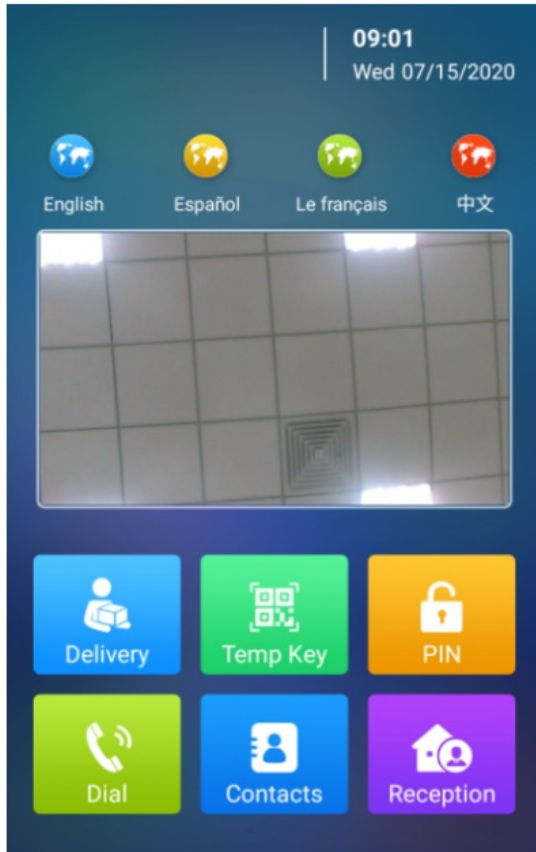
Configuration for Scenario-based Screen Display Mode

The door phones offer you four types of screen display modes for different applications: Building mode, Villa Mode, Office Mode, and Alphanumeric Mode.

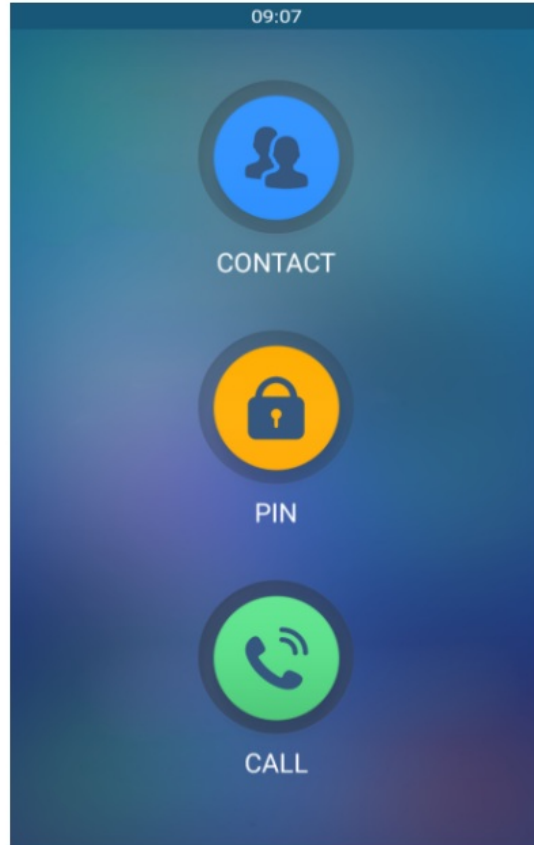
You can make the configuration on the device web **Intercom > Key/Display > Theme** interface to select the specific mode based on actual application scenarios.

Theme	
Theme	<input type="text" value="Building"/>

Please refer to the default home screen display of the application based modes below:



Building Mode Screen Display



Villa Mode Screen Display



Alphanumeric Mode Screen Display

Office mode screen display is not shown here as it shares a similar home screen display with that of Villa mode, however, the two modes vary in terms of their dial screen displays that will be explained in the following sections.

Building Mode Home Screen Configuration

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

Navigate to **Intercom > Key/Display > Key In Homepage Of The Building Theme** interface.

Key In Homepage Of The Building Theme

Voice Prompts

ID	Name	Type	Value
1	<input type="text"/>	<input type="text" value="Delivery"/>	<input type="text"/>
2	<input type="text"/>	<input type="text" value="Temp Key"/>	<input type="text"/>
3	<input type="text"/>	<input type="text" value="PIN"/>	<input type="text"/>
4	<input type="text"/>	<input type="text" value="Dial"/>	<input type="text"/>
5	<input type="text"/>	<input type="text" value="Contact"/>	<input type="text"/>
6	<input type="text"/>	<input type="text" value="Speed Dial"/>	<input type="text"/>

Tips When OpenDoor Failed

Parameter Set-up:

- **Type:** select the tab type corresponding to the ID order which indicates the tab position. For example, if you want to make the **Temp Key** tab to be displayed in the first position of the first tab row, you can click to select the type of the ID order 1. And you can change the other tab position accordingly.
- **Name:** enter a new name to replace the original type name, but it does not change the attribute of the type.
- **Value:** it is available for those features that need to be set up numbers, like the Speed Dial feature.

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

Parameter Set-up:

- **Type:** select the **Type** field for the tab type you need.
- **Select Icon:** select by clicking the tab icon you need.

Note

- The uploaded picture should be in .png format.
- Max picture size: 1MB.
- Recommend resolution: 218*176.

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

Parameter Set-up:

- **Language:** select **Visible** and **Invisible** respectively if you want the four language icons to be displayed or concealed on the home screen.
- **Language 1/2/3/4:** select the order of the language display. For example, if you set language 1 as English, then the English language will be displayed first from left to right on the screen.

Villa Mode Home Screen Configuration

You can configure the screen display for the layout of the Tenant icon, PIN icon, and Call icon on the home screen in villa mode.

Navigate to **Intercom > Key/Display > Key In Homepage Of The Office Theme And Villa Theme** interface.

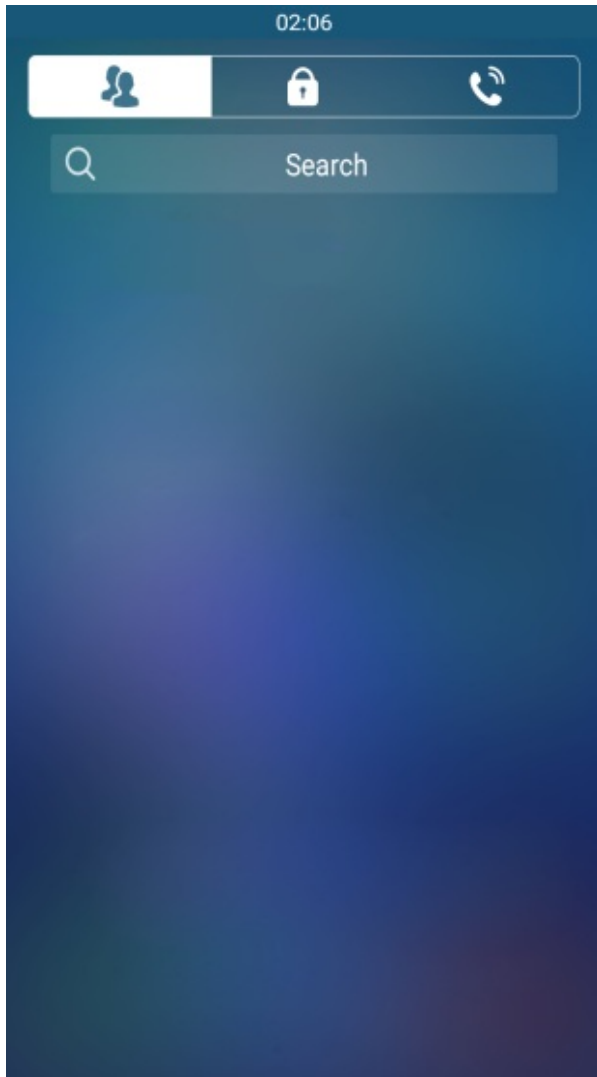
Key In Homepage Of The Office Theme And Villa Theme

Display Type: Homepage ▼

ID	Type	Name	Visible
1	Contact ▼	<input type="text"/>	Visible ▼
2	PIN ▼	<input type="text"/>	Visible ▼
3	Call ▼	<input type="text"/>	Visible ▼

Parameter Set-up:

- **Display Type:** click to select the home screen display type among the four options **Homepage, Dial, Contact, and Password**. **Homepage** is for the default home screen display of three vertical round icons, while **Dial** (Call icon), **Contact** icon, and **Password** (PIN icon) as a whole can be set up as a home screen. For example, when you switch from Building mode to Villa mode, while your previous villa mode home screen display type is **Homepage**, then the three round icons for **Contact, PIN, and Call** will be all displayed. However, if your previous display type is any one of the **Dial, Contact, Password** types, then the corresponding icons for **Dial, Contact, and Password** will be displayed in highlight together on the top of the home screen as the home screen display instead of the three round icons for the **homepage**.
- **Type:** set the type of icon you want to display on the villa mode home screen.
- **Name:** name the icons on the villa mode home screen.
- **Visible:** select **Visible** or **Invisible** for the three icons.



Note:

- Homepage type screen display will be denied if all of the icons are set **Invisible**.

Alphanumeric Mode Home Screen Configuration

Alphanumeric Mode is used in the apartment with room number that carries both English alphabetic and numbers.

You can navigate to **Intercom > Key/Display > Display Setting Of The Alphanumeric Theme.**

Display Setting Of The Alphanumeric Theme

Wall Mode

Homepage Visible

Page	Name (English)	Name (traditional Chinese)	Default Keypad
Homepage	<input type="text" value="Touch screen to continue"/>	<input type="text" value="點擊屏幕繼續"/>	<input type="text" value=""/>
Choose Tower or Concierge	<input type="text" value="Please choose Tower or Concierge"/>	<input type="text" value="請選擇座號或者管理處"/>	<input type="text" value="Alphabet"/>
Choose Floor	<input type="text" value="Please choose floor and press"/>	<input type="text" value="請選擇樓層及按"/>	<input type="text" value="Digital"/>
Choose Flat	<input type="text" value="Please choose flat and press"/>	<input type="text" value="請選擇單位及按"/>	<input type="text" value="Alphabet"/>
Enter PIN	<input type="text" value="Please enter the PIN code and"/>	<input type="text" value="請輸入密碼然後按"/>	<input type="text" value=""/>
Scan QR Code	<input type="text" value="Please scan the QR code"/>	<input type="text" value="請掃描二維碼"/>	<input type="text" value=""/>

Name (English)	Name (traditional Chinese)	Type
<input type="text" value="Concierge"/>	<input type="text" value="管理處"/>	<input type="text" value="Speed Dial"/>
<input type="text" value="QR Code"/>	<input type="text" value="二維碼"/>	<input type="text" value="Temp Key"/>
<input type="text" value="PIN"/>	<input type="text" value="密碼"/>	<input type="text" value="PIN"/>

Alphabet Keypad A B C D E F G H I J K L M

N O P Q R S T U V W X Y Z

Digital Keypad B G 0 1 2 3 4 5 6 7 8 9

Enabled Items Speed Dial Temp Key PIN Tower Floor Flat

Flat Length

Parameter Set-up:

- **Wall Mode:** enable it if you want to set it as the most peripheral device. Visitors can only be allowed to tap **Speed dial** tab (Concierge), **Temp Key** tab (QR code), **PIN** tab on the home screen(with dial pad), and they are not allowed to make calls by typing in the tower,

floor, and flat in wall mode.

- **Homepage Visible:** enable it if you want to display a poster. For example, you can enable it if you want visitors to see a poster (screen) before going to the home screen.
- **Name:** create the prompts to be displayed on the different screens **Home page, Choose Tower or Concierge, Choose Floor, Enter PIN, Scan QR Code.**
- **Default Keypad:** select numerical keypad or alphabetical keypad for Tower and Flat keypad.
- **Name:** change the icon names for **Concierge, QR Code, and PIN** if needed.
- **Alphabet Keypad:** select the alphabetical letters you want to display on the keypad.
- **Enable Items:** select to show or hide **Speed dial tab (Concierge), Temp Key tab (QR code), PIN tab, and Floor and Flat** on the screen.
- **Flat Length:** select from **1, 2 or less, 3 or less, and 4 or less.**

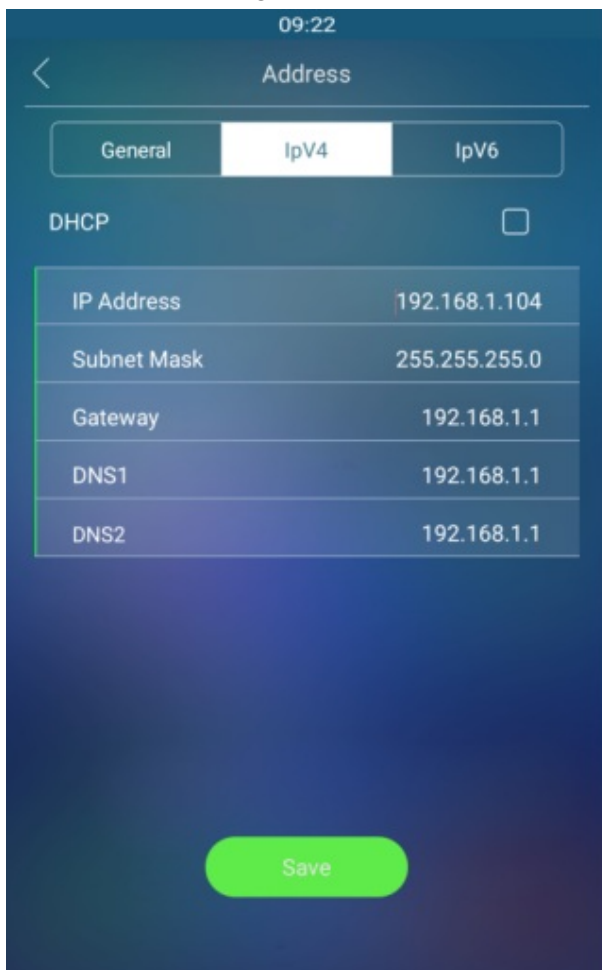


Network Setting

Device Network Connection Setting

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

To check and configure the network connection on the device **Network** screen.



Parameter Set-up:

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

- **IP Address** : set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **DNS1/DNS2**: set up DNS1/ DNS2 (**Domain Name Server**) according to your actual network environment. DNS1 is the primary DNS server address while DNS2 is the secondary server address and the door phone connects to the DNS2 server when the primary DNS server is unavailable.


To check the network on the web **Status > Network information** Interface.

Network Information

IP Channel	IPv4		
Port Type	DHCP Auto	Link Status	Connected
IP Address	192.168.36.115	Subnet Mask	255.255.255.0
Gateway	192.168.36.1	Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8		

To check and configure network connection on the device web **Network > Basic > LAN Port** interface.

LAN Port

IP Channel	IPv4 		
IPv4	<input checked="" type="checkbox"/> DHCP	<input type="checkbox"/> Static IP	
IP Address	<input type="text" value="192.168.1.104"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>	Preferred DNS Server	<input type="text" value="192.168.1.1"/>
Alternate DNS Server	<input type="text" value="192.168.1.1"/>		
IPv6	<input checked="" type="checkbox"/> DHCP	<input type="checkbox"/> Static IP	
IP Address	<input type="text"/>	Subnet Prefix Length	<input type="text"/>

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 set up device local RTP on the device web **Network > Advanced > Local RTP** interface.

Local RTP

Starting RTP Port (1024~65535)

Max RTP Port (1024~65535)

Parameter Set-up:

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

Device Deployment in Network

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

So you can do it on the web **Network > Advanced > Connect Setting** interface.

Connect Setting

Server Mode Cloud

Discovery Mode

Device Address

Device Extension

Device Location

Parameter Set-up:

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

NAT Setting

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

To set up NAT, you can do it on the web **Account > Advanced > NAT** interface.



The screenshot shows the NAT configuration page with the following settings:

- NAT** (Section Header)
- UDP Keep Alive Mes...**
- UDP Alive Msg Inter...** (5~60s)
- RPort**

Parameter Set-up:

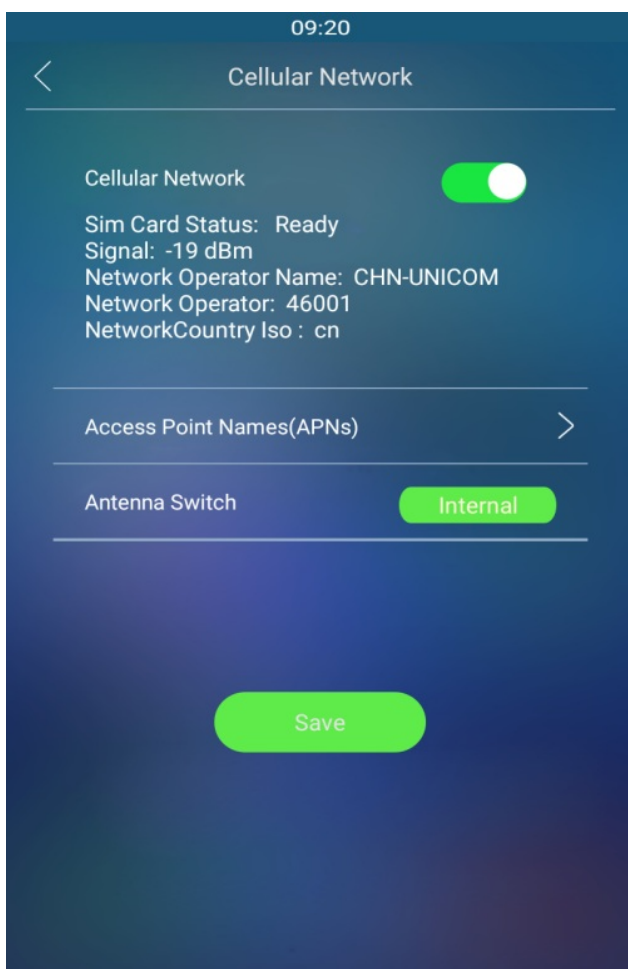
- **UDP Keep Alive Messages:** if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Msg Interval:** set the message sending time interval from 5-60 seconds, the default is 30 seconds.

- **RPort**: enable the Rport when the SIP server is in WAN (**Wide Area Network**).

LTE Wireless Connection Setting (Optional)

The LTE module enables cellular network connectivity for the device in areas where wired networks are unavailable, particularly beneficial for installations in older buildings.

Only R29C-L has an LTE module and the LTE setting can only appear after the SIM card is inserted. To configure the LTE setting on the device **Cellular Network** screen.




Parameter Set-up:

- **Cellular Network**: move the toggle switch on and off to enable or disable the LTE function.
- **Access Point Name (APNs)**: check the Cellular Network provider for the Access Point.

- **Antenna Switch:** select internal and external antenna for signal transmission. The internal antenna is a built-in antenna in the device while the external antenna is optional and is used to reinforce the signal in the compromised network environment.

LTE Data Usage Control

LTE data usage can be checked on the device web **Network > Data Usage** interface.

Data Information	
Data Used	0GB0MB 
Data Remaining	--
Data Plan Setting	
Unlimited Data	<input type="text" value="Enabled"/>
Data Limit	<input type="text" value="40"/> <input type="text" value="GB"/>
Data Reminders	<input type="text" value="80"/> %
	Action to execute when data usage reaches 80% (32G) of Monthly limit.
Start Date	<input type="text" value="1"/> (1~31)
Action To Execute	<input type="checkbox"/> Email <input type="checkbox"/> HTTP
HTTP URL	<input type="text"/>

Parameter set-up:

- **Unlimited Data:** select **Enabled** if you have unlimited data package and vice versa. The setting is disabled by default.
- **Data Limit:** set the data limit according to your actual amount of data package. The data limit is 40 GB or MB.
- **Data Reminders:** set the data percentage point to trigger the notification. For example, if the data percentage point reaches the default value 80, notification actions will be executed.

- **Start Date:** set the start date of a month to start data usage monitoring from **1 to 31**. The start date is **1** by default. For example, if you set the start date as **1** then the end day will be the last day of the month, however, if the start date is **2**, then the end date will be **23:59** of the first day of the next month. Moreover, if a month is less than 31 days, then the end date will be the last day of the month before renewing data usage monitoring on the first day of the next month.
- **Action To Execute:** click **Email** or **HTTP URL** for the Email notification or notification via HTTP URL when the data usage reaches the limit.
- **HTTP URL:** enter your **HTTP URL** for the notification purpose.

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.

Navigate to **Phone > Call Feature > Direct IP** interface.



The screenshot shows a configuration panel for 'Direct IP'. At the top, the title 'Direct IP' is displayed. Below the title, there are two settings: 'Enabled' with a checked checkbox, and 'Port' with a text input field containing '5060' and a range '(1~65535)' to its right.

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

SIP Call & SIP Call Configuration

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

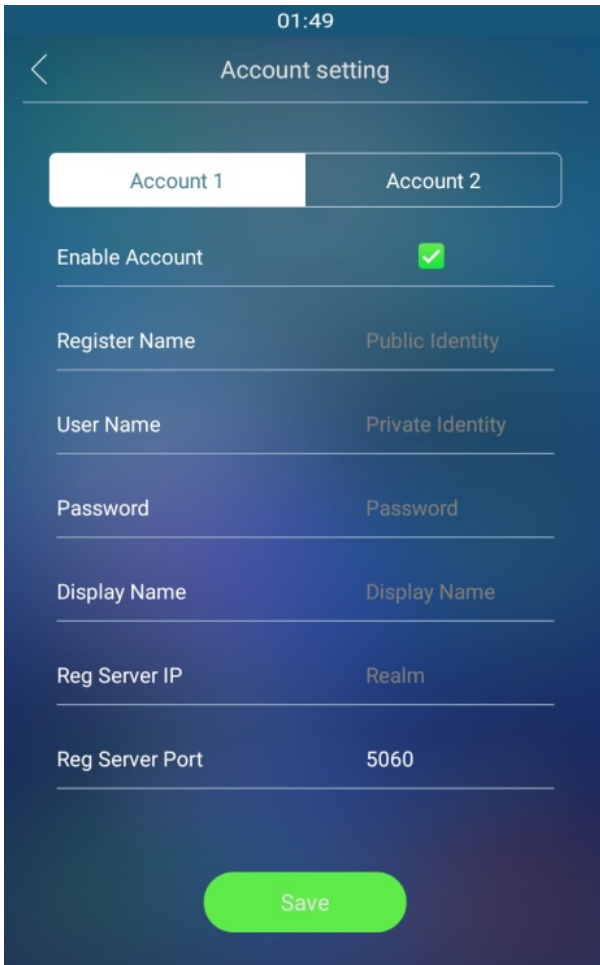
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Account Registration

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

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

To configure the SIP account on the device **Account** screen.



- **Account 1/Account 2:** The door phone supports 2 SIP accounts.
 - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.
 - The system switches to Account 2 if Account 1 is not registered.
 - To designate the account to be used for outgoing calls, select the account number for contacts or dial plan prefixes in their settings.

Tip

For configuring contact call and dial plan, see [here](#).

- **Reg Server port:** Specify the SIP account registration server port. The default is 5060. You can find the port information on the indoor monitor's PBX screen, or from third-party server providers.

Tip

See [how to register SIP account](#).

Some SIP account registration settings are only accessible through the device's web interface at **Account > Basic > SIP Account**.

SIP Account

Status	<input type="text" value="Registered"/>
Account	<input style="border-bottom: 1px solid #ccc;" type="text" value="Account 1"/>
Account Enabled	<input checked="" type="checkbox"/>
Display Label	<input type="text" value="..."/>
Display Name	<input type="text" value="CARACA"/>
Register Name	<input type="text" value="..."/>
User Name	<input type="text" value="..."/>
Password	<input type="password" value="....."/>

- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** Choose the account for configuration.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same as the username from PBX server.
- **User Name:** Same as the username from PBX server for authentication.
- **Password:** Same as the password from PBX server for authentication.

SIP Call DND&Return Code Configuration

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

You can set up DND-related parameters properly on the device web **Phone > Call Feature > DND** interface.

DND

Enabled

Return Code When ... ▼

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

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 SIP server, go to **Account > Basic > Preferred SIP Server/ Alternate SIP Server**.

Preferred SIP Server

Server IP	<input type="text" value="39.108.62.163"/>	
Port	<input type="text" value="5070"/>	(1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535s)

Alternate SIP Server

Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535s)

- **Server IP:** Enter the server's IP address or its domain name.
- **Port:** Specify the SIP server port for data transmission.
- **Registration Period:** Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified period.

Outbound Proxy Server configuration

An outbound proxy server receives and forwards all requests the designated server. It is an optional configuration, but if set it up, all future SIP requests get sent there in the first instance.

To configure the outbound proxy server, go to the device web **Account > Basic > Outbound Proxy Server** interface.

Outbound Proxy Server

Outbound Enabled

Server IP

Port (1024~65535)

Backup Server IP

Port (1024~65535)

- **Server IP:** Enter the SIP proxy IP address.
- **Port:** Set the port for establishing a call session via the outbound proxy server.
- **Backup Server IP:** Enter the SIP proxy IP address to be used when the main proxy malfunctions.
- **Port:** Set the proxy port for establishing a call session via the backup outbound proxy server.

Data Transmission Type Configuration

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

To do the configuration on the device web **Account > Basic > Transport Type** interface.

Transport Type

Transport Type UDP ▼

UDP

TCP

TLS

DNS-SRV

Cancel

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

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

Max Local SIP Port	56592	(1024~65535)
Min Local SIP Port	56582	(1024~65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input checked="" type="checkbox"/>	

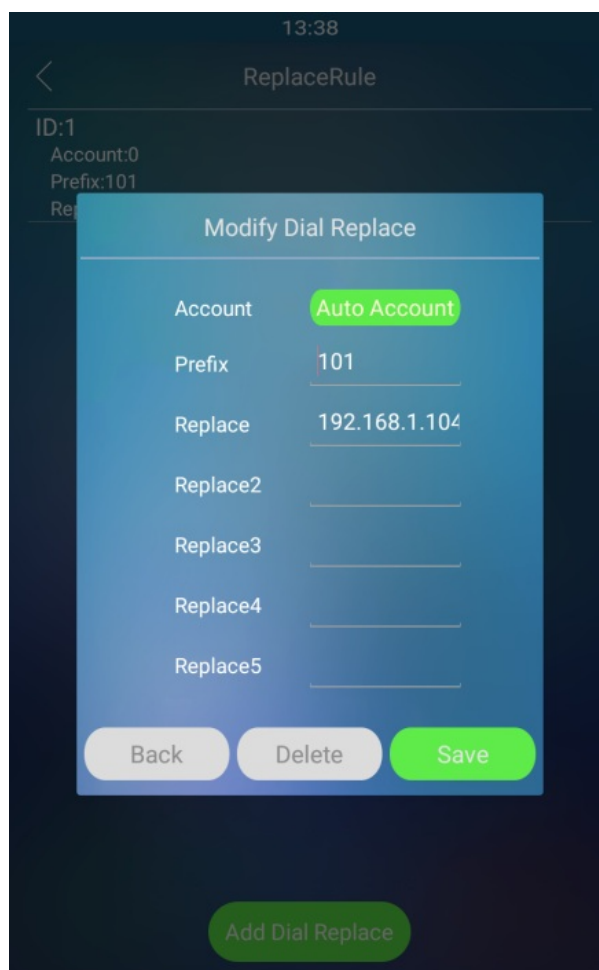
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users private and secret information from potential hackers during SIP calls.

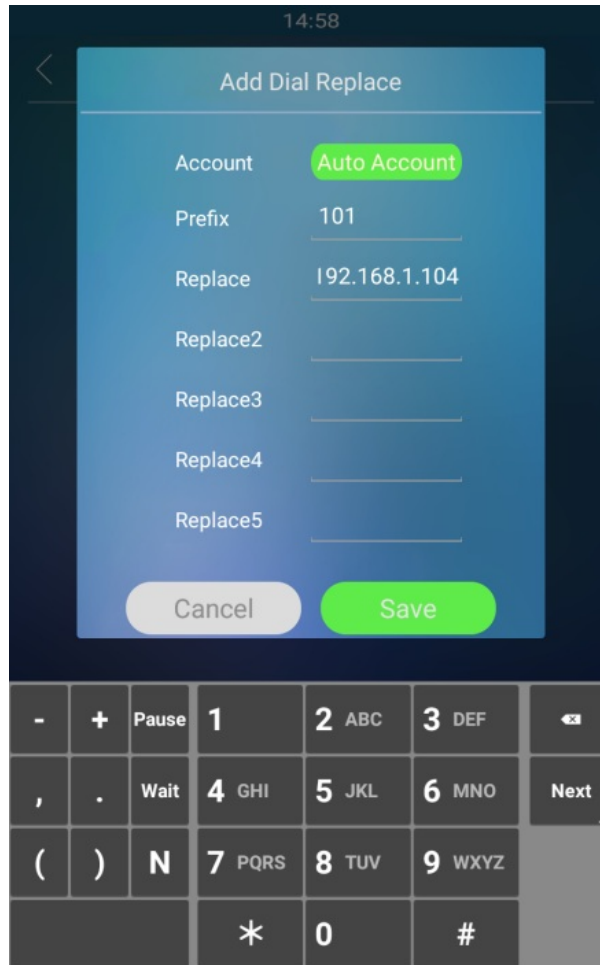
Dial Options Configuration

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.

To configure the number replacement on the device **ReplaceRule** screen.





- **Account:** Select the dial-out account.
 - **Auto:** Dial-out using the registered account. When there are 2 registered accounts, Account 1 is the default.
 - **Account 1/2:** Dial-out using the chosen account.
- **Prefix:** Specify a short number to replace the specified dialed numbers.
- **Replace 1/2/3/4/5:** Specify up to 5 numbers, which can be SIP number or IP address, to be replaced by the prefix. All these numbers will be called simultaneously when the caller dials the prefix.

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

Dial Plan

Rules Management

Not selected any files [Select File](#) [Import](#) [Export](#)

<input type="checkbox"/> Index	Account	Prefix	Replace 1	Replace 2	Replace 3	Replace 4	Replace 5
<input checked="" type="checkbox"/> 1	Auto	1111	192.168.31.3				
<input type="checkbox"/> 2							
<input type="checkbox"/> 3							
<input type="checkbox"/> 4							

Note:

- To modify a dial plan rule, check its box, and the Edit tab will appear.

Quick Dial Using Configured Dial Name

You can create one dial name on the **Quick Dial** screen in both villa mode and office mode on the device directly. You can press the dial icon by the dial name to make calls.

7:30 AM

< Quick Dial

Show Quick Dial

Quick Dial Name manager

Quick Dial Number 112

Save

7:30 AM

Contacts Lock Call

manager Call

1	2	3
4	5	6
7	8	9
*	0	#
Clr		⌫

Call

- **Show:** Displays either the time or speed dial buttons on the dial screen.
- **Quick Dial Name:** The name of the quick-dial contact.
- **Quick Dial Number:** The SIP number or IP address of the contact.

Note:

- This function only applies to Villa and Office themes.

Tip

See how to configure [Quick Dial](#).

Import/Export the Speed Dial Contacts

To import and export the speed dial contacts, navigate to **Phone > Speed Dial > Import/Export Speed Dial Contacts(.xml)**.

Import/Export Speed Dial Contacts(.xml)

Not selected any files

Speed Dial on the Home Screen

Speed dial is a feature that enables the creation of tabs or organized tab combinations to be displayed on the device's dial screen. By pressing these specific tabs, you can make swift calls without the need to enter any dial numbers.

To configure the speed dial on the web **Phone > Speed Dial > Speed Dial Contacts Management** interface.

Speed Dial Theme

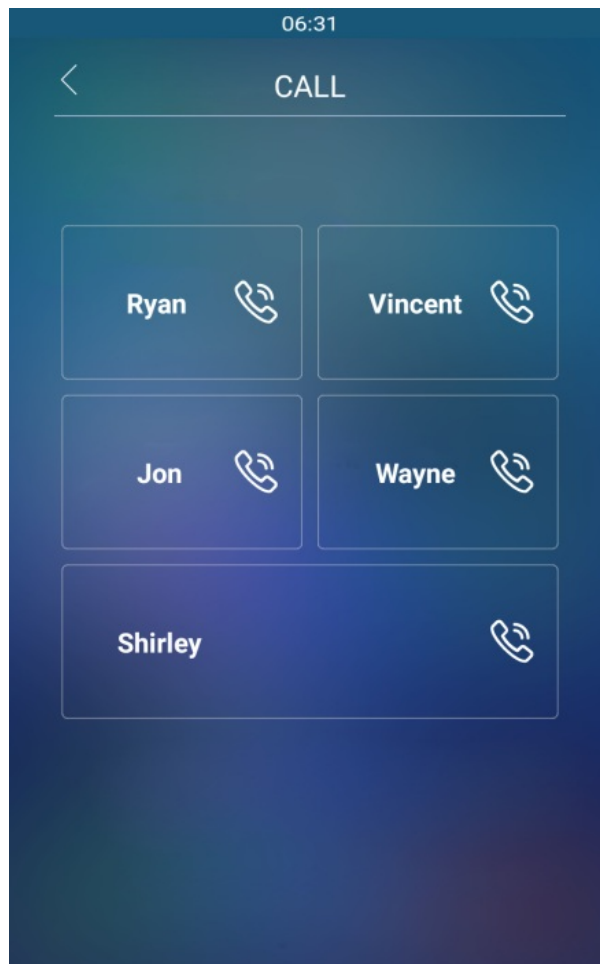
Speed Dial Theme

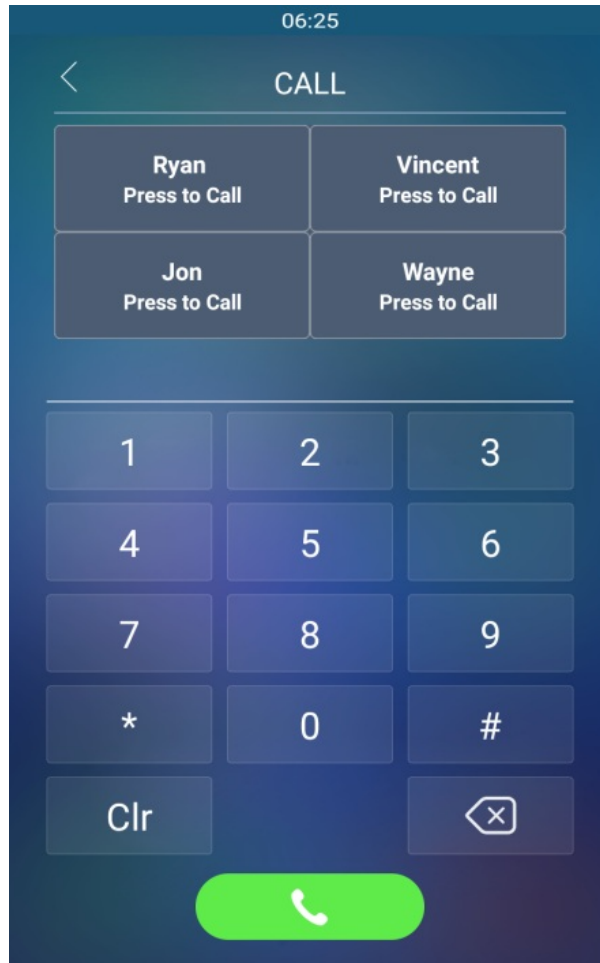
Speed Dial Contacts Management

Index	Name	Number	Submit	Clear
1	<input type="text" value="Ryan"/>	<input type="text" value="1001"/>	<input type="button" value="Submit"/>	<input type="button" value="Clear"/>
2	<input type="text" value="Jim"/>	<input type="text" value="1002"/>	<input type="button" value="Submit"/>	<input type="button" value="Clear"/>
3	<input type="text"/>	<input type="text"/>	<input type="button" value="Submit"/>	<input type="button" value="Clear"/>

- **Speed Dial Theme:** Define layouts for speed dial buttons and the keypad on the dial screen. The 9 options are explained as follows:

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





Note:

- This function exclusively applies to Villa and Office themes.

Group Speed Dial

R29 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 all the contact numbers in the group at the same. You can navigate to **Intercom > Key/Display > Speed Dial Setting**.

Speed Dial Setting

Speed Dial (Cloud)

Group ▼

Dial Out Forward

- **Group:** Determine whether to disable this function and specify the group to which it should be applied. Once selected, the phone will speed-dial all its included contacts.

Dial Key Order

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

You can navigate to Intercom > Key/Display > Keypad Display Mode of PIN Interface.



- **Display Mode:** Determine the layout of the keys in the keypad. Selecting Disorder will randomize the positions of the keys on the device.

Call Setting

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 Auto Answer feature, go to **Account > Advanced > Call** interface.

Call

Max Local SIP Port (1024~65535)

Min Local SIP Port (1024~65535)

Auto Answer

Prevent SIP Hacking

Video Transport Type

Once the feature is enabled, navigate to **Phone > Call Feature > Auto Answer** interface.

Auto Answer

Auto Answer Delay (0~5 Sec)

Mode

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

Sequence Call Configuration

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

To configure the sequence call, go to **Intercom > Basic > Sequence Call** interface.

Sequence Call

Enabled	<input type="checkbox"/>
Time Out(Sec)	<input type="text" value="20"/>
When Refused	<input type="text" value="Do Not Call Next"/>

- **Time Out(Sec):** Specify the time limit for the call between two sequential call numbers. For example, if the time value is set to 10, the call that is not answered in 10 seconds will be ended automatically and transferred to the next call number in order.
- **When Refused:** Determine whether to call the next if a call was rejected by the previously called party.
 - **Do Not Call Next:** The sequence call will stop when the call is refused.
 - **Call Next:** The device will call the next number in order when the call is refused.

Note:

- Sequence Call function requires Akuvox SmartPlus cloud service. To use this function, please contact Akuvox technical support.

Web Call Configuration

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

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

Web Call

Web Call Number	Auto ▼	Dial Out	Hang Up
-----------------	--------	----------	---------

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 do this configuration on the device web **Intercom > Basic > Max Call Time** interface.

Max Call Time

Max Call Time (2~30 Min)

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

Maximum Dial Duration Setting

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

To do this configuration on the device web **Intercom > Basic > Max Dial Time** interface.

Max Dial Time

Dial In Time (5~120 Sec)

Dial Out Time (5~120 Sec)

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

Hang Up After Open Door

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

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

Hang Up After Open Door

Enable

Type

Time Out (0~15 Sec)

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

Two-way Video Call

R29 allows you to have two-way video calls with the callee so that you can see the callee's video image. You can navigate to **Intercom > Basic** interface.

Basic

Gesture Control

Two-Way Video Ena...

Call Priority

Device Mode

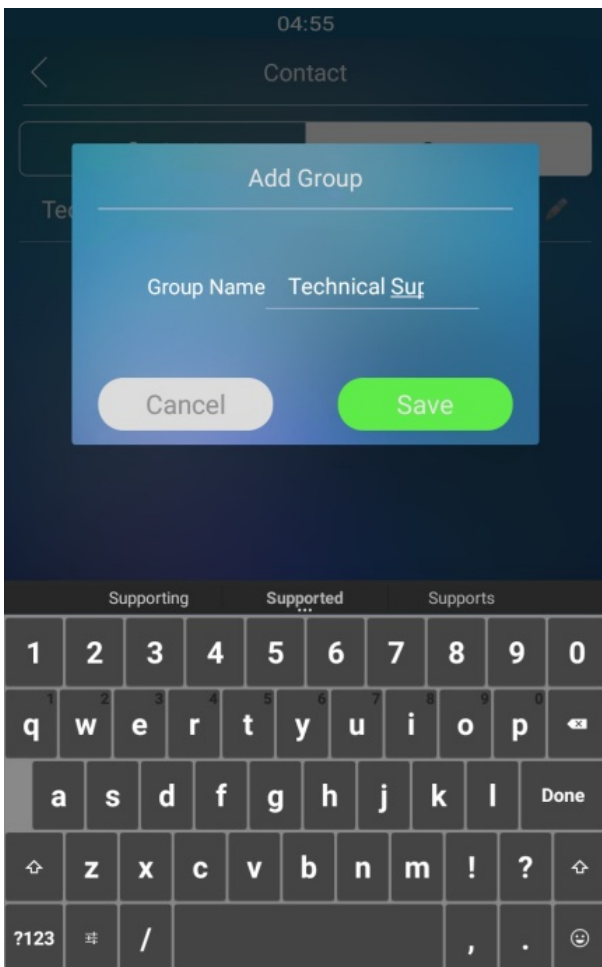
- **Two-Way Video Enabled:** Activate this feature to allow callers to see the called party's video stream during a video call. If both parties have this function enabled, they can view each other's video streams.

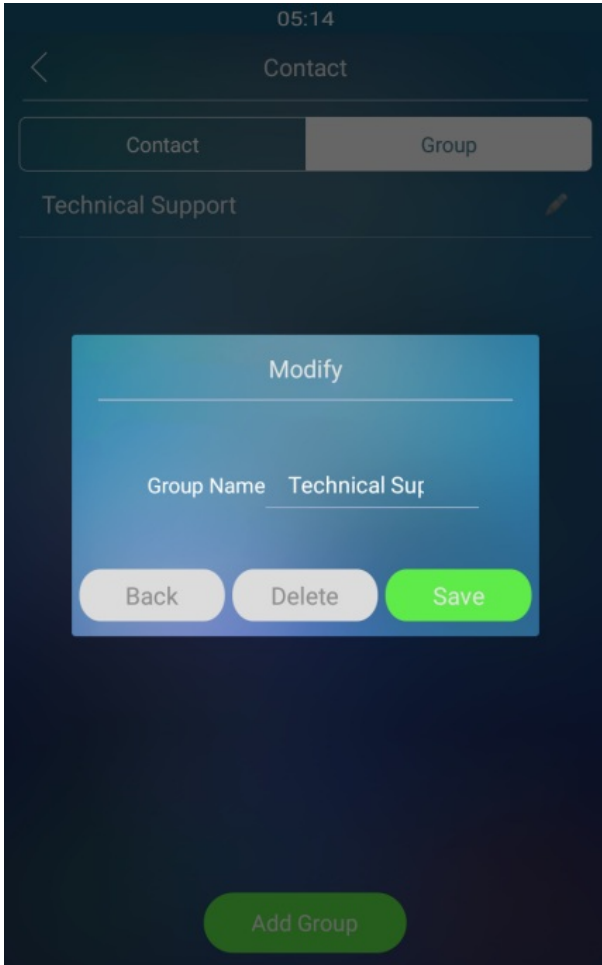
Phone Book Configuration

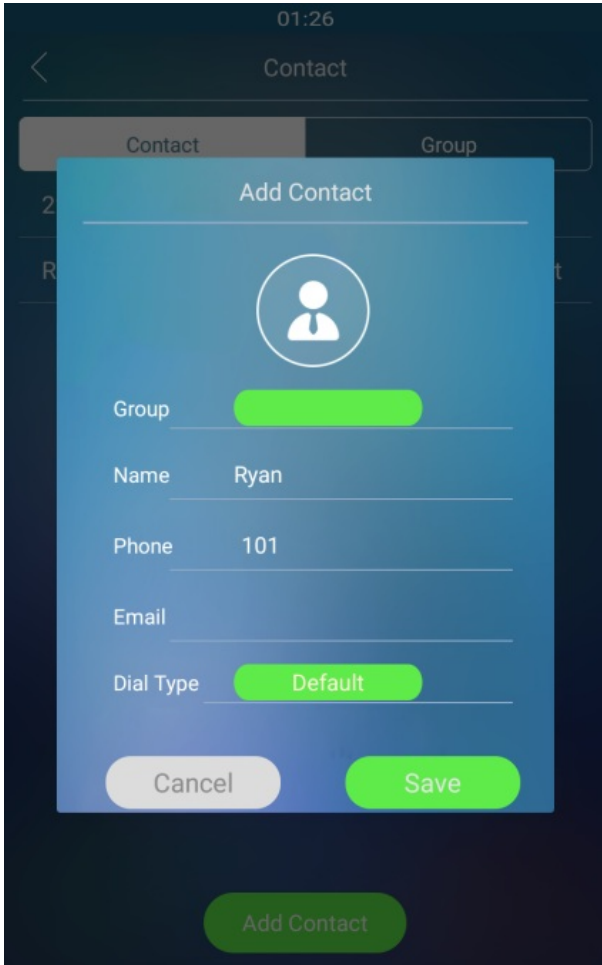
Phone Book Configuration on the Device

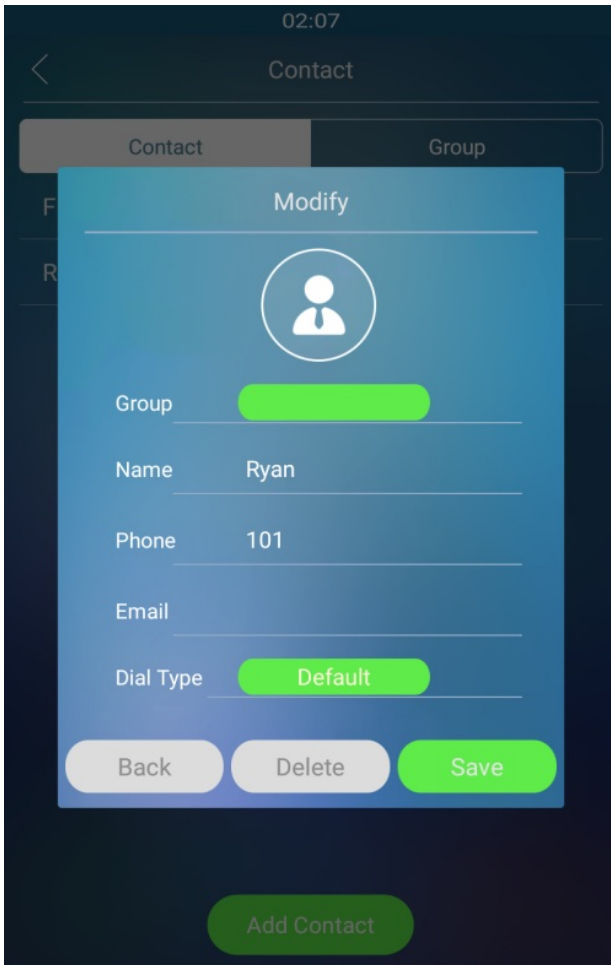
You can create contact groups for users.

To configure the phone book on the device **Contact** 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 the default option, then the contact number will be called out from SIP account 1 if the contact numbers are set up in both SIP Account 1 and 2.

Note:

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

Phone book Configuration on the Web Interface

Manage Contact Groups on the Web Interface

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

Navigate to **Contacts > Contacts List > Group** interface.

Group

<input type="checkbox"/>	Index	Name
<input checked="" type="checkbox"/>	1	Technical Sup..
<input type="checkbox"/>	2	Sales

1/1

Group Setting

Name

Contact Configuration on the Web Interface

Contact can also be configured on the web **Contacts > Contacts List > Contacts Setting** interface where you can also upload the contact pictures if needed.

Contacts Setting

Name

Phone

Email

Group

Dial Account

Lift Floor Number

Photo

Note: **Please upload the photo before editing contact if necessary**

Original Photo Cropped Photo

Parameter Set-up:

- **Phone:** the phone number of the contact. It supports IP address and SIP number.
- **Group:** choose a default or pre-configure group for the contact. Or choose Hidden Contacts to hide this contact.
- **Dial Account:** choose one high priority account to call out the contact.
- **Lift Floor Number:** Enter the floor number of the contact if needed.

Note:

- The recommended contact picture size is 2M and .jpg, png format.

Contact Management

You can search, display, edit, and delete the contacts in your contacts list on the web.

To do this configuration on device web **Contacts > Contacts List > Local Contacts List.**

Local Contacts List

Contacts List Display

Search

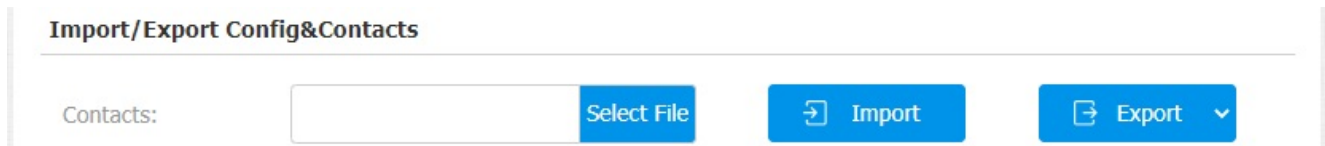
<input type="checkbox"/> Index	Name	Phone	Group	Dial Account	Email	FloorNum	Priority Of Call
<input checked="" type="checkbox"/> 1	Ryan	1003	Default	Default		0	NULL
<input type="checkbox"/> 2							
<input type="checkbox"/> 3							
<input type="checkbox"/> 4							
<input type="checkbox"/> 5							
<input type="checkbox"/> 6							
<input type="checkbox"/> 7							
<input type="checkbox"/> 8							
<input type="checkbox"/> 9							
<input type="checkbox"/> 10							

1/1

Contacts Import and Export on the Web Interface

When the contact becomes so many that you cannot afford to manage each contact one by one manually, you can import and export the contacts in batch on the device web.

Navigate to **Phone > Import/Export > Import/Export Config&Contacts** interface.



Import/Export Config&Contacts

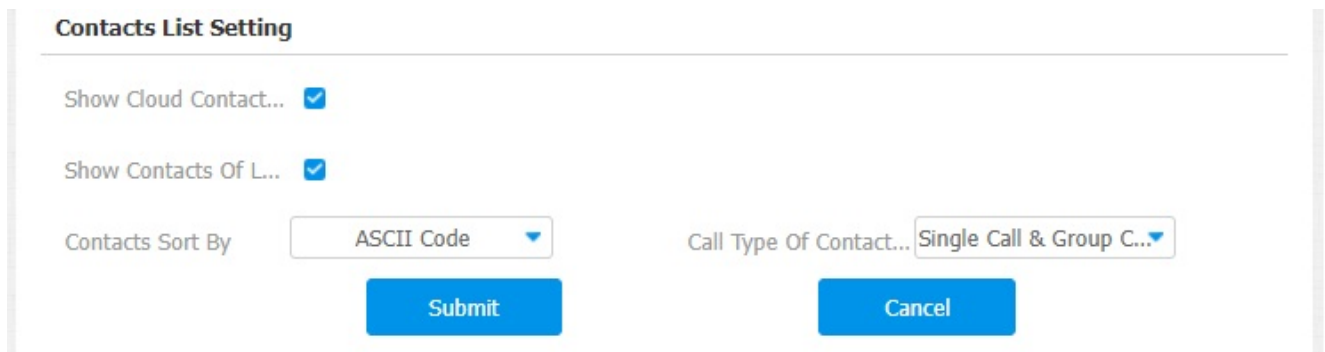
Contacts: **Select File** **Import** **Export** ▾

Note:

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

Contacts List Setting

To configure contacts list setting, navigate to **Contacts > Contact List > Contact List Setting**.



Contacts List Setting

Show Cloud Contact...

Show Contacts Of L...

Contacts Sort By Call Type Of Contact...

Submit **Cancel**

Parameter Set-up:

- **Show Cloud Contacts Enabled:** enable it if you want the contacts synchronized from SmartPlus to be displayed on the contact screen.
- **Show Contacts Of Local Group:** enable it if you the local contacts to be displayed on the contact screen.

- **Contacts Sort By:** select the display order of the contacts. Select **ASCII Code** if you want the contacts to be displayed in an order based on ASCII code; select **Room Number** if you want the contacts to be displayed in an order based on room numbers. Select **Import**.
- **Call Type Of Contact:** if you select **Single Call & Group Call**, you are allowed to make the call to individual contact person or to a contact group on the door phone. If you select **Only Single Call**, you are only allowed to make the call to individual contact person. If you select **Only Group Call**, you are only allowed to make calls to a contact group.

Contact List Display Setting

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

Navigate to **Intercom > Basic > Door Setting General** interface.

Door Setting General

Click Tenants To Dial...

Expand Tenants List ...

Hide Group Label Fo...

Contact List Search ...

Local Tenants Profile... Enabled ▼

DialPad Input Numb... Default ▼

Parameter Set-up:

- **Click Tenants To Dial:** select **Enable** or **Disable** the dial-out by pressing the contact tab. When it is enabled you can press anywhere on the contact tab to dial out. When it is disabled, you need to press the Call icon in the middle of the tab to dial out.
- **Expand Contact List View Mode:** select **Enable** or **Disable** to control contact tab size. For example, if you select **Enable** then the contact tab will be widened. And the tab will turn to normal size when the function is disabled.

- **Hide Group Label For Contact List:** select enable or disable to control the display of the group label. If you select disable, then only the contact tab will be displayed while the group tab will be concealed and vice versa.
- **Contact List Search Box Visible:** select Visible or Invisible to control the display of the **Tap here to search** field on the top of the screen. If you select **invisible**, then the **Tap here to search** field will be concealed.
- **Local Tenants Profile Display Mode:** enable or disable the function. If the function is enabled the uploaded contact profile picture is displayed next to the contact's name, if disabled the picture will not be displayed. Select **Auto** if you want to display the default contact picture.
- **Dial Pad Input Number Limit:** set the limit of numbers that can be entered on the dial pad. You can select 4,6,8,10 digits.

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.

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

SIP Account

Account Account 1 ▼

Audio Codecs

Disabled Codecs

>>

<<

Enabled Codecs

G722

PCMU

PCMA

↑

↓

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 do the configuration on device web **Account > Advanced > Video Codec** interface.

Video Codec

Name	<input checked="" type="checkbox"/> H264
Resolution	VGA ▼
Bitrate	512 ▼
Payload	104 ▼

Parameter Set-up:

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

Door Access Control Configuration

Relay Switch Setting

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

Relay			
Relay			
Relay ID	RelayA	RelayB	RelayC
Type	Default state	Default state	Default state
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	5	5	5
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	#	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	Relay1	RelayB	RelayC

- **Relay ID:** The specific relay for door access. Please note that R29Z/R29ZL has only one relay available.

- **Type:** Determine the interpretation of the Relay Status regarding the state of the door:

- **Default State:** A “Low” status in the Relay Status field indicates that the door is closed, while “High” indicates that it is opened.

- **Invert State:** A “Low” status in the Relay Status field indicates an opened door, while “High” indicates a closed one.

- **Mode:** Specify the conditions for automatically resetting the relay status.

- **Monostable:** The relay status resets automatically within the relay delay time after activation.

- **Bistable:** The relay status resets upon triggering the relay again.

- **Trigger Delay (Sec):** Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **DTMF Mode:** Set the digits of the DTMF code.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-Digit.
- **2-4 Digit DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status:** Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).
- **Relay Name:** Assign a distinct name for identification purposes.

Note

External devices connected to the relay require separate power adapters.

Web Relay Setting

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



To set up a web relay, go to **Phone > Web Relay** interface.

Web Relay

Web Relay

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

Web Relay Action Setting

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

- **Type**: Determine the type of relay activated when employing door access methods for entry.

- Disabled: Only activate the local relay.

- WebRelay: Only activate the web relay.

- Both: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.

- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **User Name**: The user name provided by the web relay manufacturer.
- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.
- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

NOTE

If the URL includes full HTTP content (e.g., `http://admin:admin@192.168.1.2/state.xml?relayState=2`), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., `"state.xml?relayState=2"`), the relay uses the entered IP address.

- **Web Relay Key:** Determine the methods to activate the web relay based on whether the DTMF code is filled.

- Filling with the configured DTMF code restricts activation to card swiping and DTMF.
- Leaving it blank enables all door-opening methods.

- **Web Relay Extension:** Specify the intercom device and the methods it can use to activate the web relay during calls.

- When an intercom device's IP/SIP is specified, only that device can trigger the web relay (except for via card swiping or DTMF) during calls.

- If left blank, all devices can trigger the relay during calls.

Security Relay Setting

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



To set up the security relay, navigate to **Intercom > Relay > Security Relay**.

Security Relay

Relay ID	Security Relay A
Connect Type	RS485
Trigger Delay(Sec)	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>
1 Digit DTMF	<input type="text" value="2"/>
2~4 Digits DTMF	<input type="text" value="013"/>
Relay Name	<input type="text" value="Security Relay A"/>
Enabled	<input type="checkbox"/>

- **Connect Type:** The security relay connects to the door phone using RS485 by default.
- **Trigger Delay (Sec):** Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **Hold Delay (Sec):** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode in the Relay section above is set to 1-Digit.
- **2~4 Digits DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Name:** Name the security relay. The name can be displayed in door opening logs. When connecting to the SmartPlus Cloud, the Cloud server will automatically assign the relay name.

Door Access Schedule Management

Manage Relay Schedule

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

To configure a relay schedule, go to **Intercom > Relay > Relay Schedule** interface.

The screenshot shows the 'Relay Schedule' configuration page. At the top, there is a 'Relay ID' dropdown menu currently set to 'RelayA'. Below it is a 'Schedule Enabled' checkbox which is checked. The main area is divided into two columns: 'All Schedules' and 'Enabled Schedules'. The 'All Schedules' column contains a list with two items: '1001:Always' and '1002:Never'. The 'Enabled Schedules' column is currently empty. Between the two columns are two blue buttons: the top one has '>>' and the bottom one has '<<', indicating the ability to move schedules between the two lists.

- **Relay ID:** Specify the relay you need to set up.
- **Schedule Enabled:** Assign particular door access schedules to the chosen relay. Simply move them to the Enabled Schedules box.

For instructions on creating schedules, kindly consult the next chapter.

Configure Door Access Schedule

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

You can manage the door access schedule on the device and the device's web interface.

Create Door Access Schedule on the Web Interface

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

To set up the schedule, navigate to the **Intercom > Schedule > Schedule Setting** interface.

To create a daily schedule:

Schedule Setting

Schedule Type

Schedule Name

Date Time : - :

To create a weekly schedule:

Schedule Setting

Schedule Type

Schedule Name

Day of Week Mon Tue Wed Thur
 Fri Sat Sun Check All

Date Time : - :

To create a longer period schedule:

Schedule Setting

Schedule Type

Schedule Name

Date Range ---

Day of Week Mon Tue Wed Thur
 Fri Sat Sun Check All

Date Time : - :

After the access control schedule is set up, you can assign the schedule on the **Intercom > Relay > Relay Schedule** interface.

Create Door Access Schedule on the Device

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

You can also create a door access schedule on the device **Schedule > Add Schedule** screen.

The screenshot shows a mobile application interface for adding a schedule. The title bar at the top reads "Add Schedule" with a back arrow on the left and the time "23:31" on the right. Below the title bar, there are several form fields, each with a label on the left and a value in a rounded green button on the right:

- Mode:** Normal
- Name:** Please enter the name (indicated by a red error message above the field)
- Start Date:** 2022/02/09
- End Date:** 2022/02/09
- Day:** ...
- Start Time:** 00:00
- End Time:** 00:00

At the bottom of the screen, there is a large green rounded button labeled "Save".

Edit the Door Access Schedule

Edit the Door Access Schedule on the Web Interface

To edit the schedule, go to the **Intercom > Schedule > Schedule Management** interface.

Schedule Management

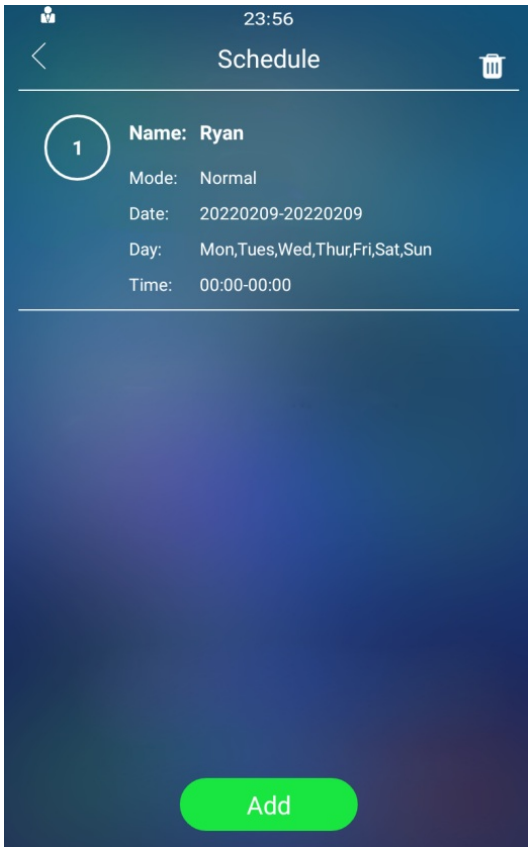
All ▾

<input type="checkbox"/> Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time
<input type="checkbox"/> 1	1002	Local	Daily	Never	-	-	-
<input type="checkbox"/> 2	1001	Local	Daily	Always	-	-	00:00:00-23:59:59
<input type="checkbox"/> 3	5030	Cloud	Daily	Akuvox	-	-	08:00:00-23:59:59
<input type="checkbox"/> 4	5024	Cloud	Daily	Resident-Building ..	-	-	00:00-23:59
<input type="checkbox"/> 5							
<input type="checkbox"/> 6							
<input type="checkbox"/> 7							
<input type="checkbox"/> 8							
<input type="checkbox"/> 9							
<input type="checkbox"/> 10							

1/1

Edit the Door Access Schedule on the Device

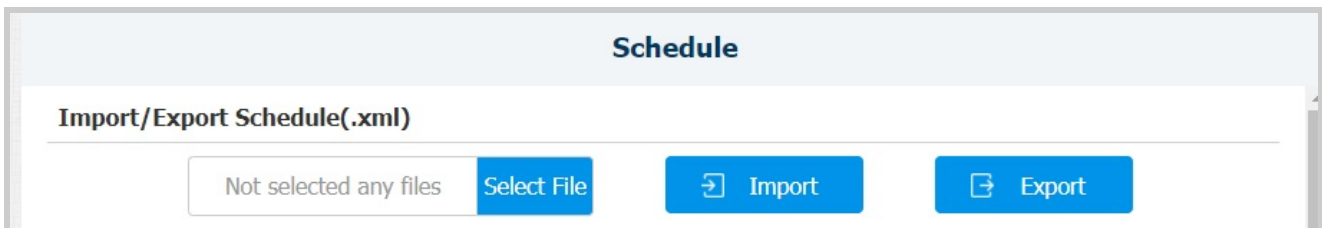
To edit the schedule, go to the device **Schedule** > **Schedule** screen.



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 import or export the schedule, go to the **Intercom > Schedule > Import/Export Schedule(.xml)** 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

You can configure and modify public PIN codes on the device and the device's web interface. To set up the Public PIN code, navigate to **Intercom > PIN Setting > Public PIN**.

Public PIN

Enabled

PIN Code (3~8 digits)

- **PIN Code:** Set a 3-8 digit PIN code accessible for universal use.

To set up a Public PIN code on the device, go to **Password > Public Key Password**.

00:10

← Password

Project Passwd Public Key Passwd

Public Key Passwd

Old Passwd old Passwd

New Passwd New Passwd

Passwd Confirm New Passwd

Save

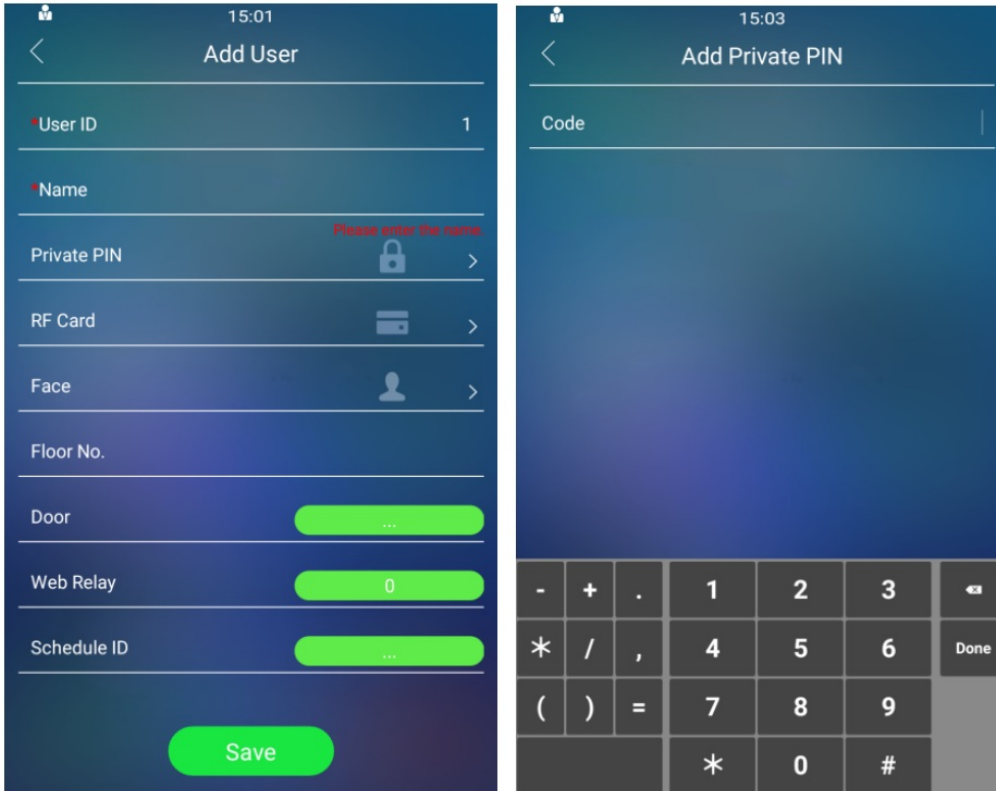
Note

- The Public PIN code will not be valid until the function is turned on.
- APT+PIN can only be applicable when the device is added to the Akuvox SmartPlus.

Configure Private PIN Code on the Device

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

To set up the private PIN code, go to **User > Add User** screen.



Note

Username must be entered first before you can create the PIN code.

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.

To set up the private PIN code, go to **Intercom > User** interface. Click **Add** to add a user.

User

User ID / Name

All ▼

Search

Reset

Add

<input type="checkbox"/>	Source	User ID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/> 1	Local	1	Ryan			⊗		0	1001-123	
<input type="checkbox"/> 2	Local	12213	Jim			⊗	0	0	1001-1	
<input type="checkbox"/> 3	Cloud	5926100 035	Ryan Che n	123123	123123	⊗		0	5024-1	
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										
<input type="checkbox"/>										

Selected:0/3

Delete

Delete All

Total:3

Prev

1/1

Next

Go To Page

1

Go

User

User Basic

User ID

2

Name

Private PIN

Code

- **User ID:** The unique identification number assigned to the user.
- **Name:** The name of this user.
- **Code:** Set a 2-8 digit PIN code solely for the use of this user. Each user can only be assigned a single PIN code.

After user information and PIN code are entered, you can scroll down to the **Access Setting** and configure private PIN code access control.

Access Setting

Relay RelayA RelayB RelayC

Web Relay

Building

Floor No.

Room No.

All Schedules

1001:Always

1002:Never

1:Ryan

>>

<<

Schedules Selected

1001:Always

- **Relay:** Specify the relay(s) to be unlocked using the door opening methods assigned to the user.
- **Web relay:** Specify the ID of web relay action commands that you've configured on the [Web Relay](#) interface. A default value of 0 indicates that the web relay will not be triggered.
- **Building:** The user's residential building.
- **Floor No. :** Specify the accessible floor(s) to the user via [the elevator](#).
- **Room No.:** The user's room number.
- **Schedule:** Grant the user access to open designated doors during preset periods by relocating the desired schedule(s) from the left box to the right one. Besides custom schedules, there are 2 default options:

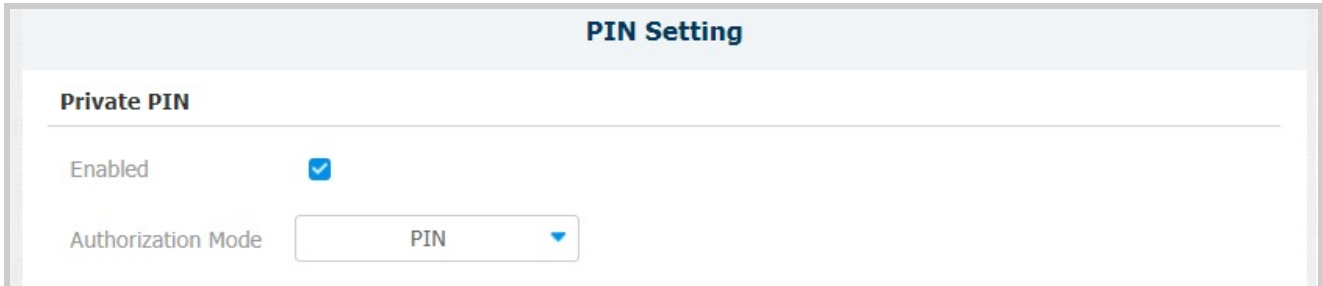
- Always: Allows door opening without limitations on door open counts during the valid period.

- Never: Prohibits door opening.

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 set up the authorization mode, go to the **Intercom > PIN Setting > Private PIN** interface.



The screenshot shows the 'PIN Setting' interface. At the top, there is a header 'PIN Setting'. Below it, the section 'Private PIN' is visible. Under 'Private PIN', there are two settings: 'Enabled' with a checked checkbox, and 'Authorization Mode' with a dropdown menu currently set to 'PIN'.

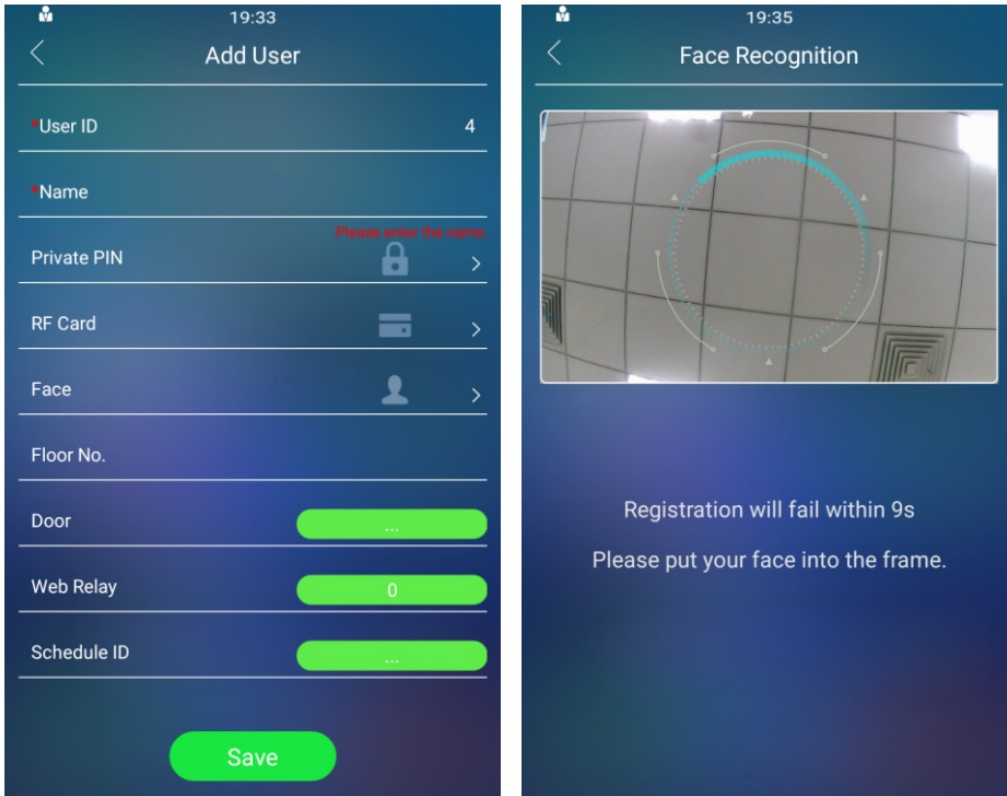
- **Authorization Mode:** Set the authentication mode for door access, including two-factor authentication for enhanced security.
 - PIN: Users are only required to enter their PIN code.
 - APT#+PIN: Users must first enter the Apartment Number, followed by their PIN code.

Configure Facial Recognition for Door Unlock

Configure Facial Recognition on the Device

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

To set up the facial recognition, go to **User > Add User** screen.



Configure Facial Recognition on the Web Interface

You can import the face data to the device on the web interface, go to **Intercom > User > Add User** interface.

User

User ID / Name All Search Reset Add

<input type="checkbox"/> Index	Source	User ID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/> 1	Local	1	testing		D4FAE432	✗	2	0	1001-1	
<input type="checkbox"/> 2	Cloud	382100841	David Valera			✗	1	0	14454-1	
<input type="checkbox"/>										

The screenshot displays a web interface for configuring a user's face. It is divided into several sections:

- User Basic:** Contains a 'User ID' field with the value '4' and a 'Name' field.
- Private PIN:** Contains a 'Code' field.
- RF Card:** Contains a 'Code' field, an 'Obtain' button, and a '+Add' button.
- Face:** Shows the 'Status' as 'Unregistered' and the 'Photo' as 'Not selected any files'. There are 'Select File' and 'Reset' buttons.

- **Status:** Indicate whether the user's face photo has been uploaded successfully.
- **Photo:** Upload a photo complying with the following requirements:
 - The photo must be in JPG, PNG, or BMP format.
 - The photo must be at least 250 x 250 pixels and no more than 2MB in size.
 - The photo must be clear and not blurred.
 - The photo should include a full face with a front view and open eyes.
 - Avoid shadows on the face or background in the photo.

Basic Facial Recognition Configuration on the Web Interface

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

To set it up, go to **Intercom > Face Setting > Face Basic** interface.

Face Basic

Facial Recognition E...

Offline Learning Ena...

Facial Recognition M... Normal ▼

Face Living Recognit... Normal ▼

Facial Recognition I... 3 ▼

Tips When Succeed Default ▼

- **Face Recognition Enabled:** Enable/disable the facial recognition function.
- **Offline Learning Enabled:** Facial recognition accuracy improves as the number of facial recognition increases.
- **Facial Recognition Matching Level:** Determine how strict the facial recognition system is in comparing a person's face with uploaded face data. Each level allows a different degree of difference or face covering (**excluding the mouth area**) to pass the recognition.

- Low: Allow slight differences from the uploaded face data, with little face coverage.

- Highest: Require the face to be identical to the uploaded one, with minimal or no covering.

- The other two levels are in between.

- **Face Living Recognition Matching Level:** Set how strict the system is in preventing fake faces.

- Close: Disable the facial anti-spoofing function. Facial verification can be passed using non-living substitutes for an authorized person's face, such as a photo.

- Highest: The system cannot be fooled by any non-living substitutes for an authorized person's face.

- The other three levels are in between.

- **Facial Recognition Interval:** Adjust the time interval between each facial recognition attempt, ranging from 1 to 8 seconds.
- **Tips when Succeed:** Set the pop-up message displayed when the door is opened by facial recognition.

- Default: The message is “Opening Door Succeeded”.
- Resident name: Display the user’s name as registered in their facial data.

Facial Recognition Improvement

{{snippet.Facial Recognition Improvement}}

To set it up, go to **Intercom > Face Setting > Face Experience Improvement** interface.

Face Experience Improvement

Face Experience Im... Disabled ▼

Export Log 2023 ▼ 11 ▼ 13 ▼
 Export

Configure RF Card for Door Unlock

You can add an RF card for the specific user for the door unlock on the web interface and the device.

Configure RF Card on the Web Interface

You can tap an RF card on the card reader and click obtain to add an RF card for the user, go to **Intercom > User > Add User** interface.

User

All ▼
Search
Reset
Add

<input type="checkbox"/> Index	Source	User ID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/> 1	Local	1	testing		D4FAE432	×	2	0	1001-1	✎
<input type="checkbox"/> 2	Cloud	3821008 41	David Val era			×	1	0	14454-1	✎
<input type="checkbox"/>										✎

User Basic

User ID	<input type="text" value="2"/>
Name	<input type="text"/>

Private PIN

Code	<input type="text"/>
------	----------------------

RF Card

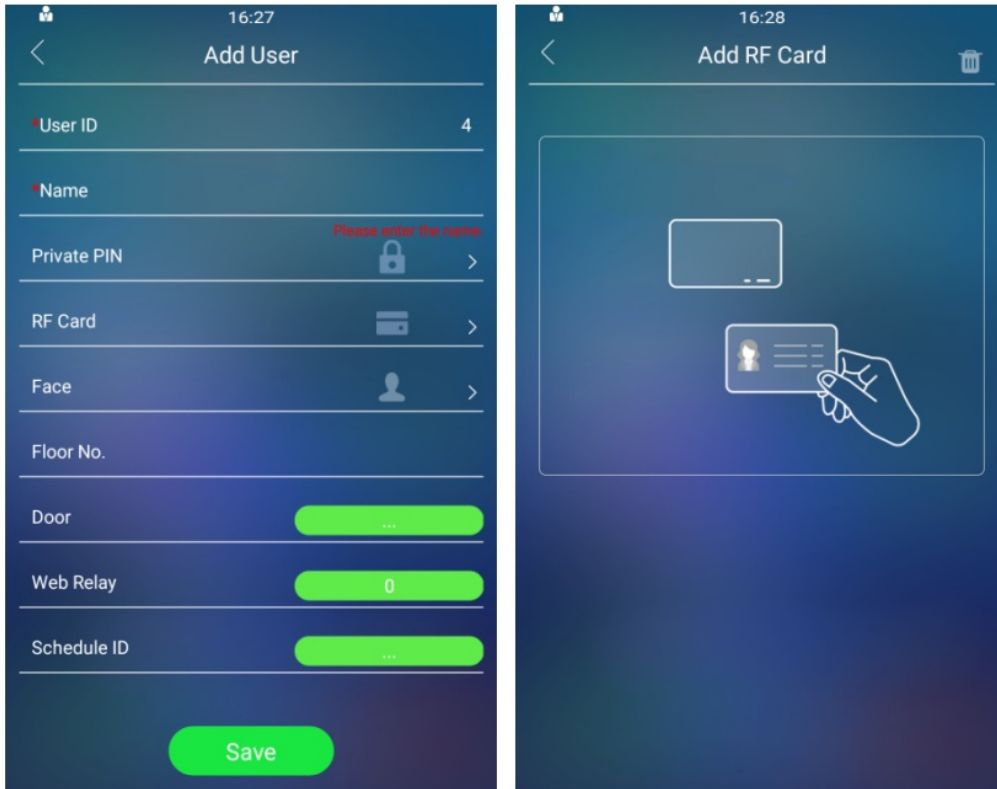
Code	<input type="text"/>	<input type="button" value="Obtain"/>
------	----------------------	---------------------------------------

- **Code:** The card number that the card reader reads.

Note:

- Each user can have a maximum of 5 cards added.
- The device allows to add 20,000 users.
- RF cards operating at 13.56 MHz and 125 KHz frequencies are compatible with the door phone for access. The supported card types as listed as bellow:
 - ID cards: EM4100, and EM4200.
 - IC cards: Mifare UltraLight C/EV1, Mifare Classic, Mifare Plus-S 2K, Mifare DESFire EV1 2K D21, Mifare DESFire EV2 D42, Mifare DESFire EV2 D22, Mifare DESFire EV1(AES-encrypted), Mifare DESFire EV2(AES-encrypted), NFC Type2 216, and NFC Type2 215.

To add an RF card on the device, you can go to **User > Add User > Add RF Card**.



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 set it up, go to **Intercom > Card Setting > RFID** interface.

RFID	
IC Card Display Mode	8HN
ID Card Order	Normal
ID Card Display Mode	8HN
Card Length	Auto

- **IC/ID Card Display Mode:** Set the card number format from the provided options. The default format in the door phone is 8HN.

IC/ID Card Control

To use the IC or ID card, navigate to **Intercom > Card Setting > Card Type Support** interface.

Card Type Support

IC Support Enabled

ID Support Enabled

NFC and Felica Card Setting

Set the device to support NFC and Felica cards on the device before they can be used.

To use the specific card, go to **Intercom > Card Setting > Contactless Smart Card** interface.

Contactless Smart Card

NFC Enabled

Felica Enabled

Note

- Due to conflicts between NFC and Felica cards when applied simultaneously, it's necessary to disable one of them to avoid issues.
- The NFC feature is not available on iPhones.

Mifare Card Encryption

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

To encrypt the card, you can navigate to **Intercom > Card Setting > Mifare Card Encryption**.

Mifare Classic Encryption

Enabled

Sector / Block /

Block Key

- **Sector/Block:** Specify the location where encrypted card data is stored. A Mifare card has 16 sectors (numbered 0 to 15), and each sector has 4 blocks (numbered 0 to 3).
- **Block Key:** Set a password to access the data stored in the predefined sector/block.

Access Authentication

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

You can navigate to **Intercom > Key/Display > Access Authentication Mode of The Building Theme**.

Access Authentication Mode of The Building Theme

Authentication Mode

(Either Voice Assistant or RF Card+PIN can be applied)

- **Authentication Mode:** Determine how to unlock the door using different methods. Please note that the order of the two-factor authentication matters.

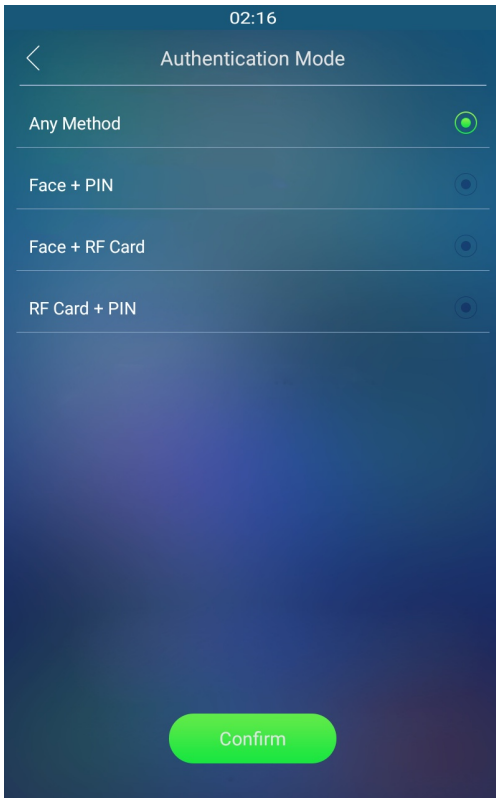
- Any Method: Allows all access methods.

- Face + PIN: Scan the face first, then enter the PIN code.

- Face + RF Card: Scan the face first, then swipe the RF card.

- RF Card + PIN: Swipe the RF card first, then enter the PIN code.

To configure it on the device, go to **Authentication > Authentication mode**.



Unlock by QR Code

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

Navigate to **Intercom > Relay > Open Relay via QR Code** interface.

Open Relay Via QR Code

Enabled

Note

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

Unlock by Bluetooth

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 Bluetooth, go to **Intercom > BLE > BLE Basic** interface.

BLE Basic

BLE Enable	<input type="text" value="Disabled"/>	BLE Mode	<input type="text" value="Central"/>
Rssi Threshold	<input type="text" value="72"/>	(-85~-50db)	
Delay	<input type="text" value="5"/>	(Sec)	

- **Rssi Threshold:** Set the received signal strength. Higher values indicate stronger signal strength, making it easier to receive the Bluetooth signal.
- **Open Door Interval (Sec):** Set the time interval between consecutive Bluetooth door access attempts.

Unlock by HTTP Command on Web Browser

The door phone supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the door phone. This will trigger the relay and open the door, even if the users are away from the device.

Navigate to **Intercom > Relay > Open Relay via HTTP**.

Open Relay Via HTTP

Enabled	<input checked="" type="checkbox"/>
Session Check	<input type="checkbox"/>
UserName	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>

- **Session Check:** Enable to enhance data transmission security.
- **UserName:** Set a username for authentication in HTTP command URLs.
- **Password:** Set a password for authentication in HTTP command URLs.

Tip:

Here is an HTTP command URL example for relay triggering.

```

http://Door phone's IP /fcgi/do?action=OpenDoor&Preset credentials for authentication
      192.168.35.127 &UserName=admin&Password=12345&DoorNum=1
                                     ID of Relay to be triggered
    
```

Note

The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide [Opening the Door via HTTP Command](#) for more information.

Unlock by Exit Button

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

Navigate to **Intercom > Input > Input A/B/C** interface.

Input A

Enabled

Trigger Electrical Level Low

Action To Execute FTP Email SIP Call HTTP TFTP Voice

HTTP URL

Action Delay 0 (0~300 Sec)

Trigger When Signal...

Execute Relay RelayA

Execute Time Always

Break-in Intrusion

Door Status DoorA: High

- **Enabled:** To use a specific input interface.

- **Trigger Electrical Level:** Set the input interface to trigger at low or high electrical level.
- **Action To Execute:** Set the desired actions that occur when the specific Input interface is triggered.
 - FTP: Send a screenshot to the preconfigured [FTP server](#).
 - Email: Send a screenshot to the preconfigured [Email address](#).
 - SIP Call: Call the [preset number](#) upon trigger.
 - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
 - TFTP: Send a screenshot to the preconfigured [TFTP server](#).
 - Voice: When triggered, the door phone will play the customized prompt instead of the default one.

TIP:

To enable the custom audio prompt, upload the audio file at
Phone>Import/Export>Upload Tone.

- **HTTP URL:** Enter the HTTP message if selecting HTTP as the action to execute. The format is [http://HTTP server's IP/Message content](#).
- **Action Delay:** Specify how many seconds to delay executing the preconfigured actions.
- **Trigger When Signal Is Hold:** To trigger the preconfigured action when the door remains opened before the timeout.
- **Execute Relay:** Specify the relay to be triggered by the actions.
- **Execute Time:** Specify whether the relay can be triggered at any time or only within a scheduled time period.
- **Break-in Intrusion:** Activate an alarm when the door is forcibly or illegally opened. Only by checking off this option can the alarm be turned off once triggered.
- **Door Status:** Display the status of the input signal.

Unlock by Reception Icon

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 a reception tab, go to **Intercom > Key/Display > Reception Action In Building** interface.

Reception Action In Building

Dial Account	<input type="text" value="Default"/>	Execute Relay	<input type="text" value="None"/>
Action To Execute	<input type="checkbox"/> HTTP		
HTTP URL	<input type="text"/>		

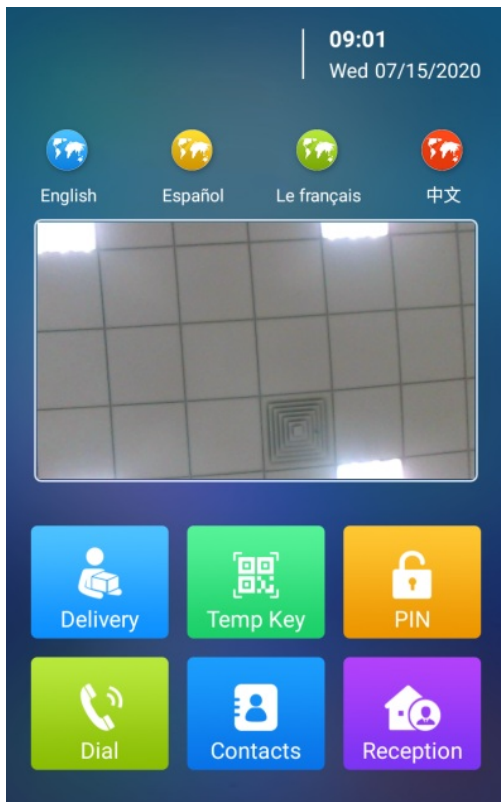
- **Dial Account:** Select the registered SIP account for making calls with receptionists or security guards. Selecting Default will use Account 1 for the calls.
- **Execute Relay:** Specify the relay(s) to be triggered by the Reception tab.
- **Action To Execute:** When checked and the HTTP URL is entered in the box below, press the Reception tab that triggers the desired action.
- **HTTP URL:** Enter the HTTP command URL. Here is an example of relay triggering:

Door phone's IP
http:///fcgi/do?action=OpenDoor&
Preset credentials for authentication

ID of Relay to be triggered

Note:

The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide [Opening the Door via HTTP Command](#) for more information.



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 DTMF codes, go to **Intercom > Relay** interface.

Relay			
Relay ID	RelayA	RelayB	RelayC
Type	Default state	Default state	Default state
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	5	5	5
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	#	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	Relay1	RelayB	RelayC

- **DTMF Mode:** Set the number of digits for the DTMF code.
- **1 Digit DTMF:** Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-Digit.
- **2-4 Digit DTMF:** Set the DTMF code based on the number of digits selected in the DTMF Mode.

Note

To open the door with DTMF, the intercom devices that send and receive the unlock command must use the same mode and code. Otherwise, the DTMF unlock may fail. See here for the detailed [DTMF configuration steps](#).

DTMF White List

To secure the door access via DTMF codes, you can set up the DTMF whitelist on the device web **Intercom > Relay > DTMF** interface so that only the caller numbers you designated in the door phone can use the DTMF code to gain door access.

DTMF

Assigned The Autho... All Numbers ▼

- **Assigned The Authority For:** Specify the contacts authorized to open doors via DTMF:

- None: No numbers can unlock doors using DTMF.
- Only Contacts List: Only numbers added to the door phone's contact list can unlock via DTMF.
- All Numbers: Any numbers can unlock using DTMF.

Note:

When selecting this option, the called indoor monitor(s) should be added into the door phone's contact list.

Unlock by Voice Assistant

Albert is a voice assistant from Akuvox. It can help you with intercom calls, door opening, arming modes, and other functions. As for the door access control, you can choose which relay to activate by this voice assistant.

To configure the voice assistance, go to **Intercom > Basic > Voice Assistant Setting** interface.

Voice Assistant Setting

Voice Assistant

Enabled Time Always ▼

Day Mon Tue Wed Thur

Fri Sat Sun Check All

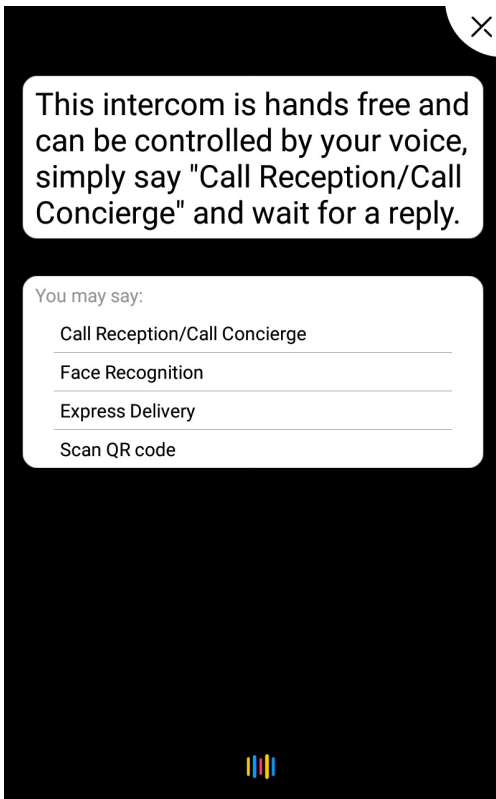
Time 00 ▼ : 00 ▼ - 00 ▼ : 00 ▼

- **Voice Assistant:** Enable/disable the voice assistant function.
- **Enable Time:** Define the operational hours for the voice assistant.

- Always: Voice assistant remains continuously enabled.
- Schedule: Voice assistant operates based on the defined schedule below.

- **Day:** Select the day(s) when the voice assistant is active.
- **Time:** Set the specific period for the voice assistance to operate.

The voice assistant function on the device is shown below:



Tip:

After being waken up, the voice assistant can perform the following tasks for users:

Function	Description
Call Reception/ Call Concierge	After waking up the voice assistant, say "Call Reception" or "Call Concierge" to make a call. Configure the reception number before the voice assistant can automatically dial it.
Face Recognition	Say "Face Recognition" to go to the facial recognition screen.
Express Delivery	Say "Express Delivery" to access the dial screen, where users can either scan the QR code or enter the temporary PIN for door access.
Scan QR Code	Say "Scan QR Code" to utilize the QR code for door access.

Body Temperature Measurement for Door Access

Body Temperature Measurement Configuration

You can configure the body temperature measurement function on the device web **Intercom > Body Temperature > Measuring Body Temperature** interface in terms of defining the normal temperature as well as making the schedule for the validity of the function etc.

Measuring Body Temperature

Mode

Mask Detection

Temperature Unit

Normal Body Tempe... (Below 99.14 °F)

Low Temperature (Below 93.20 °F)

(If the detected temperature is lower than 93.20 °F, the device will prompt low temperature, please try again later)

Action For Abnormal...

Action For Low Body...

Action To Execute SIP/IP Call HTTP

Low Temperature Ac... SIP/IP Call HTTP

Action For Normal B...

Timeout (Sec)

Execute Relay DoorA DoorB DoorC

Day Mon Tue Wed Thur
 Fri Sat Sun Check All

Time : - :

Voice Prompts Please approach Please wear a mask Normal Temperature
 Low Temperature Abnormal Temperature

Recognition Tips

OpenDoor Succeede...

OpenDoor Failed Tips

- **Mode:** Enable forehead or wrist temperature measurement, or disable the function.

- Disabled: Turn off temperature measurement.

- Forehead: Measure forehead temperature with a built-in module(R29C-B only).

- Wrist: Measure wrist temperature with the additional device(R29C-B excluded).

- **Mask Detection:** Detect whether visitors are wearing masks. When enabled, the device reminds those without masks to wear one with the prompt "Please wear a mask."
- **Temperature Unit:** Select between Celsius and Fahrenheit to specify the measurement used to express temperature.
- **Normal Body Temperature:** Define the fever cut-off temperature. For example, setting it at 37.3 degrees Celsius means any temperature higher than that is considered a fever, triggering the preset action(s) for abnormal body temperature.
- **Low Temperature:** Set the lowest normal temperature. Any temperature below this value triggers the preset designated action(s).
- **Action for Abnormal Body Temperature:** Set the actions that occur when a fever is detected.

- Action to Execute: When selected, choose the desired box in the Action to Execute field including SIP/IP Call and HTTP.

- Go to Home Page: The door phone returns to the Home screen.

- **Action for Low Body Temperature:** Set the actions that occur when a low temperature is detected.

- Try again later: The device prompts "Try again later" and executes the specified actions set under the Low Temperature Action field.

- Go To Homepage: The door phone returns to the Home screen.

- **Action to Execute:** This field only appears when Action to Execute is selected for the Action for Abnormal Body Temperature.

- SIP/IP Call: Call designated numbers, including local numbers, dial plans, SmartPlus numbers, and group ones.

- HTTP: Send a preconfigured command to the door phone to execute the specified actions.

- **Low Temperature Action:** This field only appears when "Try again later" is selected for the Action for Low Body Temperature.

- SIP/IP Call: Call designated numbers, including local numbers, dial plans, SmartPlus numbers, and group ones.
- HTTP: Send a preconfigured command to the door phone to execute the specified actions.
 - **Action for Normal Body Temperature:** Set the actions that occur when the temperature detected is normal.
 - **Timeout:** Specify the termination time for temperature measurement in case of no operation or face detection.
 - **Execute Relay:** Select the relay(s) to be triggered.
 - **Day:** Select the day(s) when the relay can be triggered.
 - **Time:** Set the specific period for the relay to be triggered.
 - **Voice Prompts:** Select the desired voice prompts for various scenarios.
 - **Recognition Tips:** Customize the prompt displayed for face verification.
 - **OpenDoor Succeeded Tips:** Customize the message displayed when the relay is triggered.
 - **OpenDoor Failed Tips:** Customize the message displayed when the relay fails to be triggered.

Body Temperature Measurement Configuration

You can configure the body temperature measurement function on the device web **Intercom > Body Temperature > Measuring Body Temperature** interface in terms of defining the normal temperature as well as making the schedule for the validity of the function etc.

Ambient Temperature Configuration

You can adjust the temperature settings according to different time segments of the day. This can help you balance the temperature variations due to different locations and times.

To set it up, navigate to **Intercom > Body Temperature > Ambient Temperature Setting** interface.

Ambient Temperature Setting

ID	Start Time	End Time	Ambient Temperature
1	02 : 00	08 : 00	25.0 (10~40°C)
2	08 : 00	14 : 00	25.0 (10~40°C)
3	14 : 00	20 : 00	25.0 (10~40°C)
4	20 : 00	02 : 00	25.0 (10~40°C)

- **Start Time/End Time:** Divide the 24 hours into four time segments.
- **Ambient Temperature:** Ambient temperature affects the sensitivity of fever detecting, with increased sensitivity at higher ambient temperature.

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.

MJPEG Image Capturing

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

Navigate to **Intercom > RTSP > MJPEG** interface.

MJPEG

Enabled



Image Quality

VGA



Parameter Set-up:

- **Image Quality:** select the quality for the image capturing among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P.**

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

- [http:// device ip:8080/picture.cgi](http://device ip:8080/picture.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 the 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.

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.

Navigate to the device web **Intercom > Live Stream** interface.

Live Stream



RTSP Stream Monitoring

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

RTSP Basic Setting

You are required to set up RTSP function on device web **Intercom > RTSP > RTSP Basic** interface in terms of RTSP Authorization, authentication, and password, etc., before you are able to use the function.

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
RTSP Authorization ...	<input type="checkbox"/>
Mjpeg Authorization ...	<input checked="" type="checkbox"/>
Authentication Mode	<input type="text" value="Digest"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>

Parameter Set-up:

- **RTSP Authorization:** enable or disable the **RTSP authorization**. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, 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.
- **User Name:** enter the name used for RTSP authorization.
- **Password:** enter the password for RTSP authorization.

RTSP Stream Setting

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

Navigate to **Intercom > RTSP > RTSP stream** interface.

RTSP Stream

Video Codecs

H.264 Video Parameters

Video Resolution

Video Framerate

Video Bitrate

2nd Video Resolution

2nd Video Framerate

2nd Video Bitrate

Dynamic Coding2

Parameter Set-up:

- **Video Codec:** select between two types of codec options: H.264 and Mjpeg according to your need.
- **Video Resolution:** select video resolutions among seven options: QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P. The default video resolution is 720P. and the video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than 720P.
- **Video Framerate:** 25fps is the video frame rate by default.
- **Video Bitrate:** select video bit-rate among six options: 128 kbps, 256kbps, 512kbps, 1024kbps, 2048 kbps, 4096kbps according to your network environment. The default video bit-rate is 2048 kbps.
- **2nd Video Resolution:** select video resolution for the second video stream channel. The default video solution is VGA.
- **2nd Framerate:** 25fps is the video frame rate by default for the second video stream channel.
- **2nd Video Bitrate:** select video bit-rate among the six options for the second video stream channel. The second video stream channel is 512 kbps by default.

- **Dynamic Coding:** if it is enabled, the dynamic coding will be automatically adopted for the video preview and monitoring on the SmartPlus App. The video resolution will be optimized when you use your SmartPlus app for the call preview for the incoming call from the door phone and for the door phone monitoring.

Note:

- R29 series supports two video stream channels for H.264 codec video stream.

ONVIF

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

Navigate to **Intercom > ONVIF > Basic Setting** interface.

Basic Setting

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

Parameter Set-up:

- **Discoverable:** Discoverable mode enables the video from the door phone camera to be searched by other devices. It is enabled by default.
- **User Name:** enter the user name. The user name is **admin** by default.
- **Password:** enter the password. The password is **admin** by default.

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

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


Note:

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

Door Phone Camera Exposure Adjustment

Door phone camera exposure can be turned on the web Intercom > **Camera** > **Camera Control** interface in order that indoor monitors or third party devices can obtain the video with improved quality.

Camera



Camera Control

Exposure Mode

Parameter Set-up:

- **Exposure Mode:** turn on the camera exposure mode if needed.

Security

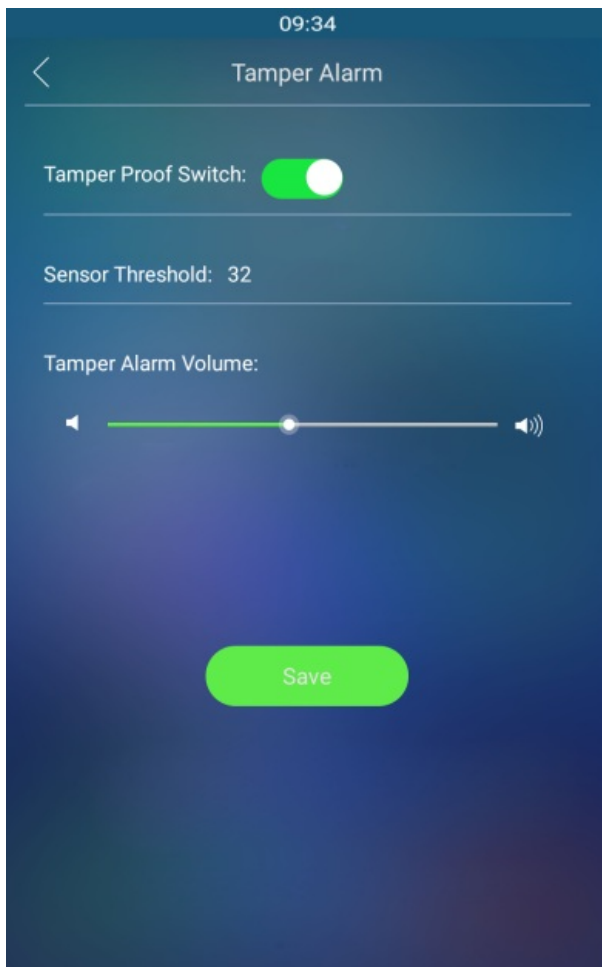
Tamper Alarm Setting

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.

Tamper Alarm Configuration on the Device

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

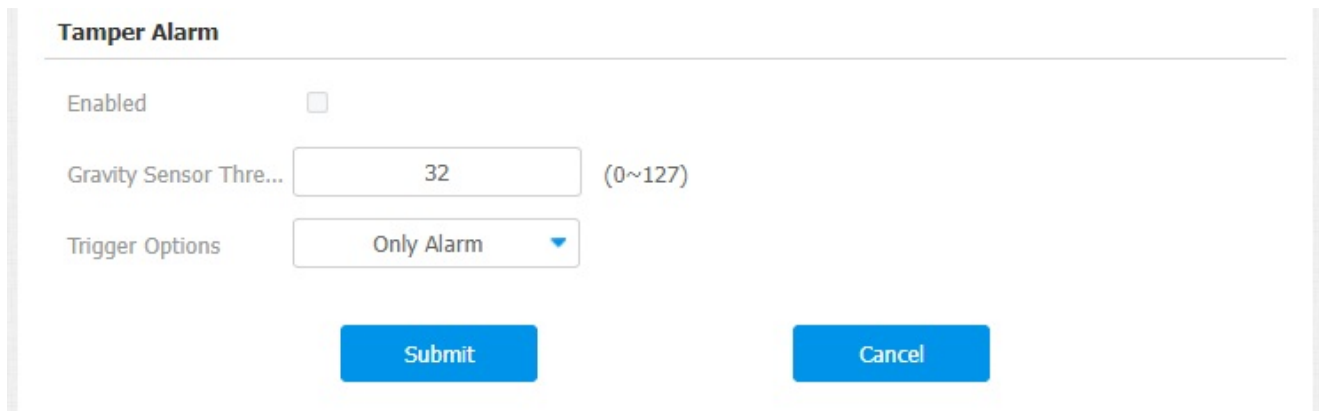
Go to **Tamper Alarm** screen.



Tamper Alarm Configuration on the Web Interface

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

Navigate to **Security > Basic > Tamper Alarm** interface.



Tamper Alarm

Enabled

Gravity Sensor Thre... (0~127)

Trigger Options

Submit **Cancel**

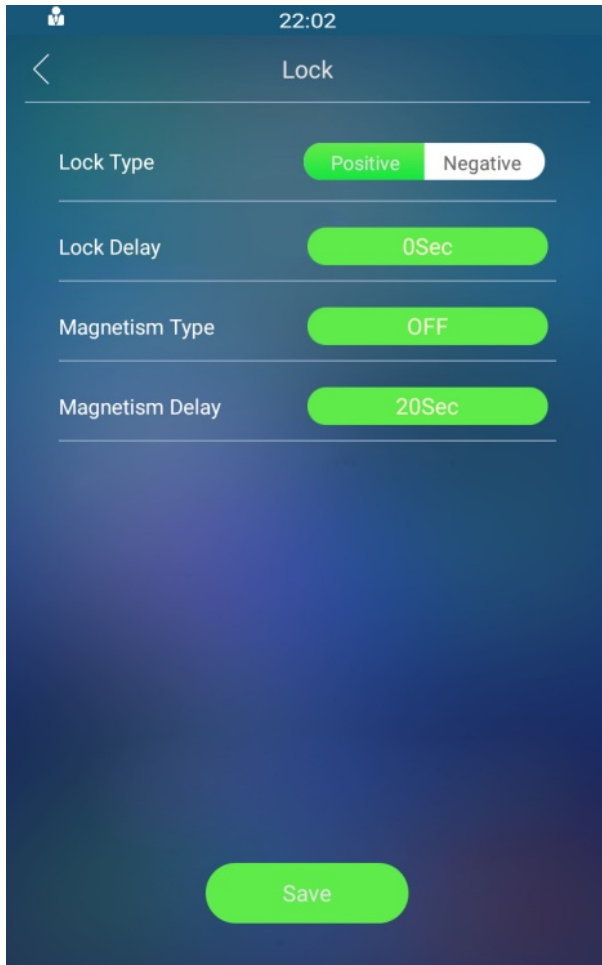
Parameter Set-up:

- **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.
- **Trigger Options:** select what can be triggered when the gravity sensor is triggered.

Lock Security

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

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



Parameter Set-up:

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

Client Certificate Setting


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

Web Server Certificate

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

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

Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete 

Web Server Certifica...


Client Certificate

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

To upload and configure client certificates on the same page.

Client Certificate

<input type="checkbox"/>	Index	Issue To	Issuer	Expire Time
<input type="checkbox"/>	1			
<input type="checkbox"/>	2			
<input type="checkbox"/>	3			
<input type="checkbox"/>	4			
<input type="checkbox"/>	5			
<input type="checkbox"/>	6			
<input type="checkbox"/>	7			
<input type="checkbox"/>	8			
<input type="checkbox"/>	9			
<input type="checkbox"/>	10			

Delete 

Cancel

Parameter Set-up:

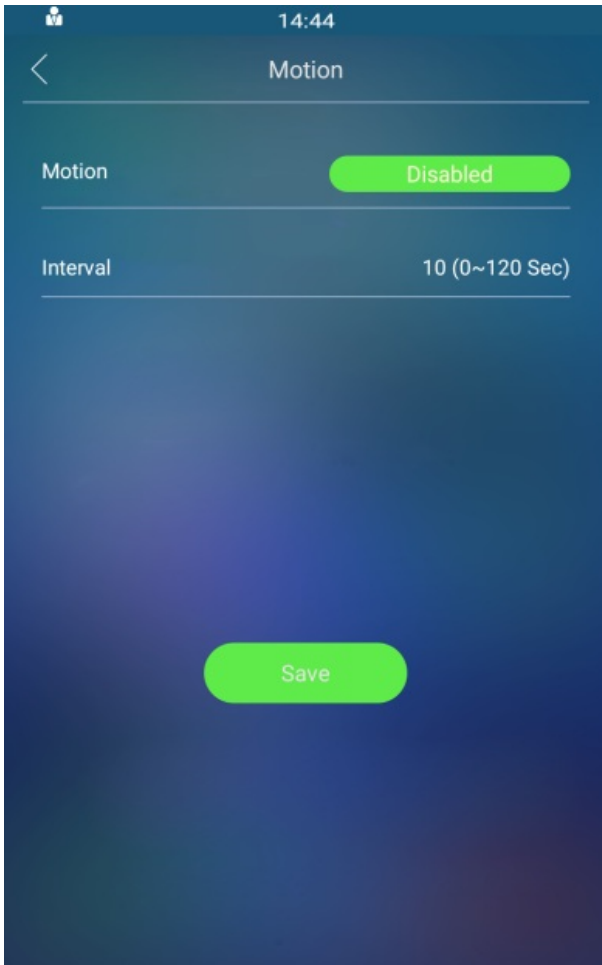
- **Index:** select the desired value from the drop-down list of Index. If you select **Auto** value, the uploaded certificate will be displayed in numeric order. If you select value from **1 to 10**, the uploaded certificate will be displayed according to the value that the user selected.
- **Select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

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.

Motion Detection Setting on the Device

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



Parameter Set-up:

- **Interval:** IR detector receives an event, and delays certain seconds set by interval before triggering motion. When triggering, it will determine whether the time when the IR received the event is within 3 seconds from the time when the trigger was triggered. If the interval is 0 second, it will not trigger motion. If the interval is 1-3 seconds, as long as the image movement is detected once in front of the IR detector, motion will be triggered. If the interval time is over 3 seconds, for example, 10 seconds, after the image movement is detected in front of the IR detector, the image movement is detected again within 7s-10s, then motion will be triggered.

Motion Detection Setting on the Web Interface

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

Navigate to **Intercom > Motion > Motion Detection Options** interface.

Motion Detection Options

Suspicious Moving O...

Timing Interval (0~120 Sec)

Detection Accuracy (0~6)

Action To Execute FTP Email SIP Call HTTP TFTP

HTTP URL

Action Relay

Motion Detection Area

The width of detected area % ~ %

The height of detected area % ~ %

Parameter Set-up:

- **Suspicious Moving Object Detection:** select **disable** to disable the motion detection. Select **IR detection** to enable the **IR sensor** based motion detection for suspicious moving objects. And select **Video detection** to enable video-based motion detection during the monitoring for the suspicious moving object.
- **Time Interval:** set the time interval in the same way as you do on the device.
- **Detection Accuracy:** set the detection accuracy for the detection sensitivity. The higher value, the greater sensitivity. The default detection accuracy value is 2.
- **Action To Execute:** select the notification type: FTP, Email, SIP Call, HTTP, TFTP. For example, if you select **FTP** then the notification will be sent in FTP to a designated serve while if you select **Email** then the notification will be sent in the form of emails when motion detection action is triggered.
- **Action relay:** select the relay to be triggered when a suspicious object is detected in the motion detection. Select **none** and no relay will be triggered.

- **The Width of Detected Area/The Height of Detected Area** : the full size of the detection area is calculated by percentage (100%) from left to right. Pick the horizontal detection range anywhere from 0% to 100%, and pick the vertical detection range anywhere from 0% to 100%. After that, you will be able to get the exact detection area you want.

Security Notification Setting

Email Notification Setting

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

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

Email Notification

Sender's Email Addr...	<input type="text"/>
Email SendName	<input type="text"/>
Receiver's Email Addr...	<input type="text"/>
Email RecvName	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>

Parameter Set-up:

- **SMTP Server Address** : enter the SMTP server address of the sender.
- **Port**: enter the port number from which the email is sent out.

- **SMTP User Name:** enter the SMTP user name, which is usually the same as sender's email address.
- **SMTP Password:** configure the password of the SMTP service, which is same as the sender's email address.

FTP Notification Setting

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

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

FTP Notification	<input type="text"/>
FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password"/>

Parameter Set-up:

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

TFTP Notification Setting

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

Navigate **Intercom > Action > TFTP Notification** interface.

TFTP Notification	
TFTP Server	<input type="text"/>

Parameter Set-up:

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

SIP Call Notification

If you want to be notified via SIP call for the security notification, you can configure the SIP call notification on the web **Intercom > Action > SIP Call Notification** interface properly.

SIP Call Notification

SIP Call Number

SIP Caller Name

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.

Navigate to **Intercom > Advanced > Encrypted display of the card** interface.

Encrypted display of the card

Enabled

Submit

Cancel

Parameter Set-up:

- **Enabled:** enable or disable the GDPR function. If enabled, the card data will be encrypted automatically when an RF card is added.

Package Delivery Notification

When your packages get delivered to your package room, you can be notified of the package delivered to you. To enable the function, you can go to **Intercom > Key/Display > Delivery Setting Of Building Theme**.

Delivery Setting Of Building Theme

Package Room

Disabled ▼

Note:

- This feature is only applicable to door phones that are connected to the Akuvox SmartPlus.

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	\$relay1 status	Http://server ip/ relaytrigger=\$relay1 status
4	Relay Closed	\$relay1 status	Http://server ip/ relayclose=\$relay1 status
5	Input Triggered	\$input1 status	Http://server ip/ inputtrigger=\$input1 status
6	Input Closed	\$input1 status	Http://server ip/ inputclose=\$input1 status
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

Path: **Phone > Action URL .**

Action URL

Active

Type

Make Call

Hang Up

RelayA Triggered

RelayB Triggered

RelayC Triggered

RelayA Closed

RelayB Closed

RelayC Closed

InputA Triggered

InputB Triggered

InputC Triggered

InputA Closed

InputB Closed

InputC Closed

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

Valid Face Recognition

Invalid Face Recognition

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 configure this feature on the web **Security > Basic > High Security Mode**.

High Security Mode

Enabled

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.

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

- | `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.

Navigate to **Phone > Call Log** interface.

Save Call Log Enabled

Call History

Time - Name/Number

<input type="checkbox"/> Index	Type	Date	Time	Local Identity	Name	Number
<input type="checkbox"/> 1	Dialed	2021-05-18	16:13:01	1003@192.168 .31.20:5070	1001	1001@192.168 .31.20:5070
<input type="checkbox"/> 2	Dialed	2021-05-18	16:12:46	1003@192.168 .31.20:5070	1001	1001@192.168 .31.20:5070
<input type="checkbox"/> 3	Dialed	2021-05-18	16:12:28	1003@192.168 .31.20:5070	1001	1001@192.168 .31.20:5070

Parameter Set-up:

- **Call History:** select call history among four options: **All**, **Dialed**, **Received**, **Missed** for the specific type of call log to be displayed.
- **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.

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

Save Door Log Enab... Export

All Time - Name/Code Search

<input type="checkbox"/> Index	Name	Code	Type	Date	Time	Status
<input type="checkbox"/> 1	FaceKey	Unknown	Face	2023-11-09	22:30:36	Failed
<input type="checkbox"/> 2	FaceKey	Unknown	Face	2023-11-09	22:30:29	Failed
<input type="checkbox"/> 3	FaceKey	Unknown	Face	2023-11-09	22:30:22	Failed
<input type="checkbox"/> 4	FaceKey	Unknown	Face	2023-11-09	22:30:14	Failed
<input type="checkbox"/> 5	FaceKey	Unknown	Face	2023-11-01	03:54:37	Failed
<input type="checkbox"/> 6	FaceKey	Unknown	Face	2023-11-01	03:54:28	Failed

Parameter Set-up:

- **Time:** select the specific time span of the door logs you want to search, check or export.
- **Name/Code:** select the **Name** and **Code** options to search the door log by the name or by the PIN code.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

You can set up the function on the web **Upgrade > Advanced > System Log** interface.

System Log

LogLevel

3

Export Log



Export

Export Debug Log



Export

Remote System Log ...

Remote System Serv...

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 Log:** click the **Export** tab to export the temporary debug log file to a local PC.
- **Export Debug Log:** click the **Export** tab to export debug log file to a local PC.
- **Remote System Server:** enter the remote server address to receive the device log. And the remote server address will be provided by Akuvox technical support.

PCAP for Debugging

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

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

PCAP

Specific Port (1~65535)

PCAP Start Stop Export

PCAP Auto Refresh

Parameter Set-up:

- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** select **Enable** or **Disable** to turn on or turn off the PCAP auto refresh function. If you set it as **Enable** then the PCAP will continue to capture data packet even after the data packets reached their 50M maximum in capacity. If you set it as **Disable** the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

User Agent

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

Path: **Account > Advanced > User Agent.**

User Agent

User Agent

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.

Navigate to **Upgrade > Basic** interface.

Firmware Version	29.30.10.15
Hardware Version	29.3.4
Upgrade	<input type="text" value="Not selected any files"/> <input type="button" value="Select File"/>
Reset:	<input type="checkbox"/> <input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>

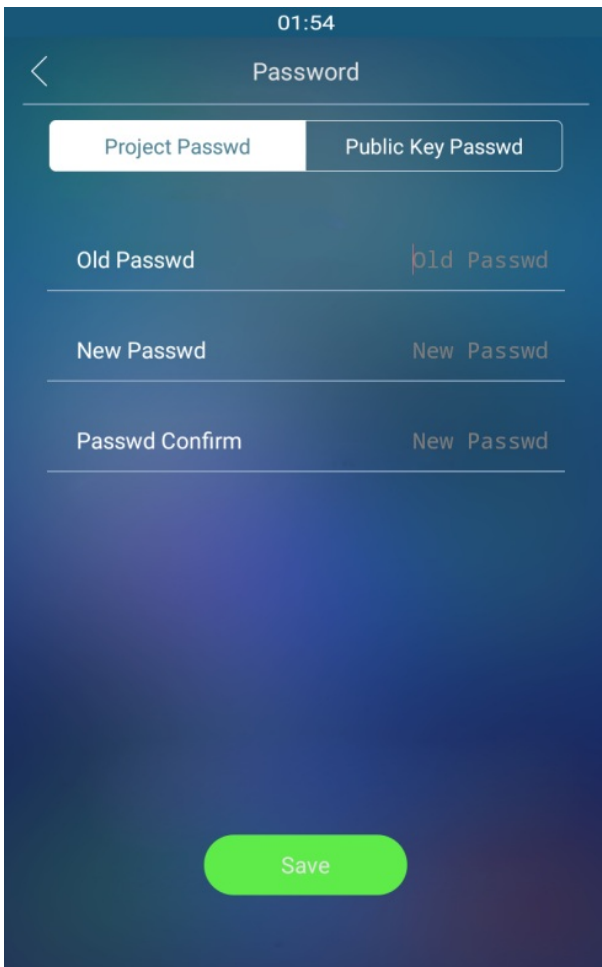
Note:

- Firmware files should be .zip format for upgrade

Password Modification

Modify Device Setting Password

Project passwords are what need to be entered before you are allowed to enter the set password, which enables you to enter the device **Password** screen for the configuration and adjustment. 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 set passwords if needed.

System PIN

Step1 PIN

Step2 PIN

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**.

Modify Device Web Interface Password

To modify device web interface password, navigate to **Security > Basic > Web Password Modify**.

Basic

Web Password Modify

User Name Change Password

Account Status

admin	Enabled
user	<input type="text" value="Enabled"/>

Change Password X

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

User Name	user
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

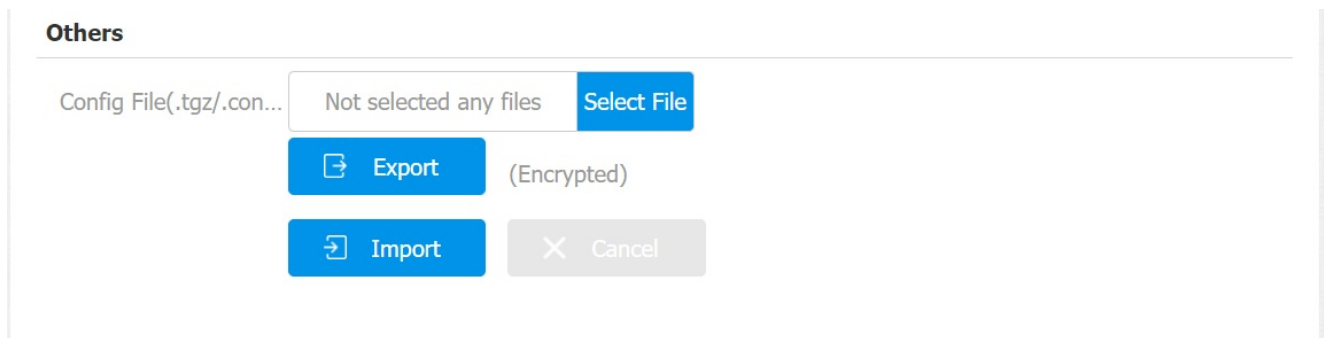
Parameter Set-up:

- **User Name:** modify the admin or user password if needed.
- **User:** enable the user account if needed.

Backup

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

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



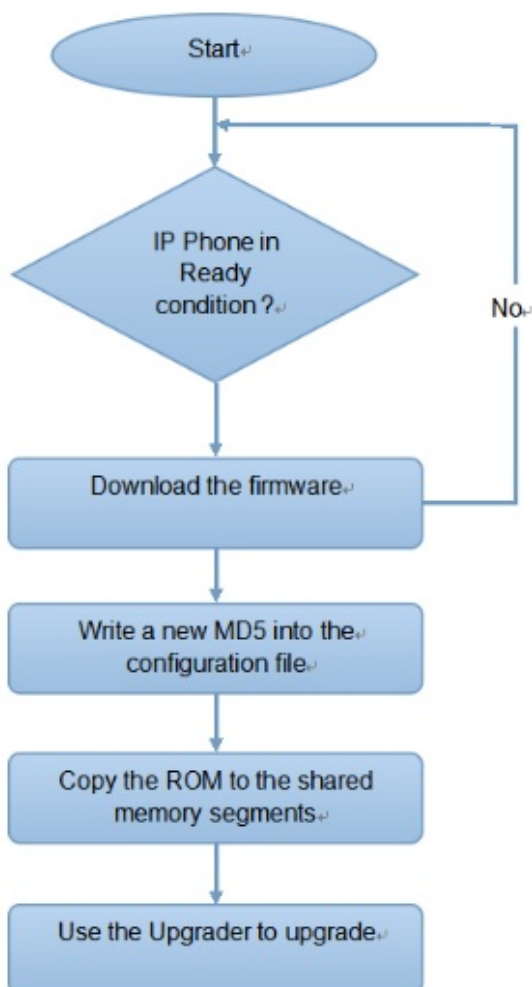
Auto-provisioning via Configuration File

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

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

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

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

Note

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

You may click [here](#) to see the detailed format and steps.

AutoP Schedule

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

To set up the schedule on the device web **Upgrade > Advanced > Automatic Autop** interface.

Automatic Autop

Mode Repeatedly ▼

Auto Clear MD5 Disabled ▼

Schedule Sunday ▼

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

Clear MD5 [Submit](#)

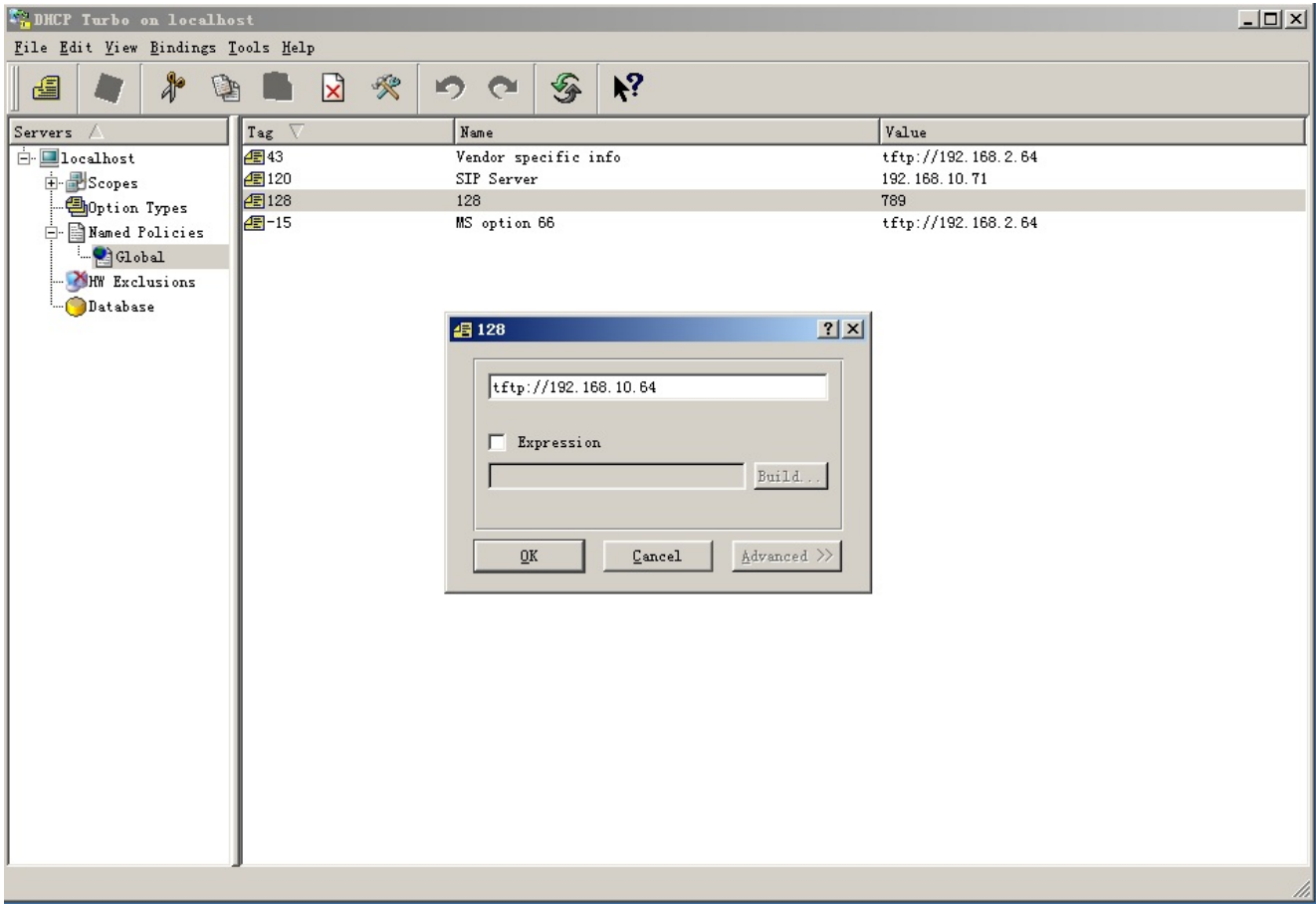
Export Autop Templ... [Export](#)

Parameter Set-up:

- **Mode:** 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 which will enable the device to perform Autop every time it boots up or according to the schedule you set up. Select **Hourly Repeat** if you want the device to perform Autop every hour.
- **Schedule:** if **Repeatedly** is selected, you can set up the time schedule for the AutoP.

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.

Navigate to **Upgrade > Advanced Interface**.

DHCP Option

Custom Option (128~254)

(DHCP Option 66/43 is Enabled by Default)

Parameter set-up:

- **Custom Option:** enter the DHCP code that matched the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66:** if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.
- **DHCP Option 43:** if the device does not get an URL from DHCP Option 66, it will

automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

Note:

- The general configuration file for the in-batch provisioning is with the format "r0000000000xx.cfg". Take R29 as an example, its format is "r000000000029.cfg" (10 zeros in total). 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 set up Autop server on **Upgrade > Advanced > Manual Autop** interface.

Automatic Autop

Mode Power On ▾

Schedule Sunday ▾

22 (0~23 hour) 0 (0~59 min)

Clear MD5 Clear

Export Autop Templ... Export

Manual Autop

URL tftp://192.168.35.88 User Name admin

Password ●●●●●● Common AES Key ●●●●●●

AES Key(MAC) ●●●●●●

AutoP Immediately

Parameter Set-up:

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

Device Integration with Third Party Device

Integration via Wiegand

If you want to integrate the door phone with third-party devices via Wiegand, you can configure the Wiegand on the web interface. Path: **Intercom > Wiegand > Wiegand**.

Wiegand	
Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Wiegand-26
IC Card Reading Order	Normal
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output CRC	Enabled
RF Card Verification	Enabled
Wiegand Open Relay	<input type="checkbox"/> RelayA <input type="checkbox"/> RelayB <input type="checkbox"/> RelayC

Parameter set-up:

- **Wiegand Display Mode:** select **Wiegand Card code format** among 8H10D; 6H3D5D; 6H8D; 8HN; 8HR; RAW.
- **Wiegand Card Reader Mode:** set the wiegand data transmission format among three options: Wiegand 26, Wiegand 34, Wiegand 58. The transmission format should be identical between the door phone and the device to be integrated.
- **IC Card Reading Order:** **Normal** means the device will read the first three bytes of the IC card number order. **Reversed** means the device will read the later three bytes of the IC card number order.
- **Wiegand Transfer Mode:** select between **Input**, **Output**, and **Convert to Card No.Output**. If the door phone is used as a receiver, then set it as **Input** for the door phone. Select **Output** if you want Wiegand output to be converted to card number before sending

it from the door phone to a receiver. For facial recognition access, the user card number corresponding to the facial recognition access will be sent out in a binary system.

- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Normal** and **Reversed**, if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Normal** and **Reversed**, if you select **Reversed** then the input card number will be reversed and vice versa.
- **Wiegand Output CRC:** tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.
- **RF Card Verification:** it is used to verify whether the card is assigned to a user. If the card is not assigned, a prompt "Opening Door Failed" will pop up on the door phone screen.

You can configure the Wiegand output mode if needed on the same interface. The output occurs when you press the PIN code on the device.

Convert To Wiegand Output

PIN

Disabled 

Parameter Set-up:

- **PIN:** select **Disabled** if you want to disable the function. Select **4 bits per digit** if you want to output the PIN code by four continuous bits as a set. Select **8 bits per digit** if you want to output the PIN code by eight continuous bits as a set.

Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature.

You can navigate to **Intercom > ONVIF > Advanced Setting** interface.

Advanced Setting


Milestone Enabled

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.

HTTP API

Enabled	<input checked="" type="checkbox"/>
Authorization Mode	Allowlist 
User Name	admin
Password	••••••••
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

Parameter set-up:

- **Enabled**: enable or disable the HPTT API function for third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Authorization Mode**: select among four options: **None**, **WhiteList**, **Basic**, **Digest** for authorization type, which will be explained in detail in the following chart.

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

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	AllowList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The 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.

Lift 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.

Lift Control List

Lift Control List

None



Parameter Set-up:

- **Lift Control List:** select integration mode among seven options: **None, OSDP, Dahua, Lift control, KEYKING, ZKT, 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 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.
5	KEYKING	Select KEYKING if you want to integrate with KEYKING lift controller.
6	ZKT	Select ZKT if you want to integrate with ZKTeco lift controller.

Note:

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

OSDP Setting

If you choose OSDP integration mode on device web **Lift Control > OSDP Advance Setting** interface, you can not only check for OSDP status but also obtain the authentication from third party devices for various applications such as door access, etc.

Osdp Advance Setting

Connect Status	Disconnected		
OSDP Address	<input type="text" value="1"/>	Dummy Card Number	<input type="text" value="0"/>
Send By	<input type="text" value="OSDP"/>	Dummy PIN Number	<input type="text"/>

Parameter Set-up:

- **Connect Status:** indicate OSDP based communication status.
- **OSDP Address :** you can obtain the specific OSDP Address from the solution provider.
- **Dummy Card Number:** enter the card number in order to obtain the authentication by the third party devices such as opening the lift door, closing the door or other forms of door access, etc.
- **Dummy PIN number:** enter the PIN code in order to obtain the authentication from third party devices such as opening the lift door, closing the door and so on.
- **Send by:** select in what way you want to send out the card number among three options: **OSDP, Wiegand and None**. If you select OSDP then the card number will be sent out to the third party devices via RS485. If you select Wiegand then the card number will be sent out via Wiegand. If you select None then the card number will not be sent out but retained in the system.

Note:

- Dummy card numbers cannot be sent if OSDP is not selected in the lift control list field.

KeyKing Setting

To integrate the KeyKing lift controller, you are required to set up the KeyKing address obtained from your solution provider. You can navigate to **Lift Control > List Control List**.

Lift Control List

Lift Control List

KEYKING

General Setting

KeyKing Address

1

Server IP

192.168.36.122

Port

80

(1~65535)

Timeout

60

(1~65535)

Floor

Parameter Set-up:

- **KeyKing Address** : select the KeyKing address provided by your solution provider. The address number must be identical to the address number on the lift controller board.

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 **Lift Control > Lift Control List**.

Lift Control List

Lift Control List

Akuvox EC32 

General Setting

Server IP

192.168.36.122

Port

80

(1~65535)

Akuvox EC32 Action

User Name

admin

Password

●●●●●●●●

Floor NO. Parameter

\$floor

URL To Trigger Spec...

/fcgi/do?action=OpenDoor&UserName=admin&Password=admin&Floor=\$

URL To Trigger All Fl...

/fcgi/do?action=OpenAll&UserName=admin&Password=admin

URL To Close All Flo...

/fcgi/do?action=CloseAll&UserName=admin&Password=admin

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.

ZKT Lift Controller

You are required to configure the ZKteco lift controller before you can connect the door phone to the lift controller. You can navigate to **Lift Control > Lift Control List**.

Lift Control List

Lift Control List

ZKT

General Setting

Server IP

192.168.36.122

Port

80

(1~65535)

Timeout

60

(1~60s)

Parameter Set-up:

- **Server IP:** enter the IP address of the ZKTeco controller server.
- **Port:** enter the port of ZKTeco controller server.
- **Timeout:** enter the lift controller timeout. For example, if you enter 30 seconds, then you have to press the floor buttons on the lift controller in 30 seconds after you, for example, swipe the card, otherwise, the button will become invalid.

Mobile Community

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

You can navigate to **Intercom > Relay > Mobile Community** interface.

Mobile Community

Enabled

HTTP URL

Device ID

Parameter Set-up:

- **HTTP URL:** enter the HTTP command. After scanning the QR code, the HTTP command

will carry the dynamic QR code information automatically before being sent to the QR code server for verification. For example: <http://wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode}&deviceId={DeviceID}>

- **Device ID**: create your device ID, which will be added to the HTTP commands automatically after you scan the QR code.

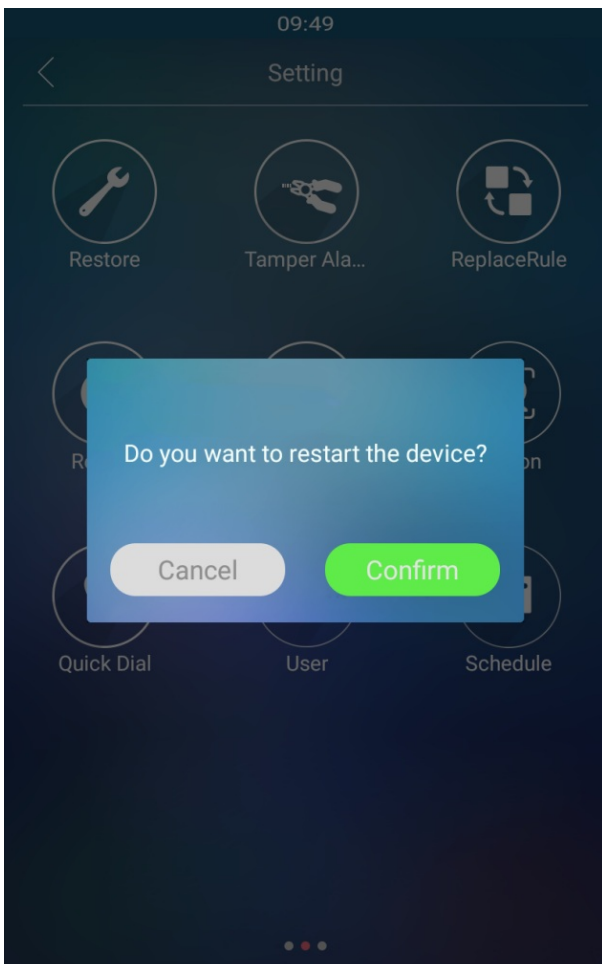
System Reboot&Reset

Reboot

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.

Go to **Reboot** setting screen.



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.

Navigate to **Upgrade > Basic** interface.

Firmware Version	29.30.10.15
Hardware Version	29.3.4
Upgrade	<input type="text" value="Not selected any files"/> <input type="button" value="Select File"/>
Reset:	<input type="checkbox"/> <input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Reset"/>
Reset Configuration to Default State(Except Data)	<input type="button" value="Reset"/>
Reboot	<input type="button" value="Reboot"/>

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

Reboot Schedule

Mode	<input type="checkbox"/>
Schedule	<input type="text" value="Every Day"/> ▼
	<input type="text" value="0"/> (0~23 hour)
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

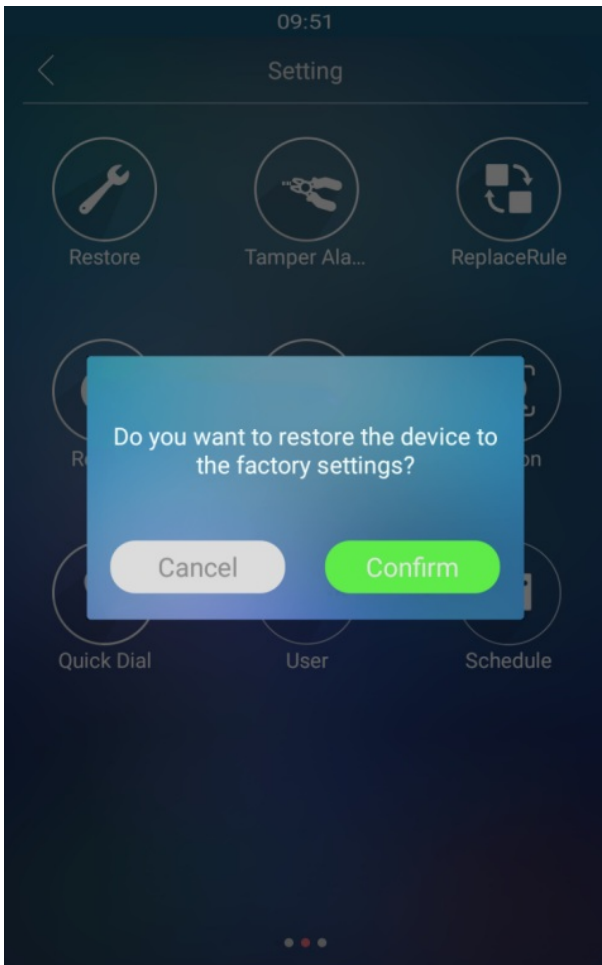
Parameter Set-up:

- **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.

Reset

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.



Reset on the Device Web Interface

Device system can also be reset on device web **Upgrade > Basic** interface without approaching the device.

Firmware Version 29.30.10.15

Hardware Version 29.3.4

Upgrade

Not selected any files [Select File](#)

Reset:

[Upgrade](#)

[Cancel](#)

Reset To Factory Setting	Reset
Reset Configuration to Default State(Except Data)	Reset

Reboot

[Reboot](#)