

# Akuvox R29 Series Door Phone Admin Guide 202305



WWW.AKUVOX.COM



# R29 SERIES DOOR PHONE Administrator Guide

## About This Manual

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 29.30.2.920 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.

## Introduction of Icons and Symbols

### Note

- Informative information and advice from the efficient use of the device.

## Product Overview



Akuvox R29 series is an Android-based IP video door phone with a touch screen. It incorporates audio and video communications, access control and video surveillance. Its finely-tuned Android OS, Cloud, and AI-based communication technology allow featured customization to better suit your operation habit. R29 series has multiple ports, such as RS485 and Wiegand ports, which can be used to easily integrate external digital systems, such as access control system and fire alarm system, helping to create a holistic control of the building entrance and its surroundings and giving you a great sense of security via a variety of access such as card, NFC, Bluetooth, QR code and newly added voice control door access in an accompaniment with body temperature measurement. R29 series door phone is applicable to residential buildings, office buildings, and their complex.

## Change Log

The change log will be updated here along with the changes in the new software version.

## Model Differences

	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.
- **Phone book:** this section involves call log, and phone book management.
- **Upgrade:** this section covers firmware upgrade, device reset&reboot, configuration file auto-provisioning, and PCAP.
- **Security:** this section is for password modification.

**Mode selection:**

1. **Discovery mode:** it is a plug and play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to the network. It is a super time-saving mode and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations previously by the administrator.
2. **Cloud mode:** Akuvox Cloud is an all-in-one management system. Akuvox Cloud is a mobile service that allows audio, video, and remote access control between smart phones and Akuvox intercoms. All configurations in the device will be issued automatically from the cloud. If users decide to use Akuvox cloud, please contact Akuvox technical support, and they will help you configure the related settings before using.
3. **SDMC mode:** SDMC (SIP Device Management Controller) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for door access, intercom, monitoring, alarm, etc. It is a convenient tool for property managers to manage, operate and maintain the community.

### Tool selection

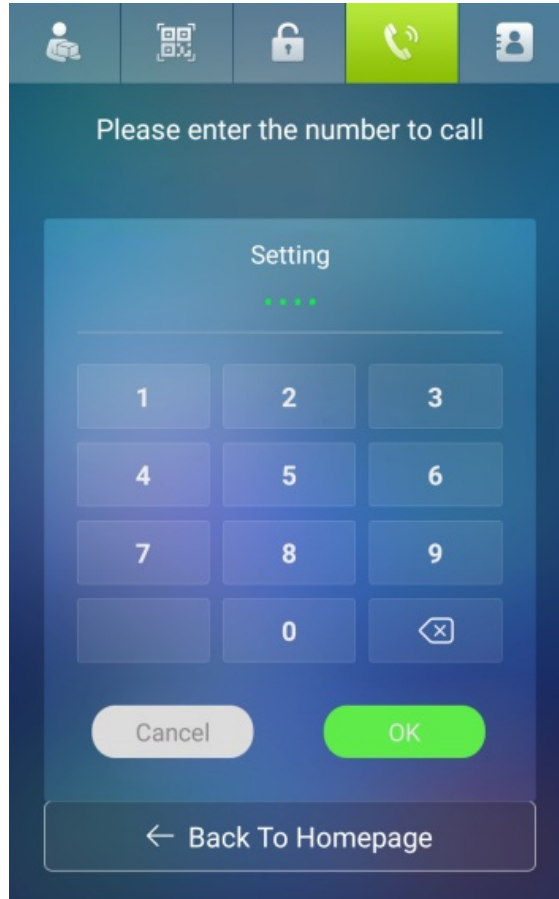
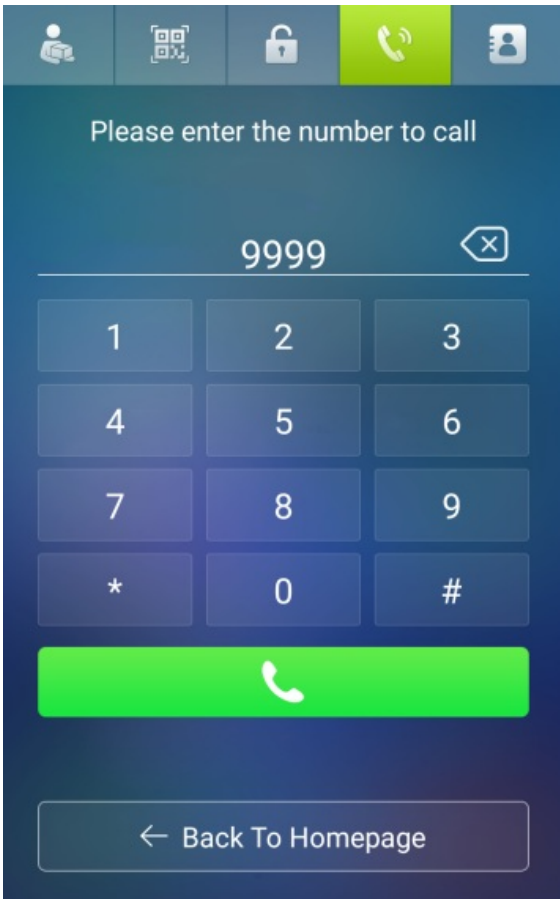
Akuvox has many configuration tools for you to set up devices more conveniently. Here we list some common tools, please contact your administrator to get the tool if you need them.

1. **SDMC:** SDMC is suitable for the management of Akuvox devices in large communities, including access control, resident information, remote device control, etc.
2. **Akuvox PC Manager:** distribute all configuration items in batch on a LAN.
3. **IP scanner:** it is used to search Akuvox device IP addresses on a LAN.
4. **FacePro:** manage face data in batch for the door phone on a LAN.

### Access the Device

Before configuring Akuvox R29 series door phones, please make sure the device is installed correctly and connects to a normal network. Using Akuvox IP scanner tool to search the device IP address in the same LAN. Then use the IP address to log in to the web browser by user name and password **admin** and **admin**. Or set up some basic settings on the device screen by pressing **9999 + Dial key + 3888** (password) on the **Dial** screen.

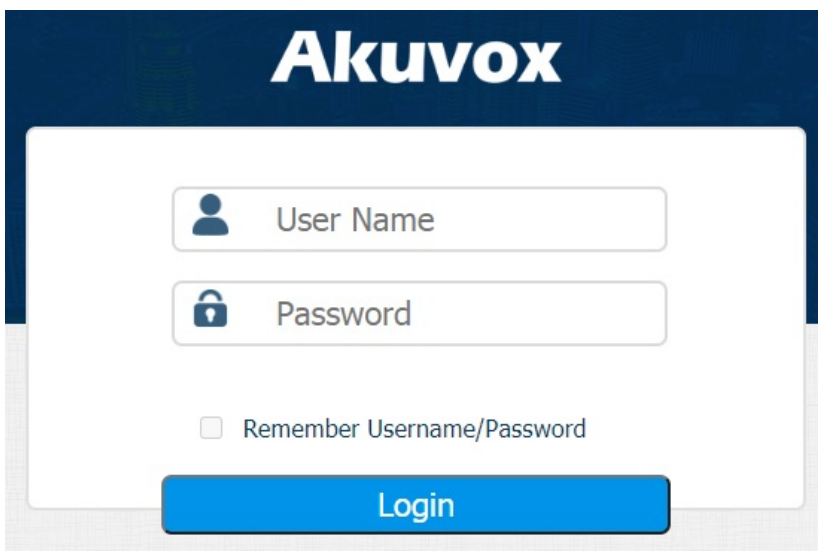
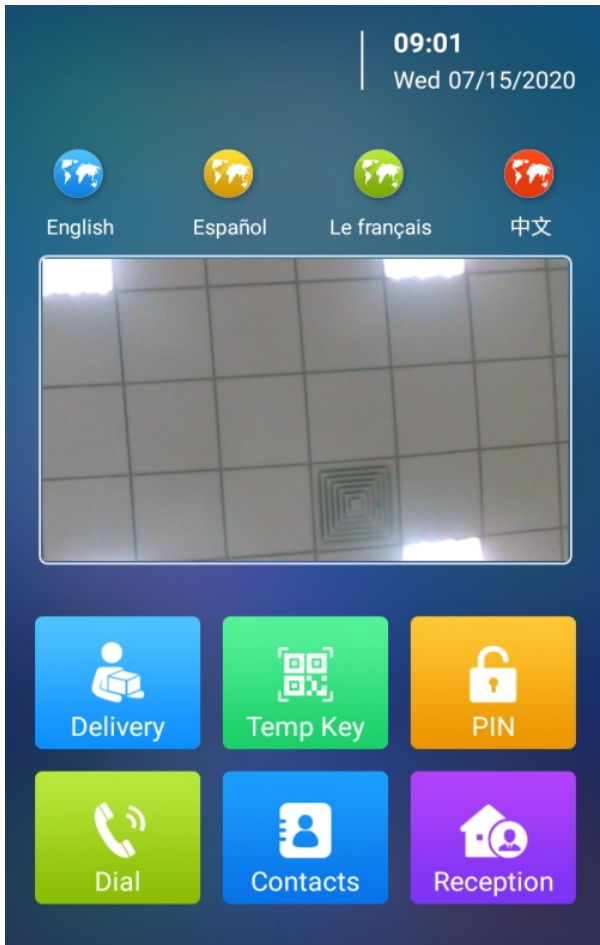
You can also access the device **Setting** screen by clicking the time bar 10 times without entering the project password **9999** using the gesture control function which can be configured on the web **Intercom > Basic > Basic** interface.



**Basic**

Gesture Control

Two-Way Video Ena...



**Note**

- You can also obtain the device IP address using the Akuvox IP scanner to log in to the device web interface. Please refer to the URL below for the IP scanner application:  
<https://knowledge.akuvox.com/docs/how-to-obtain-ip-address-via-ip-scanner-1>
- 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

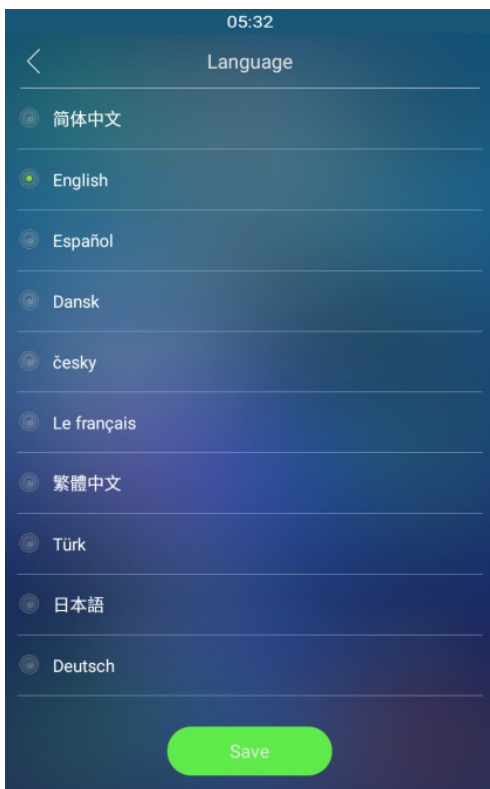
When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can either be set up directly on the device or on the device web interface according to your preference.

#### Note

- On R29Z/R29ZL the language is Chinese by default, so there is no such option when the first time boots up.

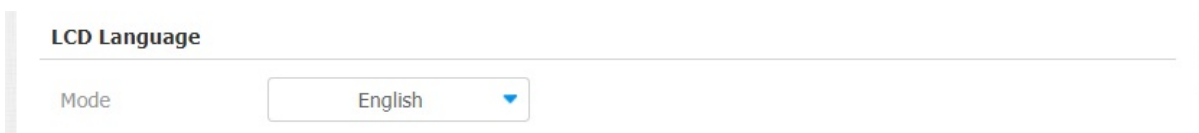
### Language Setting on the Device

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**.



### Note

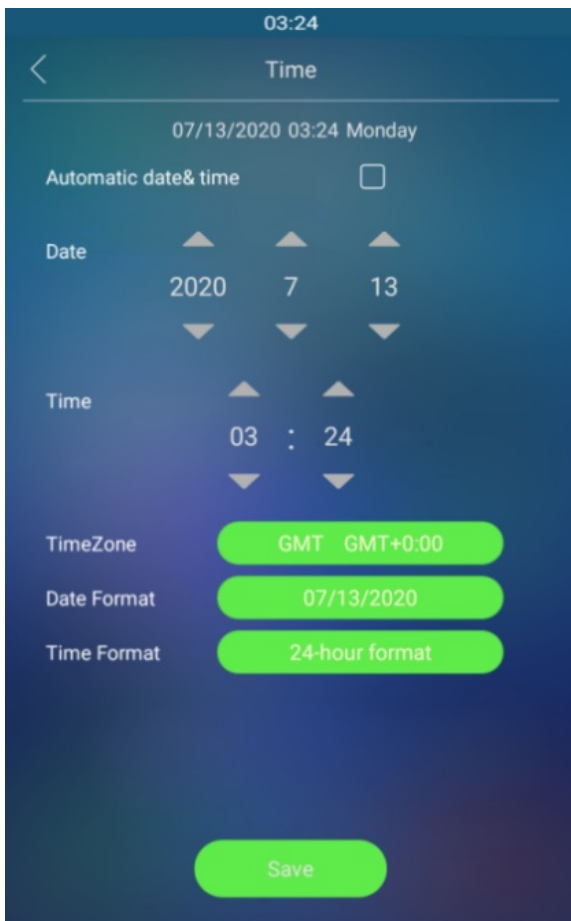
- R29Z/R29ZL only supports English and Chinese for LCD and web display.

## Time Setting

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

### 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 Zone:** select the specific time zone depending on where the device is used and then press **Confirm** tab for confirmation. The default time zone is **GMT GMT+0.00**.
- **Date Format:** select the date format you like among three format options: **M-D-Y; D-M-Y; Y-M-D** and then

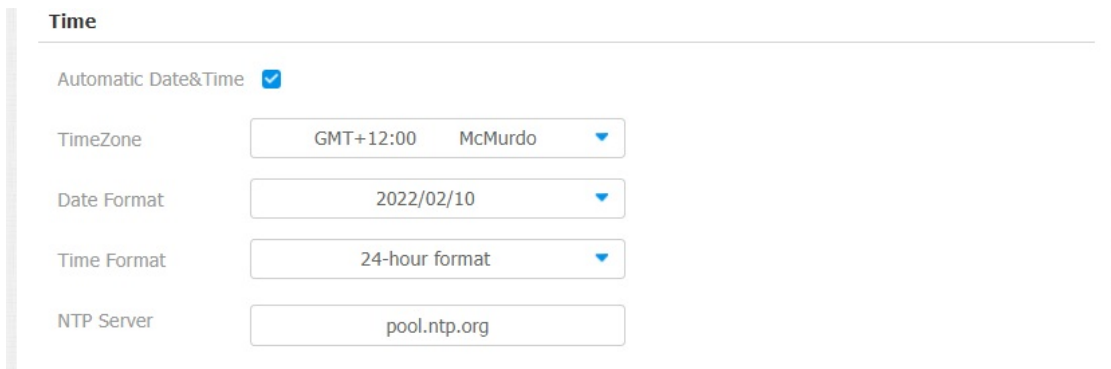


press the **Confirm** tab for confirmation.

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

## Time Setting on the Device Web Interface

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



Time	
Automatic Date&Time	<input checked="" type="checkbox"/>
TimeZone	GMT+12:00 McMurdo ▼
Date Format	2022/02/10 ▼
Time Format	24-hour format ▼
NTP Server	pool.ntp.org

### Parameter Set-up:

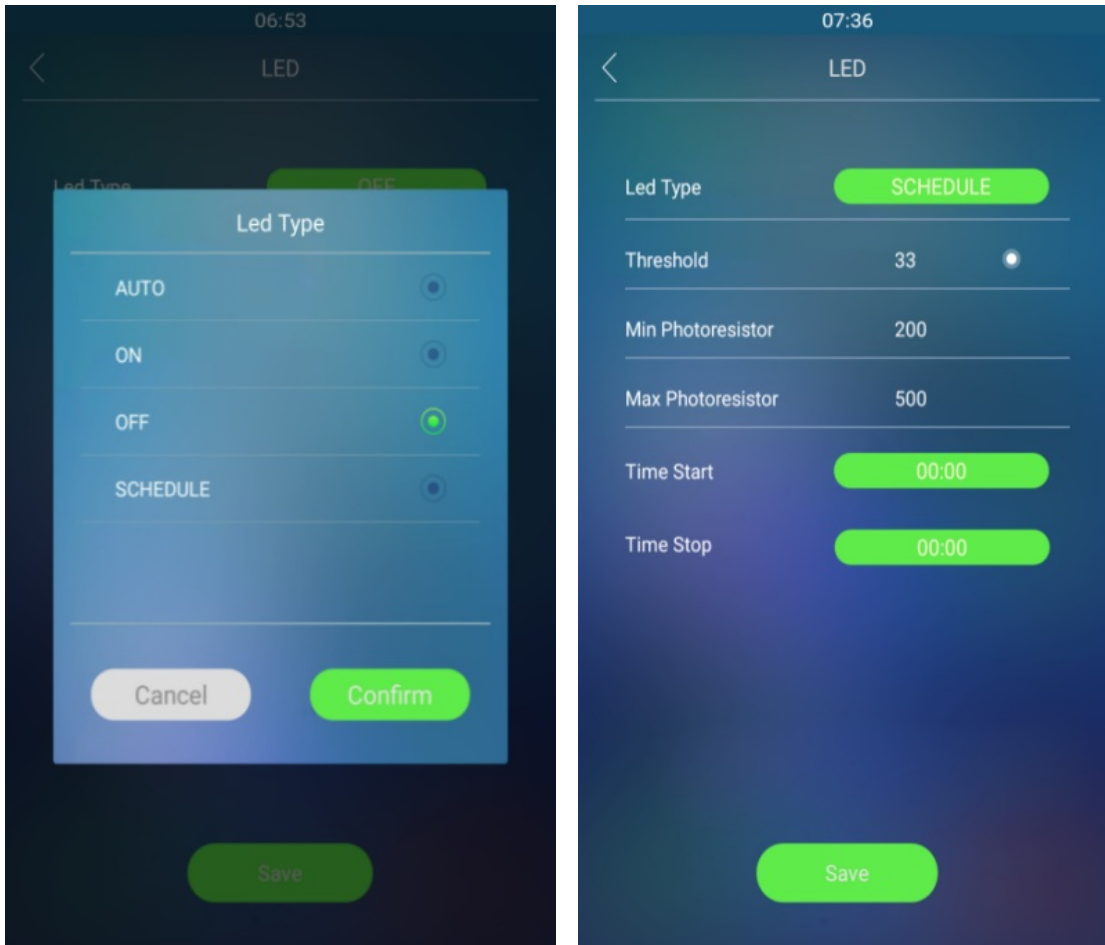
- **NTP Server:** enter the NTP server you obtained in the **NTP server** field.

## LED&LCD Setting


### Infrared LED Setting on the Device

Infrared LED is used to help you see the surrounding in front of the door phone through the door phone camera in a dark environment.

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



### Parameter Set-up:

- **Auto:** select **Auto** if you want the Infrared LED light to be turned on automatically according to the setting.
- **ON:** select **ON** to enable the Infrared LED light to stay on permanently.
- **OFF:** select **OFF** to turn off the Infrared LED light.
- **SCHEDULE:** select **SCHEDULE** to turn on the infrared LED according to the time schedule.
- **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. While 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. While 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 **Intercom > LED Setting > LED Control** 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.

**LED Control**

Card LED Enabled:

Time (H): 18 - 23 (0~23)

Submit Cancel

### Parameter Set-up:

- **Card LED Enable:** click to enable or disable the card reader LED lighting in the **Card LED Enable** field.
- **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 in web **Intercom > Advanced > LCD** interface.

**LCD**

High Contrast

Backlight Mode

Backlight Brightness...  (0~255)

Backlight Brightness...  (0~255)

Backlight Brightness...  (0~255)

Backlight Brightness...  (0~255)

Screen Touch Mode

## LCD Heat Control

To ensure the normal operation of the door phone in low-temperature environments, you can heat up the device's LCD screen according to your heat control setting. To set up the LCD heat control, navigate to **Intercom > Basic > LCD Heat Control**.

**LCD Heat Control**

Heat Switch

Heat Threshold  (-100~100C)

Interval  (0~65535s)

### Parameter Set-up:

- **Heat Switch:** enable the heat control function if needed.
- **Heat Threshold:** set up the heat control threshold from -100 °C to 100 °C. For example, if you set it at 40 °C, then the device LCD screen will be automatically heated up to 40 °C when the LCD screen is detected lower than 40 °C. The device will stop the automatic heat-up when the temperature reaches the threshold value.
- **Interval:** set up the automatic temperature detection interval for the device temperature. The device has a built-in temperature sensor.

## LED White Light Setting

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

**White Light**

---

Mode

Limit Backlight Value  (0~255)

White Light PWM Va...  (0~100)

**Parameter Set-up:**

- **Mode:** enable the white light mode.
- **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

R29 series door phone allows you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized settings to your preference.

### 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 in web **Intercom > Advanced > UI** interface.

**UI**

---

Foreground Color

Background Color

**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.

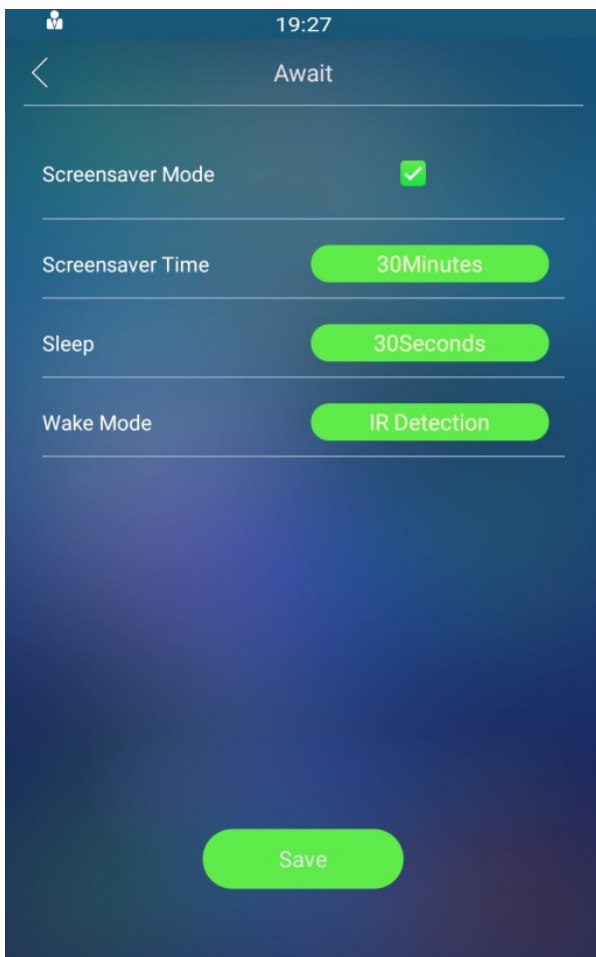
### Note

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



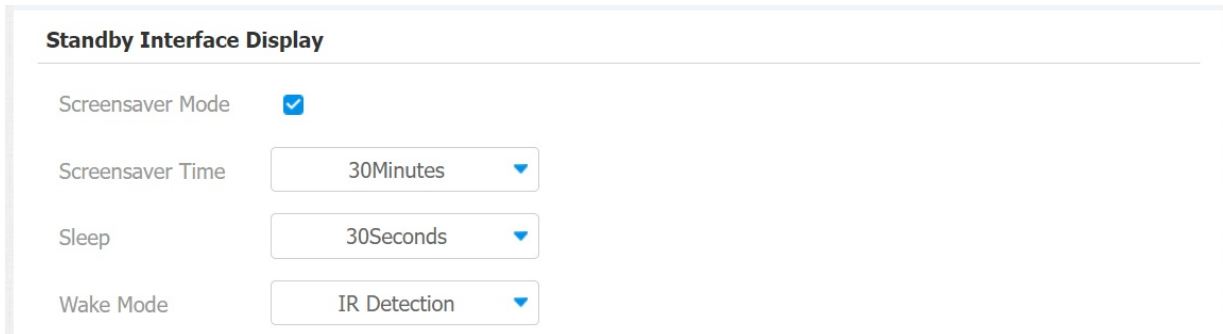
### Parameter Set-up:

- **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 detects 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.

## Await Screen Setting on the Web Interface

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



**Standby Interface Display**

Screensaver Mode

Screensaver Time

Sleep

Wake Mode

### 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 detects 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.

## Upload Screen Saver

You can upload screen saver pictures separately or in batch to the device and to the device web **Phone > Import/Export > Upload Screensaver Picture** interface for publicity purpose or for a greater visual experience. 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"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
2	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
3	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
4	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
5	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>

Please Choose ScreenSaver ID for upload

Screensaver1

(Support Size:2M; format:jpg)

**Parameter Set-up:**

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

**Note**

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

**Upload Pictures for Alphanumeric mode Screen Display**

You can upload the pictures for poster display and other background displays in alphanumeric mode. Go to **Phone > Import/Export > Import Contact Background(.png)**.

### Import Background (.png)

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

Main Page:

Other Pages:

**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.

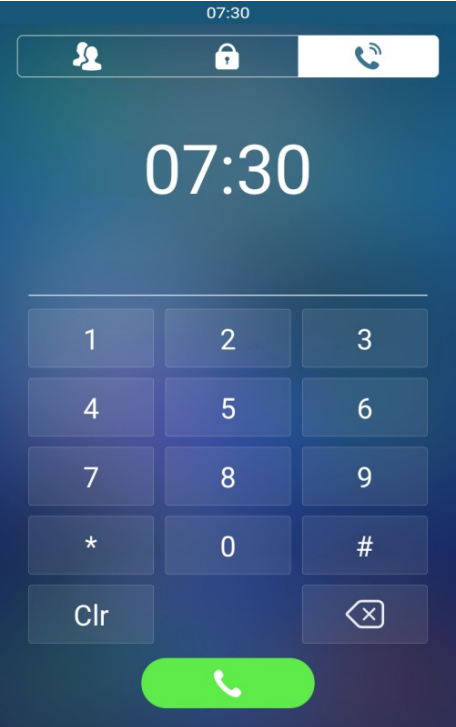
## Upload Background Picture in the Time-displaying Area

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

**Time View Background (.png)**

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

Picture  **Select File** **Import** **Reset**



The screenshot shows a mobile dial screen with a dark blue background. At the top, the time 07:30 is displayed in large white digits. Below the time is a numeric keypad with buttons for digits 1-9, \*, 0, #, a clear (Clr) button, and a backspace button. A green call button is at the bottom. The interface is framed by a light blue border.

### 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 upload the logo you like on the device. You can navigate to **Phone > Import/Export > Import Logo (.png)**.

### Import 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

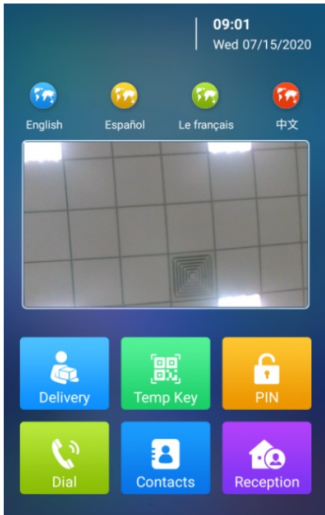
R29 series door phones offer you four types of screen display modes for the application scenarios: **Building Mode**, **Office Mode**, **Villa Mode**, and **Alphanumeric Mode**. You can make the configuration on the device web **Intercom > Key/Display > Theme** interface to select the specific mode based on actual application scenarios.

### Theme

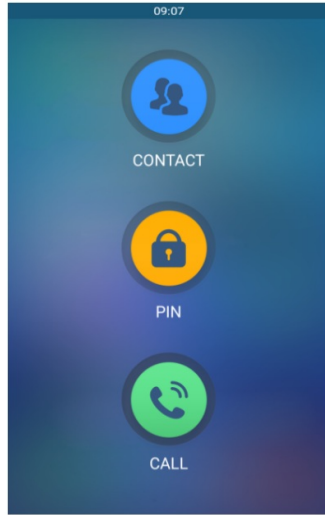
Theme

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 change the home screen display through the configuration of tab arrangement, and the language icon display as needed on the device web **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 position one of tab row one, 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.

**Select Icons**

Select Icon

Type

**Parameter Set-up:**

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

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

### Language Setting Of The Building Theme

Language

Language1	Language2	Language3	Language4
<input type="text" value="English"/>	<input type="text" value="Español"/>	<input type="text" value="Français"/>	<input type="text" value="简体中文"/>

#### 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 **Contact** icon, **PIN** icon, and **Call (Dial)** icon on the home screen in villa mode. In addition, you can set those icons as your home screen while configuring their respective smaller icons on the top of the screen in the villa mode according to your need on web **Intercom > Key/Display > Key In Homepage Of The Office Theme And Villa Theme** interface.

### Key In Homepage Of The Office Theme And Villa Theme

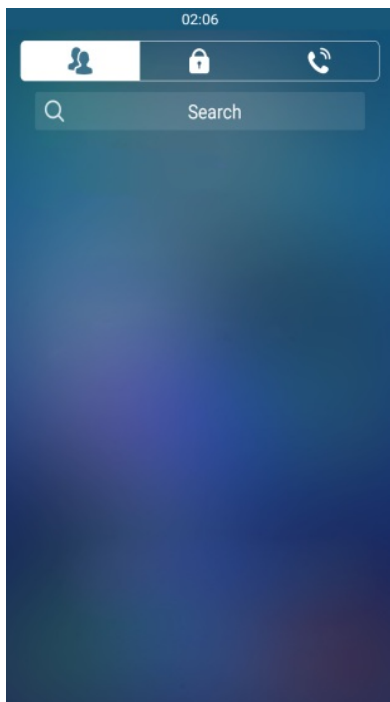
Display Type

ID	Type	Name	Visible
1	<input type="text" value="Contact"/>	<input type="text"/>	<input type="text" value="Visible"/>
2	<input type="text" value="PIN"/>	<input type="text"/>	<input type="text" value="Visible"/>
3	<input type="text" value="Call"/>	<input type="text"/>	<input type="text" value="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, if 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 any one of the icons for Dial, Contact, and Password will be displayed in highlight together on the top of the home screen with the other two 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

### 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.



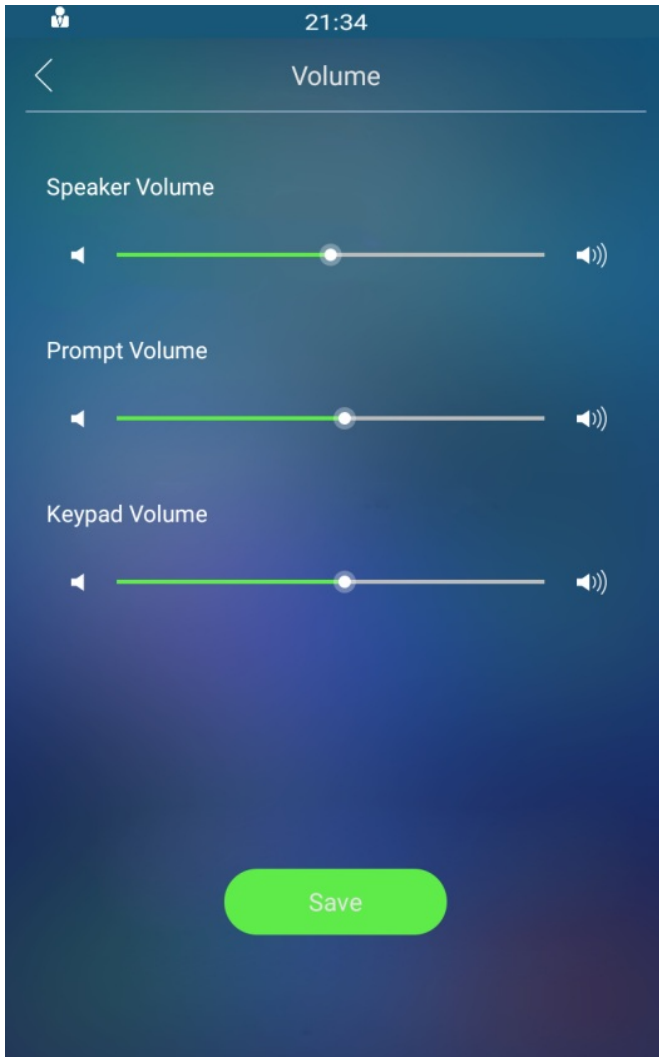
## Volume and Tone Configuration

Volume and tone configuration in R29 refers to the Call volume, the AD volume, key volume, and Mic volume and open door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

### Volume Configuration

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





**Parameter Set-up:**

- **Speaker Volume:** adjust the speaker volume.
- **Prompt Volume:** adjust the announcement volume. The announcement can be, for example, the open door success announcement, ringback sound, and other prompt sounds.
- **Keypad Volume:** adjust the volume for the button touch sound.

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)

**Parameter Set-up:**

- **Mic Volume:** adjust the volume of your voice to be heard.
- **Speaker Volume:** adjust the speaker volume during the call.
- **Keypad Volume:** adjust the volume for the button touch sound.
- **Tamper Alarm Volume:** set the tamper alarm volume.
- **Prompt Volume:** set the prompt volume.

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.



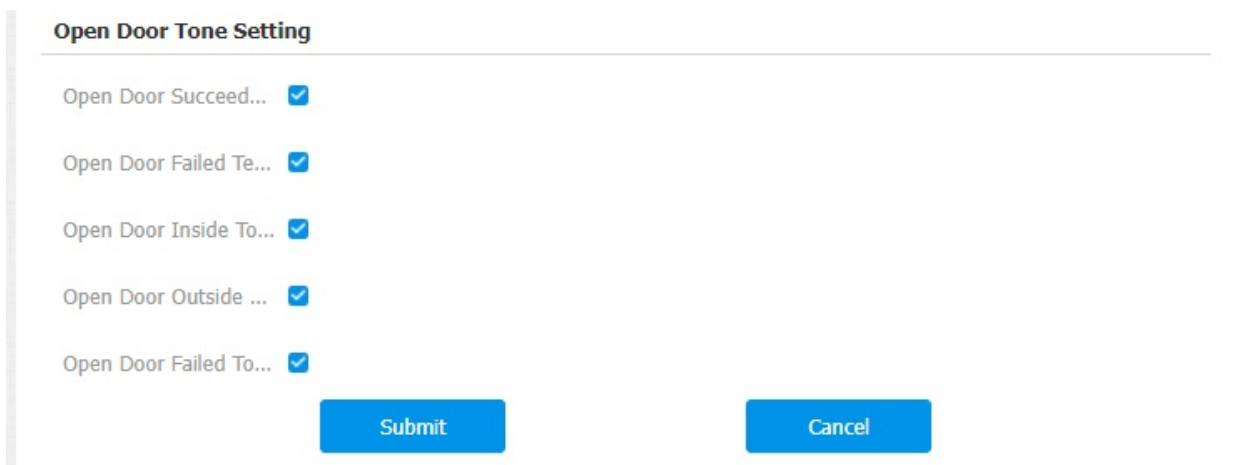
The screenshot shows a web interface titled "Others". It features a dropdown menu for "Return Code When ..." set to "486(Busy Here)". Below this, the "Call Volume" option is checked with a blue checkbox. At the bottom of the form are two blue buttons: "Submit" and "Cancel".

#### 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.



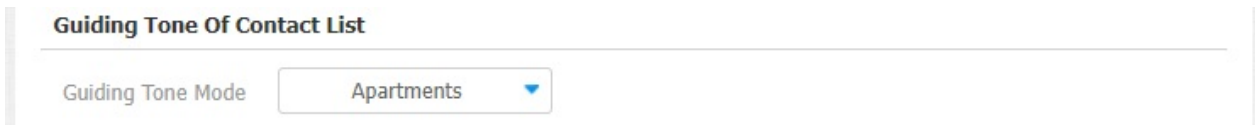
The screenshot shows a web interface titled "Open Door Tone Setting". It lists five options, each with a checked blue checkbox: "Open Door Succeed...", "Open Door Failed Te...", "Open Door Inside To...", "Open Door Outside ...", and "Open Door Failed To...". At the bottom of the form are two blue buttons: "Submit" and "Cancel".

#### Parameter Set-up:

- **Open Door Tone:** click the **Enable** and **Disable** depending on if you want to hear the tone or not.

## Contact List Guiding Tone Configuration

You can select the guiding tone on the contact list screen if needed. You can navigate to **Phone > Audio > Guiding Tone of Contact List**.



**Parameter Set-up:**

- **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.

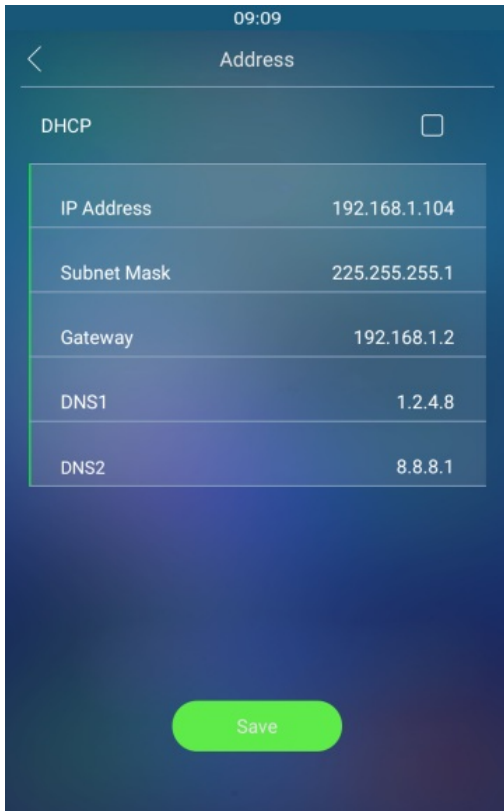
**Upload Tone (.wav)**

ID	Type	Select File	Import	Reset
1	Open Door Outside	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
2	Open Door Inside	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
3	Hello	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
4	Calling	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
5	Delivery	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
6	Temp Key	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
7	PIN	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
8	Dial	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>
9	Contacts	Not selected any files <input type="button" value="Select File"/>	<input type="button" value="Import"/>	<input type="button" value="Reset"/>

**Network Setting**

**Device Network Connection Setting**

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



**Parameter Set-up:**

- **DHCP**: select the **DHCP** mode by checking off the DHCP box. 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**: select the static IP mode by checking off the DHCP square box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your actual network environment.
- **IP Address**: set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **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			
Port Type	DHCP Auto	Link Status	Connected
IP Address	192.168.31.8	Subnet Mask	255.255.255.0
Gateway	192.168.31.1	Preferred DNS Server	192.168.31.1
Alternate DNS Server			

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

The screenshot shows the 'Basic' network configuration page. Under the 'LAN Port' section, there are several settings:

- DHCP:** Checked (checkbox with a blue checkmark).
- Static IP:** Unchecked (checkbox).
- IP Address:** 192.168.1.104
- Subnet Mask:** 255.255.255.0
- Default Gateway:** 192.168.1.1
- Preferred DNS Server:** 192.168.1.1
- Alternate DNS Server:** 192.168.1.1

## Device Local RTP configuration

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

The screenshot shows the 'Local RTP' configuration page. It contains two input fields:

- Starting RTP Port:** 11800 (range: 1024~65535)
- Max RTP Port:** 12000 (range: 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

Door phones should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address and extension numbers as opposed to other devices for device control and the convenience of the management. So you can do it on the web **Network > Advanced > Connect Setting** interface.



**Connect Setting**

Server Mode: Cloud

Discovery Mode:

Device Address: [1] [1] [1] [1] [1]

Device Extension: [1]

Device Location: [Gate1]

**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:** click **Enable** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click **Disable** if you want to conceal the device so as not to be discovered by other devices. 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**

NAT (Network Address Translation) allows hosts in an organization’s private intranet to transparently connect to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. To set up NAT, you can do it on the web **Account > Advanced > NAT** interface.



**NAT**

UDP Keep Alive Mes...

UDP Alive Msg Inter... [30] (5~60s)

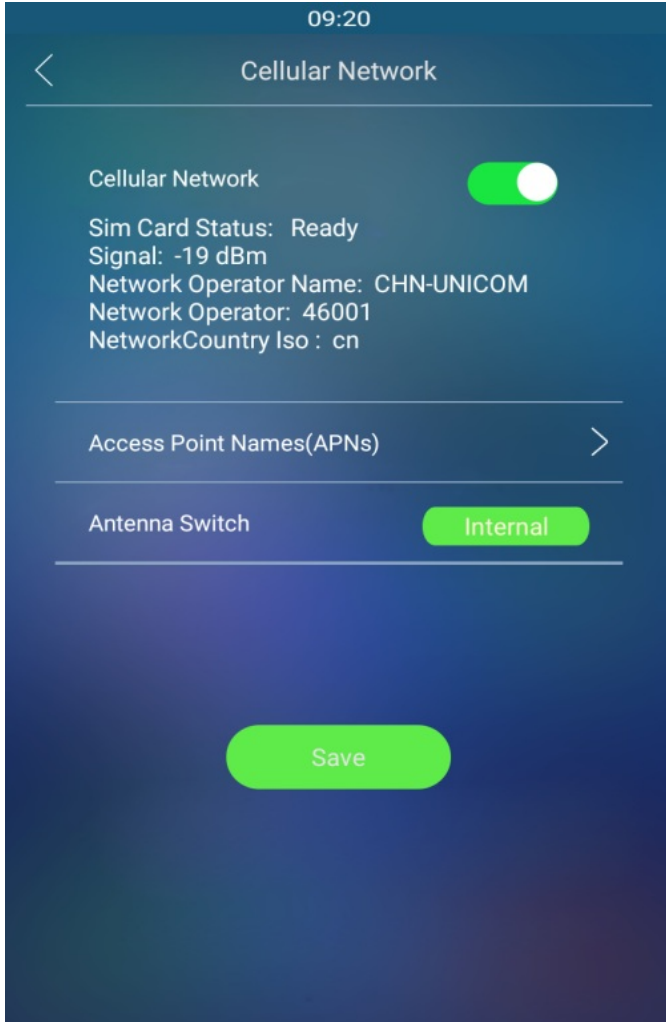
RPort

**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)**

In addition to wired connection, the device is installed with an LTE module which allows both users and installers to conduct a convenient, quick and wireless connection in the installation environment with no access to wired network such as old buildings, etc. Only R29C-L has an LTE module and the LTE setting only shows after inserting the SIM card. 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 Check

LTE data usage in R29CL door phone can be checked on the device web **Network > Data Usage > Data Information** interface.

### Data Information

Data Used	0GB0MB	
Data Remaining	--	

### LTE Data Usage Configuration

You can also manage the data usage on the web **Network > Data Usage > Data Plan Setting** interface in order to be informed on the data consumption according to your configuration.

### 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 URL	
Http URL	<input type="text"/>	
<input type="button" value="Submit"/>		<input type="button" value="Cancel"/>

### Parameter set-up:

- **Unlimited Data:** click **enable** 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 percent point reaches the default value **80** actions will be executed for the purpose of notification when it reaches **80** the data percentage point.
- **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

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

### IP call & IP Call Configuration

IP calls can be made directly on the intercom device by entering the IP number on the device. And you can also disable the direct IP call if you allow no IP call to be made on the device web **Phone > Call Feature > Direct IP** interface.



The screenshot shows a configuration panel titled "Direct IP". It has two main settings: "Enabled" and "Port". The "Enabled" setting is currently checked with a blue checkmark. The "Port" setting is a text input field containing the number "5060", with a range "(1~65535)" shown to the right of the field.

#### Parameter Set-up:

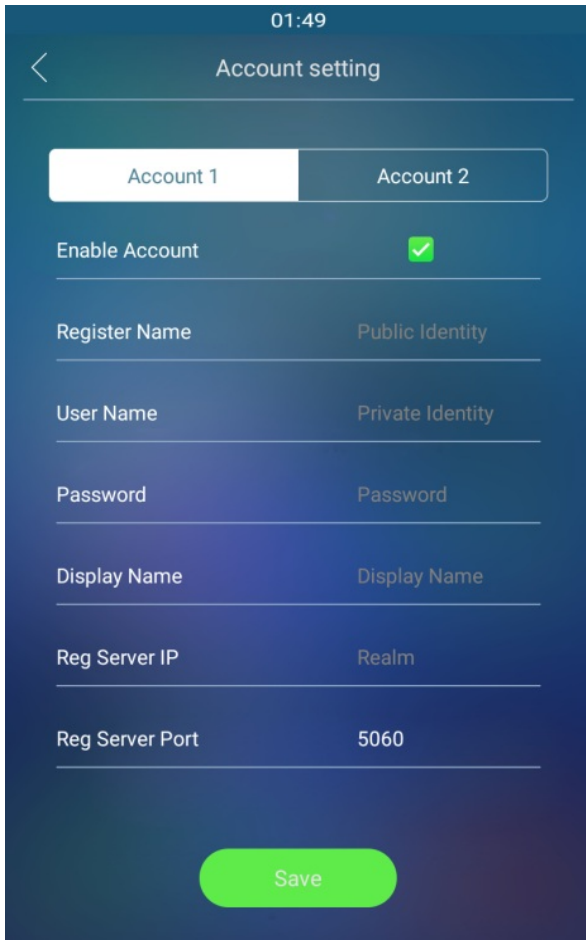
- **Enabled:** click **Enable** or **Disable** to turn the direct IP call on or off. For example, if you do not allow direct IP call to be made on the device, you can click **disable** to terminate the function.
- **Direct IP Port:** the direct IP Port is **5060** by default with the port range from **1-65535**. And you enter any values within the range other than the 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission.

### SIP Call & SIP Call Configuration

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

#### SIP Account Registration

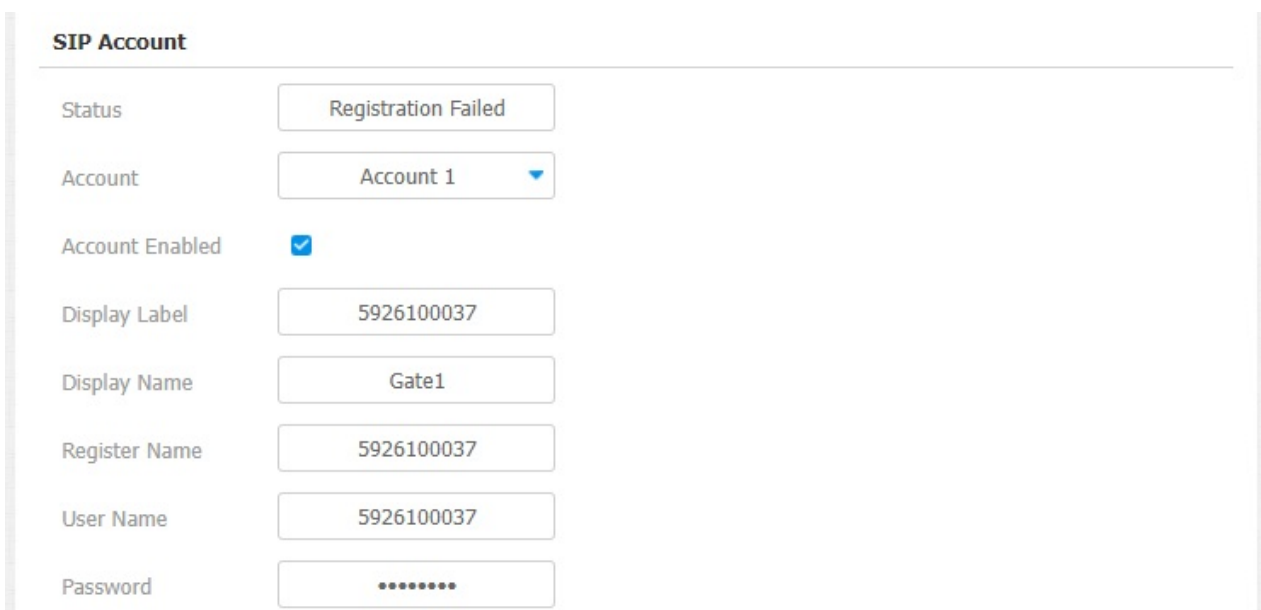
R29 series door phones support two SIP accounts that can all be registered according to your applications. You can, for example, switch between them if any one of the accounts failed and become invalid. The SIP account can be configured on the device screen and on the device web interface. To configure the SIP account on the device **Account** screen.



**Parameter set-up:**

- **Account 1/Account 2:** select Account 1 or Account 2. Account 1 is the default SIP account.
- **Reg Server port:** enter the SIP server port for communication. The SIP port is **5060** by default.

Other parameter settings for SIP account registration can not be configured on the Account setting screen as they can only be configured on the device web **Account > Basic > SIP Account** interface.



### Parameter Set-up:

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

### SIP Call DND&Return Code Configuration

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

The screenshot shows a web interface for DND configuration. It is divided into two sections: 'DND' and 'Others'. In the 'DND' section, there is an 'Enabled' checkbox which is currently unchecked. Below it is a dropdown menu labeled 'Return Code When ...' with the value '486(Busy Here)' selected. In the 'Others' section, there is a similar dropdown menu labeled 'Return Code When ...' also with '486(Busy Here)' selected.

### Parameter Set-up:

- **Enabled:** enable or disable the DND function. DND function is disabled by default.
- **Return Code When DND:** select what code should be sent to the calling device via the SIP server. **404 for Not found; 480 for Temporary unavailable; 486 for busy here.**
- **Return Code When Refuse:** select code to be sent to the caller side via the SIP server when you rejected the incoming call.

### SIP Server Configuration

Two SIP servers can be set up for the device in order to achieve call session through the SIP servers between intercom devices. SIP server 2 serves as a backup to SIP server 1. To do it, on the device web **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)

**Parameter Set-up:**

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

**Outbound Proxy Server configuration**

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

Outbound Proxy Server		
Outbound Enabled	<input type="checkbox"/>	
Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)
Backup Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024~65535)

**Parameter Set-up:**

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

**Data Transmission Type Configuration**

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

The screenshot shows the 'Transport Type' configuration page. A dropdown menu is open, displaying the following options: UDP (highlighted in blue), TCP, TLS, and DNS-SRV. A blue 'Cancel' button is located to the right of the dropdown menu.

**Parameter Set-up:**

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

**SIP Hacking Protection**

Internet phone eavesdropping is a kind of network attack, which aims to eavesdrop on the communication sessions of others in an unauthorized way. Attackers can use this malicious activity to capture and read content containing sensitive and confidential information. SIP hacking prevents SIP calls from hacking on the Internet.

The screenshot shows the 'Call' configuration page. It includes the following settings:
 

- Max Local SIP Port: 56592 (range: 1024~65535)
- Min Local SIP Port: 56582 (range: 1024~65535)
- Auto Answer:
- Prevent SIP Hacking:

**Parameters Set-up:**

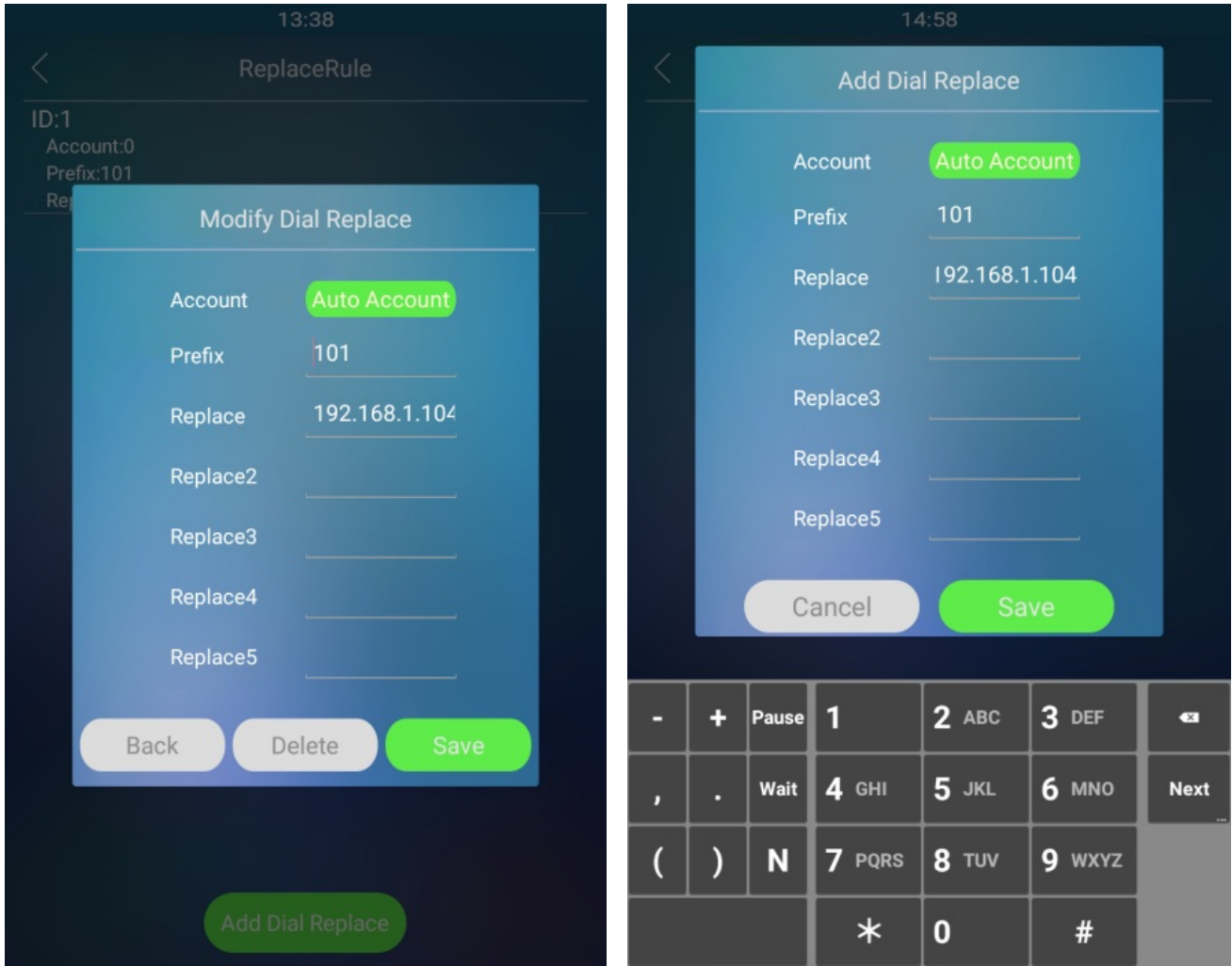
- **Prevent SIP Hacking:** enable to activate this feature during using sip call. This feature is only available for SIP call, not IP call.

**Dial Options Configuration**

R29 series offers a variety of Dial options that allows you to have a fast dial experience while relieving you off memory burden due to long and complex dial numbers.

## Quick Dial By number Replacement

If you want to replace the long and complex dial number with a shorter number that can be memorized at greater ease and convenience for making calls, you can configure the dial number replacement on the device and on the device web interface. You can replace multiple device dial numbers such as IP address with only one short number. To configure the number replacement on the device **ReplaceRule** screen.



### Parameter Set-up:

- **Account:** select the account to which you want to apply dial number replacement. The account is **Auto** by default (to call out from the account in which the dial number has been registered). You can select either account 1 or account 2 from which the number can be dialed out. if you have registered the dial number in both Account 1 and Account 2, then the number will be called out from Account 1 by default.
- **Prefix:** enter the short number to replace the dial number you wish to replace.
- **Replace 1/2/3/4/5:** enter the dial number(s) you wish to replace. It supports up to 5 number maximum for the replacement on the device configuration. For example, if you replace five original dial numbers with a common short number such as 101 then the five intercom devices with the dial number will be called at the same time when you dial 101.

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

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						

Delete 
+ Add
Edit 
Prev
1/1
Next
1
Page

**Rules Modify >>**

Account:

Replace 1:

Replace 3:

Replace 5:

Prefix:

Replace 2:

Replace 4:

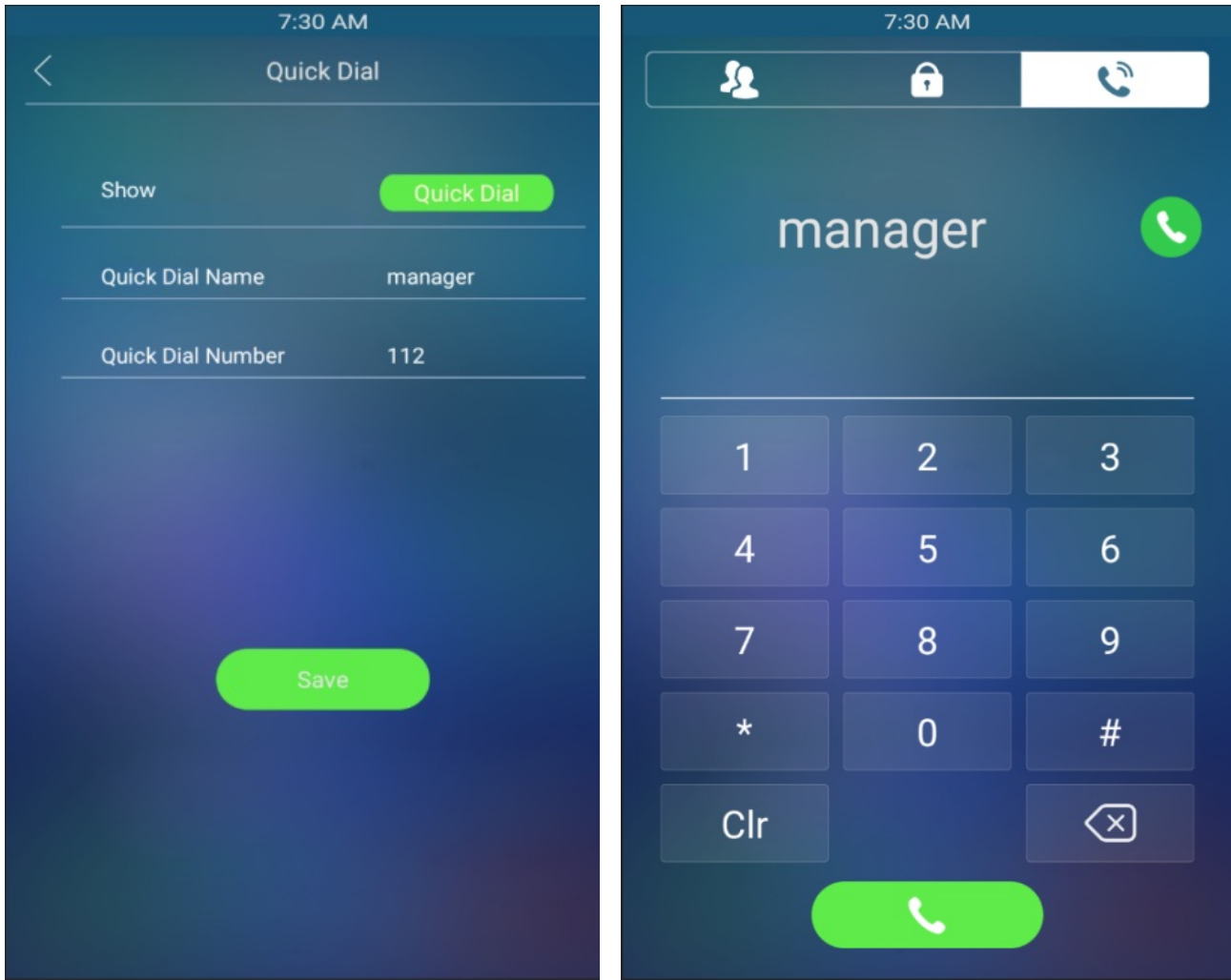
Submit
Cancel

**Note**

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

### 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.



**Parameter Set-up:**

- **Show:** select the **Quick Dial** in order to conceal the time display. If you select the clock option, then the time will be displayed on the time screen.
- **Quick Dial Name:** create a quick dial name such as **Manager** according to your need.
- **Quick Dial number:** enter the quick dial number, which can be a SIP number or an IP address number.

**Note**

- This function cannot be applied in **Building Mode**.

**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)**.





## Speed Dial on the Home Screen

Speed dial is a function that allows you to create a tab or a combination of organized tabs to be displayed on the device's dial screen. You can make calls by pressing the specific tabs to make speedy calls without entering any dial numbers. To configure the speed dial on the web **Phone > Speed Dial > Speed Dial Contacts Management** interface.

**Speed Dial Theme**

Speed Dial Theme: 2 keys + keypad

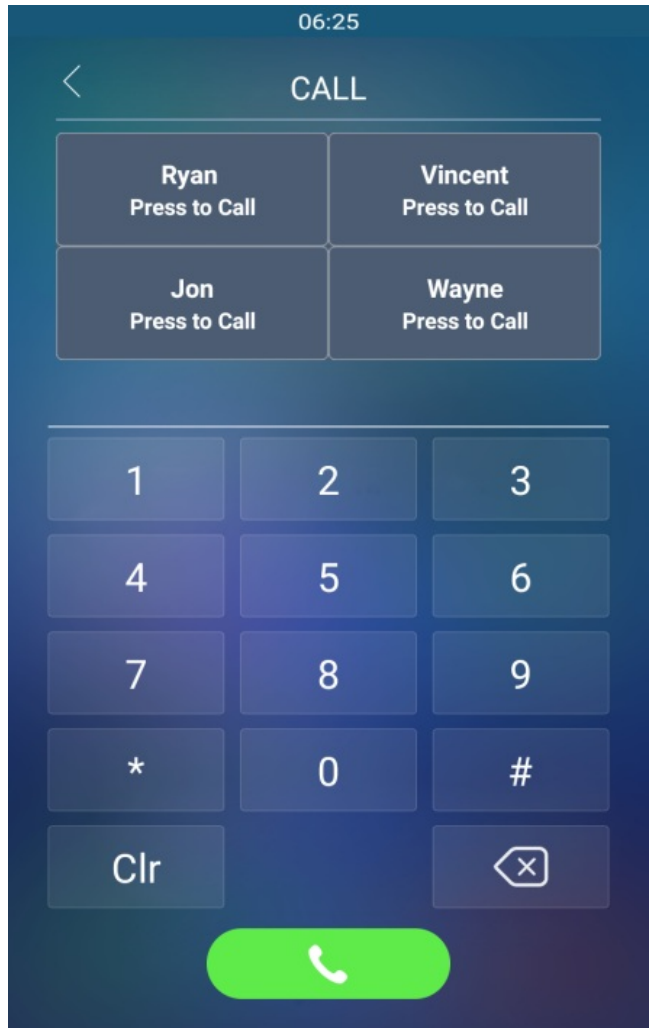
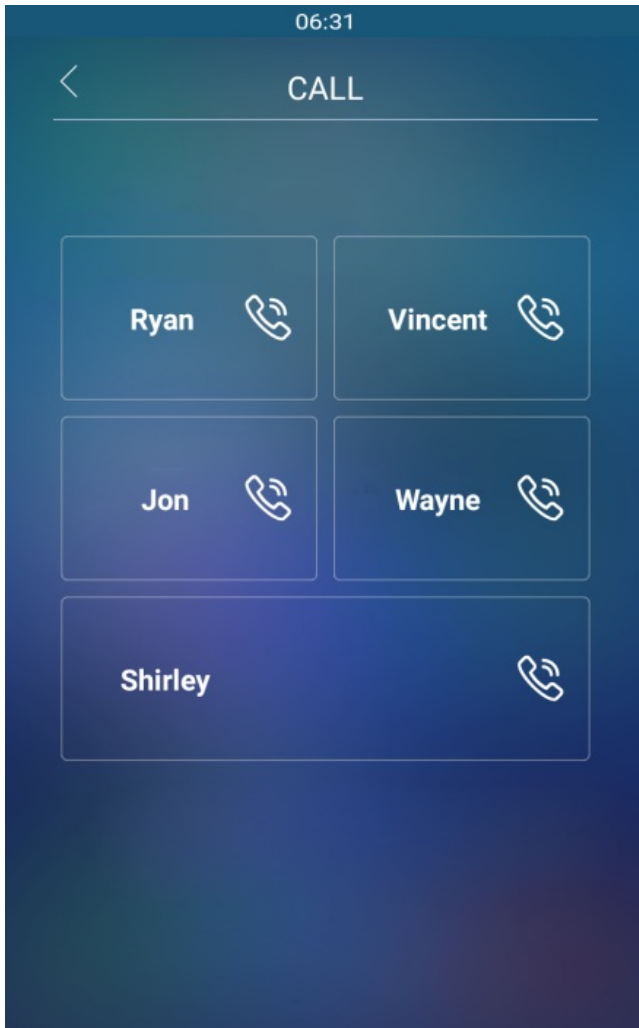
**Speed Dial Contacts Management**

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"/>

### Parameter Set-up:

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

Options	Descriptions
<b>Standard</b>	Select <b>Standard</b> if you want to display the time and key pad only with no dial tabs.
<b>Auto</b>	Select <b>Auto</b> if you want to select the dial tab layout that does match with any one of the other 8 options. For example, if you want to create 3dial tabs, 5 dial tabs or 7 tabs etc., that does not match with other options.
<b>1 Key</b>	Select <b>1 Key</b> if you display only one dial tab with no keypad.
<b>1 Key + Keypad</b>	Select <b>1 Key+Keypad</b> if you want to display one dial tab with key pad.
<b>2 Keys+ Keypad</b>	Select <b>2 Key+Keypad</b> if you want to display two dial tabs with keypad.
<b>8 Keys</b>	Select <b>8 Keys</b> if you want to display 8 dial tabs with no keypad.
<b>16 Keys</b>	Select <b>16 keys</b> if you want to display 16 dial tabs with no keypad.
<b>64 Keys</b>	Select <b>64 keys</b> if you want to display 64 dial tabs with no keypad.



**Note**

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

## Group Speed Dial

R29 allows you to make speed dial to the contacts in one contact group. So When you press the reception icon on the door phone, you can dial the all contact numbers in the group at the same. You can navigate to **Intercom > Key/Display > Speed Dial Setting**.



**Parameter Set-up:**

- **Group:** select **disable** to disable the speed dial function. And select the specific contact group if you want to make speed dial to the contacts in the selected contact group.

## Dial Key Order

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

The screenshot shows a configuration page titled "Keypad Display Mode Of PIN Interface". There is a label "Display Mode" followed by a dropdown menu that currently displays "Disorder".

### Parameter Set-up:

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

## Call Auto-answer Configuration

You can define how quickly the door phone should respond in answering the incoming SIP/IP call automatically by setting up the time related parameters. In addition, you can also define the mode in which the calls are to be answered. (video mode or audio mode) To do the configuration on the web **Account > Advanced > Call** interface.

The screenshot shows a configuration page titled "Call". It contains the following settings:

- Max Local SIP Port: 47539 (range: 1024~65535)
- Min Local SIP Port: 47529 (range: 1024~65535)
- Auto Answer:
- Prevent SIP Hacking:

After the Auto Answer is enabled, navigate to **Phone > Call Feature > Auto Answer**.

The screenshot shows a configuration page titled "Auto Answer". It contains the following settings:

- Auto Answer Delay: 0 (range: 0~5 Sec)
- Mode: Video

### Parameter Set-up:

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

## Sequence Call Configuration

Sequence call is a function supported by Akuvox cloud which releases a group of sequence call numbers for the application. You can call the targeted group of sequence calls (e.g. your extension numbers in your kitchen, bedroom, etc.) in sequential orders until the call is answered. Sequence call will complete as soon as the call is answered by any of the targeted extension devices. To do the configuration in web **Intercom > Basic > Sequence Call** interface.

The screenshot shows the 'Sequence Call' configuration panel. At the top, the title 'Sequence Call' is displayed. Below it, there is a row with the label 'Enabled' and a grey square toggle switch. The second row has the label 'Time Out(Sec)' and a dropdown menu showing the value '20' with a downward arrow.

#### Parameter Set-up:

- **Enable:** this function is controlled by Akuvox SmartPlus. You can check whether it is enabled or not.
- **Timeout(Sec):** to check the call time interval in between the sequence call number in a targeted sequence Call group. For example, if you set the time interval as 10 seconds, then the call (if not answered in 10 Sec.) will be terminated automatically and be transferred sequentially to the next sequence call number in the targeted sequence call group.

#### Note

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

## Web Call Configuration

In addition, to make IP/SIP calls directly on the device, you can also make the call on the device web **Intercom > Basic > Web Call** interface without approaching the device physically for testing purpose, etc.

The screenshot shows the 'Web Call' configuration panel. At the top, the title 'Web Call' is centered. Below it, there is a row with the label 'Web Call(Ready)', a text input field containing 'Web Call Number', a dropdown menu showing 'Auto' with a downward arrow, and two buttons: 'Dial Out' and 'Hang Up'.

#### Note

- **Auto** as the default value in the field is not clickable for selection. It enables the door phone to select an appropriate SIP account to call out.

## Call Settings

### Maximum Call Duration Setting

R29 series door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the calling automatically. To do this configuration in device web **Intercom > Basic > Max Call Time** interface.

Max Call Time	
Max Call Time	<input type="text" value="5"/> (2~30 Min)

**Parameter Set-up:**

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

### Maximum Dial Duration Setting

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

Max Dial Time	
Dial In Time	<input type="text" value="60"/> (5~120 Sec)
Dial Out Time	<input type="text" value="60"/> (5~120 Sec)

**Parameter Set-up:**

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

### Hang Up After Open Door

This feature is used to hang up the call automatically after the door is released during a call. So the caller or callee does not need to click the **Hang up** key again. To do this configuration on the web **Intercom > Basic > Hang Up After Open Door** interface.

**Hang Up After Open Door**

Type: DTMF Or HTTP

Time Out: 5 (0~15 Sec)

**Parameter Set-up :**

- **Type:** select the open door type. The door can be unlocked via the DTMF , HTTP command, DTMF Or HTTP , and DTMF, HTTP or Input.
- **Timeout:** the time out value can be set up from 1 second to 15 seconds. 5 seconds is default. The call will be automatically hung up within this value after the door is opened.

## Two-way Video Call

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

**Basic**

Gesture Control

Two-Way Video Enable

**Parameter Set-up:**

- **Two-Way Video Enable:** enable the two-way video, which allows you to see the callee’s video image on the door phone during a video c

## Audio& Video Codec Configuration for SIP Calls

### Audio Codec Configuration

R29 series supports four types of Codec (PCMU, PCMA, G729, 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 on the device web **Account > Advanced > SIP Account** interface.

**SIP Account**

---

Account Account 1 ▼

---

**Audio Codecs**

Disabled Codecs

>>

<<

Enabled Codecs

PCMU  
PCMA  
G729  
G722

↑

↓

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

## Video Codec Configuration

R29 series support 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  H264

Resolution VGA ▼

Bitrate 512 ▼

Payload 104 ▼

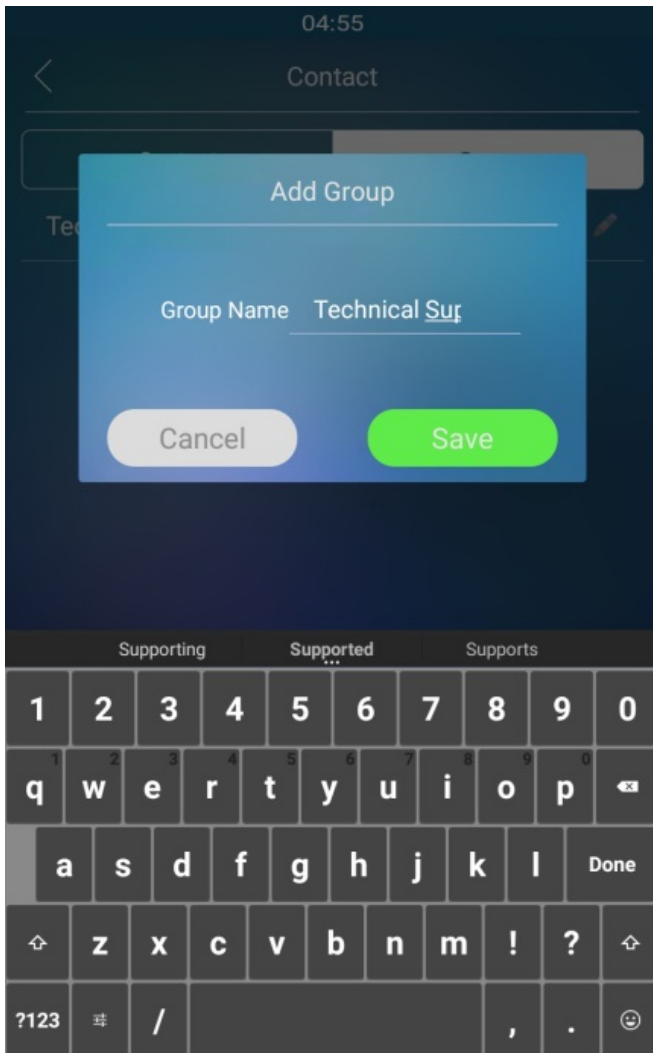
### Parameter Set-up:

- **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 4CIF.
- **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. While the default code bitrate is 2048.
- **Payload:** select the payload type (ranging from 90-118) to configure the audio/video configuration file. The default payload is 104.

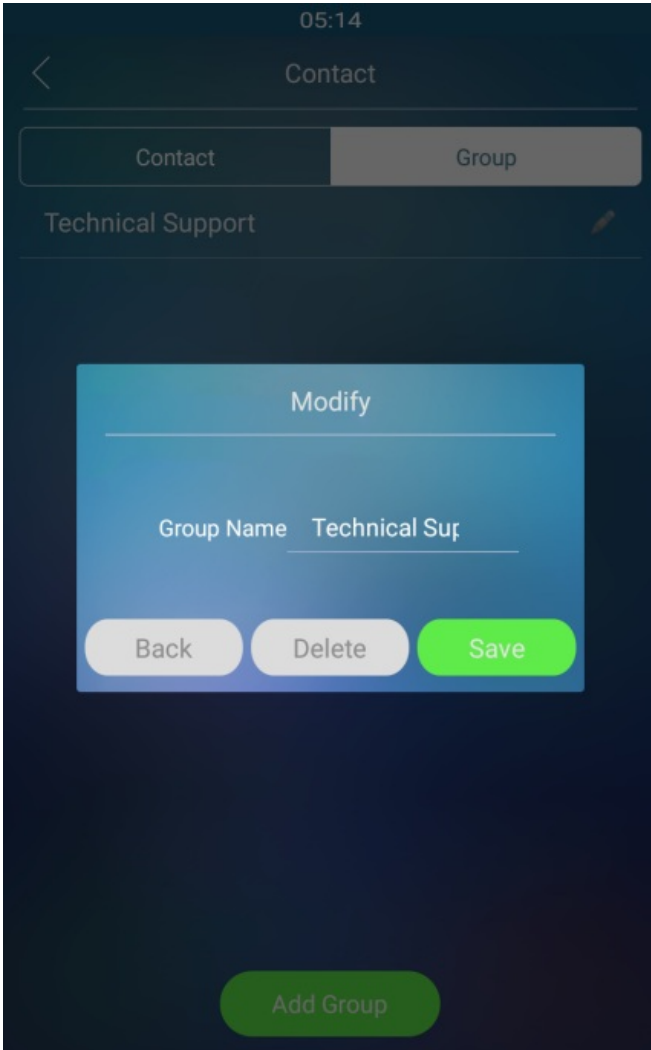
## Phone Book Configuration

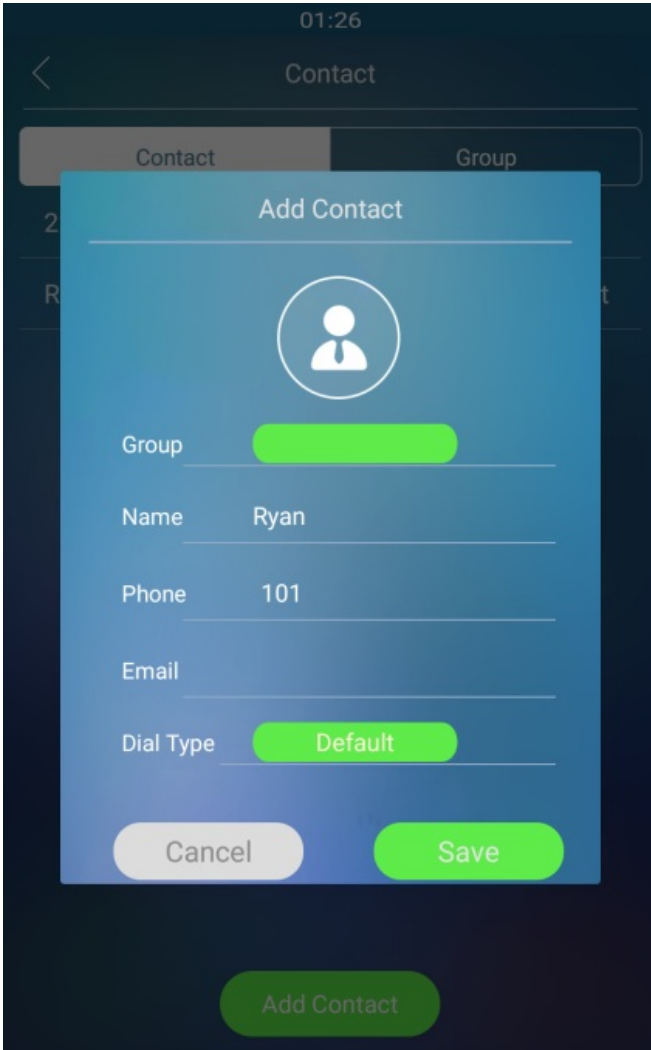
### Phone Book Configuration on the Device

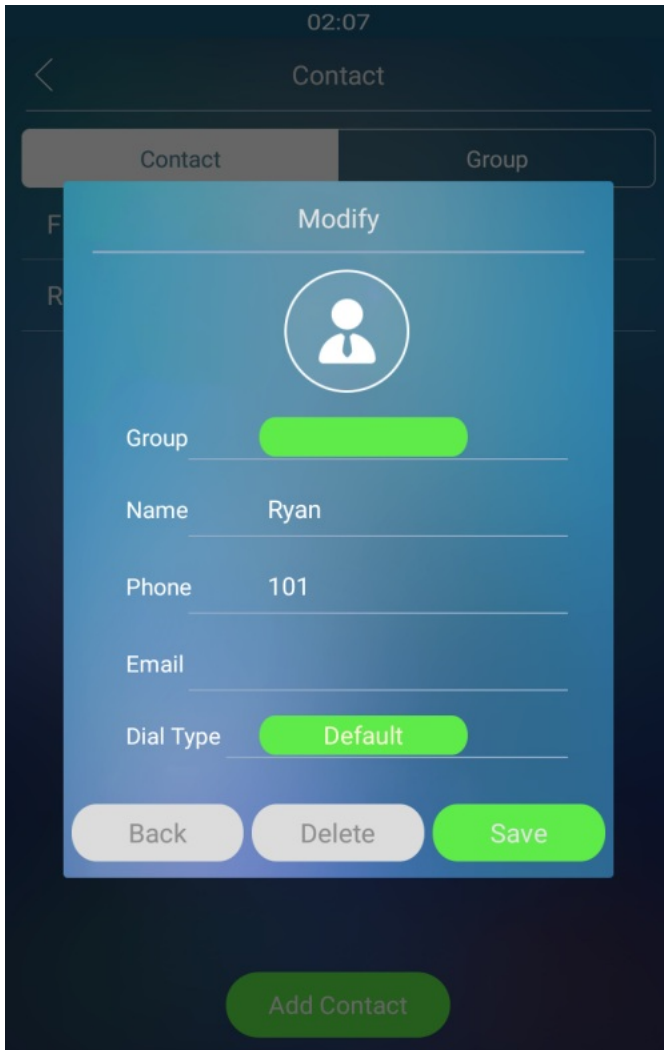
You can configure the phone book in terms of adding and modifying groups or contacts on the device directly. To configure the phone book on the device **Contact** screen.











### 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.
- **Name:** enter the contact name, which is required.
- **Phone:** enter the phone number of the contact, which is required.
- **Email:** enter the contact's Email, which is optional.
- **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

## Managing Contact Groups on the Web Interface

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

The screenshot displays the 'Group' management interface. It features two tables listing contact groups and a 'Group Setting' form below them.

**Group Table 1:**

<input type="checkbox"/>	Index	Name
<input checked="" type="checkbox"/>	1	Technical Dep..
<input type="checkbox"/>	2	
<input type="checkbox"/>	3	

**Group Table 2:**

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

**Group Setting Form:**

Name:

Buttons:

Navigation:    1/1

## Contact Configuration on the Web Interface

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

The screenshot shows the 'Contacts Setting' form with the following fields and options:

- Name:
- Phone:
- Email:
- Group:
- Dial Account:
- Lift Floor Number:
- Photo:  **Please upload the photo before editing contact if necessary**

Below the photo field, there are two image placeholders labeled 'Original Photo' and 'Cropped Photo'.

At the bottom, there is a file upload section with buttons:

### Parameter Set-up:

- **Name:** the name of the contact.
- **Phone:** the phone number of the contact. It supports IP address and SIP number.
- **Email:** the email address of contact.
- **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 phone book. Moreover, you can also dial out using the contact number directly. To do this configuration on device web **Contact > Contact List > Local Contact List**.

**Local Contacts List**

Contacts List Display All Contacts

Search  Search Reset

<input type="checkbox"/> Index	Name	Phone	Group	Dial Account	Email	FloorNum	Priority Of Call
<input checked="" type="checkbox"/> 1	Ryan	<a href="tel:1003">1003</a>	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							

Delete
Delete All
Prev
1/1
Next
1
Page

### Contacts Import and Export on the Web Interface

When the contact becomes so many that you can not afford to manage each contact one by one manually, you can import and export the contacts in batch on the device web **Phone > Import/Export > Import/Export Config&Contacts** interface.

### Import/Export Config&Contacts

Contacts:

#### 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.

## Contact 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...

#### 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 **Intercom > Basic > Door Setting General** interface to do the configuration.

### Door Setting General

Click Tenants To Dial...

Expand Tenants List ...

Hide Group Label Fo...

Contact List Search ...

Local Tenants Profile...

DialPad Input Numb...

#### 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.
- **DialPad Input Number Limit:** set the limit of numbers that can be entered on the dial pad. You can select 4,6,8,10 digits.

## 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 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

#### Parameter Set-up:

- **Relay ID:** you are allowed to set up three relay switches in total for the door access control (R29Z/R29ZL has only 1 relay).
- **Type:** if Default state is selected, the Relay Status shows Low which means the door is closed, the Relay Status shows High which means the door is opened. If Invert State is selected, the Relay Status shows High which means the door is closed, and Low means the door is opened.
- **Mode:** there are two modes Monostable and Bistable. If Monostable is selected, the relay status will be automatically reset within the relay delay time after the relay is triggered. If Bistable is selected, the relay status will be reset after the relay is triggered again.
- **Trigger Delay (Sec):** set the relay trigger delay timing (ranging from 1-10 Sec.) For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press **unlock** tab.
- **Hold Delay (Sec):** set the relay hold delay timing (ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. Then the relay will resume the initial state after maintaining the triggered state for 5s.
- **DTMF Option:** select the number of DTMF digits for the door access control (ranging from 1-4 digits) For example, you can select 1-digit DTMF code or 2-digit DTMF code, etc., according to your need.
- **DTMF:** set the 1-digt DTMF code within range from ( 0-9 and \*,#) if the DTMF Option is set as 1-digit.
- **Multiple DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DMTP Option** is set as 3-digits.
- **Relay Status:** relay status is low by default which means normally closed(NC) If the relay status is high, then it is in Normally Open status(NO).
- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.



**Note**

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

## Web Relay Setting

In addition to the relay that is connected to the door phone, you can also control the door access using the network-based web relay. To do the configuration on device web **Phone > Web Relay** interface.

**Web Relay**

**Web Relay**

---

Type

User Name

IP Address

Password

**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"/>

**Parameter Set-up:**

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

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

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

## Door Access Schedule Management

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

## Manage Relay Schedule

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

**Relay Schedule**

Relay ID: RelayB

Schedule Enabled:

### Parameter Set-up:

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

## Configure Door Access Schedule

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

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

Path: **Intercom > Schedule > Schedule Setting**.

### To create a daily schedule

**Schedule Setting**

Schedule Type: Daily

Schedule Name:

Date Time: 00 : 00 - 00 : 00

+ Add Reset

### 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:    ---

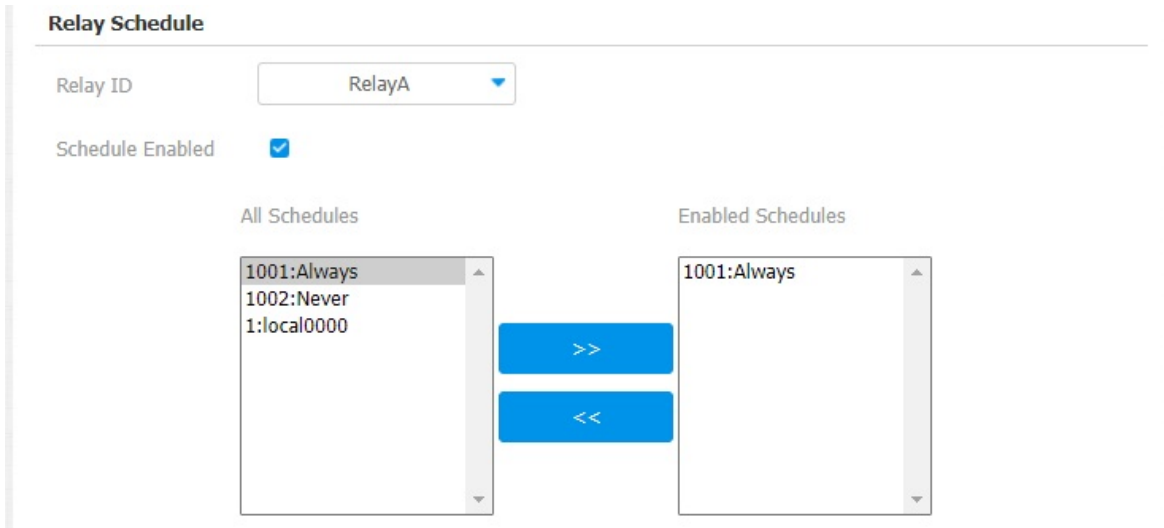
Day of Week:  Mon  Tue  Wed  Thur  
 Fri  Sat  Sun  Check All

Date Time:  :  -  :

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

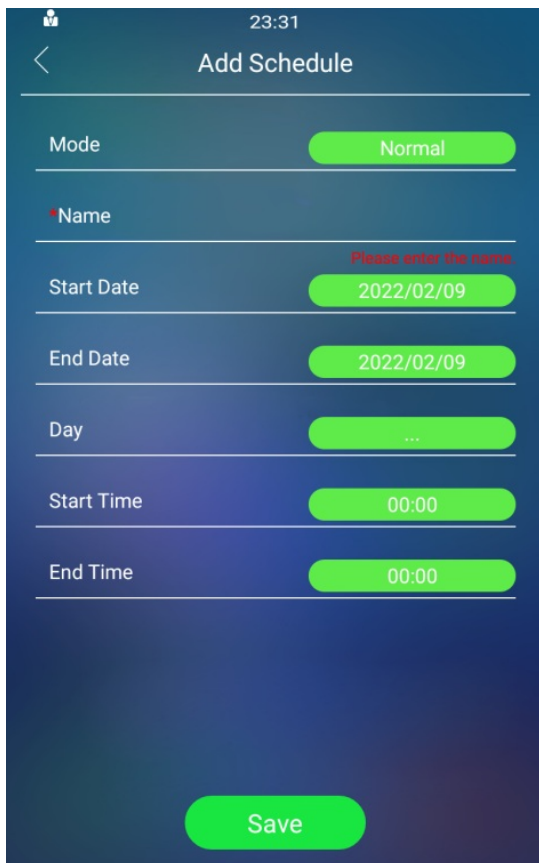
## Relay schedule

Set the corresponding relay always open at a specific time. This feature is designed for some specific scenario, for example, the time after school, or for morning work time. To do the configuration on the web **Intercom > Relay > Relay Schedule** interface.



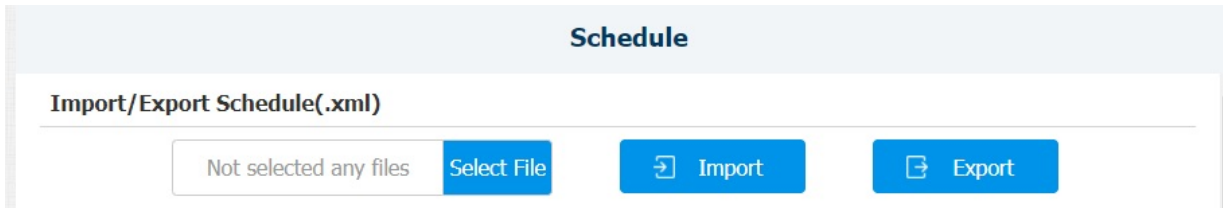
## Create Door Access Schedule on the Device

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



## Import and Export Door Access Schedule

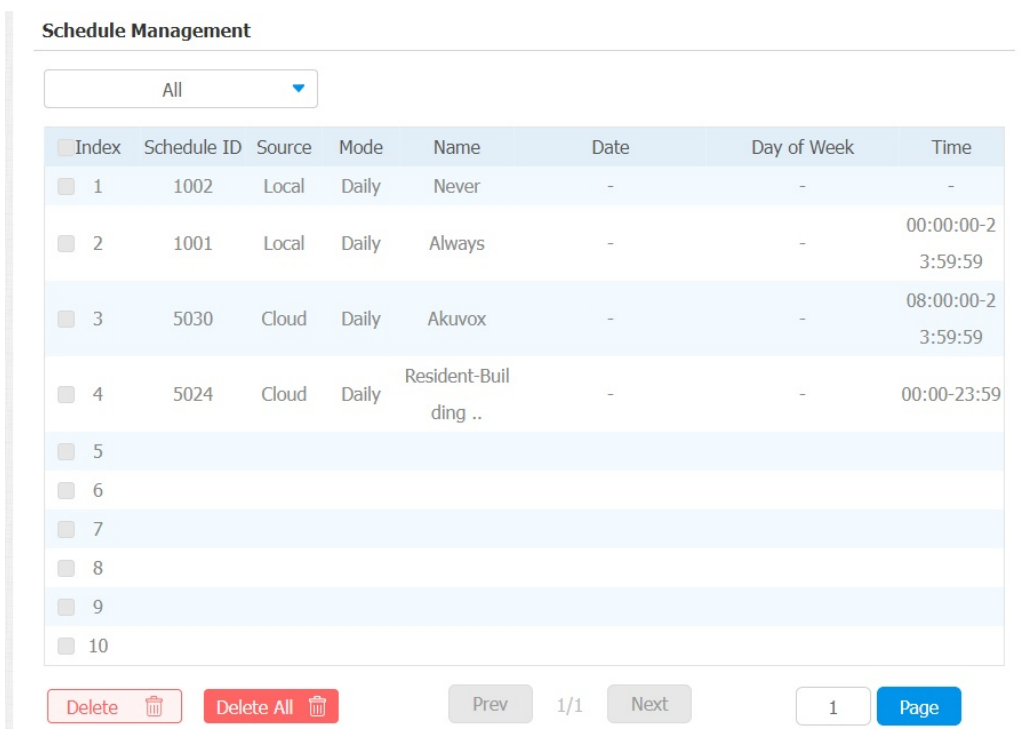
In addition to creating a door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency. Path: **Intercom > Schedule > Import/Export Schedule(.xml)**.



## Edit the Door Access Schedule

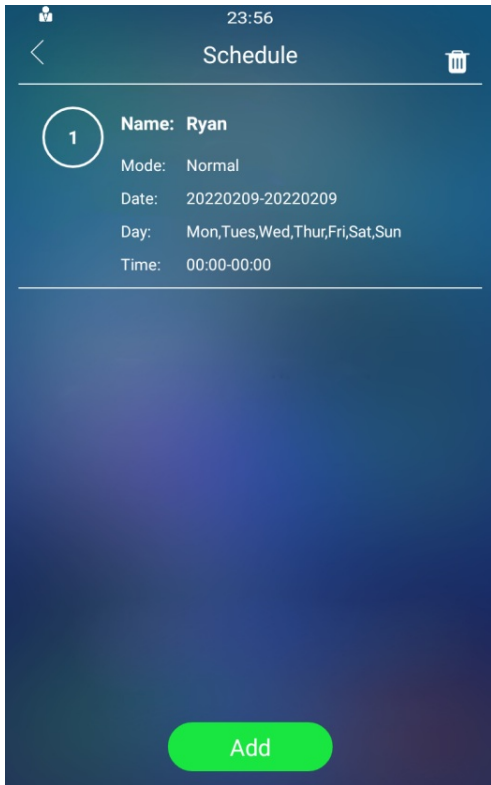
### Edit the Door Access Schedule on the Web Interface

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



### Edit the Door Access Schedule on the Device

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



## Door Unlock Configuration

R29 offers you three types of door access via PIN code, RF card, and Facial recognition. You can configure them on the device and web interface. Moreover, you can import or export the configured files to maximize your RF card configuration efficiency.

### Configure PIN Code for Door Unlock

You can create and modify both public PIN code and private PIN code for the door access on the R29 door phone.

#### Configure Public PIN code

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



#### Parameter Set-up:

- **Enabled:** tick the checkbox to enable the Public PIN code application.

- **PIN Code:** set the PIN code with digit limit ranging from **3-8**.

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

The screenshot shows the 'Password' settings screen. At the top, there is a back arrow and the title 'Password'. Below the title, there are two tabs: 'Project Passwd' and 'Public Key Passwd'. The 'Public Key Passwd' tab is selected. Under this tab, there is a toggle switch for 'Public Key Passwd' which is turned on. Below the toggle, there are three input fields: 'Old Passwd', 'New Passwd', and 'Passwd Confirm'. All three input fields contain the placeholder text 'New Passwd'. At the bottom of the screen, there is a green 'Save' button.

#### Note

- Public PIN code will not 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 configure door access by Private PIN code for the resident on the device by entering the user's name and the PIN code for door access. Path: **User > Add User**.


15:01


Add User

User ID 1

Name Please enter the name.

Private PIN  >

RF Card  >

Face  >

Floor No.

Door ...

Web Relay 0


Schedule ID ...

Save

15:03

Add Private PIN

Code

- + . 1 2 3 

\* / , 4 5 6 Done

( ) = 7 8 9

\* 0 #

### Note

- User's name must be entered first before you can create the PIN code.

### Private PIN Code on the Web Interface

On the web interface, you can not only set up PIN code but also set and select the door access schedule that you created for the validity of the PIN Code access during a certain time span you scheduled. Path: **Intercom > User**.



**User**

User ID / Name  All

<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	Ryan					0	1001-123	
<input type="checkbox"/> 2	Local	12213	Jim				0	0	1001-1	
<input checked="" type="checkbox"/> 3	Cloud	5926100035	Ryan Chen	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"/>										

Selected:0/3   Total:3  1/1  Go To Page

**User**

**User Basic**

User ID

Name

**Private PIN**

Code

**Parameter Set-up:**

- **User ID:** enter user’s ID.
- **Name:** enter the user name ( resident’s name).
- **Code:** enter the user’s private PIN.

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

### Access Setting

---

Relay

Web Relay

Building

Floor No.

Room No.

RelayA  
  RelayB  
  RelayC

49

None

All Schedules

1001:Always  
 1002:Never  
 1:Ryan

>>

<<

Schedules Selected

1001:Always

#### Parameter Set-up:

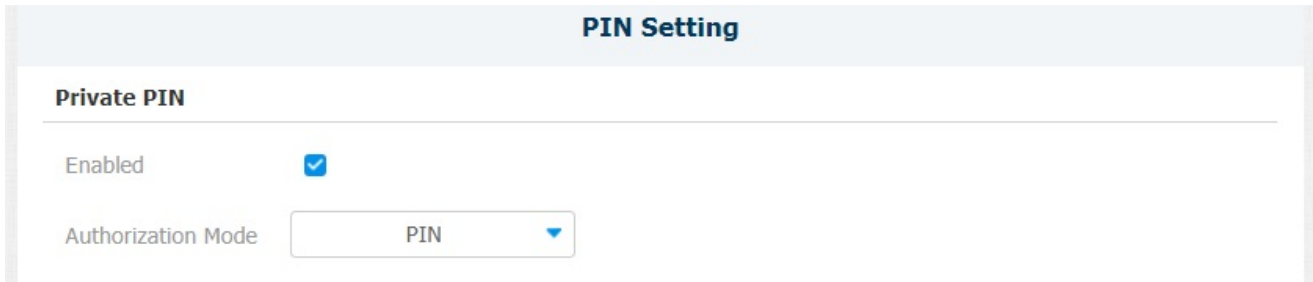
- **Relay:** select the relay(s) that you want to apply the private PIN code for the door unlock.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Building:** select the building that you want to apply the private PIN code for the door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

**Note**

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

### Configure Private PIN Access Mode

R29 offers you two types of access modes for private PIN code access, namely **PIN** and **APT#+PIN**. Path: **Intercom > PIN Setting > Private PIN**.



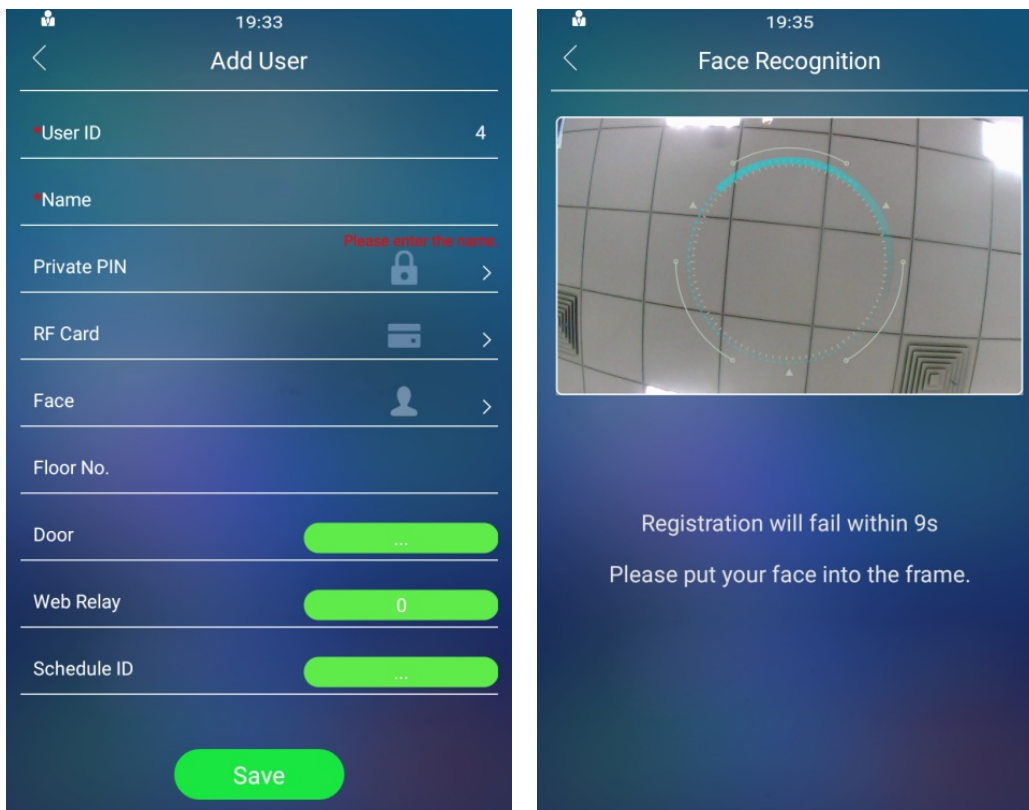
### Parameter Set-up:

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

## 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. Path: **User > User List > Add User**.



### Configure Facial Recognition on Web Interface

You can import the face data to the device on the web interface. Path: **Intercom > User > User**

### User

### User Basic

User ID	<input type="text" value="4"/>
Name	<input type="text"/>

### Private PIN

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

### RF Card

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

### Face

Status	Unregistered	
Photo	<input type="text" value="Not selected any files"/>	<input type="button" value="Select File"/>
		<input type="button" value="Reset"/>

**Parameter Set-up:**

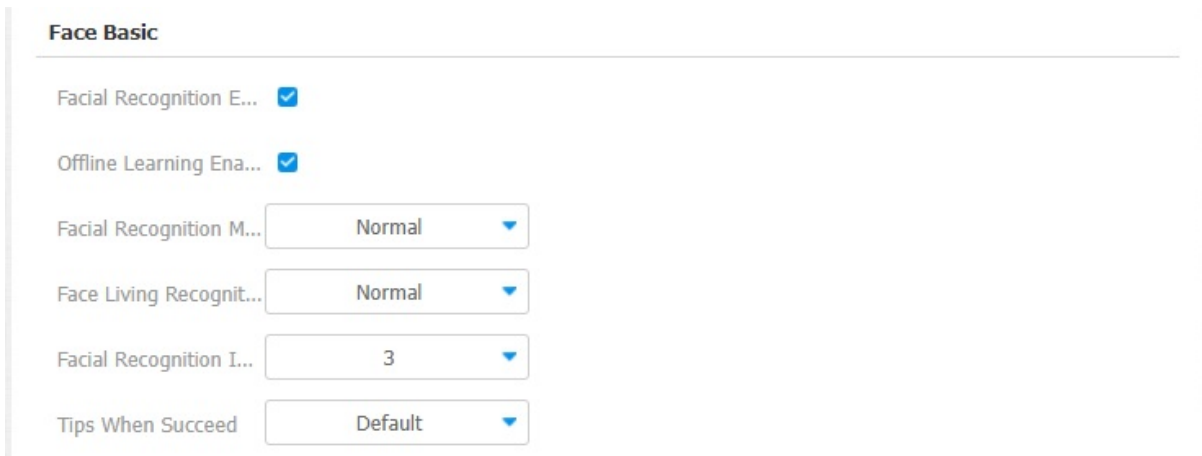
- **Status:** it will show **Registered** when the picture uploaded conforms to the format and standard otherwise it would show **Unregistered** as the default. However, the status will be changed back to **Unregistered** if the picture uploaded is cleared when you press the **Reset** tab.
- **Photo(jpg/png):** select the picture with jpg or png format to be uploaded to the device and press if you want to clear the picture uploaded.

**Note**

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

**Basic Facial Recognition Configuration on the Web Interface**

R29 series door phone allow you to adjust facial recognition accuracy, recognition intervals according to your actual need. And you can also improve the recognition quality and user experience through the basic facial recognition setting on the device web **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

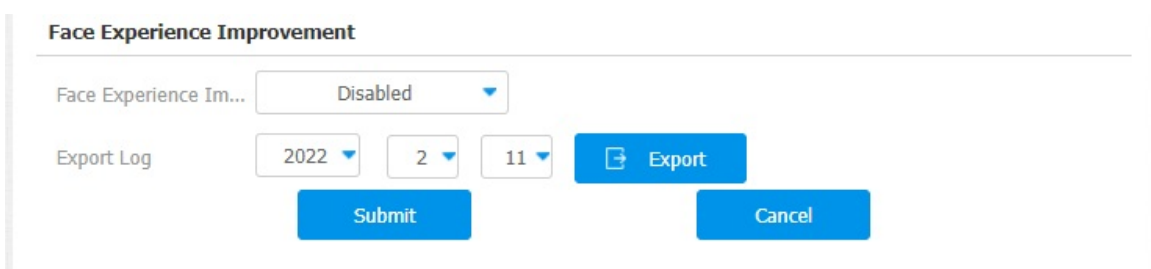
Tips When Succeed Default

**Parameter set-up:**

- **Face Recognition:** click on **Enable** to turn on the facial recognition function. Facial recognition is enabled by default.
- **Facial Recognition Matching Level:** click to select the facial recognition accuracy level among four options: **Low, Normal, High, Highest**. For example, if you select **Highest** then there will be the least possibility that someone else will be mistaken for you by mistake or in another way round in facial recognition.
- **Face Living Recognition Matching Level:** select Anti-spoofing level among four options: **Low, Normal, High, Highest**. For example, if you select **Highest** then there will be the least possibility that the device will be fooled by digital images or pictures of any kind.
- **Facial Recognition Interval:** select time interval between every two facial recognition from 1-8 minutes. For example, if you select 5 then you have to wait for 5 minutes. before you are allowed to perform facial recognition again.
- **Offline Learning:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **Tips when Succeed:** customize the tips which will be shown up when the relay is triggered by face recognition successfully.

**Facial Recognition Improvement**

If you want to improve facial recognition accuracy and user experience, you can do it by allowing your data and debug information to be uploaded to Akuvox Cloud. To do the configuration on the device web **Intercom > Face Setting > Face Experience Improvement** interface.



**Face Experience Improvement**

Face Experience Im... Disabled

Export Log 2022 2 11 **Export**

**Submit** **Cancel**

## Configuring RF Card for Door Unlock

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

### Configure RF Card on the Web Interface

You can tap an RF card on the card reader and click obtain to add RF card for the user. Path: **Intercom > User**.

The screenshot shows the 'User' management page. At the top, there is a search bar with 'Name/User ID' and a dropdown menu set to 'All'. There are buttons for 'Search', 'Reset', and 'Add'. Below this is a table with the following columns: Index, Source, User ID, Name, RF Card, Floor No., Web Relay, Schedule-Relay, and Edit. The table contains three rows, each with a checkbox in the 'Index' column and an edit icon in the 'Edit' column.

Index	Source	User ID	Name	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
<input type="checkbox"/> 1								
<input type="checkbox"/> 2								
<input type="checkbox"/> 3								

The screenshot shows the 'User Basic' configuration form. It includes fields for 'User ID' (with the value '1'), 'Name', and 'Role' (with a dropdown menu set to 'General User'). Below this is the 'RF Card' section, which has a 'Code' field, an 'Obtain' button, and a '+Add' button.

#### Parameter Set-up:

- **User ID:** enter the user ID.
- **Name:** enter the user name.
- **Role:** select the roles: general users or administrator.
- **Code:** place the card on the device card reader area and click obtain.

#### Note

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


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


16:27


## Add User

User ID 4

Name Please enter the name

Private PIN  >

RF Card  >

Face  >

Floor No.

Door ...

Web Relay 0

Schedule ID ...

Save



## Configure RF Card Code Format

If you want to integrate with the third party intercom system in terms of RF card door access, you can change the RF card code format to be identical to that applied in the third party system. **Path: Intercom > Card Setting > RFID.**

RFID	
IC Card Display Mode	8HN ▼
ID Card Display Mode	8HN ▼

### Parameter Set-up:

- **IC/ID Card Display Mode:** select the card format for the ID Card for the door access among five format options: 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR. The card code format is 8HN by default in the door phone.

## IC/ID Card Control

You can enable or disable the IC and ID card function if needed. You can navigate to **Intercom > Card Setting > Card Type Support.**



**Card Type Support**

---

IC Support Enabled

ID Support Enabled

Submit
Cancel

## NFC and Felica Card Setting

NFC and Felica card are the two types of cards that need to be enabled before you can use them as these two types of cards are not so frequently used as opposed to the conventional RF card such as IC cards and ID cards. To enable or disable the cards on the device web **Intercom > Card Setting** interface.

**Card Type Support**

---

NFC Enable Enabled ▼      Felica Enable Disabled ▼

**Note**

- As these two types of cards are in conflict with each other when being applied at the same time, therefore either one type of card should be disabled.

## Mifare/Defire Care Encryption

Mifare card and Defire card can be encrypted for greater security. To encrypt the card, you can navigate to **Intercom > Card setting > Mifare/Defire Card Encryption**.

**Mifare/Defire Card Encryption**

---

Enabled

Sector / Block 0 / 0

Block Key

### Parameter Set-up:

- Enabled:** enable the Mifare/Defire Card Encryption.
- Sector/Block:** enter the sector and block that you want the card number to be written into in the Mifare/Defire Card. For example, you can write the card number into sector 3 and block 3 in the card.
- Block Key:** enter the block password for access.

## Access Authentication

You can set up several access authentication modes. you can navigate to **Intercom > Key/Display > Access Authentication Mode of The Building Theme**.

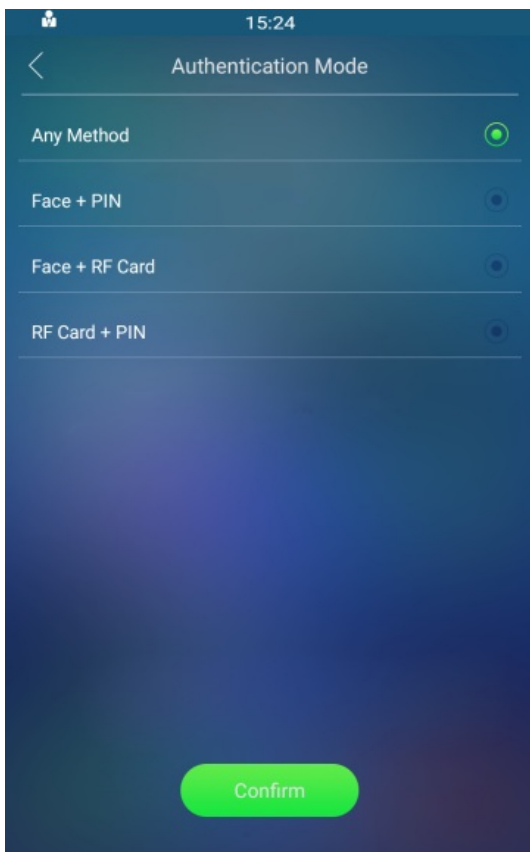
### Access Authentication Mode of The Building Theme

Authentication Mode Any method

#### Parameter Set-up:

- **Authentication Mode:** select **Any method** if you allow all the access methods to unlock the door. Select **Face + PIN** if you want to apply dual access methods (Face + PIN) for the door unlock. Select **Face + RF Card** if you want to apply dual access methods (Face+ RF Card) for the door unlock.

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



## Unlock by QR Code

QR code is another option for door access. If you want to apply for QR code access, you need to enable the QR code function on the device web **Intercom > Relay > Open Relay via QR Code** interface.

### Open Relay Via QR Code

Enabled

#### Note

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

## Unlock by Bluetooth

You can also gain door access by mobile phone with Bluetooth which is used together with Akuvox SmartPlus. You can shake the mobile phone closer to the door phone for door access. To configure Bluetooth on the device web **Intercom > BLE > BLE Basic** interface.

**BLE Basic**

---

BLE Enable  BLE Mode

Rssi Threshold  (-85~-50db)

Delay  (Sec)

**BLE Basic**

---

Enabled

Rssi Threshold  (-85~-50db)

Open Door Interval ...

### Parameter Set-up:

- **Enabled:** enable or disable the Bluetooth function. Bluetooth is turned off by default. On R29Z/R29ZL it is enabled by default.
- **Rssi Threshold:** select the signal receiving strength from -85~-50db in absolute terms, The higher value it is, the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval (Sec):** select the time interval between every two Bluetooth door accesses.

## Unlock by HTTP Command on Web Browser

You can unlock the door remotely without approaching the device physically for the door access by typing in the created HTTP command (URL) on the web browser **Intercom > Relay > Open Relay via HTTP** to trigger the relay when you are not available by the door for the door access.

**Open Relay Via HTTP**

---

Enabled

Session Check

UserName

Password

### Parameter Set-up:

- **Enable:** enable the HTTP command TO unlock function by clicking on **Enable** field.
- **Session Check:** enable it to protect data transmission security.
- **UserName:** enter the user name of the device web interface, for example, **Admin**.
- **Password:** enter the password for the HTTP command. For example, **12345**.

Please refer to the following example:

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

#### Note

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

## Unlock by Exit Button on the Door

When you need to open the door from inside using the Exit button installed by the door, you can configure the door phone Input A/B/C to trigger the three relay switches maximum for the door access on the device web **Intercom > Input > Input A/B/C** interface.

**Input A**

Enabled

Trigger Electrical Level

Action To Execute  FTP  Email  SIP Call  HTTP  TFTP

HTTP URL

Action Delay  (0~300 Sec)

Trigger When Signal...

Execute Relay

Door Status DoorA: High

### Parameter Set-up:

- **Enabled:** enable the function if needed.
- **Trigger Electrical Level:** select the trigger electrical level options between **High** and “**Low**” according to the actual operation on the exit button.
- **Action To Execute:** select the method to carry out the action among four options: FTP, Email, HTTP, TFTP.
- **Http URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after your press the button.
- **Trigger When Signal Is Hold:** if enabled, action will be triggered if the door is not closed before timeout.
- **Execute Relay:** set up relays to be triggered by the actions.

- **Door Status:** display the status of the input signal.

#### Note

- R29Z/R29ZL has only 2 Input interfaces.

## Unlock by Reception Icon

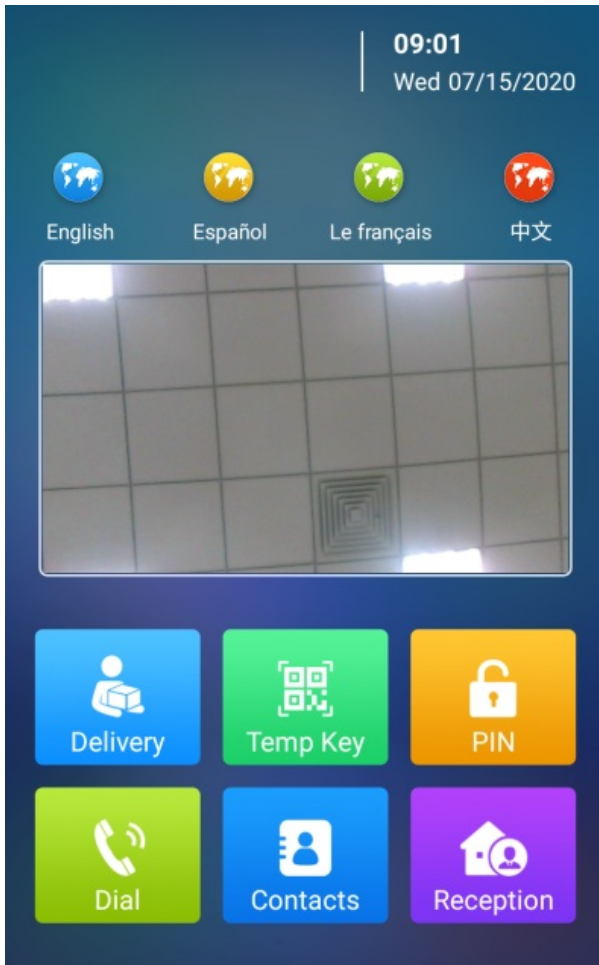
R29 series door phone provide residents and visitors quick door access by pressing the **Reception** on the home screen of the door phone. To do the configuration on device web **Intercom > Key/Display > Reception Action In Building** interface.

**Reception Action In Building**

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

### Parameter Set-up:

- **Dial Account:** select the SIP account for the application. If you select **default** then account one will be selected automatically.
- **Execute Relay:** select the relay(s) to be triggered by pressing the **Reception Icon**.
- **Action To Execute:** check the HTTP option. When this feature is triggered, the door phone will send the HTTP command to the third-party system.
- **HTTP URL:** enter the URL command to be sent for door access. For example: <http://192.168.35.127/cgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1>



## Unlock by DTMF code

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

DTMF	
Type	<input type="text" value="Info+Inband"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
Payload	<input type="text" value="101"/> (96~127)

### Parameter Set-up:

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

**Note**

- Please refer to the chapter Relay Switch Setting for the specific DTMF code setting.
- Intercom devices involved must be consistent in the DTMF type otherwise DTMF code cannot be applied.

## DTMF White List

In order 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.

**Parameter Set-up:**

- **Assigned The Authority For:** select **All** to allow all numbers for the DTMF door unlock; select **None** to deny all numbers for the DTMF door unlock; select “Only Contact List” to only allow the contact number in your door phone.

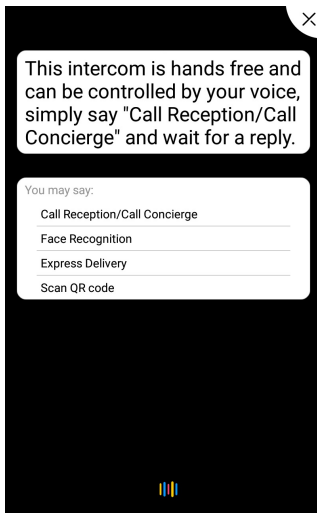
## Unlock by Voice Assistant

Voice assistant in the R29 series allow you to get door access without pressing the buttons on the device for convenience or for hygiene concern etc. Once the specific voice command is used, the voice assistant can help transfer the command into the specific action for door access. To do the configuration on the device web **Intercom > Basic > Voice Assistant Setting** interface.

**Parameter Set-up:**

- **Voice Assistant:** enable the voice assistant function if you want to apply the function.
- **Enable Time:** select between the two options **Always** and **Schedule**. If you select **Always** the voice assistant will be always enabled and if you select **Schedule** the voice assistant will be valid according to the schedule you set up.
- **Day of Week:** select the day(s) on which the voice assistant is valid, or you can select **Check All** when you want the function to be valid throughout the week.
- **Time:** select the **start time** and **end time** for the validity of the voice assistant.

The voice assistant function on the device is shown below:



<b>Call Reception/ Call Concierge</b>	This voice command is used to call to Reception or concierge for the door access as the voice assistant will automatically initiate the call using the configured number.
<b>Face recognition</b>	This voice command helps to skip to face recognition on the home screen for the door access.
<b>Express Delivery</b>	This voice command helps you to skip to the dial screen where you are required to scan the QR code in front the camera or the enter the temporary PIN for the door access.
<b>Scan QR code</b>	When this voice command is used, the screen will skip to the dial screen where you are required to hold the QR code up to the camera for the door access.

## Body Temperature Measurement for Door Access

R29 series provides you with an optional body temperature measurement function designed to be applied in the situation where the measurement becomes necessary for the safety of the residents and visitors etc. Residents and visitors are required to go through temperature measurement along with optional mask detection check before they are allowed 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)

(If the detected temperature is lower than 93.2 °F, the device will prompt low temperature, please try again later)

Action To Execute  SIP/IP Call

SIP/IP Call Number

Open Relay  DoorA  DoorB  DoorC

Day  Mon  Tue  Wed  Thur  
 Fri  Sat  Sun  Check All

Time  :  -  :

### Measuring Body Temperature

---

Mode Disabled ▾

Mask Detection Disabled ▾

Temperature Unit Fahrenheit ▾

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 To Execute ▾

Action For Low Body... Try again later ▾

Action To Execute  SIP/IP Call  HTTP

Low Temperature Ac...  SIP/IP Call  HTTP

Action For Normal B... Go To Homepage ▾

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

### Parameter Set-up:

- **Mode:** select either **Forehead** mode or **Wrist** mode for temperature measurement according to your need.
- **Mask Detection:** select **Enable** or **Disable** to turn on or turn off the mask detection. When enabled, the device will check if the visitor is wearing a mask or not while reminding the visitor with the announcement “**please wear a mask**” while visitors wearing a mask will be prompted either “**Keep face in the frame**” or “**Keep wrist close to the sensor**” depending on the mode that is selected. Warning alarm will be triggered when the body temperature measured is detected higher than the defined normal body temperature.
- **Temperature Unit:** select **Centigrade** or **Fahrenheit** you like.
- **Normal Body Temperature:** set the body temperature to the predefined body temperature as the measuring basis in either Fahrenheit or Celsius. For example, if you set the temperature at 37.3 degrees Celsius as the normal temperature, then anybody temperature measured higher than 37.3 degrees Celsius will be deemed as an abnormal temperature, while the temperature lower than 34 degrees Celsius will be deemed as low body temperature.
- **Low Temperature:** set the low temperature.
- **Action for Abnormal Body Temperature:** if **Action to Execute** is selected, then you can be notified via

SIP/IP call when abnormal temperature and low temperature is detected or an HTTP command will be sent to a designated place when the abnormal temperature is selected. If **Go to Home Page** is selected, the door phone will go back to the home screen when an abnormal temperature is detected.

- **Action for Low Body Temperature:** if **Try again later** is selected, you will be prompted “Try again later” if low body temperature is detected. If **Go To Homepage** is selected the door phone will go back to the home screen if a low body temperature is detected.
- **Timeout:** select the timeout from 1 to 8 seconds. For example, if you select **3** seconds, then the door phone will go back from the face recognition screen to the body temperature screen if timeout is reached on the face recognition due to no operation or no face is detected for 3 seconds.
- **Execute Relay:** select the relay switches to be triggered.
- **Day:** select the day on which the relay(s) is valid for the application. Or you can select **Check All** option to make the application valid throughout the week.
- **Time:** select the start time and end time for the validity of the application during a day.
- **Voice Prompts:** select the voice prompt you need.
- **Recognition Tips:** customize the tips which will be shown up when the unit detects a face.
- **OpenDoor Succeeded Tips:** customize the tips which will be shown up when the relay is triggered by face recognition successfully.
- **OpenDoor Failed Tips:** customize the tips which will be shown up when the relay is triggered by face recognition failed.

### Ambient Temperature Configuration

In order to offset the minor variations on the temperature as affected by the ambient temperature in the different places where the device is installed or at different times of the day, you are required to configure the temperature setting on the basis of time segments during a day on the device web **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)

Submit
Cancel

#### Parameter Set-up:

- **Start Time/End Time:** select the start time and end time temperature by referring to the actual temperature

measured at the time segments ranging from 10- 40°Cdegree Celsius. For example, when you divide the time into four time segments, then each of the time segments will be six hours (24 hours a day), while the end time of one segment should be the start time of the next time segment. You can divide the time segments according to your need.

- **Ambient Temperature:** enter the ambient temperature degree. Accuracy can be ensured for the actual temperature value within the range from 10- 40 degrees Celsius.

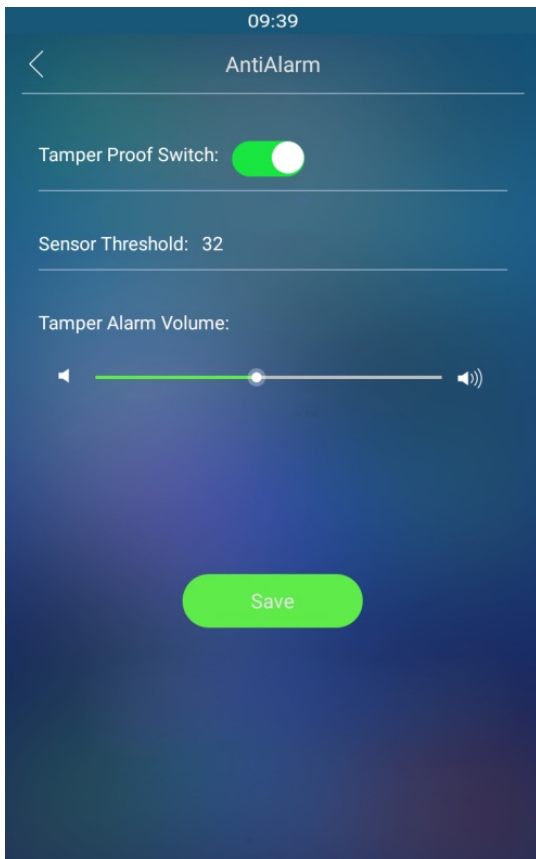
## Security

### Tamper Alarm Setting

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

### Tamper Alarm Configuration on the Device

Tamper alarm can be conveniently set up and adjusted directly on the door phone **AntiAlarm** screen. You can set up the gravity value as well as adjust the gravity sensor sensitivity according to your actual need.



### Tamper Alarm Configuration on the Web Interface

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

**Tamper Alarm**

Enabled

Gravity Sensor Thre...  (0~127)

Trigger Options

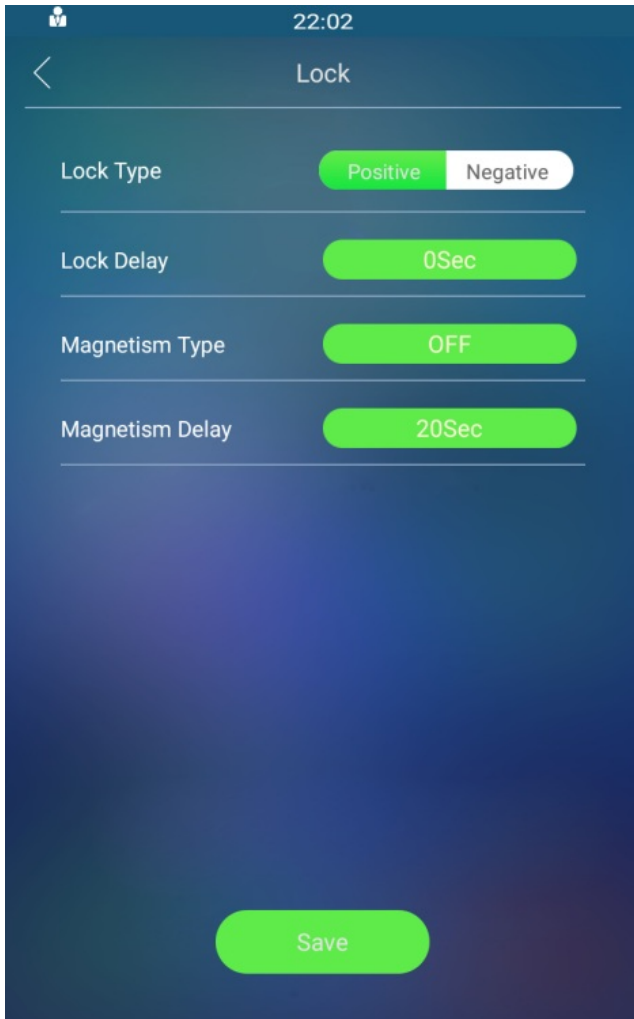
**Submit** **Cancel**

#### Parameter Set-up:

- **Tamper Alarm**: enable the anti-theft alarm function.
- **Gravity Sensor Threshold**: set the threshold for gravity sensory sensitivity. The lower the value is, the higher the value 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

R29 can be connected with third-party door locks and door sensors to ensure lock security. When the door sensor detects the door is not closed or is left ajar, it will immediately trigger the alarm for notification. On the device, go to **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 can ensure communication integrity and privacy when deploying Akuvox door phones. So, when a user needs to establish SSL protocol, it is necessary to upload corresponding certificates for verification.

**Web Server Certificate:** it is the certificate that sends to clients for authentication when clients require an SSL connection with Akuvox door phone. Currently, the format of the certificate that can be accepted by Akuvox door phone is \*.PEM file.

**Client Certificate:** when Akuvox door phone required an SSL connection with a server, the phone must verify the server to make sure it can be trusted. and the server will send its certificate to the Akuvox door phone. Then the door phone will verify this certificate according to the client certificate list.

## Web Server Certificate

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

Advanced

---

**Web Server Certificate**

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	<span style="border: 1px solid #d9534f; padding: 2px 5px; color: #d9534f;">Delete </span>

Web Server Certifica...

Not selected any files

Select File
Submit
Cancel

## Client Certificate

To upload and configure client certificates on the same page.

**Client Certificate**

	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)

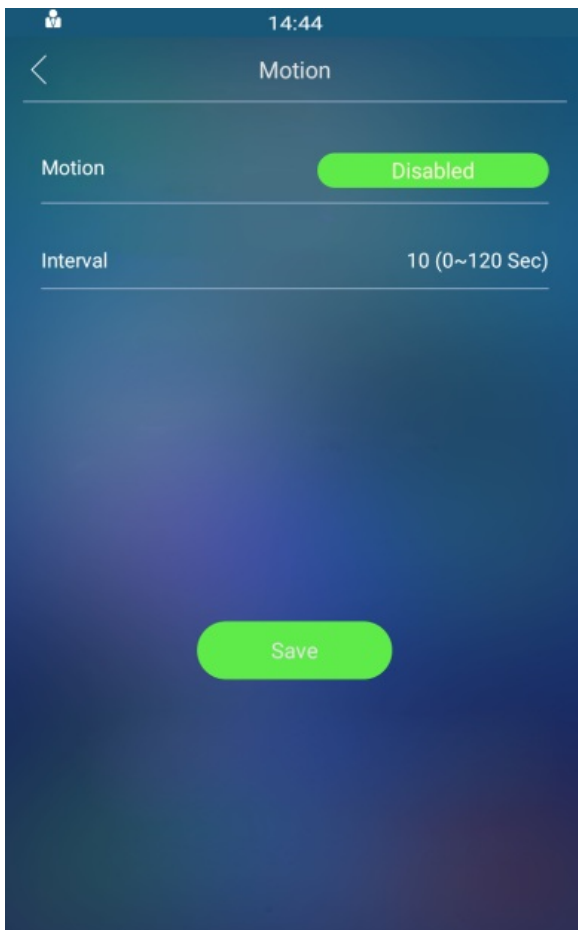
- **Only Accept Trusted certificates:** if you select **Enabled**, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If you select **Disabled**, the phone will not verify the server certificate no matter whether the certificate is valid or not.

## Motion Detection

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

### 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, delays the number of 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. 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, the interval is 10s, after the image movement is detected in front of the IR detector, the image movement is detected again within 7s-10s, that is, motion is triggered.



## Motion Detection Setting on the Web Interface

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

### 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 smaller value the greater sensitivity. The default detection accuracy value is 20.
- **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

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

The screenshot shows a web interface titled "Email Notification". It contains a form with the following fields:

- Sender's Email Addr... (text input)
- Email SendName (text input)
- Receiver's Email Addr... (text input)
- Email RecvName (text input)
- SMTP Server Address (text input)
- SMTP User Name (text input)
- SMTP Password (password input, masked with dots)
- Email Subject (text input)
- Email Content (text input)

**Parameter Set-up:**

- **Sender's Email Address:** enter the sender's email address from which the email notification will be sent out.
- **Email Send Name:** enter the name of the email sender.
- **Receiver's Email Address:** enter the receiver's email address.
- **Email RecvName:** enter the name of the email receiver.
- **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.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the contents of emails according to your need.

**FTP Notification Setting**

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

The screenshot shows a web interface titled "FTP Notification". It contains a form with the following fields:

- FTP Server (text input)
- FTP User Name (text input)
- FTP Password (password input, masked with dots)

**Parameter Set-up:**

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

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

## TFTP Notification Setting

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

TFTP Notification

TFTP Server

### 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

GDPR (**General Data Protection Regulation**) is used to encrypt the card data entered, if you want to better protect the card data you can set the GDPR function properly on the web **Intercom > Advanced > Encrypted display of the card** interface.

Encrypted display of the card

Enabled

### 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 > Package Room**.

**Delivery Setting Of Building Theme**

---

Package Room     

**Note**

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

## Action URL

R29 allows you to set up specific HTTP URL command that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occurs any changes in the relay status, input status, PIN code, and RF card access for security purpose. Path: **Phone > Actions Monitor and Image**

**Action URL**

---

Active	<input type="checkbox"/>
Make Call	<input type="text"/>
Hang Up	<input type="text"/>
RelayA Triggered	<input type="text"/>
RelayB Triggered	<input type="text"/>
RelayC Triggered	<input type="text"/>
RelayA Closed	<input type="text"/>
RelayB Closed	<input type="text"/>
RelayC Closed	<input type="text"/>
InputA Triggered	<input type="text"/>
InputB Triggered	<input type="text"/>
InputC Triggered	<input type="text"/>
InputA Closed	<input type="text"/>
InputB Closed	<input type="text"/>
InputC Closed	<input type="text"/>
Valid Code Entered	<input type="text"/>
Invalid Code Entered	<input type="text"/>
Valid Card Entered	<input type="text"/>

## High Security Mode

High security mode is designed to enhance the security, for example, it optimizes the password storage method.

Please note that once the mode is enabled, it is not allowed to downgrade the device from the version with the mode to an old one without it.

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

The screenshot displays the web configuration interface for a device. On the left, a sidebar menu includes 'Account', 'Network', 'Phone', 'Contacts', 'Upgrade', and 'Security'. The 'Security' menu is expanded, showing 'Basic' (highlighted with a red box) and 'Advanced'. The main content area is titled 'Security' and contains several sections: 'Account Status' (admin: Enabled, user: Disabled), 'Disarm Setting' (Enabled: unchecked, PIN Code: [input field]), 'Tamper Alarm' (Enabled: unchecked, Gravity Sensor Thre...: 32, Trigger Options: Only Alarm), and 'Emergency Action' (Apply Setting For: Input A, Input B, Input C). A red box highlights the 'High Security Mode' section, which is currently 'Enabled' with a checked checkbox. At the bottom, there are 'Submit' and 'Cancel' buttons.

### Important Notes

1. This mode is disabled by default when the device is upgraded to a new version with high security from an older version without the mode. However, if the device is reset to its factory settings, the mode is enabled by default.

2. Enabling this mode will make the old version tools unusable. To continue using them, you must upgrade them to the following versions.

- 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 varies depending on whether high secure mode is enabled or disabled.

- When the mode is turned on, the device only supports new HTTP formats for door opening.
  - `http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1`
  - `http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1`
- When the mode is off, the device supports the above two new formats as well as the old one:

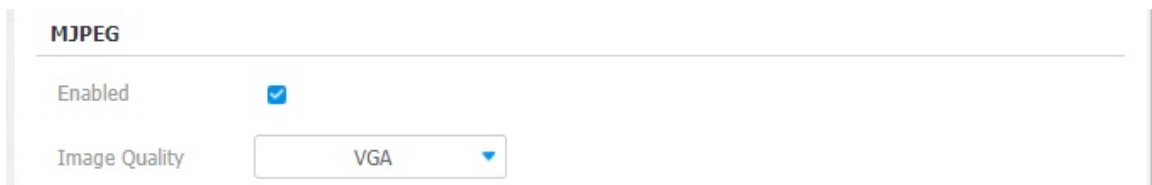
- <http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1>

4. It is not allowed to import/export tgz. format configuration files between a new version device and an old version device without high security mode.

## Monitor and Image

### Mjpeg Image Capturing

R29 series allows you to capture the Mjpeg format monitoring image if needed. You can enable the Mjpeg function and set the image quality on the web **Intercom > RTSP > Mjpeg** interface.



#### Parameter Set-up:

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

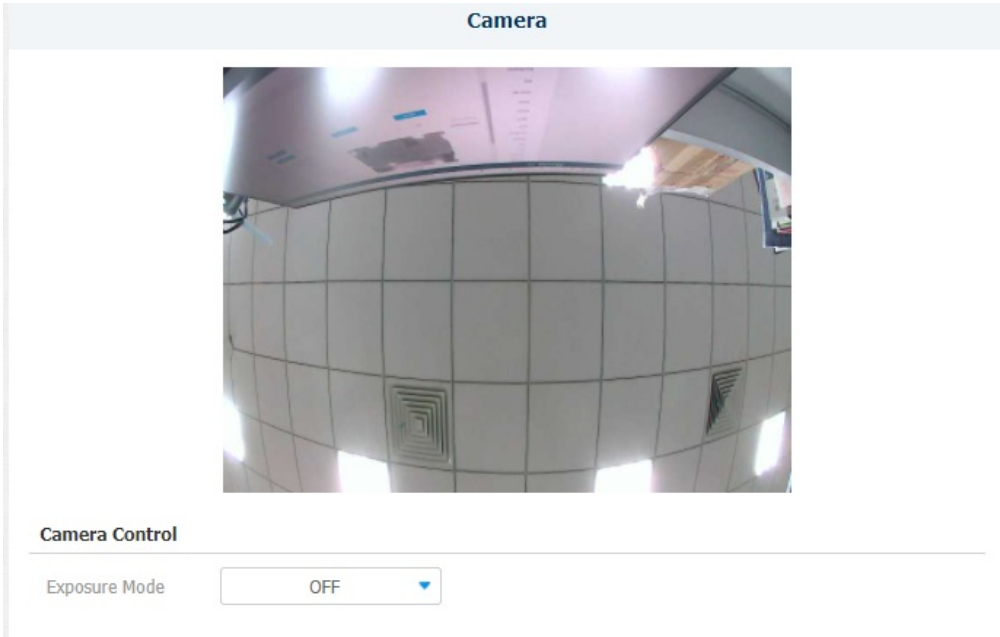
After the Mjpeg service is enabled, you can capture the image from the door phone using the following three types of URL format:

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

If you want to check the real-time video from the R29 series door phone, you can go to the device web **Intercom > Live Stream** interface to obtain the real-time video or you can also enter the correct URL on the web browser to obtain it directly.



Enter the correct URL ([http://IP\\_address:8080/video.cgi](http://IP_address:8080/video.cgi)) on the web browser if you want to obtain the real-time video directly by going to the web interface.

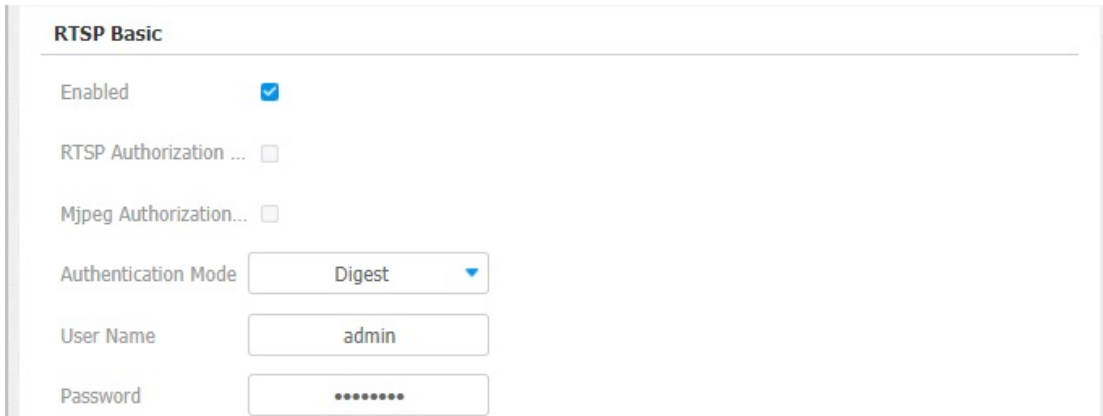


## RTSP Stream Monitoring

R29 series support the RTSP stream that allows intercom devices such as an indoor monitor or the monitoring unit from a third party to monitor or obtain the real time audio/ video (RTSP stream) from the door phone using the correct URL.

## 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

RTSP Authorization ...

Mjpeg Authorization...

Authentication Mode

User Name

Password

#### Parameter Set-up:

- **Enabled:** enable the RTSP if needed.
- **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

You can select the video codec format for the RTSP stream for the monitoring and configure video resolution and bit-rate etc., based on your actual network environment on the web **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:

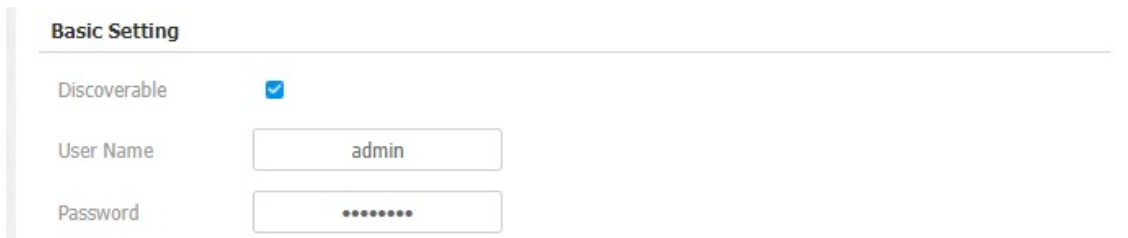
- **Video Codec:** select between two types of codec options: H.264 and Mjpeg according to your need.
- **Video Resolution:** select video resolutions among seven options: QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P. The default video resolution is 720P. and the video from the door phone might not be able 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. While 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. While 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

Real-time video from the R29 series door phone camera can be searched and obtained by the Akuvox indoor monitor or by third party devices such as NVR (Network Video Recorder) you can configure the ONVIF function in the door phone web **Intercom > ONVIF > Basic Setting** interface so that other device will be able to see the video from the door phone.



The screenshot shows a web interface titled "Basic Setting" for ONVIF configuration. It contains three fields: "Discoverable" with a checked checkbox, "User Name" with a text input field containing "admin", and "Password" with a password input field containing seven dots.

#### Parameter Set-up:

- **Onvif Mode:** select **Discoverable** or **Non- Discoverable** to turn on or turn off the ONVIF mode. If you select **Discoverable** then the video from the door phone camera can be searched by other devices. ONVIF mode is **Discoverable** by default.
- **UserName:** 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.

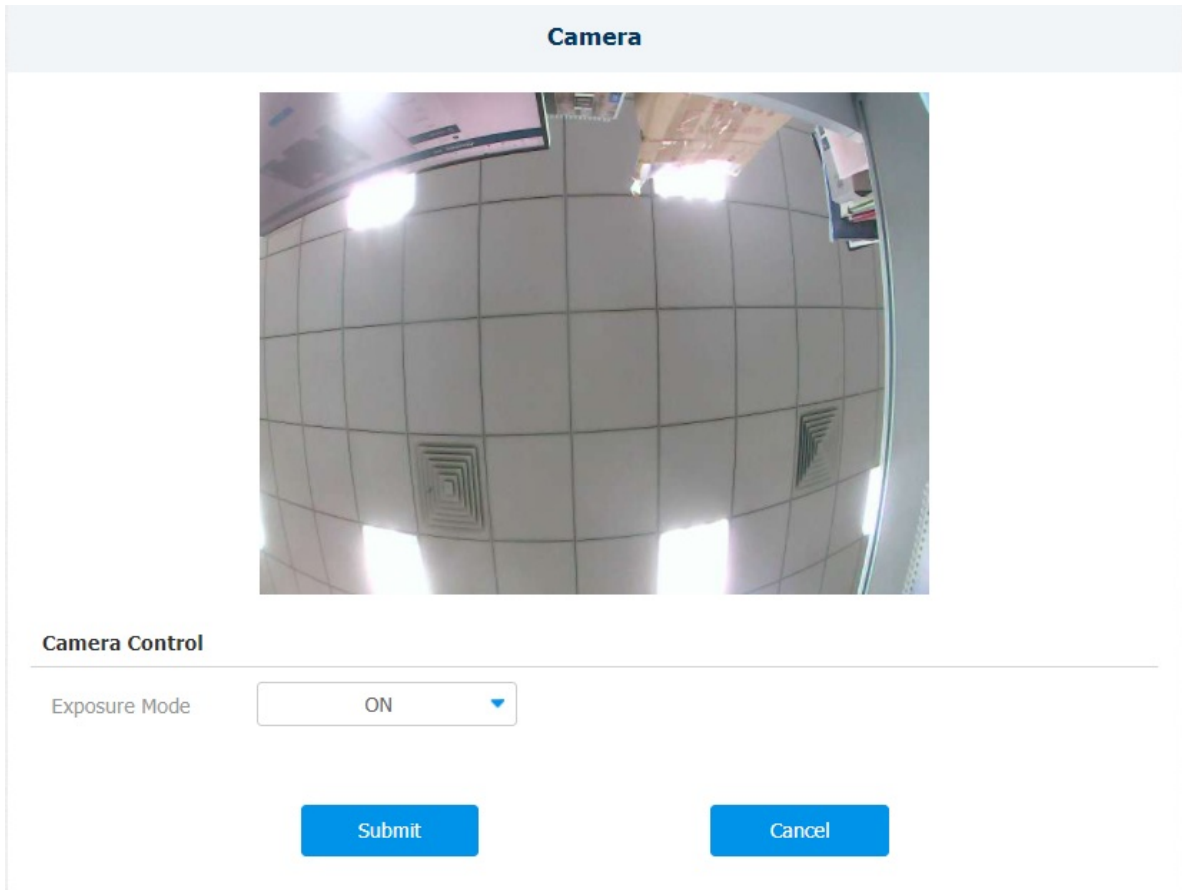
For example: [http://IP address:80/onvif/device\\_service](http://IP address:80/onvif/device_service)

#### 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.



#### Parameter Set-up:

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

## 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 **Phone > Call Log** interface and export the call log from the device if needed.

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	<a href="#">1001@192.168</a> <a href="#">.31.20:5070</a>
<input type="checkbox"/> 2	Dialed	2021-05-18	16:12:46	1003@192.168 .31.20:5070	1001	<a href="#">1001@192.168</a> <a href="#">.31.20:5070</a>
<input type="checkbox"/> 3	Dialed	2021-05-18	16:12:28	1003@192.168 .31.20:5070	1001	<a href="#">1001@192.168</a> <a href="#">.31.20:5070</a>

1/1

**Parameter Set-up:**

- **Save Call Log Enabled:** select **Enable** or **Disable** to turn on or turn off the call log function.
- **Call History:** select call history among four options: **All, Dialed, Received, Missed** for the specific type of call log to be displayed.
- **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 web **Phone > Door log** interface.

### Door Log

Save Door Log Enab... 
Export ▼

All ▼
Time
mm/dd/yyyy
-
mm/dd/yyyy
Name/Code

Search

Index	Name	Code	Type	Date	Time	Status	
<input type="checkbox"/>	1	FaceKey	Unknown	Face	2021-11-19	17:15:31	Failed
<input type="checkbox"/>	2	FaceKey	Unknown	Face	2021-11-18	19:23:14	Failed
<input type="checkbox"/>	3	FaceKey	Unknown	Face	2021-11-18	12:01:56	Failed
<input type="checkbox"/>	4	FaceKey	Unknown	Face	2021-11-15	13:51:39	Failed
<input type="checkbox"/>	5	FaceKey	Unknown	Face	2021-11-11	16:01:25	Failed
<input type="checkbox"/>	6	FaceKey	Unknown	Face	2021-11-11	15:36:42	Failed
<input type="checkbox"/>	7	FaceKey	Unknown	Face	2021-11-11	15:36:37	Failed
<input type="checkbox"/>	8	FaceKey	Unknown	Face	2021-11-11	15:36:30	Failed
<input type="checkbox"/>	9	FaceKey	Unknown	Face	2021-11-11	15:36:24	Failed
<input type="checkbox"/>	10	FaceKey	Unknown	Face	2021-11-11	15:36:18	Failed
<input type="checkbox"/>	11	FaceKey	Unknown	Face	2021-11-04	19:06:04	Failed
<input type="checkbox"/>	12		0016624075	Card	2021-11-04	15:14:17	Success
<input type="checkbox"/>	13		0016624075	Card	2021-11-04	15:02:17	Success
<input type="checkbox"/>	14	FaceKey	Unknown	Face	2021-11-04	14:18:47	Failed
<input type="checkbox"/>	15	FaceKey	Unknown	Face	2021-11-04	14:18:30	Failed

Delete 🗑
Delete All 🗑
Prev
1/5
Next
1
Page

**Parameter Set-up:**

- **Save Door Log Enable:** select **Enable** or **Disable** to turn on or turn off the door log function.
- **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 log in the door phone can be used for debugging purpose. If you want to export the system out to a local PC or to a remote server for debugging, you can set up the function on the web **Upgrade > Advanced > System Log** interface.

**System Log**

LogLevel: 7

Export Log: Export

Export Debug Log: Export

Remote System Log ...

Remote System Serv...

### Parameter Set-up:

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

## PCAP for Debugging

PCAP in R29 series door phone is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **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 fresh 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

SIP user agent (UA) is an endpoint device that supports SIP, which is used to establish connections and enable sessions between two endpoint devices. And a UA is comprised of UAC (User Agent Client) and UAS (User Agent server) with the UAC used to issue requests and UAS used to issue a response. UA acts as a SIP service provider for the specific user (device). You can customize user agent field in the SIP message. If the user agent is set to a specific value, users can see the information from PCAP. If the user agent is blank, by default, users can see the company name "Akuvox", model number and firmware version from PCAP. Path: **Account > Advanced > User Agent** interface.



The screenshot shows a web interface for configuring the User Agent. At the top, the title "User Agent" is displayed. Below the title, there is a label "User Agent" followed by a text input field containing the value "Akuvox". Below the input field, there are two buttons: "Submit" and "Cancel".

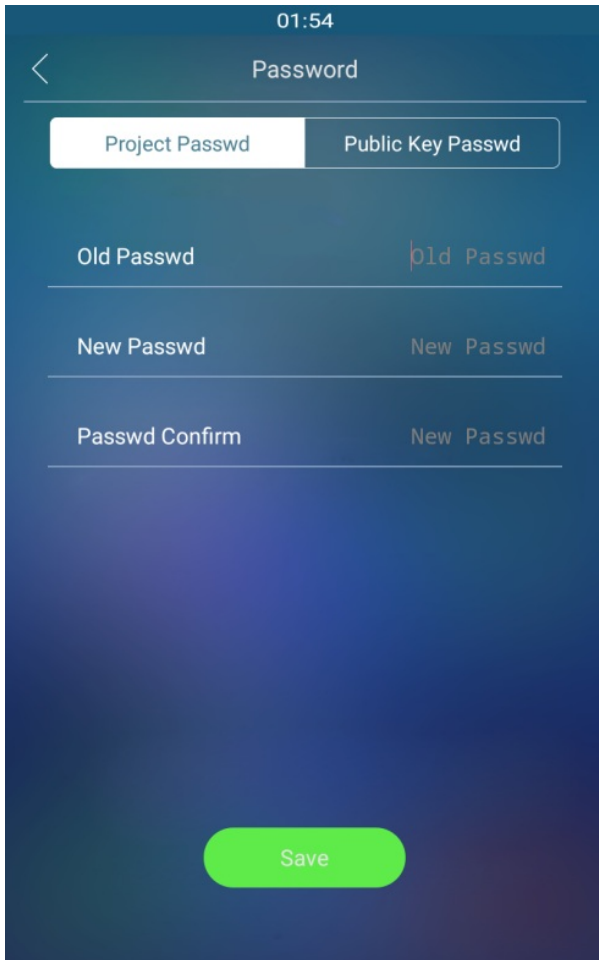
#### Parameter Set-up:

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

## Password Modification

### Modifying Device Setting Password

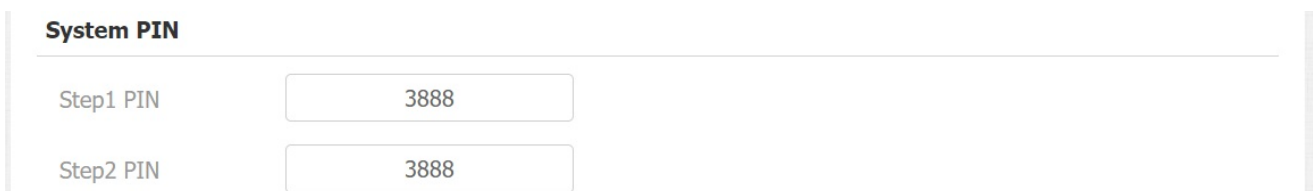
Project passwords are what need to be entered before you are allowed to enter the set password, which enables you to enter the device **Password** screen for the configuration and adjustment. You can change the project password on the device directly.



#### 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.



#### Parameter Set-up:

- **Step1PIN:** 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**.

## Modifying 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

**Change Password** X

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

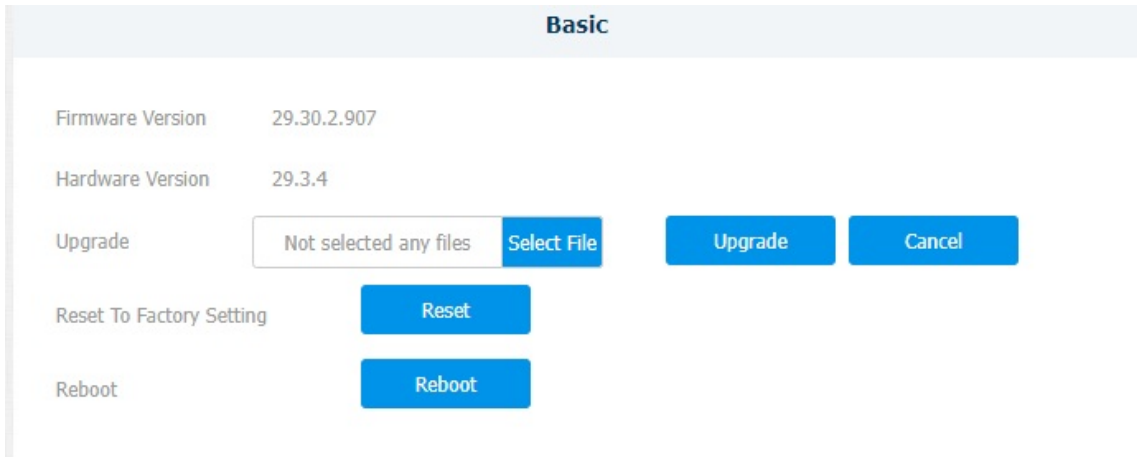
User Name	user
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>
<span style="background-color: #ccc; padding: 5px 20px; border: 1px solid #ccc; margin-right: 20px;">Ignore</span> <span style="background-color: #007bff; color: white; padding: 5px 20px; border-radius: 3px;">Change</span>	

**Parameter Set-up:**

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

## Firmware Upgrade

Firmwares of different versions for the R29 series door phone can be upgraded on the device web **Upgrade > Basic** interface.

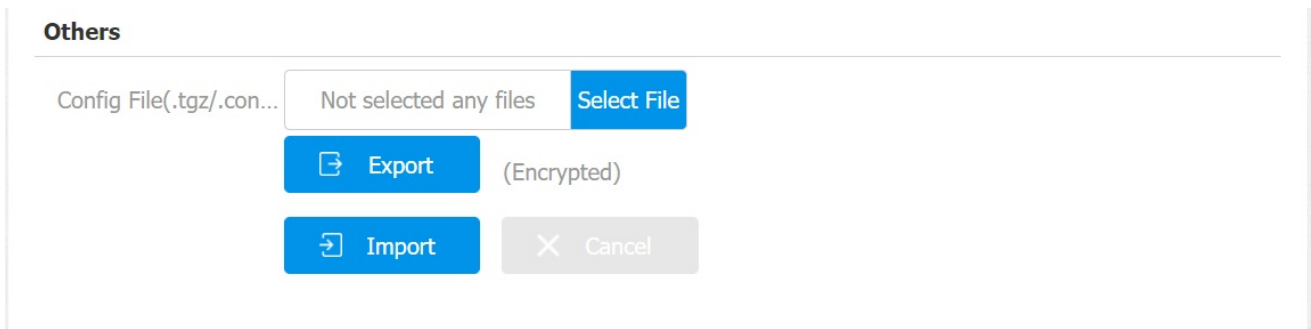


**Note**

- Firmware files should be .zip format for upgrade

## Backup

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



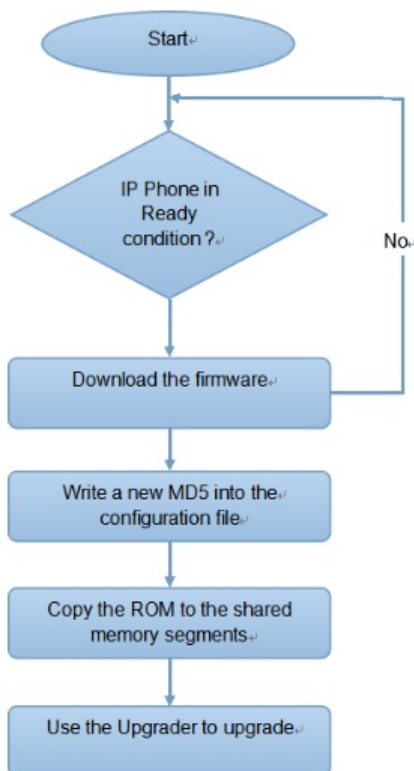
## Auto-provisioning via Configuration File

Configurations and upgrading on R29 series door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the door phone.

## Provisioning Principle

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

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 general provisioning and another one is 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. For example : r000000000083.cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files are used for auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

### Note

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

## AutoP Schedule

Akuvox provides you with different Autop methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule. To 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](#)

**Automatic Autop**

---

Mode Power On ▼

Schedule Sunday ▼

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

Clear MD5 [Clear](#)

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 code range from 128-255), you are required to configure DHCP Custom Option on the web **Upgrade > Advanced > Automatic Autop** interface.

### Automatic Autop

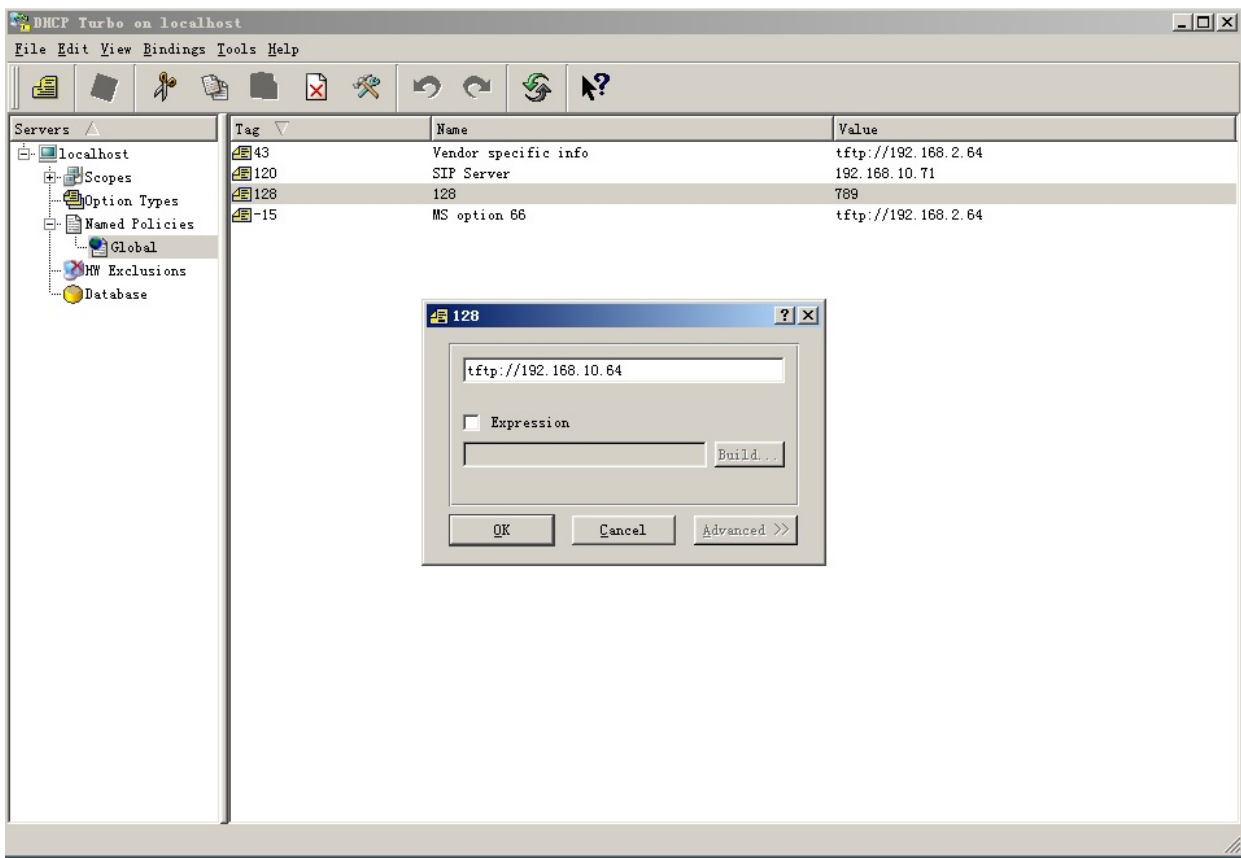
Mode

Schedule

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

Clear MD5

Export Autop Templ...



### Note

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

### 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". And taking R29 as an example, "r000000000029.cfg" (10 zeros in total), while the MAC-based configuration file for the specific device provisioning is with the format MAC\_Address of the device.cfg, for example, "0C110504AE5B.cfg".

## Static Provisioning Configuration

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

**Automatic Autop**

Mode:

Schedule:

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

Clear MD5:

Export Autop Templ...:

**Manual Autop**

URL:       User Name:

Password:       Common AES Key:

AES Key(MAC):

**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 is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.**
- **Akuvox do not provide user specified server.**
- **Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.**

**Note**

- 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)

## TR069

TR-069 (Technical Report 069) provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. For door phones, the administrators can manage all the devices on a common TR-069 Platform. IP phones can be easily and securely configured on the TR-069 platform to make mass deployment more efficient. You can **Navigate to Network > Advanced > TR069**.

TR069		
	Enabled	<input type="checkbox"/>
	Version	<input type="text" value="1.0"/>
ASC	URL	<input type="text"/>
	User Name	<input type="text"/>
	Password	<input type="password" value="*****"/>
Periodic Inform	Enabled	<input type="checkbox"/>
	Periodic Interval	<input type="text" value="1800"/> (3~24×3600s)
CPE	URL	<input type="text"/>
	User Name	<input type="text"/>
	Password	<input type="password" value="*****"/>

### Parameter Set-up:

- **Enabled:** enable the function if needed.
- **Version:** select supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE:** ACS is short for auto configuration servers as server-side, and CPE is short for customer-premise equipment as client-side devices.
- **URL:** to configure URL address for ACS or CPE.
- **User Name:** to configure username for ACS or CPE.
- **Password:** configure the password for ACS or CPE.
- **Periodic Inform:** to enable periodically inform.
- **Periodic Interval:** to configure the interval for periodic information.

#### Note

- **TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.**
- **Please refer to the link below for more information**  
<https://knowledge.akuvox.com/docs/how-to-setup-tr069?highlight=TR>

## Device Integration with Third Party Device

### Integration via Wiegand

The door phone Wiegand interface is used to connect the door phone to third party devices for data transmission via Wiegand protocol. If you want to integrate the R29 series door phone with third party devices via Wiegand, you can configure the Wiegand on the web interface. Path: Intercom > **Wiegand** > **Wiegand**.

The screenshot shows a web interface titled "Wiegand" with a horizontal line below the title. Below the line, there are seven rows of configuration options, each with a label and a dropdown menu:

- Wiegand Display Mo...: 8HN
- Wiegand Card Read...: Wiegand-26
- Wiegand Transfer M...: Output
- Wiegand Input Data...: Normal
- Wiegand Output Dat...: Normal
- Wiegand Output CRC: Enabled
- RF Card Verification: Enabled

### 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.

- **Wiegand Transfer Mode:** select Input, Output, Convert to Card No.OutputWiegand. 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.

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



#### 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 to integrate the door phone with the Milestone VMS system for monitoring purpose. You need to enable the Milestone integration first before you can integrate them. You can navigate to **Intercom > ONVIF > Advanced Setting**.



## Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third party device with the Akuvox intercom device such R29 series door phone. You can configure the HTTP API function on the web **Intercom > HTTP API** interface for the integration.

**HTTP API**

Enabled

Authorization Mode

User Name

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	WhiteList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN
4	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.

5	Digest	<p>Password encryption method, only supports MD5. MD5( Message-Digest Algorithm)</p> <p>In Authorization field of Http request header:</p> <p>WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".</p>
6	Token	This mode is used by Akuvox developer only

## Lift Control Configuration

Integration between R29 series door phone and third party devices such as intercom devices for door access and lift control should be configured in the device web-interface before the integration can be made.

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



### Parameter Set-up:

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

NO.	Integration Mode	Description
1	None	If you select <b>None</b> then the RS485 integration will be disabled.
2	OSDP	If you Select <b>OSDP</b> Mode, then the integration communication between the R29 series door phone and the third party device is via OSDP protocol. You are required to check for the device integration protocol and make sure if that they use the same integration protocol.
3	Akuvox EC32	Select <b>Akuvox EC32</b> 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 <b>KEYKING</b> if you want to integrate with KEYKING lift controller.
6	ZKT	Select <b>ZKT</b> 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.

### 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 can not 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 > KeyKing Advance Setting**.

### 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 > Akuvox EC32 & ZKT Advance Setting**.

### Akuvox EC32 & ZKT Advance Setting

---

Server IP	<input type="text"/>	
Port	<input type="text"/>	(1~65535)
Timeout	<input type="text" value="60"/>	(1~60s)

### Akuvox EC32 Action

---

User Name	<input type="text"/>
Password	<input type="text"/>
Floor NO. Parameter	<input type="text" value="\$floor"/>
URL To Trigger Spec...	<input type="text" value="/cdor.cgi?open=0&amp;door=\$floor"/>
URL To Trigger All Fl...	<input type="text" value="/cdor.cgi?open=8"/>
URL To Close All Flo...	<input type="text" value="/cdor.cgi?open=9"/>

### Parameter Set-up:

- **Server IP:** enter the IP address of the Akuvox EC32 controller server.
- **Port:** enter the port of Akuvox EC32 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 floor button will become invalid.
- **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 > Akuvox EC32 & ZKT Advance Setting**.

**Akuvox EC32 & ZKT Advance Setting**

---

Server IP

Port  (1~65535)

Timeout  (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 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**.

**Mobile Community**

---

Enabled

HTTP URL

Device ID

**Parameter Set-up:**

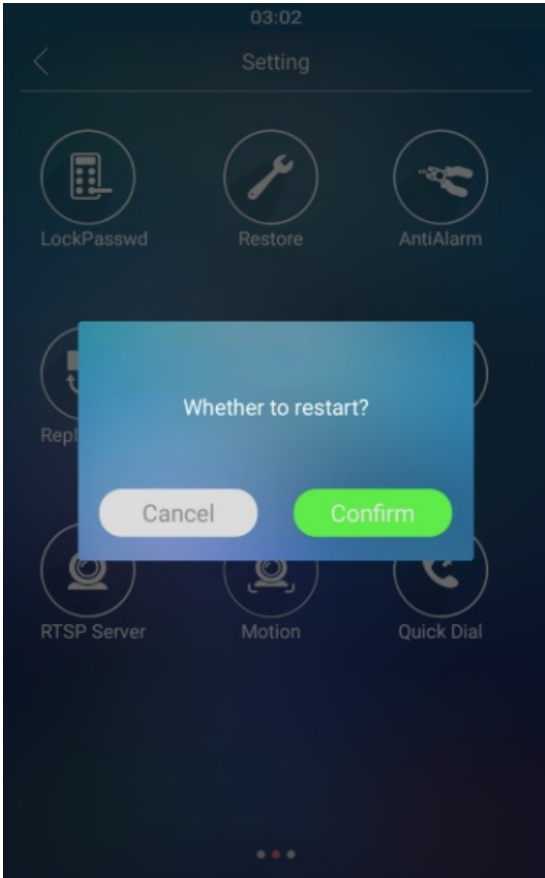
- **Enabled:** enable the function if needed.
- **HTTP URL:** enter the HTTP command. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before its being sent to the QR code server for verification. For example: <http://wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode}&deviceId={DeviceID}>
- **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

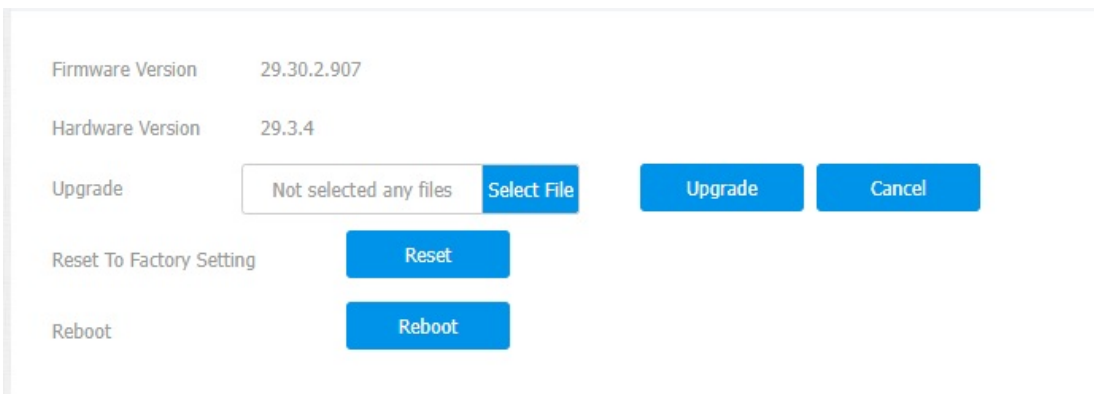
#### Reboot on the device

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



### Reboot on the web interface

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



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

**Reboot Schedule**

Mode

Schedule

(0~23 hour)

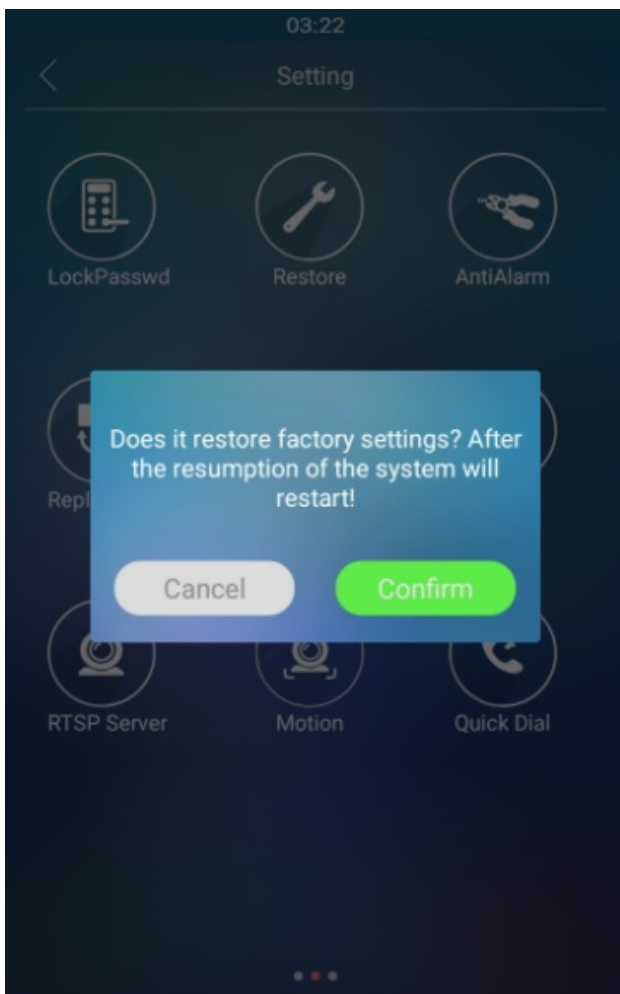
### Parameter Set-up:

- **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 also need to set up the reboot schedule. From Monday to Sunday and 00:00 to 24:00.

## Reset

### Reset on the Device

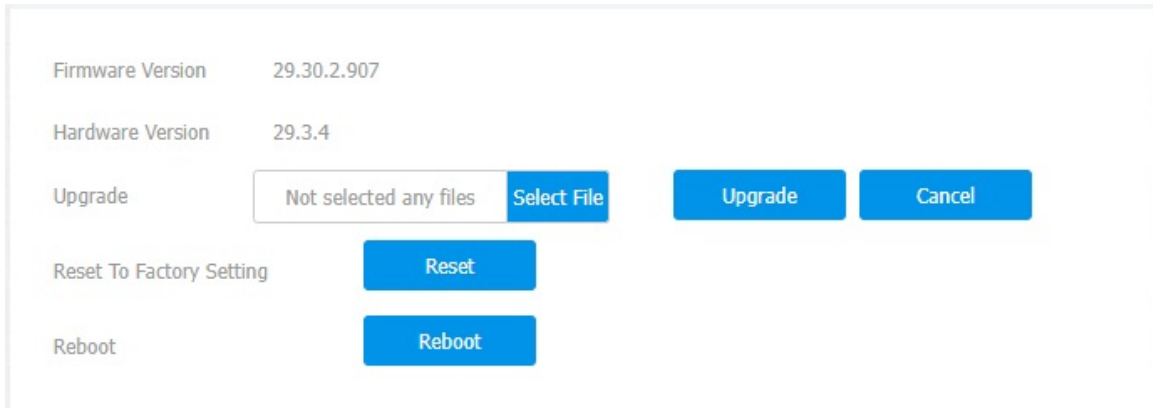
If you want to reset the device system to the factory setting, you can operate it directly on the device **Restore** screen.





## Reset on the Device Web Interface

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



## Abbreviations

**ACS:** Auto Configuration Server

**Auto:** Automatically

**AEC:** Configurable Acoustic and Line Echo Cancelers

**ACD:** Automatic Call Distribution

**Autop:** Automatical Provisioning

**AES:** Advanced Encryption Standard

**BLF:** Busy Lamp Field

**COM:** Common

**CPE:** Customer Premise Equipment

**CWMP:** CPE WAN Management Protocol

**DTMF:** Dual Tone Multi-Frequency

**DHCP:** Dynamic Host Configuration Protocol

**DNS:** Domain Name System

**DND:** Do Not Disturb

**DNS-SRV:** Service record in the Domain Name System

**FTP:** File Transfer Protocol

**GND:** Ground

**HTTP:** Hypertext Transfer Protocol

**HTTPS:** Hypertext Transfer Protocol Secure Socket Layer

**IP:** Internet Protocol

**ID:** Identification

**IR:** Infrared

**LCD:** Liquid Crystal Display

**LED:** Light Emitting Diode

**MAX:** Maximum

**POE:** Power Over Ethernet

**PCMA:** Pulse Code Modulation A-Law

**PCMU:** Pulse Code Modulation  $\mu$ -Law

**PCAP:** Packet Capture

**PNP:** Plug and Play

**RFID:** Radio Frequency Identification

**RTP:** Real-time Transport Protocol

**RTSP:** Real Time Streaming Protocol

**MPEG:** Moving Picture Experts Group

**MWI:** Message Waiting Indicator

**NO:** Normal Opened

**NC:** Normal Connected

**NTP:** Network Time Protocol

**NAT:** Network Address Translation

**NVR:** Network Video Recorder

**ONVIF:** Open Network Video Interface Forum

**SIP:** Session Initiation Protocol

**SNMP:** Simple Network Management Protocol

**STUN:** Session Traversal Utilities for NAT

**SNMP:** Simple Mail Transfer Protocol

**SDMC:** SIP Devices Management Center

**TR069:** Technical Report069

## FAQ

Q1: How to obtain the IP address of R2X?

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

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

✓ For devices with multiple numeric keyboards - R27:

While R27 power up normally, press \*2396# to enter the home screen and press 1 to go to the System Information screen to check the IP address.

✓ For devices with touch screen - X915/R29:

While it powers up normally, in the dial interface, press 9999, Dial key, 3888, and OK to enter the system setting screen. Go to the info screen to check the IP address.

✓ Common method:

Using Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: Do Akuvox devices support opus codec?

A2: For now, only Akuvox Android video IP phone R48G can support Opus audio codec.

Q3: What is the supported temperature range for the Akuvox door phone?

A3: R20/E21/R26/R23/Standard R27/Standard X915 – 14° to 112°F (-10° to 45°C)

R27/X915 with heating supporting — 40 degrees

R28 – (-40°C~55°C )

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

IP Phone – 32°~104°F(0~40°C)

Q4: Do Akuvox devices support Modbus protocol?

A4: No.

Q5: Failure in importing the X915 face data to another X915 using the exported face data.

A5: Please confirm the following steps:

The import format is zip;

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

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

A6: Onvif 18.04 profiles

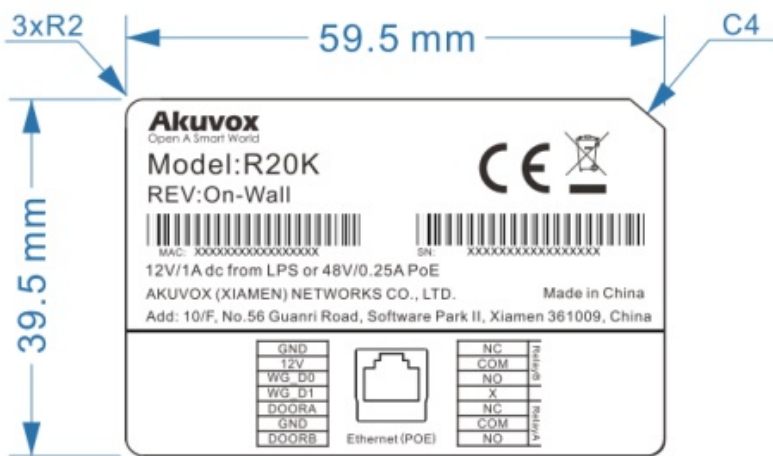
Q7: Do door phones support these card types? Prox, Legacy iClass, iClassSE, HID Mifare, HID DESFire, HID SEOS.

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

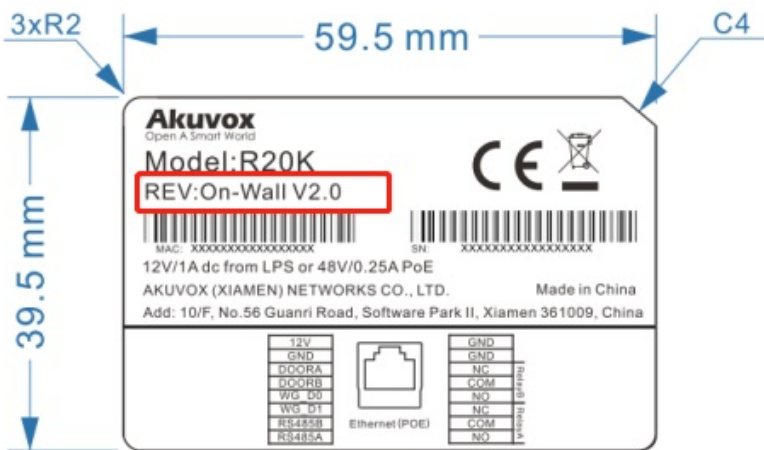
Q8: How to confirm whether my device is hardware version 1 or hardware version 2?

A8: 1.Label

• **Hardware version 1**



• **Hardware version 2**



• **Firmware Version**

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

Go to Web-Status -Firmware Version.

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

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

- **Hardware version**

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

Go to Web-Status -Firmware Version.

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

Status	
Product Information	
Model	R20K
MAC Address	0C:11:05:0B:00:6D
Firmware Version	20.30.4.8
Hardware Version	20.9.0.0.0.0.0.0

## Contact us

For more information about the product, please visit us at [www.akuvox.com](http://www.akuvox.com) or feel free to contact us by

Sales email: [sales@akuvox.com](mailto:sales@akuvox.com)

Technical support email: [support@akuvox.com](mailto:support@akuvox.com)

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

We highly appreciate your feedback about our products.

