



R29 Series Door Phone Admin Guide

About This Manual

Thank you for choosing Akuvox's R29 series door phone. This manual is intended for end users who need to properly configure the door phone. This manual is applicable to 29.30.2.13 version, and it provides all functions' configurations of R29 series door phone. Please visit Akuvox forum or consult technical support for any new information or latest firmware.

Note: Please refer to universal abbreviation form in the end of manual when meet any abbreviation letter.

Content

1. Product Overview.....	1
1.1. Instruction	1
1.2. Connector Introduction	2
2. Daily use	3
2.1. Starting	3
2.2. Make a Call	4
2.2.1. Call From Digital Keypad.....	4
2.2.2. Call From Phonebook.....	5
2.2.3. Call From Speed Dial	6
2.2.3.1. Building theme	6
2.2.3.2. Villa theme or Office theme.....	6
2.3. Receive a Call.....	6
2.4. Unlock	7
2.4.1. Unlock by PIN Codes	7
2.4.2. Unlock by Face.....	8
2.4.3. Unlock by RFID cards	8
2.4.4. Unlock by DTMF codes	9
3. Basic Features	9
3.1. Access the system setting	9
3.2. Access the website setting	10
3.2.1. Obtain IP Address.....	10
3.2.2. Access the Device Website	10
3.3. Password Modification.....	11
3.3.1. Modify the Phone System Password	11

3.3.2. Modify the Web Password.....	12
3.4. Phone configuration.....	12
3.4.1. Language.....	12
3.4.1.1. Modify the phone language	12
3.4.1.2. Modify the web language	13
3.4.2. Time	14
3.4.3. Network	15
3.4.3.1. DHCP Mode	15
3.4.3.2. Static Mode	16
3.4.3.3. Local RTP.....	17
3.4.3.4. Connect Setting.....	17
3.4.3.5. LTE configuration	18
3.4.4. Display.....	19
3.4.4.1. Await.....	19
3.4.4.2. Upload ScreenSaver	20
3.4.4.3. Theme selection.....	21
3.4.4.4. Door Setting General	21
3.4.4.5. Home View Visible Control (Villa theme)	22
3.4.4.6. Key In Homepage of The Building Theme	23
3.4.5. Volume.....	24
3.4.5.1. Volume related in device	24
3.4.5.2. Call volume in website	24
3.4.5.3. Mic volume in website	25
3.4.5.4. Open door tone	25
3.4.6. DND	26
3.5. Phonebook.....	27

3.5.1. Phonebook in devices	27
3.5.2. Phonebook in website	28
3.5.3. Import/Export contacts	29
3.5.4. Contact list setting	29
3.6. Intercom call	31
3.6.1. IP Direct Call.....	31
3.6.2. SIP Call.....	32
3.6.2.1. Account	32
3.6.2.2. SIP Account.....	33
3.6.2.3. SIP Server	35
3.6.2.4. Outbound Proxy Server	35
3.6.2.5. Transport Type	36
3.6.3. Dial Plan	36
3.6.4. Quick Dial	38
3.6.5. Speed Dial	38
3.6.6. Auto Answer.....	40
3.6.7. Robin Call	40
3.6.8. Web Call	41
3.7. Security	42
3.7.1. Mjpeg Service.....	42
3.7.2. Live Stream.....	42
3.7.3. RTSP	43
3.7.4. ONVIF.....	44
3.8. Access Control.....	45
3.8.1. Relay	45
3.8.1.1. Unlock Options.....	46

3.8.2. Unlock via RFID Cards.....	47
3.8.2.1. RFID Cards in Devices	47
3.8.2.2. RFID Cards in Website	48
3.8.2.3. Card Type Support.....	49
3.8.3. Unlock via Pin Codes	50
3.8.3.1. Private Pin Codes in Device	50
3.8.3.2. Private Pin Codes in Website	50
3.8.3.3. Public Pin Codes in device	52
3.8.3.4. Public Pin Codes in websites.....	52
3.8.4. Unlock via Face.....	53
3.8.4.1. Face in Device	53
3.8.4.2. Face in Website	54
3.8.5. Unlock via QR code.....	57
3.8.6. Unlock via Bluetooth(Optional).....	57
3.8.7. Unlock via Fingerprint(Optional).....	58
3.8.8. Unlock via HTTP Command.....	59
3.8.9. Unlock via Exit Button	60
3.8.10. Unlock via Reception in Building Theme	60
3.9. Reboot	61
3.10. Reset.....	62
4. Advanced Features	63
4.1. Phone Configuration	63
4.1.1. IR LED	63
4.1.2. LED of Display.....	65
4.1.3. High Contrast of LCD	65
4.1.4. RFID Card Code Display Related	66

4.2. Intercom	66
4.2.1. Call Time Related	66
4.2.1.1. RTP timeout	66
4.2.1.2. Max call time	67
4.2.1.3. Max dial time	67
4.2.1.4. Hang up after open door	68
4.2.2. Return Code When Refused	68
4.2.3. SIP Call Related	68
4.2.4. Call Waiting	69
4.2.5. Intercom	70
4.2.6. Codec	71
4.2.7. DTMF	72
4.2.8. Session Timer	73
4.2.9. NAT	73
4.2.10. User Agent	74
4.2.11. HTTP API	74
4.3. Access control	76
4.3.1. Webrelay	76
4.3.2. Wiegand	77
4.4. Security	78
4.4.1. Antialarm of Door Phone	78
4.4.1.1. Antialarm in device	78
4.4.1.2. Antialarm in website	79
4.4.2. Motion	80
4.4.2.1. Motion in device	80
4.4.2.2. Motion in website	81

4.4.3. Action.....	81
4.4.3.1. Email Notification	81
4.4.3.2. FTP Notification.....	82
4.4.3.3. Input Interface Triggered Action.....	83
4.4.3.4. Reception Action In Building	83
4.5. Upgrade	84
4.5.1. Web Update.....	84
4.5.2. Autop Upgrade	84
4.5.3. Backup Config File	86
4.6. Log	87
4.6.1. Call Log	87
4.6.2. Door Log.....	88
4.6.3. System Log.....	88
4.6.4. PCAP	89

1. Product Overview

1.1. Instruction

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 allows for feature customization to better suit the habit of usage of local people. R29S's multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, helping to create a holistic control of building entrance and its surroundings and giving occupants a great sense of security.

It is applicable to multi-storey residential buildings, high-rise office buildings and their complexes.

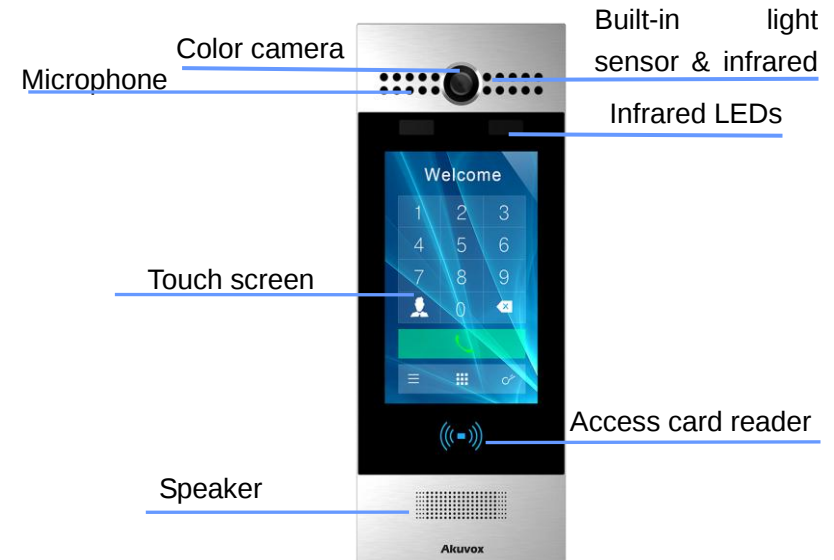


Figure 1.1 Product Description

1.2. Connector Introduction

Ethernet : Ethernet (POE) connector which can provide both power and network connection. (Note:R29C-L not support PoE function.)

12V/GND: External power supply terminal.

WG_D0/1: Wiegand terminal for wiegand access control.

RS485A/B: RS485 terminal for automation system control (e.g. Elevator control).

DOORA/B/C: Trigger signal input terminal (e.g. Press indoor button to open relay).

RelayA/B/C: NO/NC Relay control terminal.

Note: The general door phone interface diagram is only for reference.

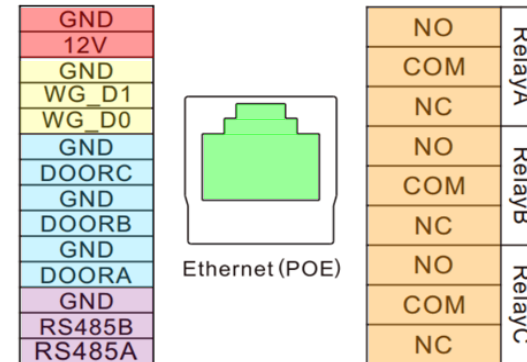


Figure 1.2-1 Connection introduction

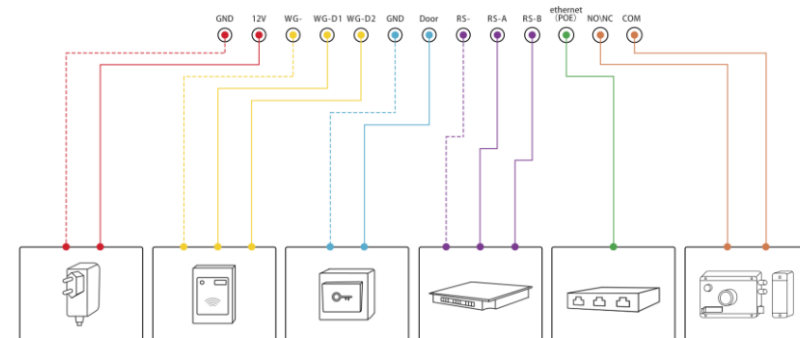


Figure 1.2-2 General interface

2. Daily use

2.1. Starting

When booting R29C-L first time, users need to choose a suitable display language for device. Tap **Start** to start the selection. R29C-L support 4 languages, including **French, English, Spanish** and **Chinese**. Then choosing the proper display theme according to specific application scenarios. R29 supports 3 themes, including **Villa, Building** and **Office**. Tap **Skip** if users are adopting Building theme and English language. Building theme and English language by default.

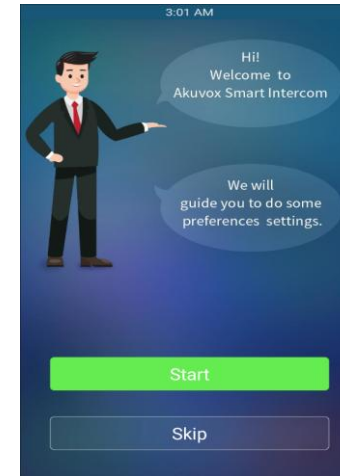


Figure 2.1.1-1 Starting

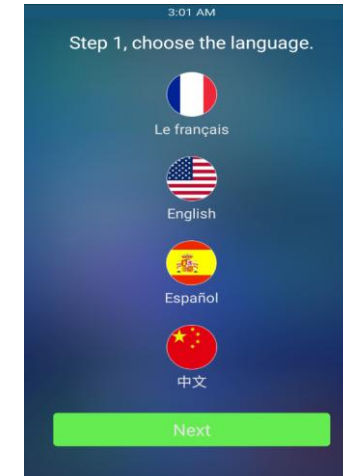


Figure 2.1.1-2 Language selection



Figure 2.1.1-3 Theme selection

2.2. Make a Call

There are three ways to make a call from the door phone to monitor units, which can be an indoor monitor or an intercom app.

2.2.1. Call From Digital Keypad

Press **Dial** (Building theme) or **Call** (Villa theme or Office theme) to enter the dial interface. Enter the number to call on the digital keypad, and press the dial icon.

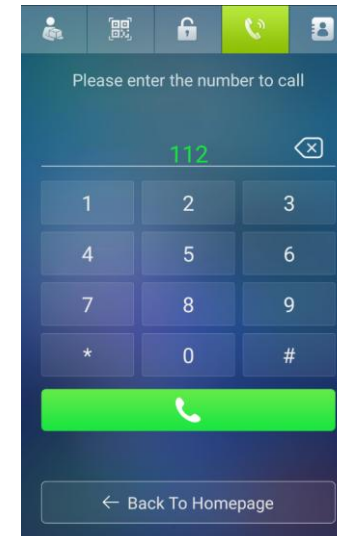


Figure 2.2.1-1 Dial interface
(Building theme)

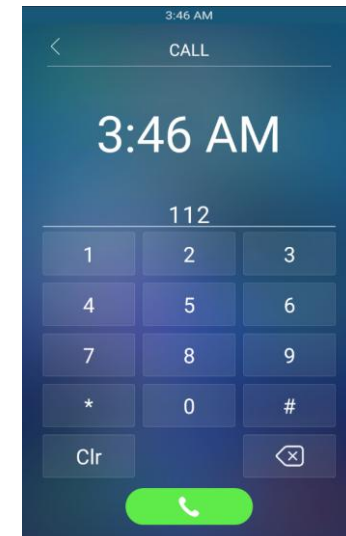


Figure 2.2.1-2 Dial interface
(Villa or Office theme)

2.2.2. Call From Phonebook

Tap **Contacts** to enter the phonebook. In the phonebook interface, to find a specific occupant, scroll up or down the pre-imported contact list, which is either a room number, an occupant's name, or the combination of both. It also supports searching the list by alphabet and then clicking the dial key next to the found contact.

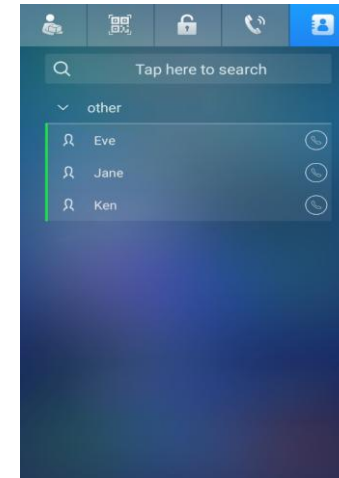


Figure 2.2.2-1 Phonebook interface

(Building theme)

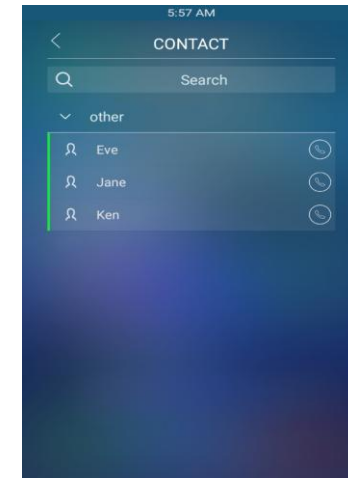


Figure 2.2.2-2 Phonebook interface

(Villa theme)

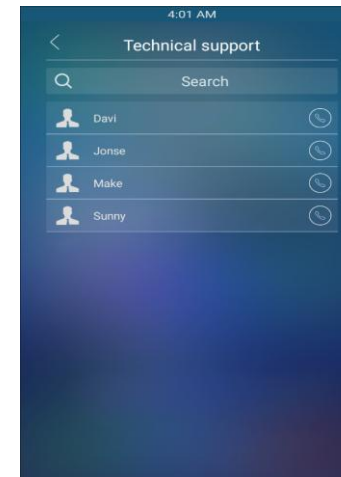


Figure 2.2.2-3 Phonebook interface

(Office theme)

2.2.3. Call From Speed Dial

2.2.3.1. Building theme

Press **Reception** to make the call directly.

2.2.3.2. Villa theme or Office theme

Press **Call** to enter the call interface, choose a speed dial number that users want to call directly.

2.3. Receive a Call

When a monitor unit calls the door phone, it will auto answer the incoming call by default. There is no need to press any answer key.

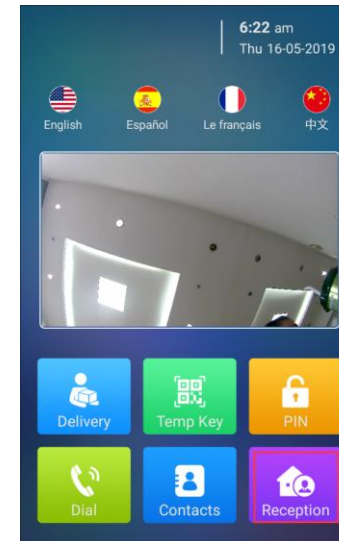


Figure 2.2.3.1 Reception

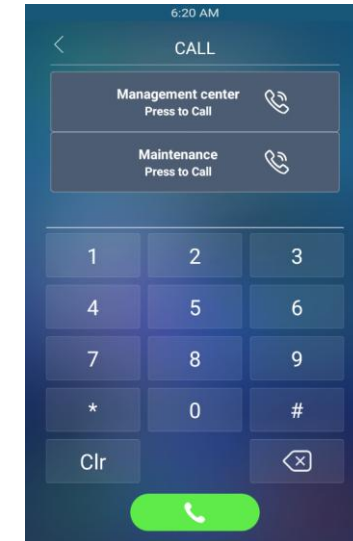


Figure 2.2.3.3 Speed dial

2.4. Unlock

2.4.1. Unlock by PIN Codes

Unlock the door by using predefined public pin or private pin. Press **PIN** icon to enter the PIN code interface, enter the “PIN code” and press **Confirm** icon to unlock, then you will hear “Welcome, please coming” along with the notification “Opening door succeeded”. If users input the wrong PIN code, the screen will shows “Invalid password” .

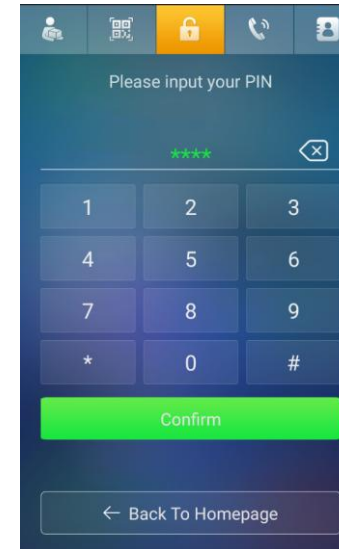


Figure 2.4.1-1 Unlock by pin code
(Building theme)

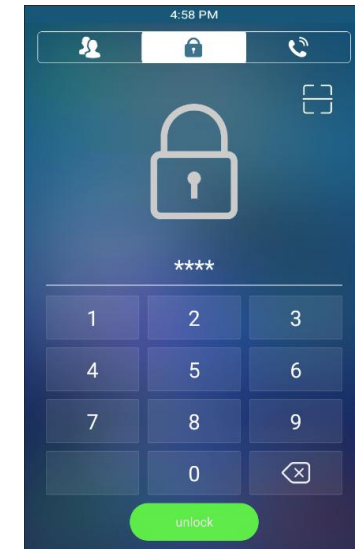


Figure 2.4.1-2 Unlock by pin code
(Villa or Office theme)

2.4.2. Unlock by Face

Stand in front of the camera of R29C-L in 0.5-1m and look at the camera, the device will recognize the predefined face less than 0.6s in the main interface(Building theme) or enter the “Password”(Villa or office theme) interface and it will announce “Welcome, please come in” along with the notification “Opening door succeeded”. Otherwise the screen will show “ Opening Door Failed ! ” .

The device must be in idle. And please make sure there is only one face in the recognition window at a time. And if the UI is villa or office theme, please click the Password page manually or set the Password page as default.

2.4.3. Unlock by RFID cards

Place the predefined users card in RFID cards reader to unlock. Under normal conditions, the phone will announce “Welcome, please coming ” and the screen will show “Opening door

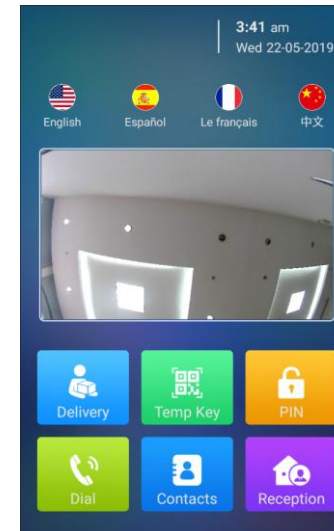


Figure 2.4.2-1 Unlock by face
(Building theme)

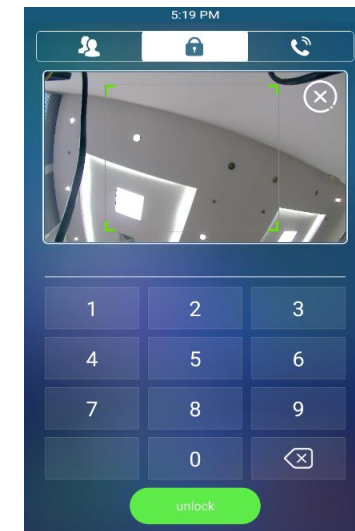


Figure 2.4.2-2 Unlock by face
(Villa or Office theme)

succeeded”. If the card has not been registered, the phone will show “Invalid password” .

2.4.4. Unlock by DTMF codes

During the calling, the president can press the predefined DTMF codes to remote unlock the door.

3. Basic Features

3.1. Access the system setting

In the Dial interface, press “9999”, “Dial key”, “3888”, “OK” to enter the system setting. System setting is easy to configure most basic phone functions.

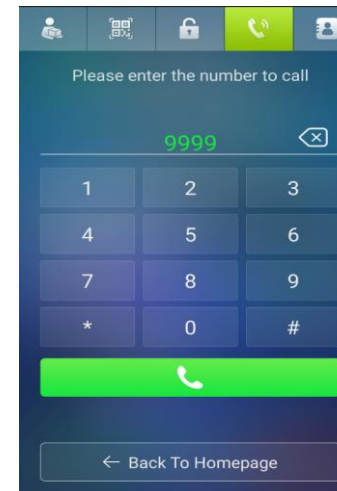


Figure 3.1-1 Access the system setting
(Building theme)

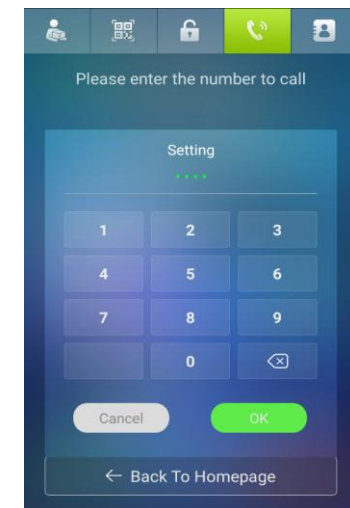


Figure 3.1-2 Access the system setting
(Building theme)

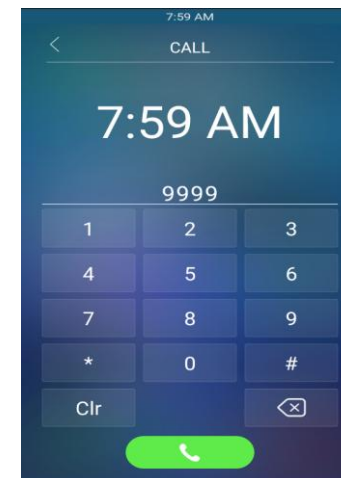


Figure 3.1-3 Access the system setting
(Villa or office theme)

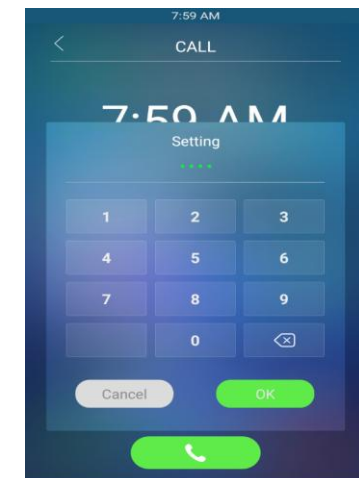


Figure 3.1-4 Access the system setting
(Villa or office theme)

3.2. Access the website setting

3.2.1. Obtain IP Address

R29 series use DHCP IP by default. Enter the phone interface and go to **Info** to check the IP address.

3.2.2. Access the Device Website

Open a web browser, and access the corresponding IP address. Enter the default user name and password to login. The default administrator's user name and password are shown below:

User Name: **admin**

Password: **admin**

Note: The recommended browser is Google Chrome.

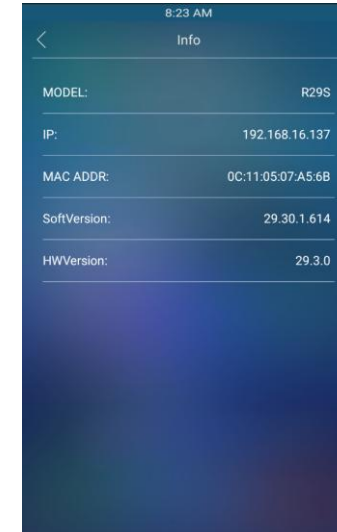


Figure 3.2.1 Info

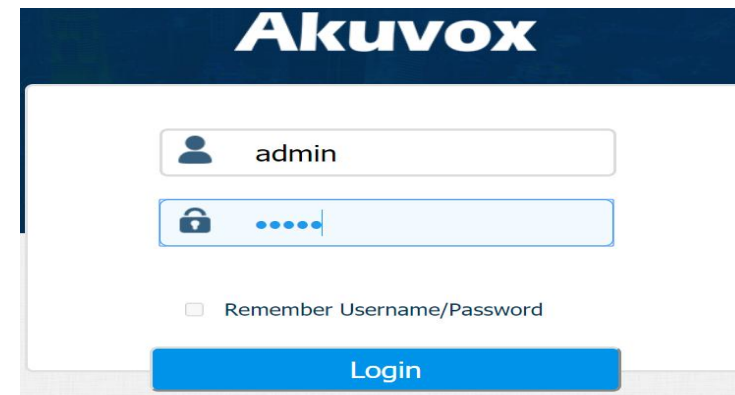


Figure 3.2.2 Access the device website

3.3. Password Modification

3.3.1. Modify the Phone System Password

Users can configure project key with this function. The public key is a password used by all occupants in a building. Project key is used by administrators for some basic settings. There are two ways to change the system password, which can be done on the phone system and on the intercom website.

In the phone interface, go to the **Password - Project Passwd** to change the project key passwd.

Project Passwd: Enter the 4 digits old project key, the default project key is "9999". Then enter the 4 digits new passwd, after entering the new passwd confirm, click **save** icon .

In the website, go to the path **Intercom - Basic - Password** to configure.

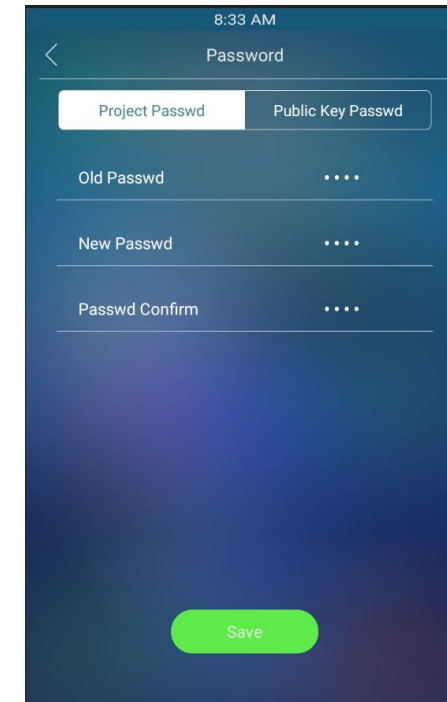


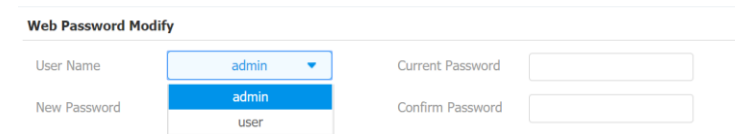
Figure 3.3.1-1 Modify the system password



Figure 3.3.1-2 Modify the system password

3.3.2. Modify the Web Password

Login to the website and go to the path **Security - Basic**, to modify password for “admin” or “user” account.



The form is titled "Web Password Modify". It contains two rows of input fields. The first row is for the "admin" user, with a dropdown menu showing "admin" and "user", and a text field for the "Current Password". The second row is for the "user" account, with a text field for the "New Password" and a text field for the "Confirm Password".

Figure 3.3.2 Modify the web password

3.4. Phone configuration

3.4.1. Language

3.4.1.1. Modify the phone language

In the phone interface, go to **Language** to configure. Now R29 series can support multiple phone language. Users can choose manually. Akuvox uses English by default.



Figure 3.4.1.1-1 Configure phone language

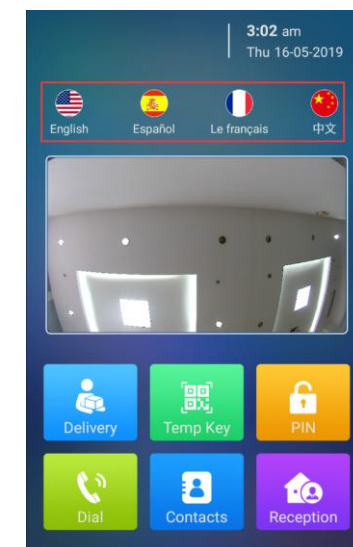


Figure 3.4.1.1-2 Configure phone language (Building theme)

On the building theme, support users to select languages on the main interface. Login to the website and go to the path **Phone -**

Language Setting Of The Building Theme



The form has a label "Language" and a dropdown menu showing "Visible".

Figure 3.4.1.1-3 Configure phone language (Building theme)

Key/Display - Language Setting Of The Building Theme to configure the display language bar. Users can choose the phone language directly from the main interface.

Users can also modify the phone language on the portal **Phone - Time/Lang - LCD Language**.

3.4.1.2. Modify the web language

Enter the intercom website and go to the path **Phone - Time/lang - Web Language** to configure. Now R29 series can support multiple web language. Users can choose manually. Akuvox uses English by default.



Figure 3.4.1.1-4 Configure Web Language

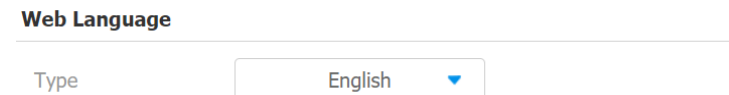


Figure 3.4.1.2 Configure Web Language

3.4.2. Time

In the phone interface, go to **Time** to configure. Choose automatic date & time setting for automatic access of time, date and time zone. Or set the time, date and time zone manually.

Users can also set the time zone configuration on the device portal
Phone - Time/Lang.

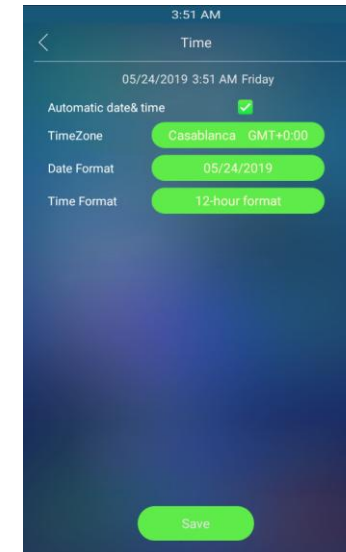


Figure 3.4.2-1 Time

Time

Automatic Date&Time ☐ Auto

Set Date: 2019 7 25

Set Time: 15 18

TimeZone: 0. Casablanca GMT+0:00

NTP Server: pool.ntp.org

Figure 3.4.2-2 Time

3.4.3. Network

In the phone interface, go to **Address** or login to the website and go to the path **Network - Basic**, dynamically or statically to obtain address.

3.4.3.1. DHCP Mode

R29 series uses DHCP mode by default which will get IP address, subnet mask, default gateway and DNS server address from DHCP server automatically.

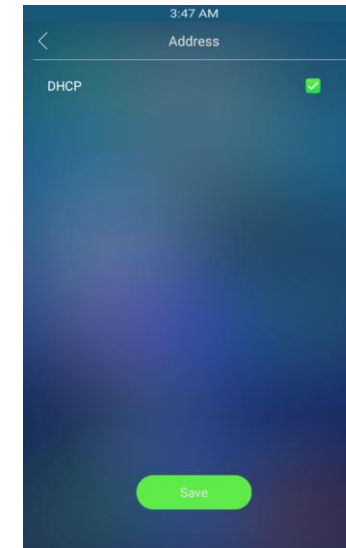


Figure 3.4.3.1-1 DHCP mode

LAN Port

	☒ DHCP	☐ Static IP	
IP Address	192.168.16.137	Subnet Mask	255.255.255.0
Default Gateway	192.168.16.1	LAN DNS1	192.168.16.1
LAN DNS2	0.0.0.0		

Figure 3.4.3.1-2 DHCP mode

3.4.3.2. Static Mode

If select static IP, users should manually setup IP address, subnet mask, default gateway and DNS server address. The figure right shows static IP setting.

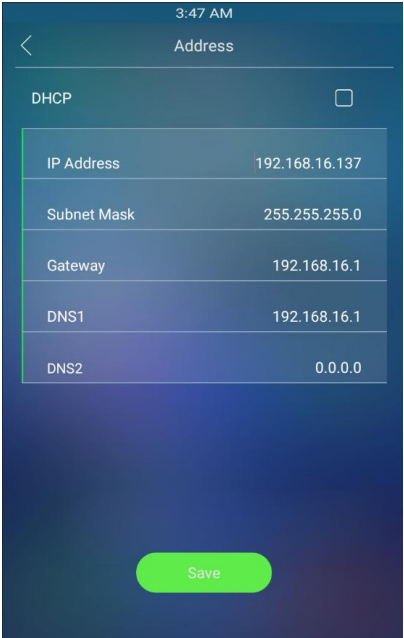


Figure 3.4.3.2-1 Static mode

LAN Port

☐ DHCP ☒ Static IP

IP Address	192.168.16.137	Subnet Mask	255.255.255.0
Default Gateway	192.168.16.1	LAN DNS1	192.168.16.1
LAN DNS2	0.0.0.0		

Figure 3.4.3.2-2 Static mode

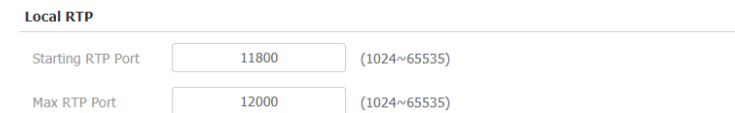
3.4.3.3. Local RTP

Go to **Network - Advanced** to configure.

Local RTP: To display and configure local RTP settings.

Starting RTP Port: Determine the minimum port that RTP stream can use.

Max RTP Port: Determine the maximum port that RTP stream can use.



The screenshot shows the 'Local RTP' configuration section. It has a title 'Local RTP' followed by a horizontal line. Below the line, there are two rows. The first row is 'Starting RTP Port' with a text input field containing '11800' and a range '(1024~65535)' to its right. The second row is 'Max RTP Port' with a text input field containing '12000' and a range '(1024~65535)' to its right.

Figure 3.4.3.3. Local RTP

3.4.3.4. Connect Setting

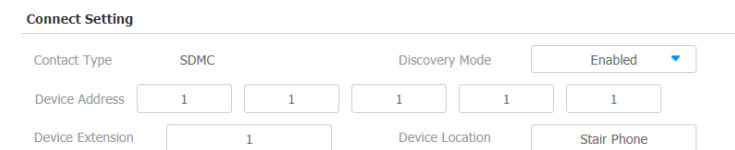
Go to **Network - Advanced** to configure.

Connect Type: Display the device connection type, there are three modes, Discovery, SDMC, Cloud.

Discovery: Enable or disable the discovery mode.

Device Address: It will show which node the device is bound.

Device Extension: Use extension number to distinguish the multiple devices in the same node.



The screenshot shows the 'Connect Setting' configuration section. It has a title 'Connect Setting' followed by a horizontal line. Below the line, there are three rows. The first row is 'Contact Type' with a dropdown menu showing 'SDMC' and 'Discovery Mode' with a dropdown menu showing 'Enabled'. The second row is 'Device Address' with five text input fields, each containing '1'. The third row is 'Device Extension' with a text input field containing '1' and 'Device Location' with a dropdown menu showing 'Stair Phone'.

Figure 3.4.3.4 Connect setting

Device Location: Used to identify the device location, which will also serve as the device display name

3.4.3.5. LTE configuration

LTE connection serves as a wireless network connection for the device in addition to the wired connection, which is convenient for a quick installation for its wireless feature.

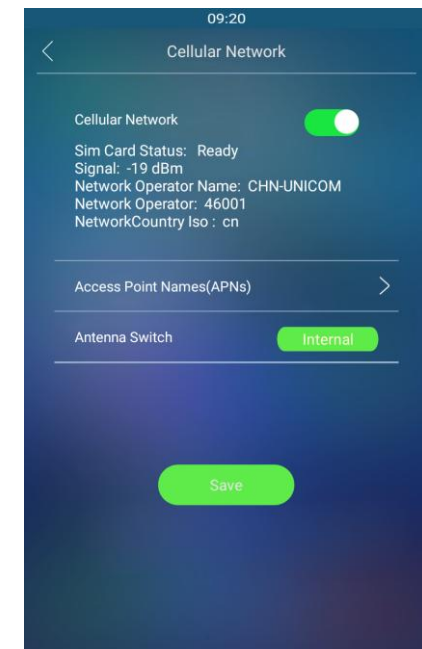
You Click **LTE** icon on home screen and go to **Cellular Network Screen** to do the configuration.

Cellular Network: To enable the disable the LTE function by moving the while ball to the left and right

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 serve as an alternative for the signal transmission.

Note: LTE and another network connections can not be available



in the same time.

3.4.4. Display

3.4.4.1. Await

In the phone interface, go to **Await** or login to the website and go to the path **Intercom - Advanced - StandBy**, to set the standby mode, standby time and unlock mode.

Standby Mode: There are three options for the standby mode. 'NO' mode is for the door phone's default dial interface to remain permanently on; "Blank" mode screen is a black screen during standby; and "Picture" mode is a chosen screensaver of your like, which can be imported in bulk by the administrator.

Standby Time: Users can set the standby time from 30 Sec to 180 Sec.

Unlocked Mode: To choose how to wake up the door phone from the standby mode.

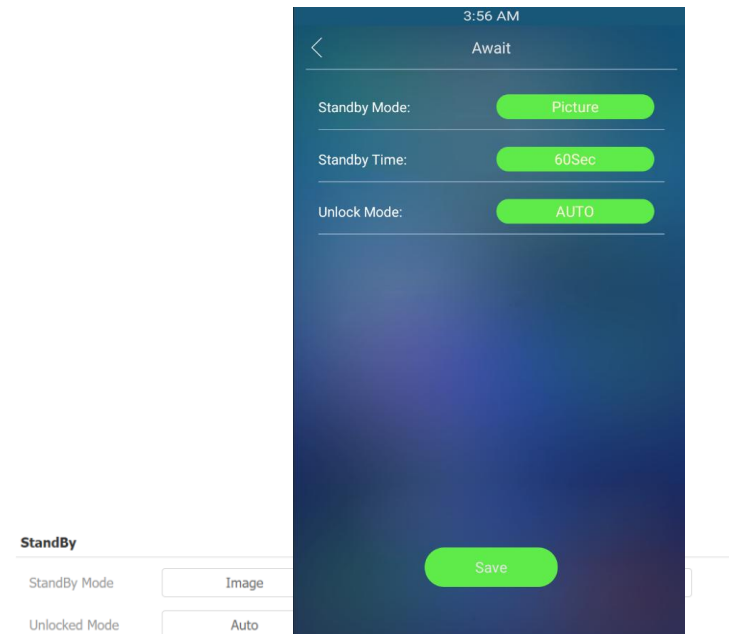


Figure 3.4.4.1-1 Await
Figure 3.4.4.1-2 StandBy

3.4.4.2. Upload ScreenSaver

In the website and go to the path **Phone - Import/Export - Upload screensaver** to configure. To upload screen saver and set the corresponding interval time and the priority. It will be displayed on screen when R29 series stand by type as picture. Up to 5 different screen savers can be supported. These pictures will scroll to display. The format must be .jpg. If the interval time is 0, it won't be displayed.

If users need to upload many pictures, please choose the ID order of the picture. For example, users need to upload the first picture as ID 1 which will be first screensaver to display, users will choose Image 1. Then users will upload the second one, users need to choose Image 2 and so on.

Screensaver1: To choose the favorite image, and upload it (the most suitable image size is 1280*800).

After uploading, the pictures will be in the list. Then users need to

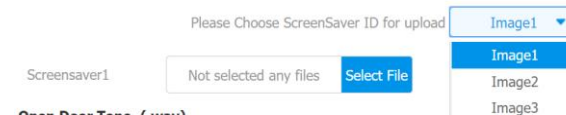


Figure 3.4.4.2-1 Upload ScreenSaver

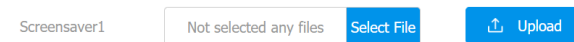


Figure 3.4.4.2-2 Upload ScreenSaver

manually setup the Interval time which means how long the image will display then change to next screensaver. Interval range from 5s to 120s. Click the **Submit** to save each one. Click **Delete** to remove the picture.

3.4.4.3. Theme selection

Go to the path **Intercom - Key/Display**. To choose the device display theme, which supports Villa, Building and Office.

3.4.4.4. Door Setting General

In the website and go to the path **Intercom - Basic - Door Setting General** to configure.

DialPad Input Number Limit: To limit the input numbers to prevent unnecessary security problems.

Upload ScreenSaver (.jpg)

ID	File Status	Interval	Submit	Delete
1	File Exists	6	<button>Submit</button>	<button>Delete</button>
2	File Exists	7	<button>Submit</button>	<button>Delete</button>
3	NULL	0	<button>Submit</button>	<button>Delete</button>
4	NULL	0	<button>Submit</button>	<button>Delete</button>
5	NULL	0	<button>Submit</button>	<button>Delete</button>

Figure 3.4.4.2-3 Upload ScreenSaver

Theme

Theme

Key In Homepage Of

Building

Office

Figure 3.4.4.3 Theme selection

DialPad Input Numb...

Figure 3.4.4.4 Dialpad input number limit

3.4.4.5. Home View Visible Control (Villa theme)

In the website and go to the path **Intercom - Key/Display - View Visible of The Villa Theme** to configure.

Users can setup the home page's default display interface, whether the home page-dial interface, contact interface, unlock interface is visible. For example, if users enable dialview, users will only see dialing interface , the other two will be hided.

Display Type: Setup the home page's default display interface. There are four types can be choice "Homepage", "Dial", "Contact", "Password".

View Control Of The Villa Theme

Display Type	Homepage ▼	DialView	VISIBLE ▼
ContactView	VISIBLE ▼	Password	VISIBLE ▼

Figure 3.4.4.4.5-1 How view visible control

3.4.4.6. Key In Homepage of The Building Theme

On the device homepage of the building theme, six icon are displayed. Users can configure their type on the website, go to **Intercom - Key/Display**. Users can customize the feature of the icon.

Name: To customize the icon display name;

Type: Select the function available for the icon on the device homepage. “NULL” means that the icon is not displayed.

Value: To fill in corresponding parameters for some types. Currently, only the “Speed Dial” type need to fill in value. In general, the value is an IP or SIP account.

Key In Homepage Of The Building Theme

ID	Name	Type	Value
1		Delivery ▼	
2		Temp Key ▼	
3		PIN ▼	
4		Dial ▼	
5		Contact ▼	
6		Speed Dial ▼	

Figure 3.4.4.4.6-1 Key in homepage

3.4.5. Volume

3.4.5.1. Volume related in device

In the phone interface, go to **Volume**, to configure the call volume, AD volume and key volume.

Call Volume: When R29 series dials out a call, it will prompt the 'du' sound. To configure the call volume by yourself.

AD Volume: When the door is opened, the phone will announce the opendoor tone. To configure the AD volume by yourself.

Key Volume: When touch the screen, that will be a prompt sound. To configure the key volume by yourself.

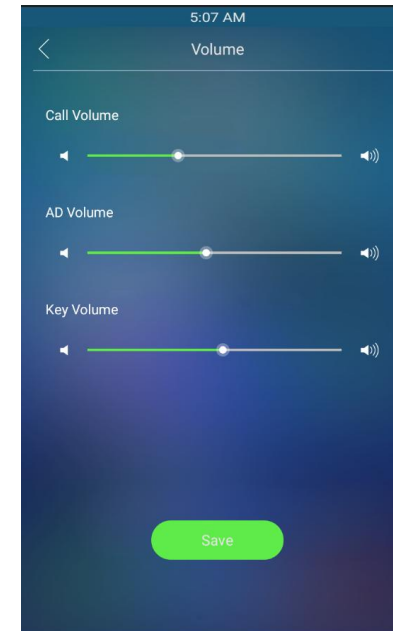


Figure 3.4.5.1 Phone volume

3.4.5.2. Call volume in website

Also users can modify the other voice settings in the website.

Call Volume: Login to the website and go to the path **Phone - Call Feature - Others** to show the volume adjustment in talking

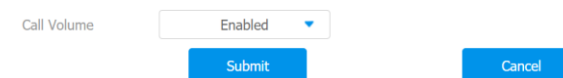


Figure 3.4.5.2 Call volume

interface.

3.4.5.3. Mic volume in website

Mic Volume: Login to the website and go to the path **Phone - Voice**, to configure Mic volume.

3.4.5.4. Open door tone

Open Door Tone: Users can also go to the path **Intercom - Door Setting General** to configure the switch whether users will hear the “Welcome! Please coming” announcement when the door is opened.

Open Door Warning: On the portal **Intercom - Advanced - Open Door Warning**, configure whether to enable open door success or failure warning.

Open Door Tone: Login to the website and go to the path **Phone - Import/Export - Open Door Tone** to upload the open door tone by



Figure 3.4.5.3 Mic volume



Figure 3.4.5.4-1 Open door warning

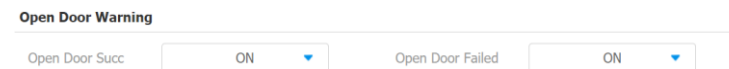


Figure 3.4.5.4-2 Open door warning

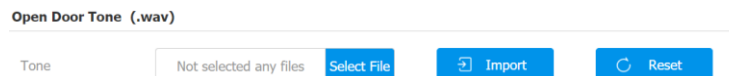


Figure 3.4.5-6 Upload the open the door tone

yourself.

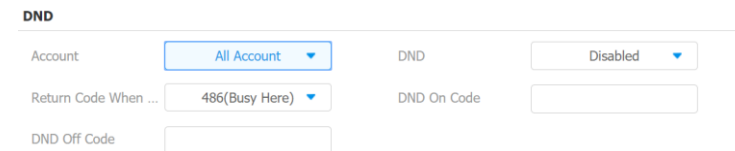
3.4.6. DND

DND allows IP phones to ignore any incoming calls. Users can login to the website and go to **Phone - Call Feature** to configure.

Return Code when DND: Determine what response code should be sent back to server when there is an incoming call if DND on.

DND On Code: The code used to turn on DND on server's side, if configured, IP phone will send a SIP message to server to turn on DND on server side if user press DND when DND is off.

DND Off Code: The code used to turn off DND on server's side, if configured, IP phone will send a SIP message to server to turn off DND on server side if user press DND when DND is on.



DND	
Account	All Account
Return Code When ...	486(Busy Here)
DND Off Code	
DND	Disabled
DND On Code	
DND Off Code	

Figure 3.4.6 DND

3.5. Phonebook

3.5.1. Phonebook in devices

In the phone interface, go to **Contact** to configure the phonebook.

Create a group: Choose group, click **Add** to enter the new group name. Press **Save** to save.

Edit a group: Choose the existed group to modify or delete.

Create a contact: Click **Add** to enter the contact's information. Choose a suitable Group and contact's name and Phone number, press **Save** to save.

Edit a contact: Choose a exist contact to edit or delete it.

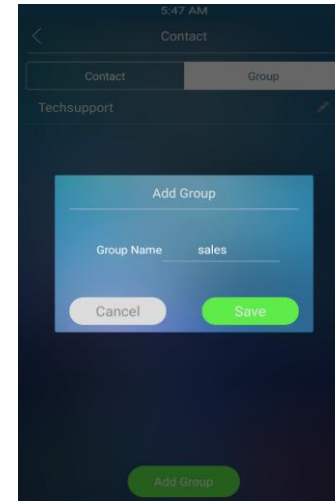


Figure 3.5.1-1 Adding group

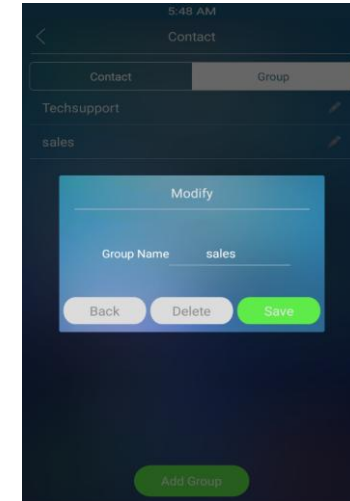


Figure 3.5.1-2 Editing group

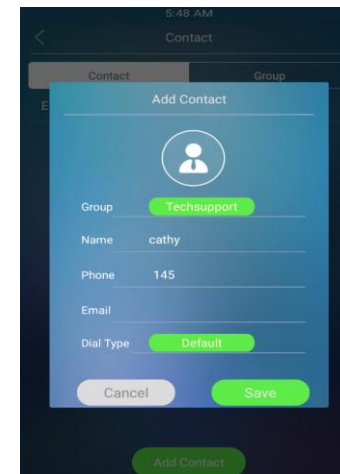


Figure 3.5.1-3 Adding contact

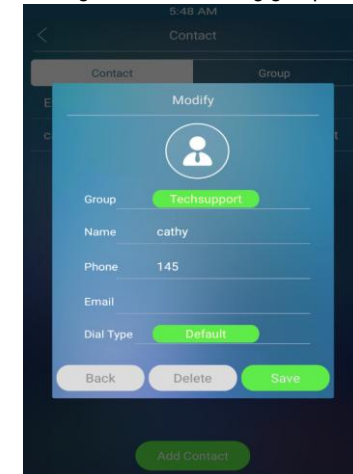


Figure 3.5.1-4 Editing contact

3.5.2. Phonebook in website

In the website, go to the path **Phonebook - Local Book** to configure the phonebook.

Contact: To display or edit all local contacts.

Search: Enter the key word to search designated contacts from local phonebook.

Contact Setting: Choose a suitable contact picture, then import (optional); Enter the corresponding contact name and phone number; Click **Add** to save.

Note: The photo only supports .jpg format.

Group: To check all group in the list or choose one to delete.

Group Setting: Enter the new group name, click **Submit** to save;

Index	Name	Phone	Group	Dial Type	Email	FloorNum	Priority Of Call
1	Eve	228	Default	Default		0	NULL

Figure 3.5-5 Phonebook

Figure 3.5-6 Contact setting

Index	Name
1	Techsupport
2	
3	
4	
5	
6	
7	
8	
9	
10	

Figure 3.5-7 Group configure

3.5.3. Import/Export contacts

Users can also login to the website and go to the path **Phone - Import/Export - Import/Export Config&Contacts** to upload or download the contact information.

Contact: Click **Export** to export the existed contact. Choose the local file and click **Import** to import the new contact. The export format is .vcf, the import format is .vcf, .csv or .xml. The import maximum is 3000.



Figure 3.5-8 Import/Export contacts

3.5.4. Contact list setting

Login to the website and go to the path **Intercom - Basic - Door Setting General**.

Item Touch: This function is convenient for users to press anywhere in the contact line to call out, don't have to call out to touch the call button.

Contact Profile Picture: To setup whether it will show contact

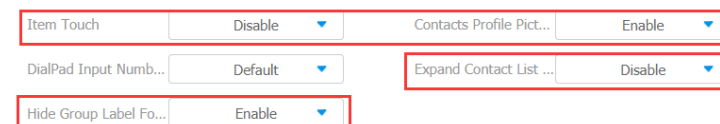


Figure 3.5.4-1 Contact display

picture or not.

Expend Contact List View Mode: With this enabled, the contact list will be displayed in view mode.

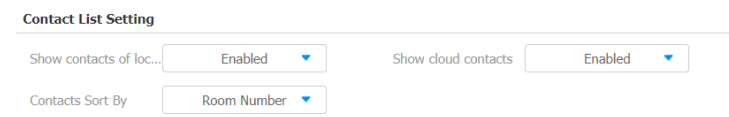
Hide Group Label For Contact List: With this enabled, the contact list will be displayed directly and there will be no group.

Login to the website and go to the path **Phonebook - Phonebook - Contact List Setting**.

Show contacts of local group: To enable/disable whether to display the contact list for local groups. If disabled, the contact interface will no longer display the local contact list, users will only be able to call as a group, not select the contacts to call.

Show cloud contacts: To enable/disable whether to display the cloud contact lists. If disabled, the cloud contact are not displayed on contact interface.

Contact Sort By: Select the sort of contact list, which supports three methods: ASCII Code, Room Number and Import. "ASCII



Contact List Setting

Show contacts of loc... Enabled

Show cloud contacts Enabled

Contacts Sort By Room Number

Figure 3.5.4-2 Contact list setting

code” means that the contact list will be displayed in order of 0~9, a~z; “Room number” means that the contact list will be displayed in order of a~z, 0~9; “Import” means that the contact list will be displayed in the same order as in the import file.

3.6. Intercom call

3.6.1. IP Direct Call

In the dial interface. Enter the number to call on the digital keypad, and tap the dial icon. Without SIP server, users can also use IP address to call each other. However, this way is only suitable in the LAN. Enter the IP address of the callee, and press the **dial** icon.

Login to the website and go to the path **Phone - Call Feature - Others** to configure the call related features.

Direct IP: To call someone with dialing IP address directly.

Direct IP Port: To configure the direct IP port.

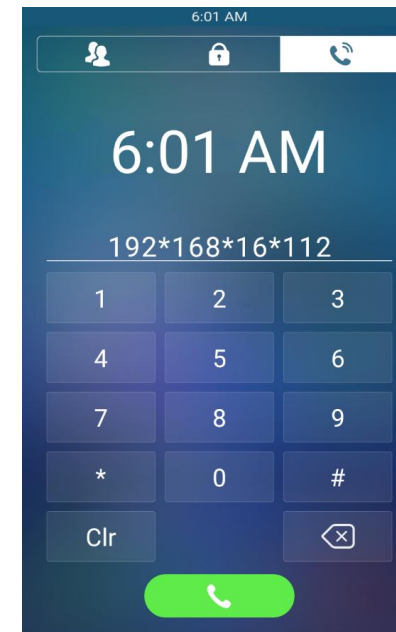


Figure 3.6.1-1 Dial interface

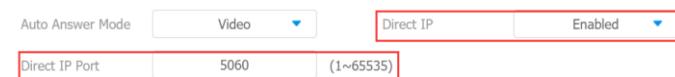


Figure 3.6.1-2 Direct IP

3.6.2. SIP Call

SIP call uses SIP number to call each other which should be supported by SIP server. Users need to register an account and fill some SIP feature parameters before using SIP call.

Login to the website and go to the path **Account - Basic** to configure SIP account and SIP server for door phone first.

3.6.2.1. Account

R29 series supports 2 accounts. According to your needs, register one or two accounts and users can switch them by themselves.

Enter the system setting interface, choose account. According to the configuration of PBX, enter the account parameters. Tick enable to active the account. If you register 2 accounts in the same time. R29 series will choose the account 1 as the default account.

3.6.2.2. SIP Account

In the phone interface, go to **Account - Account setting - Account 1&2** to configure the SIP account.

Enable Account: SIP account is only available if you enable this account.

Register Name: To enter extension number you want and the number is allocated by SIP server.

User Name: To enter user name of the extension.

Password: To enter password for the extension.

Display Name: To configure name sent to the other call party for displaying.

Note: After configurations, users can go to the **website - Account - Basic - SIP Account** to check the register status.

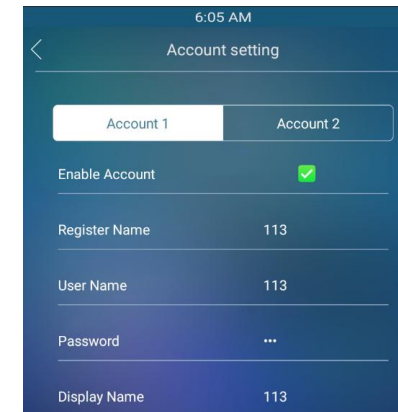


Figure 3.6.2.2-1 SIP account

Login to the website and go to the path **Account - Basic - SIP Account** to configure the SIP account.

Status: To display register result.

Account: Select the SIP account you need to configure.

Account Active: SIP account is only available if users enable this account.

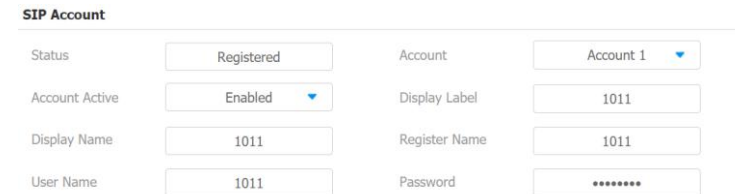
Display Label: To configure label displayed on the phone's LCD screen.

Display Name: To configure name sent to the other call party for displaying.

Register Name: To enter extension number users want and the number is allocated by SIP server.

User Name: To enter user name of the extension.

Password: To enter password for the extension.



The screenshot shows the 'SIP Account' configuration page. It features a table with two columns for configuration options. The first column lists the options: Status, Account Active, Display Name, and User Name. The second column lists the options: Account, Display Label, Register Name, and Password. Each option has a corresponding input field. The 'Status' field is set to 'Registered'. The 'Account Active' field is set to 'Enabled' with a dropdown arrow. The 'Account' field is set to 'Account 1' with a dropdown arrow. The 'Display Label' field is set to '1011'. The 'Display Name' field is set to '1011'. The 'Register Name' field is set to '1011'. The 'User Name' field is set to '1011'. The 'Password' field is masked with eight asterisks.

SIP Account	
Status	Registered
Account Active	Enabled ▼
Display Name	1011
User Name	1011
Account	Account 1 ▼
Display Label	1011
Register Name	1011
Password	*****

Figure 3.6.2.2-2 SIP account

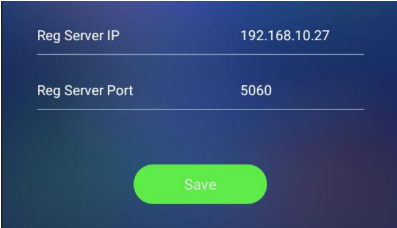
3.6.2.3. SIP Server

In the phone interface, go to **Account - Account setting - Account 1&2** to configure the SIP server. Users can also go to the path **Account - Basic - SIP Server 1&2** to configure.

Server IP: To enter SIP server's IP address or URL.

Server Port: To enter the SIP server port.

Registration Period: The registration will expire after registration period, the IP phone will re-register automatically within registration period.

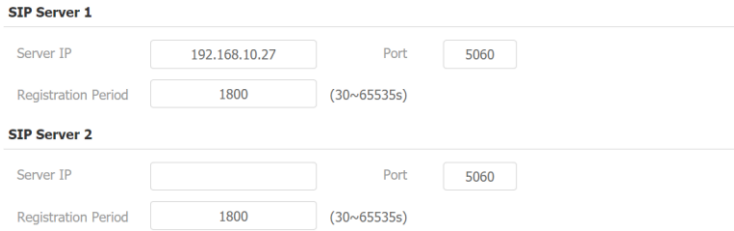


Reg Server IP 192.168.10.27

Reg Server Port 5060

Save

Figure 3.6.2.3-1 SIP server



SIP Server 1

Server IP 192.168.10.27 Port 5060

Registration Period 1800 (30~65535s)

SIP Server 2

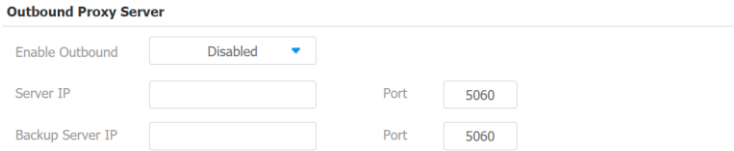
Server IP Port 5060

Registration Period 1800 (30~65535s)

Figure 3.6.2.3-2 SIP server

3.6.2.4. Outbound Proxy Server

Login to the website and go to the path **Account - Basic - Outbound Proxy Server** to display and configure outbound proxy server settings. An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server.



Outbound Proxy Server

Enable Outbound Disabled

Server IP Port 5060

Backup Server IP Port 5060

Figure 3.6.2.4 Outbound proxy server

3.6.2.5. Transport Type

To display and configure transport type for SIP message

UDP: UDP is an unreliable but very efficient transport layer protocol.

TCP: Reliable but less-efficient transport layer protocol.

TLS: Secured and Reliable transport layer protocol.

DNS-SRV: DNS record for specifying the location of services.

3.6.3. Dial Plan

● Replace Rule

Replace rule is using some simple number or symbol to replace a complicated phone number or IP address. It is more suitable for some one who want to hide the real phone number or simplify the long number. This is more convenient for users.

In the phone system, go to **Replace Rule**, click **Add**, choose a suitable account and enter the value, press **Save** to confirm. It



Figure 3.6.2.5 Transport type

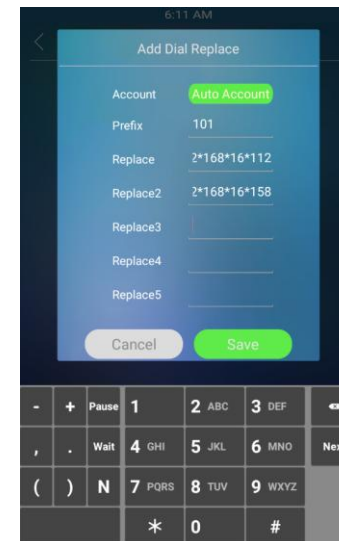


Figure 3.6.3-1 Replace rule

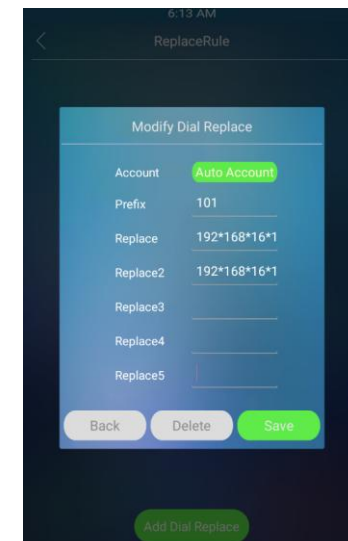


Figure 3.6.3-2 Replace rule

supports a prefix number replace 5 number at the same time, when the user press the prefix number, the 5 devices will ring at the same time. Users can edit or delete the existed replace rules.

For example:

Users can pre-configure 101 to replace 192.168.16.112 and 192.168.16.158 in the doorphone. Then, by pressing 101, the two devices can be dialed at the same time through the default account without having to remember the long phone number or dial separately.

Users can also login to the website and go to the path **Phone - Dial Plan** to configure this function. R29 allows users to modify replace rule in the website.

All replace rules will show in the list. Users can edit or delete the existed replace rules.

Rules Modify >>

Account	Account1	Prefix	1001
Replace 1	192.168.16.112	Replace 2	192.168.16.239
Replace 3		Replace 4	
Replace 5			

Submit Cancel

Figure 3.6.3-2 Dial plan

Rules Replace Rule

☐	Index	Account	Prefix	Replace 1	Replace 2	Replace 3	Replace 4	Replace 5
☐	1	Account1	1001	192.168.16.112	192.168.16.239			

Figure 3.6.3-3 Dial plan

3.6.4. Quick Dial

Quick dial is to call predefined important number quickly in main interface. This number is often set as emergency number.

In the phone interface, go to **Quick Dial**, switch the type as quick dial, enter the quick dial name and number, click **Save** to confirm.

3.6.5. Speed Dial

The speed dial contact list will be displayed in the dial interface, convenient for users to dial directly. Users can choose whether to display the list or configure whether to display both the contacts and keypad. Login to the website and go to the path **Phone - Speed Dial**.

Speed Dial Theme: Configure the speed dial list display theme. Which supports 9 themes: Standard, Auto, 1key, 1 Key+Keypad, 2 Keys+Keypad, 4Keys+Keypad, 8 Keys, 16 Keys, 64 Keys.

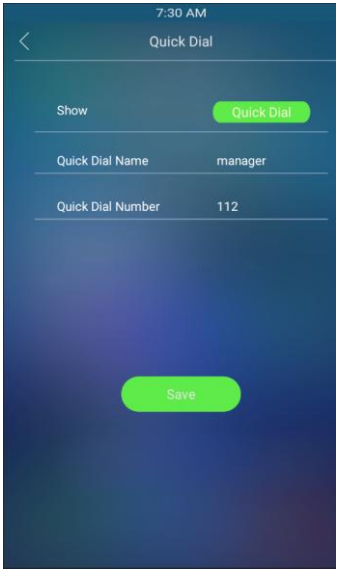


Figure 3.6.4-1 Quick dial configure

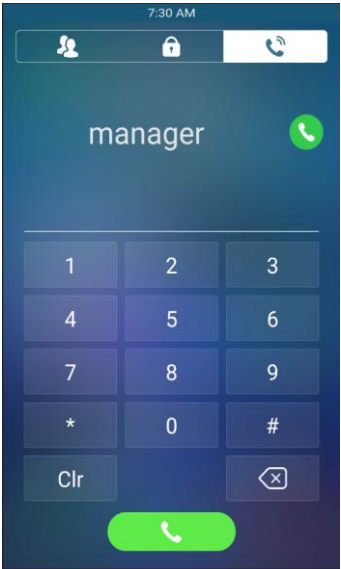


Figure 3.6.4-2 Quick dial

Speed Dial Theme				
Speed Dial Theme: 4 keys + keypad ▾				
Speed Dial Contacts Management				
Index	Name	Number	Submit	Clear
1	Eve	112	Submit	Clear
2	Cathy	113	Submit	Clear
3	Josh	114	Submit	Clear
4	Dave	115	Submit	Clear
5	Miki	116	Submit	Clear

Figure 3.6..5-1 Speed dial

Standard	It will not displayed the contact list, only display time and keypad.
Auto	The dial interface will based on the number of speed dial contacts. Null displays the time and keypad; 1~4 contacts will displays contacts and keypad; More then 4 contacts, only contacts will be displayed.
1/8/16/64 Key	The dial interface will display the speed dial contacts based on the number of keys, and the keypad will not be displayed.
1 Key+Keypad	The dial interface will display the speed dial contacts based on the number of keys, and the keypad will be displayed.
2 Keys+Keypad	
4 Keys+Keypad	

Speed Dial Contacts Management: Configure contact names and numbers, which supports up to 64 contacts. Only 8 contacts can be displayed on one page, more than 8 contacts will be displayed on the next page.

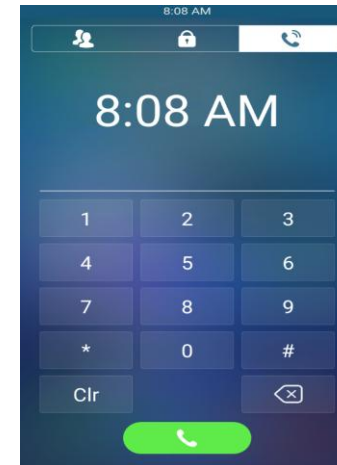


Figure 3.6..5-2 Standard

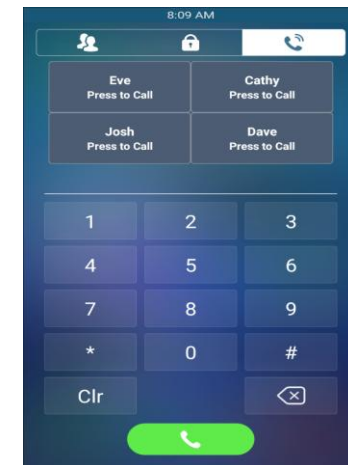


Figure 3.6..5-3 4 Keys+keypad

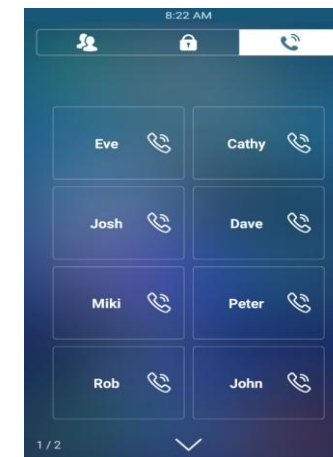


Figure 3.6..5-4 9 Keys

3.6.6. Auto Answer

Login to the website and go to the path **Account - Advanced - Call - Auto Answer** to enable the auto answer.

Login to the website and go to the path **Phone - Call Feature - Others** to configure the auto answer related function.

Return Code When Refuse: Allow users to assign specific code as return code to SIP server when an incoming call is rejected.

Auto Answer Mode: To choose video or audio mode for auto answer.

3.6.7. Robin Call

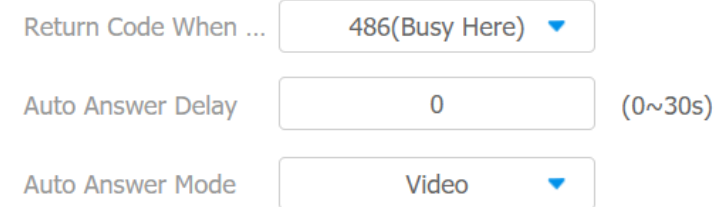
This feature is used to transfer calls to the target number in order if the calling is no answered with timeout. Login to the website and go to the path **Intercom - Basic - Basic** to check. It supports up to 10 call numbers. They will be called in order.



Auto Answer Enabled ▼

Figure 3.6.5 -1Auto answer

Others



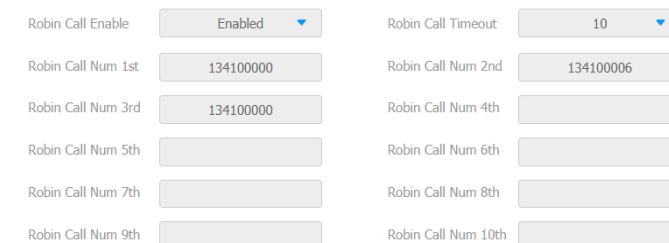
Return Code When ... 486(Busy Here) ▼

Auto Answer Delay 0 (0~30s)

Auto Answer Mode Video ▼

Figure 3.6.5 -2 Auto answer

Basic



Robin Call Enable	Enabled ▼	Robin Call Timeout	10 ▼
Robin Call Num 1st	134100000	Robin Call Num 2nd	134100006
Robin Call Num 3rd	134100000	Robin Call Num 4th	
Robin Call Num 5th		Robin Call Num 6th	
Robin Call Num 7th		Robin Call Num 8th	
Robin Call Num 9th		Robin Call Num 10th	

Figure 4.2.4 Robin call

Note: This feature should work with Akuvox Cloud. Please contact your administrator for more information.

3.6.8. Web Call

Login to the website and go to the path **Phonebook - Local Book - Dial** to dial out from website.

Dial: To dial out a call or hangup an ongoing call from website.

Dial

The image shows a web interface for making calls. It includes a text input field for a phone number, a dropdown menu currently set to 'Auto', and two blue buttons labeled 'Dial' and 'Hand Up'.

Figure 3.6.6 Web call

3.7. Security

3.7.1. Mjpeg Service

Login to the website and go to the path **Intercom - Advanced - Mjpeg Server** to configure.

Mjpeg Service Enable: Use to capture from the URL. It is convenient to check the capture remotely.

Image Quality: To choose the image quality of the capture.

Picture URL:

`http:// device ip:8080/picture.cgi`

`http://device ip:8080/picture.jpg`

`http://device ip:8080/jpeg.cgi`

3.7.2. Live Stream

Login to the website and go to the path **Intercom - Live Stream**, check the real-time video from R29. In addition, users can also

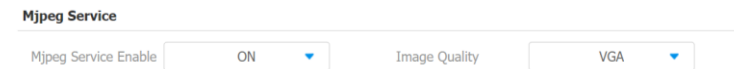


Figure 3.7.1 Mjpeg service

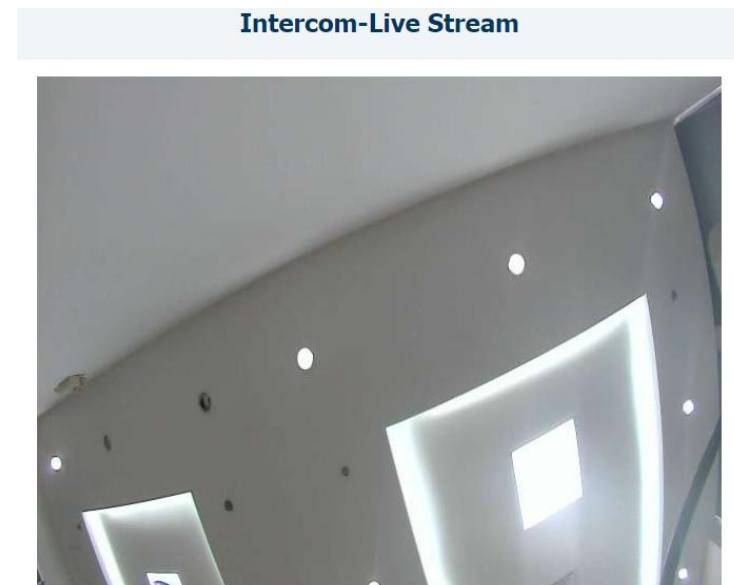


Figure 3.7.2 Live view

check the real-time picture via URL:

`http://IP_address:8080/video.cgi`

3.7.3. RTSP

- **RTSP Basic**

R29 series support RTSP stream, enter the phone system, go to **RTSP** or login to the website and go to the path **Intercom - RTSP**, to enable or disable RTSP server. The URL for RTSP stream is:
`rtsp://IP_address/live/ch00_0`

- **H.264 Video Parameters**

H.264 is a video stream compression standard. Different from H.263, it provides an approximately identical level of video stream quality but a half bit rate. This type of compression is sometimes called MPEG-4 part 10. To modify the resolution, framerate and bitrate of H.264.

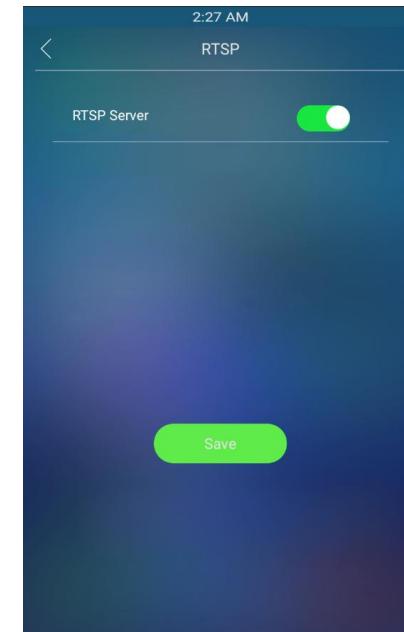


Figure 3.7.3-1 RTSP



Figure 3.7.3-2 RTSP

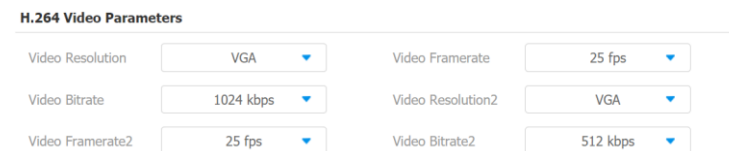


Figure 3.7.3-3 H.264 video parameters

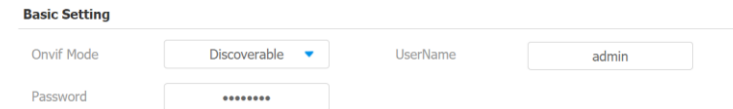
3.7.4. ONVIF

R29 series supports ONVIF protocol, which means R29 series camera can be searched by other devices, like NVR, which supports ONVIF protocol as well. Go to the path **Intercom - ONVIF** on the web GUI, to configure ONVIF mode and its username/password.

Switching ONVIF mode to “undiscoverable” means that Users must program ONVIF’s URL manually.

The ONVIF’s URL is:

http://IP_address:8090/onvif/device_service



The screenshot shows the 'Basic Setting' section of the web GUI. It contains three fields: 'Onvif Mode' with a dropdown menu set to 'Discoverable', 'UserName' with a text box containing 'admin', and 'Password' with a text box containing eight asterisks. The 'Onvif Mode' dropdown has a small blue triangle indicating it can be expanded.

Figure 3.7.4 ONVIF setting

3.8. Access Control

3.8.1. Relay

Login to the website and go to the path **Intercom - Relay** to configure.

Relay ID: R29 series supports three relays. Users can configure them respectively.

Trigger Delay: To configure the duration of the trigger relay. With the trigger condition, the relay will only be triggered if the value is reached.

Hold Delay: To configure the duration of opened relay. Over the value, the relay would be closed again.

DTMF Option: To select digit of DTMF code, R29 series supports maximum 4 digits DTMF code.

DTMF: To configure 1 digit DTMF code for remote unlock

Multiple DTMF: To configure multiple digits DTMF code for remote unlock.

Relay			
Relay ID	RelayA ▼	RelayB ▼	RelayC ▼
Trigger Delay(sec)	0 ▼	0 ▼	0 ▼
Hold Delay(sec)	5 ▼	5 ▼	5 ▼
DTMF Option	1 Digit DTMF ▼		
DTMF	# ▼	1 ▼	2 ▼
Multiple DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	RelayA	RelayB	RelayC

Figure 3.8.1 Relay

Relay Status: While the relay is triggered, the statues will be switched. When COM connects to NC, the status is Low.

Note: Relay operate a switch and does not deliver power, so users should prepare power adapter for external devices which connects to relay.

3.8.1.1. Unlock Options

Users can choose which relay want to opened. On the path **Intercom - Relay - Unlock Options**, configure to be “VISIBLE”. When users tries to open the door, it prompts the message to choose which relay to open.

Note: All relays are enabled by default. Users should choose which relay they do not want to open.

Unlock Options

Unlock Options

VISIBLE ▼

Figure 3.8.1.1-1 Unlock options

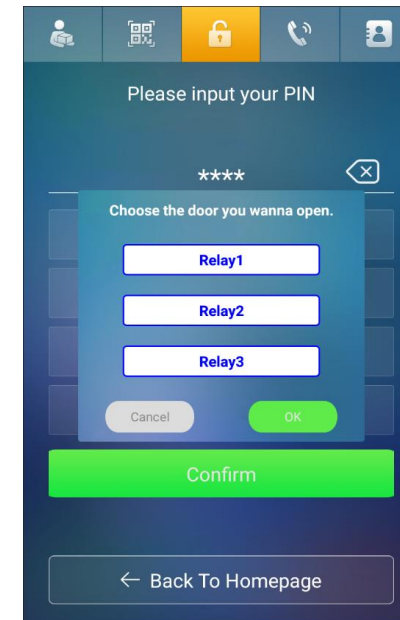


Figure 3.8.1.1-2 Unlock

3.8.2. Unlock via RFID Cards

3.8.2.1. RFID Cards in Devices

R29 series can be compatible with 13.56MHZ and 125KHZ RFID cards.

Add

Press “**Add Card**”, when you see “Please scan the RFCard to Add”, put the card near the card sensor. Then enter the device name , valid day and time in the modify prompt. Click **OK** to save.

Modify

Press “**Del Card**”, when you see “Please scan RFCard to Delete”, put the exited card near the card sensor, click **Del** to delete in the modify prompt. Or users can just choose the exited card from the list, select directly.

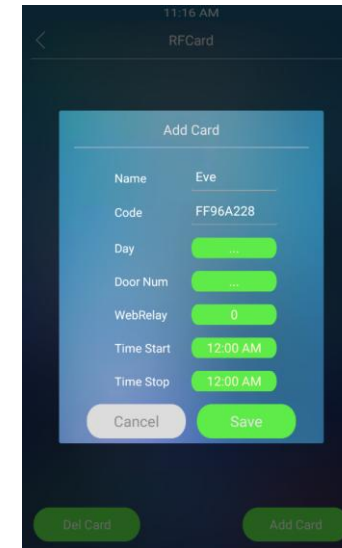


Figure 3.8.2.1-1 RF key

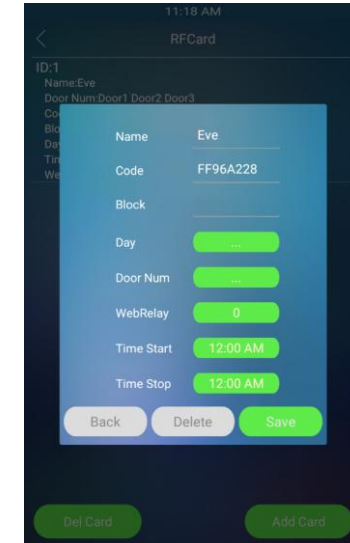


Figure 3.8.2.1-2 RF key

3.8.2.2. RFID Cards in Website

Go to the path **Intercom - Card setting**, to manage RFID cards access system.

Import/Export Card Data: Export the existed RFID cards information or import the new RFID cards information. It can only support .xml format. The maximum is 1000.

Note: Ask your administrator for the card data template if you need.

Obtain and Add Card:

- (1) Switch card status to “Card Issuing” and click “**Apply**”;
- (2) Place card on the card reader area and click “**Obtain**”;
- (3) Name card and choose which door you want to open and the valid day and time;
- (4) Click “**Add**” to add it into list.



Figure 3.8.2-3 Import/Export card data

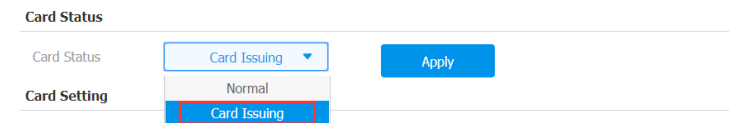


Figure 3.8.2-4 Card status

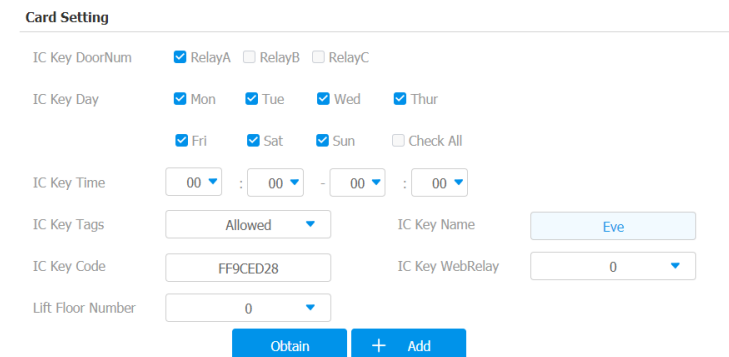


Figure 3.8.2-5 Card setting

Door Card Management:

Valid card information will be shown in the list. Administrator could delete one card's access permission or empty all the list.

Note: Remember to set card status back to normal after adding the cards.

3.8.2.3. Card Type Support

Go to the path **Intercom - Card Setting**, to choose the type of card you need. Users can choose enable the NFC or Felica.

Note: There is a conflict between these two card types, please choose one of them when needed.

Door Card Management

☐ Index	Name	Code	Relay	WebRelay	FloorNum
☐ 1	Eve	FF9CED28	1	0	0
☐ 2					
☐ 3					
☐ 4					
☐ 5					

Figure 3.8.2-6 Door card management

Card Type Support

NFC Enable Enabled ▼ Felica Enable Disabled ▼

Figure 3.8.3-1 Card type support

3.8.3. Unlock via Pin Codes

3.8.3.1. Private Pin Codes in Device

In the phone interface, go to **LockPasswd**, enter the owner name, 8 digits private keys and Device (optional). Setup the valid day and time for the password.

For example:

Owner name is Eve, private key is 1995, and I set up the valid day from Mon to Sun, click **Save** to save.

3.8.3.2. Private Pin Codes in Website

Go to the path **Intercom - Privatekey** on the web GUI, to manage RFID cards access system.

Import/Export Private Key: Export the existed private key information or import the private key from local side. It can only support .xml format. The maximum private key is 1000.

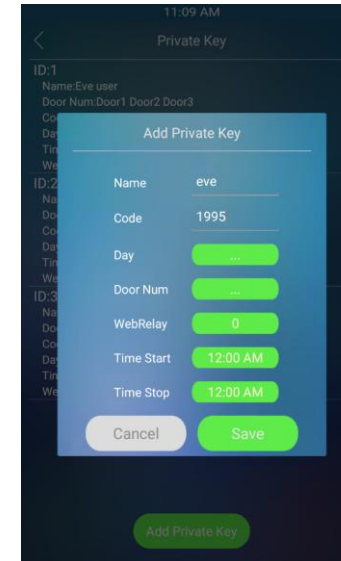


Figure 3.8.3.1-1 Adding private key

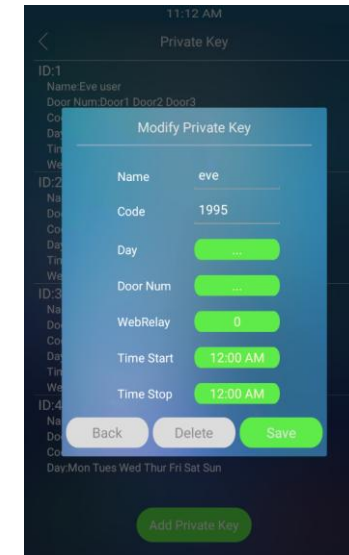


Figure 3.8.3.1-2 Editing private key



Figure 3.8.3.2-1 Import/Export private key

Obtain and Add Code:

- (1)Enter the “PKey Name” and “PKey Code”;
- (2)Select the valid day and time;
- (3)Choose which door users want to open;
- (4)Click “**Add**” to add it into list.

Private Key Management:

Valid private key information will be shown in the list. Administrator could delete private key information or empty all the list.

Private Key Setting

PKey DoorNum ☒ RelayA ☒ RelayB ☒ RelayC

PKey Day ☒ Mon ☒ Tue ☒ Wed ☒ Thur
☒ Fri ☒ Sat ☒ Sun ☐ Check All

PKey Time

PKey Name

PKey Code

Figure 3.8.3.2-2 Private key setting

Private Key Management

☐ Index	Name	Code	Relay
☐ 1	Eve	12345678	123
☐ 2			
☐ 3			

Figure 3.8.3.2-3 Private key management

3.8.3.3. Public Pin Codes in device

In the phone interface, go to **Password - Public Key Passwd**, enter the old public key, R29 series support 3 default public keys. Then enter the new password, after entering the new password Confirm, click **save** icon.

Note: Just need to enable public key password in public key password setting.

3.8.3.4. Public Pin Codes in websites

Go to the path **Intercom - Basic - Password**. Users can configure project key and public key with this function. Public key is the password used by all occupants in a building.

Public Enable: The default status is on.

PublicKey Bits Limit: Setup the key digits.

Public Key: R29 series support 3 default public keys, users can reset a new public key.

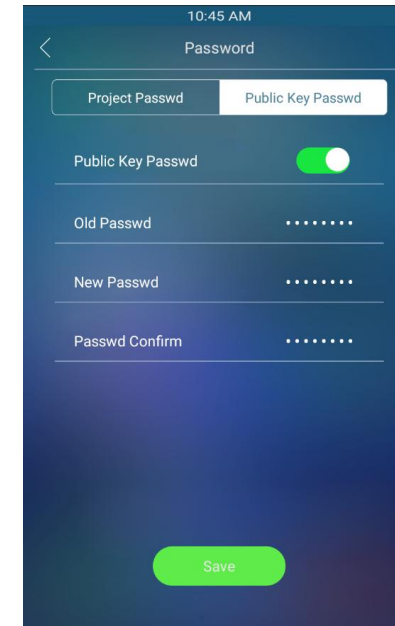


Figure 3.8.3.3 Public key

Password			
PublicKey Enable	ON	PublicKey Bits Limit	Default(8 Bits)
PublicKey_0	33333333	PublicKey_1	66666666
PublicKey_2	88888888	ProjectKey	9999

Figure 3.8.3.4 Password

3.8.4. Unlock via Face

3.8.4.1. Face in Device

Comparing with the previous access method, face recognition is so convenient that user do not need to remember the pin code or take a card. Enter device access system, click **Face** in the last page to do face registration and modification.

Register:

Please enter the face registration name and click “Register” to save the user information. Then stand in front of the camera of R29 0.5m-1m and align in the middle of the circle box on the screen until the 10s. If the face is recognized, the face ID will be automatically admitted. Or the administrator can use FacePro to import a large number of face data. Please refer to FacePro user manual for more configurations.

Note: Akuvox recommends to use the FacePro to manage the face data. It is also convenient to maintenance when firmware

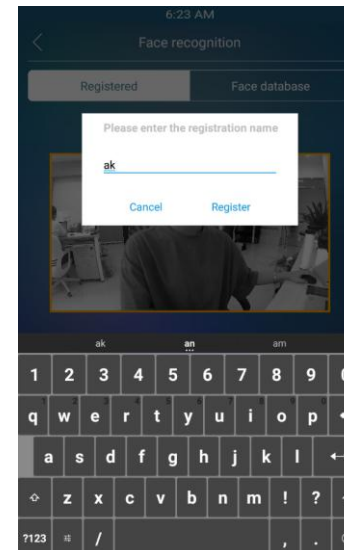


Figure 3.8.4.1-1 Face recognition

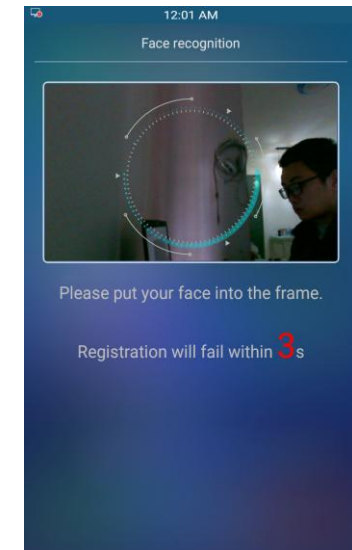


Figure 3.8.4.1-2 Face recognition

upgrading.

Modify:

Click **Face database**, choose the existed database to delete

3.8.4.2. Face in Website

Click **Intercom-Face-Face Basic** on the device web interface to configure the face parameters and information.

Face Recognition: Click **Enable** to turn on the face recognition feature. This option is enabled by default.

Offline Learning: The device will compare with the existed face data via scanning face every time. Then automatically learning and improving your face characteristic. So the common change in your face will not affect the recognition. But this feature is depending on the frequency of scanning face. If using often, the device will learn more accurately.

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

- Face Recognition: Enable
- Offline Learning: Enable
- Recognize Option: Normal
- Antispoofing Option: Normal
- Facial Recognition Interval: 5

Figure 3.8.4.2-1 Face basic

Recognize Option: : It is divided into 4 levels -Low, Normal, High or Highest. The higher level, the lower error recognition rate without live detection.

Antispoofing Option: It is divided into 4 levels -Low, Normal, High or Highest. The higher level, the lower error recognition rate with live detection.

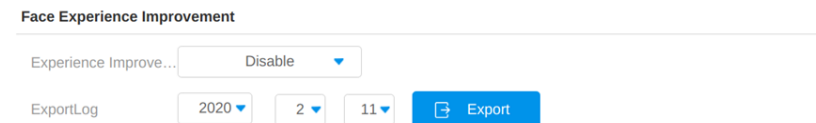
Facial recognition Interval: The interval between the two face recognitions. The maximum interval time is 8s.

Face Experience Improvement

In order to improve a better face recognition user experience, we will collect your data and debug information and upload to our cloud in specific time every day.

Face Experience Improvement: users can choose to enable or disable this function.

ExportLog: Choose a suitable day to export the data and debug information of this interval



The screenshot shows a web interface titled "Face Experience Improvement". It contains two main sections. The first section, "Experience Improve...", has a dropdown menu currently set to "Disable". The second section, "ExportLog", includes three dropdown menus for selecting a date and time: "2020", "2", and "11". To the right of these dropdowns is a blue button with a document icon and the text "Export".

Figure 3.8.4.2-2 Face experience improvement

Tips When Succeed: You can click to select “Default” door unlock success notification “Opening Door Succeeded” or you can click “Resident Name” to change the notification to the names registered for the facial recognition.

Face Setting

Lift Floor Number: Combining the face data with the corresponding floor, face data should belong to an existing contact , so the name of face must be same with the corresponding contact. When someone scans face, the device will match the face with the floor number, then release the floor button.

Face Management

You can manage your face data by importing or exporting the face data. The export format is .tgz while the import formate is .zip.

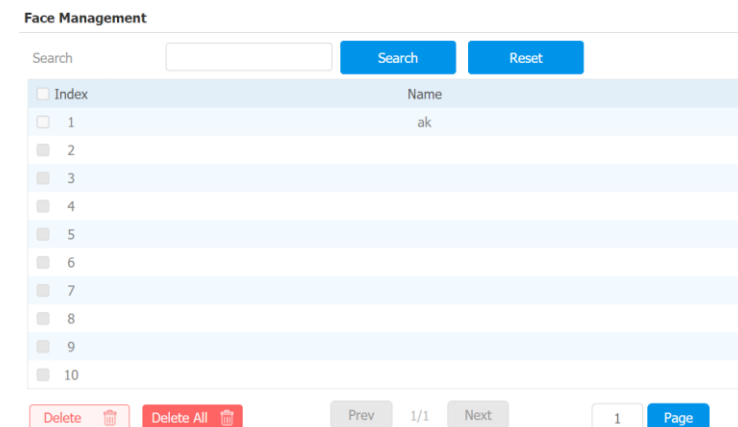
Search: Enter key word to quick search the exited face data from the list.



Face Setting

Lift Floor Number 0 Edit

Figure 3.8.4.2-3 Face setting



Face Management

Search Search Reset

Index	Name
1	ak
2	
3	
4	
5	
6	
7	
8	
9	
10	

Delete Delete All Prev 1/1 Next 1 Page

Figure 3.8.4.2-4 Face Management

Import/Export file: Because R29 series can not support the third party camera to enter the face picture now. Users need to directly retrieve face data in the R29 series, then export them the existing face file. It is convenient to share the same face data in multiple devices.

3.8.5. Unlock via QR code

On the portal **Intercom - Relay - Open Relay via QR**. Enable the QR function.

Note: This function should be work with Akuvox cloud. For more information, please contact with your administrators.

3.8.6. Unlock via Bluetooth(Optional)

On the portal **Intercom - BLE**.

BLE Enable: Enable or diable the BLE function.

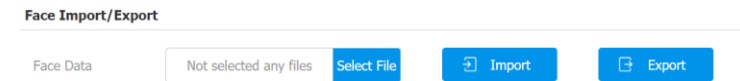


Figure 3.8.4.2-5 Face import/export

Open Relay via QR



Figure 3.8.5 Open relay via QR

BLE Basic

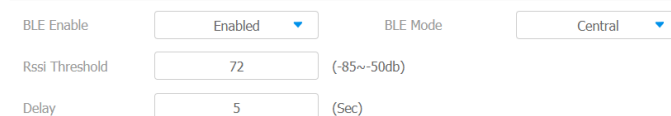


Figure 3.8.6 BLE

BLE Mode: To configure the BLE mode.

Rssi Threshold: Set the threshold of received signal strength indicator. The smaller absolute value ,the higher sensitivity.

Delay: To configure the duration of opened relay. Over the value, the relay would be closed again.

Note: This function needs to be used with Akuvox cloud, please contact your administrator for more information.

3.8.7. Unlock via Fingerprint(Optional)

Go to the path **Intercom - Fingerprint** on the web GUI, to manage finger keys access system.

Finger Key Setting:

- (1)Select the valid day and time;
- (2)Choose which door users want to open;
- (3)Enter the “Finger Name”. Lift Floor Number is optional.
- (4)Click **Obtain**, press your finger on device to record the fingerprint for three times;
- (5)Click **Add** to add this finger key.

Finger Key Setting

Finger DoorNum ☒ RelayA ☐ RelayB ☐ RelayC

Finger Day ☒ Mon ☒ Tue ☒ Wed ☒ Thur
☒ Fri ☒ Sat ☒ Sun ☐ Check All

Finger Time 00 : 00 - 00 : 00

Finger Name Lift Floor Number 0

Obtain **Add**

Please press to record the first fingerprint.

Figure 3.8.7-1 Finger key setting

Finger Key Management:

Valid finger key information will be shown in the list. Administrator could delete finger key information or empty all the list.

3.8.8. Unlock via HTTP Command

Login to the website and go to the path **Intercom - Relay - Open Relay via HTTP** to configure. Users can use a URL to remotely unlock the door. It is more convenient for users to open the door if users are not beside the devices.

Switch: Enable this function. Disable by default.

Username & Password: Users can setup the username and password for HTTP unlock.

URL format:

http://IP_address/fcgi/do?action=OpenDoor&UserName=XX&Password=XX&DoorNum=XX

Finger Key Management

	Index	Name	Code	UserID	Relay	FloorNum
☐	1	Eve	1		123	
☐	2					

Figure 3.8.7-2 Finger key management

Open Relay via HTTP

Enable	ON	UserName	admin
Password	*****		

Figure 3.8.8 Open relay via HTTP

3.8.9. Unlock via Exit Button

R29 series supports 3 input triggers Input A/B/C (DOORA/B/C). Login to the website and go to the path **Intercom - Input** to configure.

Input Service: To enable or disable input trigger service.

Trigger Option: To choose open circuit trigger or closed circuit trigger. “Low” means that connection between door terminal and GND is closed, while “High” means the connection is opened.

Door Status: To show the status of input signal.

The screenshot shows the 'Input A' configuration page. It includes a title bar 'Input A'. Below it, there are several configuration fields: 'Input Service' with a dropdown set to 'Enable'; 'Trigger Option' with a dropdown set to 'Low'; 'Action To Execute' with four checkboxes for FTP, Email, HTTP, and TFTP, all of which are unchecked; 'Http URL' with an empty text input field; 'Action Delay' with a text input set to '0' and a note '(0~300 Sec)'; and 'Open Relay' with a dropdown set to 'RelayA'. To the right of the 'Open Relay' dropdown, the text 'Door Status' and 'DoorA: High' are displayed.

Figure 3.8.9 Input

3.8.10. Unlock via Reception in Building Theme

On building theme, users can unlock the relay through pressing Reception.

Dial Type: Select the dial account, which supported account 1 or account 2;

Open Relay: When users press reception icon to call, the relay is

The screenshot shows the 'Reception Action In Building' configuration page. It has a title bar 'Reception Action In Building'. Below it, there are two main configuration areas: 'Dial Type' with a dropdown set to 'Default', and 'Open Relay' with a dropdown set to 'RelayA'.

Figure 3.8.10. Reception action in building

triggered.

Note: This feature is often to trigger the signal via relay terminal.

3.9. Reboot

In the phone interface, go to **Reboot** to click the **Reboot**, or go to the path **Upgrade - Basic** on the web GUI, click **Submit**, the device will restart.

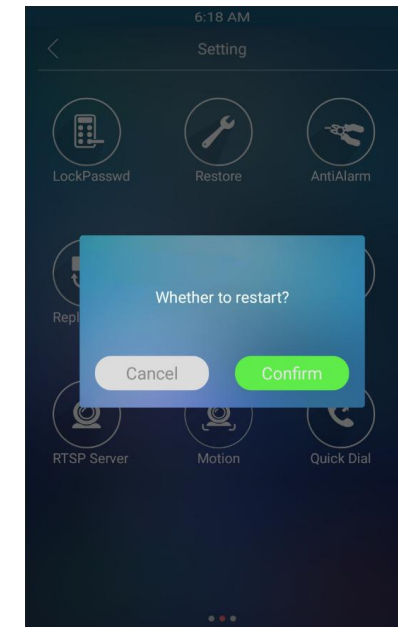


Figure 3.9-1 Reboot

Reboot



Figure 3.9-2 Reboot

3.10. Reset

In the phone interface, go to **Restore**. Click **Restore**, if users sure to restore to factory settings, please choose **Confirm** in the prompt window.

Users can also login to the website and go to the path **Upgrade - Basic**, directly click **Submit** to reset R29 series. Use this function with caution. All configuration will be removed.

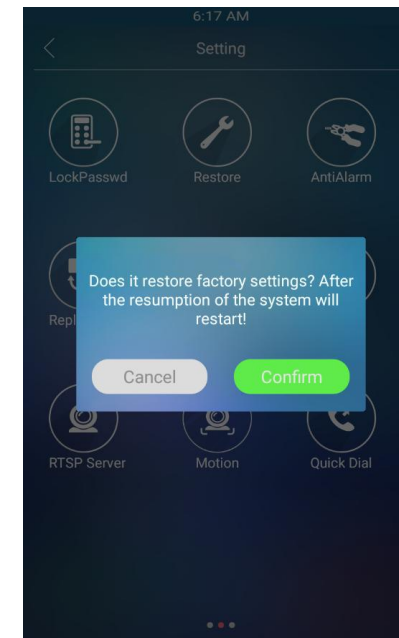


Figure 3.10-1 Restore

Reset To Factory Setting

Submit

Figure 3.10-2 Reset

4. Advanced Features

4.1. Phone Configuration

4.1.1. IR LED

The setting is for night vision, when the surrounding of R29 series is very dark, infrared LED will turn on and R29 series will turn to night mode to let the users see video clearly from the R29.

In the phone interface, go to **LED** or go to the path **Intercom - Advanced - LED** on web GUI, to configure the IR LED function.

Led Type: It can supports four modes - OFF, ON, AUTO, SCHEDULE.

If setup the LED type as auto, click **Threshold button** to sense the intensity of the current environment.

Threshold: Click the **Threshold key**, it will automatic show the

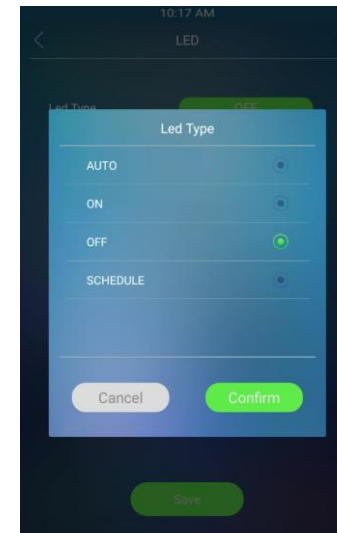


Figure 4.1.1-1 LED type

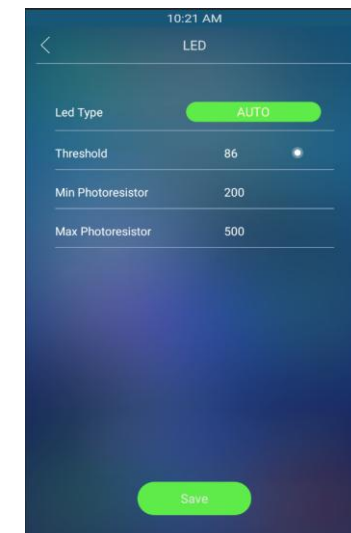


Figure 4.1.1-2 LED auto

R29C-L

Admin Guide

current intensity or user can setup the value manually. Once the environment intensity is darker than the predefined threshold value, LED will be up.

Min/Max photoresistor: Photoresistor value relates to light intensity and larger value mean that light intensity is smaller. When photoresistor value is greater than max value, LED will turn on. In contrast, when photoresistor value is less than min value, infrared LED will turn off and the device turns to normal mode.

If setup the LED type as schedule, click **Threshold button** to sense the intensity of the current environment.

Time Start/Stop: In the meantime, the R29 is forced to turn on LED.

Users can also configure the LED from website, go to the path **Intercom - Advanced - LED**.

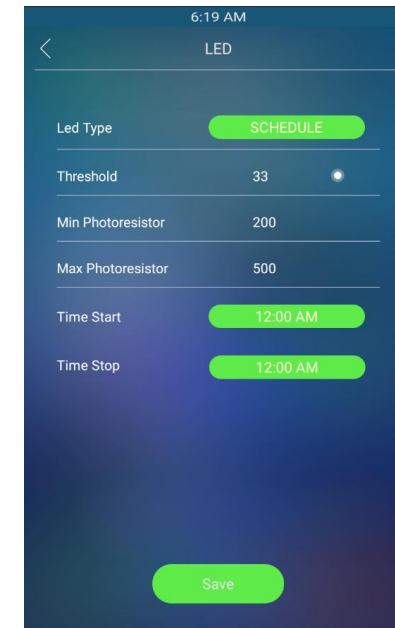


Figure 4.1.1-3 LED schedule

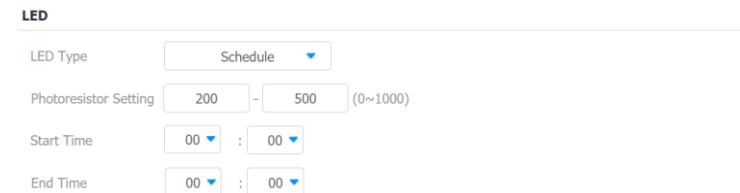


Figure 4.1.1-4 LED

4.1.2. LED of Display

Login to the website and go to the path **Intercom - LED Setting - LED Control** to configure.

Card LED Enable: To control the LED of the card reader area.

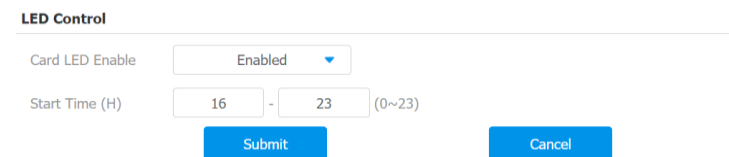
Start Time (H): Setup the LED light up time. According to the system time. For example 18-23 means the LED will continuously light up from 6:00pm to 11:00pm.

4.1.3. High Contrast of LCD

This function is used to automatically adjust the brightness of R29C-L LCD according to the brightness of the surrounding environment.

High Contrast: Enable/Disable the LCD high contrast function.

Backlight Mode: To choose how the doorphone adjust the



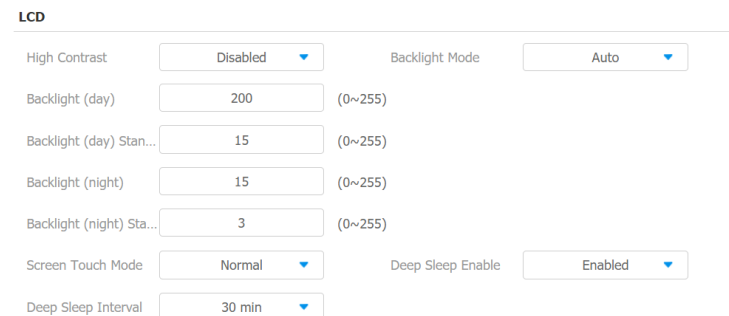
LED Control

Card LED Enable: Enabled

Start Time (H): 16 - 23 (0~23)

Submit Cancel

Figure 4.1.2 LED control



LCD

High Contrast: Disabled

Backlight Mode: Auto

Backlight (day): 200 (0~255)

Backlight (day) Stan...: 15 (0~255)

Backlight (night): 15 (0~255)

Backlight (night) Sta...: 3 (0~255)

Screen Touch Mode: Normal

Deep Sleep Enable: Enabled

Deep Sleep Interval: 30 min

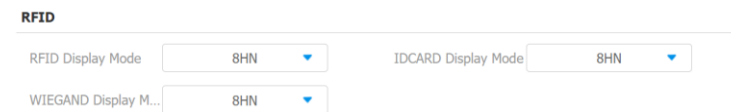
Figure 4.1.3 LCD

backlight. There are two types for users, Auto and Manual.

4.1.4. RFID Card Code Display Related

Login to the website and go to the path **Intercom - Advanced - RFID** to configure.

Display Mode: To be compatible different card number formats in different systems. The default 8HN means hexadecimal.



The screenshot shows the 'RFID' configuration section. It contains three dropdown menus: 'RFID Display Mode' set to '8HN', 'IDCARD Display Mode' set to '8HN', and 'WIEGAND Display M...' set to '8HN'.

Figure 4.1.4 RFID

4.2. Intercom

4.2.1. Call Time Related

4.2.1.1. RTP timeout

RTP Timeout: Login to the website and go to the path **Intercom -**

Door Setting General

RTP TimeOut

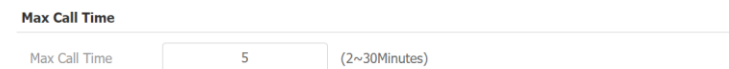
20

Figure 4.2.1.1 RTP timeout

Basic - Door Setting General to configure. This feature is specially designed for R47P. When R47P auto answer in mute status, if over the configured time R29 series did not receive the RTP message, R29 series will hang up automatically.

4.2.1.2. Max call time

Max Call Time: Login to the website and go to the path **Intercom - Basic - Max Call Time** to configure the max call time.



Max Call Time	
Max Call Time	5 (2~30Minutes)

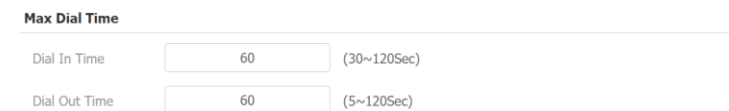
Figure 4.2.1.2 Max call time

4.2.1.3. Max dial time

Login to the website and go to the path **Intercom - Basic - Max Dial Time** to configure the max dial time.

Dial In Time: To configure the max incoming dial time, available when auto answer is disabled.

Dial Out Time: To configure the max no answer call time.



Max Dial Time	
Dial In Time	60 (30~120Sec)
Dial Out Time	60 (5~120Sec)

Figure 4.2.1.3 Max dial time

4.2.1.4. Hang up after open door

Login to the website and go to the path **Intercom - Basic - Hang Up After Open Door**.

Time Out: When the callee press the DTMF code to open the door, this call will hang up automatically after the timeout.



Hang Up After Open Door

Time Out (0~15Sec)

Figure 4.2.1.4 time our

4.2.2. Return Code When Refused

Login to the website and go to **Phone - Call Feature - Others** to configure.

Return Code When Refuse: Allows users to assign specific code as return code to SIP server when an incoming call is rejected.



Others

Return Code When ...

Figure 4.2.2 Return code when refused

4.2.3. SIP Call Related

Login to the website and go to the path **Account - Advanced - Call** to configure the SIP call related functions.

Max Local SIP Port: To configure maximum local SIP port for

designated SIP account.

Min Local SIP Port: To configure minimum local SIP port for designated SIP account.

Caller ID Header: To choose caller ID header format automatically.

Anonymous Call: If enabled, R29 series will block its information when calling out.

Anonymous Call Rejection: If enabled, calls who block their information will be screened out.

Missed Call Log: If enabled, any missed call will be recorded into call log.

Prevent SIP Hacking: If enabled, it will prevent sip message from hacking

4.2.4. Call Waiting

Login to the website and go to the path **Phone - Call Feature - Call Waiting** to configure.

Call Waiting Enable: If enabled, it allows IP phones to receive a

Call	
Max Local SIP Port	45505 (1024~65535)
Min Local SIP Port	45495 (1024~65535)
Caller ID Header	RPID-FROM
Auto Answer	Enabled
Provisional Responses...	Disabled
Register with user=...	Disabled
Invite with user=ph...	Disabled
Anonymous Call	Disabled
Anonymous Call Rej...	Disabled
Missed Call Log	Enabled
Prevent SIP Hacking	Enabled

Figure 4.2.3 SIP call related

Call Waiting	
Call Waiting Enable	Disabled
Call Waiting Tone	Enabled
On Code	
Off Code	

Figure 4.2.4 Call waiting

new incoming call when there is already an active call.

Call Waiting Tone: If enabled, it allows IP phones to play the call waiting tone to the waiting callee.

On Code: The code used to enable call waiting on server's side, if configured, IP phone will send a SIP message to server to turn on call waiting on server side if user setup calls waiting is disabled.

Off Code: The code used to disable call waiting on server's side, if configured, IP phone will send a SIP message to disable call waiting on server side if user setup call waiting is enabled.

4.2.5. Intercom

Intercom allows users to establish a call directly with the callee. Login to the website and go to the path **Phone - Call Feature - Intercom** to configure.

Active: To enable or disable Intercom feature.

Intercom Mute: If enabled, once the call established, the callee will be muted.

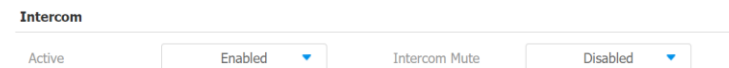


Figure 4.2.5 Intercom

4.2.6. Codec

Login to the website and go to the path **Account - Advanced** to configure the video codec and audio codec.

● Audio Codec

Sip Account: To choose which account to configure.

Audio Codec: R29 series supports four audio codec: PCMA, PCMU, G729, G722. Different audio codec requires different bandwidth, user can enable/disable them according to different network environment.

Note: Bandwidth consumption and sample rates.

Codec	Bandwidth	Sample Rates
PCMA	64kbit/s	8kHz
PCMU	64kbit/s	8kHz
G729	8kbit/s	8kHz
G722	64kbit/s	16kHz

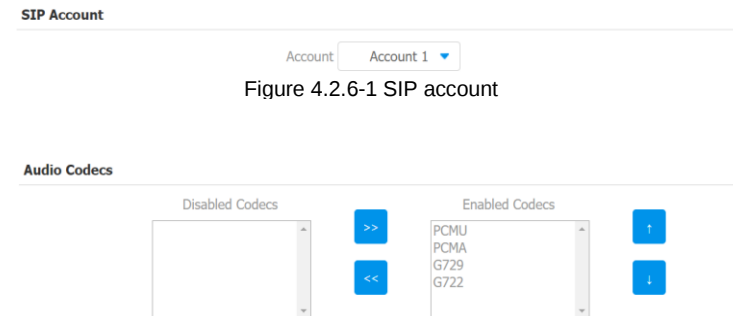


Figure 4.2.6-2 Audio codec

● Video Codec

R29 series supports H264 standard, which provides better video quality at substantially lower bit rates than previous standards.

Codec Resolution: R29 series supports four resolutions: QCIF, CIF, VGA, 4CIF and 720P.

Codec Bitrate: To configure bit rates of video stream.

Codec Payload: To configure RTP audio video profile

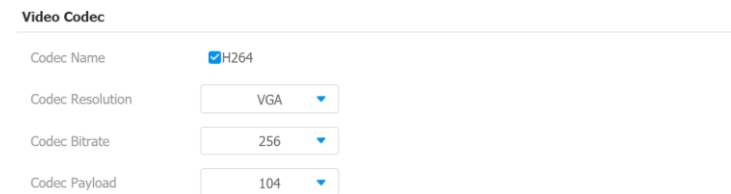
4.2.7. DTMF

Login to the website and go to the path **Account - Advanced - DTMF** to configure RTP audio video profile for DTMF and its payload type.

Type: Support Inband, Info, RFC2833 or their combination.

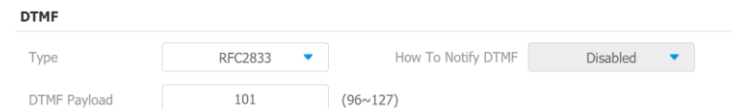
How To Notify DTMF: Only available when DTMF type is Info.

DTMF Payload: To configure payload type for DTMF.



The screenshot shows the 'Video Codec' configuration page. It has a title bar 'Video Codec'. Below it, there are four rows of configuration options: 'Codec Name' with a checked checkbox for 'H264', 'Codec Resolution' with a dropdown menu showing 'VGA', 'Codec Bitrate' with a dropdown menu showing '256', and 'Codec Payload' with a dropdown menu showing '104'.

Figure 4.2.6-3 Video codec

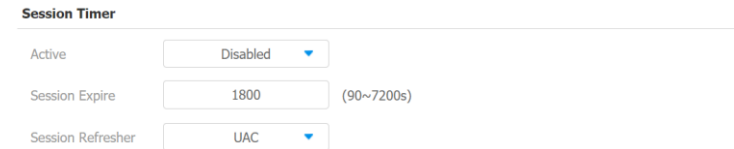


The screenshot shows the 'DTMF' configuration page. It has a title bar 'DTMF'. Below it, there are two rows of configuration options: 'Type' with a dropdown menu showing 'RFC2833' and 'How To Notify DTMF' with a dropdown menu showing 'Disabled'. Below these, there is a 'DTMF Payload' section with a text input field containing '101' and a label '(96~127)'.

Figure 4.2.7 DTMF

4.2.8. Session Timer

Go to the path **Account - Advanced - Session Timer** on the web GUI to configure. If enabled, the on going call will be disconnected automatically once the session expired unless it's been refreshed by UAC or UAS.



Session Timer		
Active	Disabled ▼	
Session Expire	1800	(90~7200s)
Session Refresher	UAC ▼	

Figure 4.2.8 Session timer

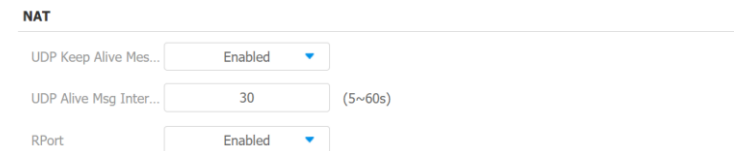
4.2.9. NAT

Login to the website and go to the path **Account - Advanced - NAT** to configure.

UDP Keep Alive Messages: The phone will send UDP keep-alive message periodically to router to keep NAT port alive.

UDP Alive Msg Interval: Keep alive message interval.

Rport: It will add remote port into outgoing SIP message for designated account.



NAT		
UDP Keep Alive Mes...	Enabled ▼	
UDP Alive Msg Inter...	30	(5~60s)
RPort	Enabled ▼	

Figure 4.2.9 NAT

4.2.10. User Agent

Login to the website and go to the path **Account - Advanced - User Agent** to configure.

User Agent: One can customize users agent field in the SIP message; if user agent is set to specific value, users can see the information from PCAP. If user agent is not set by default, users can see the company name, model number and firmware version from PCAP.

4.2.11. HTTP API

HTTP API configurations for Akuvox intercom are defined via web interface path: **Intercom - HTTP API** to disable/enable a service and select the user authentication method.

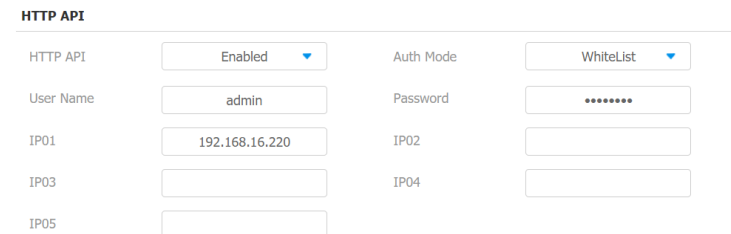
HTTP API: To enable/disable the service. If disable, system always return HTTP 403 Forbidden status when users sends the request.

Auth Mode: There are six auth modes: None, Normal, WhiteList,



User Agent

Figure 4.2.10 User Agent



HTTP API

HTTP API	Enabled	Auth Mode	WhiteList
User Name	admin	Password	*****
IP01	192.168.16.220	IP02	
IP03		IP04	
IP05			

Figure 4.2.11 HTTP API

Basic, Digests, Token.

Username/Password: Used in basic and digest auth mode. The default username/password is **admin/httpapi**.

IP01~05: Configure the white list IP.

None	No authentication is required for http api, it is only used by demo testing.
Normal	(reserved)
WhiteList	The whitelist is suitable for operation in the LAN, by judging the IP address of the visitor to confirm whether to allow access to the HTTP API.
Basic	In Authorization field of Http request header, use Base64 encode method for the information of username and password.
Digests	Password encryption method, only supports MD5. In Authorization field of Http request header: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
Token	(reserved)

4.3. Access control

4.3.1. Webrelay

R29 series supports extra web relay. This function is more safety to use DTMF code to remote unlock. Login to the website and go to the path **Phone - Web Relay** to configure.

- **Web Relay**

Type: Connect web relay and choose the type.

IP Address: Enter web relay IP address.

User Name: It is an authentication for connecting web relay.

password: It is an authentication for connecting web relay.

Note: Users can modify username and password in web relay website.

- **Web Relay Action Setting**

Web Relay Action: Web relay action is used to trigger the web relay. The action URL is provided by web relay vendor

Web Relay Key: If the DTMF keys same as the local relay, the web

Web Relay

Type	Disabled ▼	IP Address	
UserName		Password	*****

Figure 4.3.1-1 Web relay

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01			
Action ID 02			
Action ID 03			
Action ID 04			
Action ID 05			

Figure 4.3.1-2 Web relay action setting

relay will be open with local relay. But if there are different, the web relay is invalid.

Web Relay Extension: The webrelay can only receive the DTMF signal from the corresponding extension number.

4.3.2. Wiegand

Login to the website and go to the path **Intercom - Advanced - Wiegand** to configure.

Wiegand Type: Support Wiegand 26,34,58. The different number means different bits.

Wiegand Mode: Input or output. Typically, when you select input, we generally connect the wiegand input device, such as the wiegand card reader. Or R29 series can be used as output, It is generally used to connect the third-party Access Control, then R29 series change the card information as wiegand signal, then transfer to the access control module.

The screenshot shows a configuration page titled "Wiegand". It contains five settings, each with a label and a dropdown menu:

- Wiegand Type:** Set to "Wiegand-26".
- Wiegand Mode:** Set to "Input".
- Wiegand Input Order:** Set to "Normal".
- Wiegand Output Or...:** Set to "Normal".
- Wiegand Output CRC:** Set to "ON".

Figure 4.3.2 Wiegand

Wiegand Input/Output Order: To make the data from wiegand devices to be normal order or reversed order.

Wiegand Output CRC: To be compatible with the other three party wiegand access control which do not use the standard wiegand order, CRC can correct the order format.

4.4. Security

4.4.1. Antialarm of Door Phone

4.4.1.1. Antialarm in device

In the phone interface, go to **AntiAlarm** to configure it.

This function is used to trigger the alarm by perceiving the change of gravity. After the door phone has been installed, administrator can enable Antialarm function. if the device is moved illegally, the gravity of R29 series are different from the original status, then the device will ring alarm bell and send out the call to the predefined

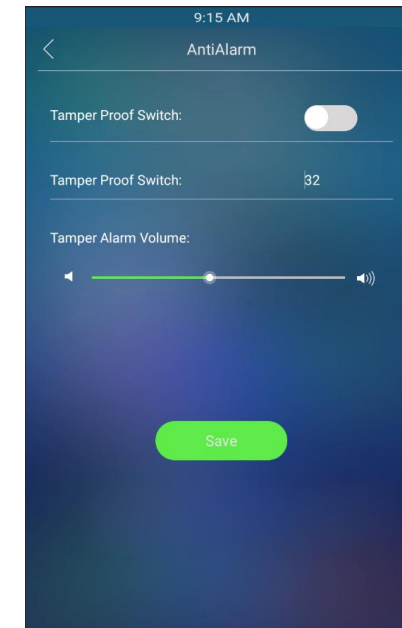


Figure 4.4.1.1 Antialarm

location. The detailed gravity sensor value can be adjusted in website.

Tamper Proof Switch: Switch this feature.

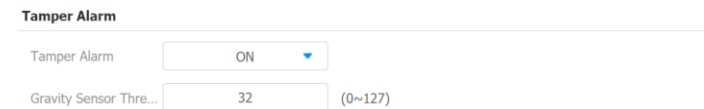
Tamper Proof Switch: The smaller the value, the more sensitive the gravity sensor is.

Tamper Alarm Volume: To configure the tamper alarm volume.

4.4.1.2. Antialarm in website

Login to the website and go to the path **Intercom - Advanced - Tamper Alarm** to configure.

R29 series integrates internal gravity sensor for the own security, and after enabling tamper alarm, if the gravity of R29 series changes dramatically, the phone will alarm. Gravity sensor threshold stands for sensitivity of sensor.



Tamper Alarm

Tamper Alarm ON

Gravity Sensor Thre... 32 (0~127)

Figure 4.4.1.2 Tamper alarm

4.4.2. Motion

4.4.2.1. Motion in device

In the phone interface, go to **Motion** to configure. By enabling the motion detection function, the door phone will detect and record any change in the surrounding, such as suspicious people loitering around, and send notification message to a monitor unit.

Timing setting

If users only enable time mode and setup the interval. R29 series will take the picture in every interval time;

Only enable detection mode, R29 series will capture if there is any change of surrounding in the detection time;

Enable timing mode and detection mode in the same time, if there is no any change of surrounding, R29 series will capture in the interval time. Otherwise, the device will take the picture in detection mode.

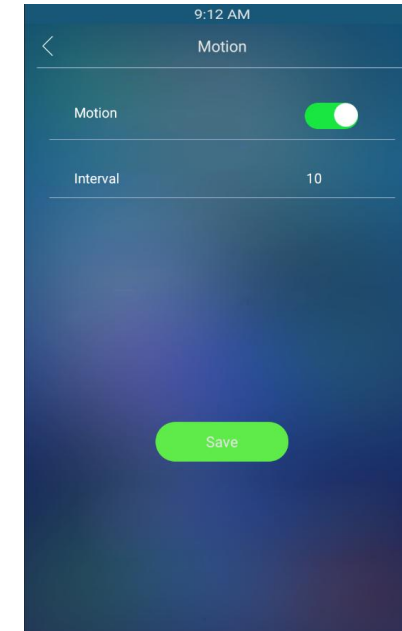


Figure 4.4.2.1 Motion

4.4.2.2. Motion in website

Login to the website and go to the path **Intercom - Motion - Motion Detection Options** to configure.

Enable: To enable or disable motion detection.

Timing Interval: R29 series will take the picture in the interval time.

Detection Accuracy: The smaller value, the capture picture is more accurate.

After you setup motion, to configure the target address where to receive the pictures.

4.4.3. Action

Login to the website and go to the path **Intercom - Action** to configure the action related features.

4.4.3.1. Email Notification

The capture will be send to the predefined email address or FTP

Motion Detection Options	
Enable	ON
Timing Interval	10 (0~65535 Seconds)
Detection Accuracy	20

Figure 4.4.2.2 Motion detection options

Email Notification			
Sender's email address	Evelyn.zhang@akuvox.com	Email SendName	Evelyn
Receiver's email address	Akuvox@Akuvox.com	Email RecvName	Akuvox
SMTP server address	smtp.exmail.qq.com	Port	554
SMTP user name	Evelyn.zhang@akuvox.com	SMTP password	*****
Email subject	test		
Email content	test		

path. It is useful for users to check the capture picture for security.

Sender's email address: To configure email address of sender.

Receiver's email address: To configure email address of receiver.

SMTP server address: To configure SMTP server address of sender.

SMTP user name: To configure user name of SMTP service (usually it is same with sender's email address).

SMTP password: To configure password of SMTP service (usually it is same with the password of sender's email).

Email subject: To configure subject of email.

Email content: To configure content of email.

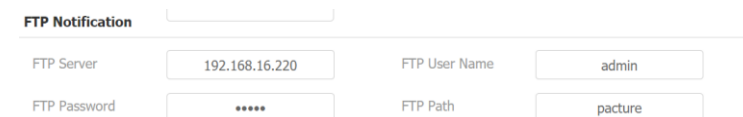
Email Test: To test whether email notification is available.

4.4.3.2. FTP Notification

FTP Server: To configure URL of FTP server.

FTP User Name: To configure user name of FTP server.

FTP Password: To configure password of FTP server.



The screenshot shows a configuration form titled "FTP Notification". It contains four input fields arranged in a 2x2 grid. The first row contains "FTP Server" with the value "192.168.16.220" and "FTP User Name" with the value "admin". The second row contains "FTP Password" with masked characters "*****" and "FTP Path" with the value "picture".

FTP Notification			
FTP Server	192.168.16.220	FTP User Name	admin
FTP Password	*****	FTP Path	picture

Figure 4.4.3.2 FTP notification

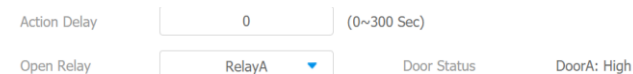
FTP Path: Enter the folder name you created in FTP server.

4.4.3.3. Input Interface Triggered Action

Go to the path **Intercom - Input** on the website to configure.

Action Delay: To configure after how long to execute to send out notifications and trigger relay.

Open Relay: To configure which relay to trigger.



Action Delay	0	(0~300 Sec)
Open Relay	RelayA ▼	Door Status DoorA: High

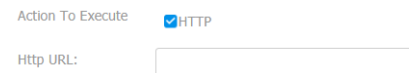
Figure 4.4.3.3 Input interface triggered action

4.4.3.4. Reception Action In Building

On the path **Intercom - Key/Display - Reception Action In Building**.

Action To Execute: To select the action when users press reception.

HTTP URL: If users choose HTTP mode, enter the URL format:
http://http server IP address/any information.



Action To Execute	☒ HTTP
Http URL:	

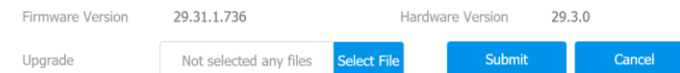
Figure 4.4.3.4 Reception action in building

4.5. Upgrade

4.5.1. Web Update

Login to the website and go to the path **Upgrade - Basic**, users can upgrade firmware.

Upgrade: Choose .zip/.rom firmware from your PC, then click **Submit** to start update.



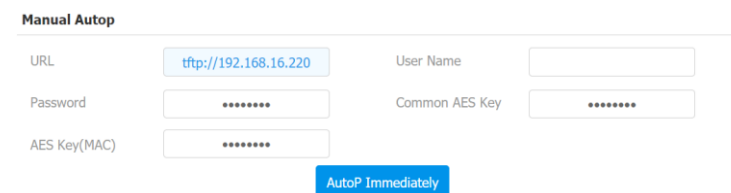
Firmware Version	29.31.1.736	Hardware Version	29.3.0
Upgrade	Not selected any files Select File Submit Cancel		

Figure 4.5.1 Web update

4.5.2. Autop Upgrade

Login to the website and go to the path **Upgrade - Advanced** to configure.

- **Manual Autop**



Manual Autop			
URL	ftp://192.168.16.220	User Name	
Password	*****	Common AES Key	*****
AES Key(MAC)	*****		
AutoP Immediately			

Figure 4.5.2-1 Manual Autop

Autop is a centralized and unified upgrade of IP telephone. It is a simple and time-saving configuration for IP phone. It is mainly used by the device to download corresponding configuration document from the server using TFTP / FTP / HTTP / HTTPS network protocol. To achieve the purpose of updating the device configuration, making the user to change the phone configuration more easily. This is a typical C/S architecture upgrade mode, mainly by the terminal device or PBX server to initiate an upgrade request.

URL: Auto provisioning server address.

User name: Configure if server needs an username to access, otherwise left blank.

Password: Configure if server needs a password to access, otherwise left blank.

Common AES Key: Used for IP phone to decipher common Auto Provisioning configuration file.

AES Key (MAC): Used for IP phone to decipher MAC-oriented auto provisioning configuration file (for example, file name could be

0c1105888888.cfg if IP phone's MAC address is 0c1105888888).

Note: AES is one of many encryption, it should be configured only when configure file is ciphered with AES, otherwise left blank.

● Automatic Autop

To display and configure Auto Provisioning mode settings.

This Auto Provisioning mode is actually self-explanatory.

For example, mode “Power on” means IP phone will go to do Provisioning every time it powers on.

● DHCP Option

To display and configure DHCP setting for AutoP. Option 66/43 is enable by default. It can support Https, Http, Ftp, Tftp server.

Customer Option: Enter the server URL. Click **Submit** to save.

4.5.3. Backup Config File

Go to the path **Upgrade - Advanced - Others** to backup the config file.

Others: To export current config file or import new config file.

The screenshot shows the 'Automatic Autop' configuration section. It includes a 'Mode' dropdown set to 'Power On', a 'Schedule' dropdown set to 'Sunday', and a time selection area with '22' for hours and '0' for minutes. Below these are buttons for 'Clear MD5' (Submit), 'Export Autop Templ...' (Export), and a 'Cancel' button.

Figure 4.5.2-2 Automatic Autop

The screenshot shows the 'DHCP Option' configuration section. It features a 'Custom Option' input field with a range of '(128~254)' and a note stating '(DHCP Option 66/43 is Enabled by Default)'.

Figure 4.5.2-3 DHCP option

The screenshot shows the 'Others' configuration section. It includes a 'Config File(.tgz/.con...)' field with a 'Select File' button. Below are buttons for 'Export' (labeled '(Encrypted)'), 'Import', and a 'Cancel' button.

Figure 4.5.3-1 Config

Note: The exported config here is encrypted.

Users can also go to the path **Phone - Import/Export - Import/Export Config&Contact** to export or import the config. Click **Export** to export the config file.

4.6. Log

4.6.1. Call Log

Login to the website and go to the path **Phonebook - Call Log**, users can see a list of call which have dialed, received or missed. And user can delete calls from list.

Call Log						
Call History		All	Active		Enabled	Export
Time		mm/dd/yyyy	-	mm/dd/yyyy	Name/Number	Filter
☐ Index	Type	Date	Time	Local Identity	Name	Number
☐ 1	Received	2019-06-04	06:06:25	106100212@47 .91.73.215:5 070	106100185	106100185@47 .91.73.215:5 070
☐ 2	Dialed	2019-06-04	06:05:19	106100212@47 .91.73.215:5 070	106100185	106100185@47 .91.73.215:5 070
☐ 3	Dialed	2019-06-04	06:05:13	106100212@47 .91.73.215:5 070	106100188	106100188@47 .91.73.215:5 070

Figure 4.6.1 Call log

4.6.2. Door Log

Login to the website and go to the path **Phone - Door Log**, users can see a list of door log which records card information and date.

4.6.3. System Log

Go to the path **Upgrade - Advanced - System Log** on web GUI. To display system log level and export system log file.

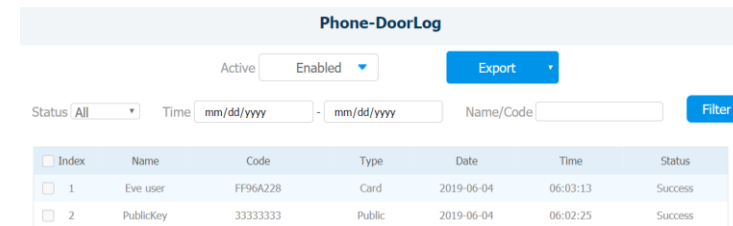
System Log Level: From level 0 to 7. The higher level means the more specific system log is saved to a temporary file. By default, it's level 3.

Export Log: Click to export temporary system log file to local PC.

Export Debug log: Click to export the debug log file to local PC.

Remote System Log: Enable/Disable remote system log.

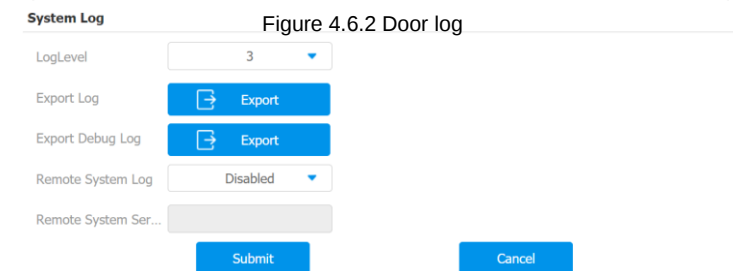
Remote System Server: Configure a server address to receive devices log remotely.



The screenshot shows the 'Phone-DoorLog' interface. At the top, there's a header 'Phone-DoorLog'. Below it, there are controls for 'Active' (set to 'Enabled') and an 'Export' button. Further down, there are filters for 'Status' (set to 'All'), 'Time' (with date pickers for 'mm/dd/yyyy'), and 'Name/Code', followed by a 'Filter' button. The main part of the interface is a table with the following data:

☐	Index	Name	Code	Type	Date	Time	Status
☐	1	Eve user	FF96A228	Card	2019-06-04	06:03:13	Success
☐	2	PublicKey	33333333	Public	2019-06-04	06:02:25	Success

Figure 4.6.2 Door log



The screenshot shows the 'System Log' configuration interface. It includes a 'LogLevel' dropdown menu currently set to '3'. Below this are two buttons for 'Export Log' and 'Export Debug Log', each with a download icon and an 'Export' label. There is a 'Remote System Log' dropdown menu set to 'Disabled'. At the bottom, there is a text input field for 'Remote System Ser...' and two buttons, 'Submit' and 'Cancel'.

Figure 4.6.3 System log

4.6.4. PCAP

Go to the path **Upgrade - Advanced - PCAP** on web GUI. To start, stop packets capturing or to export captured Packet file.

Start: To start capturing all the packets file sent or received from IP phone.

Stop: To stop capturing packets.

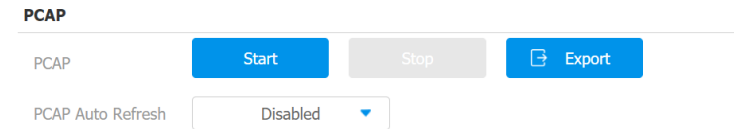


Figure 4.6.4 PCAP

Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical Provisioning

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

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

SIP: Session Initiation Protocol

SNMP: Simple Network Management Protocol

STUN: Session Traversal Utilities for NAT

SNMP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

WG: Wiegand

Contact us

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

Sales email: sales@akuvox.com

Technical support email: techsupport@akuvox.com

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



We highly appreciate your feedback about our products.

FCC Statement:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.