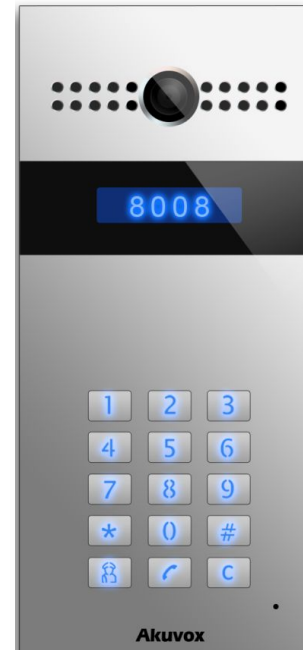




**R27A**



**R27C**

## **R27 Series Door Phone Admin Guide**

## About This Manual

Thank you for choosing Akuvox's R27A/C door phone. This manual is intended for end users who need to properly configure the door phone. This manual is applicable to 27.0.3.xx version, and it provides all functions' configurations of R27A/C. 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

<b>1. Product Overview.....</b>	<b>1</b>
1.1. Product Description.....	1
1.2. Connector Introduction.....	1
1.3. LED Status Information.....	2
<b>2. Daily Use.....</b>	<b>3</b>
2.1. Make a Call.....	3
2.2. Receive a Call.....	3
2.3. Unlock.....	4
2.3.1. Unlock by Public Pin Codes.....	4
2.3.2. Unlock by Private Pin Codes.....	4
2.3.3. Unlock by RFID Cards (Optional).....	5
2.3.4. Unlock by DTMF Codes.....	5
<b>3. Basic Features.....</b>	<b>6</b>
3.1. Access the System Setting.....	6
3.1.1. Administrator Interface.....	6
3.1.2. User Interface.....	6

3.2. Access the Website Setting.....	7
3.2.1. Obtain IP Address.....	7
3.2.2. Access the Device Website.....	7
3.3. Password Modification.....	8
3.3.1. Modify the Device Admin Code.....	8
3.3.2. Modify the Device Service Code.....	8
3.3.3. Modify the Web Password.....	9
3.4. Phone Configuration.....	9
3.4.1. Language.....	9
3.4.2. Time.....	9
3.4.3. Network.....	10
3.4.3.1. DHCP Mode.....	10
3.4.3.2. Static IP Mode.....	11
3.4.3.3. Local RTP.....	11
3.4.3.4. SNMP.....	12
3.4.3.5. VLAN.....	13
3.4.3.6. TR069.....	13

3.4.4. Display.....	14
3.4.5. Sound.....	15
3.4.6. DND.....	16
3.5. Intercom Call.....	16
3.5.1. Direct IP Call.....	16
3.5.2. SIP Call.....	17
3.5.2.1. SIP Account.....	17
3.5.2.2. SIP Server 1&2.....	18
3.5.2.3. Outbound Proxy Server.....	19
3.5.2.4. Transport Type.....	19
3.5.2.5. NAT.....	19
3.5.3. Dial Plan.....	20
3.5.4. Speed Dial.....	21
3.5.5. Auto Answer.....	22
3.5.6. Web Call.....	22
3.5.7. Multicast.....	23
3.6. Security.....	23

3.6.1. Live view.....	23
3.6.2. RTSP.....	24
3.6.3. ONVIF.....	25
3.7. Access Control.....	25
3.7.1. Relay.....	25
3.7.2. Unlock via DTMF Codes.....	26
3.7.3. Unlock via RFID Cards (Optional).....	27
3.7.3.1. RFID Cards in Device.....	27
3.7.3.2. RFID Cards in Website.....	29
3.7.4. Unlock via Pin Codes.....	30
3.7.4.1. Public Pin Codes in Device.....	30
3.7.4.2. Public Pin Codes in Website.....	30
3.7.4.3. Private Pin Codes in Device.....	31
3.7.4.4. Private Pin Codes in Website.....	31
3.7.5. Unlock via HTTP command.....	32
3.7.6. Unlock via Exit Button.....	33
3.8. Reboot.....	33

3.9. Reset.....	34
3.9.1. Reset in Device.....	34
3.9.2. Reset in Website.....	34
<b>4. Advanced Features.....</b>	<b>35</b>
4.1. Phone Configuration.....	35
4.1.1. LED.....	35
4.1.2. IR LED.....	35
4.1.3. RFID Card Code Display Related.....	36
4.1.4. Key Display Related.....	36
4.2. Intercom.....	37
4.2.1. Call Time Related.....	37
4.2.2. AEC Level.....	37
4.2.3. Intercom.....	38
4.2.4. Return Code When Refuse.....	38
4.2.5. SIP Call Related.....	38
4.2.6. Codec.....	40
4.2.7. Subscribe.....	41

4.2.8. DTMF.....	42
4.2.9. Session Timer.....	42
4.2.10. BLF List.....	42
4.2.11. Encryption.....	43
4.2.12. NAT.....	43
4.2.13. User Agent.....	44
4.3. Access Control.....	44
4.3.1. Web Relay.....	44
4.3.2. Wiegand.....	45
4.4. Security.....	46
4.4.1. Anti-alarm.....	46
4.4.2. Motion.....	47
4.4.3. Action.....	47
4.4.3.1. Action Parameters.....	47
4.4.3.2. No Answer Action.....	49
4.4.3.3. Call Event.....	49
4.4.3.4. Input Interface Triggered Action.....	50



4.4.3.5. Motion Triggered Action.....	50
4.4.3.6. Unlock via RFID Card Action.....	51
4.5. Upgrade.....	51
4.5.1. Web Upgrade.....	51
4.5.2. Autop Upgrade.....	52
4.5.3. Backup Config File.....	54
4.6. Log.....	54
4.6.1. Call Log.....	54
4.6.2. Door Log.....	55
4.6.3. System Log.....	55
4.6.4. PCAP.....	55

# 1. Product Overview

## 1.1. Product Description

Akuvox R27 is a SIP-compliant, hands-free and video door phone. It can be connected with Akuvox indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. Users can also use RFID cards to unlock the door (R27A only). It is applicable in villas, offices and so on.

## 1.2. Connector Introduction

**Ethernet (POE):** Ethernet (POE) connector which it can provide both power and network connection.

**12V/GND:** External power supply terminal if POE connector is not available.

**RS485A/B:** RS485 terminal.

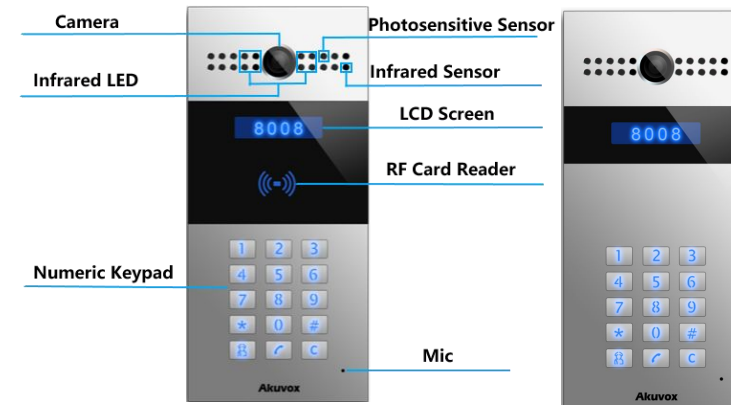


Figure 1.1 Product Description

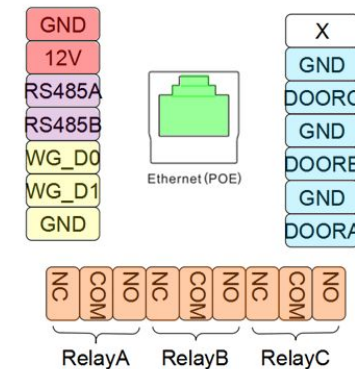


Figure 1.2-1 R27's interface

**WG\_D0/WG\_D1:** Wiegand terminal.

**DOORA/B/C:** Trigger signal input terminal.

**RelayA/B/C (NO/NC/COM):** Relay control terminal.

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

### 1.3. LED Status Information

LED Status		Description
Blue	Always on	Normal status
	Flashing	Calling
Red	Flashing	Network is unavailable
Green	Always on	Talking on a call
	Flashing	Receiving a call
Pink	Flashing	Upgrading

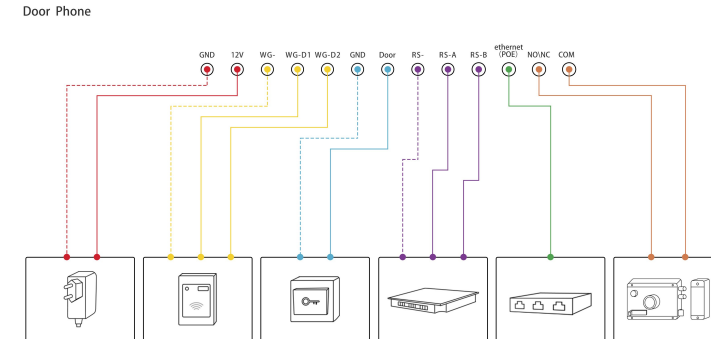


Figure 1.2-2 General interface

## 2. Daily Use

### 2.1. Make a Call

In the idle interface, press the SIP account or IP address and “Dial key” to make a call.

**Management center call :** Users can make a speed dial to management center by pressing “Management center key.”

### 2.2. Receive a Call

R27 will auto answer the incoming call by default. If users disable auto answer function, they can press “Dial key” to answer the incoming call.

## **2.3. Unlock**

### **2.3.1. Unlock by Public Pin Codes**

Users can unlock doors by using predefined public pin code. Press “#,” public pin code, “#” to unlock, and then users will hear “The door is now opened.” If users press wrong public pin code, the screen will show “Incorrect Code.” The default public pin code is 33333333. The default public pin code is 8 digits, and it can be changed to 3 to 8 digits.

### **2.3.2. Unlock by Private Pin Codes**

Users can unlock doors by using predefined private pin code. Press “#,” private pin code, “#” to unlock, and then users will hear “The door is now opened.” If users press wrong private pin code, the screen will show “Incorrect Code.” The default private pin code is 8 digits, and it can be changed to 3 to 8 digits.

### **2.3.3. Unlock by RFID Cards (Optional)**

Place the predefined user cards in RFID card reader to unlock. Under normal conditions, R27A will announce “The door is now opened.” If the card has not been registered, R27A will show “Unauthorized.” Both 13.56MHz and 125KHz RFID cards are supported on R27A.

### **2.3.4. Unlock by DTMF Codes**

Users can press the predefined DTMF code from an answer unit to remotely unlock the door during the call. Users will also hear “The door is now opened.”

## 3. Basic Features

### 3.1. Access the System Setting

#### 3.1.1. Administrator Interface

Press “\*2396#” to enter administrator interface. Administrator interface provides some advanced permissions to administrators, including “System Information,” “Admin Settings” and “System Settings.”

#### 3.1.2. User Interface

Press “\*3888#” to enter user interface. User interface includes “Public Pin Modif,” “Add User Cards” and “Add Private Pin.” These functions can only be accessed by administrator.

## 3.2. Access the Website Setting

### 3.2.1. Obtain IP Address

R27 use DHCP IP by default. Press “\*2396#” to enter administrator interface. Press “1” to enter system Information interface to check the IP address.

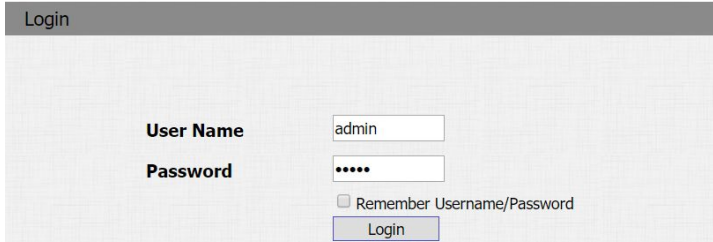
### 3.2.2. Access the Device Website

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.



Login

User Name admin

Password \*\*\*\*\*

☐ Remember Username/Password

Login

Figure 3.2.2 Access the device website



## **3.3. Password Modification**

### **3.3.1. Modify the Device Admin Code**

Admin code is used to enter administrator interface. The default code is 2396.

Press “\*2396#” to enter administrator interface. Press “2” to enter admin settings interface. Press “2” to enter admin code setting interface to input a 4-digit new admin code, and press “Dial key” to save.

### **3.3.2. Modify the Device Service Code**

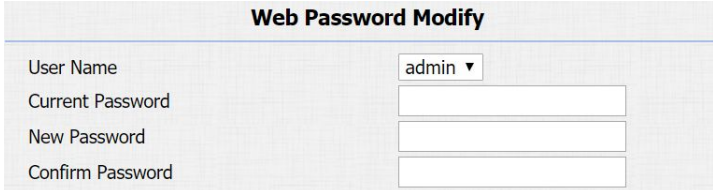
Service code is used to enter user interface. The default code is 3888.

Press “\*2396#” to enter administrator interface. Press “2” and “3” to enter service code setting interface to input a 4-digit new user code, and press “Dial key” to save.

### 3.3.3. Modify the Web Password

Go to **Security - Basic** to modify password for webpage.

To modify password for “admin” or “user” account.



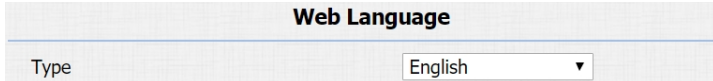
The 'Web Password Modify' form contains four fields: 'User Name' with a dropdown menu showing 'admin', 'Current Password' with a text input field, 'New Password' with a text input field, and 'Confirm Password' with a text input field.

Figure 3.3.3 Modify the web password

## 3.4. Phone Configuration

### 3.4.1. Language

Go to **Phone - Time/Lang** to select language for webpage.



The 'Web Language' form has a single field labeled 'Type' with a dropdown menu currently set to 'English'.

Figure 3.4.1 Language

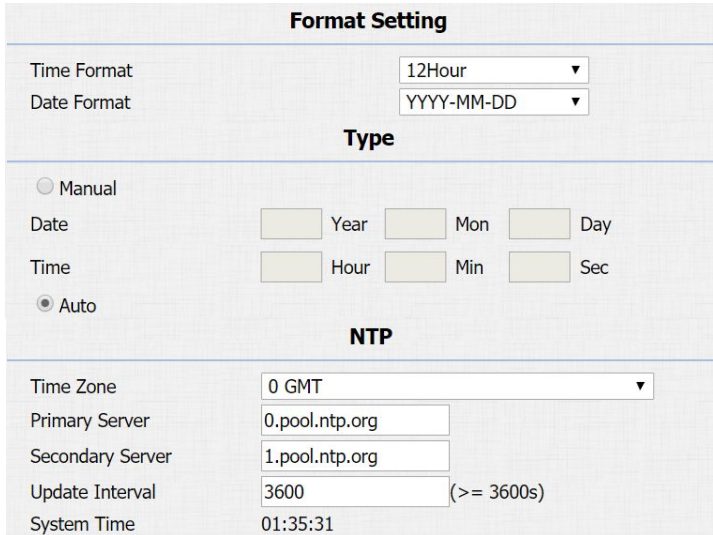
### 3.4.2. Time

Go to **Phone - Time/Lang** to configure the time related features.

**Format Setting:** To select time format and date format.

**Type:** To select configure the time manually or automatically.

**NTP:** To select local time zone for NTP server.



This block contains three stacked configuration sections. The 'Format Setting' section has 'Time Format' set to '12Hour' and 'Date Format' set to 'YYYY-MM-DD'. The 'Type' section has 'Manual' selected. The 'NTP' section has 'Time Zone' set to '0 GMT', 'Primary Server' as '0.pool.ntp.org', 'Secondary Server' as '1.pool.ntp.org', 'Update Interval' as '3600' (with a note '(>= 3600s)'), and 'System Time' as '01:35:31'.

Figure 3.4.2 Time

### 3.4.3. Network

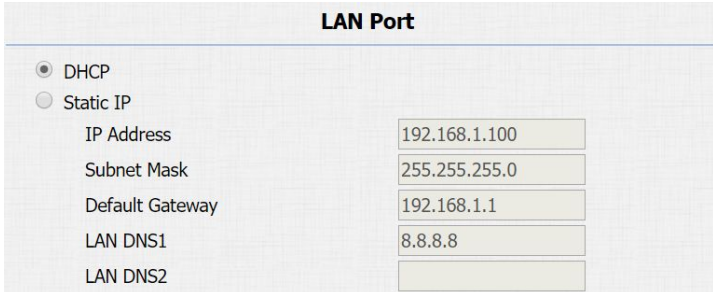
#### 3.4.3.1. DHCP Mode

At device side, press “\*2396#” to enter administrator interface.  
Press “3” to enter system setting interface, and press “1” to enter network setting interface.

Select DHCP mode, and R27 will access network automatically.

In website, go to **Network - Basic**.

R27 uses DHCP mode by default which will get IP address, subnet mask, default gateway and DNS server address from DHCP server automatically.



The screenshot shows the 'LAN Port' configuration page. At the top, 'DHCP' is selected with a radio button, while 'Static IP' is unselected. Below this, there are five input fields with the following values: IP Address (192.168.1.100), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.1), LAN DNS1 (8.8.8.8), and LAN DNS2 (empty).

LAN Port	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static IP	
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
LAN DNS1	8.8.8.8
LAN DNS2	

Figure 3.4.3.1 DHCP mode

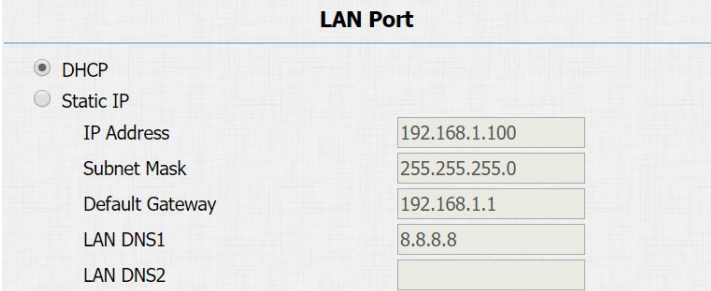
### 3.4.3.2. Static IP Mode

At device side, press “\*2396#” to enter administrator interface. Press “3” to enter system setting interface, and press “1” to enter network setting interface.

Select static IP mode, users need to setup IP address, subnet mask, default gateway and DNS server address. Press “Dial key” when finish each step.

In Website, go to **Network - Basic**.

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



The screenshot shows the 'LAN Port' configuration page. At the top, there are two radio buttons: 'DHCP' (selected) and 'Static IP'. Below these, there are five input fields for static IP configuration: 'IP Address' (192.168.1.100), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.1.1), 'LAN DNS1' (8.8.8.8), and 'LAN DNS2' (empty).

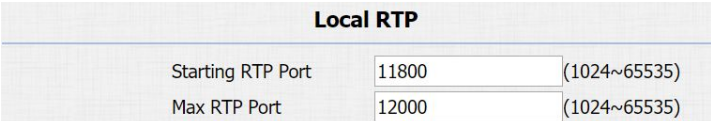
LAN Port	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static IP	
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
LAN DNS1	8.8.8.8
LAN DNS2	

Figure 3.4.3.2 Static IP mode

### 3.4.3.3. Local RTP

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

**Local RTP:** To display and configure local RTP settings.



The screenshot shows the 'Local RTP' configuration page. It contains two rows of settings: 'Starting RTP Port' with a value of 11800 and a range of (1024~65535), and 'Max RTP Port' with a value of 12000 and a range of (1024~65535).

Local RTP	
Starting RTP Port	11800 (1024~65535)
Max RTP Port	12000 (1024~65535)

Figure 3.4.3.3 Local RTP

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

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

#### 3.4.3.4. SNMP

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

**SNMP:** To display and configure SNMP settings.

**Active:** To enable or disable SNMP feature.

**Port:** To configure SNMP server's port.

**Trusted IP:** To configure allowed SNMP server address. It could be an IP address or any valid URL domain name.

**Note:** SNMP is Internet-standard protocol for managing devices on IP networks.

SNMP	
Active	Disabled ▼
Port	<input type="text"/> (1024~65535)
Trusted IP	<input type="text"/>

Figure 3.4.3.4 SNMP

### 3.4.3.5. VLAN

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

**VLAN:** To display and configure VLAN settings.

**Active:** To enable or disable VLAN feature for designated port.

**VID:** To configure VLAN ID for designated port.

**Priority:** To select VLAN priority for designated port.

**Note:** Please consult administrator for specific VLAN settings in the networking environment.

VLAN		
LAN Port	Active	Disabled ▼
	VID	1 (1~4094)
	Priority	0 ▼

Figure 3.4.3.5 VLAN

### 3.4.3.6. TR069

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

**TR069:** To display and configure TR069 settings.

**Active:** To enable or disable TR069 feature.

**Version:** To select supported TR069 version (version 1.0 or 1.1).

**ACS/CPE:** ACS is short for auto configuration servers as server side, and CPE is short for customer-premise equipment as client

TR069		
ACS	Active	Disabled ▼
	Version	1.0 ▼
	URL	
	User Name	
	Password	*****
Periodic Inform	Active	Disabled ▼
	Periodic Interval	1800 (3~24×3600s)
CPE	URL	
	User Name	
	Password	*****

Figure 3.4.3.6 TR069

side devices.

**URL:** To configure URL address for ACS or CPE.

**User Name:** To configure username for ACS or CPE.

**Password:** To configure password for ACS or CPE.

**Periodic Inform:** To enable periodically inform.

**Periodic Interval:** To configure interval for periodic inform.

**Note:** TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

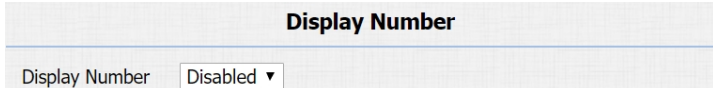
### 3.4.4. Display

Go to **Intercom - Basic** to configure display related features.

**Display Number:** To enable to display the number in LCD or not. If disabled, each number will be displayed as a star.

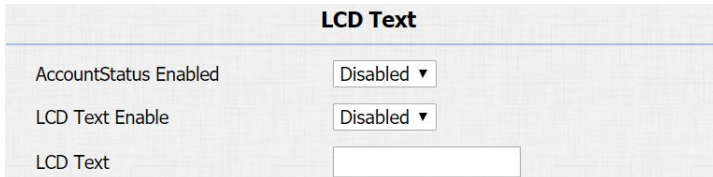
Go to **Intercom - Advanced** to configure display related features.

**LCD Text:** Users can customize the LCD text during the idle by themselves, such as “Welcome” or something else.



Display Number	
Display Number	Disabled ▼

Figure 3.4.4-1 Display number



LCD Text	
AccountStatus Enabled	Disabled ▼
LCD Text Enable	Disabled ▼
LCD Text	<input type="text"/>

Figure 3.4.4-2 LCD display

**AccountStatus Enabled:** The LCD text will only be shown if the account is valid.

**LCD Text Enable:** Switch this feature.

**LCD Text:** Display content.

### 3.4.5. Sound

Go to **Phone - Voice** to configure volume and upload tone file.

**Mic Volume:** To configure microphone volume.

**Speaker Volume:** To configure speaker volume.

**Open Door Warning:** Disable it, and users will not hear the prompt voice when the door is opened.

**RingBack Upload:** To upload the ring back tone by users themselves.

**Opendoor Tone Upload:** To upload the open door tone by users themselves.

Mic Volume	
Mic Volume	<input type="text" value="8"/> (1~15)
Speaker Volume	
Speaker Volume	<input type="text" value="8"/> (1~15)
Open Door Warning	
Open Door Warning	<input type="text" value="Enabled"/>
RingBack Upload	
<input type="button" value="Choose File"/>	No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16	
Opendoor Tone Upload	
<input type="button" value="Choose File"/>	No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16	

Figure 3.4.5 Sound



### 3.4.6. DND

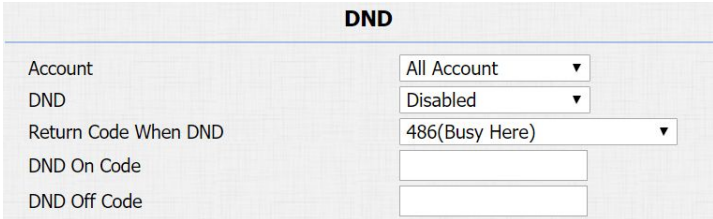
Go to **Phone - Call Feature** to configure DND feature.

**DND:** DND allows phones to ignore any incoming calls.

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

**DND On Code:** The code is used to turn on DND on server's side, if configured, door phones will send a SIP message to server to turn on DND on server side if users press DND when DND is off.

**DND Off Code:** The code is used to turn off DND on server's side, if configured, door phones will send a SIP message to server to turn off DND on server side if users press DND when DND is on.



DND	
Account	All Account ▼
DND	Disabled ▼
Return Code When DND	486(Busy Here) ▼
DND On Code	<input type="text"/>
DND Off Code	<input type="text"/>

Figure 3.4.6 DND

## 3.5. Intercom Call

### 3.5.1. Direct IP Call

Go to **Phone - Call Feature** to enable the direct IP call for door



Direct IP	Enabled ▼
-----------	-----------

Figure 3.5.1 Direct IP call

phones first.

In the idle interface, press the IP address (like IP address 192.168.1.100, users need to press “192\*168\*1\*100”) and “Dial key” to make a direct IP call.

## 3.5.2. SIP Call

SIP calls which use SIP numbers to make or receive calls should be supported by SIP server. Users need to register accounts and fill SIP feature parameters before using it.

Go to **Account - Basic** to configure SIP account and SIP server for door phones first.

### 3.5.2.1. SIP Account

**Status:** To display register result.

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

SIP Account	
Status	Registration Failed
Account	Account 1 ▼
Account Active	Enabled ▼
Display Label	R27
Display Name	Door_R27
Register Name	5101100001
User Name	5101100001
Password	••••••

Figure 3.5.2.1 SIP account

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

**Register Name:** To enter extension number which 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.

### 3.5.2.2. SIP Server 1&2

**Server IP 1:** To enter SIP server's IP address or URL.

**Server IP 2:** To display and configure secondary SIP server settings. This is for redundancy, if registering to primary SIP server fails, the phone will go to secondary SIP server for registering.

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

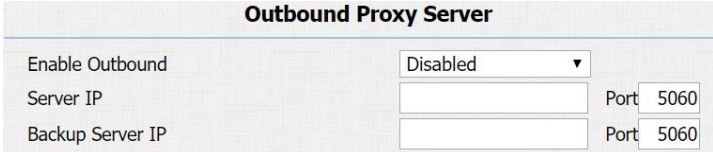
SIP Server 1		
Server IP	<input type="text" value="120.78.230.239"/>	Port <input type="text" value="5070"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)

SIP Server 2		
Server IP	<input type="text"/>	Port <input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)

Figure 3.5.2.2 SIP server 1&2

### 3.5.2.3. Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server.



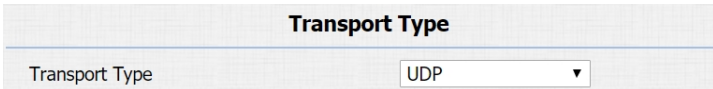
The screenshot shows the 'Outbound Proxy Server' configuration window. It contains three fields: 'Enable Outbound' is a dropdown menu set to 'Disabled'; 'Server IP' is an empty text box; 'Backup Server IP' is an empty text box. To the right of the 'Server IP' field is a 'Port' label and a text box containing '5060'. To the right of the 'Backup Server IP' field is a 'Port' label and a text box containing '5060'.

Figure 3.5.2.3 Outbound proxy server

### 3.5.2.4. 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.



The screenshot shows the 'Transport Type' configuration window. It contains one field: 'Transport Type' is a dropdown menu set to 'UDP'.

Figure 3.5.2.4 Transport type

### 3.5.2.5. NAT

To display and configure NAT settings.

- STUN: Short for session traversal utilities for NAT, a solution to solve NAT issues.



The screenshot shows the 'NAT' configuration window. It contains two fields: 'NAT' is a dropdown menu set to 'Disabled'; 'Stun Server Address' is an empty text box. To the right of the 'Stun Server Address' field is a 'Port' label and a text box containing '3478'.

Figure 3.5.2.5 NAT

**Note:** By default, NAT is disabled.

In the idle interface, press the a SIP account and “Dial key” to make a SIP call.

### 3.5.3. Dial Plan

This feature allows users to modify selected rules information.

Once users dial prefix value, it will call out replace number.

Go to **Intercom - Basic** to configure first.

#### Rules Management

R27 supports to import or export the dial plan rules, which is convenient for administrator to deal with a large number of dial plan.

The maximum dial plan is 200.

**Note:** Please consult administrator for the .xml format dial plan template file.

#### Edit Dial plan

- Click “Add” to add new replace rules.

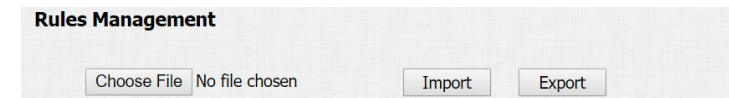


Figure 3.5.3-1 Dial plan rules management

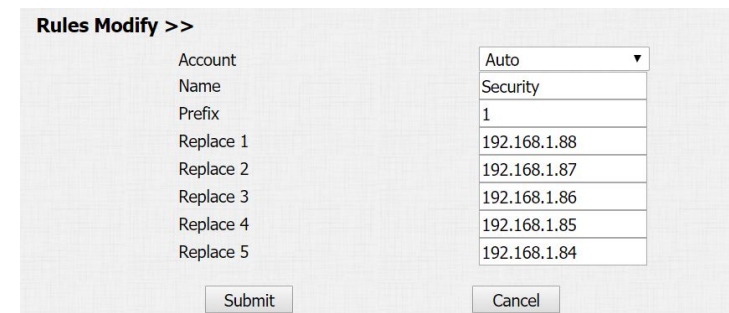


Figure 3.5.3-2 Dial plan rules

- Select account for the replace rule.
- Enter a display name for the prefix value. Input a suitable prefix value. Enter the replace number.
- Click “Submit” to save.

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

In the idle interface, press the prefix and “Dial key” to make a call.

### 3.5.4. Speed Dial

Speed dial feature is used to call out 4 numbers at the same time.

Go to **Intercom - Basic** to configure first.

After setup the number which users need to call, in the idle interface, press “Manage center key” (Manager Dial) or “Dial key” (Speed Dial) to call.

Index	Account	Name	Prefix	Replace 1	Replace 2	Replace 3	Replace 4	Replace 5	
1	Auto	Security	1	192.168.1.88	192.168.1.87	192.168.1.86	192.168.1.85	192.168.1.84	<input type="checkbox"/>
2									<input type="checkbox"/>
3									<input type="checkbox"/>
4									<input type="checkbox"/>
5									<input type="checkbox"/>
6									<input type="checkbox"/>
7									<input type="checkbox"/>
8									<input type="checkbox"/>
9									<input type="checkbox"/>
10									<input type="checkbox"/>
Page 1 ▾    Add    Edit    Delete    Prev    Next									

Figure 3.5.3-3 Dial plan

Manager Dial	
Key	Number
Manager Dial	5100100052
Manager Dial2	192.168.1.33
Manager Dial3	5100100053
Manager Dial4	5100100054

Speed Dial	
Key	Number
Speed Dial	5100100055
Speed Dial2	5100100056
Speed Dial3	192.168.1.57
Speed Dial4	5100100057

Figure 3.5.4 Speed dial

### 3.5.5. Auto Answer

Go to **Account - Advanced** to enable auto answer feature for SIP calls.

Go to **Phone - Call Feature** to enable auto answer feature for direct IP calls.

**Auto Answer Delay:** To configure delay time before an incoming call is automatically answered.

**Auto Answer Mode:** To set video or audio mode for auto answer feature. It is video by default.

Then incoming calls will be answered automatically.

### 3.5.6. Web Call

Go to **Intercom - Basic** to dial out or answer incoming calls from website.



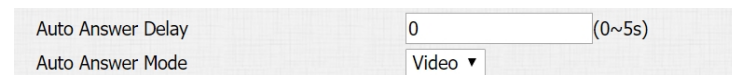
Auto Answer Enabled ▾

Figure 3.5.5-1 Auto answer for sip calls



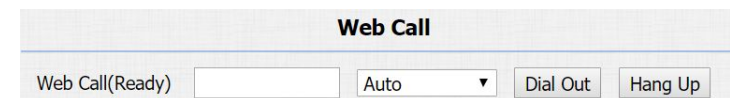
Direct IP AutoAnswer Enabled ▾

Figure 3.5.5-2 Auto answer for direct IP calls



Auto Answer Delay 0 (0~5s)  
Auto Answer Mode Video ▾

Figure 3.5.5-3 Auto answer options' parameters



Web Call

Web Call(Ready)  Auto ▾

Figure 3.5.6 Web call

### 3.5.7. Multicast

Go to **Intercom - Multicast** to configure.

**Paging Barge:** Choose the multicast number, and the range is from 1 to 10.

**Paging priority Active:** Enable or disable the multicast.

**Listening Address:** Enter IP address which users need to listen.

**Label:** Input the label for each listening address.

Multicast Setting			
Paging Barge	1 ▼		
Paging Priority Active	Enabled ▼		
Priority List			
IP Address	Listening Address	Label	Priority
1 IP Address	224.1.6.11:1200	Test	1
2 IP Address			2
3 IP Address			3
4 IP Address			4
5 IP Address			5

Figure 3.5.7 Multicast

## 3.6. Security

### 3.6.1. Live view

Go to **Intercom - Live Stream** to check the real-time video from R27.

In addition, user also can check the real-time picture via URL:  
**[http://IP\\_address:8080/picture.jpg](http://IP_address:8080/picture.jpg)**.



Figure 3.6.1 Live view



### 3.6.2. RTSP

R27 supports RTSP stream, go to **Intercom - RTSP** to enable or disable RTSP server. The URL for RTSP stream is:

**rtsp://IP\_address/live/ch00\_0.**

**RTSP Stream:** To enable RTSP video and select the video codec. R27 supports H.264 video codec by default.

**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.

**MPEG4 Video Parameters:** MPEG4 is one of the network video image compression standard. It supports the maximum compression ratio 4000:1. It is an important and common video function with great communication application integration ability and less core program space. To modify the resolution, framerate and

RTSP Basic	
RTSP Server Enabled	<input checked="" type="checkbox"/>
RTSP Stream	
RTSP Video Enabled	<input checked="" type="checkbox"/>
RTSP Video Codec	H.264 ▼
H.264 Video Parameters	
Video Resolution	VGA ▼
Video Framerate	30 fps ▼
Video Bitrate	2048 kbps ▼
MPEG4 Video Parameters	
Video Resolution	VGA ▼
Video Framerate	30 fps ▼
Video Bitrate	2048 kbps ▼

Figure 3.6.2 RTSP

bitrate of MPEG4.

### 3.6.3. ONVIF

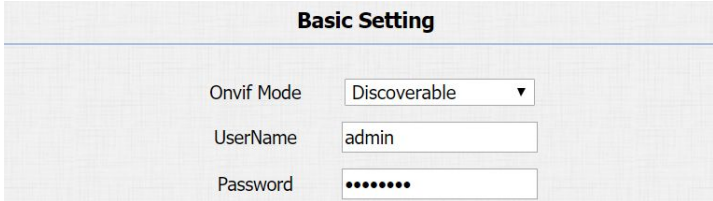
R27 supports ONVIF protocol, which means R27's camera can be searched by other devices, like NVR which supports ONVIF protocol as well.

Go to **Intercom - ONVIF** to configure ONVIF mode, its username and password.

Switching ONVIF mode to “Undiscoverable,” and it means users must program ONVIF's URL manually.

The ONVIF's URL is:

**http://IP\_address:8090/onvif/device\_service.**



Basic Setting	
Onvif Mode	Discoverable ▼
UserName	admin
Password	.....

Figure 3.6.3 ONVIF

## 3.7. Access Control

### 3.7.1. Relay

Go to **Intercom - Relay** to configure relay settings.

There are three terminals of relay: NO, NC and COM. NO stands for normally open contact. NC stands for normally closed contact.

**Relay ID:** R27 supports three relays. Users can configure them respectively.

**Relay Type:** Default state means NC and COM are normally closed, while Invert state means NC and COM are normally opened.

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

**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.

Relay			
Relay ID	RelayA ▼	RelayB ▼	RelayC ▼
Relay Type	Default state ▼	Default state ▼	Default state ▼
Relay Delay(sec)	3 ▼	3 ▼	3 ▼
DTMF Option	1 Digit DTMF ▼		
DTMF	0 ▼	0 ▼	0 ▼
Multiple DTMF			
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low

Figure 3.7.1 Relay

### 3.7.2. Unlock via DTMF Codes

Users can unlock via a DTMF code when in a call.

Go to **Intercom - Relay** to configure DTMF code parameters.

**DTMF Option:** To select digit of DTMF code, R27 support maximum to 4 digits' DTMF code.

**DTMF&Multiple DTMF:** To configure DTMF code for remote unlocking.

### 3.7.3. Unlock via RFID Cards (Optional)

#### 3.7.3.1. RFID Cards in Device

##### **Add/Clean admin card**

Press “\*2396#” to enter administrator interface. Press “2” to enter admin settings interface. Press “2” to enter admin card setting interface.

Press “1” to quickly add an admin card. When users see “Please Swipe Admin Card...,” please place admin card in the RFID card reader area. After the screen shows “An admin card is added +1,” it means adding successfully.

Press “2” to delete the current admin card. When users see

“Please Swipe Admin Card....,” and place the added admin card which users want to delete in the RFID card area. After the screen shows “An admin card is deleted,” it means deleting successfully.

#### **Add/Delete user card**

Users card is used to unlock. Press “\*3888#” to enter user interface. Press “2” to enter user card modify interface. Before adding or deleting users card, users need to swipe admin card or enter admin code.

Press “1” to add a user card, when users see “Please Swipe IC Card....,” place user card in the RFID card reader area. Then the screen will show “Add IC Card +1,” it means adding successfully.

Press “2” to delete the current user card. When users see “Please Swipe IC Card....,” and place the added IC card which users want to delete in the RFID card area. After the screen shows “An IC card is deleted,” it means deleting successfully.

### 3.7.3.2. RFID Cards in Website

Go to **Intercom - Card setting** to manage card access system.

#### Import/Export Card Data

R27A supports import or export the card data file, which is convenient for administrator to deal with a large number of cards.

The maximum card data file is 200K which is around 500 cards.

**Note:** Please consult administrator for the .xml format RFID cards template file.

#### Obtain and Add Card

- Switch card status to “Card Issuing” and click “Apply”;
- Place card on the card reader area and click “Obtain”;
- Name card, choose which door users want to open and the valid day and time;
- Click “Add” to add it into list.

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

**Import/Export Card Data(.xml)**

Choose File No file chosen Import Export

**Card Status**

Card Status Card Issuing Apply

**Card Setting**

IC Key DoorNum RelayA ☒ RelayB ☐ RelayC ☐

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

IC Key Time 06 : 00 - 12 : 00

IC Key Name Courier

IC Key Code FFB59828 Obtain Add

**Door Card Management**

Index	Name	Code	Relay	
1	Courier	FFB59828	1	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

Page 1 Prev Next Delete Delete All

Figure 3.7.3.2 RFID cards in website

**Note:** Remember to set Card Status back to “Normal” after adding cards.

## 3.7.4. Unlock via Pin Codes

### 3.7.4.1. Public Pin Codes in Device

Press “\*3888#” to enter user interface. Press “1” to enter public pin modify interface. The default public pin code is 33333333. Before users modify public pin code, they need to swipe admin card or enter admin code, and then users can enter 8-digit new public pin code, click “Dial key” to save.

### 3.7.4.2. Public Pin Codes in Website

Go to **Intercom - Basic** to configure public pin codes.

**Key Switch:** To enable or disable the password unlock, it is much useful for some special occasion which do not allow to use passwords.

Public Key	
Key Switch	Enabled ▾
Send Key	Enabled ▾
Key Value	33333333 (3-8 digit number)

Figure 3.7.4.2 Public pin code in website

**Key Value:** The public key for the all occupants in a building.

### 3.7.4.3. Private Pin Codes in Device

Press “\*3888#” to enter user interface. Press “3” to enter add private pin interface. Before adding private pin code, users need to swipe admin card or enter admin code. Then enter a 8-digit private pin code, and click “Dial key” to save.

### 3.7.4.4. Private Pin Codes in Website

Go to **Intercom - PrivateKey** to configure private pin code.

#### Import /Export Private Key

R27 supports import or export the private key file, which is convenient for administrator to deal with a large number of private keys.

The maximum private key is 500.

**Note:** Please consult administrator for the .xml format private key

**Import/Export Private Key(.xml)**

Choose File No file chosen Import Export

**Private Key Setting**

PKey DoorNum RelayA ☐ RelayB ☒ RelayC ☐

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

PKey Time 08 : 00 - 23 : 00

PKey Name Troye

PKey Code 2333 Add

Figure 3.7.4.4-1 Private pin code in website



template file.

### Obtain and Add Private Key

- Enter the “PKey Name” and 3-8 digits “PKey Code”;
- Select the valid day and time;
- Choose which door users want to open;
- Click “Add” to add it into list.

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

Private Key Management				
Index	Name	Code	Relay	
1	Troye	2333	2	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>
Page 1 ▾ Prev Next Delete Delete All				

Figure 3.7.4.4-2 Private pin code management

## 3.7.5. Unlock via HTTP command

Users can use a URL to remote unlock the door.

Go to **Intercom - Relay** to configure.

**Switch:** Enable this function. Disable by default.

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

**URL format:**

Open Relay via HTTP	
Switch	Disabled ▾
UserName	<input type="text"/>
Password	<input type="password"/>

Figure 3.7.5 Unlock via HTTP command

**http://IP\_address/fcgi/do?action=OpenDoor&UserName=&Password=&DoorNum=1.**

### 3.7.6. Unlock via Exit Button

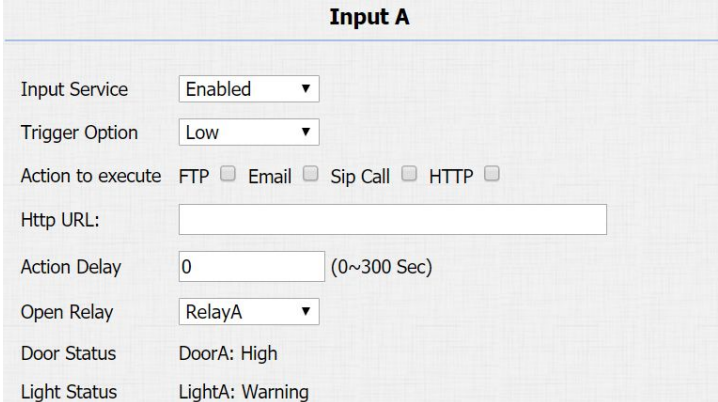
Go to **Intercom - Input** to configure input settings.

R27 supports three input triggers “Input A/B/C(DOOR A/B/C).”

**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.



Input A	
Input Service	Enabled
Trigger Option	Low
Action to execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> Sip Call <input type="checkbox"/> HTTP <input type="checkbox"/>
Http URL:	
Action Delay	0 (0~300 Sec)
Open Relay	RelayA
Door Status	DoorA: High
Light Status	LightA: Warning

Figure 3.7.6 Unlock via exit button

## 3.8. Reboot

Go to **Upgrade - Basic**, users can reboot the phone.



Reboot	Submit
--------	--------

Figure 3.8 Reboot

## 3.9. Reset

### 3.9.1. Reset in Device

Press “\*2396#” to enter administrator interface. Press “3” to enter system setting interface, and then press “2” to enter restore default setting interface. After users are sure to make the device reset to factory setting, they can swipe admin card or enter admin code, and then the device will restore.

**Note:** All configurations will be reset after restore. Please backup the data if users need.

### 3.9.2. Reset in Website

Go to **Upgrade - Basic**, users can reset the phone to factory settings.



Figure 3.9.2 Reset in website

## 4. Advanced Features

### 4.1. Phone Configuration

#### 4.1.1. LED

Go to **Intercom - LED Setting** to configure.

Users can control three parts' LED, screen, keypad and card area.

Users can also setup the valid time. For example, start time from 18 to 23 means the LED will light up from 6pm to 11pm.

#### 4.1.2. IR LED

Go to **Intercom - Advanced** to configure.

**Photoresistor:** The setting is for night vision, when the surrounding of R27 is very dark, infrared LED will turn on and R27 will turn to night mode.

LED Control	
Screen LED Enable	Disabled ▾
Start Time (H)	18 - 23 (0~23)
KeyPad LED Enable	Disabled ▾
Start Time (H)	18 - 23 (0~23)
Card LED Enable	Disabled ▾
Start Time (H)	18 - 23 (0~23)

Figure 4.1.1 LED

Photoresistor	
Photoresistor Setting	15 - 30 (0~100)

Figure 4.1.2 IR LED

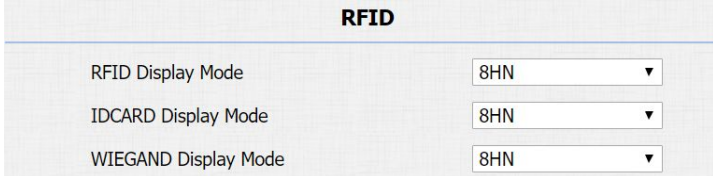
Photoresistor value relates to light intensity and larger value means that light intensity is smaller.

Users can configure the upper and lower bound and when photoresistor value is larger than upper bound, infrared LED will turn on. As contrast, when photoresistor value is smaller than lower bound, infrared LED will turn off and device turns to normal mode.

### 4.1.3. RFID Card Code Display Related

Go to **Intercom - Advanced** to configure.

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



RFID	
RFID Display Mode	8HN ▼
IDCARD Display Mode	8HN ▼
WIEGAND Display Mode	8HN ▼

Figure 4.1.3 RFID card code display related

### 4.1.4. Key Display Related

Go to **Intercom - Basic** to configure.

**Send Key:** Limit to use the “#” key. It will prevent someone to enter the LCD setting illegally.



Send Key	Enabled ▼
----------	-----------

Figure 4.1.4-1 Send key

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

## 4.2. Intercom

### 4.2.1. Call Time Related

Go to **Intercom - Basic** to configure.

**Max Call Time:** To configure the max call 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.

### 4.2.2. AEC Level

Go to **Intercom - Basic** to configure.

**AEC Level:** AEC is used to adjust the echo effect during the communication. The default value is 700. Increase the level, the echo control is better.

Door Setting General	
DialPad Input Number Limit	Default

Figure 4.1.4-2 Dialpad input number limitation

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

Figure 4.2.1 Call time related

AEC Setting	
AEC Level	700

Figure 4.2.2 AEC level

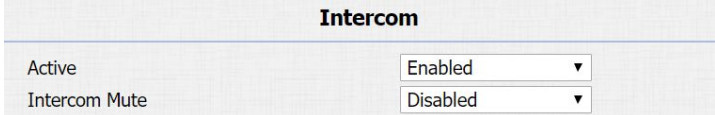
### 4.2.3. Intercom

Go to **Phone - Call Feature** to configure.

**Intercom:** Intercom allows users to establish a call directly with the callee.

**Active:** To enable or disable Intercom feature.

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



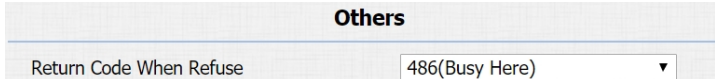
Intercom	
Active	Enabled ▼
Intercom Mute	Disabled ▼

Figure 4.2.3 Intercom

### 4.2.4. Return Code When Refuse

Go to **Phone - Call Feature** 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 Refuse	486(Busy Here) ▼

Figure 4.2.4 Return code when refuse

### 4.2.5. SIP Call Related

Go to **Account - Advanced** to configure the SIP call related.

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

designated SIP account.

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

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

**Provisional Response ACK:** 100% reliability for all provisional messages, this means it will send ACK every time the phone receives a provisional SIP message from SIP server.

**Register with user=phone:** If enabled, the phone will send user=phone within SIP message.

**Anonymous Call:** If enabled, R27 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 Hacking:** If enabled, it will prevent SIP messages from hacking.

Call		
Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)
Caller ID Header	FROM	▼
Auto Answer	Enabled	▼
Provisional Response ACK	Disabled	▼
Register with user=phone	Disabled	▼
Invite with user=phone	Disabled	▼
Anonymous Call	Disabled	▼
Anonymous Call Rejection	Disabled	▼
Missed Call Log	Enabled	▼
Prevent SIP Hacking	Disabled	▼

Figure 4.2.5 SIP call related



## 4.2.6. Codec

Go to **Account - Advanced** to configure SIP call related codec.

**Sip Account:** To choose which account to configure.

**Audio Codec:** R27 support four audio codecs: PCMA, PCMU, G729, G722. Different audio codecs require different bandwidth, users can enable/disable them according to different network environment.

**Note:** Bandwidth consumption and sample rates are as below:

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

The screenshot displays the 'SIP Account' configuration page. At the top, there's a section for 'Account' with a dropdown menu set to 'Account 1'. Below this is the 'Codecs' section, which contains two lists: 'Disabled Codecs' (currently empty) and 'Enabled Codecs' (containing PCMU, PCMA, G722, and G729). Between these lists are '>>' and '<<' buttons. To the right of the 'Enabled Codecs' list are up and down arrow buttons. Below the 'Codecs' section is the 'Video Codec' section, which includes a 'Codec Name' dropdown set to 'H264', and three other dropdowns for 'Codec Resolution' (set to '4CIF'), 'Codec Bitrate' (set to '2048'), and 'Codec Payload' (set to '104').

Figure 4.2.6-1 SIP call related codec

**Video Codec:** R27 support H.264 standard, which provides better video quality at substantially lower bit rates than previous

standards.

**Codec Resolution:** R27 support 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.

Go to **Phone - Call Feature** to configure multicast related codec.

### 4.2.7. Subscribe

Go to **Account - Advanced** to configure.

**MWI:** Message waiting indicator which is used to indicate whether there is unread new voice message.

**BLF:** BLF is short for busy lamp field which is used to monitor the designated extension status.

**ACD:** Automatic call distribution is often used in offices for customer service, such as call center. The setting here is to negotiate with the server about expire time of ACD subscription.

Multicast Codec	PCMU ▼
-----------------	--------

Figure 4.2.6-2 Multicast related codec

Subscribe		
MWI Subscribe	Disabled ▼	
MWI Subscribe Period	1800	(120~65535s)
Voice Mail Number		
BLF Expire	1800	(120~65535s)
ACD Expire	1800	(120~65535s)

Figure 4.2.7 Subscribe

### 4.2.8. DTMF

Go to **Account - Advanced** 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.

DTMF	
Type	<input type="text" value="RFC2833"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
DTMF Payload	<input type="text" value="101"/> (96~127)

Figure 4.2.8 DTMF

### 4.2.9. Session Timer

Go to **Account - Advanced** 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	<input type="text" value="Disabled"/>
Session Expire	<input type="text" value="1800"/> (90~7200s)
Session Refresher	<input type="text" value="UAC"/>

Figure 4.2.9 Session timer

### 4.2.10. BLF List

Go to **Account - Advanced** to configure to display or configure BLF list URI address.

**BLF List URI:** BLF List is short for busy lamp field list.

BLFList	
BLFList URI	<input type="text"/>
BLFList Pickup Code	<input type="text"/>
BLFList BargeIn Code	<input type="text"/>

Figure 4.2.10 BLF list

**BLFList Pickup Code:** To set the BLF pick up code.

**BLFList Bargain Code:** To set the BLF barge in code.

### 4.2.11. Encryption

Go to **Account - Advanced** to configure.

If enabled, voice will be encrypted.

Encryption	
Voice Encryption(SRTP)	Disabled ▼

Figure 4.2.11 Encryption

### 4.2.12. NAT

Go to **Account - Advanced** to display NAT related settings.

**UDP Keep Alive message:** If enabled, 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:** Remote port, if enabled, it will add remote port into outgoing SIP message for designated account.

NAT	
UDP Keep Alive Messages	Disabled ▼
UDP Alive Msg Interval	30 (5~60s)
RPort	Disabled ▼

Figure 4.2.12 NAT

### 4.2.13. User Agent

Go to **Account - Advanced** to configure. One can customize user 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.

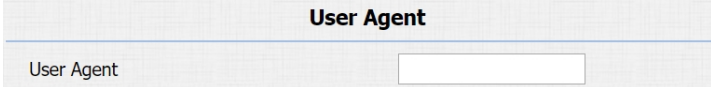
The screenshot shows a web form titled "User Agent". It contains a single input field labeled "User Agent" with a text cursor inside, ready for input.

Figure 4.2.13 User Agent

## 4.3. Access Control

### 4.3.1. Web Relay

R27 can support to connect to web relay.

Go to **Phone - WebRelay** to configure.

**Type:** Connect web relay and choose the type.

**IP Address:** Enter web relay's IP address.

**User Name:** it is an authentication for connecting web relay.

**Password:** It is an authentication for connecting web relay.

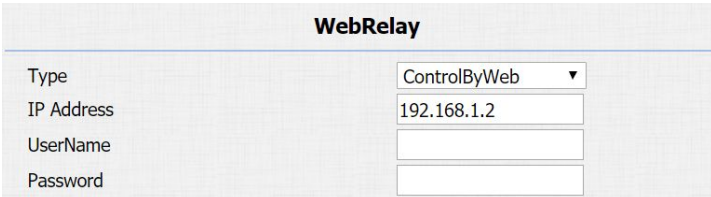
The screenshot shows a web form titled "WebRelay". It contains four fields: "Type" is a dropdown menu with "ControlByWeb" selected; "IP Address" is a text field containing "192.168.1.2"; "UserName" is an empty text field; and "Password" is an empty text field.

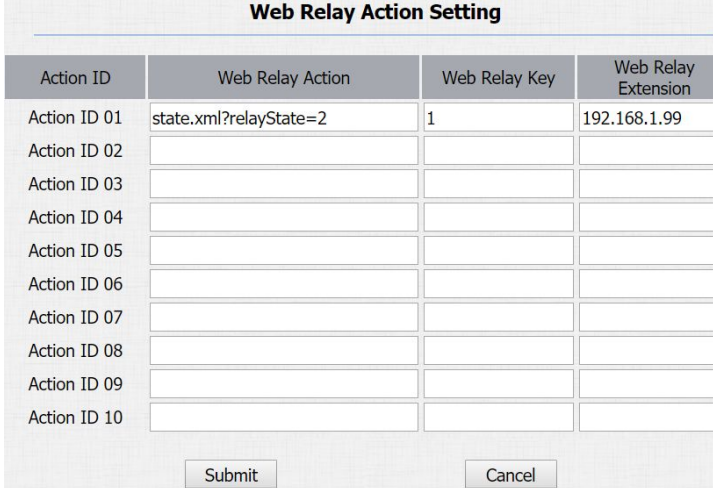
Figure 4.3.1-1 Web relay

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

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

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



The 'Web Relay Action Setting' form contains a table with 4 columns: Action ID, Web Relay Action, Web Relay Key, and Web Relay Extension. It has 10 rows for Action ID 01 to 10. Action ID 01 is pre-filled with 'state.xml?relayState=2', '1', and '192.168.1.99'. The other rows are empty. At the bottom are 'Submit' and 'Cancel' buttons.

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	state.xml?relayState=2	1	192.168.1.99
Action ID 02			
Action ID 03			
Action ID 04			
Action ID 05			
Action ID 06			
Action ID 07			
Action ID 08			
Action ID 09			
Action ID 10			

Figure 4.3.1-2 Web relay action settings

## 4.3.2. Wiegand

Using this feature to integrate with some wiegand access control. R27 can be used as wiegand input or output.

Go to **Intercom - Advanced** to configure.

**Wiegand Type:** Support Wiegand 26 or 34. The different number means different bits.



The 'Wiegand' configuration form has two fields: 'WiegandType' with a dropdown menu showing 'wiegand-26' and 'Wiegand Mode' with a dropdown menu showing 'Input'.

WiegandType	wiegand-26 ▼
Wiegand Mode	Input ▼

Figure 4.3.2 Wiegand

**Wiegand Mode:** Input or output. Typically, when users select input, we generally connect the wiegand input device, such as the wiegand card reader. Or R27 can be used as output, it is generally used to connect the third-party access control, and R27 change the card information as wiegand signal, and then transfer to the access control module.

## 4.4. Security

### 4.4.1. Anti-alarm

Go to **Intercom - Advanced** to configure.

**Tamper Alarm:** R27 integrates internal gravity sensor for its own security. After enabling tamper alarm, if the gravity of R27 changes dramatically, it will alarm. Gravity sensor threshold stands for sensitivity of sensor. Smaller the value, the more sensitive it is.

Tamper Alarm	
Tamper Alarm	Disabled ▼
Gravity Sensor Threshold	32 (0~127)

Figure 4.4.1 Anti-alarm

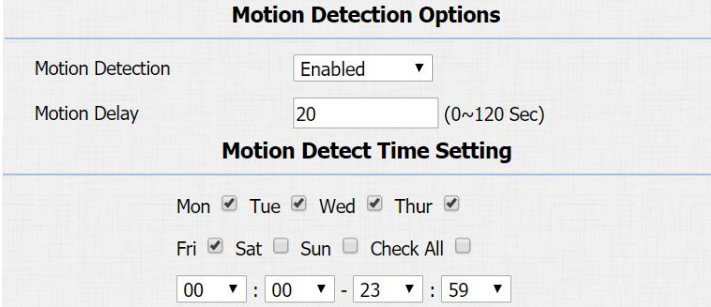
## 4.4.2. Motion

R27 supports motion detection, go to **Intercom - Motion** to configure detection related parameters.

**Motion Detection:** To enable or disable motion detection.

**Motion Delay:** To configure minimum time gap between two snapshots.

**Motion Detect Time Setting:** To configure motion detect time schedule.



The screenshot shows the 'Motion Detection Options' configuration page. It has two main sections. The first section, 'Motion Detection Options', contains 'Motion Detection' set to 'Enabled' and 'Motion Delay' set to '20' seconds, with a range of '(0~120 Sec)'. The second section, 'Motion Detect Time Setting', shows a weekly schedule: Monday, Tuesday, Wednesday, and Thursday are all checked; Friday is checked, while Saturday and Sunday are unchecked. There is also an unchecked 'Check All' option. At the bottom, a time range is set from '00:00' to '23:59' using dropdown menus.

Figure 4.4.2 Motion

## 4.4.3. Action

R27 supports to send notifications, snapshots via email and ftp transfer method, or calls via sip call method, when trigger specific actions.

### 4.4.3.1. Action Parameters

Go to **Intercom - Action** to set action receiver.



## Email Notification

**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 namer of SMTP service (usually it is same with sender's email address).

**SMTP password:** To configure password of SMTP service (usually it is the 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.

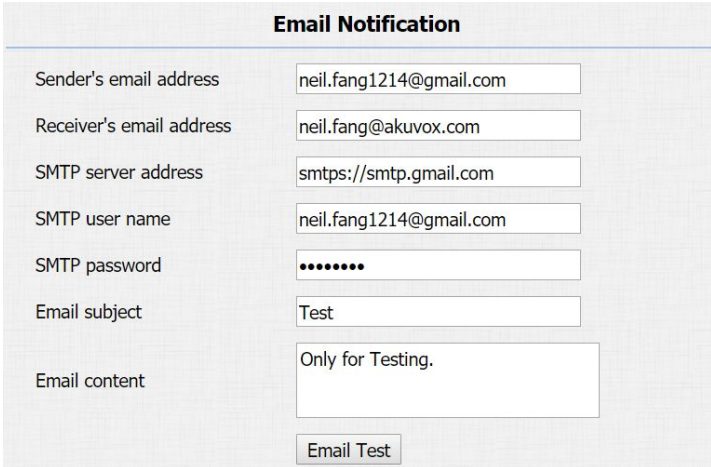
## FTP Notification

**FTP Server:** To configure URL of FTP server.

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

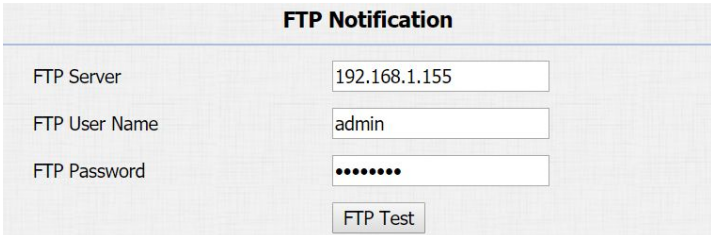
**FTP Password:** To configure password of FTP server.

**FTP Test:** To test whether FTP notification is available.



Email Notification	
Sender's email address	neil.fang1214@gmail.com
Receiver's email address	neil.fang@akuvox.com
SMTP server address	smtps://smtp.gmail.com
SMTP user name	neil.fang1214@gmail.com
SMTP password	.....
Email subject	Test
Email content	Only for Testing.
<button>Email Test</button>	

Figure 4.4.3.1-1 Email notification parameters



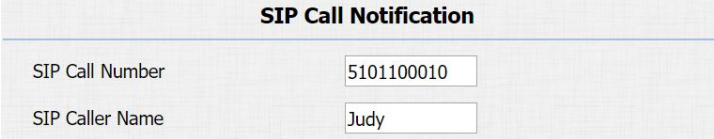
FTP Notification	
FTP Server	192.168.1.155
FTP User Name	admin
FTP Password	.....
<button>FTP Test</button>	

Figure 4.4.3.1-2 FTP notification parameters

## SIP Notification

**SIP Call Number:** To configure sip call number.

**SIP Call Name:** To configure display name of R27.



The screenshot shows a configuration form titled "SIP Call Notification". It contains two input fields: "SIP Call Number" with the value "5101100010" and "SIP Caller Name" with the value "Judy".

Figure 4.4.3.1-3 SIP call notification parameters

Five specific actions which will be triggered in R27:

### 4.4.3.2. No Answer Action

Go to **Intercom - Basic** to configure.

**No Answer Action:** For sending the notification to specified email if the call is not answered.



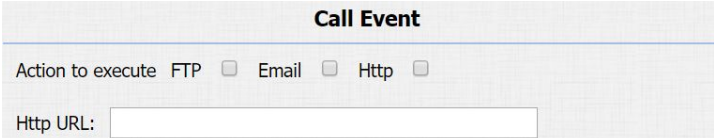
The screenshot shows a configuration field labeled "No Answer Action" with a dropdown menu set to "Disabled".

Figure 4.4.3.2 No answer action

### 4.4.3.3. Call Event

Go to **Intercom - Basic** to configure.

**Action to execute:** To choose suitable way to receive message or snapshot when dialing out.



The screenshot shows a configuration form titled "Call Event". It has three radio buttons for "Action to execute": "FTP", "Email", and "Http". Below these is a text field labeled "Http URL:".

Figure 4.4.3.3 Call event

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

#### 4.4.3.4. Input Interface Triggered Action

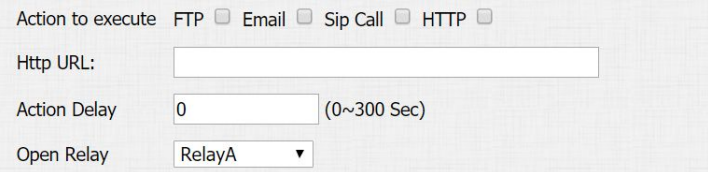
Go to **Intercom - Input** to configure.

**Action to execute:** To choose which action to execute after triggering.

**Http URL:** To configure URL, if HTTP action is chosen.

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

**Open relay:** To configure which relay to trigger.



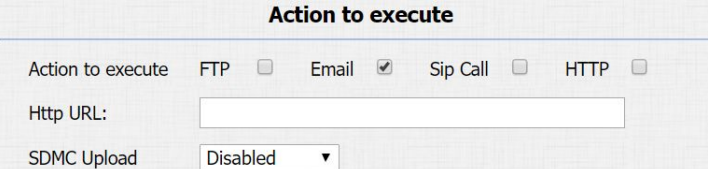
The screenshot shows a configuration form titled 'Input Interface Triggered Action'. At the top, there are four radio buttons for 'Action to execute': FTP, Email, Sip Call, and HTTP. The 'HTTP' radio button is selected. Below this, there is a text input field for 'Http URL:'. Underneath that is a numeric input field for 'Action Delay' with the value '0' and a range '(0~300 Sec)' to its right. At the bottom, there is a dropdown menu for 'Open Relay' with 'RelayA' selected.

Figure 4.4.3.4 Input interface triggered action

#### 4.4.3.5. Motion Triggered Action

Go to **Intercom - Motion** to configure.

**Action to execute:** To choose which action to execute after triggering.



The screenshot shows a configuration form titled 'Motion Triggered Action'. At the top, there are four radio buttons for 'Action to execute': FTP, Email, Sip Call, and HTTP. The 'Email' radio button is selected. Below this, there is a text input field for 'Http URL:'. Underneath that is a dropdown menu for 'SDMC Upload' with 'Disabled' selected.

Figure 4.4.3.5 Motion triggered action

**Http URL:** To configure URL, if HTTP action is chosen.

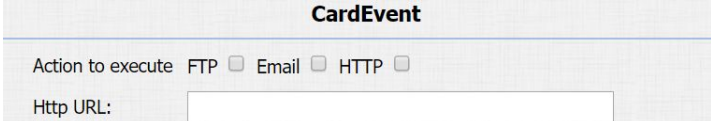
**SDMC Upload:** Upload the capture to the SDMC.

#### 4.4.3.6. Unlock via RFID Card Action

Go to **Intercom - Card Setting** to configure.

**Action to execute:** To choose which action to execute after unlocking via a RFID card.

**Http URL:** To configure URL, if HTTP action is chosen.



The screenshot shows a web form titled "CardEvent". It contains three radio buttons for "Action to execute": "FTP", "Email", and "HTTP". Below these is a text input field labeled "Http URL:".


Figure 4.4.3.6 Unlock via RFID card action

## 4.5. Upgrade

### 4.5.1. Web Upgrade

Go to **Upgrade - Basic** to do web upgrade.

**Upgrade:** Choose .rom firmware from the PC, and then click "Submit" to start update.



The screenshot shows a web form for "Web Upgrade". It displays "Firmware Version" as 27.0.3.64 and "Hardware Version" as 27.0.0.0.0.0.0.0. Below this is an "Upgrade" section with a "Choose File" button, the text "No file chosen", a "Submit" button, and a "Cancel" button.

Figure 4.5.1 Web upgrade

## 4.5.2. Autop Upgrade

Go to **Upgrade - Advanced** to configure automatically update server's settings.

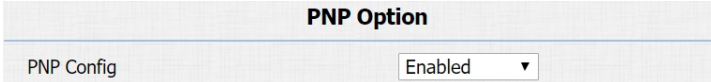
### PNP

Plug and Play, once PNP is enabled, the phone will send SIP subscription message to PNP server automatically to get auto provisioning server's address.

By default, this SIP message is sent to multicast address 224.0.1.75 (PNP server address by standard).

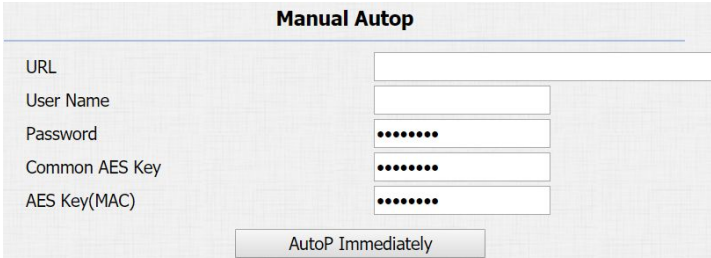
### Manual Autop

Autop is a centralized and unified upgrade for phones. It is also a simple and time-saving configuration for phones. It is mainly used by devices to download corresponding configuration documents from the server which is using TFTP / FTP / HTTP / HTTPS network protocol. Achieving the purpose for updating devices's configurations and making users to change the phone configuration



PNP Option	
PNP Config	Enabled ▼

Figure 4.5.2-1 PNP



Manual Autop	
URL	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Common AES Key	<input type="password"/>
AES Key(MAC)	<input type="password"/>
<input type="button" value="AutoP Immediately"/>	

Figure 4.5.2-2 Manual auto provision

more easily, it is a typical C/S architecture upgrade mode, which is mainly used 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.

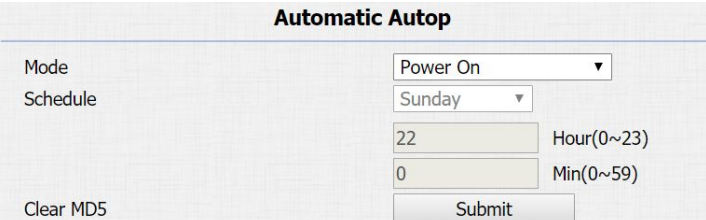
**Common AES Key:** Used for the phone to decipher common auto provisioning configuration file.

**AES Key (MAC):** Used for the phone to decipher MAC-oriented auto provisioning configuration file (for example, file name could be 0c1105888888.cfg if 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.



The screenshot shows a web-based configuration interface titled "Automatic Autop". It contains several input fields and a submit button. The "Mode" field is a dropdown menu currently set to "Power On". The "Schedule" field is a dropdown menu currently set to "Sunday". Below the schedule dropdown are two numeric input fields: the first is set to "22" and is labeled "Hour(0~23)", and the second is set to "0" and is labeled "Min(0~59)". At the bottom left is a "Clear MD5" link, and at the bottom right is a "Submit" button.

Automatic Autop	
Mode	Power On
Schedule	Sunday
	22 Hour(0~23)
	0 Min(0~59)
Clear MD5	Submit

Figure 4.5.2-3 Automatic provision

This auto provisioning mode is actually self-explanatory.

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

**Note:** Please refer to the related feature guide from forum.

### 4.5.3. Backup Config File

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

**Export Autop Template:** To export current config file.

**Others:** To export current config file (Encrypted) or import new config file.




Figure 4.5.3 Backup config file

## 4.6. Log

### 4.6.1. Call Log

Go to **Phone - Call Log**, users can see a list of call logs which have dialed, received or missed. Users can delete call logs from list.

Call History						
All						
Index	Type	Date	Time	Local Identity	Name	Number
1	Received	2018-09-30	08:28:46	192.168.35.1 0@192.168.35.10	192.168.35.68	192.168.35.6 8@192.168.35.68
2	Received	2018-09-30	08:26:40	192.168.35.1 0@192.168.35.10	192.168.35.68	192.168.35.6 8@192.168.35.68

Figure 4.6.1 Call log

## 4.6.2. Door Log

Go to **Phone - Door Log**, users can see a list of door logs which records card information and date.

## 4.6.3. System Log

Go to **Upgrade - Advanced** to configure 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. It's level 3 by default.

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

## 4.6.4. PCAP

Go to **Upgrade - Advanced** to start, stop packets capturing or to export captured packet file.

Door Log							
Index	Name	Code	Type	Date	Time	Status	
1	Courier	FFB59828	Card	2018-09-30	10:49:19	Failed	<input type="checkbox"/>
2	unKnown	1FEDBA28	Card	2018-09-30	10:49:16	Failed	<input type="checkbox"/>
3	Courier	FFB59828	Card	2018-09-30	10:49:09	Failed	<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>
11							<input type="checkbox"/>
12							<input type="checkbox"/>
13							<input type="checkbox"/>
14							<input type="checkbox"/>
15							<input type="checkbox"/>
Page 1 ▾   Prev   Next   Delete   Delete All							

Figure 4.6.2 Door log

System Log	
LogLevel	3 ▾
Export Log	Export

Figure 4.6.3 System log

PCAP	
PCAP	Start   Stop   Export
PCAP Auto Refresh	Disabled ▾

Figure 4.6.4 PCAP



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

**Stop:** To stop capturing packets.

## Abbreviations

**ACS:** Auto Configuration Server

**Auto:** Automatically

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

**ACD:** Automatic Call Distribution

**Autop:** Automatical Provisioning

**AES:** Advanced Encryption Standard

**BLF:** Busy Lamp Field

**COM:** Common

**CPE:** Customer Premise Equipment

**CWMP:** CPE WAN Management Protocol

**DTMF:** Dual Tone Multi-Frequency

**DHCP:** Dynamic Host Configuration Protocol

**DNS:** Domain Name System

**DND:** Do Not Disturb

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

**FTP:** File Transfer Protocol

**GND:** Ground

**HTTP:** Hypertext Transfer Protocol

**HTTPS:** Hypertext Transfer Protocol Secure

**IP:** Internet Protocol

**ID:** Identification

**IR:** Infrared

**LCD:** Liquid Crystal Display

**LED:** Light Emitting Diode

**MAX:** Maximum

**POE:** Power Over Ethernet

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

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

**PCAP:** Packet Capture

**PNP:** Plug and Play

**RFID:** Radio Frequency Identification

**RTP:** Real-time Transport Protocol

**RTSP:** Real Time Streaming Protocol

**MPEG:** Moving Picture Experts Group

**MWI:** Message Waiting Indicator

**NO:** Normal Opened

**NC:** Normal Connected

**NTP:** Network Time Protocol

**NAT:** Network Address Translation

**NVR:** Network Video Recorder

**ONVIF:** Open Network Video Interface Forum

**SIP:** Session Initiation Protocol

**SNMP:** Simple Network Management Protocol

**STUN:** Session Traversal Utilities for NAT

**SNMP:** Simple Mail Transfer Protocol

**SDMC:** SIP Devices Management Center

**TR069:** Technical Report069

**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](http://www.akuvox.com) or feel free to contact us by

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

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

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

**We highly appreciate your feedback about our products.**

