

**Akuvox** Smart  
Intercom



## R26B Door Phone Admin Guide

## About this manual

Thank you for choosing Akuvox's R26B door phone. This manual is intended for end users who need to properly configure the door phone. This manual is applicable to 26.31.4.xx version, and it provides all functions' configurations of R26B. 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. Making a Call	3
2.2. Receiving a Call	3
2.3. Unlock	4
2.3.1. Unlock by RFID Cards	4
2.3.2. Unlock by DTMF Codes	4
<b>3. Basic Setting</b>	<b>5</b>
3.1. Getting Started	5
3.1.1. IP Announcement	5
3.1.2. Access the device website	5
3.2. Password Modification	6

3.2.1. Modify the Web Password.....	6
3.3. Phone Configuration.....	6
3.3.1. Language.....	6
3.3.2. Time.....	7
3.3.3. Network.....	7
3.3.3.1. VLAN.....	9
3.3.3.2. TR069.....	10
3.3.4. Sound.....	11
3.3.5. DND.....	12
3.4. Intercom Call.....	13
3.4.1. Direct IP Call.....	13
3.4.2. SIP Call.....	14
3.4.2.1. SIP Account.....	14
3.4.2.2. SIP Server 1&2.....	15
3.4.2.3. Outbound Proxy Server.....	15
3.4.2.4. Transport Type.....	15
3.4.2.5. NAT.....	16

3.4.3. Auto Answer.....	16
3.4.4. Web Call.....	17
3.4.5. Push To Hang Up.....	17
3.5. Security.....	17
3.5.1. Live view.....	17
3.5.2. RTSP.....	18
3.5.3. ONVIF.....	19
3.6. Access Control.....	20
3.6.1. Relay.....	20
3.6.2. Card Setting.....	21
3.6.3. Open Relay via HTTP.....	22
3.6.4. Unlock via Exit Button.....	23
3.7. Reboot.....	24
3.8. Reset.....	24
<b>4. Advance Feature.....</b>	<b>25</b>
4.1. Phone Configuration.....	25
4.1.1. LED.....	25

4.1.2. IR LED.....	26
4.1.3. RF Card Code Display Related.....	27
4.2. Intercom.....	27
4.2.1. Call Time Related.....	27
4.2.2. Return Code When Refuse.....	28
4.2.3. SIP Call Related.....	28
4.2.4. Codec.....	29
4.2.5. DTMF.....	30
4.2.6. Session Timer.....	31
4.2.7. Encryption.....	31
4.2.8. NAT.....	31
4.2.9. User Agent.....	32
4.3. Access Control.....	33
4.3.1. Web Relay.....	33
4.4. Security.....	34
4.4.1. Anti-alarm.....	34
4.4.2. Motion.....	35

4.4.3. Action.....	35
4.4.3.1. Action Parameters.....	35
4.4.3.2. Push Button Action.....	37
4.4.3.3. Input Interface Triggered Action.....	38
4.4.3.4. Motion Triggered Action.....	38
4.4.3.5. Action URL.....	38
4.5. Upgrade.....	39
4.5.1. Web Upgrade.....	39
4.5.2. Autop Upgrade.....	40
4.5.3. Backup Config File.....	42
4.5.4. DHCP Option.....	42
4.6. Log.....	43
4.6.1. Call log.....	43
4.6.2. Door Log.....	43
4.6.3. System Log.....	43
4.6.4. PCAP.....	44

# 1. Product Overview

## 1.1. Product Description

Akuvox R26B is a SIP-compliant, hands-free, five buttons door phone. It can be connected with Akuvox indoor monitors for remote unlock control and monitor. Users can operate the indoor phone to communicate with visitors via voice and video. Users can also use RFID cards to unlock the door. It's applicable in villas, office and so on.

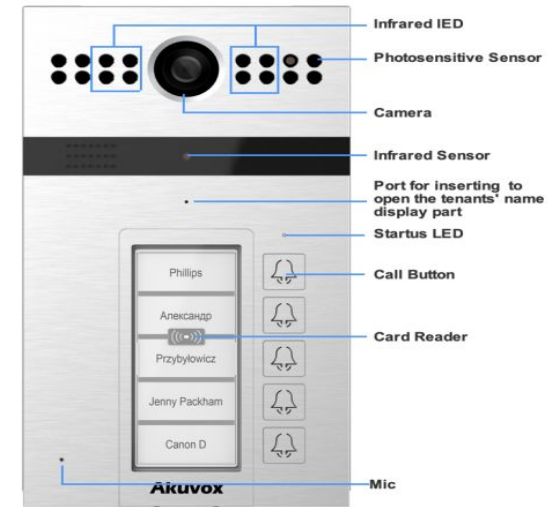


Figure 1.1 Product Description

## 1.2. Connector Introduction

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

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

**RS485 A/B:** RS485 terminal.

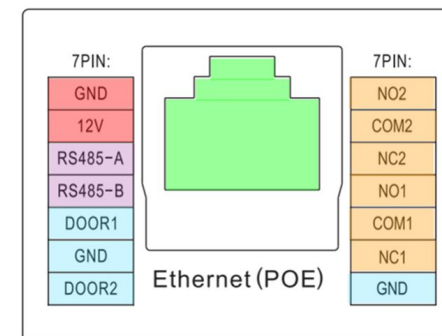


Figure 1.2-1 R26B's interface



**DOOR A/B:** Trigger signal input terminal.

**Relay A/B (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

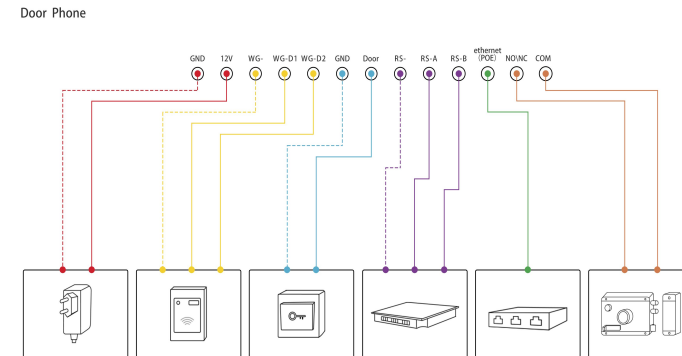


Figure 1.2-2 General interface

## 2. Daily Use

### 2.1. Making a Call

Press one of the call buttons to call out the predefined SIP account or IP address and if LED turns green, it means the call has been answered.

### 2.2. Receiving a Call

User can use IP phone or indoor monitor to call R26B and R26B will answer it automatically by default. If user disable auto answer, pressing button to answer incoming call.

## **2.3. Unlock**

### **2.3.1. Unlock by RFID Cards**

Place the predefined user cards in RFID card reader to unlock. Under normal conditions, R26B will announce “The door is now opened.” 13.56 MHz RF card is supported on R26B.

### **2.3.2. 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 Setting

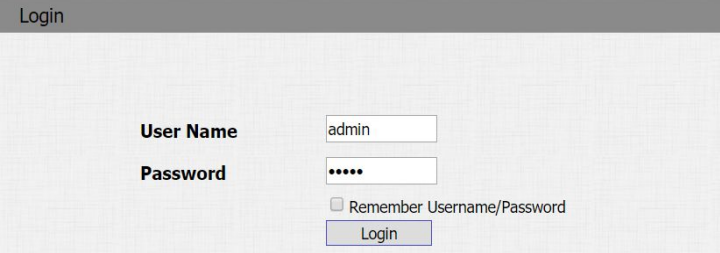
### 3.1. Getting Started

#### 3.1.1. IP Announcement

While R26B starts up normally, hold the top of call button for several seconds after the Status LED turns blue, voice system will enter IP announcement mode. In announcement mode, the IP address will be announced periodically and "IP 0.0.0.0" would be announced if no IP address is gained. Press call button again to quit the announcement mode.

#### 3.1.2. 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 User Name and Password are shown below:



Login

User Name admin

Password .....

Remember Username/Password

Login

Figure 3.1.2 Access the device website

User Name: **admin**

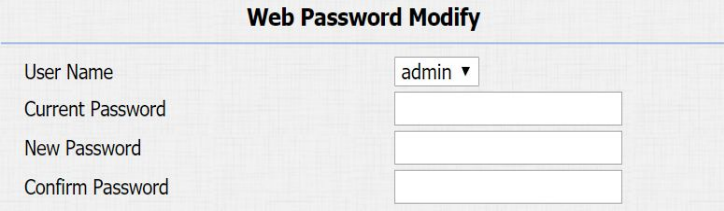
Password: **admin**

**Note:** The recommended browser is Google Chrome.

## 3.2. Password Modification

### 3.2.1. Modify the Web Password

Go to **Security - Basic** to modify password for webpage. To modify password for “admin” or “user” account.



Web Password Modify	
User Name	admin ▾
Current Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

Figure 3.2.1 Modify the web password

## 3.3. Phone Configuration

### 3.3.1. Language

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



Web Language	
Type	English ▾

Figure 3.3.1 Language

### 3.3.2. Time

Go to **Phone - Time/Lang** to configure it.

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

**Primary Server:** To configure primary NTP server address.

**Secondary Server:** To configure secondary NTP server address, it takes effect if primary NTP server is unreachable.

**Update Interval:** To configure interval between two consecutive NTP requests.

**System Time:** The current time of the phone.

NTP	
Time Zone	0 GMT
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	09:57:31

Figure 3.3.2 Time

### 3.3.3. Network

#### DHCP Mode

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

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 3.3.3.1 Static IP mode

R26B uses DHCP mode by default which will get IP address, subnet mask, default gateway and DNS server address from DHCP server automatically.

## Static IP Mode

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.

## 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.

Local RTP		
Starting RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

Figure 3.3.3-2 Local RTP

## 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 3.3.3-3 SNMP

### 3.3.3.1. VLAN

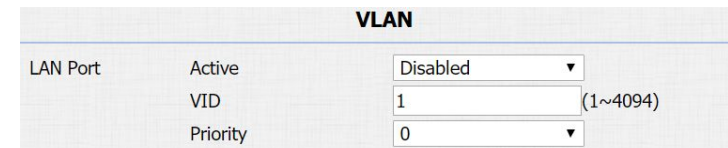
Go to **Network - Advanced** to configure.

**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.



VLAN	
LAN Port	Active Disabled ▼
VID	<input type="text"/> 1 (1~4094)
Priority	<input type="text"/> 0 ▼

Figure 3.3.3.1 VLAN



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

### 3.3.3.2. 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 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.

TR069		
ACS	Active	Disabled
	Version	1.0
	URL	
	User Name	
Periodic Inform	Password	*****
	Active	Disabled
	Periodic Interval	1800 (3~24x3600s)
CPE	URL	
	User Name	
	Password	*****

Figure 3.3.3.2 TR069

**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.

### 3.3.4. 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 opendoor tone by users themselves.

The screenshot displays a configuration page for sound settings. It is divided into five main sections: **Mic Volume**, **Speaker Volume**, **Open Door Warning**, **RingBack Upload**, and **Opendoor Tone Upload**. Each section contains a label, a value field, and a range indicator. The 'Mic Volume' and 'Speaker Volume' sections have input fields with the value '8' and a range of '(1~15)'. The 'Open Door Warning' section has a dropdown menu set to 'Enabled'. The 'RingBack Upload' and 'Opendoor Tone Upload' sections each have a 'Choose File' button, a 'No file chosen' status, and 'Upload', 'Delete', and 'Export' buttons. Below the file selection area, the file format is specified as 'wav, size: < 200KB, samplerate: 16000, Bits: 16'.

Figure 3.3.4 Sound

### 3.3.5. DND

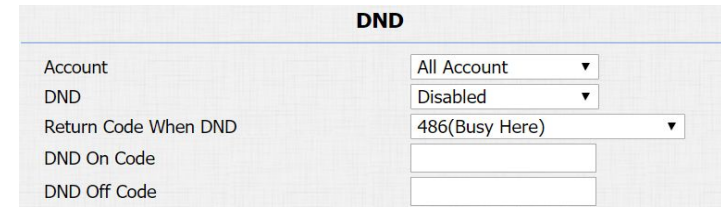
Go to **Phone - Call Feature** to configure DND feature.

**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 3.3.5 DND

## 3.4. Intercom Call

### 3.4.1. Direct IP Call

Without sip server, users can also use IP address to call each other, but this way is only suitable in the LAN.

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

Go to **Intercom - Basic** to configure the IP address of the destination(E.g.IP address 192.168.10.91).One button for each button.After, press the push button to make direct IP call.

**Note:** The push button number can also enter the SIP account.



Figure 3.4.1-1 Direct IP call

Push Button				
Key	Number1	Number2	Number3	Number4
Push Button 1	192.168.10.91	100		
Push Button 2	192.168.10.5			
Push Button 3	100			
Push Button 4	101			
Push Button 5	102			

Figure 3.4.1-2 Push button

## 3.4.2. 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.

### 3.4.2.1. SIP Account

**Status:** To display register result.

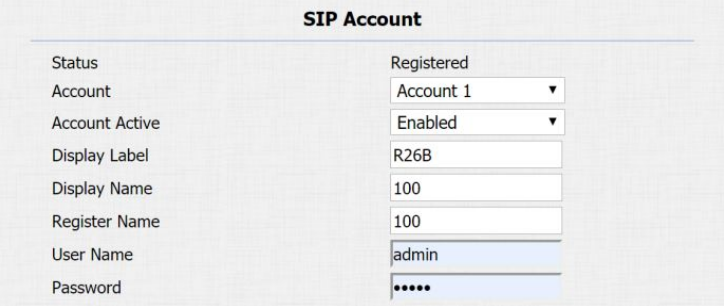
**Display Label:** To configure label displayed.

**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.



The screenshot shows a web form titled "SIP Account" with the following fields and values:

SIP Account	
Status	Registered
Account	Account 1
Account Active	Enabled
Display Label	R26B
Display Name	100
Register Name	100
User Name	admin
Password	*****

Figure 3.4.2.1 SIP Account

### 3.4.2.2. 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.

### 3.4.2.3. Outbound Proxy Server

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

### 3.4.2.4. 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.

The screenshot shows two configuration sections for SIP servers. The first section, titled 'SIP Server 1', contains two rows: 'Server IP' with a text input field containing '120.78.230.239' and a 'Port' dropdown set to '5070'; and 'Registration Period' with a text input field containing '1800' and a range '(30~65535s)'. The second section, titled 'SIP Server 2', also contains two rows: 'Server IP' with an empty text input field and a 'Port' dropdown set to '5060'; and 'Registration Period' with a text input field containing '1800' and a range '(30~65535s)'.

Figure 3.4.2.2 SIP server 1&2

The screenshot shows the 'Outbound Proxy Server' configuration section. It contains three rows: 'Enable Outbound' with a dropdown menu set to 'Disabled'; 'Server IP' with an empty text input field and a 'Port' dropdown set to '5060'; and 'Backup Server IP' with an empty text input field and a 'Port' dropdown set to '5060'.

Figure 3.4.2.3 Outbound proxy server

The screenshot shows the 'Transport Type' configuration section. It contains one row: 'Transport Type' with a dropdown menu set to 'UDP'.

Figure 3.4.2.4 Transport type

- **TLS:** Secured and reliable transport layer protocol.
- **DNS-SRV:** DNS record for specifying the location of services.

### 3.4.2.5. NAT

To display and configure NAT settings.

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

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

After configuring SIP call related parameters, users can refer to the direct IP call part to dial out a SIP call.

### 3.4.3. Auto Answer

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



NAT	
NAT	Disabled ▼
Stun Server Address	<input type="text"/>
Port	3478

Figure 3.4.2.5 NAT



Auto Answer	Enabled ▼
-------------	-----------

Figure 3.4.3 Auto answer

### 3.4.4. Web Call

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

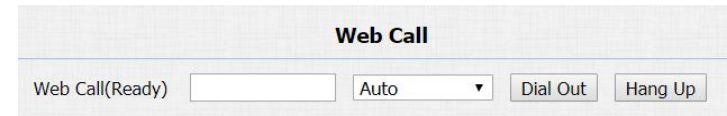


Figure 3.4.4 Web call

### 3.4.5. Push To Hang Up

Go to **Intercom - Basic** to configure. To enable or disable pushing button to hang up.

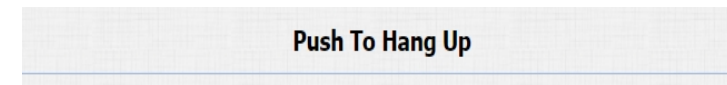


Figure 3.4.5 Push to hang up

## 3.5. Security

### 3.5.1. Live view

Go to **Intercom - Live Stream** to check the real-time video from R26B.

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 3.5.1 Live view



### 3.5.2. RTSP

R26B 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. R26B 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

The screenshot displays a configuration page for RTSP. It is organized into four main sections, each with a title bar: **RTSP Basic**, **RTSP Stream**, **H.264 Video Parameters**, and **MPEG4 Video Parameters**. In the **RTSP Basic** section, the 'RTSP Server Enabled' checkbox is checked. The **RTSP Stream** section shows 'RTSP Video Enabled' checked and 'RTSP Video Codec' set to 'H.264'. The **H.264 Video Parameters** section includes 'Video Resolution' (VGA), 'Video Framerate' (30 fps), and 'Video Bitrate' (2048 kbps). The **MPEG4 Video Parameters** section also includes 'Video Resolution' (VGA), 'Video Framerate' (30 fps), and 'Video Bitrate' (2048 kbps).

Figure 3.5.2 RTSP

less core program space. To modify the resolution, framerate and bitrate of MPEG4.

### 3.5.3. ONVIF

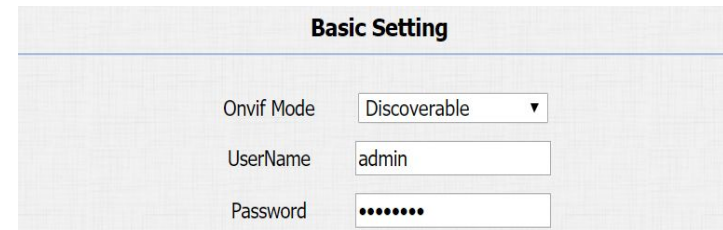
R26B supports ONVIF protocol, which means R26B's camera can be searched by other devices, like NVR which supports ONVIF protocol as well.

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.**



The screenshot shows a web interface titled "Basic Setting". It contains three configuration fields: "Onvif Mode" with a dropdown menu set to "Discoverable", "UserName" with a text input field containing "admin", and "Password" with a text input field containing seven dots.

Figure 3.5.3 ONVIF

## 3.6. Access Control

### 3.6.1. Relay

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

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

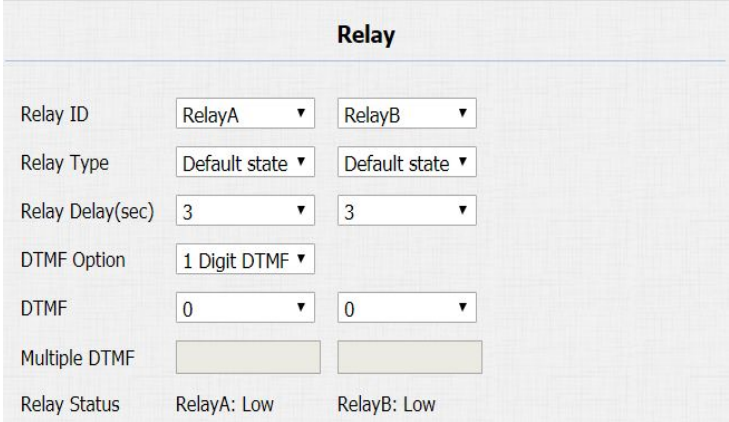
**Relay ID:**R26B supports two relays, users can configure them respectively.

**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.

**DTMF Option:** To select digit of DTMF code, R26B supports maximum 4 digits DTMF code.

**DTMF:**To configure 1 digit DTMF code for remote unlock.



The screenshot shows a configuration page titled "Relay" with two columns for "RelayA" and "RelayB". The settings are as follows:

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

Figure 3.6.1 Relay

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

**Relay Status:**Low means that COM is connecting to NC while High means that COM is connecting to NO.

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

### 3.6.2. Card Setting

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

Import/Export Card Data

R26B 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 template RFID cards data file.

#### Obtain and Add Card

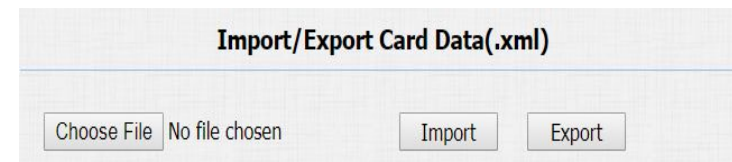


Figure 3.6.2-1 Card setting

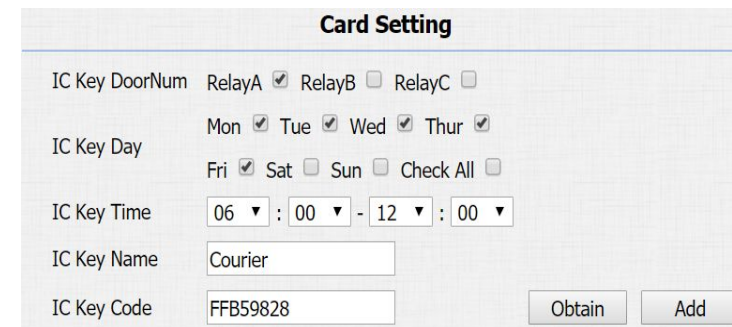


Figure 3.6.2-2 Card setting

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

**Note:** Users can use card to access only when card status has been switched to “Normal”.

### 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.

Index	Name	Code	Door	
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 3.6.2-3 Card setting

### 3.6.3. Open Relay via HTTP

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.

Open Relay via HTTP

Switch: Disabled ▾

UserName:

Password:

Figure 3.6.3 Open relay via HTTP

**URL format:**

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

### 3.6.4. Unlock via Exit Button

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

R26B supports two input triggers Input A/B (DOOR A/B).

**Input Service:** To enable or disable input trigger service.

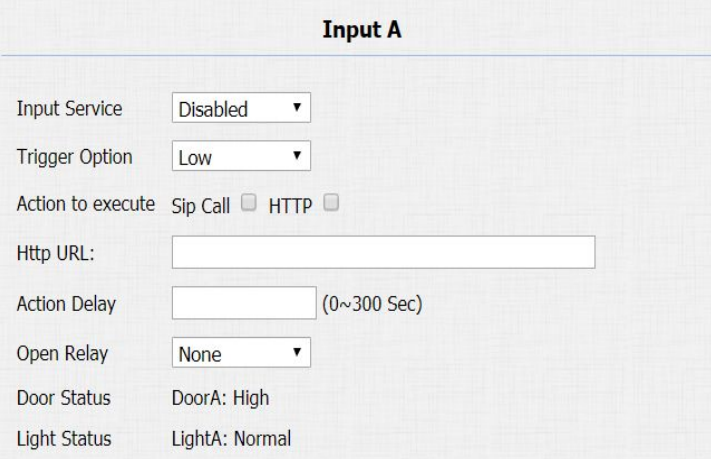
**Trigger Option:** To choose open circuit trigger or closed circuit trigger. Low means that connection between door terminal and GND is closed, while high means the connection is opened.

**Action to execute:** To choose which action to execute after the input terminal is triggered.

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

**Open Relay:** To configure relay to open.

**Door Status:** To show the status of input signal.



Input A	
Input Service	Disabled
Trigger Option	Low
Action to execute	Sip Call <input type="checkbox"/> HTTP <input type="checkbox"/>
Http URL:	<input type="text"/>
Action Delay	<input type="text"/> (0~300 Sec)
Open Relay	None
Door Status	DoorA: High
Light Status	LightA: Normal

Figure 3.6.4 Unlock via exit button

## 3.7. Reboot

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

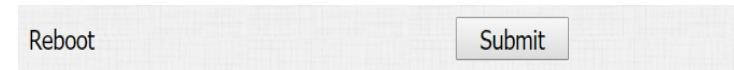


Figure 3.7 Reboot

## 3.8. Reset

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



Figure 3.8.Reset

## 4. Advance Feature

### 4.1. Phone Configuration

#### 4.1.1. LED

Go to **Intercom - LED** Setting to configure the LED status. To setup the LED lighting mode.

**State:** There is five states: Normal, Offline, Calling, Talking and Receiving.

**Color Off:** The default status is OFF.

**Color On:** It can support three color: Red, Green, Blue.

**Blink Mode:** To setup the different blink frequency.

#### LED Control:

Use HTTP URL to remote control the LED status.

#### Http format:



State	Color Off	Color On	Blink Mode
NORMAL	OFF	Blue	Always On
OFFLINE	OFF	Red	2500/2500
CALLING	OFF	Blue	2500/2500
TALKING	OFF	Green	Always On
RECEIVING	OFF	Green	2500/2500

Figure 4.1.1-1 LED



LED Control: Disabled

Figure 4.1.1-2 LED



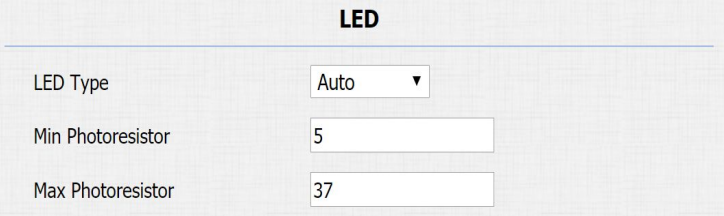
<http://PhoneIP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500>

**Status:** 1=Idle; 2=OffLine; 3=Calling; 4=Talking; 5=Receiving; **Color:** 1=Green; 2=Blue; 3=Red; **Mode:** 0=Always On; 1=Always Off; 500/1000/1500/2000/25000/3000

### 4.1.2. IR LED

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

**Photoresistor:** The setting is for night vision, when the surrounding of R26B is very dark, infrared LED will turn on and R26B will turn to night mode. Photoresistor value relates to light intensity and larger value means that light intensity is smaller. Users can configure the Min and Max bound and when photoresistor value is larger than Max bound, infrared LED will turn on. As contrast, when photoresistor value is smaller than Min bound, infrared LED will turn off and device turns to normal mode.



LED	
LED Type	Auto ▼
Min Photoresistor	5
Max Photoresistor	37

Figure 4.1.2 IR LED

### 4.1.3. RF Card Code Display Related

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

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



The screenshot shows a configuration panel titled "RFID". Below the title, there is a label "RFID Display Mode" followed by a dropdown menu. The dropdown menu is currently set to "8HN".

Figure 4.1.3 RF card code display related

## 4.2. Intercom

### 4.2.1. Call Time Related

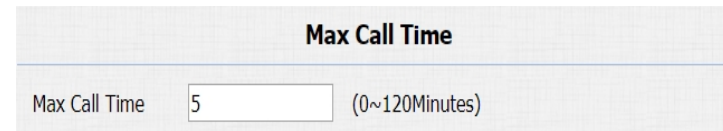
Go to **Intercom - Basic** to configure.

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

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

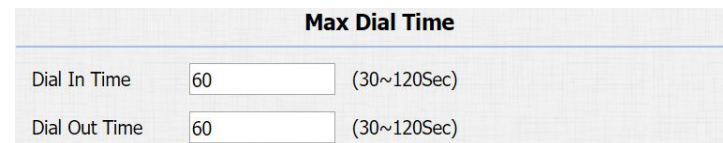
**Dial Out Time:** To configure the max no answer call time.

**Hang Up After Open Door:** To set the time that hang up the call after open the door.




The screenshot shows a configuration panel titled "Max Call Time". Below the title, there is a label "Max Call Time" followed by a text input field containing the number "5" and a unit indicator "(0~120Minutes)".

Figure 4.2.1-1 Call time related



The screenshot shows a configuration panel titled "Max Dial Time". Below the title, there are two rows. The first row has a label "Dial In Time", a text input field containing "60", and a unit indicator "(30~120Sec)". The second row has a label "Dial Out Time", a text input field containing "60", and a unit indicator "(30~120Sec)".

Figure 4.2.1-2 Call time related



The screenshot shows a configuration panel titled "Hang Up After Open Door". Below the title, there is a label "Time Out" followed by a text input field containing the number "5" and a unit indicator "(0~15)".

Figure 4.2.1-3 Hang up after open door

## 4.2.2. Return Code When Refuse

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.



Return Code When Refuse	486(Busy Here) ▼
-------------------------	------------------

Figure 4.2.2 Return code when refuse

## 4.2.3. SIP Call Related

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

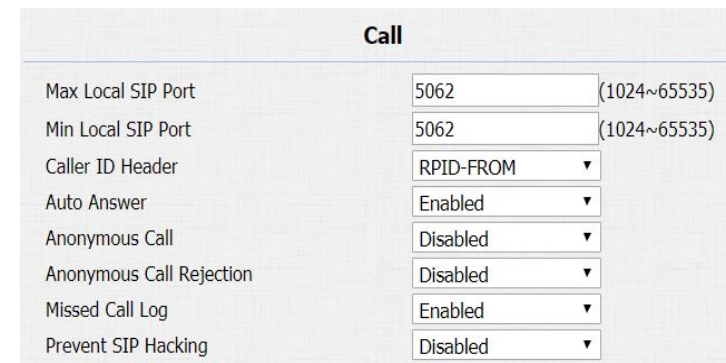
**Max Local SIP Port:** To configure maximum local SIP port for designated SIP account.

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

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

**Anonymous Call:** If enabled, R26B will block its information when calling out.

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



Call		
Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)
Caller ID Header	RPID-FROM	▼
Auto Answer	Enabled	▼
Anonymous Call	Disabled	▼
Anonymous Call Rejection	Disabled	▼
Missed Call Log	Enabled	▼
Prevent SIP Hacking	Disabled	▼

Figure 4.2.3 SIP call related

**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.

### 4.2.4. Codec

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

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

**Audio Codec:**R26B support four audio codec: PCMA, PCMU, G729, G722. Different audio codec requires 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

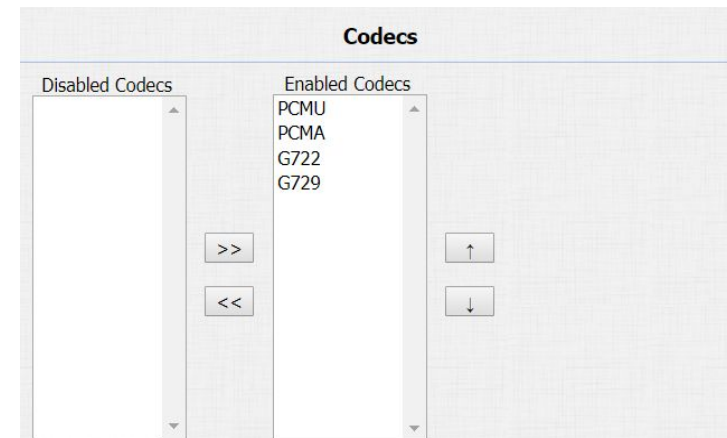


Figure 4.2.4-1 Codec

G729	8kbit/s	8kHz
G722	64kbit/s	16kHz

**Video Codec:** R26B supports H.264 standard, which provides better video quality at substantially lower bit rates than previous standards.

**Codec Resolution:** R26B 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.

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

### 4.2.5. 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.

The screenshot shows a configuration panel titled "Video Codec". It contains four rows of settings: "Codec Name" with a checked checkbox for "H264"; "Codec Resolution" with a dropdown menu set to "4CIF"; "Codec Bitrate" with a dropdown menu set to "2048"; and "Codec Payload" with a dropdown menu set to "104".

Figure 4.2.4-2 Codec

The screenshot shows a configuration panel titled "Multicast Codec" with a single dropdown menu set to "PCMU".

Figure 4.2.4-3 Codec

The screenshot shows a configuration panel titled "DTMF". It contains three rows of settings: "Type" with a dropdown menu set to "RFC2833"; "How To Notify DTMF" with a dropdown menu set to "Disabled"; and "DTMF Payload" with a text input field containing "101" and a range indicator "(96~127)".

Figure 4.2.5 DTMF

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

**DTMF Payload:** To configure payload type for DTMF.

## 4.2.6. Session Timer

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

If enabled, the on going call will be disconnected automatically once the session expired unless it's been refreshed by UAC or UAS.

## 4.2.7. Encryption

Go to **Account - Advanced** to configure it. If enabled, voice will be encrypted.

## 4.2.8. NAT

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

**UDP Keep Alive message:** If enabled, R26B will send UDP keep-alive message periodically to router to keep NAT port alive.

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

Figure 4.2.6 Session timer

Encryption	
Voice Encryption(SRTP)	Disabled ▼

Figure 4.2.7 Encryption

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

Figure 4.2.8 NAT

**UDP Alive Msg Interval:** Keep alive message interval.

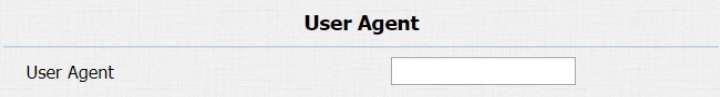
**Rport:** Remote Port, if enabled, it will add remote port into outgoing SIP message for designated account.

## 4.2.9. User Agent

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

To customize user agent field in the SIP message.

If users agent is set to specific value, users could see the information from network package. If user agent is not set by default, users could see the company name, model number and firmware version from network package.



The image shows a configuration interface for the 'User Agent' field. The title 'User Agent' is centered at the top. Below it, there is a label 'User Agent' on the left and an empty text input box on the right.

Figure 4.2.9 User agent

## 4.3. Access Control

### 4.3.1. Web Relay

R26B can support extra web relay which is connected with the door phone via network.

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

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

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

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

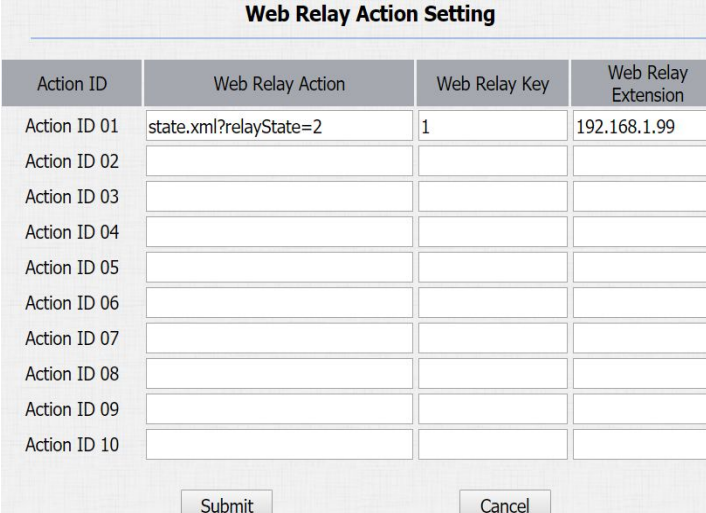
**Password:** It is an authentication for connecting web relay.

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



Figure 4.3.1-1 Web relay



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



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

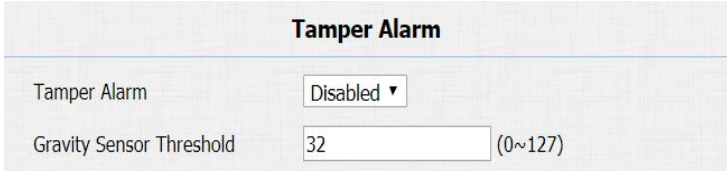
**Note:** Users can modify username and password in web relay website.

## 4.4. Security

### 4.4.1. Anti-alarm

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

R26B integrates internal gravity sensor for the own security, and after enabling tamper alarm, if the gravity of R26B changes dramatically, the phone will alarm. Gravity sensor threshold stands for sensitivity of sensor.



The screenshot shows a configuration panel titled "Tamper Alarm". It contains two settings: "Tamper Alarm" is set to "Disabled" via a dropdown menu, and "Gravity Sensor Threshold" is set to "32" in a text input field, with a range of "(0~127)" indicated to the right.

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

Figure 4.4.1 Anti-alarm

## 4.4.2. Motion

R26B supports motion detection, go to **Intercom - Motion** to configure detection parameter.

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

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

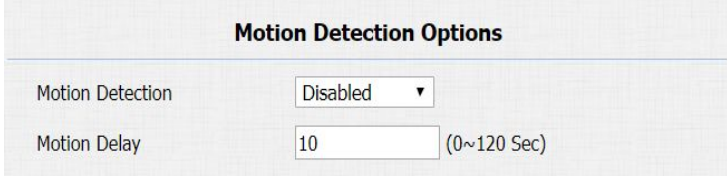
**Motion Detect Time Setting:** To make motion detect time for a whole week.

## 4.4.3. Action

R26B supports to send notifications, snapshots via email and ftp transfer method, or calls via SIP call method, when trigger specific actions.

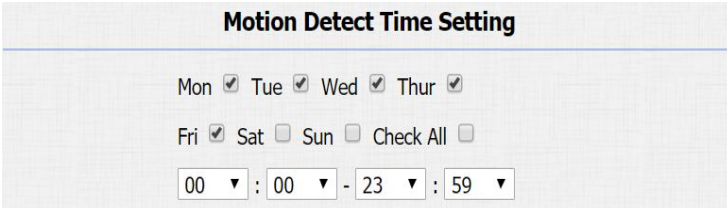
### 4.4.3.1. Action Parameters

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



The screenshot shows a configuration panel titled "Motion Detection Options". It contains two settings: "Motion Detection" is set to "Disabled" via a dropdown menu, and "Motion Delay" is set to "10" seconds, with a range of "(0~120 Sec)" indicated to the right.

Figure 4.4.2-1 Motion



The screenshot shows a configuration panel titled "Motion Detect Time Setting". It features a row of checkboxes for days of the week: Mon (checked), Tue (checked), Wed (checked), and Thur (checked). Below this is another row: Fri (checked), Sat (unchecked), Sun (unchecked), and a "Check All" checkbox (unchecked). At the bottom, there are four dropdown menus for time selection, showing "00 : 00 - 23 : 59".

Figure 4.4.2-2 Motion

## 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 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.

## 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.

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

- Sender's email address:
- Receiver's email address:
- SMTP server address:
- SMTP user name:
- SMTP password:
- Email subject:
- Email content:
- Email Test:

Figure 4.4.3.1-1 Action parameters

The screenshot shows two web forms. The top form is titled "FTP Notification" and contains the following fields and controls:

- FTP Server:
- FTP User Name:
- FTP Password:
- FTP Test:

The bottom form is titled "SIP Call Notification" and contains the following fields and controls:

- SIP Call Number:
- SIP Caller Name:

Figure 4.4.3.1-2 Action parameters

## SIP Call Notification

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

**SIP Call Name:** To configure display name of R26B.

Three specific actions which will be triggered in R26B:

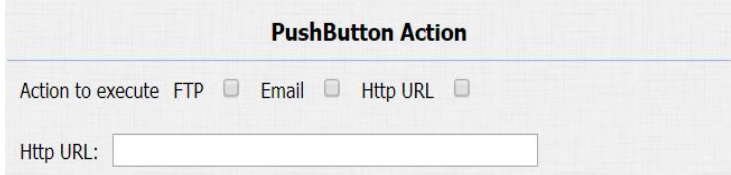
### 4.4.3.2. Push Button Action

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

Enable this function, the device will record any changes of the surrounding environment then send the message or picture to the corresponding receiver.

**Action to execute:** Tick the suit the suitable way to receive the action message.

**HTTP URL:** If you tick HTTP URL, and then enter the HTTP server IP address in the HTTP URL area. When the device detects any changes, it will send HTTP network package.



The screenshot shows a configuration window titled "PushButton Action". It contains three radio button options for "Action to execute": "FTP", "Email", and "Http URL". Below these options is a text input field labeled "Http URL:".

Figure 4.4.3.2 PushButton action

### 4.4.3.3. 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.

### 4.4.3.4. Motion Triggered Action

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

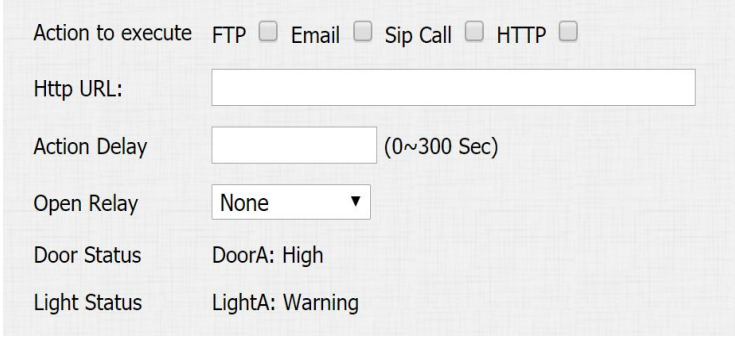
**Action to execute:** To choose which action to execute after triggering.

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

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

### 4.4.3.5. Action URL

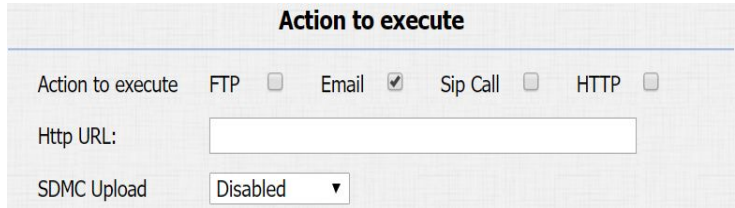
Action URL can be triggered by some predefined incidents.



The screenshot shows a configuration form for 'Input Interface Triggered Action'. It includes the following fields and options:

- Action to execute:** Radio buttons for FTP, Email, Sip Call, and HTTP.
- Http URL:** A text input field.
- Action Delay:** A text input field with a range of (0~300 Sec).
- Open Relay:** A dropdown menu currently set to 'None'.
- Door Status:** A text field set to 'DoorA: High'.
- Light Status:** A text field set to 'LightA: Warning'.

Figure 4.4.3.3 Input interface trigger action



The screenshot shows a configuration form for 'Motion Triggered Action'. It includes the following fields and options:

- Action to execute:** Radio buttons for FTP, Email (checked), Sip Call, and HTTP.
- Http URL:** A text input field.
- SDMC Upload:** A dropdown menu currently set to 'Disabled'.

Figure 4.4.3.4 Motion trigger action

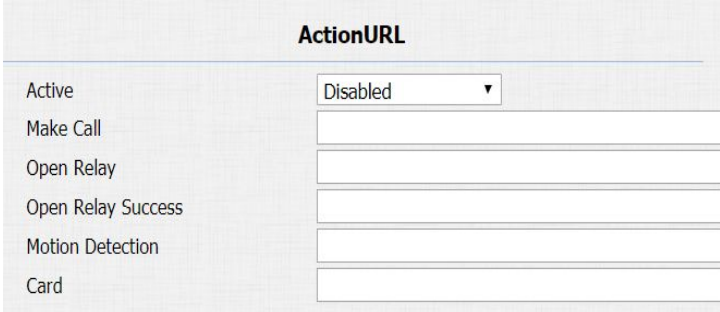
Go to **Phone - Action URL**, pick Active to be “Enabled”, pick to demand triggered incident, each “HTTP” request to have to including the key and value, use “=” to separate, each value starting with “\$.” For example, “Open Relay Success” incident, input `http://server IP address/help.xml?mac=$mac`, when the relay of R26B is triggered successfully, the phone will send a HTTP packet to the server, through the HTTP package to know the MAC of the phone.

## 4.5. Upgrade

### 4.5.1. Web Upgrade

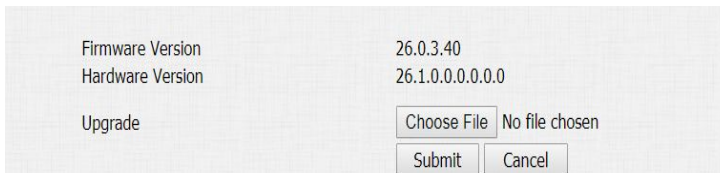
Go to **Upgrade - Basic**, users can upgrade firmware. Reset to factory setting and reboot.

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



ActionURL	
Active	Disabled
Make Call	
Open Relay	
Open Relay Success	
Motion Detection	
Card	

Figure 4.4.3.5 Action URL



Firmware Version	26.0.3.40
Hardware Version	26.1.0.0.0.0.0.0
Upgrade	<input type="button" value="Choose File"/> No file chosen
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Figure 4.5.1 Web update

## 4.5.2. Autop Upgrade

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

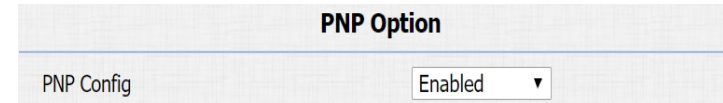
### PNP Option

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).

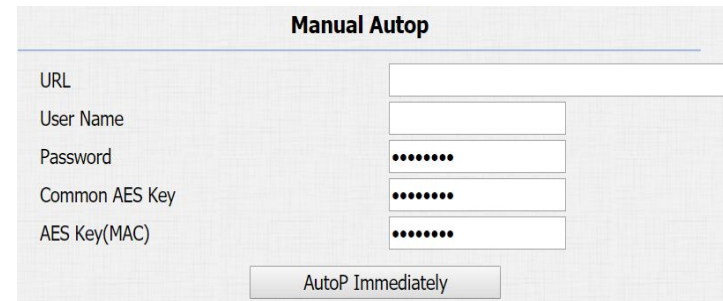
### Manual Autop

Autop (Auto-Provisioning) is a centralized and unified upgrade of telephone. It is a simple and time-saving configuration for 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 users to change the phone



The screenshot shows a configuration panel titled "PNP Option". Below the title, there is a label "PNP Config" followed by a dropdown menu currently set to "Enabled".

Figure 4.5.2-1 Autop update



The screenshot shows a configuration panel titled "Manual Autop". It contains five input fields: "URL", "User Name", "Password", "Common AES Key", and "AES Key(MAC)". The "Password", "Common AES Key", and "AES Key(MAC)" fields are masked with dots. Below the input fields is a button labeled "AutoP Immediately".

Figure 4.5.2-2 Autop update

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 phone to decipher common auto provisioning configuration file.

**AES Key (MAC):** Used for 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.

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

Figure 4.5.2-3 Autop update



This auto provisioning mode is actually self-explanatory.  
For example, mode "Power on" means phone will go to do provisioning every time it powers on.

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

### 4.5.4. 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.



Figure 4.5.3-1 Backup config file

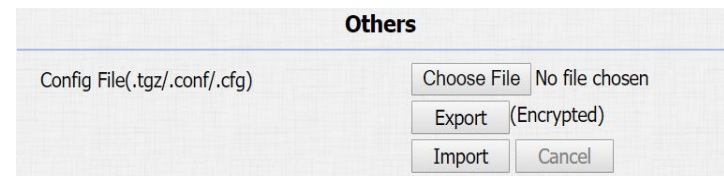


Figure 4.5.3-2 Backup config file

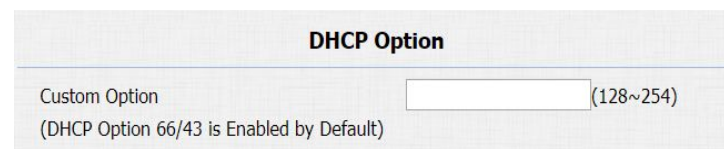


Figure 4.5.4 DHCP Option

**Note:** To make DHCP autop URL works, the PNP should be disable.

## 4.6. Log

### 4.6.1. Call log

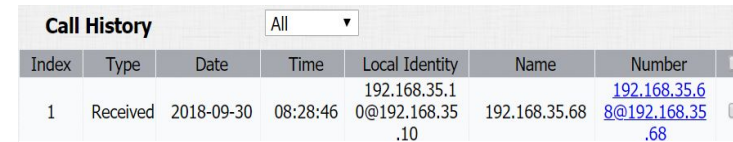
Go to **Phone - Call Log**, users can see a list of call log which have dialed, received or missed. Users can delete calls from list.

### 4.6.2. Door Log

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

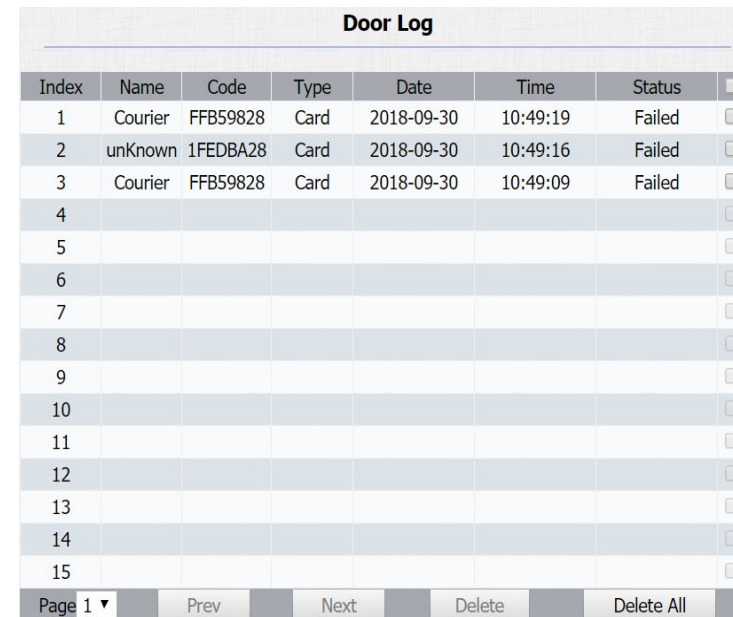
### 4.6.3. System Log

Go to **Upgrade - Advanced** to configure system log level and export system log file.



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	<a href="#">192.168.35.6</a> <a href="#">8@192.168.35</a> .68	<input type="checkbox"/>

Figure 4.6.1 Call log



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 level:** From level from 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.

### 4.6.4. PCAP

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

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

**Stop:** To stop capturing packets.

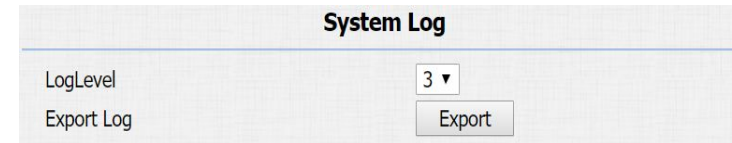


Figure 4.6.3 System log

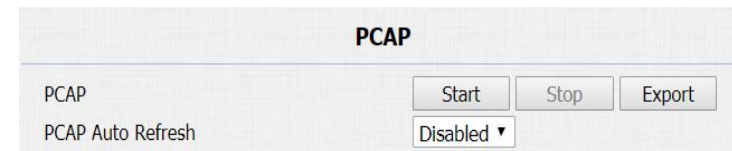


Figure 4.6.4 PCAP

## Abbreviations

**ACS:**Auto Configuration Server

**Auto:**Automatically

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

**ACD:**Automatic Call Distribution

**Autop:**Automatic 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  
**SMTP:** 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.**

