

Akuvox Smart
Intercom



R20K Door PhoneAdmin Guide

About This Manual

Thank you for choosing Akuvox's R20Kdoor phone. This manual is intended for end users who need to properly configure the door phone. This manual is applicable to 20.30.3.xx version, and it provides all functions' configurations of R20K. Please visit Akuvox forum or consult technical support for any new information or latest firmware.

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

Content

1. Product Overview	1
1.1. Product Description	1
1.2. Connector Introduction	1
2. Daily Use	3
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	5
2.3.4. Unlock by DTMF Codes	5
3. Basic Features	6
3.1. Access the Website Setting	6
3.1.1. Obtain IP Address	6
3.1.2. Access the Device Website	6
3.2. Password Modification	7

3.2.1. Modify the Device Admin Code	7
3.2.2. Modify the Web Password	7
3.3. Phone Configuration	7
3.3.1. Language	7
3.3.2. Time	8
3.3.3. Network	8
3.3.4. Sound	9
3.4. Intercom Call	9
3.4.1. Direct IP Call	9
3.4.2. SIP Call	10
3.4.3. SIP Account	10
3.4.4. SIP Server 1&2	11
3.4.5. Outbound Proxy Server	11
3.4.6. Transport Type	12
3.4.7. NAT	12
3.4.8. Speed Dial	13
3.4.9. Auto Answer	13

3.4.10. Web Call	14
3.5. Security	14
3.5.1. Live view	14
3.5.2. RTSP	14
3.5.3. ONVIF	16
3.6. Access Control	16
3.6.1. Unlock via DTMF	16
3.6.2. Unlock via RFID Card.....	18
3.6.3. Unlock via Pin Code	19
3.6.4. Unlock via HTTP command	21
3.6.5. Unlock via Exit Button.....	21
3.7. Reboot	22
3.8. Reset.....	22
4. Advanced Features	23
4.1. Phone Configuration	23
4.1.1. LED.....	23
4.1.2. IR LED	23

4.1.3. RFID Card Code Display Related	24
4.2. Intercom	25
4.2.1. Call Time Related	25
4.2.2. SIP Call Related.....	25
4.2.3. Codec	26
4.2.4. DTMF.....	28
4.2.5. Session Timer	28
4.2.6. Encryption.....	29
4.2.7. NAT	29
4.2.8. User Agent.....	29
4.3. Access Control	30
4.3.1. Web Relay	30
4.3.2. Wiegand.....	31
4.4. Security	32
4.4.1. Anti-alarm.....	32
4.4.2. Motion	32
4.4.3. Action	33

4.5. Upgrade	36
4.5.1. Web Upgrade	36
4.5.2. Autop Upgrade	36
4.5.3. Backup Config File	37
4.6. Log	38
4.6.1. Call Log	38
4.6.2. Door Log	38
4.6.3. System Log	38
4.6.4. PCAP	39

1. Product Overview

1.1. Product Description

Akuvox R20K 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



Figure 1.1 Product Description

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.

WG_D0/WG_D1: Wiegand terminal.

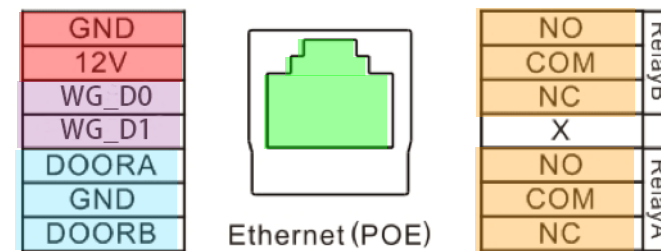


Figure 1.2-1 Connector Interface

DOORA/B: Trigger signal input terminal.

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

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

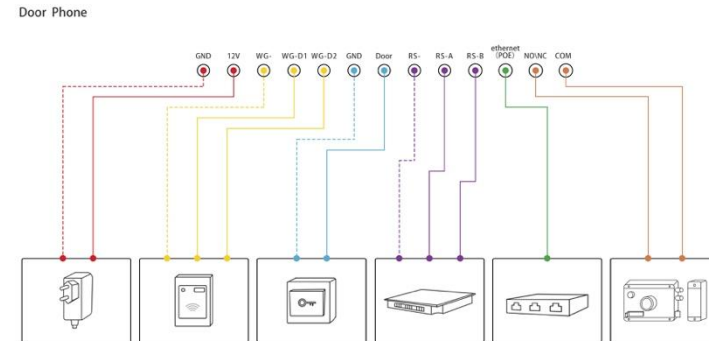


Figure 1.2-2 General interface

2. Daily Use

2.1. Make a Call

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

R20K 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

Place the predefined user cards in RFID card reader to unlock. Under normal conditions, R20K will announce “The door is now opened.” If the card has not been registered, R20K will show “Unauthorized.” Both 13.56MHz and 125KHz RFID cards are supported on R20K.

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 Website Setting

3.1.1. Obtain IP Address

R20K use DHCP IP by default. Press “*3258*” to and voice system will enter IP announcement mode. In IP announcement mode, the IP address will be announced.



The screenshot shows the 'Basic' settings page. It contains the following fields and options:

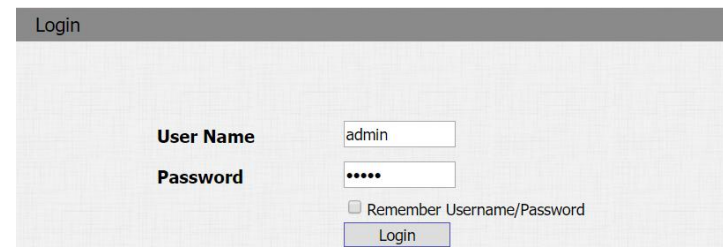
Basic		
IP Broadcast Key	3258	Press *3258* to broadcast the IP.
Select Account	Auto	
Robin Call Enable	Disabled	
Robin Call Timeout	20	
DTMF Unlock	Push Button Number	

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's user name and password are shown below:

User Name: **admin**

Password: **admin**



The screenshot shows the 'Login' page. It contains the following fields and options:

Login	
User Name	admin
Password
<input type="checkbox"/> Remember Username/Password	
<input type="button" value="Login"/>	

Figure 3.2.2 Access the device website

Note: The recommended browser is Google Chrome.

3.2. Password Modification

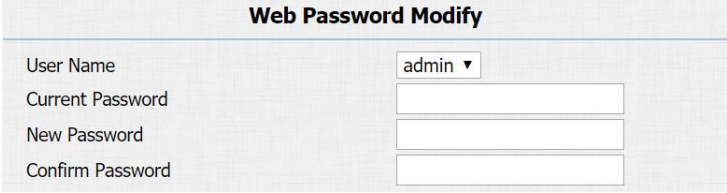
3.2.1. Modify the Device Admin Code

Go to **Intercom – Basic** to modify device admin code.

3.2.2. 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 3.3.3 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 3.4.1 Language

3.3.2. Time

NTP: To select local time zone for NTP server.

3.3.3. Network

DHCP Mode

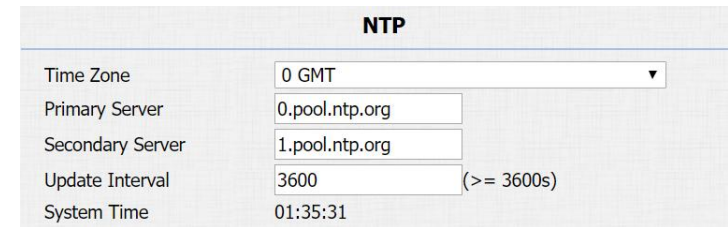
In Website, go to Network - Basic.

R20K 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.

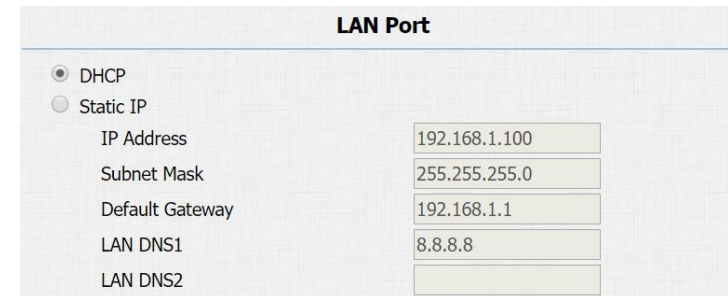
If select static IP, users should manually setup IP address, subnet mask, default gateway and DNS server address. The figure right shows static IP settings.



The screenshot shows the NTP configuration page. It includes a dropdown menu for Time Zone set to '0 GMT', input fields for Primary Server (0.pool.ntp.org) and Secondary Server (1.pool.ntp.org), an Update Interval of 3600 seconds (with a note that it must be greater than or equal to 3600s), and a System Time of 01:35:31.

NTP	
Time Zone	0 GMT
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	01:35:31

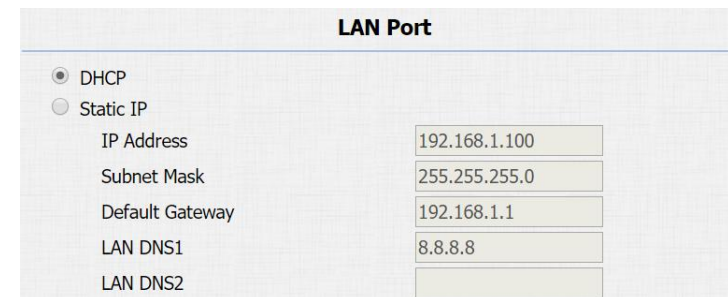
Figure 3.3.2.1 Time



The screenshot shows the LAN Port configuration page with DHCP mode selected. The fields are: 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



The screenshot shows the LAN Port configuration page with Static IP mode selected. The fields are: 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

3.3.4. 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.

3.4. Intercom Call

3.4.1. Direct IP Call

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

The screenshot displays a configuration page for sound settings. It is divided into several sections:

- Mic Volume:** A text input field containing the value '8' and a range indicator '(1~15)' to its right.
- Speaker Volume:** A text input field containing the value '8' and a range indicator '(1~15)' to its right.
- Open Door Warning:** A dropdown menu currently set to 'Enabled'.
- RingBack Upload:** A section with a 'Choose File' button, the text 'No file chosen', and three buttons: 'Upload', 'Delete', and 'Export'. Below this is the text 'File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16'.
- Opendoor Tone Upload:** A section with a 'Choose File' button, the text 'No file chosen', and three buttons: 'Upload', 'Delete', and 'Export'. Below this is the text 'File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16'.

Figure 3.4.5 Sound

The screenshot shows a single configuration item: 'Direct IP' with a dropdown menu set to 'Enabled'.

Figure 3.5.1 Direct IP call

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.

3.4.2.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.

3.4.3.SIP Account

Status: To display register result.

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.

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

User Name: To enter user name of the extension.

Password: To enter password for the extension.

3.4.4.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.

3.4.5.Outbound Proxy Server

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

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

Outbound Proxy Server		
Enable Outbound	<input type="text" value="Disabled"/>	
Server IP	<input type="text"/>	Port <input type="text" value="5060"/>
Backup Server IP	<input type="text"/>	Port <input type="text" value="5060"/>

Figure 3.5.2.3Outbound proxy server

3.4.6. Transport Type

To display and configure transport type for SIP message.

- UDP: UDP is an unreliable but very efficient transport layer protocol.
- TCP: Reliable but less-efficient transport layer protocol.
- TLS: Secured and reliable transport layer protocol.
- DNS-SRV: DNS record for specifying the location of services.

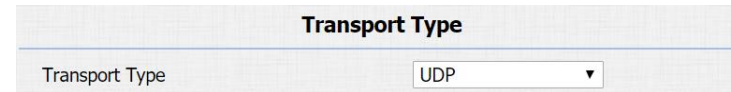
3.4.7. NAT

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.

Press the a SIP account and “Dial key”to make a SIP call.



The screenshot shows a configuration window titled "Transport Type". It contains a single field labeled "Transport Type" with a dropdown menu currently set to "UDP".

Figure 3.5.2.4Transport type



The screenshot shows a configuration window titled "NAT". It contains three fields: "NAT" with a dropdown menu set to "Disabled", "Stun Server Address" with an empty text input field, and "Port" with a text input field containing the value "3478".

Figure 3.5.2.5NAT

3.4.8. 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. Press “Managecenter key” (Manager Dial) to call.

3.4.9. 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.

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

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

3.4.10. Web Call

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

3.5. Security

3.5.1. Live view

Go to **Intercom - Live Stream** to check the real-time video from R20K.

In addition, user also can check the real-time picture via URL:
http://IP_address:8080/picture.jpg.

3.5.2. RTSP

R20K 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.



Figure 3.5.6 Web call



Figure 3.6.1 Live view

RTSP Stream: To enable RTSP video and select the video codec.

R20K 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 bitrate of MPEG4.

The screenshot displays a configuration interface for RTSP. It is organized into four distinct sections, each with a title and a light blue background. The first section, 'RTSP Basic', contains a single checkbox labeled 'RTSP Server Enabled' which is checked. The second section, 'RTSP Stream', contains a checked checkbox for 'RTSP Video Enabled' and a dropdown menu for 'RTSP Video Codec' set to 'H.264'. The third section, 'H.264 Video Parameters', includes three dropdown menus: 'Video Resolution' (VGA), 'Video Framerate' (30 fps), and 'Video Bitrate' (2048 kbps). The final section, 'MPEG4 Video Parameters', also includes three dropdown menus: 'Video Resolution' (VGA), 'Video Framerate' (30 fps), and 'Video Bitrate' (2048 kbps).

Figure 3.6.2 RTSP

3.5.3. ONVIF

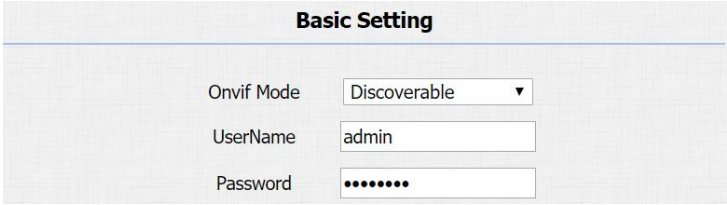
R20K supports ONVIF protocol, which means R20K's camera can be searched by other devices, like NVR which supports ONVIF protocol as well.

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

3.6. Access Control

3.6.1. Unlock via DTMF

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:R20K 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.

DTMF Option:To select digit of DTMF code, R20K support maximum to 4digits' DTMF code.

DTMF&Multiple DTMF:To configureDTMF code for remote unlocking.

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.

The screenshot shows a configuration page titled "Relay". It contains two columns of settings for "RelayA" and "RelayB".

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

Figure 3.7.1 Relay

3.6.2. Unlock via RFID Card

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

Import/Export Card Data

R20K 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 20K which is around 500 cards.

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

Enable ID/IC Card

Switch to enable to support IC/ID card.

Schedule Management

Select schedule which was created on **Intercom – Schedule** to set up valid time for cards.

Obtain and Add Card

- Switch card status to “Card Issuing” and click “Apply”;
- Place card on the card reader area and click “Obtain”;

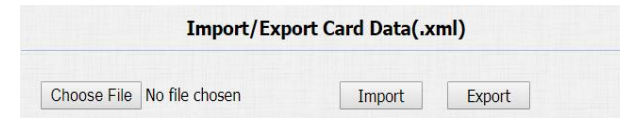


Figure 3.6.2-1 Card setting

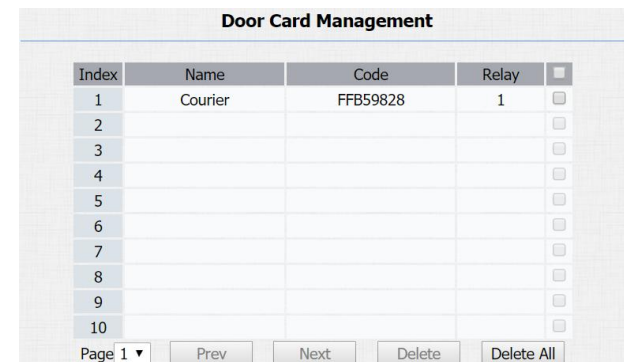
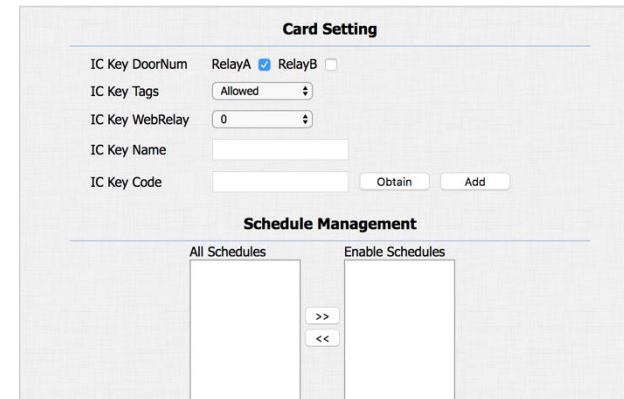


Figure 3.7.3.2 RFID cards in website

- 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 onecard’s access permission or empty all the list.

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

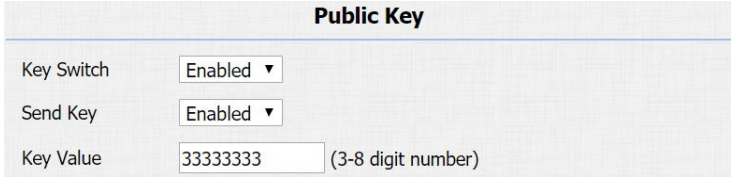
3.6.3.Unlock via Pin Code

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.

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



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

Private Pin Codes in Website

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

Import /Export Private Key

R20K 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 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.

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

Private Key Management

Index	Name	Code	Relay	<input type="checkbox"/>
1	Troye	2333	2	<input checked="" 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

3.6.4.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:

http://IP_address/cgi/do?action=OpenDoor&UserName=&Password=&DoorNum=1.

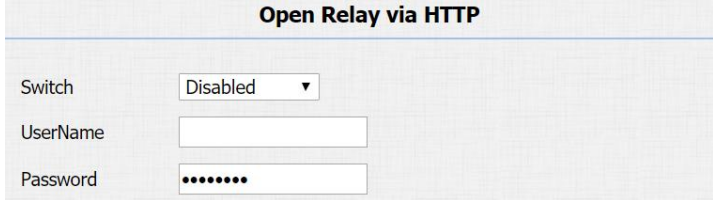
3.6.5.Unlock via Exit Button

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

R20K supports 2 input triggers “Input A/B (DOOR A/B).”

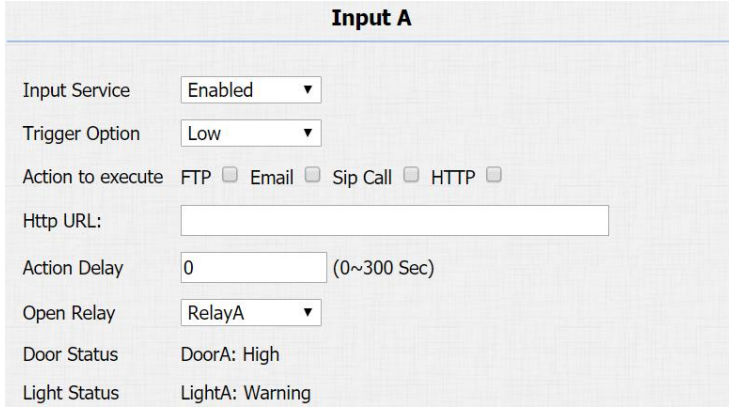
Input Service:To enable or disable input trigger service.

Trigger Option:To choose open circuit trigger or closed circuit trigger.“Low” means that connection between door terminal and



The screenshot shows a configuration page titled "Open Relay via HTTP". It contains three main fields: a "Switch" dropdown menu currently set to "Disabled", a "UserName" text input field, and a "Password" text input field with masked characters (dots).

Figure 3.7.5 Unlock via HTTP command



The screenshot shows a configuration page titled "Input A". It contains several settings: "Input Service" is a dropdown menu set to "Enabled"; "Trigger Option" is a dropdown menu set to "Low"; "Action to execute" has four radio buttons: "FTP", "Email", "Sip Call", and "HTTP", all of which are currently unselected; "Http URL:" is a text input field; "Action Delay" is a text input field set to "0" with a note "(0~300 Sec)"; "Open Relay" is a dropdown menu set to "RelayA"; "Door Status" is set to "DoorA: High"; and "Light Status" is set to "LightA: Warning".

Figure 3.7.6 Unlock via exit button

GND is closed, while “High” means the connection is opened.

Door status: To show the status of input signal.

3.7. Reboot

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

3.8. Reset

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

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



Figure 3.8 Reboot



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.

LED Status is to set up **Status LED** which can change light mode on different condition.

Users can control 2 parts' LED, 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.

The screenshot shows the 'LED Status' and 'LED Control' configuration sections. The 'LED Status' section contains a table with columns for State, Color Off, Color On, and Blink Mode. The 'LED Control' section contains three dropdown menus for LED Control, KeyPad LED Enable, and Card LED Enable, all set to 'Disabled'.

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

LED Control	Disabled
KeyPad LED Enable	Disabled
Card LED Enable	Disabled

Figure 4.1.1 LED

Photoresistor: The setting is for night vision, when the surrounding of R20K is very dark, infrared LED will turn on and R20K will turn to night mode.

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.

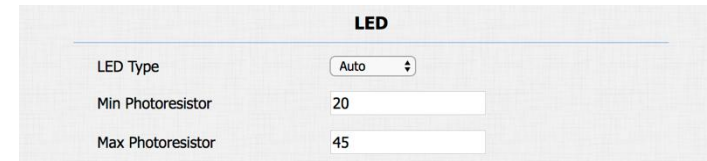


Figure 4.1.2 IR LED

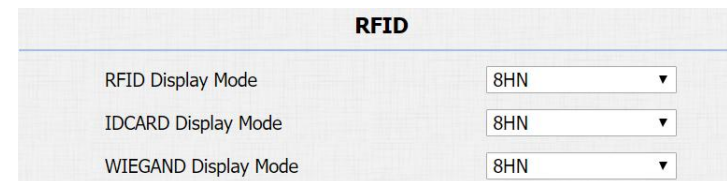


Figure 4.1.3 RFID card code display related

4.2. Intercom

4.2.1. Call Time Related

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

Max Call Time: To configure the max call time.

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

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

Max Dial Time		
Dial In Time	<input type="text" value="60"/>	(30~120Sec)
Dial Out Time	<input type="text" value="60"/>	(30~120Sec)

Figure 4.2.1 Call time related

4.2.2. SIP Call Related

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

MaxLocal SIP Port:To configure maximum local SIP port for designated SIP account.

MinLocalSIPPort: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,R20K 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.

4.2.3.Codec

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

Sip Account: To choose which account to configure.

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

SIP Account	
Account	Account 1 ▼
Codecs	
Disabled Codecs	Enabled Codecs
	PCMU PCMA G722 G729
>>	↑
<<	↓
Video Codec	
Codec Name	<input checked="" type="checkbox"/> H264
Codec Resolution	4CIF ▼
Codec Bitrate	2048 ▼
Codec Payload	104 ▼

Figure 4.2.6-1 SIP call related codec

Audio Codec: R20K 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

Video Codec: R20K support H.264 standard, which provides better video quality at substantially lower bit rates than previous standards.

Codec Resolution: R20K 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.

4.2.4.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.

4.2.5.Session Timer

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

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



Figure 4.2.6-2 Multicast related codec

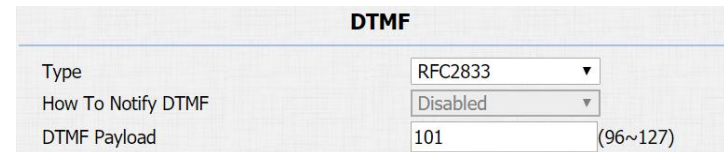


Figure 4.2.8 DTMF



Figure 4.2.9 Session timer

4.2.6. Encryption

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

If enabled, voice will be encrypted.



Encryption	
Voice Encryption(SRTP)	Disabled

Figure 4.2.11 Encryption

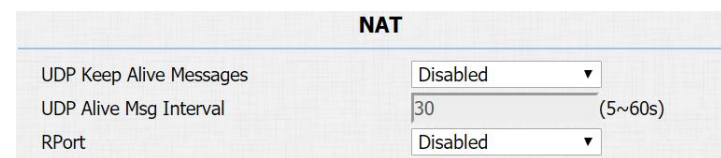
4.2.7. NAT

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

4.2.8. 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



User Agent	
User Agent	

Figure 4.2.13 User Agent

by default, users can see the company name, model number and firmware version from PCAP.

4.3. Access Control

4.3.1. Web Relay

R20K can support to connect to web relay.

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

Type: Connect web relay and choose the type.

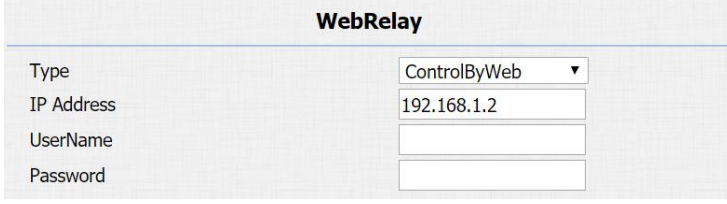
IP Address: Enter web relay's IP address.

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

Password: It is an authentication for connecting web relay.

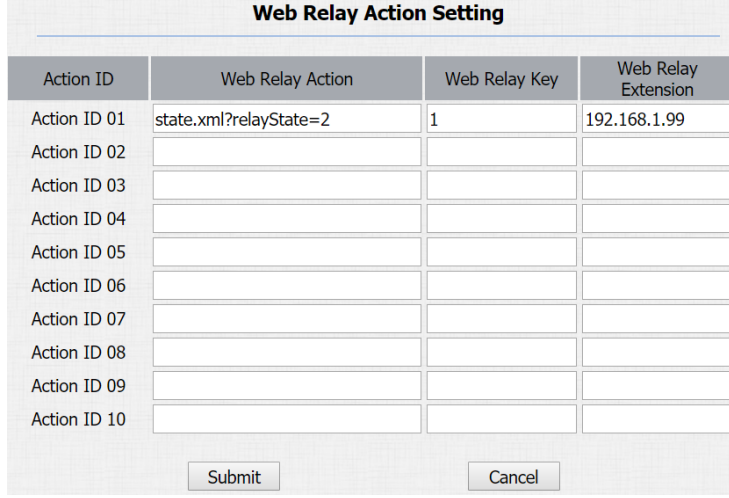
Web Relay Action: Web relay action is used to trigger the web relay. The action URL is provided by web relay vendor.

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.



The image shows a configuration form titled "WebRelay". It contains four fields: "Type" with a dropdown menu set to "ControlByWeb", "IP Address" with the value "192.168.1.2", "UserName" with an empty text box, and "Password" with an empty text box.

Figure 4.3.1-1 Web relay



The image shows a table titled "Web Relay Action Setting". The table has four columns: "Action ID", "Web Relay Action", "Web Relay Key", and "Web Relay Extension". The first row is populated with "Action ID 01", "state.xml?relayState=2", "1", and "192.168.1.99". The remaining rows (Action ID 02 to 10) are empty. Below the table 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

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.

4.3.2. Wiegand

Using this feature to integrate with some wiegand access control. R20K 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.

Wiegand Mode: Input or output. Typically, when users select input, we generally connect the wiegand input device, such as the wiegand card reader. Or R20K can be used as output, it is generally used to connect the third-party access control, and R20K change the card information as wiegand signal, and then transfer to the access control module.



Wiegand	
WiegandType	wiegand-26 ▼
Wiegand Mode	Input ▼

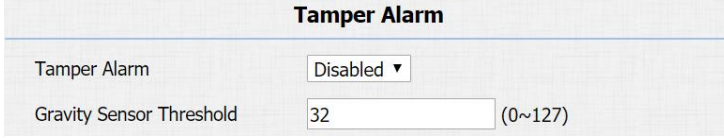
Figure 4.3.2 Wiegand

4.4. Security

4.4.1. Anti-alarm

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

Tamper Alarm:R20K integrates internal gravity sensor for its own security. After enabling tamper alarm, if the gravity of R20K changes dramatically, it will alarm. Gravity sensor threshold stands for sensitivity of sensor. Smaller the value, the more sensitive it is.



The screenshot shows the 'Tamper Alarm' configuration section. It includes a dropdown menu for 'Tamper Alarm' set to 'Disabled' and a text input field for 'Gravity Sensor Threshold' with the value '32' and a range '(0~127)'.

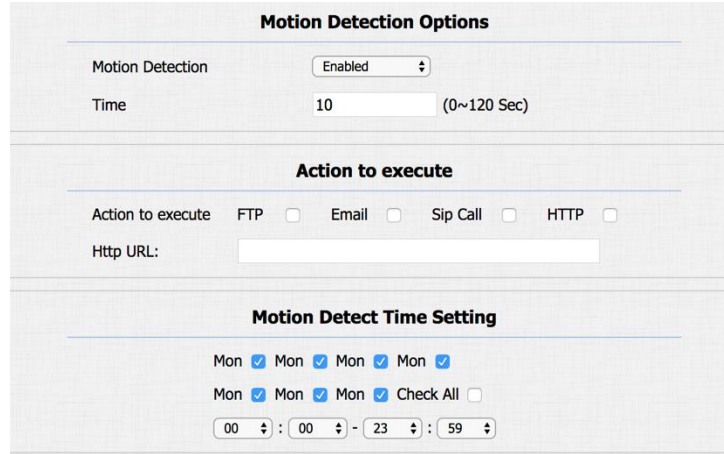
Figure 4.4.1 Anti-alarm

4.4.2. Motion

R20K supports motion detection, go to **Intercom - Motion** to configure detection related parameters.

Motion Detection: To enable or disable motion detection.

Action to execute: To choose suitable way to receive message or snapshot when detecting motion.



The screenshot shows the 'Motion Detection Options' configuration section. It includes a dropdown menu for 'Motion Detection' set to 'Enabled' and a text input field for 'Time' with the value '10' and a range '(0~120 Sec)'. Below this is the 'Action to execute' section with radio buttons for 'FTP', 'Email', 'Sip Call', and 'HTTP'. The 'Http URL:' field is empty. At the bottom is the 'Motion Detect Time Setting' section with checkboxes for 'Mon' (all checked) and 'Check All' (unchecked), and a time range selector set to '00 : 00 - 23 : 59'.

Figure 4.4.2 Motion

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

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

4.4.3. Action

R20K 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.

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

Figure 4.4.3.1-1 Email notification parameters

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 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.

SIP Notification

SIP Call Number: To configure sip call number.

SIP Call Name: To configure display name of R20K.

FTP Notification	
FTP Server	192.168.1.155
FTP User Name	admin
FTP Password
<input type="button" value="FTP Test"/>	

Figure 4.4.3.1-2 FTP notification parameters

SIP Call Notification	
SIP Call Number	5101100010
SIP Caller Name	Judy

Figure 4.4.3.1-3 SIP call notification parameters

Five specific actions which will be triggered in R20K:

4.4.3.2. Input Interface Triggered Action

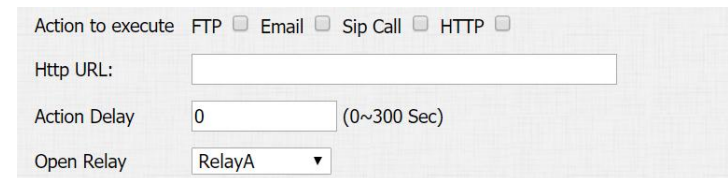
Go to **Intercom - Input** to configure.

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 for 'Input Interface Triggered Action'. It includes the following fields and options:

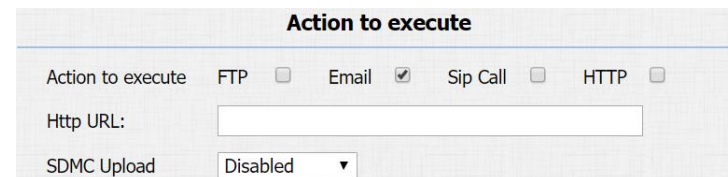
- Action to execute:** A row of radio buttons for FTP, Email, Sip Call, and HTTP, all of which are currently unselected.
- Http URL:** An empty text input field.
- Action Delay:** A text input field containing the value '0', with '(0~300 Sec)' written to its right.
- Open Relay:** A dropdown menu currently showing 'RelayA'.

Figure 4.4.3.4 Input interface triggered action

4.4.3.3. 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 for 'Motion Triggered Action'. It includes the following fields and options:

- Action to execute:** A row of radio buttons for FTP, Email, Sip Call, and HTTP. The 'Email' radio button is selected.
- Http URL:** An empty text input field.
- SDMC Upload:** A dropdown menu currently showing 'Disabled'.

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.

4.5. 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.



Firmware Version	20.31.3.204
Hardware Version	20.9.0.0.0.0.0.0
Upgrade	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Submit"/> <input type="button" value="Cancel"/>

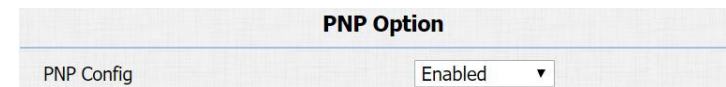
Figure 4.5.1 Web upgrade

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.



PNP Option	
PNP Config	Enabled ▼

Figure 4.5.2-1 PNP

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

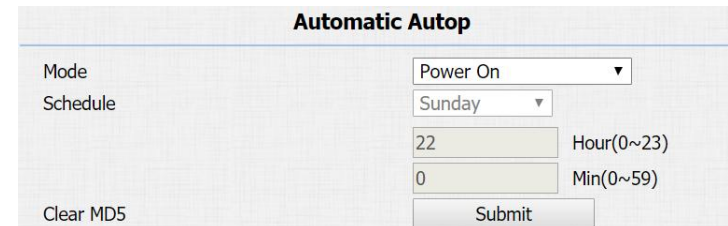
Automatic Autop

To display and configure auto provisioning mode settings.

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.



The screenshot shows a web interface titled "Automatic Autop". It contains the following elements:

- Mode:** A dropdown menu currently set to "Power On".
- Schedule:** A dropdown menu currently set to "Sunday".
- Hour(0~23):** A text input field containing the number "22".
- Min(0~59):** A text input field containing the number "0".
- Clear MD5:** A text label.
- Submit:** A button.

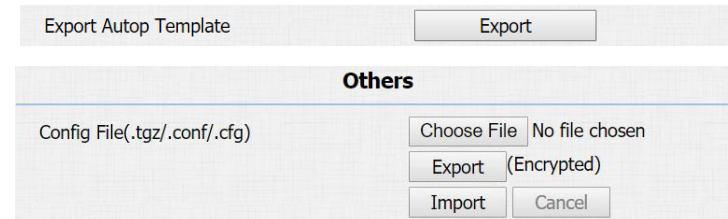
Figure 4.5.2-3 Automatic provision

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.



The screenshot shows a web interface with two main sections:

- Export Autop Template:** A section with a text label and an "Export" button.
- Others:** A section with a text label "Config File(.tgz/.conf/.cfg)" and a file selection area. The file selection area includes a "Choose File" button, the text "No file chosen", an "Export (Encrypted)" button, an "Import" button, and a "Cancel" button.

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	192.168.35.68@192.168.35.68	<input type="checkbox"/>
2	Received	2018-09-30	08:26:40	192.168.35.1 0@192.168.35.10	192.168.35.68	192.168.35.68@192.168.35.68	<input type="checkbox"/>

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.

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

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.

System Log	
LogLevel	3 ▾
Export Log	Export

Figure 4.6.3 System log

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.

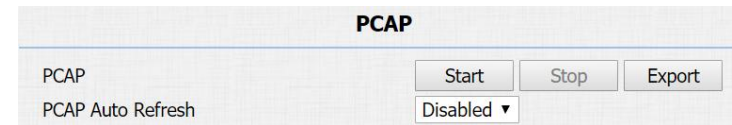


Figure 4.6.4 PCAP

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 μ -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 or feel free to contact us by

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

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

We highly appreciate your feedback about our products.



FCC Statement:

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

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

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

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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