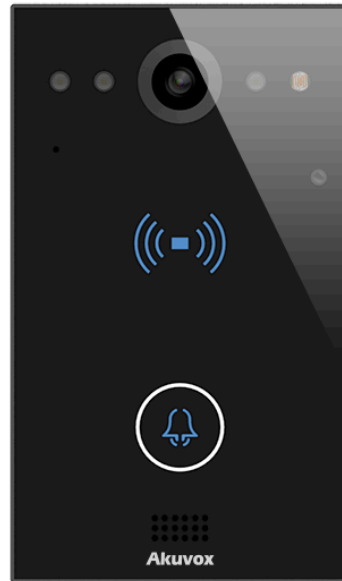


Akuvox Smart
Intercom



E11R Door Phone Admin Guide

About This Manual

Thank you for choosing Akuvox's **E11R** door phone. This manual is intended for end users, who need to properly configure the door phone. This manual is applicable to 111.31.XXX.XXX version, and it provides an overview of the most essential functions and features of the product. 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.....	2
1.3. LED Status Information	3
2. Daily Use	4
2.1. Making a Call	4
2.2. Receiving a Call	4
2.3. Unlock	5
2.3.1. Unlock by RF Card	5
2.3.2. Unlock by DTMF Codes.....	5
3. Basic Features	6
3.1. Access the website setting.....	6
3.1.1. IP Announcement.....	6
3.1.2. Access the device website	6
3.2. Password Modification	7
3.2.1. Modify the web password	7

3.3. Phone Configuration	7
3.3.1. Language	7
3.3.2. Network Setting	8
3.3.3. Sound	9
3.3.4. Chime bell	10
3.4. Intercom Call	10
3.4.1. Direct IP Call	10
3.4.2. SIP Call	11
3.4.3. Auto Answer	14
3.4.4. Web Call	14
3.4.5. No Answer Call	15
3.5. Security	15
3.5.1. Live view	15
3.5.2. RTSP	16
3.5.3. Onvif	16
3.6. Access Control	17
3.6.1. Relay	17

3.6.2. Unlock via DTMF code	18
3.6.3. Unlock via RF Card(Optional).....	18
3.6.4. Unlock via HTTP command	19
3.6.5. Unlock via Exit Button	20
3.6.6. Wiegand.....	21
3.7. Reboot.....	21
3.8. Reset.....	22
4. Advanced Features	23
4.1. Phone Configuration	23
4.1.1. LED	23
4.1.2. IR LED	24
4.2. Intercom	25
4.2.1. Call Time Related	25
4.2.2. Return Code When Refuse.....	25
4.2.3. Sip Call Related	25
4.2.4. Codec	26
4.2.5. Session Timer	28

4.2.6. Encryption	28
4.2.7. NAT	28
4.2.8. User Agent	29
4.3. Access Control	30
4.3.1. Web Relay	30
4.4. Security	31
4.4.1. Anti-alarm.....	31
4.4.2. Motion	31
4.4.3. Action	32
4.5. Upgrade	35
4.5.1. Web Upgrade.....	35
4.5.2. Backup config file.....	35
4.6. Log	36
4.6.1. Call Log.....	36
4.6.2. Door Log	36
4.6.3. System Log	37
4.6.4. PCAP	37

1. Product Overview

1.1. Product Description

Akuvox E11R is a SIP-compliant, hands-free one button video outdoor 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. It is applicable in villas, offices and so on.

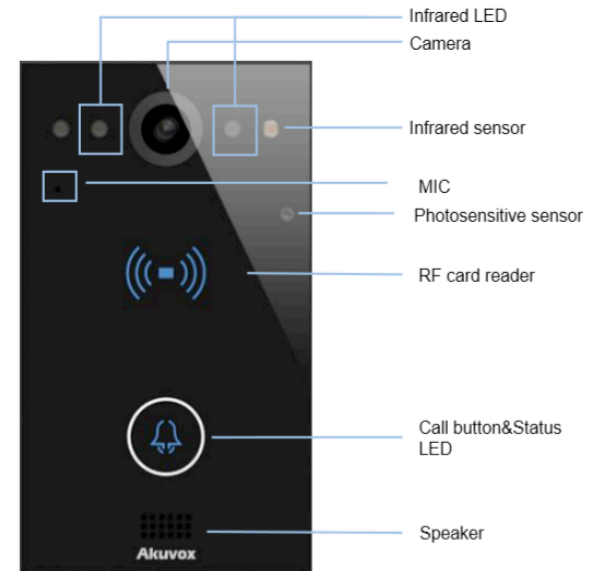


Figure 1.1 Product Description

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 connector is not available.

WG_D0/WG_D1: Wiegand terminal.

DOORA/B: Trigger signal input terminal.

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

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



Figure 1.2.1 Connector Introduction

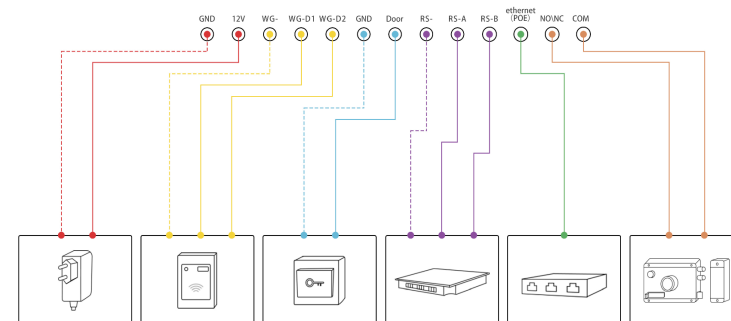


Figure 1.2-2 General interface

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

2. Daily Use

2.1. Making a Call

Press the call button to call out the predefined number or IP address and if LED turns green, it means the call has been answered.

2.2. Receiving a Call

Users can use IP phone or indoor monitor to call E11R and E11R will answer it automatically by default. If auto answer is disabled, pressing call button to answer the incoming call.

2.3. Unlock

2.3.1. Unlock by RF Card

Place the predefined user cards in RFID card reader to unlock. Under normal conditions, E11R will announce “The door is now opened”. Both 13.56MHz and 125KHz RFID cards are supported on E11R.

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 Features

3.1. Access the website setting

3.1.1. IP Announcement

While E11R starts up normally, hold the call button for several seconds after the Status LED turns blue, voice system will enter IP announcement mode. In IP 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’s user name and password are shown as below:

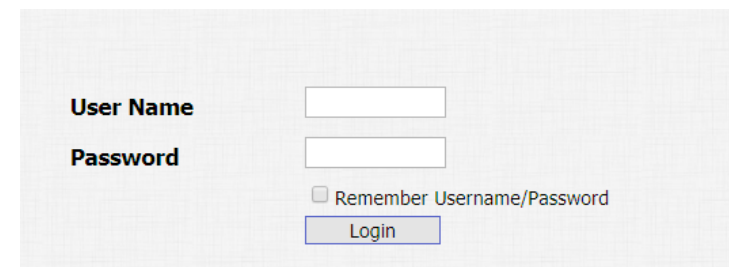


Figure 3.1.2 Access the device website

User Name: **admin**

Password: **admin**

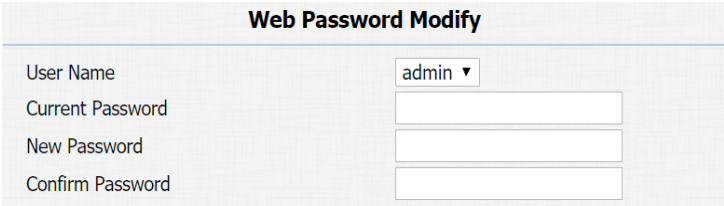
Note: The recommended browser is Google Chrome.

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.



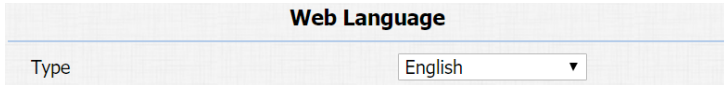
Web Password Modify	
User Name	admin ▾
Current Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

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. Network Setting

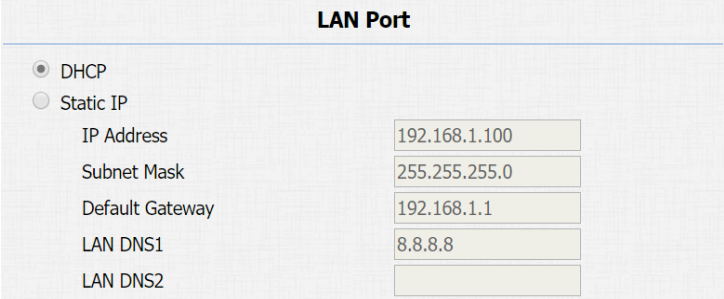
Go to **Network - Basic**, dynamically or statically to obtain address.

3.3.2.1. DHCP

E11R uses DHCP by default, it will get IP address, Subnet Mask, Default Gateway and DNS server address from DHCP server automatically.

3.3.2.2. Static IP

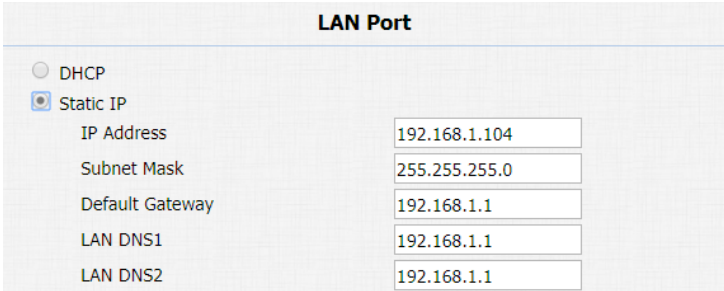
If selected, you could manually set IP address, Subnet Mask, Default Gateway and DNS server. The figure 3.3.2.2 shows static IP setting.



The screenshot shows the 'LAN Port' configuration interface. The 'DHCP' radio button is selected. Below it, the 'Static IP' radio button is unselected. The following fields are visible:

Field	Value
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 3.3.2.1 DHCP mode



The screenshot shows the 'LAN Port' configuration interface. The 'Static IP' radio button is selected. The following fields are visible:

Field	Value
IP Address	192.168.1.104
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
LAN DNS1	192.168.1.1
LAN DNS2	192.168.1.1

Figure 3.3.2.2 Static IP mode

3.3.3. 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.

IP Announcement: To configure the valid time when IP Announcement is available and the loop time of IP Announcement.

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

Opendoor Tone Upload: To upload the opendoor tone by users themselves.

The screenshot shows the 'Sound' configuration page with the following sections and controls:

- Mic Volume:** A text input field containing '8' with a range indicator '(1~15)' to its right.
- Speaker Volume:** A text input field containing '8' with a range indicator '(1~15)' to its right.
- Open Door Warning:** A dropdown menu currently set to 'Enabled'.
- IP Announcement:** Two text input fields: 'IP Announcement active time' with '0' and range '(0~180)', and 'IP Announcement Loop times' with '1' and range '(0~10)'.
- RingBack Upload:** A file upload section with a 'Choose File' button, 'No file chosen' text, and 'Upload', 'Delete', and 'Export' buttons. Below the buttons, it displays 'File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16'.
- Opendoor Tone Upload:** A file upload section with a 'Choose File' button, 'No file chosen' text, and 'Upload', 'Delete', and 'Export' buttons. Below the buttons, it displays 'File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16'.

Figure 3.3.3 Sound

3.3.4. Chime bell

The chime bell is used to amplify the ringtone volume and help users not miss the call.

Go to **Web-Intercom-Basic-Chime Bell** to configure it.

Choose Relay A or Relay B then when the relay is triggered, the bell will ring with the call established for better sound amplification.

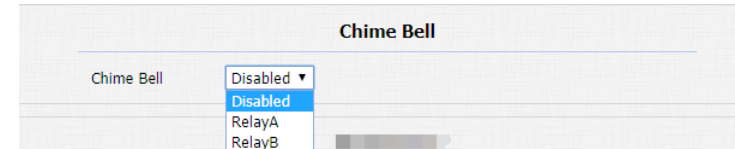


Figure 3.3.4-Chime bell

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.

Then, go to **Intercom - Basic** to configure the IP address of the destination(E.g. IP address 192.168.1.100). It supports up to 8 lines simultaneously.



Figure 3.4.1-1 Direct IP call

Push Button				
Key	Number1 / 5	Number2 / 6	Number3 / 7	Number4 / 8
Push Button	192.168.1.100			

Figure 3.4.1-2 Push Button Number

After all, press the push button to make 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.

3.4.2.1. SIP Account

Status: To display register result.

Account: To switch the account to be configured. E11R supports 2 SIP accounts.

Account Active: To enable the account, it is disabled by default.

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

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

SIP Account	
Status	Registered
Account	Account 1
Account Active	Enabled
Display Label	Front Door_R20
Display Name	Front Door
Register Name	508100038
User Name	508100038
Password	*****

Figure 3.4.2.1 SIP account

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.

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, the phone will re-register automatically within registration period.

3.4.2.2. Outbound Proxy Server

An outbound proxy server is used to receive all initiating request

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 3.4.2.2 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 3.4.2.3 Outbound proxy server

messages and route them to the designated SIP server.

3.4.2.3. Transport Type

To display and configure transport type for SIP message.

There are 4 transport types in total.

- **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.

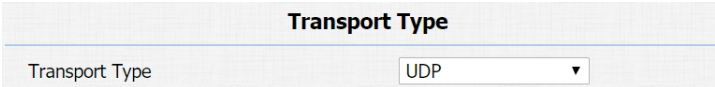
3.4.2.4. NAT

To display and configure NAT settings.

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

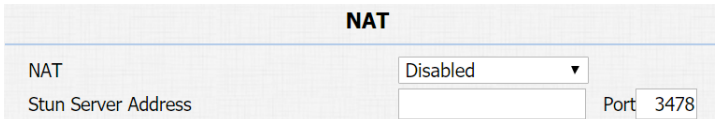
Note: By default, NAT is disabled.

After all, press the push button to make direct IP 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 3.4.2.4 Transport 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 3.4.2.5 NAT

3.4.3. 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 by default.

Then incoming calls will be answered automatically.

3.4.4. Web Call

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



Figure 3.4.3-1 Auto answer for sip calls



Figure 3.4.3-2 Auto answer for direct IP calls

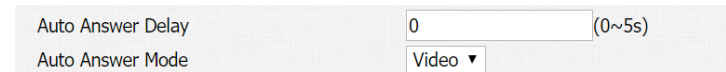


Figure 3.4.3-3 Auto answer options' parameters



Figure 3.4.4 Web call

3.4.5. No Answer Call

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

No Answer Call: If enabled, E11R will call to No Answer Call1 and No Answer Call2 in sequence automatically when push button call is not answered over timeout(30s by default).



No Answer Call	Disabled ▾
No Answer Call1	<input type="text"/>
No Answer Call2	<input type="text"/>

Figure 3.4.5- No Answer Call

3.5. Security

3.5.1. Live view

Go to **Intercom - Live Stream** to check the real-time video from E11R.

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



Figure 3.5.1 Live view

3.5.2. RTSP

E11R 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.

3.5.3. Onvif

E11R supports ONVIF protocol, which means E11R's camera can be searched by other devices, like NVR, which supports ONVIF protocol as well.

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

Switching ONVIF Mode to Undiscoverable means that User must program ONVIF's URL manually.

The ONVIF's URL is:

http://IP_address:8090/onvif/device_service.

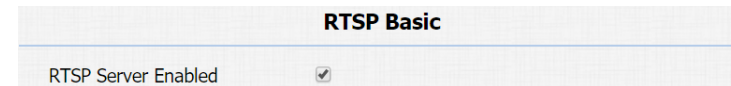


Figure 3.5.2 RTSP

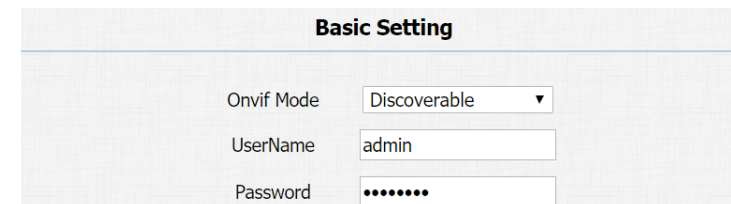


Figure 3.5.3 ONVIF

3.6. Access Control

3.6.1. Relay

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

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

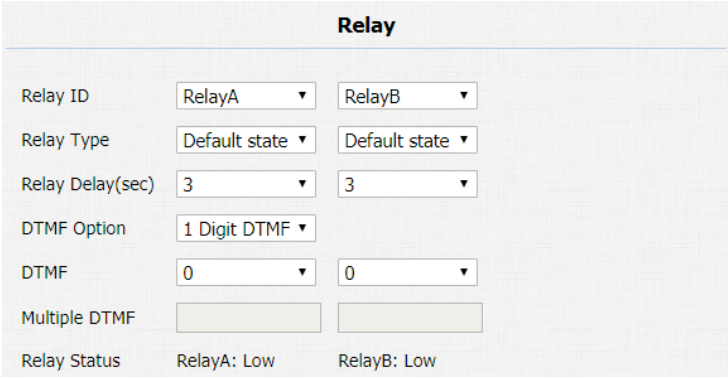
Relay ID: E11R supports two relays, user can configure them respectively.

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

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

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

Note: Relay operates a switch and does not deliver power, so user should prepare power adapter for external devices which connects



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

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	0
Multiple DTMF		
Relay Status	RelayA: Low	RelayB: Low

Figure 3.6.1 Relay

to relay.

3.6.2. Unlock via DTMF code

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.”

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

DTMF Option: To select digit of DTMF code, E11R support maximum 4 digits DTMF code.

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

3.6.3. Unlock via RF Card(Optional)

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

Import/Export Card Data

E11R supports import or export the card data file, which is

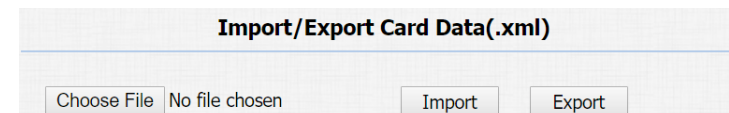


Figure 3.6.3-1 Import/Export Card Data

convenient for administrator to deal with a large number of cards.

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

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

Obtain and Add Card

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

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

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

3.6.4. Unlock via HTTP command

Users can use a URL to remote unlock the door.

The screenshot displays a web interface for managing RFID cards. It is divided into three main sections: Card Status, Card Setting, and Door Card Management.

- Card Status:** A dropdown menu is set to "Card Issuing" with an "Apply" button next to it.
- Card Setting:** Includes a dropdown for "IC Key DoorNum" (set to 1), a text input for "IC Key Name" (containing "Courier"), and a text input for "IC Key Code" (containing "FFB59828"). There are "Obtain" and "Add" buttons.
- Door Card Management:** A table with columns: Index, Name, Code, Relay, and a checkbox. The first row contains: Index 1, Name Courier, Code FFB59828, Relay 1, and a checked checkbox. Rows 2 through 10 are empty.

At the bottom of the table, there are navigation controls: "Page 1" (dropdown), "Prev", "Next", "Delete", and "Delete All" buttons.

Figure 3.6.3-2 RFID cards in website

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/fcgi/do?action=OpenDoor&UserName=&Password=&DoorNum=1.

3.6.5. Unlock via Exit Button

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

E11R 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.

Door status: To show the status of input signal.

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 3.6.4 Unlock via HTTP command

The screenshot shows a configuration page titled "Input A". It contains several fields: "Input Service" dropdown set to "Disabled", "Trigger Option" dropdown set to "Low", "Action to execute" with radio buttons for FTP, Email, Sip Call, and HTTP, an empty "Http URL" text input field, "Open Relay" dropdown set to "None", and "Door Status" showing "DoorA: High".

Figure 3.6.5 Unlock via exit button

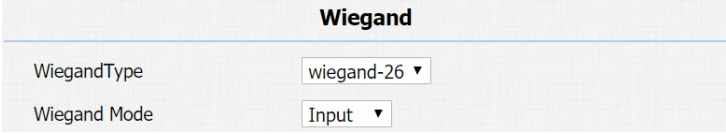
3.6.6. Wiegand

Using this feature to integrate with some wiegand access control. E11R 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, E11R will receive the data from wiegand port. We generally connect the wiegand input device, such as the wiegand card reader. Or E11R can be used as output, it is generally used to connect the third-party access control, and E11R sends the data as wiegand signal, and then transfer to the access control module.



Wiegand	
WiegandType	wiegand-26 ▼
Wiegand Mode	Input ▼

Figure 3.6.6 Wiegand

3.7. Reboot

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



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

Figure 3.7 Reboot

3.8. Reset

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

Reset To Factory Setting

Submit

Figure 3.8 Reset in website

4. Advanced Features

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.

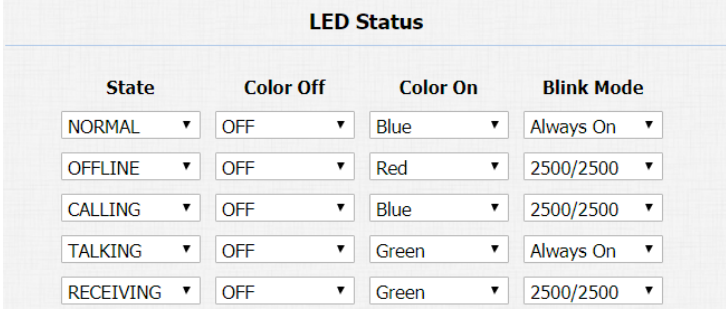
Blink Mode: To setup the different blink frequency.

LED Control:

Use Http URL to remote control the LED status.

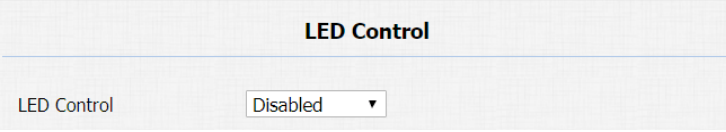
Http format:

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



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	
LED Control	Disabled

Figure 4.1.1-2 LED

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 E11R is very dark, infrared LED will turn on and E11R 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.

Photoresistor	
Photoresistor Setting	<input type="text" value="15"/> - <input type="text" value="30"/> (0~100)

Figure 4.1.2 IR LED

4.2. Intercom

4.2.1. Call Time Related

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

Max Call Time: To configure the max call time.

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

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

4.2.2. Return Code When Refuse

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

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

4.2.3. Sip Call Related

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

Max Call Time		
Max Call Time	<input type="text" value="5"/>	(2~120Minutes)
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

Others	
Return Code When Refuse	<input type="text" value="486(Busy Here)"/>

Figure 4.2.2 Return code when refuse

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, E11R will block its information when calling out.

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

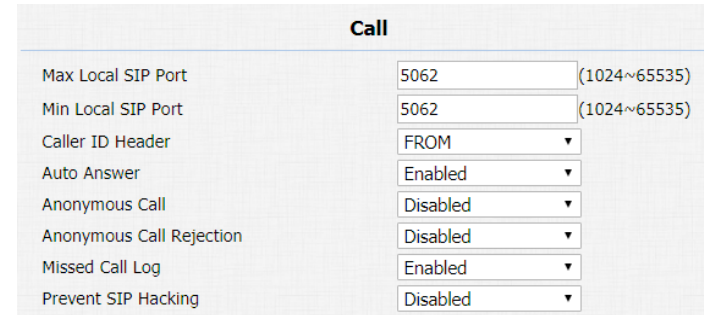
Missed Call Log: If enabled, any missed call will be recorded into call log.

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

4.2.4. 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	▼
Anonymous Call	Disabled	▼
Anonymous Call Rejection	Disabled	▼
Missed Call Log	Enabled	▼
Prevent SIP Hacking	Disabled	▼

Figure 4.2.3 SIP call related

Audio Codec: E11R supports 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: E11R supports H.264 standard, which provides better video quality at substantially lower bit rates than previous standards.

Codec Resolution: E11R 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.

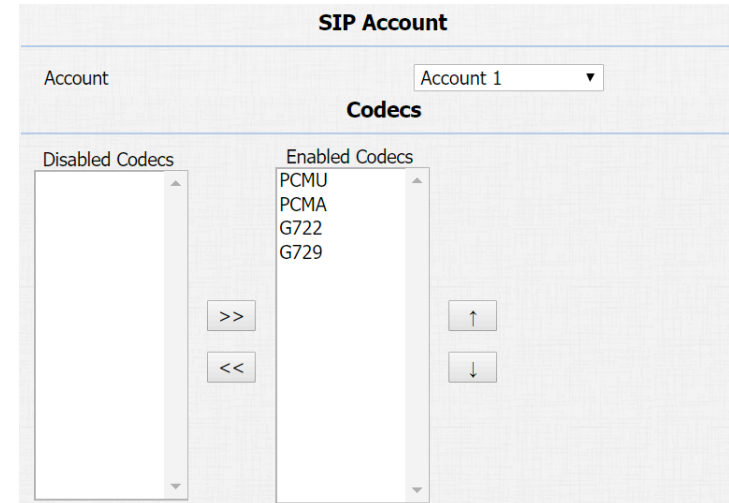


Figure 4.2.4-1 SIP call related codec

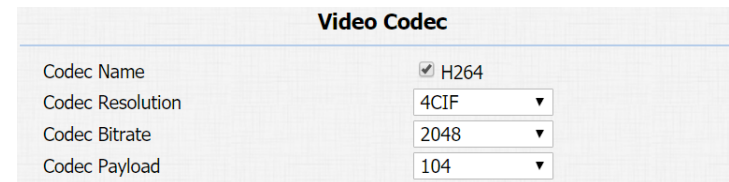


Figure 4.2.4-2 Video codec setting



Figure 4.2.4-2 Multicast related codec

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

4.2.5. Session Timer

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

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

4.2.6. Encryption

Go to the path **Account - Advanced** If enabled, voice will be encrypted.

4.2.7. NAT

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

UDP Keep Alive message: If enabled, IP phone 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 4.2.5 Session timer

Encryption	
Voice Encryption(SRTP)	Disabled ▼

Figure 4.2.6 Encryption

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

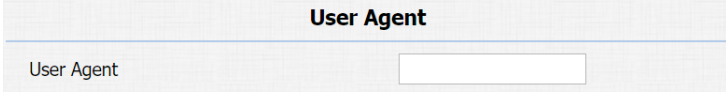
Figure 4.2.7 NAT

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.

4.2.8. 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 blank, by default, users can see the company name “Akuvox”, model number and firmware version from PCAP.



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 4.2.8 User Agent

4.3. Access Control

4.3.1. Web Relay

E11R supports extra web relay.

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

Type: Connect web relay and choose the type.

IP Address: Enter web relay IP address.


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

Password: It is an authentication for connecting web relay.

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

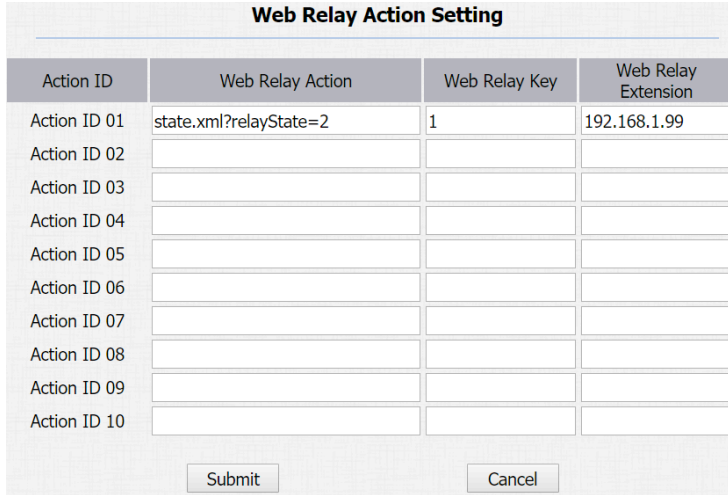
Web Relay Key: If the DTMF keys are same with the local relay, the web relay will be open with local relay. But if there are different, the web relay is invalid.

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



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

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

4.4. Security

4.4.1. Anti-alarm

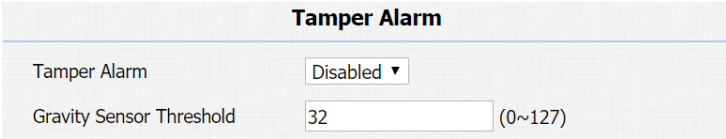
Go to **Intercom - Advanced** to configure.

Tamper Alarm: E11R integrates internal gravity sensor for the own security, and after enabling tamper alarm, if the gravity of E11R changes dramatically, the phone will alarm. Gravity sensor threshold stands for sensitivity of sensor.

4.4.2. Motion

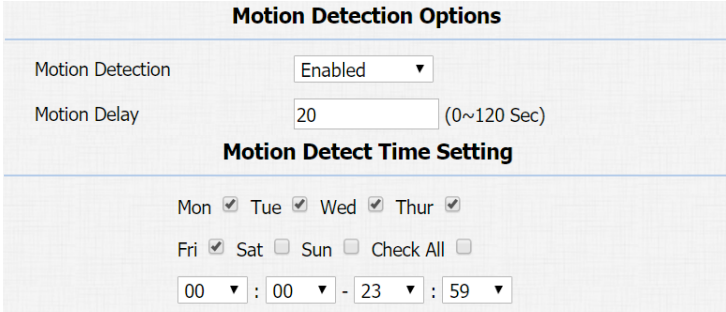
E11R supports motion detection, go to **Intercom - Motion** to configure detection parameter.

Motion Detection: To enable or disable Motion Detection.



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' set to '32', with a range indicator '(0~127)' to its right.

Figure 4.4.1 Anti-alarm



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 'Motion Delay' set to '20', with a range indicator '(0~120 Sec)' to its right. Below this is the 'Motion Detect Time Setting' section, which includes checkboxes for days of the week: Mon (checked), Tue (checked), Wed (checked), Thur (checked), Fri (checked), Sat (unchecked), and Sun (unchecked), along with a 'Check All' checkbox (unchecked). At the bottom, there are four dropdown menus for time selection: '00', '00', '23', and '59', separated by colons and a hyphen.

Figure 4.4.2 Motion

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

Motion Detect Time Setting: To make Motion Detect Time for a whole week.

4.4.3. Action

E11R supports to send notifications, snapshots via email and ftp transfer method, or calls via sip call method, when trigger specific actions.

4.4.3.1. Action Parameters

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

Email Notification

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

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

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

The screenshot shows a configuration window titled "Email Notification". It contains several input fields and a button:

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 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 E11R.

Three specific actions which will be triggered on E11R:

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

Figure 4.4.3.1-2 FTP notification parameters

SIP Call Notification	
SIP Call Number	<input type="text" value="5101100010"/>
SIP Caller Name	<input type="text" value="Judy"/>

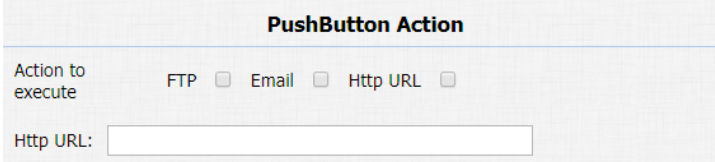
Figure 4.4.3.1-3 SIP call notification parameters

4.4.3.2. Pushbutton Action

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

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

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



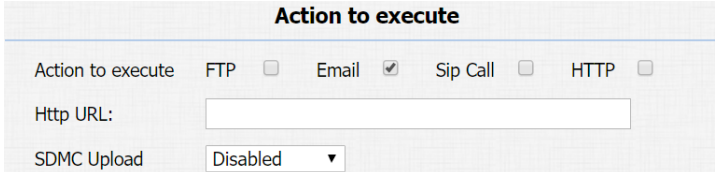
The screenshot shows a configuration window titled "PushButton Action". It contains three radio buttons for "Action to execute": "FTP" (unchecked), "Email" (unchecked), and "Http URL" (checked). Below these is a text input field labeled "Http URL:".

Figure 4.4.3.2 Pushbutton 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 window titled "Action to execute". It contains four radio buttons for "Action to execute": "FTP" (unchecked), "Email" (checked), "Sip Call" (unchecked), and "HTTP" (unchecked). Below these is a text input field labeled "Http URL:". At the bottom, there is a dropdown menu for "SDMC Upload" currently set to "Disabled".

Figure 4.4.3.3 Motion triggered action

4.4.3.4. Input Interface Triggered Action

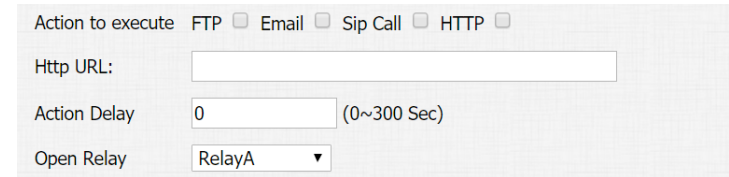
Go to **Intercom - Input** to configure.

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

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

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

Open relay: To configure which relay to trigger.



The screenshot shows a configuration form with the following fields and options:

- Action to execute:** Radio buttons for FTP, Email, Sip Call, and HTTP. The HTTP option is selected.
- Http URL:** A text input field.
- Action Delay:** A numeric input field with the value '0' and a range '(0~300 Sec)'.
- Open Relay:** A dropdown menu with 'RelayA' selected.

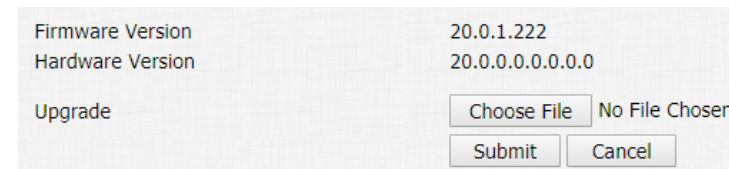
Figure 4.4.3.4 Input interface triggered action

4.5. Upgrade

4.5.1. Web Upgrade

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

Upgrade: Choose .rom firmware from your PC, then click “Submit” to update.



The screenshot shows the 'Web upgrade' configuration form with the following details:

- Firmware Version:** 20.0.1.222
- Hardware Version:** 20.0.0.0.0.0.0.0
- Upgrade:** A section containing a 'Choose File' button (with 'No File Chosen' text), a 'Submit' button, and a 'Cancel' button.

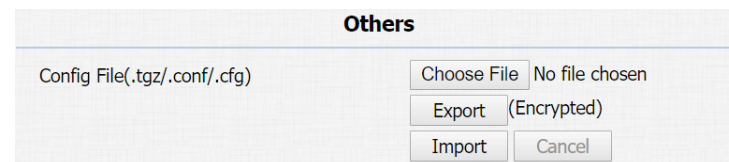
Figure 4.5.1 Web upgrade

4.5.2. Backup config file

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

Export Config File: To export current config file.

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



The screenshot shows the 'Backup config file' configuration form under the 'Others' section:

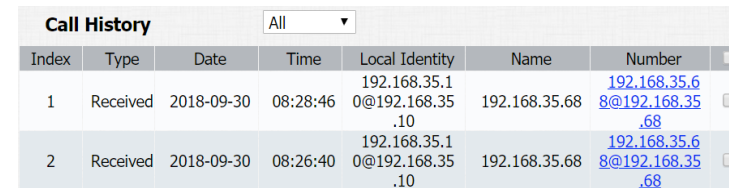
- Config File(.tgz/.conf/.cfg):** A section containing a 'Choose File' button (with 'No file chosen' text), an 'Export (Encrypted)' button, an 'Import' button, and a 'Cancel' button.

Figure 4.5.2 Backup config file

4.6. Log

4.6.1. Call Log

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

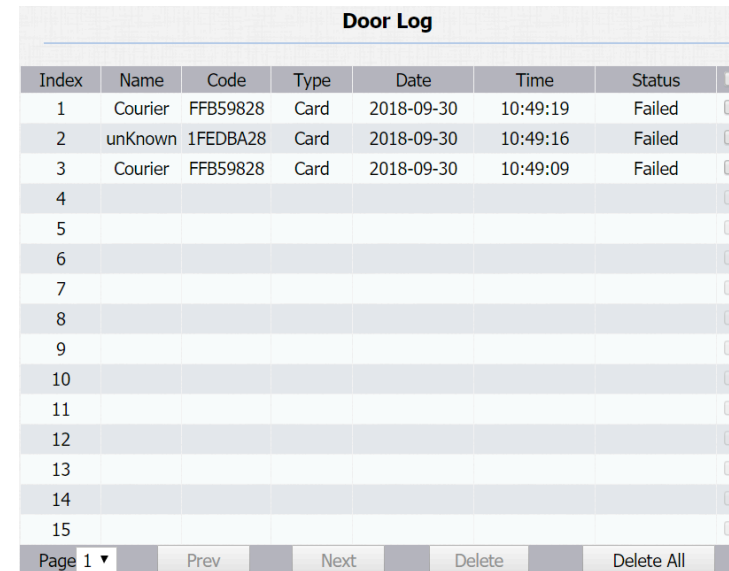


Call History							All
Index	Type	Date	Time	Local Identity	Name	Number	
1	Received	2018-09-30	08:28:46	192.168.35.1 0@192.168.35 .10	192.168.35.68	192.168.35.68@192.168.35.68	<input type="checkbox"/>
2	Received	2018-09-30	08:26:40	192.168.35.1 0@192.168.35 .10	192.168.35.68	192.168.35.68@192.168.35.68	<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 log 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.

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

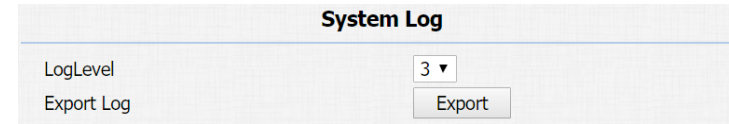


Figure 4.6.3 System log

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.

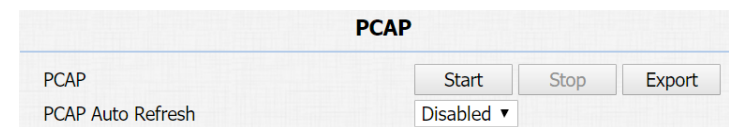


Figure 4.6.4 PCAP

E11R
ACS: Auto Configuration Server
Admin Guide

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

R069: Technical Report069

CP: Transmission Control Protocol

LS: Transport Layer Security

FTP: Trivial File Transfer Protocol

DP: User Datagram Protocol

RL: Uniform Resource Locator

LAN: Virtual Local Area Network

IG: 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.

