

About This Manual

Thank for choosing Akuvox E12S door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 312.30.2.9 version, and it provides all the configurations for the functions and features of Akuvox door phone. Please visit [Akuvox forum](#) or consult technical support for any new information or latest firmwares.

Introduction of Icons and Symbols



Warning:

- Always abide by this information in order to prevent the persons from injury.



Caution:

- Always abide by this information in order to prevent the damages to the device.



Note:

- Informative information and advice from the efficient use of the device.



Tip:

- Useful information for the quick and efficient use of the device.

Related Documentation

You are advised to refer to the related documents for more technical information via the link below:

<https://knowledge.akuvox.com>



FCC Caution:

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.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.

Table of Contents

1. Product Overview	1
2. Change Log	2
3. Model Specification	3
4. Introduction to Configuration Menu	4
5. Access the Device	6
5.1. Obtain Device IP Address	6
5.2. Access the Device Setting on the Web Interface	6
6. Language and Time Setting	7
6.1. Language Setting	7
6.2. Time Setting	8
7. LED Setting	10
7.1. Infrared LED Setting	10
7.2. LED Display Status	11
7.3. Set up LED Display from HTTP URL	12
7.4. LED Setting on Card Reader Area	12
8. Volume and Tone Configuration	14
8.1. Volume Configuration	14
8.2. Open Door Tone Configuration	15
8.3. Upload Tone Files	16
8.3.1. Upload Ringback Tone	16
8.3.2. Upload Open Door Tone	16
9. Network Setting	18
9.1. Network Status	18
9.2. Device Network Configuration	18
9.3. Device Deployment in Network	19
9.4. Device Local RTP configuration	20
9.5. NAT Setting	21
10. Intercom Call Configuration	22
10.1. IP call & IP Call Configuration	22
10.2. SIP Call & SIP Call Configuration	23
10.3. SIP Account Registration	23
10.4. SIP Server Configuration	24
10.5. Configure Outbound Proxy Server	25
10.6. Configure Data Transmission Type	25
10.7. Configure Calling Feature	26
10.7.1. DND	26
10.7.2. Push Button Call	27
10.7.3. Robin Call	28
10.7.4. Web Call	29
10.7.5. Auto Answer	29
10.7.6. Multicast	30

10.7.7. Configure Maximum Call Duration	31
10.7.8. Maximum Dial Duration	32
11. Audio& Video Codec Configuration for SIP Calls	33
11.1. Audio Codec Configuration	33
11.2. Video Codec Configuration	34
11.3. Configure DTMF Data Transmission	35
12. Access White List Configuration	36
12.1. Managing Contact Group	36
12.2. Managing Contacts	37
13. Relay Setting	38
13.1. Relay Switch Setting	39
13.2. Select Chime Bell Relay	40
13.3. Web Relay Setting	40
14. Door Access Schedule Management	43
14.1. Configure Door Access Schedule	43
14.1.1. Manage Door Access Schedule	43
15. Door Unlock Configuration	46
15.1. Configure Access Card Format	46
15.2. Configure Access Card for Door Unlock	47
15.3. Import and Export Card Data of Access Control	48
15.4. Configure Open Relay via HTTP for Door Unlock	49
15.5. Configure Exit Button for Door Unlock	50
16. Security	52
16.1. Tamper Alarm Setting	52
16.2. Motion Detection	52
16.2.1. Configure Motion Detection	53
16.3. Security Notification Setting	54
16.3.1. Email Notification Setting	54
16.3.2. FTP Notification Setting	55
16.3.3. SIP Call Notification Setting	56
16.3.4. HTTP URL Notification Configuration	56
16.3.5. TFTP Notification Setting	57
16.4. Security Action Configuration	57
16.4.1. Configure Push button Action	57
16.4.2. Configure Motion Action	58
15.4.3. Configure Input Action	58
16.5. Voice Encryption	59
16.6. User Agent	60
17. Monitor and Image	61
17.1. RTSP Stream Monitoring	61
17.1.1. RTSP Basic Setting	61
17.1.2. RTSP Stream Setting	62
17.2. MJPEG Image Capturing	64
17.3. ONVIF	66

17.4. Live Stream	67
18. Logs	68
18.1. Call Logs	68
18.2. Door Logs	69
19. Debug	71
19.1. Event Log	71
19.2. System Log	72
19.3. PCAP	73
20. Firmware Upgrade	75
21. Backup	76
22. Auto-provisioning via Configuration File	77
22.1. Provisioning Principle	77
22.2. Configuration Files for Auto-provisioning	78
22.3. AutoP Schedule	79
22.4. PNP Configuration	80
22.5. Static Provisioning Configuration	80
23. Integration with Third Party Device	82
23.1. Integration via Wiegand	82
23.2. Integration via HTTP API	83
24. Password Modification	86
24.1. Modifying Device Web Interface Password	86
24.2. Configure Web Interface Automatic Logout	86
25. System Reboot&Reset	87
25.1. Reboot	87
25.2. Reset	87
26. Abbreviations	88
27. Contact us	90


1. Product Overview

The security that comes with being able to control who comes into your building along with the ability to verbally and visually confirm their identity is immeasurable. Akuvox E12S is a SIP-compliant, hands-free and video(optional) 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. The door phone enables you to easily monitor an entrance door or gate and gives you the peace of mind knowing that your facility is more secure.

2. Change Log

The change log will be updated here along with the changes in the new software version.

3. Model Specification

Model & Feature	E12S 
Button	1 Physical button
Housing Material	Plastic
Camera	2 Mega pixels, automatic lighting
Relay In	2
Relay Out	1
RS485	√
PoE	√
RAM	128MB
ROM	16MB
Card Reader	√
IP Rating	IP65
IK Rating	X
Wall Mounting	√
Flush Mounting	X

4. Introduction to Configuration Menu

- **Status:** this sections gives you basic information such as product information, Network Information, and account information etc.
- **Account:** this section concerns SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, etc.
- **Network:** this section mainly deals with DHCP&Static IP setting, RTP port setting, and device deployment etc.
- **Intercom:** this section covers Intercom settings, Call Log etc.
- **Surveillance:** this section covers Motion Detection, RTSP, MJPEG, ONVIF, Live stream.
- **Access Control:** this section covers Input control, Relay, Card settings, Face Recognition setting, Private PIN Code, Wiegand connection etc.
- **Tenants:** this section involves Tenants management and Dial Plan.
- **Device:** this section includes Light settings, tab&button display, LCD settings and Voice settings.
- **Settings:** this section includes Time&language, Action settings, Door settings, Schedule for access control.
- **Upgrade:**this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault Diagnosis.
- **Security:** this section is for Password modification.

- **Mode selection :**
 1. **Discovery mode:** It is a plug and play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to network. It is super time-saving mode

and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations previously by the administrator.

2. **Cloud mode:** Akuvox Cloud is an all-in-one management system. Akuvox Cloud is the mobile service that allows audio, video, remote access control between smart phones and Akuvox intercoms. All configurations in the device will be issued automatically from cloud. If users decide to use Akuvox cloud, please contact Akuvox technical support, and they will help you configure the related settings before using.
3. **SDMC mode:** SDMC (**SIP Device Management Controller**) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for the door access, intercom, monitoring, alarm etc.,. It is a convenient tool for property manager to manage , operate and maintain the community.

● Tool selection

Akuvox has many configuration tools for you to set up devices more conveniently. Here we list some common tools, please contact your administrator to get the tool if you need them.

1. **SDMC:** SDMC is suitable for the management of Akuvox devices large communities, including access control, resident information, remote device control etc.
2. **Akuvox Upgrade tool:** Upgrade Akuvox devices in batch on a LAN (**Local Area Network**)
3. **Akuvox PC Manager:** Distribute all configuration items in batch on a LAN.
4. **IP scanner:** it is used to search Akuvox device IP addresses on a LAN.
5. **FacePro:** Manage face data in batch for the door phone on a LAN.

5. Access the Device

E12S system setting can be accessed on the device web interface.

5.1. Obtain Device IP Address

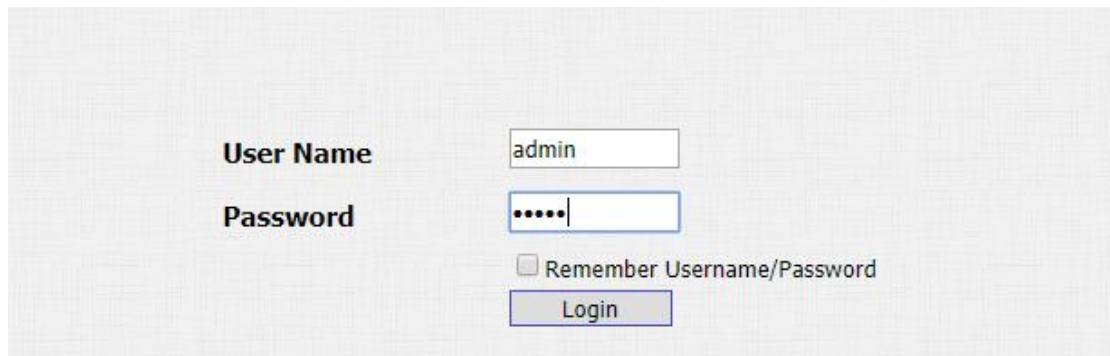
Check the Device IP address by holding the push button for 5s. Or searching the device IP by the IP scanner in the same LAN network. Just click **Scan** tab in IP scanner to check the device IP.

The screenshot shows the 'IP Scanner' web interface. At the top, it says 'Online Device : 7'. Below this is a search input field with 'Search' and 'Refresh' buttons. A table lists the following data:

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C11050785A9	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A8102020128A		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C11050A5951	R29	1.1.1.1.1	29.30.2.16

5.2. Access the Device Setting on the Web Interface

Enter the device IP address on the web browser in order to log in the device web interface where you can configure and adjust parameter etc. The initial user name and password are all "admin" and please be case-sensitive to the user names and passwords entered.



User Name: admin

Password:

Remember Username/Password

Login

**Tip:**

- You can also obtain the device IP address using the Akuvox IP scanner to log in the device web interface. Please refer to the URL below for the IP scanner application:
[http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s\[\]=ip&s\[\]=scanner](http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s[]=ip&s[]=scanner)

**Note:**

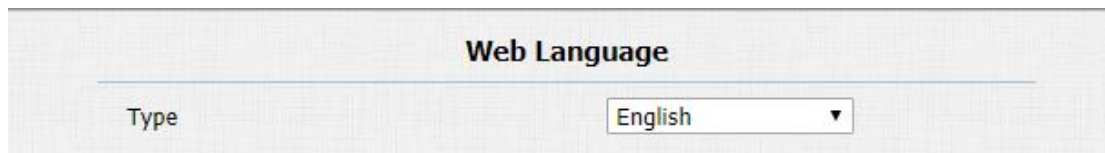
- Google Chrome browser is strongly recommended.

6. Language and Time Setting

6.1. Language Setting

When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can be set up on the

device web **Phone > Time/Lang > Web Language** interface according to your preference.



Parameter Set-up:

- **Type:** choose a suitable web language. Normally, English is the default web language.

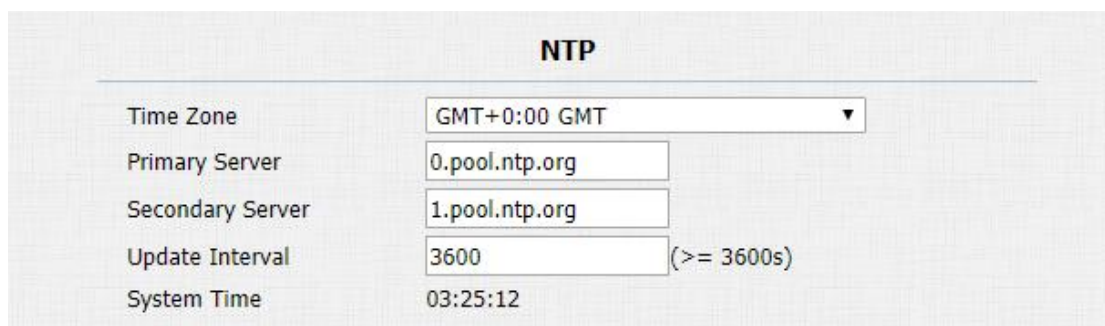


Note:

- For E12S, the operation path is **Setting > Time/Lang > Web Language**

6.2. Time Setting

The set-up on the the device web interface is identical with the setting on the device, it however allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. And when your time zone is selected, the device will automatically notify the NPT server of its time zone in order that the NTP server can synchronize the time zone set-up to your device.



Parameter Set-up:

- **Time Zone:** select the specific time zone depending on where the device is used and then press **Confirm** tab for the confirmation. The default time zone is **GMT GMT+0.00**.
- **Primary/Secondary Server:** the time zone server, normally it will automatically obtain the time when connecting to the network. The secondary server will take effect when the primary server is invalid.
- **Update Interval:** to configure interval between two consecutive NTP requests.

You can also set up time manually, select the **Manual** checkbox, and input time data.

Type

Manual

Date Year Mon Day

Time Hour Min Sec

Auto

7. LED Setting

7.1. Infrared LED Setting

Infrared LED is applied in the dark environment in which a resident might not be able to see a visitor clearly via the video from the door phone. If the infrared LED is turned off, the door phone will turn to night mode so that you can have a clear view of the visitor.

LED	
LED Type	<input type="text" value="Auto"/>
Min Photoresistor	<input type="text" value="20"/>
Max Photoresistor	<input type="text" value="45"/>

Parameter Set-up:

- **LED Type:** select "**Auto**" if you want the Infrared LED light to be turned on automatically according to the setting. select "**Always ON**" to enable the Infrared LED light to stay on permanently. select "**Always OFF**" to turn off the Infrared LED light. LED mode is set "**Always OFF**" by default. select "**Schedule**" to turn on the infrared LED according to the time schedule.
- **Min/Max Photoresistor:** set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the **ON-OFF** of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default Minimum and maximum photoresistor value is from "**0**" minimum to "**1000**" maximum respectively.
- **Start Time:** set the start time for the infrared LED to be turned on.
- **End Time:** set the end time for the infrared LED to be turned off.

Note:

- **Start Time** and **End Time** will not be displayed unless you select **Specific Time** for your LED mode.

7.2. LED Display Status

LED display adjustment is used to display the light changes of call button in the six status - normal(idle), offline, calling, talking and receiving a call. and the user can also verify the current mode of the device through the LED status. To setup on device web **Intercom > LED Setting** interface.

LED Status

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 ▼

The default LED Display Status:

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

Parameters Set-up:

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

- **Color Off:** the default status is **OFF**.
- **Color On:** it can support three colors: **Red, Green, Blue**.
- **Blink Mode:** to setup the different blink frequency.

 **Note:**

- The Status and Color off item can not be changed.
- The LED of upgrading mode can not be adjusted.
- E12S support three colors: **Red, Blue and Purple**.

7.3. Set up LED Display from HTTP URL

Akuvox door phones support to use HTTP URL to remote control the LED display status. You can enter the HTTP URL in the browser to manage the LED color and frequency.



Parameters Set-up:

- **HTTP URL format:**
`http://PhoneIP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500`
- **Status:** 1=Idle; 2=OffLine; 3=Calling; 4=Talking; 5=Receiving; Color: 1=Green; 2=Blue; 3=Red; Mode: 0=Always On; 1=Always Off; 500/1000/1500/2000/25000/3000

7.4. LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want to have the LED light on the card reader area to stay on, you can also set the timing for the exact time

span during which the LED light can be disabled in order to reduce the electrical power consumption.

Card LED Enable	Enabled ▼
Start Time (H)	18 - 06 (0~23)

Parameters Set-up:

- **Enabled:** Tick the check box if want to enable the card reader LED lighting and vice versa.
- **Start Time- End Time (H):** enter the time span for the LED lighting to be valid, e.g. if the time span is set from **8-0 (Sart time- End time)** it means LED light will stay on during the time span from **8:00 am to 12:00 pm** during one day (24 hours).

8. Volume and Tone Configuration

Volume and tone configuration in Akuvox door phone refers to the microphone volume, speaker volume, temper alarm volume, ringback tone and open door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

8.1. Volume Configuration

To set up the volumes, you can set up on device web **Phone > Voice** interface.

Mic Volume	
Mic Volume	<input type="text" value="8"/> (1~15)
Speaker Volume	
Speaker Volume	<input type="text" value="8"/> (1~15)
Tamper Alarm Volume	
Tamper Alarm Volume	<input type="text" value="8"/> (1~15)
Ringback Volume	
Ringback Volume	<input type="text" value="8"/> (1~15)
Voice Prompt Volume	<input type="text" value="15"/> (1~15)

Parameters Set-up:

- **Mic Volume:** Adjust the mic volume as needed.
- **Speaker Volume:** Adjust the speaker volume as needed.
- **Tamp Alarm Volume:** Adjust the volume for the tamper alarm.

- **Ringback volume:** Adjust the volume for the ringback tone.
- **Voice Prompt Volume:** Adjust the volume for voice prompt.

 **Note:**

- For E12S, the operation path is **Device > Voice > Volume control**.
- **Voice Prompt Volume** can only be configured on E12S.

8.2. Open Door Tone Configuration

You can not only enable or disable the Open Door Tone but also controls the prompt words that accompanies the tone on web **Intercom > Voice** interface.

Open Door Warning

Open Door Succ Warning	Enabled ▼
Open Door Failed Warning	Enabled ▼

Open Door Tone Setting

Open Door Inside Tone Enabled	<input type="checkbox"/>
Open Door Outside Tone Enabled	<input type="checkbox"/>

Parameters Set-up:

- **Open Door Success Warning:** click the field **Enabled** or **Disabled** depending on if you want to hear the prompt words that accompanies that **Open Door Success** tone.
- **Open Door Failed Warning:** click the field **Enabled** or **Disabled** depending on if you want to hear the prompt words that accompanies that **Open Door Failed** tone.
- **Open Door Inside Tone Enabled:** select the checkbox to enable the open door inside tone.

- **Open Door Outside Tone Enabled:** select the checkbox to enable the open door outside tone.

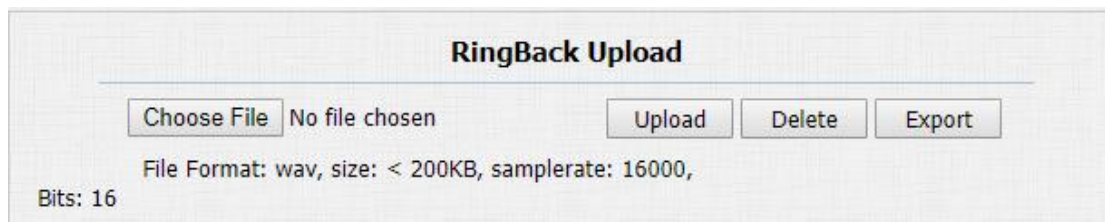
 **Note:**

- For E12S, the operation path is **Device > Voice**

8.3. Upload Tone Files

8.3.1. Upload Ringback Tone

You can customize the ringback tone if you need. Please follow the prompt about the file size and format.



The screenshot shows a web interface titled "RingBack Upload". It features a "Choose File" button, followed by the text "No file chosen". To the right are three buttons: "Upload", "Delete", and "Export". Below these elements, the text reads: "File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16".

8.3.2. Upload Open Door Tone

You can customize the door open tone if you need. Outside tone is used to open door via card or DTMF. Inside tone is used to open door via triggered input interface. Please follow the prompt about the file size and format.

Opendoor Outside Tone Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 8k/16k, Bits: 16

Opendoor Inside Tone Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 8k/16k, Bits: 16

9. Network Setting

9.1. Network Status

To check the network status on the web **Status > Network Information** interface.

Network Information	
LAN Port Type	DHCP Auto
LAN Link Status	Connected
LAN IP Address	192.168.1.3
LAN Subnet Mask	255.255.255.0
LAN Gateway	192.168.1.1
LAN DNS1	192.168.1.1
LAN DNS2	192.168.1.1

9.2. Device Network Configuration

You can check for the door phone's network connection info and configure the default DHCP mode (**Dynamic Host Configuration Protocol**) and static IP connection for the device on the device web **Network > Basic** interface.

LAN Port

DHCP
 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	

Parameter Set-up:

- **DHCP:** select the **DHCP** mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway and DNS server address automatically.
- **Static IP:** select the static IP mode by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your actual network environment.
- **IP Address:** set up the IP Address if the static IP mode is selected.
- **Subnet Mask:** set up the subnet Mask according to your actual network environment.
- **Default Gateway:** set up the correct gateway default gateway according to the IP address of the default gateway.
- **LAN DNS1/2:** set up preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address and the door phone will connects to the alternate server when the primary DNS server is unavailable .

9.3. Device Deployment in Network

Door phones should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address

and extension numbers as opposed to other devices for the device control and the convenience of the management. So you can do it on web **Network > Advanced > Connect Setting** interface.

Connect Setting

Server Type	<input type="text" value="SDMC"/>
Discovery Mode	<input type="text" value="Disabled"/>
Device Address	<input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="Door Unit"/>

Parameter Set-up:

- **Server Type:** it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC** or **Cloud and None**. **None** is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **Discovery Mode:** click **"Enable"** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click **"Disable"** if you want to conceal the device so as not to be discovered by other devices.
- **Device Address:** specify the device address by entering device location information from the left to the right :**Community, Unit, Stair, Floor, Room** in sequence.
- **Device extension:** enter the device extension number for the device you installed.
- **Device Location:** enter the location in which the device is installed and used.

9.4. Device Local RTP configuration

For the device network data transmission purpose, device needs to be set up with a range of RTP port (**Real-time Transport Protocol**) for establishing an exclusive range of data transmission in the network.

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

Parameter Set-up:

- **Starting RTP Port:** enter the Port value in order to establish the start point for the exclusive data transmission range.
- **Max RTP port:** enter the Port value in order to establish the end point for the exclusive data transmission range.

9.5. NAT Setting

NAT (**Network Address Translation**) allows hosts in an organization's private intranet to transparently connect to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. To do this configuration on web **Account > Advance > NAT** interface.

NAT		
UDP Keep Alive Messages	<input type="text" value="Enabled"/>	▼
UDP Alive Msg Interval	<input type="text" value="30"/>	(5~60s)
RPort	<input type="text" value="Enabled"/>	▼

Parameter Set-up:

- **UDP Keep Alive Messages:** If enabled, the device will send out the message to the SIP server so that SIP server will recognize if the device is in online status.
- **UDP Alive Msg Interval:** set the message sending time interval from 5-60 seconds, the default is 30 seconds.

- **RPort**: enable the Rport when the SIP server is in WAN (**Wide Area Network**).

10. Intercom Call Configuration

Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

10.1. IP call & IP Call Configuration

IP call can be made directly on the intercom device by entering the IP number on the device. And you can also disable the direct IP call if you do not allow IP call to be made on the device.

Direct IP	Enabled ▾
Direct IP AutoAnswer	Enabled ▾
Direct IP Port	5060 (1~65535)

Parameters Set-up:

- **Direct IP Call**: click “**Enable**” or “**Disable**” to turn the direct IP call on or off. For example if you do not allow direct IP call to be made on the device, you can click “**Disable**” to terminate the function.
- **Direct IP AutoAnswer**: click “**Enable**” or “**Disable**” to turn the direct IP call on or off when the phone automatically answer the incoming call.
- **Direct IP port** : set up the IP direct call port, 5060 is the default port.

10.2.SIP Call &SIP Call Configuration

You can make SIP call (**Session Initiation Protocol**) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

10.3.SIP Account Registration

Akuvox door phones support two SIP accounts that can all be registered according to your applications. You can for example, switch between them if any one of the account failed and become invalid. The SIP account can be configured on the device and on the device interface.To perform the SIP account setting on the Web **Account > Basic > SIP Account** Interface.

SIP Account	
Status	UnRegistered
Account	Account 1 ▾
Account Active	Disabled ▾
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	••••••

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account Active:** click **Enable** or **Disable** to activate or deactivate the registered SIP account.
- **Display Name:** configure the name, for example the device's name to be shown on the device being called to.
- **User Name:** enter the user name obtained from SIP account administrator.

- **Account:** select the exact account (Account 1&2) to be configured.
- **Display Label:** configure the device label to be shown on the device screen.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

10.4.SIP Server Configuration

SIP servers can be set up for device in order to achieve call session through SIP server between intercom devices. To do this configuration also on web **Account > Basic > SIP Server** interface.

SIP Server 1		
Server IP	<input type="text" value="192.168.35.11"/>	Port <input type="text" value="5060"/>
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)

Parameter Set-up:

- **Preferred SIP Server:** enter the primary server IP address number or its URL.
- **Alternate SIP Server:** enter the backup SIP server IP address or its URL.
- **Port:** set up SIP server port for data transmission.
- **Registration Period:** set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is "1800", ranging from **30-65535s**.

10.5. Configure Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish call session via port-based data transmission. To set it up on the device web **Account > Basic > Outbound Proxy Server** Interface.

Outbound Proxy Server			
Enable Outbound	<input type="text" value="Enabled"/>		
Server IP	<input type="text" value="112.39.22.140"/>	Port	<input type="text" value="5060"/>
Backup Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>

Parameter Set-up:

- **Enable Outbound:** click “Enable” and “Disable” to turn on or turn off the outbound proxy server.
- **Preferred Server IP:** enter the SIP address of the primary outbound proxy server.
- **Port:** enter the Port number for establish call session via the primary outbound proxy server
- **Alternate Server IP:** set up Backup Server IP for the backup outbound proxy server.
- **Port:** enter the port number for establishing call session via the backup outbound proxy server.

10.6. Configure Data Transmission Type

SIP message can be transmitted in three data transmission protocols: **UDP (User Datagram Protocol)**, **TCP(Transmission Control Protocol)**, **TLS (Transport Layer Security)** and **DNS-SRV**. In the meantime, you can also identify the server from which the data come from. To do this configuration

on web **Account > Basic > Transport Type** interface.

Parameter Set-up:

- **UDP:**select “UDP” for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP:** select “TCP” for Reliable but less-efficient transport layer protocol.
- **TLS:** select “TLS” for Secured and Reliable transport layer protocol.
- **DNS-SRV:** select “DNS-SRV” to obtain DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

10.7. Configure Calling Feature

10.7.1. DND

DND (**Do not disturb**) setting allows you not to be disturbed by any unwanted incoming SIP calls. You can set up DND related parameters properly on the device web **Phone > Call Feature** interface to block SIP calls you do not intend to answer. In the meantime, you can also define the code to be sent to the SIP server when you want to reject the call.

Parameter Set-up:

- **Account:** select “Account1”, “Account2” or “All account” for the DND application.
- **DND:** enable or disable the DND function. DND function is disabled by default.
- **Return Code When DND:** select what code should be sent to the calling device via SIP server. **404** for “Not found”; **480** for “ Temporary unavailable” **486** for “busy here”.
- **DND On Code:** turn on the DND on server using the Code obtained. The DND on Code is **78** by default.
- **DND Off Code:** turn off the DND on server using the code obtained. The DND off Code is **79** by default.
- **Return Code When Refuse:** select code to be sent the caller side via SIP server when you rejected the incoming call.

 **Note:**

- For E12S, the operation path is **Intercom > Call Feature**

10.7.2. Push Button Call

Push buttons which are used to initiate calls. Each push button can be bound to 6 sip numbers or IP addresses maximum, that means users can make 6 numbers at the one time by pressing push button.

Push Button						
Key	Number1	Number2	Number3	Number4	Number5	Number6
Push Button 1	111	112	113	114	115	116
Push Button 2	192.168.1.4	192.168.1.5	192.168.1.6			
Push Button 3						
Push Button 4						
Push Button 5						

Note:

- E12S has only one push button.
- E12S supports 8 lines, which means users can connect to 8 contacts simultaneously by pressing push button.

10.7.3. Robin Call

Robin call is used to initiate multiple numbers which set up in Push Button one by one. If the previous callee do not answer within the robin call timeout, the call will be transferred to next one. If the call is answered by one of the callee, the call will not be transferred any more.

Robin Call	
Robin Call Enable	Disabled ▼
Robin Call Timeout	60 ▼

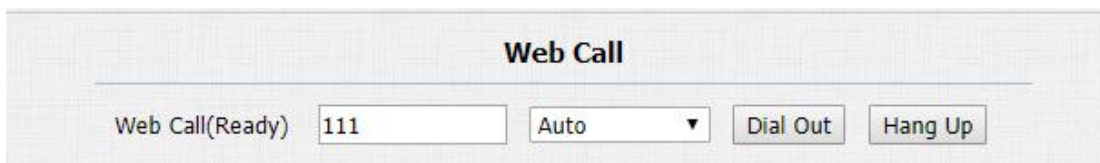
Parameters Set-up:

- **Robin Call Enable:** Enable or disable the robin call function. It is disabled by default.

- **Robin Call Timeout:** Call out time value for each number, range from 5 - 60s.

10.7.4. Web Call

In addition to making IP/SIP call directly on the device, you can also make the call on the device web interface without approaching to device physically for testing purpose etc.



Parameters Set-up:

- **Auto/Account1/Account2:** To choose a suitable SIP account to make a web call. If you call out using IP address, Account selection is no need to chosen.

10.7.5. Auto Answer


You can define how quick the door phone should response in answering the incoming SIP/IP call automatically by setting up the time related parameters. In addition, you can also define the mode in which the calls are to be answered (video mode or audio mode). To enable this feature on web **Account > Advanced** interface, you can set up the related parameters on web **Phone > Call Feature**.



Parameters Set-up:

- **Auto Answer:** Turn on the the Auto Answer function by clicking “**Enable**”.

- **Auto Answer Delay:** Set up the delay time (from 0-5 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Auto Answer Mode:** Set up the video or audio mode you preferred for answering the call automatically.

 **Note:**

- For E12S, the operation path is **Intercom > Call Feature**.

10.7.6. Multicast

Multicast uses one-to-many mode to communicate in a range. Door phone can be a listener and receive the audio from the listened part.

Multicast Setting

Paging Barge 1 ▼

Paging Priority Active Enabled ▼

Priority List

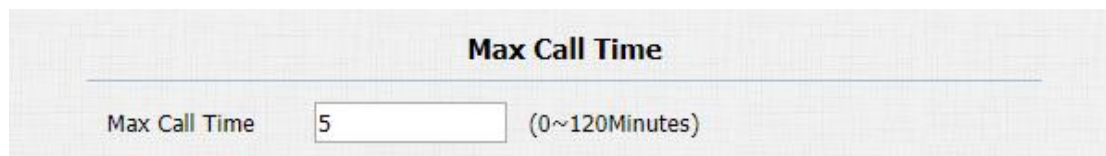
IP Address	Listening Address	Label	Priority
1 IP Address	<input type="text" value="224.1.6.11:1200"/>	<input type="text" value="Akuvox"/>	1
2 IP Address	<input type="text"/>	<input type="text"/>	2
3 IP Address	<input type="text"/>	<input type="text"/>	3
4 IP Address	<input type="text"/>	<input type="text"/>	4
5 IP Address	<input type="text"/>	<input type="text"/>	5
6 IP Address	<input type="text"/>	<input type="text"/>	6
7 IP Address	<input type="text"/>	<input type="text"/>	7
8 IP Address	<input type="text"/>	<input type="text"/>	8
9 IP Address	<input type="text"/>	<input type="text"/>	9
10 IP Address	<input type="text"/>	<input type="text"/>	10

Parameters Set-up:

- **Paging Barge:** multicast or how many multicast calls are higher priority than SIP call, if you disable Paging Priority Active, SIP call will have high priority.
- **Paging Priority Active:** multicast calls are called in order of priority or not.
- **Listening Address:** Enter the multicast IP address you want to listen. The multicast IP address need to be same as the listened part and the multicast port can not be same for each IP address. Multicast IP address is from 224.0.0.0 to 239.255.255.255.
- **Label:** Enter the label for each listening address.

10.7.7. Configure Maximum Call Duration

Door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the calling automatically.



Max Call Time

Max Call Time (0~120Minutes)

Parameters Set-up:

- **Max Call Time:** Enter the call time duration according to your need (Ranging from 0-120 min.). The default call time duration is 5 min.

Note:

- Max call time of device is also related with max call time of SIP server. If using SIP account to make a call, please pay attention to the max call time of SIP server. If the max call time of SIP server is shorter than the max call time of device , the shorter one is available.

10.7.8. Maximum Dial Duration

Maximum Dial duration is consisted of Maximum dial in time duration and the maximum dial out time. Maximum dial in time refers to the maximum time duration before the door phone hang up the call if the call is not answered by the door phone. In contrary, Maximum dial out time refers to the maximum time duration before the door phone hang up itself automatically when the call from the door phone is not answered by the intercom device being called.

Max Dial Time		
Dial In Time	<input type="text" value="60"/>	(1~120Sec)
Dial Out Time	<input type="text" value="60"/>	(1~120Sec)

Parameters Set-up:

- **Dial in Time:** Enter the dial in time duration for you door phone (ranging from 30-120 sec.) for example, if you set the dial in time duration is 60 second in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 second is the dial in time duration by default.
- **Dial out Time:** Enter the dial in time duration for your door phone (ranging from 5-120 sec.) for example, if you set the dial out time duration is 60 second in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answer by the device being called.

**Note:**

- Max dial time of device is also related with max dial time of SIP server. If using SIP account to make a call, please pay attention to the max dial time of SIP server. If the max dial time of SIP server is shorter than the max dial time of device, the shorter one is available.

11. Audio & Video Codec Configuration for SIP Calls

11.1. Audio Codec Configuration

Akuvox door phone supports four types of Codec (PCMU, PCMA, G729, G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of the sound quality. You can select the specific codec with different bandwidth and sample rate flexibly according to the actual network environment. To do the configuration on device web **Account > Advanced** interface.

SIP Account

Account Account 1 ▼

Codecs

Disabled Codecs

>>

<<

Enabled Codecs

PCMU

PCMA

G722

G729

↑

↓

Please refers to the bandwidth consumption and sample rate for the four codecs types below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz

11.2.Video Codec Configuration

Akuvox door phone support H264 codec that provides a better video quality at much lower bit rate with different video quality and payload. To set up

video codec on web **Account > Advanced** interface.

Video Codec

Codec Name	<input checked="" type="checkbox"/> H264
Codec Resolution	4CIF ▼
Codec Bitrate	2048 ▼
Codec Payload	104 ▼

Parameter Set-up:

- **Codec Name:** Check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Codec Resolution:** select the code resolution for the video quality among four options: "QCIF", "CIF", "VGA", "4CIF" and "720P" according to your actual network environment. The default code resolution is 4CIF.
- **Codec Bitrate:** select the video stream bit rate (Ranging from 320-2048). The greater the bitrate, the data transmitted in every second is greater in amount therefore the video will be clearer.. While the default code bitrate is 2048.
- **Codec Payload:** select the payload type (ranging from 90-118) to configure audio/video configuration file. The default payload is 104.

11.3. Configure DTMF Data Transmission

In order to achieve the door access via DTMF code or some other applications, you are required to properly configure DTMF on web **Account > Advanced > DTMF** in order to establish a DTMF-based data transmission between the door phone and other intercom device for the third party integration.

DTMF

Type	RFC2833 ▼
How To Notify DTMF	Disabled ▼
DTMF Payload	101 (96~127)

Parameter Set-up:

- **Type:** select DTMF mode among five options: **"Inband"**, **"RFC2833"**, **"Info+Inband"** and **"Info+RFC2833"** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF:** select among four types: **"Disable"** "DTMF" **"DTMF-Relay"** **"Telephone-Event"** according to the specific type adopted by the third party device. You are required to set it up only when the third party device to be matched with adopts **"Info"** mode
- **DTMF Payload:** set the payload according the the specific data transmission payload agreed on between the sender and receiver during the data transmission.

12. Access White List Configuration

Akuvox door phone supports to store up to 500 contacts that can give an access permission to the indoor monitor or another devices. Access White list includes group setting and contact setting and management. To setup it on web **Access Whitelist > Access Whitelist**.

12.1.Managing Contact Group

Enter the group name in the Name column and set up the ring and the description information for the group to add a new group. Check and manage the existing groups in the group list.

Group

Index	Name	Ring	Description	
1	test1	Auto	akuvox group	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>

Delete
Delete All

Group Setting

Name

Ring

Auto ▼

Description

Add
Edit
Cancel

Parameter Set-up:

- **Name:** the group name.
- **Ring:** the incoming call ring for the group.
- **Description:** the remarked information for the group.

12.2.Managing Contacts

You can search, create, display ,edit and delete the contacts in your phone book.

Contact All Contacts ▾

Search Search Reset

Index	Name	Phone Num	Group	Ring	<input type="checkbox"/>
1	Aku..	112425	test1	Auto	<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Page 1 ▾ Prev Next Move To All Contacts ▾ Delete Delete All

Contact Setting

Name Phone Num

Group Default ▾ Ring Auto ▾

Add Edit Cancel

Parameters Set-up:

- **Name:** enter the contact name, which is required.
- **Phone:** enter the phone number of the contact, which is required.
- **Group:** click the green tab to select the group name you have created. You cannot select the group name if no group name has been created.
- **Account:** select which SIP account will be used to call out. If using IP direct call, it is not available.
- **Priority of Call:** up to 3 numbers in one group and setup the call sequence for these numbers.

13. Relay Setting

13.1. Relay Switch Setting

You can configure the relay switch(es) and DTMF for the door access on the web **Intercom > Relay** interface.

The screenshot shows the 'Relay' configuration page with the following settings:

Parameter	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

Parameter Set-up:

- **Relay Delay (Sec):** set the relay trigger delay timing (Ranging from 1-10 Sec.) For example, if you set the delay time as "5" Sec. Then the relay will not triggered until 5 seconds after you press "unlock " tab.
- **DTMF Option:** select the number of DTMF digit for the door access control (**Ranging from 1-4 digits**) For example, you can select 1 digit DTMF code or 2-digit DTMF code etc., according to your need.
- **DTMF :** set the 1-digit DTMF code within range from (**0-9 and *,#**).
- **Multiple DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMF Mode** is set as 3-digits.
- **Relay Status:** relay status is low by default which means normally closed(NC) If the relay status is high, then it is in Normally Open status(NO).

**Note:**

- Only the external devices connected to the relay switch needs to be powered by power adapters as relay switch does not supply power.

**Note:**

- If DTMF mode is set as “**1 Digit DTMF**” , you cannot edit DTMF code in **2~4 Digits DTMF** field. And if you set DTMF mode from 2-4 in **2~4 Digits DTMF** field, you can not edit DTMF code in **1 Digit DTMF** field.

13.2. Select Chime Bell Relay

This function is used to trigger a relay when call out. It is often used in some specific scenario.

**Parameters Set-up:**

- **Apply Setting to:** there are three options can be chosen “None” “Relay A” “Relay B”. which one is chosen, it will be triggered after press call button.

13.3. Web Relay Setting

In additional to the relay that is connected to the door phone, you can also control the door access using the network-based web relay on the device and on the device web interface.

Web relay needs to be set up on the web **Phone > WebRelay** interface where

you are required to fill in such information as relay IP address, password, web relay action etc before you can achieve the door access via web relay.

Web Relay

Type Disabled ▼

IP Address

UserName

Password

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 02	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 03	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 04	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 05	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 06	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 07	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 08	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 09	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 10	<input type="text"/>	<input type="text"/>	<input type="text"/>

Parameter Set-up:

- **Type:** select among three options **“Disabled”** **“WebRelay”** and **“Both”**. Select **“Webrelay”** to enable the web relay. Select **“Disable”** to disable the web relay. Select **“Both”** to enable both local relay and web relay.
- **IP Address:** enter the we relay IP address provided by the web relay manufacturer.
- **User Name:** enter the User name provided by the web relay manufacturer.
- **Password:** enter the password provided by the web relay manufacturer. The passwords is authenticated via HTTP and you can define the passwords using **“http get”** in Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without adding ip, username, pwd, you can fill in the HTTP command in the web relay action, so you can configure multiple webrelays

- **Web Relay Key:** it can be null or enter the configured DTMF code, when the door is unlock via DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension:** it can be null or enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below:

[http://admin:admin@192.168.1.2/state.xml?relayState=2.](http://admin:admin@192.168.1.2/state.xml?relayState=2)



Note:

- For E12S, the operation path is **Access Control > Web Relay.**

14. Door Access Schedule Management

You are required to configure and make schedule for the user-based door access via RF card, Private PIN and Facial recognition.

14.1. Configure Door Access Schedule

You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. More over, you can edit your door access schedule if needed.

14.1.1. Manage Door Access Schedule

You can create the door access schedule on a daily or monthly basis and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis. To do this configuration on web **Intercom > Schedules** interface.

Schedule Setting

Schedule Type: Daily ▼

Schedule Name:

Date Time: HH ▼ : MM ▼ - HH ▼ : MM ▼

Add
Reset

Schedule Manage

Index	Type	Name	Date	Day of Week	Time	
1	Daily	Test	-	-	04:00-18:00	<input type="checkbox"/>
2						<input type="checkbox"/>
3						<input type="checkbox"/>
4						<input type="checkbox"/>
5						<input type="checkbox"/>
6						<input type="checkbox"/>
7						<input type="checkbox"/>
8						<input type="checkbox"/>
9						<input type="checkbox"/>
10						<input type="checkbox"/>

Page: 1 ▼
Prev
Next
Delete
Delete All

Parameters Set-up:

- **Schedule Type:** set the type of time period. There are three types to choose from: Daily, Weekly, and Normal. The default is Daily.
- **Schedule Name:** set the name of the time period.
- **Date Time:** set the corresponding time period.
- **Day of Week:** select the corresponding day of the week. This field will only be displayed when the Week and Normal types are selected.
- **Date Range:** set the corresponding date. This field will only be displayed when the Normal type is selected.



Note:

- For E12S, the operation path is **Setting > Schedule**.

15. Door Unlock Configuration

Akuvox door phone offer you many types of door access. You can configure them on the device and web interface. More over, you can import or exporting the configured files to maximize your RF card configuration efficiency.

15.1. Configure Access Card Format

If you want to integrate with the third party intercom system in terms of RF card door access, you can change the RF card code format to be identical with that applied in the third party system. You can do this configuration on web **Intercom > Advanced** interface.

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

Parameters Set-up:

- **ICCARD Display Mode:** Select the card code format for the **IC card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR**. The card code format is 8HN by default in the door phone.
- **IDCard Display Mode:** Select the card format for the **ID Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR**. The card code format is 8HN by default in the door phone.
- **WIEGAND Display Mode:** Select the card format for the **WIEGAND Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR**. The card code format is 8HN by default in the door phone.

15.2. Configure Access Card for Door Unlock

You can manage the card number and corresponding parameters on web **Intercom > Card Setting** interface.

ID/IC Enabled

IC Enabled

ID Enabled

Card Status

Card Status

Card Setting

IC Key DoorNum RelayA RelayB

IC Key Tags

IC Key Name

IC Key Code

Schedule Management

All Schedules

Enable Schedules

Parameters Set-up:

- **IC/ID Enable:** to active the IC or ID card type.
- **Card Status:** select “**Car Issuing**” in the field before adding the RFID card and change the status back to “**Normal**” after the card is added.
- **IC key DoorNum:** select the relay switch available for the RIFD card door access.

- **IC Key Tags:** select the frequency of the validity the RFID card for the door access among three options: **“Allow” “Schedule” and “Forbidden”** For example, if you select **“Allowed”** then the card is always valid for unlimited door access according to your setting. If you select **“Schedule”** you are required to set up the specific time of the RFID card access validity. If you select **“Forbidden”** then the RFID card will never be valid for the door access.
- **Frequency:** if select the Tags as **“schedule”**, you also need to set up the using frequency which means the number of times the card can be used in a special time period.
- **IC key Code:** find the RFID card code in the field.
- **Schedule Management:** select an available time for the card from All Schedule to Enable Schedule.

 **Note:**

- RF card with 13.56 MHz and 125 KHz can be applicable to the door phone for the door access.

15.3.Import and Export Card Data of Access Control

Akuvox door phones support card data of access control to shared among Akuvox door phones through import and export while you can also export the card data out of the door phone and then import to a third party device on web **Intercom > Card Setting** interface.

Import/Export Card Data(.xml)

No file chosen

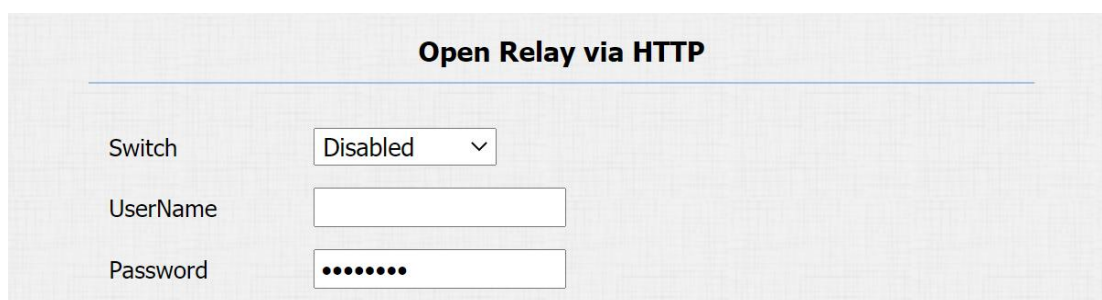
Card AES Key

 **Note:**

- For E12S, the operation path is **Access Control > Card Setting**.

15.4. Configure Open Relay via HTTP for Door Unlock

You can unlock the door remotely without approaching the device physically for the door access by typing in the created the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access. To do this configuration on web **Intercom > Relay** interface.



Open Relay via HTTP

Switch

UserName

Password

Parameter Set-up:

- **Enable:** enable the HTTP command unlock function by clicking on **Enable** field.
- **User Name:** enter the user name of the device web interface, for example **"Admin"**.
- **Password:** enter the password for the HTTP command. For example : **"12345"**.

Please refer to the following example:

<http://192.168.35.127/cgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1>



Note:

- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.
- For E12S, the operation path is **Access Control > Relay**.

15.5. Configure Exit Button for Door Unlock

When you need to open the door from inside using the Exit button installed by the door, you can configure the door phone Input to trigger the relay for the door access on web **Intercom > Input** interface.

Input A

Input Service:

Trigger Option:

Action to execute: FTP Email Sip Call HTTP

Http URL:

Action Delay: (0~300 Sec)

Open Relay:

Door Status: DoorA: High

Parameter set-up:

- **Input service:** Select “ **Enable** “ to be able to use the Input function.
- **Trigger Option:** Select the trigger options according the actual operation on the exit button.
- **Action To Execute:** select the method to carry out the action among four options: FTP, Email, HTTP, TFTP.
- **Http URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For

example, if you set the action delay time at 5 seconds., then the corresponding actions will be carried out 5 seconds after your press the button.

- **Open Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

**Note:**

- For E12S, the operation path is **Access Control > Input**.

16. Security

16.1. Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm while sending out calls to the designated location. Tamper alarm will be triggered off when the door phone changes its gravity value as opposed to its original gravity value set up when the device is installed.

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

Parameter Set-up:

- **Tamper Alarm:** click to select "ON " in the Tamper Alarm field in order to enable the anti-theft alarm function.
- **Gravity Sensor Threshold:** set the threshold for the gravity sensory sensitivity. The lower the value is, the more sensitive the gravity sensor. The gravity sensor value is 32 by default.

16.2. Motion Detection

Motion Detection is often used for unattended surveillance video and automatic alarm. The images collected by the camera at different frame rates will be calculated and compared by the CPU according to a certain algorithm. When the picture changes, if someone walks by, the lens is moved, the number obtained by the calculation and comparison result will exceed the threshold and indicate that the system can the corresponding processing is made automatically.

16.2.1. Configure Motion Detection

You can turn on the motion detection and set up the motion detection interval on the device.

Motion Detection Options

Motion Detection Disabled ▾

Time 10 (0~120 Sec)

Motion Detect Time Setting

Mon Tue Wed Thur

Fri Sat Sun Check All

00 ▾ : 00 ▾ - 23 ▾ : 59 ▾

Parameter Set-up:

- **Motion Detection:** To enable or disable Motion Detection.
- **Time:** set the time interval for the motion detection. If you set the default time interval as "10" Sec, then the motion detection time span will be 10 seconds. Assuming that we set the time interval as "10" then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) any where between 7-10 seconds once the movement is detected. "10" Sec interval is a complete cycle of the motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the " **Time interval minus three**"

16.3. Security Notification Setting

16.3.1. Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web **Intercom > Action > Email Notification** interface properly. The email notification will show as the captures.

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"/>	

Parameter set-up:

- **Sender's email address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's Email Address:** enter the receiver's email address.
- **SMTP Server Address:** enter the SMTP server address of the sender.
- **SMTP User Name:** enter the SMTP user name, which is usually the same with sender's email address.
- **SMTP Password:** configure the password of SMTP service, which is same with sender's email address.
- **Email Subject:** enter the subject of the email.

- **Email Content:** compile the emails contents according to your need

**Note:**

- For E12S, the operation path is **Setting > Action > Email Notification**

16.3.2. FTP Notification Setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the web **Intercom > interface > FTP Notification** properly.

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"/>

Parameter set-up:

- **FTP Server:** enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name:** enter the FTP server user name.
- **FTP Password:** enter the FTP server password.

**Note:**

- For E12S, the operation path is **Setting > Action > FTP Notification**

16.3.3. SIP Call Notification Setting

In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered. To configure a SIP call notification on web **Intercom > Action > SIP Call Notification** interface.

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

Parameter Set-up:

- **SIP Call Number:** To configure SIP call number.
- **SIP Call Name:** To configure display name of door phone.



Note:

- For E12S, the operation path is **Setting > Action > SIP Call Notification**

16.3.4. HTTP URL Notification Configuration

Akuvox door phones support to sending the HTTP notification to the third party when some features are triggered. HTTP notification can be set up specific chapters, please check chapter 15.4. The URL format: **http://http server IP address/any information**.

Action to execute	FTP <input type="checkbox"/>	Email <input type="checkbox"/>	Http URL <input type="checkbox"/>
Http URL:	<input type="text"/>		

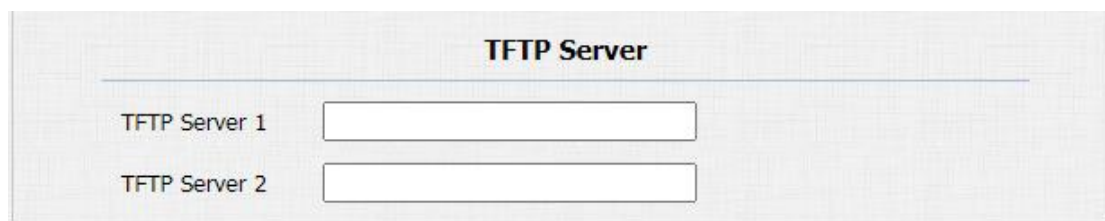
Parameter Set-up:

- **Http URL:** tick the check box to enable HTTP URL notification.

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

16.3.5. TFTP Notification Setting

Akuvox door phones support to send the capture via TFTP server when using Motion Detection. This feature need to work with SDMC server. Enter the SDMC server address then you can get the image in SDMC server.



TFTP Server

TFTP Server 1

TFTP Server 2

Parameter Set-up:

- **TFTP Server 1/2:** enter TFTP server address. You can enter the SDMC server address in Server 1, and the indoor monitor address which in the same house in Server 2. When Motion Detection is triggered , the SDMC and indoor monitor will receive the capture at the same time.



Note:

- E12S does not support to send the capture via TFTP server.

16.4. Security Action Configuration

16.4.1. Configure Push button Action

When pressing the push button, the door phone will trigger the pre-configured action type, the notification can be sent out by the Email, FTP notification or a SIP call. To do this configuration on web **Intercom > Basic**

interface.

PushButton Action

Action to execute FTP Email Http URL

Http URL:

Parameter Set-up:

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

16.4.2. Configure Motion Action

When the Motion Detection feature is working , you can make it trigger an action. To do this configuration on web **Intercom > Motion** interface.


Action to execute

Action to execute FTP Email Sip Call HTTP

Http URL:

Parameter Set-up:

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

 **Note:**

- For E12S, the operation path is **Surveillance > Motion**

When Input interface is working , it can also trigger an action. You can do this configuration on web **Intercom > Input** interface.

Action to execute FTP Email Sip Call HTTP


Http URL:

Action Delay (0~300 Sec)

Open Relay

Parameter Set-up:

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

 **Note:**

- For E12S, the operation path is **Access Control > Input**

16.5.Voice Encryption

SRTP(Secure Real-time Transport Protocol) is a protocol defined on the basis of Real-time Transport Protocol. The data of the transmission protocol provides encryption, message authentication, integrity assurance and replay protection. To configure this feature on web **Account > Advanced > Encryption** interface.

Encryption

Voice Encryption(SRTP)

Parameter Set-up:

- **Voice Encryption(SRTP):** choose **Disabled**, **Optional** or **Compulsory** for SRTP. If it is **Optional** or **Compulsory**, the voice during the call is encrypted, and you can grab the RTP packet to view

16.6. User Agent

You 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.

User Agent	
User Agent	<input type="text"/>

Parameter Set-up:

- **User Agent:** support to enter another specific value, Akuvox is by default.

17. Monitor and Image

17.1. RTSP Stream Monitoring

Akuvox door phones support RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or obtaining the the real time audio/ video (RTSP stream) from the door phone using the correct URL.

17.1.1. RTSP Basic Setting

You are required to set up RTSP function on device web **Intercom > RTSP > RTSP Basic** interface in terms of RTSP Authorization, authentication and password etc before you are able to use the function.

RTSP Basic

RTSP Server Enabled	<input checked="" type="checkbox"/>
RTSP Authorization	<input type="checkbox"/>
MJPEG Authorization	<input type="checkbox"/>
RTSP Authentication Type	Basic ▾
RTSP User Name	admin
RTSP Password	••••••••

Parameter Set-up:

- **RTSP Server Enable:** click on Enable and Disable in **RTSP Enable** field to turn on or turn off the RTSP function.
- **RTSP Authorization:** click on Enable and Disable in RTSP Authorization field to enable or disable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, RTSP Password on the intercom device such as indoor monitor for authorization.

- **RTSP User Name:** enter the name used for RTSP authorization.
- **RTSP User Password:** enter the password for RTSP authorization.
- **RTSP Authentication Type:** select RTSP authentication type between "Basic" and "Digest". "Basic" is the default authentication type.



Note:

- For E12S, the operation path is **Surveillance > RTSP**.

17.1.2. RTSP Stream Setting

You can select the video codec format for the RTSP stream for the monitoring and configure video resolution and bit-rate etc based on your actual network environment on the web **Intercom > RTSP > RTSP stream** interface.

RTSP Stream	
RTSP Audio Enabled	<input type="checkbox"/>
RTSP Video Enabled	<input checked="" type="checkbox"/>
RTSP Video2 Enabled	<input checked="" type="checkbox"/>
RTSP Audio Codec	PCMU ▾
RTSP Video Codec	H.264 ▾

Parameter Set-up:

- **RTSP Audio Enabled:** tick to enable RTSP audio which means , the door phone can also send audio information to the monitor by RTSP.
- **RTSP Video Enabled:** the door phone can send the video information to the monitor. After enabling RTSP feature, the video RTSP is enabled by default and can not be modified.

- **RTSP Video2 Enabled:** Akuvox door phones support 2 RTSP streams, you can enable the second one.
- **RTSP Audio Codec:** choose a suitable audio codec for RTSP audio.
- **RTSP Video Codec:** choose a suitable video codec for RTSP video.

H.264 And H.265 Video Parameters

Video Resolution	720P ▼
Video Framerate	30 fps ▼
Video Bitrate	2048 kbps ▼
Video2 Resolution	VGA ▼
Video2 Framerate	30 fps ▼
Video2 Bitrate	512 kbps ▼

Parameter Set-up:

- **Video Resolution:** select video resolutions among seven options: "QCIF", "QVGA", "CIF", "VGA", "4CIF", "720P". The default video resolution is "4CIF". and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than "4CIF".
- **Video Framerate:** "30fps" is the video frame rate by default.
- **Video Bitrate:** select video bit-rate among six options: "128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs" according to your network environment. The default video bit-rate is " 2048 kpbs".
- **Video2 Resolution:** select video resolution for the second video stream channel. While the default video solution is "VGA".
- **Video2 Framerate:** select the video framerate for the second video stream channel. "25fps" is the video frame rate by default for the second video stream channel.
- **Video2 Bitrate:** select video bit-rate among the six options for the second video stream channel. While the second video stream channel is "512 kpbs" by default.

17.2.MJPEG Image Capturing

Akuvox door phones allow you to capture the Mjpeg format monitoring image if needed. You can enable the Mjpeg function on **Intercom > RTSP > RTSP Basic** and set the image quality on the web **Intercom > RTSP > MJPEG Video Parameters** interface.

RTSP Basic

RTSP Server Enabled	<input checked="" type="checkbox"/>
RTSP Authorization	<input type="checkbox"/>
MJPEG Authorization	<input type="checkbox"/>
RTSP Authentication Type	Basic ▼
RTSP User Name	admin
RTSP Password	••••••••

MJPEG Video Parameters

Video Resolution	VGA ▼
Video Framerate	30 fps ▼
Video Quality	90 ▼

Parameter Set-up:

- **MJPEG Authorization:** tick it to access device video or real-time screenshots through a browser (http address such as: http://device IP:8080/video.cgi (dynamic video), http://device IP:8080/jpeg.cgi (static screenshot))

- **Video Resolution:** select video resolutions among seven options: "QCIF", "QVGA", "CIF", "VGA", "4CIF", "720P",. The default video resolution is "4CIF". and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than "4CIF".

- **Video Framerate:** "30fps" is the video frame rate by default.

- **Video Quality:** the video bitrate, from 50 to 90.

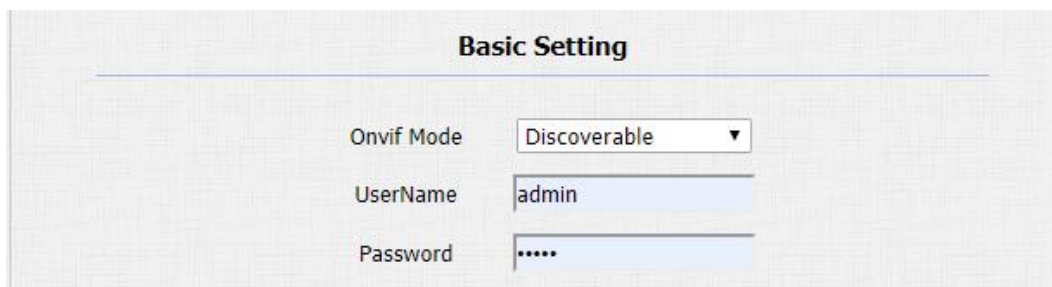


Note:

- For E12S, the operation path is **Surveillance > RTSP > MJPEG Video Parameters**

17.3.ONVIF

Real-time video from the door phone camera can be searched and obtained by the Akuvox indoor monitor or by the third party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function on the web **Intercom > ONVIF** interface so that other device will be able to see the video from the door phone.



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

Parameter Set-up:

- **Discoverable:** tick the check box to enable the Discoverable ONVIF mode. If you select "**Discoverable**" then the video from the door phone camera can be searched by other devices.
- **User Name:** enter the user name. The user name is "**admin**" by default.
- **Password:** enter the password. The password is "**admin**" by default.

After the setting is complete, you can enter the ONVIF URL on the third party device to view the video stream.

For example: **http://IP address:80/onvif/device_service**



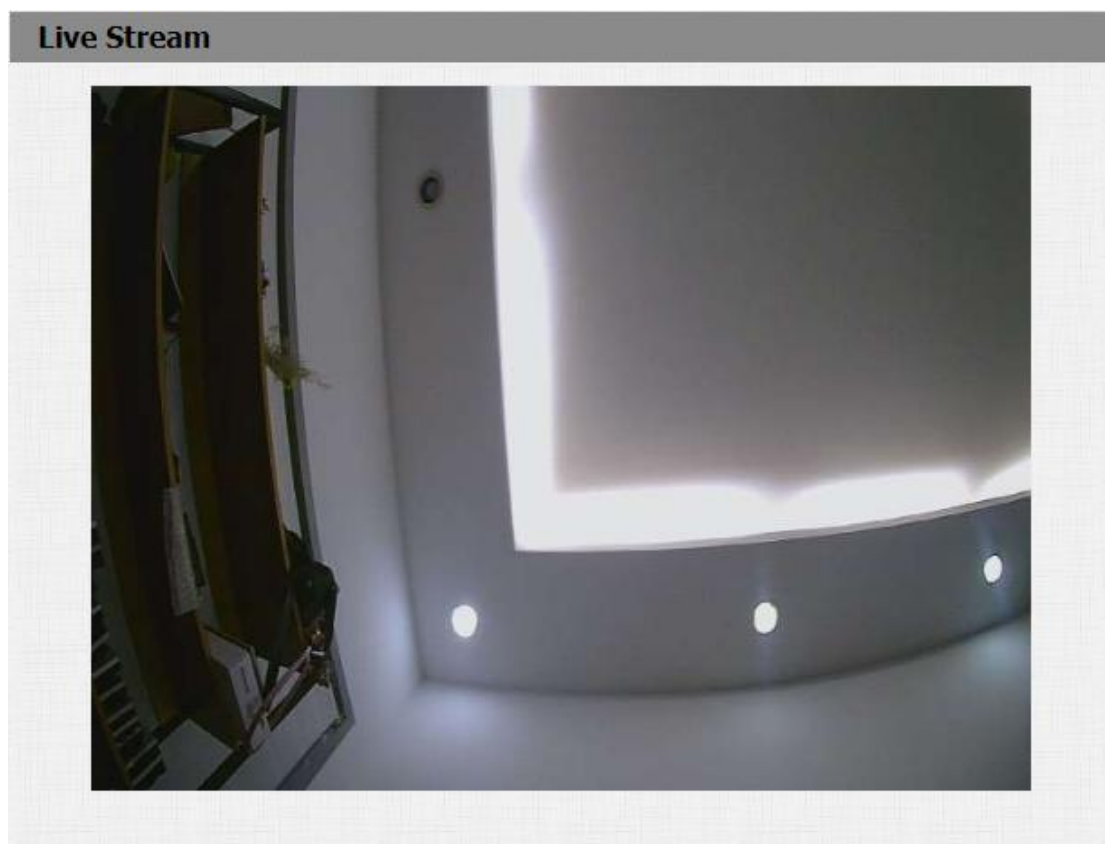
Note:

- Fill in the specific IP address of the door phone in the URL.

17.4.Live Stream

If you want to check the real-time video from the door phone, you can go to the the device web **Intercom > Live Stream** interface to obtain the real-time video or you can also enter the correct URL on the we browser to obtain it directly.

To check the real time video using URL, you can Enter the correct URL (http://IP_address:8080/video.cgi) on the web browser if you want to obtain the real-time video directly instead of going to the web interface.

**Note:**

- For E12S, the operation path is **Surveillance > Live Stream**

18. Logs

18.1.Call Logs

If you want to check on the calls inclusive of the dial-out calls , received calls and missed calls in a certain period of time, you can check and search the call log on the device web **Phone > Call Log** interface.

Call History						
			All	▼	Hang Up	
Index	Type	Date	Time	Local Identity	Name	Number
1	Dialed	2021-02-04	09:30:33	192.168.31.2 @192.168.31.2	Unknown	192.168.35.1 12@192.168.35.112
2	Received	2021-02-04	09:29:57	192.168.31.2 @192.168.31.2	192.168.35.112	192.168.35.1 12@192.168.35.112
3	Dialed	2021-02-04	09:29:06	192.168.31.2 @192.168.31.2	Unknown	192.168.35.1 12@192.168.35.112

Parameter Set-up:

- **Call History:** select call history among four options: "All", "Dialed" " Received" " Missed" for the specific type of call log to be displayed.
- **Hangup:** to hangup the call from web.
- **Index:** the order of the call logs.
- **Date:** the date for the call log.
- **Time:**the time for the call log.
- **Name/Number:** the name and number for the contact.



Note:

- Only R20 V2 version supports Hangup feature.
- For E12S, the operation path is **Intercom > Call Log**.

18.2. Door Logs

If you want to search and check and import/export on the various types of door access history, you can search and check the door logs on the device web **Phone > Door Log** interface.

Door Log

Door Log

Index	Name	Code	Type	Date	Time	Status	<input type="checkbox"/>
1							<input type="checkbox"/>
2							<input type="checkbox"/>
3							<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>
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

Import/Export Door Log(.xml)

选择文件

未选择任何文件

Import

Export

Parameter Set-up:

- **Index:** the order of the call logs.
- **Name:** If it is a locally added key or card, the corresponding added name will be displayed. If it is an unknown key or card, it will display Unknown.
- **Code:** If opening the door via PIN code, the corresponding PIN code will be displayed. If opening the door via RF cards, the corresponding card number will be displayed, and if the door is opened by HTTP command, it will be empty.
- **Type:** If opening the door via PIN code, **Password** will be displayed. If opening the door via RF cards, **Card** will be displayed, and if the door is opened by HTTP command, **Http** will be displayed.
- **Date:** The date for opening the door.
- **Time:** the time for opening the door.
- **Status:** the door opening result **Success** or **Failed**.

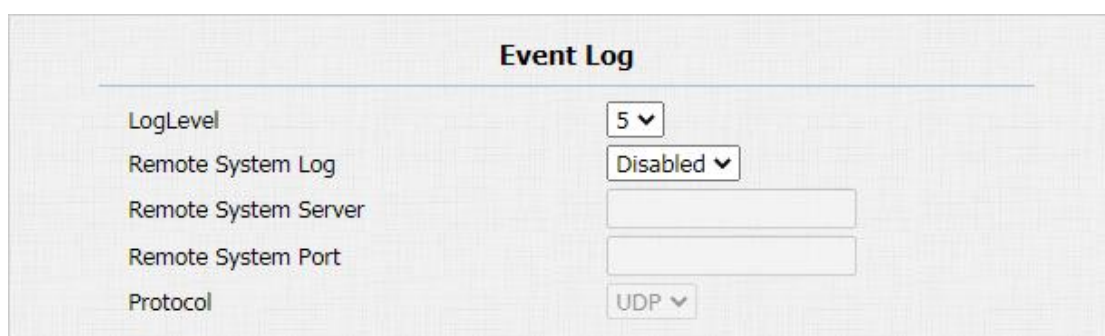
**Note:**

- Only R20 V2 version supports Import/Export feature.
- For E12S, the operation path is **Access Control > Door Log**.

19. Debug

19.1.Event Log

It is used to export device-specific logs (calling, card issue, door opening, download application configuration files for upgrading, network configuration, hacker incidents, etc.) to the remote server. To configure it on web **Upgrade > Advanced > Event Log** interface.



Event Log	
LogLevel	5 ▾
Remote System Log	Disabled ▾
Remote System Server	<input type="text"/>
Remote System Port	<input type="text"/>
Protocol	UDP ▾

Parameter Set-up:

- **LogLevel:** select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is "5". the higher the level is, the more complete the log is.
- **Remote System Log:** select "Enable" or "Disable" if you want to enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the the device **log**. And the remote server address will be provided by Akuvox technical support.
- **Remote System Port:** the port of remote server.
- **Protocol:** the transmission protocol defaults to UDP. After the remote log export function is enabled, the drop-down box can choose between UDP and TCP two transmission protocols.

**Note:**

- Only R20 V2 version supports Event Log feature.

19.2. System Log

System log in the door phone can be used for debugging purpose. If you want to export the system out to a local PC or to a remote server for debugging , you can set up the function on the web **Upgrade > Advanced > System Log** interface.

System Log	
LogLevel	3 ▾
Export Log	Export
Remote System Log	Disabled ▾
Remote System Server	<input type="text"/>
Remote System Port	<input type="text"/>

Parameter Set-up:

- **LogLevel:** select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is "3". the higher the level is, the more complete the log is.
- **Export Log:** click the **Export** tab to export temporary debug log file to a local PC.
- **Export Debug Log:** click the **Export** tab to export debug log file to a local PC.
- **Remote System Log:** select "Enable" or "Disable" if you wan to enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the

the device **log**. And the remote server address will be provided by Akuvox technical support.

**Note:**

- For E12S, the operation path is **Upgrade > Diagnose > System Log**.

19.3.PCAP

PCAP in Akuvox door phone is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **Upgrade > Advanced > PCAP** interface properly before using it.

PCAP

Specific Port (1-65535)

PCAP

PCAP Auto Refresh Enabled

Parameter set-up:

- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** click **Start** tab and **Stop** tab to capture the a certain range of data packets before clicking **Export** tab to export the data packets to you Local PC.
- **PCAP Auto Refresh:** select "**Enable**" or "**Disable**" to turn on or turn off the PCAP auto fresh function. If you set it as " Enable" then the PCAP will continue to capture data packet even after the data packets reached its

1M maximum in capacity. If you set it as “ **Disable**” the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

**Note:**

- For E12S, the operation path is **Upgrade > Diagnose > PCAP**.

20. Firmware Upgrade

Firmwares of different versions for Akuvox door phone can be upgraded on the device web **Upgrade > Basic** interface.

Firmware Version	20.0.1.222
Hardware Version	20.0.0.0.0.0.0.0
Upgrade	<input type="button" value="Choose File"/> No File Chosen
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Parameter Set-up:

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

21. Backup

Configuration files can be imported to or exported out of the device to your local PC on the device web **Upgrade > Advanced > Others** interface if needed.



The screenshot shows a web interface titled "Others". It features a text input field containing "Config File(.tgz/.conf/.cfg)". To the right of this field are four buttons: "Choose File" (with "No file chosen" text to its right), "Export (Encrypted)", "Import", and "Cancel".

Parameter Set-up:

- **Export Config File:** to export current config file.
- **Export/Import:** to export current config file (Encrypted) or import new config file.



Note:

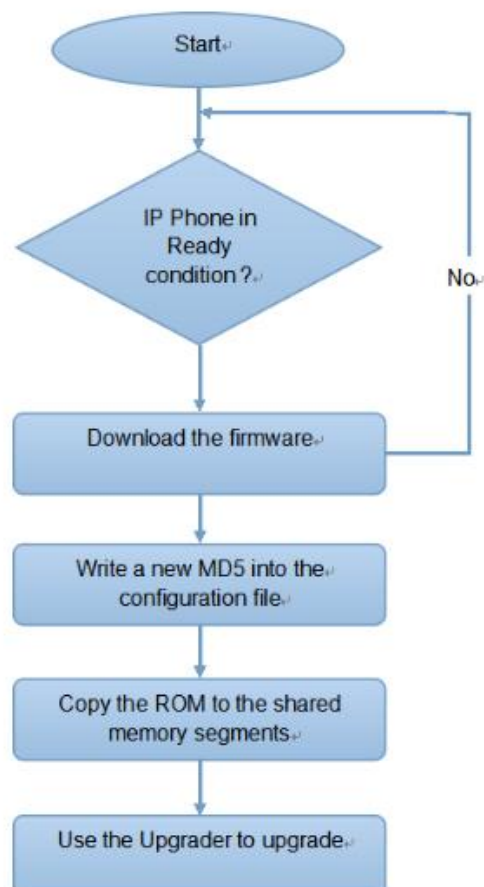
- For E12S, the operation path is **Upgrade > Diagnose > Others**.

22. Auto-provisioning via Configuration File

Configurations and upgrading on Akuvox door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the door phone.

22.1. Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade the devices in batch via third party servers. **DHCP, PNP, TFTP, FTP, HTTPS** are the protocols used by the Akuvox intercom devices to access the URL of the address of the third party server which stores configuration files and firmwares, which will then be used to to update the firmware and the corresponding parameters on the door phone.



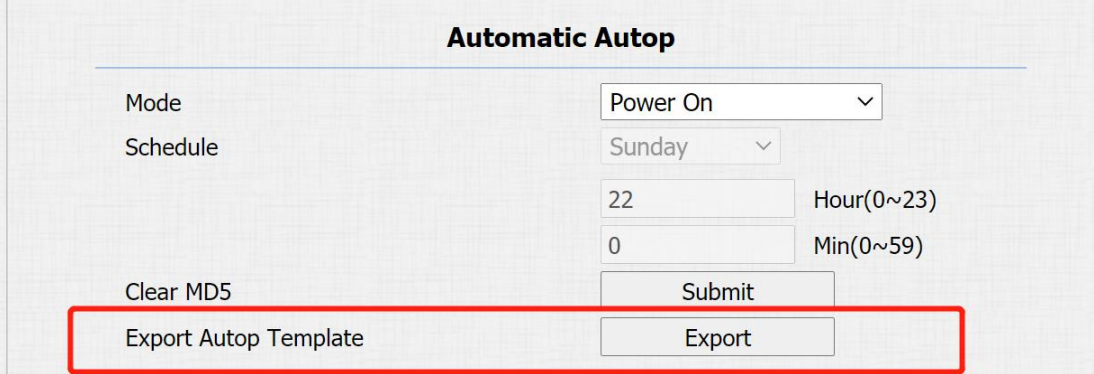
22.2. Configuration Files for Auto-provisioning

Configuration files have two formats for the auto-provisioning. one is the general configuration files used for the general provisioning and other one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown as below:

- **General configuration provisioning:** a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example : r000000000020.cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files is used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.

To get the Autop configuration file template on **Upgrade > Advanced > Automatic Autop** interface.



Automatic Autop

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



Note:

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

22.3.AutoP Schedule

Akuvox provides you with different Autop methods that enable the door phone to perform provisioning for itself in a specific time according to your schedule.

Automatic Autop

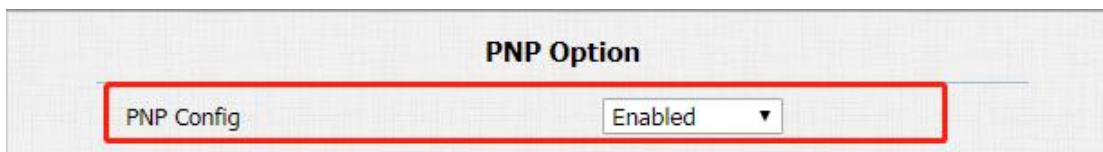
Mode	Power On ▼				
Schedule	Sunday ▼				
	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; border-bottom: 1px solid #ccc; padding: 2px;">22</td> <td style="width: 40%; padding: 2px;">Hour(0~23)</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; padding: 2px;">0</td> <td style="padding: 2px;">Min(0~59)</td> </tr> </table>	22	Hour(0~23)	0	Min(0~59)
22	Hour(0~23)				
0	Min(0~59)				

Parameter Set-up:

- **Mode:** select **"Power on"**, **" Repeatedly"**, **"Power On + Repeatedly"**, **"Hourly Repeat"** as your Autop schedule.
 Select **"Power on"**, if you want the device to perform Autop every time it boots up.
 Select **" Repeatedly"**, if you want the device to perform Autop according to the schedule you set up.
 Select **"Power On + Repeatedly"**, if you want to combine **Power On** Mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
 Select **"Hourly Repeat"**, if you want the device to perform Autop every hour.

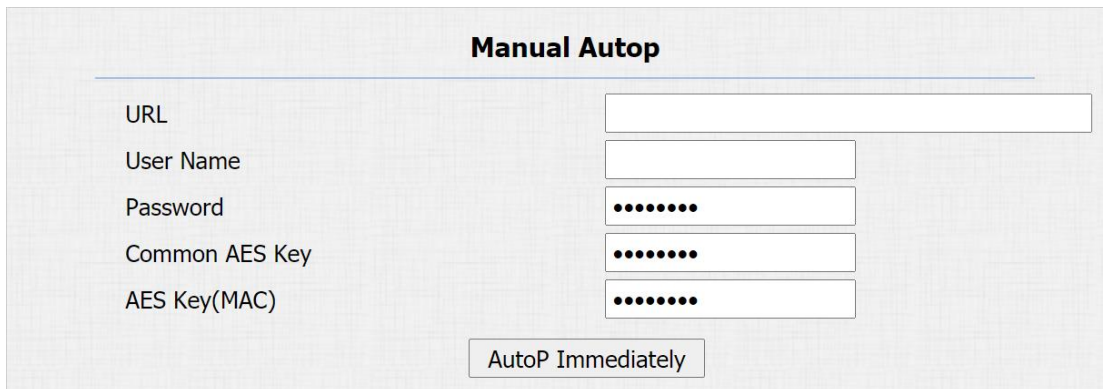
22.4.PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. To do this configuration on web **Upgrade > Advanced > PNP Option** interface.



22.5.Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the door phone will perform the auto provisioning on a specific timing according to Autop schedule you set up. In addition,TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.



Parameter set-up:

- **URL:** set up tftp, http, https, ftp server address for the provisioning
- **User Name:** set up a user name if the server needs an user name to be accessed to otherwise leave it blank.
- **Password:** set up a password if the server needs a password to be accessed to otherwise leave it blank.

- **Common AES Key:** set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key (MAC):** set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

 **Note:**

- AES is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

 **Note:****Server Address format:**

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
- ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/ (use the default port 80)
- http://192.168.0.19:8080/ (use other ports, such as 8080)
- HTTPS: https://192.168.0.19/ (use the default port 443)

 **Tip:**

- Akuvox do not provide user specified server.
- Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

23. Integration with Third Party Device

23.1. Integration via Wiegand

If you want to integrate Akuvox door phone with the third party devices via Wiegand, you can configure the Wiegand on the web interface.



The screenshot shows a web interface titled "Wiegand" with two configuration fields:

Wiegand	
WiegandType	wiegand-26 ▼
Wiegand Mode	Input ▼

Parameter set-up:

- **Wiegand Type:** set the wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Mode::** set the Transfer mode between **Input** or **Output** if the door phone is used as a receiver then set it as " Input" for the door phone and vice versa.

23.2. Integration via HTTP API

HTTP API is designed to achieve an network-based integration between the third party device with the Akuvox intercom device. You can configure the HTTP API function on the web **Intercom > HTTP API** interface for the integration.

Parameter Set-up:

- **HTTP API:** select “**Enable**” or “**Disable**” to enable or disable the HTTP API function for the third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode:** select among four options: “**None**” “**WhiteList**” “**Basic**”, “**Digest**” for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when “**Basic**” and “**Digest**” authorization mode is selected. The default user name is “Admin”.
- **Password:** enter the password when “**Basic**” and “**Digest**” authorization

mode is selected. The default user name is "Admin".

- **IP01-IP05:** enter the IP address of the third party devices when the "WhiteList" authorization is select for the integration.

Please refer to the following description for the Authentication mode

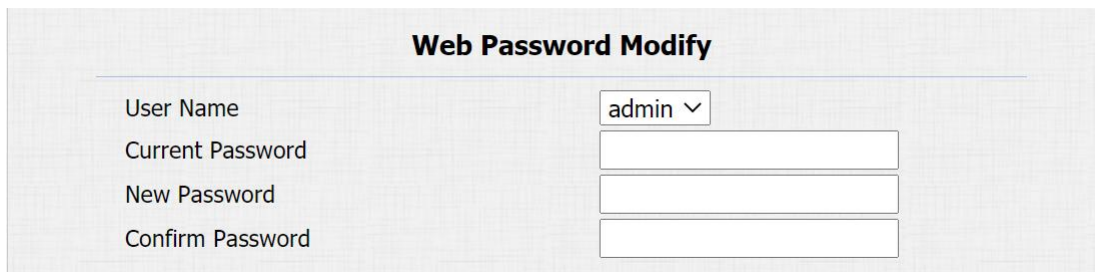
NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developer only.
3	WhiteList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In Authorization field of Http request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".

6	Token	This mode is used by Akuvox developer only.
---	-------	---

24. Password Modification

24.1. Modifying Device Web Interface Password

To change the default web password on web **Security > Basic** interface. Select "**admin**" for the administrator account and "**User**" for the User Account. Click the **Change Password** tab to change the password.

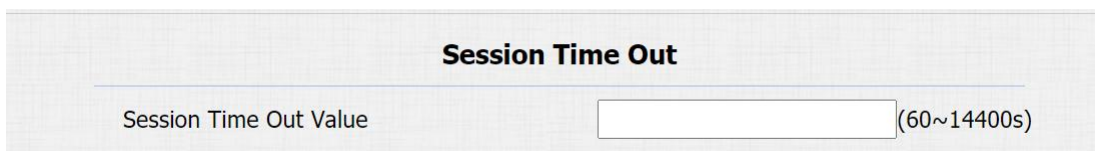


Web Password Modify

User Name	admin ▾
Current Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

24.2. Configure Web Interface Automatic Logout

It is a protection design. When there is no operation on the website and when the Session Time Out Value time is reached, the website will automatically log out.



Session Time Out

Session Time Out Value	<input type="text"/>	(60~14400s)
------------------------	----------------------	-------------

Parameters Set-up:

- **Session Time Out Value:** The range from 60 to 14400 sec. If there is no operation over the time, you need to log in the website again.

25. System Reboot&Reset

25.1.Reboot

If you want to restart the device system, you can operate it on the device **Upgrade > Basic** web interface as well.

Reboot	<input type="button" value="Submit"/>
--------	---------------------------------------

25.2.Reset

If you want to reset the device system to the factory setting, you can it on the web **Upgrade > Basic** interface.

Reset To Factory Setting	<input type="button" value="Submit"/>
--------------------------	---------------------------------------

26. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

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

27. 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.

