



E21

DOOR PHONE

Administrator Guide

About This Manual

Thank you for choosing Akuvox E21 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to:

Firmware Version	Hardware Version
221.30.1.106	V2.0
321.30.1.101	V4.0

Please visit [Akuvox forum](#) or consult technical support for any new information or latest firmware.

Introduction of Icons and Symbols



Note:

- Informative information and advice from the 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>

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	8
6.1. Language Setting	8
6.2. Time Setting	8
7. LED Setting	10
7.1. Infrared LED Setting	10
8. Volume and Tone Configuration	12
8.1. Volume Configuration	12
8.2. Open Door Warning	12
8.3. Upload Tone Files	13
9. Network Setting	14
9.1. Network Status	14
9.2. Device Network Configuration	14
9.3. Device Local RTP configuration	15
9.4. SNMP Setting	16
9.5. VLAN Setting	16
9.6. TR069 Setting	17
9.7. Device Web HTTP Setting	19
9.8. Device Deployment in Network	19
9.9. NAT Setting	20
10. Intercom Call Configuration	22
10.1. IP call & IP Call Configuration	22
10.2. SIP Call & SIP Call Configuration	22
10.2.1. SIP Port	23
10.2.2. Prevent SIP Hacking	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	26
10.7. Configure NAT	27
10.8. Configure Calling Feature	27
10.8.1. DND	27
10.8.2. Manager Dial Call	28
10.8.3. Call Hang-up	28
10.8.4. Web Call	29

10.8.5. Auto Answer	29
10.8.6. Multicast	30
10.8.7. Configure Maximum Call Duration	32
10.8.8. Maximum Dial Duration	32
11. Audio& Video Codec Configuration for SIP Calls	34
11.1. Audio Codec Configuration	34
11.2. Video Codec Configuration	35
11.3. Video Codec Configuration for IP Direct Calls	36
11.4. Configure DTMF Data Transmission	37
12. Relay Setting	38
12.1. Relay Switch Setting	38
12.2. Web Relay Setting	39
13. Door Access Schedule Management	42
13.1. Relay schedule	42
13.2. Configure Door Access Schedule	43
13.2.1. Create Door Access Schedule	43
14. Door Unlock Configuration	45
14.1. Configure Open Relay via HTTP for Door Unlock	45
14.2. Configure Open Relay via DTMF	46
14.3. Configure Exit Button for Door Unlock	46
15. Security	48
15.1. Client Certificate Setting	48
15.1.1. Web Server Certificate	48
15.2. Motion Detection	48
15.2.1. Configure Motion Detection	49
15.3. Action URL	50
15.4. Security Notification Setting	51
15.4.1. Email Notification Setting	51
15.4.2. FTP Notification Setting	52
15.4.3. SIP Call Notification Setting	53
15.4.4. HTTP URL Notification Configuration	54
15.5. Security Action Configuration	54
15.5.1. Configure Push Button Action	54
15.5.2. Configure Motion Action	55
15.5.3. Configure Input Action	55
15.6. Voice Encryption	55
15.7. User Agent	56
16. Monitor and Image	57
16.1. RTSP Stream Monitoring	57
16.1.1. RTSP Basic Setting	57
16.1.2. RTSP Stream Setting	58
16.2. MJPEG Image Capturing	60
16.3. ONVIF	61
16.4. Live Stream	62

17. Logs	63
17.1. Call Logs	63
18. Debug	64
18.1. System Log	64
18.2. PCAP	65
18.3. Remote Debug	65
19. Firmware Upgrade	67
20. Backup	68
21. Auto-provisioning via Configuration File	69
21.1. Provisioning Principle	69
21.2. Configuration Files for Auto-provisioning	70
21.3. AutoP Schedule	71
21.4. PNP Configuration	71
21.5. Static Provisioning Configuration	72
22. Integration with Third Party Device	74
22.1. Integration via HTTP API	74
22.2. Integration with Milestone	76
23. Password Modification	77
23.1. Modifying Device Web Interface Password	77
24. System Reboot&Reset	78
24.1. Reboot	78
24.1.1. Reboot Schedule	78
24.2. Reset	78
25. Abbreviations	79
26. FAQ	81
27. Contact us	84



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 E21 series is SIP-compliant door phones. They 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	E21V	E21A
		
Button	1 Physical button	1 Physical button
Housing Material	Aluminum	Aluminum
Camera	2 Mega pixels, automatic lighting	X
Relay In	2	2
Relay Out	2	2
RS485	X	X
PoE	√	√
WiFi	X	X
RAM	128MB	128MB
ROM	128MB	128MB
Card Reader	X	X
IP Rating	IP65	IP65
IK Rating	X	IK10
Wall Mounting	X	X
Flush Mounting	√	√

4. Introduction to Configuration Menu

- **Status:** this section 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 a 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 a 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 the cloud. If users decide to use Akuvox cloud, please contact Akuvox technical support, and they will help you configure the related settings before using them.
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 managers 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 in 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

E21 series system setting can be accessed on the device web interface.

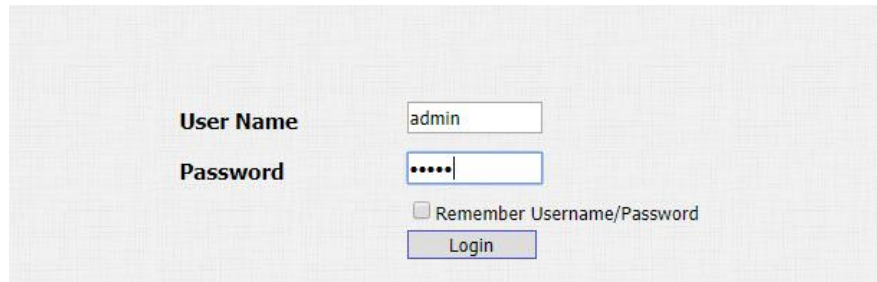
5.1. Obtain Device IP Address

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 the IP scanner to check the device IP.

IP Scanner					
Online Device : 7					
<input type="text"/>			Search	Refresh	
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 to device web interface where you can configure and adjust parameters 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

**Note:**

- You can also obtain the device IP address using the Akuvox IP scanner to log in to the device web interface. Please refer to the URL below for the IP scanner application:
<https://knowledge.akuvox.com/docs/how-to-obtain-ip-address-via-ip-scanner-1?highlight=IP%20SCANNER>
- 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 **Device > Time/Lang > Web Language** interface according to your preference.



The screenshot shows a web interface for 'Time/Lang' settings. Under the 'Web Language' section, there is a 'Type' label and a dropdown menu currently displaying 'English'.

Parameter Set-up:

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

6.2. Time Setting

The set-up on 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. You can navigate to **Device > Time/Lang > NTP**.

NTP	
Time Zone	GMT+0:00 GMT ▼
Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org
Update Interval	3600 (>= 3600s)
System Time	03:25:12

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**.
- **Preferred/Alternate Server:** enter the NTP server address. The alternate server will take effect when the primary server is invalid.
- **Update Interval:** to configure the interval between two consecutive NTP requests.
- **System Time:** indicate the current device time.

7. LED Setting

7.1. Infrared LED Setting

Infrared LED is applied in a dark environment in which a resident might not be able to see a visitor clearly via the video from the door phone. You can navigate to **Intercom > LED Setting > LED Setting**.

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

Parameter Set-up:

- **State:** there are five states: **Normal**, **Offline**, **Calling**, **Talking**, and **Receiving**.
- **Color Off:** you can turn off LED light.
- **Color On:** set color of LED light, it can support four colors: **Red**, **Green**, **Blue**, **Yellow**.

- **Blink Mode:** select **Always ON** to enable the Infrared LED light to stay on permanently. Select **Always OFF** to turn off the Infrared LED light. Or, you can set up the different blink frequencies.

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 **Device > Voice** interface.

Mic Volume	
Mic Volume	<input type="text" value="8"/> (1~15)

Speaker Volume	
Speaker Volume	<input type="text" value="8"/> (1~15)

Parameters Set-up:

- **Mic Volume:** adjust the mic volume as needed.
- **Speaker Volume:** adjust the speaker volume as needed.

8.2. Open Door Warning

You can enable or disable the Open Door Warning on the web **Device > Voice** interface.

Open Door Warning	
Open Door Succ Warning	<input type="text" value="Enabled"/> ▾
Open Door Failed Warning	<input type="text" value="Enabled"/> ▾

Parameters Set-up:

- **Open Door Succ Warning:** to enable or disable the open door success prompt.
- **Open Door Failed Warning:** to enable or disable the open door failure prompt.

8.3. Upload Tone Files

You can customize the ringback tone, open door success tone, and open door failure tone if you need. Please follow the prompt about the file size and format. Navigate to **Device > Voice** interface.

RingBack Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 16000,
Bits: 16

Opendoor Succ Tone Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 16000,
Bits: 16

Opendoor Failed Tone Upload

No file chosen

File Format: wav, size: < 200KB, samplerate: 16000,
Bits: 16

Parameter Set-up:

- **RingBack:** the tone that will go off when you call to others.
- **OpenDoor Succ Tone:** the tone that will go off when you opened door successfully.
- **Open Door Succeeded Inside Warning:** the tone that will go off when you failed to open door.

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	192.168.2.23
LAN Subnet Mask	255.255.255.0
LAN Gateway	192.168.2.1
LAN DNS1	192.168.2.1
LAN DNS2	

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.

Network-Basic

LAN Port

☒ DHCP
 ☐ Static IP

IP Address

Subnet Mask

Default Gateway

LAN DNS1

LAN DNS2

192.168.1.100

255.255.255.0

192.168.1.1

8.8.8.8

Submit

Cancel

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/ LAN DNS2:** 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 connect to the alternate server when the primary DNS server is unavailable.

9.3. Device Local RTP configuration

For the device network data transmission purpose, the device needs to be set up with a range of RTP ports (**Real-time Transport Protocol**) for establishing an exclusive range of data transmission in the network. Path: **Network > Advanced > Local RTP** interface.

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:

- **Min 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.

9.4. SNMP Setting

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. SNMP is widely used in the network management system to monitor network-attached devices for conditions that may draw network administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried by managing applications. These variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs). To do the configuration on the web **Network > Advanced > SNMP** interface.

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

Parameter Set-up:

- **Active:** to enable or disable SNMP feature.
- **Port:** to configure SNMP server's port.
- **Trusted IP:** to configure allowed SNMP server address. It could be an IP address or any valid URL domain name.

9.5. VLAN Setting

Virtual Local Area Network is a logical grouping of two or more nodes which

are not necessarily on the same physical network segment but which share the same logical IP domain. To be specific, the purpose of VLAN is to separate layer 2 broadcast domain. Within trunk links, the tagged packet will only be sent to those ports with the same VLAN ID. This is usually achieved by switch or router. User can benefit from deployed VLAN, such as: *Security: if without VLAN, all host will be included in unique broadcast domain. Therefore, the consequence of ARP attack will affect all end devices in the organization. *Performance: The nature of network broadcast is to flood frames among the network. In certain conditions, it is unnecessary to receive broadcast frame. To save bandwidth for high efficiency, it will be better to separate the broadcast domain by deploying VLAN. To do the configuration on the web **Network > Advanced > VLAN** interface.

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

Parameter Set-up:

- **Active:** to enable or disable VLAN feature for designated port.
- **VID:** to configure VLAN ID for designated port.
- **Priority:** to select VLAN priority for designated port.

9.6. TR069 Setting

TR-069 (Technical Report 069) is the document number of the technical report, defined by the Broadband Forum, that specifies the "CPE WAN management protocol" or CWMP. It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. To do the configuration on the web **Network > Advanced > TR069** interface.

TR069		
ACS	Active	Disabled ▾
	Version	1.0 ▾
	URL	<input type="text"/>
	User Name	<input type="text"/>
Periodic Inform	Password	*****
	Active	Disabled ▾
CPE	Periodic Interval	1800 (3~24×3600s)
	URL	<input type="text"/>
	User Name	<input type="text"/>
	Password	*****

Parameter Set-up:

- **Active:** to enable or disable TR069 feature.
- **Version:** to select supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE:** ACS is short for auto configuration servers as server side, and CPE is short for customer-premise equipment as client side devices.
- **URL:** to configure URL address for ACS or CPE.
- **User Name:** to configure username for ACS or CPE.
- **Password:** to configure password for ACS or CPE.
- **Periodic Inform:** to enable periodically inform.
- **Periodic Interval:** to configure interval for periodic inform.



Note:

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

9.7. Device Web HTTP Setting

This function is used to manage whether the device website is allowed to be accessed. The door phone supports two types of remote access methods HTTP and HTTPS(encryption). To do this configuration on the web **Network > Advanced > Web Server** interface.

Web Server	
Http Enable	Enabled <input type="button" value="v"/>
Https Enable	Enabled <input type="button" value="v"/>
Http Port	80 (80,1024~65534)

Parameters Set-up:

- **HTTP Enabled:** set whether HTTP access to the device web page is allowed, Enabled is allowed, Disabled is not allowed, the default is Enabled.
- **HTTPS Enabled:** set whether HTTPS access to the device web page is allowed, Enabled is allowed, Disabled is not allowed, the default is Enabled.
- **HTTP Port:** set up the port for HTTP access method. 80 is the default port.

9.8. 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	SDMC ▼
Discovery Mode	Enabled ▼
Device Address	1 . 1 . 1 . 1 . 1
Device Extension	1
Device Location	Stair Phone

Parameter Set-up:

- **Server Mode:** 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.

9.9. 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	Disabled ▾
UDP Alive Msg Interval	30 (5~60s)
RPort	Disabled ▾

Parameter Set-up:

- **UDP Keep Alive Messages:** if enabled, the device will send out the message to the SIP server so that the 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. Path: **Device > Call Feature > Others**

Others	
Return Code When Refuse	486(Busy Here) ▾
Auto Answer Delay	0 (0~5s)
Auto Answer Mode	Audio ▾
Direct IP	Enabled ▾
Direct IP AutoAnswer	Enabled ▾
Direct IP Port	5060 (1~65535)

Parameters Set-up:

- **Enabled:** choose **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.
- **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.

10.2.1. SIP Port

You can set up the port for SIP call from 1024 to 65535. The default is 5062.

Path: Account > Advanced > Call.

Call	
Max Local SIP Port	5062 (1024~65535)
Min Local SIP Port	5062 (1024~65535)

10.2.2. Prevent SIP Hacking

This function can help you to avoid hack. The device can only receive call from the numbers added to push button list if you enable Prevent SIP Hacking Function.

Call	
Max Local SIP Port	5062 (1024~65535)
Min Local SIP Port	5062 (1024~65535)
Auto Answer	Enabled
Prevent SIP Hacking	Disabled

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 accounts 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	<input type="password"/>

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account:** select the exact account (Account 1&2) to be configured.
- **Account Active:** click **Enable** or **Disable** to activate or deactivate the registered SIP account.
- **Display Label:** configure the device label to be shown on the device screen.
- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **User Name:** enter the user name obtained from 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 servers between intercom devices. To do this configuration also on web

Account > Basic > SIP Server interface.

SIP Server 1		
Server IP	<input type="text"/>	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:

- **SIP Server 1:** enter the primary server IP address number or its URL.
- **SIP Server 2:** 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 span. 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.

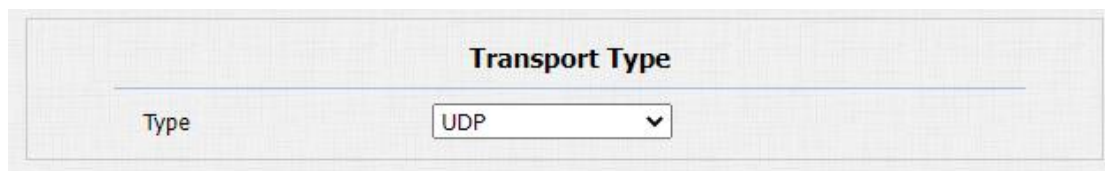
Outbound Proxy Server		
Enable Outbound	<input type="text" value="Disabled"/>	
Server IP	<input type="text"/>	Port <input type="text" value="5060"/>
Backup Server IP	<input type="text"/>	Port <input type="text" value="5060"/>

Parameter Set-up:

- **Enable Outbound:** choose **Enable** and **Disable** to turn on or turn off the outbound proxy server.
- **Server IP:** enter the SIP address of the primary outbound proxy server.
- **Backup 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.



Transport Type	
Type	UDP ▼

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 NAT

NAT (Net Address Translator) function allows a devices that deployed in local network connect to Internet that in different LAN. Path: **Account > Basic > NAT**.

NAT	
NAT	STUN
Stun Server Address	Port 3478

Parameter Set-up:

- **NAT:** choose **STUN** (Short for Simple Traversal of UDP over NATS) to enable the function, you need to install NAT sever. The default is **Disable**.
- **Stun Server Address:** enter the STUN server IP, and the default port is **3478**.

10.8. Configure Calling Feature

10.8.1. 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 **Device > 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.

DND	
Account	All Account
DND	Disabled
Return Code When DND	486(Busy Here)
DND On Code	
DND Off Code	

Parameter Set-up:

- **Account:** choose one account or set all accounts, which do not receive SIP calls.
- **DND:** enable or disable the DND function. DND function is disabled by default.
- **Return Code When DND:** select code to be sent to the caller side via SIP server when you rejected the incoming call.
- **DND On Code:** the Code is used to turn on DND on server's side, if configured, IP phone will send a SIP message to server to turn on DND on server side if you press DND when DND is off.
- **DND Off Code:** the Code is used to turn off DND on server's side, if configured, IP phone will send a SIP message to server to turn off DND on server side if you press DND when DND is on.

10.8.2. Manager Dial Call

Manager Dial is used to quickly initiate the pre-configured numbers by pressing the push button on door phone. You can create up 8 numbers. To do the configuration on the web **Intercom > Basic > Push Button** interface.

Push Button				
Key	Number1/5	Number2/6	Number3/7	Number4/8
Manager Dial	192.168.2.21	192.168.2.11		

10.8.3. Call Hang-up

You can hang up the call on the door phone by pressing the push button if needed. To enable the push-button call hang-up, navigate to **Intercom > Basic**.

Push To Hang Up

Push To Hang Up Enabled ▾

10.8.4. 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. You can navigate to **Intercom > Basic > Web Call**.

Web Call

Web Call(Ready)

Auto ▾
Dial Out
Hang Up

Parameters Set-up:

- **Web Call (Ready):** enter the IP/SIP number to dial out.

10.8.5. Auto Answer

You can define how quickly the door phone should respond 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 > Call** interface, you can set up the related parameters on web **Device > Call Feature > Others**.

Call

Max Local SIP Port	<input style="width: 150px;" type="text" value="5062"/>	(1024~65535)
Min Local SIP Port	<input style="width: 150px;" type="text" value="5062"/>	(1024~65535)
Auto Answer	Enabled ▾	
Prevent SIP Hacking	Disabled ▾	

Others	
Return Code When Refuse	486(Busy Here) ▾
Auto Answer Delay	0 (0~5s)
Auto Answer Mode	Audio ▾
Direct IP	Enabled ▾
Direct IP AutoAnswer	Enabled ▾
Direct IP Port	5060 (1~65535)

Parameters Set-up:

- **Auto Answer Mode/Direct IP Auto Answer:** turn on the Auto Answer function by choosing **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:** the default is auto answer with voice call.

10.8.6. 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. Path: **Device > Multicast**.

Multicast

Multicast Setting

Multicast Priority Paging Barge

1 ▼

Paging Priority Enabled

☒

Priority List

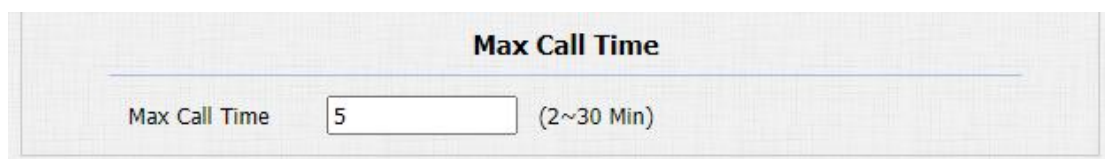
IP Address	Listening Address	Label	Priority
1st IP Address	224.1.6.21:51230	AKUVOX	1
2nd IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	2
3rd IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	3
4th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	4
5th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	5
6th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	6
7th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	7
8th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	8
9th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	9
10th IP Address	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	10

Parameters Set-up:

- **Multicast Priority 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 enabled:** 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 needs to be the same as the listened part and the multicast port can not be the 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.

10.8.7. 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. You can navigate **Intercom > Basic > Max Call Time**.



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 the 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.

10.8.8. Maximum Dial Duration

Maximum Dial duration consist 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 hangs up the call if the call is not answered by the door phone. On the contrary, Maximum dial out time refers to the maximum time duration before the door phone hangs up itself automatically when the call from the door phone is not answered by the intercom device being called. You can navigate to **Intercom > Basic > Max Dial Time**.

Max Dial Time		
Dial In Time	<input type="text" value="60"/>	(5~120 Sec)
Dial Out Time	<input type="text" value="60"/>	(5~120 Sec)

Parameters Set-up:

- **Dial in Time:** enter the dial in time duration for your door phone (ranging from 30-120 sec.) for example, if you set the dial in time duration is 60 seconds 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 seconds 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 seconds in your door phone, then the door phone will hang up the call it dialed out automatically if the call is not answered 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 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.

The screenshot displays the 'SIP Account' configuration page. At the top, there is a section for 'Account' with a dropdown menu currently set to 'Account 1'. Below this is the 'Codecs' section, which is divided into two columns: 'Disabled Codecs' and 'Enabled Codecs'. The 'Enabled Codecs' column contains a list of four codecs: PCMU, PCMA, G722, and G729. Between the two columns are two buttons: '>>' and '<<'. To the right of the 'Enabled Codecs' list are two buttons: an upward arrow and a downward arrow. The 'Disabled Codecs' column is currently empty.

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



Note:

- Since E21A does not have camera, it does not support some functions related to camera.

Akuvox door phone support H264 codec that provides a better video quality at a much lower bit rate. To set up video codec on web **Account > Advanced** interface.

Video Codec

Name	<input checked="" type="checkbox"/> H264
Resolution	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">4CIF ▼</div>
Bitrate	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">2048 ▼</div>
Payload	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">104 ▼</div>

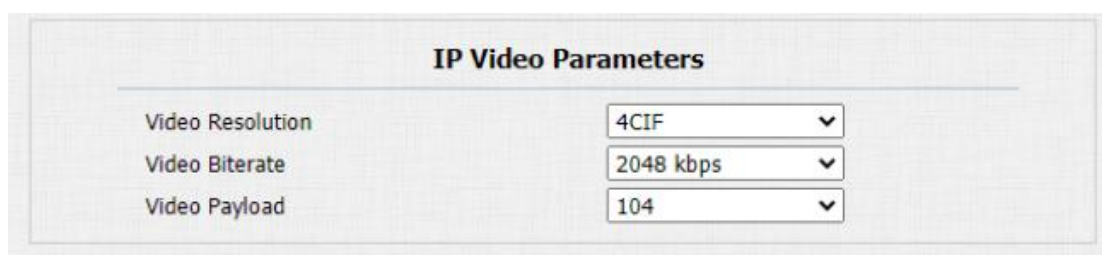
Parameter Set-up:

- **Name:** check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **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.

- **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.
- **Payload:** select the payload type (ranging from 90-118) to configure audio/video configuration file. The default payload is 104.

11.3.Video Codec Configuration for IP Direct Calls

You can select the IP call video quality by selecting the proper codec resolution according to your actual network condition. To do so , you can go to **Device > Call Feature > IP Video Parameters**.



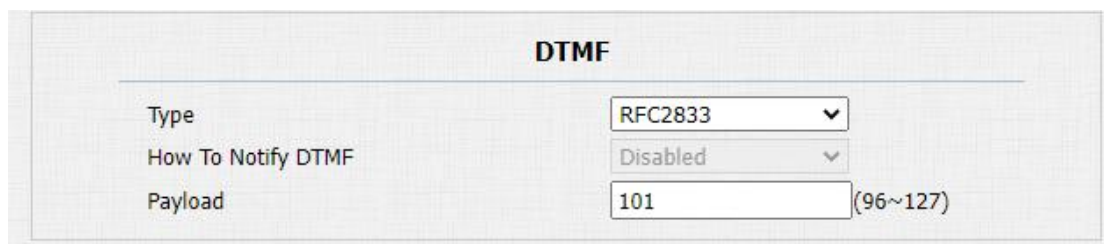
IP Video Parameters	
Video Resolution	4CIF
Video Biterate	2048 kbps
Video Payload	104

Parameter Set-up:

- **Video Resolution:** select the code resolution for the video quality among four options: **CIF, VGA, 4CIF, and 720P**. The default code resolution is 4CIF.
- **Video Bitrate:** select video bit-rate among six options: **64 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps** according to your network environment. The default video bit-rate is **2048 kbps**.
- **Video Payload:** select the payload type (ranging from 90-118) to configure audio/video configuration file. The default payload is **104**.

11.4. 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 devices for the third party integration.



DTMF	
Type	RFC2833
How To Notify DTMF	Disabled
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**, and **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.
- **Payload:** set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

12. Relay Setting

12.1. 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. It has a title bar 'Relay' and a sub-header 'Relay'. Below this, there are two columns of settings for 'RelayA' and 'RelayB'.

	RelayA	RelayB
Relay ID	RelayA	RelayB
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 ID:** you are allowed to set up three relay switches in total for the door access control.
- **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 be triggered until 5 seconds after you press **unlock** tab.
- **DTMF Option:** select the number of DTMF digits 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 ***,#**) if the DTMF Option is set as **1-digit**.
- **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 **DMTP**

Option 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 need 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.

12.2.Web Relay Setting

In addition 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 **Device > 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

Web Relay

Type
IP Address
User Name
Password

Disabled ▼

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<div style="border: 1px solid #ccc; height: 20px;"></div>	<div style="border: 1px solid #ccc; height: 20px;"></div>	<div style="border: 1px solid #ccc; height: 20px;"></div>
Action ID 02	<div style="border: 1px solid #ccc; height: 20px;"></div>	<div style="border: 1px solid #ccc; height: 20px;"></div>	<div style="border: 1px solid #ccc; height: 20px;"></div>
Action ID 03	<div style="border: 1px solid #ccc; height: 20px;"></div>	<div style="border: 1px solid #ccc; height: 20px;"></div>	<div style="border: 1px solid #ccc; height: 20px;"></div>

Parameter Set-up:

- **Type:** select among three options **Disabled**, **Web Relay**, and **Both**. Select **Web relay** 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 web 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 password 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 web relays. See the HTTP command example below:
 - a. If you do not fill in IP address in the IP Address Field above, fill in a complete HTTP command.
For example, Http://admin:admin@192.168.1.2/state.xml?relayState=2.
(HTTP://:@IP address>/state.xml?relayState=2)
 - b. If you have already filled in the IP address above, fill in the omitted HTTP command, eg. state.xml?relayState=2.

- **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.

13. 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.

13.1. Relay schedule

Set the corresponding relay always open at a specific time. This feature is designed for some specific scenarios, for example, the time after school, or for morning work time. To do the configuration, navigate to **Intercom Relay > Relay Schedule** interface.

The screenshot shows the 'Relay Schedule' configuration page. At the top, there's a title 'Relay Schedule'. Below it, there are two dropdown menus: 'Relay ID' set to 'RelayA' and 'Schedule Enable' set to 'Enabled'. Below these are two large empty boxes labeled 'All Schedules' and 'Enable Schedules'. Between these boxes are two buttons: '>>' and '<<'. Each box has a vertical scrollbar on its right side.

Parameter Set-up:

- **Relay ID:** choose on the relay you need to set up.
- **Schedule Enabled:** it is disabled by default. Only choose to enable it, that you can select the schedule. For creating the schedule, please refer to door access schedule configuration.

13.2. 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. Moreover, you can edit your door access schedule if needed.

13.2.1. Create 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 Normal

Schedule Name

Date Range 20220215 - 20220215

Day of Week

Mon ☐
Tue ☐
Wed ☐
Thur ☐

Fri ☐
Sat ☐
Sun ☐
Check All ☐

Date Time

HH : MM

-

HH : MM

Add
Reset

Schedules Management

All

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	
1	1002	Local	Daily	Never	-	-	-	<input type="checkbox"/>
2	1001	Local	Daily	Always	-	-	00:00:00-23:59:59	<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 Time:** set the corresponding date. This field will only be displayed when the Normal type is selected.

14. Door Unlock Configuration

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

14.1. 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 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 > Open Relay Via HTTP** interface.



Open Relay via HTTP

Switch	Disabled ▾
UserName	<input type="text"/>
Password	<input type="password" value="••••••••"/>

Parameter Set-up:

- **Switch:** enable or disable the HTTP command unlock function.
- **UserName:** 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/fcgi/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.

14.2. Configure Open Relay via DTMF

You can unlock door by DTMF, and set authorization for which numbers can open door by DTMF. **Path: Intercom > Relay > Open Relay Via DTMF**

Parameter Set-up:

- **Disabled:** disable open door by DTMF.
- **Whitelist number:** door can be opened via DTMF by the device added to push button list.
- **All number:** enable all devices can open door via DTMF.

14.3. 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	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Disabled ▼</div>
Trigger Option	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Low ▼</div>
Action to execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> Sip Call <input type="checkbox"/> HTTP <input type="checkbox"/>
Http URL:	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
Action Delay	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0</div> (0~300Sec)
Open Relay	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">None ▼</div>
Door Status	DoorA: Low

Parameter Set-up:

- **Input Service:** enable or disable the function.
- **Trigger Option:** select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action To execute:** select the method to carry out the action among four options: FTP, Email, HTTP, and Sip Call.
- **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 minutes after your press the button.
- **Open Relay:** set up relays to be triggered by the actions.
- **Door Status:** display the status of the input signal.

15. Security

15.1. Client Certificate Setting


Certificates can ensure communication integrity and privacy when deploying Akuvox door phone. So, when the user needs to establish SSL protocol, it is necessary to upload corresponding certificates for verification.

Web Server Certificate: it is the certificate that sends to clients for authentication when clients require an SSL connection with Akuvox door phone. Currently, the format of the certificate can be accepted by Akuvox door phone is *.PEM file.

Client Certificate: When Akuvox door phone Phone required an SSL connection with servers, the phone must verify the server to make sure it can be trusted. and the server will send its certificate to the Akuvox door phone. Then the door phone will verify this certificate according to client certificate list.

15.1.1. Web Server Certificate

To upload Web Server certificate on the device web interface **Security > Advanced > Web Server Certificate**.



Advanced

Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

Web Server Certificate Upload(.PEM/.DER/.CER)

Choose File No file chosen Submit Cancel

15.2. Motion Detection

Motion Detection is often used for unattended surveillance video and automatic alarms. 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.

15.2.1. Configure Motion Detection

You can turn on the motion detection and set up the motion detection interval on the device. Path: **Intercom > Motion > Motion Detection Options**.

Motion Detection

Motion Detection Options

Motion Detection: Disabled

Time: 10 (0~120 Sec)

Motion Detect Time Setting

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

Start Time - End Time: 00 : 00 - 23 : 59

Parameter Set-up:

- **Motion Detection:** select **Disable** to disable the motion detection. Select **Enable** to enable the IR sensor based motion detection for the suspicious moving objects.
- **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 seconds interval, then the alarm will be triggered at 7 seconds (the first trigger point) and motion detection action can be triggered (sending out notification) anywhere 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**.

- **Day:** set up the motion detection schedule.
- **Start Time- End Time:** set up the start time and end time on daily basis.

15.3. Action URL

E21 allows you to set up specific HTTP URL command that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occur any changes in the relay status, input status, PIN code, and RF card access for security purposes. Path: **Device > Action URL**.

For example :

`http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn`

Akuvox supports the following parameter format for the event below.

NO.	Event	Parameter	Example
-----	-------	-----------	---------

		format	
1	Make Call	\$remote	Http://server ip/Callnumber=\$remote
2	Hang Up	\$remote	Http://server ip/Callnumber=\$remote
3	Relay Triggered	\$relay1status	Http://server ip/relaytrigger=\$relay1status
4	Relay Closed	\$relay1status	Http://server ip/relayclose=\$relay1status
5	Input Triggered	\$input1status	Http://server ip/inputtrigger=\$input1status
6	Input Closed	\$input1status	Http://server ip/inputclose=\$input1status
7	Valid Code Entered	\$code	Http://server ip/validcode=\$code
8	Invalid Code Entered	\$code	Http://server ip/invalidcode=\$code
9	Valid Card Entered	\$card_sn	Http://server ip/validcard=\$card_sn
10	Invalid Car Entered	\$card_sn	Http://server ip/invalidcard=\$card_sn
11	Tamper Alarm Triggered	\$alarm status	Http://server ip/tampertrigger=\$alarm status

15.4.Security Notification Setting

15.4.1. 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.

Action	
Email Notification	
Sender's Email Address	<input type="text"/>
Receiver's Email Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
Email Test	<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 as the sender's email address.
- **SMTP Password:** configure the password of SMTP service, which is the same as the sender's email address.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the contents of emails according to your need.
- **Email Test:** click **Email Test** to test if you can receive the Email.

15.4.2. FTP Notification Setting

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

FTP Notification	
FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password"/>
FTP Test	<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.
- **FTP Test:** run the test to see if FTP notification can be sent and received by the FTP server.

15.4.3. 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.

15.4.4. HTTP URL Notification Configuration

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

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**.

15.5. Security Action Configuration

15.5.1. Configure Push Button Action

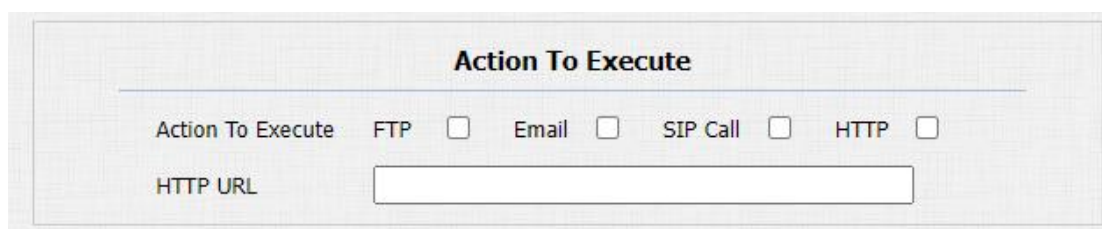
When pressing the push button, the door phone will trigger the preconfigured action type, the notification can be sent out by Email, FTP notification or SIP call. To do this configuration on web **Intercom > Basic** interface.

Parameter Set-up:

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

15.5.2. 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.



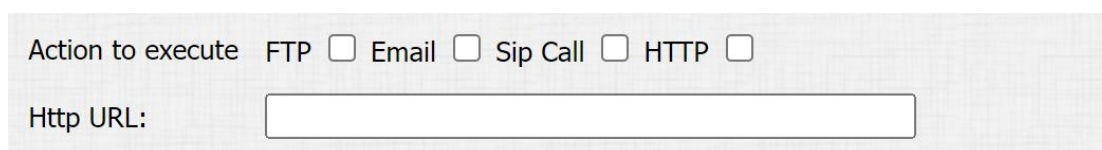
The screenshot shows a web interface titled "Action To Execute". It contains four radio buttons for selecting an action: "FTP", "Email", "SIP Call", and "HTTP". Below these buttons is a text input field labeled "HTTP URL".

Parameter Set-up:

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

15.5.3. Configure Input Action

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



The screenshot shows a web interface titled "Action to execute". It contains four radio buttons for selecting an action: "FTP", "Email", "Sip Call", and "HTTP". Below these buttons is a text input field labeled "Http URL:".

Parameter Set-up:

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

15.6.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

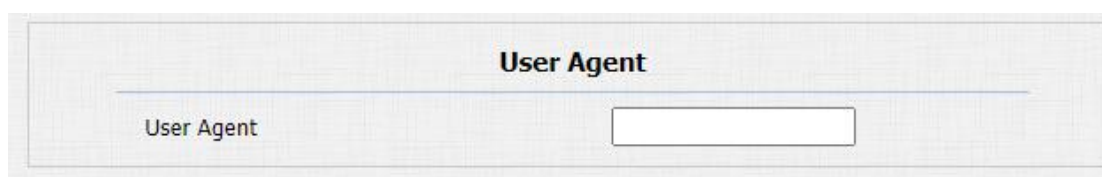
Voice Encryption(SRTP) Disabled ▼

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.

15.7. User Agent

You can customize user agent field in the SIP message. If user agent is set to a 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. Path: **Account > Advanced > User Agent**.



User Agent

User Agent

Parameter Set-up:

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

16. Monitor and Image

16.1. RTSP Stream Monitoring

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

16.1.1. 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	
Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input type="checkbox"/>
Authentication Mode	Basic ▼
User Name	admin
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 Enabled:** 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.

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

Parameter Set-up:

- **Audio Enabled:** tick to enable RTSP audio which means, the door phone can also send audio information to the monitor by 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.
- **Video2 Enabled:** Akuvox door phones support 2 RTSP streams, you can enable the second one.
- **Audio Codec:** choose a suitable audio codec for RTSP audio.

- **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 ▼
2nd Video Resolution	VGA ▼
2nd Video Framerate	30 fps ▼
2nd Video 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: **64 kbps**, **256kbps**, **512 kbps**, **1024 kbps**, **2048 kbps** according to your network environment. The default video bit-rate is **2048 kbps**.
- **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. **30fps** is the video frame rate by default for the second video stream channel.
- **Video2 Bitrate:** select video bitrate among the six options for the second video stream channel. While the second video stream channel is **512 kbps** by default.

16.2.MJPEG Image Capturing

Akuvox door phone 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	
RTSP Basic	
Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input type="checkbox"/>
Authentication Mode	Basic ▼
User Name	admin
Password	*****

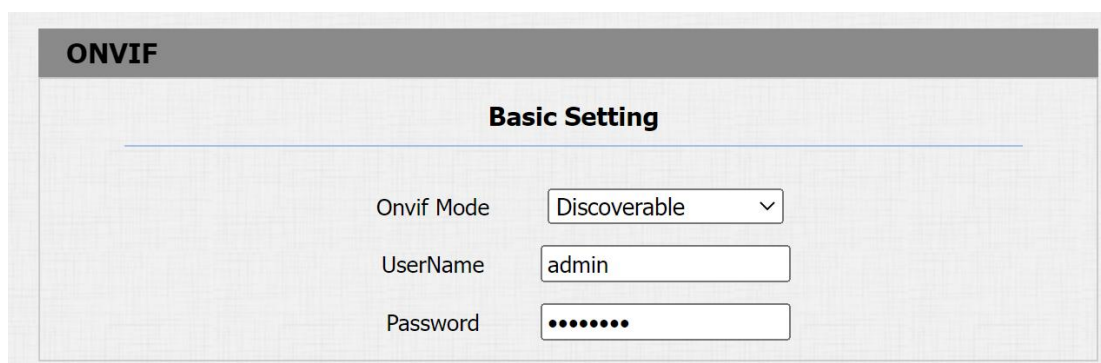
MJPEG Video Parameters	
Video Resolution	VGA ▼
Video Framerate	30 fps ▼
Video Quality	90 ▼

Parameter Set-up:

- **Video Resolution:** select video resolutions among seven options: **CIF, VGA, 4CIF, 720P, and 1080P**. 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.

16.3.ONVIF

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



The screenshot shows the ONVIF configuration page. At the top is a grey header with the text 'ONVIF'. Below it is a section titled 'Basic Setting' with a horizontal line underneath. There are three configuration items: 'Onvif Mode' with a dropdown menu showing 'Discoverable', 'UserName' with a text box containing 'admin', and 'Password' with a text box containing seven dots.

Parameter Set-up:

- **Onvif Mode:** 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.

16.4.Live Stream

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



17. Logs

17.1. 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 **Device > Call Log** interface.

Call Log							
Call History		All ▾					
Index	Type	Date	Time	Local Identity	Name	Number	
1	Dialed	2023-03-14	04:01:50	192.168.2.23 @192.168.2.23	192.168.2.24	192.168.2.24 @192.168.2.24	
2	Dialed	2023-03-14	04:01:40	192.168.2.23 @192.168.2.23	192.168.2.24	192.168.2.24 @192.168.2.24	
3	Dialed	2023-03-14	04:01:29	192.168.2.23 @192.168.2.23	192.168.2.24	192.168.2.24 @192.168.2.24	
4	Dialed	2023-03-14	04:00:49	192.168.2.23 @192.168.2.23	192.168.2.24	192.168.2.24 @192.168.2.24	
5	Dialed	2023-03-14	04:00:17	192.168.2.23 @192.168.2.23	192.168.2.24	192.168.2.24 @192.168.2.24	
6	Received	2023-03-14	03:59:19	192.168.2.23 @192.168.2.23	192.168.2.25	192.168.2.25 @192.168.2.25	

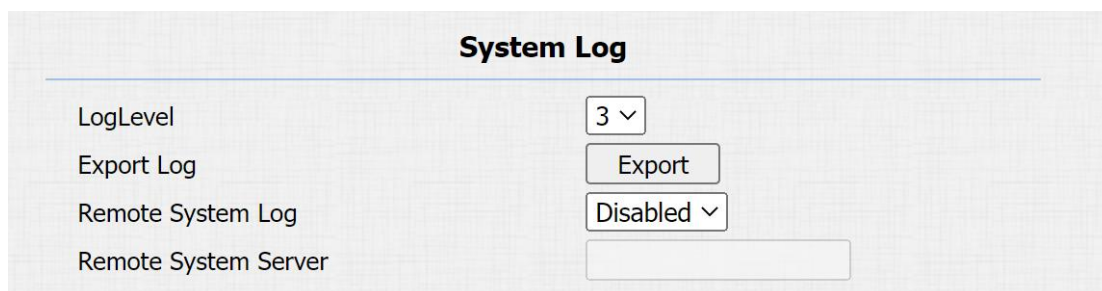
Parameter Set-up:

- **Call History:** select call history among four options: **All**, **Dialed**, **Received**, **Missed** for the specific type of call log to be displayed.

18. Debug

18.1. 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.



The screenshot shows the 'System Log' configuration page. It has a title 'System Log' at the top. Below it, there are four settings: 'LogLevel' with a dropdown menu showing '3', 'Export Log' with an 'Export' button, 'Remote System Log' with a dropdown menu showing 'Disabled', and 'Remote System Server' with an empty text input field.

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

18.2.PCAP

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

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 a certain range of data packets before clicking **Export** tab to export the data packets to your 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 packets even after the data packets reached their 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.

18.3.Remote Debug

The function allows you to debug remotely, you can access the backend files of device and log remotely. **Path: Intercom > Advanced.**

Remote Debug Server

Service	<input type="text" value="Enabled"/>
Connect Status	DisConnected
IP	<input type="text"/>
Port	<input type="text"/> (1024~65535)

Parameter Set-up:

- **IP:** the IP address of remote service.
- **Port:** the port of remote service, from 1024 to 65535.

19. Firmware Upgrade

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

Upgrade-Basic


Firmware Version	321.30.1.101
Hardware Version	321.0
Upgrade	<div>Choose File No file chosen</div> <div>Submit Cancel</div>
Reset To Factory Setting	<div>Submit</div>
Reboot	<div>Submit</div>

**Note:**

- Do not disconnect the device from internet and power supply when the firmware upgrade is in progress, otherwise, it might cause upgrade failure or system breakdown.

20. 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.



Others

Config File(.tgz/.conf/.cfg)

Choose File No file chosen

Export (Encrypted)

Import Cancel

Parameter Set-up:

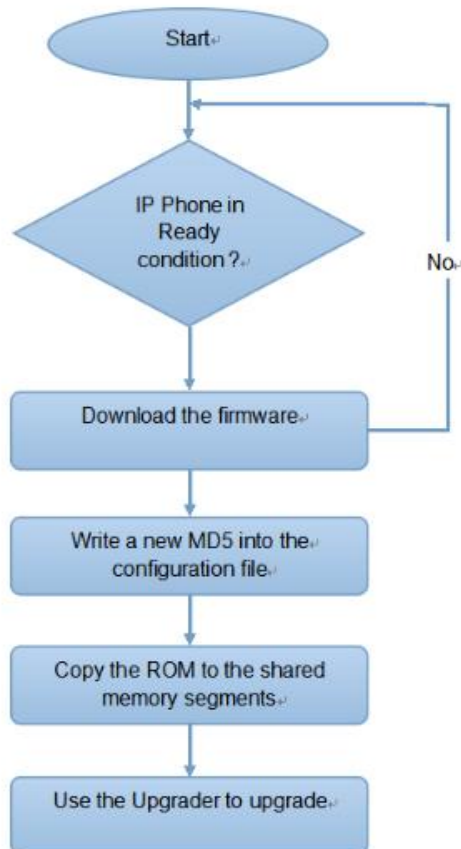
- **Export Config File:** to export current config file.
- **Export/Import:** to export current config file (Encrypted) or import new config file.

21. 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.

21.1.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 update the firmware and the corresponding parameters on the door phone.



21.2. Configuration Files for Auto-provisioning

Configuration files have two formats for the auto-provisioning. One is general configuration files used for general provisioning and other one is 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 : r0000000000020.cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files are 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	<div style="border: 1px solid #ccc; padding: 2px 5px;">Power On</div> ▼	
Schedule	<div style="border: 1px solid #ccc; padding: 2px 5px;">Sunday</div> ▼	
	<div style="border: 1px solid #ccc; padding: 2px 5px; width: 60px;">22</div>	Hour(0~23)
	<div style="border: 1px solid #ccc; padding: 2px 5px; width: 60px;">0</div>	Min(0~59)
Clear MD5	<div style="border: 1px solid #ccc; padding: 2px 10px;">Submit</div>	
Export Autop Template	<div style="border: 1px solid #ccc; padding: 2px 10px;">Export</div>	


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.

21.3.AutoP Schedule

Akuvox provides you with different Autop methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule. Path:**Upgrade > Advanced > Automatic Autop** interface.

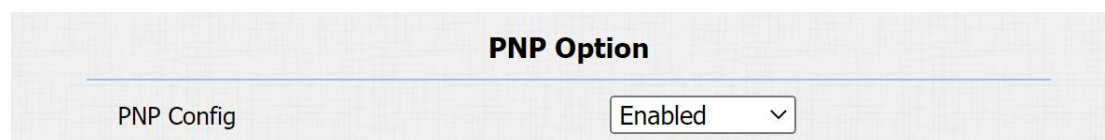
Automatic Autop	
Mode	Power On <input type="button" value="v"/>
Schedule	Sunday <input type="button" value="v"/>
	<div>22 <input type="button" value="v"/> Hour(0~23)</div> <div>0 <input type="button" value="v"/> Min(0~59)</div>

Parameter Set-up:

- **Mode:** 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.
- **Schedule:** if **Repeatedly** is selected, you can set up the time schedule for the AutoP.

21.4.PNP Configuration

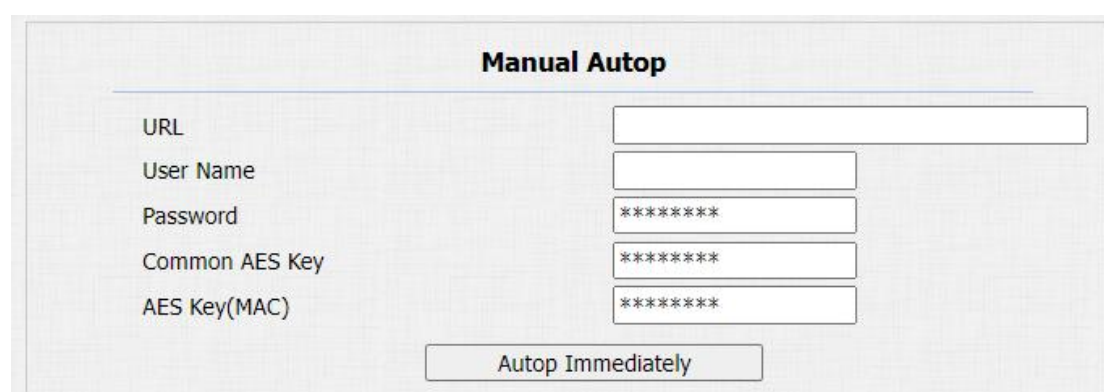
Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. To do this configuration on web **Upgrade > Advanced > PNP Option** interface.



The image shows a web interface titled "PNP Option". Below the title, there is a label "PNP Config" and a dropdown menu currently set to "Enabled".

21.5.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 at a specific time 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.



The image shows a web interface titled "Manual Autop". It contains several input fields for configuration: "URL", "User Name", "Password", "Common AES Key", and "AES Key(MAC)". Each field has a corresponding input box, with the last three having masked text (asterisks). Below these fields is a button labeled "Autop Immediately".

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 a user name to be accessed otherwise leave it blank.
- **Password:** set up a password if the server needs a password to be accessed otherwise leave it blank.
- **Common AES Key:** set up AES code for the intercom to decipher the 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)

**Note:**

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

22. Integration with Third Party Device

22.1. 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.

HTTP API	
HTTP API	Enabled
Auth Mode	Digest
User Name	admin
Password	*****
IP01	
IP02	
IP03	
IP04	
IP05	

Parameter Set-up:

- **HTTP API:** enable or disable the HPTT 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.
- **Authorization Mode:** select among four options: **None**, **WhiteList Basic**, **Digest**, and **Token** 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.

- **IP 01-05:** enter the IP address of the third party devices when the "WhiteList" authorization is selected for the integration.

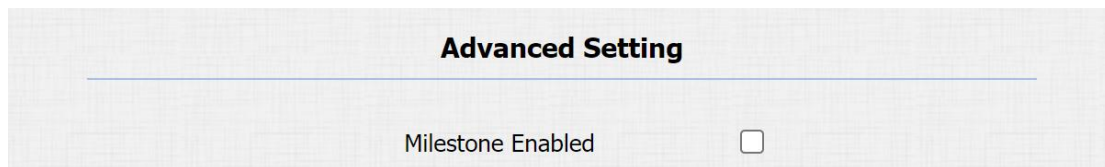
Please refer to the following description for the Authentication mode:

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 developers 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 developers only.

22.2.Integration with Milestone

The door phone allows you to see its video stream on the Milestone software.

Path: Intercom > ONVIF > Advanced Setting.



Note:

- Please read the details and configuration of the integration in <https://knowledge.akuvox.com/docs/integration-with-milestone-v1-202008019>

23. Password Modification

23.1. 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.

Security-Basic

Web Password Modify

User Name

admin ▾

Change Password

Account Status

Admin

Enabled ▾

User

Disabled ▾

Change Password

The password must be at least eight characters long containing one uppercase letter, one lowercase letter and one digit at least

User Name

user

Old Password

New Password

Confirm Password

Ignore

Change

24. System Reboot&Reset

24.1.Reboot

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

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

24.1.1. Reboot Schedule

Set to reboot device at a specific time. **Path: Upgrade > Advanced > RebootSchedule.**

RebootSchedule	
Mode	Disabled ▾
Schedule	Every Day ▾
	0 Hour(0~23)

24.2.Reset

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

Reset To Factory Setting	Reset
--------------------------	-------

25. 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

26. FAQ

Q1: How to obtain IP address of R2X

A1: ✓ For devices with a single button - E21/ R20/ R23/ R26:

While E21/ R20/ R23/ R26 power up normally, hold the call button for 5 seconds after the statue LED turns blue and it will enter into IP announcement mode. In announcement mode, the IP address will be announced repeatedly. Press call button again to quit the announcement mode.

✓ For devices with multiple numeric keyboard - R27:

While R27 power up normally, press "*2396#" to enter home screen and press "1" to go to system Information screen to check the IP address.

✓ For devices with touch screen - X915/R29:

While it power up normally, in the dial interface, press "9999", "Dial key", "3888" and "OK" to enter the system setting screen. Go to info screen to check the IP address.

✓ Common method:

Using Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: Do Akuvox devices support opus codec?

A2: For now, only Akuvox Android video IP phone R48G can support Opus audio codec.

Q3: What is the supported temperature range for akuvox doorphone?

A3: R20/E21/R26/R23/Standard R27/Standard X915 -- 14° to 112°F (-10° to 45°C)

R27/X915 with heating supporting --- 40 degrees

R28 -- (-40°C~55°C)

Indoorphone -- 14° to 112°F (-10° to 45°C)

IPPhone -- 32°~104°F(0~40°C)

Q4: Do Akuvox devices support Modbus protocol?

A4: No.

Q5: Failure in importing the X915 face data to another X915 using the exported face data.

A5: Please confirm the following steps:

The import format is zip;

1. After you export, you need to unzip the .tgz folder, then make the unzipped folder into .zip again.

Q6: Which version of ONVIF do R20 and X915 support?

A6: Onvif 18.04 profiles

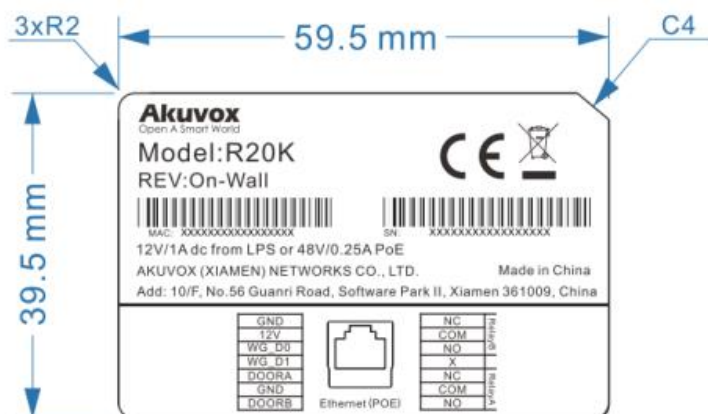
Q7: Do door phones support these card types? Prox, Legacy iClass, iClassSE, HID Mifare, HID DESFire, HID SEOS

A7: Sorry, they are not supported. They need to be implemented via hardware modifications.

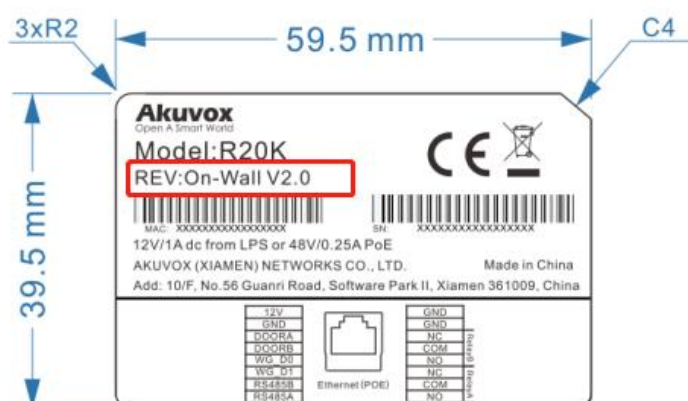
Q8: How to confirm whether my device is hardware version 1 or hardware version 2?

A8: 1.Label

- **Hardware version 1**



- **Hardware version 2**



- **Firmware Version**

The firmware is different between hardware version1 and hardware version 2.

Go to **Web> Status > Firmware Version**.

20.X.X.X is hardware version 1.

220.X.X.X is hardware version 2.

- **Hardware version**

The firmware is different between hardware version1 and hardware version 2.

Go to Web-Status -Firmware Version.

If the hardware version is 220.x, then the device is hardware version 2.

Status	
Product Information	
Model	E21V
MAC Address	5E05697F6F63
Firmware Version	321.30.1.101
Hardware Version	321.0

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.

